Rudeminer, Blacksquid and Lucifer Walk Into A Bar

research.checkpoint.com/2020/rudeminer-blacksquid-and-lucifer-walk-into-a-bar/

September 15, 2020

September 15, 2020
Research by David Driker, Amir Landau

Background

Lucifer is a Windows crypto miner and DDOS hybrid malware. Three months ago, researchers published a report detailing its unique activities. More recently, we found evidence that the attackers behind this campaign started their operations in 2018.

What started as a miner with self-spreading capabilities that targeted the Windows system, has now evolved into a multi-platform and multi-architecture malware targeting Linux, and IoT devices as well.

Data collected from ThreatCloud shows recent hits on over 25 organizations in the US, Ireland, the Netherlands Turkey and India. Attacks have come from a variety of domains including manufacturing, legal, insurance and also the banking industry.

The current main attack vector for IoT devices is through exploitation of the vulnerability known as CVE-2018-10561, which targets unpatched Dasan GPON router devices.
The malware has several capabilities: multiple types of DDOS attacks, full command-and-control operations able to download and execute files, remote command execution, Monero mining using the Xmrig miner, and self-spreading in Windows systems through various exploitation techniques.
From the details presented in this blog, we believe this campaign continues to grow and evolve over time as it upgrades its abilities and increases its monetization strategies.

Campaign overview
Attacks originate from servers that were compromised by the attacker. Figure 1 shows the infection chain is multi-platform, and targets Windows, Linux and IoT devices. Infected Windows machines then continue to spread the malware both inside the network and to remote targets.

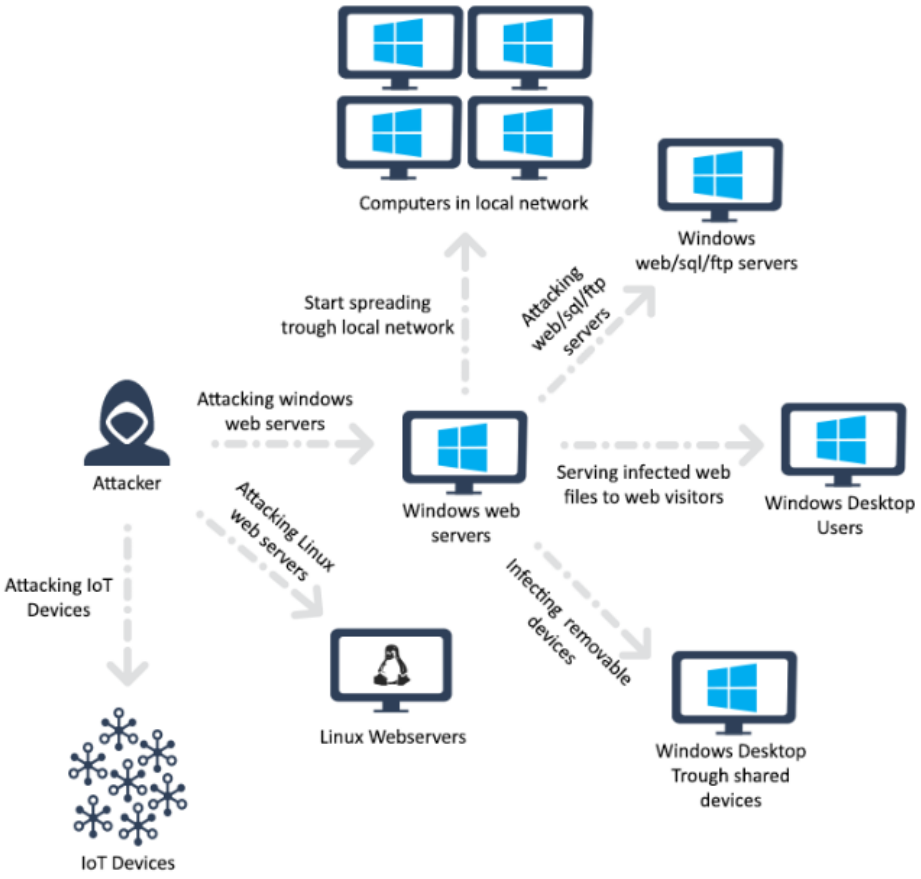

Figure 1: The updated infection chain.

