Maltego Handbook for Cyber Threat Intelligence

handbook

MALTEGO

Table of Contents

About Cyber Threat Intelligence

1.

Growing Demands for Cyber Threat Intelligence

Cyber threats and attack methods are evolving in complexity, with businesses facing threats from attackers driven by various motives. These threats encompass everything from ransomware and phishing campaigns to insider threats, all of which could result in data breaches. Companies can no longer only work on a traditional and reactive basis but utilize insights from past incidents and current alerts to swiftly identify and address potential future threats. In this context, Maltego emerges as a critical platform for helping companies deal with the complexities of streamlining the entire lifecycle of threat intelligence, from collection and processing to analysis as part of their advanced security measures. Moreover, adopting these advanced security measures has become essential for businesses to protect their digital assets.

They are turning to **incident observations** and **cyber threat intelligence (CTI)** to enhance their understanding of security events, allowing them to anticipate and proactively defend against future threats. CTI, in particular, plays a critical role in refining digital forensics and enhancing the incident response process. This handbook will delve into the intricacies of CTI, presenting its applications along with a detailed playbook for leveraging Maltego in CTI use cases. These use cases are designed to provide ready workflows for collecting threat intelligence, tracking malware infrastructure, assessing vulnerability and attack surface, profiling threat actors, and analyzing attacks and TTPs.

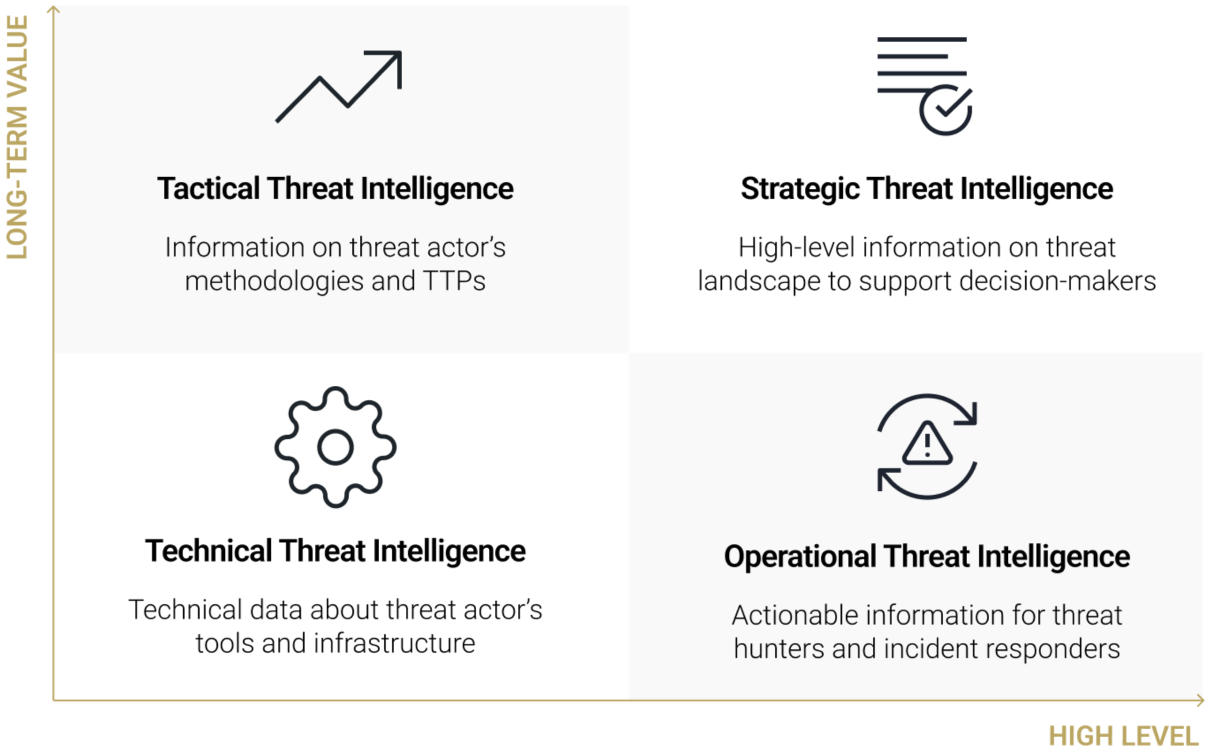
INVESTIGATOR NOTE

Although CTI primarily concentrates on the digital realm, it's imperative to also consider the geopolitical dynamics of the real world to accurately interpret an attack or threat. Incorporating these parameters is crucial for providing decision-makers with a comprehensive understanding that aids in reducing risk.

Levels of Cyber Threat Intelligence

Cyber threat intelligence can be categorized into four levels:

- **Strategic Threat Intelligence:** It is high-level information including real-life factors such as economic conditions, political climates, the business impact of risks, and emerging trends in attack methodologies. Sources such as whitepapers, policy documents, and publications contribute to this knowledge base, aiming to enlighten non-technical stakeholders such as high-level executives and management.
- **Operational Threat Intelligence:** It is high-level but actionable information including the timing, objectives, and specific methods utilized by threat actors. It equips cybersecurity teams with the foresight needed to predict attacks and to understand the schematics behind threat actors' operations, particularly useful for threat hunters and incident responders. It covers specifics on attack vectors, like domains employed to control comprised systems, and information from external sources like the dark web, all to facilitate the assembly of TTPs.
- **Tactical Threat Intelligence:** It is information



Tactical Threat Intelligence

Information on threat actor's methodologies and TTPs

Strategic Threat Intelligence

High-level information on threat landscape to support decision-makers

Technical Threat Intelligence

Technical data about threat actor's tools and infrastructure

Operational Threat Intelligence

Actionable information for threat hunters and incident responders

that outlines the TTPs employed by threat actors, utilizing frameworks like Mitre ATT&CK to track internal threat information feeds such as network traffic data. It provides a technical context that allows IT admins and SOC managers to detect system breaches or familiarize themselves with prevalent attack strategies. Furthermore, this information supports the improvement of security measures and the protection of businesses.

- **Technical Threat Intelligence:** It is information that includes specific technical indicators or evidence of threat actor's tools and infrastructures, aimed at SOC staff to block malicious activities. Such information can include identified malicious IP addresses, phishing email subject lines or content, rogue URLs, or samples of malware and exploits. For example, if adversaries leverage corporate emails as an entry point into an organization (as identified through tactical threat intelligence), the specific email subject lines used would be classified as technical threat intelligence.

With this categorization in place, each operational team and individual can access the most relevant intelligence to their role. The goal of categorizing threat intelligence is to facilitate the identification and mitigation of risks, potentially even leading to the attribution of actors, given their diverse motivations and targets. For example, a bank may request its threat intelligence team to create reports on well-known, persistent cybercriminal groups in the industry to avoid becoming their target.

Below are the typical motivations and targets associated with different types of cyber threat actors.

1. Nation States: Engage in cyber espionage and sabotage against rival countries to gather intelligence and weaken their capabilities.

- Motivations: Intelligence gathering for economic and geopolitical advantage.
- Targets: Other nations' networks, activities, and critical infrastructure.

2. Criminal Groups: Employ cyber threats to illicitly acquire financial gains and sensitive information through various online scams and malware.

- Motivations: Financial profit and identity theft.
- Targets: Financial institutions, individuals, and government agencies.

CYBER THREAT ACTOR	MOTIVATION	TARGETS
NATION STATES	Economic or military	Other countries, their activities, and infrastructure
CRIMINAL GROUPS	Profit	Financial institutions, individuals, and government agencies
TERRORIST GROUPS	Support for their cause	Government agencies, critical infrastructure, & media outlets
HACKTIVISTS	Publicity and social justice	Government agencies and corporations
THRILL-SEEKERS	Satisfaction	Anything and Everything
INSIDER THREATS	Discontent, revenge, and financial gain	Digital assets and/networks within organization

3. Terrorist Groups: Utilize cyber tactics to gather intelligence, disrupt state functions, or instill fear within populations or specific groups.

- Motivations: Ideological propaganda and disruption of state operations.
- Targets: Government agencies(websites), critical infrastructure, and media outlets.

4. Hacktivists: Conduct cyberattacks such as unauthorized data breaches and online vandalism to highlight or protest against social, environmental, or political issues.

- Motivations: Political change, social justice, environmental protection.
- Targets: Government agencies and corporations.

5. Thrill-seekers: Engage in hacking for excitement and challenge, often without a specific financial or ideological motive.

- Motivations: Personal amusement and demonstration of skill.
- Targets: Anything that is random or opportunistic, ranging from websites to personal accounts.

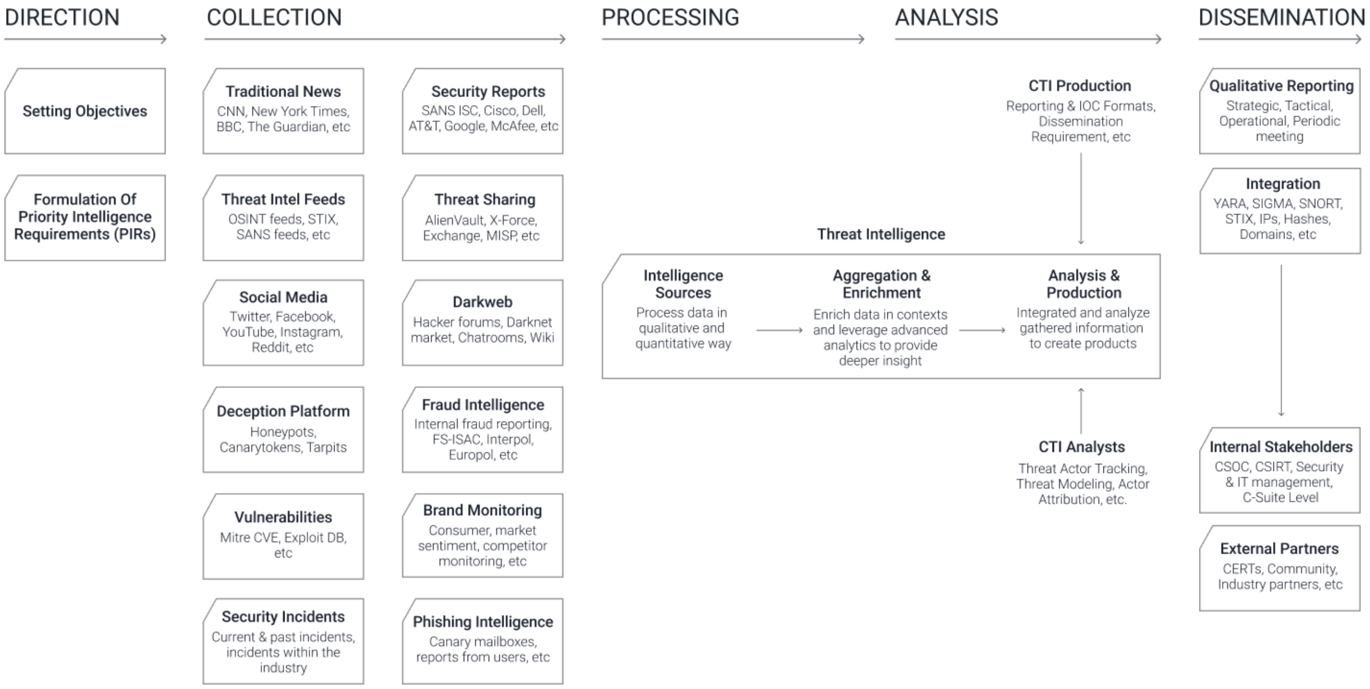
6. Insider Threats: Pose a risk to organizations from within, either maliciously intending to harm the organization or inadvertently causing security breaches.

- Motivations: Dissatisfaction, revenge, and financial gain
- Targets: Employer's data and systems and sensitive internal information.

Lifecycle of Cyber Threat Intelligence

Numerous approaches to cyber threat intelligence exist, tailored to the specific requirements and priorities of the teams and different cases. However, the most widely adopted lifecycle model of cyber threat intelligence is one that has been developed through decades of intelligence efforts by government and military organizations like the CIA and the NSA. This model outlines the process of developing raw information into finished intelligence in six essential phases: **Direction, Collection, Processing, Analysis, Dissemination, and Feedback.**

CYBER THREAT INTELLIGENCE LIFECYCLE OVERVIEW



DIRECTION

Setting Objectives

Formulation Of Priority Intelligence Requirements (PIRs)

COLLECTION

Traditional News
CNN, New York Times, BBC, The Guardian, etc

Security Reports
SANS ISC, Cisco, Dell, AT&T, Google, McAfee, etc

Threat Intel Feeds
OSINT feeds, STIX, SANS feeds, etc

Threat Sharing
AlienVault, X-Force, Exchange, MISP, etc

Social Media
Twitter, Facebook, YouTube, Instagram, Reddit, etc

Darkweb
Hacker forums, Darknet market, Chatrooms, Wiki

Deception Platform
Honeypots, Canarytokens, Tarpits

Fraud Intelligence
Internal fraud reporting, FS-ISAC, Interpol, Europol, etc

Vulnerabilities
Mitre CVE, Exploit DB, etc

Brand Monitoring
Consumer, market sentiment, competitor monitoring, etc

Security Incidents
Current & past incidents, incidents within the industry

Phishing Intelligence
Canary mailboxes, reports from users, etc

PROCESSING

ANALYSIS

CTI Production
Reporting & IOC Formats, Dissemination Requirement, etc

Threat Intelligence

Intelligence Sources
Process data in qualitative and quantitative way

Aggregation & Enrichment
Enrich data in contexts and leverage advanced analytics to provide deeper insight

Analysis & Production
Integrated and analyze gathered information to create products

CTI Analysts
Threat Actor Tracking, Threat Modeling, Actor Attribution, etc.

DISSEMINATION

Qualitative Reporting
Strategic, Tactical, Operational, Periodic meeting

Integration
YARA, SIGMA, SNORT, STIX, IPs, Hashes, Domains, etc

Internal Stakeholders
CSOC, CSIRT, Security & IT management, C-Suite Level

External Partners
CERTs, Community, Industry partners, etc

Methodology of Cyber Threat Intelligence

2.

The MITRE ATT&CK Framework for Cyber Threat Intelligence

Regardless of the maturity level of cybersecurity teams, the organization who want to move toward a threat-informed defense can utilize MITRE ATT&CK framework in different levels:

- **Level 1:** Designed for teams with limited resources or those in the initial phases of development
- **Level 2:** Suited for the mid-level teams starting to mature
- **Level 3:** Tailored for more sophisticated teams with advanced cybersecurity measures and resources.

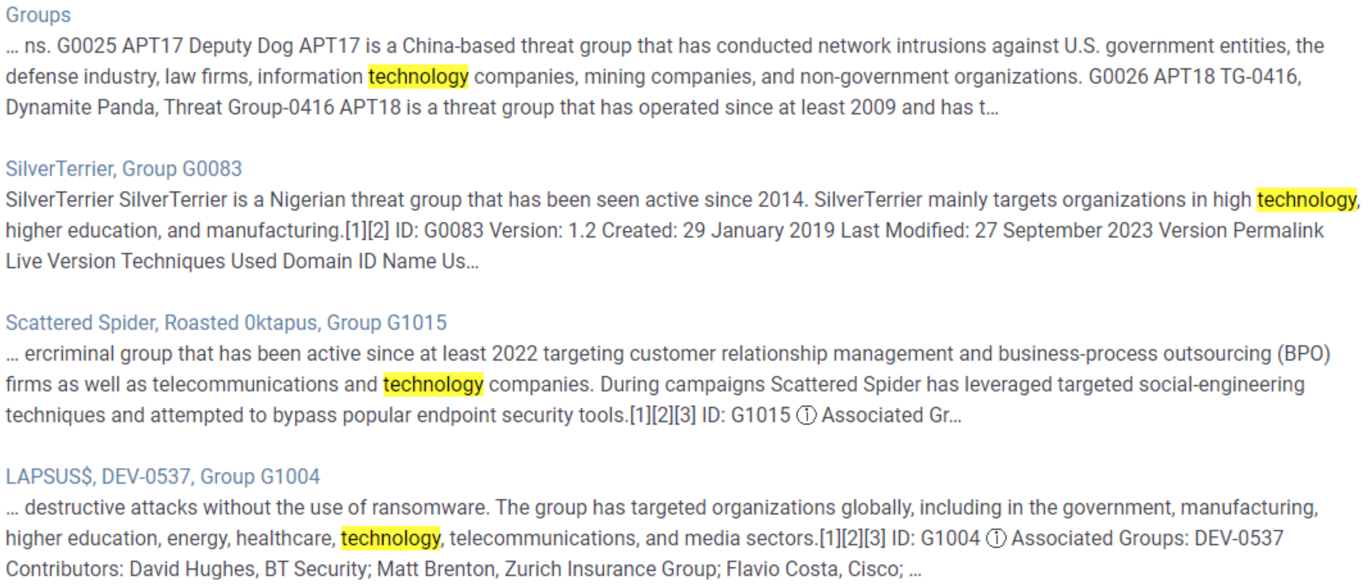
Level 1 Threat intelligence

For organizations embarking on establishing a threat intelligence capability, it's practical to begin by concentrating on a singular threat actor that poses a risk to your company, sector, or geographical area. This approach allows for a focused examination of the specific techniques employed by that threat actor.

For example, assume that your organization operates in the U.S. technology sector. A useful starting point would be to explore the MITRE ATT&CK homepage and search the keyword "**technology**".

You will come across various threat groups with specific interests in the **technology sector**. One example is the "Scattered Spider" group, known for their focus on large corporations and their external IT support services. This particular group's activities make it a crucial starting point for your threat intelligence efforts due to its direct relevance to your organization.

By selecting this threat actor group within the database, you're led to a page that offers a wealth of information about "Scattered Spider." The ATT&CK framework enriches your understanding by listing associated groups and detailing the techniques this group deploys. Such insights are pivotal for comprehending the operational methods of the threat actor, enabling your organization to devise targeted defenses against their specific tactics.



