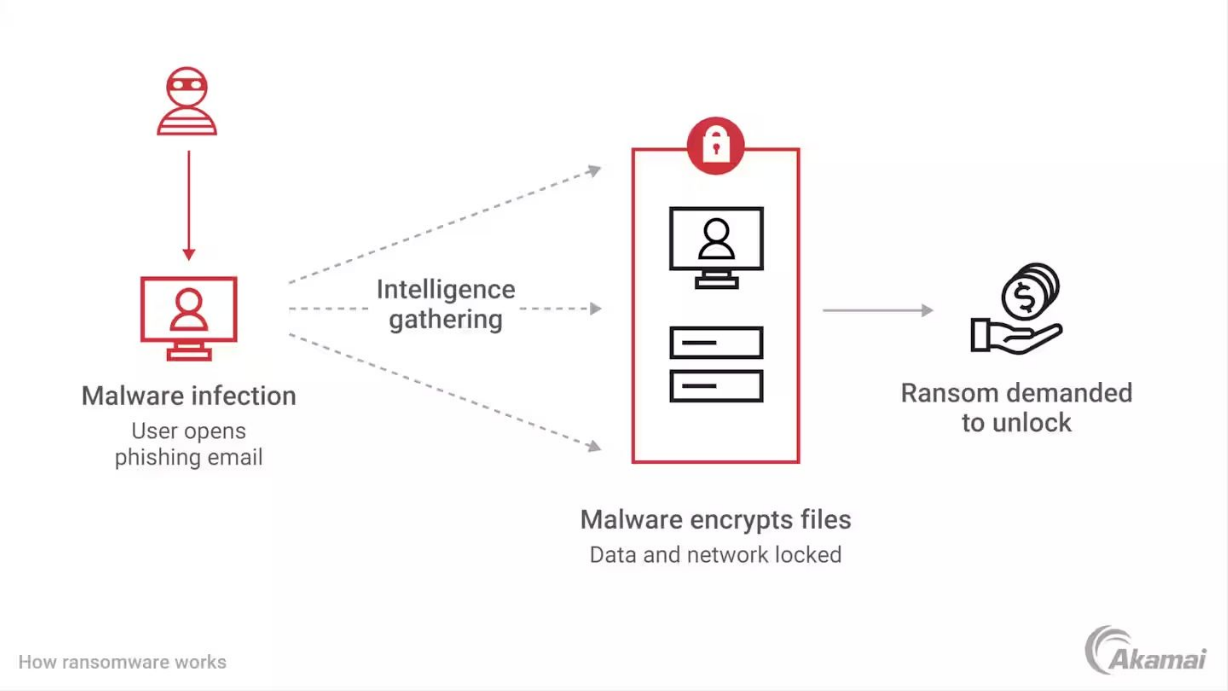
Ransomware

Liuhai and Ryan

How Does Ransomware Work?



