MISP Threat Sharing

a Decade of Successes and Failures in Threat Information Sharing

Christophe Vandeplas
Alexandre Dulaunoy

TLP:WHITE

Cyber-Defence Campus Conference - EPFL - 2020

There was never a plan. There was just a series of mistakes.

Robert Caro, journalist.

What the hell is the MISP project?

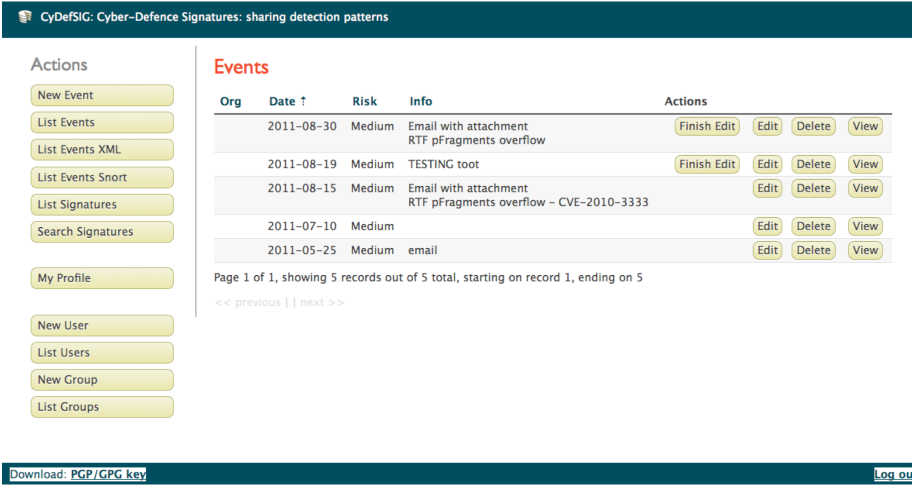
- MISP is a threat information sharing platform - free and open source software.
    - Many export formats which support IDSes (e.g. Suricata, Bro, Snort), SIEMs, Host scanners (e.g. OpenIOC, STIX, STIX2, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ)
- Also a collection of open standards (RFCs), collaborative common vocabularies such as taxonomies, galaxies (e.g. threat-actors or ATT&CK), common object templates and many sub-projects (more than 40 repositories and +300 contributors).
- Assist users in creating, collaborating on, automating, analyzing and sharing threat information
- Is a community-based development, today led by CIRCL.lu

MISP origins & Initial core concepts [1]

- Origins
  - Started as personal project at home around May 2011 as CyDefSIG.
  - To address frustration of re-typing IOCs from reports, scanned docs to export to IDS systems.
  - No initial license.
- Initial core concepts
  - Everything is private, those with access can see everything
  - Only technical data, nothing sensitive or classified
  - No difference between humans and machines

[1] Let's discuss these further over the next 20 minutes

Initial look



Events

Org	Date ↑	Risk	Info	Actions
	2011-08-30	Medium	Email with attachment RTF pFragments overflow	Finish Edit Edit Delete View
	2011-08-19	Medium	TESTING toot	Finish Edit Edit Delete View
	2011-08-15	Medium	Email with attachment RTF pFragments overflow - CVE-2010-3333	Edit Delete View
	2011-07-10	Medium		Edit Delete View
	2011-05-25	Medium	email	Edit Delete View

Page 1 of 1, showing 5 records out of 5 total, starting on record 1, ending on 5

Model of "governance"

- Initially no governance, democracy with development by users.
- No initial license, led to challenge to open source afterwards.
- Dictatorship instead of democracy (especially dishonest democracies)
- Gathering ideas, issues, use-cases, code from the community is key, listen to them but reserve the **right to veto**
  - Prevents malevolent community members from blocking the process/imposing tunnel-visioned ideas
- **Don't wait for the perfect implementation**, start small extend it later
- If the idea doesn't seem suitable for the above, shelf it asap
- Creation of a foundation?

