SİBERKOZA PLATFORM CYBER THREAT INTELLIGENCE REPORT

AYŞENUR ASLAN

İÇİNDEKİLER

1. WEEK 1: SHARPENİNG THE KNİVES

1.1 MITRE ATT&CK framework

After reviewing the latest updates and additions to the MITRE ATT&CK framework, I refreshed my understanding of the attack stages, tactics, techniques, and procedures (TTPs) commonly used by attackers.

The ATT&CK framework categorizes attacks under the following tactics:

1. Initial Access
2. Execution
3. Persistence
4. Privilege Escalation
5. Defense Evasion
6. Credential Access
7. Discovery
8. Lateral Movement
9. Collection
10. Exfiltration
11. Command and Control
12. Impact

Under each tactic, there is a range of techniques and procedures commonly employed by attackers, which clearly define the methods they use to compromise and exploit the target system.

The latest updates and additions reflect the fact that attackers are transitioning to more sophisticated and complex attack techniques, enhancing their ability to evade defense mechanisms. Additionally, there is a focus on new threat areas such as attacks in cloud environments and IoT (Internet of Things) devices.

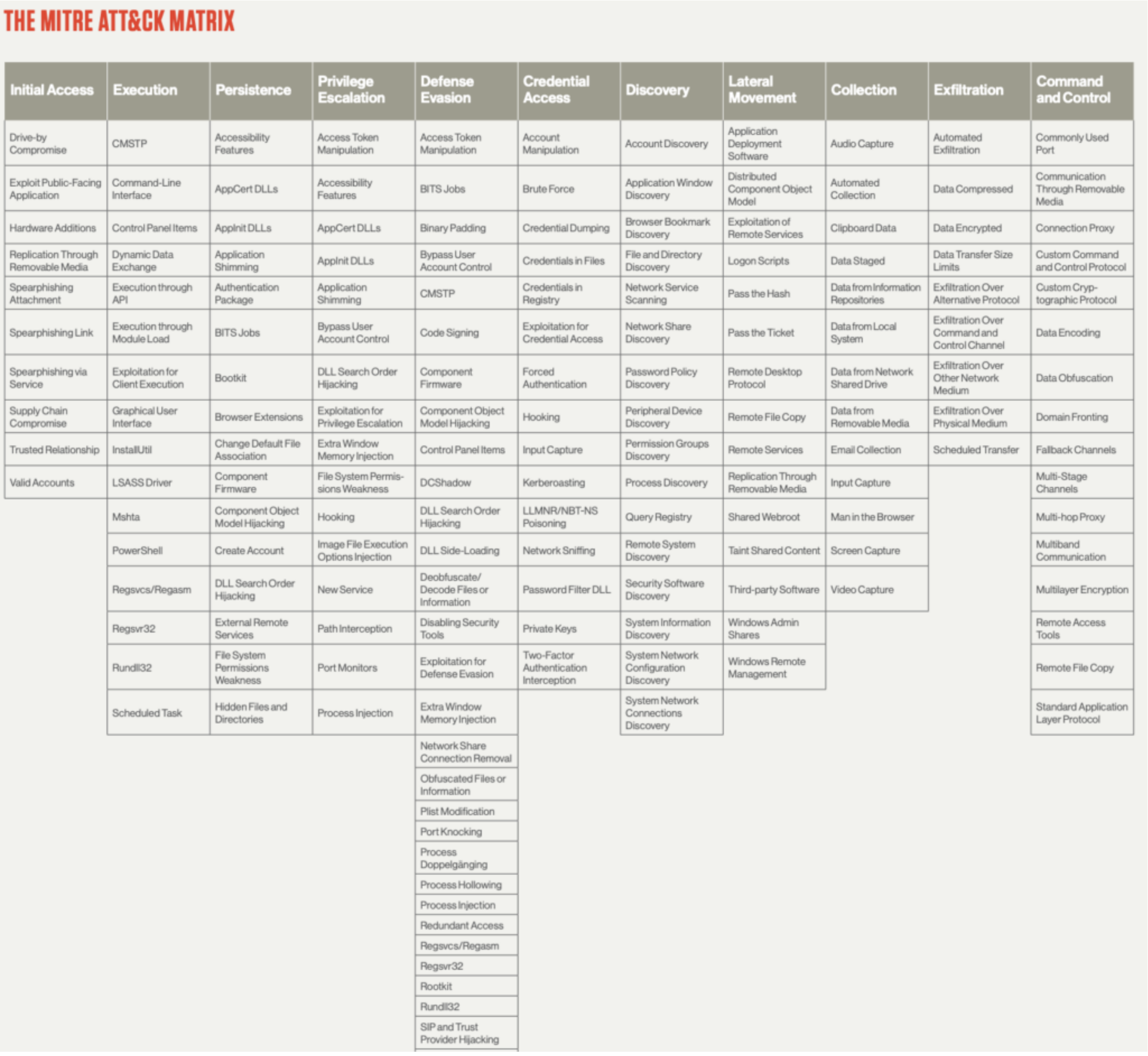
These updates and additions enable security professionals to understand a broader attack surface and implement effective defense measures, aiding them in enhancing their defense strategies.

Additionally, the latest updates to the MITRE ATT&CK framework also highlight the evolving nature of cyber threats and the need for continuous adaptation in defense strategies. Attackers are increasingly leveraging advanced tactics such as living off the land (LotL) techniques, which involve the use of legitimate tools and processes already present in the target environment to evade detection.

Moreover, there is a growing emphasis on the importance of threat intelligence sharing and collaboration among organizations to better understand and mitigate emerging threats. The framework encourages the integration of threat intelligence feeds and the use of shared resources to enhance detection and response capabilities.

Furthermore, the inclusion of cloud-specific attack techniques underscores the significance of securing cloud environments as organizations increasingly migrate their infrastructure and services to the cloud. This highlights the need for robust cloud security measures and awareness among security teams to address the unique challenges posed by cloud-based attacks.

Overall, the MITRE ATT&CK framework continues to evolve to address the changing threat landscape, providing valuable insights and guidance for cybersecurity professionals to effectively defend against sophisticated adversaries.



THE MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permissions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection		System Network Connections Discovery				Standard Application Layer Protocol
				Network Share Connection Removal						
				Obfuscated Files or Information						
				Plist Modification						
				Port Knocking						
				Process Doppelgänging						
				Process Hollowing						
				Process Injection						
				Redundant Access						
				Regsvcs/Regasm						
				Regsvr32						
				Rootkit						
				Rundll32						
				SIP and Trust Provider Hijacking						

1.2 CISA SET

CISA CSET (Cybersecurity Evaluation Tool) is a portal that provides cybersecurity evaluation tools and resources for organizations to assess their security posture and enhance their cybersecurity resilience. Upon exploring this platform, I focused on tools relevant to threat intelligence gathering, including vulnerability scanners and malware analysis platforms.

1. Vulnerability Scanners: CSET offers various vulnerability scanning tools designed to identify weaknesses and security gaps within an organization's IT infrastructure. These tools scan networks, systems, and applications to detect known vulnerabilities and misconfigurations that could be exploited by attackers. By identifying and prioritizing vulnerabilities, organizations can take proactive measures to remediate them and reduce their exposure to potential cyber threats.

2. Malware Analysis Platforms: CSET also provides access to malware analysis platforms that enable organizations to analyze and dissect malicious software samples. These platforms help security analysts understand the behavior and characteristics of malware, identify indicators of compromise (IOCs), and develop effective countermeasures to prevent malware infections and mitigate their impact. By analyzing malware samples, organizations can enhance their threat intelligence capabilities and improve their ability to detect and respond to cyber threats effectively.

Overall, CISA CSET serves as a valuable resource for organizations seeking to strengthen their cybersecurity defenses and enhance their threat intelligence capabilities. By leveraging the tools and resources available on this platform, organizations can conduct comprehensive security assessments, identify vulnerabilities and threats, and implement proactive security measures to protect their assets from cyber attacks.

1.3 ANALYSİS OF THREATPOST'S 2023 THREAT LANDSCAPE REPORT

ThreatPost's 2023 Threat Landscape Report provides valuable insights into the prominent threats, trends, and attacker motivations impacting the cyber landscape. Here's a summary of the key findings:

1. Prominent Threats:

- Ransomware Attacks: Ransomware continues to be a dominant threat, targeting organizations across various sectors and causing significant financial and operational damage.

- Supply Chain Compromises: Attacks targeting software supply chains have increased, with threat actors infiltrating trusted vendors to distribute malware and exploit vulnerabilities.

- Nation-State Threats: Nation-state actors pose a significant threat, conducting espionage, sabotage, and cyber warfare campaigns targeting government agencies, critical infrastructure, and private sector organizations.

2. Trends:

- Sophistication of Attacks: Cyberattacks are becoming increasingly sophisticated, leveraging advanced techniques such as zero-day exploits, fileless malware, and supply chain hijacking.

- Expansion of Attack Surface: The proliferation of IoT devices, cloud services, and remote work environments has expanded the attack surface, providing adversaries with more opportunities to exploit vulnerabilities.

- Evolution of Ransomware: Ransomware operators are evolving their tactics, including double extortion schemes, targeting of critical infrastructure, and collaboration with affiliate groups.

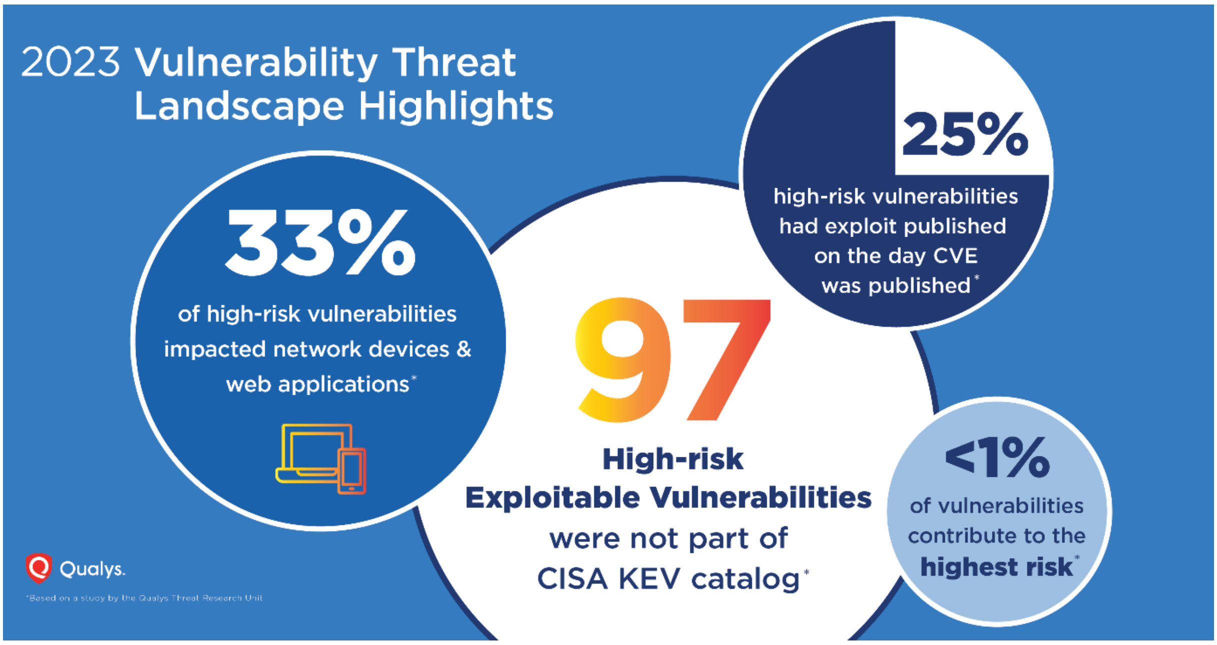
3. Attacker Motivations:

- Financial Gain: Many cyberattacks are motivated by financial gain, with ransomware operators demanding large ransom payments and threat actors monetizing stolen data through dark web markets.

- Espionage and Sabotage: Nation-state actors engage in cyber espionage and sabotage campaigns to steal sensitive information, disrupt critical services, and gain geopolitical advantage.

- Ideological and Political Motivations: Some threat actors are driven by ideological or political motives, targeting organizations or individuals perceived as adversaries or aligned with specific ideologies.

In summary, ThreatPost's 2023 Threat Landscape Report highlights the persistent threat of ransomware attacks, supply chain compromises, and nation-state threats in the cyber landscape. The report also underscores the evolving nature of cyber threats, with attackers leveraging sophisticated techniques and targeting emerging attack surfaces. Understanding these key findings is essential for organizations to strengthen their cybersecurity defenses and mitigate the impact of evolving cyber threats.



1.4 SANS INSTITUTE RESOURCES

Research on Cyber Threats and Threat Intelligence from SANS Institute

The SANS Institute is renowned for its comprehensive resources on cybersecurity, including research papers, reports, and training materials. In exploring their offerings, I focused on cyber threats and threat intelligence, selecting several relevant resources to delve deeper into specific topics.

