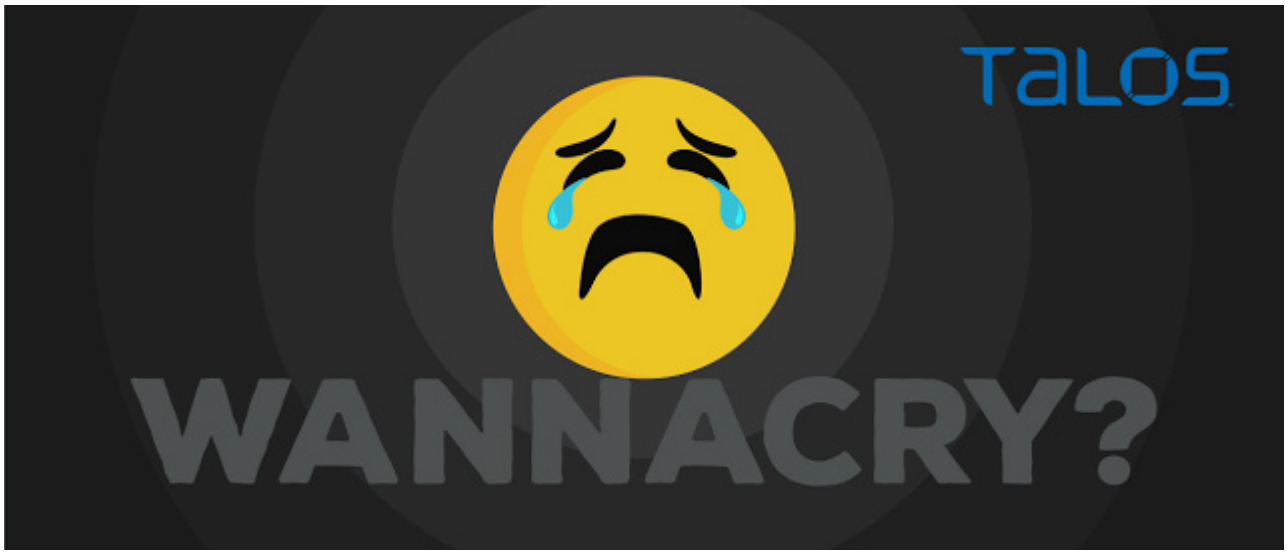
2017 年 5 月 12 日，星期五

三号恶意软件已登场：尝试了解“WannaCry”

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



执行摘要

据报道，全球众多组织遭遇严重的勒索软件攻击，西班牙电信公司、英国国民保健署和美国联邦快递均未能幸免。发起这场攻击的恶意软件是一个被称为“WannaCry”的勒索软件变种。

该恶意软件能够通过 TCP 端口 445（服务器消息块/SMB）进行密集扫描，以类似于蠕虫病毒的方式传播，它会感染主机、加密主机上存储的文件，然后要求受害者以比特币支付赎金。值得注意的是，这种威胁不仅仅通过扫描内部范围来确定传播区域，还能够基于在互联网上其他面向外部的主机中发现的漏洞进行传播。

此外，Talos 还发现 WannaCry 样本利用的是 DOUBLEPULSAR，这是一种顽固的后门程序，通常用于在以前受感染的系统中访问和执行代码。这种后门程序允许安装和激活其他软件（例如恶意软件）。攻击者通常会在成功利用 SMB 漏洞（已在 Microsoft 安全公告 MS17-010 中进行修复）后安装这种后门程序。该后门程序与最近公开发布的 Shadow Brokers 缓存所包含的攻击框架有关。自发布以来，安全行业及各种地下黑客论坛已对其进行广泛分析和研究。

