Emerging Threats

Keeping informed

Introduction

Assignments

Your final grade will be the sum of four assignments each worth 25%. Assignments are to be submitted via BrightSpace in PDF format (no docx). Due dates will be determined when assignments are assigned. If you fail to submit an assignment on time, 5% will be deducted from your mark on the assignment for each day (including weekends) it is late for a maximum of 5 days. After that, you will receive a 0%.

TTP

Tactics, Techniques and Procedures

Tactics - Beginning-to-end strategies hackers follow to accomplish their goals

Techniques - Non-specific, common methods or tools that a criminal will use.

Procedures - Step-by-step orchestration of an attack.

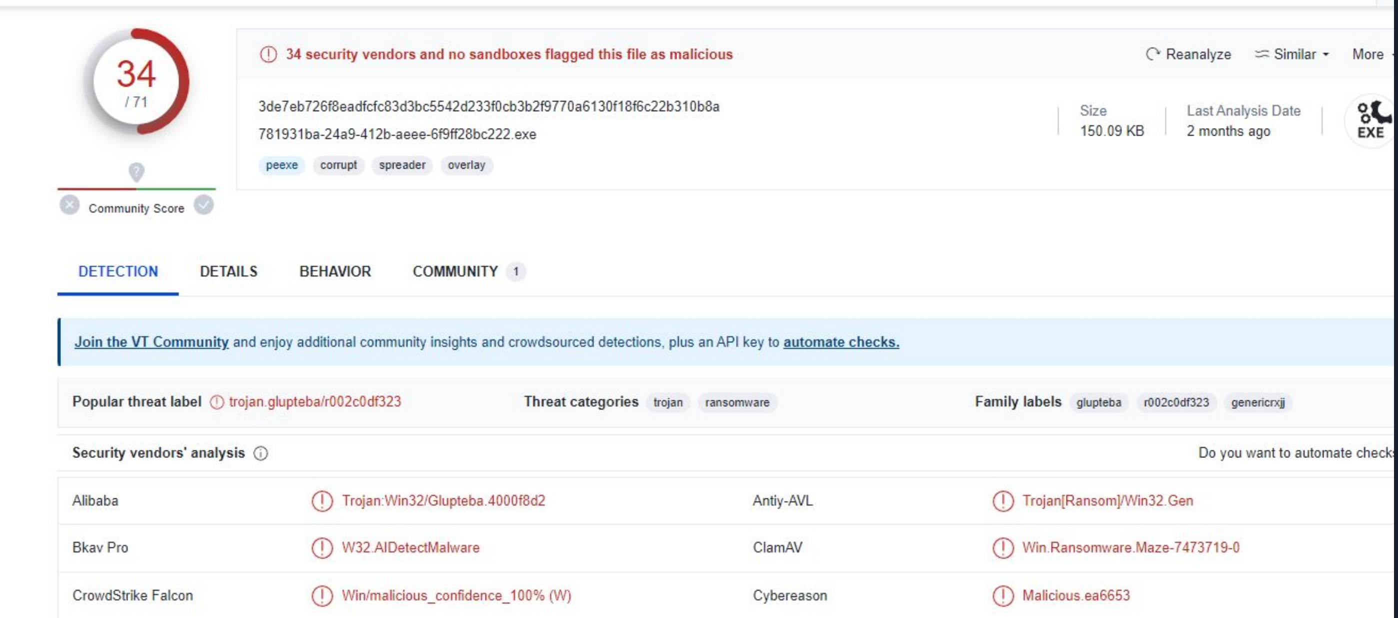
Indicator (IoC)

Signs or characteristics of an attack.

- Traffic to IP Addresses
- File hashes
- System commands

IoC Example - File Hash

Every file will have a hash that can uniquely identify it. If a certain file hash is discovered to be malicious, it can be used as an IoC. Below is Mazer Ransomware:



34 security vendors and no sandboxes flagged this file as malicious

3de7eb726f8eadfcfc83d3bc5542d233f0cb3b2f9770a6130f18f6c22b310b8a

781931ba-24a9-412b-aeee-6f9ff28bc222.exe

peexe corrupt spreader overlay

Size 150.09 KB

Last Analysis Date 2 months ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.glupteba/r002c0df323