1. **"SANS 2023 Cyber Threat Intelligence Survey"**

- This survey report provides insights into the current landscape of cyber threat intelligence (CTI) practices, challenges, and trends. It covers areas such as the effectiveness of CTI programs, integration with security operations, and emerging threats. Through this report, I gained valuable insights into the strategies and tactics organizations are employing to combat evolving cyber threats.

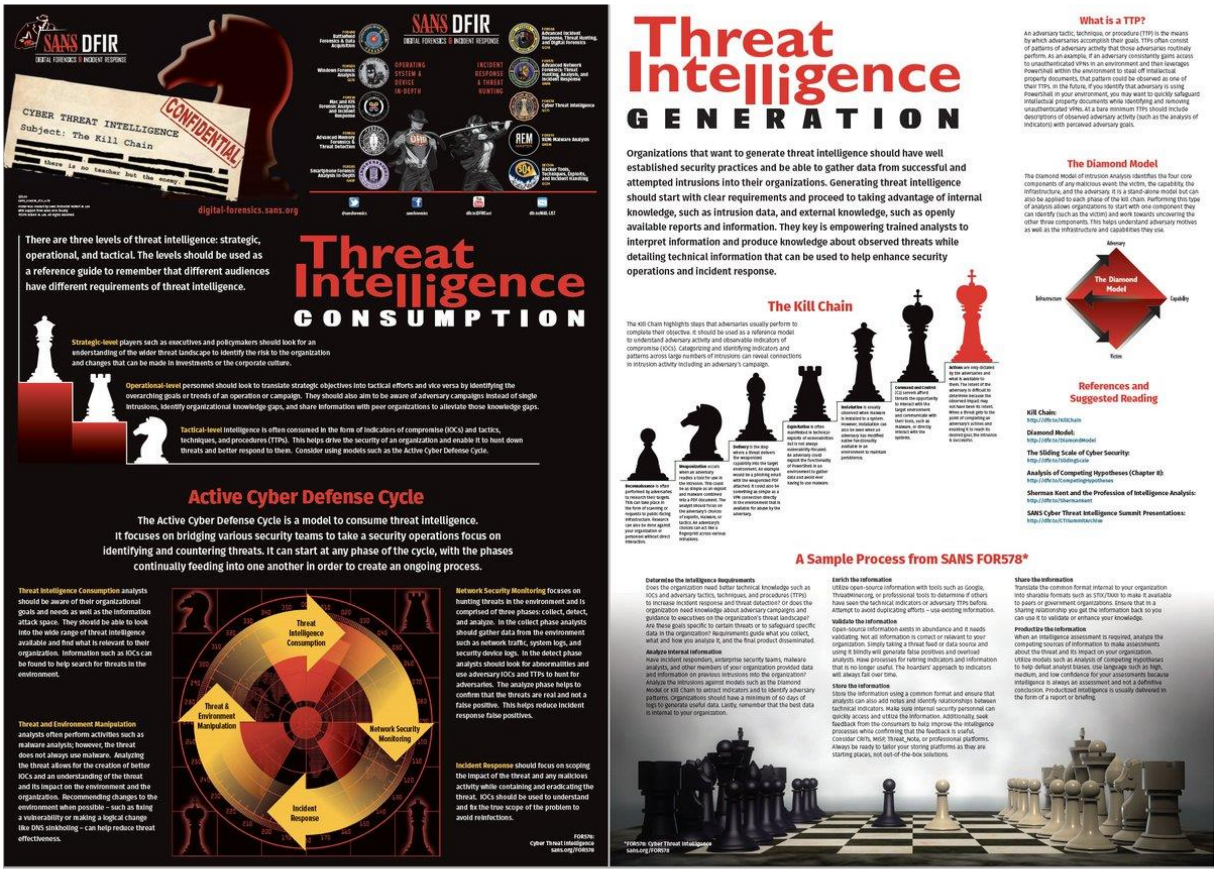
2. **"Threat Hunting and Incident Response Summit"**

- SANS hosts summits that bring together industry experts and practitioners to discuss cutting-edge strategies for threat hunting and incident response. By exploring the materials from these summits, including presentation slides, whitepapers, and recorded sessions, I gained deeper insights into proactive threat detection techniques, incident response best practices, and real-world case studies.

3. **"SEC511: Continuous Monitoring and Security Operations"**

   - This SANS training course focuses on building robust security operations centers (SOCs) capable of continuous monitoring and rapid incident response. By reviewing the course syllabus and sample materials, such as lecture slides and hands-on labs, I learned about the tools, techniques, and processes necessary to detect and respond to cyber threats effectively.

Through my exploration of these SANS Institute resources, I gained a deeper understanding of cyber threats and threat intelligence, including current trends, best practices, and practical implementation strategies for enhancing organizational cybersecurity posture. These resources serve as valuable assets for cybersecurity professionals seeking to stay ahead in an ever-evolving threat landscape.


SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE
CYBER THREAT INTELLIGENCE
Subject: The Kill Chain
CONFIDENTIAL
there is no teacher but the enemy.
digital-forensics.sans.org
Battlefield Forensics & Data Acquisition
Windows Forensic Analysis
Mac and iOS Forensic Analysis and Incident Response
Advanced Memory Forensics & Threat Detection
Smartphone Forensic Analysis In-Depth
OPERATING SYSTEM & DEVICE IN-DEPTH
INCIDENT RESPONSE & THREAT HUNTING
Advanced Incident Response, Threat Hunting, and Digital Forensics
Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response
Cyber Threat Intelligence
REM: Malware Analysis
Hacker Tools, Techniques, Exploits, and Incident Handling
Threat Intelligence Consumption
Network Security Monitoring
Incident Response
Threat & Environment Manipulation
Adversary
Infrastructure
The Diamond Model
Capability
Victim

Threat Intelligence CONSUMPTION

There are three levels of threat intelligence: strategic, operational, and tactical. The levels should be used as a reference guide to remember that different audiences have different requirements of threat intelligence.

Strategic-level players such as executives and policymakers should look for an understanding of the wider threat landscape to identify the risk to the organization and changes that can be made in investments or the corporate culture.

Operational-level personnel should look to translate strategic objectives into tactical efforts and vice versa by identifying the overarching goals or trends of an operation or campaign. They should also aim to be aware of adversary campaigns instead of single intrusions, identify organizational knowledge gaps, and share information with peer organizations to alleviate those knowledge gaps.

Tactical-level intelligence is often consumed in the form of indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs). This helps drive the security of an organization and enable it to hunt down threats and better respond to them. Consider using models such as the Active Cyber Defense Cycle.

Active Cyber Defense Cycle

The Active Cyber Defense Cycle is a model to consume threat intelligence. It focuses on bridging various security teams to take a security operations focus on identifying and countering threats. It can start at any phase of the cycle, with the phases continually feeding into one another in order to create an ongoing process.

Threat Intelligence Consumption analysts should be aware of their organizational goals and needs as well as the information attack space. They should be able to look into the wide range of threat intelligence available and find what is relevant to their organization. Information such as IOCs can be found to help search for threats in the environment.

Threat and Environment Manipulation analysts often perform activities such as malware analysis; however, the threat does not always use malware. Analyzing the threat allows for the creation of better IOCs and an understanding of the threat and its impact on the environment and the organization. Recommending changes to the environment when possible – such as fixing a vulnerability or making a logical change like DNS sinkholing – can help reduce threat effectiveness.

Network Security Monitoring focuses on hunting threats in the environment and is comprised of three phases: collect, detect, and analyze. In the collect phase analysts should gather data from the environment such as network traffic, system logs, and security device logs. In the detect phase analysts should look for abnormalities and use adversary IOCs and TTPs to hunt for adversaries. The analyze phase helps to confirm that the threats are real and not a false positive. This helps reduce incident response false positives.

Incident Response should focus on scoping the impact of the threat and any malicious activity while containing and eradicating the threat. IOCs should be used to understand and fix the true scope of the problem to avoid reinfections.

FOR578:
Cyber Threat Intelligence
sans.org/FOR578

Threat Intelligence GENERATION

Organizations that want to generate threat intelligence should have well established security practices and be able to gather data from successful and attempted intrusions into their organizations. Generating threat intelligence should start with clear requirements and proceed to taking advantage of internal knowledge, such as intrusion data, and external knowledge, such as openly available reports and information. They key is empowering trained analysts to interpret information and produce knowledge about observed threats while detailing technical information that can be used to help enhance security operations and incident response.

The Kill Chain

The Kill Chain highlights steps that adversaries usually perform to complete their objective. It should be used as a reference model to understand adversary activity and observable indicators of compromise (IOCs). Categorizing and identifying indicators and patterns across large numbers of intrusions can reveal connections in intrusion activity including an adversary's campaign.

Reconnaissance is often performed by adversaries to research their targets. This can take place in the form of scanning or requests to public facing infrastructure. Research can also be done against your organization or personnel without direct interaction.

Weaponization occurs when an adversary readies a tool for use in the intrusion. This could be as simple as an exploit and malware combined into a PDF document. The analyst should focus on the adversary's choices of exploits, malware, or tactics. An adversary's choices can act like a fingerprint across various intrusions.

Delivery is the step where a threat delivers the weaponized capability into the target environment. An example would be a phishing email with the weaponized PDF attached. It could also be something as simple as a VPN connection directly to the environment that is available for abuse by the adversary.

Exploitation is often manifested in technical exploits of vulnerabilities but is not always vulnerability-focused. An adversary could exploit the functionality of PowerShell in an environment to gather data and avoid ever having to use malware.

Installation is usually observed when malware is installed to a system. However, installation can also be seen when an adversary has modified native functionality available in an environment to maintain persistence.

Command and Control (C2) servers afford threats the opportunity to interact with the target environment and communicate with their tools, such as malware, or directly interact with the systems.

Actions are only dictated by the adversaries and what is available to them. The intent of the adversary is difficult to determine because the observed impact may not have been its intent. When a threat gets to the point of completing an adversary's actions and enabling it to reach its desired goal, the intrusion is successful.

What is a TTP?

An adversary tactic, technique, or procedure (TTP) is the means by which adversaries accomplish their goals. TTPs often consist of patterns of adversary activity that those adversaries routinely perform. As an example, if an adversary consistently gains access to unauthenticated VPNs in an environment and then leverages PowerShell within the environment to steal off intellectual property documents, that pattern could be observed as one of their TTPs. In the future, if you identify that adversary is using PowerShell in your environment, you may want to quickly safeguard intellectual property documents while identifying and removing unauthenticated VPNs. At a bare minimum TTPs should include descriptions of observed adversary activity (such as the analysis of indicators) with perceived adversary goals.

The Diamond Model

The Diamond Model of Intrusion Analysis identifies the four core components of any malicious event: the victim, the capability, the infrastructure, and the adversary. It is a stand-alone model but can also be applied to each phase of the kill chain. Performing this type of analysis allows organizations to start with one component they can identify (such as the victim) and work towards uncovering the other three components. This helps understand adversary motives as well as the infrastructure and capabilities they use.

References and Suggested Reading

Kill Chain:
http://dfir.to/KillChain

Diamond Model:
http://dfir.to/DiamondModel

The Sliding Scale of Cyber Security:
http://dfir.to/SlidingScale

Analysis of Competing Hypotheses (Chapter 8):
http://dfir.to/CompetingHypotheses

Sherman Kent and the Profession of Intelligence Analysis:
http://dfir.to/ShermanKent

SANS Cyber Threat Intelligence Summit Presentations:
http://dfir.to/CTISummitArchive

A Sample Process from SANS FOR578*

Determine the Intelligence Requirements
Does the organization need better technical knowledge such as IOCs and adversary tactics, techniques, and procedures (TTPs) to increase incident response and threat detection? Or does the organization need knowledge about adversary campaigns and guidance to executives on the organization's threat landscape? Are these goals specific to certain threats or to safeguard specific data in the organization? Requirements guide what you collect, what and how you analyze it, and the final product disseminated.

Analyze Internal Information
Have incident responders, enterprise security teams, malware analysts, and other members of your organization provided data and information on previous intrusions into the organization? Analyze the intrusions against models such as the Diamond Model or Kill Chain to extract indicators and to identify adversary patterns. Organizations should have a minimum of 60 days of logs to generate useful data. Lastly, remember that the best data is internal to your organization.

Enrich the Information
Utilize open-source information with tools such as Google, ThreatMiner.org, or professional tools to determine if others have seen the technical indicators or adversary TTPs before. Attempt to avoid duplicating efforts – use existing information.

Validate the Information
Open-source information exists in abundance and it needs validating. Not all information is correct or relevant to your organization. Simply taking a threat feed or data source and using it blindly will generate false positives and overload analysts. Have processes for retiring indicators and information that is no longer useful. The hoarders' approach to indicators will always fail over time.

Store the Information
Store the information using a common format and ensure that analysts can also add notes and identify relationships between technical indicators. Make sure internal security personnel can quickly access and utilize the information. Additionally, seek feedback from the consumers to help improve the intelligence processes while confirming that the feedback is useful. Consider CRITs, MISP, Threat_Note, or professional platforms. Always be ready to tailor your storing platforms as they are starting places, not out-of-the-box solutions.

Share the Information
Translate the common format internal to your organization into sharable formats such as STIX/TAXII to make it available to peers or government organizations. Ensure that in a sharing relationship you get the information back so you can use it to validate or enhance your knowledge.

