Identification and detection of cyber-attacks and actors using threat intelligence

Endre Bangerter

Bern University
of Applied Sciences

https://www.bfh.ch/

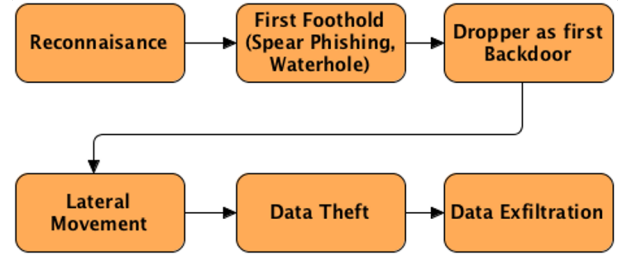
https://threatray.com/

Who are the attackers?

	Hacktivists	Cybercriminals	Mercenaries	State level actors
Objectives	Visibility, impact	Money	Money & objectives of pf sponsor	Information theft, disruption, manipulation, economic power
Targeting	Loose targeting, room for opportunities	Opportunistic, weakly targeted, large scale attacks	Targeted	Targeted, tendency to come back after being caught
Victims	Companies, individuals	Mainly individuals, but also companies	Any	Government, companies, NGOs, individuals (e.g., journalists)
Target platforms	Web servers, common platforms	Common platform (mainly Windows, some MacOS)	Common platforms, mobile	Any, including some exclusive
Capabilities & funding	Low	Medium to advanced	Depends	Whole spectrum, will use whatever is effective
Operating principle	Short term impact	Rather short term, until they get money	Depends	Long term subversion, keep coming back
Attack tools	Free tools	Black and grey market, commercial tools, free tools	Often commercial and free tools	From highly exclusive and advanced to free tools
Defense	Reactive often good enough	Commonplace techniques	Depends	Advanced security to none

Based on Slides by Recuritiy Labs, ACM CCS 2013

Anatomy of cyberattacks



Modus operandi, cyber kill-chain

CC server
(command & control)

Email attachment
Web
USB key
…

Infection

Commands
Data exfiltration
Deployment of new tools

Malware installation

Patient o

lateral movement

Malware installation

Target

Steal information (data exfiltration, credentials, etc.)
Modify information (e.g., e-banking transactions)
Abuse infected system (e.g., spamming)
Attack other systems

Attacks are leaving traces / artifacts

- **On a compromised endpoint**
  - Hashes
  - Filenames of dropped files or email attachments
  - Registry entries
  - Mutexes
  - Process names
  - ...
- **On network infrastructure such a proxies, firewalls, DNS, etc.**
  - IP addresses or domain of CC
  - CC protocol characteristics
  - ....

- Some attackers are erasing evindence willfully For instance, Advanced attackers habe strict rules when to abort operations and to delete their tools

Technical threat intelligence – IOCs

Not all artifacts are useful...

"**Indicator of compromise (IoC) in computer forensics** is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion" (Wikipedia)

IOC Example: an IP address 5.182.210.226 that it is known to be a Trickbot C2 server.

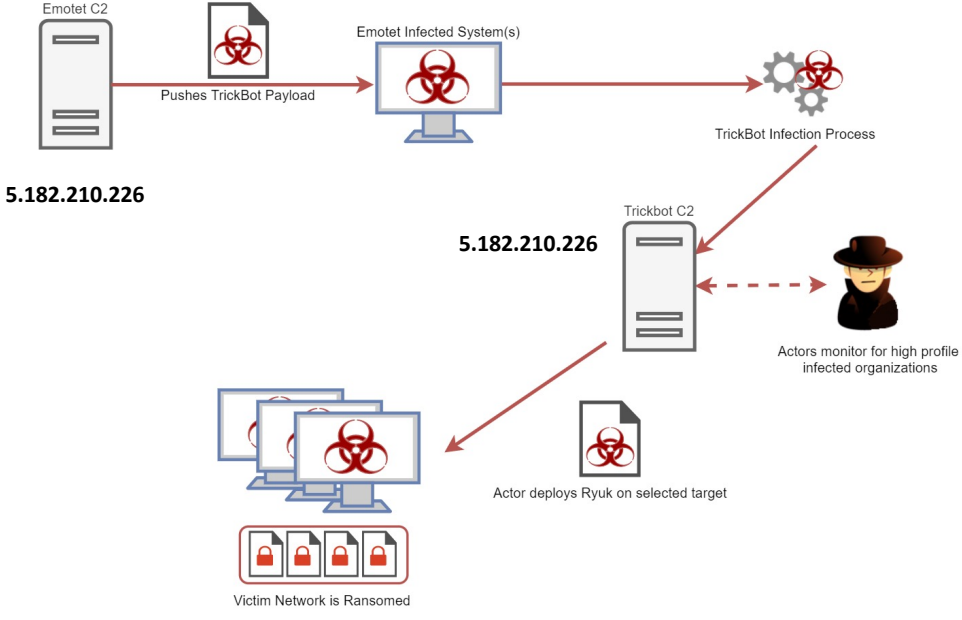
IOCs are also known as technical threat intelligence.

