赛门铁克称 WannaCry 与黑客组织 Lazarus 有关，但没提朝鲜

2017-05-24 李勤 宅客频道

宅客频道消息，5月23日，宅客频道收到赛门铁克公司发来的一则消息，**称勒索软件 WannaCry 攻击事件中使用的工具和基础设施与 Lazarus 有着紧密联系。**该团伙曾对索尼影业公司进行摧毁性攻击，还曾从孟加拉央行盗取8100万美元。

宅客频道了解到，此前，网传 Lazarus 幕后有朝鲜的支持，是一“朝鲜黑客组织”，但是，赛门铁克称，**WannaCry 攻击事件并不具有民族或国家所资助活动的特点，更像是典型的网络犯罪活动。**

以下是赛门铁克对此的具体分析报告：

在5月12日WannaCry全球性爆发前，其早期版本(Ransom.Wannacry) 曾在二月、三月和四月份用以执行少量目标性攻击。早期版本的WannaCry和2017年5月的版本基本相同，只是传播方式有所差别。

赛门铁克安全响应团队对WannaCry早期攻击进行了分析，发现网络攻击者所使用的工具、技术和基础设施与之前Lazarus攻击时间中所见到的有大量共同点，这说明Lazarus极有可能就是传播WannaCry的幕后黑手。

尽管与Lazarus有关联，但WannaCry攻击事件并不具有民族或国家所资助活动的特点，更像是典型的网络犯罪活动。这些早期版本的WannaCry使用盗取的认证信息在网络中传播，而不是利用泄露的 “永恒之蓝” 利用工具。“永恒之蓝”导致WannaCry于5月12日期快速在全球范围扩散。

关系总结

在WannaCry于二月份的首次攻击之后，我们在受害者网络上发现了与Lazarus有关恶意软件的三个组成部分：Trojan.Volgmer和Backdoor.Destover的两个变体，后者是索尼影业公司攻击事件中所使用的磁盘数据清除工具。

Trojan.Alphanc用以在三月和四月份中传播WannaCry，该病毒是Backdoor.Duuzer的修正版，而Backdoor.Duuzer之前与Lazarus有所关联。

Trojan.Bravonc与Backdoor.Duuzer和Backdoor.Destover使用相同的IP地址以进行命令和控制，而后两者均与Lazarus有所关联。

Backdoor.Bravonc的代码混淆方法和WannaCry与Infostealer.Fakepude（与Lazarus有所关联）相似。

而且，WannaCry和之前与Lazarus相关的Backdoor.Contopee之间存在共享代码。

二月份的攻击

2017年2月10日，赛门铁克发现了WannaCry在网络中作乱的首个证据，当时有一家机构受到了感染。在首次感染的两分钟内，机构中的100多台计算机便遭到了感染。

网络攻击者在受害者网络上留下了几个工具，从而提供了WannaCry传播方式的确凿证据。我们在一台受影响的计算机上发现了两个文件，即mks.exe和hptasks.exe（参见附录C：感染指标）。

mks.exe这个文件是Mimikatz(Hacktool.Mimikatz)的一个变体，而Mimikatz则是广泛用于目标性攻击中的密码转储工具。第二个文件hptasks.exe用以使用mks.exe盗取的密码，在其他网络计算机上复制和执行WannaCry。

WannaCry通过hptasks.exe传播有两个阶段的过程。

在第一阶段，hptasks运行后可传递一个IP地址的目标清单，将其作为一个参数。在给出这条命令时，hptasks将在一个名为“cg.wry”的文件中读取之前盗取的认证信息，并用其连接IP地址范围组内的所有计算机。所有连接尝试均记录于log.dat文件。

如果成功连接远程计算机，则Admin$或C$\Windows这两个文件夹中将不存在带有.res后缀名的文件，之后hptasks.exe将把表2中列出的文件复制在远程计算机之上。

在hptasks.exe在远程计算机上执行WannaCry之后，第二阶段开始。

hptasks可将多个参数传递到远程计算机上的WannaCry安装程序，包括一个组新的IP地址。如果WannaCry作为参数与这些IP地址一起运行，则不能加密本地计算机上的文件。

然而，WannaCry可与传递的IP地址相连，使用文件c.wry资源段中嵌入的认证信息，访问这些计算机上的Admin$和C$分享文件，之后远程对这些文件进行加密。

除hptasks.exe和mks.exe外，我们在受害者网络的第二台计算机上发现了恶意软件的另外五个组成部分。这五个工具由三个与Lazarus有关。有两个是索尼影业公司攻击事件中所用工具Destover (Backdoor.Destover)的变体。第三个是Trojan.Volgmer，Lazarus之前曾用此恶意软件攻击南韩的目标。