Groups

… ns. G0025 APT17 Deputy Dog APT17 is a China-based threat group that has conducted network intrusions against U.S. government entities, the defense industry, law firms, information technology companies, mining companies, and non-government organizations. G0026 APT18 TG-0416, Dynamite Panda, Threat Group-0416 APT18 is a threat group that has operated since at least 2009 and has t…

SilverTerrier, Group G0083

SilverTerrier SilverTerrier is a Nigerian threat group that has been seen active since 2014. SilverTerrier mainly targets organizations in high technology, higher education, and manufacturing.[1][2] ID: G0083 Version: 1.2 Created: 29 January 2019 Last Modified: 27 September 2023 Version Permalink Live Version Techniques Used Domain ID Name Us…

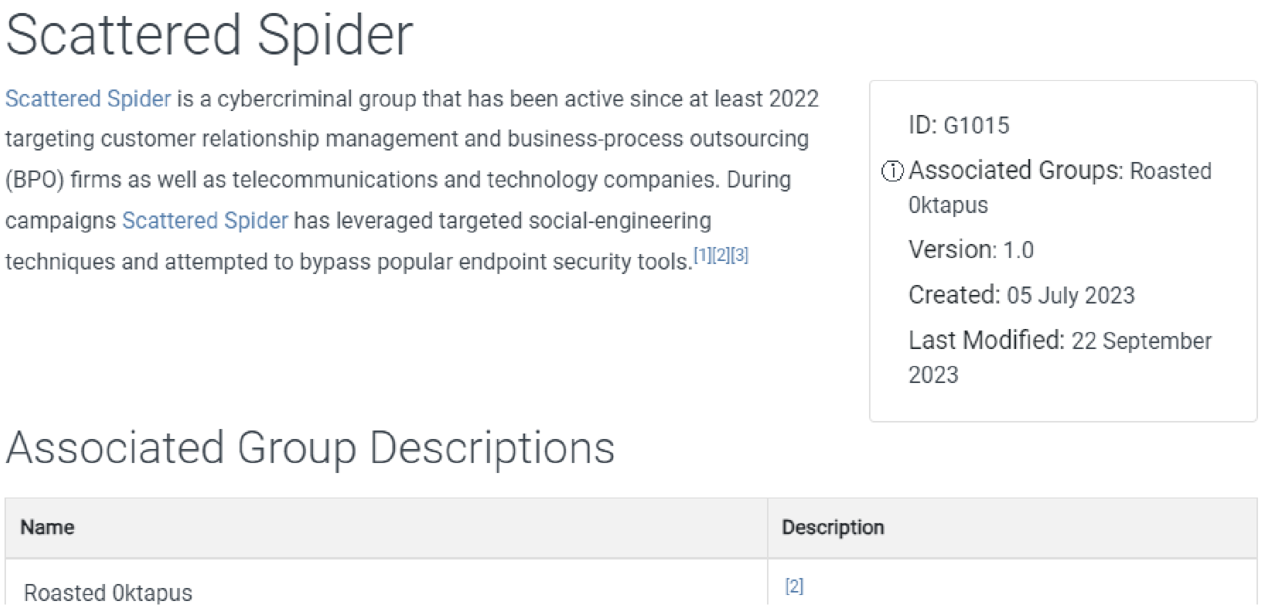
Scattered Spider, Roasted 0ktapus, Group G1015

… ercriminal group that has been active since at least 2022 targeting customer relationship management and business-process outsourcing (BPO) firms as well as telecommunications and technology companies. During campaigns Scattered Spider has leveraged targeted social-engineering techniques and attempted to bypass popular endpoint security tools.[1][2][3] ID: G1015 ⓘ Associated Gr…

LAPSUS$, DEV-0537, Group G1004

… destructive attacks without the use of ransomware. The group has targeted organizations globally, including in the government, manufacturing, higher education, energy, healthcare, technology, telecommunications, and media sectors.[1][2][3] ID: G1004 ⓘ Associated Groups: DEV-0537 Contributors: David Hughes, BT Security; Matt Brenton, Zurich Insurance Group; Flavio Costa, Cisco; …

Source: MITRE ATT&CK



Scattered Spider

Scattered Spider is a cybercriminal group that has been active since at least 2022 targeting customer relationship management and business-process outsourcing (BPO) firms as well as telecommunications and technology companies. During campaigns Scattered Spider has leveraged targeted social-engineering techniques and attempted to bypass popular endpoint security tools.[1][2][3]

ID: G1015

ⓘ Associated Groups: Roasted 0ktapus

Version: 1.0

Created: 05 July 2023

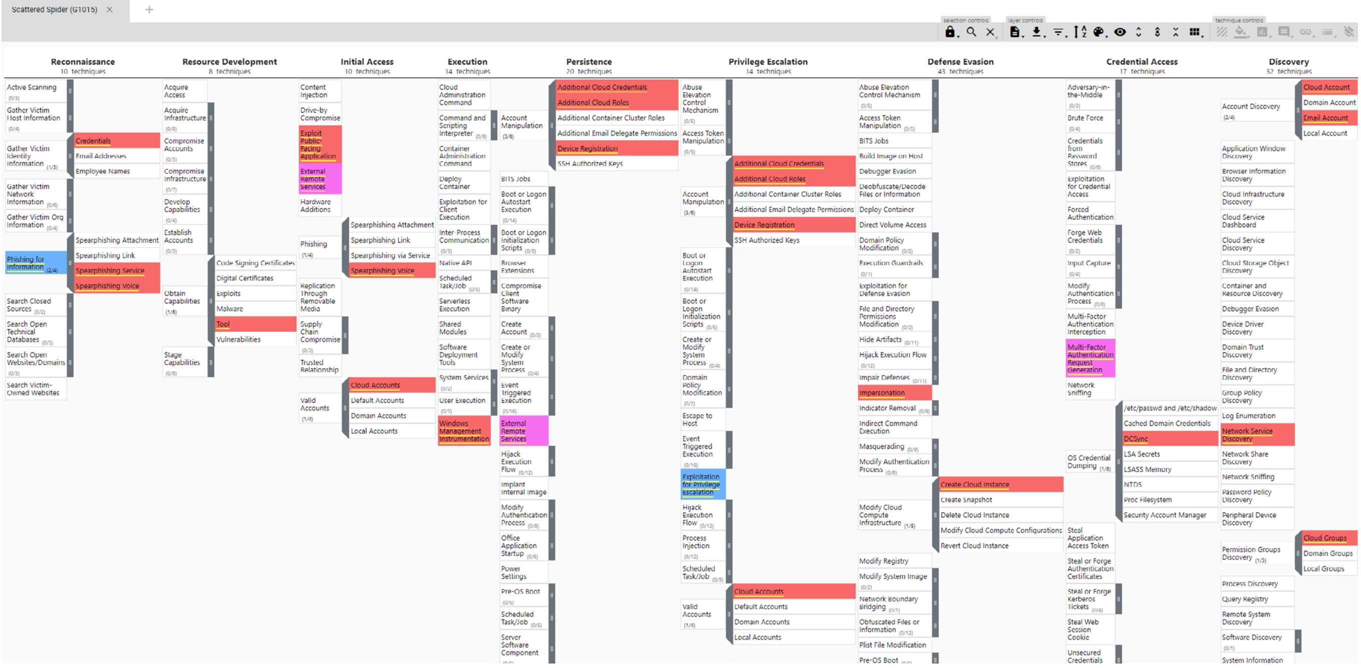
Last Modified: 22 September 2023

Associated Group Descriptions

Name	Description
Roasted 0ktapus	[2]

Source: MITRE ATT&CK

The ATT&CK framework employs the ATT&CK Navigator for visualizing techniques utilized by threat groups, such as "Scattered Spider". This tool is essential for annotating and navigating the framework's matrices. To view a group's techniques in the Navigator, simply click the "ATT&CK Navigation Layers" button found beside the "Techniques Used" section on the group's detail page. Techniques used by the group are highlighted, facilitating easy identification and analysis. Once these techniques have been identified, analysts can move to the next step of their investigation using Maltego. This shift involves conducting cursory searches on related IoCs through databases such as AlienVault OTX or Flashpoint, leveraging the insights gained from the ATT&CK Navigator to guide their search. Continue reading, and you'll discover our use case for collecting threat intelligence towards the conclusion!


Scattered Spider (G1015)
Reconnaissance 10 techniques
Resource Development 8 techniques
Initial Access 10 techniques
Execution 14 techniques
Persistence 20 techniques
Privilege Escalation 14 techniques
Defense Evasion 43 techniques
Credential Access 17 techniques
Discovery 32 techniques

Source: MITRE ATT&CK

Level 2 Threat intelligence

For organizations with a mid-level team of threat analysts, mapping threat intelligence to the MITRE ATT&CK framework can be a proactive step towards a more advanced security posture. Instead of solely depending on pre-existing mappings, creating your own based on internal incident reports or external threat intelligence, like blog posts, can provide deeper insights into the specific threats your organization faces. In enhancing this process, Maltego becomes invaluable, offering the ability to pivot across disparate data sources. Using Maltego, you can pivot from IoCs to uncover further related IPs, domains, URLs, hashes, etc., deepening your understanding of threats.

> INVESTIGATOR NOTE
> The Cybersecurity and Infrastructure Security Agency (CISA) has released a guide on best practices for MITRE ATT&CK mapping to aid threat analysts map adversary behavior to the framework.

Level 3 Threat intelligence

For organizations with an advanced CTI team, you can map additional data, both internal and external to ATT&CK to refine defense priorities. This can include leveraging data from incident response activities, OSINT reports, threat intelligence subscriptions, real-time alerts, and the organization's historical data. After mapping out this information, you can compare threat groups and prioritize commonly used techniques. You may then combine the data to discover the most consistently employed techniques, which will aid your CIRT team in deciding what to focus on. This allows your organization to prioritize tactics and inform the professionals about which ones they should concentrate on detecting and mitigating. Integrating Maltego into your threat intelligence process can significantly enhance your team's capabilities. With custom integrations to your incident tickets, threat databases, and SIEMs, you can tie external data to internal data for the most complete picture of your threat landscape.

Other Critical Frameworks

MITRE has developed several critical frameworks for threat intelligence, among them are:

- **The Trusted Automated Exchange of Intelligence Information (TAXII):** a protocol enabling automated, secure exchange of cyber threat information between organizations and security systems.
- **Structured Threat Information eXpression (STIX):** a universally accepted and standardized way to define and share CTI
- **The Cyber Observable eXpression (CybOX):** a technique for documenting observables in cybersecurity incidents

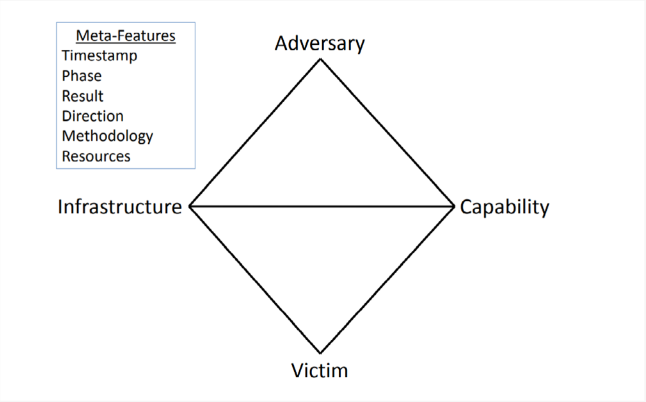
> INVESTIGATOR NOTE
> Maltego features STIX 2.1 integration and STIX-powered OpenCTI integration, developed in collaboration with ANSSI, the French National Cybersecurity Agency. ANSSI contributed open-source Transforms, supported by Maltego's development efforts. Explore this open-source project on GitHub and learn more on our blog.

The Diamond Model of Intrusion Analysis

The diamond model for intrusion analysis is a model for mapping activities of threat actors. It helps threat intelligence analysts to identify relationships between events and analyze events to learn about threat actor's behavior. It is named so because of the shape formed by the relationship between the 4 core features of an intrusion event:

- **Adversary:** intruder/attacker
- **Capabilities:** adversary's tools and/or techniques
- **Infrastructure:** physical and/or logical resources used by adversary
- **Victim:** organization or system hit by adversary

You start with one point on the diamond and pivot to discover and learn more about the other points. For example, learning about a victim can lead to learning more about the adversary's capabilities and infrastructure.



Source: The Diamond Model of Intrusion Analysis

Cyber Threat Intelligence Tools

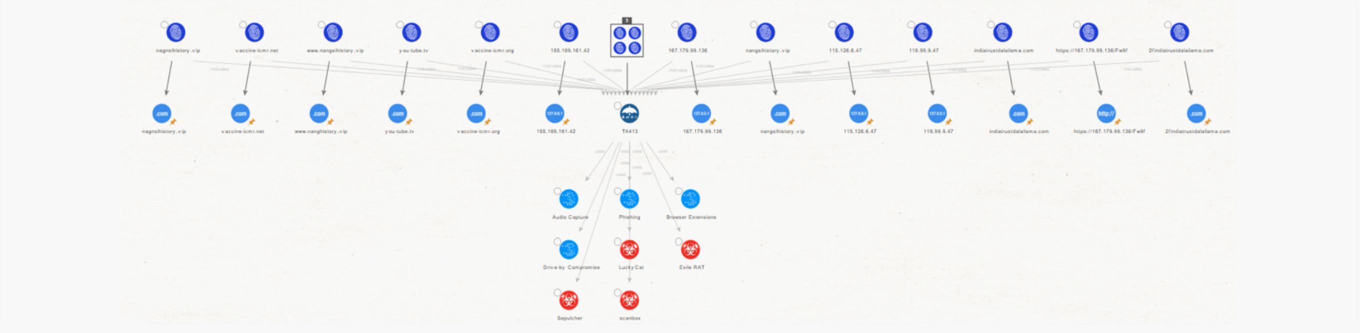
The cyber threat intelligence field is witnessing growth, incorporating a wide array of tools from both open-source projects and commercial vendors. These tools are adept at facilitating the automated gathering and processing of data, alongside offering capabilities for the visualization, mapping, correlation, and dissection of TTPs. **This is where Maltego's biggest strength comes in, empowering investigators by aggregating the most relevant data from both internal and external sources into a unified interface. It facilitates easy connections with a wide array of tools, enhancing the efficiency and effectiveness of investigations.**

Threat intelligence tools are specifically crafted to accumulate, process, and scrutinize threat data from a variety of sources, including internal, technical, and human inputs. Meanwhile, traditional security tools like SIEMs and security analytics platforms are employed to collect and correlate security events and log data. This integration of intelligence and security tools enriches the analysis of cyber threats.

For blue teams aiming to evaluate their visibility or coverage against the TTPs deployed by adversaries, tools like DeTTECT serve as invaluable resources for assessing and comparing the quality of data log sources. Another tool, Decider, offers structured guidance questions that assist analysts in aligning adversary behaviors with their operational framework.

When delving into threat intelligence data, Threat Intelligence Platforms (TIPs) emerge as prominent and widely utilized tools. For those interested in engaging with TIPs, platformsu such as MISP (Malware Information Sharing Platform) or OpenCTI (Open Cyber Threat Intelligence) are recommended starting points. Both platforms enable the collection, management, and dissemination of intelligence not just within an organization but also among various stakeholders, fostering a collaborative approach to cybersecurity.

Read more about investigating TA413 threat actor group using OpenCTI.

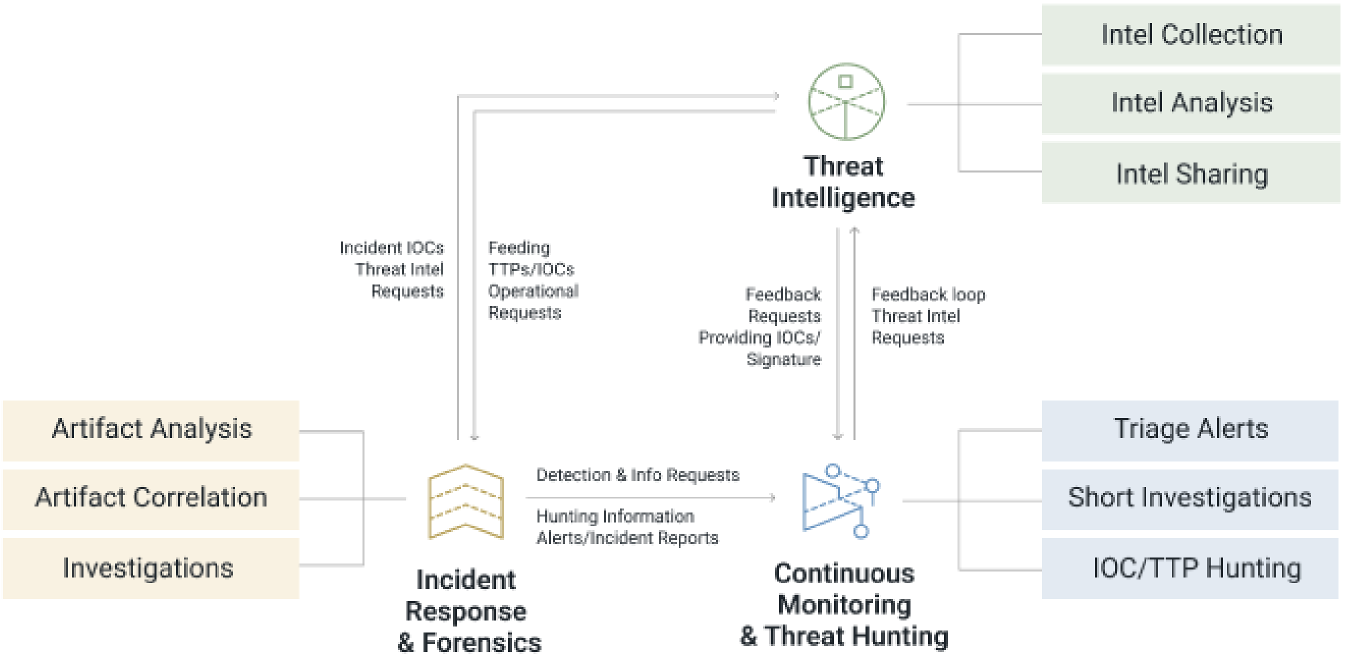


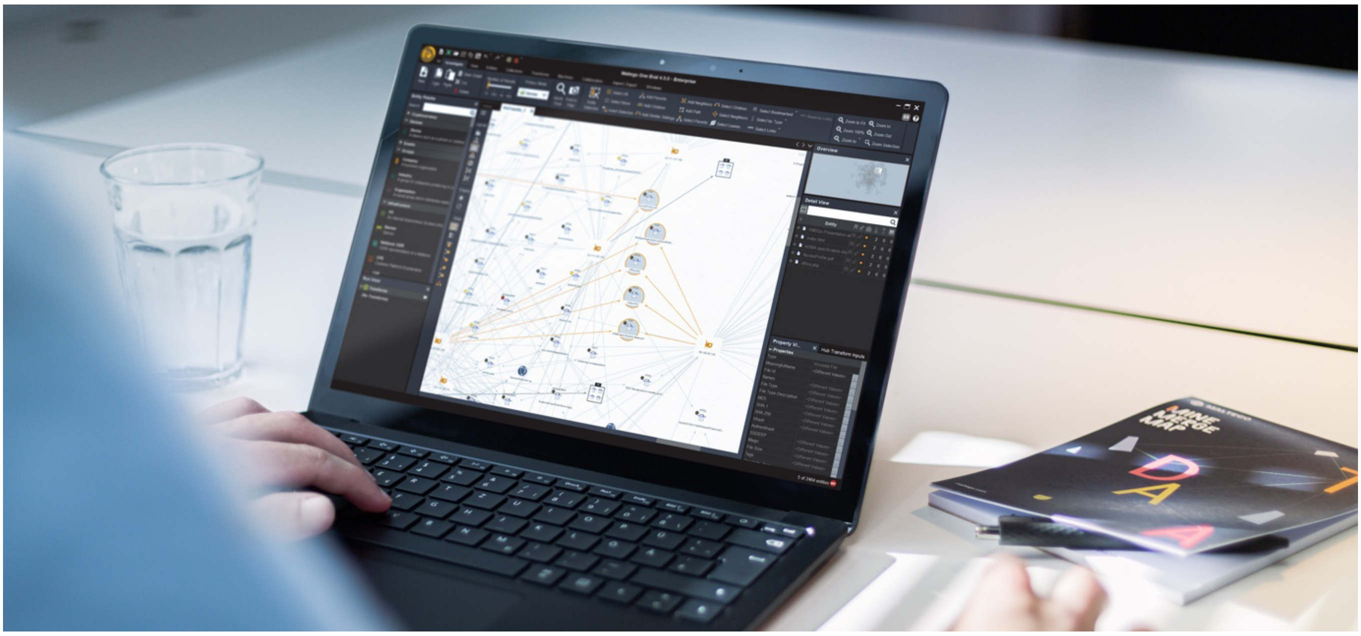
Applications of Cyber Threat Intelligence

Tailoring cyber threat intelligence to align with the specific requirements of each position and organization is crucial. Possessing a sophisticated level of threat intelligence empowers stakeholders to make swift, well-informed decisions. Additionally, it enables security professionals to more accurately grasp the decision-making processes of threat actors, facilitating earlier detection of threats and the implementation of automated responses. This approach also allows for the evaluation of the efficacy of existing security measures. Let's first find out how it can benefit each function:

FUNCTIONS	BENEFITS
Security Operations and Incident Response	Intelligence accelerates their alert triage, minimizes false positives, provides context for better decision-making, and enhances their capability to respond faster, manage, and prioritize threats.
Vulnerability management team	Intelligence provides relevant context and risk assessment that enables them to reduce downtime and focus on the most critical vulnerabilities first.
Threat Intel Analyst	Intelligence provides deeper and more expansive knowledge about motivations and TTPs of threat actors, as well as current security trends to generate more valuable analyses.
Brand protection teams	Intelligence tools assist in monitoring unsanctioned web and social media mentions, data breaches, employee impersonations, counterfeit products, typosquatting, phishing attacks, and more, enhancing brand safety.
Third-party risk programs	Intelligence provides current insights into the security postures of vendors, suppliers, and other external partners, aiding in the management of third-party risks.
Fraud Prevention Teams	Intelligence helps to identify online threats and leaked credentials to detect fraud campaigns, strengthen risk-based authentication methods, and improve defenses against online fraud.
Executives Management	Intelligence equips leaders with a comprehensive understanding of the risks faced by their organizations, available mitigation strategies, potential threats, and their implications on business operations, guiding informed security policy and strategy development.

Reference: SANS Institute





Key Use Cases Involving Cyber Threat Intelligence

In this handbook, we will focus on five commonly known use cases, providing scenarios to demonstrate how you can utilize Maltego for cyber threat intelligence and make your threat intelligence analysis effortless:

1. Threat Intelligence Collection
2. Malware Infrastructure Tracking
3. Vulnerability and Attack Surface Assessment
4. Threat Actors Profiling
5. Attacks and TTPs Analysis

If you haven't installed Maltego on your computer yet, now is the perfect opportunity to discover our unique offering for Enterprise CTI Plan tailored just for your team!