Productize the Information
When an intelligence assessment is required, analyze the competing sources of information to make assessments about the threat and its impact on your organization. Utilize models such as Analysis of Competing Hypotheses to help defeat analyst biases. Use language such as high, medium, and low confidence for your assessments because intelligence is always an assessment and not a definitive conclusion. Productized intelligence is usually delivered in the form of a report or briefing.

*FOR578: Cyber Threat Intelligence
sans.org/FOR578

2. Week 2: Hunting on the Surface Web

2.1 CISA THREAT MATRIX

Analyzing Recent Incidents and Threats from CISA Threat Matrix

In monitoring the Cybersecurity and Infrastructure Security Agency (CISA) Threat Matrix and subscribing to relevant alerts and advisories, I gained valuable insights into the current threat landscape and potential risks targeting various sectors and critical systems.

1. **Ransomware Attacks on Critical Infrastructure**:

   - Recent incidents highlighted a concerning trend of ransomware attacks targeting critical infrastructure sectors such as energy, healthcare, and transportation. These attacks have the potential to disrupt essential services and cause significant financial and operational damage.

2. **Supply Chain Compromises**:

   - CISA advisories have underscored the persistent threat of supply chain compromises, where adversaries infiltrate trusted vendors or service providers to gain access to target organizations' networks. These incidents pose a substantial risk to organizations relying on third-party services or software.

3. **Exploitation of Zero-Day Vulnerabilities**:

   - CISA alerts have highlighted the exploitation of zero-day vulnerabilities in widely used software and systems. Threat actors leverage these vulnerabilities to conduct targeted attacks, often with devastating consequences. Patch management and vulnerability remediation remain critical priorities for organizations to mitigate these risks.

4. **Phishing and Social Engineering Attacks**:

   - CISA advisories frequently address the ongoing threat of phishing and social engineering attacks, emphasizing the importance of user awareness training and robust email security measures. These attacks continue to be a primary vector for delivering malware, stealing credentials, and compromising sensitive data.

5. **Emerging Threats and TTPs**:

   - CISA alerts regularly highlight emerging threats and adversary tactics, techniques, and procedures (TTPs), enabling organizations to proactively adapt their security controls and defenses. Staying informed about evolving threats is essential for maintaining a resilient cybersecurity posture.

Through my analysis of recent incidents and threats from the CISA Threat Matrix, I gained a deeper understanding of the evolving cybersecurity landscape and identified potential risks relevant to my organization's sector and critical systems. By leveraging this intelligence, organizations can enhance their threat detection capabilities, strengthen defenses, and mitigate the impact of cyber threats. Ongoing vigilance and proactive measures are essential to staying ahead of malicious actors and safeguarding against emerging threats.

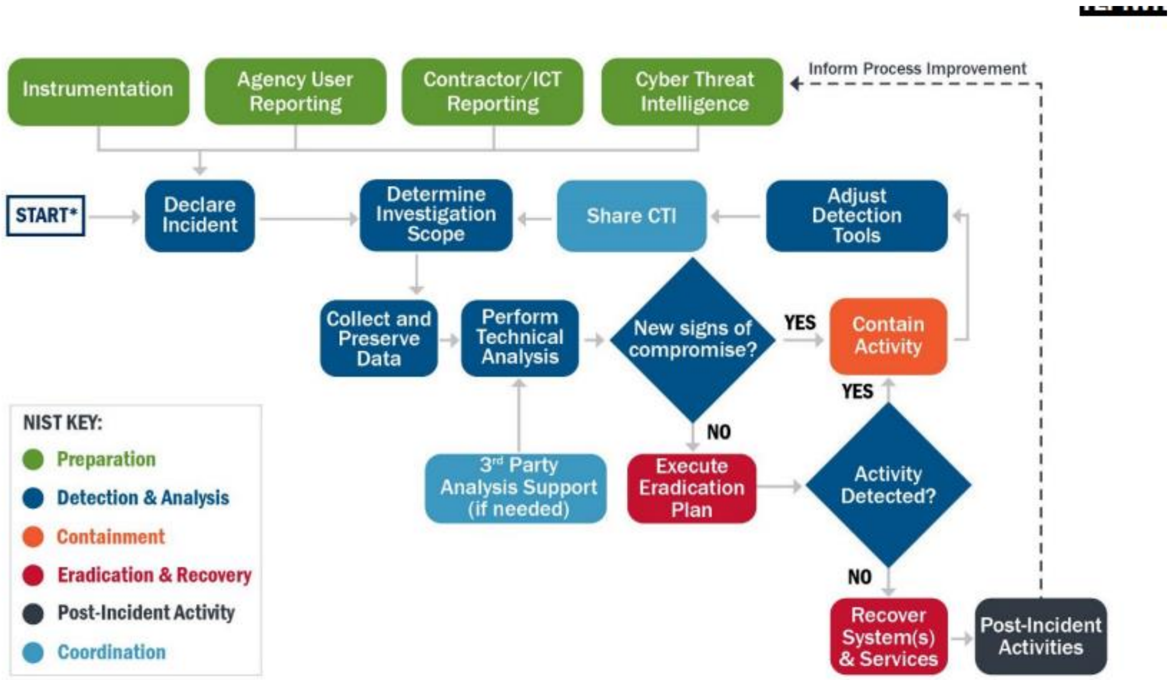
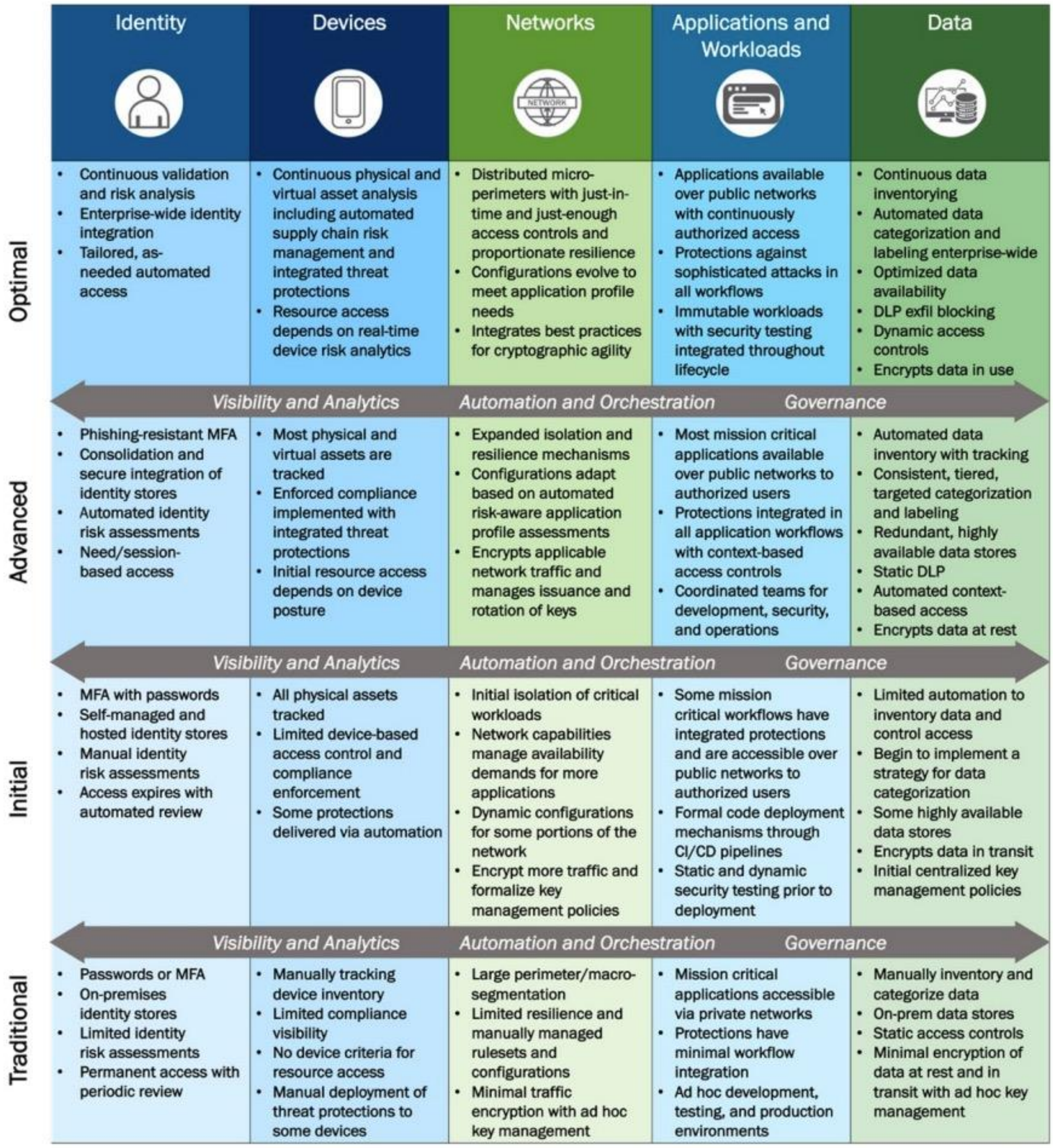


Figure 1: Incident Response Process



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
		Visibility and Analytics	*Automation and Orchestration*		*Governance*
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
		Visibility and Analytics	*Automation and Orchestration*		*Governance*
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
		Visibility and Analytics	*Automation and Orchestration*		*Governance*
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

2.2 THREAT NEWS SITES

Cybersecurity Threat News Scan Report

In regularly scanning cybersecurity news sites for reports on emerging vulnerabilities, malware campaigns, and attacker tactics, I've gained valuable insights into the evolving threat landscape. Here's a summary of what I've learned:

1. Emerging Vulnerabilities:

- News reports have highlighted the discovery of several critical vulnerabilities in widely used software and systems, including operating systems, web applications, and IoT devices.

- Vulnerabilities such as remote code execution (RCE), privilege escalation, and authentication bypass pose significant risks to organizations' security posture if left unpatched.

2. Malware Campaigns:

- Recent news coverage has detailed various malware campaigns targeting organizations across different sectors, including ransomware, trojans, and botnets.

- Notable malware variants, such as Ryuk, TrickBot, and Emotet, continue to evolve in sophistication and evasion techniques, posing challenges to traditional security defenses.

3. Attacker Tactics:

- Reports have shed light on the tactics, techniques, and procedures (TTPs) employed by cybercriminals and nation-state actors to infiltrate networks and exfiltrate sensitive data.

- Tactics such as phishing, supply chain attacks, and zero-day exploits remain prevalent, emphasizing the need for robust cybersecurity measures and threat intelligence sharing.

4. Focus Areas and Prioritization:

- Aligning with my organization's focus areas and risk profile, I've prioritized news coverage of threats relevant to critical infrastructure sectors, cloud environments, and remote work security.

- By prioritizing threats based on their potential impact, I can allocate resources effectively to mitigate the most pressing risks and bolster our defensive posture.

5. Proactive Measures:

- Regularly monitoring cybersecurity news sites enables proactive threat intelligence gathering and early detection of emerging threats.

- Leveraging this information, my organization can implement timely security patches, update threat detection signatures, and enhance employee awareness training to mitigate the risk of cyberattacks.

In conclusion, scanning cybersecurity news sites for reports on emerging threats provides invaluable insights into the evolving threat landscape, enabling organizations to stay informed, proactive, and resilient in the face of cyber threats. By prioritizing threats aligned with focus areas and potential impact, organizations can effectively allocate resources and mitigate risks to safeguard their digital assets and operations.

2.3 THREAT SHARING COMMUNITIES

Exploration of Threat Sharing Communities: OTX and VirusTotal

In delving into threat sharing communities such as OTX (Open Threat Exchange) and VirusTotal, I've gained valuable insights into ongoing discussions and campaigns related to my chosen threats. Here's a summary of what I've learned:

1. Ongoing Discussions and Campaigns:

- Within OTX and VirusTotal, I discovered active discussions and reports regarding emerging vulnerabilities, malware campaigns, and attacker tactics relevant to my focus areas.

- Community members share insights, analysis, and threat intelligence, fostering collaboration and collective defense against cyber threats.

2. Indicators of Compromise (IOCs):

- Through OTX and VirusTotal, I analyzed indicators of compromise (IOCs) such as IP addresses, domain names, file hashes, and URLs associated with known malware campaigns and malicious activity.

- By correlating IOCs across multiple sources and leveraging threat intelligence feeds, I gained a comprehensive understanding of the tactics and infrastructure employed by threat actors.

3. Malware Samples Analysis:

- Both OTX and VirusTotal provide access to malware samples uploaded by users and security researchers, allowing for in-depth analysis of malicious code and behavior.

- By examining malware samples, including ransomware, trojans, and exploit kits, I gained insights into attacker techniques, malware capabilities, and potential impact on targeted systems.

4. Attacker Techniques and Potential Impact:

- Analysis of IOCs and malware samples revealed common attacker techniques such as spear-phishing, command and control (C2) communication, and lateral movement within networks.

