2018 年 5 月 23 日，星期三

新型 VPNFilter 恶意软件将“魔爪”伸向全球至少 50 万台网络设备

简介

数月以来，Talos 一直与公、私部门的威胁情报合作伙伴以及执法机构合作，研究可能由国家支持或国属高级分子对我们称为“VPNFilter”的复杂模块化恶意软件系统的广泛使用。我们尚未完成研究，但近期活动使我们深信，正确的前进方向是即时分享调查结果，以便受影响方可采取适当行动保护自己。特别是，该恶意软件代码与 BlackEnergy 恶意软件代码重叠，而后者是针对乌克兰设备的多起大规模攻击的罪魁祸首。虽然这尚未最终定论，但我们还观察到，具有潜在破坏性的恶意软件 VPNFilter 正在利用专用于乌克兰的命令和控制 (C2) 基础设施，以惊人的速度感染该国主机。综合考量这些因素，我们认为最好在完成研究前发布目前取得的调查结果。尽早发布意味着我们尚未获得所有答案 - 我们甚至尚未发现所有问题 - 所以这篇博客代表我们到目前为止的调查结果，在继续调查的过程我们将随时更新。

此次攻击行动的规模和能力之大令人担忧。我们携手合作伙伴，估计至少有 54 个国家/地区的最少 50 万台设备受到感染。受 VPNFilter 影响的已知设备包括小型办公和家庭办公 (SOHO) 环境中的 Linksys、MikroTik、NETGEAR 和 TP-Link 网络设备以及 QNAP 网络附加存储 (NAS) 设备。据观察，尚无其他供应商（包括思科）受到 VPNFilter 感染，但我们将继续调查。这种恶意软件在网络设备上的行为尤为令人不安，因为通过 VPNFilter 恶意软件组件能够窃取网站凭证和监控 Modbus SCADA 协议。最后，该恶意软件具有破坏性，可能导致受感染设备无法使用，这可以在个别受害者计算机上触发或集体触发，并可能切断全球成千上万台受害者计算机的互联网接入。

这种威胁发起者所针对的设备类型很难保护。这些设备通常位于网络外围，不具备适当的入侵防御系统 (IPS)，且通常无可用的基于主机的保护系统，如防病毒 (AV) 软件包。我们不确定在任何特定情况下使用的特定漏洞，但大多数目标设备（尤其旧版本）具有能使攻击长驱直入的已知公开漏洞或默认凭证。所有这些都促成了这种威胁至少自 2016 年以来的悄然增长。

这篇博文为您呈现 Talos 博客中的常规技术发现。此外，我们将利用我们的调查结果和分析师背景，详细介绍这一威胁背后的间谍情报技术，以讨论威胁发起者的可能思维过程和决策。我们还将讨论如何防御这种威胁以及如何处理可能受感染的设备。最后，我们将分享目前为止所观察到的危害表现 (IOC)，但我们坚信还存在更多未知。

