Threat intelligence, detection and response @ scale

Jan Schejbal

Branko Spasojevic

Drazen Popovic

Domagoj Klasic

Overview

- Intro
- Attacks
- Prevention
- Monitoring / Visibility
- Response
- Delegating Trust
- Summary

$ whois

- We work in the IT security team at Google
  - Not a presentation about security at Google
  - Many open source Google tools
  - Only public information
  - Examples of breaches from non-Google public reports

Attackers

- Operations
  - Opportunistic
  - Targeted
- Tactics
  - Ransomware
  - Botnets
  - Adware
  - Malware
- Motivation
  - Hacktivism
  - Nation states
  - Professional services

Cyber Threat Intelligence (CTI)

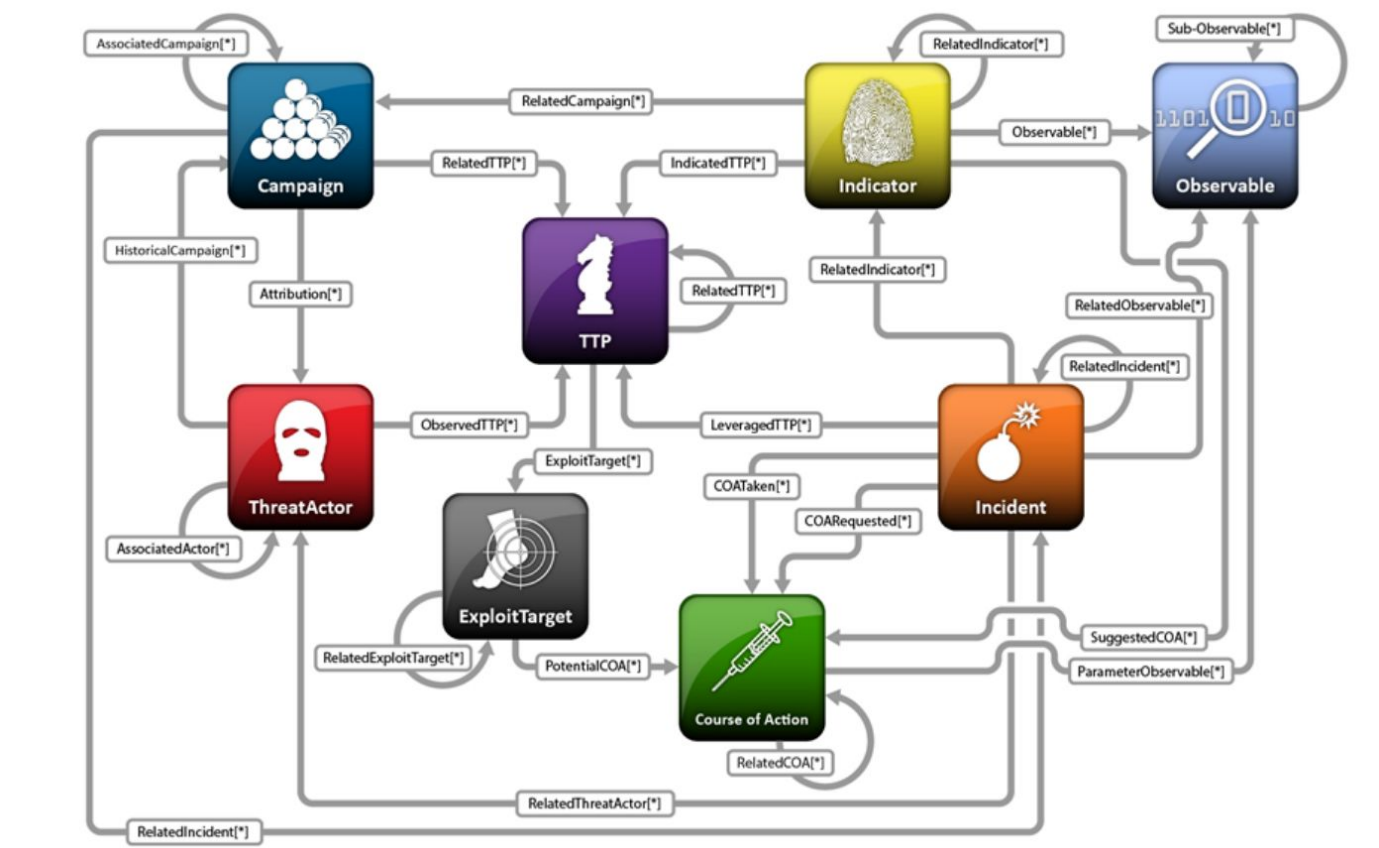
"*Intelligence is often defined as information that has been refined and analyzed to make it actionable.*"

"*Threat intelligence is the analysis of adversaries—their capabilities, motivations, and goals.*"

Mission:

- Understanding and studying the adversary gives us ability to predict their actions and defend more strategically.