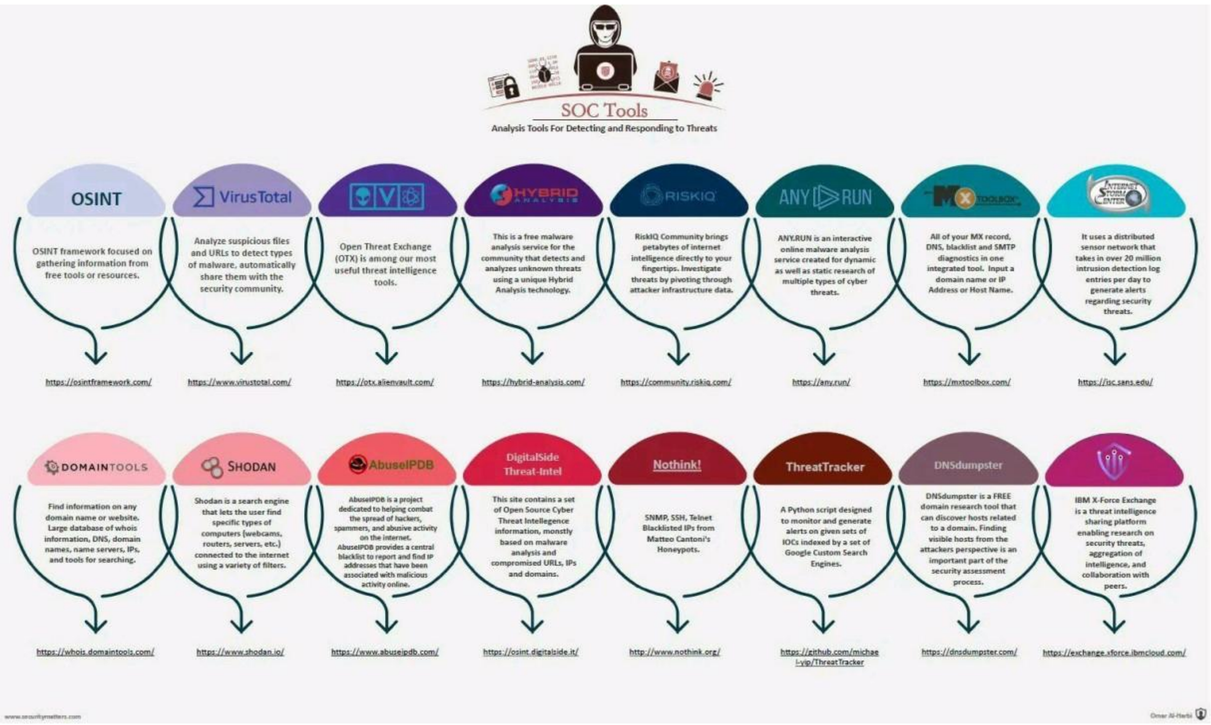
- Understanding these techniques enables proactive threat hunting, detection, and mitigation strategies to defend against cyberattacks and minimize their impact on organizations.

5. Collaboration and Information Sharing:

- Participation in threat sharing communities facilitates collaboration, information exchange, and collective defense efforts among security professionals, researchers, and organizations.

- By contributing to the community and sharing relevant threat intelligence, I can strengthen the collective resilience of the cybersecurity community and enhance our ability to counter emerging threats effectively.

In conclusion, my exploration of threat sharing communities such as OTX and VirusTotal has provided valuable insights into ongoing discussions, campaigns, and threat indicators relevant to my focus areas. By analyzing IOCs, malware samples, and attacker techniques, I've enhanced my understanding of the evolving threat landscape and identified proactive measures to defend against cyber threats effectively. Continued engagement in these communities will enable me to stay informed, collaborate with peers, and contribute to the collective effort to combat cybercrime.



SOC Tools

Analysis Tools For Detecting and Responding to Threats

OSINT: OSINT framework focused on gathering information from free tools or resources. https://osintframework.com/

VirusTotal: Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community. https://www.virustotal.com/

OTX: Open Threat Exchange (OTX) is among our most useful threat intelligence tools. https://otx.alienvault.com/

HYBRID ANALYSIS: This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology. https://hybrid-analysis.com/

RISKIQ: RiskIQ Community brings petabytes of internet intelligence directly to your fingertips. Investigate threats by pivoting through attacker infrastructure data. https://community.riskiq.com/

ANY RUN: ANY.RUN is an interactive online malware analysis service created for dynamic as well as static research of multiple types of cyber threats. https://any.run/

MX TOOLBOX: All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a domain name or IP Address or Host Name. https://mxtoolbox.com/

INTERNET STORM CENTER: It uses a distributed sensor network that takes in over 20 million intrusion detection log entries per day to generate alerts regarding security threats. https://isc.sans.edu/

DOMAINTOOLS: Find information on any domain name or website. Large database of whois information, DNS, domain names, name servers, IPs, and tools for searching. https://whois.domaintools.com/

SHODAN: Shodan is a search engine that lets the user find specific types of computers (webcams, routers, servers, etc.) connected to the internet using a variety of filters. https://www.shodan.io/

AbuseIPDB: AbuseIPDB is a project dedicated to helping combat the spread of hackers, spammers, and abusive activity on the internet. AbuseIPDB provides a central blacklist to report and find IP addresses that have been associated with malicious activity online. https://www.abuseipdb.com/

DigitalSide Threat-Intel: This site contains a set of Open Source Cyber Threat Intellegence information, monstly based on malware analysis and compromised URLs, IPs and domains. https://osint.digitalside.it/

Nothink!: SNMP, SSH, Telnet Blacklisted IPs from Matteo Cantoni's Honeypots. http://www.nothink.org/

ThreatTracker: A Python script designed to monitor and generate alerts on given sets of IOCs indexed by a set of Google Custom Search Engines. https://github.com/michael-yip/ThreatTracker

DNSdumpster: DNSdumpster is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process. https://dnsdumpster.com/

IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with peers. https://exchange.xforce.ibmcloud.com/

www.securitymatters.com

Omar Al-Harbi

2.4 MAPPİNG THREATS TO MITRE ATT&CK FRAMEWORK

Through the gathered intelligence, I've mapped identified threats to relevant stages and tactics in the MITRE ATT&CK framework. Here's a brief report summarizing the findings:

1. Ransomware Attacks:

- **Initial Access:** Threat actors commonly gain initial access through phishing emails containing malicious attachments or links, exploiting vulnerabilities in remote desktop protocols (RDP), or exploiting misconfigurations in internet-facing services.

- **Execution:** Upon gaining access, attackers execute ransomware payloads on compromised systems, encrypting files and demanding ransom payments.

- **Impact:** The impact stage includes actions such as data encryption, file deletion, and displaying ransom notes to victims, causing disruption to critical business operations.

2. Supply Chain Compromises:

- **Initial Access:** Adversaries exploit vulnerabilities in software supply chains to gain initial access, often targeting software vendors or service providers trusted by the target organization.

- **Execution:** Once inside the target network, attackers utilize various techniques such as code injection, malicious updates, or supply chain hijacking to deploy malware payloads or conduct reconnaissance.

- **Impact:** Supply chain compromises can lead to the distribution of malicious software to multiple organizations, resulting in data breaches, unauthorized access, and potential downstream impacts.

3. Phishing and Social Engineering Attacks:

- **Initial Access:** Phishing emails serve as the primary vector for initial access, exploiting human factors through social engineering techniques to trick users into revealing credentials or downloading malicious attachments.

- **Execution:** Attackers leverage harvested credentials to gain unauthorized access to systems and conduct reconnaissance, escalating privileges and deploying additional malware payloads as necessary.

- **Impact:** Phishing and social engineering attacks can result in unauthorized access to sensitive data, compromise of user accounts, and potential financial losses for targeted organizations.

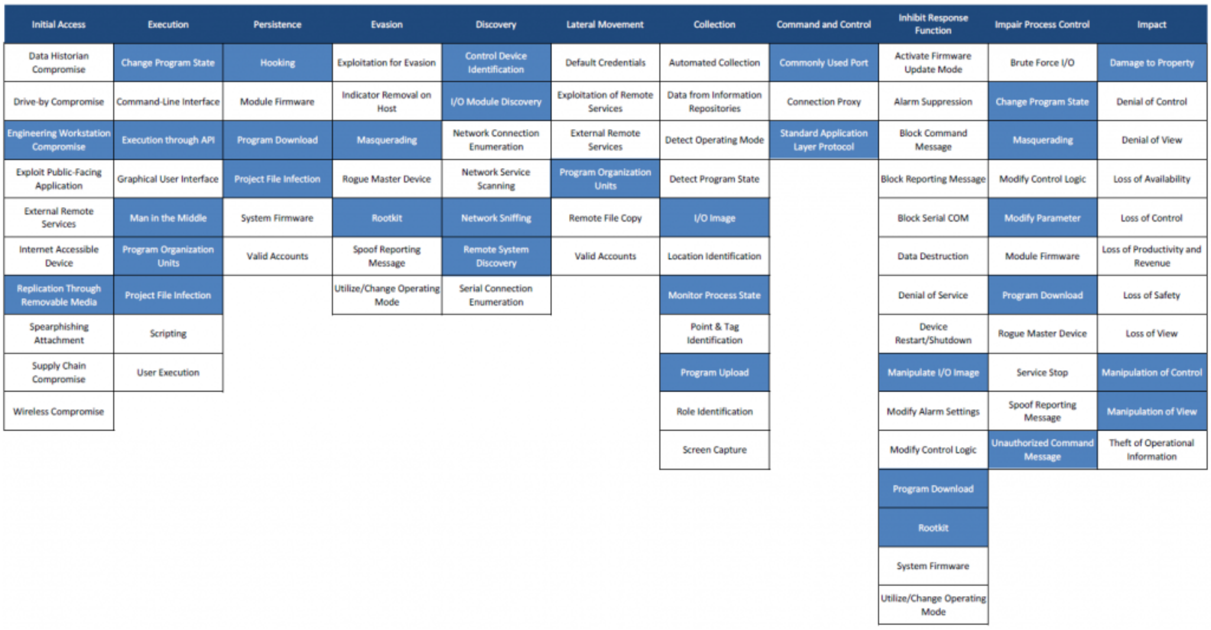
4. Exploitation of Zero-Day Vulnerabilities:

- **Initial Access:** Attackers exploit previously unknown vulnerabilities (zero-days) in software or systems to gain initial access, bypassing existing security controls.

- **Execution:** Upon exploitation, attackers may escalate privileges, execute arbitrary code, or establish persistence within the compromised environment.

- **Impact:** Zero-day exploits can lead to data breaches, system compromise, and disruption of critical services, with potential long-term consequences for affected organizations.

By mapping identified threats to relevant stages and tactics in the MITRE ATT&CK framework, I've visualized attack patterns and assessed potential vulnerabilities within my organization. This analysis helps prioritize security measures, enhance threat detection capabilities, and strengthen defenses against evolving cyber threats.



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

2.5 PRİORİTİZİNG IDENTİFİED THREATS

After conducting a comprehensive analysis, I've ranked the identified threats based on their severity, likelihood of occurrence, and potential impact on our organization. Here's a summary of the prioritized threats:

1. **Ransomware Attacks:**

- **Severity:** High

- **Likelihood:** Moderate to High

- **Impact:** Severe disruption to critical business operations, data loss, financial losses, and reputational damage.

- **Rationale:** Ransomware attacks pose a significant and immediate threat, with the potential for catastrophic consequences. Given their high severity and likelihood, prioritizing defenses against ransomware is paramount.

2. **Supply Chain Compromises:**

- **Severity:** High

- **Likelihood:** Moderate

- **Impact:** Wide-reaching impact on multiple organizations, data breaches, unauthorized access, and downstream disruptions.

- **Rationale:** Supply chain compromises can result in cascading impacts across interconnected networks, making them a critical threat requiring proactive mitigation measures.

3. **Phishing and Social Engineering Attacks:**

- **Severity:** Medium to High

- **Likelihood:** High

- **Impact:** Unauthorized access to sensitive data, compromise of user accounts, and potential financial losses.

- **Rationale:** Phishing and social engineering attacks exploit human vulnerabilities and are frequently used by adversaries to gain initial access. Addressing user awareness and implementing robust email security measures are essential defenses.

