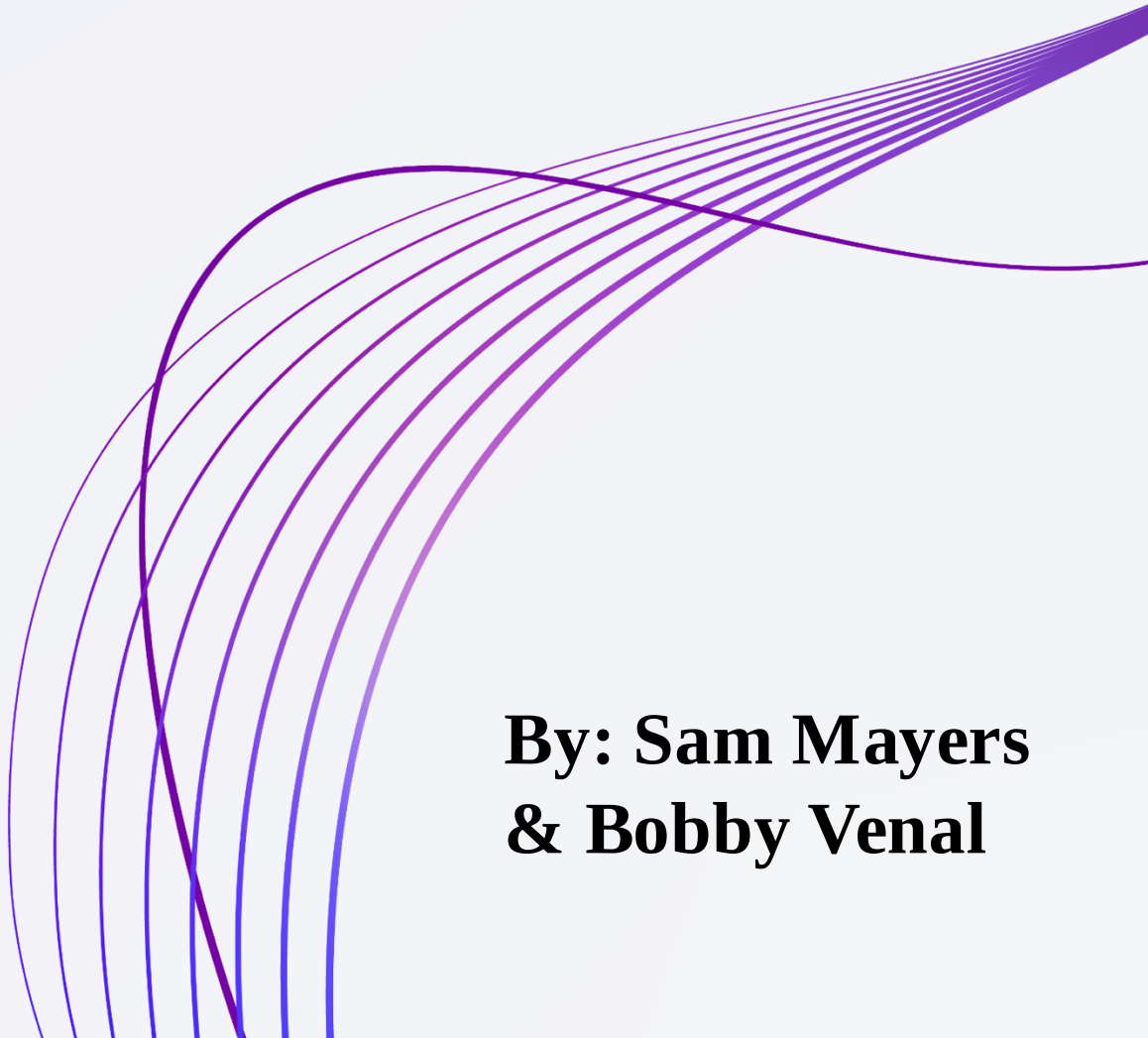
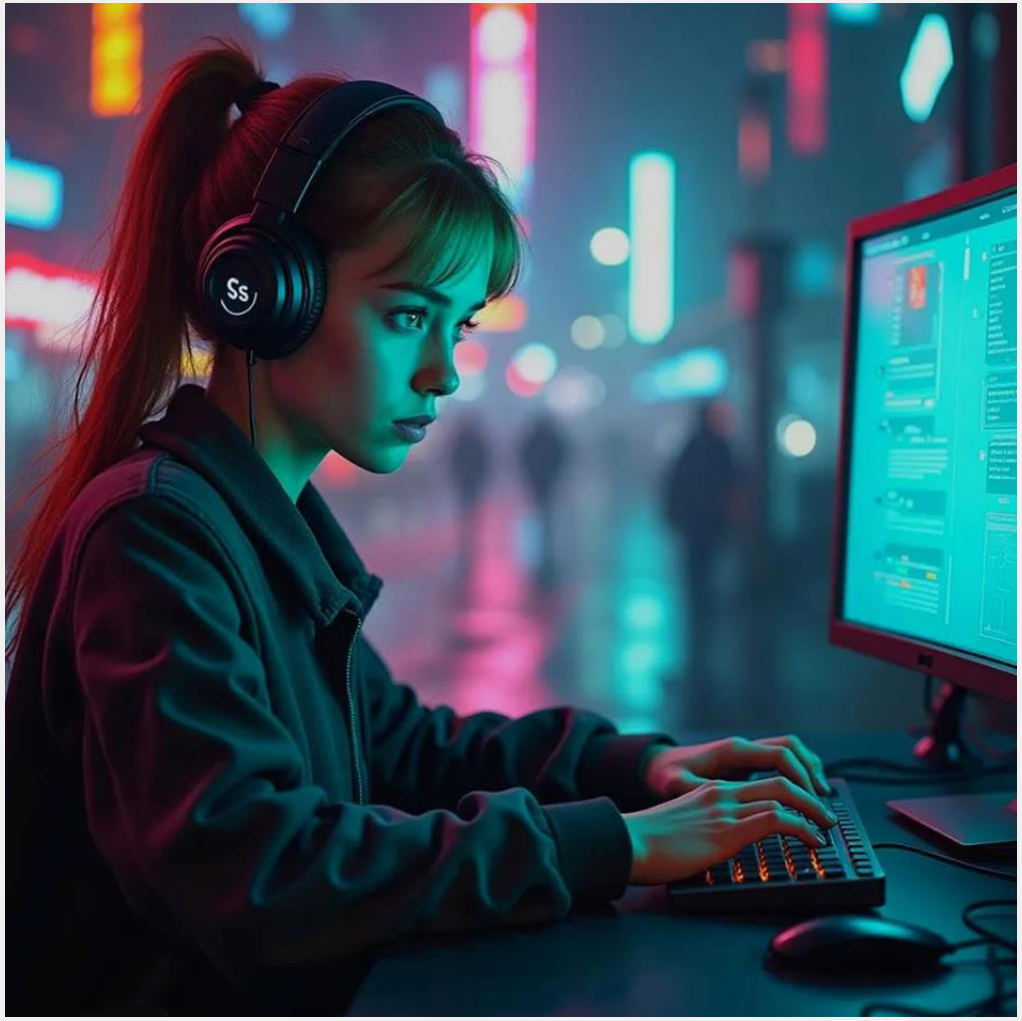
Introduction to Cyber Threat Intelligence (CTI)



By: Sam Mayers
& Bobby Venal



whoami

- @xprotectszn (or fire)
- LinkedIn
- Security Researcher
- Sam.mayers.is
- Run 2 nonprofits
  - Physical Security Village (Defcon)
  - ClearSear.ch
- Baking and Hiking

whoami

- @lsl_bobby
- Sam’s boss

Who are Beazley Security

- ~4,000 incidents per year
- >50,000 policy holders in 73 countries
- Tens of thousands endpoints monitored
- All 100% focused on reducing risk and increasing cyber resilience
- Located across Americas, Europe, UK, and Asia Pacific

http://ccsc.c2society.org/

Agenda

1. Introduction to Cyber Threat Intelligence (CTI)
2. CTI Lifecycle and Intelligence Process
3. Indicators of Compromise and Threat Indicators
4. Threat Actor Profiling
5. Threat Intelligence Platforms
6. Data Enrichment and Correlation in Cyber Threat Intelligence
7. Collaborative Threat Intelligence Sharing
8. Tools
9. Intro to Malware Analysis (if time)

Introduction to Cyber Threat Intelligence (CTI)

Overview of CTI

"Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes." - NIST

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Cyber Threat Intelligence (CTI) is the practice of gathering, analyzing, and sharing information about cyber threats, including their origins, motives, and capabilities. The primary goal of CTI is to provide actionable insights that help organizations understand, anticipate, and respond to cyber threats effectively.

Significance in the Cybersecurity Landscape

- Proactive Defense
- Enhanced Incident Response
- Informed Decision-Making
- Collaboration and Information Sharing
- Importance in the Modern Era

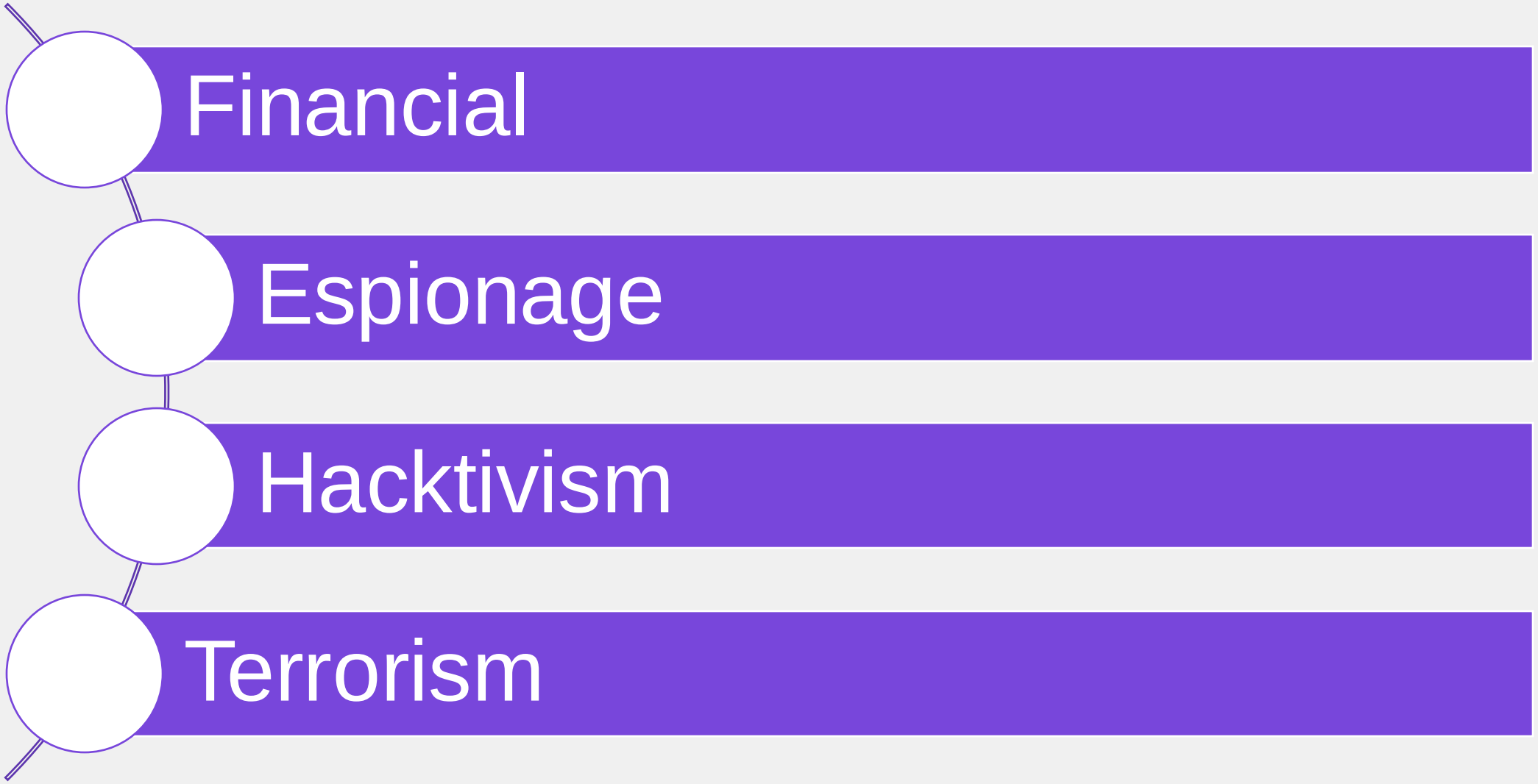
Types of Threat Intelligence

Type	Scope	Audience	Purpose	Examples
Strategic	High-level trends	Executives, policymakers	Long-term planning	Nation-state cyber threats
Tactical	TTPs and adversary methods	SOC analysts, responders	Improve defense mechanisms	Phishing tactics, MITRE ATT&CK mappings
Operational	Campaign-specific insights	Incident response teams	Contextual understanding	Ransomware campaigns targeting healthcare
Technical	Detailed IoCs and artifacts	Analysts, automated tools	Immediate threat mitigation	Malicious IPs, file hashes

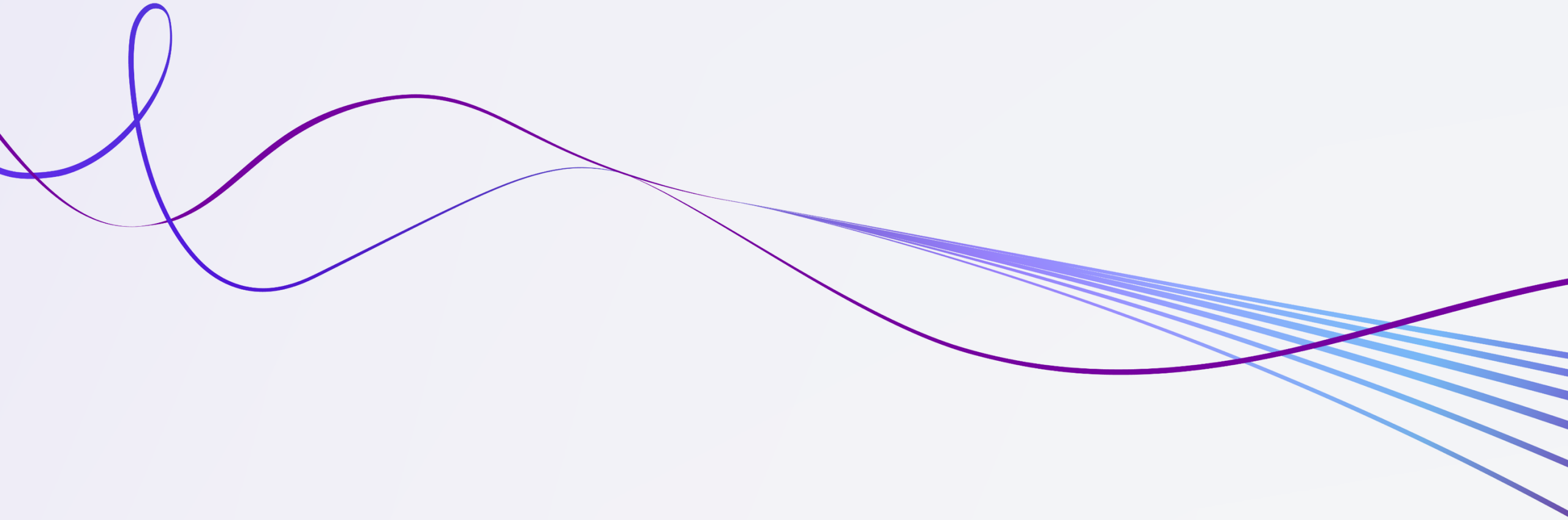
Current Threat Landscape:

- Ransomware (RaaS)
- Supply chain attacks
- Phishing campaigns
- Critical vulnerabilities
- State-sponsored attacks

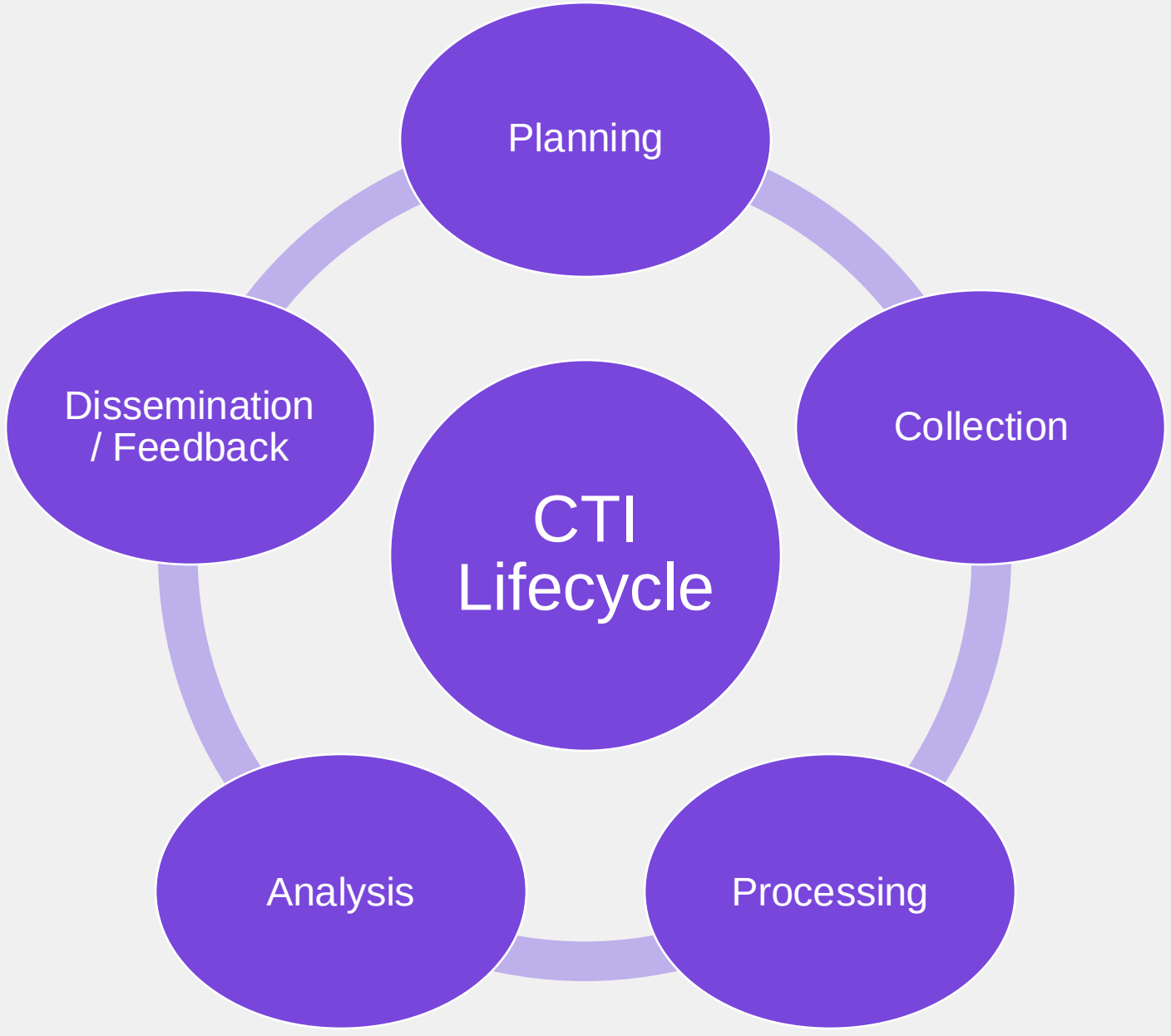
Current Threat Landscape:



Questions on CTF platform



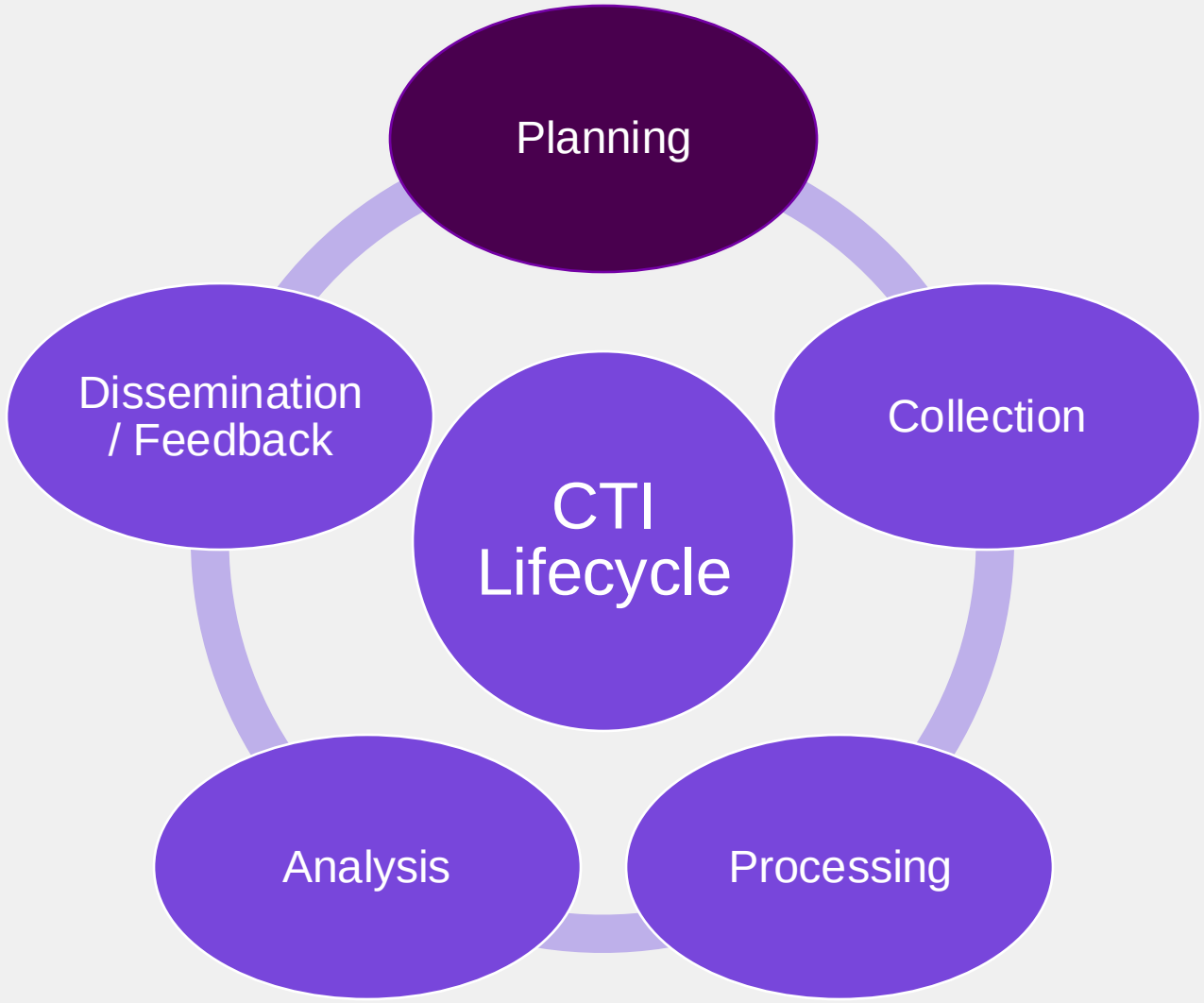
CTI Lifecycle and Intelligence Process


Planning
Collection
Processing
Analysis
Dissemination / Feedback
CTI Lifecycle

CTI Lifecycle

Planning

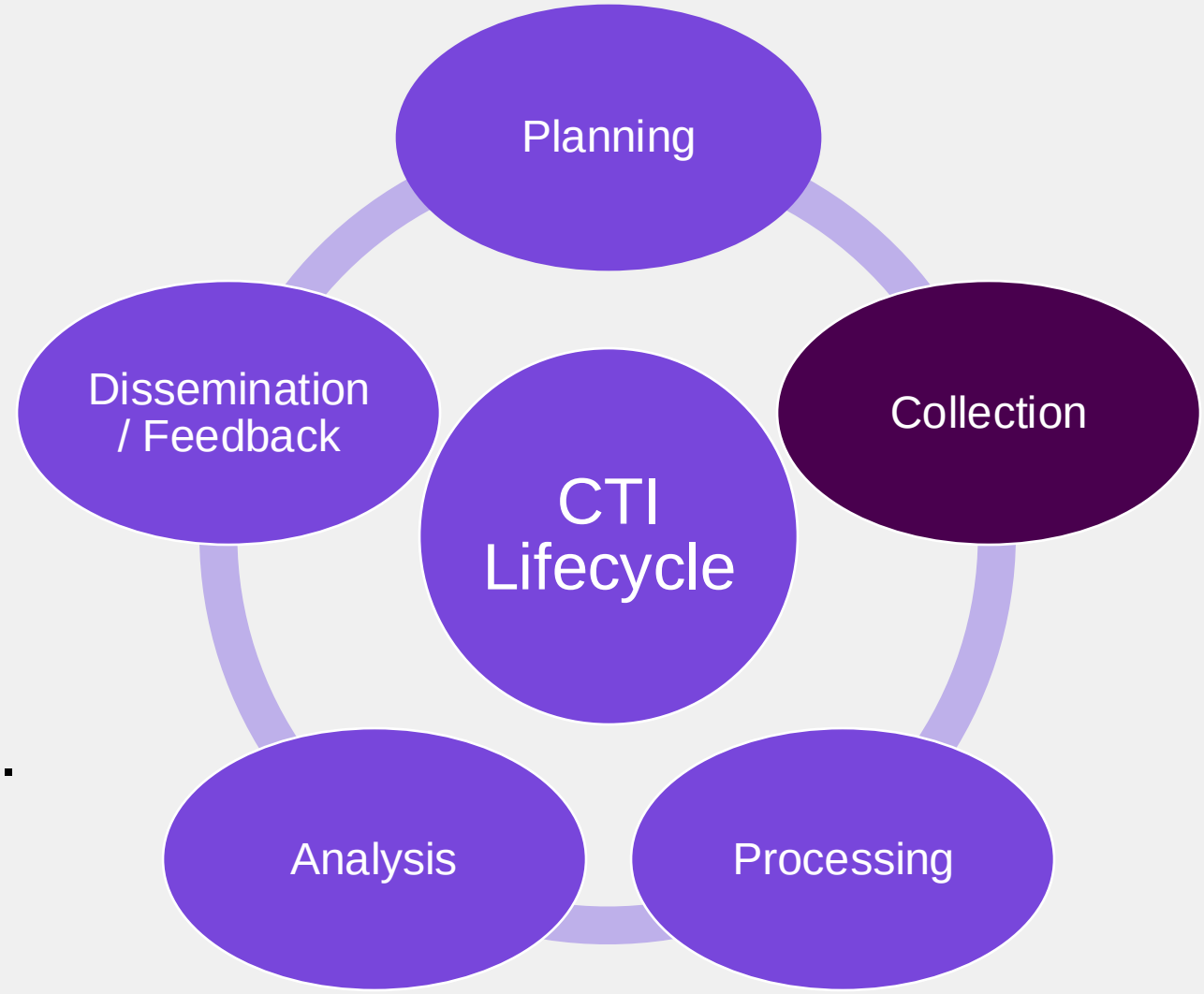
- Identify the organization's intelligence needs, priorities, and goals.
- Establish key questions the intelligence should answer
  - Which threat actors are targeting our industry?



CTI Lifecycle

Collection

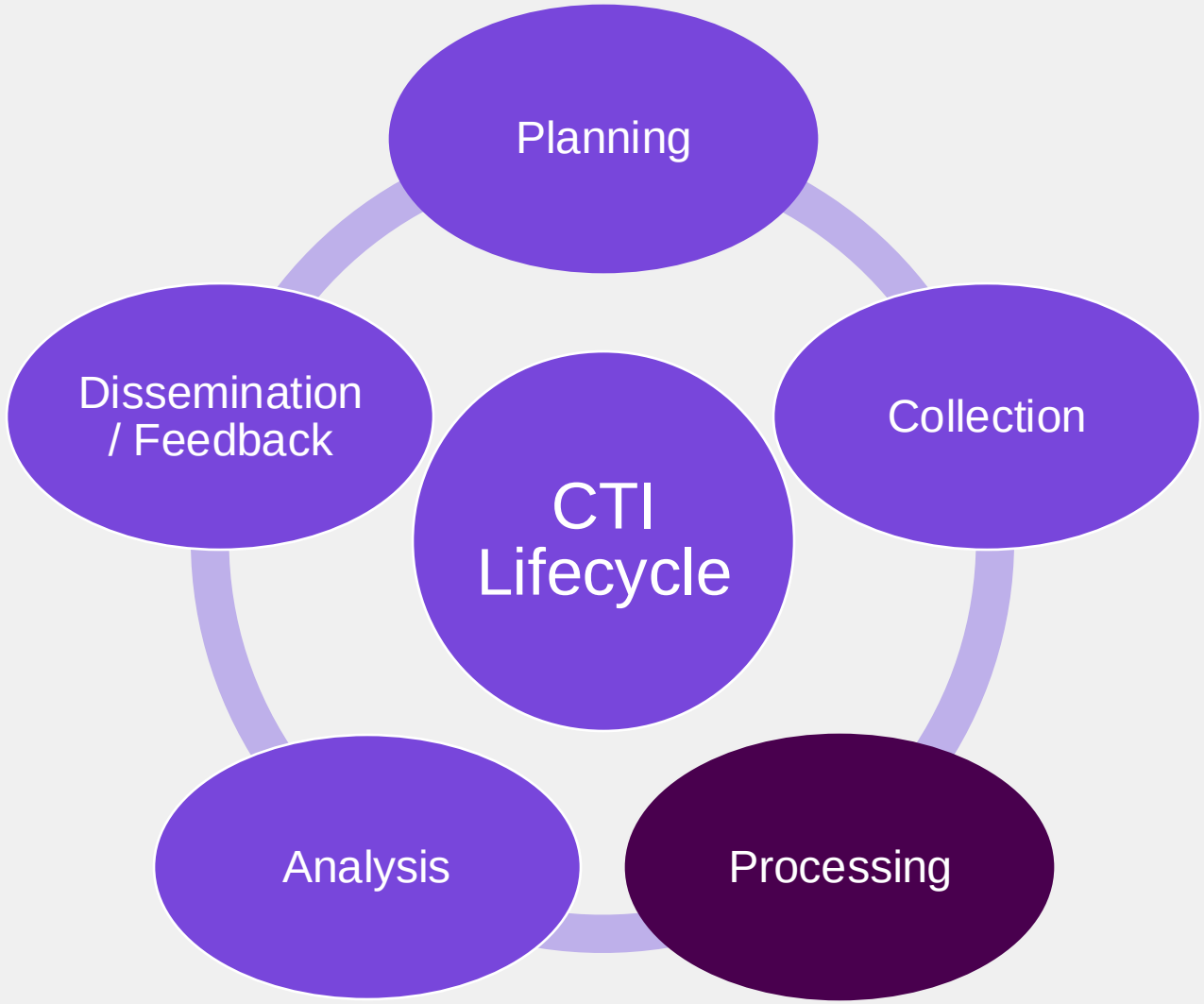
- Gathering raw data from relevant sources to answer the intelligence questions defined in the planning stage.
- Tools - VirusTotal, Shodan, GreyNoise, Logs, Recorded Future.



CTI Lifecycle

Processing

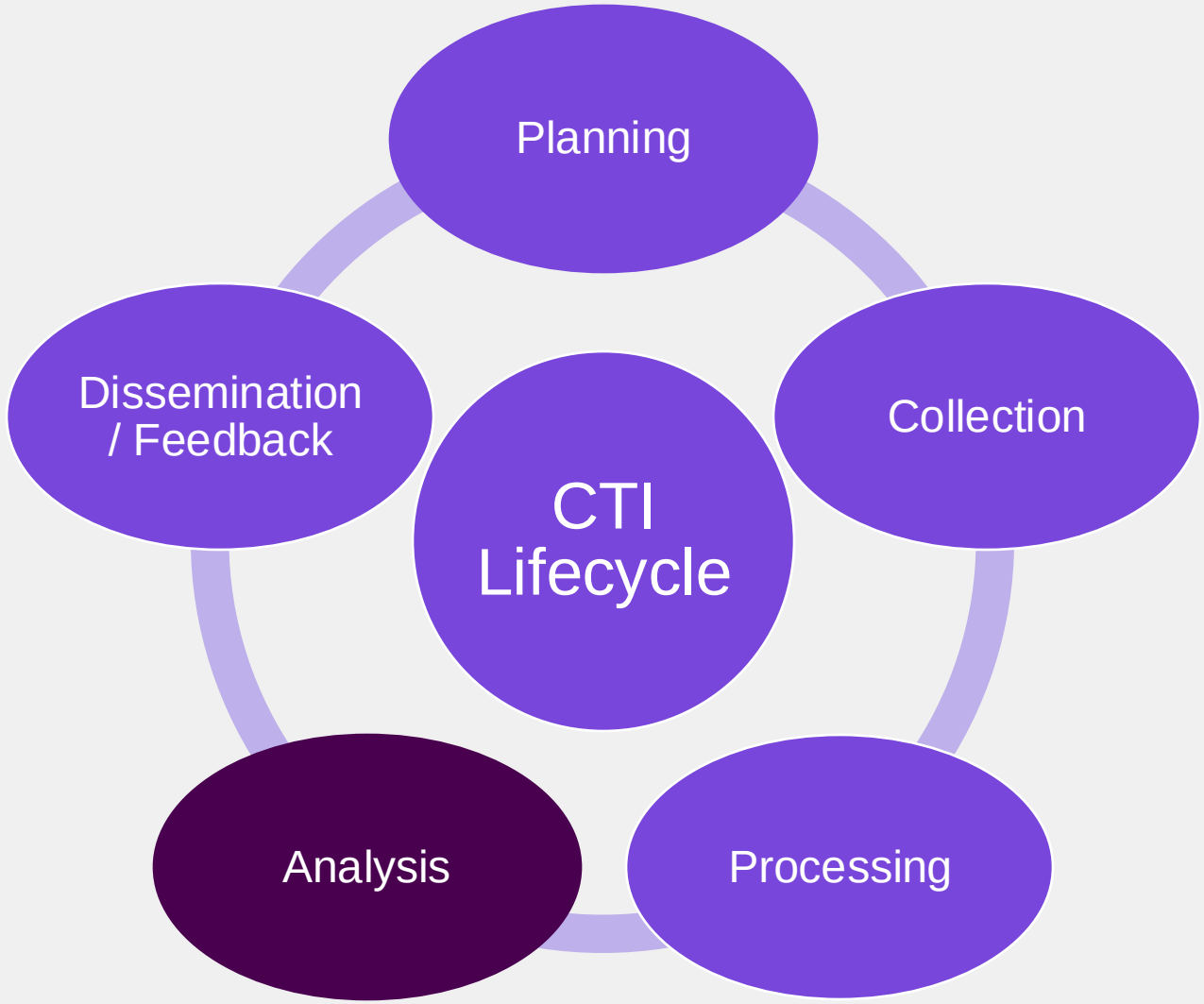
- Converting raw data into a standardized, structured format for easier analysis.
- De-duplicate and parse data IoCs.
- Clean, organized, and relevant data ready for analysis.



CTI Lifecycle

Analysis

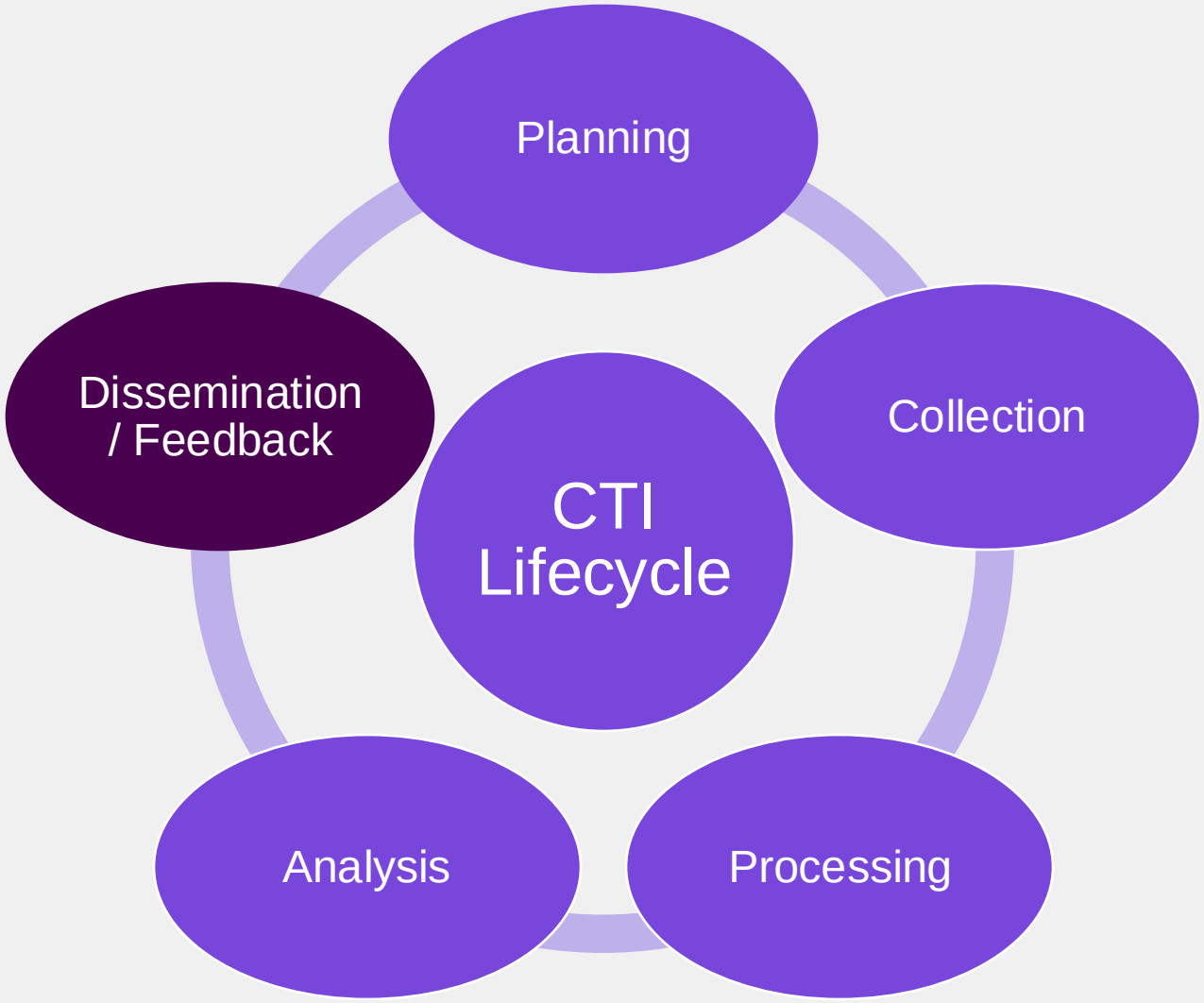
- Interpreting processed data to derive actionable insights and answer intelligence questions.
- Correlate IoCs with known TTPs or campaigns.
- Identify trends, patterns, and potential threats specific to the organization.