Using IOCs / CTI to identify ransomware attacks

There are multiple ransomware gangs / cybercrime groups, need to understand their TTPs (tactics, techniques, procedures) to reliably identify them.

Need to know that Emotet and Trickbot actors are often collaborating, often resulting in ransomware attacks (this is also threat intelligence)

Example: IOCs of the Emotet and Trickbot C2 can be used to identify ongoing ransomware attack.



Cyber threat intelligence

Threat intelligence is information about attacks & attacker that allows defenders to *improve (speed, depth) their defense and response capabilities.*

Big hype, but quite natural, any amateur athlete will investigate adversaries to improve her odds.

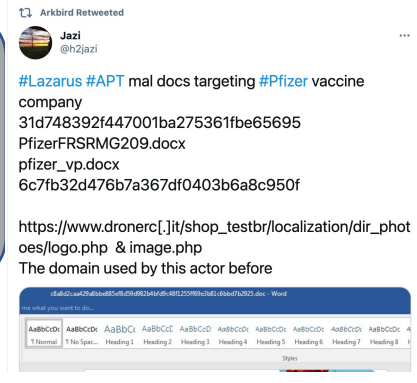
Truly exciting and promising field. There is lots of data, which turn CTI into analytics and ML problems.

CTI can be used in all phases of cyber defense during attacks, after attacks in incident response etc.

Sources of threat intelligence, where to get IOCs?

Information Sharing and Analysis Centers (ISACs)

Open-source intelligence


Arkbird Retweeted

Jazi
@h2jazi

#Lazarus #APT mal docs targeting #Pfizer vaccine company
31d748392f447001ba275361fbe65695
PfizerFRSRMG209.docx
pfizer_vp.docx
6c7fb32d476b7a367df0403b6a8c950f

https://www.dronerc[.]it/shop_testbr/localization/dir_photoes/logo.php & image.php
The domain used by this actor before

Commercial vendors

From within your organization / company

Detection vs. identification

- **Detection** of an attack simply is evil / is not evil type of statement.
- **Identification** is detection plus intelligence on the actor, intent, tooling (as seen in ransomware example).
- **Identification is much more useful than detection**, since it allows to assess risk and choose appropriate reaction.

Attribution

- **Who?** Identification of individuals, groups, organizations, countries behind cyber attacks.

- **Actor / threat groups** are -- like criminal gangs – abstract entities to whom similar attacks can be attributed, but the individuals in the group, their origin is not necessarily known

- **Attribution, why?**
  - For diplomatic measures, retribution, prosecution (deterrence)
  - For intelligence and risk-based defense (improved defense)