4. **Exploitation of Zero-Day Vulnerabilities:**

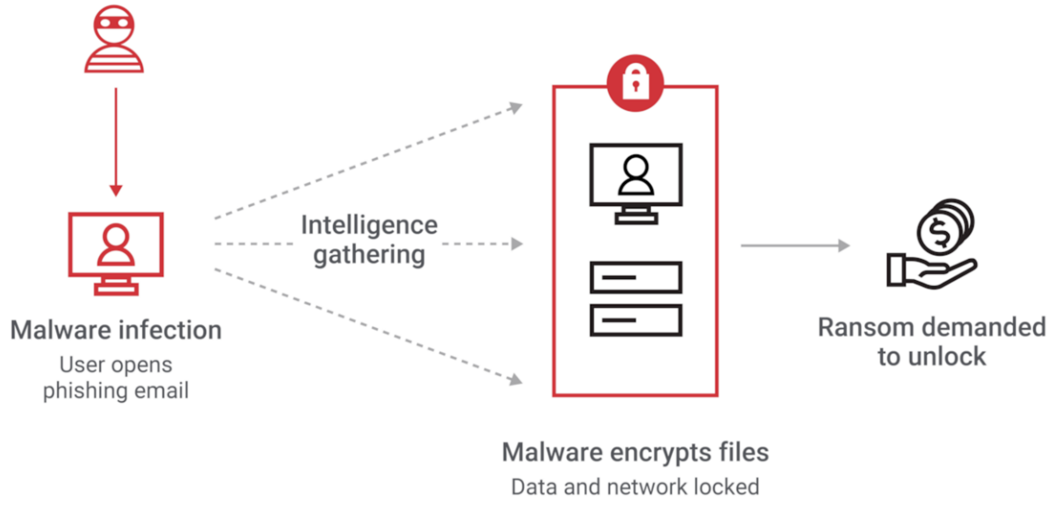
- **Severity:** Medium

- **Likelihood:** Low to Moderate

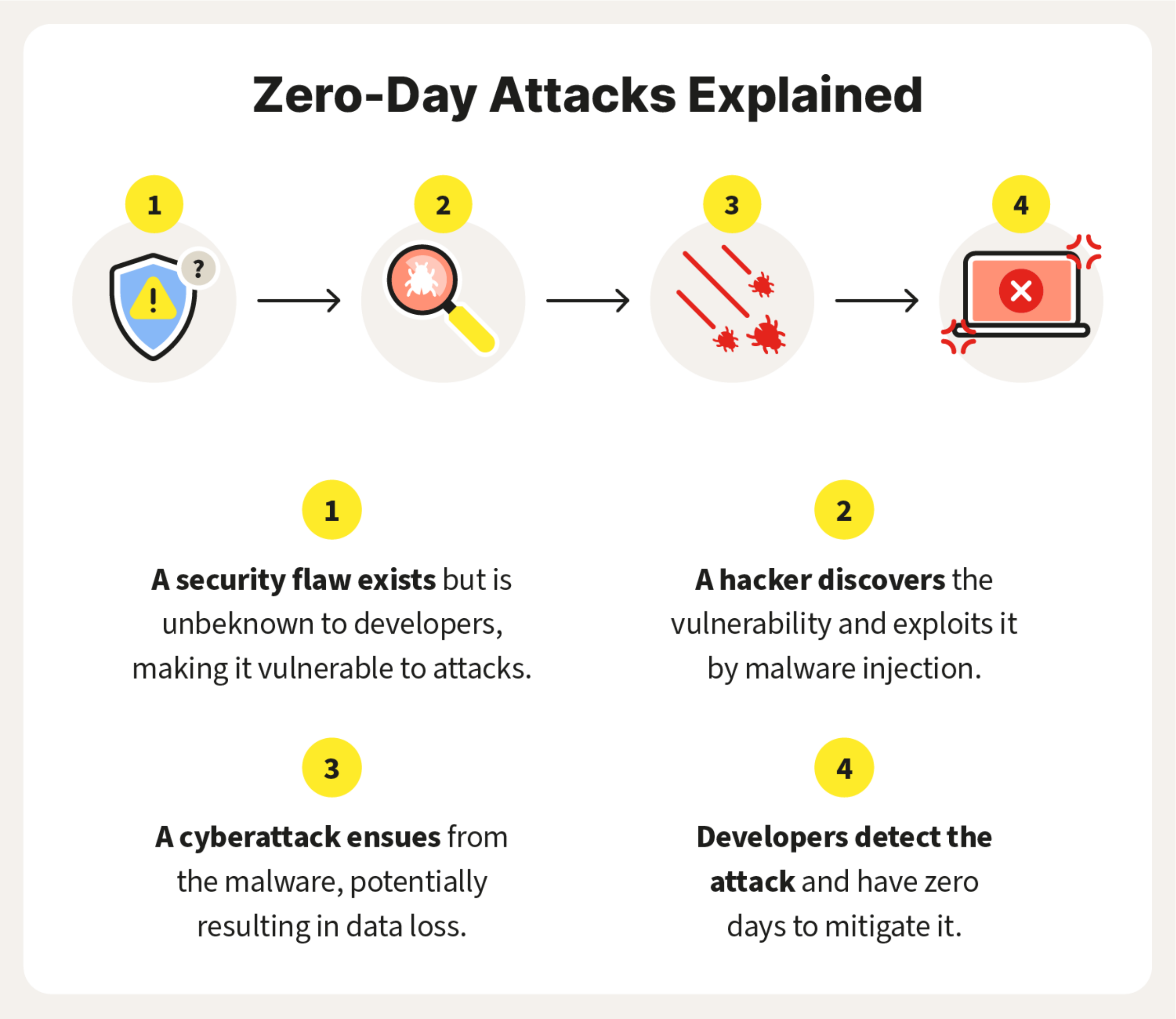
- **Impact:** Data breaches, system compromise, and disruption of critical services.

- **Rationale:** While zero-day vulnerabilities pose a serious threat, their occurrence is less frequent compared to other threats. Nonetheless, proactive vulnerability management and patching remain critical to mitigating this risk.

Based on this prioritization, our initial defensive efforts will focus on strengthening defenses against ransomware attacks, implementing supply chain security measures, enhancing email security to mitigate phishing attacks, and maintaining vigilance against emerging vulnerabilities. By addressing these critical threats first, we can better protect our organization's assets, operations, and reputation from cyber threats.



How ransomware works



Zero-Day Attacks Explained

1

A security flaw exists but is unbeknown to developers, making it vulnerable to attacks.

2

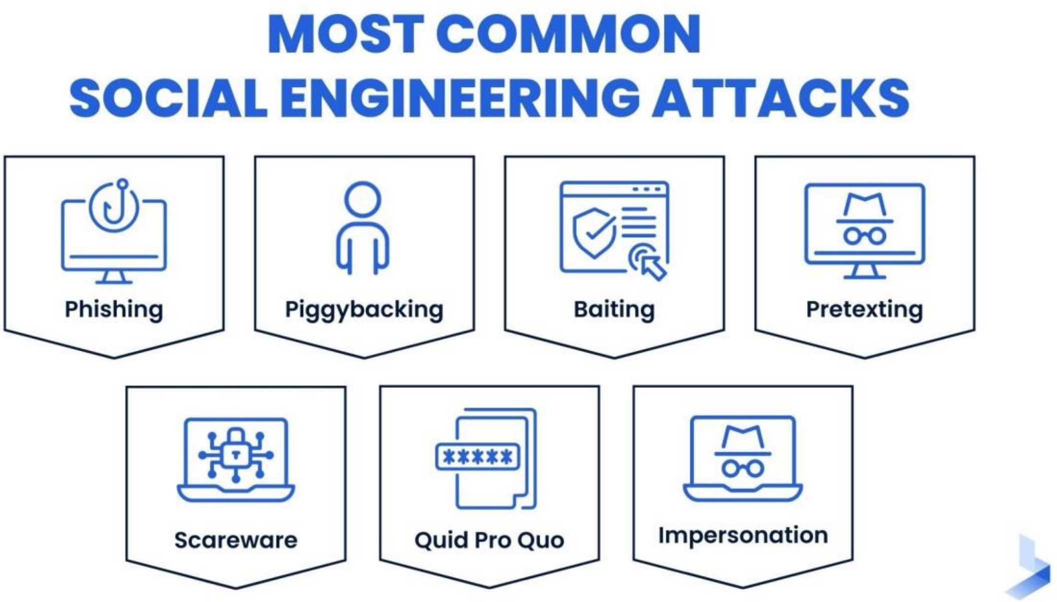
A hacker discovers the vulnerability and exploits it by malware injection.

3

A cyberattack ensues from the malware, potentially resulting in data loss.

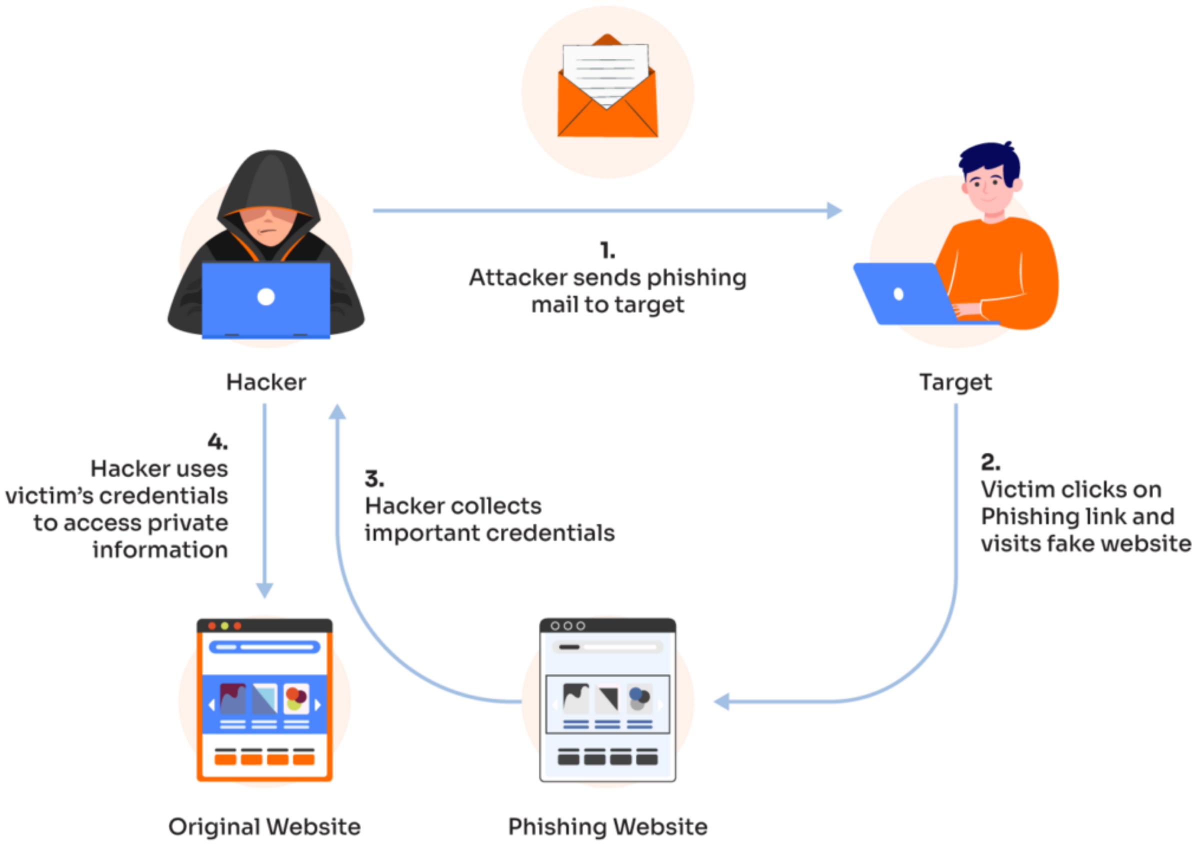
4

Developers detect the attack and have zero days to mitigate it.



MOST COMMON SOCIAL ENGINEERING ATTACKS

- Phishing
- Piggybacking
- Baiting
- Pretexting
- Scareware
- Quid Pro Quo
- Impersonation


1.
Attacker sends phishing mail to target
Hacker
Target
4.
Hacker uses victim's credentials to access private information
3.
Hacker collects important credentials
2.
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

3. WEEK 3: DEEP DİVE AND INTELLİGENCE FUSİON

3.1 DEEP DİVE ON PRİORİTİZED THREATS

In conducting deeper research on the prioritized threats, I focused on ransomware attacks and supply chain compromises, utilizing identified resources to analyze their tactics, techniques, motivations, and potential impact in detail. Here's a summary of my findings:

1. Ransomware Attacks:

Tactics, Techniques, and Procedures (TTPs):

- **Initial Access:** Threat actors commonly gain initial access through phishing emails containing malicious attachments or links, exploiting vulnerabilities in remote desktop protocols (RDP), or exploiting misconfigurations in internet-facing services.

- **Execution:** Once inside the target network, attackers escalate privileges and deploy ransomware payloads across the network, encrypting files and demanding ransom payments.

- **Impact:** Ransomware attacks can cause severe disruption to critical business operations, data loss, financial losses, and reputational damage.

Motivations:

- Financial Gain: Ransomware operators seek financial gain by extorting ransom payments from victims in exchange for decryption keys.

- Disruption and Destruction: Some ransomware attacks may aim to disrupt operations, cause chaos, or inflict damage to targeted organizations, motivated by ideology, revenge, or geopolitical interests.

Potential Impact:

- Severe Business Disruption: Ransomware attacks can cripple operations, leading to downtime, loss of productivity, and disruption of services.

- Data Loss and Financial Losses: Organizations may incur significant financial losses due to ransom payments, remediation costs, regulatory fines, and legal liabilities.

- Reputational Damage: Public disclosure of a ransomware incident can damage an organization's reputation, erode customer trust, and impact business relationships.

2. Supply Chain Compromises:

Tactics, Techniques, and Procedures (TTPs):

- **Initial Access:** Attackers exploit vulnerabilities in software supply chains to gain initial access, often targeting software vendors or service providers trusted by the target organization.