CTI Lifecycle

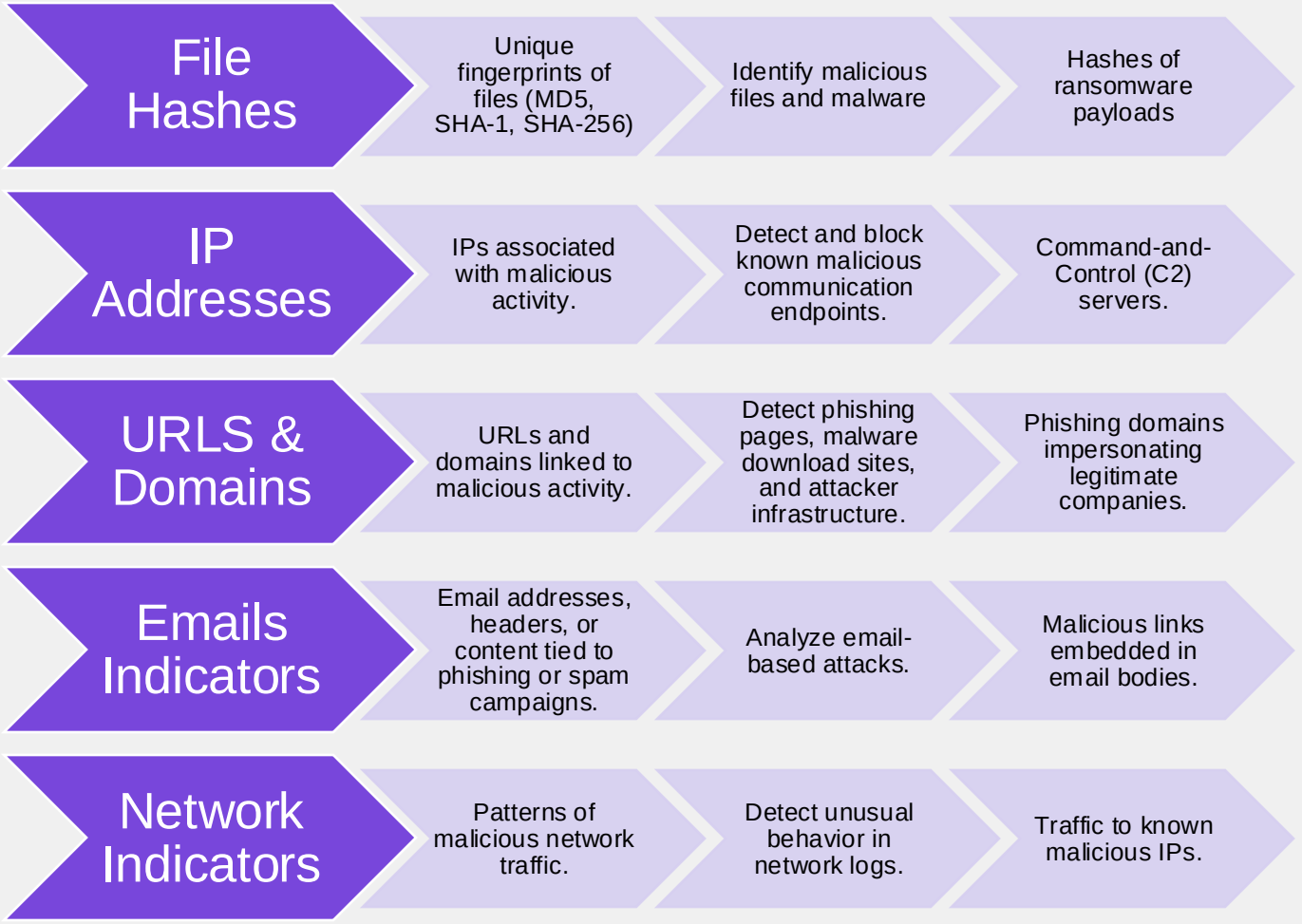
Dissemination

- Sharing the derived intelligence with relevant stakeholders in a timely and accessible format.
- Generate reports or dashboards tailored to specific audiences.
- Integrate intelligence into detection systems.



Indicators of Compromise and Threat Indicators

Indicators of Compromise (IoCs)



TTPs (Tactics, Techniques, and Procedures)

- **Tactics, Techniques, and Procedures (TTPs)** describe the *how* and *why* behind adversarial behavior:
  - **Tactics**: High-level goals attackers aim to achieve during a campaign.
  - **Techniques**: Specific methods used to accomplish those goals.
  - **Procedures**: Variations or implementations of techniques, tailored to specific environments or objectives.

Mapping TTPs to MITRE ATT&CK

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

- An open framework that documents and categorizes TTPs observed in real-world cyberattacks. It provides a structured knowledge base for understanding, detecting, and responding to adversarial behavior.

MITRE ATT&CK Website

Structure of MITRE ATT&CK

- **Tactics**:
  - Represent the *why* behind an adversary's action (the goal they aim to achieve at a specific stage of the attack).
  - Examples:
    - **Initial Access**: How attackers infiltrate a network.
    - **Persistence**: How attackers maintain their presence after initial compromise.
    - **Privilege Escalation**: How attackers gain higher-level permissions.

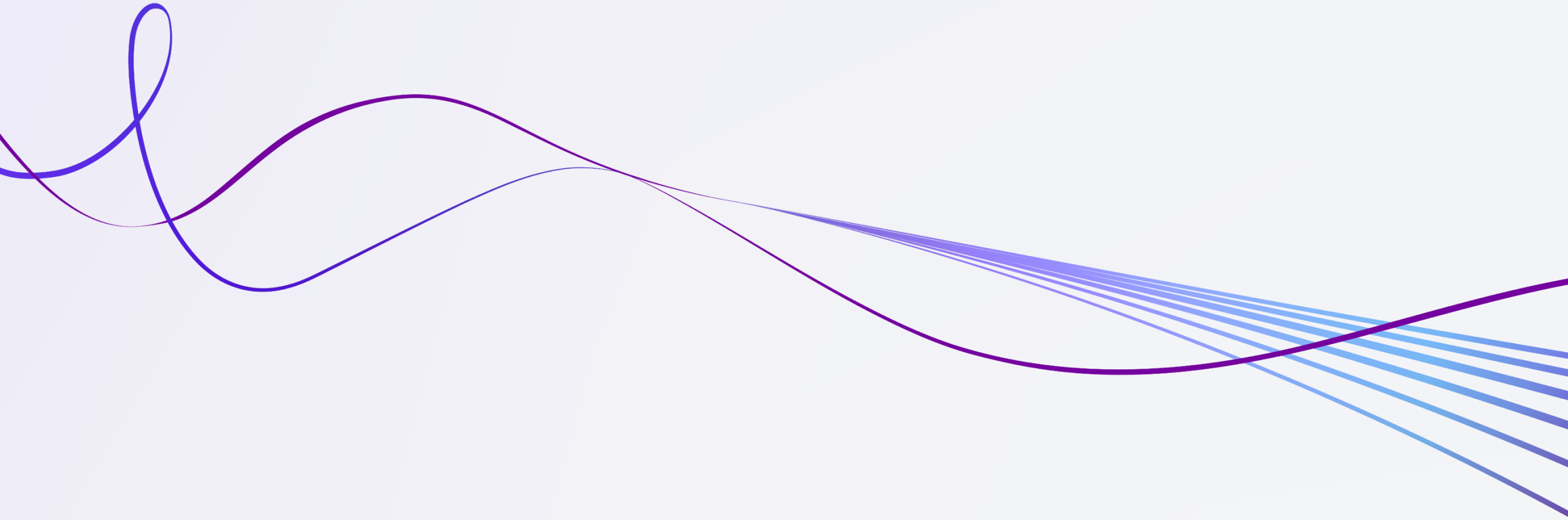
Structure of MITRE ATT&CK

- **Techniques**:
  - Represent the *how* attackers achieve a specific goal (tactic).
  - Examples:
    - **Phishing (T1566)**: Delivering malicious emails to trick users into providing credentials or executing malware.
    - **Credential Dumping (T1003)**: Extracting stored credentials from compromised systems.

Structure of MITRE ATT&CK

- **Sub-Techniques**:
  - Provide more granular details about techniques.
  - Example:
    - **Spear Phishing Attachment (T1566.001)**: Sending a malicious email with an attachment to exploit a vulnerability or trick the user.
    - **Masquerade Task or Service (T1036.004):** Adversaries modify the properties of legitimate tasks or services to disguise malicious activity.

Questions on CTF platform



Threat Actor Profiling

Threat Actor Profiling

Threat Actor Profiling involves analyzing and documenting the characteristics, motivations, and methodologies of adversaries to better understand their behavior and anticipate their actions.

By profiling threat actors, organizations can develop proactive defenses and tailor their incident response strategies.

Building Threat Actor Profiles

- **Identity**:
  - Known aliases and group names.
  - Example:
    - **APT29 (Cozy Bear)**
    - **FIN7**
- **Motivations**:
  - Why the actor conducts attacks.
  - Examples:
    - **Financial gain** (cybercriminal groups like FIN7).
    - **Espionage** (state-sponsored groups like APT28).
    - **Hacktivism** (groups like Anonymous).
    - **Terrorism** (groups leveraging attacks to instill fear).

Building Threat Actor Profiles

- **Objectives**:
  - Typical targets and goals.
  - Examples:
    - Stealing intellectual property or government secrets.
    - Disrupting critical infrastructure.
    - Deploying ransomware for financial extortion.
- **Methodologies (TTPs)**:
  - How the actor operates, including tactics, techniques, and procedures (TTPs).
  - Use frameworks like **MITRE ATT&CK** to categorize:
    - Initial access (e.g., phishing).
    - Persistence (e.g., creating scheduled tasks).
    - Exfiltration (e.g., data compression and transfer).

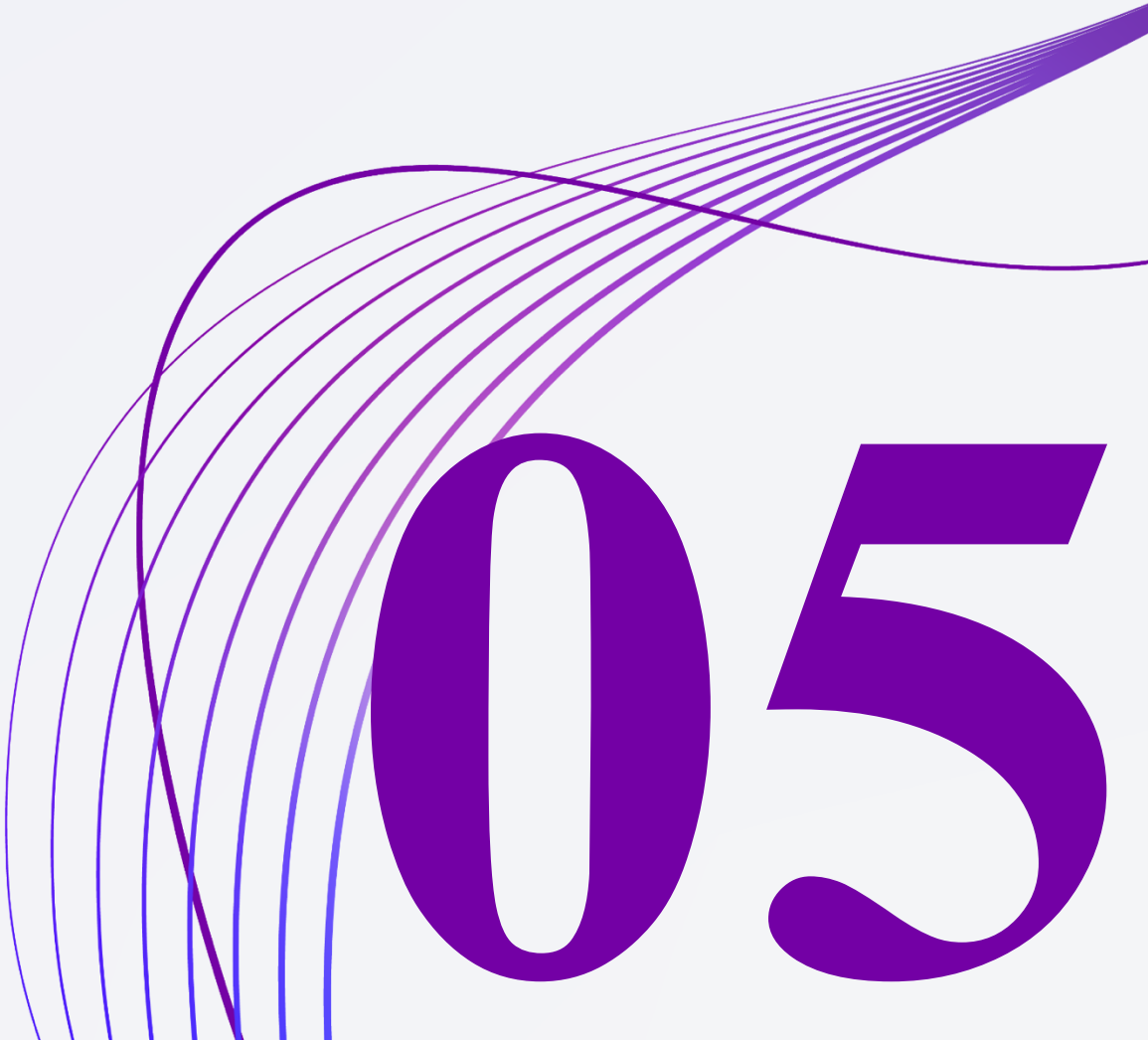
Building Threat Actor Profiles

- **Tools**:
  - Malware, exploits, and frameworks used.
  - Examples:
    - **Cobalt Strike**
    - **Mimikatz**
    - Custom-built malware like **Drovorub**.
- **Infrastructure**:
  - Command-and-Control (C2) servers, domains, IP addresses.
  - Examples:
    - Domain names registered to impersonate legitimate organizations.

Building Threat Actor Profiles

- **Geopolitical Context**:
  - State-sponsored actors often align their campaigns with national interests.
  - Example:
    - **APT41**, a Chinese group, blends espionage and cybercrime.
- **Known Campaigns**:
  - Past attack campaigns, including victims and methods used.
  - Example:
    - **NotPetya** ransomware by Russian actors targeting Ukraine.

Threat Intelligence Platforms (TIPs)



Threat Intelligence Platforms (TIPs)

- Threat Intelligence Platforms (TIPs) are centralized systems designed to collect, process, analyze, and share threat intelligence data.
- These platforms help security teams manage Indicators of Compromise (IoCs), correlate threat data, and automate intelligence workflows.

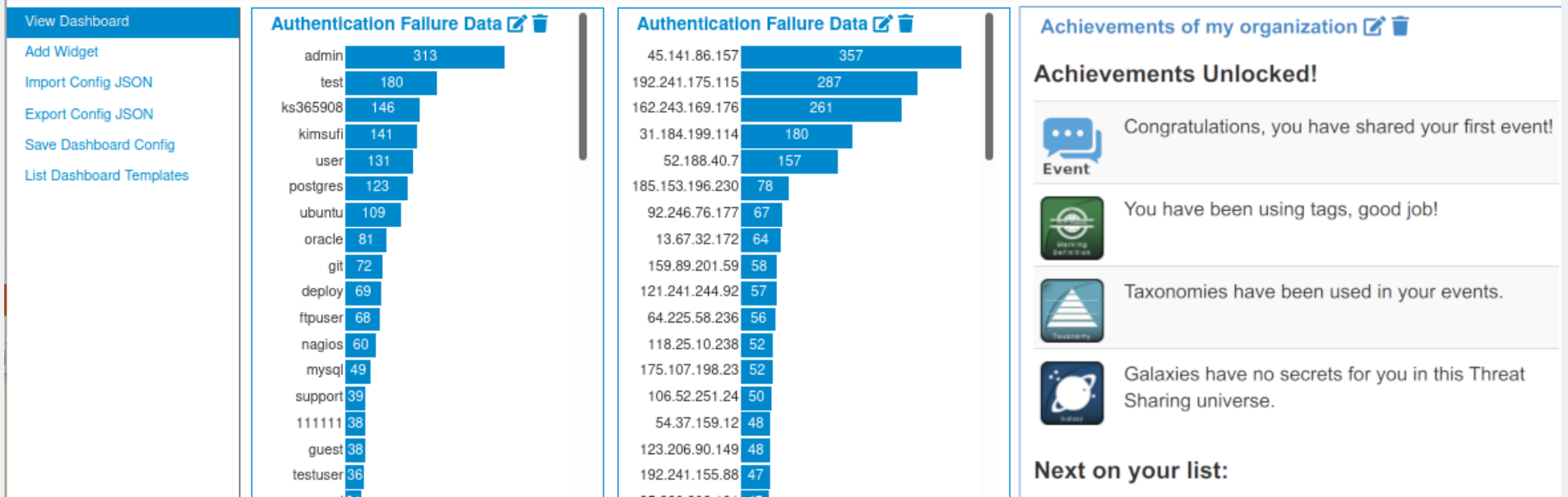
Why Use TIPs?

- **Centralized threat intelligence management**
  - Store and analyze IoCs in one place.
- **Collaboration and sharing**
  - Enable information sharing among organizations, ISACs, and security communities.
- **Automation**
  - Integrate with Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR), and Security Orchestration, Automation, and Response (SOAR) solutions.
- **Threat correlation**
  - Identify patterns and relationships between different threats.