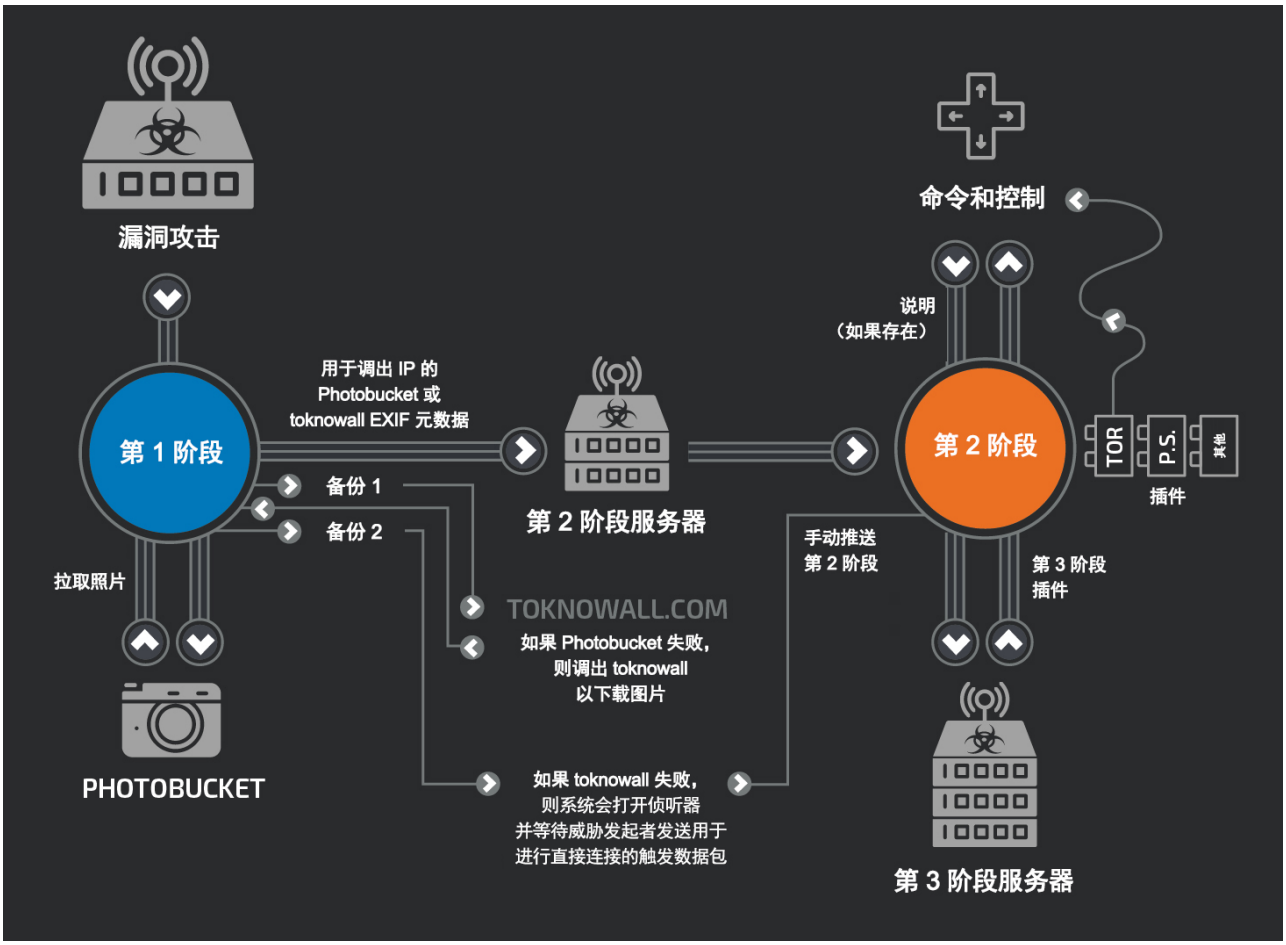
简要的技术分解

VPNFilter 恶意软件是一个多阶段的模块化平台，具有多种功能，可支持情报收集和破坏性的网络攻击操作。

第 1 阶段恶意软件会在计算机重启后继续存在，这与大多数其他针对物联网设备的恶意软件不同，因为恶意软件通常无法在设备重新启动后存续。第 1 阶段的主要目的是获取持久据点，以能够部署第 2 阶段恶意软件。第 1 阶段利用多个冗余命令和控制 (C2) 机制发现当前第 2 阶段部署服务器的 IP 地址，使得这种恶意软件极其强大并能够处理不可预测的 C2 基础设施变化。

第 2 阶段恶意软件（通过不会在重启后存续）拥有主力情报收集平台中的常见功能，例如文件收集、命令执行、数据泄露和设备管理。但是，第 2 阶段的某些版本还具有自毁功能，可覆盖设备固件的关键部分并重新启动设备，使设备无法使用。基于威胁发起者表现出的对这些设备的了解，以及第 2 阶段版本中的现有功能，我们非常肯定地评估威胁发起者可能将这种自毁指令部署至其控制的大多数设备，而不管命令是否内置于第 2 阶段恶意软件中。

此外，还存在多个用作第 2 阶段恶意软件插件的第 3 阶段模块。这些插件为第 2 阶段提供附加功能。在撰写本文时，我们了解到两个插件模块：用于收集通过设备传输的流量的数据包嗅探器（包括窃取网站凭证和监控 Modbus SCADA 协议）和允许第 2 阶段通过 Tor 进行通信的通信模块。我们非常肯定地评定，存在我们尚未发现的其他几个插件模块。



间谍情报技术讨论

我们极为肯定地评定，这种恶意软件用于创建可扩展且难以确定属性的基础设施，可用于服务威胁发起者的多种操作需求。由于受影响设备为企业或个人所合法拥有，因此从受感染设备进行的恶意活动可能会被错误地归咎于实际上是攻击受害者的那些人。内置于恶意软件各阶段和插件的功能极其广泛，能够使威胁发起者以多种方式利用设备。

高级威胁发起者（包括民族国家）将尽力使其网络活动难以确定归属，除非出于利益而公开他们进行的特定行为。为此，高级威胁发起者使用多种技术（包括由他人所有的共同基础设施）执行其操作。在连接至最终受害者前，威胁发起者可轻松使用感染此恶意软件的设备作为跳点，以便混淆其真实起点。