There is an interesting sequence of strings presented in malware:

```
Welcome to Satan DDoS!
This version is BlackSquidMining,SpreadMiner,Complete version
This version has Wwindows,Linux86,LinuxX64,armv7,armv8,mips
Mode of infection FTP,IPC,SMB,WMI,MSSQL,EternalBlue,Eternalromance,CVE-2017-8464,thinkphp,HFS,phpstudy,Laravel,durpal,Shareddisk,sharedirectory.....
Thank you for purchasing!
```

Figure 2: Strings found in recent Windows, Linux, ARM and MIPS samples.

Further investigation of those strings leads us to two campaigns, one that was discovered by TrendMicro which they called BlackSquid, and another that was discovered by Tencent and called Rudeminer/Spreadminer.

It also possible to link those two campaigns to the Lucifer campaign by following the money trail, or in our case, the XMR wallets used.

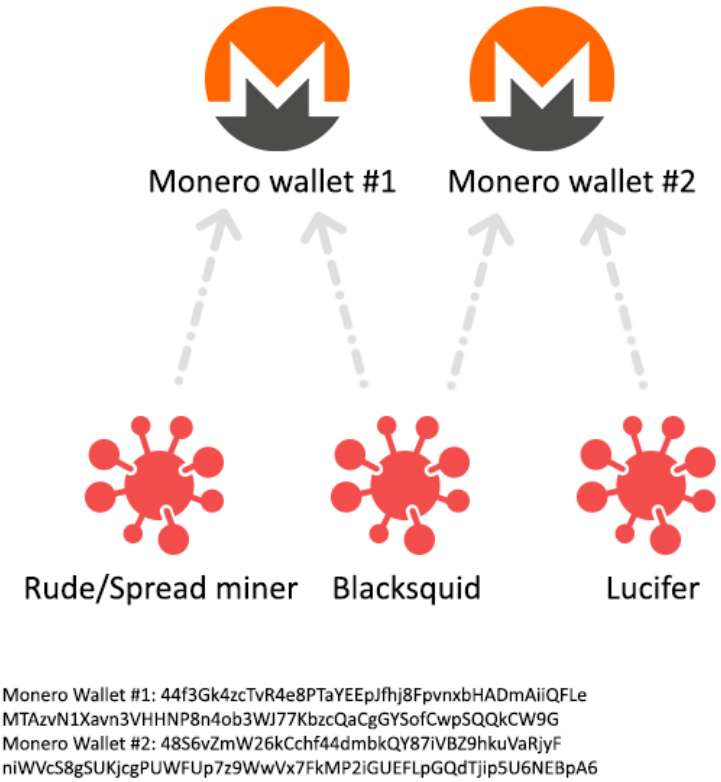

Figure 3: Linking the three campaign through the XMR wallets used.

When we explored the Blacksquid samples that use the first wallet in Figure 3, we found two almost identical samples (sample one and sample two).

The two samples share the same mutex pattern:
`BlacksquidXMRstratum+tcp://[Miner pool address]:[port]`
The first sample uses wallet number one in figure 3, and the second sample uses wallet number two.
The second wallet was also used in various other Lucifer samples (sample three), thus enabling us to link the two malware.

Linking the Blacksquid campaign to Spreadminer was trickier, as the sample provided in the Tencent article (sample one) used a custom XMR mining pool without an XMR wallet.
However, we were able to find an almost identical sample (sample two), which uses wallet number one.

The XMR wallet used in the Blacksquid campaign leads to samples from the end of 2018, indicating that the attackers began their operations even earlier.

