

Ticketnummer	Bijbehorende tickets	Weigeringsgrond (codering)	Datum	Type incident	Omschrijving	Sector
3981			2-mei-13	Instabiele website	Overheidswebsite instabiel, bleek door DDoS te komen.	Rijksoverheid
3985	3984, 3986,		2-mei-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector.	Financieel
3988	3987, 3989, 3990,		4-mei-13	Aanvallen op energiecentrales gemeld	Buitenlandse energiecentrales waren slachtoffer van een digitale aanval. Deze informatie bleek niet langer relevant.	Energie
3991			6-mei-13	Website defacement	Melding website defacement.	Overige
3993	3992, 3994,		6-mei-13	DNS amplification attack	Melding gekregen van DDoS op buitenlands IP.	Telecom/ICT
3998	3997, 3999,		7-mei-13	Phishing	Melding van phishing-mails uit name van rijksoverheidpartijen.	Rijksoverheid
4001	4000, 4002,		7-mei-13	DDoS-aanval	Berichtgeving over DDoS aanvallen tegen buitenlandse partijen in de financiële sector.	Financieel
4004	4003, 4005,		7-mei-13	DNS amplification aanval	Melding gekregen van DDoS op buitenlands IP.	Telecom/ICT
4006	3995, 3996, 4007, 4016, 4028,		7-mei-13	Mogelijke compromittatie van server	Melding mogelijke compromittatie server organisatie.	Rijksoverheid
4009	4008, 4010,		7-mei-13	Mogelijke DDoS	Melding mogelijke DDoS-aanval op organisatie. Oorzaak bleek misconfiguratie bij klant van organisatie.	Rijksoverheid
4012	4011, 4013, 4014, 4015, 4021,		8-mei-13	DDoS-aanval	Melding DDoS op overheidswebsite.	Rijksoverheid
4018	4017, 4019, 4020,		8-mei-13	Phishing aanval	Verzoek tot assistentie voor het doen van een NTD.	Telecom/ICT
4023	4022, 4024,		10-mei-13	DDoS-aanval	DDoS-aanval op website overheidspartij.	Rijksoverheid
4025	4026, 4027,		12-mei-13	Mogelijke DDoS-aanval	Melding van actiegroep op social media dat website overheidspartij down zou zijn door DDoS. Nader onderzoek gaf geen indicatie voor DDoS.	Rijksoverheid
4031	4030, 4032, 4033,		13-mei-13	Trojan	Verzoek tot assistentie voor het doen van een NTD.	Telecom/ICT
4034	4029, 4035, 4036,		13-mei-13	Melding Linux/CDorked infections	Melding gecompromitteerde systemen	Telecom/ICT
4039	4038, 4040, 4052, 4056, 4069, 4070,		14-mei-13	Phishing website verzoek NTD	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4042	4041, 4043,		16-mei-13	Melding van openstaande wifi-netwerken	Responsible Disclosure melding dat een wifi-netwerk niet goed was beveiligd bij een partij in de gezondheidssector.	Gezondheidszorg
4044	4045, 4048, 4075, 4076, 4077,		16-mei-13	Kwetsbaarheden in webshop	Webshopsoftware gebruikt door verschillende overheidspartijen bleek onveilig te zijn na pentest.	Rijksoverheid
4047			16-mei-13	IP's van SCADA-systemen online gezet	Bericht met IP's van SCADA systemen welke publiek toegankelijk waren	Meerdere
4050	4049, 4051, 4054,		17-mei-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4053			22-mei-13	Actieve C&C Server	Melding van een actieve Command&Control server bij Nederlandse hoster.	Telecom/ICT
4055			27-mei-13	Melding van DDoS	Melding gekregen van DDoS-aanval op buitenlands IP.	Telecom/ICT
4058	4057, 4059,		29-mei-13	Indicatoren van misbruik	Indicatoren over mogelijke digitale spionage	Rijksoverheid
4061	4060, 4062,		30-mei-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4064	4063, 4065,		30-mei-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT

4066	4067		30-mei-13	Kwetsbaarheden in systemen	Melding van kwetsbare SCADA systemen welke publiek toegankelijk zijn.	Meerdere
4068			31-mei-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4071			31-mei-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4072			31-mei-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4073			31-mei-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4074			31-mei-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4081	4079, 4082, 4083,		4-jun-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4085	4084, 4086, 4087,		4-jun-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4089	4088, 4090,		4-jun-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4092	4091, 4093, 4094,		5-jun-13	Gerichte aanval	Gerichte aanval tegen overheidspartij.	Rijksoverheid
4096	4095, 4097,		6-jun-13	Melding reverse proxy probleem	Melding van een publiek toegankelijke reverse proxy bij een overheidspartij.	Rijksoverheid
4099	4098, 4100, 4101, 4102,		6-jun-13	Command&Control servers	Command&Control servers aangetroffen.	Meerdere
4105	4103, 4106,		7-jun-13	Mogelijk botnetverkeer	Melding van mogelijk botnetverkeer in het netwerk van een bank.	Financieel
4107	4104, 4108,		7-jun-13	Melding DDoS-aanval	Melding van Ddos-aanval op een overheidsinstelling.	Rijksoverheid
4110			13-jun-13	Kwaadwillende website	NTD verzoek voor phishing-site gericht tegen een overheidspartij	Rijksoverheid
4111			13-jun-13	Mogelijke downadup infectie	Melding van een mogelijke infectie in een netwerk van een organisatie in de gezondheidszorg.	Gezondheidszorg
4113	4112, 4114,		13-jun-13	Ddos-aanval	Melding over een DDoS-aanval op buitenlandse partij waarbij Nederlandse IP's zijn gebruikt.	Telecom/ICT
4116	4115, 4117,		13-jun-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4118			14-jun-13	Mogelijke dreiging vanuit een actiegroep.	Melding van mogelijke dreiging vanuit een actiegroep.	Rijksoverheid
4122			19-jun-13	Downadup hits	Downadup infectie in Nederlandse systemen	Telecom/ICT
4123			21-jun-13	Melding van mogelijke spionage	Melding van overheidspartij die vermoedt slachtoffer te zijn van spionage.	Rijksoverheid
4124	4125, 4126, 4131,		24-jun-13	Phishingmail	Melding mogelijke phishing mail uit naam van overheidspartij. Blijkt niet zo te zijn.	Rijksoverheid
4129	4128, 4130,		24-jun-13	Mogelijke DDoS-aanval	Melding mogelijke DDoS-aanval op partij in financiële sector. Bleek een storing te zijn.	Financieel
4133	4132, 4134,		26-jun-13	Slachtoffers Buget Botnet	Buitgemaakte informatie in Buget botnet betreffende Nederlandse partijen.	Meerdere
4136	4135, 4137, 4141,		27-jun-13	Phishingsite	NTD verzoek voor phishingsite gericht tegen organisatie in financiële sector	Financieel
4139	4138, 4140,		27-jun-13	Phishingsite	Verzoek tot assistentie voor het verrichten van een NTD	Telecom/ICT

4143	4142, 4144,		29-jun-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4147	4146, 4148,		1-jul-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4151			3-jul-13	Confickerinfectie	Malwareinfectie in netwerk sector Telecom en ICT.	Telecom/ICT
4152			3-jul-13	Massadefacement	Een server werd gebruikt voor massadefacement	Telecom/ICT
4154			5-jul-13	Phishingactiviteit	NTD verzoek voor phishingsite gericht tegen organisatie in financiële sector	Financieel
4155			5-jul-13	Phishingactiviteit	NTD verzoek voor phishingsite gericht tegen organisatie in financiële sector.	Financieel
4156	4150, 4157,		8-jul-13	Actieve Command&Control server	Melding actieve Command&Control server bij Nederlandse hoster.	Telecom/ICT
4158	4153, 4159,		8-jul-13	BGP hijack	BGP hijack van IP-space.	Overige
4160			8-jul-13	Phishingactiviteit	NTD verzoek voor phishingsite gericht tegen organisatie in financiële sector.	Financieel
4162	4161, 4164,		8-jul-13	Overlast door Externe scan	Website overheidspartij ondervond veel overlast van een onbekend persoon die een geautomatiseerde tool gebruikte om kwetsbaarheden te vinden.	Rijksoverheid
4163	4119		9-jul-13	DDoS-aanval	Melding onderwijsinstelling dat zij slachtoffer waren van DDoS-aanvallen.	Onderwijs
4166			10-jul-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector.	Financieel
4168	4167, 4169,		10-jul-13	Kwaadwillende site	Buitgemaakte gebruikersgegevens aangetroffen op website.	Telecom/ICT
4170	4165, 4171,		10-jul-13	Gecompromiteerde webserver	Compromitatie webserver van organisatie. Klantgegevens waren buitgemaakt.	Telecom/ICT
4172	4171, 4173, 4178,		10-jul-13	Gecompromiteerde webserver	Compromitatie webserver van organisatie. Klantgegevens waren buitgemaakt.	Telecom/ICT
4176	4175, 4177,		11-jul-13	Kwaadaardige Javascript in netwerk	Melding buitenlandse partij over malafide bestanden op Nederlandse server.	Telecom/ICT
4180	4179, 4181,		11-jul-13	Phishingaanval	Verzoek tot assistentie voor het verrichten van een NTD	Telecom/ICT
4182			12-jul-13	Mogelijk testsystemen publiek beschikbaar	Testsystemen overheidspartij publiekelijk beschikbaar.	Rijksoverheid
4184	4183, 4185, 4186, 4187, 4189,		14-jul-13	Meerdere B58-DGA2 infecties	Automatisch detectiesysteem; malwarebesmetting bij meerdere organisaties.	Meerdere
4190	4188		15-jul-13	Mogelijke virusbesmetting	Mogelijke infectie op systeem van organisatie binnen de gezondheidszorg.	Gezondheidszorg
4191			15-jul-13	Phishingsite	NTD verzoek voor phishingsite gericht tegen organisatie in financiële sector.	Financieel
4192			15-jul-13	Phishingactiviteit	Verzoek tot assistentie voor het verrichten van een NTD.	Telecom/ICT
4194	4193, 4195, 4196,		16-jul-13	Geïnfecteerde hosts	Ebury infecties in Nederlandse systemen.	Telecom/ICT
4198	4197, 4199, 4200, 4201,		18-jul-13	Beveiligingslek in bepaalde insulinepompen niet gepatcht.	Kwetsbaarheid in insulinepompen ontdekt.	Gezondheidszorg
4204			20-jul-13	Defacement site	Melding van defacement site van buitenlandse ambassade in Nederland.	Overige

4206	4205, 4207, 4208, 4209, 4210, 4227, 4237, 4303, 4304, 4307,		22-jul-13	Simkaartkwetsbaarheid	Kwetsbaarheid in bepaalde simkaarten	Telecom/ICT
4211			23-jul-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4212			23-jul-13	Kwaadwillende activiteit	NTD verzoek voor phishing-site gericht tegen Nederlands bedrijf	Overige
4213			23-jul-13	Kwaadwillende activiteit	NTD verzoek voor phishing-site gericht tegen Nederlands bedrijf	Overige
4214			23-jul-13	Kwetsbaarheid	Kwetsbaarheid in besturingssysteem.	Telecom/ICT
4216	4215, 4217,		23-jul-13	Veiligheidsincident	Melding van mogelijke malwaresites in het buitenland	Financieel
4219	4218, 4220, 4221, 4222,		23-jul-13	MMS malware	Malware verstuurd via e-mail uit naam van Nederlandse organisatie.	Telecom/ICT
4224	4223, 4225,		24-jul-13	Verzoek ondersteuning bij NTD	Verzoek tot assistentie voor het verrichten van een NTD	Telecom/ICT
4230	4229, 4231,		25-jul-13	Gecompromiteerde IP-adressen	Gecompromiteerde IP-adressen door Citadel-botnet.	Meerdere
4232			25-jul-13	Malware infectie	Gecompromiteerde systemen door Citadel malware.	Rijksoverheid
4233			25-jul-13	Phishingactiviteit	Phishing e-mail die actief gericht was op overheidspersoneel.	Rijksoverheid
4235	4234, 4236,		25-jul-13	Cookie zonder HttpOnly vlag	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4241	4239, 4244,		29-jul-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4242	4240, 4243,		29-jul-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4247	4245, 4248, 4249,		29-jul-13	Logindata gevonden	Melding over gevonden logindata van klanten van bedrijf in financiële sector.	Meerdere
4250			29-jul-13	keylog data	Melding over gevonden logindata van klanten van bedrijf in financiële sector.	Financieel
4251	4246, 4252,		29-jul-13	Melding over toegang tot systemen	Melding van ethische hacker over het toegang kunnen verkrijgen tot interne systemen van Nederlandse ISP.	Telecom/ICT
4254	4253, 4255,		29-jul-13	Mogelijke zero-day	Mogelijke nieuwe kwetsbaarheid tegengekomen.	Telecom/ICT
4257	4256, 4258,		29-jul-13	DDoS-aanval	Melding over een DDoS op buitenlandse partij waarbij Nederlandse IP's zijn gebruikt.	Telecom/ICT
4260	4259		29-jul-13	DDoS-aanval	Melding dat een Nederlandse gemeente was getroffen door een DDoS-aanval.	Gemeenten
4262	4261, 4263,		30-jul-13	Phishing informatie	Verzoek tot assistentie voor het verrichten van een NTD	Telecom/ICT
4267	4265, 4274, 4276,		31-jul-13	DDoS-aanval	Melding DDoS-aanvallen op meerdere gemeentesites	Gemeenten
4269	4268, 4270,		31-jul-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4272	4271, 4273,		31-jul-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4278			1-aug-13	Zeus p2p	Melding over een Zeus control panel. Was al weer offline tegen de tijd dat de melding was ontvangen.	Telecom/ICT

4279	4266, 4275, 4280,		1-aug-13	Lijst met targets van actiegroep	Verschillende Nederlandse overheidspartijen en particuliere bedrijven genoemd als doelwit van een actiegroep	Rijksoverheid
4281	4277, 4282,		1-aug-13	Verspreiding van ransomware	Actieve drive-by-downloadinfectie op website van medium.	Meerdere
4284	4283, 4285, 4286, 4288,		2-aug-13	DDoS-aanval	Website overheidspartij slachtoffer van DDoS-aanval.	Rijksoverheid
4289	4238, 4290,		2-aug-13	BGP-Configuratiefout	Hulpverzoek vanuit buitenlandse overheid om te assisteren bij BGP-configuratiefout waardoor buitenlandse overheidspartij last ondervond.	Telecom/ICT
4291			5-aug-13	Malware verspreid na mogelijke hack op DNS	Hack op DNS-server had tot gevolg dat bezoekers van legitieme websites werden herleid naar een malafide server waar malware werd verspreid.	Rijksoverheid
4293	4292, 4294,		6-aug-13	Lijst met mogelijke doelwitten	Lijst met mogelijke doelwitten van actiegroep tegen financiële sector.	Financieel
4295			6-aug-13	Melding DDoS-aanval	Melding DDoS-aanval organisatie.	Telecom/ICT
4297	4296		6-aug-13	veiligheidsprobleem: inloggegevens t.b.v. upload CIOT gegevens publiekelijk openbaar	Melding van publiek toegankelijke logingegevens.	Meerdere
4299	4298		8-aug-13	XSS kwetsbaarheid	XSS kwetsbaarheid in bepaalde simkaarten.	Rijksoverheid
4301	4300, 4302,		8-aug-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4305	4264, 4306,		8-aug-13	Hulpverzoek	Verzoek tot assistentie voor het verrichten van een NTD.	Telecom/ICT
4309	4308, 4310,		8-aug-13	Phishing	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4312	4311, 4313,		9-aug-13	Gecompromitteerde website	Website partij in Nederland mogelijk gebruikt in APT-aanval.	Overige
4316	4315, 4317,		12-aug-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4318	4319, 4320,		12-aug-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4322	4321, 4323,		14-aug-13	Zero-day exploit	Mogelijke nieuwe kwetsbaarheid in specifieke anti-virussoftware gemeld.	Telecom/ICT
4325	4324, 4326,		14-aug-13	Logingegevens gevonden	Credentials gevonden van overheidsinstelling	Rijksoverheid
4328			15-aug-13	Massa defacements	Een server werd gebruikt voor massadefacement	Telecom/ICT
4330			16-aug-13	Incidentmelding acunetix scan	Melding van organisatie dat er een product tegen hun site is gebruikt om op kwetsbaarheden te scannen.	Rijksoverheid
4331	4329, 4332, 4333, 4334, 4335, 4337, 4338, 4340, 4341, 4389, 4738,		16-aug-13	Melding DDoS-aanval	Melding van DDoS-aanval op overheidspartij.	Rijksoverheid
4336			19-aug-13	Melding mogelijke blacklisting	Melding van overheidspartij dat deze problemen had met het bereiken van bepaalde sites vanuit het interne netwerk; mogelijk door blacklisting.	Rijksoverheid
4339			20-aug-13	Melding DDoS-aanval	Melding DDoS-aanval op private partij.	Websites
4342			21-aug-13	Mail-blacklist	Melding gemeente die op een mail-blacklist is gezet.	Gemeenten
4344	4343, 4345,		22-aug-13	Gerichte aanval	Gerichte aanval tegen overheidspartij	Rijksoverheid
4346			26-aug-13	Beveiligingsrisico applicatie-platform combinatie	Melding dat een applicatie-platform dat gebruikt werd door de overheid een beveiligingsrisico bevatte.	Rijksoverheid
4347			27-aug-13	Uitval	Mogelijke dreiging tegen Nederlandse financiële sector.	Meerdere

