DSCI
THREAT INTELLIGENCE
AND RESEARCH INITIATIVE

THREAT ADVISORY

JUNE 2020
New Linux Malware & Variants continue to hit businesses: **Kaiji Malware**

**Threat Identification – DTINR6001**

**Synopsis**

Kaiji Malware is currently under development phase, targeting IoT devices via SSH brute-force attacks. The malware is designed to infect Linux-based servers and smart IoT devices and use the infected devices to launch DDoS attacks.

**Infection and Propagation Vector**

The malware is written in the Go programming language. Attackers use botnets to initiate the Brute-force attack to get the root access of the IoT devices and Linux servers after scanning for open Secure Shell (SSH) ports. Without gaining the root access, attacker can’t manipulate network packet for DDoS attacks or for any other operations.

As Kaiji malware spreads via SSH, brute-force attacks targeting only the root users.

Once SSH connection is made, a bash script is executed which makes an environment for the malware:

1. A `/usr/bin/lib` directory is created where Kaiji is installed under the system tool name like `netstat`, `ps`, etc.
2. The SSH brute-force module continues to spread and another SSH relies on hijacking local SSH keys to infect the previous host connected to the server in the past.

Although the malware files are stripped but can be retrieved using `IDAGolangHelper`. As the function definitions embedded within the Golang binary, it can’t be altered using `strip` command. Now once, the malware is executed it copies itself to `/tmp/seeintlog` and launches the instances for further operations. There are 13 instances which are named in English representation of Chinese words. (Fig.1)
This malware is under development phase. The source code of the malware includes “demo” strings and the rootkit module would often call itself too many times. This results in the exhaustion of the device’s memory, leading to a crash. The C&C servers of Kaiji often went offline, leaving infected devices without any master server, and exposed to being hijacked by other botnets.

**Characteristics and Symptoms:**

Fetches commands from the C2. These include:

- DDoS instructions
- SSH brute-force instructions, including host range and a password to attempt login
- Run shell command
- Replace C2 servers
- Delete itself and remove all persistence

For DDoS operations, a target and an attack technique are retrieved. Attacks include:

- Two TCPFlood implementations (one with raw sockets)
- Two UDPFlood implementations (one with raw sockets)
- IPSpoof attack
- SYNACK attack
- SYN attack
- ACK attack
Signature/ IoCs

4e8d4338cd3b20cb027a8daf108c654c10843e549c3f3da6646ac2bb8ffbe24d  
9198853b8713560503a4b76d9b854722183a94f6e9b2a46c06cd2865ced329f7  
98aae62701d3a8a7a19028437bc2d1156eb9bfc08661c25db5c2e26e364dca  
0ed0a9b9ce741934f8c7368cdf3499b2b60d866f7cc7669f65d0783f3d7e98f7  
f4a64ab3ff0b4a94fd07a55565f24915b7a1aaec58454df5e47d8f8a2ee22a  
9f090a241eece74a69e06a5ffed876c7a37a2ff31e171924673b6bb5f1552814c  
370efd28a8c7ca50275957b47774d753aab6d7c504f0b81a90c7f96c591ae97  
357acbadb9069b8484f4fdead1aa946e2eb4a505583058f91f40903569fe3f3  
cu.versiondat.xyz  
1.versionday.xyz  
www.aresboot.xyz  
www.6x6.com  
www.2s11.com

Mitigation

- Create a strong and unique SSH login password
- Require better SSH key-based authentication
- Set their system not to receive SSH connection requests on a standard network port
- Disable SSH logins for the root account
- Regularly update the firmware on your routers and IoT things

Threat Identification – DTINR6002

PyXie RAT: PyXie RAT is a Python-based Trojan malware which gives attackers almost full control of Windows systems

Synopsis

PyXie RAT is delivered by side-loading technique that leverages legitimate applications to exploit the victim, further installing the malicious payload using PowerShell to escalate privileges and obtain persistence on the machine. Then finally connection is established with command and control server along with downloading the final payload.
**Infection and Propagation**

The creators of the PyXie RAT have used code from a couple of infamous hacking tools and made sure that their creation is difficult to study and analyse.

