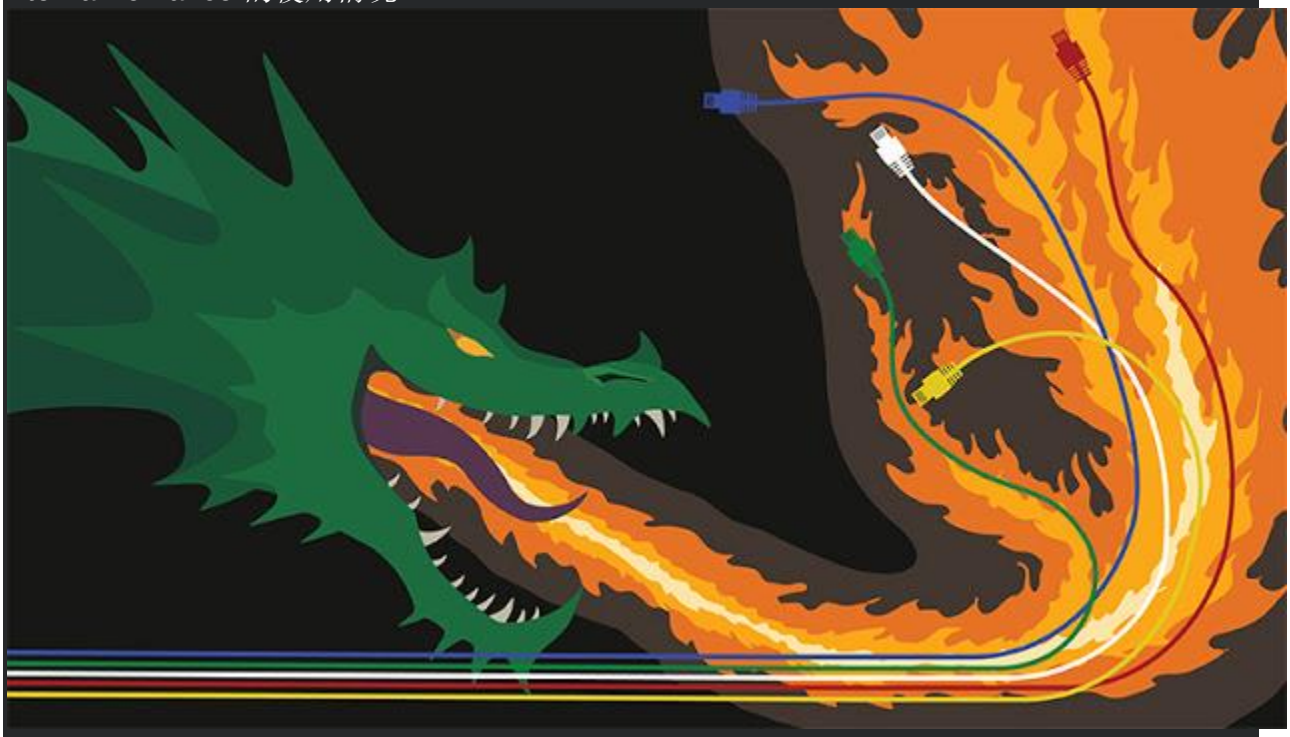
2017 年 6 月 27 日

# 新的勒索软件变种“Nyetya”危害系统全球

***注意：*** *Talos 针对新威胁进行了积极研究，此博客文章就此进行讨论。这类信息只能视为初步信息，并将随着研究继续持续更新。*

*更新时间为 2017 年 06 月 28 日下午 07：09 EDT：更新以反映作为用于入侵系统机制的 EternalRomance 的使用情况。*



自从 SamSam 在 2016 年 3 月针对美国医疗保健机构展开攻击以来，有关解决勒索软件通过未修补网络漏洞的扩散，Talos 一直备受关注。2017 年 5 月，WannaCry 勒索软件利用了 SMBv1 内的漏洞，并在互联网上大规模爆发。

现在，一种新的恶意软件版本已经浮出水面，它与被称为 Petrwrap 和 GoldenEye 等 的 Petya 勒索软件明显不同。Talos 正在将这个新的恶意软件变体确定为 Nyetya。该样本利用 EternalBlue、EternalRomance、WMI 和 PsExec 在受影响的网络内部横向渗透。稍后将在“恶意软件功能”的博客中对此行为进行详细介绍。与 WannaCry 不同，Nyetya 显示没有包含外部扫描组件。

