]HackingTeam[

# Remote Control System

## Exploits Specifications

THIS DOCUMENT IS STRICTLY CONFIDENTIAL

# Index

⚠ **Disclaimer Note:** The actual exploits duration is unpredictable, due to the nature of the exploit itself, however Hacking Team offers different solutions to its customers including other exploits available at the moment and other infection vectors

# Objectives

As a result of the release of new stealth, powerful and reliable exploits targeting Microsoft Internet Explorer, we ask you to read the following specifications for a correct and successful use of the exploits themselves.

# 1 Exploit for Internet Explorer

## Exploit requirements

- **Exploit License**
- **Internet Explorer 6,7,8,9,10 - 32bit (default installed version)**
- **Windows XP, Vista, 7 , Windows 8 (32/64 bit)**
- **Adobe Flash v11.1.102.55 or above for Internet Explorer**
- **Microsoft Office Word 2007/2010/2013 OR Java 6.x/7.x plugin for IE must be installed on the system (for Windows 8 Java plugin for IE must be installed)**

***Notes:***

- If some of the above requirements are not met, the agent will not be installed, while the website is correctly displayed
- No alert message is displayed when accessing the exploiting website, no user interaction is required, only browsing the infecting URL
- All the infections are one-shot: the exploiting website will try to infect only the first user that browses it; all subsequent visitors will see the site's content with no exploit.

# 2 How to deliver the exploit

Hacking Team offers three different ways to deliver the IE exploit

## 2.1 Hosted

We offer our anonymous network infrastructure to host a fake website that will infect the target and then redirect to a chosen website(e.g.http://www.cnn.com).

### The client sends us

- Silent Installer
- URL to redirect the user to (optional)

### We send to the client

- a one-shot URL that must be sent to the target

## 2.2 Custom Website Hosted

We offer our anonymous network infrastructure to host a fake website prepared by the client that will infect the target.

### The client sends us

- Silent Installer
- HTML code for the fake website

### We send to the client

- a one-shot URL that must be sent to the target

## 2.3 Custom website hosted by the client

Client's infrastructure will be used to host a fake website that will infected the target. Our anonymous network infrastructure will be used to host only the exploits components.

### The client sends us

- Silent Installer
- URL where the client's fake website will be hosted

### We send to the client

- A zip file with the HTML that must be integrated into the client's fake website

# 3 Hints

- **The HTML code could be**

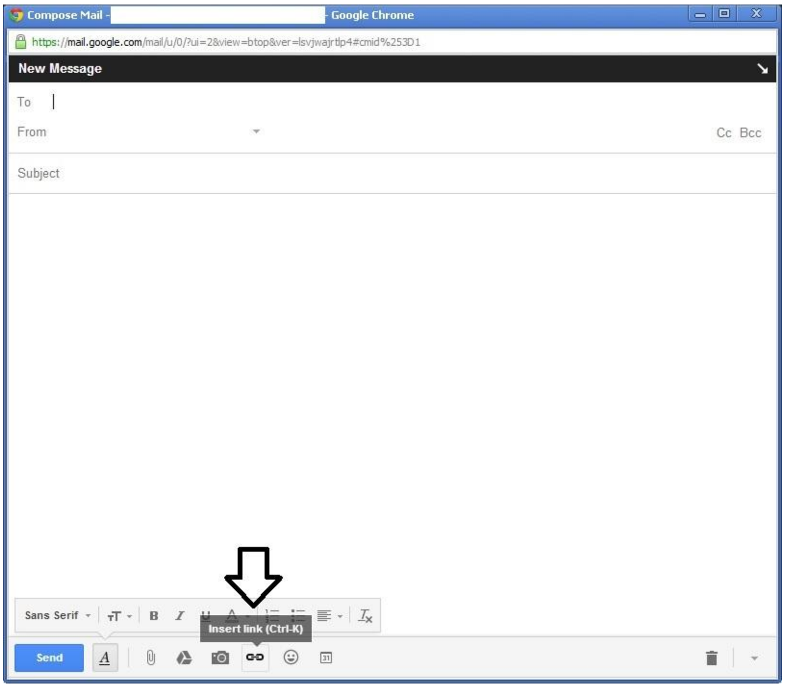
```
<html>
        <head></head>
        <body>
                Here's the link you are waiting for:
              <ahref="http://IP_ADDRESS_FOR_EXPLOIT/documents/zjqiaphk/9j03
ny8lnnys.html">http://URL_VIEWED_BY_TARGET/news/162456</a>
       </body>
</html>
```

where href is the attribute which specifies the link's destination and where the target downloads the exploit, even if the targets cannot see it, but only the URL specified (ex. cnn.com, google.com, etc)