From those findings, we created the following timeline:

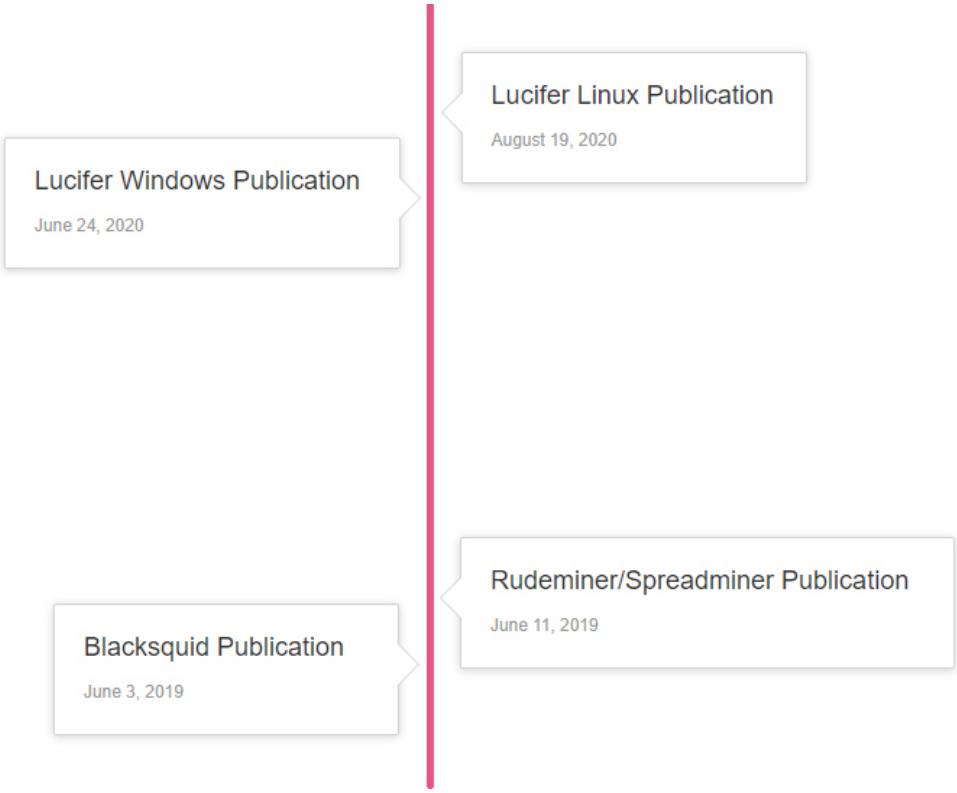

Figure 4: Timeline of the appearance of variants in this campaign.

Another interesting string can be found in the Linux variant of the malware:

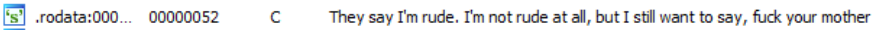

Figure 5: String used in the Linux version of the malware.

We believe this string is a response to Tencent publication which called the malware “Rude.”

These findings indicate that the attackers behind this campaign have been active for more than a year and a half, and that the malware keeps evolving and upgrading its code base.

From publicly available data, we estimate that the Lucifer campaign yielded the attacker 18.643456520496 XMR, which is approximately $1769.
As the old XMR wallet is now blocked, it’s not possible to know how much money was made in the Blacksquid and Spreadminer campaigns. The addition of the DDOS capabilities indicates that the attackers are seeking to expand the malware’s money-making methods.

The Windows self-spreading capabilities are based on outdated and publicly-available exploits, and the use of brute-force.
The Windows self-capabilities have undergone only minor changes over time, which may indicate that the attackers have been successful with those methods.
Like the old saying goes: “If it ain’t broke, don’t fix it.”

The first samples of the new campaign were uploaded to VirusTotal in February 2020, followed by later samples in the months since. New samples are still being detected.
The first and only ARM sample to date was uploaded to VirusTotal on May 10.

Figure 6: ARM sample listing in VirusTotal.

This sample was not determined to be malicious.
The ARM sample only has DDOS capabilities, and has different behavior from the Linux sample, possibly due to the restrictions caused by IoT devices.