Malware infection

User opens phishing email

Intelligence gathering

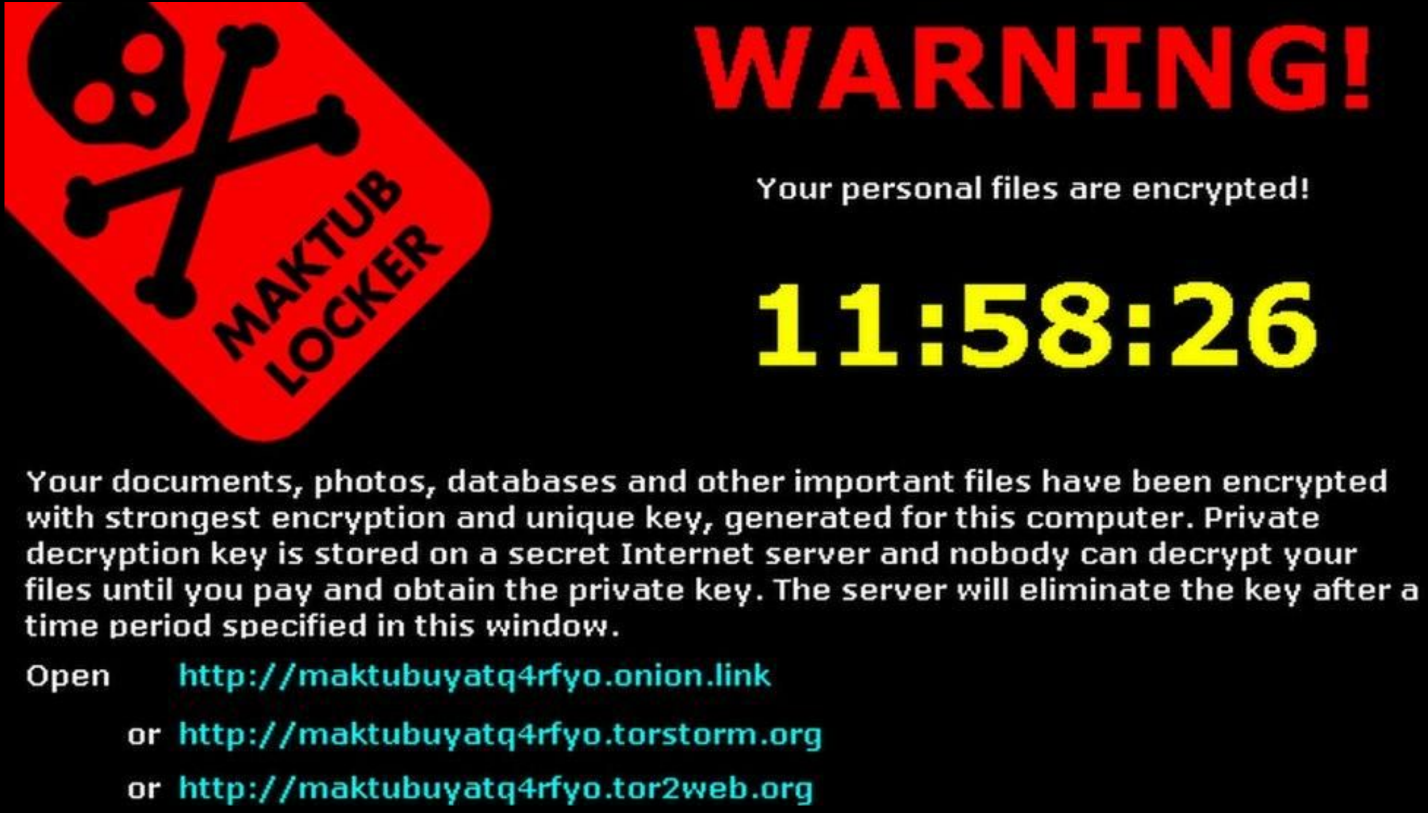
Malware encrypts files

Data and network locked

Ransom demanded to unlock

How ransomware works

Ransomware Example



WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://maktubuyatq4rfyo.onion.link

or http://maktubuyatq4rfyo.torstorm.org

or http://maktubuyatq4rfyo.tor2web.org

What is Ransomware Detection?

Ransomware detection notifies user(s) when:

1. Ransomware is present on their system
2. Their files are already being encrypted,
3. Guides users through recovery steps in the event of Ransomware

These methods can be implemented through tools like

1. Intrusion Detection Systems (IDS),
2. Endpoint Detection
3. Response (EDR) solutions
4. Threat intelligence platforms

How to Detect Ransomware?