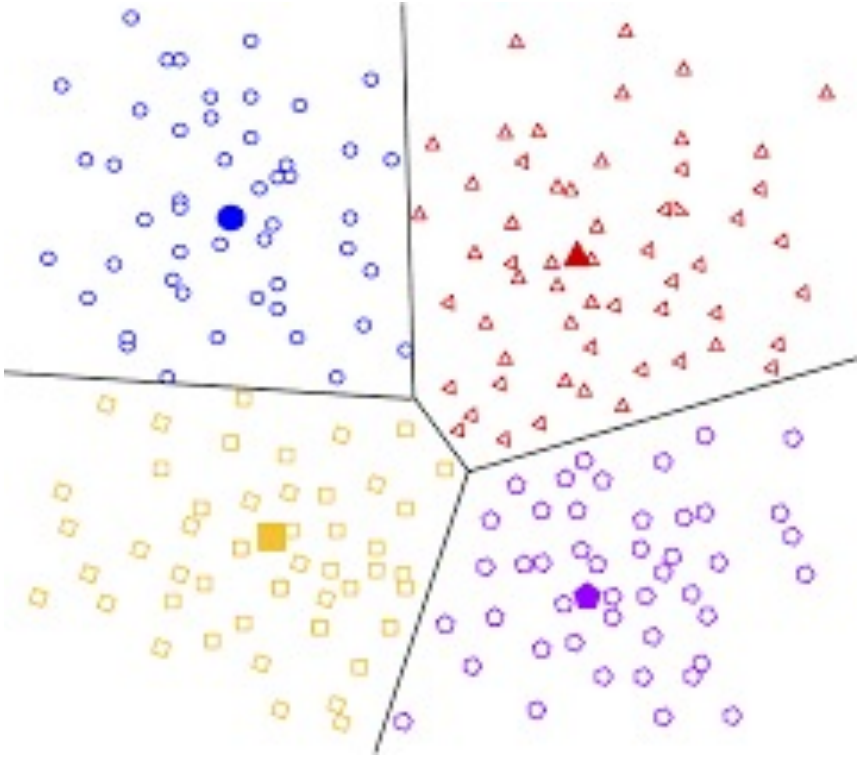
- Unlike in the physical world, where law enforcement is in charge mostly, cyber attacks are in most of the cases handled by enterprise security teams. **Their main interest is improved defense and thus actor groups.**

Actor groups

Bronze Butler, Tick, RedBaldNight, Stalker Panda		2010-Jun 2019	
Buhtrap, Ratopak Spider		2015-Jun 2019	
Cadelle		2011	
Callisto Group	[Unknown]	2013	
Calypso		2016	
Carbanak, Anunak		2013-Aug 2018	●
CardinalLizard		2014	
Careto, The Mask	[Unknown]	2007-Feb 2014	●
Chafer, APT 39		2014-Sep 2020	●
Chimera		2018-Oct 2019	
CIA		1947-Sep 2018	●
↳ Subgroup: Longhorn, The Lamberts		2009	
↳ Subgroup: [Unnamed group USA]		2019-Mar 2020	
Clever Kitten		2013	
Cobalt Group		2016-Oct 2019	●
Cold River	[Unknown]	2019	

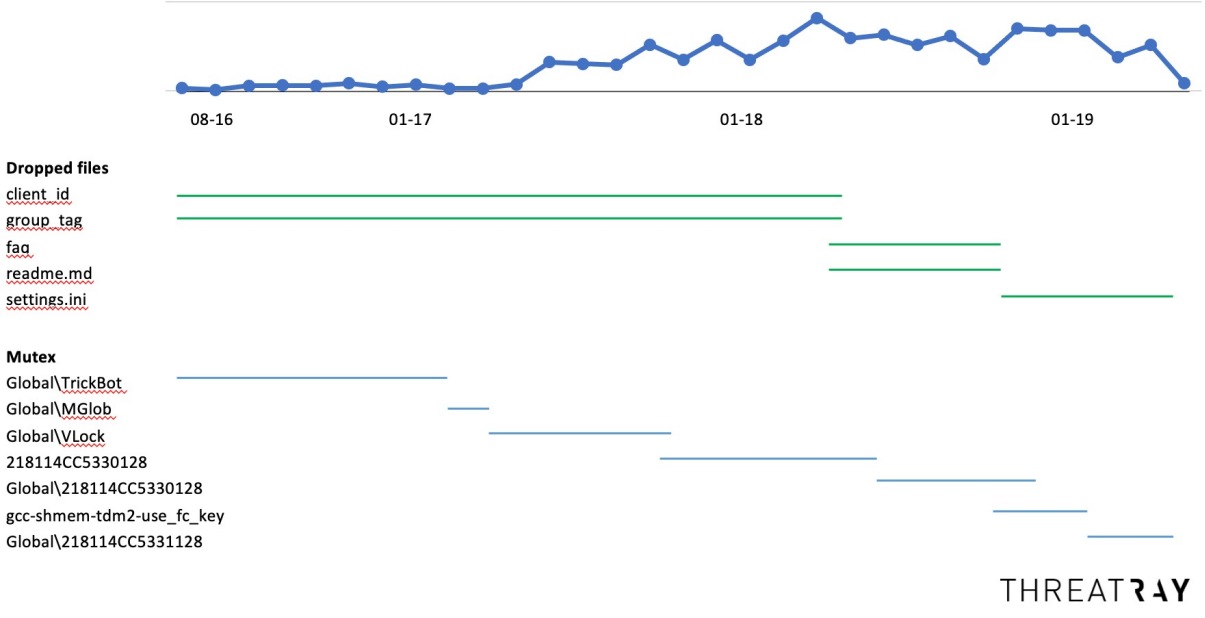
https://apt.thaicert.or.th/cgi-bin/listgroups.cgi

