博客

思科 Talos 深度解析“WannaCry"勒索软件

博客作者：Martin Lee、Warren Mercer、Paul Rascagneres 和 Craig Williams

要点综述

据报道称，全球多家组织遭到了一次严重的勒索软件攻击，西班牙的 Telefonica、英国的国民保健署、以及美国的 FedEx 等组织纷纷中招。发起这一攻击的恶意软件是一种名为“WannaCry”的勒索软件变种。

该恶意软件会扫描电脑上的 TCP 445 端口（Server Message Block/SMB），以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件，然后要求以比特币的形式支付赎金。

此外，Talos 还注意到 WannaCry 样本使用了 DOUBLEPULSAR，这是一个由来已久的后门程序，通常被用于在以前被感染的系统上访问和执行代码。这一后门程序允许在系统上安装和激活恶意软件等其他软件。它通常在恶意软件成功利用 SMB 漏洞后被植入，后者已在 Microsoft 安全公告 MS17-010 中被修复。在 Shadow Brokers 近期向公众开放的工具包中，一种攻击性漏洞利用框架可利用此后门程序。自这一框架被开放以来，安全行业以及众多地下黑客论坛已对其进行了广泛的分析和研究。

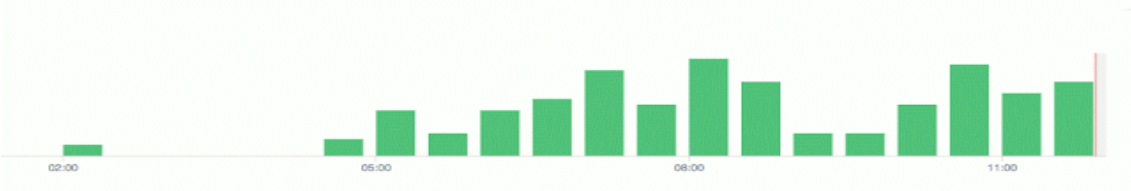
WannaCry 似乎并不仅仅是利用与这一攻击框架相关的 ETERNALBLUE（永恒之蓝）模块，它还会扫描可访问的服务器，检测是否存在 DOUBLEPULSAR 后门程序。如果发现有主机被植入了这一后门程序，它会利用现有的后门程序功能，并使用它来通过 WannaCry 感染系统。如果系统此前未被感染和植入 DOUBLEPULSAR，该恶意软件将使用 ETERNALBLUE 尝试利用 SMB 漏洞。这就造成了近期在互联网上观察到的大规模类似蠕虫病毒的活动。

组织应确保运行 Windows 操作系统的设备均安装了全部补丁，并在部署时遵循了最佳实践。此外，组织还应确保关闭所有外部可访问的主机上的 SMB 端口（139 和 445）。

请注意，针对这一威胁我们当前还处于调查阶段，随着我们获知更多信息，或者攻击者根据我们的行动作出响应，实际情况将可能发生变化。Talos 将继续积极监控和分析这一情况，以发现新的进展并相应采取行动。因此，我们可能会制定出新的规避办法，或在稍后调整和/或修改现有的规避办法。有关最新信息，请参阅您的 Firepower Management Center 或 Snort.org。

