



When a botnet cries: detecting botnets infection chains

Speakers



Erwan Chevalier & Guillaume Couchard

@r1chev & @Wellan129

Threat & Detection Research team at Sekoia.io

Detection tech leads



Agenda

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



Botnets infection chains



PRESS RELEASE

Qakbot Malware Disrupted in International Cyber Takedown



Tuesday, August 29, 2023



For Immediate Release

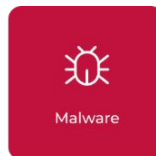
Office of Public Affairs

Qakbot Malware Infected More Than **700,000** Victim Computers, Facilitated Ransomware Deployments, and Caused Hundreds of Millions of Dollars in Damage Worldwide



Intrusion Set

Attackers using IcedID



Malware

Can be dropped by



Malware

Downloads

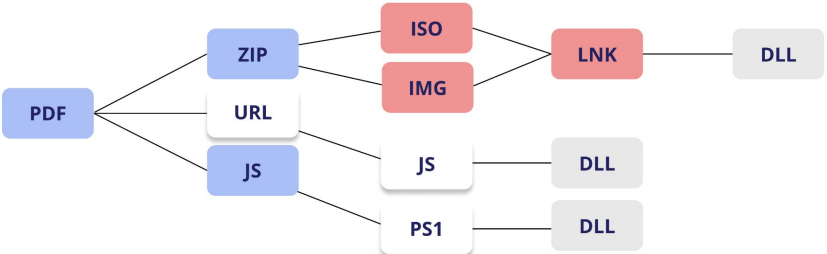
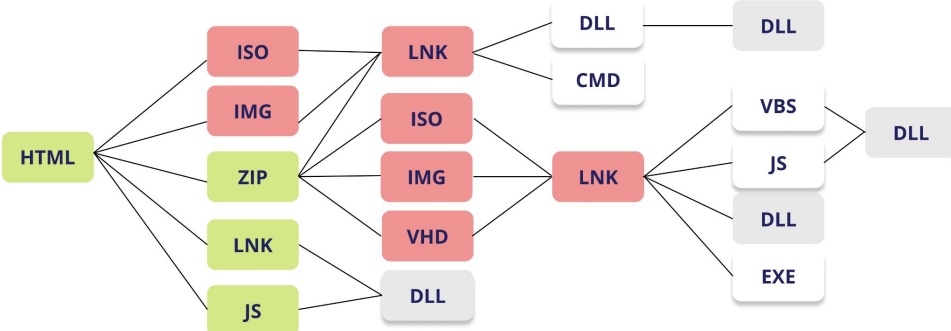
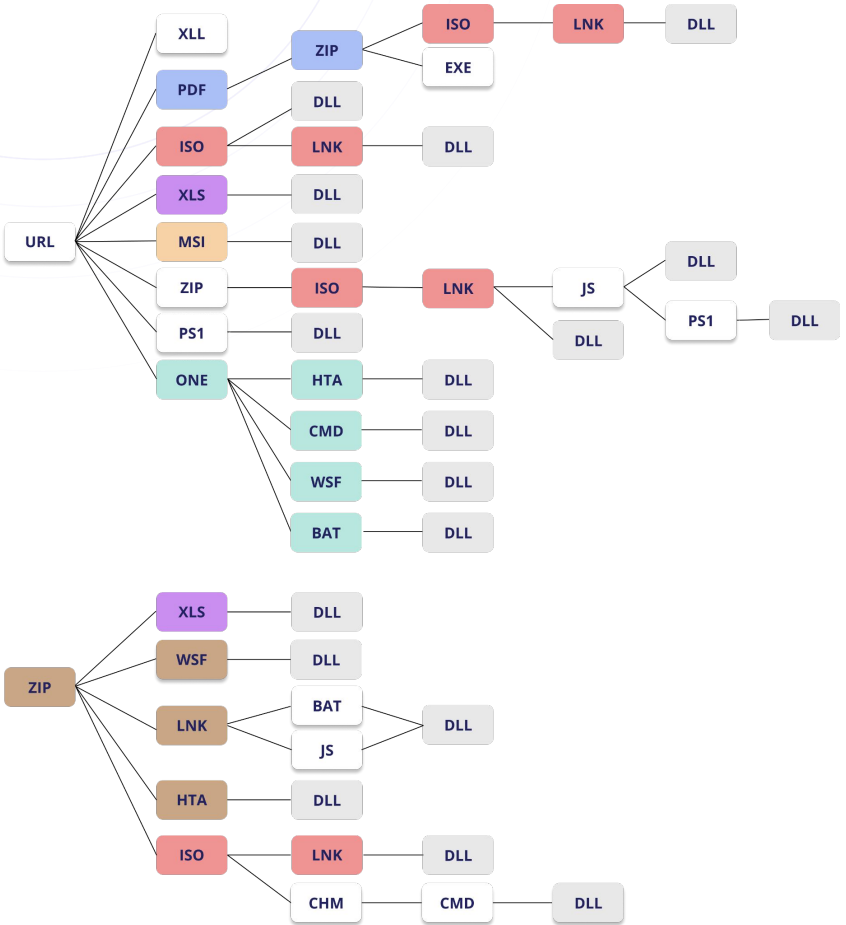
- Conti
- Quantum
- TA551
- Wizard Spider
- ...