The malware is executed in the following steps:

1. **Loader**
2. **Installation and persistence**
3. **Cobalt-Mode Downloader**

The loader was found in an open-source Tetris game, modified to load encrypted shellcode payload named “setting.dat”.

Firstly, the campaign uses a side loading technique to load components of malware. In this, two variants are present which are found in most computers:

- **LMIGuardianDll.dll**, side-loaded by a signed binary (LmiGuardianSvc.exe) from LogMeIn.
- **Goopdate.dll**, side-loaded by a signed binary (GoogleUpdate.exe) from Google.

Once loaded, the malicious DLL will then locate encrypted payload and appending a .dat extension to it.

The malware gets installed automatically in the second phase, setting up persistence, and spawning a new process to inject the third stage payload. In this phase, malware fingerprints victim machine with a Hardware ID hash which is used in various functions and in the encryption process. The Hardware ID is calculated using MD5 hash, which is information collected from the system.

Moreover, if the payload is running with administrator privileges, then malware will automatically escalate its own privileges. This includes the following steps:

1. Creating and starting a temporary service.
2. Respawning and running as a local system process.
3. To gain persistence, malware deletes the temporary service from the service control manager.

In the third phase, a downloader named COBALT MODE is initiated to debug information left in previously analysed samples.

The primary functions of cobalt mode include:

1. Connecting to C2 server
2. Downloading an encrypted payload
3. Decrypting of the payload
4. Mapping and execution of the payload in the address space
5. Spawning of a new process for code injection
After all the above process, Python RAT is compiled into an executable format and loads an archive containing the PyXie RAT bytecode from memory.

**Characteristics and Symptoms**

As PyXie RAT is executed, it can be very impactful and have the following abilities to perform:

1. It starts the keylogger which collects keystrokes that are then transferred to C&C server
2. Record video via the webcam
3. Initiate a remote desktop connection
4. Collect files from any removable storage devices that may be plugged in
5. Collect login credentials from FTP clients as well as Web browsers
6. Injection of custom websites that may be utilized later for phishing operations

Fig. 2. [https://threatvector.cylance.com/en_us/home/meet-pxie-a-nefarious-new-python-rat.html](https://threatvector.cylance.com/en_us/home/meet-pxie-a-nefarious-new-python-rat.html)
Signature/ IoCs