- **Execution:** Upon gaining access, attackers deploy malware payloads or conduct reconnaissance within the target network, leveraging techniques such as code injection, malicious updates, or supply chain hijacking.

- Impact: Supply chain compromises can lead to data breaches, unauthorized access, and downstream disruptions affecting multiple organizations.

*Motivations:

- Wide-Reaching Impact: Supply chain compromises offer attackers a pathway to infiltrate multiple organizations through trusted channels, maximizing the potential impact of their attacks.

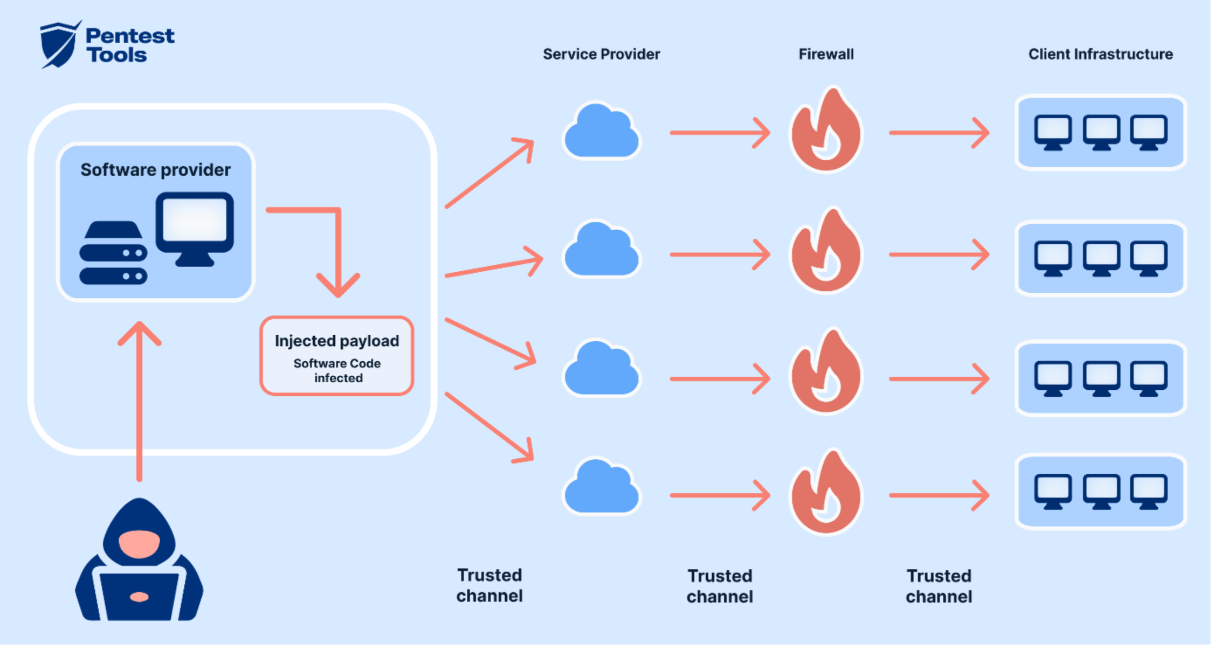
- Strategic Advantage: Adversaries may seek to gain strategic advantages, such as stealing intellectual property, gaining competitive insights, or disrupting critical services, by compromising supply chains.

Potential Impact:

- Cascading Impact: Supply chain compromises can propagate downstream, affecting interconnected networks, partners, and customers, leading to widespread data breaches, financial losses, and operational disruptions.

- Loss of Trust and Credibility: Organizations implicated in supply chain compromises may suffer reputational damage, loss of customer trust, and erosion of business relationships, with long-term consequences for their viability and competitiveness.

By conducting a deep dive on these prioritized threats, I've gained a deeper understanding of their tactics, motivations, and potential impact. Armed with this knowledge, I can better formulate defensive strategies, allocate resources effectively, and mitigate the risks posed by ransomware attacks and supply chain compromises to our organization.



3.2 FUSION PRACTICE

In synthesizing information from diverse sources, including news sites, threat feeds, and research papers, I've constructed a comprehensive picture of the chosen threat landscape. Here's a summary of my findings:

Threat: Ransomware Attacks on Critical Infrastructure

1. Threat Description:

- Ransomware attacks targeting critical infrastructure sectors, such as energy, healthcare, and transportation, have been on the rise.

- These attacks typically involve adversaries infiltrating networks, encrypting data, and demanding ransom payments in exchange for decryption keys.

2. Tactics, Techniques, and Procedures (TTPs):

- Threat actors commonly employ phishing emails, exploit kits, and vulnerable remote desktop protocols (RDP) to gain initial access to target networks.

- Once inside, they utilize lateral movement techniques to escalate privileges and deploy ransomware payloads across the network.

3. Impact and Consequences:

- Ransomware attacks on critical infrastructure can have severe consequences, including operational disruptions, financial losses, and potential risks to public safety.

- Organizations may face regulatory scrutiny, reputational damage, and legal liabilities in the aftermath of such incidents.

4. Mitigation Strategies:

- Implementing robust cybersecurity measures, such as regular software patching, network segmentation, and multi-factor authentication (MFA), can help mitigate the risk of ransomware attacks.

- Organizations should prioritize incident response planning, including regular backups, offline storage of critical data, and training personnel on detecting and responding to ransomware threats.

5. Conflicting or Missing Information:

- While there is substantial information available on the tactics and impact of ransomware attacks, there may be discrepancies in reporting specific attack vectors or targeted sectors.

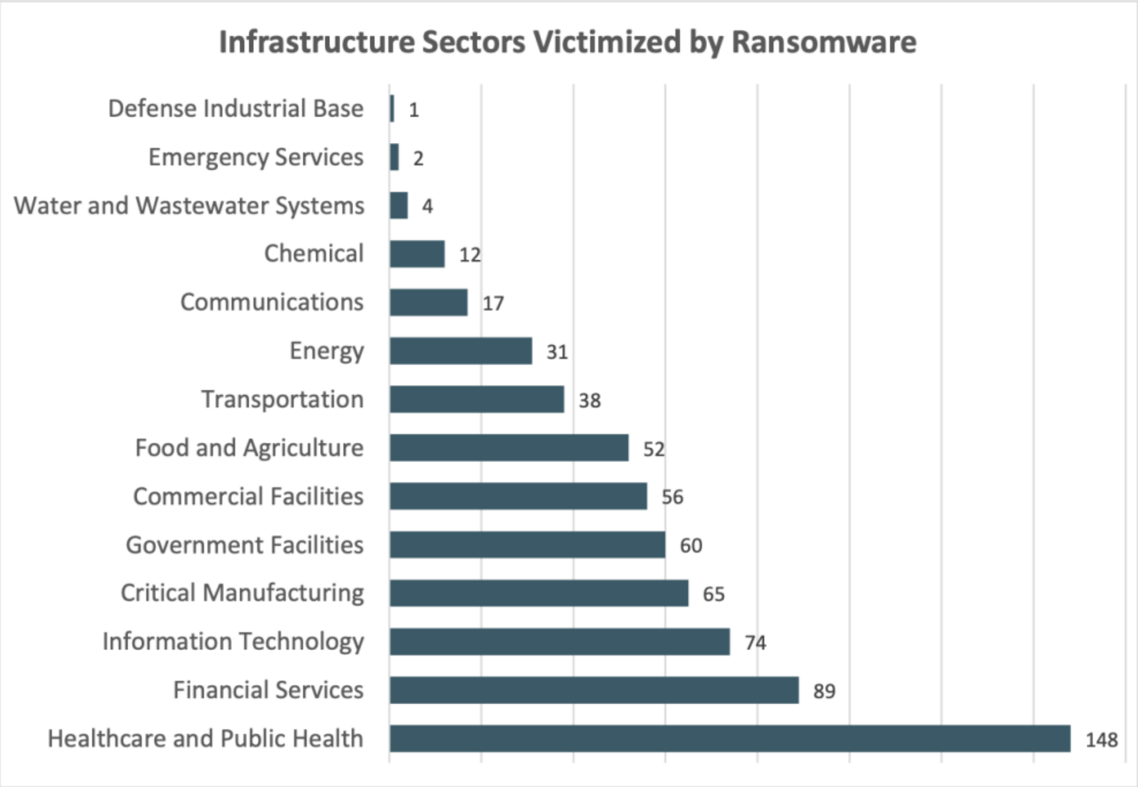
- Additional sources, such as incident reports from affected organizations or cybersecurity agencies, could provide more granular details on recent ransomware incidents and their implications.

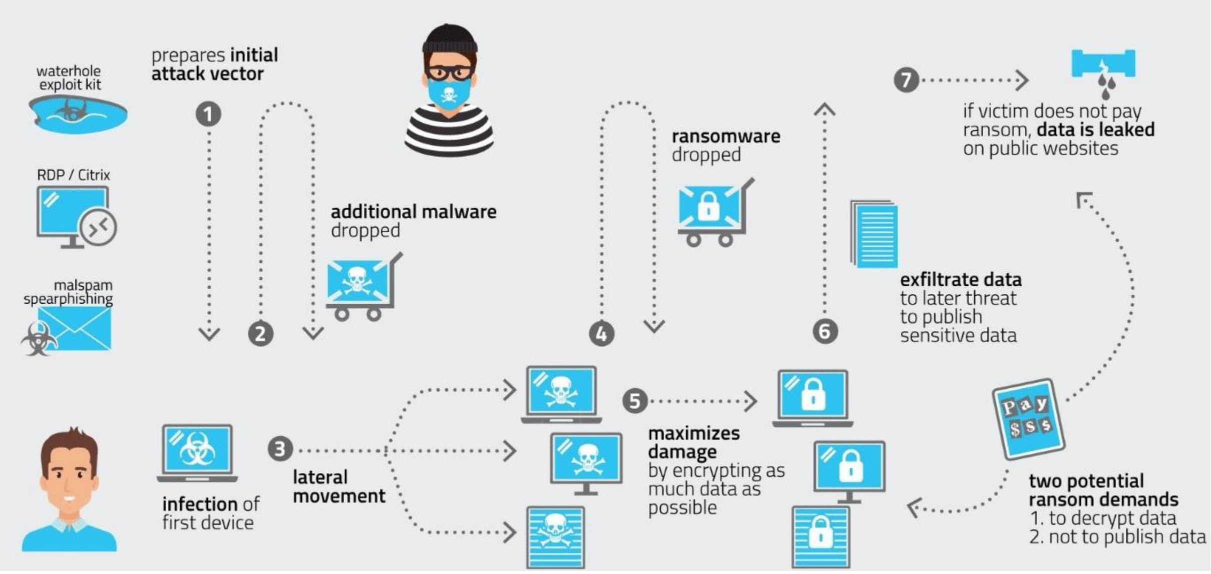
6. Further Research Opportunities:

- Investigating case studies of recent ransomware attacks on critical infrastructure sectors can provide valuable insights into adversary techniques and defensive strategies.

- Analyzing threat intelligence reports and threat actor profiles may shed light on the motives and capabilities of ransomware operators targeting critical infrastructure.

By integrating insights from multiple sources, including news articles, threat intelligence feeds, and research papers, I've developed a nuanced understanding of the ransomware threat landscape targeting critical infrastructure. Identifying conflicting or missing information highlights the importance of ongoing research and collaboration across cybersecurity domains to effectively combat this evolving threat.




waterhole exploit kit
RDP / Citrix
malspam spearphishing
prepares initial attack vector
1
2
additional malware dropped
3
lateral movement
infection of first device
4
ransomware dropped
5
maximizes damage by encrypting as much data as possible
6
exfiltrate data to later threat to publish sensitive data
7
if victim does not pay ransom, data is leaked on public websites
Pay $$$
two potential ransom demands
1. to decrypt data
2. not to publish data

3.3 SOURCE CREDİBİLİTY ASSESSMENT

In evaluating the credibility and trustworthiness of the information gathered on ransomware attacks targeting critical infrastructure, I've considered various factors, including the expertise, reputation, and potential biases of the sources. Here's a summary of my assessment:

1. News Sites:

- Expertise: Established news outlets with dedicated cybersecurity reporters or investigative teams possess expertise in gathering and verifying information on cyber threats.

- Reputation: Well-known news organizations with a history of accurate reporting and adherence to journalistic ethics are generally considered credible sources.

- Biases: While news sites strive for objectivity, individual reporters or editorial biases may influence the framing or interpretation of cybersecurity events.

2. Threat Intelligence Feeds:

- Expertise: Threat intelligence providers leverage advanced tools and methodologies to collect, analyze, and disseminate information on emerging cyber threats.

- Reputation: Credible threat intelligence feeds are backed by reputable cybersecurity firms or industry consortiums with a track record of delivering accurate and timely intelligence.

- Biases: Some threat intelligence feeds may focus on specific threat actors or attack vectors, potentially leading to biases in reporting or analysis.

3. Research Papers:

- Expertise: Research papers authored by cybersecurity experts, academics, or industry professionals contribute valuable insights into emerging threats, vulnerabilities, and mitigation strategies.

