AhnLab

安全月刊

2018.10 Vol.71

Miner 恶意代码

挖矿恶意代码的最新攻击技术

使用“Exploit kit”和“Smoke Loader”的挖矿恶意代码

勒索软件和挖掘加密货币（Cryptocurrency，虚拟货币）恶意代码是不仅对个人用户造成损害，还会对企业造成损害的常见的一种恶意软件。根据韩国互联网振兴院发布的数据，今年上半年传播的勒索软件和挖掘加密货币恶意代码的比例呈现相似水准。这两个恶意代码的目标（受害者）和传播方法以及传播数量方面都非常相似。近年来，挖掘加密货币恶意代码利用漏洞工具包（Exploit Kit）传播，此漏洞利用工具以通过恶意广告技术传播勒索软件而闻名。
在这方面，AhnLab安全应急响应中心（ASEC）在最近发布的2018年第三季度ASEC报告中详细介绍了漏洞利用工具包和挖掘加密货币恶意代码。

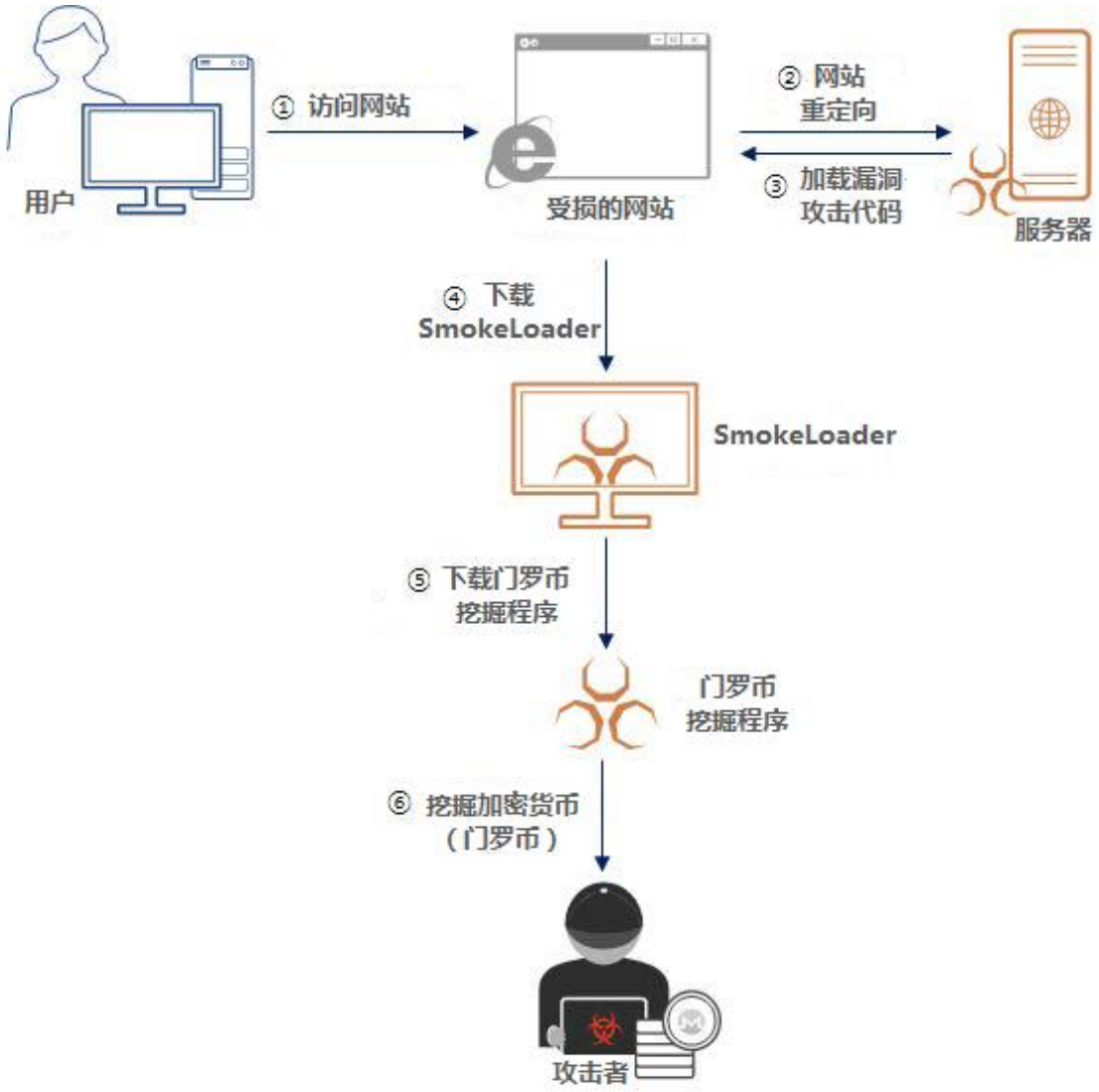
从去年年底开始，偷偷利用系统资源挖掘（Mining）加密货币的挖矿（Miner）恶意代码不断增加，并且正在使用各种攻击技术。最近利用RIG漏洞利用工具包（RIG Exploit Kit）和Smoke Loader的挖矿恶意代码已被确认。RIG漏洞利用工具包是一种攻击工具，可以利用各种漏洞传播恶意程序，曾被利用于分发Matrix、Cerber和最近的GandCrab勒索软件。Smoke Loader是一种Dropper类恶意代码，可以下载另一个恶意代码。最初，它主要用于信息泄露，但后来被用来下载挖矿恶意代码。