目前还没有识别出该勒索软件的传播源头。无法确认电子邮件是传播源头的早期报告。基于观察到的在外散播行为、已知的缺乏、可行的外部扩散机制和其他研究，我们认为有些感染可能与乌克兰税务会计软件 MeDoc 的更新系统有关。Talos 还在持续研究此恶意软件的传播源头。

与所有勒索软件一样，Talos 不建议支付赎金。基于勒索软件的这个特定点，应该注意的是，用于支付验证和解密密钥共享的相关邮箱已被 posteo.de 网站关闭。这将使得所有成功付款无效，攻击者在收到支付的赎金后没有可用的通信方式验证受害者的支付或者分配解密密钥。恶意软件也没有可用来直接连接命令和控制远程解锁的方法。Nyetya 不完全是勒索软件（其中它会提示您通过支付赎金取回您的数据），并且更多地是一个“擦除”系统，它意味着能轻易地擦除系统。

## 恢复用户凭证

负责传播恶意软件的 Perfc.dat 文件在其资源部分包含嵌入可执行文件。勒索软件将该可执行文件以临时文件属性放置在用户的 %TEMP% 文件夹内，用命名管道参数运行（包含 GUID）。主要可执行文件通过此命名管道与放置的可执行文件通信。例如：

```
C:\WINDOWS\TEMP\561D.tmp, \\.\pipe\{C1F0BF2D-8C17-4550-AF5A-65A22C61739C}
```

放置的 .tmp 可执行文件似乎基于 Mimikatz，这是一种流行的开源软件，通过使用几种不同技术用于恢复计算机内存的用户凭证。***但是，Talos 已确认可执行文件并非 Mimikatz 工具。***

然后利用 WMIC 和 PsExec 使用恢复的凭证在远程系统中启动恶意软件。例如：

```
Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process
call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1
```

## 恶意软件功能

Perfc.dat 具有进一步危害系统所需的功能，并包含一个单个未命名的导出功能模块，称为 #1。该库尝试通过 Windows API AdjustTokenPrivileges 获取当前用户的管理权限

（SeShutdowPrivilege 和 SeDebugPrivilege）。一旦成功，Nyetya 将重写磁盘上的启动分区记录（MRB），在 Windows 中把磁盘称为 PhysicalDrive 0。不管 MBR 重写成功与否，恶意软件将继续通过 schtasks 创建计划的任务，在完成感染一小时后重新启动系统。

在勒索软件散播过程中，恶意软件通过 NetServerEnum API 呼叫遍历网络上所有可见主机，然后扫描所有开放了 TCP 139 端口的主机。这样做是为了编译暴露了这个端口和易于感染的主机列表。

一旦主机被感染，Nyetya 将使用几种机制进行散播：

1. EternalBlue - 与 WannaCry 入侵的方式相同。
2. EternalRomance - 由“ShadowBrokers”泄露的 SMBv1 入侵
3. PsExec - Windows 系统自带的管理工具。
4. WMI - Windows 管理工具，Windows 自带组件。

这些机制用于尝试在其他主机上安装和执行 perfc.dat 以横向扩散恶意软件。

对于还没有应用 MS17-010 的系统，则利用 EternalBlue 和 EternalRomance 漏洞攻击危害系统。针对受害者系统启动的漏洞攻击取决于预定目标的操作系统。

- EternalBlue
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows 7
- EternalRomance
  - Windows XP
  - Windows Server 2003
  - Windows Vista

利用当前用户的 Windows Token（来自上面的“恢复用户凭证”部分），在联网的主机上 PsExec 被用于运行以下命令（其中 w.x.y.z 是 IP 地址）来安装恶意软件。

```
C:\WINDOWS\dllhost.dat \\w.x.y.z -accepteula -s -d
C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1
```