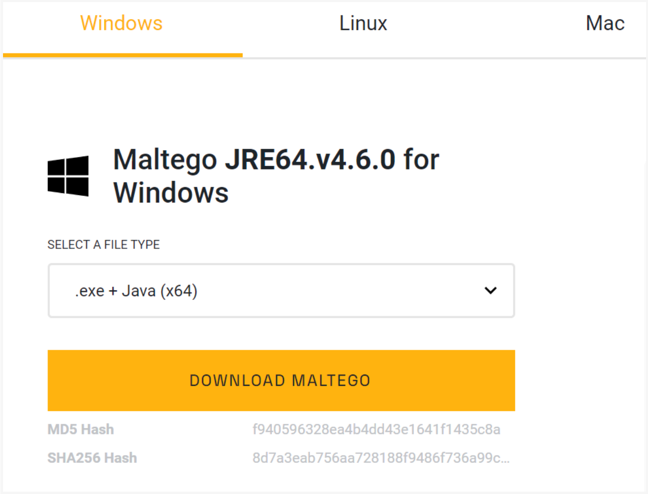
Setting up Maltego

4.

Set up your Maltego Desktop Client following the simple steps below. For more information, please check step-by-step guide here.

1. Download Maltego

Install Maltego Desktop Client that is compatible with your operating system (Windows, Linux, or Mac).



Maltego JRE64.v4.6.0 for Windows

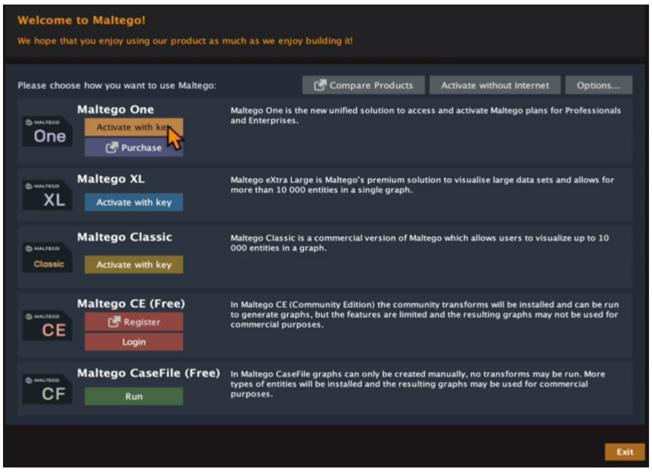
SELECT A FILE TYPE

.exe + Java (x64)

MD5 Hash	f940596328ea4b4dd43e1641f1435c8a
SHA256 Hash	8d7a3eab756aa728188f9486f736a99c...

2. Activate Maltego

Launch Maltego Desktop Client on your device. On the welcome screen, you will likely see an option to activate the product. Select Maltego One and click “Activate with Key.” Type in or paste the License key you should have received in your email. Then click “Next.”



Welcome to Maltego!

We hope that you enjoy using our product as much as we enjoy building it!

Please choose how you want to use Maltego:

Maltego One

Maltego One is the new unified solution to access and activate Maltego plans for Professionals and Enterprises.

Maltego XL

Maltego eXtra Large is Maltego's premium solution to visualise large data sets and allows for more than 10 000 entities in a single graph.

Maltego Classic

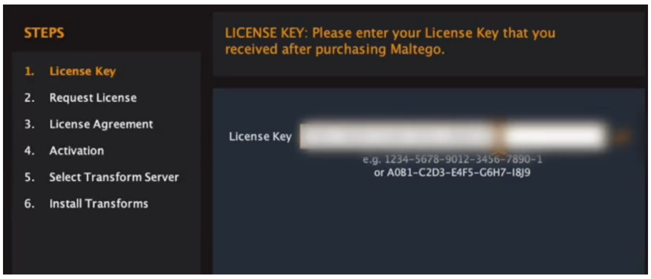
Maltego Classic is a commercial version of Maltego which allows users to visualize up to 10 000 entities in a graph.

Maltego CE (Free)

In Maltego CE (Community Edition) the community transforms will be installed and can be run to generate graphs, but the features are limited and the resulting graphs may not be used for commercial purposes.

Maltego CaseFile (Free)

In Maltego CaseFile graphs can only be created manually, no transforms may be run. More types of entities will be installed and the resulting graphs may be used for commercial purposes.



STEPS

1. License Key
2. Request License
3. License Agreement
4. Activation
5. Select Transform Server
6. Install Transforms

LICENSE KEY: Please enter your License Key that you received after purchasing Maltego.

License Key [redacted]

e.g. 1234-5678-9012-3456-7890-1
or A0B1-C2D3-E4F5-G6H7-I8J9

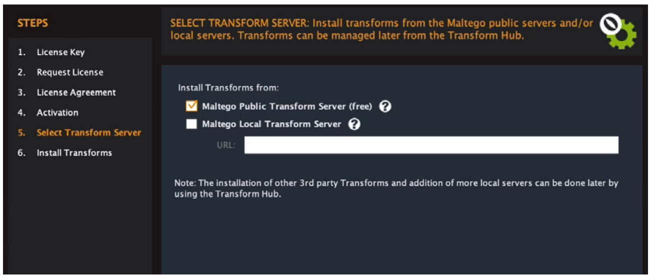
3. Read and accept the License Agreement

Read and accept the General Terms and Conditions for Software Licenses and Accompanying Services and click “Next.”

4. Install Transform Servers

Select Maltego Public Transform Server. And wait for Maltego to install the transforms.

Note: On-Premise (CTAS) Maltego users, please find more information here.



STEPS

1. License Key
2. Request License
3. License Agreement
4. Activation
5. Select Transform Server
6. Install Transforms

SELECT TRANSFORM SERVER: Install transforms from the Maltego public servers and/or local servers. Transforms can be managed later from the Transform Hub.

Install Transforms from:

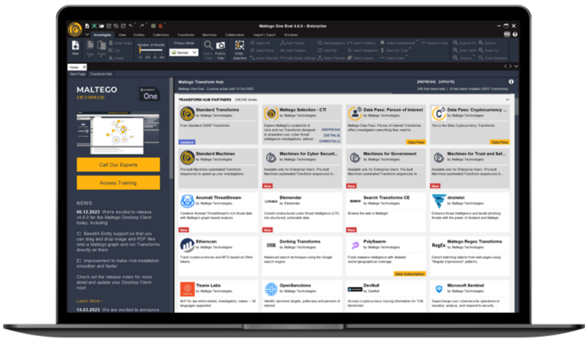
☑ Maltego Public Transform Server (free)

☐ Maltego Local Transform Server

URL:

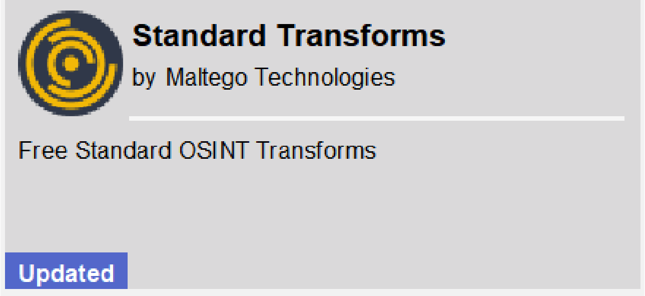
Note: The installation of other 3rd party Transforms and addition of more local servers can be done later by using the Transform Hub.

5. Install Hub Items & Start Investigating!



Install the Maltego Standard Transforms and Maltego Selection – CTI. You are all set for now. Elevate your security with the world’s most used cyber investigation tool.

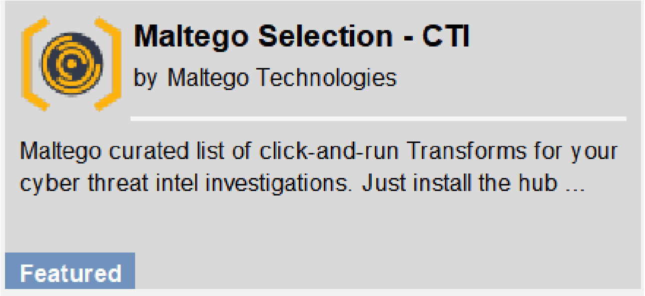
Happy investigating!



Standard Transforms
by Maltego Technologies

Free Standard OSINT Transforms

Maltego Standard Transforms: It refers to a set of Transform Hub items that contain core OSINT Transforms, Entities, and Machines which are developed and maintained by Maltego.



Maltego Selection - CTI
by Maltego Technologies

Maltego curated list of click-and-run Transforms for your cyber threat intel investigations. Just install the hub ...

Maltego Selection – CTI: It is a curated list of click-and-run Transforms that come out-of-the box for Maltego users. It enables users to quickly access relevant Transforms from various data integrations with one click and begin their cyber threat intelligence investigations without delay.

Top Maltego Hub Items for Cyber Threat Intelligence 5.

Maltego simplifies the use of diverse data sources and multiple tools by merging SIEMs, logs, ticketing systems, internal databases, threat intelligence, OSINT, and vulnerability scanners into one unified platform. It further improves investigative processes by offering versatile access to data that caters to different requirements, skill levels, and workflows. Below, you will find lists of top-tier intelligence and workflows solutions for various CTI investigative scenarios. These solutions and lists that have proven to be among our users' favorites and are suitable for all budget sizes.

Maltego Selection — CTI

Maltego enhances CTI investigations by offering a curated selection of click-and-run Transforms, designed to streamline your workflows without requiring additional logins or purchases. If you're new to CTI or uncertain where to begin, Maltego provides practical solutions with pre-designed Transforms. It is ideal for tasks like enriching IP addresses or finding IoCs among others. Simply install these user-friendly, ready-to-use Transforms from the Maltego Desktop Client to accelerate your CTI investigation effortlessly.

WHAT'S INCLUDED IN **MALTEGO SELECTION – CTI?**

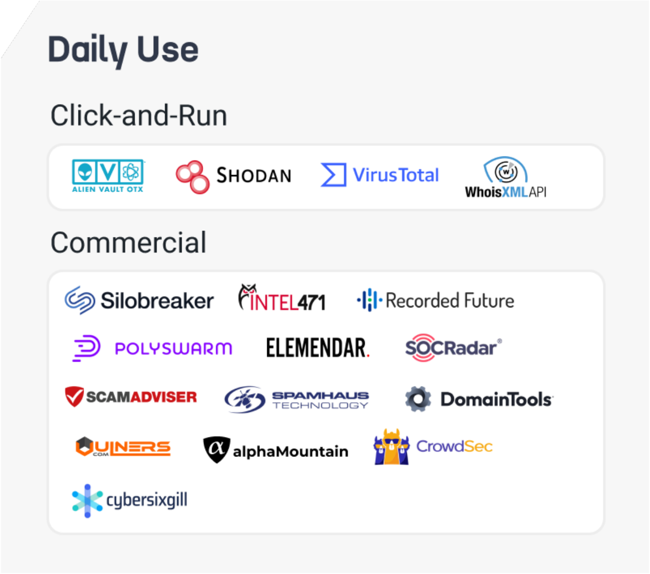
The list includes data sources from Censys, alphaMountain, Abuse.ch URLhaus, AbuseIPDB, PolySwarm, OpenPhish, urlscan.io, and DNSTwist as of April 2024.

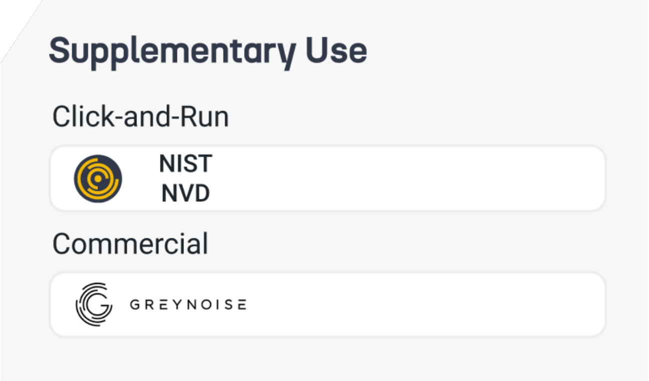
Maltego CTI modules (Part of Maltego Data Pass)

Following our curated list of click-and-run Transforms for CTI, we want to address the challenge of tool fatigue from using multiple tools and disparate data sources. Say farewell to juggling several API keys and data integrations and welcome the convenience of having all relevant data in one place. Maltego introduces credit-based subscriptions designed for quick and enhanced CTI investigations, streamlining your access to a wide range of data sources from multiple vendors, all without the need for external API management.

At the end of this document, we showcased five widely known investigations for cyber threat intelligence, utilizing specific data resources available through the Maltego Data Pass for CTI. Continue reading to discover more details at the end of this document!

Additional Hub Items for Daily and Supplementary Use





Supplementary Use

Click-and-Run

NIST NVD

Commercial

GREYNOISE

Here are more Hub items for **daily and supplementary use** for CTI, updated as of April 2024. This list includes newly integrated items and is presented without any implied hierarchy or preference.

NOTE
For more information on our CTI-specific data integrations, including out-of-the-box access to household CTI feeds, customizable SIEM and TIP connectors that streamline CTI workflows, and access to over 100 ready-made connectors for OSINT and your external data sources, please visit the Data Hub page on our website.

Advanced Hub Items for Workflow Integration

To enhance CTI investigations and achieve faster clarity while improving workflow efficiency for advanced and expert Maltego users, consider integrating cybersecurity operations tools such as Microsoft Sentinel, IBM Qradar, ATT&CK MISP, OpenCTI, and others into Maltego. These integrations provide threat intelligence teams with real-time data and insights, empowering them to proactively identify and analyze emerging threats. Bring your own tools within the Maltego interface and merge the most relevant data together to advance your threat analysis!

ATT&CK – MISP

Query MISP threat sharing instances and other MISP events, attributes, objects, tags, and galaxies.

IBM QRadar

Extract and map context of IoCs from event logs and offenses.

Microsoft Sentinel

Analyze and respond to security incidents with a holistic view on potential vulnerabilities.

OpenCTI

Query and explore threat intelligence data from OpenCTI instances using STIX2 Entities.

ServiceNow

Create and search incident data, associated metadata and relevant structured Entities, and more.

Splunk

Cross-reference IP Addresses, domains, hashes, URLs, and other IoCs with internal intelligence.

Team Cymru Orbit

Discover, monitor, and manage external digital risks and vulnerabilities across the entire supply chain.

From Data to Insights: Key Use Cases

6.

Use Case 1 Threat Intelligence Collection

Context

An organization specializes in customer relationship management and, while it has remained unaffected by cyber incidents, recognizes the risk posed by the well-known cyber threat group, Scattered Spider, within their industry. At the request of the SOC manager, the threat intel team has been tasked with collecting indicators of compromise (IoCs) related to Scattered Spider to enhance their cybersecurity measures. The team plans to leverage data from Threat Intelligence Platforms (TIPs), and private intel providers via Maltego integrations including **AlienVault OTX** and **Flashpoint**, to compile comprehensive IoCs associated with Scattered Spider.

Goal

The Threat Intel team wants to gather IoCs associated with Scattered Spider.

Starting Point

Names or alias of the said threat actors: Scattered Spider

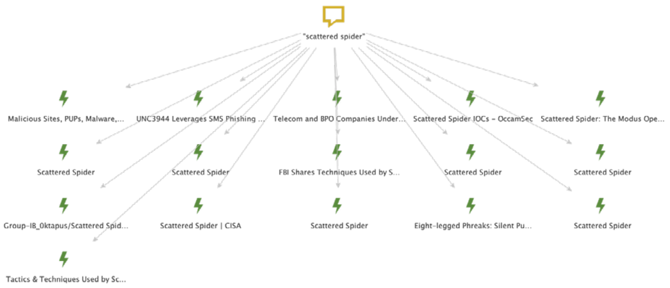
Playbook using AlienVault OTX

Step 1 – Starting off

- **Overview:** In this initial step, we are consolidating all entry points into our investigation. We are starting with what we know about a particular threat actor.
- **Maltego task:** Paste known names and aliases of your target threat actor into Maltego as phrase Entities. In this case, paste “Scattered Spider.”

Step 2 – Searching for Pulses on the Threat Actor Online

- **Overview:** To gather information on a threat actor, one efficient approach is leveraging the AlienVault OTX community Instead of manually searching in the browser and copying results to Maltego, we can utilize Maltego’s integration with AlienVault OTX to directly import relevant data. By executing the “Search Pulses” Transform, we can sift through the pulse* database—collections of threat data and indicators added by the OTX community—to pinpoint references to the threat actor, streamlining the process.
- **Maltego task:** Select the phrase Entity containing the names and aliases and run the following Transform:
  - `Search Pulses [OTX]`

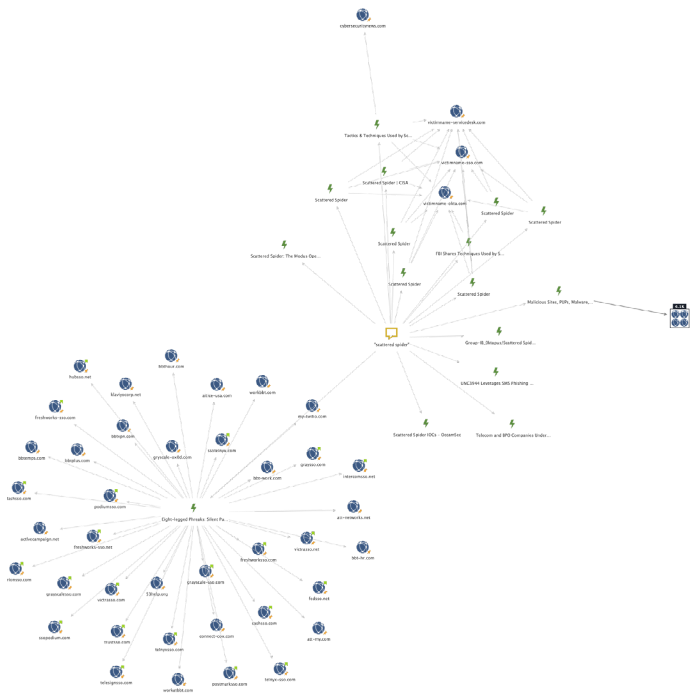

"scattered spider"
Malicious Sites, PUPs, Malware,...
UNC3944 Leverages SMS Phishing ...
Telecom and BPO Companies Under...
Scattered Spider IOCs – OccamSec
Scattered Spider: The Modus Ope...
Scattered Spider
Scattered Spider
FBI Shares Techniques Used by S...
Scattered Spider
Scattered Spider
Group-IB_Oktapus/Scattered Spid...
Scattered Spider | CISA
Scattered Spider
Eight-legged Phreaks: Silent Pu...
Scattered Spider
Tactics & Techniques Used by Sc...

WHAT IS A PULSE?

The OTX community reports on and receives threat data in the form of pulses. OTX pulses provide you with a summary of the threat, the related IoCs, a view into the software targeted, and other valuable details to help you detect the threat in your environment.

Step 3 – Extracting Domains from Pulses

- **Overview:** In the case of Scattered Spider, examining domains they mimic offers insight into their potential targets. By utilizing Maltego, investigators can pinpoint these domains from pulses, highlighting entities and extracting domain details. This step will be crucial for blue teams and researchers aiming to identify the threat actor's victims. In general, effective investigation hinges on sifting through a vast collection of pulses to isolate the relevant ones. By strategically pinning and focusing on relevant data, investigators can refine their workflow, like opening relevant links in new tabs for later review on the AlienVault website. Alternatively, manual organization of Entities—either by dragging around or deleting them—helps in distilling the investigation to the most significant findings, ensuring a focused and efficient analysis process.
- **Maltego task:** Select all the pulses containing the names and aliases and run the following Transform to extract domains:
  - `To Domain Indicators [OTX]`



Step 4 – Filtering for relevant URLs

- **Overview:** Next, we want to drill into specific results that interest us. You can manually select the website Entities that appear relevant to your search, or alternatively, you can select all results at once that have a weight exceeding 70 for convenience and run a transform to get the specific URLs you want. Then we will evaluate the association of our threat actor.
- **Maltego task:** Select all results and run Transform:
  - **To URLs `[show Search Engine results]`**

Step 5 – End of your investigation! Expand your research

- **Overview:** Once filtered, we now are left with 22 domains linked with the threat actor. You can expand your search to collect more comprehensive IoCs by utilizing additional integrations connected to the ones you've already gathered. Simultaneously, you can proactively block these identified domains to mitigate potential phishing attempts.

> NOTE
> The playbook outlined above represents just the initial phase of collecting IoCs. It can be extended to uncover new IoCs through various other integrations.