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

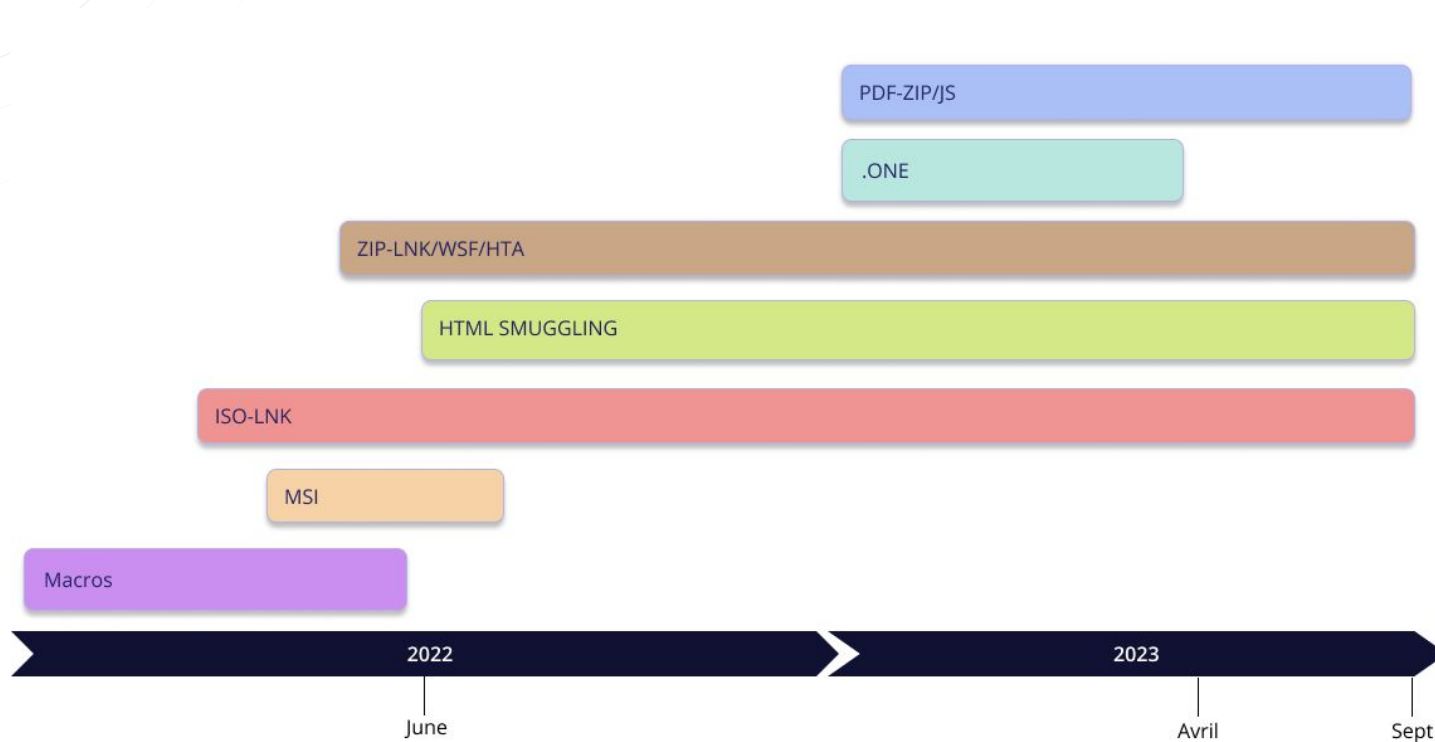
- Cobalt Strike
- Egregor
- Maze
- Metasploit
- ...