该恶意软件也可用于收集流经设备的数据。此类数据可用于简单的数据收集目的，或评估设备所服务网络的潜在价值。如果网络被视为具有威胁发起者可能感兴趣的信息，则其或许选择继续收集通过设备的内容或选择传播至连接网络以收集数据。在本文发布时，我们尚未获得能够进一步利用设备所服务网络的第三阶段插件。然而，我们已经看出其确实存在的迹象，且我们能够评定，如此高级的威胁发起者很可能会自然地将该功能纳入这种模块化恶意软件中。

最后，通过使用“kill”命令可将这种恶意软件用于进行大规模的破坏性攻击，导致部分或全部物理设备无法使用。此命令出现在我们观察到的众多第 2 阶段示例中，但也可通过利用所有第 2 阶段示例中的“exec”命令触发。在多数情况下，大多数受害者无法恢复这一操作，因为此项操作需要的技术能力、专门技术或工具是一般消费者所不具备的。我们对该功能极为担忧，这也是我们在过去几个月中一直悄然研究这种威胁的主要原因之一。

观察到的关注活动

在我们研究这种威胁时，我们实施了监控和扫描，来了解这一威胁的范围和受感染设备的行为。我们的分析表明，这是种全球性广泛部署的威胁，正在积极寻求扩张其范围。在继续进行研究的同时，我们也观察到与此威胁发起者具有潜在关联的活动表现出可能的数据泄露活动。

5 月初，我们观察到受感染设备在端口 23、80、2000 和 8080 执行 TCP 扫描。这些端口表现出对正在使用这些端口的其他 Mikrotik 和 QNAP NAS 设备进行扫描。这些扫描针对 100 多个国家/地区的设备。

我们还利用遥感勘测来发现全球潜在的受感染设备。此外，我们评估了其集体行为，以试图确定 C2 基础设施的其他功能。众多这些受害者 IP 表现出极其明显的数据泄露行为。

最后，在 5 月 8 日，我们观察到 VPNFilter 感染活动急剧增加。几乎发现的所有新受害者都位于乌克兰。还值得注意的是，大多数乌克兰受感染设备均共享来自世界其他地方的位于 IP 46.151.209[.]33 上的单独第 2 阶段 C2 基础设施。到目前为止，我们意识到了 BlackEnergy 和 VPNFilter 间的代码重叠，且先前在乌克兰发生的攻击时间表明下一场攻击即将来临。鉴于这些因素以及在与合作伙伴磋商后，我们决定不等研究完成而立即公布已掌握的信息。