Popular Threat Intelligence Platforms

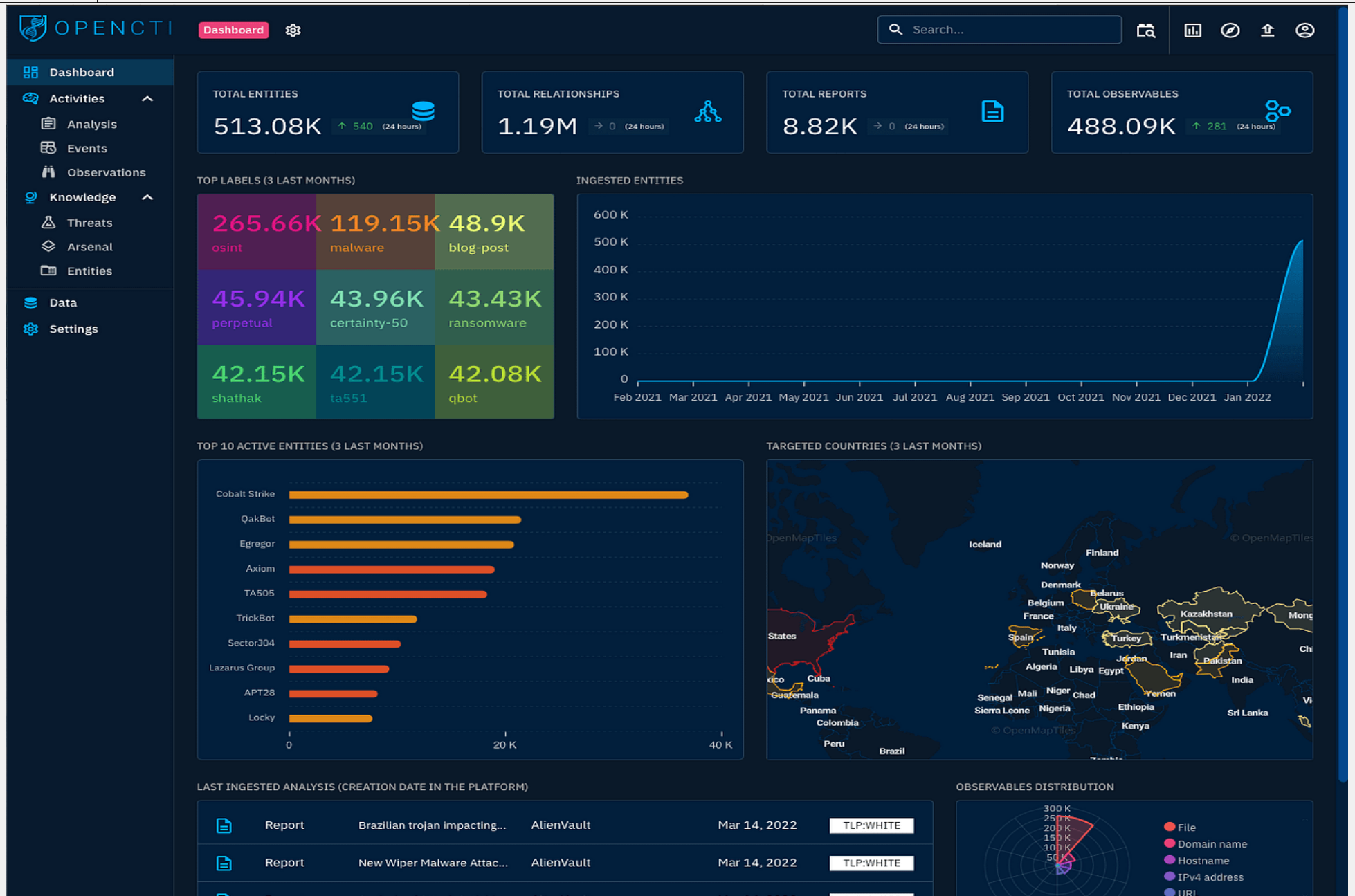
- **MISP (Malware Information Sharing Platform)**
  - Open-source platform widely used by government agencies, CSIRTs, and enterprises.
  - Supports STIX/TAXII for structured threat intelligence sharing.
  - Features event-based organization, correlation, and visualization of IoCs.


Malicious activities
Event ID 10878
Uuid 5aec700c-0eb8-468
Org CIRCL
Owner org CIRCL
Contributors
Email alexandre.dulaunoy(
Tags
Date 2018-05-04
Threat Level Low
Analysis Initial
Distribution All communities
Info Malicious activities
Published No
#Attributes 2
Last change 2018/05/04 02:38:12
Extends
Extended by
Sightings 0 (0)
Activity
Pivots Galaxy Event graph
10878: Malici...
Distribution graph [atomic event]
Your organisation only
This community only
Connected communities
All communities
Sharing group
All Attributes Object attributes
Your organisation only
Connected communities
This community only
All communities
Sharing group
Event not distributed to any sharing group
Display
Filters
Threat Level
Low
Analysis
Initial
Event Info
Ransomware found on a production server
Extends event
5ad8687b-0e10-4a8b-a157-46a5950d210f
Matched event
Id: 10728
Analysis: Completed
Threat level: Low
Tags:
circl:osint-feed
tip:white
malware_classification:malware-category="Ransomware"
osint:source-type="blog-post"
misp-galaxy:ransomware="CSGO Ransomware"
misp-galaxy:ransomware="MC Ransomware"
Info: OSINT - Minecraft & CS:GO Ransomware Strive For Media Attention
Collapse node
Edit node
Search for value
Delete selected item
Open contextual menu
attribute: ftp.ftp0118.info
object: ip-port
attribute: down.down0116.info
attribute: 8888
attribute: 209.58.186.145
estimative-language:confidence-in-analytic-judgment="high"
High


View Dashboard
Add Widget
Import Config JSON
Export Config JSON
Save Dashboard Config
List Dashboard Templates
Authentication Failure Data
admin 313
test 180
ks365908 146
kimsufi 141
user 131
postgres 123
ubuntu 109
oracle 81
git 72
deploy 69
ftpuser 68
nagios 60
mysql 49
support 39
111111 38
guest 38
testuser 36
Authentication Failure Data
45.141.86.157 357
192.241.175.115 287
162.243.169.176 261
31.184.199.114 180
52.188.40.7 157
185.153.196.230 78
92.246.76.177 67
13.67.32.172 64
159.89.201.59 58
121.241.244.92 57
64.225.58.236 56
118.25.10.238 52
175.107.198.23 52
106.52.251.24 50
54.37.159.12 48
123.206.90.149 48
192.241.155.88 47
Achievements of my organization
Achievements Unlocked!
Event
Congratulations, you have shared your first event!
You have been using tags, good job!
Taxonomies have been used in your events.
Galaxies have no secrets for you in this Threat Sharing universe.
Next on your list:

Popular Threat Intelligence Platforms

- **OpenCTI (Open Cyber Threat Intelligence Platform)**
  - Designed for strategic, operational, and technical threat intelligence management.
  - Supports structured data ingestion, visualization, and integration with other security tools.
  - Includes TTP mapping and attack campaign tracking.


OPENCTI
Dashboard
Search...
Dashboard
Activities
Analysis
Events
Observations
Knowledge
Threats
Arsenal
Entities
Data
Settings
TOTAL ENTITIES
513.08K
540 (24 hours)
TOTAL RELATIONSHIPS
1.19M
0 (24 hours)
TOTAL REPORTS
8.82K
0 (24 hours)
TOTAL OBSERVABLES
488.09K
281 (24 hours)
TOP LABELS (3 LAST MONTHS)
265.66K osint
119.15K malware
48.9K blog-post
45.94K perpetual
43.96K certainty-50
43.43K ransomware
42.15K shathak
42.15K ta551
42.08K qbot
INGESTED ENTITIES
600 K
500 K
400 K
300 K
200 K
100 K
0
Feb 2021 Mar 2021 Apr 2021 May 2021 Jun 2021 Jul 2021 Aug 2021 Sep 2021 Oct 2021 Nov 2021 Dec 2021 Jan 2022
TOP 10 ACTIVE ENTITIES (3 LAST MONTHS)
Cobalt Strike
QakBot
Egregor
Axiom
TA505
TrickBot
SectorJ04
Lazarus Group
APT28
Locky
0
20 K
40 K
TARGETED COUNTRIES (3 LAST MONTHS)
Iceland
Finland
Norway
Denmark
Belarus
Belgium
Ukraine
France
Kazakhstan
Italy
Spain
Turkey
Turkmenistan
Tunisia
Iran
Jordan
Pakistan
Algeria
Libya
Egypt
India
Cuba
Guatemala
Mali
Niger
Chad
Yemen
Senegal
Sierra Leone
Nigeria
Ethiopia
Sri Lanka
Panama
Colombia
Kenya
Peru
Brazil
© OpenMapTiles
LAST INGESTED ANALYSIS (CREATION DATE IN THE PLATFORM)
Report Brazilian trojan impacting... AlienVault Mar 14, 2022 TLP:WHITE
Report New Wiper Malware Attac... AlienVault Mar 14, 2022 TLP:WHITE
OBSERVABLES DISTRIBUTION
300 K
250 K
200 K
150 K
100 K
50 K
File
Domain name
Hostname
IPv4 address
URL

Key Frameworks in CTI

- **MITRE ATT&CK**
  - A globally accessible knowledge base that categorizes adversary tactics, techniques, and procedures (TTPs).
- **Use Cases**
  - Threat hunting and detection.
  - Mapping adversary behavior to defensive controls.
  - Aligning intelligence reports with structured attack techniques.

Key Frameworks in CTI

- **Cyber Kill Chain (Lockheed Martin)**
  - A step-by-step model describing the stages of a cyber attack.
- **Stages:**
  - Reconnaissance: Gathering information about the target.
  - Weaponization: Creating malicious payloads.
  - Delivery: Transmitting malware (e.g., phishing, drive-by downloads).
  - Exploitation: Executing malicious code on the victim system.
  - Installation: Establishing persistence (e.g., backdoors, rootkits).
  - Command and Control (C2): Enabling remote control of the compromised system.
  - Actions on Objectives: Exfiltration, lateral movement, destruction.
- **Use Cases:**
  - Helps organizations understand attack progression.
  - Aids in designing security controls for each phase.

Data Enrichment and Correlation in Cyber Threat Intelligence

06

What is Data Enrichment?

- Data enrichment is the process of adding additional context to raw Indicators of Compromise (IoCs) to make them more actionable.
- It transforms basic IoCs (e.g., an IP address) into intelligence by associating them with threat actors, campaigns, timestamps, and historical data.

Why is Data Enrichment Important?

- Reduces false positives
  - Adds context to determine if an IoC is truly malicious.
- Speeds up investigations
  - Provides relevant historical and attributional data.
- Improves detection and response
  - Helps analysts make informed decisions.
- Enhances threat hunting
  - Identifies patterns that could indicate broader campaigns.

Key Data Enrichment Techniques

- **Reputation Lookups**
  - Checking IoCs against public and commercial Threat Intelligence Feeds.
  - Sources: VirusTotal, GreyNoise, Recorded Future.
  - Example:
    - Checking if an IP (45.156.23.12) has been reported as a C2 server.
- **Historical Data Analysis**
  - Reviewing how an IoC was used in previous attacks.
  - Example:
    - Finding that a file hash was previously linked to TrickBot malware.

Key Data Enrichment Techniques

- **Attribution and Actor Mapping**
  - Linking IoCs to threat actor profiles and known campaigns.
  - Example:
    - A domain was used in a phishing campaign by APT29 (Cozy Bear).
- **Geo-Location and ASN Analysis**
  - Identifying the location and hosting provider of an IP.
  - Example:
    - An IP traced to a data center in Russia raises suspicion.

Key Data Enrichment Techniques

- **Passive DNS & WHOIS Data**
  - Analyzing past DNS resolutions to identify changes in domains.
  - Example:
    - Discovering that a phishing domain recently changed ownership.
- **Behavioral Analysis**
  - Examining malware execution behavior via sandboxing.
  - Example:
    - A file hash was observed dropping a keylogger in a sandbox.

What is Data Correlation in CTI?

- Correlation links multiple IoCs and threat intelligence sources to uncover relationships and broader attack campaigns.
- It helps analysts detect patterns, link incidents, and assess risk.

Key Correlation Techniques

- **TTP-Based Correlation (MITRE ATT&CK)**
  - Identifying if multiple IoCs map to the same TTPs.
  - Example:
    - An IP flagged in multiple Initial Access (T1566) phishing campaigns.
- **Temporal Correlation**
  - Checking if IoCs appear in multiple incidents over time.
  - Example:
    - An IP involved in Emotet infections in 2022 reappears in 2024.

Key Correlation Techniques

- **Infrastructure Linkage**
  - Connecting different IoCs that use shared hosting, domains, or IPs.
  - Example:
    - Two phishing domains registered with the same email address.
- **Campaign-Based Correlation**
  - Associating IoCs with known malware families and APT groups.
  - Example:
    - A newly discovered malware sample has a 40% code similarity to a Lazarus Group implant.

Collaborative Threat Intelligence Sharing

Why is Threat Intelligence Sharing Important?

- Threat actors operate in coordinated networks, leveraging shared tools, exploits, and infrastructure.
- To counter these threats effectively, cybersecurity defenders must also collaborate.
- Threat intelligence sharing enables organizations to:
  - **Enhance detection and response**
    - Sharing IoCs and TTPs enables early detection of emerging threats.
  - **Reduce attack surface**
    - Organizations can proactively block **malicious domains, IPs, and malware** identified by others
  - **Strengthen community defense**
    - Public and private sector collaboration improves security for everyone.

Threat Intelligence Collaboration

- ISACs (Information Sharing and Analysis Centers)
  - Industry-specific groups (e.g., FS-ISAC for financial institutions) that share threat data.
- Public-Private Partnerships (PPP)
  - Governments, CERTs (Computer Emergency Response Teams), and private companies collaborate to fight cybercrime.
- Platforms like MISP and OpenCTI
  - Enable real-time sharing and correlation of threat data.

Structured Threat Information Expression and Transport

- **STIX (Structured Threat Information Expression)**
  - A standardized format for representing cyber threat intelligence, including IoCs, TTPs, and threat actor details.
  - Enables machine-readable threat intelligence that can be processed automatically.

STIX IoC Example

```
{
  "type": "indicator",
  "id": "indicator--aab123cd-45ef-6789-001a-bcdefg23456",
  "pattern": "[ipv4-addr:value = '192.168.1.100']",
  "created": "2024-02-06T12:34:56.000Z",
  "labels": ["malicious-activity"]
}
```

https://oasis-open.github.io/cti-documentation/stix/examples.html

Structured Threat Information Expression and Transport

- **TAXII (Trusted Automated Exchange of Intelligence Information)**
  - A transport mechanism that allows sharing of STIX-formatted intelligence securely and efficiently.
  - Used to distribute threat intelligence between organizations, SOCs, and TIPs.

Traffic Light Protocol

- The Traffic Light Protocol (TLP) is a simple yet widely used information classification system designed to facilitate controlled threat intelligence sharing among trusted parties.
- Why is TLP Important?
  - Prevents overexposure of sensitive threat intelligence.
  - Ensures that only authorized individuals or groups receive certain information.
  - Encourages collaboration by setting clear rules on data sharing.
  - Helps maintain trust among cybersecurity communities, ISACs, and organizations.

Traffic Light Protocol

- TLP:WHITE – Unrestricted/Public Sharing
  - Purpose
    - Information that can be freely shared without any restrictions.
  - Who Can Receive It?
    - Anyone, including the general public, media, and external organizations.
  - How Should It Be Handled?
    - Can be published on websites, in blogs, security reports, and social media.
    - No special precautions needed.
  - Examples:
    - Cybersecurity awareness materials (e.g., how to recognize phishing).
    - Public reports on ransomware trends by security vendors (e.g., CrowdStrike, Mandiant).
    - Vulnerability advisories published by security researchers.

Traffic Light Protocol

- TLP:GREEN – Community-Wide Sharing
  - Purpose
    - For broader but still controlled sharing within trusted groups, industries, or ISACs.
  - Who Can Receive It?
    - Any trusted community members, cybersecurity professionals, ISAC participants.
  - How Should It Be Handled?
    - Can be shared within organizations and partner organizations, but not publicly.
    - Can be used in training, security briefings, and industry collaboration.
  - Examples:
    - A new phishing campaign targeting the finance sector.
    - Threat actor TTPs seen in multiple industries.
    - Security best practices to counter a new exploit.

Traffic Light Protocol

- TLP:AMBER – Limited Sharing
  - Purpose
    - For use within the recipient's organization or specific trusted communities.
  - Who Can Receive It?
    - Internal teams, partners, or trusted vendors.
    - The information should only be shared with those who need to know.
  - How Should It Be Handled?
    - Recipients can share within their organization but not externally.
  - Example restriction
    - "TLP:AMBER – Only for XYZ Security Team Use.”
  - Examples:
    - Malware analysis reports affecting company systems.
    - A list of malicious IPs and domains targeting your industry.

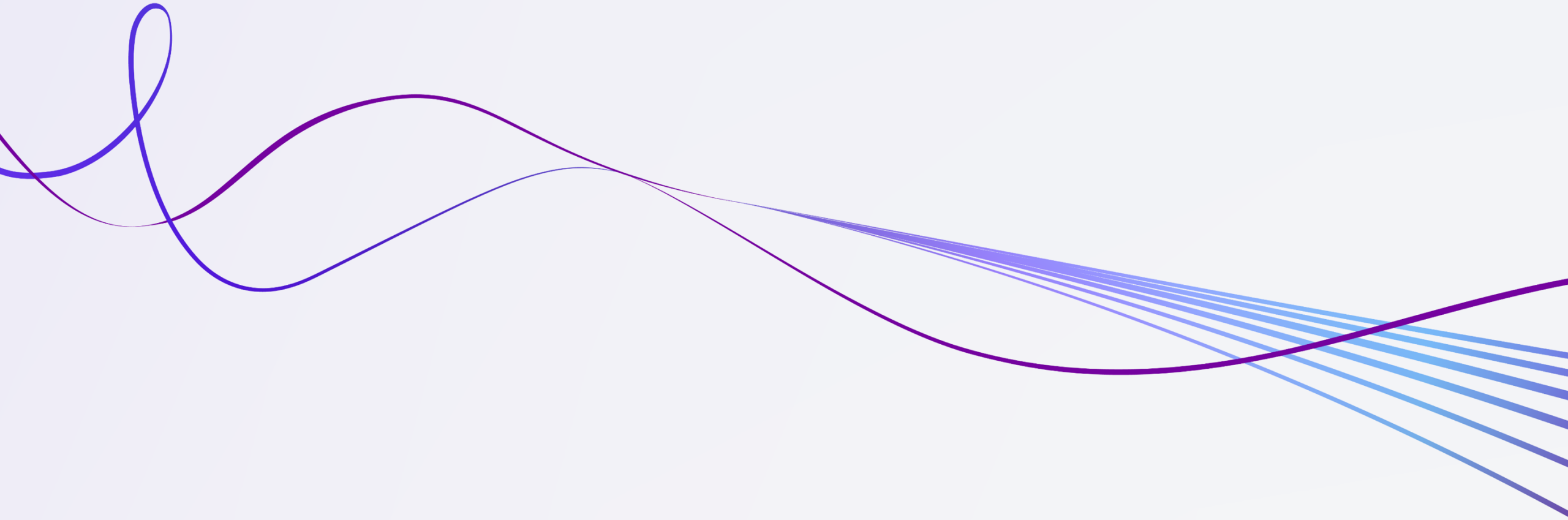
Traffic Light Protocol

- TLP:AMBER+STRICT – Restricted Internal Sharing
  - Purpose
    - A sub-classification of TLP:AMBER that restricts sharing within specific internal teams only.
  - Who Can Receive It?
    - Only the named individuals or internal security teams.
    - Sharing beyond the defined group requires explicit permission.
  - How Should It Be Handled?
    - Must be explicitly labeled as TLP:AMBER+STRICT.
    - No automatic forwarding or distribution within the organization.
  - Examples:
    - Ongoing security incident response details that should not be broadly shared.
    - Threat intelligence that includes sensitive business or operational data.
    - Active vulnerability exploitation details that, if mishandled, could pose a risk to security operations.