1d970f2e7af9f62ae6786c35fcd6bc48bb860e2c8ca74d3b818990cd3a978b2b
3a47e59c37de42304b345a16ba6a3d78fc44b21c4d0e3a0332ee21f1d13845
3a7a46bb94acee94c86a34cb0b355317de8404c91de3f00b40e8257b80c64741
56e96ce15ebd90c197a1638a91e8634d6c5b0b4d8ef28891dfc470a28d08078
5937746fc1a5119d9a8040249b0ca2aededf2f86b55be8159385b6ca7a4d6f40
7303fa1ca4e0f4c0edf994134636ef06cd999efb71f5f1007d185840ac16675d
78471db16d7bd484932c8eb72f7001db510f4643b3449d71d63767911ca363b
814357417a9a57e43d50cb3347c9d287b99955mb08ae4e53e12b463f7441a0
92a8b74cafa5eda3851cc49f4f26db70e5ef0259bc7926139302013e5d73fd285
a765df03ffa343a7a420a0a57dbb5643663692ab6162c3561f9f7b0ad5623
c3b3f46a25c850971e1262d09870db755391dce575dc7976f90c1b3f81215de
ca9400b2fff71c401fe752aba967fa8e7009b64114c9c431e9e1a9c3e8f79497
d271569d5557087aeecc340bfb70179b73265b29bed2e774d9a2403546c7dd5ff
de44656b4a3d86e0a0d6686f2340bbec0dcd45da8676d78b0042e0f022863c84e6634b2650b322e6edf6e5b2b476689052f72556715272cc18fe8ea27862bd01e8c888217067f19fd161eda737646c6494a4d90e1a1cae14f7cc
edd1480fe3d83dc4dc5992cf8436bc1f33bc065504ccf4b14670e9e2c57a89
f9290c938d134a480b41d99ac2c5513a964de001602ed34c3638d5eb577bf8f
6634d76255e921686360e00024dfb0f16b6420986f0e5a5b3e805ce7959d9cf9
do31081b8c211994b5406b7f2544c0d6ebcbb8384f23e393f804b49563ed112
f4666cb20544bf203155142cf1445e65b0e7566a93ecfb5edc74ab7ed60f9573
ca68f02bd01650383af68f0c129482f2af38329dd1e6a18822ad6fc2c3d00b2
d767235e628422ada7f1e976a3cf771049286edf22195930282ffbd6229afa7b29
50a44b19b38caee4aa0e20470204145fa1ac1f2162c735f192cb2896cda1a4b86a
610c3536ceaf0e4ad0d60c683052ee7272e29049ceac909b1de55ac1206f49
7ee6253f06e563a81815a125367f6dad5f3f3bf41e1a1c63f6761b3a3ebeb90
265e5e1389b3145f2b2ca1a01767a5484bc361dc3795120656dcabc121234a
8d2b3b0cb0b32618b86ec362ac142177f5890917e384c85bbd464f1255e9c7f
d1429f54baaad423a8596140af3f07df9f762373ad625bda730051929463847
ade8f07bf7918343bf307ec35837327e7a850edac5ab5b2cd037134af8d57
fd93858f4e7356bebe30d0d0fe07376e3d6f164bb78725e1543b093558c6f6
a50b5e824e261157c4f850d2412d8091ae850b1011493c7b393c1905fc234
0d14a1b5574dc12f6286d37d0a624232fb63079416b98c2e1cb5c61f8c266ff
625c22b21277cb8a7e1b7019a1c21b64bf0a2baef57a530a386fd70a71a6d0
b7da341a28a19618b53e649a27740dfeca3144ce0e0d505704b56335cc55bd
d612144c1f64a063530aba5bfae7f4e4ae134bc55dfc067439471934b841b00
ce093636697f07ea4e86733888e97e421393929ecdf0d66ed9b4d992ab
3259dd0efed1d28a149d4e8c4f980a19199d9bead951ee12313ea26521185f2e
5fede5eb43732c7f098ac7b68b1350c6524962215b476de571819b6e5a71fc
f6ff873e1bd3d06b6182792ae8bd781f4f60be39d49085ba3d64658456260402
608f34a79e5656593b284ef0d24f8ea89bc007e5654ae0969e6d9f92ec87d32
b1f54b88c97b6808779f166be6de6aa9effbc38a0a8b27a565fb35531094680
d50f28cf50121f1fde1cd28655e07519dadcf94218b15c701c526ab0f6acb915
56934547dfc0d7cf6e1686ae2f62060e94c094dd5c3b5aaf3d3a904d20a693
73609f8ebdd14c69709d9162ec8d7786f5264e910573df73881f85b03163bd40e
2cbe5de547ad250140c7eb3cd73e4331c49cf5a472e2806f93bf0d9df09886
840985b782648d57de302936257ba3d537d21616cb81f9dce000eaf176a56c8
e48e88542ec4cd6f1aa794abc846f336822b1104557c0dfe67c6f6e3e5231367
cb2619b7ab52d612012386d88a0d983c270d9346169b752d5a5010564efc55c
88565b4c707230ea34d4528205056264cd70d797b64eb7d89181b00187a69
91c62841844bde653e0357193a881a42c0bc9ffcc75e67a69c4f511c66e4c46fd18
ddf83c02effea8ae9ec2833bf40187bed23ec33c6b82af94632f98004ea82
edcfdd2a26b4579ecacf453b9d0f073233fb66d53c4986324646abc8b3084dc5