本文将介绍利用RIG漏洞利用工具包和Smoke Loader来挖掘典型的加密货币“门罗币（Monero）”的挖矿恶意代码的分发到shell代码运行的详细攻击过程。

用于分发挖矿恶意代码的漏洞及文件

攻击者使用RIG漏洞利用工具包来分发挖掘门罗币加密货币的挖矿恶意代码。RIG漏洞利用工具是一种利用多个漏洞的攻击工具。此次挖矿恶意代码分发利用了Internet Explorer相关漏洞CVE-2018-8174和CVE-2016-0189，以及Adobe Flash Player漏洞CVE-2018-4878。CVE-2018-8174是Windows VB脚本引擎的远程执行代码漏洞，最近经常被利用。攻击者利用这些漏洞和脚本文件、Flash文件（SWF）和可执行文件（Portable Executable，PE）感染了挖矿的恶意代码。

此挖矿恶意代码通过易受攻击的网站或在线广告网站分发，并且使用了用于勒索软件感染的恶意广告（Malvertising）技术。感染用户计算机的挖矿恶意代码继续下载并运行Smoke Loader程序，在用户计算机上安装门罗币挖矿程序，并通过此程序进行挖掘加密货币。这种挖矿恶意代码的感染及运行过程总结如【图1】所示。



【图1】挖矿恶意代码的攻击过程

RIG漏洞利用工具的漏洞攻击过程

当用户使用没有最新安全修补程序的Web浏览器访问受感染的网站或不安全的广告页面时，攻击者会尝试使用CVE-2018-8174漏洞进行攻击。使用RIG漏洞利用工具的漏洞攻击过程可分为四个步骤，如【图2】所示。

【图2】漏洞攻击的四个步骤

■ **第一步骤：重定向到特定登录页面**

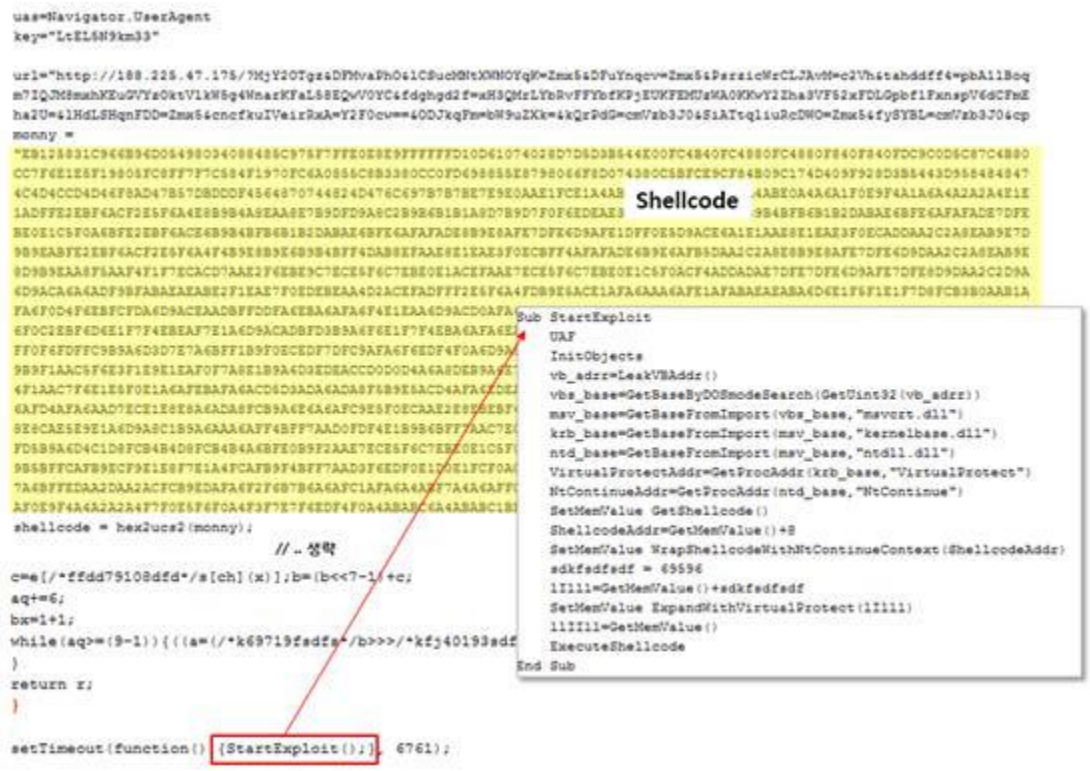
- 根据HTTP标头中包含的位置（Location）信息自动重定向（Redirection）到特定页面。

