(http://blog.nsfocus.net/)

全新恶意软件VPNFilter控制全球至少50万台网络设备

a day ago (http://blog.nsfocus.net/vpnfilter/) 田泽夏 (http://blog.nsfocus.net/author/tianzexia/)
（）

阅读： 81

近日，有一款名为VPNFilter的恶意软件被发现感染了至少50万的网络设备，Talos团队在近几个月来一直在与各威胁情报厂商和执法机构合作，通过研究后发现，这款恶意软件十分先进，可能是由国家资助或与国家级别的攻击者发起的，是一种先进的模块化恶意软件系统（modular malware system）。 本文揭示了该恶意软件的技术细节并提出了防护措施。

虽然目前研究还没有完全完成，但是公开的信息应该会有助于受影响的客户可以及时的采取防护措施。 值得一提的是，该恶意软件的代码与BlackEnergy恶意软件有相似的代码片段，BlackEnergy恶意软件曾经针对乌克兰设备发起过多次大规模攻击。 虽然还无法完全肯定，但VPNFilter作为一种潜在的破坏性恶意软件，利用特别的CC（Command & control）措施，正在以惊人的速度主动感染乌克兰主机。综合这些

因素，现在虽然还没有完全分析完成，但公布目前的结果可以很好的帮助各方采取相应的防护措施。

该恶意软件的破坏能力和影响规模都是值得注意的，在Talos 与其合作伙伴的统计下，全球至少54个国家/地区受影响，感染的设备数量至少为500,000。 受VPNFilter影响的已知设备有小型和家庭办公室（SOHO）空间中的Linksys，MikroTik，NETGEAR和TP-Link网络设备以及QNAP网络附加存储（NAS）设备。 目前没有其他供应商，包括思科（Cisco），被观察到被VPNFilter感染。 这种恶意软件在网络设备上的行为尤其令人关注，因为VPNFilter恶意软件的组件可以窃取网站证书并监控Modbus SCADA协议。 最后，恶意软件具有破坏性能力，可能导致受感染的设备无法使用，这可能会在个别受害者机器上触发或集体触发，因此有可能切断全球数十万受害者的互联网接入。

另外，受该恶意软件攻击的设备很难进行防护。 因为它们经常位于网络的外围，没有入侵保护系统（IPS），并且通常没有可用的基于主机的保护系统，如防病毒（AV）软件。 目前研究人员还无法确认感染是如何进行的，但大多数设备，尤其是旧版本，都存在已知的公开的漏洞，这使得攻击者的攻击变得容易了很多也导致了自2016年以来这种威胁的悄然增长。

文章目录

更多内容

执行步骤

VPNFilter是一个多阶段的，模块化的，具有多种功能的，可支持情报收集和破坏性网络攻击操作的恶意软件。

第一阶段恶意软件通过重新启动而持续存在，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活。 阶段1的主要目的是获得持久的立足点，并能够部署后续的恶意软件。阶段1利用多个冗余C&C（C2）机制来发现当前阶段部署服务器的IP地址，使得这种恶意软件非常强大并且能够处理不可预测的C2基础设施变化。

第二阶段的恶意软件不会在重新启动后持续存在，它拥有情报收集平台的功能，例如文件收集，命令执行，数据泄露和设备管理。 但是，阶段2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，使其无法使用。 目前经研究人员分析，该自毁功能很可能会被部署到所有受感染的设备上。

此外，第二阶段的恶意软件还拥有多个插件作为后续的第三阶段模块 ，提供附加功能。截止目前，共有两个插件模块：用于收集通过设备的流量的数据包嗅探器，包括窃取网站证书和监视Modbus SCADA协议以及允许阶段2通过Tor进行通信的通信模块。