Signature Based Detection

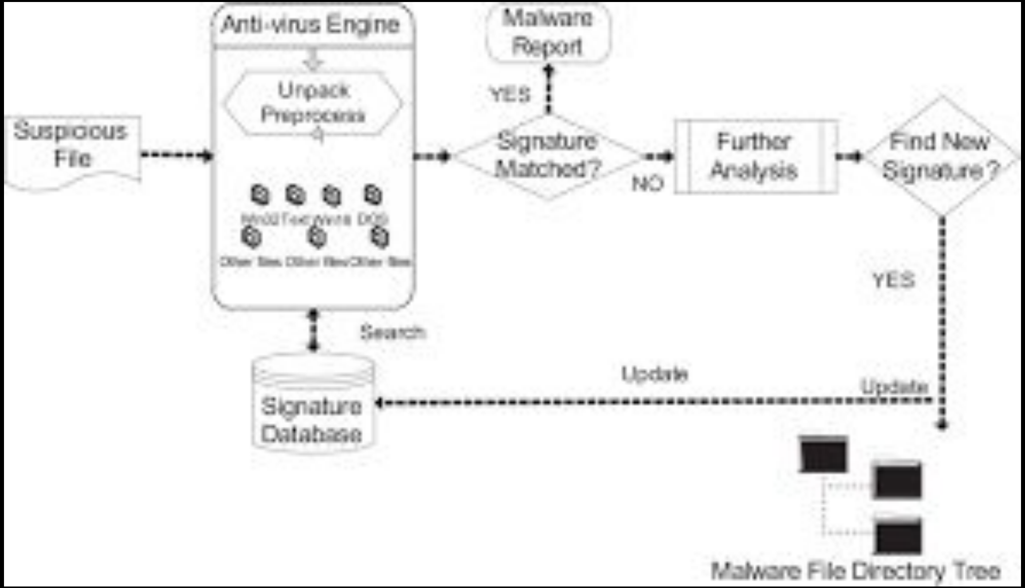
Behavior Based Detection

Traffic Based Detection

Signature Based Detection

An attack signature can be generated based on characteristics of the payload
Compares known signature against files or network traffic

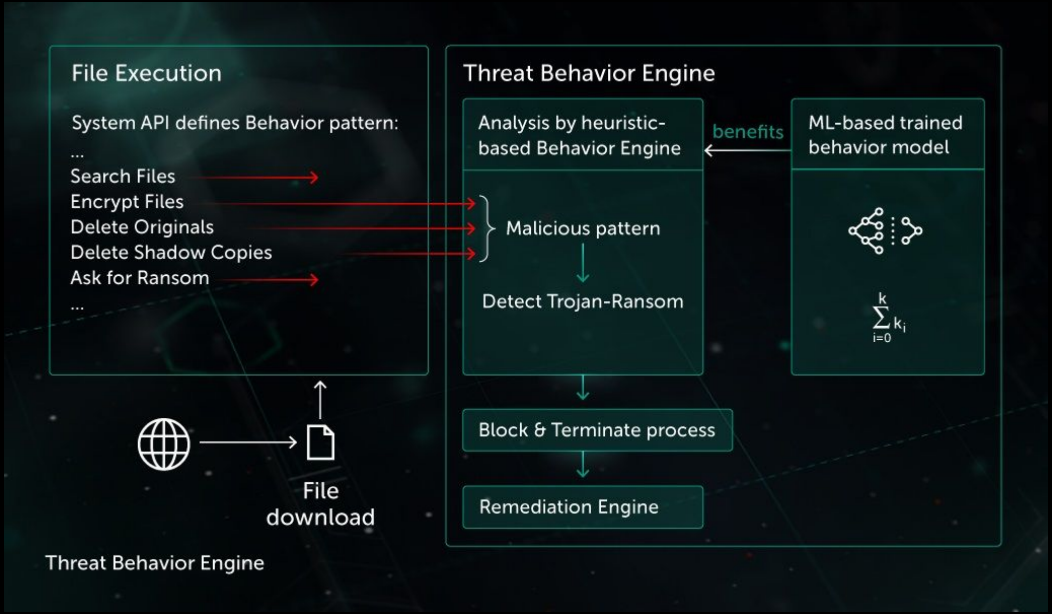
Detection tool: Corelight or Fidelis Network