Threat categories trojan ransomware

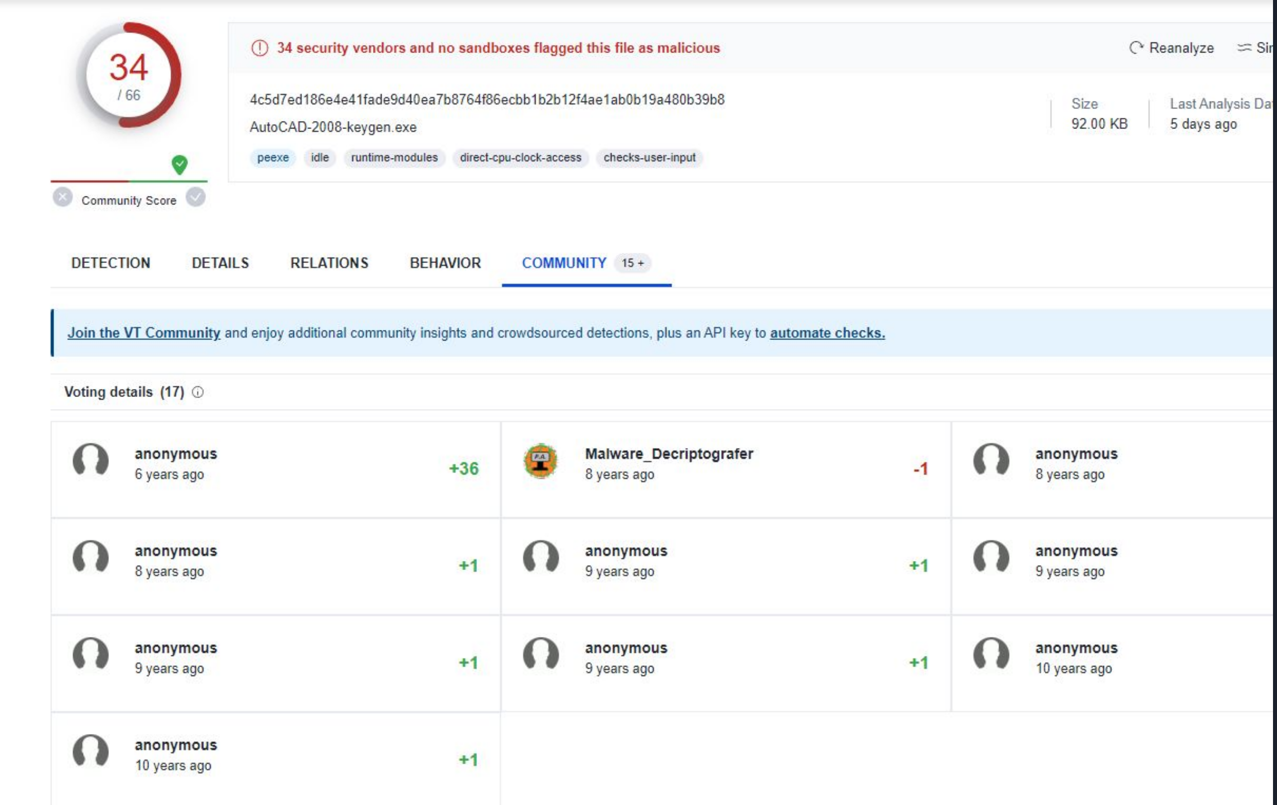
Family labels glupteba r002c0df323 genericrxjj

Security vendors' analysis

Do you want to automate check

Alibaba	Trojan:Win32/Glupteba.4000f8d2	Antiy-AVL	Trojan[Ransom]/Win32.Gen
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Ransomware.Maze-7473719-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.ea6653

Community Ratings



34 / 66

Community Score

34 security vendors and no sandboxes flagged this file as malicious

Reanalyze Sir

4c5d7ed186e4e41fade9d40ea7b8764f86ecbb1b2b12f4ae1ab0b19a480b39b8

AutoCAD-2008-keygen.exe

peexe idle runtime-modules direct-cpu-clock-access checks-user-input

Size
92.00 KB

Last Analysis Da
5 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Voting details (17)