在推进公开披露期间，我们又于 5 月 17 日观察到集中在乌克兰的新一批 VPNFilter 受害者大幅增长。这使我们更加确定了要尽快发布我们的研究成果。

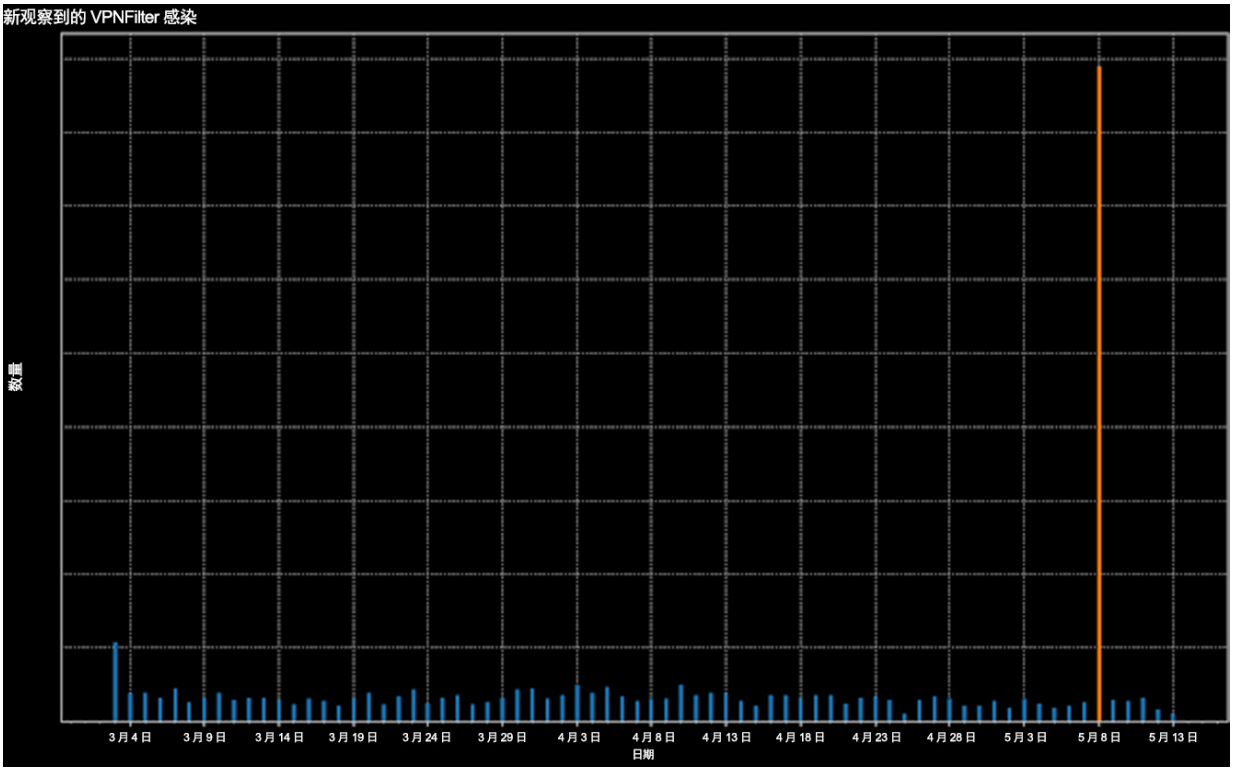


图 1。随时间推移新观察到的 VPNFilter 感染

抵御这种威胁

由于受影响设备的性质，抵御这种威胁极其困难。其中大多数设备均直接连接至互联网，与潜在攻击者之间不存在安全设备或安全服务。并且一个事实是大多数受影响设备具有众所周知的漏洞且普通用户难以修补，这进一步加剧了面临的挑战。此外，大多数设备没有内置的防恶意软件功能。这三个事实综合起来使得防范这一威胁极其困难，导致拦截恶意软件、消除漏洞或阻止威胁的机会严重受限。

尽管面临这些挑战，Talos 已发布了从多个角度应对这种威胁的防御措施，以充分利用现存的有限选择。我们开发和部署了超过 100 个 Snort 签名，用于检测和阻止与此威胁相关联设备上可能的众所周知的漏洞。这些规则已部署到公共 Snort 集中，任何人均可使用这些规则帮助保护其设备。此外，我们已按惯常做法视情况将某些域名/IP 列入黑名单，并将与此威胁相关的散列进行“定罪”以覆盖受思科安全生态系统保护的那些设备。我们已就此问题与 Linksys、Mikrotik、Netgear、TP-Link 和 QNAP 进行了沟通。（注：QNAP 已意识到 VPNFilter 的某些方面，且先前已做好威胁防范工作。）最后，我们还在本文发布前与国际执法机构和网络威胁联盟的其他成员分享了这些指标和我们的研究成果，以便他们能够迅速采取行动，帮助在更大范围内应对这一威胁。

建议

我们建议：

- SOHO 路由器和/或 NAS 设备的用户将设备重置为出厂默认设置并重新启动，以清除具有破坏性的非持久性潜在第 2 阶段和第 3 阶段恶意软件。
- 为用户提供 SOHO 路由器的互联网服务提供商代表客户重新启动路由器。
- 如果您有任何已知或疑似受此威胁影响的设备，请务必与制造商合作确保您的设备具有最新版本的修补程序。如果不是最新版本，则应立即应用更新的修补程序。
- ISP（互联网服务提供商）积极与其客户合作，确保设备已经过修补，且应用最新的固件/软件版本。