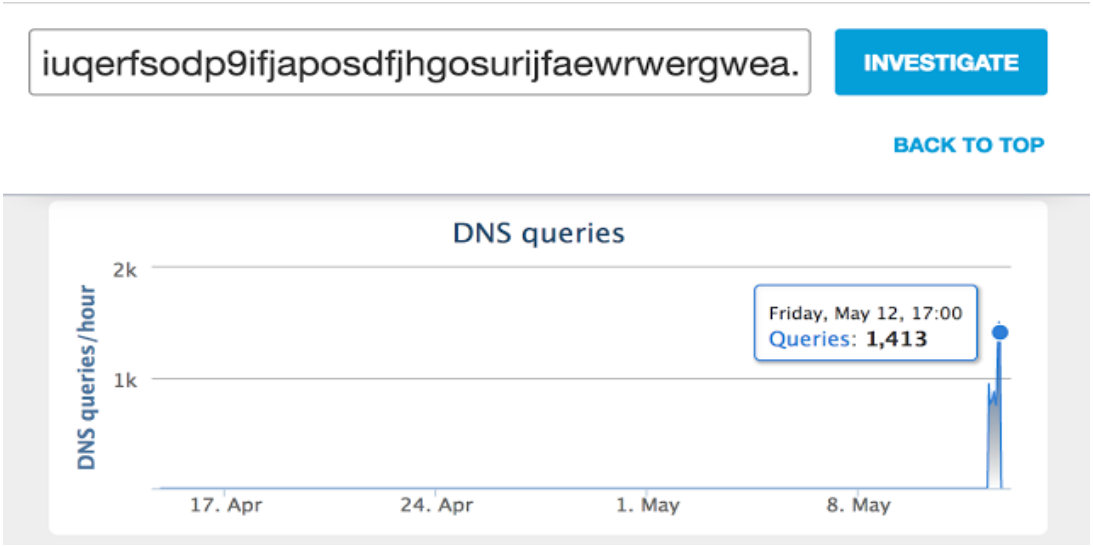
攻击详细信息

我们注意到从东部标准时间早上 5 点（世界标准时间上午 9 点）前开始，网络中针对联网主机的扫描开始急速攀升。



基础设施分析

Cisco Umbrella 研究人员在 UTC 时间 07:24，观察到来自 WannaCry 的 killswitch 域名（iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com）的第一个请求，此后在短短 10 小时后，就上升到 1,400 的峰值水平。



该域名组成看起来就像是人为输入而成，大多数字符均位于键盘的上排和中间排。

鉴于此域名在整个恶意软件执行中的角色，与其进行的通信可能被归类为 kill switch 域名：

```
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// : "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();
  result = 0;
}
return result;
```

以上子程序会尝试对此域名执行 HTTP GET 操作，如果失败，它会继续进行感染操作。然而，如果成功，该子程序将会结束。该域名被注册到一个已知的 sinkhole，能够有效使这一样本结束其恶意活动。

Email Address	Associated Domains	Email Type	Last Observed
BotnetSinkhole@gmail.com	36 Total - 35 malicious	Administrative, Registrant, Technical	Current

Nameserver	Associated Domains	Last Observed
ns2.sinkhole.tech	46 Total - 35 malicious	Current
ns4.sinkhole.tech	36 Total - 34 malicious	Current
ns1.sinkhole.tech	48 Total - 37 malicious	Current
ns3.sinkhole.tech	38 Total - 36 malicious	Current

原始注册信息有力证明了这一点，其注册日期为 2017 年 5 月 12 日：

```
Domain Name: IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM
Registrar: NAMECHEAP INC.
Sponsoring Registrar IANA ID: 1068
Whois Server: whois.namecheap.com
Referral URL: http://www.namecheap.com
Name Server: NS1.SINKHOLE.TECH
Name Server: NS2.SINKHOLE.TECH
Name Server: NS3.SINKHOLE.TECH
Name Server: NS4.SINKHOLE.TECH
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 12-may-2017
Creation Date: 12-may-2017
Expiration Date: 12-may-2018
```

恶意软件分析

初始文件 mssecsvc.exe 会释放并执行 tasksche.exe 文件，然后检查 kill switch 域名。之后它会创建 mssecsvc2.0 服务。该服务会使用与初次执行不同的入口点执行 mssecsvc.exe 文件。第二次执行会检查被感染电脑的 IP 地址，并尝试联接到相同子网内每个 IP 地址的 TCP 445 端口。当恶意软件成功联接到一台电脑时，将会建立联接并传输数据。我们认为这一网络流量是一种利用程序载荷。已有广泛报道指出，这一攻击正在利用最近被泄露的漏洞。Microsoft 已在 MS17-010 公告中修复了此漏洞。我们当前尚未完全了解 SMB 流量，也未完全掌握这一攻击会在哪些条件下使用此方法进行传播。

tasksche.exe 文件会检查硬盘，包括映射了盘符的网络共享文件夹和可移动存储设备，如“C:/”和“D:/”等。该恶意软件之后会检查具有附录中所列后缀名的文件，然后使用 2048 位 RSA 加密算法对其进行加密。在加密文件的过程中，该恶意软件会生成一个新的文件目录“Tor/”，在其中释放 tor.exe 和九个供 tor.exe 使用的 dll 文件。此外，它还会释放两个额外的文件：taskdl.exe 和 taskse.exe。前者会删除临时文件，后者会启动 @wanadecryptor@.exe，在桌面上向最终用户显示勒索声明。@wanadecryptor@.exe 并不包含在勒索软件内，其自身也并非勒索软件，而仅仅是用来显示勒索声明。加密由 tasksche.exe 在后台完成。