anonymous
6 years ago
+36

Malware_Decriptografer
8 years ago
-1

anonymous
8 years ago

anonymous
8 years ago
+1

anonymous
9 years ago
+1

anonymous
9 years ago

anonymous
9 years ago
+1

anonymous
9 years ago
+1

anonymous
10 years ago

anonymous
10 years ago
+1

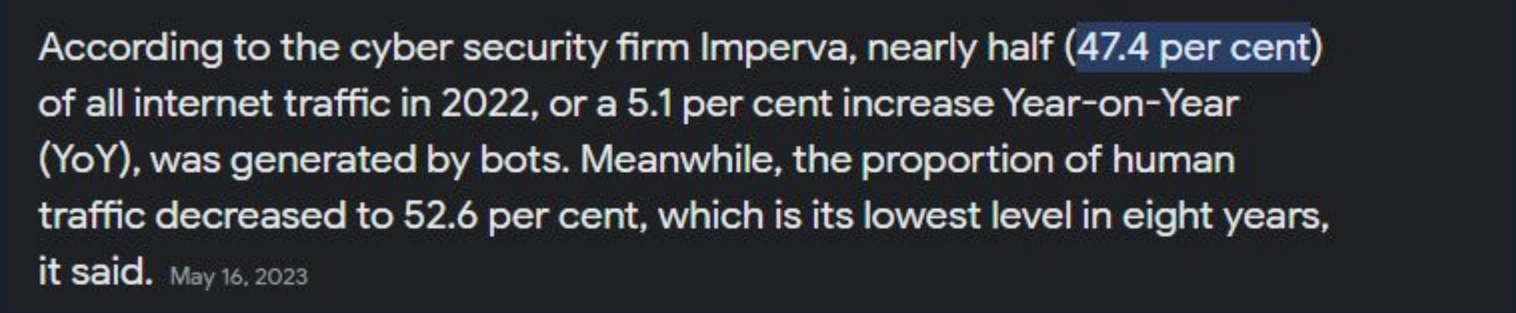
The World of Threat Actors

- Script Kiddies
- Inside Actors
- Hacktivists
- Organized Crime
- Nation-State Actors

Script Kiddies

- Very basic understanding of coding/hacking
- Opportunistic (low hanging fruits)
- Gets scripts online or uses metasploit

Script Kiddies

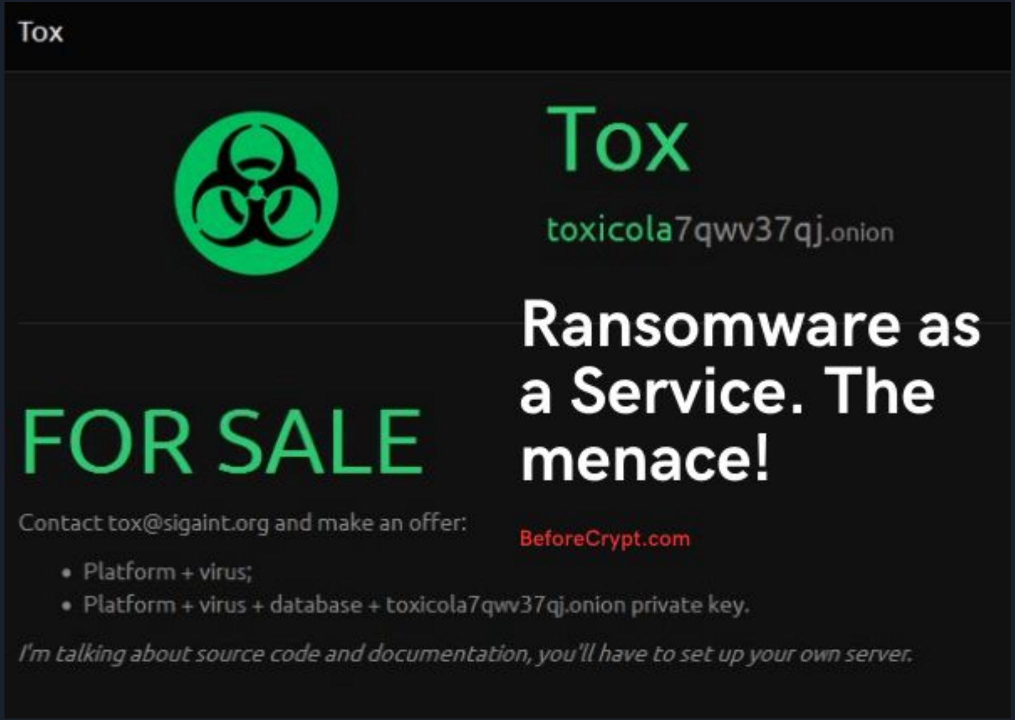


According to the cyber security firm Imperva, nearly half (47.4 per cent) of all internet traffic in 2022, or a 5.1 per cent increase Year-on-Year (YoY), was generated by bots. Meanwhile, the proportion of human traffic decreased to 52.6 per cent, which is its lowest level in eight years, it said. May 16, 2023

Script Kiddies

- Admin page brute-forcing
- Wordpress vulnerabilities
- Exchange server CVEs
- Run-and-root scripts

Script Kiddies



Tox

Tox

toxicola7qwv37qj.onion

Ransomware as a Service. The menace!

FOR SALE

BeforeCrypt.com

Contact tox@sigaint.org and make an offer:

- Platform + virus;
- Platform + virus + database + toxicola7qwv37qj.onion private key.

I'm talking about source code and documentation, you'll have to set up your own server.

