Turla Mosquito行动的发展趋势分析

2018年5月29日发布

导语：ESET研究人员观察到臭名昭著的间谍组织Turla发生了重大变化。

Turla是一个臭名昭着的间谍组织，至少已经活跃了十年。它在2008年攻击美国国防部时被曝光[1]。此后，Turla涉及了多起政府和国防工业等敏感企业的安全事件[2]。

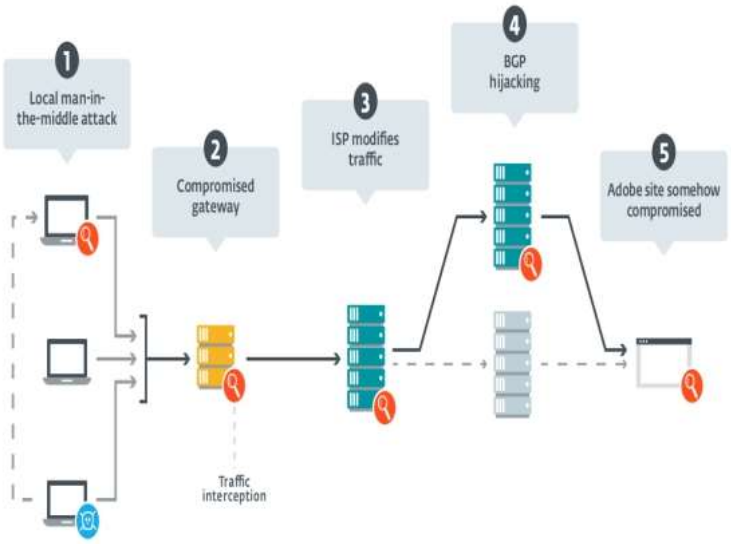
我们2018年1月的白皮书[3]首次公开分析了Turla Mosquito行动。我们还公布了IoC指标[4]。从那以后，Mosquito行动一直非常活跃，攻击者一直在忙着改变策略，尽可能隐身。

从2018年3月开始，我们观察到该行动发生了重大变化：现在它利用开源开发框架Metasploit，放弃了定制的Mosquito后门。当然，这并不是Turla第一次使用通用工具。过去，我们已经看到了使用开源的口令dump工具，如Mimikatz。然而，据我们所知，这是Turla首次将Metasploit用作第一阶段后门，而不是依靠自己的工具，如Skipper [5]。

传播

正如我们之前的分析[3]所描述的那样，典型的Mosquito行动其攻击媒介仍然是一个伪装的Flash安装程序，实际上其安装了Turla后门和合法的Adobe Flash Player。其典型的目标仍然是东欧的使领馆。

我们展示了当用户通过HTTP从get.adobe.com下载Flash安装程序时发生的危害。在终端和Adobe服务器之间的节点上截获流量，Turla的运营者用木马化版本替换了合法的Flash可执行文件。下图显示了理论上可以拦截流量的不同节点。请注意，我们认为可以排除第五种可能性，因为就我们所知Adobe/Akamai没有受到危害。

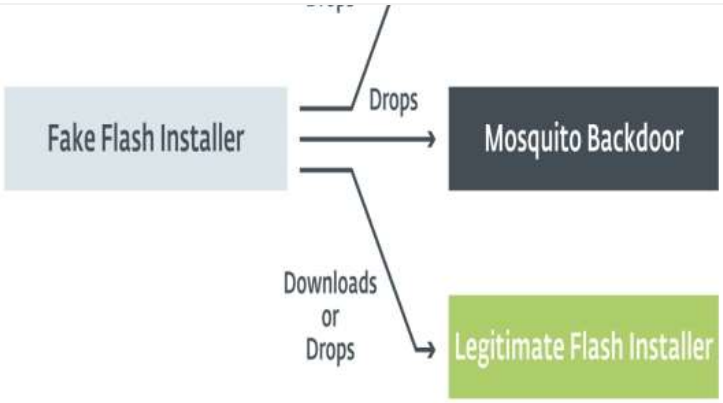


尽管后来发现无法拦截流量，但我们发现了一个仍在模拟Flash安装程序的新可执行文件，名为flashplayer28_xa_install.exe。因此，我们认为最早的攻击方法仍在使用中。