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

Welcome to the jungle



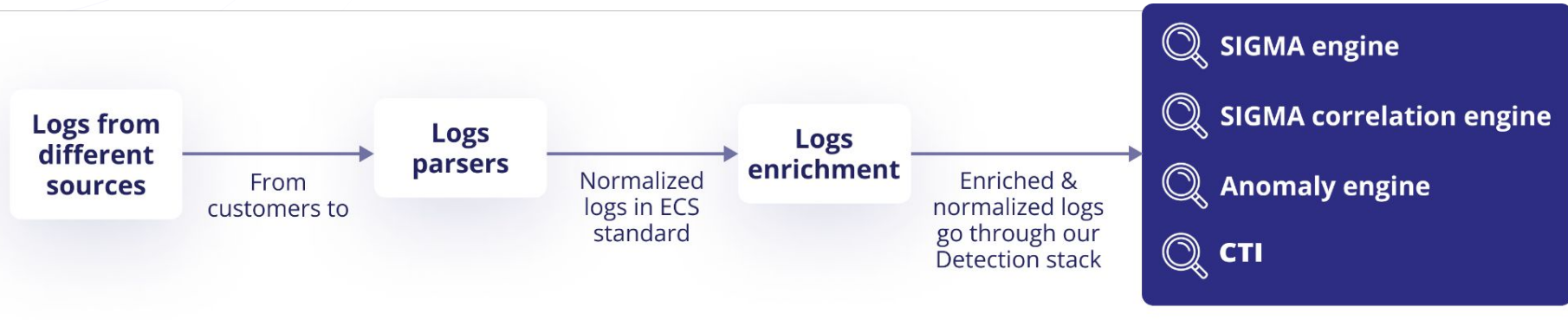
"Root" infection chains timeline





Enhancing detection with Correlation

Telemetry and research environment



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

Sigma Correlation



```