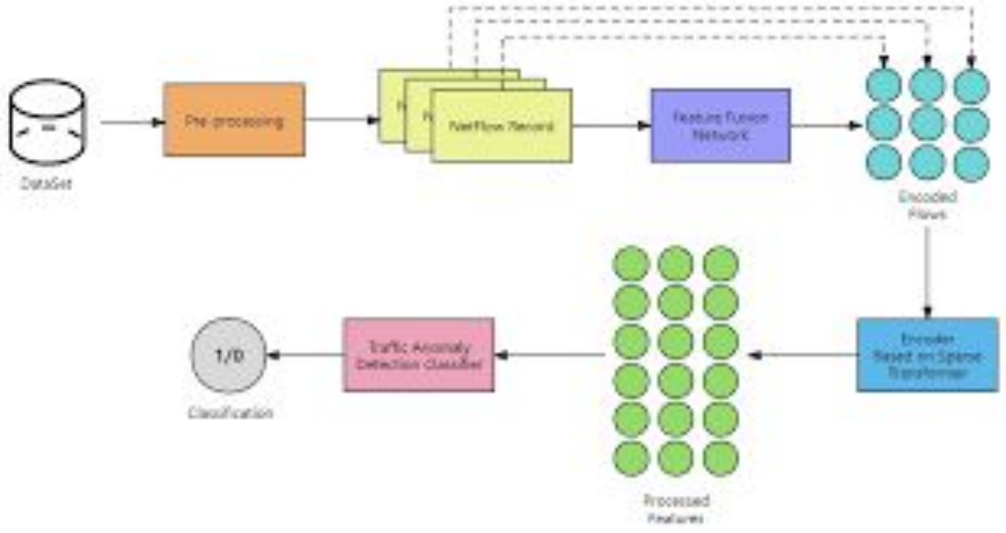
Behavior Based Detection

Identifying suspicious patterns of activity rather than relying on known malware signatures

Detection tool: Cynet360 or CrowdStrike Falcon



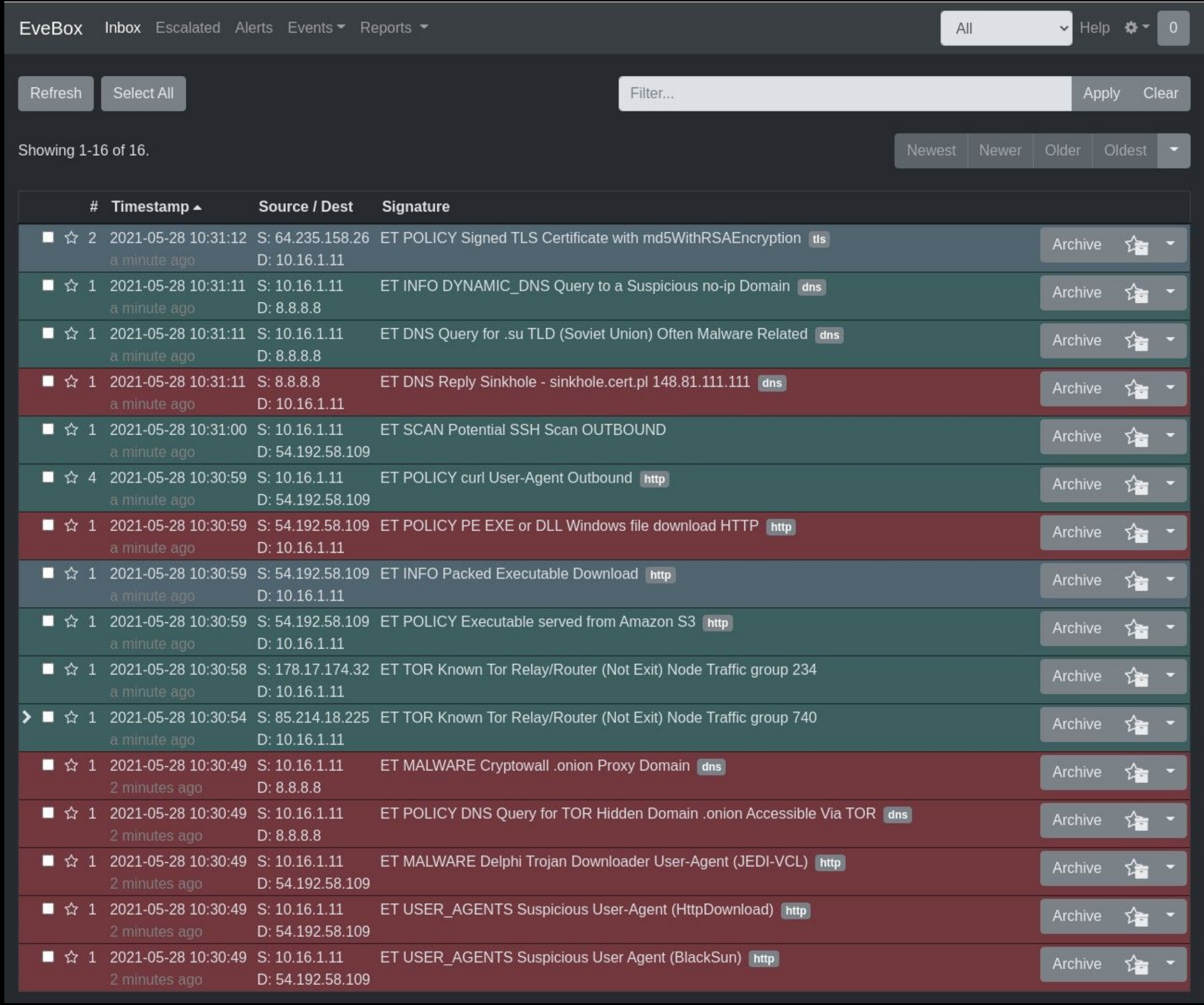
Traffic Based Detection



Monitoring network traffic for unusual patterns and behaviors that might indicate a ransomware attack