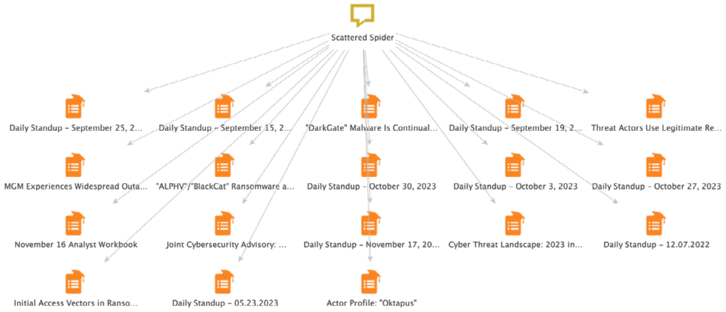
Playbook using Flashpoint

Step 1 – Starting off

- **Overview:** This step here is exactly the same as the one above for using AlienVault OTX. However, we aim to compare the differences in results between free threat intelligence communities and private intel providers to evaluate their depth and breadth of information.
- **Maltego task:** Paste the name "Scattered Spider" as phrase Entity in Maltego.

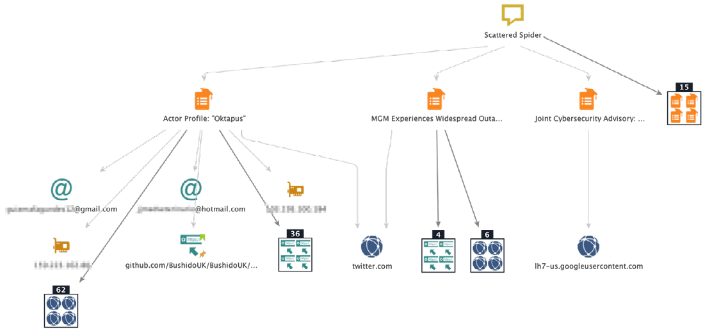
Step 2 – Searching for Reports on the Threat Actor Online

- **Overview:** To gather information on a threat actor again, one option is to search for reports related to the threat actor in the browser and then copy the results back to Maltego. However, manually reviewing each page of results and pasting them back to Maltego can be incredibly time-consuming. Thanks to Maltego's integration, you have the advantage of directly accessing IoCs and technical data from Flashpoint datasets, as well as information from both finished intelligence reports and analytical intelligence reports produced by Flashpoint.
- **Maltego task:** From the phrase Entity, we will add Flashpoint reports to our graph by running the following Transform:
  - `[FR] Phrase to Report`


Scattered Spider
Daily Standup – September 25, 2...
Daily Standup – September 15, 2...
"DarkGate" Malware Is Continual...
Daily Standup – September 19, 2...
Threat Actors Use Legitimate Re...
MGM Experiences Widespread Outa...
"ALPHV"/"BlackCat" Ransomware a...
Daily Standup – October 30, 2023
Daily Standup – October 3, 2023
Daily Standup – October 27, 2023
November 16 Analyst Workbook
Joint Cybersecurity Advisory: ...
Daily Standup – November 17, 20...
Cyber Threat Landscape: 2023 in...
Daily Standup – 12.07.2022
Initial Access Vectors in Ranso...
Daily Standup – 05.23.2023
Actor Profile: "Oktapus"

Step 3 – Extracting IoCs from Reports

- **Overview:** Next, we will extract IoCs from these reports. Grabbing relevant indicators out of reports (typically in PDFs) can be easily done through Maltego Transform.
- **Maltego task:** Extract IoCs from these reports by running Transforms:
  - `[FR] Report to Email Address or [FR] Report to Domain`


Scattered Spider
Actor Profile: "Oktapus"
MGM Experiences Widespread Outa...
Joint Cybersecurity Advisory: ...
15
[redacted]@gmail.com
[redacted]@hotmail.com
[redacted]
[redacted]
github.com/BushidoUK/BushidoUK/...
36
twitter.com
4
6
lh7-us.googleusercontent.com
62

NOTE
The reports displayed on the graph are directly accessible on the Flashpoint website.

Step 4 – Taking strategic next steps

- **Overview:** Upon extracting IoCs from reports, you should immediately block any domains clearly associated with your organization that appear malicious. If certain domains raise suspicion but aren't overtly malicious, further your investigation by broadening your search to gather more relevant and comprehensive IoCs, making use of additional integrations. Eliminate any irrelevant IoCs from your findings to maintain focus. Remember to update your threat databases with the refined results for future reference.
- **Maltego task:** Gather more information about IoCs

If you want to read more about this use case, check out our blog for Advanced IoCs Collection with OSINT and Threat Intelligence Feeds

Use Case 2
Malware Infrastructure Tracking

Context

An organization's threat intelligence team notices unusual outbound traffic patterns during routine network monitoring. This discovery is prompted by an external research report from a security vendor, which reports that several of its clients have fallen victim to an APT group known for stealing digital assets using malware. Following this report, the team investigated further and collected the IP addresses from the malware samples. Armed with these findings, the team is set to expand their investigation to uncover malware infrastructure using **VirusTotal**.

Goal

Uncover and understand the malware infrastructure from the vendor research report.

- Analyze the malware's infrastructure to enhance defensive strategies
- Identify additional websites associated with malware

Starting points

IP addresses from the malware samples

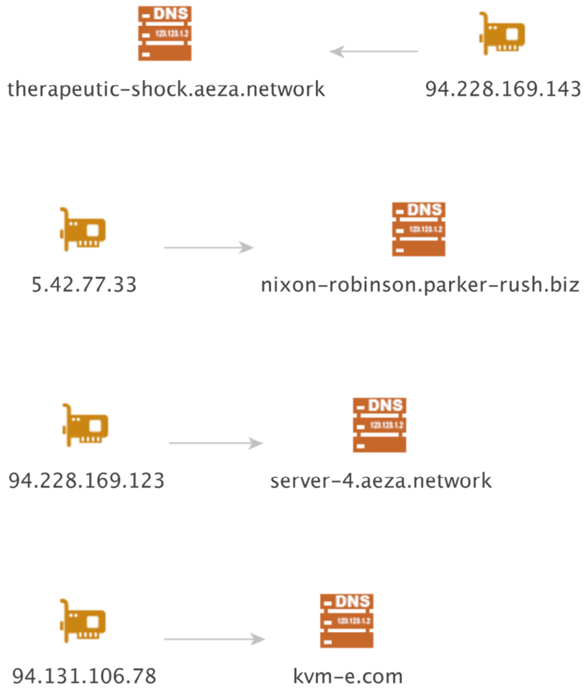
- 5.42.77.33
- 94.228.169.143
- 94.228.169.123
- 94.131.106.78

Playbook

INVESTIGATOR TIP

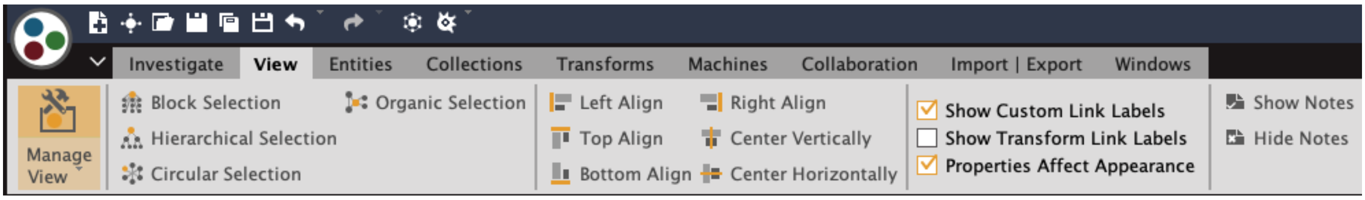
PRELIMINARY ASSESSMENT

We will extract certain IP addresses linked with the Darkgate malware report to replicate the specified scenario above and initiate our investigation with these IP addresses from the malware samples at hand. It is essential to verify that these IP addresses are not associated with content delivery networks (CDNs). Typically, our workflow involves using VirusTotal to identify samples that have communicated with these IP addresses, aiming to discover additional samples linked to the same threat actor. A significant challenge arises if the IP addresses belong to CDNs. These servers, utilized by major services like Discord or Facebook, expedite content sharing with their users. The problems begin when threat actors exploit these CDNs to disseminate malicious content. As CDNs can be used by a variety of threat actors, if we apply our usual workflow on an IP from a CDN, we could result in all sorts of samples, most of which are likely unrelated to the threat actor under investigation. How can we verify this? We can perform a reverse DNS lookup transform. Simply select the IP addresses and run **To DNS [Reverse DNS]**. As a result, in this case, CDNs do not appear to be associated with the IP addresses, allowing us to continue with our standard procedure for examining the malware infrastructure.



Step 1 – Starting off

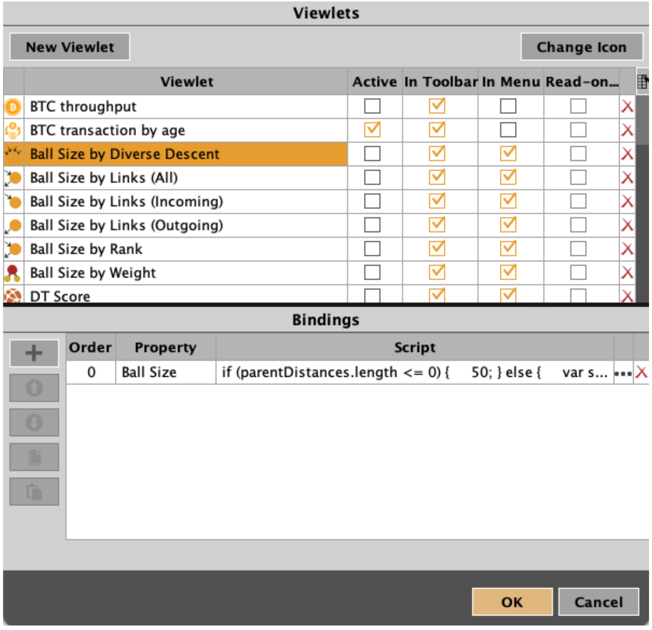
- **Overview:** We've got four IP addresses from malware samples. Our first step is to analyze these IP addresses. We will map out all the important details throughout the following steps.
- **Maltego task:** Paste four IP addresses into Maltego and run Transform:
  - `To Communicating Files [VirusTotal Public API]`



☑ Show Custom Link Labels
☐ Show Transform Link Labels
☑ Properties Affect Appearance

Step 2 – Sorting the Samples by Time

- **Overview:** As a result of step 1, we got a total of 249 samples linked to four IP address. However, given the large volume of data, individual evaluation of Entities is impractical. Fortunately, there's a useful feature designed for such situations. By applying the View feature, you can figure out the data represented in graphs easily.
- **Maletgo task:** Go to View tab at the top of your screen. Click on the Manage View button. This will open the Mange View window. Here, you can create, remove, and organize your Views.



Viewlet	Active	In Toolbar	In Menu	Read-on...
BTC throughput	☐	☑	☐	☐
BTC transaction by age	☑	☑	☐	☐
Ball Size by Diverse Descent	☐	☑	☑	☐
Ball Size by Links (All)	☐	☑	☑	☐
Ball Size by Links (Incoming)	☐	☑	☑	☐
Ball Size by Links (Outgoing)	☐	☑	☑	☐
Ball Size by Rank	☐	☑	☑	☐
Ball Size by Weight	☐	☑	☑	☐
DT Score	☐	☑	☑	☐

Order	Property	Script
0	Ball Size	if (parentDistances.length <= 0) { 50; } else { var s...

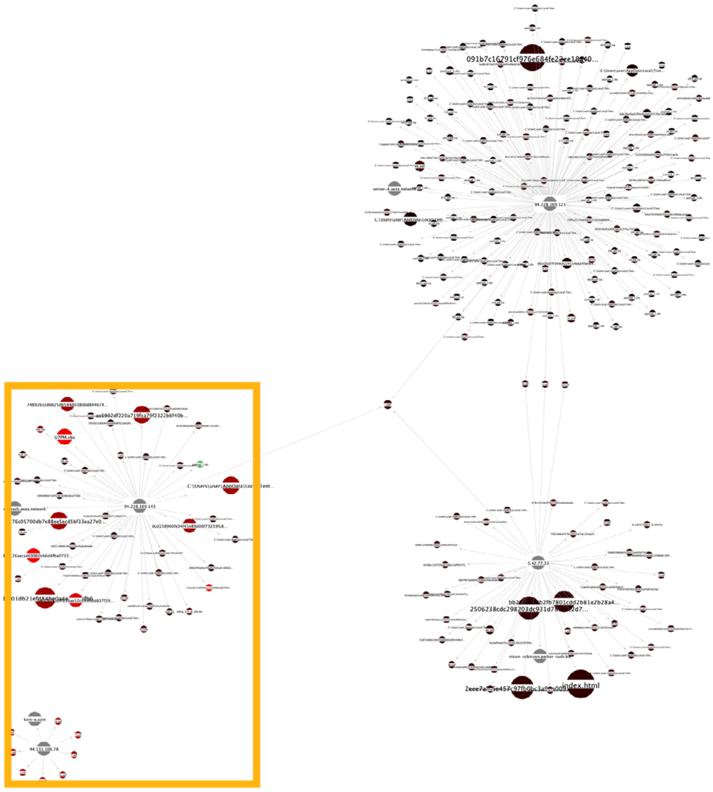
INVESTIGATOR NOTE

In our case, it is set to do two tricks when applying Views:

- It alters the color of the Entity based on the submission time of the file, with brighter red indicating a more recent submission.
- It changes the size of the Entity based on the frequency of submission, meaning the more times a file has been submitted, the larger the Entity will appear

Step 3 – Identifying the Most Recent Samples

- **Overview:** After applying Views, it became apparent that the two groups of Entities in the bottom left corner are associated with the most recent samples. Given that the articles providing the original IP addresses are several months old, it's prudent to concentrate on these newer samples to ensure our analysis is based on the latest information.
- **Maltego task:** Select clusters in bright red and copy them to a new graph.



Step 4 – Extracting Hashes from the Recent Samples

- **Overview:** Now we want to extract hashes from the most recent samples by using VirusTotal Public API Transform. This will generate outputs of standard hashes such as MD5, SHA1, and SHA256, which are designed to uniquely identify individual files. Additionally, it includes hashes like vhash, which are intended to be identical for slightly varied versions of the same file. This explains why some hashes are shared among different files in our graph.
- **Maltego task:** Select all the samples in the graph and run Transform:
  - `To Hash [VirusTotal Public API]`

INVESTIGATOR NOTE

To visualize these hashes, you can use the default **"Ball Size by Incoming Links"** view.

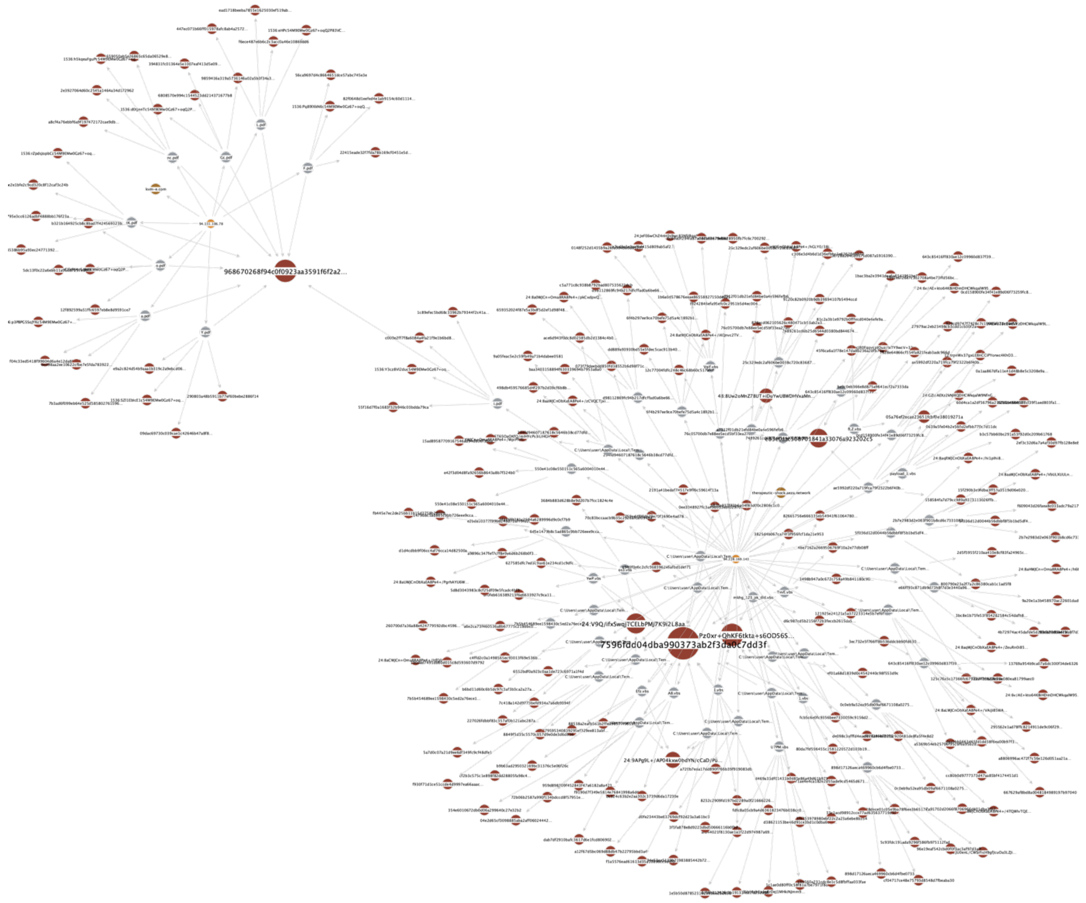
Step 5 – Narrowing Down to the Most Common Vhashes.

- **Overview:** Now, we have many hashes on the graph. Let's focus on one of the most common vhashes in our graph: **7596fdd04dba990373ab2f3da0c7dd3f**. Utilizing this vhash, we aim to generate a query that will uncover more recent, yet similar, samples. This task can be approached in two steps:

  1. First, query samples with this exact vhash. This can be done using the "vhash" search modifier (check the complete list)

  2. Second, query samples that were initially submitted within the last 30 days. This can be done using the "fs" search modifier.

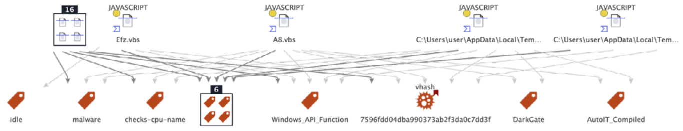
In addition, the files associated with this vhash are all JavaScript files. Hence, we'll refine our search to this file by adding "type" search modifier. Consequently, this query is formatted as: **vhash:7596fdd04dba990373ab2f3da0c7dd3f fs:30d+ type:js.** Executing this query, however, may yield numerous results, some of which might not be pertinent to Darkgate.


968670268f94c0f0923aa3591f6f2a2...
24:V9Q/ifxSwqj7CELbPMJ7K9i2L8aa...
Pz0xr+QhKF6tkta+s6OD56S...
7596fdd04dba990373ab2f3da0c7dd3f
24:9APg9L+/AP04kxw0bdYN/cCaD/Pu...

- **Maltego task:** Get more information from the samples.

Step 6 – Extracting Tags and Applying YARA Rules to Verify Match

- **Overview:** To delve deeper into our sample, we will extract its tags and apply YARA rules to verify if they match with malware samples.
- **Maltego task:** Run transforms:
  - `To YARA Rules [VirusTotal Premium API] and To Tags [VirusTotal Public API].`



Step 7 – Refining Query

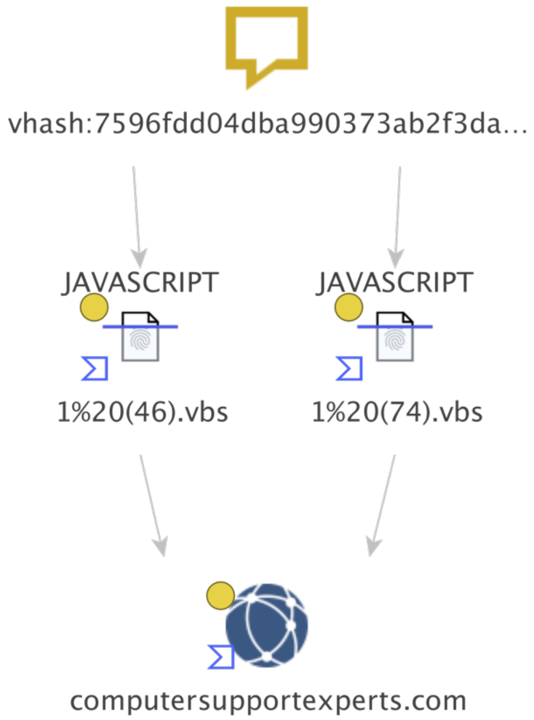
- **Overview:** To refine our query, we'll incorporate the most frequently occurring tags and a YARA and paste the new format into Maltego.