4351			28-aug-13	Verzoek om informatie	Vraag vanuit financiële sector of het NCSC meer informatie had omtrent een gerucht dat meerdere bedrijven in de financiële sector gecompromiteerd zouden zijn.	Financieel
4352	4349, 4350, 4372,		28-aug-13	Oproep van actiegroep	Oproep vanuit actiegroep om rondom Prinsjesdag overheidsites te hacken.	Rijksoverheid
4356			30-aug-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector.	Financieel
4357			30-aug-13	Mogelijke kwetsbaarheden	Onderzoeker meldt op dat hij allerlei kwetsbaarheden heeft gevonden. Hij heeft bericht dat hij deze data met NCSC kan delen.	Overige
4361	4360, 4362, 4371,		2-sep-13	Lekken van persoonsgegevens	Melding dat een website van een bedrijf in de transportsector informatie van gebruikers lekte.	Transport
4363			2-sep-13	Melding DDoS-aanval	Melding van DDoS-aanval op onderwijsinstelling.	Onderwijs
4366			2-sep-13	Phishingactiviteit	Verzoek tot assistentie voor het verrichten van een NTD.	Overige
4367	4364, 4365, 4368, 4370,		3-sep-13	Mogelijke gerichte aanval via e-mail	Organisatie in de chemisch en nucleaire sector heeft via e-mail kwaadaardige scripts ontvangen. Geen indicaties voor gerichte aanval.	Chemisch en Nucleair
4376	4375, 4377,		10-sep-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4379	4374, 4380,		11-sep-13	Crisisnummer overheidspartij onbereikbaar	Crisisnummer overheidspartij onbereikbaar.	Rijksoverheid
4382	4381, 4383,		11-sep-13	DDoS-aanval op IT dienstverlener scholengemeenschap	Melding van IT dienstverlener scholengemeenschap dat zij slachtoffer waren van een DDoS-aanval.	Onderwijs
4384			12-sep-13	DDoS-bot	NCSC werd gewezen op de broncode van een DDoS-bot. Geen indicatie van actief misbruik.	Overige
4387	4386, 4388, 4422,		12-sep-13	Melding van kwetsbaarheid	Ethische hacker meldde kwetsbaarheid in website IT-dienstverlener. Dienstverlener meldde dat de kwetsbaarheid is verholpen, maar dat de hacker niet ethisch te werk is gegaan.	Telecom/ICT
4393			13-sep-13	Malware melding	Melding van sites in Nederland die malware serveren.	Telecom/ICT
4394	4390, 4395, 4396, 4397,		13-sep-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4399	4398, 4400,		13-sep-13	Phishing site	Verzoek tot assistentie voor het verrichten van een NTD	Financieel
4402	4401, 4403, 4412, 4416, 4429,		13-sep-13	Mogelijke kwetsbaarheid in mailserver	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de mailserver van een overheidspartij.	Rijksoverheid
4405	4404, 4406, 4417,		14-sep-13	Melding van mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4408	4407, 4409,		14-sep-13	Melding van mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4410	4391, 4411,		16-sep-13	Multinational gedefaced	CMS systeem multinational gecompromiteerd.	Multinational
4414	4413, 4415, 4418,		16-sep-13	Hack bij buitenlandse ISP	Compromitatie netwerk buitenlandse ISP.	Telecom/ICT
4420	4419		17-sep-13	Malware	Melding van ransomware welke verspreid werd via spammails.	Overige
4423	4421		18-sep-13	Openstaande poorten	Responsible Disclosure melding over een mogelijke kwetsbaarheid op de server van een overheidspartij.	Rijksoverheid

4425	4424, 4426, 4427,		18-sep-13	Mogelijke kwetsbaarheden	Vraag van ethische hacker over hoe en waar hij precies melding kan doen van gevonden kwetsbaarheden.	Overige
4431	4430, 4432,		18-sep-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4434			19-sep-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4435			19-sep-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4436	4433, 4442, 4460, 4461, 4462, 4465, 4466,		19-sep-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4438			19-sep-13	Assistentieverzoek	Verzoek tot assistentie voor het verrichten van een NTD-verzoek.	Telecom/ICT
4448			20-sep-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4449			20-sep-13	Mogelijke phishing melding	Vraag gekregen van partner CERT-team over een mogelijke Responsible Disclosure melding	Rijksoverheid
4451	4450, 4452, 4455, 4565, 4566, 4571,		22-sep-13	SQL injectie en XSS melding	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4453			23-sep-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4456	4454		23-sep-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Telecom/ICT
4457	4441, 4444, 4446,		23-sep-13	Melding bulk e-mail	Melding van provincie dat er veel e-mail met hierin malware binnen kwam welke afkomstig leek te zijn van een internationaal transportbedrijf	Provincies
4467			27-sep-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij	Rijksoverheid
4468			28-sep-13	Phishingactiviteit	Verzoek tot assistentie voor het verrichten van een NTD-verzoek.	Financieel
4470	4471, 4501,		28-sep-13	Melding actief misbruikt lek in webbrowser	Melding nieuwe kwetsbaarheid in webbrowser.	Telecom/ICT
4472			29-sep-13	Melding op website	Melding van site defacement.	Onderwijs
4473	4469		30-sep-13	Phishingactiviteit	Verzoek tot assistentie voor het verrichten van een NTD-verzoek.	Financieel
4475	4474, 4476,		30-sep-13	XSS-kwetsbaarheden	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4477			30-sep-13	XSS-gevoeligheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4478			30-sep-13	Actieve Zeus C&C	Melding van actieve Zeus Command&Control	Telecom/ICT
4487	4481, 4488,		1-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gemeenten
4489	4482, 4490,		1-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gemeenten
4491	4483, 4492,		1-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gemeenten
4493	4479		1-okt-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4494	4485, 4495,		1-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Rijksoverheid

4496	4484, 4497,		1-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Chemisch en Nucleair
4498	4486, 4499,		1-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Industrie
4505			2-okt-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4507	4506, 4508, 4509, 4510, 4511,		2-okt-13	Signed FakeAV malware met C&C in Nederland	Melding van malware welke door een geldig certificaat is ondertekend, en gebruik maakt van infrastructuur bij een Nederlandse hoster.	Telecom/ICT
4514			3-okt-13	Mogelijke botnet-host	Mogelijke botnet-host op netwerk.	Telecom/ICT
4517	4516, 4518, 4519,		3-okt-13	Melding DDoS-aanval	Melding van buitenlands CERT-team over een DDoS-aanval op buitenlandse partij waarbij Nederlandse IP's zijn gebruikt.	Telecom/ICT
4520			3-okt-13	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek aan een Nederlandse hoster.	Financieel
4523	4502, 4524,		4-okt-13	Watering hole aanval	Melding van mogelijke APT-aanval	Meerdere
4525			4-okt-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4527	4515, 4526,		4-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4531			5-okt-13	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek aan een Nederlandse hoster.	Financieel
4532			7-okt-13	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek aan een Nederlandse hoster.	Financieel
4533	4354, 4359, 4437, 4439, 4440, 4503,		7-okt-13	Melding mogelijk XSS-kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4534	4445, 4459, 4463, 4464,		7-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4535			7-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4536			7-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4537			7-okt-13	Lek in videoplayer	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4538			7-okt-13	Malware activiteit	NTD verzoeken in verband met malware bij hosts.	Meerdere
4540			8-okt-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4541			8-okt-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4542	4539, 4543, 4544,		8-okt-13	XSS in websites	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4545	4501, 4504, 4512, 4513, 4521, 4528, 4529, 4530,		8-okt-13	Issue zero day	Melding nieuwe kwetsbaarheid in webbrowser.	Telecom/ICT
4550	4549, 4551, 4552, 4553,		11-okt-13	Mogelijke phishingwebsite	Melding van partij in financiële sector over mogelijke phishing site.	Financieel
4556	4555		11-okt-13	Ponmocup botnet melding	Gecompromitteerde systemen in netwerken gezondheidszorg.	Gezondheidszorg
4557	4554, 4581,		11-okt-13	Kwetsbaarheid in SSL	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid

4559	4558, 4560, 4561,		12-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Meerdere
4563	4562, 4564, 4801,		14-okt-13	Hack: broncode en klantgegevens buitgemaakt	Bij een hack bij een softwareontwikkelaar waren broncode en klantgegevens buitgemaakt.	Meerdere
4569	4458, 4570,		15-okt-13	Mogelijke SQL-injection op website	Melding van mogelijke kwetsbaarheid in websites	Onderwijs
4573	4572, 4574,		15-okt-13	Gecompromitteerde logingegevens	Melding over mogelijk gecompromitteerde logingegevens.	Telecom/ICT
4575	4385, 4576,		15-okt-13	Open DNS resolver achter IP	DNS resolver binnen netwerk was niet correct geconfigureerd waardoor deze misbruikt kon worden in DDoS-aanvallen.	Rijksoverheid
4577	4546, 4547, 4748,		15-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4579	4578, 4580,		15-okt-13	Gecompromitteerde hosts gebruikt in DDoS-aanvallen	Melding over gecompromitteerde systemen in netwerk welke misbruikt werden voor DDoS-aanvallen.	Telecom/ICT
4583	4582, 4584,		16-okt-13	Phishing-site	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4585			16-okt-13	Ongewone inhoud e-mail	Melding over ongewone inhoud in e-mail van overheidswebsite welke op een ongebruikelijk tijdstip was verstuurd.	Rijksoverheid
4586			16-okt-13	Zeus Botnet	Vraag van buitenlandse partner of het NCSC kon assisteren bij het nemen van acties tegen een server binnen het Zeus botnet.	Telecom/ICT
4587			17-okt-13	Actieve C&C server	Melding van een actieve Command&Control server.	Rijksoverheid
4589	4588		17-okt-13	SSL Cookie	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4591	4590, 4592,		17-okt-13	Spontaan rebooten van systemen	Vraag van organisatie of het NCSC wellicht wist waarom sommige van de systemen van de organisatie spontaan rebooten.	Rijksoverheid
4593	4567, 4568,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4595	4594, 4596,		18-okt-13	Misbruikte server	Melding van buitenlands CERT-team over een server in Nederland die misbruikt werd om andere systemen te compromitteren.	Telecom/ICT
4598	4597, 4599,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4601	4600, 4602,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4604	4603, 4605,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4608	4607, 4609,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4612	4611, 4613,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4615	4614, 4616,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4618	4617, 4619,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Transport
4621	4620, 4622,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg

4623			18-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Telecom/ICT
4625	4624, 4626,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4628	4627, 4629,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4631	4630, 4632,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Energie
4634	4633, 4635,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Financieel
4637	4636, 4638,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4640	4639, 4641,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4644	4642, 4645,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4646	4643, 4647,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Financieel
4649	4648, 4650,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Financieel
4653	4652, 4654,		18-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Chemisch en Nuclear
4656	4655, 4657,		20-okt-13	Phishingaanval	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4659	4658, 4660, 4661,		21-okt-13	Melding publiek toegankelijke beheerinterfaces	Responsible Disclosure melding over publiek toegankelijke beheerinterfaces voor servers.	Rijksoverheid
4663	4662, 4664,		21-okt-13	Phishingsite	Verzoek tot assistentie voor het doen van een NTD verzoek aan een Nederlandse hoster.	Telecom/ICT
4675	4672, 4676, 4677,		24-okt-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4678	4673, 4679, 4680, 4681,		24-okt-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4682	4674, 4683, 4684, 4791,		24-okt-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4688	4687, 4689,		24-okt-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4690	4685, 4691, 4692,		24-okt-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4693	4686, 4694, 4695,		24-okt-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4700			25-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4702	4701, 4703, 4709, 4714, 4740,		25-okt-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een kwetsbaarheid in de website van een aanbieder van mobiele telefonie.	Telecom/ICT
4706	4705, 4707,		28-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4708	4704		28-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg

4710			28-okt-13	Nep-website	NTD verzoek voor nep-site onder de naam van organisatie in Transport sector	Transport
4711	4667, 4712, 4713,		28-okt-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4716	4715, 4717,		29-okt-13	Incident mailservers op blacklist	Overheidspartij stond met mailservers op een blacklist	Rijksoverheid
4720	4378		29-okt-13	Certificaat verlopen	Melding gekregen over een SSL-certificaat op een overheidswebsite die verlopen was.	Rijksoverheid
4722	4447, 4500,		29-okt-13	Logdata - lek in website	Melding over publiek toegankelijke logdata op een overheidswebsite.	Rijksoverheid
4723	4719, 4724, 4725, 4726,		29-okt-13	XSS-kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4727	4718, 4728, 4729, 4730,		29-okt-13	XSS-kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4731	4721, 4732, 4733,		29-okt-13	XSS-kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4735			30-okt-13	Torpig besmetting	Gecompromitteerde systemen in netwerk.	Energie
4742	4741, 4746,		1-nov-13	Foutmeldingen website	Overheidswebsite vertoonde enkele foutmeldingen.	Rijksoverheid
4744	4743, 4745,		1-nov-13	Phishingmail	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
4749			1-nov-13	Gerichte aanval	Gerichte aanval tegen overheidspartij.	Rijksoverheid
4753	4752, 4754,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Rijksoverheid
4756	4755, 4757,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gemeenten
4759	4758, 4760,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gemeenten
4762	4761, 4763,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Rijksoverheid
4764			4-nov-13	Phishingmail	Phishingmail tegen overheidspartij.	Rijksoverheid
4766	4765, 4767,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Rijksoverheid
4769	4768, 4770,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gemeenten
4772	4771, 4773,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Telecom/ICT
4775	4774, 4776,		4-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gezondheidszorg
4777	4734, 4751, 4778,		5-nov-13	Phishingactiviteit	Melding van phishingmail.	Financieel
4782	4779, 4780, 4781, 4783, 4784,		5-nov-13	DDoS-aanval	Melding buitenlands CERT-team over Nederlandse IP's die betrokken waren in een DDoS-aanval.	Telecom/ICT
4786	4785, 4787,		5-nov-13	Ondersteuning onderzoek	Verzoek om ondersteuning door het NCSC bij een zaak.	Rijksoverheid
4788			5-nov-13	Phishingactiviteit	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Financieel
4789			5-nov-13	Phishingactiviteit	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Financieel
4792			6-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4793			6-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid

4794			6-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4795			6-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Energie
4796			6-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4806	4803, 4804, 4805, 4807,		8-nov-13	Kwetsbaarheid in website overheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4809			9-nov-13	Mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4811			9-nov-13	Mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4813			9-nov-13	Mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4814			9-nov-13	Mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4815			9-nov-13	Mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4818	4810, 4816,		11-nov-13	Mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4819			11-nov-13	Malware infecties	Lijst met systemen binnen netwerk van Rijksoverheid welke geïnfecteerd waren met malware.	Rijksoverheid
4821			12-nov-13	Malwarebesmetting	Systemen binnen netwerk van ISP geïnfecteerd met malware.	Telecom/ICT
4822			12-nov-13	Melding malware-infectie	Systemen binnen netwerk van organisatie binnen gezondheidszorg waren geïnfecteerd met malware.	Gezondheidszorg
4823			12-nov-13	Melding malware-infectie	Systemen binnen netwerk van gemeente waren geïnfecteerd met malware.	Gemeenten
4824			12-nov-13	Melding malware-infectie	Systemen binnen netwerk van multinational waren geïnfecteerd met malware.	Multinational
4825			12-nov-13	Melding malware-infectie	Systemen binnen netwerk van overheidsinstelling waren geïnfecteerd met malware.	Rijksoverheid
4831			13-nov-13	Mogelijk gecompromitteerd systeem	Systemen binnen netwerk van hoster waren geïnfecteerd met malware.	Telecom/ICT
4832			13-nov-13	Malwarebesmetting	Systemen binnen netwerk van ISP waren geïnfecteerd met malware.	Telecom/ICT
4833			13-nov-13	Malwarebesmetting	Systemen binnen netwerk van ISP waren geïnfecteerd met malware.	Telecom/ICT
4835	4834, 4836,		13-nov-13	Clickjacking kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij	Rijksoverheid
4837			13-nov-13	Watering hole aanval	Melding buitenlandse overheidssite welke gebruikt wordt als watering hole.	Rijksoverheid
4838			13-nov-13	Malwarebesmetting	Malwarebesmetting van systemen binnen het netwerk van een partij binnen de telecom en ICT sector.	Telecom/ICT
4839			13-nov-13	Malwarebesmetting	Malwarebesmetting van systemen binnen het netwerk van een partij binnen de telecom en ICT sector.	Telecom/ICT
4840			13-nov-13	Mogelijke malware-infectie	Automatisch detectiesysteem; mogelijke malwarebesmetting	Telecom/ICT

4842			13-nov-13	Mogelijke Ebury-infecties	Mogelijke malware-infecties binnen netwerk van Nederlandse ISP.	Telecom/ICT
4844	4843, 4845,		14-nov-13	Verdachte activiteit op social media	Vraag vanuit overheidspartij over verdachte activiteiten op een social media-account van een conferentie.	Rijksoverheid
4850	4790, 4851, 4852,		15-nov-13	APT-aanval	Melding van mogelijke APT-aanval	Rijksoverheid
4853	4849, 4855, 5003, 5086,		15-nov-13	Downtime	Storing bij een van de PKI-overheidspartijen waardoor het voor een korte periode niet mogelijk was om PKI-overheidscertificaten te controleren middels de CRL.	Meerdere
4857	4808, 4858,		18-nov-13	Beveiligingsproblemen website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4859	4856, 4860,		18-nov-13	Beveiligingsproblemen website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4862	4861, 4863,		18-nov-13	Beveiligingsproblemen website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4866	4865, 4867,		19-nov-13	Modem kwetsbaarheid	Melding van mogelijk onveilige configuratie in modems van Nederlandse ISP.	Telecom/ICT
4869	4868, 4872, 4873, 4874, 4898, 4924, 4943, 4947,		19-nov-13	DDoS-aanval	DDoS-aanval op infrastructuur waar meerdere overheidspartijen van gebruik maakten.	Rijksoverheid
4870			19-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting	Overige
4871			19-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting	Gezondheidszorg
4876	4875		19-nov-13	Melding DDoS-aanval	Melding van DDoS-aanval op onderwijsinstelling.	Onderwijs
4877			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Energie
4878			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	ZBO
4879			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4880			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4881			20-nov-13	Verdachte URL: Melding mogelijke phishing vanuit netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4882			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4883			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Chemisch en Nuclear
4884			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4885			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4886			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4887			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4888			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4889			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten

4890			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4891			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4892			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Overige
4896	4895		20-nov-13	Phishing activiteiten	NTD verzoek voor domeinen.	Rijksoverheid
4897			20-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4905	4903, 4906, 4907, 4994,		20-nov-13	SQL Injectie op website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
4925			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Energie
4926			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4927			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4928			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Telecom/ICT
4929			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Chemisch en Nucleair
4930			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
4931			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Overige
4932			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4934			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4935			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gemeenten
4936			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	ZBO
4937			21-nov-13	Melding mogelijke malware-besmetting binnen netwerk	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
4983	4982		22-nov-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
5049	5037, 5050,		25-nov-13	Critical Stored XSS kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
5052	5051		25-nov-13	Melding mogelijk lek	Melding van overheidspartij dat er een mogelijk gegevenslek was op hun website. Een klant kon gegevens van een andere persoon inzien. Dit bleek te komen door een fout van een medewerker bij de betreffende overheidspartij.	Rijksoverheid
5054	5053, 5055, 5056,		26-nov-13	Mogelijke aanval	Melding van mogelijke aanval gericht op overheidspartijen	Rijksoverheid