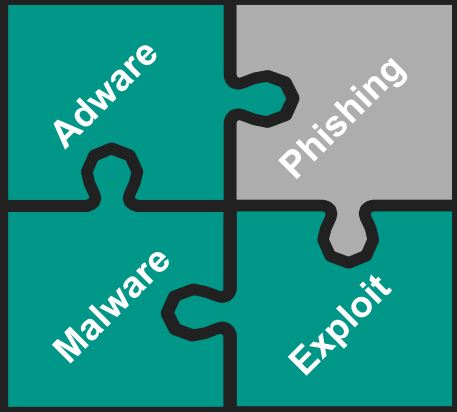
CTI concepts



Attacks

Credential phishing

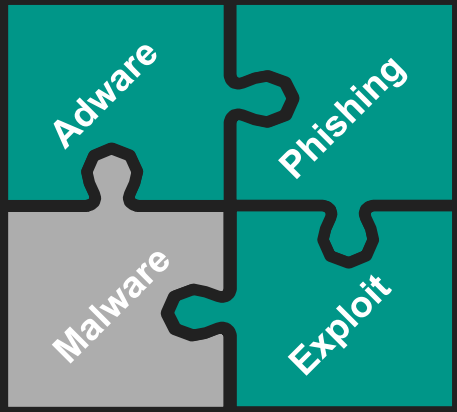
- Targeted or opportunistic
- Many available automated phishing services
- Drive image phishing
- Domain mimicking



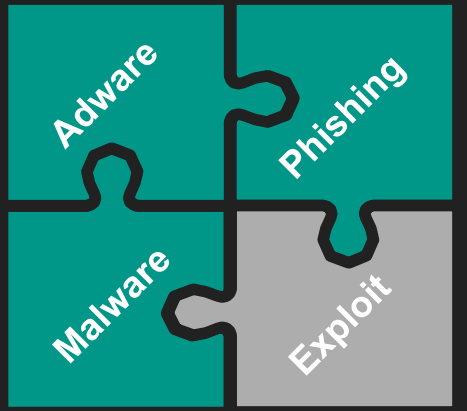
- Good phishing can trick anyone
  - Users fall even for really bad phishing
- Regular 2-factor is phishable!
  - Online banking

Malware

- File extension confusion
- Document embedding
- Infected executable attachment/link
- Infected documents
  - Macros + Social Engineering
  - Exploits
- Infected USB drives
- Supply-chain attacks



Exploit Kits / Waterhole / Vulnerabilities



- Attacker adds exploit kit to hacked website
- Victim visits website
- Exploit kit exploits vulnerability in unpatched software
- APTs may use zero day exploits
  - You *will* get owned
- Also possible: E-mail link to victim
- Scanning infrastructure to find entry point

Photo: Author unknown :(

Prevention

Policy

- Do users have root?
  - Some need it
- How much bureaucracy?
- What is allowed?
  - What is tolerated?
  - What remains unseen?
  - What is technically possible?
    - ⇒ How much adware and keygens do your users run?
- Technical users do weird but legit things
  - Noise problem for detection

Security reviews

- Make security part of your development process
  - Security reviews by security engineers
- Review your vendors and their products
- Hire a 3rd party security company if needed

Inventory management

- Enforce updates
- Set policies
  - Balanced password policy!
- Limit user permissions

Anti-virus

- Catches *many, but not all* untargeted attacks
- May catch *some* targeted attacks
- Downsides:
  - False positives
  - Security holes
  - Slow systems → low user acceptance