由于威胁发起者可能采取破坏性行动，出于高度谨慎，我们建议所有 SOHO 或 NAS 设备均采取这些措施，无论这些设备是否已知受此威胁的影响。

多阶段技术细节

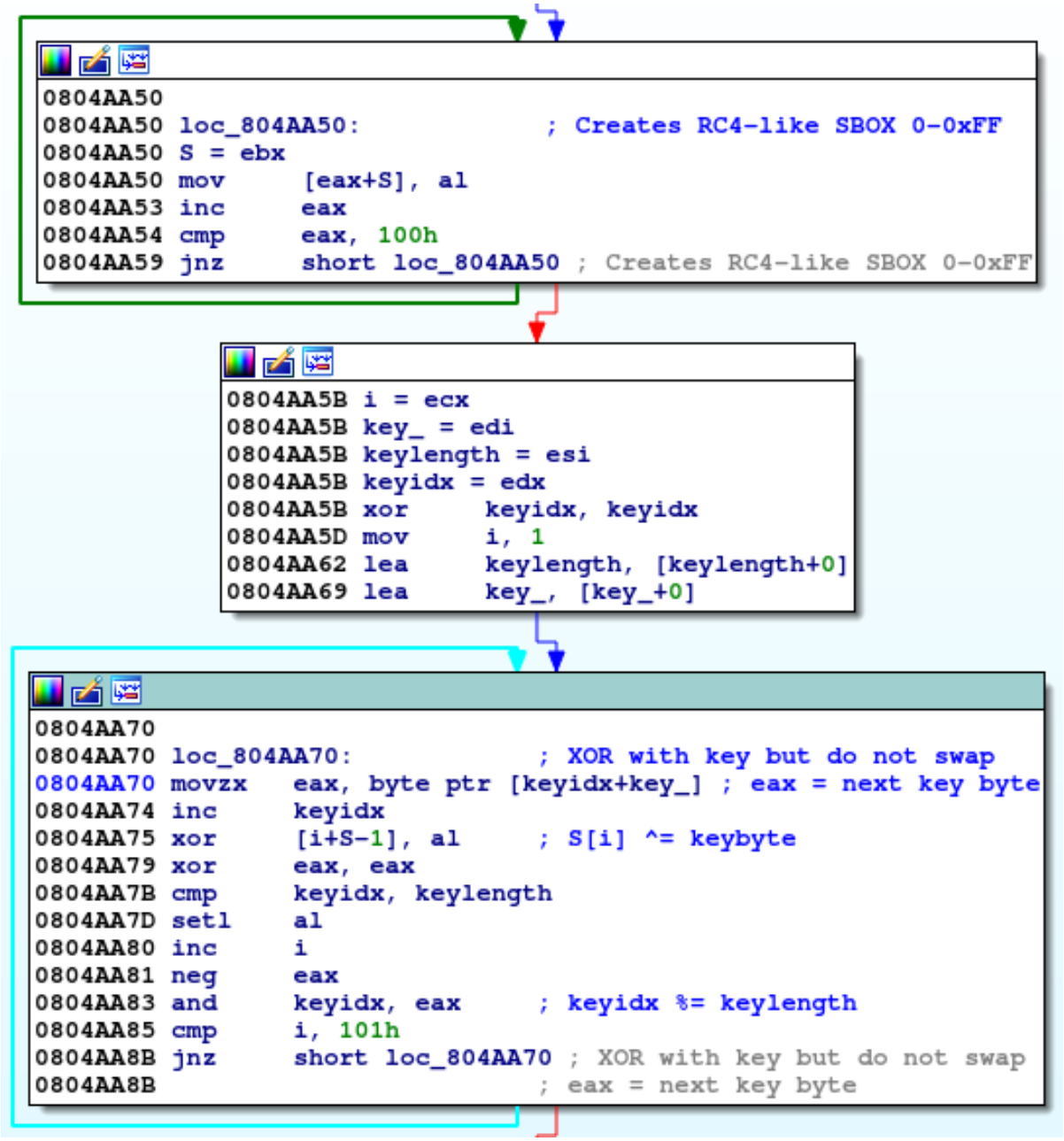
漏洞攻击

在本文发布时，就威胁发起者如何利用受影响设备，我们尚没有确凿的证据。但是，我们发现的所有受影响产品/型号均存在众所周知的公开漏洞。由于高级威胁发起者往往仅使用实现目标所需的最少资源，因此我们非常肯定地评定，VPNFilter 无需零日攻击技术。

第 1 阶段（持久性加载程序）

VPNFilter 第 1 阶段恶意软件感染基于 Busybox 和 Linux 运行固件的设备，并面向多种 CPU 架构编译。这些第一阶段二进制文件的主要目的是找到一台提供功能更全面的第二阶段的服务器，以及下载和维护下一阶段在受感染设备上的持久性。其能够修改非易失性配置内存 (NVRAM) 值，并将其自身添加至 Linux 任务安排程序 crontab 中以实现持久性。这与先前的物联网恶意软件有所不同，如转瞬即逝的 Mirai，只需简单的设备重启即会消失。

Talos 分析了用于 MIPS 和 x86 处理器的示例。C2 通信和其他恶意软件下载通过 Tor 或 SSL 加密连接进行。虽然二进制文件本身在被剥离后不会被混淆，但某些字符串以加密形式存储，且仅在运行时解密。在静态分析中，解密例程看起来与 RC4 非常相似，但似乎恶意软件作者将 S-box 的初始化搞错了。在置换步骤中，值被异或，但未交换。对此 RC4 实现的分析表明，该实现与在 BlackEnergy 中使用的（执法机构认为始自于国家行为者的）实现相同。



RC4 初始化会对内部状态初始化置换阶段中的值进行异或运算。正如您在最后的基本块中所见，代码不交换 S[i] 和 S[j] 的值（与下面的 RC4 伪代码相比）。