> Most frequently occurring tags and a YARA: **crowdsourced_yara_rule:Windows_API_Function tag:checks-cpu-name tag:malware**
> After adding it, our search string would look like the following format:
> **`vhash:7596fdd04dba990373ab2f3da0c7dd3f fs:30d+ crowdsourced_`yara_rule:Windows_API_Function type:js tag:checks-cpu-name tag:malware**

- **Maltego task:** Paste the new string into Maltego as a phrase Entity and run Transform:
  - `Raw Intelligence Search [VirusTotal Premium API].`

Step 8 – Pinpointing the Download Domains of Identified Samples

- **Overview:** The previous step resulted in two samples. Now, we will trace the download origins to identify the domains from which they were downloaded.
- **Maltego task:** Run Transform:
  - `To Domains in the Wild [VirusTotal Premium API]`


vhash:7596fdd04dba990373ab2f3da...
JAVASCRIPT
1%20(46).vbs
JAVASCRIPT
1%20(74).vbs
computersupportexperts.com

Step 9 – End of Investigation

- **Overview:** The previous step revealed the specific web domain, **computersupportexperts[.]com,** associated with the malware sample. This provides a crucial lead in our investigation into the malware's distribution network. Reviewing this domain within the VirusTotal GUI, it's observed that it frequently interacts with numerous MSI files. This pattern aligns with the characteristics of Darkgate malware, as outlined in this article. This discovery effectively connects the domain to Darkgate activities. Voilà!

Use Case 3
Vulnerability and Attack Surface Assessment

Context

An organization’s threat Intelligence team has been notified of a newly identified vulnerability that may affect the organization’s assets. This alert originated from a stakeholder, which could be a threat intelligence provider, CSIRT/ CERT notifications, or directly from the vendor involved with the organization. For this investigation, we will investigate Maltego’s domain as if it were one of the organization’s own domain, in order to evaluate its vulnerability and attack surface using **Maltego’s L1 footprint Machine, Shodan, Censys, and Team Cymru.**

Goal

Assessing a newly discovered vulnerability based on a report from a stakeholder. This involves analyzing the attack surface by identifying which assets are at risk of exposure to this vulnerability and prioritizing mitigation efforts accordingly.

Starting points

Domain

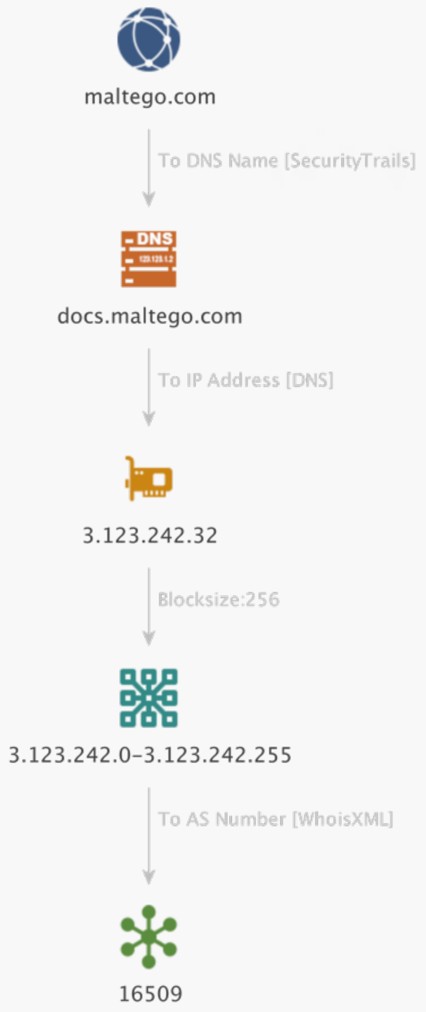
Playbook

Step 1 – Pre-investigation: Mapping the domain

- **Overview:** Our investigation will begin with domain mapping. To simulate the scenario above, we’ll employ the Maltego domain: maltego[.]com. We plan to execute a Level 1 Network Footprint using the Maltego Machine. This is very handy to reduce a lot of manual work, enabling us to gather all essential information within 1-3 minutes.
- **Maltego task:** Follow the steps below and run L1 Network Footprint with Maltego Machines.

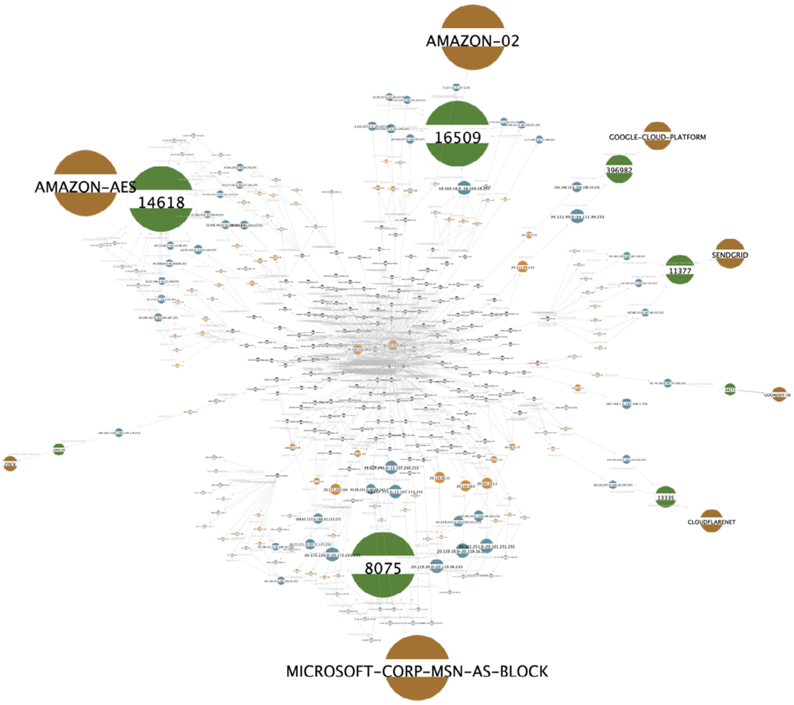
STEPS FOR CREATING L1 NETWORK FOOTPRINT WITH MALTEGO MACHINE:

- Identify DNS names associated with the domain from various sources, including passive DNS data, search engines, and dictionary, etc.
- Convert the identified DNS names into their corresponding IP addresses
- Group these IP addresses into their respective netblocks, which are specific ranges of IP addresses.
- Link each netblocks with the Autonomous System (AS) it is part of.
- Connect the AS to the company responsible for its operation, providing insight into which organization oversees the IPs where these services are hosted.



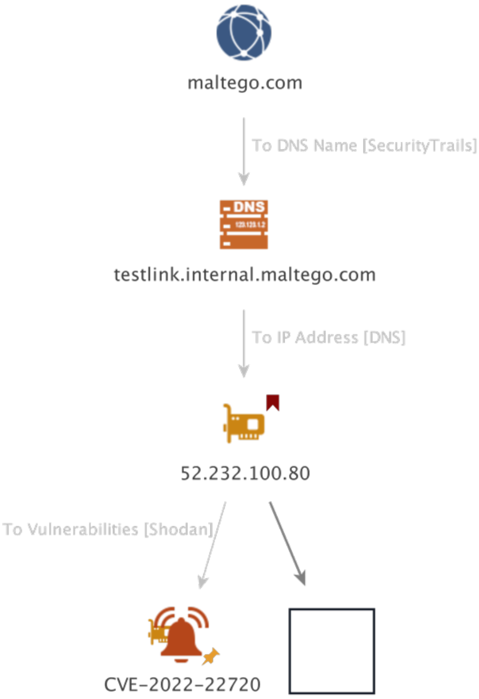
Step 2 – Investigating Vulnerability of the Domain

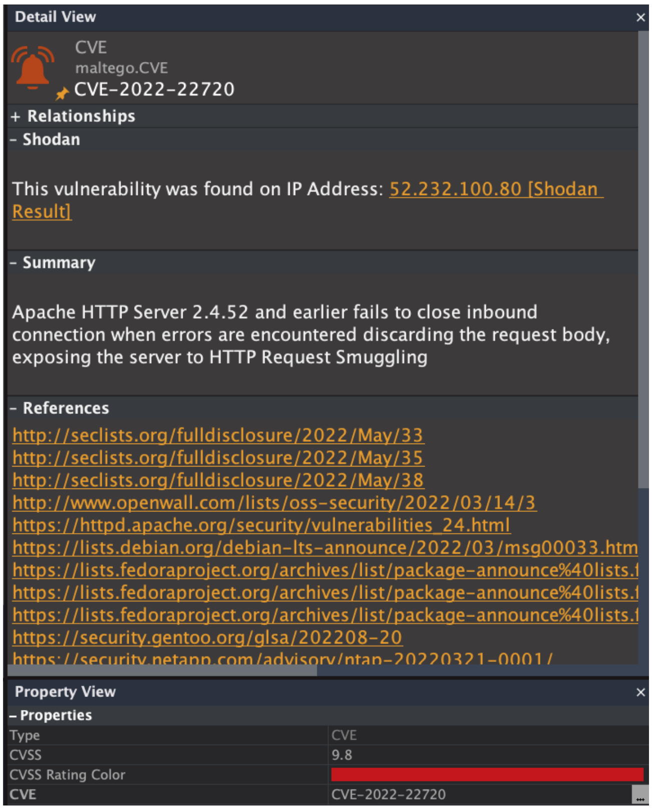
- **Overview:** After running L1 Network Footprint with Maltego Machines, this gives us the final graph below. The number of incoming links to each Entity indicates its size, revealing that the vast majority of IP addresses associated with this domain are managed by Amazon. Now that we have some understanding of our domain, it's time to assess vulnerability.
- **Maltego task:** Select all IP addresses that belong to the domain and run Transform:
  - `To Vulnerabilities [Shodan]`



Step 3 – Understanding CVSS Scores

- **Overview:** The previous step resulted in one IP address associated with multiple Common Vulnerabilities and Exposures (CVEs). Each CVE entity will be detailed, including its Common Vulnerabilities Severity Score (CVSS), which ranges from 1 to 10. The CVSS provides a measure of the severity of a vulnerability, considering factors such as ease of exploitation, the potential impact, and other relevant aspects that indicate the urgency and seriousness of the vulnerability.


maltego.com
To DNS Name [SecurityTrails]
testlink.internal.maltego.com
To IP Address [DNS]
52.232.100.80
To Vulnerabilities [Shodan]
CVE-2022-22720



CVE
maltego.CVE
CVE-2022-22720

+ Relationships

- Shodan

This vulnerability was found on IP Address: 52.232.100.80 [Shodan Result]

- Summary

Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

- References

http://seclists.org/fulldisclosure/2022/May/33
http://seclists.org/fulldisclosure/2022/May/35
http://seclists.org/fulldisclosure/2022/May/38
http://www.openwall.com/lists/oss-security/2022/03/14/3
https://httpd.apache.org/security/vulnerabilities_24.html
https://lists.debian.org/debian-lts-announce/2022/03/msg00033.htm
https://lists.fedoraproject.org/archives/list/package-announce%40lists.f
https://lists.fedoraproject.org/archives/list/package-announce%40lists.f
https://lists.fedoraproject.org/archives/list/package-announce%40lists.f
https://security.gentoo.org/glsa/202208-20
https://security.netapp.com/advisory/ntap-20220321-0001/

- Properties

Type	CVE
CVSS	9.8
CVSS Rating Color	🟥
CVE	CVE-2022-22720

INVESTIGATOR NOTE

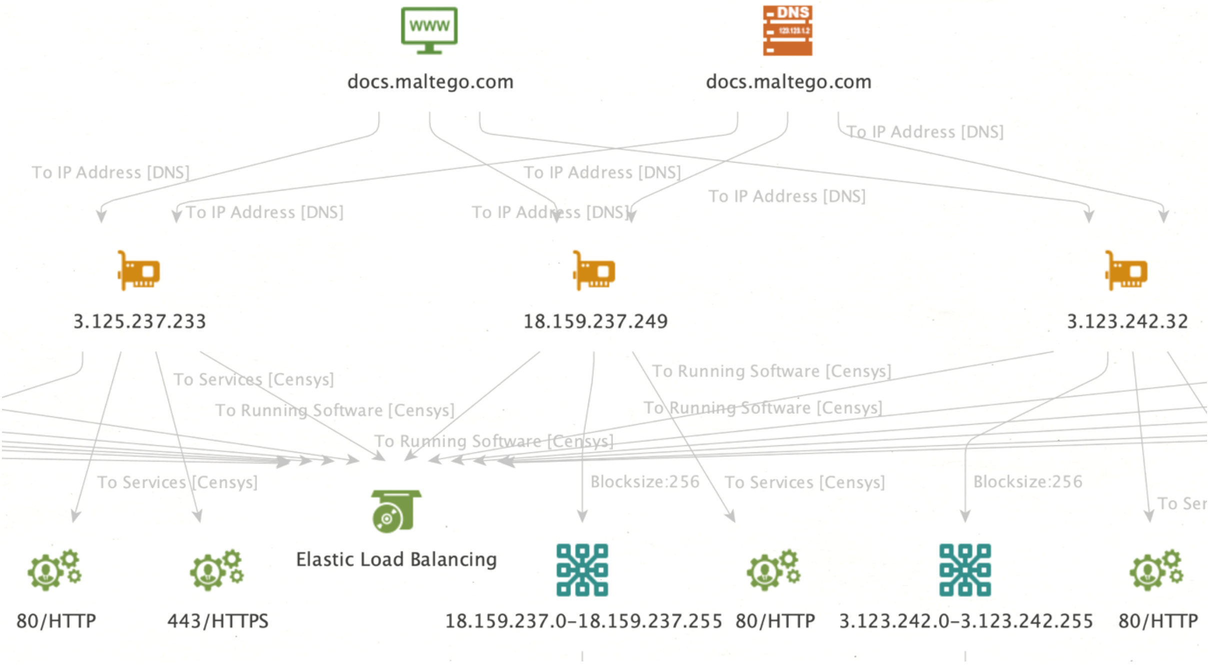
Maltego has a property for the CVSS score, and additionally, employs an overlay (in colors green, yellow, or red) on the Entity to visually indicate the severity of the CVSS score. However, in instances where there are many vulnerabilities, prioritizing becomes essential. To address this, Maltego utilizes the Weight property to represent the CVSS score, calculating the weight of a CVE at its CVSS score multiplied by 10. This enables users to select all CVEs within their graph and sort them by weight in the Detail View, providing a prioritized list of CVEs based on their CVSS scores.

Step 4 – Accessing Network Exposure

- **Overview:** To better understand what our network looks like from an outside perspective, we can use Censys to extract the services and operating systems used in the IP addresses exposed to the Internet. By using Censys, we can outline open ports on these IP addresses and gather more information about the technologies they use. Although Censys does not allow you to directly link a CVE to an IP address, you can extract software or operating system running on a particular IP. If the version number is available, you can check yourself for known CVEs linked to that platform.
- **Maltego task**: Select all IP addresses that belong to Maltego and run the following Transforms:
  - `To Running Software [Censys]`
  - `To Services [Censys]`

Step 5 – Examining Network from Inside

- **Overview:** In the previous step of this use case, we looked at our domain from an outside perspective and confirmed that several of these IPs use Elastic Load Balancing (ELB). To gain a more comprehensive understanding of our operation, we will employ an additional data provider. This provider will deploy an agent within our network, offering a different perspective. For this purpose, we will use Team Cymru's Orbit.
- **Maltego task:** Drag a maltego.cymru.Instance from the Entity and run the following

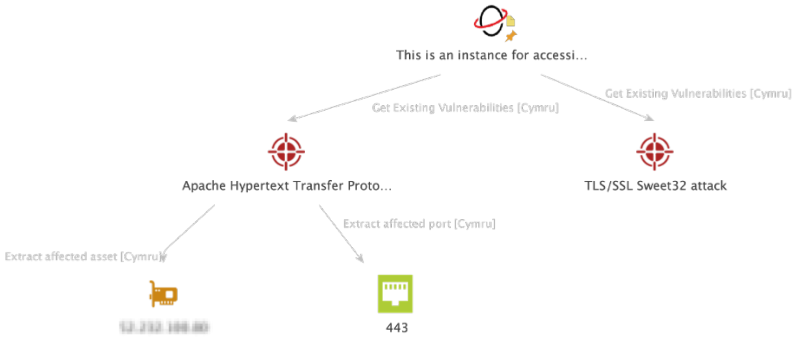


Transforms:

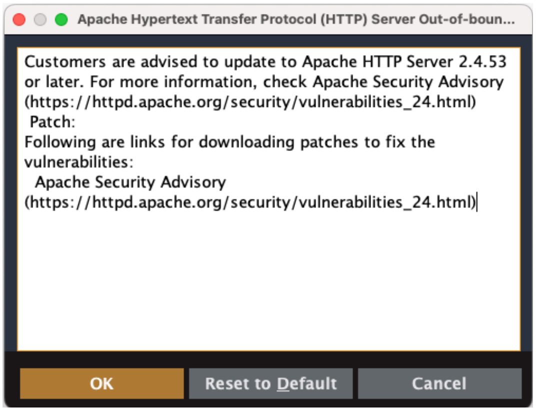
- **`Get Existing Vulnerabilities [Cymru] (with respective inputs: “High” and “No”)`**

From the Entities generated by the previous Transform, execute the following:

- **`Extract affected port [Cymru]`**
- **`Extract affected asset [Cymru]`**


This is an instance for accessi...
Get Existing Vulnerabilities [Cymru]
Get Existing Vulnerabilities [Cymru]
Apache Hypertext Transfer Proto...
TLS/SSL Sweet32 attack
Extract affected port [Cymru]
Extract affected asset [Cymru]
[redacted]
443

The first Transform will list the detected CVEs running on our services. We can then pivot from it to gather more information, such as a list of the affected assets, including the IPs and domains impacted by this vulnerability. We can also extract the specific port associated with the affected service.


Apache Hypertext Transfer Protocol (HTTP) Server Out-of-boun...
OK
Reset to Default
Cancel

Customers are advised to update to Apache HTTP Server 2.4.53 or later. For more information, check Apache Security Advisory (https://httpd.apache.org/security/vulnerabilities_24.html)
Patch:
Following are links for downloading patches to fix the vulnerabilities:
Apache Security Advisory
(https://httpd.apache.org/security/vulnerabilities_24.html)

To assist with remediation, Orbit is also adding a “Recommendation” property that provides guidance on the best way to address vulnerability. In our case, a simple update is all that’s required.

Step 6 - It’s time for remediation!

- **Overview:** The severity indications and impact assessments provided by Maltego’s CVSS scores and Orbit’s recommendation property will help us decide the prioritization for applying patches. Additionally, examining the DNS names associated with these vulnerable IP addresses will give insight into which services could be compromised if the identified CVEs were to be exploited.

You can utilize your organization’s domain to replicate this investigation and uncover any vulnerabilities in your IT infrastructure. Happy patching!

Use Case 4
Threat Actors Profiling

Context

A different team within the organization has requested the threat intelligence team to investigate several prominent threat actors responsible for different ongoing malicious campaigns affecting similar companies in the industry. The team will leverage data providers from **Cybersixgill, SOCradar, Elemendar,** and **STIX 2 Utilities.**

Goal

The threat intelligence team aims to thoroughly profile the identified threat actors and gather further evidence related to their activities by identifying past attack patterns.

Approach

Our investigation will begin with a preliminary examination based on the known identifiers(names) of the threat actors to collect initial IoCs. Subsequently, throughout our use cases 4 and 5, we will enhance our analysis by analyzing TTPs across various campaigns and actors. This will involve an in-depth comparison to determine which TTPs are more prevalent. The latter part of our investigation will focus on identifying any consistencies in the use of these TTPs by the threat actors.

INVESTIGATOR NOTE
Please note that the methodology for profiling threat actors can vary significantly depending on whether the actor's objectives are short-term and opportunistic or long-term and strategic. Additionally, real-world threat actors may not strictly adhere to established frameworks or common policies and may often mimic tactics adopted by other cybercriminals.