Inside Actors

- Can be technically experienced or not
- Sell credentials
- Disgruntled employees
- Taking a job for the purpose of installing ransomware
- Dumb employees
- Business email compromise
- Authenticated customer

Inside Actors

- A threat because they:
  - Are already inside
  - Trusted
  - Know the environment (potentially)
  - Know the people
- Go after:
  - Data (selling or destroying)
  - Reputational damage (impersonation)

Hacktivists

Hacktivists

- Activism
- Fear mongering
- Target specific organizations
- Target essential services
  - Utilities
  - Healthcare

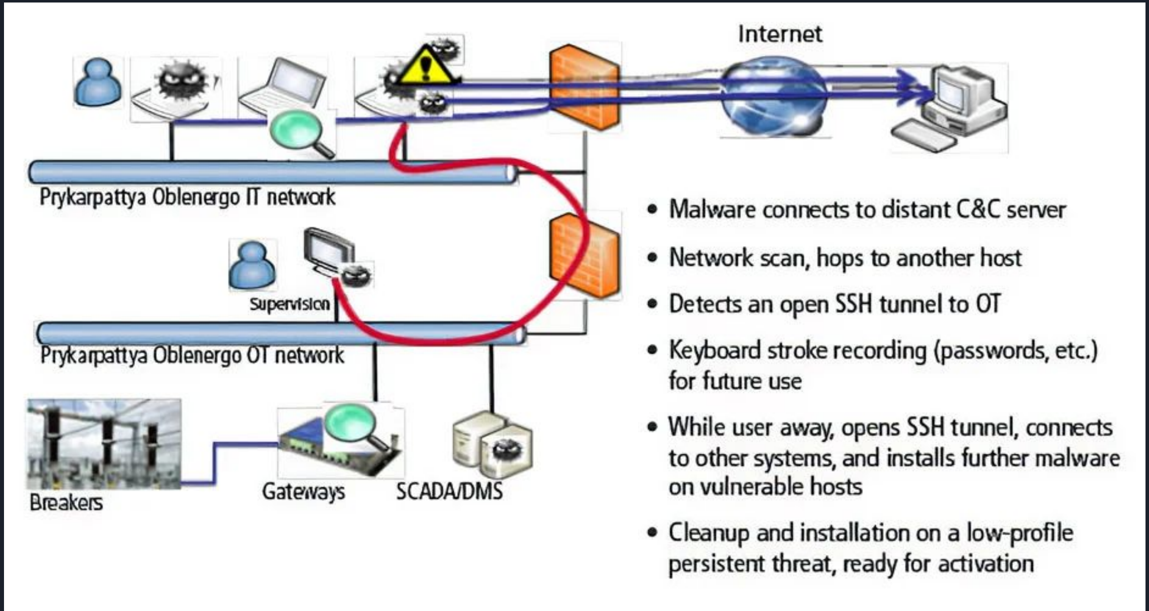
Hacktivists

- Use advanced social engineering
  - MFA bypass
  - Visahing
  - Long email campaigns
- Zero-days
- DDoS attacks

Nation-State Actors

- A lot of time and budget
- Develop Zero-days
- Work with companies to create zero-days (allegedly)
- Used for war efforts
- Go after critical infrastructure

Nation-State Actors


Internet
Prykarpattya Oblenergo IT network
Supervision
Prykarpattya Oblenergo OT network
Breakers
Gateways
SCADA/DMS

- Malware connects to distant C&C server
- Network scan, hops to another host
- Detects an open SSH tunnel to OT
- Keyboard stroke recording (passwords, etc.) for future use
- While user away, opens SSH tunnel, connects to other systems, and installs further malware on vulnerable hosts
- Cleanup and installation on a low-profile persistent threat, ready for activation