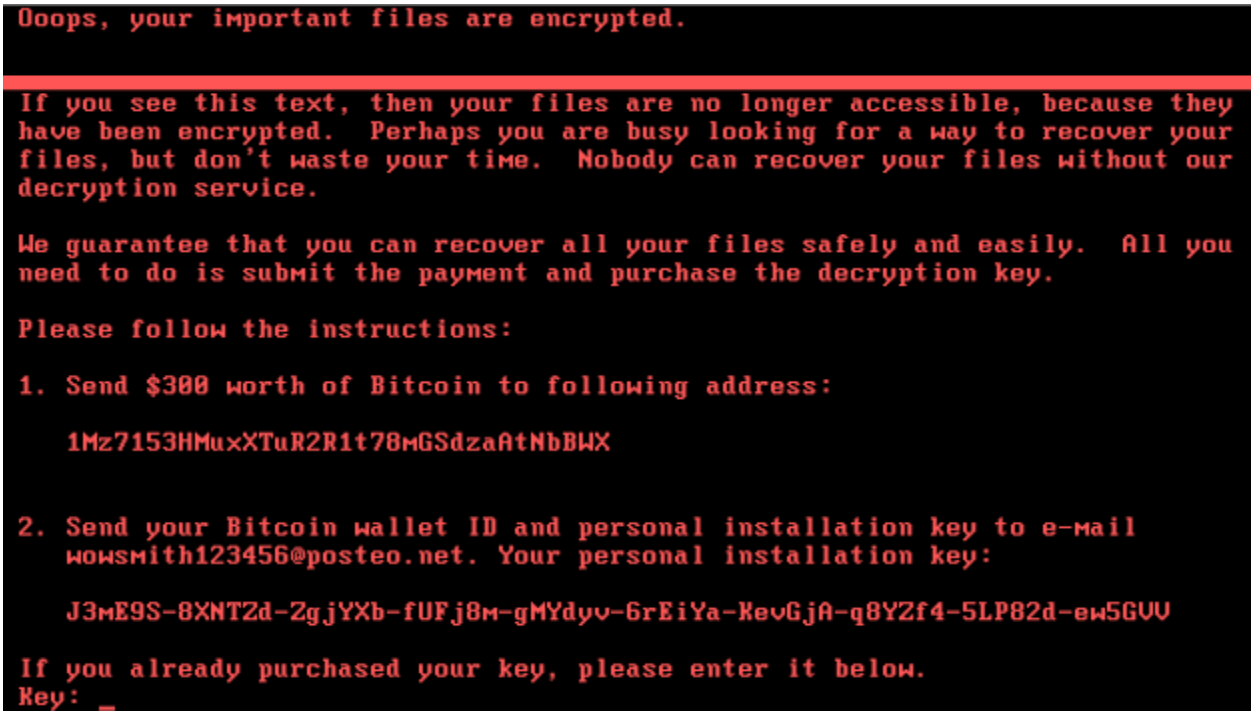
利用当前用户的用户名和密码(作为用户名和密码)，从上面的“恢复用户凭证”部分检索，WMI 被用于执行以下命令实现相同功能。

```
Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process
call create "C:\Windows\System32\rundll32.exe \"C:\Windows\perfc.dat\" #1"
```

一旦危害系统成功，恶意软件将使用 2048 位 RSA 加密主机上的文件。此外，恶意软件使用以下命令清理被感染主机上的活动日志：

```
wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl
Application & fsutil usn deletejournal /D %c:
```

重启 MBR 被重写的系统时，会看到此消息。




被 Nyetya 入侵的系统的截屏。

## 规避和预防

客户可以有几种方式缓解并防止 Nyetya 影响您的环境。

- 首先，我们强烈建议尚未应用 MS17-010 访问的客户立即执行。鉴于漏洞的严重程度和利用它的可用工具的广泛度，明智的作法是进行漏洞修补。
- 确保您的系统部署了防恶意软件，可以检测和封锁已知的恶意可执行文件的实施。
- 执行灾难恢复计划包括备份和存储离线备份主机的数据。攻击者经常将备份机制作为攻击目标，以降低用户在不支付赎金的情况下恢复文件的可能性。
- 如果可能，在网络上禁用 SMBv1 并移动到更新版本的 SMB。（SMBv2 使用 Microsoft Vista 引入）

由于 Nyetya 尝试在被感染的主机上重写 MBR，Talos 使用 MBRFilter 进行了测试，以防止允许系统 MBR 进行任何更改。此测试已经得到了成功证实，并且主机 MBR 保持良好状态。对于可以执行此操作的用户和企业，我们建议使用 MBRFilter。注意 MBRFilter 是 Talos 提供的开源项目，不提供保修或保证。

## 防护

思科客户可以通过以下产品和服务对 Nyetya 进行防护。

| PRODUCT | PROTECTION |
|---|---|
| AMP | ✔ |
| CloudLock | N/A |
| CWS | N/A |
| Email Security | N/A |
| Network Security | ✔ |
| Threat Grid | ✔ |
| Umbrella | N/A |
| WSA | N/A |