The dangers of dishonest democracies

- Can easily become a pay to play governed body
  - **Having to pay for membership is a massive red flag**
  - Voluntary participation in meetings locks out smaller players that **can't afford full time dedicated people**
- Decision making processes still have to exist, though they often carry dangers
  - Process becoming too cumbersome if true consensus is sought
  - **Decision making restricted to those with more resources** to be constantly present for voting processes
  - Without dictatorship-like veto powers, malicious loud voices with often nefarious agendas have disproportional weight

Our initial failures with democracies

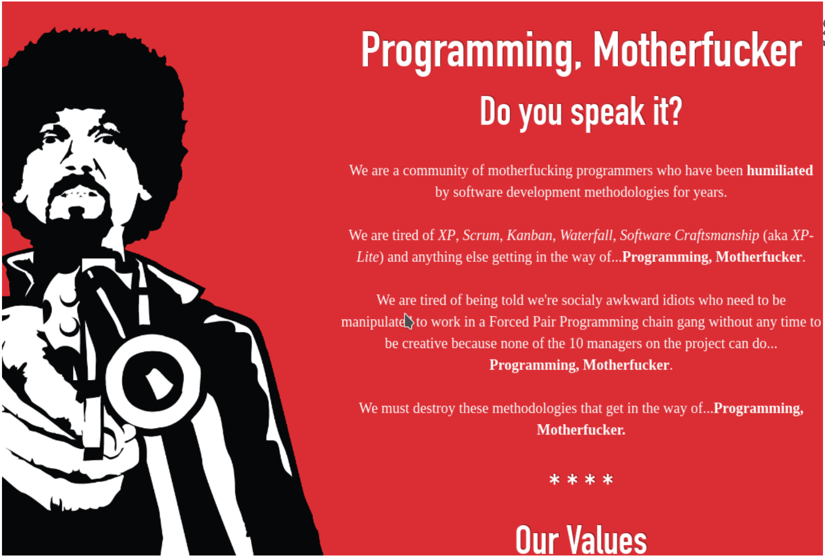
- **Caving to political pressure**
  - Several organisations fighting for MISP to not include context early on (2012-2013) as it wasn't their use-case
  - Took us until 2014-2015 to recover from the set-back
  - Fun fact: Since then the users mostly resistant to the inclusion of these features are heavy users of said features
- **Accepting bad ideas "as is" from organisations to be more inclusive**
  - Even insignificant modifications will hurt the integrity and conventions of your tooling / format
  - The impact might not reveal itself until years down the road
- Dictatorship for the common good.

Why standardise at all?

- More and more requests from **other tools/vendors to integrate with MISP**
  - Complaints about having to go through a jungle of PHP or Python code to figure out how to do it
- Validation from 3rd parties on the format and overall design
- Describing the scope of the native MISP formats
- Help other projects use a sane and broad exchange - and most importantly, adaptable set of standards

Development process based on failures

- All ideas need **real-world and practical validation**
- Be willing to throw away features that ”sure seemed like a good idea at the time”
- Fail as early as possible (and be proud of your failures)
- Failures can often be used to pinpoint better alternatives
- Format follows the implementation (**code is law**)



Programming, Motherfucker

Do you speak it?

We are a community of motherfucking programmers who have been **humiliated** by software development methodologies for years.

We are tired of *XP*, *Scrum*, *Kanban*, *Waterfall*, *Software Craftsmanship* (aka *XP-Lite*) and anything else getting in the way of...**Programming, Motherfucker**.

We are tired of being told we're socialy awkward idiots who need to be manipulated to work in a Forced Pair Programming chain gang without any time to be creative because none of the 10 managers on the project can do... **Programming, Motherfucker**.

We must destroy these methodologies that get in the way of...**Programming, Motherfucker.**

* * * *

Our Values

[2]

[2] https://github.com/adulau/pmf/blob/master/raw.md.txt Programming Methodology Framework aka PMF

Staying with theoretical models for too long...

- The same mistakes will be made anyway
- **Piling mistakes on shaky foundations** will be more difficult to undo later
  - Technical reasons (inheritance of the *crap*)
  - Sunk cost fallacy *mistakes seen as failure with any suggestion to rectify it being taboo*
- We generally had two main design goals when it comes to the format:
  - **Design the format, in a way, to be as simple as possible** to be able to map whatever information we want to convey
  - Every field, every setting, every relation that doesn't have an immediately useful use is a **failure**
  - Enhance the format when it's needed instead of planning ahead - **code is law**

Piling mistakes on shaky foundations (another view)

Scoping the format

- One of the most challenging tasks is having a **clear scope** and a unified vision on what problems we intend to solve
- This can be fluid over time, but the format should stay coherent at any specific point in time with the other components
- Our guiding principle as **a sharing format was to keep complexity levels at a minimum but cover a large spectrum of use-cases**
- We are firm believers that our multi-purpose nature will hinder us at ever being as good at specialised tasks as the relevant specialised formats in the field (Suricata, Bro, Snort, Yara, Sigma or Gene)
- Don't be oblivious to other developments. Being a "follower" and aligning yourself is not a sign of weakness but rather one of being co-operative.