- Reputation: Peer-reviewed journals or reputable organizations such as SANS Institute are recognized for their rigorous review processes and commitment to academic integrity.

- Biases: Researchers may have affiliations with particular companies, government agencies, or advocacy groups, which could influence their findings or recommendations.

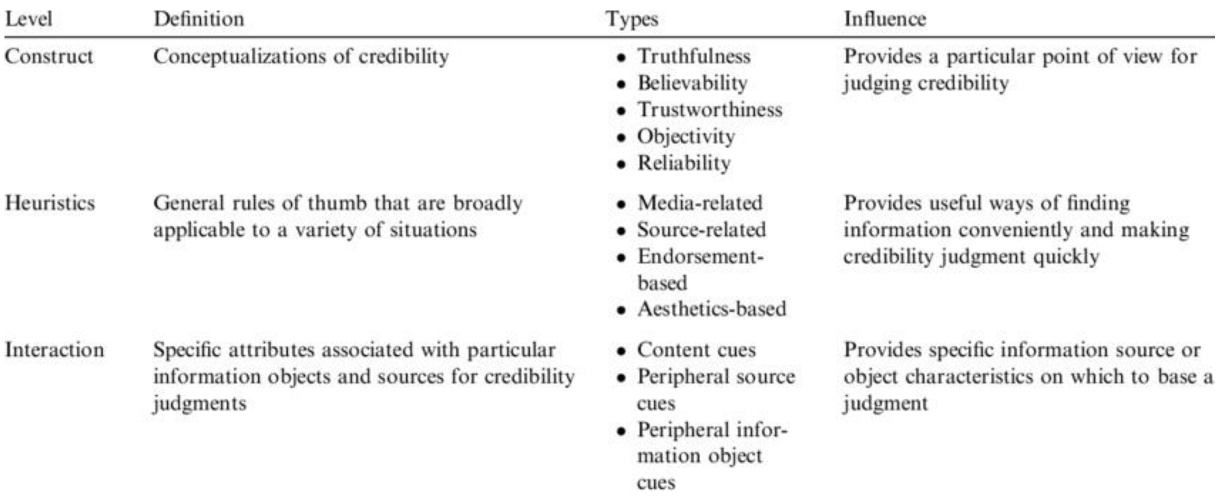
*Overall Assessment

- The information gathered from news sites, threat intelligence feeds, and research papers offers a diverse range of perspectives on ransomware attacks targeting critical infrastructure.

- While individual sources may exhibit biases or limitations, cross-referencing information from multiple reputable sources enhances the overall credibility and reliability of the analysis.

- Critical thinking and discernment are essential when evaluating the validity of findings and recommendations, taking into account the expertise, reputation, and potential biases of each source.

By carefully assessing the credibility of the information gathered, I can ensure that my analysis is grounded in reliable and trustworthy sources, thereby enhancing the quality and integrity of my insights into the ransomware threat landscape targeting critical infrastructure.



Level	Definition	Types	Influence
Construct	Conceptualizations of credibility	• Truthfulness • Believability • Trustworthiness • Objectivity • Reliability	Provides a particular point of view for judging credibility
Heuristics	General rules of thumb that are broadly applicable to a variety of situations	• Media-related • Source-related • Endorsement-based • Aesthetics-based	Provides useful ways of finding information conveniently and making credibility judgment quickly
Interaction	Specific attributes associated with particular information objects and sources for credibility judgments	• Content cues • Peripheral source cues • Peripheral information object cues	Provides specific information source or object characteristics on which to base a judgment

3.4 MITIGATION RECOMMENDATIONS FOR PRIORITIZED THREATS

Following a deeper understanding of the prioritized threats, I've developed preliminary recommendations for mitigating them:

1. Ransomware Attacks:

- Recommendations:

  - Implement robust backup and disaster recovery solutions to ensure data resilience and rapid restoration in the event of a ransomware attack.

  - Deploy endpoint detection and response (EDR) solutions to detect and respond to ransomware activities, including file encryption and suspicious behavior.

  - Conduct regular user awareness training to educate employees about phishing tactics, malware prevention, and incident reporting procedures.

  - Apply the principle of least privilege to limit user access rights and restrict privileges to critical systems and data.

  - Establish incident response plans and conduct tabletop exercises to simulate ransomware scenarios and validate response procedures.

2. Supply Chain Compromises

- Recommendations

  - Assess and monitor the security posture of third-party vendors and service providers, including their software development practices and security controls.

  - Implement supply chain risk management frameworks to identify, assess, and mitigate risks associated with vendor dependencies and interdependencies.

  - Establish contractual agreements with vendors to enforce security requirements, including regular security assessments, vulnerability management, and incident response capabilities.

  - Implement network segmentation to isolate critical systems and data from third-party connections, reducing the blast radius of supply chain compromises.

  - Enhance threat intelligence sharing and collaboration with industry peers and information sharing communities to stay informed about emerging supply chain threats and vulnerabilities.

3. Phishing and Social Engineering Attacks:

- Recommendations:

- Deploy email security solutions to detect and block phishing emails, malicious attachments, and suspicious URLs before they reach users' inboxes.

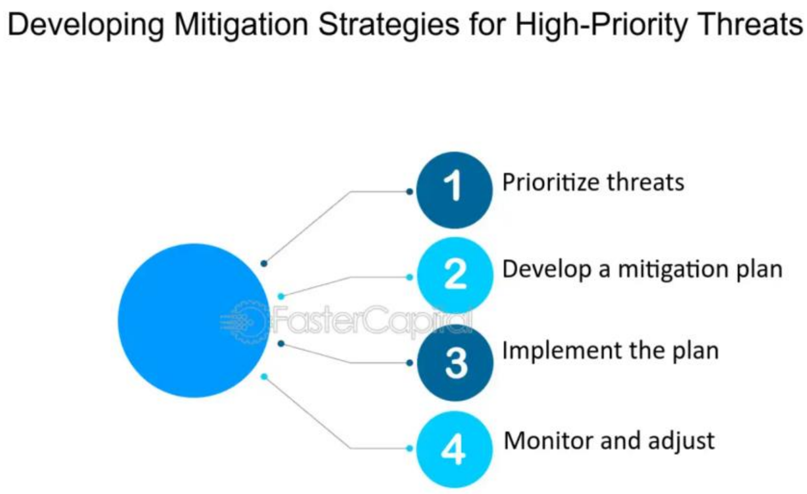
- Implement multi-factor authentication (MFA) to add an extra layer of security and protect against credential theft and unauthorized access.

- Conduct regular phishing simulations and security awareness training to educate employees about common phishing tactics and how to identify and report suspicious emails.

- Implement email authentication mechanisms such as SPF, DKIM, and DMARC to prevent email spoofing and domain impersonation.

- Establish incident response procedures to promptly detect and respond to phishing incidents, including user account compromises and data exfiltration attempts.

By prioritizing investments in security controls that address the most critical attack vectors and vulnerabilities identified, organizations can enhance their resilience to ransomware attacks, supply chain compromises, and phishing/social engineering threats. These recommendations serve as a foundation for developing a comprehensive cybersecurity strategy aimed at mitigating the impact of prioritized threats and safeguarding the organization's assets, operations, and reputation.


Developing Mitigation Strategies for High-Priority Threats
1
Prioritize threats
2
Develop a mitigation plan
3
Implement the plan
4
Monitor and adjust

4. WEEK 4: ADVANCED THREAT HUNTİNG AND TEMPLATE CREATİON

4.1 EXPLORATION OF ZEEK

I chose to explore Zeek , an open-source network security monitoring tool, to analyze network traffic and conduct investigations based on prioritized threats. Here's a summary of what I've learned:

1. Basic Functionalities:

- Zeek is a powerful network analysis framework that captures, parses, and analyzes network traffic in real-time.

- It provides visibility into network activity, including protocol analysis, connection logging, and file extraction, enabling threat detection and incident response.

2. Key Features:

- Protocol Analysis: Zeek decodes network protocols such as HTTP, DNS, FTP, and SMTP, extracting metadata and generating logs for analysis.

- Connection Logging: Zeek logs network connections, including source and destination IP addresses, ports, and protocol information, facilitating network traffic monitoring and analysis.

- File Extraction: Zeek can extract files transferred over the network, allowing for the analysis of potentially malicious payloads and attachments.

- Customizable Scripts: Zeek supports the development of custom scripts (Bro scripts) to extend its functionality and perform specific analysis tasks tailored to organizational needs.

3. Implementation:

- I deployed Zeek on a test network to monitor network traffic and analyze potential threats based on the prioritized threats identified earlier.

- Using Zeek's built-in protocols analyzers and logging capabilities, I captured and analyzed network traffic in real-time, focusing on identifying suspicious activities related to ransomware, supply chain compromises, and phishing/social engineering attacks.

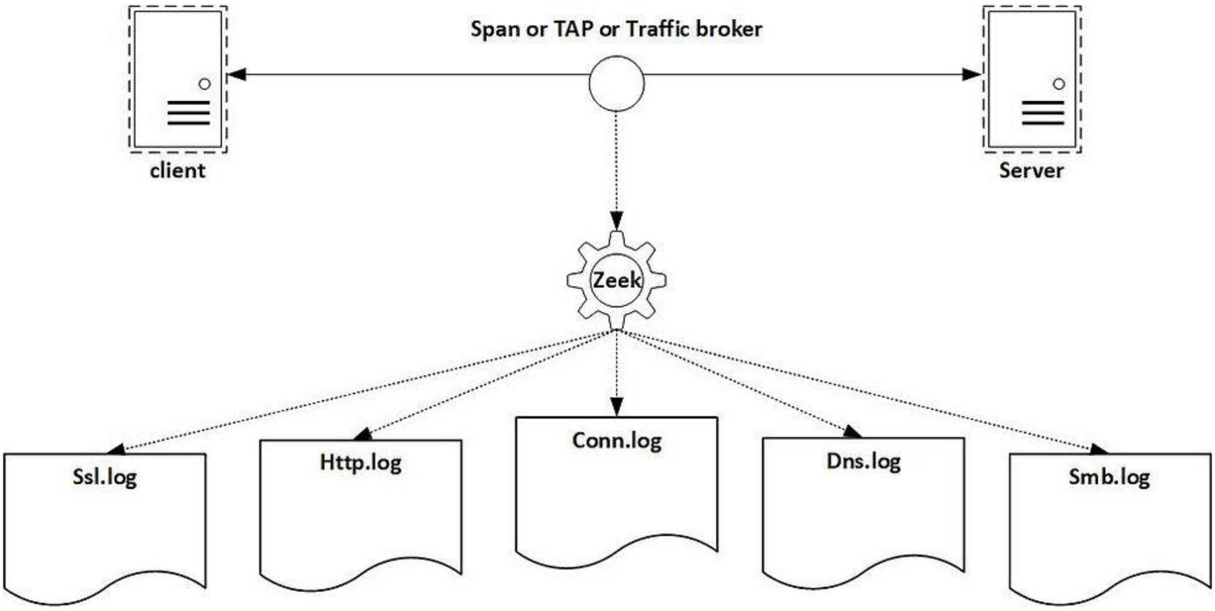
4. Benefits:

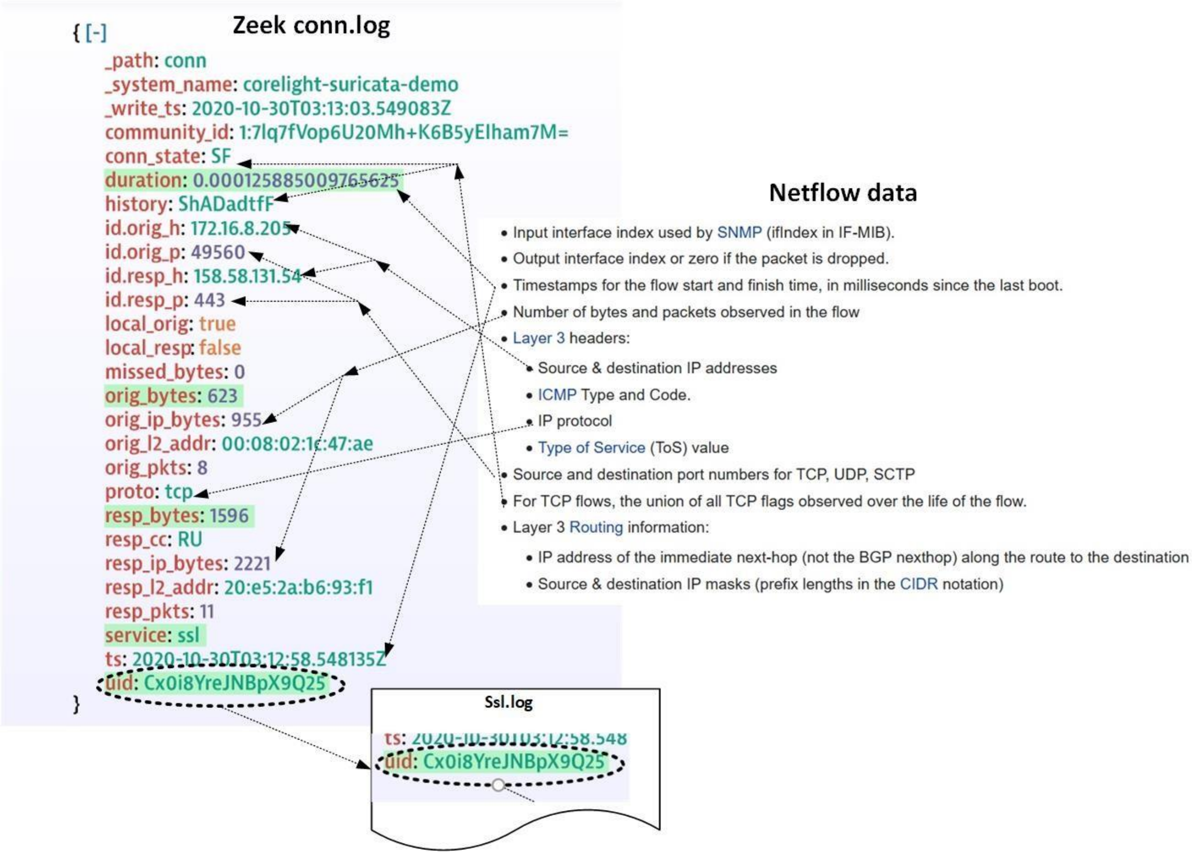
- Zeek provides granular visibility into network traffic, allowing for the detection of anomalies, suspicious behavior, and potential security incidents.