Traffic Light Protocol

- TLP:RED – Most Restricted
  - Purpose
    - Strictly confidential information that, if leaked, could cause severe damage to individuals, organizations, or national security.
  - Who Can Receive It?
    - Only the intended recipients (e.g., security teams, senior executives).
  - How Should It Be Handled?
    - Do NOT share outside the specified group.
    - No email forwarding, public discussion, or inclusion in reports unless explicitly authorized.
  - Examples:
    - A zero-day vulnerability found in critical infrastructure.
    - Nation-state cyber attack intelligence impacting national security.
    - Ongoing law enforcement cybercrime investigations.

Questions on CTF platform



Tools

VirusTotal (VT)

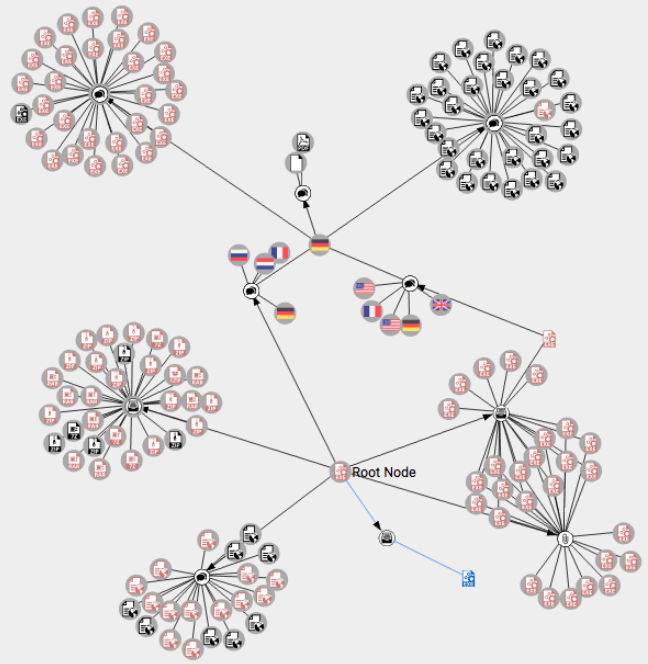
- VirusTotal (VT) is a popular cloud-based malware detection and analysis platform, acquired by Google in 2012 and now operated by Google Cloud.
- It allows users to analyze suspicious files, URLs, domains, and IP addresses by scanning them against multiple antivirus engines, URL scanners, and threat intelligence feeds.
- The platform provides real-time insights into malicious activity, enabling security analysts, incident responders, and researchers to identify and respond to potential threats effectively.

VirusTotal (VT)

- VirusTotal's Core Functions:
  - File analysis
    - Submit files to be scanned by over 70 antivirus engines.
  - URL scanning
    - Analyze URLs for potential phishing sites or malicious content.
  - Domain and IP reputation
    - Investigate domains and IPs for malicious behavior.
  - Threat hunting
    - Identify patterns, relationships, and malicious artifacts across datasets.
  - API integration
    - Automate threat intelligence collection and integration into other security platforms.

VirusTotal (VT)

- VirusTotal Web Interface
- VirusTotal Community
- VirusTotal Graph
- VirusTotal Intelligence
- VirusTotal API

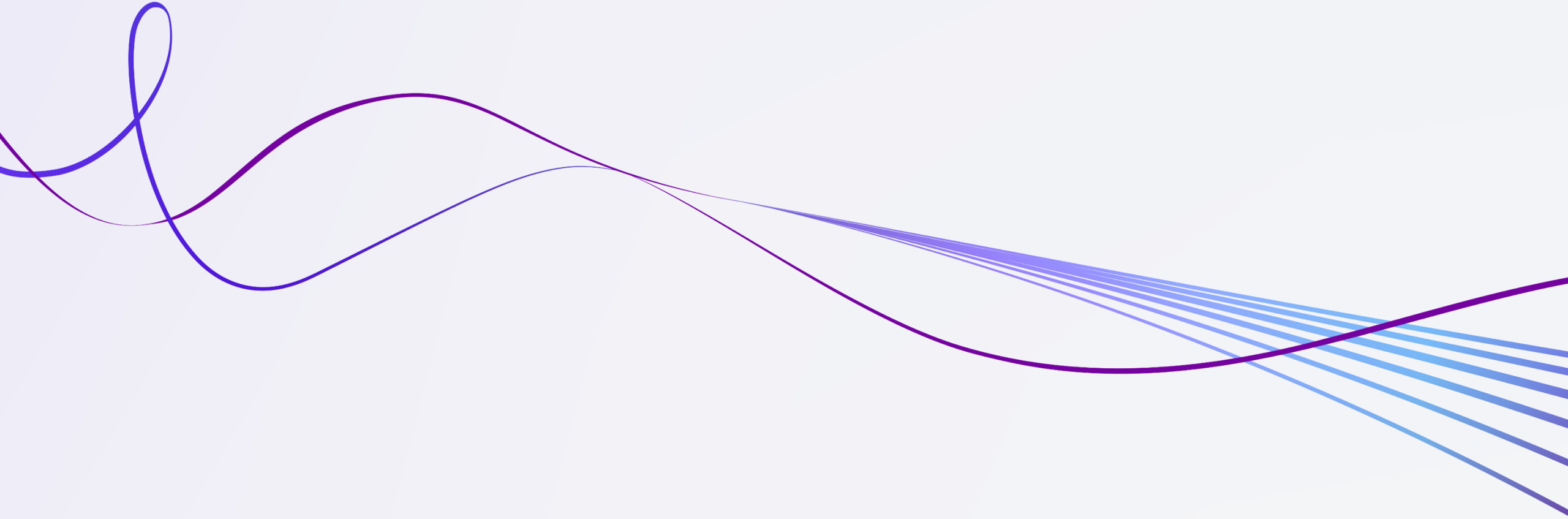


VirusTotal (VT)

VirusTotal Analysis Process

- **File Scanning**
- **Behavioral Analysis (Dynamic Analysis)**
- **Static Analysis**
- **Network Indicators**
- **Correlation & Relationship Analysis**

Questions on CTF platform



Shodan

- Shodan is a specialized search engine designed to discover internet-connected devices.
- Unlike traditional search engines like Google that index websites, Shodan indexes devices, services, and systems exposed to the internet.
- It is often referred to as the "Google for Hackers" because of its ability to identify vulnerable devices and provide detailed insights into internet-facing systems.

What Can Shodan Find?

- Shodan scans the internet and indexes metadata from devices and services across various protocols.
- Examples of devices Shodan can find:
  - Servers and Routers
  - IoT devices (CCTV cameras, smart TVs, baby monitors, thermostats)
  - Industrial Control Systems (ICS) (SCADA systems, power grids, water treatment plants)
  - Databases (MongoDB, Elasticsearch, PostgreSQL)
  - Web Applications (public websites, development environments)
  - Network Infrastructure (firewalls, VPN gateways)

How Does Shodan Work?

- **Service Banner Collection**
  - For each discovered device, Shodan captures **banner information** exposed by network services. Banners contain metadata such as:
  - **Service name and version** (e.g., Apache 2.4.29)
  - **Operating system and software fingerprints**
  - **SSL/TLS certificates**
  - **Device manufacturer details**
- **Data Indexing**
  - The collected data is indexed into **Shodan's searchable database**. Users can query this data to **find devices by IP, location, software version, or open ports**.

How Does Shodan Work?

- **Internet-Wide Scanning**
  - Shodan scans the **entire IPv4 address space** across multiple ports and protocols, such as:
    - **HTTP (80/443)** – Web servers
    - **SSH (22)** – Remote access services
    - **RDP (3389)** – Remote desktop access
    - **FTP (21)** – File transfer servers
  - **ICS Protocols (502/44818)**

ANY.RUN

- ANY.RUN is an interactive malware analysis platform that provides real-time insights into malicious files, URLs, and network activity.
- Unlike many other malware sandboxes that run analyses in a fully automated, passive environment, ANY.RUN is interactive, allowing users to manually interact with the malware during execution.
- ANY.RUN is widely used by:
  - Cybersecurity researchers for dynamic malware analysis.
  - Incident responders for investigating suspicious files or URLs.
  - Threat intelligence analysts for tracking malware families.

Key Features of ANY.RUN

- Interactive Malware Analysis
  - Run suspicious files in a virtual machine (VM) with interactive control.
  - Manually click buttons, enter text, open files, and browse to observe malware behavior.
- Real-Time Process Tree Visualization
  - Displays a dynamic process tree showing parent-child relationships.
  - Processes are color-coded based on behavior:
    - Benign operations.
    - Suspicious activities.
    - Malicious behaviors (e.g., code injection, persistence mechanisms).

Key Features of ANY.RUN

- Network Traffic Analysis
  - Captures live network traffic for in-depth command-and-control (C2) communication analysis.
  - Displays:
    - DNS requests
    - HTTP/HTTPS traffic
    - TCP/UDP connections
    - SSL/TLS certificates
- File System Activity Monitoring
  - Tracks file creation, modification, deletion, and exfiltration.
  - Monitors:
    - Registry modifications.
    - Dropped files and payloads.

Key Features of ANY.RUN

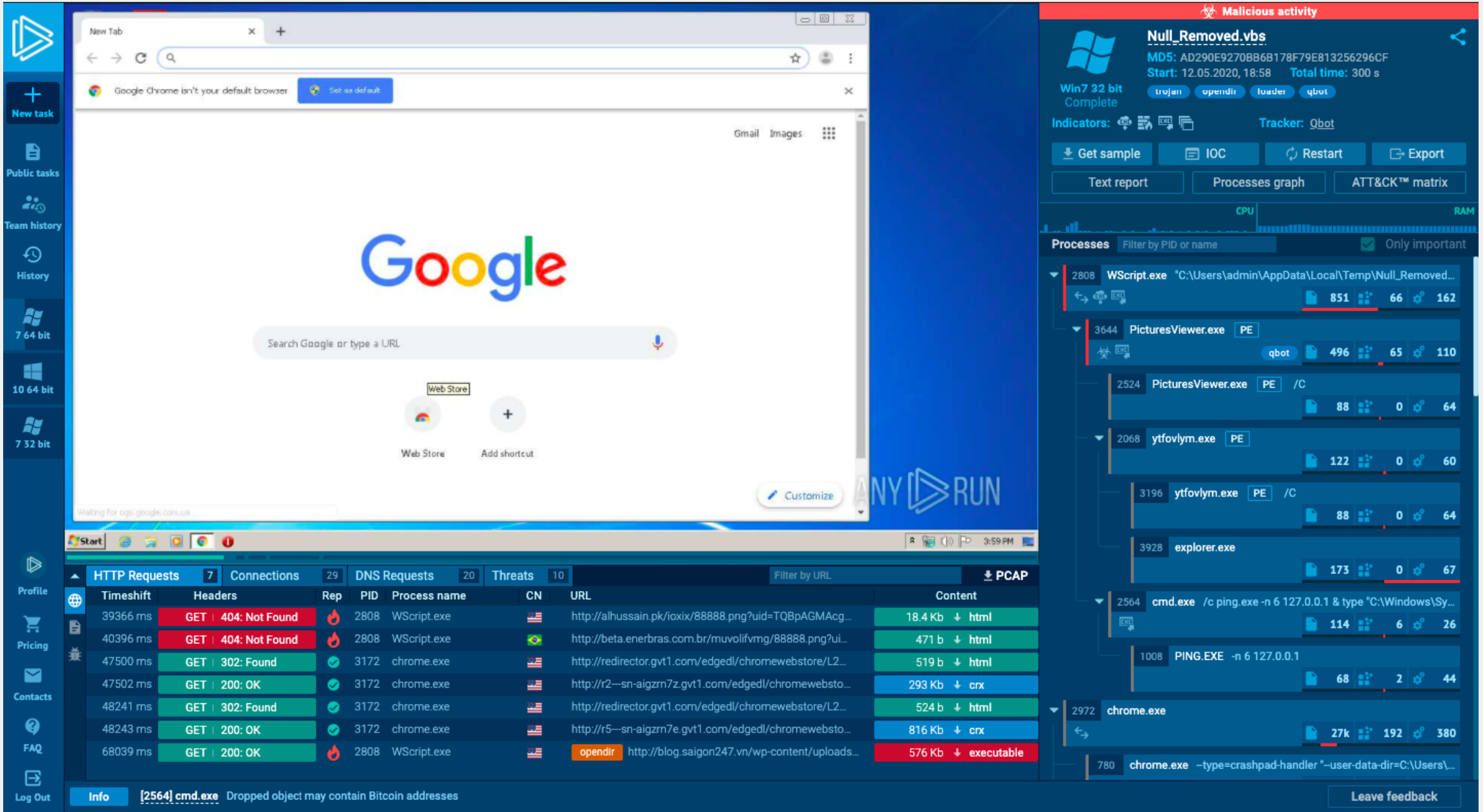
- Interactive Command Execution Analysis
  - Track PowerShell, CMD, and bash command execution.
  - Identify encoded commands often used to obfuscate malicious intent.
  - De-obfuscates Base64-encoded PowerShell scripts automatically.
- MITRE ATT&CK Mapping
  - Maps observed tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK framework.
  - Helps analysts understand attacker behavior and potential goals.
- YARA Rule Integration
  - Apply custom YARA rules to detect malware patterns in real-time.
  - Helps in identifying new variants of known malware families.

Key Features of ANY.RUN

- Browser Interaction Simulation
  - Analyze malicious websites and web-based attacks (e.g., phishing, watering hole attacks).
  - Simulate browser-based interactions to reveal redirect chains, malicious scripts, and exploit kits.

ANY.RUN

- ANY.RUN supports analyzing the following file types:
  - Executable files: .exe, .dll, .sys.
  - Scripts: .bat, .cmd, .ps1, .vbs.
  - Archives: .zip, .rar, .7z.
  - Documents: .docx, .xlsx, .pdf (often used for macro-based attacks).
  - Email files: .eml, .msg for analyzing phishing campaigns.
  - URLs & Domains: Analyze malicious websites or C2 endpoints.


New task
Public tasks
Team history
History
7 64 bit
10 64 bit
7 32 bit
Profile
Pricing
Contacts
FAQ
Log Out
New Tab
Google Chrome isn't your default browser
Set as default
Gmail
Images
Google
Search Google or type a URL
Web Store
Add shortcut
Customize
ANY RUN
Malicious activity
Null_Removed.vbs
MD5: AD290E9270BB6B178F79E813256296CF
Start: 12.05.2020, 18:58
Total time: 300 s
Win7 32 bit
Complete
trojan
opendir
loader
qbot
Indicators:
Tracker: Qbot
Get sample
IOC
Restart
Export
Text report
Processes graph
ATT&CK™ matrix
CPU
RAM
Processes
Filter by PID or name
Only important
2808 WScript.exe "C:\Users\admin\AppData\Local\Temp\Null_Removed...
851 66 162
3644 PicturesViewer.exe PE
qbot
496 65 110
2524 PicturesViewer.exe PE /C
88 0 64
2068 ytfovlym.exe PE
122 0 60
3196 ytfovlym.exe PE /C
88 0 64
3928 explorer.exe
173 0 67
2564 cmd.exe /c ping.exe -n 6 127.0.0.1 & type "C:\Windows\Sy...
114 6 26
1008 PING.EXE -n 6 127.0.0.1
68 2 44
2972 chrome.exe
27k 192 380
780 chrome.exe --type=crashpad-handler "--user-data-dir=C:\Users\...
HTTP Requests 7
Connections 29
DNS Requests 20
Threats 10
Filter by URL
PCAP
Timeshift Headers Rep PID Process name CN URL Content
39366 ms GET | 404: Not Found 2808 WScript.exe http://alhussain.pk/ioxix/88888.png?uid=TQBpAGMAcg... 18.4 Kb html
40396 ms GET | 404: Not Found 2808 WScript.exe http://beta.enerbras.com.br/muvolifvmg/88888.png?ui... 471 b html
47500 ms GET | 302: Found 3172 chrome.exe http://redirector.gvt1.com/edgedl/chromewebstore/L2... 519 b html
47502 ms GET | 200: OK 3172 chrome.exe http://r2---sn-aigzrn7z.gvt1.com/edgedl/chromewebsto... 293 Kb crx
48241 ms GET | 302: Found 3172 chrome.exe http://redirector.gvt1.com/edgedl/chromewebstore/L2... 524 b html
48243 ms GET | 200: OK 3172 chrome.exe http://r5---sn-aigzrn7e.gvt1.com/edgedl/chromewebsto... 816 Kb crx
68039 ms GET | 200: OK 2808 WScript.exe opendir http://blog.saigon247.vn/wp-content/uploads... 576 Kb executable
Info
[2564] cmd.exe Dropped object may contain Bitcoin addresses
Leave feedback

Abuse.ch

- Abuse.ch is a non-profit cybersecurity project dedicated to tracking and disrupting malicious activities on the internet.
- Abuse.ch provides free access to threat intelligence about malware, botnets, phishing, ransomware infrastructure, and malicious domains.
- The platform is widely recognized for its community-driven approach and collaboration with international security teams.
- It helps defenders identify, block, and mitigate cyber threats by sharing real-time indicators of compromise (IoCs).

Abuse.ch

- Abuse.ch is a non-profit cybersecurity project dedicated to tracking and disrupting malicious activities on the internet.
- Abuse.ch provides free access to threat intelligence about malware, botnets, phishing, ransomware infrastructure, and malicious domains.
- The platform is widely recognized for its community-driven approach and collaboration with international security teams.
- It helps defenders identify, block, and mitigate cyber threats by sharing real-time indicators of compromise (IoCs).

"To make the internet safer by providing actionable threat intelligence to everyone… for free."

Abuse.ch

- URLhaus (URL-based Malware Tracking)
  - URLhaus tracks URLs used for distributing malware.
  - Key Features:
    - Real-time tracking of malware distribution sites.
    - Community-driven platform—researchers worldwide report malicious URLs.
    - Provides public and API access to the latest malware-hosting domains.

Sharing malicious URLs being used for malware distribution

Abuse.ch

- MalwareBazaar (Malware Sample Exchange)
  - MalwareBazaar is a community-driven repository for malware samples. Security researchers use it to share, analyze, and categorize malware binaries.
  - Key Features:
    - Searchable malware database by hash (MD5/SHA256), YARA rules, file type, or malware family.
    - Malware samples tagged with malware family names (e.g., Emotet, TrickBot, QakBot).
    - AI-assisted malware tagging to automatically classify new malware variants.

Sharing newly observed malware samples

Abuse.ch

- ThreatFox (Open Threat Intelligence Platform)
  - ThreatFox is an open-source platform for sharing and accessing IoCs related to malware, phishing, and C2 infrastructure.
  - Key Features:
    - Track IoCs by malware family (e.g., Redline Stealer, QakBot, Remcos RAT).
    - Supports TLP classifications (e.g., TLP:WHITE for public sharing).
    - STIX and MISP export formats for easy integration with security tools.