Tradecraft讨论

Talos认真评估后，认为这种恶意软件是用来创建一个广泛的，难以追踪的，可用于满足攻击者的多种需求的平台。 由于受影响的设备由企业或个人合法拥有，因此从受感染设备进行的恶意活动可能会导致无法确认攻击的准确发生地区。 同时，内置于恶意软件各个阶段和插件的功能非常灵活，可以使攻击者以多种方式利用设备。

APT的幕后人员，包括民族国家，将尽力使其网络活动的归属判断变得极其困难，除非为了满足他们自己一些独特的需求，才会公开宣告归属。 为此，攻击者使用了多种技术，包括由他人拥有的共同基础设施来执行其操作。 在连接到最终受害者的终端设备之前，攻击者可以轻松使用受感染的设备作为中转，以便混淆它们的真实位置。

恶意软件也可以用来收集设备的数据。 除了单纯的数据收集，攻击者可能也会评估该设备所在网络的潜在价值。如果攻击者判断该设备网确实有价值，可能会选择继续收集信息并且连接到设备所在的网络来获取更多信息。 截止目前，研究人员尚未获得能够进一步利用设备所服务的网络的第三阶段插件，但是的确发现了该功能插件存在的痕迹，攻击者可以很轻松的讲这个功能加入到模块化的恶意软件中。

最后，攻击者可以通过使用“kill”命令使感染的设备进行大规模的破坏性攻击，这会导致部分或全部物理设备无法使用。 该命令出现在观察到的许多阶段2样本中，但也可以通过利用所有阶段2样本中的“exec”命令来触发。 在大多数情况下，大多数受害者无法恢复此项，因为恢复所需要的技术能力，专有技术或一些工具通常是平台用户所没有的。 这就使得情况变得十分危急，迫使研究人员们进行更多的研究。

观察到的恶意行为

在5月初，研究人员通过扫描观察到该威胁涉及全球。随后在端口23,80,2000和8080上进行TCP扫描受感染设备，这些端口表明了该恶意软件在扫描其他Mikrotik和QNAP NAS设备，针对100多个国家/地区。 这些受害者中的许多IP似乎很明确的表现其数据泄露的行为。

最后，在5月8日，Talos团队观察到VPNFilter感染行为急剧增加。 几乎所有新的受害者都位于乌克兰。 还值得注意的是，大多数乌克兰感染共享了来自世界其他地方的独立第2阶段C2基础设施，IP 46.151.209 [。] 33。 在这一点上，研究人员意识到BlackEnergy和VPNFilter之间的代码重叠，根据之前乌克兰的攻击，这一轮攻击很可能即将发生。 在5月17日，乌克兰的受感染设备再次大幅增加，鉴于这些因素，Talos团队决定提前公开研究结果。

技术细节

利用

目前，研究人员还没发现攻击者是如何利用这些受感染的设备的，但是鉴于这些设备都存在公开的漏洞，推测VPNFilter不需要其他的0-day攻击技术。

阶段1加载器

VPNFilter的阶段1恶意软件会感染基于Busybox和Linux运行固件的设备，并针对多种CPU架构进行编译。 这些第一阶段二进制文件的主要目的是找到一台提供更全面的第二阶段的服务器，并下载并维护受感染设备的下一阶段的持久性。 它能够修改非易失性配置内存（NVRAM）值并将其自身添加到Linux作业调度程序crontab中以实现持久性，这与以前的物联网恶意软件有所不同。

Talos分析了用于MIPS和x86处理器的样本。 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之后不会被混淆，但某些字符串以加密形式存储，并且仅在运行时解密。 在静态分析中，解密程序看起来与RC4非常相似，但看起来恶意软件作者得在初始化s-box时出了错。 在置换步骤中，值被异或，但未交换。 对RC4实施情况的分析表明，它与BlackEnergy中使用的执法机构(https://translate.googleusercontent.com/translate_c?depth=1&hl=zh-CN&ie=UTF8&prev=_t&rurl=translate.google.com&sl=en&sp=nmt4&tl=zh-CN&u=https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf&xid=17259,15700022,15700124,15700149,15700168,15700173,15700186,15700189,15700190,15700201,15700205&usg=ALkJrhgQVADDC8HuzI40NiZMFrQpQNja7w)相同， 并认为应该来自国家级别的行为。