Designing a standard with sharing in mind (an organic approach)

- The original sharing aspects of the MISP format (in 2011) were quite limited (private flag)
  - If I want to keep it within my organisation, simply set the flag
  - If not set any organisation can see it on the MISP instance
- Utterly simplistic, only worked on communities using a hosted MISP
- **Not known practical cyber security sharing models** known at that time

Designing a standard with sharing in mind (an organic approach)

- The second step of sharing (in late 2012) based on feedback from the previous iteration
- Needed to be extended once communities started self-hosting MISP **to be able to control the distance of the data-flow**
- Distribution levels
  - Organisation only (private)
  - Community
  - Connected community
  - All

Designing a standard with sharing in mind (going all out)

- Still not covering all use-cases, certain types of users wanting more granularity
- **Extending the current sharing models with a mixed sharing model** via sharing groups (in 2015)
    - Sharing groups (distribution lists)
    - Complex system for persistent and special ad-hoc use-cases (e.g. short-term information exchange)
- Next step: Multiple sharing groups/nested sharing groups

Privacy aware sharing

- Multiple initiatives to improve privacy-aware sharing
- Usually only compatible for a subset of use-cases, such as network detection. (not response, nor intel)
- 2012/2013 - Bloom filters (A Dulaunoy)[3]
  - Non-reversible hash sets for lookup - SIEM, IDS, loganalysis
  - Bruteforce of IPv4 very easy
- 2016/2017 - Private Sharing of IOCs and Sightings (UTwente)[4] [5]
  - Use crypto and salt
- 2020 - Distributed Privacy-Preserving Threat-Intelligence Platforms (Armasuisse, EPFL)

[3] https://github.com/MISP/misp-bloomfilter

[4] https://research.utwente.nl/en/publications/private-sharing-of-iocs-and-sightings

[5] https://github.com/MISP/misp-privacy-aware-exchange

A little bit about human creativity...

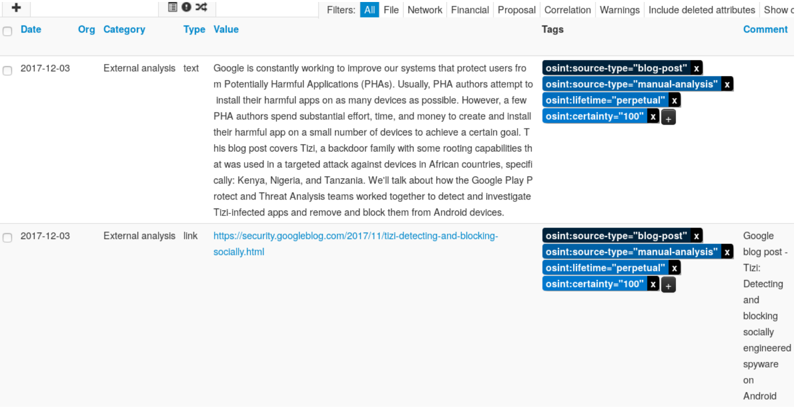
The great failure of free-text tagging

- **Humans can be very creative** especially when they have a playground
- Free-text tagging was a nifty feature in early version of MISP but we underestimated the creativity of the human mind
- "TLP AMBER", "TLPAMBER", "TLP-amber", "TLP:AMBER", "TLP=AMBER" and "TLP/AMBER", "tlp:amber"
- Classifications must be globally used to be efficient. In 2015, we designed a complete taxonomy system to initially support TLP
- As of Today, we have **more than 120 taxonomies**[6] (from markings, classification taxonomies or even crowdsourced support to allow collaborative analysis)

[6] https://www.misp-project.org/taxonomies.html

Taxonomy

- It solved the "creativity issue" but we were only allowing tagging at event level. Attribute level tagging was then introduced in 2016.