5058	5057, 5059, 5078,		26-nov-13	Mogelijkheid tot inzien contactgegevens	PKI-meldplicht waarbij een PKI-overheidspartij melding heeft gemaakt dat op een van hun portals het mogelijk was contactgegevens van andere klanten in te zien.	Rijksoverheid
5061	5060, 5062,		26-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Overige
5063			27-nov-13	Diverse sites onveilig gehost	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de websites van verschillende overheidspartijen.	Rijksoverheid
5065	5064, 5066, 5071,		27-nov-13	Verdachte URL	Verzoek tot assistentie voor het doen van een NTD verzoek aan een Nederlandse hoster.	Meerdere
5069	5067, 5068,		27-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Telecom/ICT
5070			27-nov-13	Mogelijk security incident	Melding gemeente over mogelijk security incident. Ze hebben contact opgenomen met een bedrijf dat forensisch onderzoek komt doen.	Gemeenten
5079	5075, 5076, 5077,		28-nov-13	Mogelijke phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
5090	5089, 5106, 5124,		28-nov-13	Melding kwetsbaarheid	Melding over kwetsbaarheid in softwareproduct van Nederlandse partij.	Overige
5092	5091, 5093,		29-nov-13	DDoS aanval	Melding van Nederlandse hoster welke slachtoffer is van een DDoS-aanval en daarnaast ook afgeperst werd door de aanvallers.	Telecom/ICT
5097	5096, 5098,		29-nov-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
5102	5101, 5103, 5104,		29-nov-13	Phishingsite	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
5108	5107, 5109,		2-dec-13	Botnet	NTD verzoeken voor het neerhalen van Kelihos botnet.	Meerdere
5111	5105, 5110, 5340, 5345,		3-dec-13	XSS-Injectie	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
5117	5116, 5118,		3-dec-13	Onveilige routers	Melding van twee studenten dat zij in hun onderzoek een tweetal consumentenrouters hebben aangetroffen welke met standaard logingegevens vanaf het internet toegankelijk waren	Telecom/ICT
5122	5119, 5121, 5123,		3-dec-13	Potentieel botnet	Melding van organisatie uit financiële sector over verdacht verkeer dat ze waarnemen op hun netwerk. Vraag aan NCSC of wij meer informatie hebben over het verkeer dat zij zien.	Financieel
5125			3-dec-13	Melding verdachte site	Melding van organisatie dat zij een verdachte site waren tegengekomen welke dreigt met DDoS-aanvallen op bezoekers van de site. Geen indicatie dat dit ook daadwerkelijk het geval was	Rijksoverheid
5127	5126, 5128, 5200, 5242, 5259, 5368, 5371,		4-dec-13	Kwaadaardige mail	Melding buitenlandse CERT-partner over mogelijke APT-aanval richting overheidspartij. Geen indicatie bij de overheidspartij van compromitatie.	Rijksoverheid
5130	5129		4-dec-13	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	ZBO

5131			4-dec-13	DDoS-aanval	Verzoek tot assistentie van een organisatie bij een DDoS-aanval op deze organisatie.	Financieel
5133			4-dec-13	Vertrouwelijk document op internet.	Melding van een publiek toegankelijk mogelijk vertrouwd overheidsrapport. Dit rapport bleek via een WOB-verzoek geopenbaard te zijn.	Rijksoverheid
5135	5134, 5144,		5-dec-13	Mogelijke kwetsbaarheid http-only flag	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
5138	5137, 5260,		5-dec-13	Pony botnet	Mogelijke slachtoffers van pony botnet in Nederland.	Overige
5142	5141, 5143,		5-dec-13	Gecompromiteerde webserver	Melding gecompromiteerd systeem bij overheidspartij. Deze partij heeft een DDoS-script gevonden met verwijzingen naar buitenlandse opsporingsdienst, dit leek enkel een commentaar te zijn in het DDoS-script, en geen daadwerkelijk doelwit.	Rijksoverheid
5161	5162, 5163,		6-dec-13	Botnet	NTD-verzoeken verstuurd i.v.m. het neerhalen van b68-botnet.	Meerdere
5165	5164, 5166,		6-dec-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen financiële sector	Financieel
5169	5140, 5170, 5171,		6-dec-13	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
5172	5168		6-dec-13	DDoS-aanval	Melding Nederlandse hoster dat zij slachtoffer zijn geweest van een DDoS-aanval.	Telecom/ICT
5174	5173, 5175,		6-dec-13	Mogelijk kwetsbaarheid: X-content-type-options	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
5261			10-dec-13	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Telecom/ICT
5262			10-dec-13	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek aan een Nederlandse hoster.	Telecom/ICT
5263			10-dec-13	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek aan een Nederlandse hoster.	Telecom/ICT
5264			10-dec-13	Phishingactiviteit	Er is melding gemaakt van phishing-activiteit	Onbekend
5283			11-dec-13	XSS-kwetsbaarheid	Er is melding gemaakt van een XSS-kwetsbaarheid.	Onderwijs
5284			11-dec-13	XSS-kwetsbaarheid	Er is melding gemaakt van meerdere XSS-kwetsbaarheden.	Overige
5314	5313, 5322, 5323, 5324, 5325, 5347,		13-dec-13	Mogelijke DDoS-aanval	Er is melding gemaakt van een mogelijke DDOS-aanval.	Drinkwater
5326			15-dec-13	Verzoek contactgegevens	Een beveiligingsonderzoeker was op zoek naar contactgegevens om een RD-melding te kunnen melden.	Telecom/ICT
5331			16-dec-13	Informatielek	Er is melding gemaakt van een informatielek (pdf-bestand) op het internet.	Rijksoverheid
5332			16-dec-13	XSS-kwetsbaarheid	Er is melding gemaakt van XSS-kwetsbaarheid in een overheidswebsite. Dit bleek geen overheidswebsite te zijn.	Overige
5336	5335, 5337, 5338, 5339,		17-dec-13	Misbruik website	Melding over misbruik van een website-loket van een gemeente	Gemeenten
5341	5199, 5342,		17-dec-13	Melding XSS-kwetsbaarheden	Melding over geconstateerde XSS-kwetsbaarheden en onjuiste ServerSignature-instellingen in een website van een Rijksoverheidsorganisatie.	Rijksoverheid

5343	5204, 5285, 5344,		17-dec-13	XSS-kwetsbaarheid	Melding over een XSS-kwetsbaarheid in een overheidswebsite.	Rijksoverheid
5346	4610, 5312, 5348, 5352, 5495,		17-dec-13	Kwetsbaarheid websites	Melding over diverse kwetsbare overheidswebsites	Meerdere
5350	5349, 5351,		17-dec-13	Documenten gelekt	Er is melding gemaakt van gelekte documentatie (PDF-documentatie) op het internet.	Rijksoverheid
5357	5356		18-dec-13	ICT-incident bij website	Er is in groten getale gevoelige informatie, zoals gebruikersnaam en wachtwoord, gelekt van één specifieke website.	Overige
5360	5359, 5361,		19-dec-13	XSS-kwetsbaarheid	Er is melding gemaakt van een XSS-kwetsbaarheid in een overheidswebsite. De kwetsbaarheid is geverifieerd en doorgestuurd naar de eigenaar van de website	Rijksoverheid
5363	5362, 5364,		19-dec-13	DDoS activiteiten	Melding gemaakt van herhalende DDOS-incidenten op de website en verbinding van een scholengemeenschap.	Onderwijs
5386	5365, 5367, 5385,		23-dec-13	XSS-kwetsbaarheden	Er is melding gemaakt van meerdere XSS-kwetsbaarheden bij een overheidswebsite.	Rijksoverheid
5387	5366		23-dec-13	Phishingactiviteit	Hulpverzoek voor het offline halen van een phishingpagina gericht op het achterhalen van betalinggegevens.	Financieel
5394	5390, 5395,		23-dec-13	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5396	5391, 5397,		23-dec-13	Mogelijke malwarebesmetting	Melding van mogelijke besmetting van een website	Overige
5398	5393, 5399,		23-dec-13	Mogelijke malwarebesmetting	Melding van mogelijke besmetting van een website van een organisatie binnen de gezondheidszorg	Gezondheidszorg
5400	5392, 5401,		23-dec-13	Mogelijke malwarebesmetting	Melding van mogelijke besmetting van een website van een organisatie in de energiesector	Energie
5404	5403, 5405, 5406,		24-dec-13	Phishingaanval	Hulpverzoek voor het offline halen van een phishingpagina met daarop een betalingsverzoek	Financieel
5407			24-dec-13	Phishingpagina	Hulpverzoek voor het offline halen van een phishingpagina	Financieel
5409	5408, 5410,		24-dec-13	Crime SSL kwetsbaarheid	Kwetsbaarheid gevonden op twee overheidswebsite vatbaar voor de CRIME-aanval door TLS-compressie die niet was uitgeschakeld.	Rijksoverheid
5414	5413, 5415, 5416, 5424,		24-dec-13	kwetsbaarheden gevonden op website	Er is melding gemaakt van verschillende kwetsbaarheden (CSRF en het ontbreken van beveiligingsmaatregelen) in een website van een overheidsinstelling.	Rijksoverheid
5417			25-dec-13	Phishingactiviteit	Melding over phishingactiviteiten	Financieel
5420			27-dec-13	Phishingactiviteit	Melding over phishingactiviteiten	Onbekend
5422	5421, 5423, 5934,		29-dec-13	SQLi-kwetsbaarheid	Melding over een SQLi-kwetsbaarheid in een overheidswebsite	Rijksoverheid
5431	5428, 5432,		31-dec-13	Malwaresite	Informatie over mogelijke malwareverspreiding	Telecom/ICT
5434	5433, 5435, 5439, 5895,		1-jan-14	Mogelijke kwetsbaarheid	Er is melding gemaakt van een CSRF-kwetsbaarheid op een zoekformulier van een overheidswebsite	Rijksoverheid
5437	5436, 5438,		2-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een organisatie binnen de Telecom en ICT sector	Telecom/ICT
5441	5440, 5442,		3-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting	Overige

5444	5443, 5445,		3-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een organisatie binnen de gezondheidszorg	Gezondheidszorg
5447	5446, 5448,		3-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5450	5449, 5451,		3-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting van een organisatie binnen de Telecom en ICT sector	Telecom/ICT
5453	5452, 5454,		3-jan-14	Malware	Er is melding gemaakt dat de advertentieserver van een grote organisatie malafide advertenties verspreidde	Telecom/ICT
5461	5459, 5462,		6-jan-14	Phishingactiviteit	Hulpverzoek voor het offline halen van een phishingpagina gericht op het achterhalen van gevoelige informatie.	Financieel
5463	5460		6-jan-14	Fraude	Melding over VOIP telecomfraude	Overige
5466	5465, 5467,		6-jan-14	DDoS-aanval	Er is melding gemaakt van een DDoS-aanval op een webserver.	Telecom/ICT
5469	5468, 5470, 5471,		6-jan-14	Open NTP servers	Openstaande NTP-servers.	Meerdere
5473	5472, 5474,		7-jan-14	Phishingactiviteit	Hulpverzoek voor het offline halen van een phishingpagina gericht op het achterhalen van gevoelige informatie.	Financieel
5477	5476, 5478,		7-jan-14	Malware	Informatie verkregen over malware infecties	Meerdere
5479	5475, 5480, 5481, 5499,		8-jan-14	Cross-site scripting en lekken	Er is melding gemaakt van een XSS-kwetsbaarheid in diverse overheidswebsites.	Rijksoverheid
5482	5304, 5384, 5425, 5541, 5738, 5747, 5752,		8-jan-14	Beveiligingslek	Er is melding gemaakt van een SQLi-kwetsbaarheid op de website van een hogeschool.	Onderwijs
5484	5483, 5485, 5486,		8-jan-14	Kwetsbaarheid	Er is een kwetsbaarheid gevonden in een product.	Overige
5488	5487, 5489,		8-jan-14	XSS-kwetsbaarheden	Ter informatie heeft het NCSC een Responsible Disclosure melding gekregen met verzoek tot ondersteuning	Financieel
5492	5490, 5491, 5493,		8-jan-14	Phishingactiviteit	Er is melding gemaakt van Phishingpagina gericht aan de gebruikers van een bank.	Financieel
5505			10-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting	Overige
5507	5506, 5508,		10-jan-14	Phishingactiviteit	Hulpverzoek voor het offline halen van een phishingpagina gericht op het achterhalen van gevoelige informatie.	Financieel
5510	5509, 5511,		10-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een financiële instelling	Financieel
5525			13-jan-14	Torpig infectie	Melding van mogelijke besmetting van een website van een Rijksoverheidsorganisatie	Rijksoverheid
5526	5538		13-jan-14	Citadel infectie in netwerk waargenomen	Melding van mogelijke malware besmetting	Overige
5527			13-jan-14	Torpig infectie	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5528			13-jan-14	Torpig infectie	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5529			13-jan-14	Torpig infectie	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5535	5534, 5536, 5537,		14-jan-14	Phishingactiviteit	Hulpverzoek voor het offline halen van een phishingpagina gericht op het achterhalen van gevoelige gegevens	Financieel
5539			14-jan-14	Defacement	Defacement van websites in netwerk	Overige

5543	5411, 5412, 5544, 6615,		15-jan-14	Malafide servers	Hulpverzoek voor het offline halen van malafide servers die worden gebruikt voor gerichte aanvallen naar een buitenlandse overheid	Overige
5546	5545, 5547,		15-jan-14	Configuratiefout	Er is Responsible Disclosure melding gemaakt van een configuratiefout die tijdelijk een Denial-of-Service veroorzaakt van een website van een rijksoverheidsorganisatie.	Rijksoverheid
5548			15-jan-14	Torpig infectie	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5549			15-jan-14	Phishingactiviteit, oplichting	Er is melding gemaakt van een phishingpagina voor het verkrijgen van bitcoins.	Telecom/ICT
5556	5554, 5557,		16-jan-14	Phishingactiviteit	Melding door creditcardmaatschappij van een website die wordt gebruikt voor het ontplooiën van phishing-activiteiten	Financieel
5558	5555, 5559, 5563,		16-jan-14	Phishingactiviteit	Melding door creditcardmaatschappij van een website die wordt gebruikt voor het ontplooiën van phishing-activiteiten	Financieel
5560	5553, 5561, 5562,		16-jan-14	Phishingactiviteit	Melding gemaakt van meerdere websites die worden gebruikt voor het ontplooiën van phishing-activiteiten	Financieel
5566	5565, 5567,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5568	5542, 5569, 5570,		16-jan-14	Melding kwetsbaarheid	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5573	5572, 5574,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5576	5575, 5577,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5579	5578, 5580,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een organisatie uit de energie sector	Energie
5582	5581, 5583,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een financiële instelling	Financieel
5585	5584, 5586,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
5588	5587, 5589,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting	Overige
5591	5590, 5592,		16-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke besmetting van een website van een organisatie binnen de gezondheidszorg	Gezondheidszorg
5598	5596, 5599,		17-jan-14	Phishingactiviteit	Melding door creditcardmaatschappij van een website die wordt gebruikt voor het ontplooiën van phishing-activiteiten	Financieel
5600	5597, 5601, 5602,		17-jan-14	Phishingactiviteit	Melding over een website die wordt gebruikt voor het ontplooiën van phishing-activiteiten	Financieel
5605	5604, 5606,		17-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een organisatie binnen de gezondheidszorg	Gezondheidszorg
5608	5607, 5609,		17-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting	Overige
5611	5610, 5612,		17-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting	Overige
5614	5613, 5615, 5616,		17-jan-14	kwaadaardige mail	Informatie ontvangen over kwaadaardige mail	Onbekend
5622			19-jan-14	Domain tasting	Informatie verkregen over een groep die aan domain tasting doet	Meerdere
5624	5623, 5625,		19-jan-14	DDoS-aanval	Er is melding gemaakt van een langdurige DDOS-aanval op een onderwijsgroep.	Onderwijs

5629	5628, 5630,		20-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een organisatie binnen de gezondheidszorg	Gezondheidszorg
5632	5631, 5633,		20-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een financiële instelling	Financieel
5635	5634, 5636,		20-jan-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting	Overige
5638	5637		20-jan-14	DDoS-aanval	Er is melding gemaakt van een langdurige DDOS-aanval op een software ontwikkelaar.	Telecom/ICT
5640	5639, 5641, 5642,		20-jan-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina voor het verkrijgen van gevoelige informatie.	Telecom/ICT
5644	5643, 5645, 5646,		20-jan-14	Phishingactiviteit	Er is melding, door een creditcardmaatschappij, gemaakt voor een phishingpagina.	Financieel
5651	5650, 5652,		22-jan-14	DDoS-aanval	Er is melding gemaakt van een DDOS-aanval op een mediabedrijf.	Media
5657	5654, 5658, 5660,		23-jan-14	SQLi-kwetsbaarheid	Er is een Responsible Disclosure melding gemaakt van een SQLi-kwetsbaarheid op de website van een websitelerancier.	Overige
5659	5653, 5661,		23-jan-14	Logbestand gelekt	Er is een Responsible Disclosure melding gemaakt van een logbestand dat via het internet te raadplegen is, waardoor een deel van de configuratie van een webserver te herleiden was.	Rijksoverheid
5662			23-jan-14	MITM-aanval	Er is een Responsible Disclosure melding gemaakt van een cookie die niet middels HTTPS werd verzonden, waardoor bij een MITM-aanval de informatie in het cookie kon worden achterhaald.	Rijksoverheid
5663			23-jan-14	XSS-kwetsbaarheid	Er is melding gemaakt van een XSS-kwetsbaarheid in een website van een onderwijsinstelling	Onderwijs
5664			23-jan-14	XSS-kwetsbaarheid	Er is melding gemaakt van een XSS-kwetsbaarheid in een website van een onderwijsinstelling	Onderwijs
5669	5668, 5670,		24-jan-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina, gericht op het verkrijgen van inloggegevens van gebruikers voor een webwinkel.	Overige
5672	5671, 5673,		24-jan-14	XSS-kwetsbaarheid	Er waren een drietal XSS-kwetsbaarheden gevonden op een site van de overheid.	Rijksoverheid
5684	5683, 5685, 5687,		30-jan-14	Ondersteuning SSL-cipher suite	Er is gemeld dat een overheidswebsite anonieme SSL-ciphersuite ondersteund waardoor een SSL MITM/aanval mogelijk is.	Rijksoverheid
5686			30-jan-14	Phishingactiviteit	NTD-verzoek voor phishingwebsite	Onbekend
5693	5692, 5694,		31-jan-14	WiFi-netwerk niet beschikbaar	Er is een mogelijke aanval gemeld op infrastructuur van de overheid.	Rijksoverheid
5712	5711		3-feb-14	Kwetsbaarheid in softwareproduct	Melding kwetsbaarheid in een softwareproduct.	Telecom/ICT
5718			4-feb-14	NTD verzoek	Er is informatie ontvangen met daarbij een hulpverzoek voor het versturen van een NTD-verzoek	Overige
5726	5725, 5727,		6-feb-14	XSS-kwetsbaarheid	Melding gemaakt van een XSS-kwetsbaarheid op de website van de overheid.	Rijksoverheid
5728			6-feb-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Telecom/ICT
5732	5730		7-feb-14	Malwarebesmetting	Melding gemaakt van een overheidswebsite die is besmet met malware.	Rijksoverheid
5733	5734		7-feb-14	Spam/adware melding	Melding gemaakt van een besmette website.	Rijksoverheid