- Its open-source nature and extensibility make it a valuable tool for organizations seeking cost-effective network security monitoring solutions.

- Zeek's community-driven development model ensures continuous improvement and innovation, with regular updates and contributions from a diverse community of users and developers.

In conclusion, my exploration of Zeek has provided valuable insights into its basic functionalities and capabilities for network traffic analysis and threat hunting. By leveraging Zeek's features, organizations can enhance their network security posture, detect and respond to threats more effectively, and strengthen their overall cybersecurity defenses.





```
{ [-]
    _path: conn
    _system_name: corelight-suricata-demo
    _write_ts: 2020-10-30T03:13:03.549083Z
    community_id: 1:7lq7fVop6U20Mh+K6B5yElham7M=
    conn_state: SF
    duration: 0.000125885009765625
    history: ShADadtfF
    id.orig_h: 172.16.8.205
    id.orig_p: 49560
    id.resp_h: 158.58.131.54
    id.resp_p: 443
    local_orig: true
    local_resp: false
    missed_bytes: 0
    orig_bytes: 623
    orig_ip_bytes: 955
    orig_l2_addr: 00:08:02:1c:47:ae
    orig_pkts: 8
    proto: tcp
    resp_bytes: 1596
    resp_cc: RU
    resp_ip_bytes: 2221
    resp_l2_addr: 20:e5:2a:b6:93:f1
    resp_pkts: 11
    service: ssl
    ts: 2020-10-30T03:12:58.548135Z
    uid: Cx0i8YreJNBpX9Q25
}
```

- Input interface index used by SNMP (ifIndex in IF-MIB).
- Output interface index or zero if the packet is dropped.
- Timestamps for the flow start and finish time, in milliseconds since the last boot.
- Number of bytes and packets observed in the flow
- Layer 3 headers:
  - Source & destination IP addresses
  - ICMP Type and Code.
  - IP protocol
  - Type of Service (ToS) value
- Source and destination port numbers for TCP, UDP, SCTP
- For TCP flows, the union of all TCP flags observed over the life of the flow.
- Layer 3 Routing information:
  - IP address of the immediate next-hop (not the BGP nexthop) along the route to the destination
  - Source & destination IP masks (prefix lengths in the CIDR notation)

```
ts: 2020-10-30T03:12:58.548
uid: Cx0i8YreJNBpX9Q25
```

4.2 DEVELOPMENT OF CUSTOMİZED THREAT ANALYSİS TEMPLATES

In response to organizational needs, I have adapted existing threat analysis templates, such as MITRE ATT&CK or CISA Threat Matrix, to fit our specific reporting format and requirements. Here's a summary of what I've learned:

1. Understanding Organizational Requirements:

- I identified key stakeholders and gathered requirements to understand the specific needs and reporting formats preferred within our organization.

- This step ensured that the customized threat analysis templates would align with organizational goals and facilitate effective communication and decision-making.

2. Adaptation of Existing Templates:

- Leveraging the structure and components of established threat analysis frameworks like MITRE ATT&CK or CISA Threat Matrix, I tailored the templates to suit our organization's unique context and priorities.

- This involved modifying sections, adding or removing fields, and adjusting the level of detail to better capture relevant threat information and analysis.

3. Customization for Documentation and Reporting:

- I designed the customized threat analysis templates to facilitate comprehensive documentation of threat details, analysis findings, and mitigation recommendations.

- The templates include sections for capturing threat actor tactics, techniques, and procedures (TTPs), impact assessments, and actionable mitigation strategies tailored to our organization's specific environment and risk profile.

4. Integration with Existing Processes:

- To ensure seamless integration into existing workflows, I incorporated the customized threat analysis templates into our incident response, risk management, and security operations processes.

- This enables consistent and standardized documentation of threat analysis across the organization, enhancing collaboration and knowledge sharing among security teams.

5. Training and Adoption:

- I conducted training sessions to familiarize relevant personnel with the customized threat analysis templates and their usage.

- By providing guidance on how to effectively document threat details, analyze findings, and formulate mitigation recommendations using the templates, I promote widespread adoption and adherence to standardized reporting practices.

In conclusion, the development of customized threat analysis templates tailored to our organization's specific needs and reporting format ensures the comprehensive documentation of threat intelligence, analysis, and mitigation strategies. By aligning with organizational requirements and integrating seamlessly into existing processes, these templates facilitate effective communication, decision-making, and response to cybersecurity threats.

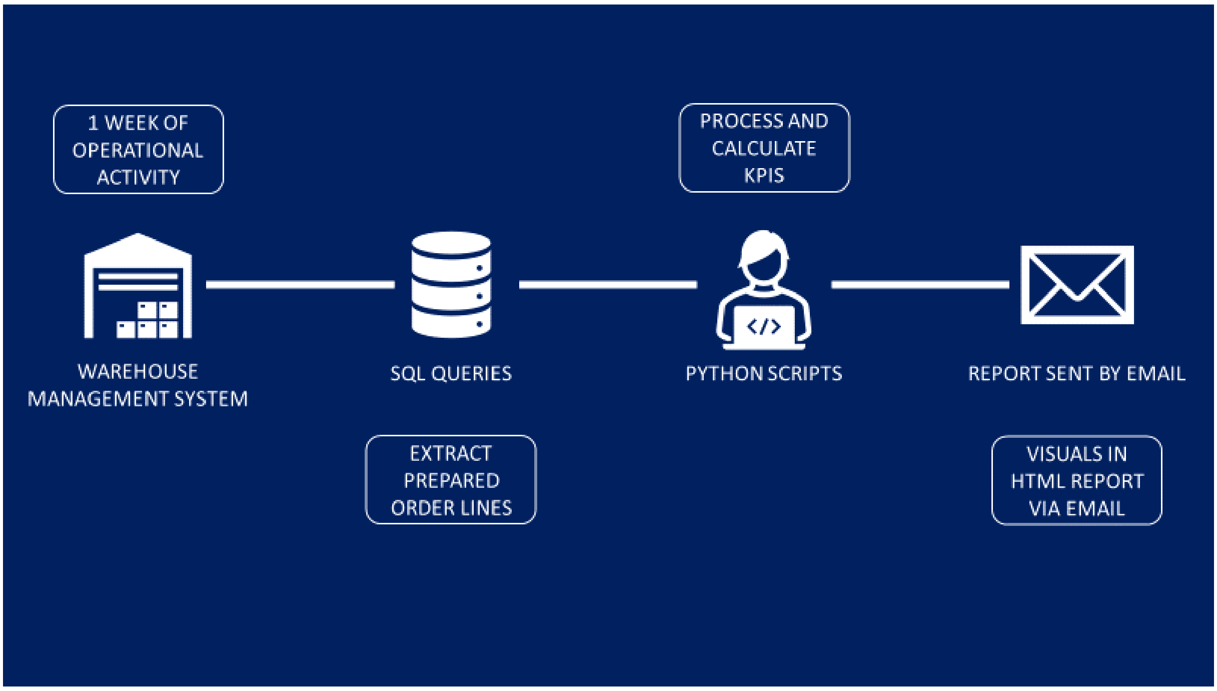
4.3 AUTOMATING REPORTING TASKS

Through the exploration of Python scripting and automation tools, I've learned to streamline repetitive tasks, such as data analysis, report generation, and vulnerability scanning. Here's a summary of my findings:

1. Python Scripting for Automation:

- Python provides powerful libraries and tools for automating various tasks, including data manipulation, analysis, and reporting.

- By writing Python scripts, I can automate repetitive processes, such as parsing log files, extracting relevant information, and generating reports.


1 WEEK OF OPERATIONAL ACTIVITY
PROCESS AND CALCULATE KPIS
WAREHOUSE MANAGEMENT SYSTEM
SQL QUERIES
PYTHON SCRIPTS
REPORT SENT BY EMAIL
EXTRACT PREPARED ORDER LINES
VISUALS IN HTML REPORT VIA EMAIL

2. Efficiency Gains:

- Automation of reporting tasks using Python scripting or other automation tools saves time and improves efficiency by reducing manual effort and minimizing human errors.

- Tasks that previously required hours of manual labor can now be completed in a fraction of the time, allowing for more focus on strategic activities.

3. Integration with Existing Tools:

- Python scripts can be integrated with existing tools and platforms used within the organization, such as SIEM systems, vulnerability scanners, and reporting frameworks.

- This integration enables seamless data exchange and workflow automation, enhancing overall operational efficiency.

4. Scalability and Flexibility:

- Automation tools and scripts can be scaled to handle large volumes of data and accommodate evolving business requirements.

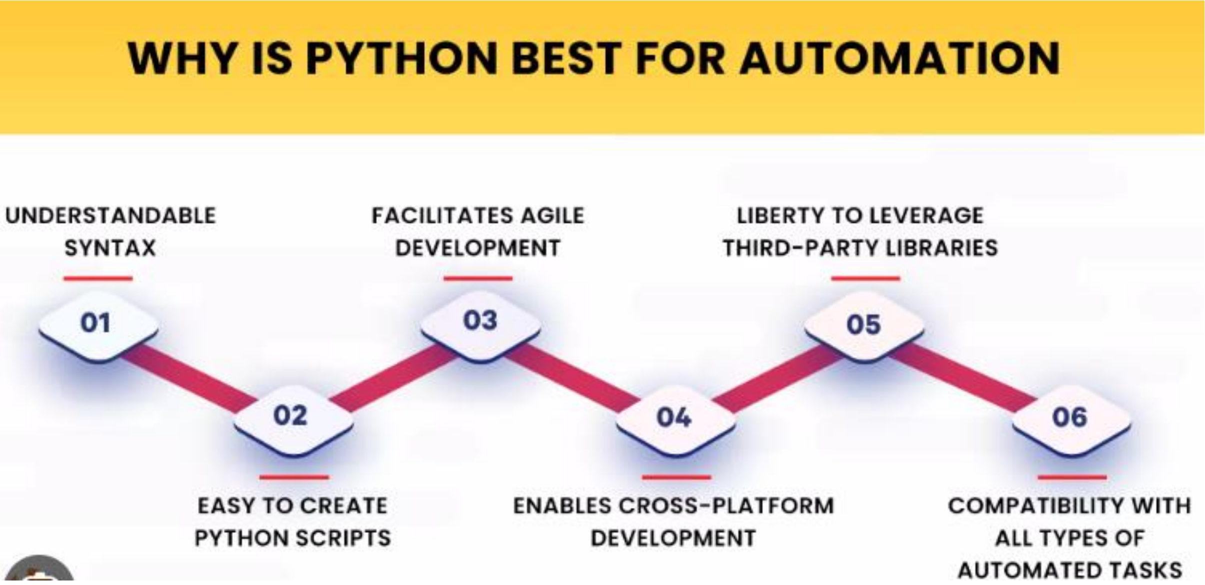
- Python's versatility and flexibility allow for customization and adaptation of automation solutions to suit specific use cases and organizational needs.

5. Continuous Improvement:

- Automation facilitates continuous improvement by enabling iterative refinement of processes and workflows over time.

- By monitoring performance metrics and gathering feedback, I can identify opportunities for further automation and optimization, driving ongoing efficiency gains.

In conclusion, leveraging Python scripting and automation tools to automate reporting tasks offers significant benefits in terms of time savings, efficiency gains, and scalability. By streamlining repetitive processes, organizations can allocate resources more effectively, improve operational agility, and focus on higher-value activities that contribute to overall business objectives.


WHY IS PYTHON BEST FOR AUTOMATION
UNDERSTANDABLE SYNTAX
01
FACILITATES AGILE DEVELOPMENT
03
LIBERTY TO LEVERAGE THIRD-PARTY LIBRARIES
05
02
EASY TO CREATE PYTHON SCRIPTS
04
ENABLES CROSS-PLATFORM DEVELOPMENT
06
COMPATIBILITY WITH ALL TYPES OF AUTOMATED TASKS