+

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show c

□	Date	Org	Category	Type	Value	Tags	Comment
□	2017-12-03		External analysis	text	Google is constantly working to improve our systems that protect users from Potentially Harmful Applications (PHAs). Usually, PHA authors attempt to install their harmful apps on as many devices as possible. However, a few PHA authors spend substantial effort, time, and money to create and install their harmful app on a small number of devices to achieve a certain goal. This blog post covers Tizi, a backdoor family with some rooting capabilities that was used in a targeted attack against devices in African countries, specifically: Kenya, Nigeria, and Tanzania. We'll talk about how the Google Play Protect and Threat Analysis teams worked together to detect and investigate Tizi-infected apps and remove and block them from Android devices.	osint:source-type="blog-post" x osint:source-type="manual-analysis" x osint:lifetime="perpetual" x osint:certainty="100" x +	
□	2017-12-03		External analysis	link	https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html	osint:source-type="blog-post" x osint:source-type="manual-analysis" x osint:lifetime="perpetual" x osint:certainty="100" x +	Google blog post - Tizi: Detecting and blocking socially engineered spyware on Android

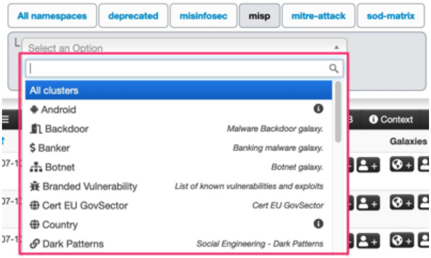
Ongoing effort to standardise MISP

- IETF draft document for the MISP core format
- IETF draft documents for the MISP supporting formats
  - Ensuring a separation between the core format and the **extensible and reusable** formats such as taxonomies, galaxies, warninglists and objects.
- Available at `https://www.misp-standard.org/`
- The standard documents are written from the software implementation in MISP (in other words, we don't like committee meeting).

MISP STANDARD
collaborative intelligence

A list of the currently described MISP formats

- MISP core format:
  - Events, Attributes, Objects, Tags, Sharing Groups, Proposals...
  - Allows synchronisation between MISP instances, and other products
- MISP JSON formats:
  - MISP taxonomies - 120+
  - MISP galaxies - about 25 with 6500 elements
  - MISP warninglists - about 50
  - MISP object-templates - about 250 types



All namespaces | deprecated | misinfosec | misp | mitre-attack | sod-matrix

Select an Option

All clusters

Android

Backdoor — Malware Backdoor galaxy.

Banker — Banking malware galaxy.

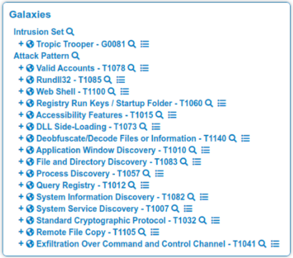
Botnet — Botnet galaxy.

Branded Vulnerability — List of known vulnerabilities and exploits

Cert EU GovSector — Cert EU GovSector

Country

Dark Patterns — Social Engineering - Dark Patterns



Galaxies

Intrusion Set
- Tropic Trooper - G0081

Attack Pattern
- Valid Accounts - T1078
- Rundll32 - T1085
- Web Shell - T1100
- Registry Run Keys / Startup Folder - T1060
- Accessibility Features - T1015
- DLL Side-Loading - T1073
- Deobfuscate/Decode Files or Information - T1140
- Application Window Discovery - T1010
- File and Directory Discovery - T1083
- Process Discovery - T1057
- Query Registry - T1012
- System Information Discovery - T1082
- System Service Discovery - T1007
- Standard Cryptographic Protocol - T1032
- Remote File Copy - T1105
- Exfiltration Over Command and Control Channel - T1041

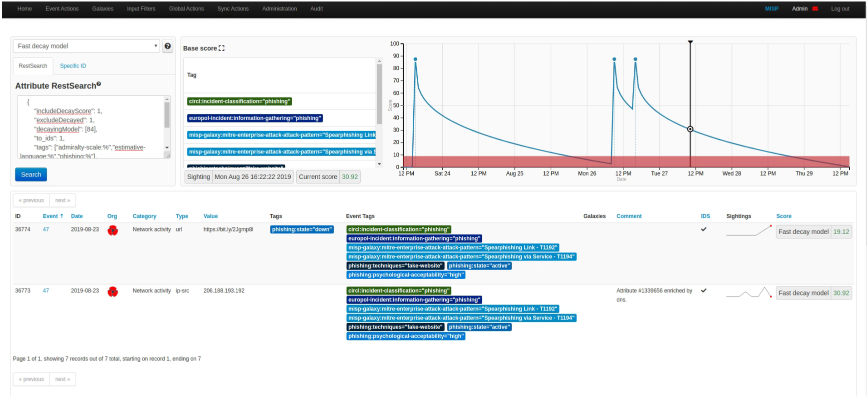
ATT&CK®

Theory and practice sometimes clash. And when that happens, theory loses. Every single time.