The C2 server has a publicly accessible HFS server that allows us to witness the campaign's evolution:

Name .extension	Size	Timestamp	Hits
Lin64	1.1 MB	2020/7/28 23:21:06	85
Lin86	949.1 KB	2020/7/26 15:52:51	42
office.exe	152.0 KB	2020/7/29 15:42:12	68

Name .extension	Size	Timestamp	Hits
pornographic.exe	9.6 MB	2020/7/23 1:13:25	37

Name .extension	Size	Timestamp	Hits
Lin64	1.1 MB	2020/7/26 15:52:50	119
Lin86	949.1 KB	2020/7/26 15:52:51	31

文件名 .扩展名	大小(类型)	修改时间	点击量
Linux64	1.1 MB	2020/8/11 23:06:53	1116
Linux86	949.3 KB	2020/8/11 23:06:54	12
Win.exe	10.3 MB	2020/8/11 23:07:00	144
X64	3.1 MB	2020/8/11 23:00:46	788
X86	3.4 MB	2020/8/11 23:00:47	6

Name .extension	Size	Timestamp	Hits
Linux64	1.1 MB	2020/8/11 18:14:00	635
SB360..exe	216.1 KB	2020/7/23 18:37:21	42

Figure 7: Latest binary samples uploaded to the C2 HFS public server.

As you can see, the campaign keeps evolving and releasing new versions. The `"office.exe"`, `"sb360..exe"` executables that were uploaded are variants of the gh0st RAT, indicating that attackers want to expand the malware capabilities in infected machines.

The Linux, ARM, MIPS versions were not stripped of debugging symbols. This allowed us to link the code base of the new versions for all platforms to a Chinese DDoS program from 2009, called "Storm Attack Tool VIP 2009." It is possible to find downloadable versions of this program through various open-source Chinese websites.