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap values of S[i] and S[j]
endfor
```

一旦恶意软件完成初始化，即开始从种子 URL 下载页面。在 MIPS 示例缓存和除一个 x86 示例 URL 以外的所有 URL 中，URL 均指向图像共享主机 Photobucket.com。恶意软件从 URL 引用的图库中下载第一个图像，然后继续提取下载服务器的 IP 地址。IP 地址提取自 EXIF 信息中的六个 GPS 经纬度整数值。

如果第 1 阶段无法连接至 Photobucket、无法从 Photobucket 下载图像，或无法通过从 Photobucket 下载的图像成功获取 IP 地址，恶意软件则会转至备份域 toknowall[.]com 下载图像并尝试相同的过程。

如果备份域的连接尝试失败，第 1 阶段会打开一个侦听器，等待特定触发数据包打开连接，以便威胁发起者交互连接至设备。打开侦听器后，其会从 api.ipify[.]org 中查看触发数据包的公共 IP 并存储以供稍后比较。然后，在任何数据包到达任何端口时，侦听器均会执行一系列检查以识别触发数据包。如果数据包符合预定义的一组标准，则侦听器将从该数据包中提取 IP 地址并尝试第 2 阶段下载。

侦听器操作

1. 检查所有带 SYN 标志设置的 TCP/IPv4 数据包
2. 检查目标 IP 是否与侦听器打开后找到的内容匹配（注：如果侦听器未能从 api.ipify[.]org 中获取 IP，则会跳过此检查）
3. 确保数据包具有八个或更多字节
4. 扫描字节 \x0c\x15\x22\x2b 的数据
5. 紧接在 4 字节标记后的字节可以理解为 IP，则 \x01\x02\x03\x04 变为 -> 1.2.3[.]4
6. 对于第 2 阶段，照例调出新接收的 IP
7. 确认第 2 阶段至少为 1,001 个字节（注：这比其他调出方法少得多，其他的会要求第 2 阶段至少为 100,000 个字节）

第 2 阶段（非持久性）

第 2 阶段恶意软件首先通过创建模块文件夹 (/var/run/vpnfilterm) 和工作目录 (/var/run/vpnfilterw) 来设置工作环境。之后，它会运行一个循环，首先到达 C2 服务器，然后执行从 C2 中检索的命令。命令名称使用与第 1 阶段中一样断开的 RC4 函数加密。幸运的是，较早版本的 x86 第 2 阶段示例非常详细，并调试打印了其执行的所有步骤。较新版本的 x86 第 2 阶段不包含调试打印，MIPS 示例也不包含。

x86 示例可执行以下操作：

- kill：用 0 覆盖 /dev/mtdblock0 的前 5,000 个字节，然后重新启动设备（有效地对其进行刷新）。
- exec：执行 shell 命令或插件。
- tor：设置 Tor 配置标志（0 或 1）。

- copy：将文件从客户端复制到服务器。
- seturl：设置当前配置面板的 URL。
- proxy：设置当前的代理 URL。
- port：设置当前的代理端口。
- delay：设置主循环执行间的时延。
- reboot：如果设备启动超过 256 秒，则重新启动设备，并在参数中指定版本名称。
- download：将 URL 下载到文件。这可应用于所有设备或仅应用于特定的版本名称。

MIPS 示例另具有以下操作：

- stop：终止恶意软件进程。
- relay：来自 x86 版本的“delay”命令的拼写错误版本。

安装 Tor 模块前，第 2 阶段会将其配置中存储的一个或多个 IP 用作 Tor 的 SOCKS5 代理，并尝试与其配置中找到的控制面板进行通信。如在第 1 阶段中，恶意软件与代理间的通信将通过经验证的 SSL 连接进行连接。安装 Tor 模块后，第 2 阶段会通过本地 SOCKS5 代理连接到 .onion 域，而本地 SOCKS5 代理由该模块通过普通 HTTP 提供。我们使用了伪 SOCKS5 代理，将所有流量重定向至 INetSim 进行分析。

从恶意软件到服务器的请求示例：

{

"uq":"px(01:02:03:04:05:06)",

"pv":"pPRXi686QNAPX86",

"ad":"10.0.0.1",

"bv":"0.11.1a/0.3.9qa",

"nn":"YnVpbGRyb290",

"tn":"",

"on":"1"

}

恶意软件将此请求编码成一个 JSON 对象，然后进行 base64 编码并发送至 HTTP POST 参数“me”中的路径 /bin32/update.php。由于版本“Windows NT 5.3”不存在，请求中使用的用户代理是特有的（Mozilla/6.1（兼容 MSIE 9.0、Windows NT 5.3、Trident/5.0））。

- uq：受感染设备的唯一 ID（恶意软件网络接口的 MAC 地址）。
- pv：恶意软件运行的平台版本
- ad：恶意软件设备的公共 IP 地址
- bv：第 1 阶段加载程序 (0.3.9qa) 和第 2 阶段二进制文件 (0.11.1a) 的版本
- nn：节点名称
- tn：Tor 标志
- on：onion 标志

服务器对消息的响应：

{

"tr":3060,

"pxs":["217.12.202.40","94.242.222.68","91.121.109.209"],

"tor":"tor 1",

"mds":[]

}

- tr：设置主循环时延。
- pxs：连接到的面板列表。这些是 C2 服务器。
- tor：设置 Tor 模块的名称和版本。
- mds：要获取的模块列表。各条目格式为“<command_id> <module_id> <module_name> <module_args (base64-encoded)>”。恶意软件通过将 POST 表单参数 me 设为添加架构的模块名称（例如，适用于 Tor 模块的 tor_i686），从 /bin32/update.php 下载模块，并在每次迭代中执行该模块。一个空白命令列表（如上面的示例响应）会通过停用命令和终止与其相关联的任何正在运行的进程来清除任何现有命令。