Linus Torvalds

More data = more challenges - IOC Decay model

- Much more data shared within multiple communities
- Quality VS Quantity
- Filters needed for export



Attribute RestSearch

```
{
    "includeDecayScore": 1,
    "excludeDecayed": 1,
    "decayingModel": [84],
    "to_ids": 1,
    "tags": ["admiralty-scale:%","estimative-
language:%","phishing:%"],
```

Tag
circl:incident-classification="phishing"
europol-incident:information-gathering="phishing"
misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Link
misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing via S

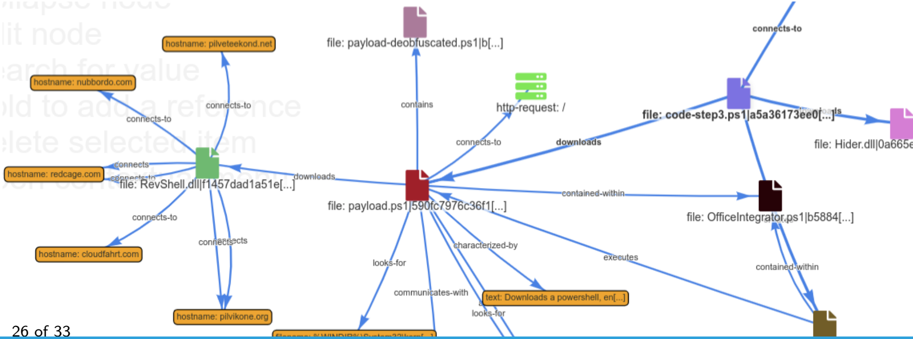
Sighting Mon Aug 26 16:22:22 2019 Current score 30.92

ID	Event ↑	Date	Org	Category	Type	Value	Tags	Event Tags	Galaxies	Comment	IDS	Sightings	Score
36774	47	2019-08-23		Network activity	url	https://bit.ly/2Jgmp8l	phishing:state="down"	circl:incident-classification="phishing" europol-incident:information-gathering="phishing" misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Link - T1192" misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing via Service - T1194" phishing:techniques="fake-website" phishing:state="active" phishing:psychological-acceptability="high"			✓		Fast decay model 19.12
36773	47	2019-08-23		Network activity	ip-src	206.188.193.192		circl:incident-classification="phishing" europol-incident:information-gathering="phishing" misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing Link - T1192" misp-galaxy:mitre-enterprise-attack-attack-pattern="Spearphishing via Service - T1194" phishing:techniques="fake-website" phishing:state="active" phishing:psychological-acceptability="high"		Attribute #1339656 enriched by dns.	✓		Fast decay model 30.92

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

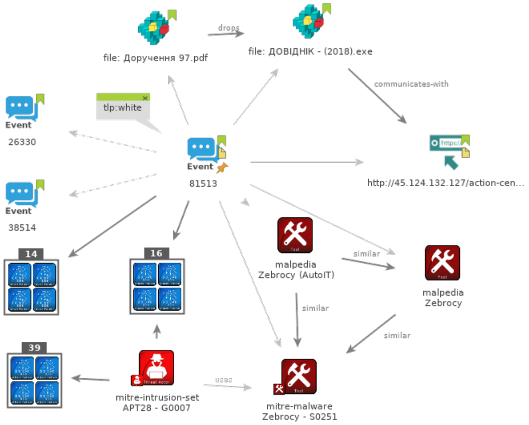
More data = more opportunities - relation graph

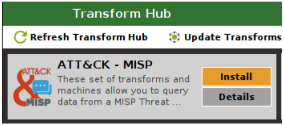
- Wish for better understanding story around the different attributes/objects:
    - email contains attachment
    - document contains scripts
    - scripts drop DLL
    - executable connects-to CnC
- Object relationships with dynamic graph



Analysts always want more...