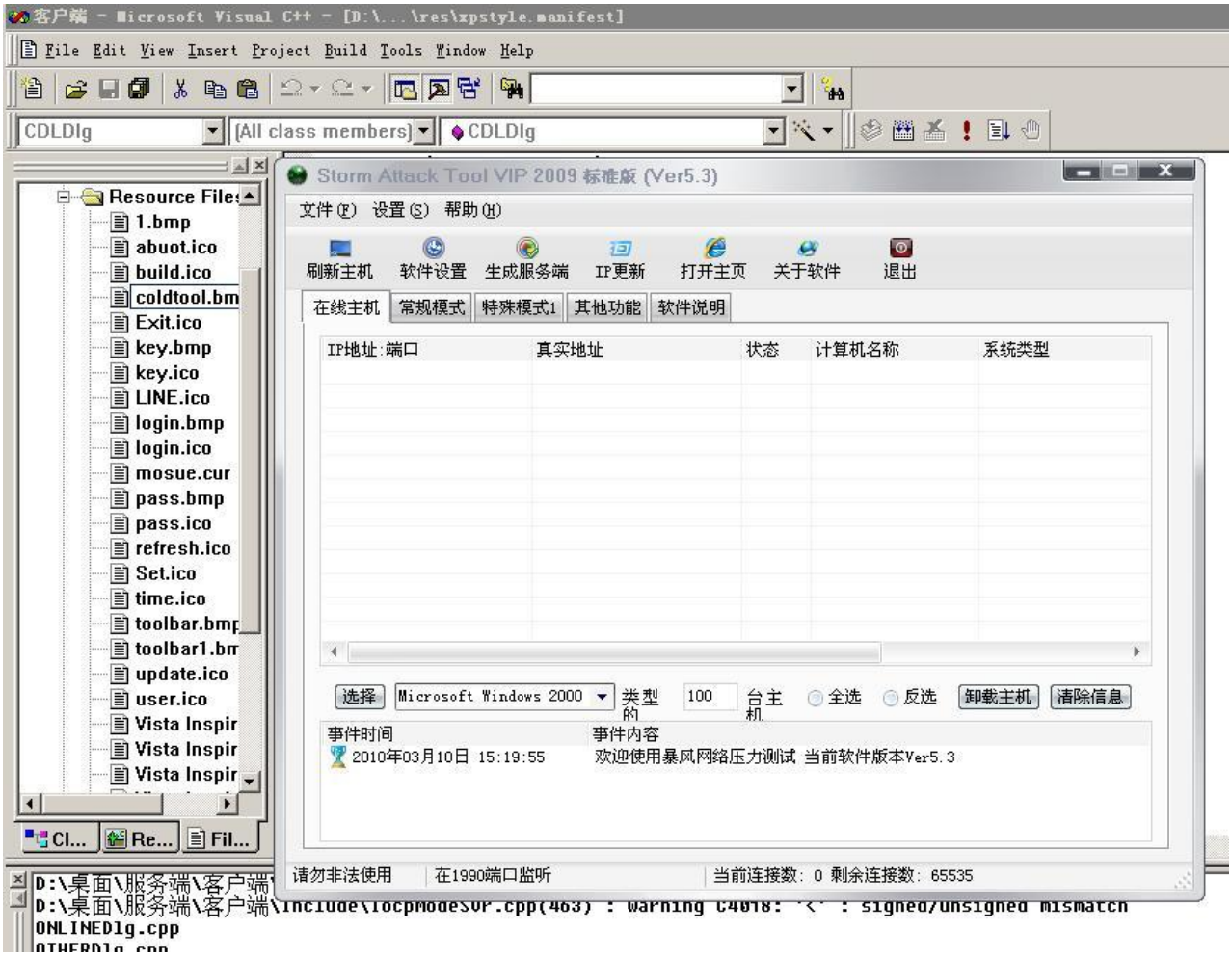

Figure 8: An image of the Storm attack tool panel.

All of the DDoS attacks in the latest version of this campaign are taken from this software. The rest of the malware is heavily modified for other functionality, such as full C&C operations, Monero mining, self-spreading in the Windows system, and the port for Linux and IoT devices.

In the rest of this article, we take an in-depth look at the Linux, ARM and MIPS samples.

Linux x86/x64

The Linux version is different from the Windows one in that it does not have self-spreading capabilities. In addition, the Linux samples were not stripped of the debugging information.

After successful exploitation, the malware uses the daemon command to detach itself from the terminal and run in the background as a daemon.
The malware checks if it is able to set up a socket which is used to
bind to a port. The port number depends on the version; the latest version uses port 20580.
If the malware is unable to set up a socket or bind to it, it exits.
After the bind, there is no call to the listen function to actually start listening on the port.
The purpose of the socket is not to communicate but to
enforce the behavior that there can only be one process of the malware running at a time, as there cannot be multiple sockets using the same port.

The malware sets up three signal handler functions for the following signals:

- **SIGPIPE** – When there is a write operation to a broken pipe. This is useful for when the socket dies.
- **SIGTERM** – Request to terminate the program.
- **SIGINT** – Request for the program to shut down gracefully.

The malware executes this command:

```
/sbin/service crond start;chkconfig –level 35 crond on;
```

The first part of the command starts the `crond` service. The second part sets the `crond` service to run at the following run levels:

- Multi-User mode, console logins only.
- Multi-User mode, with display manager as well as console logins (X11).

The `chkconfig` command fails because its missing another hyphen before `-level 35`.
These two commands only apply to CentOS/RHEL based distributions.

The next goal for the malware is to increase the file descriptor limit.
One of the defining features of UNIX is “everything is a file.” This is also true for sockets.
When the malware initiates a DDoS attack, it needs to open as many sockets as possible, to drive as much traffic as possible to the target.
This can be achieved by increasing the file descriptor limit in the OS settings.
To change the file descriptor limit, the malware first performs a check on the User ID.
When a program is running as root, its User ID is zero.
If the malware is running with the User ID zero (root), it:

- Executes the command: ulimit -HSn 65536
- Adds the line “fs.file-max to 6553560” to the file /etc/sysctl.conf
- Adds these lines to the file /etc/security/limits.conf:
- * soft noproc 65535
- * hard noproc 65535
- * soft nofile 65535
- * hard nofile 65535

If it is not running with the User ID zero, it issues two commands in the following order:

1. ulimit -HSn 4096
2. ulimit -HSn 10240

The malware runs these two commands first with a smaller limit and then a greater limit. If the increase fails, the smaller limit is the fallback option.

Persistence of the malware only happens if the User ID is zero:

1. If the file `/etc/rc.local` exists, the malware either writes or appends this line in the file:
   MALWARE_PATH start
2. The malware writes this line in the file/etc/crontab:
   */1 * * * * MALWARE_PATH

The /etc/rc.local script is executed after all normal system services have started.
The line added in the crontab causes Linux to execute the malware every minute.