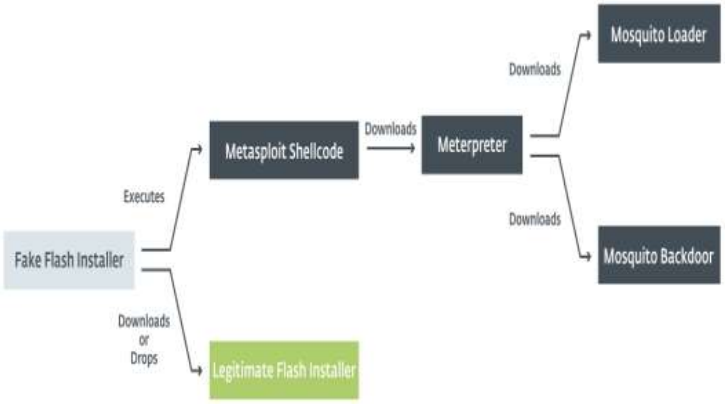
分析

在2018年3月初，作为定期追踪Turla的一部分，我们观察到了Mosquito行动的一些变化。尽管他们没有采用开创性的技术，但这是Turla战术、技术和程序（TTPs）的重大转变。

以前，感染链是一个伪装的Flash安装程序释放一个加载程序和主后门。如下图所示：



最近，我们观察到最终后门投放的方式发生了变化。Turla的行动仍然依赖伪装的Flash安装程序，但不是直接释放这两个恶意DLL，而是执行Metasploit shellcode，并从Google Drive中下载合法Flash安装程序并安装。之后，shellcode下载一个Meterpreter，这是一个典型的Metasploit有效载荷[6]，允许攻击者控制被入侵的机器。最后，机器可能会收到典型的Mosquito后门。下图总结了新的过程。



由于使用了Metasploit，我们猜测操作人员会手动进行利用过程。攻击的时间框架相对较短，因为最后的后门在入侵开始后的三十分钟内被投放。

shellcode是一个典型的Metasploit shellcode，使用shikata_ga_nai编码器[7]进行七次迭代保护。下面的屏幕截图显示了编码和解码的有效载荷。

```
seg000:00000000              fcmovb  st, st(2)
seg000:00000002              fnstenv byte ptr [esp-0Ch]
seg000:00000006              mov     edx, 4F90B585h
seg000:0000000B              pop     ebp
seg000:0000000C              sub     ecx, ecx
seg000:0000000E              mov     cl, 83h
seg000:00000010              add     ebp, 4
seg000:00000013              xor     [ebp+13h], edx
seg000:00000016              add     edx, eax
seg000:00000018              cmpsb
seg000:00000019              jb      short near ptr 0FFFFFFD5h
seg000:0000001B              bound   edi, [eax-1FACFD5Eh]
seg000:00000021              xchg    dl, [edi+37h]
seg000:00000025              std
seg000:00000026              cmp     eax, 0BD4CFEEEh
seg000:0000002B              rol     dword ptr [edx-44h], 3Dh
seg000:0000002F              arpl    [eax+41h], dx
seg000:00000032              adc     dword ptr [edi], 64h ; 'd'
seg000:00000035              neg     dword ptr ds:0E7A3BEE3h[ecx*2]
seg000:0000003C              retn
```

```
seg000:0000018D                 push    ebx
seg000:0000018E                 push    ebx
seg000:0000018F                 push    ebx
seg000:00000190                 push    edi
seg000:00000191                 push    ebx
seg000:00000192                 push    esi
seg000:00000193                 push    3B2E55EBh       ; HttpOpenRequest
seg000:00000198                 call    ebp
seg000:0000019A                 xchg    eax, esi
seg000:0000019B                 push    0Ah
seg000:0000019D                 pop     edi
seg000:0000019E
seg000:0000019E loc_19E:                                ; CODE XREF: seg000:000001CF↓j
seg000:0000019E                 push    3380h
seg000:000001A3                 mov     eax, esp
seg000:000001A5                 push    4
seg000:000001A7                 push    eax
seg000:000001A8                 push    1Fh
seg000:000001AA                 push    esi
seg000:000001AB                 push    869E4675h       ; InternetSetOptionA
seg000:000001B0                 call    ebp
seg000:000001B2                 push    ebx
seg000:000001B3                 push    ebx
seg000:000001B4                 push    ebx
seg000:000001B5                 push    ebx
seg000:000001B6                 push    esi
seg000:000001B7                 push    7B18062Dh       ; HttpSendRequestA
seg000:000001BC                 call    ebp
```