- Open model of MISP allows integration with any tool.
- MISP-Maltego is one example of many integrations
- https://github.com/MISP/MISP-maltego



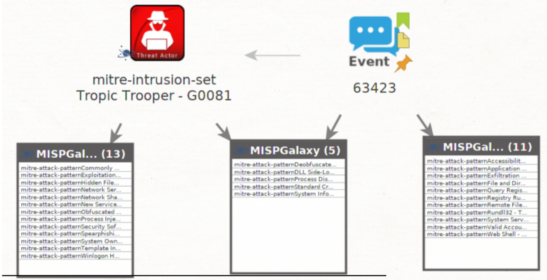


ATT&CK - MISP

These set of transforms and machines allow you to query data from a MISP Threat ...

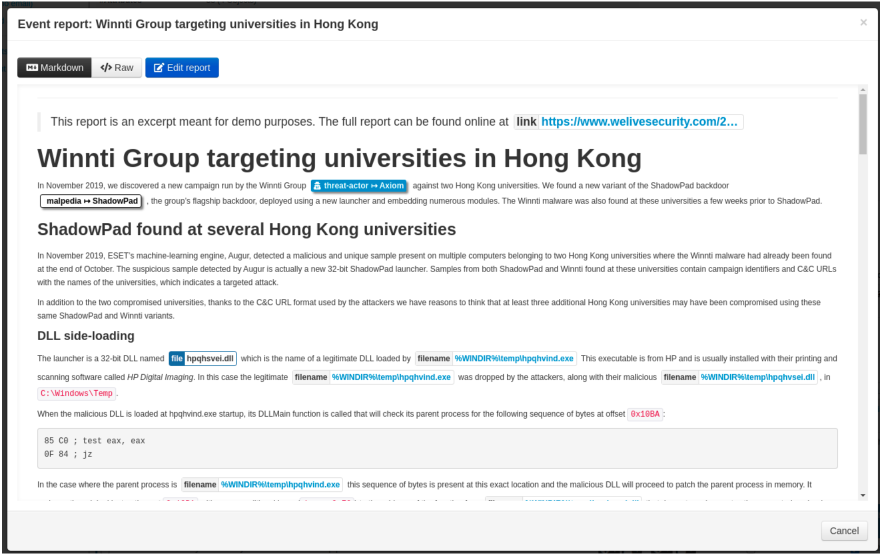
Analysts also have their challenges...

- Having access to data is one of the challenges.
- Understanding the limitations of data is tougher. [7]
    - Meaning of words
    - Consistency of encoding - we love automation
    - Completeness - of data, attack AND attacker knowledge
    - Correctness - be careful with automation


Threat Actor
mitre-intrusion-set
Tropic Trooper - G0081
Event
63423
MISPGal... (13)
mitre-attack-patternCommonly ...
mitre-attack-patternExploitation...
mitre-attack-patternHidden File...
mitre-attack-patternNetwork Ser...
mitre-attack-patternNetwork Sha...
mitre-attack-patternNew Service...
mitre-attack-patternObfuscated ...
mitre-attack-patternProcess Inje...
mitre-attack-patternSecurity Sof...
mitre-attack-patternSpearphishi...
mitre-attack-patternSystem Own...
mitre-attack-patternTemplate In...
mitre-attack-patternWinlogon H...
MISPGalaxy (5)
mitre-attack-patternDeobfuscate...
mitre-attack-patternDLL Side-Lo...
mitre-attack-patternProcess Dis...
mitre-attack-patternStandard Cr...
mitre-attack-patternSystem Info...
MISPGal... (11)
mitre-attack-patternAccessibilit...
mitre-attack-patternApplication ...
mitre-attack-patternExfiltration ...
mitre-attack-patternFile and Dir...
mitre-attack-patternQuery Regis...
mitre-attack-patternRegistry Ru...
mitre-attack-patternRemote File...
mitre-attack-patternRundll32 - T...
mitre-attack-patternSystem Serv...
mitre-attack-patternValid Accou...
mitre-attack-patternWeb Shell - ...

[7] https://www.misp-project.org/2019/10/27/visualising_common_patterns_attack.html

Analysts always want more... (cont.)