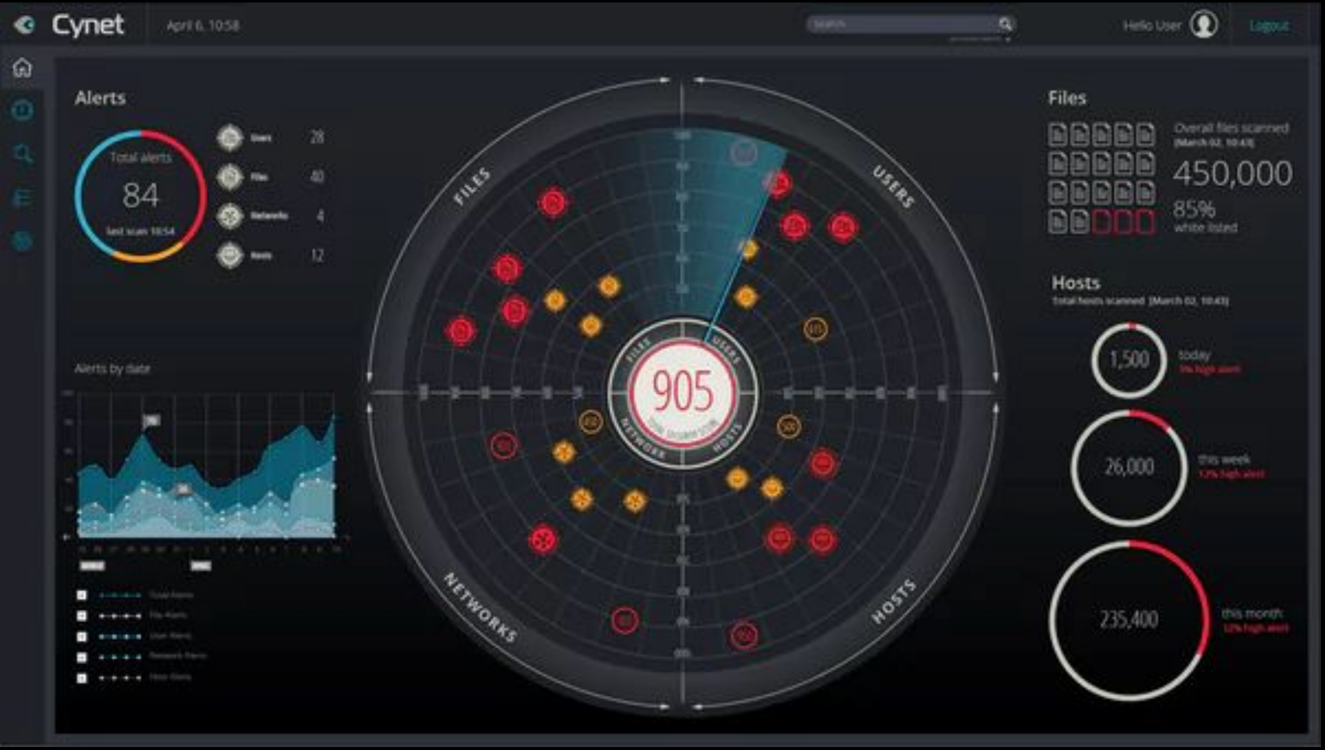
Detection tool: Corelight Suricata

Suricata IDS on Corelight



Showing 1-16 of 16.