Filename
core/__init__.pyx /core/active_host.pyx /core/backdoor.pyx /core/beacon.pyx
/core/commands.pyx /core/conf/__init__.pyx /core/conf/config.pyx /core/debug.pyx
/core/destruct.pyx /core/entry_point.pyx /core/initialize.pyx /core/install.pyx
/core/ipc/__init__.pyx /core/ipc/exclude.pyx /core/ipc/ipc.pyx
/core/ipc/mimikatz.pyx /core/keylog.pyx /core/mitm/__init__.pyx
/core/mitm/cert_gen.pyx /core/mitm/proxy.pyx /core/mitm/web_dump.py
/core/mitm/web_fakes.pyx /core/mitm/web_injects.pyx
/core/mitm/web_screens.pyx /core/modules/__init__.pyx
/core/modules/aes_cfc.pyx /core/modules/bot_lib.pyx /core/modules/cookies.pyx
/core/modules/crc64.pyx /core/modules/decorators.pyx
/core/modules/description.pyx /core/modules/ffmpeg_instructions.py
/core/modules/ffmpeg_rec.pyx /core/modules/find_files.pyx
/core/modules/keepass.pyx /core/modules/link_file.pyx /core/modules/logmein.py
/core/modules/multipart.pyx /core/modules/os_ver.pyx /core/modules/rdp.pyx
/core/modules/rdp_creds.pyx /core/modules/recent_files.pyx
/core/modules/research_domain.pyx /core/modules/sharphound.pyx
/core/modules/smb_scan.pyx /core/modules/socks5.pyx /core/modules/sysinfo.py
/core/modules/tools.pyx /core/modules/webdav.py
/core/modules/winapi_stubs.pyx /core/modules/windnsquery.pyx
/core/modules/winfiletime.pyx /core/nmc.pyx /core/obfuscate/__init__.pyx
/core/obfuscate/boolean_obfuscator.pyx /core/obfuscate/number_obfuscator.pyx
/core/obfuscate/obfuscate.pyx /core/obfuscate/string_obfuscator.pyx
/core/passwords.pyx /core/protect.pyx /core/pwnage.py /core/software.pyx
/core/systems.pyx /core/transport/__init__.pyx /core/transport/dns.pyx
/core/transport/github.pyx /core/transport/google.pyx /core/transport/12p.pyx
/core/transport/slack.pyx /core/transport/tcp.pyx /core/transport/tor.pyx
/core/transport/twitter.pyx /core/transport/udp.pyx /core/transport/xmpp.pyx
Domain

arymar.com
benreat.com
planlamaisemon.com
teamchuan.com
tedxns.com
athery.bit
babloom.bit
floppys.bit
104.200.67.173
hwartless.bit
cloudflare.com
foods-pro.com
dopearos.com
fearlesslyhuman.org
185.82.202.109
192.52.167.241
ololo.space

Recommendations

- Do not open suspicious and irrelevant emails, especially those received from unknown/suspect senders
- Block the installation of programs from unknown sources
- Download from relevant and trusted sources
- Do a regular backup of the data
- Use trusted scanner to detect the malware

Threat Identification – DTINR6003

Aria-body RAT: Aria-body is a malicious piece of a program, also known as Aria-body RAT (Remote Access Trojan). This malware was first discovered in May 2020.
**Synopsis**
This malware remains silent and keeps an eye on the backend processes, software used, etc. The malware spread mainly through infected email attachments, malicious online advertisements, social engineering and software cracks. It allows remote access and control over an infected machine. It has been observed that Aria-body malware is employed primarily for stealing information that can locate and exfiltrate specific data targeting the government organizations around the world.