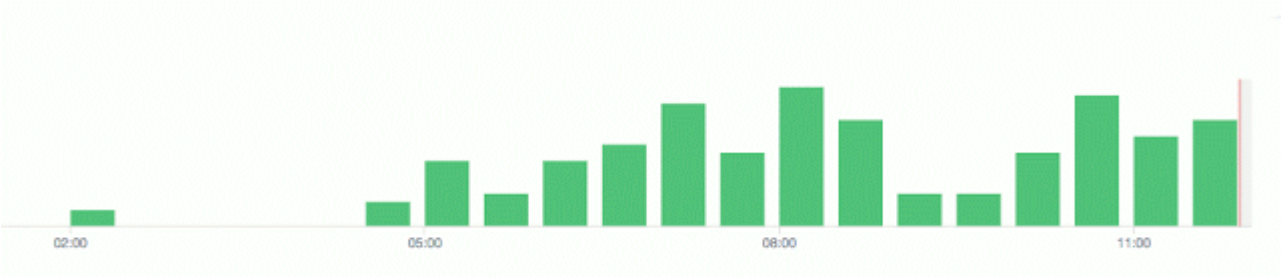
WannaCry 似乎主要使用 ETERNALBLUE 模块和 DOUBLEPULSAR 后门程序。该恶意软件最初通过 ETERNALBLUE 利用 SMB 漏洞。如果利用成功，它会植入后门程序 DOUBLEPULSAR 并利用其安装恶意软件。如果利用失败但已安装 DOUBLEPULSAR 后门程序，则该恶意软件将依然利用此后门程序安装勒索软件负载。这是导致在互联网中观察到大量类似蠕虫的攻击活动的原因

各组织应确保对运行 Windows 的设备进行全面修复，并按照最佳实践进行部署。此外，组织还应阻止所有外部主机访问 SMB 端口（139 和 445）。

请注意，我们仍然在积极调查这一威胁，随着我们了解更多信息，或者攻击者对我们的措施做出反应，情况可能会发生变化。Talos 将继续积极监控和分析这一威胁态势，了解它的新发展，并相应采取应对措施。因此，后期我们会制定新的防护措施，或者调整和/或修改现有的防护措施。如需获取最新信息，请参阅 Firepower 管理中心或 Snort.org。

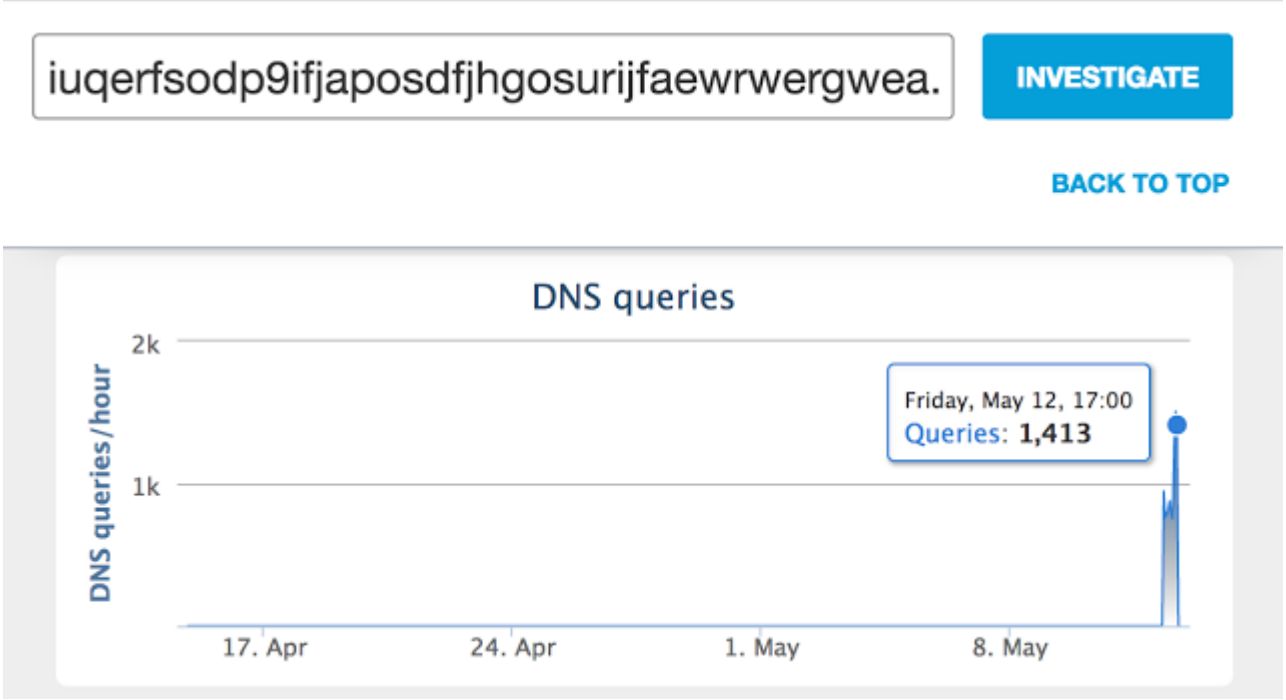
攻击活动详细信息

我们观察到，针对诱捕系统的互联网扫描在临近美国东部标准时间早上 5 点（协调世界时上午 9 点）时开始增加。



基础设施分析

思科 Umbrella 研究人员在 07:24（协调世界时）首次观察到访问其中一个 WannaCry 自杀开关域 (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com) 的请求，然后在大约 10 小时后请求数量上升到峰值，超过了 1400 个。