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

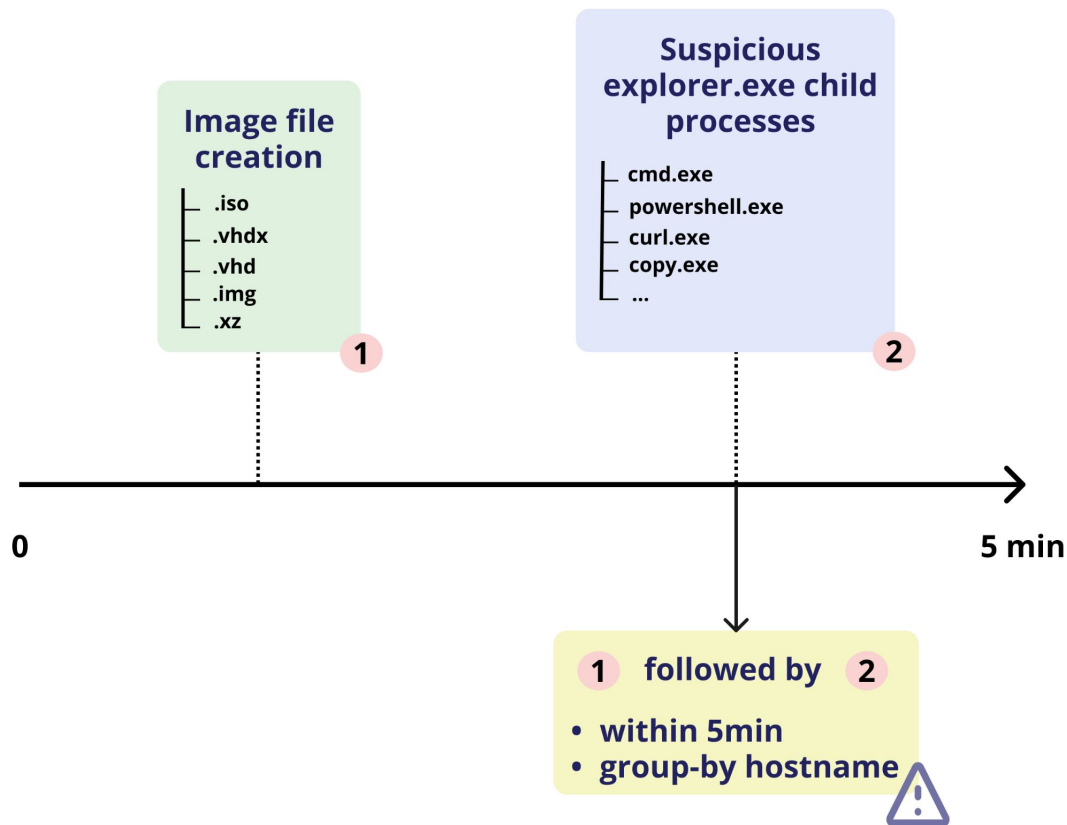
Process c:\windows\system32\wscript.exe created by bob on Bob-computer 60

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
```

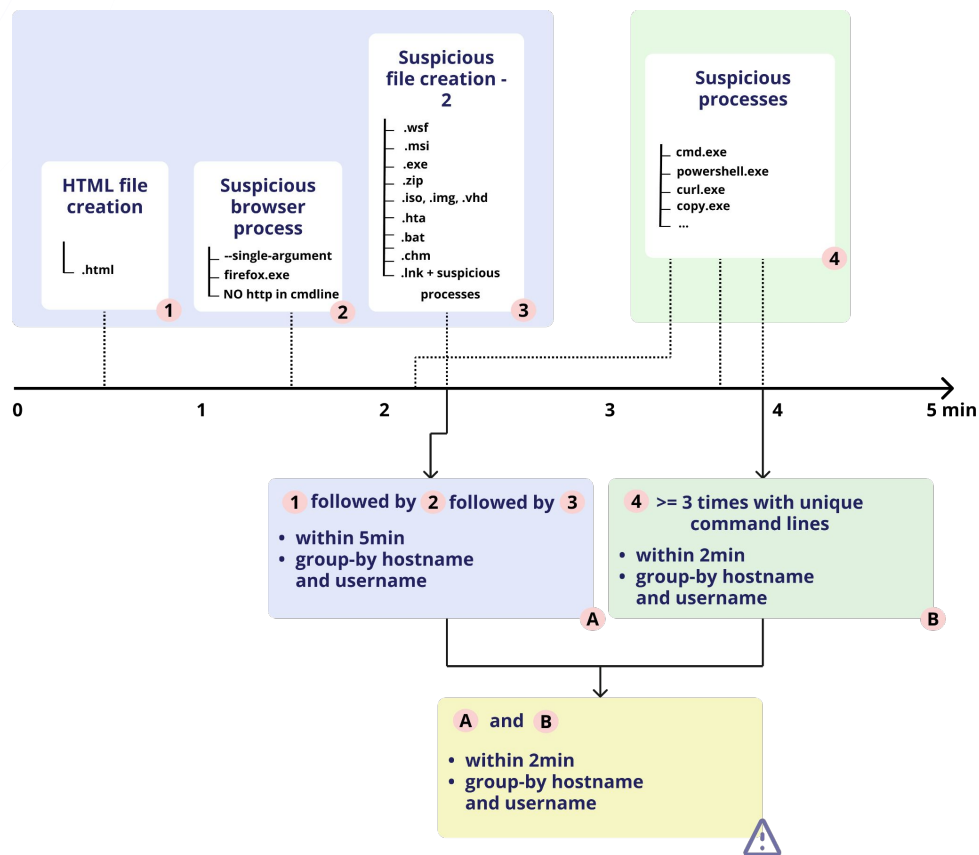
ISO-LNK infection chain - correlation rule