@wanadecryptor@.exe 会执行 tor.exe 文件。这一新执行的进程将会启动到 Tor 节点的网络联接，让 WannaCry 能够通过 Tor 网络代理发送其流量，从而保持匿名。

与其他勒索软件变种类似，该恶意软件也会删除受害人电脑上的任意卷影副本，以增加恢复难度。它通过使用 WMIC.exe、vssadmin.exe 和 cmd.exe 完成此操作。

Process ID	Process Name	Command Line
29 (cmd.exe)	cmd.exe	cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
30 (vssadmin.exe)	vssadmin.exe	vssadmin delete shadows /all /quiet
35 (WMIC.exe)	WMIC.exe	wmic shadowcopy delete

WannaCry 使用多种方法辅助其执行，它使用 attrib.exe 来修改+h 标记（hide），同时使用 icacls.exe 来赋予所有用户完全访问权限（“icacls ./grant Everyone:F /T /C /Q”）。

该恶意软件被设计成一种模块化服务。我们注意到与该勒索软件相关的可执行文件由不同的攻击者编写，而非开发服务模块的人员编写。这意味着该恶意软件的结构可能被用于提供和运行不同的恶意载荷。

加密完成后，该恶意软件会显示以下勒索声明。这一勒索软件非常有趣的一点是，其勒索屏幕是一个可执行文件，而非图像、HTA 文件或文本文件。

组织应该意识到，犯罪分子在收到勒索赎金后，并无义务提供解密秘钥。Talos 强烈呼吁所有被攻击的人员尽可能避免支付赎金，因为支付赎金的举动无疑就是在直接资助这些恶意活动的壮大。

规避与预防

希望避免被攻击的组织应遵循以下建议：

- 确保所有 Windows 系统均安装了全部补丁。至少应确保安装了 Microsoft 公告 MS17-010。
- 根据已知的最佳实践，具有可通过互联网公开访问的 SMB（139 和 445 端口）的任意组织应立即阻止入站流量。

此外，我们强烈建议组织考虑阻止到 TOR 节点的联接，并阻止网络上的 TOR 流量。ASA Firepower 设备的安全情报源中列出了已知的 TOR 出口节点。将这些节点加入到黑名单将能够避免与 TOR 网络进行出站通信。

除了以上的规避措施外，Talos 强烈鼓励组织采取以下行业标准建议的最佳实践，以预防此类及其他类似的攻击活动。

- 确保您的组织运行享有支持的操作系统，以便能够获取安全更新。
- 建立有效的补丁管理办法，及时为终端及基础设施内的其他关键组件部署安全更新。
- 在系统上运行防恶意软件，确保定期接收恶意软件签名更新。
- 实施灾难恢复计划，包括将数据备份到脱机保存的设备，并从中进行恢复。攻击者会经常瞄准备份机制，限制用户在未支付赎金的情况下恢复其文件的能力。

规避办法

Snort 规则：42329-42332、42340、41978

下方列出了客户可以检测并阻止此威胁的其他办法。

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

高级恶意软件防护（AMP）能够有效避免执行这些攻击者使用的恶意软件。

CWS 或 WSA 网络扫描能够阻止访问恶意网站，并发现这些攻击中使用的恶意软件。

Email Security 可以阻止攻击者在其攻击活动中发送的恶意电子邮件。

IPS 和 NGFW 的网络安全防护功能可以提供最新的签名，用来检测攻击者发起的恶意网络活动。

AMP Threat Grid 能够帮助发现恶意软件二进制文件，并在所有思科安全产品中建立防护措施。

Umbrella 能够阻止对与恶意活动相关的域名进行 DNS 解析。

Talos 介绍

Talos 团队由业界领先的网络安全专家组成，他们分析评估黑客活动，入侵企图，恶意软件以及漏洞的最新趋势。包括 ClamAV 团队和一些标准的安全工具书的作者中最知名的安全专家，都是 Talos 的成员。这个团队同时得到了 Snort、ClamAV、Senderbase.org 和 Spamcop.net 社区的庞大资源支持，使得它成为网络安全行业最大的安全研究团队。也为思科的安全研究和安全产品服务提供了强大的后盾支持。

思科公司简介

思科（NASDAQ：CSCO）是全球科技领导厂商，自 1984 年起就专注于成就互联网。我们的人才、产品和合作伙伴都致力于帮助社会实现安全互联，并且把握未来的数字化机遇。更多信息，敬请访问 http://apjc.thecisconetwork.com。

###