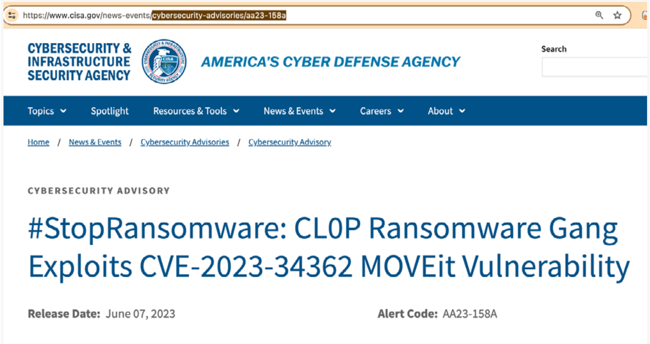
Starting Point

Threat Actor Names

Playbook Part 1 – Using STIX 2 Utilities

Step 1 – Starting off

- **Overview:** We aim to gather threat advisories potentially linked to specific threat actors of interest. To achieve this, we will drop several dorking expressions to narrow down the sources of the information and the commonly used URL paths where this information can be found.
- **Maltego task:** Drop several Maltego Phrase entities including the dorking expressions such as the following and Run **Search with Custom Dork transform [Google Dorking]:**
  - `site:cisa.gov and inurl:/cybersecurity-advisories`
  - `site:cisa.gov and inurl:/cybersecurity-advisories AND Cl0p`
  - `site:cisa.gov and inurl:/cybersecurity-advisories AND ALPHAV`



https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

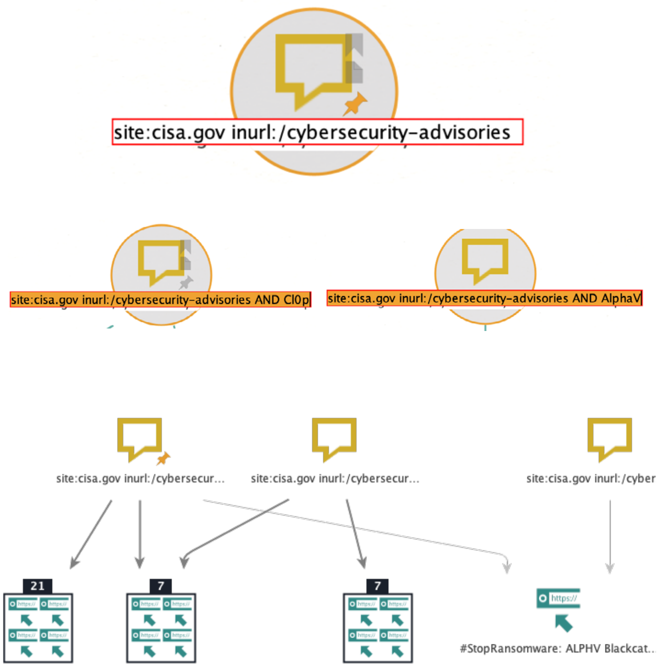
CYBERSECURITY ADVISORY

#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

Release Date: June 07, 2023

Alert Code: AA23-158A

Picking up CISA as an example of organization that provides threat intelligence, we can note that advisories include the "cybersecurity-advisories" string in the URL so we can customize our dorks accordingly.



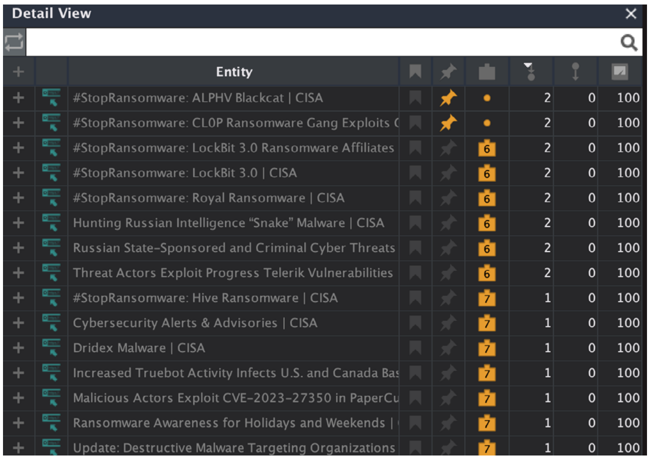
site:cisa.gov inurl:/cybersecurity-advisories
site:cisa.gov inurl:/cybersecurity-advisories AND Cl0p
site:cisa.gov inurl:/cybersecurity-advisories AND AlphaV
site:cisa.gov inurl:/cybersecur...
site:cisa.gov inurl:/cybersecur...
site:cisa.gov inurl:/cyber
21
7
7
https://
#StopRansomware: ALPHV Blackcat...

INVESTIGATOR NOTE
Every threat intel team may prioritize different websites for structured intelligence gathering, such as Sharing and Analysis Centers (ISACs), national Computer Security Incident Response Teams (CSIRTs) or agencies, and open intelligence communities.

Step 2 – Triaging Results

- **Overview:** From the various results we gather, we review and triage them based on the advisory titles.
- **Maltego task:** Select the URL entities and observe the titles in the Detail View. While reviewing them, you can perform two actions: **1.** Sort them based on the number of incoming links

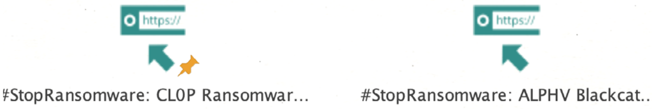
2. Pin the ones that are of interest to the analyst



Detail View

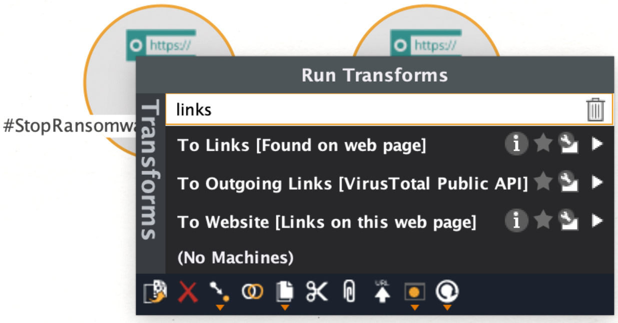
	Entity						
+	#StopRansomware: ALPHV Blackcat | CISA		📌	●	2	0	100
+	#StopRansomware: CL0P Ransomware Gang Exploits C		📌	●	2	0	100
+	#StopRansomware: LockBit 3.0 Ransomware Affiliates			6	2	0	100
+	#StopRansomware: LockBit 3.0 | CISA			6	2	0	100
+	#StopRansomware: Royal Ransomware | CISA			6	2	0	100
+	Hunting Russian Intelligence "Snake" Malware | CISA			6	2	0	100
+	Russian State-Sponsored and Criminal Cyber Threats			6	2	0	100
+	Threat Actors Exploit Progress Telerik Vulnerabilities			6	2	0	100
+	#StopRansomware: Hive Ransomware | CISA			7	1	0	100
+	Cybersecurity Alerts & Advisories | CISA			7	1	0	100
+	Dridex Malware | CISA			7	1	0	100
+	Increased Truebot Activity Infects U.S. and Canada Bas			7	1	0	100
+	Malicious Actors Exploit CVE-2023-27350 in PaperCu			7	1	0	100
+	Ransomware Awareness for Holidays and Weekends |			7	1	0	100
+	Update: Destructive Malware Targeting Organizations			7	1	0	100

As we can observe in the URL Entities titles, the first two results are highly related to the names of our threat actors mentioned in the dorking sentence while the others might only mention them. Therefore, we can directly copy these results to a new graph for further analysis.


https://
#StopRansomware: CL0P Ransomwar...
https://
#StopRansomware: ALPHV Blackcat..

Step 3 – Obtaining Structured Intelligence Links

- **Overview:** We need to identify the structured intelligence linked to the threats mentioned, typically referenced in advisories using the Structured Intelligence Information eXpression (STIX) standard. This intelligence is commonly available in XML and JSON formats.
- **Maltego task:** Extract the links on the advisories and run **To Links [found on web page]**. Once the results are obtained, go to the Investigative menu and click on "**Select Children entities**." In the Detail View, filter these results by selecting those results that end in .JSON. Sync these results with the main graph and consider adding their parent Entities to better understand where they come from.



Run Transforms

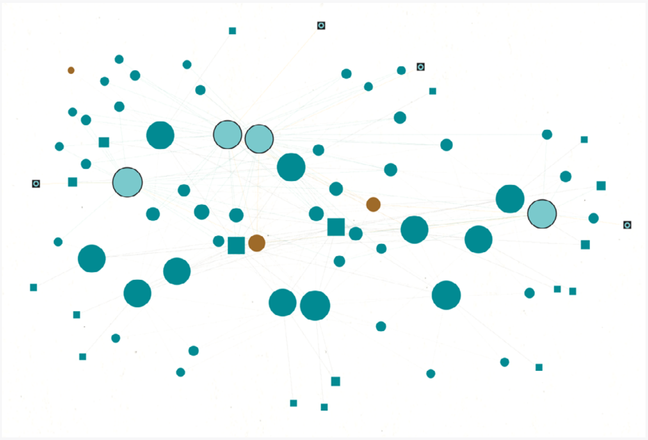
links

To Links [Found on web page]

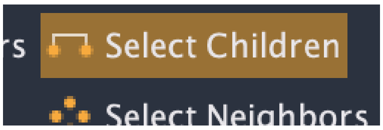
To Outgoing Links [VirusTotal Public API]

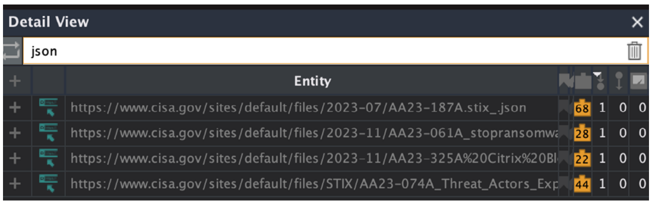
To Website [Links on this web page]

(No Machines)



INVESTIGATOR NOTE
Graphs can quickly become overloaded with links from websites, many of which may not be relevant to the information we seek. However, we can effectively filter out irrelevant links by focusing on specific file formats, such as JSON and XML, which are commonly used in structured intelligence. We can then copy the relevant links to a new graph for further analysis.



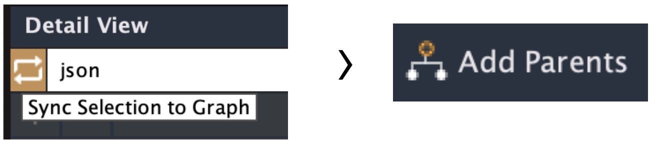


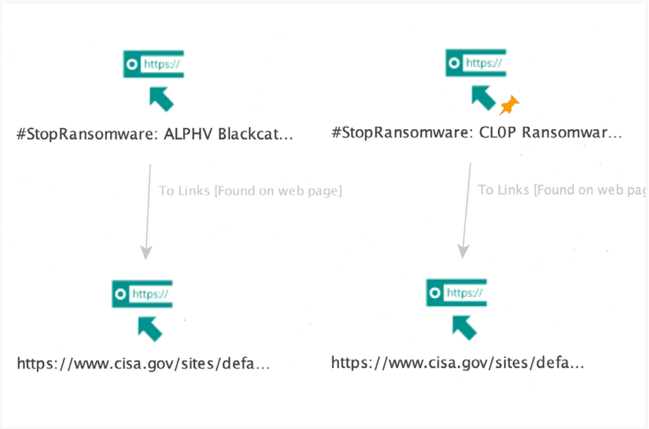
Detail View

json

	Entity					
+	https://www.cisa.gov/sites/default/files/2023-07/AA23-187A.stix_.json	68	1	0	0
+	https://www.cisa.gov/sites/default/files/2023-11/AA23-061A_stopransomwa	28	1	0	0
+	https://www.cisa.gov/sites/default/files/2023-11/AA23-325A%20Citrix%20Bl	22	1	0	0
+	https://www.cisa.gov/sites/default/files/STIX/AA23-074A_Threat_Actors_Exp	44	1	0	0

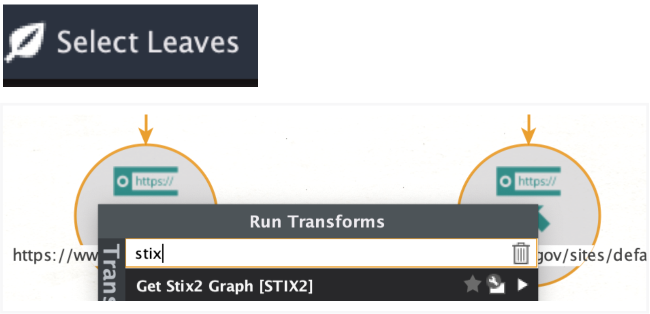
Once we identify the relevant Entities, we can add their parents Entities back into our selection for a more comprehensive view. This is done by synching the selection and then using the "Add Parents" option found in the Investigation tab. This approach helps us understand the broader context and source of the information.

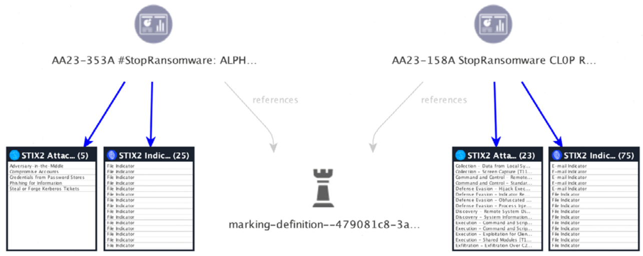


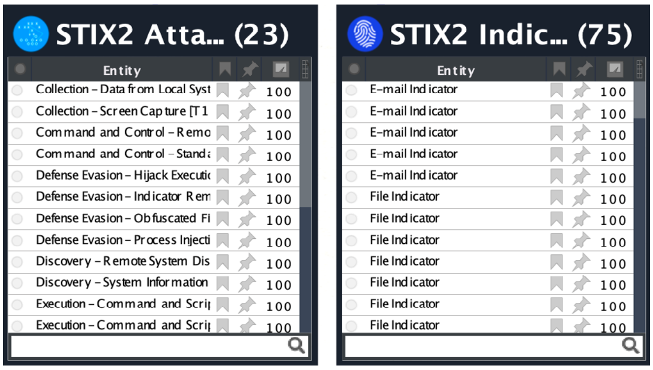

https://
#StopRansomware: ALPHV Blackcat...
https://
#StopRansomware: CL0P Ransomwar...
To Links [Found on web page]
To Links [Found on web pag
https://
https://www.cisa.gov/sites/defa...
https://
https://www.cisa.gov/sites/defa...

Step 4 – Obtaining Intel Using STIX Transforms

- **Overview:** Now, the goal is to extract the structured intelligence compiled in those STIX packages, which is crucial for our team to better understand what the identified threat actors are capable of.
- **Maltego task:** Select the URL containing. JSON Entities by clicking on "**Select Leaves**" Entities and then run **Get STIX2 Graph [STIX2]** included in the STIX Utilities Hub Item.




AA23-353A #StopRansomware: ALPH...
AA23-158A StopRansomware CL0P R...
references
references
STIX2 Attac... (5)
STIX2 Indic... (25)
marking-definition--479081c8-3a...
STIX2 Atta... (23)
STIX2 Indic... (75)



STIX2 Atta... (23)

Entity			
Collection – Data from Local Syst			100
Collection – Screen Capture [T1			100
Command and Control – Remo			100
Command and Control – Standa			100
Defense Evasion – Hijack Executio			100
Defense Evasion – Indicator Rem			100
Defense Evasion – Obfuscated Fi			100
Defense Evasion – Process Injecti			100
Discovery – Remote System Dis			100
Discovery – System Information			100
Execution – Command and Scrip			100
Execution – Command and Scrip			100

STIX2 Indic... (75)

Entity			
E-mail Indicator			100
E-mail Indicator			100
E-mail Indicator			100
E-mail Indicator			100
E-mail Indicator			100
File Indicator			100
File Indicator			100
File Indicator			100
File Indicator			100
File Indicator			100
File Indicator			100
File Indicator			100

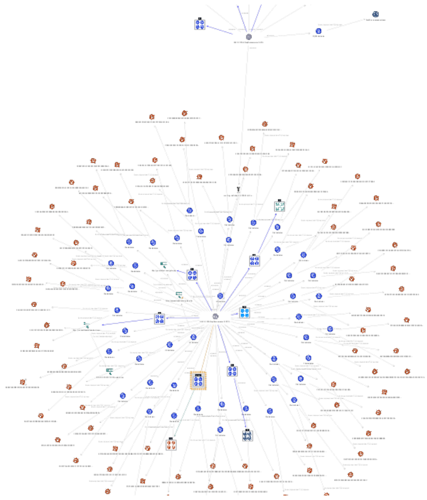
INVESTIGATOR NOTE

STIX includes various types of Entities such as Indicators, Attack Patterns (TTP), Malware, Tools, among others. For a more operational profiling, focusing on indicators can reveal details about the underlying infrastructure. Conversely, for a more tactical profiling, concentration on TTPs can provide deeper insights into the methodologies and strategic patterns used by threat actors.

Step 5 – Extracting Indicators

- **Overview:** In this step, we will analyze the links obtained from the previous step to identify structured intelligence associated with the mentioned threats, using the STIX standard for classification.
- **Maltego task:** Extract the links from the advisories and run **To Links [found on web page]** again. Once we obtain the results, select "**Select Children entities**" from the Investigative menu. In the Detail View, filter the results by choosing those that end in

.JSON. Then, synchronize these results with the main graph. Consider adding Entities to better trace their origins.



We can then select the newly obtained Entities such as emails, hashes, or domains, and copy them to a new graph for further analysis.

Step 6 – In-depth Analysis of Indicators to Profile Threat Actor

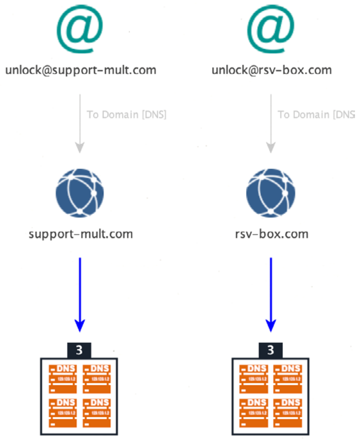
- **Overview:** Indicators from threat actors can now be leveraged to profile their infrastructure using various existing data sources, including Passive DNS information (DNSDB), Whois Registration (WhoisXML, DomainTools), and ASN/Network Information (WhoisXML, AbuseIPDB). Additionally, indicators such as email addresses can be utilized to identify personas or identities, potentially revealing details about the individuals or groups involved.
- **Maltego task:** Select the email Entities and run the following:

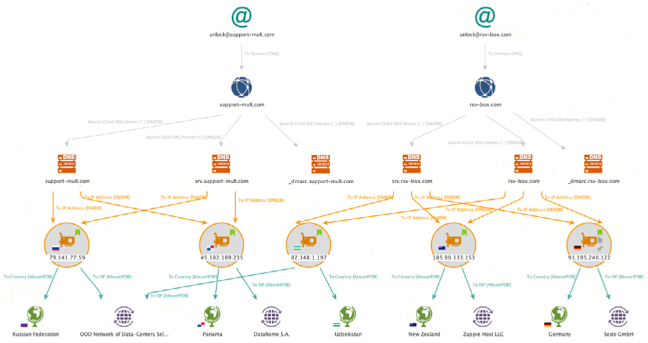
  1. To Domain [DNS] transform from Standard Transforms to look for domains registered with these emails.

  2. Search Child DNS Names [dnsdb] from FarSight DNSDB Hub item to obtain a list of hostnames.

  3. To IP Address [DNSDB] to obtain a list of IPs.

  4. To Country and To ISP [AbuseIPDB] Transforms to obtain countries and service providers linked with the obtained IPs.

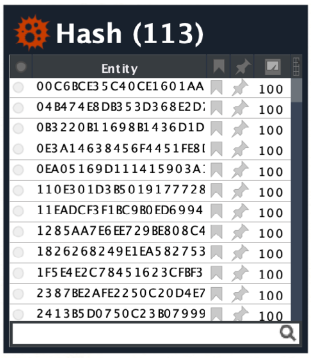




This initial analysis will offer valuable insight by connecting the dots between both domains and a few IP addresses located in Russia and Uzbekistan, which are associated with the same service provider.

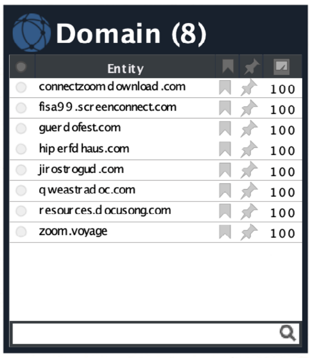
INVESTIGATOR NOTE

We could advance our research by leveraging the obtained IP address to gather further malware intelligence and more detailed infrastructure information about hostnames and sites hosted on these IPs. This approach will assist us in identifying common operational links. Simultaneously, we could undertake a similar in-depth analysis using other indicators extracted from the intelligence reports, such as hashes and domains, to expand our understanding of the threat landscape.