**Infection and Propagation**
After infiltration and establishing contact with the cybercriminals C&C server, it starts investigating the infected device. It gathers data concerning the infected computer like Operating System, its architecture and version, public IP addresses, network details, etc. This RAT can collect information about the software installed on the system, as well as any running processes.

Meanwhile, it typically follows three infection methods (Fig.3):

1. Using RTF file
2. With the help of malicious DLL, DLL hijacking technique to load a malicious DLL through Outlook and Avast proxy
3. Directly via an executable file, which acts as a loader

This is how the injection of the Trojan/executable loader helps to create Aria-body backdoor:

---

*Fig.3. https://research.checkpoint.com/2020/naikon-apt-cyber-espionage-reloaded/*
1. Persistence via the Start-up folder
2. Inject itself to another process such as rundll32.exe and dllhost.exe
3. Decrypt two blobs: Import Table and the loader configuration
4. Utilize a DGA (Domain generation algorithm), if required
5. Initiates the request to C&C address in order to retrieve the next stage payload
6. Decrypt the received payload DLL *(Aria-body backdoor)*
7. Load and execute an exported function of the DLL – calculated using djb2 hashing algorithm.

**Characteristics and Symptoms**

Once the backdoor is created, it comes with the following capabilities:

1. Directories can be created and deleted
2. Screen capture
3. Search file
4. Launch files using ShellExecute
5. Enumerate process loaded modules
6. Gather TCP and UDP table status listing
7. Close a TCP session
8. Collect OS information
9. Verify location using *(checkip.amazonaws.com)*
10. Key-logger
11. Stealing from USB drives
12. Reverse socks proxy module
13. Loading extensions module

Aria-body has both a 32-bit and a 64-bit variant, with similar functionality.

**Signature/ IOCs**

```
2ce4d68a120d76e703298f27073e1682a84bde7bd586166e6f20ba106ca6ef138e8cb69
04 4cab6bf0b63cea04c4a44af1cf25e214771c4220ed48fff5ca834efa117e5db
```
```
a8ee5b59d255a13172ec4704915a048b48d4fe2ca8e4d71ea8ead6bae629de47ef7
7a7 04416f97890a7bbee354e1382b40823dfd74a69a235373be55ebd28ec8035326
```
```
e4f097ff8ce8877a6527170af9555f9e476ad95cbfeaa448cb177c2de9c272141c11b8f4
2b67693cd1ba0b8b502d02e63550aad438b12b93b355d16eaca3a9a056cc4b0cbd
```
```
537b21c71eb8381ed7d150576e3e8a48be04013156a96ff50646c5de1b9a1d7de99f
0d1 9728197c938bad0bd638279f4bd5168c8ace09c5e3441010a88964f6730e7c6
```
```
43798a772bc4c841fc3f0b0a157c1df3223e64a1bfb25bc5ea95890ca438232adcc7c3
5 6e1591f794fe36f5aca5999f367525f58008c27220deed69d288a2888915c
```
C&C
realteksgjdredj.com
spool.jtjewifyn.com
blog.toptogear.com
mon-eneews.com
wdrfjkg129.com
n91t78dxt3.com
kyawtun119.com
www.ajtkgygth.com
news.nyhedmgtxck.com
dathktdga.com
www.rrgwmwmwgk.com
dns.jmrmmftym.com
www.kyemtyjah.com
rad.geewkmy.com
cpc.mashresearchb.com
www.qisxnikm.com
dns.seekvibega.com
sugano.trictaltmk.com
bbs.forcejoyt.com

Recommendations
● Use authentic source to download an application
● Use proper antivirus so that the unwanted execution doesn’t take place
● Do not click on suspicious links
● Organizations and individual users to be aware of these threats
Threat Identification – DTINR6004

Eking Ransomware: Eking is part of a ransomware family called Phobos. It encrypts victim’s files, modifies them, and drops a couple of ransom notes. It was spotted in May 2020.

