VPNFilter分析

angel010 / 2018-05-28 16:16:16 / 浏览数 3376 技术文章 技术文章 顶(0) 踩(0)

简介

VPNFilter恶意软件的代码与BlackEnergy恶意软件有重叠，而BlackEnergy恶意软件对乌克兰的目标设备发起了多次大规模攻击。而VPNFilter也以惊人的速度感染了乌克兰

该攻击活动的规模和能力都是让人担忧的。研究人员预计有超过54个国家的50万设备被感染。已知受VPNFilter影响的设备有家用和小型办公场所使用的Linksys, MikroTik, NETGEAR,TP-Link网络设备，以及QNAP
NAS设备。VPNFilter在网络设备上的行为也是让人担忧的，因为恶意软件的组件会窃取网站的身份凭证并监控Modbus SCADA协议。

最后，恶意软件还有一个破坏性的能力，就是让受感染的设备无法使用。这可以在单个设备上触发，也可以大规模地触发，比如同时切断上万设备的网络连接。

被攻击的终端设备也很难防护，因为这些设备一般都位于网络的边界，没有IPS的保护，也没有可用的基于主机的保护系统。从已知的情况来看，目前大多数被攻击的设备，

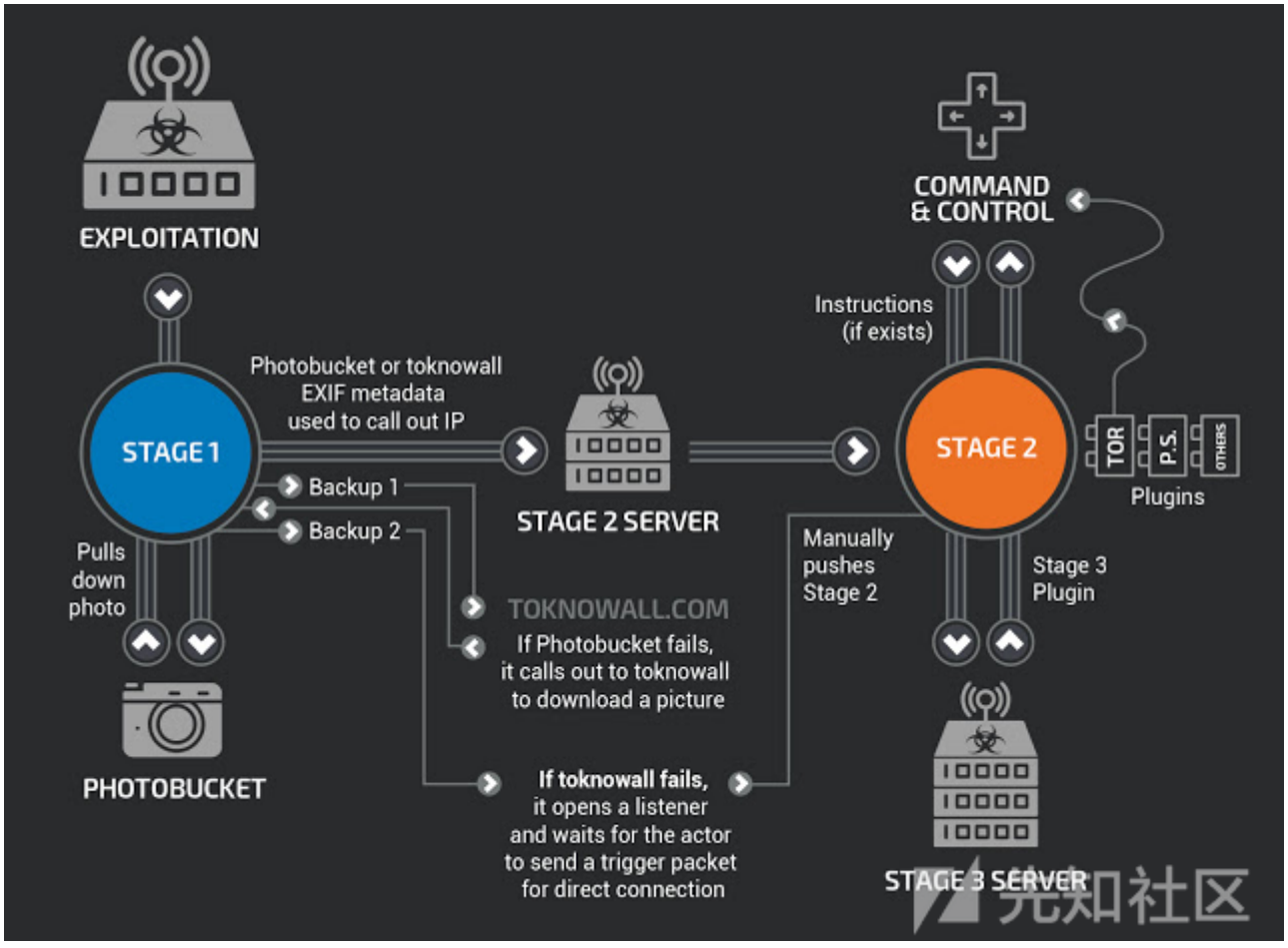
技术总结

VPNFilter恶意软件是一个多阶段的、支持多平台的进行情报收集和破坏性的网络攻击活动。

在stage 1，恶意软件通过重启来达到驻留的目的。因为大多数的攻击物联网设备的恶意软件在重启后都不能存留。Stage 1的主要目的是完成驻留和启用stage 2的恶意软件。Stage 1使用了多个冗余的C2机制来发现当前stage 2阶段的服务器，这让恶意软件在应对C2基础设施的变化上极具鲁棒性。