After the malware configures its persistence, it decrypts these five strings:

- C&C address: qf2020[.]top
- Parameter list for the Xmr miner: -o stratum+tcp://pool.supportxmr.com:3333 -u 4AfAd5hsdMWbuNyGbFJVZjcMLeKHvrXnT155DWh8qGkYRPbVGKBT9q1Z5gcFXqmwUuh2Kh6t2sTnHXPysYrGf2m9KqBwz9e -p X
- Parameter list for the Xmr miner: -o stratum+tcp://gulf.moneroocean.stream:10001 -u 4AfAd5hsdMWbuNyGbFJVZjcMLeKHvrXnT155DWh8qGkYRPbVGKBT9q1Z5gcFXqmwUuh2Kh6t2sTnHXPysYrGf2m9KqBwz9e -p X -a cn/r
- Location for the Xmr miner: /tmp/spreadtop
- URL of the Xmr miner: 122[.]112[.]179[.]189:50208/X64

After the initialization, the malware begins the main logic by starting these five threads:

- Mining thread
  It first downloads the miner and saves it into /tmp/spread.
  This enables it to make sure the miner is running, and if needed, stop or restart the mining process.
- Process killer thread

The thread attempts to locate and kill processes whose name starts with the one of these strings:

- Linux-
- 25000
- Linux2.6
- Linux2.7
- LinuxTF
- Miner
- Get the network usage thread
- Get the CPU usage thread

- Send mining, CPU usage and network usage reports to the C&C server

```
43 50 55 28 53 74 6f 70  29 7c 30 2e 30 30 7c 31   CPU(Stop )|0.00|1
25 7c 30 2e 30 30 7c 67  75 6c 66 2e 6d 6f 6e 65   %|0.00|g ulf.mone
72 6f 6f 63 65 61 6e 2e  73 74 72 65 61 6d 3a 31   roocean. stream:1
30 30 30 31 00                                     0001.
```

Figure 9: Example of a report message

After the threads are set up, the malware starts an infinite loop and maintains a constant connection to the C&C.
The C&C command modes:

Mode 4	Start a DDOS attack on the target.
Mode 5	Stop the current DDOS attack or re-enable a future attack.
Mode 6	Download and execute a file.
Mode 7	Execute a command.
Mode 8	Disable usage reports.
Mode 9	Enable usage reports.
Mode 10	Switch to a different mining pool and kill the current mining process.
Mode 11	Disable mining.
Mode 12	Enable mining.

Linux ARM/MIPS

The ARM/MIPS versions are simpler versions of the Linux one – they only contain DDoS capabilities.
Initialization is almost the same as in the Linux version.
They use the daemon to detach and the socket bind method to ensure there is only one running process.
The malware only sets up a signal handler for the SIGPIPE.
If it is running as root, it increases the file descriptor limit to 20480 and writes its path to the /etc/rc.local file for persistence.
If it is not running as root, it increases the file descriptor limit to 4096.
Then the malware decrypts the C&C address: tyz2020[.]top

After the initialization, the malware starts the main logic by starting this one thread: Watchdog communication thread
First it checks if any of these devices exist: /dev/watchdog or /dev/misc/watchdog.
If one of them exists, the Watchdog timeout is increased to 15 seconds using the ioctl WDIOC_SETTIMEOUT.
Then the thread starts an infinite loop to send the ioctl WDIOC_KEEPALIVE to Watchdog every 10 seconds.

The Watchdog role is to ensure the system is stable.
In the case of a system issue, the user space Watchdog stops writing to the Watchdog device, and the kernel Watchdog restarts the device.

By using this thread, the malware ensures the watch device always has data written into the Watchdog device. This prevents the reboot of the device.

As seen previously, after the thread is set up, the malware starts an infinite loop and maintains a constant connection to the C&C. The C&C command modes:

Mode 4	Start a DDOS attack on the target.
Mode 5	Stop the current DDOS attack or re-enable a future attack.

Conclusion

As we show in this article, this campaign is continually evolving to cross between platforms and adding new ways to gain profit and spread itself. Even though the attacker uses known attacks for infecting machines and self-spreading, not all the systems are always updated. Brute forcing can be effective when the organization has a weak password policy.