高级恶意软件防护 (AMP) 解决方案可以有效防止执行威胁发起者使用的恶意软件。

网络安全设备（例如 NGFW、NGIPS 和 Meraki MX）可以检测与此威胁相关的恶意活动。

AMP Threat Grid 可帮助识别恶意二进制文件，使所有思科安全产品都有内置保护措施。

目前还没识别出邮件和 Web 是攻击源头。此外，目前还没有与此恶意软件相关的已知 C2 元素。如果该恶意软件在您网络的这些系统之间传输，将会受到阻止。

客户打开源 Snort 用户规则集，可以在 Snort.org 上下载 Snort.org 出售的最新规则包，保持最新状态。

## NGIPS/Snort 规则

以下 NGIPS/Snort 规则可以检测此威胁：

- 42944 - OS-WINDOWS Microsoft Windows SMB remote code execution attempt
- 42340 - OS-WINDOWS Microsoft Windows SMB anonymous session IPC share access attempt
- 41984 - OS-WINDOWS Microsoft Windows SMBv1 identical MID and FID type confusion attempt

以下 NGIPS/Snort 规则提供感染流量的检测告警：

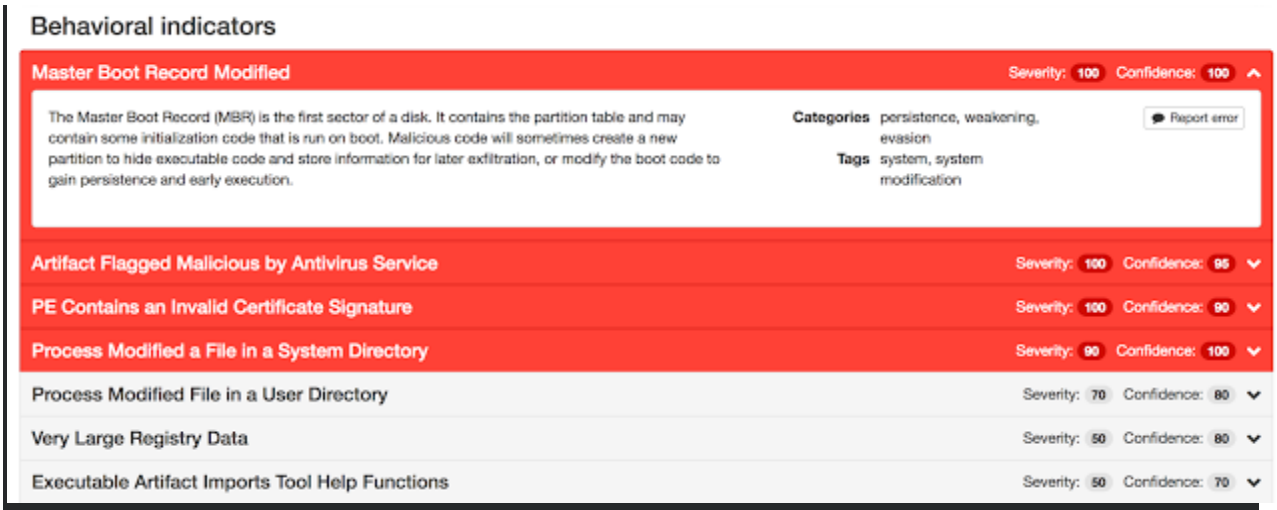
- 5718 - OS-WINDOWS Microsoft Windows SMB-DS Trans unicode Max Param/Count OS-WINDOWS attempt
- 1917 - INDICATOR-SCAN UPnP service discover attempt
- 5730 - OS-WINDOWS Microsoft Windows SMB-DS Trans Max Param OS-WINDOWS attempt
- 26385 - FILE-EXECUTABLE Microsoft Windows executable file save onto SMB share attempt
- 43370 - NETBIOS DCERPC possible wmi remote process launch

## AMP 覆盖范围

- W32.Ransomware.Nyetya.Talos

## Threat Grid

Threat Grid 能够检测与 Nyetya 恶意行为相关的恶意软件样本。




## 危害表现 (IOC)

## AMP 覆盖范围

- W32.Ransomware.Nyetya.Talos

## SHA256

- 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
- eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998 (password stealer)

发布者：ALEXANDER CHIU；发布时间：14:02
标签： AMP，覆盖范围，勒索软件，SMBV1，SNORT