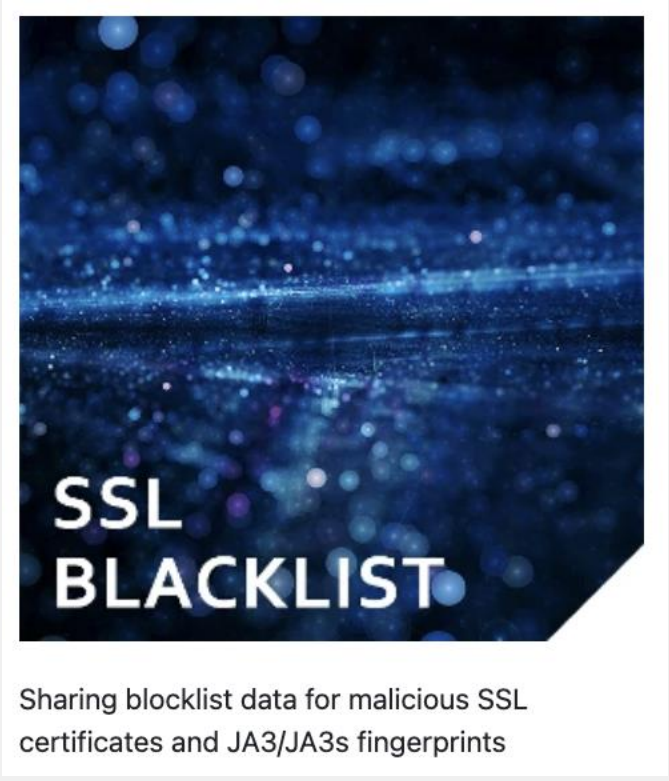
Sharing indicators of compromise (IOCs) associated with malware.

Abuse.ch

- Feodo Tracker (Banking Trojan Tracking)
  - Feodo Tracker focuses on tracking malware families associated with banking trojans, such as:
    - Dridex
    - TrickBot
    - Emotet
    - QakBot (Qbot)
  - Key Features:
    - Monitors Command & Control (C2) servers for active banking trojans.
    - Provides real-time blocklists for security teams to blacklist C2 infrastructure.
    - Supports C2 tracking by malware family.

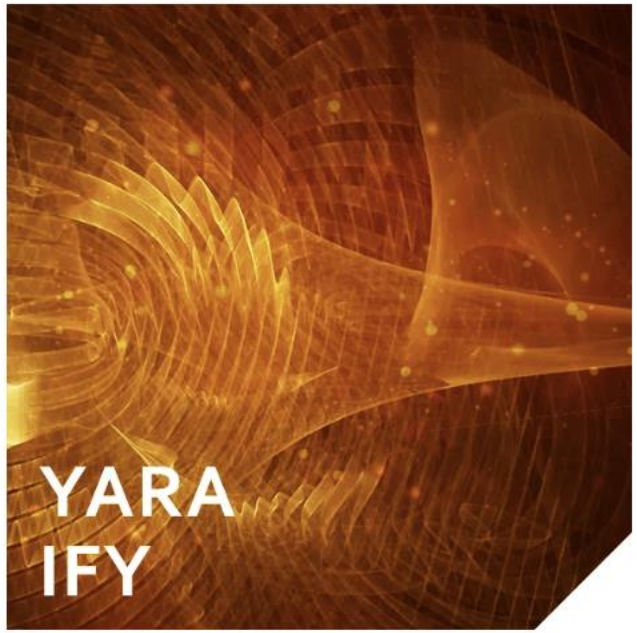
Abuse.ch

- SSLBL (SSL Blacklist)
  - SSLBL tracks malicious SSL/TLS certificates used by malware campaigns.
  - Key Features:
    - Monitors malicious certificates associated with phishing, malware delivery, and C2 servers.
    - Tracks TLS fingerprint anomalies (JA3 and JA3S hashes).
    - Provides lists of malicious certificates for firewall and proxy integration.



Abuse.ch

- YARAify (YARA Rule-Based Malware Detection)
  - YARAify is a malware analysis platform by Abuse.ch that uses YARA rules to detect, classify, and contextualize malicious files.
  - Key Features:
    - Automated Malware Detection: Uses community-contributed and Abuse.ch-defined YARA rules.
    - Multiple Submission Methods: Submit files, URLs, or hashes (MD5, SHA1, SHA256) via the web interface or API.



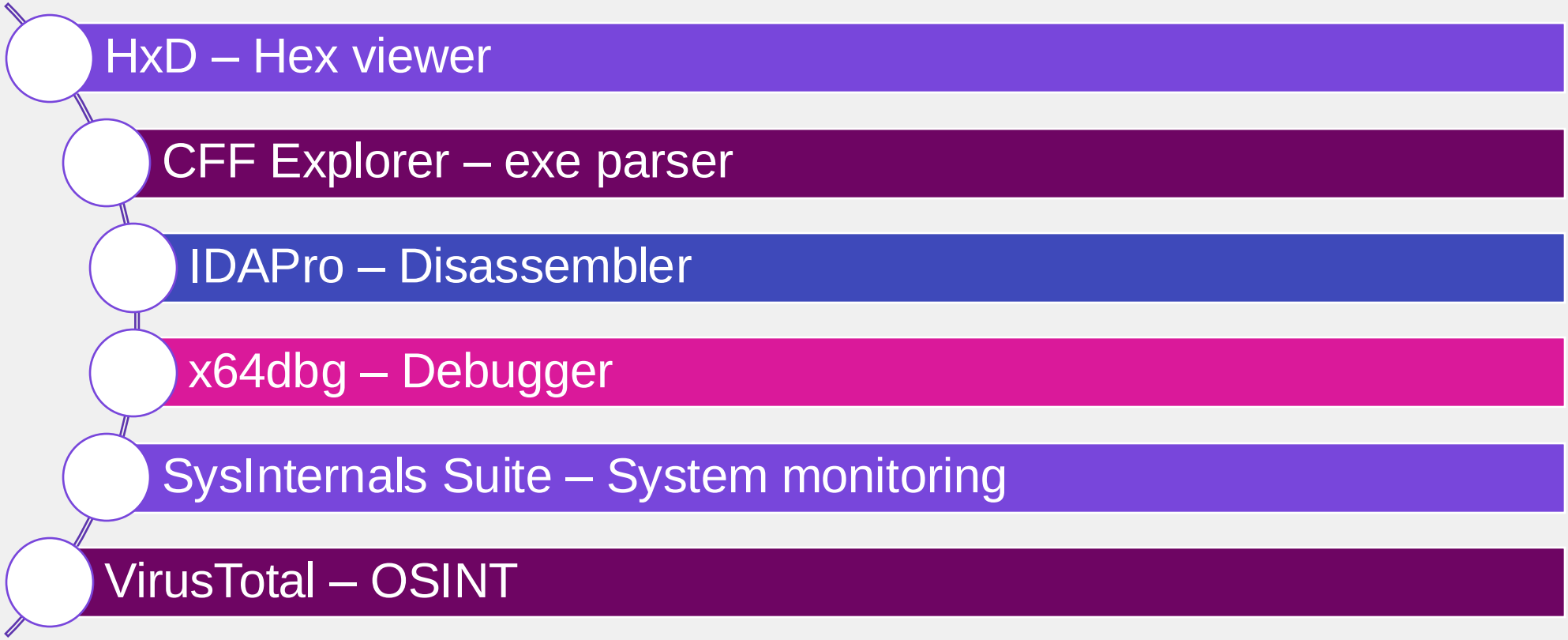
A large repository of YARA rules to identify and classify malware - use to share rules, hunt, and scan