Synopsis

The motive of the ransomware is to encrypt the user data and ask for ransom to retrieve their data. This is widely spread via malicious attachments, emails, unauthorized download, cracked software, etc. Unlike another ransomware, it’s not easy to bypass the key as the encryption used is much more complicated. So, we either have some good practices in place to mitigate this kind of an attack or we can become a victim of it.

Infection and Propagation

Eking ransomware modify files by adding victim’s ID, decphob@tuta.io email address and adding the ".eking" extension to their filenames. For example, it can modify "one.jpg" to "one.jpg.id[1E857D00-2275].[decphob@tuta.io].eking". It shows a ransom note in a pop-up window ("info.hta") and creates another one in a text file ("info.txt") (Fig.4)

Victims must contact Eking ransomware developers by writing them an email to decphob@tuta.io or decphob@protonmail.com address and wait for further directions. If victims are not answered in 24 hours, then they should try to contact cybercriminals via the provided Tor website link.
Characteristics and Symptoms
The type of cryptography mechanism applied by Eking has still not been correctly examined. However, it is certain that each victim may be given a specific decryption key which is unique. It is impossible to restore the files without the key available (Fig.5).

Signature/ IOCs
- MD5
  1c2a87f4cf2a34ea24b73221cc64802e
- SHA1
  4b9851ec58d83528a5542672331f5c7255566ec7c
- SHA256
  4f2a4b35cda0c85b4a0ead82e8af588d7812d79206a104ff638619aa869aade4
- SSDEEP
  6144:/uG8eelhCqmhCuG2YS6FNBet6LESwn+60Whfh7Ole1tFWP8IEtiaDCiuoSFT:V8e0hCqyCQYPbBe8fwUWhfh7Ole1t0Ph

Recommendations
- Do not open suspicious emails
- Use spam filters and an antivirus program to detect and filter malicious emails

Fig.5. https://adware.guru/remove-eking-virus/
Enable an endpoint security product or endpoint protection suite
Keep your software up-to-date
Back up data on a regular basis and keep archived copies offsite

**Threat Identification – DTINR6005**

**Optimal Promo:** Optimal Promo is a potentially unwanted application (PUA), a web browser hijacker and targets Mac based systems.

**Synopsis**
This is an adware-type application. Users download and install browser hijackers unintentionally or unknowingly helping an attacker to intercept the information, keeping a track of their search along with other useful information.

**Infection and Propagation**
The potentially unwanted applications are distributed via method “bundling”. PAUs are included in setups as additional offers and information that can be found in their settings like Custom, Advanced and Manual. Generally, users don’t check and change those settings when they download and install programs. Thus, PUAs are downloaded or installed alongside with wanted software and can also be downloaded unknowingly when we click on the deceptive ads.

**Characteristics and Symptoms**
Optimal Promo operates by delivering intrusive ad campaigns, alerting browsing settings and promoting a fake search engine - Safe Finder. Third-party graphical content is enabled, typically on any visited website. After the installation of PUA, it delivers pop-ups, banners, surveys, coupons and other intrusive advertisements. It also slows the browsing speed, limits webpage visibility, redirect to dubious websites with any deceptive click over the ads and can even execute scripts to install software. Browser hijackers modify browser options. After this, it promotes the Safe finder to search that query whenever any search is initiated (Fig.6).
Therefore, if any browser hijacker gets installed on a browser or on an operating system, uninstall it immediately.

**Signature/Reference Hashes**

- **Promoted-URL**
  - akamaihd[.]net

**Recommendations**

- To avoid the risks of bundling, download software only from the most reliable and credible source
- Block malicious attachments to reduce the attack surface
- Do not follow links and look out for messages that look different and suspicious
- Keep your software up to date
- Uninstall any unwanted application or extension
- Use of antivirus will help in filtering malicious content