Event report: Winnti Group targeting universities in Hong Kong
×
Markdown
Raw
Edit report
Cancel

> This report is an excerpt meant for demo purposes. The full report can be found online at link https://www.welivesecurity.com/2...

Winnti Group targeting universities in Hong Kong

In November 2019, we discovered a new campaign run by the Winnti Group threat-actor ↦ Axiom against two Hong Kong universities. We found a new variant of the ShadowPad backdoor malpedia ↦ ShadowPad , the group's flagship backdoor, deployed using a new launcher and embedding numerous modules. The Winnti malware was also found at these universities a few weeks prior to ShadowPad.

ShadowPad found at several Hong Kong universities

In November 2019, ESET's machine-learning engine, Augur, detected a malicious and unique sample present on multiple computers belonging to two Hong Kong universities where the Winnti malware had already been found at the end of October. The suspicious sample detected by Augur is actually a new 32-bit ShadowPad launcher. Samples from both ShadowPad and Winnti found at these universities contain campaign identifiers and C&C URLs with the names of the universities, which indicates a targeted attack.

In addition to the two compromised universities, thanks to the C&C URL format used by the attackers we have reasons to think that at least three additional Hong Kong universities may have been compromised using these same ShadowPad and Winnti variants.

DLL side-loading

The launcher is a 32-bit DLL named file hpqhsvei.dll which is the name of a legitimate DLL loaded by filename %WINDIR%\temp\hpqhvind.exe This executable is from HP and is usually installed with their printing and scanning software called *HP Digital Imaging*. In this case the legitimate filename %WINDIR%\temp\hpqhvind.exe was dropped by the attackers, along with their malicious filename %WINDIR%\temp\hpqhvsei.dll , in `C:\Windows\Temp`.

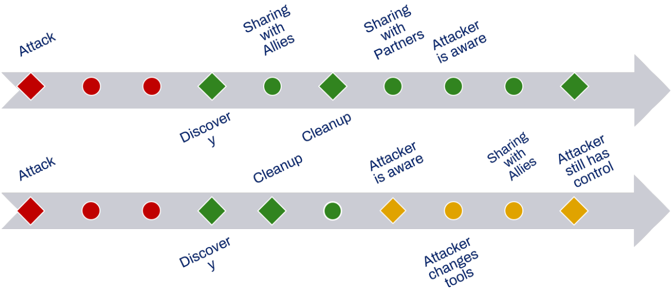
When the malicious DLL is loaded at hpqhvind.exe startup, its DLLMain function is called that will check its parent process for the following sequence of bytes at offset `0x10BA`:

```
85 C0 ; test eax, eax
0F 84 ; jz
```

In the case where the parent process is filename %WINDIR%\temp\hpqhvind.exe this sequence of bytes is present at this exact location and the malicious DLL will proceed to patch the parent process in memory. It

Creating sharing communities

- Secrecy, classification & distrust - Prisoner's dilemma
- Leechers vs seeders vs observers
- *I know what I need, and I am right.*[8]
- Use-cases & objectives / producer & consumer - can be conflicting
- Who: # teams in one org / power-games of information control
- Speed: Timeliness of sharing is crucial



[8] We believe we do, but in reality we don't.

Initial - not so good - concepts

- Everything is private, no ACL / everyone can see everything
  - 1 year later: distribution - my org only, this community, connected community, all
  - 3 years later: sharing groups
- Only technical data, nothing sensitive or classified
  - Massive value of extra metadata - tags, taxonomies, galaxies, relationships
  - Need for victim-related info
  - Some orgs now sync MISP over airgaps
- No difference between humans and machines
  - Same functionality over WebUI and REST API
  - XML format became JSON
  - Exports in many many many formats, automation, and more...

Lessons identified

- Frustrations are good, when used as stimulator for improvement.
- Always first put a license on code before using.
- By giving you will receive - allow other to continue what you've started.
- Try and do - PMF - KISS - no months of over-engineering.
- Interoperability and open formats is a must!
- You do not know what you, nor others need.
- Failures can often be used to pinpoint better alternatives
- Getting the right data to the right people is difficult.
- There is still a long road ahead...

Q&A

The art of information sharing is to share more, smarter and faster with your friends and allies than your adversaries would like to.

Christophe Vandeplas

- info@misp-project.org
- https://www.misp-project.org/
- https://github.com/MISP/
- https://twitter.com/MISPProject