Intro to Malware Analysis

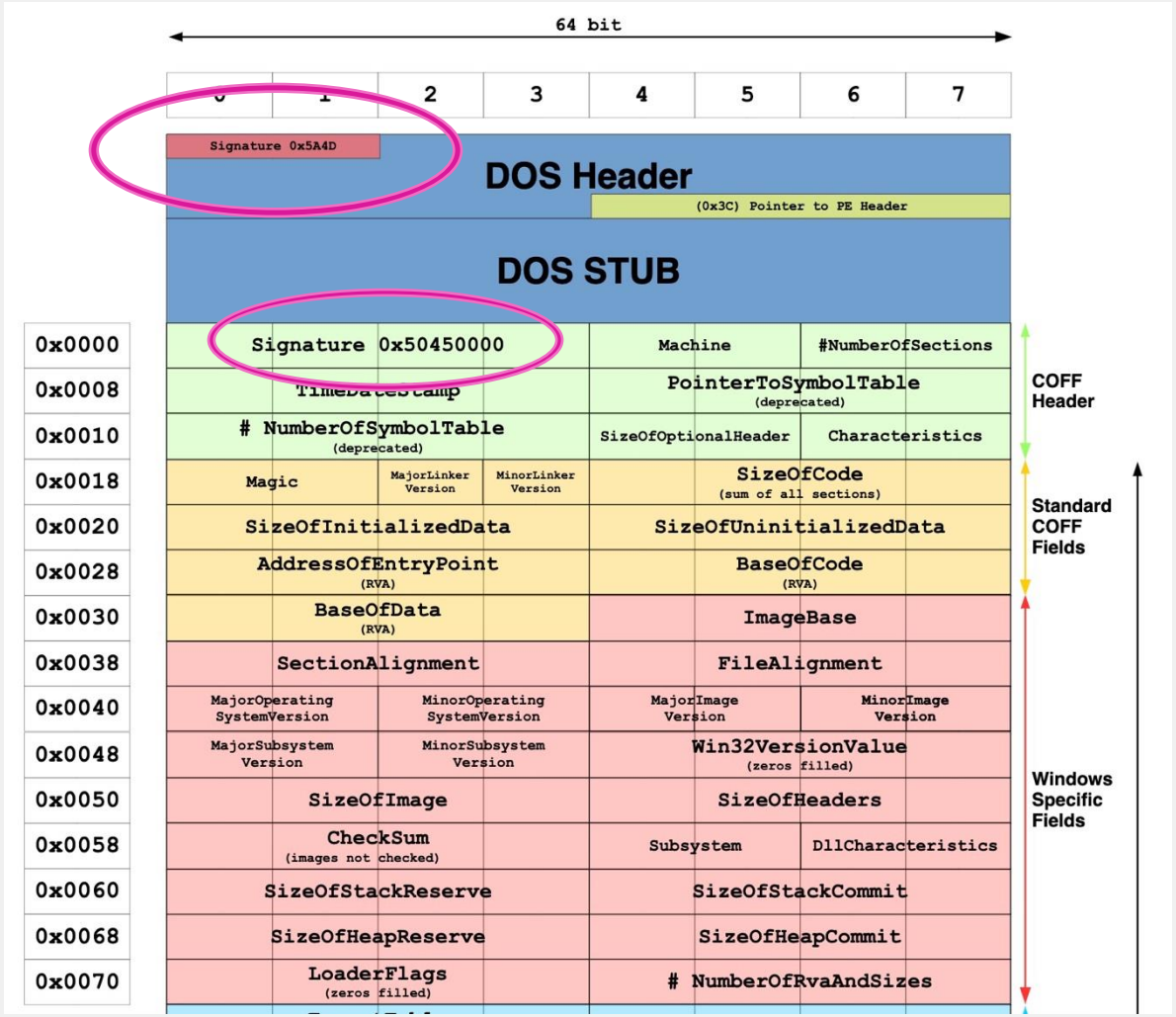
Agenda

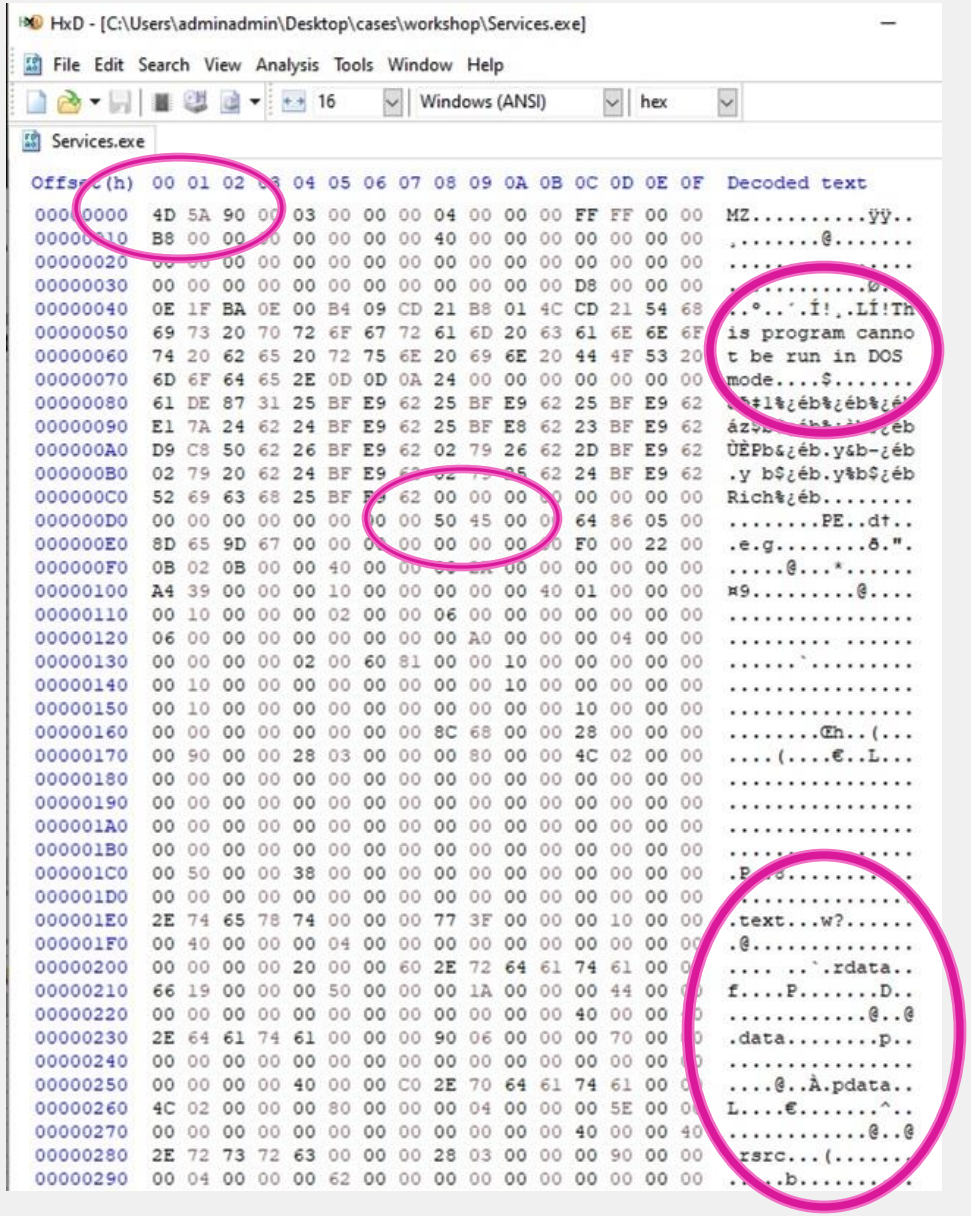

Focus on Executables
Static Analysis
Dynamic Analysis
Research Pivots

Tools covered



PE file structure

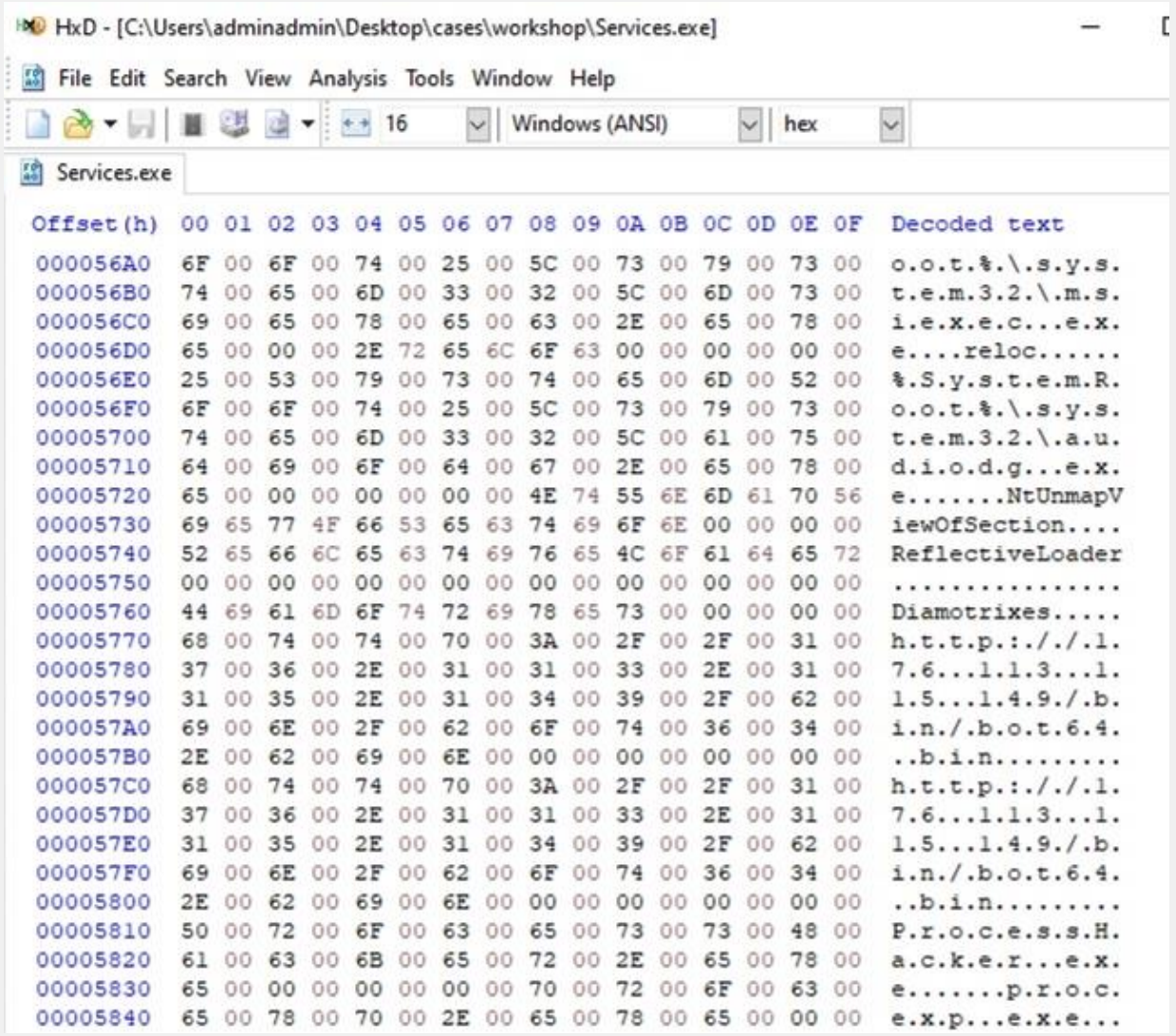




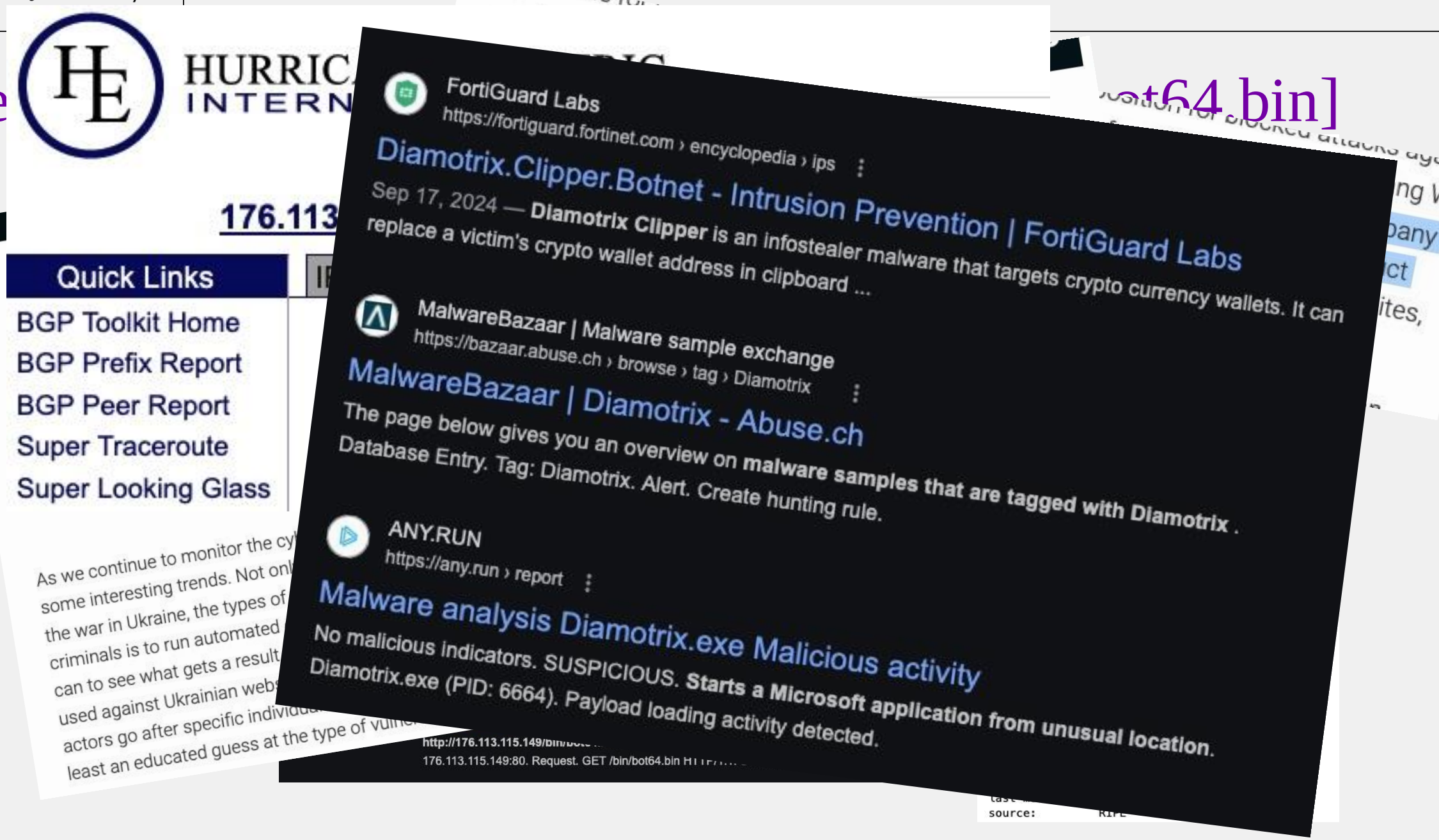
Exercise / Q&A Break

Q : Using HxD, can you find a URL?

A : Offset 0x5770

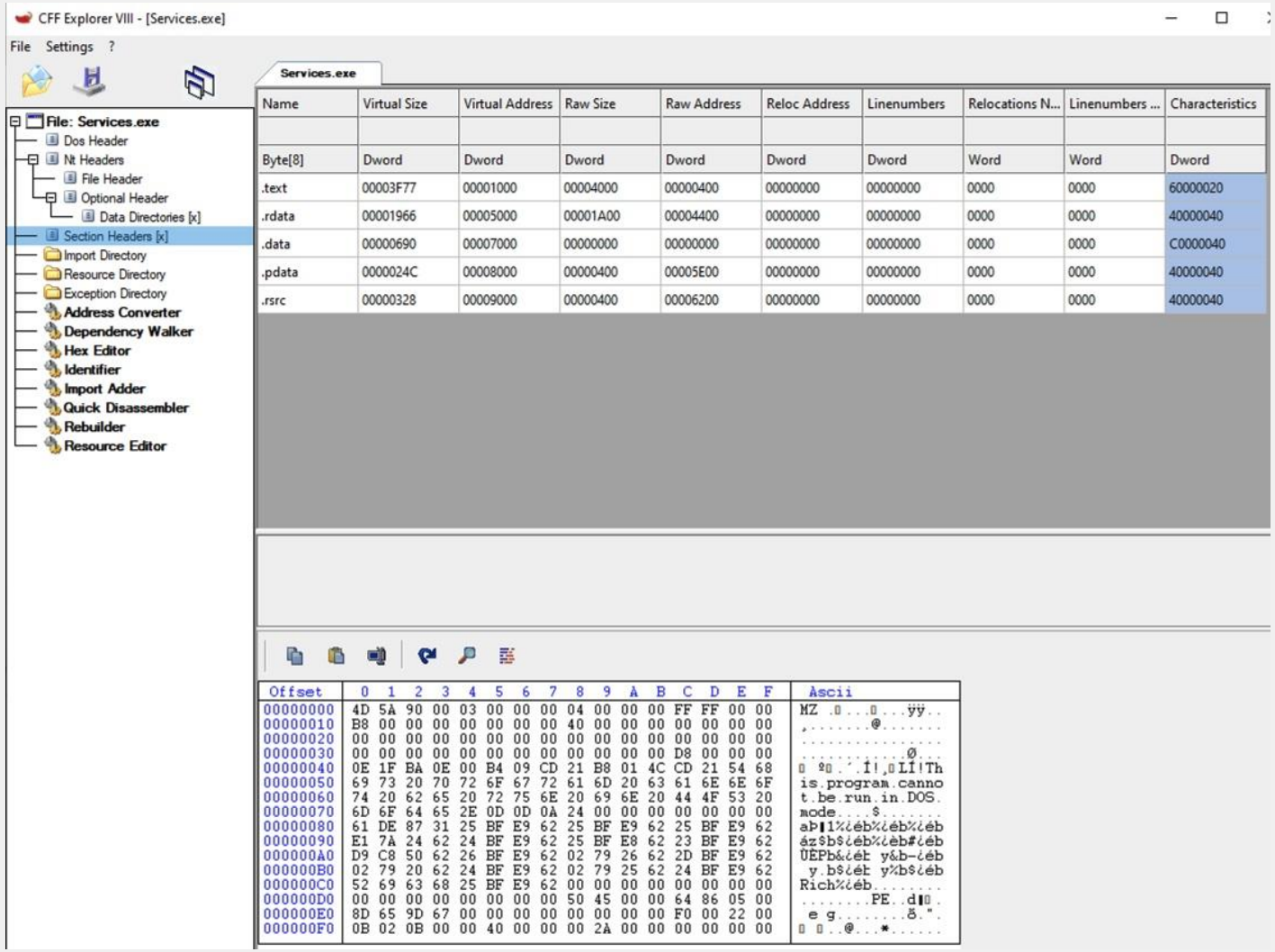


Re bot64.bin]

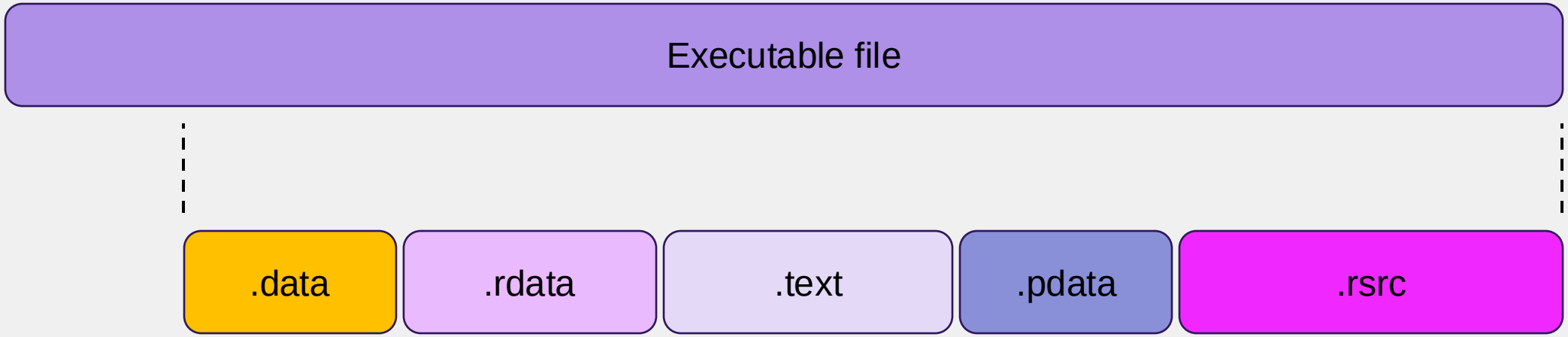

HURRIC
INTERN
176.113
Quick Links
BGP Toolkit Home
BGP Prefix Report
BGP Peer Report
Super Traceroute
Super Looking Glass
As we continue to monitor the cy
some interesting trends. Not onl
the war in Ukraine, the types of
criminals is to run automated
can to see what gets a result
used against Ukrainian webs
actors go after specific individu
least an educated guess at the type of vul
FortiGuard Labs
https://fortiguard.fortinet.com › encyclopedia › ips
Diamotrix.Clipper.Botnet - Intrusion Prevention | FortiGuard Labs
Sep 17, 2024 — Diamotrix Clipper is an infostealer malware that targets crypto currency wallets. It can replace a victim's crypto wallet address in clipboard ...
MalwareBazaar | Malware sample exchange
https://bazaar.abuse.ch › browse › tag › Diamotrix
MalwareBazaar | Diamotrix - Abuse.ch
The page below gives you an overview on malware samples that are tagged with Diamotrix . Database Entry. Tag: Diamotrix. Alert. Create hunting rule.
ANY.RUN
https://any.run › report
Malware analysis Diamotrix.exe Malicious activity
No malicious indicators. SUSPICIOUS. Starts a Microsoft application from unusual location. Diamotrix.exe (PID: 6664). Payload loading activity detected.
http://176.113.115.149/bin/bot
176.113.115.149:80. Request. GET /bin/bot64.bin
ng Way
pany
ct
ites,
source:

PE file structure : CFF Explorer

- Parse Fields
- Parse Sections
- Read Configuration
- Edit Entries



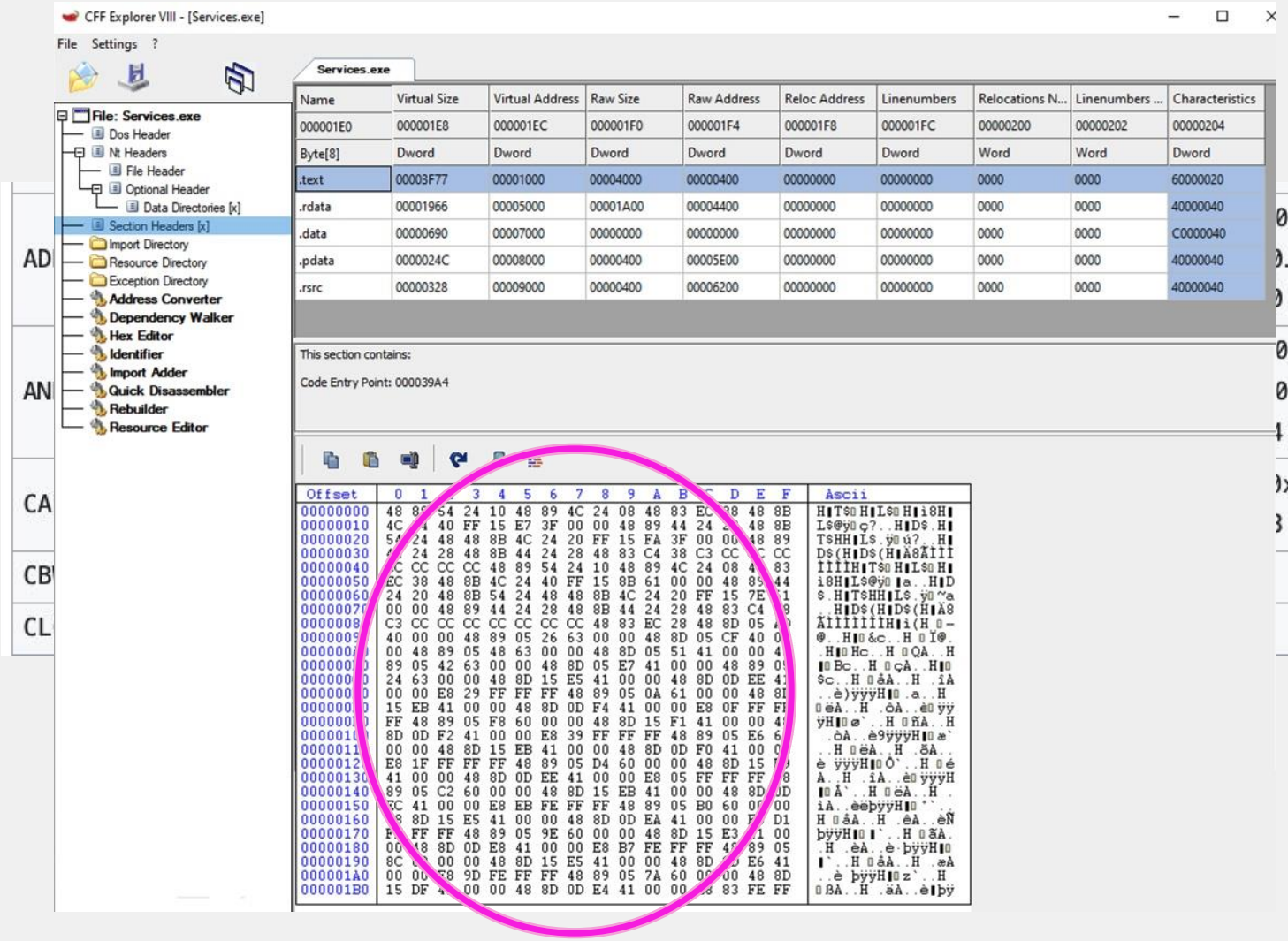
PE file structure : Sections



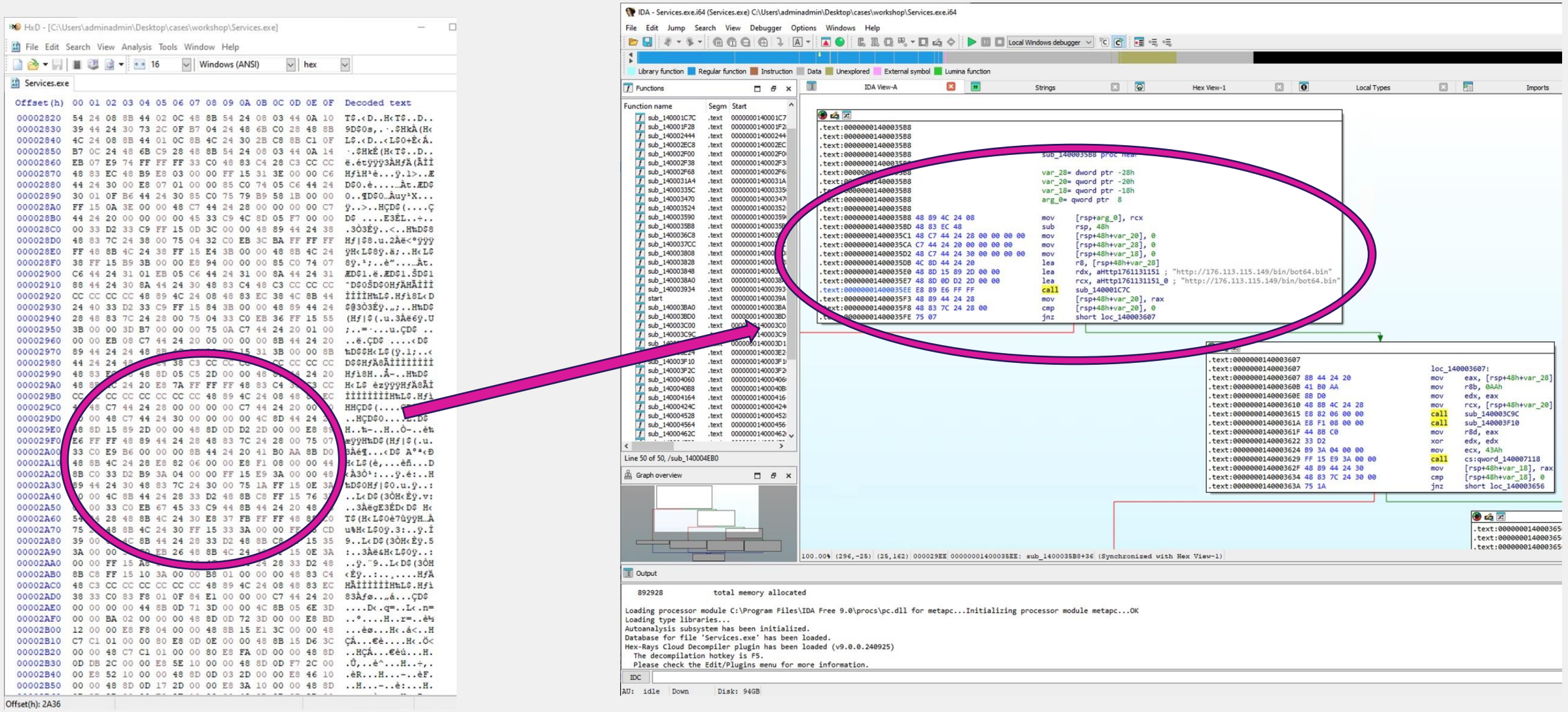
- .data – initialized data
- .rdata – read-only initialized data
- .rsrc – resource directory (“files” a program needs)
- .text – executable code

Static Analysis : Disassembly

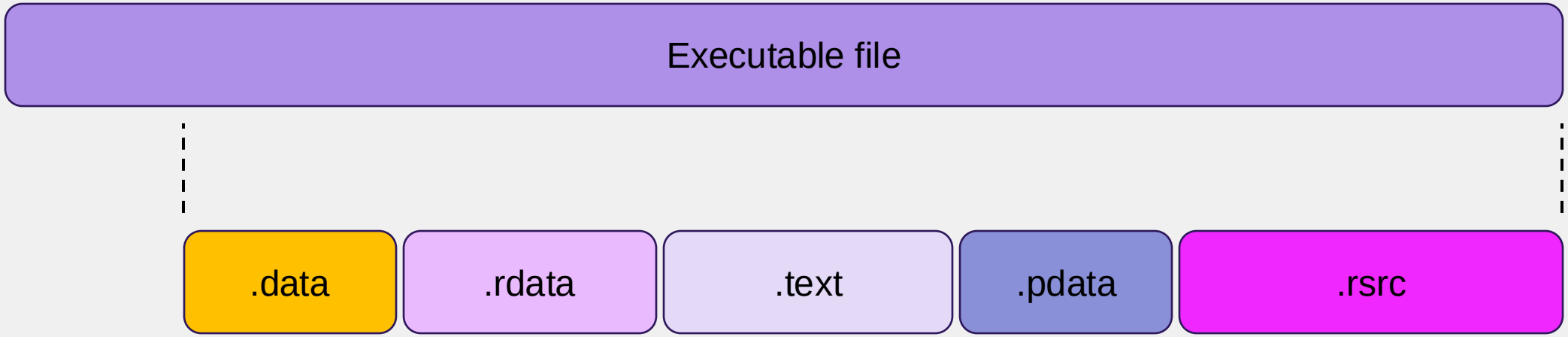
- The .text section
- Actual CPU instructions
- Hex values <-> CPU operations