一旦恶意软件完成初始化，它就开始从种子URL下载相关页面。 在MIPS示例缓存和x86示例中，除一个URL之外的所有URL都指向图像共享主机Photobucket.com。 恶意软件从URL所引用的库中下载第一个映像，然后继续提取下载服务器的IP地址。 IP地址是从EXIF信息中的六个GPS纬度和经度整数值中提取的。

如果阶段1无法连接或从Photobucket中的图像IP地址下载图像或成功获取IP地址，则恶意软件会去备份的域toknowall [。] com下载图像并尝试相同的过程。

如果对备份域的尝试失败，则阶段1将打开一个侦听器（listener），该侦听器等待特定的触发包打开连接，以便演员交互连接到设备。 当侦听器打开时，它会从api.ipify [。] org中检查其公共IP并将其存储以供以后比较。 然后，当任何数据包到达任何端口时，监听器执行一系列检查来识别触发数据包。 如果数据包符合预定义的一组标准，它将从数据包中提取IP地址并尝试进行第2阶段下载。

listener行为：

- 检查所有设置了SYN标志的TCP / IPv4数据包
- 检查目标IP是否与侦听器打开时找到的内容匹配（注意：如果侦听器未能从ipify [。] org获取IP，它将跳过此检查）
- 确保数据包有八个或更多字节
- 扫描字节\ x0c \ x15 \ x22 \ x2b的数据
- 紧接在该4字节标记之后的字节被解释为IP，因此\ x01 \ x02 \ x03 \ x04变为- > 1.2.3 [。] 4
- 向第2阶段的平常呼叫新收到的IP
- 确认阶段2至少为1,001字节（注意：这比其他标注方法小得多，要求阶段2为100,000或更多）

阶段2（非持续）

阶段2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，它将运行在一个循环中，首先到达C&C服务器，然后执行从C&C中检索的命令。 命令名使用与阶段1中相同的RC4函数进行加密。幸运的是，较早版本的x86阶段2示例非常详细，并且调试打印了它执行的所有步骤。 较新版本的x86和MIPS样本在阶段2中不包含调试打印。

x86示例可以执行以下操作：

- kill：用零覆盖/ dev / mtdblock0的前5,000个字节，然后重启设备（有效地对其进行刷新）。
- exec：执行一个shell命令或插件。
- tor：设置Tor配置标志（0或1）。
- 复制：将文件从客户端复制到服务器。
- seturl：设置当前配置面板的URL。
- 代理：设置当前的代理URL。
- 端口：设置当前的代理端口。
- delay：设置主循环执行之间的延迟。
- 重启：如果设备启动超过256秒，则重新启动设备，并在参数中指定生成名称。
- 下载：将URL下载到文件。这可以应用于所有设备或只是一个特定的构建名称。

MIPS示例具有以下附加操作：

- 停止：终止恶意软件进程。
- relay：x86版本的 `delay` 命令的拼写错误版本。

在安装Tor模块之前，阶段2会将其配置中存储的一个或多个IP作为SOCKS5代理服务器使用，并尝试与其配置中找到的控制面板进行通信。 与阶段1一样，恶意软件与代理之间的通信将通过验证的SSL连接进行连接。 当安装Tor模块时，它将通过模块提供的本地SOCKS5代理通过普通的HTTP连接到.onion域名。

恶意软件将请求编码成一个JSON对象，然后以base64编码并发送到HTTP POST参数“me”中的路径/bin32/update.php。

阶段3（非持续）

研究人员已经分析了恶意软件的两个插件模块，一个数据包嗅探器和一个允许恶意软件通过Tor进行通信的通信插件，以及几个还未被发现的模块。 在Talos获取的最初样本中，有一个MIPS阶段2的插件，它是一个数据包嗅探器。 它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，它专门跟踪Modbus TCP / IP数据包。 生成的日志文件放置在第2阶段的工作目录/ var / run / vpnfilterw中。 这使得攻击者可以了解，捕获并跟踪流经设备的流量。