三月和四月份的攻击

自3月27日起，至少有五家机构遭到了新版WannaCry的感染。这些攻击事件似乎没有什么固定模式，受攻击的机构涉及各个行业，地理位置也各种各样。然而，这些攻击事件揭示了WannaCry和Lazarus背后之间关系的其他证据。

为了部署WannaCry，这些攻击使用了两种不同的后门程序：Trojan.Alphanc和Trojan.Bravonc。Alphanc用以将WannaCry放置于至少属于两名已知受害者的计算机之上，将略微调整的恶意软件部署至所有受害者的计算机上。

Alphanc的大量代码与Backdoor.Duuzer相同，而后者是索尼影业攻击事件中所用数据清除工具Destover的子类（参见附录B：共享代码）。事实上，赛门铁克研究人员认为Alphanc就是Duuzer的演变程序。Duuzer之前与Backdoor.Joanap和Trojan.Volgmer的活动也有所联系，而后两者先前均与Lazarus有关联。

赛门铁克研究人员能够创建Alphanc在受害者系统上活动的详细时间表，从该病毒登录系统开始到WannaCry部署完毕为止。

Alphanc活动时间表

Alphanc作为armsvc.exe部署至目标计算机之上，并在几分钟后自行复制，并使用新文件名javaupdate.exe。样本从以下位置开始执行：

```
cmd.exe /c "copy c:\Users\Administrator\AppData\armsvc.exe
c:\windows\system32\javaupdate.exe >
C:\Users\REDACTED\AppData\Local\Temp\NK15DA.tmp" 2>&1
```

几分钟后，系统将创建并执行认证信息转储器mks.exe（与二月份WannaCry使用的认证信息转储器相同）。之后三天没有任何活动，随后网络攻击者送回并部署RAR版本并创建密码保护文档。

片刻之后，一个名为“g.exe”的网络扫描程序开始运行。该程序对网络攻击者所选择IP地址范围中的所有IP地址进行域名解析，很可能是为了确定其感兴趣的计算机。

在网络攻击者将配置文件送回本地网络前，活动会有一个两天的间隔。所用命令示例包括：

```
cmd.exe /c "net view >
C:\Users\REDACTED\AppData\Local\Temp\NK2301.tmp" 2>&1
cmd.exe /c "net view /domain >
C:\Users\REDACTED\AppData\Local\Temp\NK6C42.tmp" 2>&1
cmd.exe /c "time /t >
C:\Users\REDACTED\AppData\Local\Temp\NKC74F.tmp" 2>&1
```

之后，javaupdate.exe创建文件taskhcst.exec。这便是勒索软件WannaCry。.exec后缀名重新更名为.exe，如下所示。这很可能是一个安全检查，使网络攻击者不会错误地过早执行此文件。

```
cmd.exe /c "ren C:\Windows\taskhcst.exec taskhcst.exe >

C:\Users\REDACTED\AppData\Local\Temp\NK833D.tmp" 2>&1
```

将近45分钟之后，网络攻击者将后门程序javaupdate.exe复制至远程计算机之上。

之后，网络攻击者还在此计算机粘贴了一个名为“bcremote.exe”的文件；该文件和二月份攻击中名为hptasks.exe的工具相同，用以在网络上传播WannaCry。WannaCry随后复制此文件的配置文件，并最终进行自我复制：

```
cmd.exe /c "net use \\REDACTED\ipc$ REDACTED /u:REDACTED >
C:\Users\REDACTED\AppData\Local\Temp\NK2E.tmp" 2>&1
cmd.exe /c "copy c:\windows\system32\javaupdate.exe
\\REDACTED\c$\windows\javaupdate.exe >
C:\Users\REDACTEDAppData\Local\Temp\NK3E49.tmp" 2>&1
cmd.exe /c "copy c:\windows\beremote.exe \\REDACTED\c$\windows\ >
C:\Users\REDACTED\AppData\Local\Temp\NK4DD5.tmp" 2>&1
```

```
cmd.exe /c "copy c:\windows\c.wry \\REDACTED\c$\windows\ >
C:\Users\REDACTED\AppData\Local\Temp\NK7228.tmp" 2>&1
cmd.exe /c "copy c:\windows\taskh*.exe \\REDACTED\c$\windows\ >
C:\Users\REDACTED\AppData\Local\Temp\NK7DCF.tmp" 2>&1
```