Static Analysis : Disassembly – IDAPro

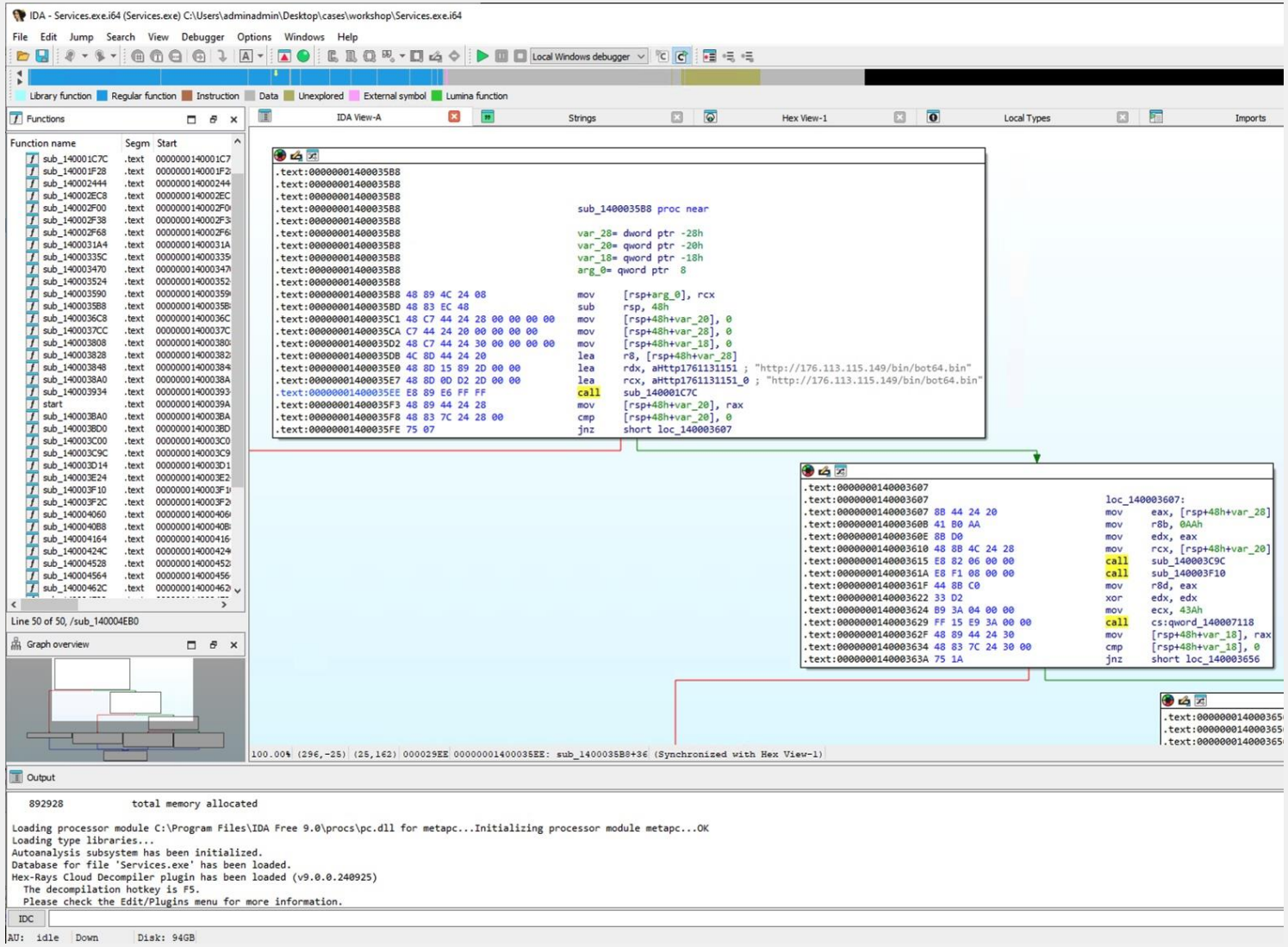


PE file structure : Disassembly of Sections



- .data – initialized data
- .rdata – read-only initialized data
- .rsrc – resource directory (“files” a program needs)
- .text – executable code

Static analysis : IDAPro



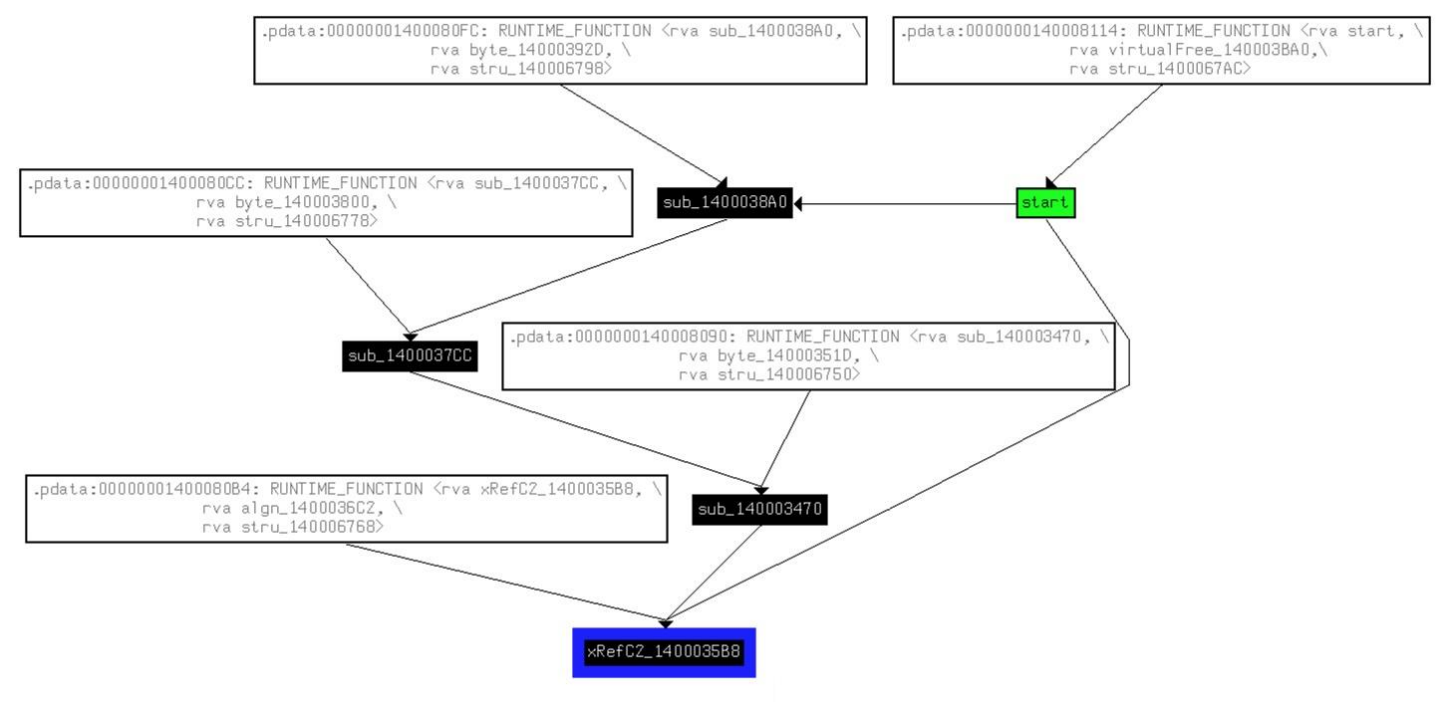
Exercise / Q&A Break

Q : What subroutines (by hex address) reference our URL string? What are the call chains from start?

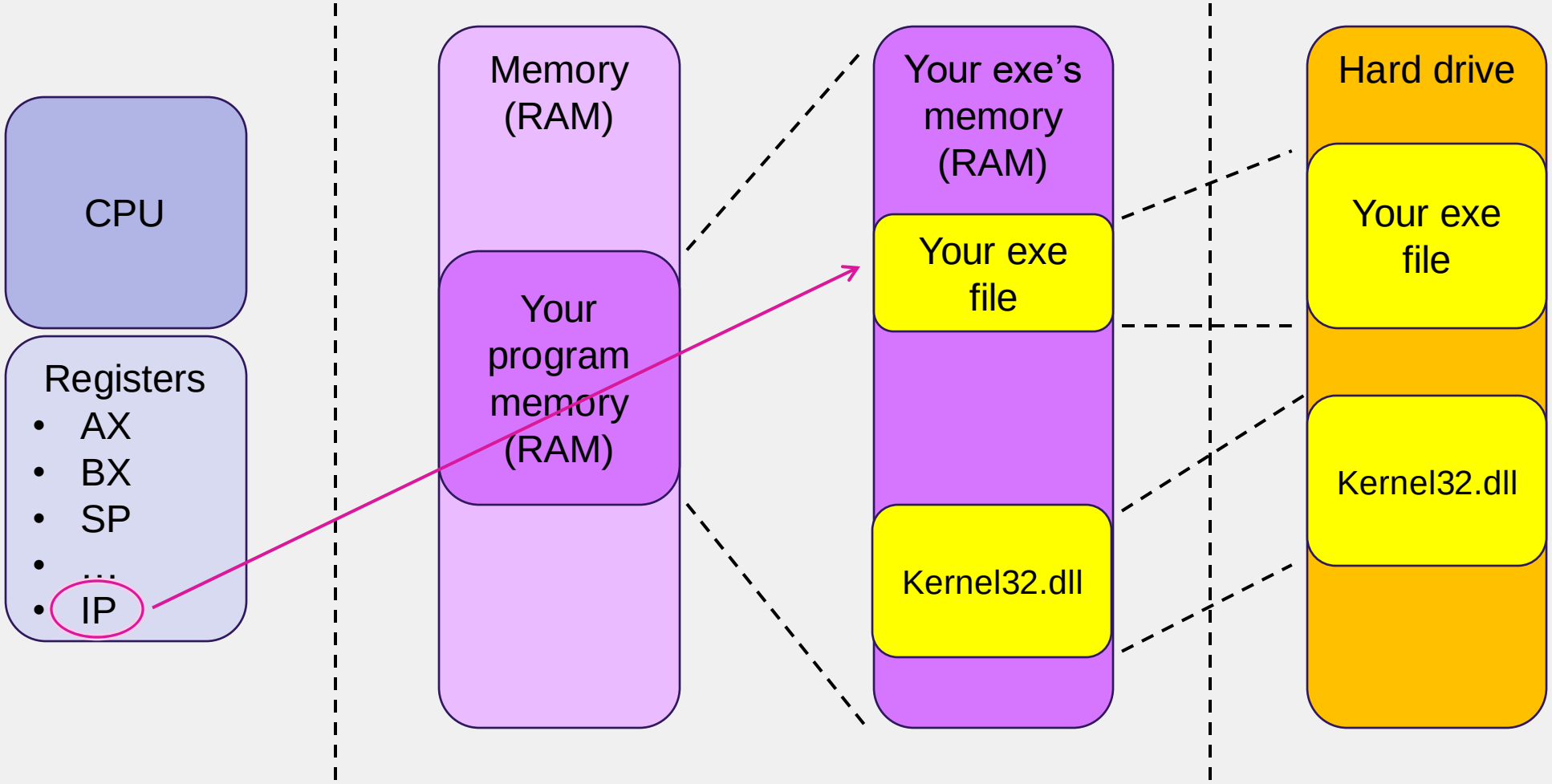
A : Initially, the only subroutine referencing the URL is 0x1400035B8

Two call chains to that subroutines:

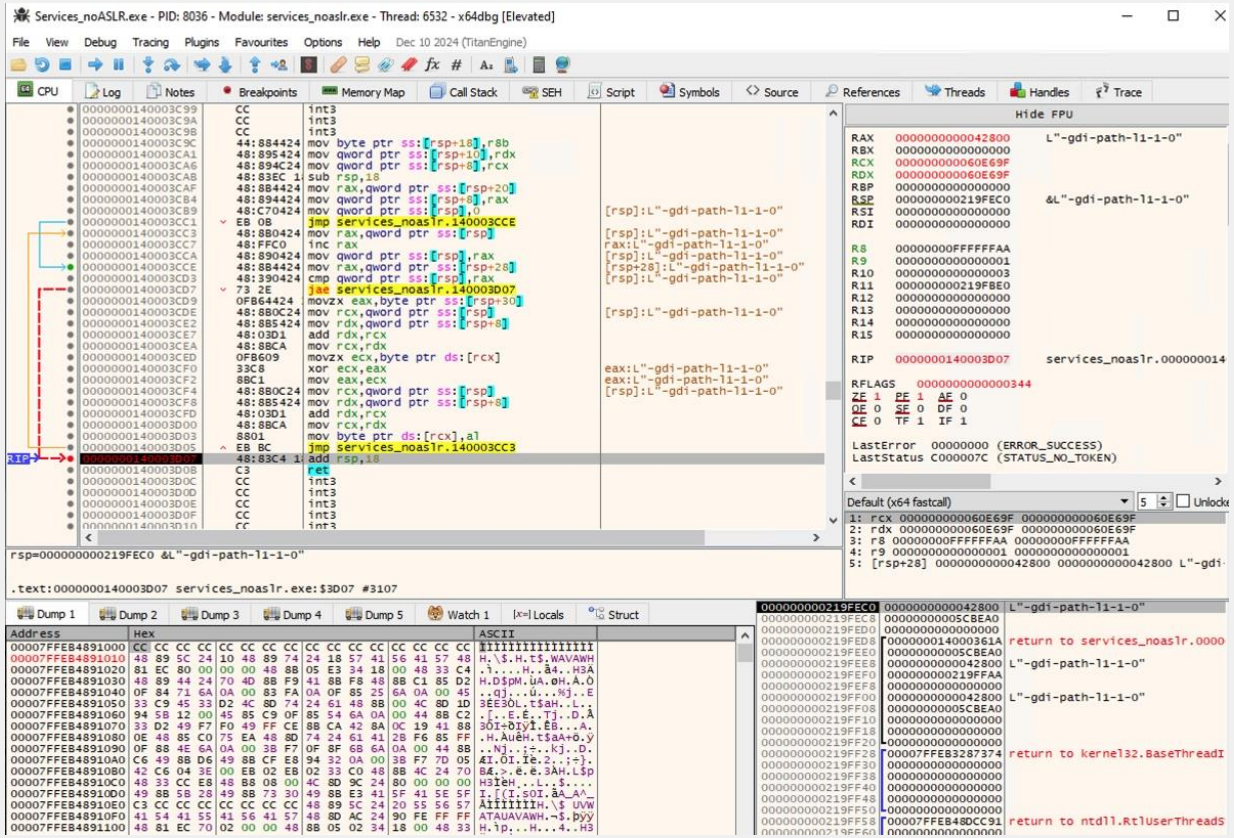
- start -> 0x1400035B8
- start -> 0x1400038A0 -> 0x1400037CC -> 0x140003470 -> 0x1400035B8

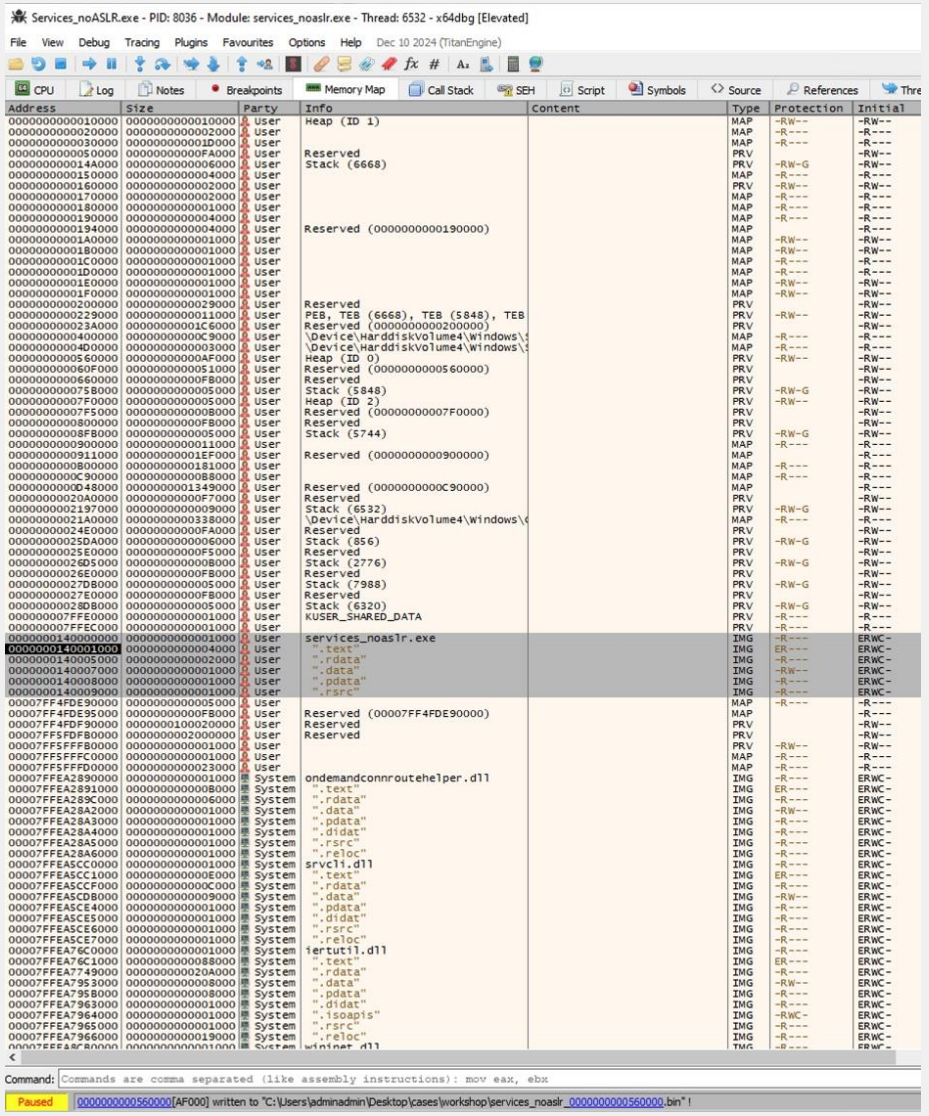


Dynamic analysis : what happens when you run a file?



Dynamic analysis : x64dbg, sysinternals suite





Exercise / Q&A Break

Q : What is this program doing with the file it gets from the URL?

A : It downloads a binary file then XOR deciphers it.

THANK YOU!!!
Any questions??