Hash (113)

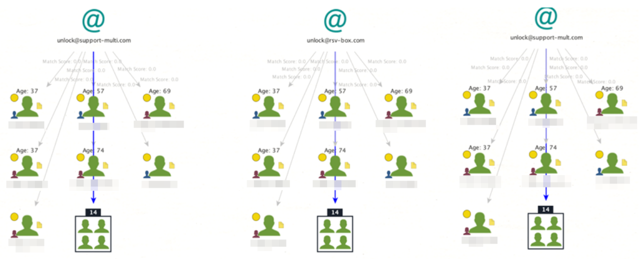
	Entity			
○	00C6BCE35C40CE1601AA			100
○	04B474E8DB353D368E2D			100
○	0B3220B11698B1436D1D			100
○	0E3A14638456F4451FE8			100
○	0EA05169D111415903A			100
○	110E301D3B5019177728			100
○	11EADCF3F1BC9B0ED6994			100
○	1285AA7E6EE729BE808C4			100
○	1826268249E1EA582753			100
○	1F5E4E2C78451623CFBF3			100
○	2387BE2AFE2250C20D4E7			100
○	2413B5D0750C23B07999			100

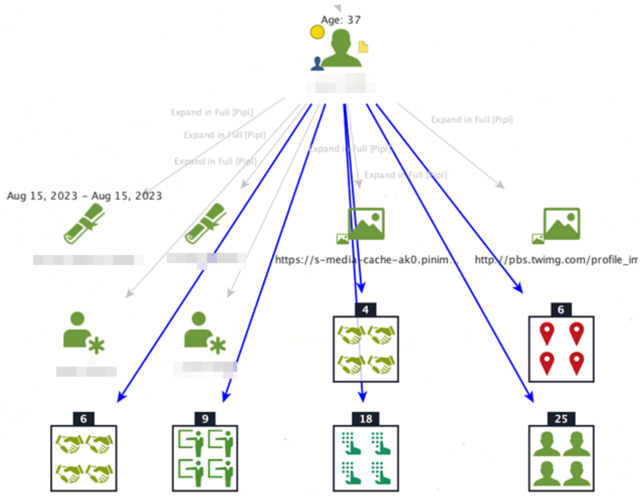


Domain (8)

	Entity			
○	connectzoomdownload.com			100
○	fisa99.screenconnect.com			100
○	guerdofest.com			100
○	hiperfdhaus.com			100
○	jirostrogud.com			100
○	qweastradoc.com			100
○	resources.docusong.com			100
○	zoom.voyage			100

Last but not least, we can conduct a Person of Interest (PoI) investigation on the email addresses identified as indicators using various Hub Items like Pipl, District4, and Constella Intelligence. This will allow us to uncover hidden identities and additional information by locating associated social media accounts, forums, or other websites linked to these emails. For this process, we strongly recommend you visit our PoI guide.



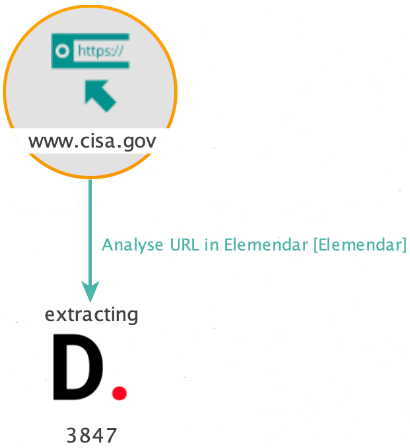


Age: 37
Expand in Full [Pipl]
Aug 15, 2023 – Aug 15, 2023
https://s-media-cache-ak0.pinim...
http://pbs.twimg.com/profile_im
4
6
6
9
18
25

Playbook Part 2: Using Elemendar

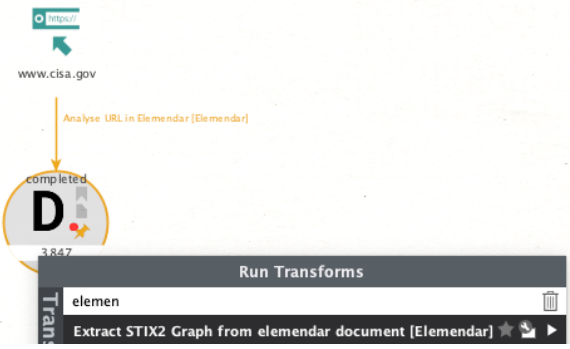
Step 1 – Starting off

- **Overview:** It is common to encounter intelligence reports written in natural human language that lack structured threat intelligence capable of being processed by tools, such as those that utilize STIX language. Let's find out how to process these kinds of reports.
- **Maltego task:** Drop the URL of the report you want to process and run a Transform, **Analyse URL in Elemendar [Elemendar]**. In a few seconds, you will see that Elemendar is collecting and extracting information, with a text indicatior showing that the processing is still ongoing.



INVESTIGATOR NOTE

Elemendar Hub item is designed to read human-friendly reports. It leverages AI technology trained with CTI reports, allowing the tool to understand the report like an analyst. This technology helps document the intelligence in STIX format, which can be then matched with our Maltego Entities.



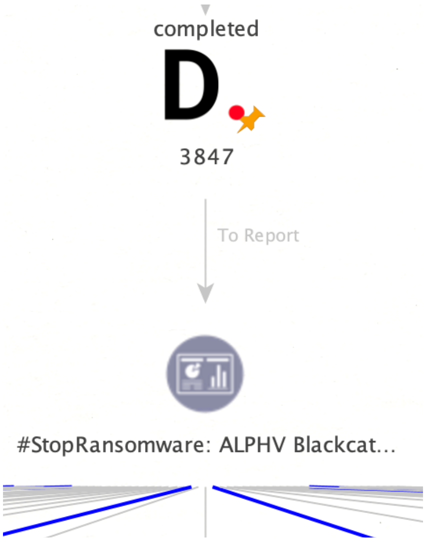
Run Transforms

elemen

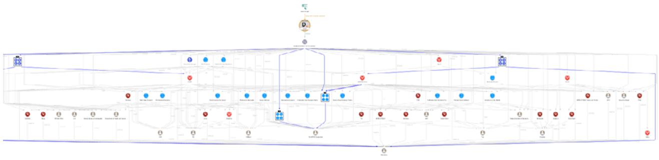
Extract STIX2 Graph from elemendar document [Elemendar]

Step 2 – Extract STIX Graphs

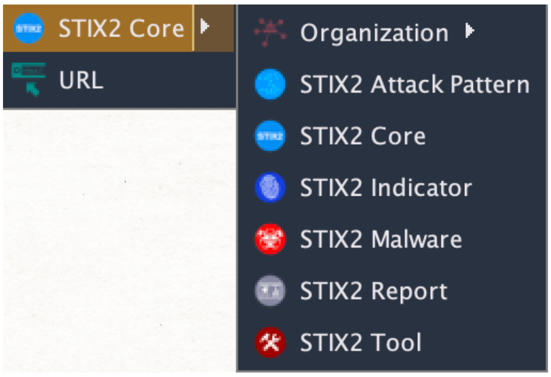
- **Overview:** Once Elemendar completes the processing and extraction of intel from our report, we will utilize this to extract a STIX graph.
- **Maltego Task:** After the Elemendar document shows that processing has finished, select it and run the Transform **Extract STIX2 Graph from Elemendar document [Elemendar].**



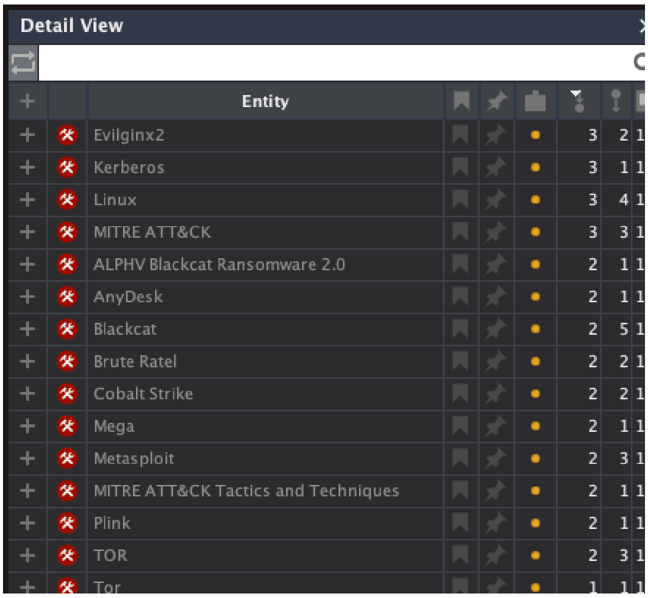
A graph will populate on the Maltego, starting from a root node that represents a STIX report.



You can easily view the information extracted by Elemendar by selecting Entities by type using the Investigate tab:



Once you select one of the Entity types, you can explore the list in the Detail View, where you have the option to filter them using keywords or sort them based on the number of incoming or outgoing links.



Detail View

Entity					
Evilginx2	●	3	2	1
Kerberos	●	3	1	1
Linux	●	3	4	1
MITRE ATT&CK	●	3	3	1
ALPHV Blackcat Ransomware 2.0	●	2	1	1
AnyDesk	●	2	1	1
Blackcat	●	2	5	1
Brute Ratel	●	2	2	1
Cobalt Strike	●	2	2	1
Mega	●	2	1	1
Metasploit	●	2	3	1
MITRE ATT&CK Tactics and Techniques	●	2	1	1
Plink	●	2	1	1
TOR	●	2	3	1
Tor	●	1	1	1

Use Case 5
Attacks and TTPs Analysis

Context

The Threat Intelligence team from a global organization regularly works to build and update the threat landscape, which includes a map highlighting the top threat actors that might target their nation state. To effectively construct strategic intelligence outcomes, the team will engage in several tactical intelligence deliverables to better understand and investigate a threat actor landscape based on geographical data or other indicators. The team will leverage data providers from **SOCRadar** and **Cybersixgill.**

Goal

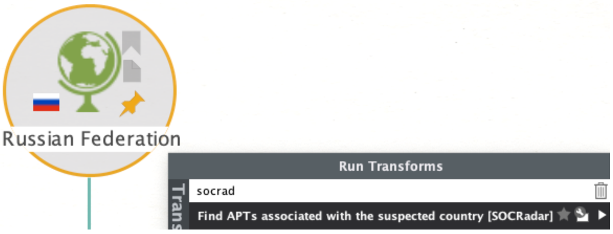
To gather information on Threat Actors suspected of operating within a specific region or targeting organizations in a particular country.

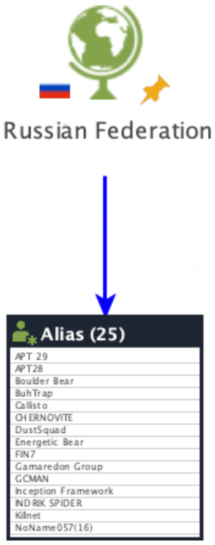
Starting Point
Country

Playbook using SOCRadar:

Step 1 – Starting off

- **Overview:** Intelligence providers are documenting existing intelligence about attribution; however, this information should be carefully considered by examining the corresponding reports to verify the supporting evidence.
- **Maltego task:** Drop a Country entity and run Transform **Find APTs associated with the suspected country [SOCRadar]**.

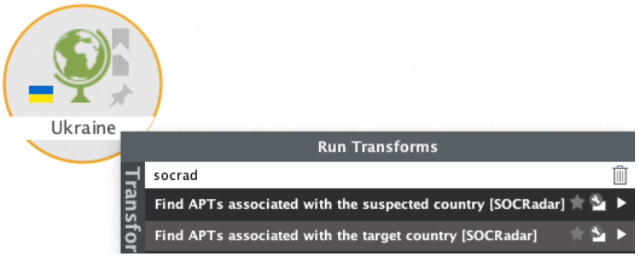




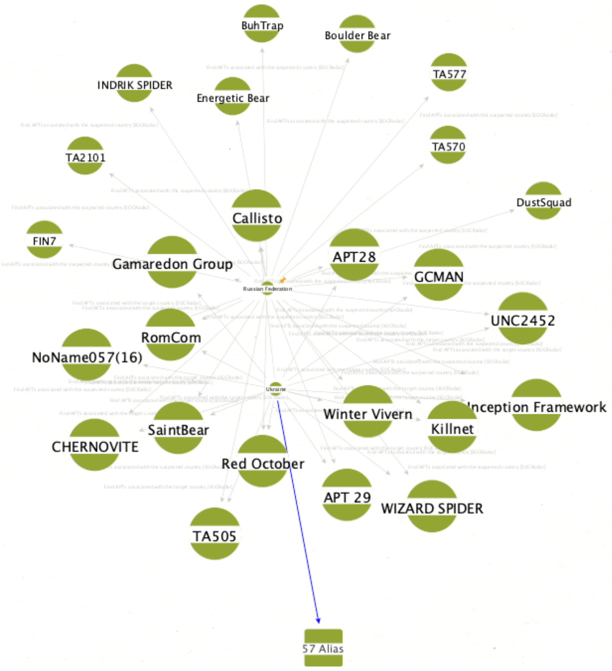
APT 29
APT28
Boulder Bear
BuhTrap
Callisto
CHERNOVITE
DustSquad
Energetic Bear
FIN7
Gamaredon Group
GCMAN
Inception Framework
INDRIK SPIDER
Killnet
NoName057(16)

Step 2 – Listing Threat Actors Targeting a Specific Country

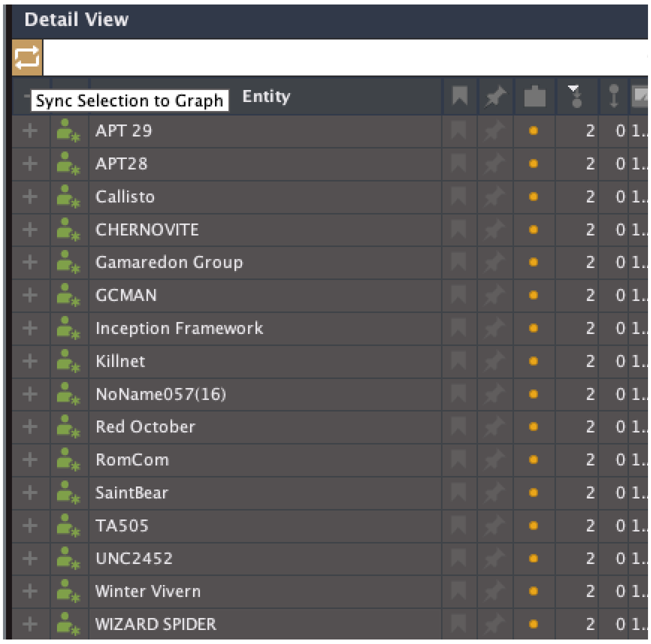
- **Overview:** Intelligence providers are also documenting existing information about victims who have been attacked or compromised. Much of this information is publicly available through announcements or claims made by threat actors when they leak samples or fully disclose data stolen from victims.
- **Maltego task:** Drop a Country entity and run transform **Find APTs associated with the suspected country [SOCRadar]**.


Ukraine
Run Transforms
Transfor
socrad
Find APTs associated with the suspected country [SOCRadar]
Find APTs associated with the target country [SOCRadar]

We can see that some of the threat actors are suspectedly linked to the Russian Federation and have simultaneously targeted Ukraine. To get a better visual representation of these connections, we can switch to an Organic View.



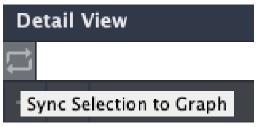
Simultaneously, we can select the Alias Entities that represent the threat actors, move to the Detail View, and sort them by the number of incoming links related to the Russian Federation and Ukraine.



Detail View

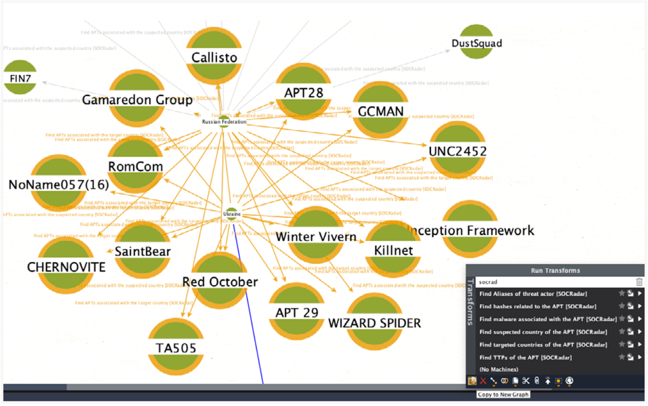
Sync Selection to Graph	Entity			
+	APT 29	●	2	0 1..
+	APT28	●	2	0 1..
+	Callisto	●	2	0 1..
+	CHERNOVITE	●	2	0 1..
+	Gamaredon Group	●	2	0 1..
+	GCMAN	●	2	0 1..
+	Inception Framework	●	2	0 1..
+	Killnet	●	2	0 1..
+	NoName057(16)	●	2	0 1..
+	Red October	●	2	0 1..
+	RomCom	●	2	0 1..
+	SaintBear	●	2	0 1..
+	TA505	●	2	0 1..
+	UNC2452	●	2	0 1..
+	Winter Vivern	●	2	0 1..
+	WIZARD SPIDER	●	2	0 1..

Now, we can select these Entities and synchronize them with the graph to observe their connections and then copy them to a new graph for further analysis.



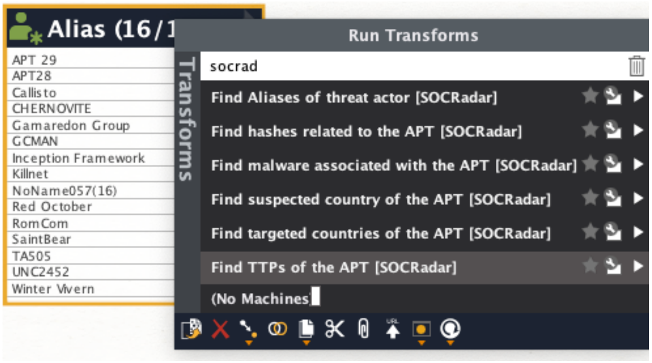
Detail View

Sync Selection to Graph


DustSquad
Callisto
FIN7
Gamaredon Group
APT28
GCMAN
Russian Federation
UNC2452
RomCom
NoName057(16)
Ukraine
Winter Vivern
Inception Framework
Killnet
SaintBear
CHERNOVITE
Red October
APT 29
WIZARD SPIDER
TA505
Run Transforms
socrad
Find Aliases of threat actor [SOCRadar]
Find hashes related to the APT [SOCRadar]
Find malware associated with the APT [SOCRadar]
Find suspected country of the APT [SOCRadar]
Find targeted countries of the APT [SOCRadar]
Find TTPs of the APT [SOCRadar]
(No Machines)
Copy to New Graph

Step 3 – Extracting TTPs

- **Overview:** As we focus on a specific group of threat actors, our goal is to identify and understand any commonalities and anomalies that may exist among them. This will help us better comprehend their operations and potential vulnerabilities.
- **Maltego task:** Select the Alias Entities representing the threat actors and run the Transform **Find TTPs of the APT [SOCRadar]**.



Alias (16/1

APT 29
APT28
Callisto
CHERNOVITE
Gamaredon Group
GCMAN
Inception Framework
Killnet
NoName057(16)
Red October
RomCom
SaintBear
TA505
UNC2452
Winter Vvern

Transforms

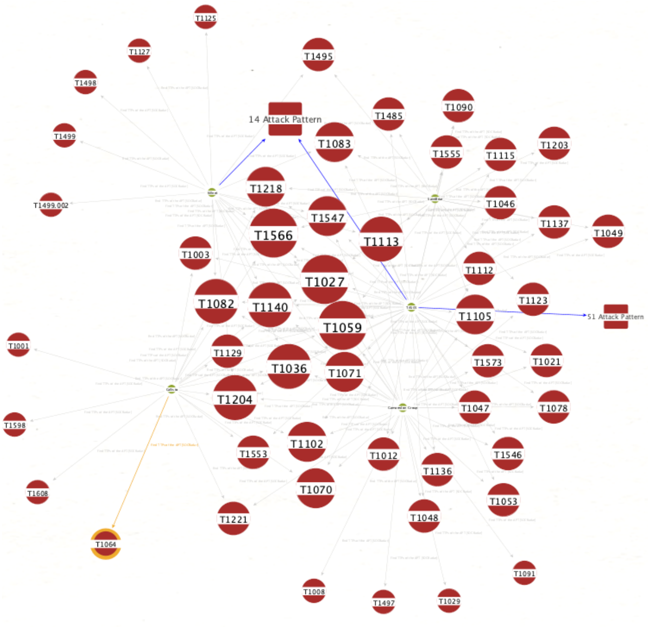
Run Transforms

socrad

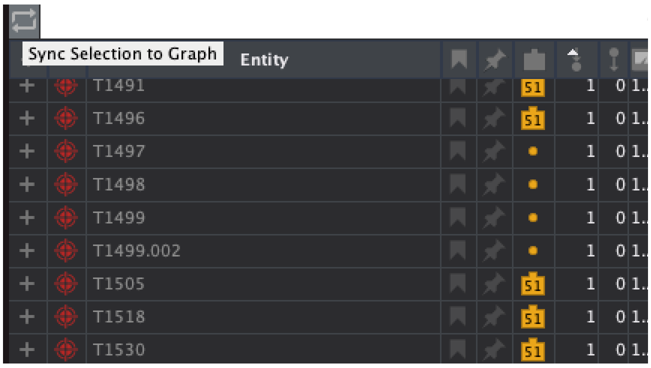
Find Aliases of threat actor [SOCRadar]
Find hashes related to the APT [SOCRadar]
Find malware associated with the APT [SOCRadar]
Find suspected country of the APT [SOCRadar]
Find targeted countries of the APT [SOCRadar]
Find TTPs of the APT [SOCRadar]
(No Machines)

This action will populate AttackPattern Entities within our graph, highlighting instances where certain behaviors are shared, which was expected. Now let's delve deeper into understanding these connections.