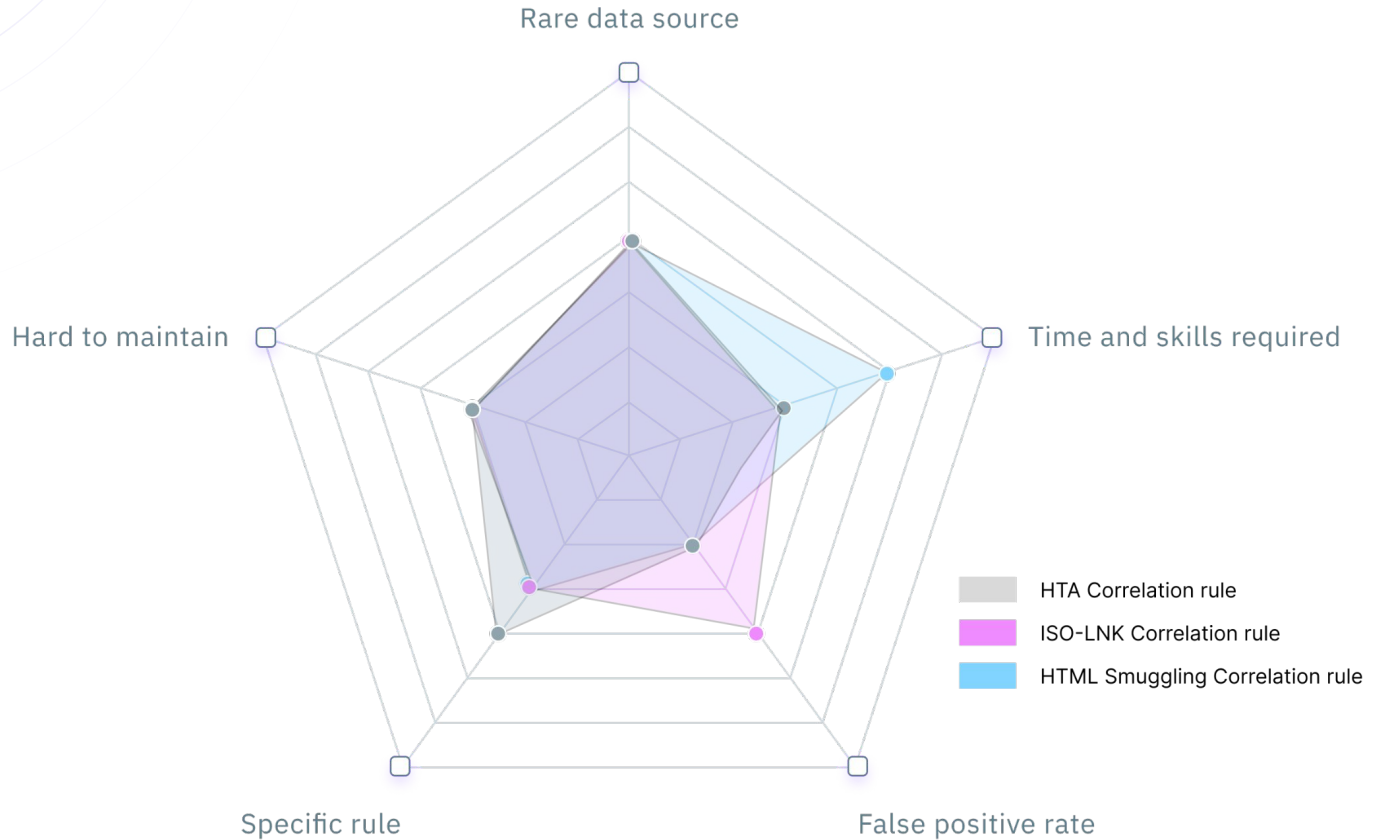


-  SEKOIA.IO  15:44:06
Alert created
-  Event  15:43:30
Process `c:\windows\system32\cmd.exe` created by `bob` on  Bob-computer 
-  Event  15:43:30
Process `c:\windows\system32\xcopy.exe` created by `bob` on  Bob-computer 
-  Event  15:43:17
File create to `C:\Users\bob\Downloads\SurplicianRectilineation.zip` on  Bob-computer 
-  Event  15:43:14
Process `c:\program files\mozilla firefox\firefox.exe` created by `bob` on  Bob-computer 
-  Event  15:43:04
`borisux.html` created by `c:\program files\mozilla firefox\firefox.exe` on  Bob-computer 