Stage 2的恶意软件在重启之后是不能驻留的，具有情报收集的功能，包括文件收集、命令执行、数据泄漏和设备管理等。但一些版本的stage 2还具有自破坏的能力，可以覆写设备固件的关键部分、重启设备，让设备不可用。基于攻击者对这些设备和对stage 2现有能力的了解，研究人员认为攻击者对所控制的大多数的设备都使用了自毁命令。

还有多个stage 3模块作为stage 2恶意软件的插件。这些插件提供给stage 2的恶意软件一些额外的功能，包括收集流量的packet sniffer和允许stage 2与Tor进行通信的模块。研究人员认为还有其他的模块没有被发现。



情报讨论

研究人员认为该恶意软件是用来创建一个服务与攻击者多个运营需求的基础设计。因为这些受感染的设备是被企业或个人合法拥有的，所以这样设备的活动可能会被错误地

恶意软件可以被用来收集流经设备的数据。这可以直接作为数据收集使用，或判定网络的潜在价值。如果网络对攻击者来说有潜在的价值，攻击者可能会继续收集流经设备的
3插件。但研究人员发现了一些线索，研究人员认为这些高级单元非常有可能会含有该模块中恶意软件所拥有的功能。

最后，恶意软件可以用kill命令来进行大规模地破坏性活动，这会使用大量的物理设备不可用。这个命令在很多stage 2的样本中出现过，但可以用所有的stage
2样本中的exec命令来触发。在大多数的例子中，对大多数的受害者来说，这个动作是不可逆的，因为首先需要技术能力、还需要了解原理、受害者还需要有必要的工具。

如何应对威胁

因为受感染的设备的一些天生的性质，导致了应对威胁困难重重。许多设备都是直接联网的，在这些设备和潜在的攻击者之间是没有安全设备和服务的。而且许多设备都有已

建议

研究人员提出了以下建议：
使用SOHO路由器或NAS设备的用户应该重置设备到工厂模式的默认配置，并重启设备来移除潜在的stage 2和stage
3阶段的恶意软件。提供SOHO路由器的ISP应该以为客户去考虑，重启路由器。如果用户的设备有上面提到的漏洞，那么用户应该确保设备的固件版本和系统是最新的。ISP