一旦shellcode被解码，它会通过https://209.239.115 [.] 91/6OHEJ联系C＆C，指导下载另一阶段的shellcode。根据遥测技术，我们确定下一个阶段是Meterpreter。该IP地址已被指向之前看到的Mosquito的C＆C域名psychology-blog.ezua [.] com，该域名于2017年10月正式解析。

最后，伪装的Flash安装程序从Google Drive URL下载合法的Adobe安装程序，然后执行该安装程序，让用户认为所有内容都正确无误。

其它工具

除了新的伪Flash安装程序和Meterpreter，我们还观察到其他几个被使用的工具。

• 一个只包含Metasploit shellcode的自定义可执行文件，用于维护对Meterpreter会话的访问。它被保存到：C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\msupdateconf.exe，开机自启动。

• 另一个用于执行PowerShell脚本的自定义可执行文件。

• 使用Google Apps脚本作为C&C服务器的Mosquito JScript后门程序。

• 使用Metasploit模块ext_server_priv.x86.dll [8]进行权限提升。

总结

本文介绍了过去几个月Turla Mosquito行动的发展趋势。我们观察到的主要变化是使用开源渗透测试项目Metasploit作为定制Mosquito后门的第一阶段。这对防御针对涉及Turla的攻击事件做出事件响应可能有参考价值。

C&C

· https://209.239.115[.]91/6OHEJ

· https://70.32.39[.]219/n2DE3

合法Flash installer的链接

· https://drive.google[.]com/uc?authuser=0&id=1s4kyrwa7gCH8I5Z1EU1IZ_JaR48A7UeP&export=download

IoCs

Filename	SHA1	SHA256	ESET detection name
flashplayer28_xa_install.exe	33d3b0ec31bfc16dcb1b1ff82550aa17fa4c07c5	f9b83eff6d705c214993be9575f8990aa8150128a815e849c6faee90df14a0ea	Win32/TrojanDownloader.Agent.DWY trojan
msupdateconf.exe	114c1585f1ca2878a187f1ce7079154cc60db7f5	1193033d6526416e07a5f20022cd3c5c79b73e8a33e80f29f9b06cdc3cb12e26	Win32/Turla.DH trojan
msupdatesmal.exe	994c8920180d0395c4b4eb6e7737961be6108f64	6868cdac0f06232608178b101ca3a8afda7f31538a165a045b439edf9dadf048	Win32/Turla.DH trojan

参考文献

[2] MELANI, "Technical Report about the Malware used in the Cyberespionage against RUAG," 25 09 2016. [Online]. Available: https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html.

[3] ESET, "Diplomats in Eastern Europe bitten by a Turla mosquito," ESET, 01 2018. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2018/01/ESET_Turla_Mosquito.pdf.

[4] ESET, "Mosquito Indicators of Compromise," ESET, 09 01 2018. [Online]. Available: https://github.com/eset/malware-ioc/tree/master/turla#mosquito-indicators-of-compromise.

[5] M. Tivadar, C. Istrate, I. Muntean and A. Ardelean, "Pacifier APT," 01 07 2016. [Online]. Available: https://labs.bitdefender.com/wp-content/uploads/downloads/pacifier-apt/.

[6] "About the Metasploit Meterpreter," [Online]. Available: https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/.

[7] "Unpacking shikata-ga-nai by scripting radare2," 08 12 2015. [Online]. Available: http://radare.today/posts/unpacking-shikata-ga-nai-by-scripting-radare2/.

[8] "meterpreter/source/extensions/priv/server/elevate/," Rapid7, 26 11 2013. [Online]. Available: https://github.com/rapid7/meterpreter/tree/master/source/extensions/priv/server/elevate.

TRex
这个人很懒，什么也没留下
发私信




发表评论

昵称 请输入昵称

邮箱 请输入邮箱地址

发表评论