Identification of actor groups



Big data, similarity search and clustering problem

IOCs and their lifetime – intelligence is reactive



IOCs and their value

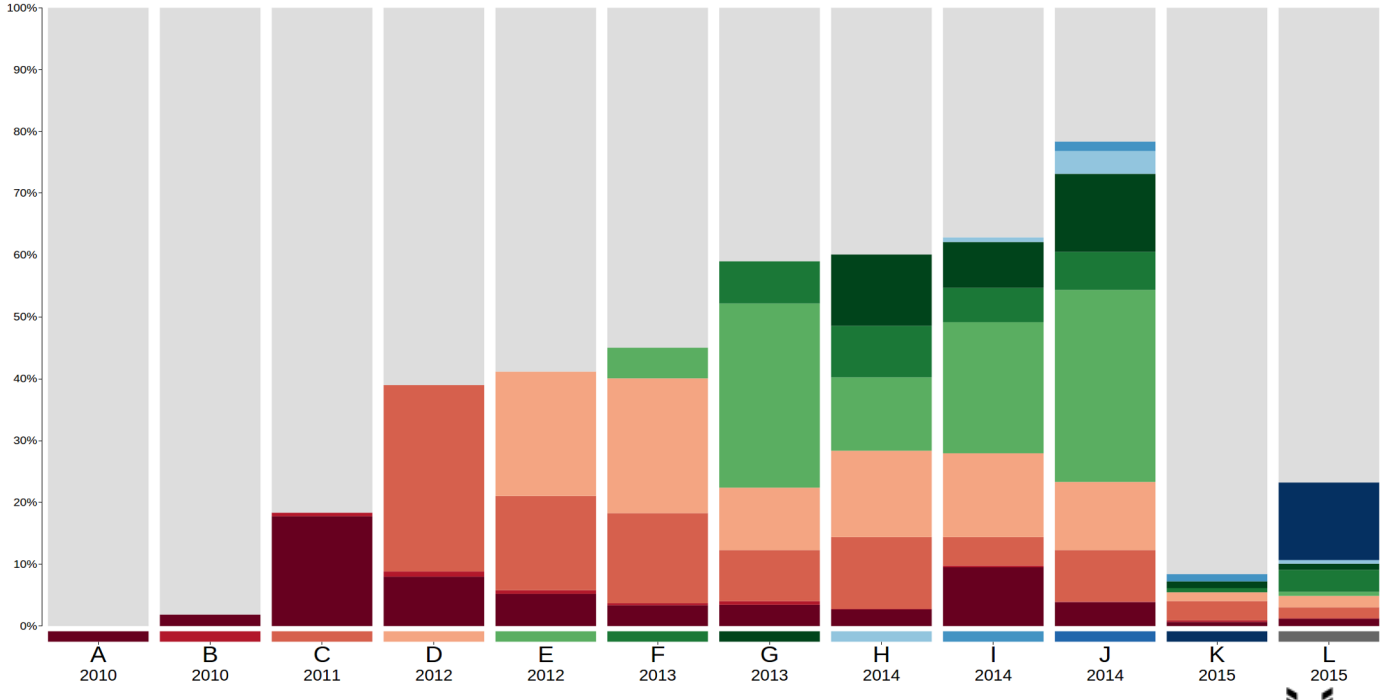
State of the art

THREATRAY

http://detect-respond.blogspot.ch/2013/03/the-pyramid-of-pain.html

TTP = tactics, techniques, procedures

Malware code as long-lived IOC – APT 29 / Dukes



THREATRAY

Conclusions

- Modern cyber defense is largely data and analytics driven
- Cyber threat intelligence is a key component for identifying attacks
- Advanced analytics technologies and products such as Threatray give deep visibility into threat intelligence data resulting in superior malware defense capabilitties.

Get in touch: endre.bangerter@bfh.ch
endre@threatray.com