#	Timestamp	Source / Dest	Signature
2	2021-05-28 10:31:12 a minute ago	S: 64.235.158.26 D: 10.16.1.11	ET POLICY Signed TLS Certificate with md5WithRSAEncryption tls
1	2021-05-28 10:31:11 a minute ago	S: 10.16.1.11 D: 8.8.8.8	ET INFO DYNAMIC_DNS Query to a Suspicious no-ip Domain dns
1	2021-05-28 10:31:11 a minute ago	S: 10.16.1.11 D: 8.8.8.8	ET DNS Query for .su TLD (Soviet Union) Often Malware Related dns
1	2021-05-28 10:31:11 a minute ago	S: 8.8.8.8 D: 10.16.1.11	ET DNS Reply Sinkhole - sinkhole.cert.pl 148.81.111.111 dns
1	2021-05-28 10:31:00 a minute ago	S: 10.16.1.11 D: 54.192.58.109	ET SCAN Potential SSH Scan OUTBOUND
4	2021-05-28 10:30:59 a minute ago	S: 10.16.1.11 D: 54.192.58.109	ET POLICY curl User-Agent Outbound http
1	2021-05-28 10:30:59 a minute ago	S: 54.192.58.109 D: 10.16.1.11	ET POLICY PE EXE or DLL Windows file download HTTP http
1	2021-05-28 10:30:59 a minute ago	S: 54.192.58.109 D: 10.16.1.11	ET INFO Packed Executable Download http
1	2021-05-28 10:30:59 a minute ago	S: 54.192.58.109 D: 10.16.1.11	ET POLICY Executable served from Amazon S3 http
1	2021-05-28 10:30:58 a minute ago	S: 178.17.174.32 D: 10.16.1.11	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 234
1	2021-05-28 10:30:54 a minute ago	S: 85.214.18.225 D: 10.16.1.11	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 740
1	2021-05-28 10:30:49 2 minutes ago	S: 10.16.1.11 D: 8.8.8.8	ET MALWARE Cryptowall .onion Proxy Domain dns
1	2021-05-28 10:30:49 2 minutes ago	S: 10.16.1.11 D: 8.8.8.8	ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR dns
1	2021-05-28 10:30:49 2 minutes ago	S: 10.16.1.11 D: 54.192.58.109	ET MALWARE Delphi Trojan Downloader User-Agent (JEDI-VCL) http
1	2021-05-28 10:30:49 2 minutes ago	S: 10.16.1.11 D: 54.192.58.109	ET USER_AGENTS Suspicious User-Agent (HttpDownload) http
1	2021-05-28 10:30:49 2 minutes ago	S: 10.16.1.11 D: 54.192.58.109	ET USER_AGENTS Suspicious User Agent (BlackSun) http


Cynet
April 6, 10:58
Hello User
Logout
Alerts
Total alerts
84
last scan 10:54
Users 28
Files 40
Networks 4
Hosts 12
Alerts by date
Total Alerts
File Alerts
User Alerts
Network Alerts
Host Alerts
FILES
USERS
NETWORKS
HOSTS
905
Files
Overall files scanned
(March 02, 10:43)
450,000
85%
white listed
Hosts
Total hosts scanned (March 02, 10:43)
1,500
today
26,000
this week
235,400
this month