5736	5731, 5735, 5737, 6456,		7-feb-14	XSS-kwetsbaarheid	Melding gemaakt van een XSS-kwetsbaarheid op de website van een organisatie binnen de telecom en ICT sector.	Telecom/ICT
5739			7-feb-14	Mailserver op spamlijst	Melding gemaakt dat een mailserver van een Rijksoverheidsorganisatie op een spamlijst staat.	Rijksoverheid
5743	5742, 5744,		8-feb-14	Phishingactiviteit	Melding gemaakt van een tweetal phishingpagina's.	Financieel
5760	5759, 5761,		10-feb-14	Mogelijke DDoS	Er is melding gemaakt van een mogelijke DDOS-aanval op een organisatie in de financiële sector.	Financieel
5763	5762, 5764, 5765,		10-feb-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina.	Financieel
5767	5766, 5768,		10-feb-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina met daarbij het verzoek voor contactgegevens.	Financieel
5770	5769, 5771,		10-feb-14	DDoS- aanval	Er is melding gemaakt van een DDOS-aanval op één van de klanten van een organisatie in de telecom en ICT sector.	Telecom/ICT
5776			12-feb-14	Kwetsbare website	Er is melding gemaakt dat een overheidswebsite kwetsbaar is voor een BEAST-aanval.	Rijksoverheid
5782	5781, 5783,		13-feb-14	NDS-alert	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
5785	5784, 5786,		13-feb-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina.	Financieel
5795	5794, 5796, 5852, 5853,		17-feb-14	DNS Misconfiguratie	Er is melding gemaakt van onjuist geconfigureerde zone file voor een domein van de overheid.	Rijksoverheid
5798	5797, 5799,		17-feb-14	Mixed content op website	Er is melding gemaakt van mixed content op een overheidswebsite, waardoor mogelijk malafide content kan worden geladen.	Rijksoverheid
5805			18-feb-14	Phishingactiviteit	Er is melding, door een engeriemaatschappij, gemaakt van verschillende phishingemails met daarbij verzoek voor assistentie.	Energie
5814	5813, 5815, 5816,		20-feb-14	Valse website	Er is melding gemaakt van een valse, gekopieerde website waarschijnlijk om inlogcredentials te stelen.	Gezondheidszorg
5824	5823, 5825, 5918,		21-feb-14	Valse website	Er is melding gemaakt van een valse webshop.	Telecom/ICT
5828	5827, 5829,		22-feb-14	Configuratiefouten	Er is melding gemaakt van meerdere configuratiefouten op een systeem met mogelijk gevoelige informatie die publiekelijk bereikbaar is.	Transport
5831			24-feb-14	DDoS-aanval	DDoS-aanval en gesignaleerde informatie op social media.	Rijksoverheid
5834	5806, 5807, 5808, 5809, 5810,		24-feb-14	Oud datalek	Er is melding gemaakt van een oud datalek waarbij via zoekresultaten nog informatie publiek beschikbaar is.	Gemeenten
5836	5835, 5837,		24-feb-14	Mogelijke BGP hijack	Er is melding gemaakt van een mogelijke BGP-hijack voor een website van de overheid.	Rijksoverheid
5839	5838, 5840,		24-feb-14	XSS-kwetsbaarheid	Er is melding gemaakt van XSS-kwetsbaarheid in de website van een internet service provider.	Telecom/ICT
5845			25-feb-14	Phishingactiviteit	NTD-verzoek voor phishingwebsite.	Onbekend
5848			26-feb-14	Openstaande webshell	Er is melding gemaakt van een openstaande webshell op een website.	Onbekend
5850	5849, 5851,		27-feb-14	Kwaadaardige script	Er is een melding gemaakt van een website die middels een malafide script gevoelige informatie probeert te achterhalen.	Rijksoverheid
5855	5854, 5856, 5857, 5858, 5859,		27-feb-14	Phishingactiviteit	Er is melding gemaakt van een phishingemail voor het achterhalen van gevoelige informatie.	Rijksoverheid

5865	5861, 5866,		28-feb-14	Malwarebesmetting	Er is melding gemaakt van een malwarebesmetting op een computer van de overheid, betreft een oefening.	Rijksoverheid
5871	5869, 5870, 5872, 5873,		28-feb-14	Walwarebesmetting	Er is melding gemaakt van mogelijke malwarebesmettingen.	Onbekend
5875	5874, 5876,		28-feb-14	Kwetsbaarheid in webapplicatie	Er is informatie ontvangen over een veiligheidsincident ontstaan door een mogelijke kwetsbaarheid in een overheidssysteem.	Rijksoverheid
5877			28-feb-14	Phishingactiviteit	NTD-verzoek voor phishingwebsite.	Onbekend
5882	5881, 5883,		2-mrt-14	XSS kwetsbaarheid	Er is een XSS-kwetsbaarheid gemeld voor overheidswebsite.	Rijksoverheid
5890	5889, 5891,		3-mrt-14	Open Admin interface	Er is een admin-interface publiekelijk bereikbaar voor een overheidswebsite.	Rijksoverheid
5897	5896, 5941,		4-mrt-14	Cryptolockerbesmetting	Melding van cryptowarebesmetting bij een overheidsorganisatie.	ZBO
5903	5901, 5902, 5905, 5908,		4-mrt-14	Kwaadaardige mail	Er is informatie ontvangen omtrent een malafide email.	Overige
5904			4-mrt-14	Publiekelijk beschikbaar certificaat en wachtwoord	Er is gemeld dat een certificaat, inclusief wachtwoord van een provincie online staan.	Provincies
5910	5909, 5911		6-mrt-14	Informatie verkregen	Er is informatie ontvangen over een specifiek incident	Onbekend
5919			7-mrt-14	Kwetsbare website	Er is melding gemaakt dat een overheidswebsite kwetsbaar is voor een BEAST-aanval.	Rijksoverheid
5923	5922		7-mrt-14	DDoS-aanval	Er is informatie ontvangen over een DDoS-aanval	Onbekend
5924			7-mrt-14	Malwaremelding	Er is informatie ontvangen over een mail met malafide bijlage	Overige
5928	5927		8-mrt-14	E-mailadressen beschikbaar op PGP-server	Er is melding gemaakt dat er emailadressen van medewerkers van een overheidsorganisatie op een PGP-server staan. Dit bleek geen kwetsbaarheid, er was bewust voor gekozen.	Rijksoverheid
5937	5920, 5938, 5939,		11-mrt-14	onjuiste HTTP-header-implementatie	Er is melding gemaakt van onjuiste HTTP-header-implementatie op een overheidswebsite. Deze implementatie bleek geen kwetsbaarheid te vormen voor de website.	Rijksoverheid
5942			12-mrt-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
5943			13-mrt-14	Mogelijke defacement	Mogelijke defacement gedetecteerd.	Onderwijs
5944			13-mrt-14	Mogelijke defacement	Mogelijke defacement gedetecteerd.	Onderwijs
5948			13-mrt-14	DDoS-aanval	Er is melding gemaakt van een DDoS-aanval.	Energie
5952	5949, 5953, 5954, 5955, 5980,		14-mrt-14	DDoS-aanval	Er is informatie ontvangen over een DDoS-aanval.	Onbekend
5963	5962		17-mrt-14	Vertrouwelijke mail per ongeluk naar derde gestuurd	Er is melding gemaakt van abusievelijk verstuurd gevoelige informatie naar een derde partij.	Rijksoverheid
5964			17-mrt-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
5965			17-mrt-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Gezondheidszorg
5966			17-mrt-14	Verdachte DNS-requests	Er is informatie ontvangen over verdachte DNS-requests	Onbekend
5968	5967, 5969,		17-mrt-14	Watering Hole aanval	Er is informatie ontvangen over mogelijke compromittering	Transport

5970			17-mrt-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Rijksoverheid
5971			17-mrt-14	Mogelijke malware besmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Overige
5974			17-mrt-14	Indicators of Compromise	Er is informatie ontvangen over indicators of compromise	Onbekend
5975	5972, 5976,		17-mrt-14	Botnet	Er is informatie ontvangen over Nederlandse hosts betrokken bij een botnet.	Gemeenten
5977	5961, 5978, 5979, 5986,		17-mrt-14	DNS-hijack kwetsbaarheid	Er is melding gemaakt van DNS-hijack kwetsbaarheid op een overheidswebsite.	Rijksoverheid
5981	5960, 5982,		17-mrt-14	SQLi-kwetsbaarheid	Er is melding gemaakt van SQLi-kwetsbaarheid op een overheidswebsite.	Rijksoverheid
5984	5983, 5985,		17-mrt-14	Mogelijke Uroburos	Er is melding gemaakt van een hit bij een overheidsorganisatie. Bleek een false-positive melding.	Rijksoverheid
5997			18-mrt-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
5998			18-mrt-14	Malwareverspreiding	Malwareverspreiding via populaire websites in het .nl domein	Overige
5999			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6000			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6001			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6002			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6003			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6004			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6005			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6006			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6007			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6008			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6009			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6010			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6011			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6012			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6013			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6014			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6015			18-mrt-14	Melding m.b.t. malwareverspreiding	Er vindt malverspreiding plaats via een website.	Overige
6017	6016, 6018, 6019, 6020, 6021,		18-mrt-14	Phishingactiviteit	Er is melding gemaakt van voor meerdere phishingpagina's.	Financieel
6022			18-mrt-14	Beveiligingslek app	Er bevindt zich een Remote Code Executie kwetsbaarheid in een App.	Rijksoverheid
6037			19-mrt-14	Directory Traversal Aanval	Er is melding gemaakt van een directory traversal attack op een website van de overheid	Rijksoverheid
6049	6048, 6050, 6071,		20-mrt-14	Melding van meerdere DDoS-aanvallen	Hulpverzoek voor het achterhalen van aanval van grote DDOS-aanvallen op een social media platform.	Onbekend
6053	5996		20-mrt-14	Hulpverzoek	Hulpverzoek voor risicoinschatting omtrent malware.	Rijksoverheid
6054			20-mrt-14	Foutmelding bij NTD melding	Hulpverzoek bij het versturen van NTD-verzoek. De verzender krijgt foutmelding terug.	Onbekend
6055			20-mrt-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
6056			20-mrt-14	Hackpoging	Er is melding gemaakt van een hackpoging bij een ZBO.	ZBO
6074			21-mrt-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid

6076	6072, 6073, 6077, 6078,		21-mrt-14	Malware/phishcampagne	Er is melding gemaakt van een phishingcampagne waarbij aansluiting werd gezocht bij een groot evenement dat door de overheid werd georganiseerd.	Rijksoverheid
6103	6102, 6104,		23-mrt-14	Mislukte aanval	Ter informatie is het NCSC geïnformeerd over een aanval op een overheidswebsite.	Rijksoverheid
6105			23-mrt-14	Poortscan	Het NCSC is geïnformeerd omtrent een poortscan op een IP van een overheidsorganisatie.	Rijksoverheid
6114	6112		24-mrt-14	Banner Disclosure	Er is een banner-disclosure kwetsbaarheid gemeld in een website van de overheid.	Rijksoverheid
6115	6113, 6116,		24-mrt-14	Malafide website	Er is melding gemaakt van een malafide website.	Onbekend
6118			24-mrt-14	DNS verzoeken NDS sensor	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
6121	6120		24-mrt-14	DDoS-aanval	Melding over een DDoS aanval.	ZBO
6123	6122, 6125,		24-mrt-14	Adviesvraag omtrent mogelijk incident	Vraag om advies omtrent een mogelijk incident bij een groot evenement dat werd georganiseerd door de overheid.	Rijksoverheid
6124			24-mrt-14	Hackpogingen	Ter informatie heeft een energiebedrijf informatie gestuurd over drie mogelijke hackpogingen	Energie
6127	6126, 6128,		24-mrt-14	SSH-scan op systeem	Het NCSC is geïnformeerd omtrent een poortscan op een IP van een overheidsorganisatie.	Rijksoverheid
6130	6129, 6131, 6132, 6138, 6143,		24-mrt-14	Phishingactiviteit	Melding ontvangen over een website die wordt gebruikt voor het ontplooiën van phishingactiviteiten	Rijksoverheid
6133	5958, 5973,		24-mrt-14	Gehackte server	Er is melding gemaakt van een gehackte server die onderdeel was van een groot botnet.	Telecom/ICT
6134	6057		24-mrt-14	DDoS -aanval	Er is melding gemaakt van een DDOS-aanval gericht op website van een organisatie in reisbranche	Overige
6140	6139, 6141,		25-mrt-14	Zero day gebruikt in APT's.	Beveiligingsadvies over een zero-day door een partij in de sector telecom en ICT.	Telecom/ICT
6145	6117		25-mrt-14	Mogelijke kwetsbaarheid	Er is melding gemaakt van een mogelijke command injection kwetsbaarheid op een overheidswebsite.	Rijksoverheid
6166	6165, 6167, 6187, 6188, 6189, 6190, 6191, 6192, 6193, 6194,		27-mrt-14	NDS-melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
6169	6168, 6170,		27-mrt-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
6172	6171, 6173,		27-mrt-14	DDoS-aanval	Melding van een DDoS aanval	Telecom/ICT
6174	6142		27-mrt-14	Mogelijke kwetsbaarheid	Melding van een mogelijke information disclosure kwetsbaarheid op een overheidswebsite.	Rijksoverheid
6175			27-mrt-14	Spamrun melding	Er is melding gemaakt van een spamrun gericht op klanten van een telecombedrijf	Telecom/ICT
6184	6183, 6185,		28-mrt-14	Melding over infectie virus	Melding over een malwarebesmetting op een computer van de overheid.	Rijksoverheid
6186			28-mrt-14	Gelekte gegevens	Er is melding gemaakt van bankgegevens die worden gelekt	Financieel
6196	6195, 6197,		28-mrt-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidsorganisatie	Rijksoverheid
6200	6199, 6201,		28-mrt-14	Phishingactiviteit	Er is, door een creditcardmaatschappij, melding gemaakt van een phishingpagina waarbij om contactgegevens werd verzocht.	Financieel

6221	6220, 6222,		31-mrt-14	Phishingactiviteit	Er is, door een creditcardmaatschappij, melding gemaakt van een phishingpagina waarbij om contactgegevens werd verzocht.	Financieel
6224	6223, 6225, 6226,		31-mrt-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina gericht op het achterhalen van gevoelige informatie.	ZBO
6228	6227, 6229,		31-mrt-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina gericht op het achterhalen van gevoelige informatie.	Transport
6235			1-apr-14	Melding CSRF kwetsbaarheid	Er is melding gemaakt van een CSRF-kwetsbaarheid op het zoekveld van een overheidswebsite.	Rijksoverheid
6236			1-apr-14	Phishingactiviteit	Er is, door een creditcardmaatschappij, melding gemaakt van een phishingpagina waarbij om contactgegevens werd verzocht.	Financieel
6238	6237, 6239, 6240, 6264, 6338,		1-apr-14	Spoofing kwetsbaarheid	Responsible Disclosure melding omtrent een gevonden spoofing-kwetsbaarheid op een overheidwebsite.	Rijksoverheid
6251	6144, 6250, 6252, 6253,		2-apr-14	Verdacht domein	Attendering op mogelijk verdachte domeinen.	Rijksoverheid
6266	6265, 6267, 6318, 6283, 6374		3-apr-14	Phishingactiviteit	Er is melding gemaakt van meerdere phishingpagina's.	Rijksoverheid
6271	6270, 6272,		3-apr-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een onderwijsinstelling.	Onderwijs
6274	6273, 6281,		3-apr-14	NDS-melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
6276	6275, 6277, 6278,		3-apr-14	Phishingactiviteit	Er is melding gemaakt van een phishingpagina voor het achterhalen van gevoelige gegevens.	Rijksoverheid
6279	6268, 6280, 6282,		3-apr-14	XSS-kwetsbaarheid	Responsible Disclosure melding omtrent een gevonden XSS-kwetsbaarheid op een overheidwebsite.	Rijksoverheid
6284			3-apr-14	DDoS-aanvallen	Ter informatie is het NCSC geïnformeerd dat een organisatie aangifte gaat doen van DDOS-aanvallen	Transport
6295			4-apr-14	Defacement	Mogelijk defacement van een systeem gedetecteerd	Onderwijs
6297	6296, 6298,		4-apr-14	Verdacht gedrag telefoons	Verdacht gedrag telefoons na bezoek buitenland.	Rijksoverheid
6316	6315, 6317,		7-apr-14	Statistieken op website publiekelijk toegankelijk	Er is Responsible Disclosure melding gemaakt van publiek bereikbare statistieksystemen van de overheid	Rijksoverheid
6371	6370, 6372,		10-apr-14	Phishingactiviteit	Er is melding gemaakt van een phishingmail gericht op het achterhalen van gevoelige gegevens van een ambtenaar.	Rijksoverheid
6375	6373, 6376, 6377, 6378, 6379,		10-apr-14	DDoS-aanval	Hulpverzoek voor het offline halen van verschillende Nederlandse IP-adressen die participeren in een DDOS-aanval op een organisatie in het buitenland.	Onbekend
6382	6381, 6383,		10-apr-14	NDS-melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
6391	6390, 6392, 6393,		11-apr-14	Phishingactiviteit	Phishingpagina waarbij misbruik werd gemaakt van end-of-life product en diverse organisaties.	Financieel
6415	6414, 6416, 6417,		14-apr-14	Phishingactiviteit	Er is melding gemaakt van meerdere phishingpagina's.	Rijksoverheid