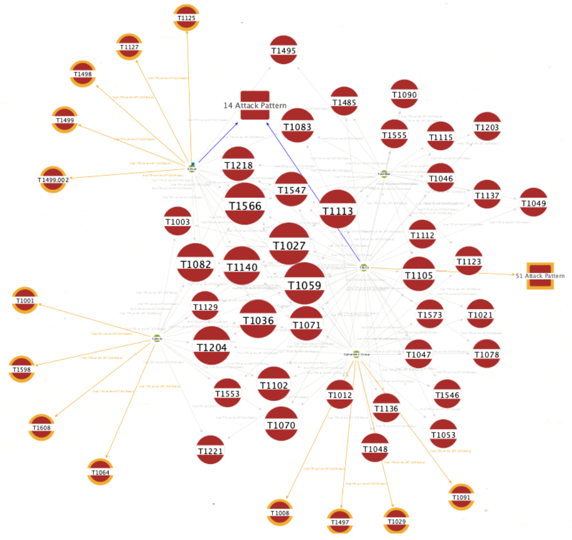
Subsequently, we can then switch to Organic View and opt for a Viewlet that increases the size of Entities in proportion to the volume of incoming links (representing more referenced TTPs).



When navigating to the Detail View, we can observe that certain TTPs are exclusively linked to a single Threat Actor, while others may have multiple associations.

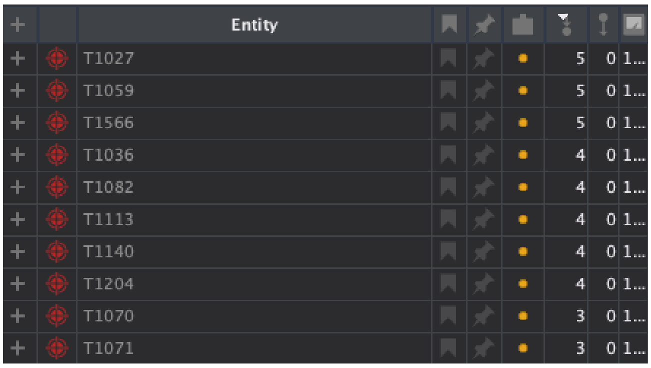


Entity					
T1491	51	1	0	1..
T1496	51	1	0	1..
T1497	●	1	0	1..
T1498	●	1	0	1..
T1499	●	1	0	1..
T1499.002	●	1	0	1..
T1505	51	1	0	1..
T1518	51	1	0	1..
T1530	51	1	0	1..

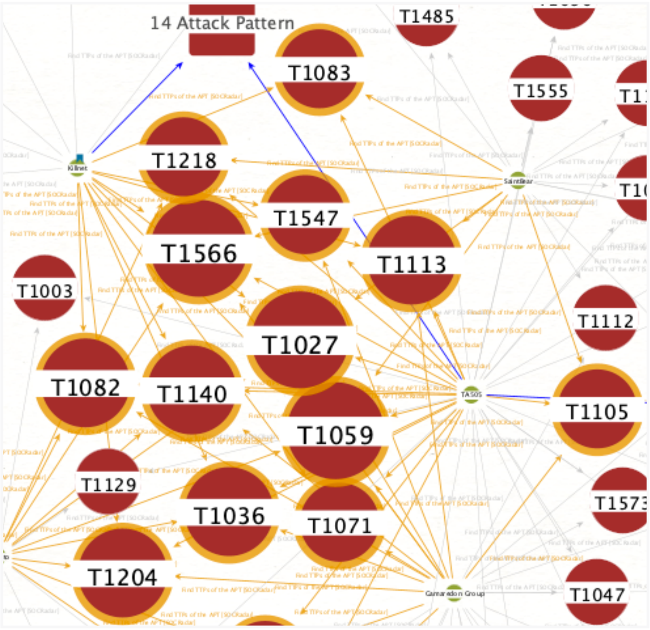


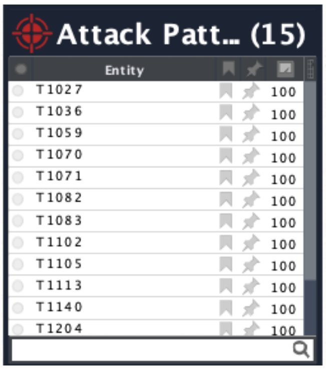
4. Step 4 – Understanding Top TTPs

- **Overview:** We aim to understand which TTPs are most commonly utilized by these threat actors.
- **Maltego task:** Select the AttackPattern Entities with more than 3 incoming links in the Detail View and copy them to a new graph.



Entity				
T1027	●	5	0	1...
T1059	●	5	0	1...
T1566	●	5	0	1...
T1036	●	4	0	1...
T1082	●	4	0	1...
T1113	●	4	0	1...
T1140	●	4	0	1...
T1204	●	4	0	1...
T1070	●	3	0	1...
T1071	●	3	0	1...





Entity	
T1027	100
T1036	100
T1059	100
T1070	100
T1071	100
T1082	100
T1083	100
T1102	100
T1105	100
T1113	100
T1140	100
T1204	100

This will offer a solid starting point for further exploration. We can pivot these TTPs into Threat Intelligence Platforms like MISP, OpenCTI, or other emerging datasets focused on cybersecurity functions such as Detection and Threat Actor Simulation. Many of these resources, including those from MITRE ATT&CK and other industry initiatives, can be seamlessly integrated into Maltego through APIs and the TAXII protocol. Stay tuned for these updates!

Playbook using SOCRadar and Cybersixgill

Building on our analysis of attacks and TTPs in use case 5, we will introduce another playbook to obtain detailed information about a specific threat actor within our threat landscape. We will use the same starting point but incorporate an additional data provider, Cybersixgill, to enhance our investigation.

Goal

To collect in-depth analysis about a specific threat actor in our threat landscape.

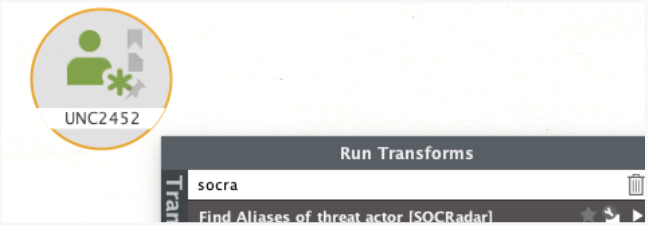
Starting Point

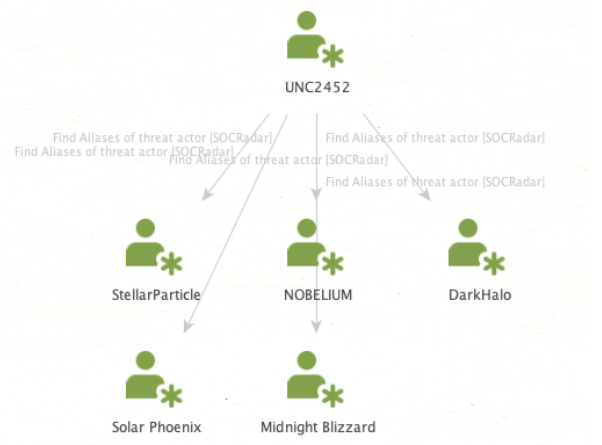
Country

Playbook

Step 1 – Starting off

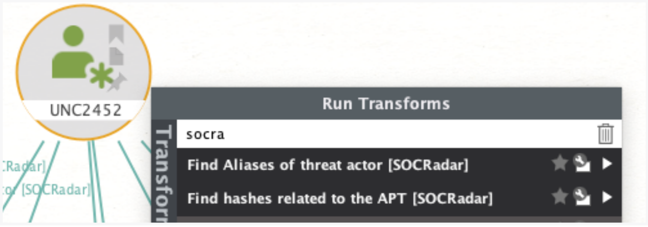
- **Overview:** We would like to identify other aliases used by the threat actor (UNC2452).
- **Maltego task:** Drop the name of the threat actor into Maltego and then run Transform **Find Aliases of Threat Actor [SOCRadar]**



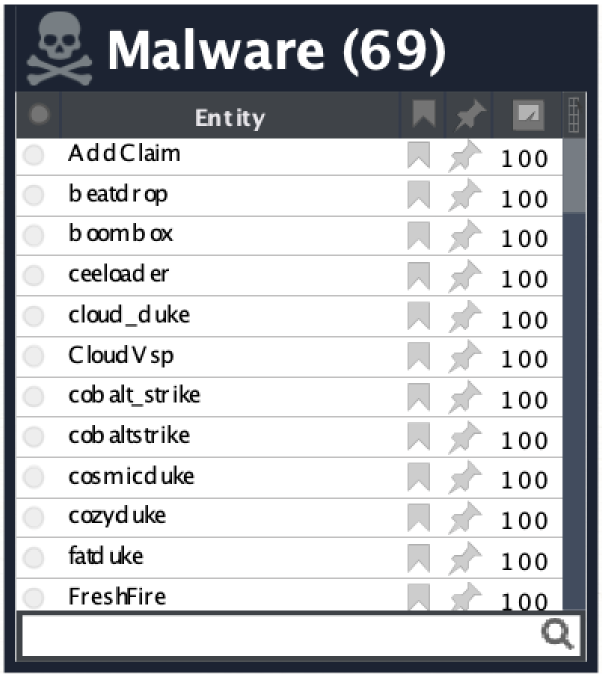

UNC2452
Find Aliases of threat actor [SOCRadar]
Find Aliases of threat actor [SOCRadar]
Find Aliases of threat actor [SOCRadar]
Find Aliases of threat actor [SOCRadar]
Find Aliases of threat actor [SOCRadar]
StellarParticle
NOBELIUM
DarkHalo
Solar Phoenix
Midnight Blizzard

Step 2 – Extracting Indicators

- **Overview:** In this step, we aim to discover additional information on the indicators, including hashes, tools, and any other relevant data.
- **Maltego task:** Select the threat actor (UNC2452) and run transform **Find Malware associated with the APT [SOCRadar]**.

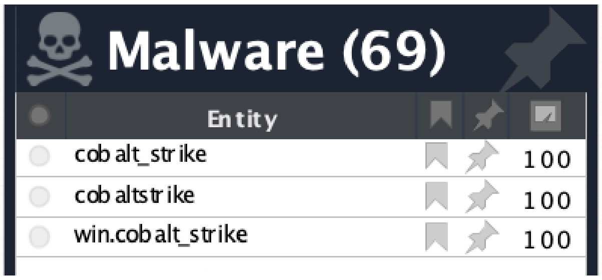

UNC2452
[SOCRadar]
Transforms
Run Transforms
socra
Find Aliases of threat actor [SOCRadar]
Find hashes related to the APT [SOCRadar]

We can see that various malware types are associated with the threat actor. This can be filtered from the collection using a specific keyword like "cobalt," which stands for "Cobalt Strike."



Malware (69)

Entity	
AddClaim	100
beatdrop	100
boombox	100
ceeloader	100
cloud_duke	100
CloudVsp	100
cobalt_strike	100
cobaltstrike	100
cosmicduke	100
cozyduke	100
fatduke	100
FreshFire	100



Malware (69)

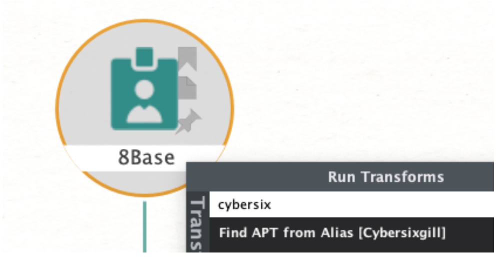
Entity	
cobalt_strike	100
cobaltstrike	100
win.cobalt_strike	100

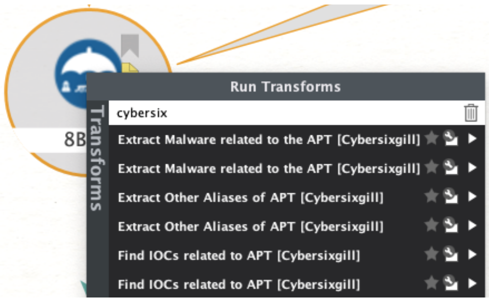
INVESTIGATOR NOTE

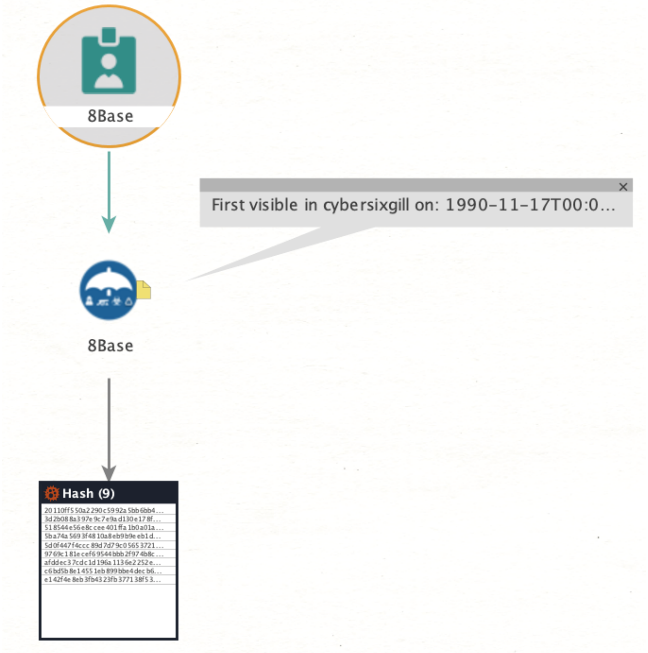
If we run **To hashes** Transform on the threat actor, we will not be able to retrieve any results.

Step 3 – Obtaining Additional Intelligence from Related Threat

- **Overview:** We would like to obtain additional intelligence in this step.
- **Maltego task:** Drop the name of the threat actor into Maltego and then run transform **Find APT from Alias [Cybersixgill]**




8B
Run Transforms
Transforms
cybersix
Extract Malware related to the APT [Cybersixgill]
Extract Malware related to the APT [Cybersixgill]
Extract Other Aliases of APT [Cybersixgill]
Extract Other Aliases of APT [Cybersixgill]
Find IOCs related to APT [Cybersixgill]
Find IOCs related to APT [Cybersixgill]



First visible in cybersixgill on: 1990-11-17T00:0...

```
20110ff550a2290c5992a5bb6bb4...
3d2b088a397e9c7e9ad130e178f...
518544e56e8ccee401ffa1b0a01a...
5ba74a5693f4810a8eb9b9eeb1d...
5d0f447f4ccc89d7d79c05653721...
9769c181ecef69544bbb2f974b8c...
afddec37cdc1d196a1136e2252e...
c6bd5b8e14551eb899bbe4decb6...
e142f4e8eb3fb4323fb377138f53...
```

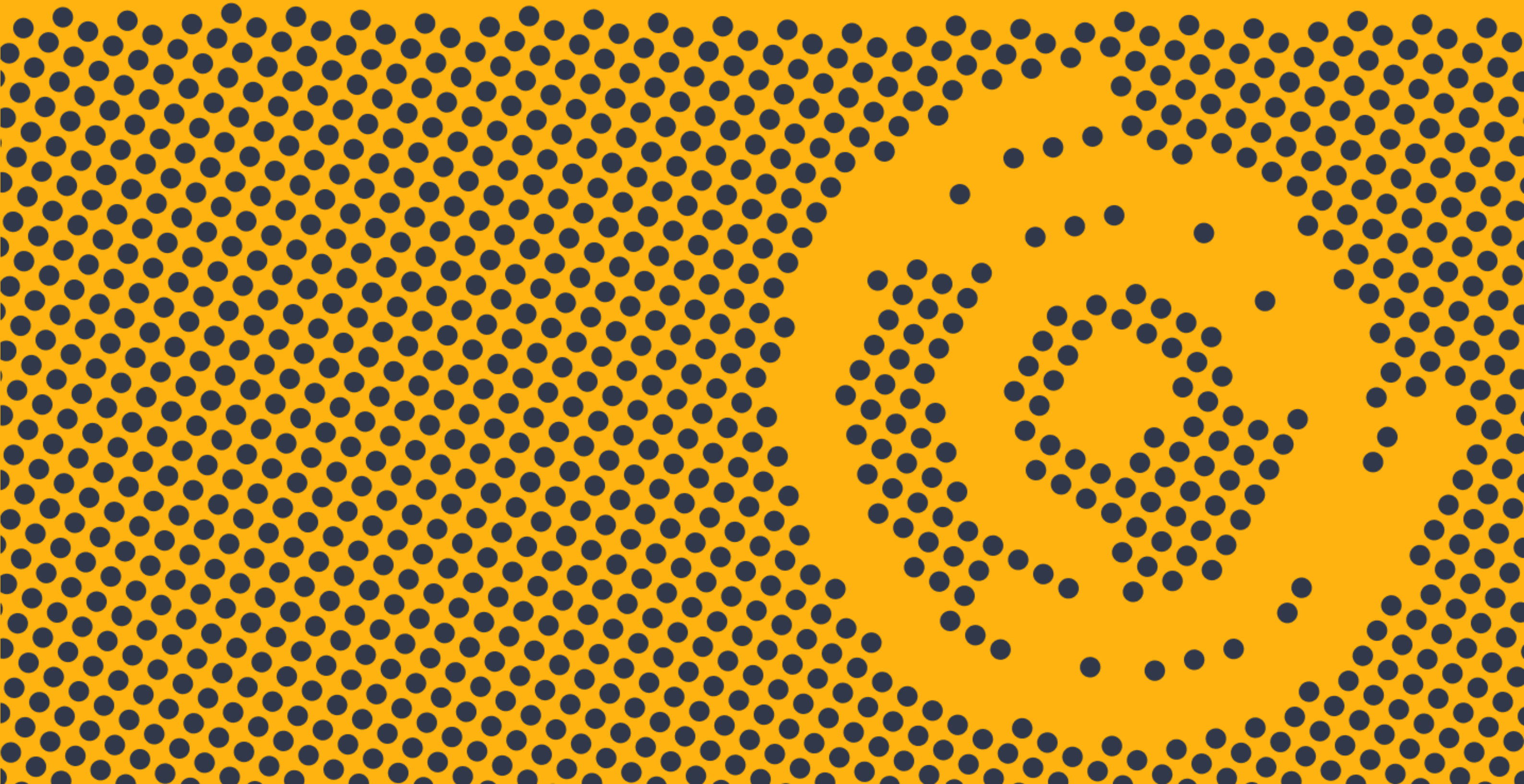
The steps described enable us to pivot the identified TTPs into various Threat Intelligence Platforms, such as MISP, OpenCTI, or those focusing on malware intelligence like VirusTotal. All these platforms can be effortlessly integrated into Maltego, facilitating a streamlined process that spans the entire threat intelligence lifecycle—from collection and processing to analysis.

This concludes our handbook. Dive into a world where data-driven security decisions enhance your cybersecurity efforts. Discover our unique offerings and elevate your security with the world's most used cyber investigation platform today!

Learn more about how we can empower your investigations at **maltego.com**

Maltego is the all-in-one investigation platform that accelerates complex cyber investigations from hours to minutes. The Maltego platform powers preliminary quick OSINT investigations for digital profiling with Maltego Search as well as complex link analysis for large datasets with Maltego Graph. Through Maltego Evidence and Maltego Monitor, the platform enables investigators to collect, monitor, and preserve social media intelligence real-time for prosecution and public safety. Whether cyber threat intelligence teams or law enforcement, Maltego equips your teams with the most essential and relevant data, with out-of-the-box access to common data sources and over 100 ready-made connectors to more. Mine, merge, and map all your essential intelligence in one place, and uncover hidden truths with Maltego!

MINE • MERGE • MAP / DATA



Email: contact@maltego.com
Phone: +49-89-24418490

MALTEGO