]HackingTeam[

Remote Control System

Exploits Specifications

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 Word and Power Point, we ask you to read the following specifications for a correct and successful use of the exploits themselves.

1 Exploit for Microsoft Word and Power Point

Supported Versions:	
	Microsoft Office
	2007
	2010
	2013
	Adobe Flash
	v11.1.102.55 or above for Internet Explorer
Document extensions	
	docx
	ppsx

1.1 How it works

Requirements:

- Exploit license
- Scout generated from the factory of the designated target
- Document (docx, ppsx) to use for the infection

When the file (Word or Power Point) is opened 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: the document will try to exploit the vulnerability and infect the target only the first time it is opened; all subsequent times only a document with no exploit will be opened.

Notes:

With Office 2007 the target has to choose the option "I recognize the content. Allow it to play"

2 Download the exploit from internet

When you download a file using a modern browser the file is tagged as coming from internet and that's why MS Office opens it using **Protected Mode**.

Protected Mode for Microsoft Office is a security feature that opens documents coming from potentially risky locations, like Internet, in read-only mode and with active content disabled.

A simple way to get around this problem is sending the document in a rar container.

This way the .rar file will be tagged as coming from internet but the file contained in the archive won't be tagged.
That behavior is not related with the exploit itself, it is Windows standard procedure when opening a document downloaded from the internet.

2.1 Best Practices:

- Send it in a **.rar** file over the Internet
- Use **usb key** or **other external devices**