	6320, 6327, 6328, 6329, 6330, 6331, 6332, 6333, 6334, 6335, 6336, 6337, 6338, 6339, 6340, 6341, 6342, 6343, 6344, 6345, 6346, 6347, 6348, 6349, 6350, 6351, 6352, 6353, 6354, 6355, 6356, 6380,						
6426	6389,		15-apr-14	Gelekte e-mailadressen	Er is melding gemaakt van een zeer groot aantal gelekte emailadressen	Meerdere	
6428	6427		15-apr-14	DDoS-aanval	Hulpverzoek voor ondersteuning DDoS-aanval	Overige	
6447	6401, 6448,		17-apr-14	Melding kwetsbaarheid	Er is melding gemaakt van een Insecure Prefix handling-kwetsbaarheid op een overheidswebsite	Rijksoverheid	
6449	6400, 6450, 6451,		17-apr-14	Melding vanuit PKI-melplicht	Er is melding gemaakt vanuit PKI-meldplicht	Telecom/ICT	
6453	6452, 6454, 6455,		17-apr-14	DDoS-dreiging	Er is melding gemaakt van een DDOS-dreigement op een hoster.	Telecom/ICT	
6470	6469, 6471, 6472,		18-apr-14	Information Disclosure kwetsbaarheid	Er is information-disclosure kwetsbaarheid gemeld die betrekking heeft op een overheidsorganisatie.	Overige	
6473	6468, 6478,		18-apr-14	XSS-kwetsbaarheid	Melding van een XSS-kwetsbaarheid in een website	Overige	
6475	6474, 6476, 6477,		18-apr-14	Verdachte activiteiten	Er is melding gemaakt van verdachte activiteiten.	Onbekend	
6488	6487, 6489, 6490, 6540,		19-apr-14	Certificaatproblemen	Er is melding gemaakt van een certificaat-issue op een overheidswebsite.	Rijksoverheid	
6492	6491, 6493, 6494,		19-apr-14	Mogelijk datalek	Er is melding gemaakt van een mogelijk datalek.	Rijksoverheid	
6495			19-apr-14	Phishingactiviteit	Ter informatie een Nederlandse bank geïnformeerd over een mogelijk phishingdomein	Financieel	
6504	6503, 6505,		20-apr-14	Melding mogelijk gelekte informatie	Er is melding gemaakt van mogelijk gelekte informatie over providerdata en emailadressen	Telecom/ICT	
6526	6525, 6527,		22-apr-14	Melding certificaatfouten	Er is melding gemaakt van certificaatfouten op een overheidswebsite	Rijksoverheid	
6529	6528, 6530,		22-apr-14	Indicator of Compromise n.a.v. malware campagne	Er is melding gemaakt van detectiehit op eerdere gedeelte indicators of compromise van een malwarecampagne.	Gezondheidszorg	
6550	5540, 5844,		24-apr-14	Mogelijke kwetsbaarheid	Responsible Disclosure melding van SQLi-kwetsbaarheid op een overheidswebsite.	Rijksoverheid	
6551	4812, 4820,		24-apr-14	Mogelijke malware-besmetting	Melding van mogelijke malware besmetting bij een financiële instelling	Financieel	
6560	6559, 6561,		25-apr-14	NDS-melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid	
6613	6612, 6614,		29-apr-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidorganisatie	Rijksoverheid	
6617	6616, 6618,		29-apr-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een Rijksoverheidorganisatie	Rijksoverheid	
6620	6619		29-apr-14	DDoS-aanval	Melding van DDoS-aanval op een overheidspartij.	Rijksoverheid	
6637	6636, 6638,		30-apr-14	Command&Control centre	Er is melding gemaakt van een C&C-server in het netwerk van een Nederlandse provider.	Telecom/ICT	
6653	6652, 6654, 6656,		1-mei-14	XSS-kwetsbaarheid	Responsible Disclosure melding van een geconstateerde XSS-kwetsbaarheid in een overheidswebsite.	ZBO	
6663	6662, 6664,		2-mei-14	Phishingactiviteit	Ter informatie heeft een overheidspartij een DDoS-aanval gemeld aan het NCSC	Rijksoverheid	

6673	6674		3-mei-14	XSS-kwetsbaarheid	Er is melding gemaakt van een XSS-kwetsbaarheid in een gemeentewebsite.	Gemeenten
6675	6676, 6691,		3-mei-14	SQLi-kwetsbaarheid	Er is melding gemaakt van een SQLi-kwetsbaarheid in een overheidswebsite.	Rijksoverheid
6688	6667, 6689, 6690,		6-mei-14	Phishingactiviteit	Er is melding gemaakt van meerdere phishingpagina's gericht op het achterhalen van gevoelige informatie.	Rijksoverheid
6707	6706, 6708,		7-mei-14	Phishingactiviteit	Er is door een creditcardmaatschappij melding gemaakt voor een phishingpagina waarbij werd verzocht om contactgegevens.	Financieel
6721	6720, 6722,		8-mei-14	Phishingactiviteit	Er is melding gemaakt van meerdere phishingpagina's	Onbekend
6725	6723, 6726, 6727,		8-mei-14	Phishingactiviteit	Er is melding gemaakt van een phishing campagne	Financieel
6734	6733, 6735,		9-mei-14	Phishingactiviteit	Er is door een creditcardmaatschappij melding gemaakt voor een phishingpagina waarbij werd verzocht om contactgegevens.	Financieel
6768	6758		12-mei-14	SSL-kwetsbaarheid	Melding van SSL-kwetsbaarheid in een overheidswebsite.	Rijksoverheid
6769	6756, 6777,		12-mei-14	CSRF token kwetsbaarheid in website	Melding van CSRF-kwetsbaarheid in een overheidswebsite.	Rijksoverheid
6771	6770, 6772, 6778, 6779, 6820,		12-mei-14	Phishingactiviteit	Melding van meerdere websites die worden gebruikt voor het ontplooiën van phishingactiviteiten.	Rijksoverheid
6773	6757, 6774, 6775,		12-mei-14	Kwetsbaarheid website	melding van information disclosure kwetsbaarheid in een overheidswebsite	Rijksoverheid
6780	6747, 6781, 6782,		12-mei-14	Melding XSS en SQLi kwetsbaarheden	Melding van twee kwetsbaarheden, te weten de SQLi-kwetsbaarheid en de XSS-kwetsbaarheid, bij gemeenten.	Gemeenten
6799	6798, 6800, 6801,		13-mei-14	Phishingactiviteit	Melding van meerdere website die worden gebruikt voor het ontplooiën van phishingactiviteiten.	Rijksoverheid
6802	6783, 6803,		13-mei-14	X-Frame Clickjacking kwetsbaarheid	Melding van een X-Frame Clickjacking kwetsbaarheid in een overheidswebsite.	Rijksoverheid
6804	6797, 6805,		13-mei-14	Phishingactiviteit	Melding van een website die wordt gebruikt voor het ontplooiën van phishing activiteiten.	Transport
6807	6806		13-mei-14	Kwetsbaarheden in website	Melding van meerdere kwetsbaarheden, te weten SQLi, Shell injection en integer overflow, in een overheidswebsite.	Rijksoverheid
6822	6821, 6823, 6836, 6855, 6904, 6962, 6969, 6972,		14-mei-14	Website geeft ongeauthenticeerd toegang tot persoonsgegevens	Responsible Disclosure melding van website die ongeautoriseerden toegang geeft tot persoonsgegevens.	Overige
6851	6838, 6852, 7038,		16-mei-14	Melding meerdere kwetsbaarheden op websites	Er zijn meerdere kwetsbaarheden gemeld op overheidswebsites.	Rijksoverheid
6859	6857, 6858, 6860, 6861, 6863, 6864,		16-mei-14	Phishingactiviteit	Melding van phishing incident.	Rijksoverheid
6890	6776, 6889, 6891, 6903,		19-mei-14	Hack	Er is melding gemaakt van een hackincident.	Overige
6907			20-mei-14	Phishingactiviteit	Er is melding gemaakt van een mogelijk phishingincident	Rijksoverheid
6916	6915, 6917, 6918, 6929, 6990,		21-mei-14	Phishingactiviteit	Melding van website die wordt gebruikt voor het ontplooiën van phishingactiviteiten.	Rijksoverheid
6920	6919, 6921,		21-mei-14	Phishing-activiteiten	Hulpverzoek voor het offline halen van een domein dat wordt gebruikt voor het ontplooiën van phishing activiteiten.	Onbekend

6923	6922, 6924,		21-mei-14	Phishingactiviteit	Melding van website die wordt gebruikt voor het ontplooiën van phishingactiviteiten.	Overige
6932	6931, 6933,		22-mei-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting bij een transport organisatie.	Transport
6938	6934, 7133,		22-mei-14	Melding clickjacking kwetsbaarheid	Er is melding gemaakt van clickjacking kwetsbaarheid in een overheidswebsite. Het NCSC heeft de eigenaar van de website op de hoogte gesteld	Rijksoverheid
6939	6937, 6941, 6942, 6970, 6971, 7016,		22-mei-14	Phishingactiviteit	Er is melding gemaakt van een phishingsite.	Rijksoverheid
6940	6784		22-mei-14	Information disclosure kwetsbaarheid	Er is een information disclosure kwetsbaarheid gemeld van een overheidswebsite.	Rijksoverheid
6944	6943		22-mei-14	MIME-Sniffing kwetsbaarheid	Er is een MIME-Sniffing kwetsbaarheid gemeld voor een overheidswebsite.	Rijksoverheid
6947	6946, 6948,		22-mei-14	Publieke SNMP-configuratie	Publiekelijk bereikbare SNMP-configuratie bekend geworden.	Gemeenten
6960			23-mei-14	Website ondersteund geen PFS	Er is melding gemaakt dat een overheidswebsite geen perfect forward secrecy ondersteund.	Rijksoverheid
6963	6961, 6964,		23-mei-14	Publiek bereikbare servers	Social media bericht over publiek bereikbare servers waarbij aanpassingen kunnen worden doorgevoerd.	Rijksoverheid
6965	6945, 6966,		23-mei-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
6968	6950		23-mei-14	MIME-Sniffing kwetsbaarheid	Er is een MIME-Sniffing kwetsbaarheid gemeld voor een overheidswebsite.	Rijksoverheid
6974	6973, 7014, 7015, 7023,		23-mei-14	XSS-kwetsbaarheid	Er is een XSS-kwetsbaarheid voor meerdere websites gemeld.	Overige/ Onderwijs
6976	6975, 6977, 7010,		23-mei-14	Onjuiste certificate chain	Er is melding gemaakt van een onjuiste certificate chain op een overheidswebsite. De melder heeft zelf contact gezocht met de systeemeigenaar.	Rijksoverheid
6979	6978, 6980, 6981, 7007,		23-mei-14	Phishingactiviteit	Er is melding gemaakt van phishingmail en site.	Rijksoverheid
6992	6991, 6993, 6994,		24-mei-14	Phishingactiviteit	Er is melding gemaakt van een phishingsite.	Rijksoverheid
7009	7008		26-mei-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
7019	7018		26-mei-14	Phishingactiviteit	Er is melding gemaakt van een phishingactie.	Rijksoverheid
7020	7017, 7021, 7022,		26-mei-14	Phishingactiviteit	Er is melding gemaakt van een phishing activiteit.	Financieel
7025	7024, 7026,		26-mei-14	Kwetsbare website	Er is melding gemaakt van meerdere kwetsbaarheden voor een overheidswebsite.	Rijksoverheid
7028	7027, 7029,		26-mei-14	Publiek bereikbaar configuratiebestand	Er is een publiek bereikbaar configuratiebestand.	Gemeenten
7037			27-mei-14	MIME-Sniffing kwetsbaarheid	Er is een MIME-Sniffing kwetsbaarheid gemeld voor een overheidswebsite.	Rijksoverheid
7050	7049, 7051, 7053, 7131,		27-mei-14	Cyberaanval	Er is een melding gemaakt van een cyberaanval op een overheidsorganisatie.	Rijksoverheid
7065	7064		28-mei-14	Configuratieprobleem telefoons	Er is een configuratie issue gemeld met betrekking tot telefonie.	Rijksoverheid
7068	7067, 7069, 7070,		28-mei-14	Foutieve configuratie telefoons	Melding misbruik van foute configuratie telefoons.	Telecom/ICT
7084	7048, 7071, 7085, 7139,		29-mei-14	Gekopieerde website	Er is melding gemaakt van gekopieerde website die mogelijk voor malafide doeleinden gebruikt kan worden.	Transport
7092	7086, 7093,		29-mei-14	Mogelijke malwarebesmetting	Er is melding gemaakt van mogelijke virusinfecties bij een gemeente.	Gemeenten
7094	7075, 7095, 7096,		29-mei-14	Phishingactiviteit	Er is melding gemaakt van een phishingsite.	Rijksoverheid

7101	7100, 7102,		29-mei-14	Clickjacking kwetsbaarheid	Er is een clickjacking-kwetsbaarheid gemeld op een overheidswebsite.	Rijksoverheid
7113			30-mei-14	Content-spoofing-kwetsbaarheid	Er is een content-spoofing-kwetsbaarheid gevonden op een overheidswebsite.	Rijksoverheid
7134			2-jun-14	Cache-management-kwetsbaarheid	Er is een cache-management-kwetsbaarheid gemeld op een overheidswebsite.	Onbekend
7135	6573		2-jun-14	Phishingactiviteit	Er is melding gemaakt van meerdere phishingdomeinen.	Onbekend
7137	7136, 7138, 7226, 7227,		2-jun-14	Phishingactiviteit	Er is melding gemaakt van een phishingsite.	Rijksoverheid
7141	7140, 7142,		2-jun-14	Botnet	Er is informatie gedeeld over een gecoördinerende botnet takedown.	Onbekend
7144			2-jun-14	Incidentinformatie	Incidentinformatie met betrekking tot SCADA systemen	Gemeenten
7155	7154, 7156,		3-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7157	7153, 7158,		3-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Transport
7159	7152, 7160,		3-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7164	7154, 7165,		3-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7168	7167		3-jun-14	Strict-Transport-Security-kwetsbaarheid	Er is een Strict-Transport-Security-kwetsbaarheid gemeld voor een overheidswebsite	Rijksoverheid
7169	7166		3-jun-14	Strict-Transport-Security-kwetsbaarheid	Er is een Strict-Transport-Security-kwetsbaarheid gemeld voor een overheidswebsite	Rijksoverheid
7170	6879, 7171,		3-jun-14	XSS-kwetsbaarheid	Er is melding gemaakt van XSS-kwetsbaarheid in een website van een organisatie.	Drinkwater
7172	6881, 7173,		3-jun-14	Information disclosure kwetsbaarheid	Er is een information-disclosure-kwetsbaarheid gemeld in een overheidswebsite.	Rijksoverheid
7174	7153, 7175,		3-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Transport
7177	7176, 7178,		3-jun-14	DNS-kwetsbaarheid	Er is een DNS-kwetsbaarheid gemeld voor een website.	Rijksoverheid
7181	7180, 7182,		3-jun-14	APT-aanval	Er is informatie ontvangen over een APT-aanval.	Onbekend
7237	7234, 7235, 7236,		8-jun-14	Mogelijk gecompromiteerd emailaccount	Er is een melding gemaakt van een mogelijk gecompromiteerd emailaccount van een overheidsorganisatie.	Rijksoverheid
7248			9-jun-14	NDS melding	Het NDS-systeem heeft een hit gedetecteerd.	Rijksoverheid
7263	7262, 7264,		10-jun-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek.	Overige
7267	7265, 7266,		10-jun-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek.	Onbekend
7276			11-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7277			11-jun-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek.	Overige
7279	7278, 7280,		11-jun-14	Mogelijke infecties	Mogelijke malware infecties overheidspartij.	Rijksoverheid
7292			12-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7297			12-jun-14	DDoS-aanval	Melding DDoS-aanval op website.	Overige

7308	7307, 7309,		13-jun-14	Mogelijk gerichte aanval	Mogelijke gerichte aanval tegen overheidspartij.	Rijksoverheid
7310			13-jun-14	Publiek toegankelijke webapplicatie	Melding dat er een webapplicatie van een softwareleverancier publiek toegankelijk was. Hierdoor waren gegevens binnen deze applicatie door Google vindbaar.	Gemeenten
7324			15-jun-14	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen overheidspartij	Rijksoverheid
7326			15-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7327			15-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7329	7328, 7330, 7357,		15-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7340	7339, 7341, 7342,		16-jun-14	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen overheidspartij	Rijksoverheid
7344	7309		16-jun-14	Mogelijke gerichte aanval	Mogelijke gerichte aanval tegen overheidspartij.	Rijksoverheid
7350			16-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7351			16-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7352			16-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7353			16-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7354			16-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7355			16-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7363	7362, 7364, 7365,		16-jun-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek.	Financieel
7367	7366, 7368,		16-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7378	7377, 7379,		17-jun-14	Spearphish IoCs	Indicatoren ontvangen voor gerichte aanval op overheidspartij.	Rijksoverheid
7388			18-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7401			19-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7403	7400, 7409,		19-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een online winkel.	Overige
7407	7406, 7408,		19-jun-14	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen transportsector	Transport
7428	7426		20-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7429			20-jun-14	Indicators of Compromise	Rapport met indicators of compromise ontvangen.	Rijksoverheid
7439			21-jun-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek.	Overige
7470	7465, 7466, 7467, 7468, 7469,		24-jun-14	Mogelijke gecompromitteerde e-mailadressen	Geattendeerd op lijst met mogelijk gecompromitteerde e-mailadressen.	Meerdere

7481	7480, 7482,		25-jun-14	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen overheidspartij	Rijksoverheid
7484	7483, 7485,		25-jun-14	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen financiële sector	Financieel
7489	7488, 7490,		25-jun-14	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
7508	7507, 7509, 7519,		26-jun-14	Open IMPI interface	Publiek toegankelijke beheerinterfaces in netwerk.	Onderwijs
7511	7510, 7512,		26-jun-14	Open IMPI interface	Publiek toegankelijke beheerinterfaces in netwerk.	Telecom/ICT
7514	7513, 7515,		26-jun-14	Open IPMI interface	Publiek toegankelijke beheerinterfaces in netwerk.	MSP
7517	7516, 7518,		26-jun-14	DDoS-aanvallen	Er is een melding gemaakt van DDoS-aanvallen.	Gemeenten
7530	7529, 7531,		27-jun-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek.	Overige
7534	7533, 7535,		27-jun-14	Malwarebesmetting	Er is een melding gemaakt van malwareinfecties binnen netwerk van een organisatie.	Rijksoverheid
7555			28-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7557	7556, 7558,		28-jun-14	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen financiële sector	Financieel
7573			29-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7579	7578, 7580,		30-jun-14	Mogelijke kwetsbaarheid in systemen	Responsible disclosure melding over een mogelijke kwetsbaarheid in systemen gebruikt door partijen binnen de energiesector.	Energie
7582	7581, 7583, 7584,		30-jun-14	Mogelijke kwetsbaarheid in website	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7585			30-jun-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7606			1-jul-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7609	7608, 7610, 7611,		1-jul-14	Verdachte URL	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Onbekend
7613			1-jul-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7627	7626, 7647,		2-jul-14	Melding incident	Overheidspartij vraagt om assistentie bij een incident.	Rijksoverheid
7650	7649, 7651, 7672,		3-jul-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidsinstelling.	Rijksoverheid
7653	7652, 7654,		3-jul-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een organisatie in de transportsector.	Transport
7656	7655, 7657,		3-jul-14	Mogelijk veiligheidsprobleem	Melding mogelijk malafide DNS-verzoeken op domeinen van Rijksoverheid.	Rijksoverheid
7659	7658, 7660, 7795,		3-jul-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidsinstelling.	Rijksoverheid
7673	7671, 7674, 7675,		4-jul-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidsinstelling.	Rijksoverheid
7695	7687, 7696,		7-jul-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding betreffende een website van een Rijksoverheidspartij.	Rijksoverheid
7711	7710, 7712,		8-jul-14	Verdachte URL	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Financieel