■ **第二步骤：重定向到漏洞攻击站点**

- 通过上一步中重定向站点中包含的iFrame标记（<iframe>），在用户不知情的情况下访问漏洞攻击站点。

■ **第三步骤：执行漏洞攻击命令**

在之前步骤的漏洞攻击站点中，有一些代码可以攻击CVE-2018-8174，CVE-2018-4878和CVE-2016-0189等三个漏洞，以增加攻击成功的可能性。如果用户的系统未应用与此漏洞相关的修补程序，则将利用此漏洞执行shell代码。 此时，shell代码是针对每个漏洞制作的，此shell代码会下载恶意文件后运行。



【图3】用于CVE-2018-8174漏洞攻击的shell代码

■ **第四步骤：下载漏洞攻击文件并运行**

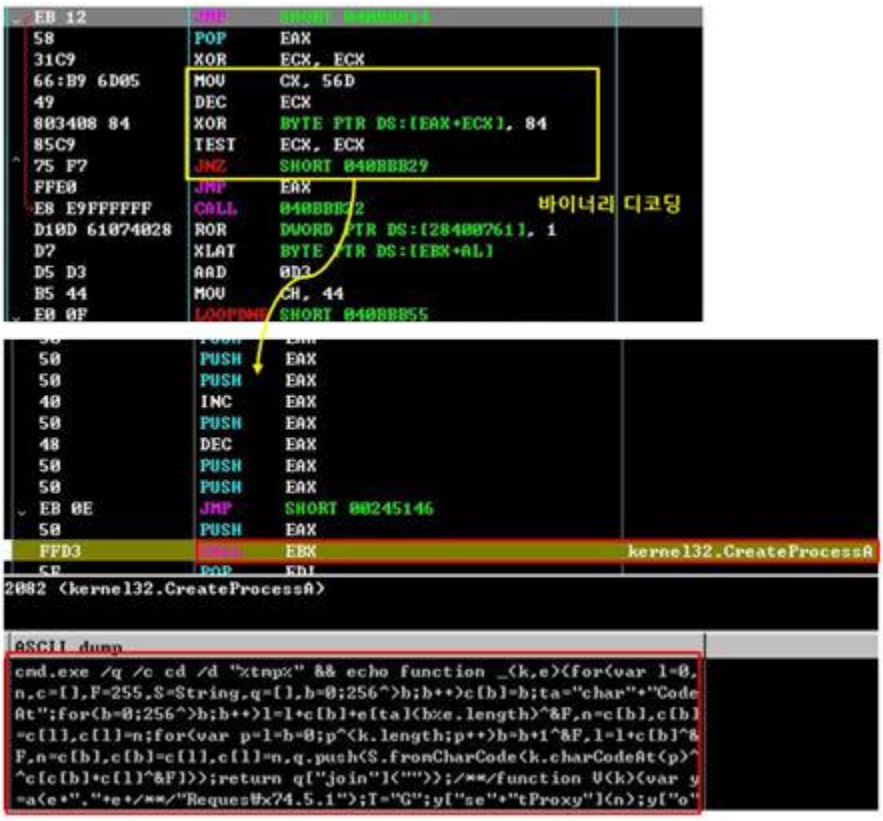
- 在这三个漏洞中，CVE-2018-4878是一个Adobe Flash Player漏洞，需要利用Flash文件。因此，在上一步中执行的shell代码从漏洞攻击站点下载并运行其他Flash文件。

下载并运行SmokeLoader

如果通过上述四个步骤成功利用此漏洞，则攻击者可以控制用户系统的Web浏览器。攻击者在用户系统的Web浏览器中执行shell代码。执行的shell代码运行包括脚本信息作为参数的CMD程序，如【图4】所示。