Binary whitelisting

- Surprisingly practical
- Stops low-level stuff
  - Good protection even against advanced attacks
  - Can be bypassed e.g. by in-memory malware
- Provides visibility
- Example: Santa + UpVote
  - For Mac
  - Open Source
- Commercial solutions

https://openclipart.org/detail/189356/santa-claus

Certificate authentication

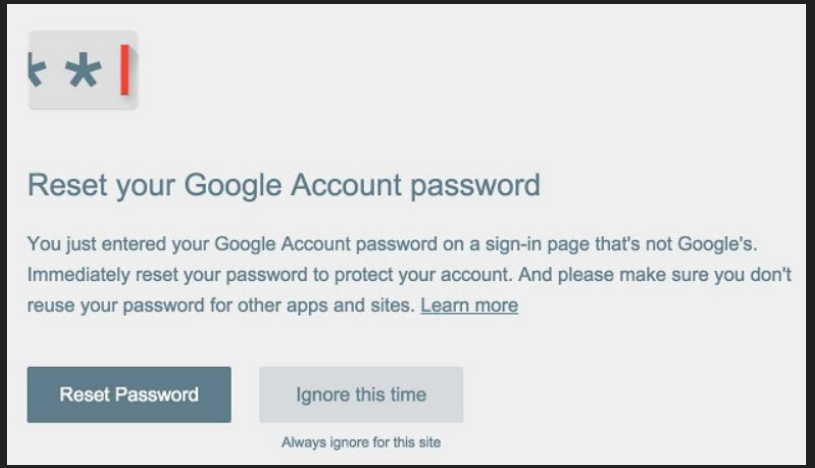
- Network (802.1X)
- Web services
- VPN
- Limits access after successful phishing
- Makes monitoring easier
- Transparent if implemented well

U2F / Security key

- Open standard
- Convenience *and* security
- Phishing resistant
  - User presence check
  - Cryptographic auth

Password Alert

- Detects password reuse and phishing
- Chrome extension
  - Stores truncated hash
  - Only alerts sent to server
  - Detects pages similar to official login page



Blocking of malicious sites / C2

- Firewall
- Proxy
- DNS
- Host-based solutions
- Sinkhole

Challenges

- Laptops outside the corporate network
- Mobile devices
- BYOD
- Unauthorized devices
- Non-standard systems

Monitoring & Visibility

How not to learn about an attack...


```
$ aria2c -S ~/Downloads/hackedteam.torrent
*** BitTorrent File Information ***
Creation Date: Sun, 05 Jul 2015 00:54:51 GMT
Created By: Transmission/2.84 (14307)
Total Length: 387GiB (415,768,052,618)
Name: Hacked Team
```

How **do** you detect an attack?

- How can you observe this?
- Assume e.g.:
  - E-mail with malicious link (malware download),
  - HTTP C2
  - Windows lateral movement
  - SFTP exfil

Log collection

- Host logs - infections, lateral movement
- Additional host based monitoring - infections
- Privacy vs Security
- Network logs
  - DNS - C2, exfil
  - IDS - C2
  - HTTP (Proxy and/or sniffer) - C2
  - HTTPS (Metadata or MitM)
  - Netflow - (C2), exfil
  - Full packet capture - C2, (exfil)

Analysis

- Make logs queryable (SQL) - https://cloud.google.com/bigquery/
- Curio
  - Based on Dremel (BigQuery-like system)
  - Continuous log processing
  - Manually written rules
- Custom signals
- Correlation of signals
- Manual hunting
- Follow up with manual investigations

Investigations

- Involved machines/accounts?
- Possible explanations?
- Does the traffic match what the rule is supposed to detect?
- Other alerts/indicators?

- Lots of manual (log) analysis -> Does not scale
  - Need automated analysis
  - Build analysis expert system

Investigations

- Big data brings challenges and opportunities
  - Prevalence
    - Example with hashes, filenames
  - Entropy
  - Behaviour anomaly detection
    - User, host
  - Investigation similarity recommendation system
  - Predictive badness classification

Response

You've found a confirmed attack.

- (Try not to) panic
- Call in external help?
- Find out what is happening - day(s)
- Get rid of attacker - day(s)
- Find out what happened - weeks to months
- Rebuild (everything?) - days to weeks
- They'll be back…

Photo by SeamsGeeky via Etsy

IT incident response

- There will be chaos.
- There will be rooms full of stacked computers and drives.
- There will be long work days/nights.
- Have a plan
- Keep it organized
  - Incident Command System
  - used by emergency services (firefighters etc.)

Photo: Manuel F. Guerrero, U.S. Marine Corps, via Wikipedia

Conclusion

- Defense in depth
- Keep it practical
- Be prepared
- Get external help where needed
- Using external services *can* be safer

Thank you
for your attention!

Q&A