HTML Smuggling - correlation rule



Rules balance





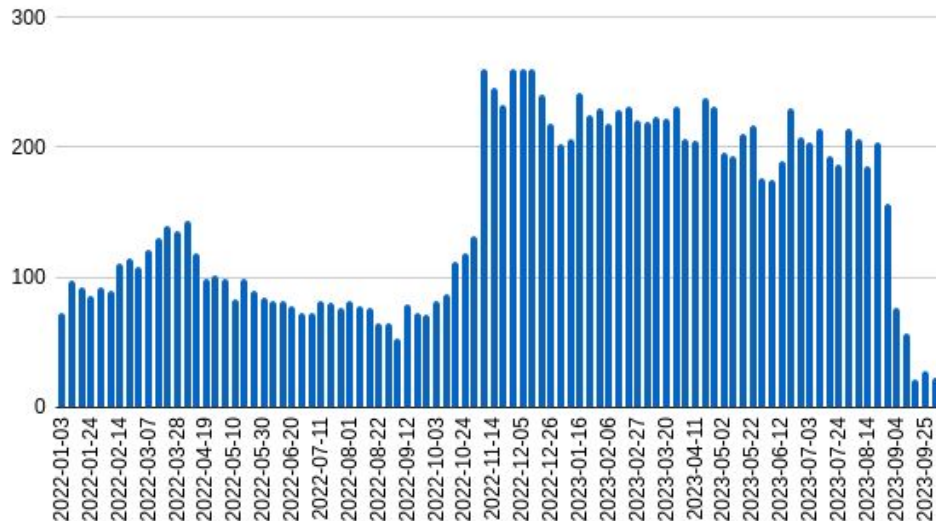
Detection integration with CTI at scale

C2 Trackers

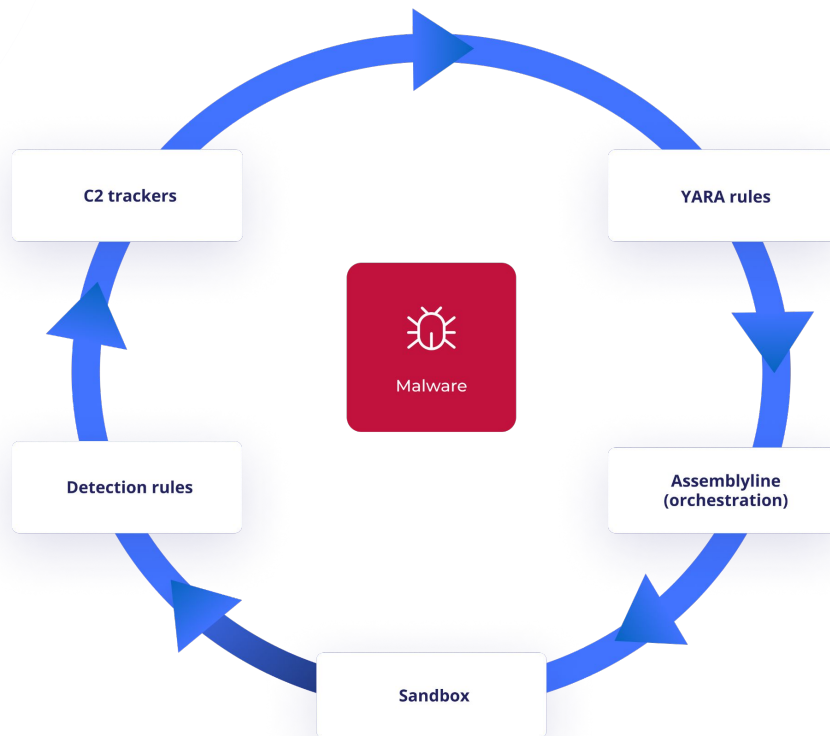


```
"cipher_selected": "TLS_CHACHA20_POLY1305_SHA256",  
"certificates": {  
  "1" "encoding": {  
    "leaf_fp_sha_256": "DISPLAY_HEX"  
  },  
  "leaf_fp_sha_256": "2f4055d179d0dbca38dcf7473ffbbc00558333bcb3d067d489504878bcc87972",  
  "leaf_data": {  
    "names": [  
      "tqcs.biz"  
    ],  
    "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"  
      ],  
      "2" "organization": [  
        "Paevjwyc Xmo Fbkfiodak"  
      ],  
      "3" "province": [  
        "GI"  
      ],  
      "4" "country": [  
        "AU"  
      ],  
      "5" ]  
    },  
    "subject": {  
      "common_name": [  
        "tqcs.biz"  
      ],  
      "6" "organizational_unit": [  
        "Ekejyrjli Ivbtdgu Ogovau"  
      ],  
      "country": [  
        "AU"  
      ]  
    }  
  }  
}
```