第 3 阶段（非持久性）

我们已分析该恶意软件的两个插件模块，即数据包嗅探器和允许恶意软件通过 Tor 进行通信的通信插件。可以肯定，很可能还有若干个我们尚未发现的插件模块。在 Talos 获得的初始示例中，有一个 MIPS 第 2 阶段插件，其为数据包嗅探器。该插件通过原始套接字拦截所有网络流量，并查找 HTTP 基本身份验证中使用的字符串。此外，它还专门跟踪 Modbus TCP/IP 数据包。其生成的日志文件位于第 2 阶段工作目录 /var/run/vpnfilterw 中。这使得攻击者能够了解、捕获并跟踪流经设备的流量。

Tor 插件模块部分链接到第 2 阶段，但具有单独的 Tor 可执行文件，该文件被下载至 /var/run/tor 并在与第 2 阶段不同的进程中运行。Tor 二进制文件采用静态链接和剥离二进制文件的形式，看起来像标准的 Tor 客户端。其在 /var/run/torrc 中创建配置文件和在 /var/run/tord 中创建工作目录。

结论

VPNFilter 是种具有扩张性、强劲、功能强大且危险的威胁，将难以实施防御措施的设备作为目标。其高度模块化的框架允许快速更改威胁发起者的操作基础设施，以服务其错误归因、情报收集和寻找攻击平台的目标。

该恶意软件的破坏能力尤其让我们担心。我们发现威胁发起者愿意刻录用户设备来掩盖其踪迹，而不仅仅是删除恶意软件痕迹。如果某一命令符合威胁发起者的目标，则该命令会被广泛执行，这可能会导致成千上万台设备无法使用，使全球范围内或满足威胁发起者目的的重点区域中成千上万名受害者无法接入互联网。

虽然针对物联网设备的威胁不足为奇，但是被更高级的民族、国家的威胁发起者使用这些设备进行网络操作（可能导致设备被破坏）这一事实大大增加了处理此问题的紧迫性。我们呼吁整个安全界与我们联手，来积极应对这一威胁。

随着威胁不断发展，我们将继续监控 VPNFilter，并与我们的合作伙伴合作，以确保我们的客户持续受到保护并向公众公布调查结果。

危害表现 (IOC)

如前所述，我们高度怀疑还有其他我们目前尚未发现的这一恶意软件的其他 IOC 和版本。以下 IOC 列表包含我们迄今所掌握的情况。

已知 C2 域和 IP

与第 1 阶段相关联

photobucket[.]com/user/nikkireed11/library
photobucket[.]com/user/kmila302/library
photobucket[.]com/user/lisabraun87/library
photobucket[.]com/user/eva_green1/library
photobucket[.]com/user/monicabelci4/library
photobucket[.]com/user/katyperry45/library
photobucket[.]com/user/saragray1/library
photobucket[.]com/user/millerfred/library
photobucket[.]com/user/jeniferaniston1/library
photobucket[.]com/user/amandaseyfried1/library
photobucket[.]com/user/suwe8/library
photobucket[.]com/user/bob7301/library
toknowall[.]com

与第 2 阶段相关联

91.121.109[.]209
217.12.202[.]40
94.242.222[.]68
82.118.242[.]124
46.151.209[.]33
217.79.179[.]14
91.214.203[.]144
95.211.198[.]231
195.154.180[.]60
5.149.250[.]54
91.200.13[.]76
94.185.80[.]82
62.210.180[.]229
zuh3vcyskd4gipkm[.]onion/bin32/update.php

已知文件散列

第 1 阶段恶意软件

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec
0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92

第 2 阶段恶意软件

9683b04123d7e9fe4c8c26c69b09c2233f7e1440f828837422ce330040782d17
d6097e942dd0fdc1fb28ec1814780e6ecc169ec6d24f9954e71954eedbc4c70e

4b03288e9e44d214426a02327223b5e516b1ea29ce72fa25a2fcef9aa65c4b0b
9eb6c779dbad1b717caa462d8e040852759436ed79cc2172692339bc62432387
37e29b0ea7a9b97597385a12f525e13c3a7d02ba4161a6946f2a7d978cc045b4
776cb9a7a9f5afbaffdd4dbd052c6420030b2c7c3058c1455e0a79df0e6f7a1d
8a20dc9538d639623878a3d3d18d88da8b635ea52e5e2d0c2cce4a8c5a703db1
0649fda8888d701eb2f91e6e0a05a2e2be714f564497c44a3813082ef8ff250b

第 3 阶段插件

f8286e29faa67ec765ae0244862f6b7914fcdde10423f96595cb84ad5cc6b344
afd281639e26a717aead65b1886f98d6d6c258736016023b4e59de30b7348719

自签证书指纹