组成域的字符看起来基本是人工输入的，大部分落在键盘的顶行和中间行。

根据此域在整个恶意软件执行过程中扮演的角色，可以将它的通信类型归类为自杀开关域。

```
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;
```

上述子例程尝试对此域发出 HTTP GET 请求，如果失败，会继续实施感染。但如果成功，子例程会退出。此域注册到一个众所周知的 sinkhole 中，可有效让这一样本终止其恶意活动。

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

原始注册信息进一步印证了这一点，因为该域注册于 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”植入并执行“tasksche.exe”，此 exe 用于测试自杀开关域。完成后会创建 mssecsvc2.0 服务，这是恶意软件持续感染受害者的一种方法。该服务通过与初始执行不同的入口点执行“mssecsvc.exe”。第二次执行的是 2 个线程。第一个线程检查受感染计算机的 IP 地址，并尝试连接到同一子网中每个主机/IP 地址的 TCP445 (SMB)；第二个线程生成互联网中的随机 IP 地址，以执行相同的操作。恶意软件成功连接到计算机后，会发起连接并传输数据。恶意软件利用 Microsoft 在公告 MS17-010 中已修复的 SMB 漏洞 (ETERNALBLUE) 来植入 DOUBLEPULSAR 后门程序。该后门程序用于在新的受危害系统中执行 WANNACRY。

文件 tasksche.exe 检查磁盘驱动器，包括映射到某个盘符（例如“C:/”、“D:/”等）的网络共享和可移动存储设备。然后，恶意软件会检查带有附录列出的文件扩展名的文件，并使用 2048 位 RSA 加密算法对这些文件进行加密。加密文件后，恶意软件会创建一个新的文件目录“Tor/”，并在其中植入 tor.exe 和 tor.exe 所使用的九个 dll 文件。此外，它还会植入两个其他文件：taskdl.exe 和 taskse.exe。前者可删除临时文件，而后者可启动 @wanadecryptor@.exe，以在桌面上向终端用户显示勒索信。@wanadecryptor@.exe 本身并不是勒索软件，它只是一封勒索信。tasksche.exe 在后台执行加密。

tor.exe 文件由 @wanadecryptor@.exe 执行。这一新执行的过程可发起到 Tor 节点的网络连接。这使得 WannaCry 可通过 Tor 网络代理其流量，尝试保持匿名状态。

与其他勒索软件变种类似，该恶意软件也会删除受害者计算机上的所有卷影副本，从而增大恢复难度。它通过使用 WMIC.exe、vssadmin.exe 和 cmd.exe 实现这一目的。

进程 ID	进程名称	命令行
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 使用多种方法尝试帮助其执行，包括利用 attrib.exe 修改 +h 标记（隐藏），并利用 icacls.exe 允许所有用户具有完全访问权限，即“icacls ./grant Everyone:F /T /C /Q”

该恶意软件被设计成模块化服务。我们注意到，与勒索软件关联的可执行文件的编写者与服务模块的开发者不同。这意味着这种恶意软件的架构或许可用于传送和运行不同的恶意负载。

完成加密后，恶意软件会显示以下勒索信。该勒索软件变种一个有趣的地方是，勒索屏幕实际上是可执行文件，而不是图片、HTA 文件或文本文件。

各组织应意识到，支付赎金后，犯罪分子并没有提供解密密钥的义务。Talos 强烈呼吁所有受攻击的人员尽可能避免支付赎金，因为这会直接资助这些恶意活动的发展。

规避和预防

希望规避受攻击风险的组织应遵循以下建议：

- 确保所有基于 Windows 的系统已全面修补。至少确保已应用 Microsoft 公告 MS17-010。
- 根据已知的最佳实践，拥有可通过互联网公开访问的 SMB（端口 139 和 445）的任何组织应立即阻止入站流量。