相同程序还会在网络上的第二台服务器上进行，执行bcremote.exe命令后，WannaCry便在整个网络中开始传播。

Trojan.Bravonc

有关Trojan.Bravonc的运行信息很少，该程序用以将WannaCry放于至少两名其他受害者的计算机之上，表明其与Lazarus团伙有着相当明确的关联。

该程序连接IP地址87.101.243.252上的命令和控制(C&C)服务器，该IP地址与Destover（Lazrus的一款知名工具）示例中使用的IP地址相同。Blue Coat在《从首尔到索尼报告》中也提及了此IP地址。

我们还发现Duuzer用此IP地址作为C&C服务器。Bravonc和Destover的一个变体还共享密码相关代码（参见附录B：共享代码）。此外，Bravonc的传播方式（在SMB上使用硬编码认证信息）与Lazarus相关的另一个工具Joanap使用了相同的技术。

五月份攻击：WannaCry开始在全球范围内传播

5月12日，整合已泄露“永恒之蓝”利用工具的新版WannaCry发布了，“永恒之蓝”可使用Windows中的两个已知漏洞（CVE-2017-0144和CVE-2017-0145）将勒索软件传播至受害者网络中未安装补丁的计算机之上，也可将其传播至与互联网连接的其他安全防范薄弱的计算机之上。

整合“永恒之蓝”之后，WannaCry从仅能在受限数量目标性攻击中使用的危险工具转变成一个近年来最为恶性的恶意软件。

这种恶意软件造成了大范围破坏，很多机构受到感染，还有一些机构被迫对计算机进行离线软件升级。MalwareTech的一篇网络安全博文介绍了对该恶意软件杀手锏的发现和触发原理，从而制限制了它的传播和危害。

早期版本的WannaCry和5月12日攻击中所使用的在很大程度上是相同的，但也有一些小更改，主要是后者对“永恒之蓝”利用工具进行了整合。

用以加密Zip文件的密码嵌入于WannaCry 释放器之中，与其他两个版本相似（“wcry@123”、“wcry@2016”和 “WNcry@2ol7”），说明这两个版本软件的作者可能来自同一个团伙。

第一个版本的WannaCry使用了少量的比特币客户端，而且传播性不广，这说明其不是众多网络犯罪团伙所共享的工具。同时也进一步证明了两个版本的WannaCry都由一个团伙所操作。

WannaCry与Lazarus相关联

除了WannaCry传播工具的相同性之外，WannaCry本身和Lazarus团伙还有着很多关联。该勒索软件与恶意软件Backdoor.Contopee共享了一些代码，而后者先前与Lazarus有所关联。

Contopee的一个变体使用了自定义SSL工具， 其加密套件与WannaCry所用的相同。在这两个例子中，加密套件均使用了相同组的密码，共75个不同密码可供选择（与拥有300多个密码的OpenSSL不同）。

此外，WannaCry的代码混淆方法与Infostealer.Fakepude类似，而后者先前与Lazarus有所关联；而且，三月和四月份用以传播WannaCry的恶意软件Trojan.Alphanc也与Lazarus 有所关联（请参见上文）。

偶然泄漏使WannaCry变成了全球性威胁

对少量WannaCry早期攻击事件的发现，提供了该勒索软件与Lazarus团伙有所关联的强力证据。

这些早期攻击明显使用了先前与Lazarus 相关的工具、代码和基础设施，而且通过后门程序和盗取认证信息进行传播的方式也与Lazarus先前的攻击相一致。

“永恒之蓝”利用工具的泄漏使网络攻击者能够将WannaCry变得更为强大，远远比该勒索软件在依赖自有工具时强大得多。

这是因为网络攻击者借此能够绕过很多之前必须执行的步骤，无需再盗取认证信息并在计算机之间互相复制粘贴。

黑客老王：一个人的黑客史

吴石：站在0和1之间的男人

黑客衰大：45天攻入姑娘的心

黑客段子手“呆子不开口”

“特斯拉破解第一人”刘健皓

唐青昊：虚拟世界的越狱者

MOSEC：盘古团队的野心优雅

让周鸿祎“三顾茅庐” 的 黑客 MJ

美女黑客张婉桥的“爱丽丝奇遇记”

TK教主和玄武实验室的几个小故事

把老婆训练成女黑客的漏洞大神黄正

“真爱”黑客 Fooying 手把手教你追妹子

更多精彩正在整理中……

“喜欢就赶紧关注我们”

宅客『Letshome』

雷锋网旗下业界报道公众号。

专注先锋科技领域，讲述黑客背后的故事。

长按下图二维码并识别关注