7713	7532, 7714,		8-jul-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7716	7715, 7717, 7735,		8-jul-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7750	7747, 7749,		11-jul-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in een app.	Overige
7772	7758		14-jul-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7774	7775		14-jul-14	Kwetsbaarheid in besturingssysteem	Melding van kwetsbaarheid betreffende certificaten in besturingssysteem.	Meerdere
7783			15-jul-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7784			15-jul-14	Phishingactiviteit	Melding van phishing-campagne waarbij e-mailadressen zijn gebruikt die alleen intern beschikbaar zouden moeten zijn geweest.	Overige
7824	7823, 7825, 7826,		19-jul-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
7836	7835, 7837, 7838,		20-jul-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij	Rijksoverheid
7847	7846, 7848, 7849, 7946,		21-jul-14	Ebury gecompromiteerde hosts	Lijst ontvangen met Ebury-besmettingen in Nederland.	Telecom/ICT
7851	7850		21-jul-14	Verdachte URL	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7880	7881, 7882, 7883,		24-jul-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Websites
7896	7895, 7897,		25-jul-14	DDoS-aanval	Lijst ontvangen met IP-adressen die volgens melder betrokken waren bij een DDoS-aanval.	Overige
7900	7898, 7899, 7901,		25-jul-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
7923	7922, 7924, 7925,		27-jul-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
7933	7648, 7934,		28-jul-14	Verdachte URL	Verzoek tot assistentie voor het doen van een NTD.	Onbekend
7944	7943, 7945, 8107,		30-jul-14	Watering hole	Melding van een watering hole gericht op een organisatie	Chemisch en Nucleair
7948	7947, 7949, 7950,		30-jul-14	DDoS-aanval	DDoS-aanval op een doelwit buiten Nederland gebruik makende van Nederlandse infrastructuur.	Overige
7968	7967		31-jul-14	Malware-infecties	Extern datarapport over een aantal malwareinfecties in Nederland.	Onbekend
7983	7982, 7984, 7985, 7986,		1-aug-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
7988	7987, 7989,		1-aug-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Onbekend
8020	8014		4-aug-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
8030	8029, 8031,		5-aug-14	Watering hole aanval	Melding van een watering hole gericht op een organisatie.	Chemisch en Nucleair

8076	8075, 8328,		6-aug-14	Gecompromitteerde accounts	Lijst met gecompromitteerde emailaccounts ontvangen.	Telecom/ICT
8077	8044, 8080,		6-aug-14	Melding open FTP	Melding van open FTP bereikbaar via internet van een zorginstelling.	Gezondheidszorg
8090	8091, 8095, 8442, 8506, 8507, 8899, 9100, 9213, 9214, 9238, 9247, 9248, 9249, 9251, 9278, 9279, 9280, 9282, 9304, 9305, 9332, 9379, 9380, 9382, 9383, 9389, 9392, 9415, 9439, 9440, 9441, 9512, 8703		6-aug-14	Hack	Dataset met logingegevens en kwetsbare websites. Subset van de gegevens met Nederlandse slachtoffers ontvangen.	Meerdere
8101			6-aug-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
8102			6-aug-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
8103	8081, 8104,		6-aug-14	DDoS-aanval	DDoS-aanval op een doelwit buiten Nederland gebruik makende van Nederlandse infrastructuur.	Onbekend
8132	8131, 8133,		7-aug-14	DDoS-aanval	Er is melding gemaakt van een DDOS-aanval gericht op website van een organisatie in reisbranche.	Overige
8184	8183, 8185, 8186, 9114,		11-aug-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Financieel
8208	8207, 8209, 8210, 8211,		13-aug-14	Kwetsbare webservers	RD melding met betrekking tot Nederlandse webservers.	Telecom/ICT
8223	8222, 9057,		14-aug-14	Wifi-uitval	WiFi-netwerk uitgevallen na misbruik kwetsbaarheid.	Transport
8263	8262		18-aug-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
8271			19-aug-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
8286	8272, 8287, 8294,		20-aug-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een organisatie in de financiële sector.	Financieel
8288	8273, 8289,		20-aug-14	Melding van malware	Melding van malware gehost in Nederland.	Financieel
8290	8276, 8291,		20-aug-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8293	8292		20-aug-14	Spearphishing aanval	Spear phishing gericht op management van een Nederlandse multinational.	Chemisch en Nuclear
8306			21-aug-14	Verdachte URL	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
8307			21-aug-14	Verdachte URL	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
8308			21-aug-14	Verdachte URL	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
8309			21-aug-14	Verdachte URL	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
8311	8310		21-aug-14	DDoS-aanval	DDoS-aanval op een financiële dienstverlener.	Financieel
8325	8324, 8326, 8327,		22-aug-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid

8333	8332, 8334, 8338,		22-aug-14	DDoS-aanval	DDoS-aanval op een doelwit buiten Nederland gebruik makende van Nederlandse infrastructuur.	Onbekend
8336	8335, 8337,		22-aug-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8355	8354, 8356, 8357,		23-aug-14	DDoS-aanval en malwareverspreiding	Lijst met IP's en credentials ontvangen van systemen in Nederland die gebruikt werden voor DDoS en het verspreiden van malware.	Telecom/ICT
8377	7586, 8376, 8378, 8379, 8380, 8382, 8385, 8386, 8387, 8388, 8389, 8503, 8824, 8954, 8957, 9494, 9495, 9639, 9791, 9941, 10142, 10409, 10575, 10578, 10679, 10680, 10791, 10978, 11101, 11259, 11368, 11510, 11707, 11833, 12179, 12295, 12419, 12499, 12500, 12501,		25-aug-14	Ebury infecties	Gecompromiteerde systemen.	Telecom/ICT
8398	8397, 8399, 8400, 8401, 8402, 8403, 8404, 8405, 8406, 8407, 8408, 8409, 8410, 8411, 9583, 9584, 9585, 9586, 9587, 9588, 9589, 9590, 9788, 9789, 9943, 9944, 10046, 10158, 10195, 10331, 10410, 10738, 10739,		26-aug-14	Brobot-URL's	Nederlandse systemen hostten malware	Telecom/ICT
8413	8412, 8414, 8415,		26-aug-14	Verdachte URL	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8424	8423, 8425, 8447, 8535, 8536, 8537, 8538, 8539, 8542, 8543, 8560,		27-aug-14	Mogelijke kwetsbaarheid	Nieuwe kwetsbaarheid aangetroffen in systeem tijdens penetratietest bij een overheidspartij.	Rijksoverheid
8440	8439		28-aug-14	Melding	Kwetsbaar van het NAS-systeem was blootgesteld aan het internet.	Rijksoverheid
8443			28-aug-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Onbekend
8445	8444, 8446, 8482, 8664,		28-aug-14	Mogelijke malware besmetting	IoC's ontvangen voor malware.	Energie
8566	8561, 8564, 8616,		3-sep-14	XSS kwetsbaarheid	RD melding mogelijke XSS kwetsbaarheid	Rijksoverheid
8584	8583, 8585, 8587,		4-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8590	8589		4-sep-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
8609	8608, 8610, 8611, 8665,		5-sep-14	Verdachte URL	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8613	8612, 8614, 8615,		5-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8617			5-sep-14	Mogelijk botnet	Indicators of compromise ontvangen over mogelijk botnet.	Telecom/ICT

8619	8618, 8620,		5-sep-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding betreffende online beschikbare documenten met mogelijk gevoelige informatie.	Financieel
8667	8666, 8668,		8-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8670	8669, 8671,		8-sep-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid bij een overheidspartij.	Rijksoverheid
8684	8683, 8685,		9-sep-14	Verlopen van certificaat	Certificaat van een systeem verlopen	Rijksoverheid
8688	8686, 8687, 8689,		9-sep-14	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting	Rijksoverheid
8704	8238, 8239, 8259, 8274, 8275,		10-sep-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in een website van een Nederlands transportbedrijf.	Transport
8717	8716, 8718,		11-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
8719			11-sep-14	Beveiligingsincident	Website overheidspartij misbruikt voor het hosten van afbeeldingen.	Rijksoverheid
8741			12-sep-14	Melding mogelijke gecompromiteerde website	Kwetsbare CMS-plugin gebruikt voor het uploaden van bestanden.	Overige
8743			12-sep-14	DDoS-aanval	DDoS-aanval op een onderwijsinstelling	Onderwijs
8761	8760, 8762,		13-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Onbekend
8789	8744		15-sep-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Onbekend
8797	8788, 8798,		16-sep-14	Malware	Verkeer geassocieerd met malware, bleek van een Tor-exit-node te zijn.	Overige
8799			16-sep-14	DDoS-aanval	Melding over een DoS-aanval waarbij gebruik is gemaakt van het Simple Service Discovery Protocol	Telecom/ICT
8800			16-sep-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een semi-overheidspartij.	ZBO
8803	8802, 8827, 8828, 8829, 8860,		16-sep-14	Watering hole-aanval	Informatie over wateringhole-aanval verkregen.	Meerdere
8805	8804, 10194,		16-sep-14	Actieve glasvezel	Actieve glasvezelverbinding in een oud pand van een Rijksoverheidspartij.	Rijksoverheid
8853	8852, 8854,		18-sep-14	Omzeiling authenticatie	Responsible Disclosure melding betreffende de mogelijkheid om de authenticatie van een applicatie te omzeilen	Overige
8856	8886, 8890, 8892, 8923, 8924, 8925, 8926, 9101, 9127, 9331, 9444, 9580, 9581, 9666, 10610, 10644, 10668,		18-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op verschillende overheidspartijen.	Rijksoverheid
8858	8857, 8859,		18-sep-14	Mogelijk incident	Mogelijk misbruik systeem Nederlands bedrijf.	Onbekend
8862	8861, 9116,		18-sep-14	Private key naar verkeerde partij	Melding dat een hostingpartij een private key naar een verkeerd persoon heeft gestuurd	Rijksoverheid / Telecom en ICT
8884	8883, 8885, 8891, 9275,		19-sep-14	Melding vanuit PKI-meldplicht	PKI-meldplicht-melding over een storing in een CRL-server.	Telecom/ICT
8894	8893, 8895,		19-sep-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Telecom/ICT

8904			19-sep-14	Oplichting	Melding over oplichting van een klant van een energiebedrijf	Energie
8947	8946, 8948,		22-sep-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
8949	8945, 8951, 8952,		22-sep-14	Malware	Indicator of Compromise ontvangen over malware	Rijksoverheid
8956			22-sep-14	Gerichte aanval	Melding over malware die is ontvangen via e-mail waarbij mogelijk sprake was van een gerichte aanval	Rijksoverheid
8959	8900, 8955, 8960,		22-sep-14	Gehackt e-mailadres	Melding van gehackt e-mailadres en misbruik privé-e-mailadres medewerker van buitenlandse vertegenwoordiging.	Overige
8962	8330, 8963, 8978, 10826,		22-sep-14	Verkeerd verzonden e-mails	Melding van e-mailverkeer naar adressen gelijkend op rijksoverheid e-mailadressen	Rijksoverheid
8967			22-sep-14	Defacement	Melding over een defacement van een website van een gemeente.	Gemeenten
8980	8979, 8981,		23-sep-14	Melding kwetsbaarheden	Melding kwetsbaarheden in systemen mogelijk in gebruik door Nederlandse luchtvaartmaatschappijen, betrokken organisaties ingelicht.	Transport
9000	8998, 8999,		24-sep-14	Malafide webshop	Verzoek om hulp bij NTD-verzoek malafide webshop.	Telecom/ICT
9006	9005, 9007,		24-sep-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Telecom/ICT
9008			24-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank en verzoek om assistentie bij NTD	Financieel
9027	9023, 9046,		25-sep-14	Reputatieschade	IP's van rijksoverheid stond onterecht op lijst malafide IP's van een antivirusbedrijf.	Rijksoverheid
9029	9028, 9030,		25-sep-14	Typosquatter	Melding ontvangen over typosquatter-domein	Telecom/ICT
9031			25-sep-14	Malafide IP-adressen.	Melding ontvangen over malafide IP's	Overige
9049			26-sep-14	Targeted Attack Indicator	Targeted Attack Indicator ontvangen uit betrouwbare bron	Rijksoverheid
9051	9050, 9052, 9053,		26-sep-14	DDoS-aanval	Melding van een DDoS-aanval die gebruik maakte van Nederlandse infrastructuur.	Telecom/ICT
9055	9054, 9056,		26-sep-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
9059	9058		26-sep-14	DDoS-aanval	DDoS-aanval op Rijksoverheidsorganisatie	Rijksoverheid
9098	9097, 9099,		30-sep-14	Shellshock scans vanaf netwerk	Melding shellshock-scans vanaf netwerk Nederlandse hoster.	Overige
9128			2-okt-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Financieel
9150	9133, 9135, 9151, 9157,		3-okt-14	Mogelijke Phishingactiviteit	Melding spearphishing-aanval.	Rijksoverheid
9171			4-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9192	9191, 9193, 9194,		6-okt-14	Gecompromitteerde credentials	Informatie van gecompromitteerde credentials van meerdere organisaties	Meerdere
9195	9189, 9196,		6-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9197	9190, 9198,		6-okt-14	Indicator of Compromise	IoC's ontvangen voor watering holes.	Rijksoverheid

9202			6-okt-14	Phishingactiviteit	Melding over een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
9216			7-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid bij een overheidspartij.	Rijksoverheid
9217			7-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid bij een overheidspartij.	Rijksoverheid
9218			7-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid bij een overheidspartij.	Rijksoverheid
9233	9219		8-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid bij een overheidspartij.	Rijksoverheid
9237	9235, 9242,		8-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9239	8855, 9667, 9836,		8-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure melding over mogelijke kwetsbaarheid in systeem van een Nederlandse gemeente	Gemeenten
9240	9221, 9243, 9245, 9246,		8-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij	Rijksoverheid
9241	8261		8-okt-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank.	Financieel
9268			9-okt-14	Hulpverzoek	Hulpverzoek voor NTD.	Financieel
9269			9-okt-14	Phishingactiviteit	Phishing e-mail ontvangen vanuit een Nederlandse bank.	Financieel
9270	9267, 9271, 9273,		9-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure melding over vermoedelijke kwetsbaarheid bij Rijksoverheidspartij	Rijksoverheid
9272			9-okt-14	Melding DDoS-aanval	Melding DDoS-aanval op financiële dienstverlener.	Financieel
9274	8903, 9349, 9384, 9568, 10461, 11020,		9-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheden in websites van een buitenlandse visumaanvraagverwerker.	Overige
9287	9285, 9288, 9289,		10-okt-14	DDoS-aanval	Melding van Layer 7 DOS-aanval	Telecom/ICT
9319	9317, 9318, 9320, 9359,		12-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9323	9322, 9324,		12-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9328			13-okt-14	Mogelijke malwarebesmetting	NDS melding van mogelijke malwarebestemming bij Rijksoverheidspartij	Rijksoverheid
9335	9334, 9337, 9358,		13-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9336			13-okt-14	Melding DDoS-aanval	Melding van DDoS-aanval op Rijksoverheidspartij	Rijksoverheid
9338			13-okt-14	Malware	Melding van malware-besmetting via website	Onbekend

9351	9348, 9350, 9352, 9353, 9356, 9357, 9360, 9361, 9362, 9381, 9390, 9391, 9406, 9407, 9409, 9414, 9417, 9418, 9419, 9503, 9505, 9508, 9513, 9516, 9517, 9518, 9529, 9531, 9551, 9758, 9884,		14-okt-14	Cryptolocker op phishingdomein	Phishingcampagne met cryptolocker.	Meerdere
9364	9363, 9443,		14-okt-14	Cryptoware	Melding van cryptolocker-infectie bij rijksoverheidspartij	Rijksoverheid
9365	9408		14-okt-14	Cryptoware	Melding van cryptolocker-infectie bij rijksoverheidspartij	Rijksoverheid
9387	9386, 9388,		15-okt-14	Poortscan	Poortscan met gespoofed IP	Rijksoverheid
9411	9410, 9412, 9413,		16-okt-14	Gerichte aanval	Melding van gerichte aanval op financiële instelling	Financieel
9437	9436, 9438,		17-okt-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij private organisatie	Publiek
9462	9461, 9463,		18-okt-14	Mogelijke malwarebesmetting	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Financieel
9497	9493, 9496, 9499,		20-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9500	9498, 9501,		20-okt-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de gezondheidszorg	Gezondheidszorg
9506	9504, 9507,		20-okt-14	Torrentlocker melding	Melding van torrentlocker-infectie bij rijksoverheidspartij.	Rijksoverheid
9510	9509		20-okt-14	Mogelijke malwarebesmetting	NDS-melding over mogelijke malwarebesmetting bij een Rijksoverheidsinstelling	Rijksoverheid
9511			20-okt-14	Mogelijke malwarebesmetting	NDS-melding over mogelijke malwarebesmetting bij een Rijksoverheidsinstelling	Rijksoverheid
9515	9514, 9552,		20-okt-14	DDoS-aanval	Melding over DDoS-aanvallen op scholengemeenschap	Overige
9582			24-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure melding over kwetsbaarheid bij Gemeente	Gemeenten
9591			24-okt-14	DDoS-aanval	Melding van DDoS-aanval op een doelwit buiten Nederland, waarbij gebruik is gemaakt van Nederlandse infrastructuur.	Overige
9592	9593, 9594, 9595, 9596, 9597, 9598, 9599, 9601, 9603, 9604, 9605, 9606, 9607, 9640, 9641, 9642, 9643, 9644, 9645, 9646, 9647, 9648, 9649, 9650,		24-okt-14	Malware-infecties	Lijst met malwareinfecties ontvangen	Meerdere
9602	9600		24-okt-14	Hack website	Hack van website van buitenlandse financiële instelling. Credentials online gezet.	Financieel
9651	9482		27-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid

9652	9481		27-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9653	9480		27-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9654	9479		27-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9655	9478		27-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9656	9477		27-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9669	9670, 9672, 9673, 9674, 9675, 9676, 9677, 9678,		28-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9679	9671, 9680, 9681, 9682, 9683, 9684, 9685, 9686, 9687, 9688, 9689, 9690, 9691, 9692, 9964, 10004, 10010, 10197, 10309, 10489,		28-okt-14	Asprox download proxies	Melding proxies voor Asprox-malware.	Meerdere
9693	9631		28-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over mogelijke kwetsbaarheden in de website van een overheidspartij.	Rijksoverheid
9708	9707		29-okt-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Rijksoverheidsorganisatie	Rijksoverheid
9710	9709		29-okt-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Rijksoverheidsorganisatie	Rijksoverheid
9713	9712		29-okt-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de Transportsector	Transport
9716	9715, 9718,		29-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een Gemeente.	Gemeenten
9719	9714		29-okt-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding van een mogelijke kwetsbaarheid in een website van de Rijksoverheid	Rijksoverheid
9722	9721, 9723,		29-okt-14	Informatie over kwetsbaarheden	Melding van kwetsbaarheden in routers	Telecom/ICT
9735	9734		30-okt-14	Gecompromitteerde credentials	Credentials van gemeente aangetroffen op verdachte website	Gemeenten
9738	9737, 9739, 9740, 9741, 9756, 9757,		30-okt-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlands bedrijf.	Overige
9754	9753, 9755,		31-okt-14	Phishing-site	Verzoek tot assistentie voor het doen van een NTD verzoek.	Financieel
9793	9792, 9794,		3-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding ontvangen van mogelijke kwetsbaarheid bij een Nederlandse gemeente	Gemeenten

9795	9004, 9796, 9798, 9803, 9948,		3-nov-14	Kwetsbaarheid NAS-systemen	Melding met lijst met IP's van kwetsbare NAS-systemen ontvangen	Telecom/ICT
9806	9805, 9808, 12422		3-nov-14	Lijst met ip-adressen gelekt	Lijst met IP security camera's met default credentials.	Overige
9833	9832		5-nov-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Financieel
9835	9834, 9837,		5-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9839	9838, 9840, 9847, 9863, 9864, 9865,		5-nov-14	Ransomware	Melding van Torrentlocker-infectie bij een organisatie in de financiële sector.	Financieel
9842	9841, 9843, 9844, 10372, 10373,		5-nov-14	Mogelijke kwetsbaarheid	Kwetsbaarheid aangetroffen in systemen van een CSP.	Overige
9849	9848, 9850,		5-nov-14	Defacement	Melding van mogelijk defacement van een website van een gemeente	Gemeenten
9880	9879, 9881,		7-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Rijksoverheidsorganisatie	Rijksoverheid
9882			7-nov-14	DDoS	Melding van afpersing door middel van DDoS aanvallen	Financieel
9918	9915, 9916, 9917, 9919, 9920, 9921,		9-nov-14	Defacement	Melding van defacement van een website van een kerk	Overige
9923	9922, 9940,		9-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9936	9933, 9934, 9935, 9937, 9947,		10-nov-14	Botnet	Lijst ontvangen met sinkholedata botnet.	Meerdere
9963			11-nov-14	Gecompromitteerde credentials	Credentials van een Rijksoverheids-medewerker aangetroffen op verdachte website	Rijksoverheid
9966	9965, 9967,		11-nov-14	Defacement	Melding van defacement van een website van een energieleverancier	Energie
9972	9968, 9969, 9970, 9971, 9973,		11-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over mogelijke kwetsbaarheid in een website van de Rijksoverheid.	Rijksoverheid
9976			11-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
9993			12-nov-14	Phishingactiviteit + gestolen laptop	Melding van phishing-site, credentials buitgemaakt van een medewerker	Provincies
9996	9975, 9977, 9999, 10005,		12-nov-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een energiebedrijf.	Energie
9997	9974, 9980,		12-nov-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
10001	9998, 10002, 10047, 10048, 10049, 10050, 10051, 10052, 10053, 10054, 10055, 10056, 10057,		12-nov-14	Indicators of Compromise bij CMS	Lijst met IoC's ontvangen voor CMS-malware.	Meerdere
10035	10034, 10036,		13-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Rijksoverheidsorganisatie	Rijksoverheid
10038	10037, 10039,		13-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de Transportsector	Transport

10041	10040, 10042,		13-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Rijksoverheidsorganisatie	Rijksoverheid
10044	10043, 10045,		13-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de Transportsector	Transport
10060	10059, 10061,		13-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de gezondheidszorg	Gezondheidszorg
10063	10062, 10064,		13-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de gezondheidszorg	Gezondheidszorg
10069	10068, 10070,		13-nov-14	DDoS-aanval	Melding van DDoS-aanval op webwinkel	Overige
10099	10098, 10100, 10162, 10163,		14-nov-14	Mogelijk incident	Melding van storing in een meetsysteem	Rijksoverheid
10135	10119, 10134, 10136,		16-nov-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Financieel
10143			17-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
10155	10154, 10156,		18-nov-14	Gecompromitteerde credentials	E-mailadres behorende bij rijksoverheidsorganisatie aangetroffen op verdachte website	Rijksoverheid
10157			18-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding van mogelijke kwetsbaarheid in een website van de Rijksoverheid.	Rijksoverheid
10160			18-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Gemeenten	Gemeenten
10161			18-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Rijksoverheidsorganisatie	Rijksoverheid
10196			20-nov-14	Melding Command and Control server	Melding ontvangen van Command and Control server IP's gehost bij Nederlandse hoster.	Telecom/ICT
10213	10212, 10214,		21-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
10218	10217, 10219, 10220, 10221, 10222,		21-nov-14	NTD verzoek	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Telecom/ICT
10265	10264, 10266, 10335, 10336, 10337, 10338, 10342, 10343, 10348, 10350,		24-nov-14	Informatieverzoek	Lijst kwetsbare apps ontvangen.	Meerdere
10268	10215, 10216, 10223,		24-nov-14	Cryptoware	Melding van een malwarcampagne gericht op een webwinkel.	Overige
10281	10282		25-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de Transportsector	Transport
10284			25-nov-14	Phishing	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Financieel
			25-nov-14	Verdachte URL	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Financieel
10286			25-nov-14	Spam	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Onbekend
10310			26-nov-14	Defacement	Melding van defacement op website	Overige
10333	10332, 10339,		27-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij Rijksoverheidsorganisatie	Rijksoverheid
10341	10340		27-nov-14	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij organisatie in de gezondheidszorg	Gezondheidszorg
10345	10344, 10346, 10347,		27-nov-14	BGP hijack	Melding BGP Hijack.	Rijksoverheid

10365	10364, 10366, 10367,		28-nov-14	Hack	Hack bij dienstverlener gemeenten.	Gemeenten
10391	10390, 10392, 10423, 10443,		29-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
10395	10394, 10396, 10397, 10398, 10412,		30-nov-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een OSCP-responder	Rijksoverheid
10416	10371, 10420, 11307		1-dec-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
10422	10421, 10424, 10425, 10426, 10427, 10428, 10429, 10430, 10431, 10432, 10433, 10434, 10435, 10436,		1-dec-14	Geodo infecties	Melding met lijst van computer geïnfecteerd met Geodo	Meerdere
10438	10439, 10440,		1-dec-14	Verlopen certificaten gevonden.	Uitval OSCP-responder bij een CSP.	Overige
10442	10441		1-dec-14	NTD verzoek	Verzoek tot assistentie voor het doen van een NTD-verzoek.	Financieel
10459	10458, 10460, 10462, 10463, 10490,		2-dec-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een overheidspartij.	Rijksoverheid
10465	10464, 10466,		2-dec-14	Defacement website	Defacement website provinciale politieke partij.	Politieke Partijen
10467			2-dec-14	Lijst met domeinnamen en ipadressen	Lijst ontvangen met mogelijke hosting kinderporno.	Overige
10487	10486, 10488,		3-dec-14	Melding vanuit PKI-meldplicht	Melding van bevinding bij CSP. Private keys/pins/puks werden niet meer opgeschoond omdat een script niet draaide.	Overige
10525	10508, 10526,		5-dec-14	Geconstateerde kwetsbaarheid	RD-melding betreffende een lek in een website van een bemiddelingsbureau waarmee persoonsgegevens kunnen worden verkregen.	Overige
10528	10527, 10529,		5-dec-14	Zeus dropper	Verzoek tot assistentie voor het doen van een NTD-verzoek.	Telecom/ICT
10531	10530, 10532, 10699, 10700,		5-dec-14	Malware	Melding van mogelijke malwareinfecties bij de Rijksoverheid.	Rijksoverheid
10573	10572, 10574,		8-dec-14	Phishing-site	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Financieel
10592	10591, 10593, 10594,		9-dec-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank.	Financieel
10596	10595		9-dec-14	Mogelijke malwarebesmetting	Melding van mogelijke malware besmetting	Transport
10608	10607, 10609,		10-dec-14	Defacement	Melding van mogelijk defacement	Gezondheidszorg
10612	10611, 10613,		10-dec-14	Mogelijke hack	Mogelijke hack bij een organisatie.	Overige
10615	10614, 10616, 10645,		10-dec-14	Phishingactiviteit	Melding van Citadel-dropper.	Financieel
10677	10676, 10678, 10681, 10682,		15-dec-14	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij en van een gemeente.	Meerdere
10697	10696, 10698,		16-dec-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
10702	10701, 10703,		16-dec-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank.	Financieel
10704			16-dec-14	DDoS-aanval	Melding van DDoS-aanval gebruik makend van Nederlandse infrastructuur.	Overige
10706	10705, 10707,		16-dec-14	Mogelijke kwetsbaarheid	RD-melding mogelijke kwetsbaarheid emailserver	Rijksoverheid

10721	10720, 10722, 10810,		17-dec-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Financieel
10723			17-dec-14	Phishingactiviteit	Melding phishing-site Nederlandse bank.	Financieel
10725	10724, 10726, 10727, 10737, 10740,		17-dec-14	Phishingactiviteit	Melding van een phishingcampagne gericht op een organisatie.	Overige
10758	10757, 10759,		19-dec-14	Defacement	Melding defacement van website van een buitenlandse ambassade in Nederland.	Overige
10790	10789, 10792,		22-dec-14	Botnet C&C server	Melding van een botnet Command and Control server bij Nederlandse hoster.	Telecom/ICT
10794	10788, 10793, 10795,		22-dec-14	Malware	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Overige
10798	10796, 10799,		22-dec-14	Malware	Melding van malware op een server.	Financieel
10828	10827, 10829,		24-dec-14	Fraudulente activiteit	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Financieel
10832	10815, 10830, 10831, 10833,		24-dec-14	Malware	Melding vanuit een Nederlandse bank betreffende een email met malware	Financieel
10847	10846, 10848,		25-dec-14	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Financieel
10872	10871, 10873, 10874,		27-dec-14	Cryptoware	Melding van een cryptoware Command and Control server gehost in Nederland.	Overige
10887	10888, 10889, 10890,		29-dec-14	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in een systeem van een overheidspartij	Rijksoverheid
10902	10899, 10900, 10901,		30-dec-14	Potentiële backdoors	Melding van mogelijke compromittering van Nederlandse websites.	Telecom/ICT
10913	10912, 10914,		31-dec-14	Phishingactiviteit	Verzoek om assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Financieel
10927	10926		1-jan-15	Defacement van website	Melding defacement van een website van een evenement	Gemeenten
10929	10928, 10930, 10931,		1-jan-15	Fraudulente website	Verzoek om assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Financieel
10944	9804		2-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
10954	10953, 10955,		3-jan-15	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij een organisatie in de gezondheidssector	Gezondheidszorg
10968	10965, 10966, 10967, 10969		4-jan-15	Spambot	Melding dat een spambot probeerde om veel berichten op een CMS te plaatsen van een rijksoverheidswebsite, waardoor veel emails met moderator requests werden geproduceerd.	Rijksoverheid
10982	10981, 10983,		5-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure-melding over een mogelijke kwetsbaarheid in de website van een hostingbedrijf.	Telecom/ICT
10996	10995, 10997,		6-jan-15	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank.	Financieel
10999	10998, 11000,		6-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een systeem van een academische zorginstelling dat is blootgesteld aan het internet	Gezondheidszorg

11013	11012, 11014,		7-jan-15	Mogelijke compromittering accounts	Melding dat e-mails en accounts van een rijksoverheidsinstelling mogelijk zijn gecompromitteerd.	Rijksoverheid
11015	11016		7-jan-15	Online gezette gegevens van slachtoffers	Melding dat een hackersgroep een verzameling van al eerder uitgegeven gegevens online op heeft gezet op een tor-site.	Meerdere
11018	11017, 11019,		7-jan-15	Gecompromitteerde website	Melding Nederlandse website die gecompromitteerd is.	Telecom/ICT
11021	11022, 11023,		7-jan-15	XSS kwetsbaarheid + SSL problemen	Social media bericht met melding XSS en SSL issues op een website.	Overige
11037	11036, 11038, 11039,		8-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een gemeente.	Gemeenten
11041	11040, 11042, 11043, 11044,		8-jan-15	Phishingactiviteit	Melding van een phishingemail gericht op een overheidspartij.	Rijksoverheid
11046	11045, 11047,		8-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
11057			9-jan-15	Malware	Melding ontvangen over malwareverkeer	Onbekend
11060	11061, 11062,		9-jan-15	BGP hijack van IP-space	Melding van een hijack van een IP-blok behorend aan een buitenlands bedrijf door een Nederlands bedrijf.	Telecom/ICT
11076	11075, 11077,		10-jan-15	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek naar een Nederlandse hoster.	Overige
11103	11102, 11104, 11105,		12-jan-15	Gecompromitteerde credentials	Melding van gecompromitteerde credentials van Rijksoverheidsinstelling	Partners Rijksoverheid
11108	11109		12-jan-15	Hack	Social media-accounts gehacked.	Overige
11110	11107, 11111,		12-jan-15	Gecompromitteerde website	Melding Nederlandse website welke gecompromitteerd is	Telecom/ICT
11133			14-jan-15	Gecompromitteerde website	Melding Nederlandse website welke gecompromitteerd is.	Telecom/ICT
11134	11122, 11135, 11136, 11137,		14-jan-15	Unrestricted database access	Melding met lijst van publiek toegankelijke redis- en memcached-instanties in Nederland	Meerdere
11159	11154, 11208, 11209, 11212, 11213, 11214, 11215, 11216, 11217, 11218, 11219, 11220, 11221,		15-jan-15	Trojaninfecties	Melding met lijst van met malware besmette computers	Meerdere
11181	11180, 11182, 11230,		16-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Financieel
11222	11223, 11224, 11530, 11675,		16-jan-15	Afwijkend gedrag DDoS-appliance	DDoS-appliance vertoonde afwijkend gedrag.	Financieel
11226	11225, 11227, 11228,		16-jan-15	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank.	Financieel
11243	11242, 11244, 11245, 11370,		17-jan-15	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank.	Financieel
11250	11249, 11251,		18-jan-15	Verdachte URL	Er is melding gemaakt van een phishingpagina.	Financieel
11261	11260, 11262, 11263, 11276,		19-jan-15	Phishingactiviteit	Melding van een phishingcampagne gericht op een Nederlandse bank.	Financieel
11275	11274		20-jan-15	Malware	Melding met lijst van met malware besmette computers	Overige

11301	11302		21-jan-15	Mogelijke malwarebesmetting	NDS-allertering van mogelijke malwarebesmetting	Financieel
11310	11311, 11312,		22-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
11315	11314, 11316,		22-jan-15	Gerubriceerd document op overheidswebsite	Melding van een mogelijk gerubriceerd document wat publiek toegankelijk is via een overheidswebsite.	Rijksoverheid
11330	11329, 11331, 11332,		23-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over meerdere mogelijke kwetsbaarheden in websites van verschillende overheidspartijen.	Rijksoverheid
11333	11305, 11334,		23-jan-15	Lijst met IP-adressen en mogelijke root wachtwoorden	Lijst ontvangen met IP-adressen en bijbehorende logingegevens.	Telecom/ICT
11369			26-jan-15	DDoS-aanval	Melding DDoS-aanval op website niet-organisatie.	Overige
11372	11371, 11373, 11408, 11418,		26-jan-15	Phishingactiviteit	Mogelijke spearphishing aanval op verschillende overheidspartijen.	Rijksoverheid
11375	11374, 11376,		27-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de mailservers van een overheidspartij.	Rijksoverheid
11388	11387, 11389, 11395,		27-jan-15	Phishingactiviteit	Melding overheidspartij dat verschillende mensen binnen de organisatie gerichte phishingmails ontvangen.	Rijksoverheid
11425	11424, 11426,		29-jan-15	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in financiële sector	Financieel
11435	11420, 11436,		29-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een organisatie in de gezondheidszorg	Gezondheidszorg
11438	11437, 11609,		29-jan-15	Mogelijke spearphishingaanval	Melding mogelijke spearphishing aanval private partij.	Overige
11443	11442, 11444, 11445, 11511, 11743,		29-jan-15	Phishingactiviteit	NTD verzoek voor phishing-site gericht tegen organisatie in verzekeringssector	Verzekeringen
11461	11439, 11463, 11512,		30-jan-15	Mogelijke kwetsbaarheid	Melding kwetsbaarheid in software zoals gebruikt door gemeente.	Gemeenten
11479	11478, 11480,		31-jan-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
11508	11507		2-feb-15	Phishingactiviteit	Melding van phishingactiviteiten via oude overheidsdomeinen	Rijksoverheid
11525	11523		3-feb-15	Phishingactiviteit	Melding van mogelijke phishingactiviteiten.	Overige
11527	11526, 11528, 11531,		3-feb-15	Phishingactiviteit	Melding van phishingactiviteiten gericht tegen organisatie in financiële sector	Financieel
11542	11529, 11543,		4-feb-15	CRL Incident	Storing in CRL-systeem overheid-partij. Betreffende partij heeft bij het NCSC melding hiervan gemaakt samen met uitleg over maatregelen die ze hebben genomen.	Telecom/ICT
11544	11541, 11545,		4-feb-15	Phishingactiviteit	Melding van phishingactiviteiten gericht tegen organisatie in financiële sector	Financieel
11561	11559, 11560, 11562,		5-feb-15	Phishingactiviteit	Melding van phishingactiviteiten gericht tegen organisatie in financiële sector	Financieel
11571	11440, 11441,		6-feb-15	Phishingactiviteit	Melding organisatie in transportsector van phishingmails uit hun naam.	Transport