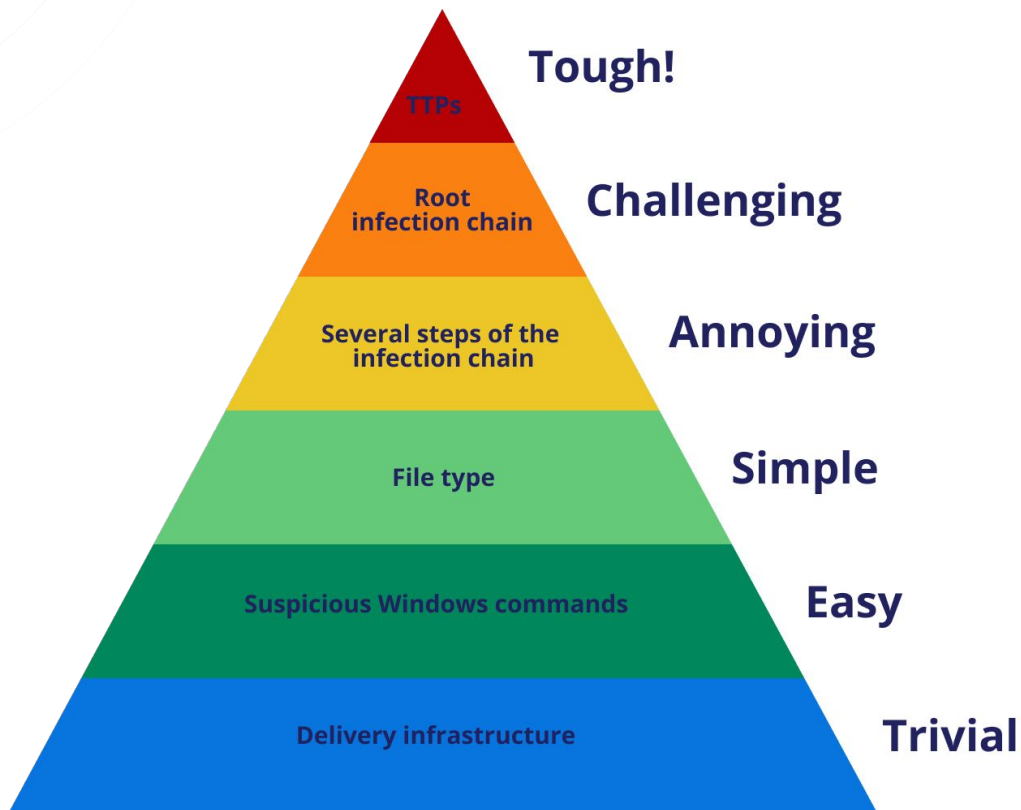
Qbot



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/appendix_meta_rules.md

<https://github.com/pr0xylife>

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