Cynet

Analyzing Ransomware

Unusual Outbound Traffic

Sudden spikes in data leaving network

Unusual C2 (command and control) server communications

Connections to Malicious or Blacklisted Domains

Contact occurs with a known ransomware infrastructure

Suspicious SMB and RDP activity

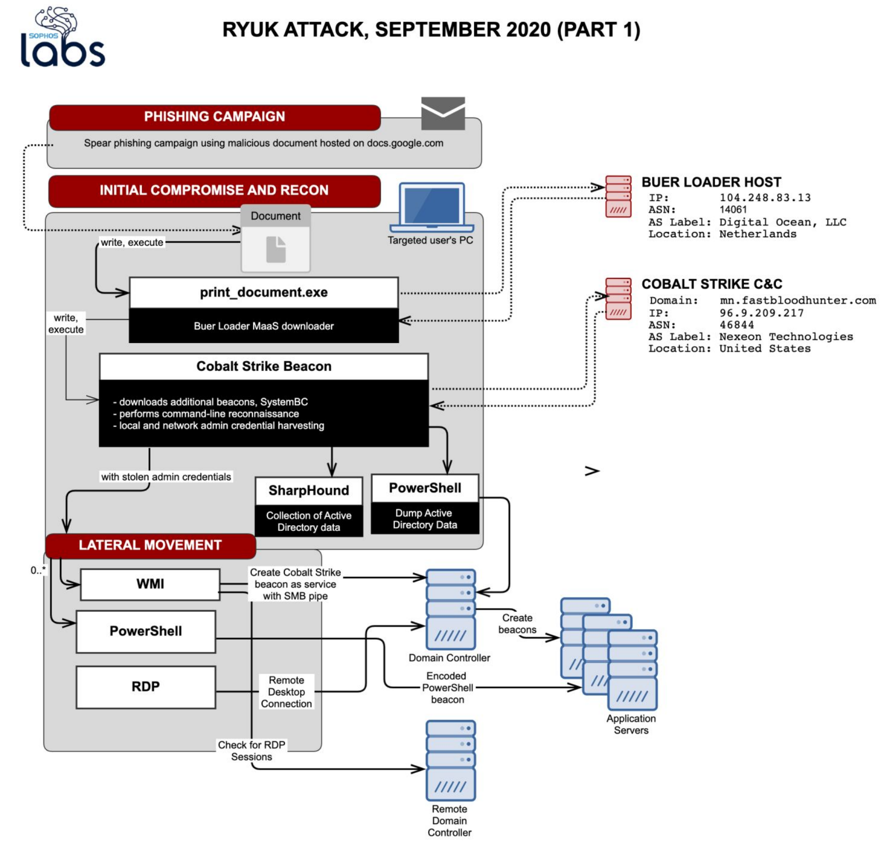
Increased file sharing or remote desktop use

Lateral Movements within network

Rapid File Rename or Encryption Events

Bulk renaming/encrypting over SMB

Case Study: Ryuk



RYUK ATTACK, SEPTEMBER 2020 (PART 1)

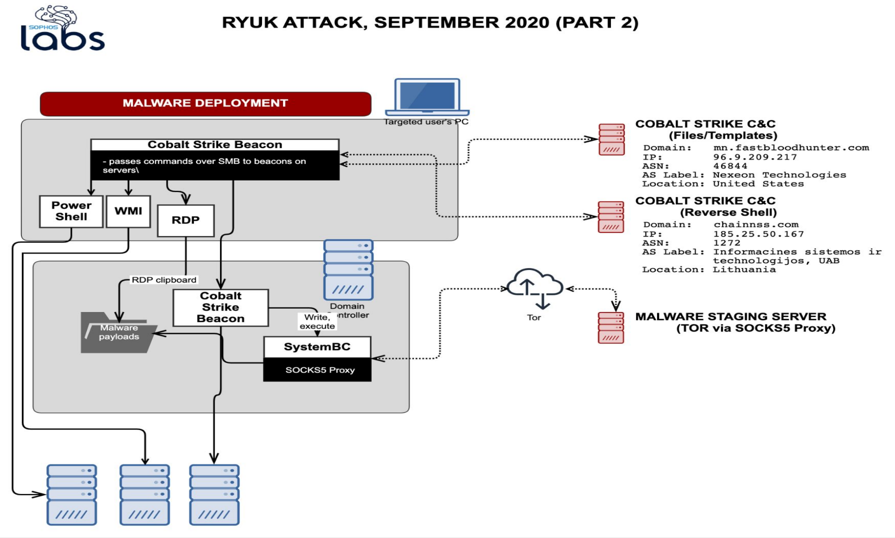
SOPHOS
labs
PHISHING CAMPAIGN
Spear phishing campaign using malicious document hosted on docs.google.com
INITIAL COMPROMISE AND RECON
Document
Targeted user's PC
write, execute
print_document.exe
Buer Loader MaaS downloader
write,
execute
Cobalt Strike Beacon
- downloads additional beacons, SystemBC
- performs command-line reconnaissance
- local and network admin credential harvesting
with stolen admin credentials
SharpHound
Collection of Active Directory data
PowerShell
Dump Active Directory Data
LATERAL MOVEMENT
0..*
WMI
PowerShell
RDP
Create Cobalt Strike beacon as service with SMB pipe
Remote Desktop Connection
Check for RDP Sessions
Encoded PowerShell beacon
Create beacons
Domain Controller
Application Servers
Remote Domain Controller
>

BUER LOADER HOST

```
IP:        104.248.83.13
ASN:       14061
AS Label:  Digital Ocean, LLC
Location:  Netherlands
```