11573	11572, 11574,		6-feb-15	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD verzoek naar een Nederlandse hoster.	Financieel
11576	11575, 11577, 11578, 11608,		6-feb-15	Phishingactiviteit	Melding van phishingactiviteiten gericht tegen Rijksoverheid	Rijksoverheid
11580	11579, 11581,		6-feb-15	Phishingactiviteit	Melding van phishingactiviteiten gericht tegen organisatie in financiële sector	Financieel
11591	11590, 11592,		7-feb-15	Defacement van website	Melding compromittatie website van ziekenhuis.	Gezondheidszorg
11612	11610, 11614, 11615, 11616, 11617,		9-feb-15	Gecompromitteerde websites	Melding dat meerdere Nederlandse websites gecompromitteerd zijn.	Telecom/ICT
11613	11611, 11776,		9-feb-15	Openstaande database-servers	Lijst met mogelijk openstaande database-servers ontvangen.	Meerdere
11626	11625, 11627, 11645,		10-feb-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
11643	11642, 11644,		11-feb-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over een mogelijke kwetsbaarheid in de website van een overheidspartij.	Rijksoverheid
11647			11-feb-15	Verdachte activiteiten vanuit IP-adres	Melding van een partij over verdachte activiteiten vanuit een Nederlands IP-adres met het verzoek of het NCSC meer informatie heeft over dit IP-adres.	Financieel
11658	11649		12-feb-15	Phishingactiviteit	Melding private partij over phishing activiteiten uit hun naam.	Overige
11659	11624, 11648, 11660, 11661, 11663, 11709, 11712, 11740, 11741,		12-feb-15	DDoS-aanval	DDoS-aanval op website overheidspartij.	Rijksoverheid
11662			12-feb-15	DDoS-aanval	DDoS-aanval op website overheidspartij.	Rijksoverheid
11676			13-feb-15	Indicator of Compromise	Melding buitenlands CERT-team over een aanval op hun infrastructuur vanuit Nederlandse IP-adressen.	Overige
11711	11710, 11713, 11714,		16-feb-15	Phishingactiviteit	Verzoek tot assistentie voor het doen van een NTD-verzoek aan een Nederlandse hoster.	Telecom/ICT
11727	11726, 11728, 11729,		17-feb-15	Gecompromitteerde credentials	Melding dat credentials van overheidsinstelling en organisatie uit de transport-sector zijn gecompromitteerd	Meerdere
11745	11744, 11746,		19-feb-15	Defacement	Melding dat website buitenlandse ambassade is gecompromitteerd.	Overige
11773	11771, 11772, 11774,		20-feb-15	Mogelijke malwarebesmetting	Automatisch detectiesysteem; mogelijke malwarebesmetting.	Rijksoverheid
11778	11777, 11779, 11780, 11781, 11782, 11783, 11784,		20-feb-15	Kwetsbaarheid in software	Melding van kwetsbaarheid in software	Meerdere
11786	11785, 11788,		20-feb-15	Mogelijk kwetsbare systemen	Lijst ontvangen met IP-adressen van mogelijk kwetsbare, publiek toegankelijke systemen	Meerdere
11790	11789, 11791, 11792, 11793,		20-feb-15	Melding van openbare lijst met IP-adressen	Melding van lijst met IP-adressen in Nederland van publiek toegankelijke ICS/SCADA systemen.	Onbekend
11795	11794, 11796, 11797, 11973, 11987,		20-feb-15	Hack	Melding van een hack bij een telecom/ICT organisatie.	Telecom/ICT
11799	11798, 11800,		20-feb-15	Melding vanuit PKI-meldplicht	Melding vanuit PKI-meldplicht betreffende continuïteit OCSP-server	Telecom/ICT
11846	11845		24-feb-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding dat website geen bescherming biedt tegen mirroring.	Rijksoverheid

11858	11859, 11860,		25-feb-15	SIEM melding	Melding over verdacht netwerkverkeer	Rijksoverheid
11862	11861, 11863,		25-feb-15	Cryptoware	Melding over cryptoware infectie	Rijksoverheid
11864			25-feb-15	Cryptoware	Melding over cryptoware infectie	Rijksoverheid
11877	11876, 11883, 11884,		26-feb-15	Malware	Melding over een besmetting van een computer	Gemeenten
11878			26-feb-15	Lek website	Melding over een lek in een website	Websites
11880	11865, 11881, 11882, 12002, 12023, 12024, 12151, 12209, 12346, 12351, 12352, 12353, 12354, 12355, 12678, 12697,		26-feb-15	Ramnit sinkhole	Indicators of compromise aangeboden door partner.	Meerdere
11886	11885, 11887,		26-feb-15	Kwetsbaarheid in NTP-server	Melding van een kwetsbare NTP-server die mee heeft gedaan in een DDoS-aanval	Onbekend
11898			27-feb-15	Spam	Melding dat medewerker e-mail heeft ontvangen met een malware executable	Rijksoverheid
11899			27-feb-15	Cryptoware	Informatie over cryptoware besmettingen bij gemeenten	Gemeenten
11903	11902, 11904, 11942		27-feb-15	Hack	Melding van hack bij organisatie in telecom/ICT sector.	Telecom/ICT
11907	11906, 11908,		27-feb-15	Gecompromitteerde credentials	Melding van gecompromitteerde credentials van financiële instelling	Financieel
11921	11920, 11922, 11923,		28-feb-15	Phishingactiviteit	Verzoek om assistent bij neerhalen phishing pagina	Financieel
11924			28-feb-15	Defacement website	Melding over defacement op website	Onderwijs
11944	11943, 11945, 11960,		1-mrt-15	Mogelijke kwetsbaarheid	Melding van kwetsbaar SCADA-systeem	Transport
11956	11955, 11957, 11958, 11959,		2-mrt-15	Gecompromitteerde servers	Melding van besmette systemen	Onbekend
11971	11972		3-mrt-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding van XSS-kwetsbaarheid in overheidswebsite	Provincies
11989	11988		4-mrt-15	Cryptoware	Melding over cryptoware infectie	Waterschap
11990			4-mrt-15	Malware	Buitenlands hulpverzoek voor website met malware in Nederland	Telecom/ICT
11991			4-mrt-15	Mogelijk incident	Melding van mogelijk incident bij een overheidsorganisatie.	Rijksoverheid
12006	12004		5-mrt-15	Cryptoware	Melding van diverse cryptoware infecties die bestanden versleuteld hebben	Rijksoverheid
12012	12011, 12013,		5-mrt-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding van XSS-kwetsbaarheid in bij onderwijsinstelling	Onderwijs
12025			7-mrt-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding SQL injection-kwetsbaarheid	Media
12051			9-mrt-15	Stacktrace website	Responsible Disclosure melding over overheidswebsite die teveel informatie teruggeeft	Rijksoverheid
12052			9-mrt-15	Cryptoware / ransomware	Cryptoware/ransomware besmettingen bij overheidsinstelling.	Rijksoverheid
12054	12053		9-mrt-15	Cryptoware	Melding over cryptoware infectie	Rijksoverheid
12063			10-mrt-15	Gecompromitteerde credentials	melding van gecompromitteerde credentials van organisatie in de gezondheidszorg	Gezondheidszorg
12068	11974, 12067,		10-mrt-15	Cryptoware	Melding over cryptoware infectie	Rijksoverheid
12070			10-mrt-15	Cryptoware	Melding over cryptoware infectie	Gezondheidszorg
12071	12072		10-mrt-15	Cryptoware	Melding over cryptoware infectie	Gezondheidszorg
12073			10-mrt-15	Defacement	Melding van defacement van website	Onderwijs
12085			11-mrt-15	Cryptoware	Melding over cryptoware infectie	Rijksoverheid
12087	12086, 12088,		11-mrt-15	DNS requests	Diverse NDS-allertingen op DNS requests	Rijksoverheid
12091	12090		11-mrt-15	Melding van DDoS-aanval	melding van een DDoS-aanval	Financieel

12092			11-mrt-15	Kwetsbaarheid in product	Melding over gevonden kwetsbaarheid in softwareproduct	MSP
12093			11-mrt-15	Gelekte gegevens	Melding dat credentials van overheidsinstelling zijn gecompromitteerd	Rijksoverheid
12107	12106		12-mrt-15	Cryptoware	Melding cryptoware besmetting	Drinkwater
12108	12105		12-mrt-15	Cryptoware	Melding cryptoware besmetting	Rijksoverheid
12110	12109		12-mrt-15	Phishingactiviteit	Melding dat mailbox van medewerker is misbruikt voor het versturen van spam	Rijksoverheid
12125	12123		13-mrt-15	Hackpogingen en ongewenste e-mails	Melding van server die actief op zoek gaat naar kwetsbaarheden om spam te versturen	Onbekend
12126	11900, 12124, 12243, 12244, 12335,		13-mrt-15	Mogelijke spearphishing-aanval	Indicators of compromise verkregen van partner over een mogelijke spearphishing-aanval.	Rijksoverheid
12133	12128, 12134,		13-mrt-15	Cryptoware	Melding cryptoware besmetting	Rijksoverheid
12135	12131, 12132, 12408,		14-mrt-15	Cryptoware	Melding cryptoware besmetting	Rijksoverheid
12180	11152, 11546,		16-mrt-15	Malware ontvangen	Malware ontvangen.	Overige
12181	12182		16-mrt-15	Cryptoware	Melding Ransomware Malware	Telecom/ICT
12186	12187, 12188, 12189, 12262,		16-mrt-15	Fraude	Melding van valse webshops	Rijksoverheid
12190	12191		16-mrt-15	Cryptoware	Melding cryptoware besmetting	Gezondheidszorg
12193	12194		16-mrt-15	Cryptoware	Melding cryptoware besmetting	Gezondheidszorg
12195	12196		16-mrt-15	Cryptoware	Melding cryptoware besmetting	Gemeenten
12197	12198		16-mrt-15	Cryptoware	Melding cryptoware besmetting	Financieel
12213	12212, 12214,		17-mrt-15	Cryptoware	Melding cryptoware besmetting	Rijksoverheid
12216	12215		17-mrt-15	Cryptoware	Melding cryptoware besmetting	Gemeenten
12217	12218, 12219, 12220, 12221,		17-mrt-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12222	12223, 12224, 12225,		17-mrt-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12259	12258, 12260, 12261, 12263,		20-mrt-15	Malafide SSL-certificaat	Melding van malafide SSL-certificaat in omloop voor internetprovider	Telecom/ICT
12285	12284		22-mrt-15	Cryptoware	Melding mogelijke cryptoware besmetting	Rijksoverheid
12286			23-mrt-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over kwetsbaarheid in website	Overige
12297	12296, 12298,		23-mrt-15	Mogelijke defacement van website	Melding van mogelijke defacement website.	Gezondheidszorg
12299	12300		23-mrt-15	Mogelijke defacement van website	Melding van mogelijke defacement website.	Gezondheidszorg
12313	12312, 12314,		24-mrt-15	Openbaar gemaakte credentials	Credentials van medewerker rijksoverheid openbaar gemaakt.	Rijksoverheid
12315	12316, 12317,		24-mrt-15	Malware	Melding van verspreiding van malware via website	Websites
12337	12336, 12338,		25-mrt-15	Malware	Melding van verspreiding van malware via website	Websites
12340	12339, 12345,		25-mrt-15	Phishingactiviteit	Melding dat vermoedelijk phishing e-mails zijn verstuurd	Rijksoverheid
12343	12341, 12344,		25-mrt-15	Mailboxhack	Melding dat mailbox van medewerker is gebruikt voor het versturen van spam	Rijksoverheid
12347	12150		25-mrt-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12368	12367, 12369, 12370,		26-mrt-15	Phishingactiviteit	Melding van phishingactiviteiten	Financieel
12373	12372, 12374, 12396, 12460,		26-mrt-15	Fraude	Melding van frauduleuze e-mails vanuit Rijksoverheidsorganisatie	Rijksoverheid
12386	12385, 12387, 12388,		27-mrt-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Telecom/ICT
12390	12389, 12391, 12392,		27-mrt-15	Brute Force aanvallen	Melding van Brute-Force aanvallen op webmail omgeving	Rijksoverheid
12423	11313		30-mrt-15	Phishingactiviteit	Melding van phishingactiviteiten	Websites
12434	12433, 12435, 12436, 12458, 12471, 12472,		31-mrt-15	Melding vanuit PKI meldplicht	Melding over foutieve uitgifte van certificaat.	Telecom/ICT

12439	12437, 12438, 12448, 12449, 12716, 13023, 13024,		31-mrt-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over pen directory bij een ambassade in Nederland	Overige
12451	12450, 12452, 12453,		1-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12455	12454, 12457,		1-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12456	12426, 12427, 12428,		1-apr-15	Melding van harddisk met data	Melding van aangetroffen harde schrijf met gegeven	Overige
12475	12474, 12476,		3-apr-15	Website vertoont vreemde tekens	Korte tijdelijke verstoring door update	Rijksoverheid
12477			3-apr-15	Defacement website	Melding over defacement op website	Media
12540	12539, 12541,		9-apr-15	Hack	Melding over hack bij een mediabedrijf	Media
12544	12543, 12545,		9-apr-15	Cryptoware	Melding cryptoware besmetting	Rijksoverheid
12547	12546, 12548,		9-apr-15	Cryptoware	Melding cryptoware besmetting	Gemeenten
12562	12552, 12563,		10-apr-15	Verkeerde omgang met certificaten.	Certificaat gevonden in een browserextensie.	Rijksoverheid
12576	12575, 12577,		11-apr-15	Cryptoware	Melding van cryptowareverspreiding via website	Financieel
12599	12598, 12600,		14-apr-15	Defacement website	Melding van defacement op website	Websites
12614	12613		15-apr-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over BEAST kwetsbaarheid in website	Rijksoverheid
12627	12628, 12629,		15-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Telecom/ICT
12640	12031		16-apr-15	Cryptoware	Melding cryptoware besmetting	Rijksoverheid
12657	12655		17-apr-15	Malware-onderzoek	Mogelijke besmetting werkstation	Rijksoverheid
12665	12664, 12666,		17-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12700	12699, 12701,		20-apr-15	Mogelijke kwetsbaarheid	Twee responsible disclosure meldingen ontvangen	Rijksoverheid
12702	12698, 12703, 12704,		20-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12714	12713		20-apr-15	Adressen e-mail/ hash dump	Credentials gepubliceerd van partij in onderwijs sector	Onderwijs
12729	12425		20-apr-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding over kwetsbaarheid in mobiele handelsplatforms	Overige
12741	9657		21-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Energie
12742	9668		21-apr-15	Accountgegevens openbaar gemaakt	Accountgegevens behorend bij Rijksoverheids-organisatie openbaar gemaakt.	Rijksoverheid
12743	9711		21-apr-15	DDoS-aanval	Systeem in Nederland mogelijk betrokken bij DDoS-aanval.	Websites
12744	9720		21-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12745	9736		21-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Financieel
12746	9797		21-apr-15	Mogelijke malwarebesmetting	Indicators of compromise verkregen van organisatie over mogelijke malwarebesmetting.	Energie
12747	9807		21-apr-15	Security vulnerability	Responsible Disclosure melding over BEAST kwetsbaarheid in website	Rijksoverheid
12748	12749, 12750,		21-apr-15	Melding cryptolocker besmettingen	Melding van bestemmingen met cryptolocker	Rijksoverheid
12751	11211		21-apr-15	Trojan infecties	Melding van trojan-bestemming in Nederland	Financieel
12754	12753, 12755,		21-apr-15	DDoS-aanval	Verzoek om assistentie bij DDoS-aanval	Overige
12758	9533		22-apr-15	phishingactiviteit	Verzoek om assistentie bij phishing site	Financieel
12768	9354		22-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12770	9445		22-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12771	9532		22-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12772	9534		22-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12773	9535		22-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12774	9549		22-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12776	9442		22-apr-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding van diverse kwetsbaarheden	Rijksoverheid
12777	9492		22-apr-15	Gevonden bug	Responsible Disclosure melding over BEAST kwetsbaarheid in website	Rijksoverheid

12778	9619		22-apr-15	Mogelijke kwetsbaarheid	Responsible Disclosure melding van XSS-kwetsbaarheid in website	Websites
12779	6559		22-apr-15	NDS-allertering	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12780	6573		22-apr-15	Mogelijk compromittatie server	Melding mogelijke compromittatie van server	MSP
12781	6655		22-apr-15	DDoS-aanval	Melding van DDoS-aanval	Rijksoverheid
12783	6692		22-apr-15	Host met vals SSL-certificaat in .nl	Melding opvallend SSL-certificaat op Nederlandse website	Websites
12785	6797		22-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Websites
12786	8510		22-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12787	11229		22-apr-15	Malware infectie	Melding trojan-besmetting in Nederland	Overige
12789	11246		22-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Overige
12790	11247		22-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Overige
12791	8763		22-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Rijksoverheid
12792	6666		22-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Rijksoverheid
12793	6665		22-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Rijksoverheid
12795	12794, 12801, 12840, 12841, 13124,		22-apr-15	Spearphishing	Melding mogelijke spearphishing aanval	Chemisch en Nuclear
12796	11303		22-apr-15	Cryptoware	Melding cryptoware besmetting	Gemeenten
12797	11422		22-apr-15	Mogelijke besmetting met netwiredRC RAT	Melding mogelijke besmetting met Remote Access Toolkit	Rijksoverheid
12798	11001		22-apr-15	Melding van Malware	Melding over malware gehost op Nederlandse server	Websites
12799	11462		22-apr-15	Defacement	Melding defacement van website	Websites
12800	11056		22-apr-15	DDoS-aanval	Melding van DDoS-aanval	Rijksoverheid
12823	8540		23-apr-15	Mogelijke malwarebesmetting	Melding van mogelijke malwarebesmetting bij partij in transportsector.	Transport
12824	8559		23-apr-15	Phishingactiviteit	Verzoek tot ondersteuning bij phising website	Websites
12825	8588		23-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12826	8642		23-apr-15	NDS-melding	Melding vanuit het Nationaal Detectie Systeem	Rijksoverheid
12838	8042		24-apr-15	Melding betreffende 'forward secrecy is disable'	Responsible Disclosure melding betreffende 'forward secrecy'	Rijksoverheid
12843	12842, 12844, 12845,		25-apr-15	Mogelijke malwareverspreiding	Melding mogelijke malwareverspreiding via websites	Media
12847	12717		25-apr-15	Adressen e-mail/ hash dump	Credentials gepubliceerd van partij in gezondheidszorg	Gezondheidszorg
12849	12848, 12850, 12861, 12862, 12863,		25-apr-15	Malwareverspreiding	Malwareverspreiding via e-mail.	Onbekend
12877	8224, 8225,		26-apr-15	DDoS-aanval	Melding van DDoS-aanval	Financieel
12905	12906		28-apr-15	DDoS-aanval	Melding van DDoS-aanval	Verzekeringen
12908	12566		28-apr-15	Probleem met app	Responsible Disclosure melding over kwetsbaarheden in app	Rijksoverheid
12969	7325		30-apr-15	Phishingactiviteit	Melding van phishingactiviteiten op website	Websites
7902		A				
9800	9799, 9801, 9802,	A				
10305	10306, 10307, 10308, 10349, 10683, 10979, 10980, 11273, 11708,	A				
10445	10444, 10446,	A				
11150	11149, 11151,	A				
12026		A				
12129	12127, 12130,	A				
12184	12183, 12185,	A				

Uitzonderingsgronden:	Uitleg:
A	Informatie die een lopend onderzoek van politie/justitie zou doorkruisen; deze wordt geweigerd op grond van art. 10 lid 2 sub c Wob.