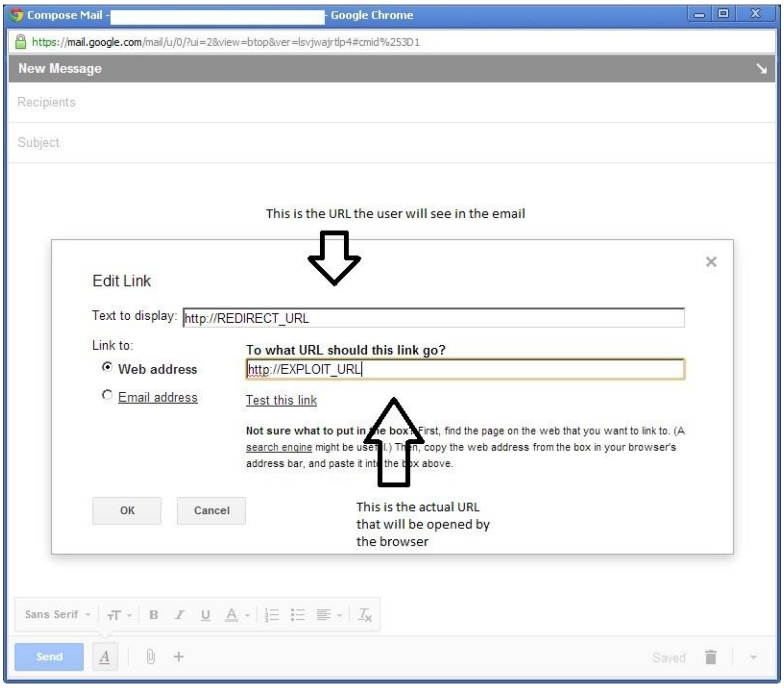
- **For delivering it, we suggest you to create an html e-mail with an hyperlink to this URL, because the URL might arouse suspicious**

- **Furthermore you can create an html email directly from gmail.com**

    - In order to do it there are some simple steps:
        - Connect to gmail
        - Push the "compose" button
        - Click on the button with a chain icon: "Insert link" or press Ctrl-K


Compose Mail - Google Chrome
https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=lsvjwajrtlp4#cmid%253D1
New Message
To
From
Cc Bcc
Subject
Sans Serif
Insert link (Ctrl-K)
Send

- Write the URL of the site where you want to redirect the target on the field: "Text to display:" and write the exploit URL received from us on the field "Web address"



Compose Mail - [redacted] Google Chrome

https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=lsvjwajrtlp4#cmid%253D1

New Message

Recipients

Subject

This is the URL the user will see in the email

Edit Link

Text to display: http://REDIRECT_URL

Link to:

● Web address

○ Email address

To what URL should this link go?

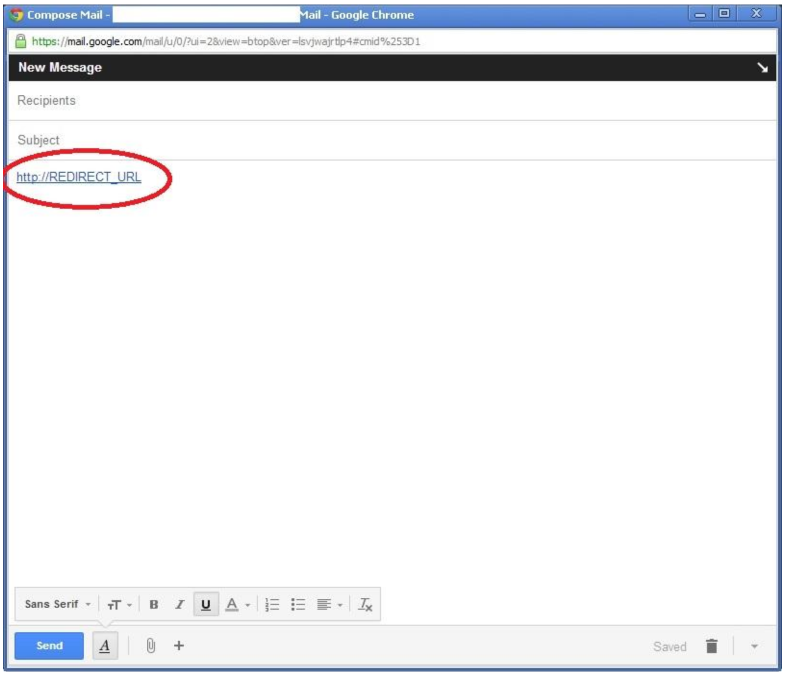
http://EXPLOIT_URL

Test this link

**Not sure what to put in the box?** First, find the page on the web that you want to link to. (A search engine might be useful.) Then, copy the web address from the box in your browser's address bar, and paste it into the box above.

OK Cancel

This is the actual URL that will be opened by the browser



Compose Mail - [redacted]Mail - Google Chrome

https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=lsvjwajrtlp4#cmid%253D1

New Message

Recipients

Subject

http://REDIRECT_URL

# 4 How it works

When the website is opened through IE the vulnerability is exploited, then the agent is downloaded from HT anonymous network infrastructure.

The agent is installed after the first user logout/login. Wait 5 minutes after the login (in order to start the agent is waiting for user input, so the counter will start at the first user input) and then the scout will syncronize. After the first sync it is possible to proceed to upgrade the agent from scout to elite. Then wait 20 minutes for the next sync. The time of the subsequent synchronizations will match the configuration made on RCS console.

This exploit is one-shot.