如果运行CMD程序 ， 要将另外执行的脚本命令存储在%TEMP%\T32.tmp文件中 ， 并使用Windows脚本程序（WScript）运行该文件。此时，脚本命令包括将SmokeLoader从Web服务器下载到用户系统并执行它的命令。

当下载到用户系统中的SmokeLoader被运行时，它会将自己注册到注册表中，以便每次启动系统时都会自动运行。SmokeLoader检查受感染系统的环境以逃避安全解决方案的检测，并定期连接到C＆C服务器以下载并运行新的恶意文件。



【图4】由shell代码运行的CMD程序

该SmokeLoader的主要特征和运行方式总结如下。

1) 检查运行环境

按如下方式检查受感染系统的环境条件，并结束自己或结束特定程序的运行。

- 检查Windows操作系统版本：如果运行的环境是在 Windows Vista或更低版本，则将结束自己。

- 检查是否是虚拟机（Virtual Machine）：检查特定路径中是否包含特定值以判断是否为虚拟机，如果是虚拟机，则结束自己。

- 检查分析程序是否运行：在进程列表和Window Class列表中检查主要分析程序是否运行，然后结束该程序。

2) 自我复制

将自己复制到路径“%APPDATA%\Microsoft\Windows\[随机路径]”，复制后文件名为“[随机文件名].exe”。

3) 注册自动运行

在autorun文件夹中创建一个链接文件（.LNK）并注册自动运行，以便复制文件可以在系统重启后自动运行。

4）检查互联网连接可用性

通过尝试连接到特定URL来检查互联网可用性。如果无法连接，以6秒的间隔重复连接。

5）下载另一个恶意程序

连接到C＆C服务器并将恶意程序（文件名为“wuauclt.exe”）下载到“%TEMP%\[随机路径]”，并运行。

使用门罗币挖矿程序（Monero Miner）挖掘虚拟货币

通过上述过程，SmokeLoader从C＆C服务器下载并运行门罗币挖矿程序。这样运行的门罗币挖矿程序将自身复制到注册表路径，以便每次重新启动系统时自动运行。为了不让用户知道感染事实，它还将其代码注入到正常的应用程序Windows Update Application Launcher（Wuapp.exe）中。此时注入的代码由UPX形式制作，其中删除PE文件的一些头信息以避免被存储器分析技术检测到。

门罗币挖矿程序在挖掘加密货币时将一个线程和服务器“sg.mimexmr.com:4444（位于新加坡）”作为挖掘池使用。此挖掘池是一个配置为使用较少的CUP/GPU资源的端口，防止用户知道加密货币挖掘程序正在运行。由ASEC证实，目前该挖矿程序的挖掘池由不正当使用而帐户已被阻止，因此无法挖掘加密货币。

对于利用各种漏洞的挖矿恶意代码和变化多端的SmokeLoader，需要提高警惕

最近，不仅是针对个人，而且针对企业系统的挖矿恶意代码的传播也正在增加。这是因为企业服务器等高配置系统对加密货币挖掘很有效。当公司的服务器或业务系统感染了挖矿恶意代码时，它导致不仅仅是系统性能下降的问题，还有可能导致业务生产力和连续性的问题。

值得注意的是，在挖矿恶意代码感染过程中出现的SmokeLoader可以下载各种文件。这一次只是下载了加密货币挖掘程序，但由于取决于攻击者的意图可以安装勒索软件或后门程序，它可以导致信息泄露或系统破坏等更大的损害。

另一方面，正如我们了解的情况，挖矿恶意代码如大多数恶意代码（包括勒索软件）也使用操作系统和软件的漏洞。最近，不仅是利用Windows操作系统漏洞，而且利用主要的开源操作系统（如Mac OS、Jenkins、Apache Struts 2和Apache Tomcat）漏洞的事例也不断增加。因此，公司和机构应努力提高员工的安全意识，并计划有效地应用和管理操作系统的最新安全补丁和公司使用的主要软件。

V3产品群检测到此次挖矿恶意代码相关的文件的诊断名如下：

<V3产品群诊断名>

Trojan/JS.Exploitloader

SWF/Cve-2018-4878.Exp.3

Trojan/Win32.HDC

Trojan/Win32.Infostealer

要想查看更多有关上述罗币挖矿恶意代码的信息，请参考2018年第三季度的ASEC报告。

▶打开2018年第三季度ASEC报告(Vol.92)

AhnLab

安全月刊

http:// cn.ahnlab.com

http://global.ahnlab.com

http://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com