d113ce61ab1e4bfcb32fb3c53bd3cdeee81108d02d3886f6e2286e0b6a006747
c52b3901a26df1680acbfb9e6184b321f0b22dd6c4bb107e5e071553d375c851
f372ebe8277b78d50c5600d0e2af3fe29b1e04b5435a7149f04edd165743c16d
be4715b029cbd3f8e2f37bc525005b2cb9cad977117a26fac94339a721e3f2a5
27af4b890db1a611d0054d5d4a7d9a36c9f52dffeb67a053be9ea03a495a9302
110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8
fb47ba27dceea486aab7a0f8ec5674332ca1f6af962a1724df89d658d470348f
b25336c2dd388459dec37fa8d0467cf2ac3c81a272176128338a2c1d7c083c78
cd75d3a70e3218688bdd23a0f618add964603736f7c899265b1d8386b9902526
110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8
909cf80d3ef4c52abc95d286df8d218462739889b6be4762a1d2fac1adb2ec2b
044bfa11ea91b5559f7502c3a504b19ee3c555e95907a98508825b4aa56294e4
c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412
8f1d0cd5dd6585c3d5d478e18a85e7109c8a88489c46987621e01d21fab5095d
d5dec646c957305d91303a1d7931b30e7fb2f38d54a1102e14fd7a4b9f6e0806
c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412

已知受影响设备

已知受到此威胁影响的设备如下所列。由于这项研究的规模之大，我们的许多观察结果是远程而非在设备上得出的，因此在很多情况下难以确定具体的版本号和型号。需要指出的是，所有这些设备均具有相关的公开已知漏洞。

鉴于对此威胁的观察结果，我们极为肯定地评定，此列表并不完整且可能有其他设备受到影响。

LINKSYS 设备：

E1200
E2500
WRVS4400N

用于云核心路由器的 MIKROTIK ROUTEROS 版本：

1016
1036
1072

NETGEAR 设备：

DGN2200
R6400
R7000
R8000
WNR1000
WNR2000

QNAP 设备：

TS251
TS439 Pro

运行 QTS 软件的其他 QNAP NAS 设备

TP-LINK 设备：

R600VPN

覆盖范围

思科高级恶意软件保护 (AMP)、云网络安全 (CWS)、网络安全、ThreatGrid、Umbrella 和网络安全设备 (WSA) 均可保护思科客户免受此威胁的侵害。此外，StealthWatch 和 StealthWatch Cloud 可用于查找与已知 C2 IP 地址和域进行通信的设备。

在 StealthWatch 中，需要进行两项配置以发送存在与恶意 IP 地址进行通信的风险通告。

- 第一步是使用 Java 用户界面在“外部主机”下创建名“VPNFilter C2”的新主机组。
- 创建后，您可能需要验证目前没有正在进行的通信。
- 验证方式为右键点击最近创建的“VPNFilter C2”主机组，然后导航至“热门”-> “对话”-> “总计”。
- 查看这些热门对话，即可轻松发现是否存在活动流量。
- 如果无活动流量，您可以创建风险通告，以在观察到任何进出“VPNFilter C2”主机的流量时生成风险通告。
- 风险通告的配置方式为：创建一个自定义事件，并在网络用户界面中选择适当的主机或对象。

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

VPNFILTER 特定 SNORT 检测：

45563 45564 46782 46783

防范受影响设备中已知漏洞的 SNORT 规则：

25589 26276 26277 26278 26279 29830 29831 44743 46080 46081 46082 46083 46084 46085 46086 46287 46121 46122 46123 46124 41445 44971 46297 46298 46299 46300 46301 46305 46306 46307 46308 46309 46310 46315 46335 46340 46341 46342 46376 46377 37963 45555 46076 40063 44643 44790 26275 35734 41095 41096 41504 41698 41699 41700 41748 41749 41750 41751 44687 44688 44698 44699 45001 46312 46313 46314 46317 46318 46322 46323 40866 40907 45157

CLAMAV 签名：

Unix.Trojan.Vpnfilter-6425811-0
Unix.Trojan.Vpnfilter-6425812-0
Unix.Trojan.Vpnfilter-6550590-0
Unix.Trojan.Vpnfilter-6550591-0
Unix.Trojan.Vpnfilter-6550592-0

发布者：WILLIAM LARGENT；发布时间：9:00
标签：AMP、CLAMAV、物联网、SNORT 规则、TALOS、威胁情报、威胁研究、VPNFILER