COBALT STRIKE C&C

```
Domain:    mn.fastbloodhunter.com
IP:        96.9.209.217
ASN:       46844
AS Label:  Nexeon Technologies
Location:  United States
```



RYUK ATTACK, SEPTEMBER 2020 (PART 2)

COBALT STRIKE C&C
(Files/Templates)

```
Domain:    mn.fastbloodhunter.com
IP:        96.9.209.217
ASN:       46844
AS Label:  Nexeon Technologies
Location:  United States
```

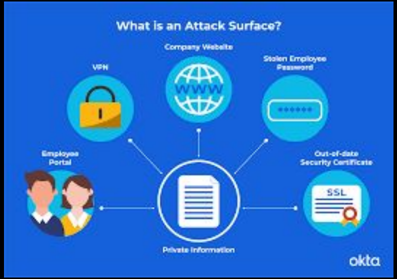
COBALT STRIKE C&C
(Reverse Shell)

```
Domain:    chainnss.com
IP:        185.25.50.167
ASN:       1272
AS Label:  Informacines sistemos ir
           technologijos, UAB
Location:  Lithuania
```

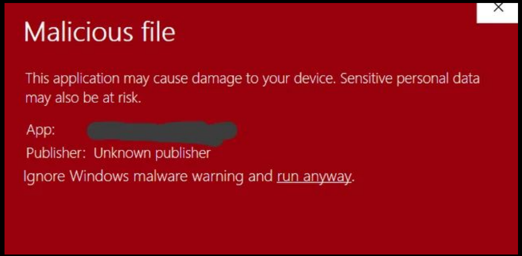
MALWARE STAGING SERVER
(TOR via SOCKS5 Proxy)

Challenges in Detection

Larger attack surface with today's networks



Difficulty distinguishing malicious vs. normal file access at scale


Malicious file

This application may cause damage to your device. Sensitive personal data may also be at risk.

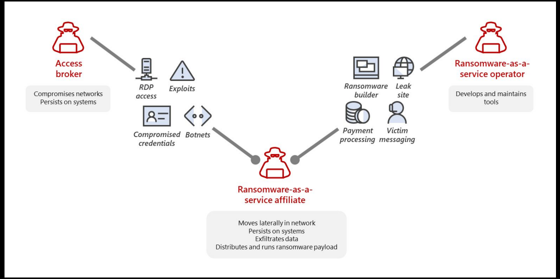
App: [redacted]

Publisher: Unknown publisher

Ignore Windows malware warning and run anyway.

Low user awareness leading to phishing

Rise of Ransomware as a Service (RAAS)

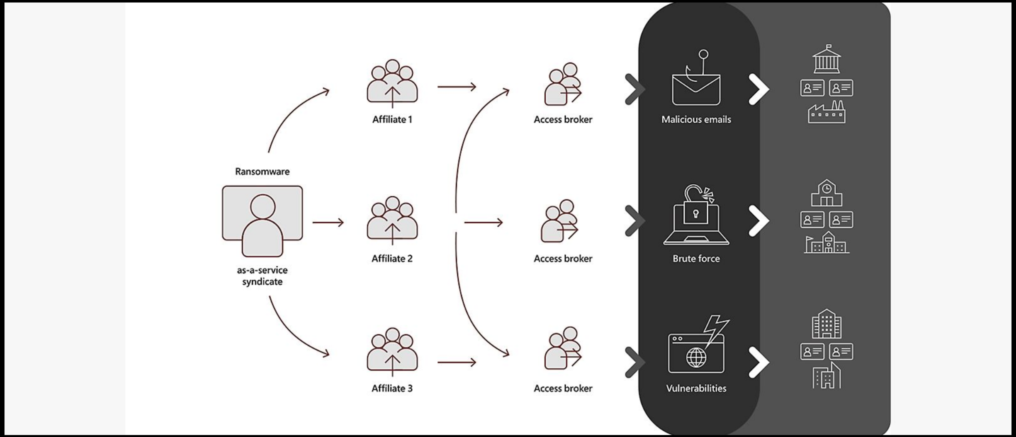


Future Trends

AI and ML models for **detecting abnormal patterns** and **faster automated forensic analysis tools**

Improved **threat intelligence sharing between organizations**

Ransomware-as-a-Service (RaaS) will make attacks more frequent and harder to track



QUESTIONS?