Tor插件模块部分链接到阶段2，但有一个单独的Tor可执行文件，该文件被下载到/ var / run / tor并运行在与阶段2分离的进程中。Tor二进制文件看起来像标准的Tor客户端，静态链接和剥离二进制的形式。 它在/ var / run / torrc中创建一个配置文件，并在/ var / run / tord中创建一个工作目录。

防护措施

由于受影响的设备的性质，针对此威胁进行防御非常困难。 他们中的大多数直接连接到互联网，他们和潜在的攻击者之间没有安全设备或服务。 由于大多数受影响的设备都具有已知的漏洞，这一事实进一步加剧了防护的难度。 另外，大多数设备没有内置的反恶意软件功能。 这使得该威胁非常难以抵消，拦截恶意软件，消除漏洞或阻止威胁的机会极其有限。

尽管面临这些挑战，Talos团队针对与此威胁关联的设备公开已知的漏洞，开发并部署了超过100个Snort签名。 这些规则已经部署在公共Snort集中，任何人都可以使用这些规则来帮助保护他们的设备。 此外，恶意的域名/ IP已被列入黑名单。 Talos就该威胁与Linksys，Mikrotik，Netgear，TP-Link和QNAP进行了沟通。

建议用户采取以下措施：

- SOHO路由器和/或NAS设备的用户将它们恢复出厂默认设置并重新启动，以消除潜在的破坏性阶段2和阶段3的恶意软件。

- 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，与制造商合作非常重要，以确保您的设备具有最新的修补程序版本。如果不是，则应立即应用更新的修补程序。
- 互联网服务提供商积极与他们的客户合作，以确保他们的设备升级更新到最新的固件/软件版本。

由于攻击者可能采取破坏性行动，因此建议大家谨慎对待所有SOHO或NAS设备并采取这些措施，无论设备是否已知受该恶意软件影响。

结论

VPNFilter是一种广泛，强大，功能强大且危险的威胁，其高度模块化的框架允许攻击者对其进行快速改变，提供情报收集和和其他服务。

VPNFilter的破坏性能力值得关注。 攻击者利用受感染的用户设备来掩盖他们的踪迹，而不仅仅是删除恶意软件的痕迹，同时，攻击者可能随时运行“kill”命令，可能会导致成千上万的设备无法使用，导致全球数十万受害者无法访问互联网，或者在特定区域限制用户的网络使用。

虽然对物联网设备的攻击并不是什么新鲜事，但这些设备正被国家级别的团队用于进行网络破坏，这加剧了各方厂商处理此问题的紧迫性。

参考链接：

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

https://www.fortinet.com/blog/threat-research/defending-against-the-new-vpnfilter-botnet.html
(https://www.fortinet.com/blog/threat-research/defending-against-the-new-vpnfilter-botnet.html)

IOCs

如前所述，我们高度怀疑目前还没有意识到这个恶意软件还有其他IOC和版本。 下面的IOC清单包含了迄今所知道的情况。

已知的C2域和IP

与第一阶段相关

的photobucket [。] COM /用户/ nikkireed11 /库
的photobucket [。] COM /用户/ kmila302 /库
的photobucket [。] COM /用户/ lisabraun87 /库
的photobucket [。] COM /用户/ eva_green1 /库
的photobucket [。] COM /用户/ monicabelci4 /库
的photobucket [。] COM /用户/ katyperry45 /库
的photobucket [。] COM /用户/ saragray1 /库
的photobucket [。] COM /用户/ millerfred /库
的photobucket [。] COM /用户/ jeniferaniston1 /库
的photobucket [。] COM /用户/ amandaseyfried1 /库
的photobucket [。] COM /用户/ suwe8 /库
的photobucket [。] COM /用户/ bob7301 /库
toknowall [。] COM