As of this writing, these are the capacities used by the attacker on all architectures and platforms:

Operating System	DDoS capabilities	C&C communication	Self-spreading
Windows	Yes	Full C&C communication	Yes
Linux	Yes	Full C&C communication	No
ARM	Yes	DDoS commands only	No
MIPS	Yes	DDoS commands only	No

We believe that this campaign will continue to evolve, including modifying the current self-spreading methods and capabilities in Windows and adding them to the Linux, ARM and MIPS versions.

Check Point protections

Check Point's IoT Protect protects every IoT device across the entire network and protects the network from any IoT related attack.

It is based on two security functions:

1. Prevent unauthorized access and malicious intent from reaching the IoT devices.
2. Identify infected devices and prevent them from compromising other network elements.

Check Point offers security solutions for both IoT networks and IoT and OT devices. These solutions are tailored for different environments including Enterprise Smart Office, Smart Building, Industrial, and Healthcare.

Anti-Bot Protections

The Anti-Bot blade includes network signatures for the behavior command-and-control operation, as well as C&C domains.

IPS Protections

- Rejetto HTTP File Server Remote Code Execution (CVE-2014-6287)
- Jenkins Stapler Web Framework Remote Code Execution (CVE-2018-1000861)
- Oracle WebLogic WLS Security Component Remote Code Execution (CVE-2017-10271)
- NoneCMS ThinkPHP Remote Code Execution (CVE-2018-20062)
- Drupal Core Remote Code Execution (CVE-2018-7600)
- Apache Struts2 Struts1_Plugin Remote Code Execution
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0144)
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0145)
- Microsoft LNK Remote Code Execution (CVE-2017-8464; CVE-2018-0978)
- Dasan GPON Router Authentication Bypass (CVE-2018-10561)

Anti-Virus Protections

The Anti-Virus blade includes hashes signatures for all variants.

IOCs

C2
122[.]112[.]179[.]189
guyeyuyu[.]com

qianduoduo[.]pw
qf2020[.]top
tyz2020[.]top

Linux samples:

53c2a0f3c3775111cbf8c09cd685e44a434bdd2d4dc0b9af18266083fb4b41e8
82934ed1f42986bdad8e78049e27fcb0b8e43a5b0b9332aa913b901c7344cbc6
ebcaed78aab7b691735bb33d5c33dd6dd447a0a538ff84d0d115c2b35831d43d
d9f1878b029202195e0aeefb8406ea13d1ed57f8042636858dfd71f204ca0b05
7caf6f673d224effa207c3b3f9a0ce65eabe60230fbc70e52091f0e2f3c1f09c
bcdadf4930abab3773df1c184fd2b6fa34b5cb8543177d76daf2b9f7c1f36c4f
ECA3E0DE0A9FA7CAC75617C57839E7D62C53E4690483C08A849E624A2C79D8D9
49A8F1F9A771283771E5733EF05C3D525806318EEC7C82A049EE2B05B4259204

ARM sample:
3ea56bcf897cb8909869e1bfc35f47e1c8a454dd891c5396942c1255aa09b0ce

Monero wallets:

44rygo7VfwEYdEbe1ruyZNLfrV19snk3REQpfb5LU9Yxf98z7Ws9EZPPbUgvozZyfYXCb3vsRJRT8wTGe3FipsLb93NaDULN
45sep79Asuwcjz8dLTu7XtJBTX7yYf7uo6qT9ymFBQXv8gjZsDPyd46Hoh6DM8pAXkLnsw9U7veZWU1DqMjKRoryAn3zEq1
43VqbHtuooiNC8rMEeoiB6LzUTyBfPaup3DxAUxRxmqo2fGRDGkyzx68ehdh43Zbn5LHwdFAcztskQW2bAoxMtm9NwJDi7R
4AfAd5hsdMWbuNyGbFJVZjcMLeKHvrXnT155DWh8qGkYRPbVGKBT9q1Z5gcFXqmwUuh2Kh6t2sTnHXPysYrGf2m9KqBwz9e
48S6vZmW26kCchf44dmbkQY87iVBZ9hkuVaRjyFniWVcS8gSUKjcgPUWFUp7z9WwVx7FkMP2iGUEFLpGQdTjip5U6NEBpA6