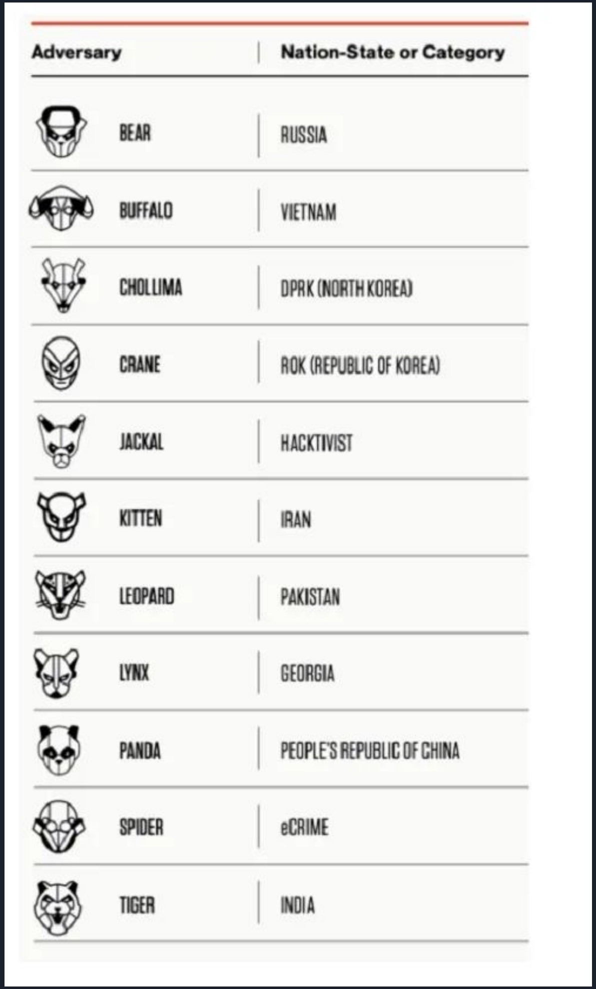
Nation-State Actors

“Dragos Security concluded that the attack was not merely to cause short-term disruption but to cause long-lasting damage that could last weeks or months”

https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

Nation-State Actors

Crowdstrike’s categorization of threat actors:



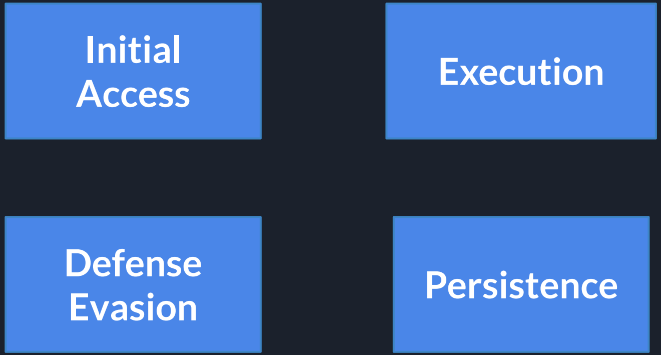
Adversary	Nation-State or Category
BEAR	RUSSIA
BUFFALO	VIETNAM
CHOLLIMA	DPRK (NORTH KOREA)
CRANE	ROK (REPUBLIC OF KOREA)
JACKAL	HACKTIVIST
KITTEN	IRAN
LEOPARD	PAKISTAN
LYNX	GEORGIA
PANDA	PEOPLE'S REPUBLIC OF CHINA
SPIDER	eCRIME
TIGER	INDIA

MITRE Tactics

Recon

Resource Development

Phase 1: Discovery



Initial Access

Execution

Defense Evasion

Persistence

Phase 2: Exploitation

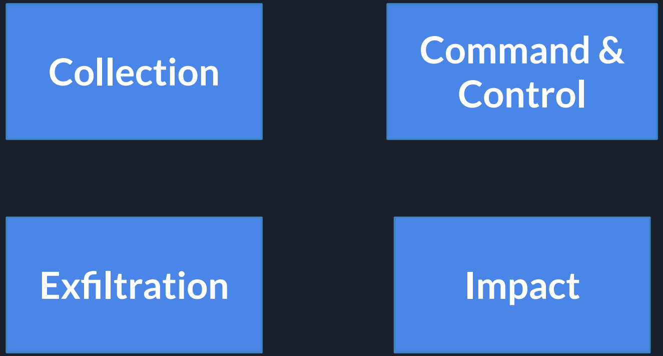
Privilege Escalation

Credential Access

Lateral Movement

Discovery

Phase 3: Privilege Escalation



Collection

Command & Control

Exfiltration

Impact

Phase 4: Causing Damage

Keeping Informed

Good Sources - Crowdstrike Threat Report

- On Brightspace for you
- Easy to sign up for for future editions

Conferences

- AtlSecCon
- ISACA
- Black Hat
- Defcon
- Fal Con

News

- https://thehackernews.com
- Youtube

Traffic Maps

- https://threatmap.checkpoint.com/
- https://cybermap.kaspersky.com/

Try Hack Me

- https://tryhackme.com/room/outlookntlmleak

Set up Google Alerts

1. https://www.google.com/alerts (Need google account)
2. Enter your topic
   a. Breach, Zero-day, Exploit, Cyber attack, etc.
3. Enter your settings
   a. Once per week
4. Create Alert
5. Make sure the emails aren’t going into spam

Old Techniques and Procedures

Should I only learn new TTP?

- No
  - People do not keep their systems up to date
  - Some defenses are way behind