与第二阶段相关

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 [。]洋葱/ bin32中/ update.php

已知的文件哈希

第一阶段恶意软件

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec
0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92

第二阶段恶意软件

9683b04123d7e9fe4c8c26c69b09c2233f7e1440f828837422ce330040782d17

d6097e942dd0fdc1fb28ec1814780e6ecc169ec6d24f9954e71954eedbc4c70e

4b03288e9e44d214426a02327223b5e516b1ea29ce72fa25a2fcef9aa65c4b0b

9eb6c779dbad1b717caa462d8e040852759436ed79cc2172692339bc62432387

37e29b0ea7a9b97597385a12f525e13c3a7d02ba4161a6946f2a7d978cc045b4

776cb9a7a9f5afbaffdd4dbd052c6420030b2c7c3058c1455e0a79df0e6f7a1d

8a20dc9538d639623878a3d3d18d88da8b635ea52e5e2d0c2cce4a8c5a703db1

0649fda8888d701eb2f91e6e0a05a2e2be714f564497c44a3813082ef8ff250b

第三阶段插件

f8286e29faa67ec765ae0244862f6b7914fcdde10423f96595cb84ad5cc6b344
afd281639e26a717aead65b1886f98d6d6c258736016023b4e59de30b7348719

自签名证书指纹

d113ce61ab1e4bfcb32fb3c53bd3cdeee81108d02d3886f6e2286e0b6a006747

c52b3901a26df1680acbfb9e6184b321f0b22dd6c4bb107e5e071553d375c851

f372ebe8277b78d50c5600d0e2af3fe29b1e04b5435a7149f04edd165743c16d

be4715b029cbd3f8e2f37bc525005b2cb9cad977117a26fac94339a721e3f2a5

27af4b890db1a611d0054d5d4a7d9a36c9f52dffeb67a053be9ea03a495a9302

110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8

fb47ba27dceea486aab7a0f8ec5674332ca1f6af962a1724df89d658d470348f

b25336c2dd388459dec37fa8d0467cf2ac3c81a272176128338a2c1d7c083c78

cd75d3a70e3218688bdd23a0f618add964603736f7c899265b1d8386b9902526

110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8

909cf80d3ef4c52abc95d286df8d218462739889b6be4762a1d2fac1adb2ec2b

044bfa11ea91b5559f7502c3a504b19ee3c555e95907a98508825b4aa56294e4

c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412

8f1d0cd5dd6585c3d5d478e18a85e7109c8a88489c46987621e01d21fab5095d

d5dec646c957305d91303a1d7931b30e7fb2f38d54a1102e14fd7a4b9f6e0806

c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412

已知受影响的设备

已知下列设备受此威胁的影响。 根据这项研究的规模，我们的观察很多都是遥远的，而不是在设备上，因此在很多情况下很难确定具体的版本号和模型。 应该指出的是，所有这些设备都有公开的已知漏洞。

鉴于我们对这种威胁的观察，我们高度自信地评估此列表不完整，其他设备可能受到影响。

LINKSYS DEVICES：

E1200

E2500

WRVS4400N

MIKROTIK ROUTEROS适用于云核心路由器的版本：

1016

1036

1072

NETGEAR设备：

DGN2200

R6400

R7000

R8000

WNR1000

WNR2000

威联通设备：

TS251

TS439 Pro

其他运行QTS软件的QNAP NAS设备

TP-LINK设备：

R600VPN

VPNFILTER特定的SNORT检测：

45563 45564 46782 46783

SNORT规则可防止受感染设备中的已知漏洞：

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 46311 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

声 明

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）成立于2000年4月，总部位于北京。在国内外设有30多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，为客户提供入侵检测/防护、抗拒绝服务攻击、远程安全评估以及Web安全防护等产品以及专业安全服务。