此外，组织应认真考虑阻止到 TOR 节点的连接和网络中的 TOR 流量。已知的 TOR 出口节点已在 ASA FirePOWER 设备的安全情报源中列出。将此列入黑名单将阻止到 TOR 网络的出站通信。

除了以上列出的风险规避措施，Talos 还强烈建议组织采取以下行业标准建议的最佳实践，以预防攻击和其他类似的恶意活动。

- 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。
- 实施有效的补丁管理，及时向终端和基础设施的其他关键部分部署安全更新。

- 在系统上运行防恶意软件，并确保定期接收恶意软件签名更新。
- 实施灾难恢复计划，包括将数据备份到保持离线状态的设备中，并从中进行恢复。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。

防护

Snort 规则：42329-42332、42340、41978

开源 Snort 用户规则集客户可以在 Snort.org 上下载最新的可用规则包，以保持最新状态。

思科客户可通过其他方式检测并阻止此威胁，包括：

产品	防护
AMP	✔
CloudLock	不适用
CWS	✔
邮件安全	不适用
网络安全	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

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。

CWS 或 WSA Web 扫描功能可以阻止访问恶意网站，并检测这些攻击中所用的恶意软件。

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。

Umbrella 可防止对与恶意活动相关的域进行 DNS 解析。

StealthWatch 可以检测网络扫描活动、网络传播和与 CnC 基础设施的连接，从而与此活动建立联系，通知管理员。

IoC

文件名

- d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa b.wnry
- 055c7760512c98c8d51e4427227fe2a7ea3b34ee63178fe78631fa8aa6d15622 c.wnry
- 402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c r.wnry
- e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b s.wnry
- 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79 taskdl.exe
- 2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d taskse.exe
- 97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6 t.wnry
- b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25 u.wnry

观察到的 IP

- 188[.]166[.]23[.]127:443 - Tor 出口节点
- 193[.]23[.]244[.]244:443 - Tor 出口节点
- 2[.]3[.]69[.]209:9001 - Tor 出口节点
- 146[.]0[.]32[.]144:9001 - Tor 出口节点
- 50[.]7[.]161[.]218:9001 - Tor 出口节点
- 128.31.0[.]39 - Tor 出口节点
- 213.61.66[.]116 - Tor 出口节点
- 212.47.232[.]237 - Tor 出口节点
- 81.30.158[.]223 - Tor 出口节点
- 79.172.193[.]32 - Tor 出口节点

Tor C2

- xxlvbrloxvriy2c5.onion
- cwwnhwhlz52maqm7.onion
- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- 76jdd2ir2embyv47.onion

观察到的散列值

- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
- 428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f

- 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
- 62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
- 72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
- 85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
- a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
- a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
- 2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
- 7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
- a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
- fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
- 9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa

Tor 项目

在网络 PCAP 中存在一些看起来很奇特的域，这些域是来自 Tor 的项目，一般不认为它们是 IOC，不应将它们视为恶意域。

附录

该勒索软件加密的文件名列表：

```
.der、.pfx、.key、.crt、.csr、.p12、.pem、.odt、.sxw、.stw、.3ds、.max、.3dm、
.ods、.sxc、.stc、.dif、.slk、.wb2、.odp、.sxd、.std、.sxm、.sqlite3、.sqlitedb
、.sql、.accdb、.mdb、.dbf、.odb、.mdf、.ldf、.cpp、.pas、.asm、.cmd、.bat、.vbs
、.sch、.jsp、.php、.asp、.java、.jar、.class、.mp3、.wav、.swf、.fla、.wmv、
.mpg、.vob、.mpeg、.asf、.avi、.mov、.mp4、.mkv、.flv、.wma、.mid、.m3u、.m4u、
.svg、.psd、.tiff、.tif、.raw、.gif、.png、.bmp、.jpg、.jpeg、.iso、.backup、
.zip、.rar、.tgz、.tar、.bak、.ARC、.vmdk、.vdi、.sldm、.sldx、.sti、.sxi、
.dwg、.pdf、.wk1、.wks、.rtf、.csv、.txt、.msg、.pst、.ppsx、.ppsm、.pps、.pot、
.pptm、.pptx、.ppt、.xltm、.xltx、.xlc、.xlm、.xlt、.xlw、.xlsb、.xlsm、.xlsx、
.xls、.dotm、.dot、.docm、.docx、.doc
```

发布者：ALEXANDER CHIU；发布时间：18:09
标签：防护、恶意软件研究、MS17-010、勒索软件