多stage技术分析

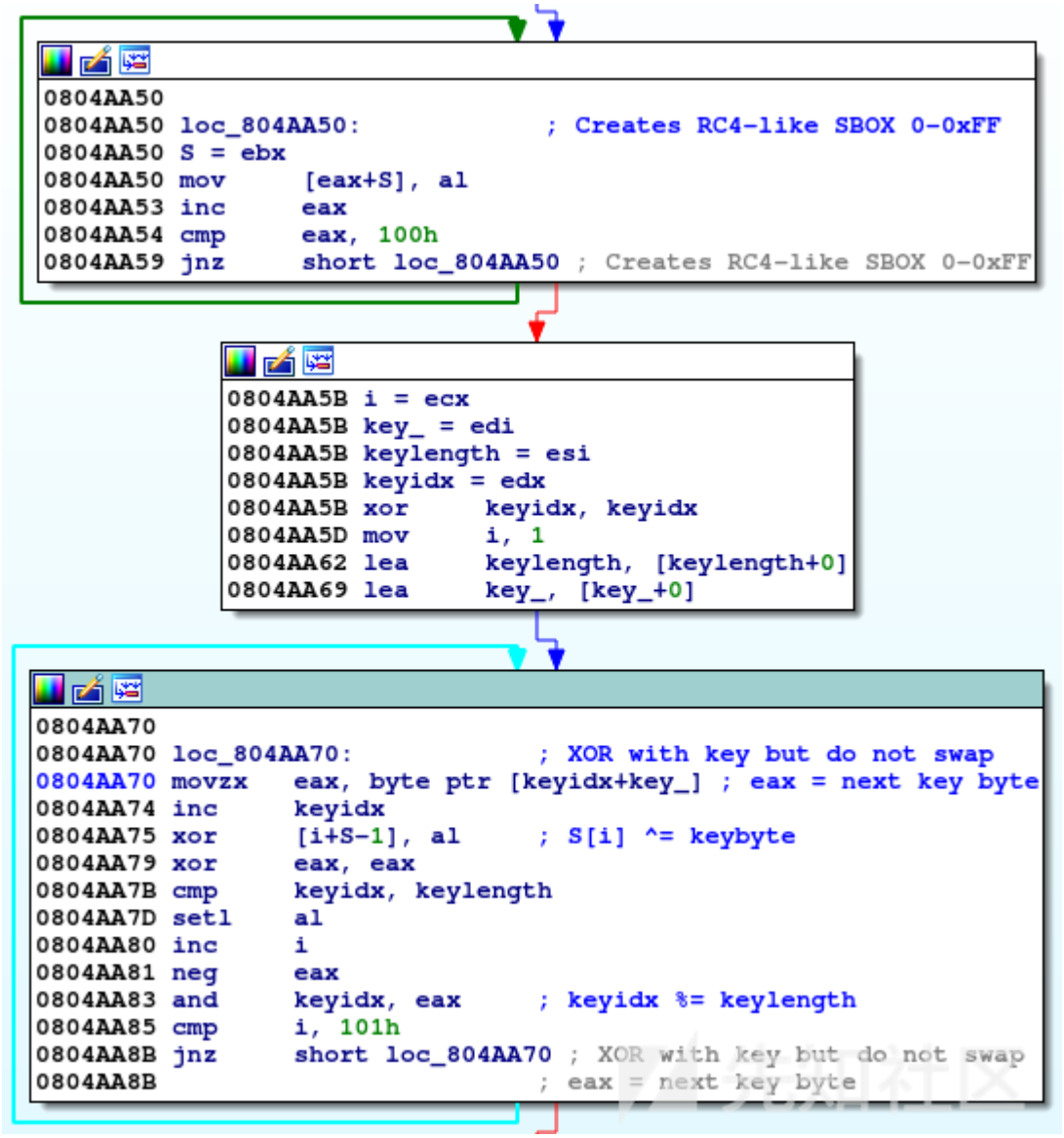
利用

截止发稿，研究人员仍不清楚威胁单元是如何利用这些受影响的设备的。但所有这些受影响的设备和型号都有一个共同点：拥有公开的漏洞。因为高级的威胁者一般都会用最

STAGE 1 (PERSISTENT LOADER)

VPNFilter的stage 1恶意软件感染的设备运行的固件都是基于Busybox和Linux的，这些固件会编译为不同的CPU架构。Stage
1阶段的恶意软件的主要目的就是定位提供stage 2恶意软件的服务器，并在受感染的设备上下载和保持驻留。可以通过修改一些非易失性设置（non-volatile
configuration
memory，NVRAM）的值，把自己加入到crontab中来达到驻留的目的。这与Mirai这样的物联网恶意软件是不同的，因为那些恶意软件在设备重启后就消失了。

研究人员分析了MIPS和x86处理器的样本，发现C2通信和其他的恶意软件下载是通过Tor和SSL加密连接完成对。当二进制文件本身没有混淆的话，一些字符串是以一种加密



RC4初始化过程会对内部状态初始化阶段的值进行XOR运算。就如上面的最后一个基本区块中描述的一样，代码不会交换S[i]和S[j]的值。

```
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过程，就会从seed
URL下载页面。在样本中，缓存指向的是Photobucket.com，一个图片分享的主机。恶意软件会从URL的图片库中下载第一张图片，然后提取下载服务器的IP地址。IP地址是

如果stage 1没有成功连接或从Photobucket的图片上获取IP地址，恶意软件就会到备份的域名toknowall[.]com去下载图片，去获取IP地址。

如果这个连接备份域名的过程也失败了，stage
1就会开启一个监听器来等待特殊的触发包来建立一个攻击者与设备之间的连接。监听器开启后，就会从api.ipify[.]org检查公网的IP地址，并保存进行后续的比较。当有包到

如果包满足预设的标准，就从包中提取IP地址然后尝试stage 2的下载。

STAGE 2 (非驻留)

Stage
2恶意软件首先会创建一个模块文件夹(/var/run/vpnfilterm)和工作目录(/var/run/vpnfilterw)来完成整个工作环境的设定。之后会运行loop，首先会到达C2服务器，然后执
stage2样本非常冗长，debug会打印执行的所有步骤。X86 stage 2的新版本并不含有debug print，MIPS样本中也没有。

STAGE 3 (非驻留)

研究人员分析了恶意软件的两个插件莫款，恶意软件用packet sniffer和通信插件通过Tor通信。packet sniffer会检查所有的网络流量，并寻找HTTP基本认证使用的字符串。然后记录Modbus TCP/IP包，产生的日志保存在stage 2的工作目录下/var/run/vpnfilterw。这让攻击者可以理解、获取、记录流经设备的流量。

Tor插件模块是与stage 2关联的，但还有一个单独的Tor可执行文件要下载到/var/run/tor目录中，并以一个与stage 2独立的进程去运行。Tor二进制文件看起来是一个标准的Tor客户端，会在/var/run/torrc和工作目录/var/run/tord创建配置文件。

结论

VPNFilter是一个大规模、鲁棒的、有很多功能的、危险的威胁，而且攻击的目标设备很难防护。高度模块化的架构可以让攻击者的运营基础设施迅速变化，服务情报收集、

https://blog.talosintelligence.com/2018/05/VPNFilter.html