北京神州绿盟信息安全科技股份有限公司于2014年1月29日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

文章分类： 威胁通报 (http://blog.nsfocus.net/category/threatalerts/)
文章关键词： vpnfilter (http://blog.nsfocus.net/tag/vpnfilter/), 恶意软件 (http://blog.nsfocus.net/tag/%e6%81%b6%e6%84%8f%e8%bd%af%e4%bb%b6/)
转载请注明： “转自绿盟科技博客” ： 原文链接 (http://blog.nsfocus.net/vpnfilter/).
文章收录：

← 绿盟科技互联网安全威胁周报——第 201821周 (http://blog.nsfocus.net/weeklyreport-201821/)

Drupal远程代码执行漏洞威胁态势分析 → (http://blog.nsfocus.net/drupal-threat-analysis/)

发表评论

要发表评论，您必须先登录 (http://blog.nsfocus.net/wp-login.php?redirect_to=http%3A%2F%2Fblog.nsfocus.net%2Fvpnfilter%2F)。

热门文章

【预警通告】Red Hat DHCP Client Script代码执行漏洞 （CVE-2018-1111） (http://blog.nsfocus.net?p=12622)

【处置建议】Oracle WebLogic反序列化漏洞（CVE-2018-2628）安全处置建议 (http://blog.nsfocus.net?p=12076)

移动APP安全测试要点 (http://blog.nsfocus.net?p=1950)

路由器漏洞分析入门：D-Link Service.Cgi远程命令执行漏洞 (http://blog.nsfocus.net?p=12607)

【干货分享】手把手简易实现shellcode及详解 (http://blog.nsfocus.net?p=5957)

【绿盟大讲堂】CTF夺旗赛最强秘籍Part1：密码学和隐写术 (http://blog.nsfocus.net?p=9255)

【威胁通告】Spring多个漏洞 （CVE-2018-1257 ~ CVE-2018-1261） (http://blog.nsfocus.net?p=12528)

【Web安全】渗透测试介绍|附实例 (http://blog.nsfocus.net?p=12352)

最新文章

【安全报告】网络安全威胁月报——201805 (http://blog.nsfocus.net/monthly-report-201805/)

Drupal远程代码执行漏洞威胁态势分析 (http://blog.nsfocus.net/drupal-threat-analysis/)

全新恶意软件VPNFilter控制全球至少50万台网络设备 (http://blog.nsfocus.net/vpnfilter/)

绿盟科技互联网安全威胁周报——第 201821周 (http://blog.nsfocus.net/weeklyreport-201821/)

【数据安全】GDPR正式生效 企业如何建设隐私数据安全防护？ (http://blog.nsfocus.net/gdpr/)

【安全测试】性能测试进阶（Part3-并发测试的方法） (http://blog.nsfocus.net/test-3/)

【安全测试】性能测试进阶（Part2-新建测试的方法） (http://blog.nsfocus.net/test-2/)

【安全测试】性能测试进阶（Part1-基本概念） (http://blog.nsfocus.net/test-1/)

两步邮件订阅，方便获取文章

欢迎订阅！现在已有4 410个朋友订阅了。
在后续邮件的尾部，您可以退订及修改订阅内容。
选择订阅组：

- ☐ **最新文章**
- ☐ **技术分享**
- ☐ **漏洞分析**

- [ ] **运维安全**
- [ ] **Web安全**
- [ ] **安全报告**

邮件 *

马上订阅!

友情链接

绿盟科技官网 (http://www.nsfocus.com.cn)

绿盟威胁情报中心NTI (https://nti.nsfocus.com/)

绿盟科技博客原创作者群

(http://shang.qq.com/wpa/qunwpa?idkey=8e92557f79faf7236be9b5b96a263deb2e937f55514f6d2cd694c8e246d21d25)