Cutting Edge Solutions India (Pvt) Ltd. (CESI)

Whitepaper on Threat Analytics and Threat Hunting When Engaging Encr ypted Data and Encrypted Digital Transmissions

TABLE OF CONTENTS

©Cutting Edge Solutions India Private Limited 2024

Threat Intelligence For Encrypted Digital Data Analysis

ABSTRACT

The increasing prevalence of encryption in digital communications necessitates advanced methods for detecting and mitigating cyber threats without compromising privacy. Traditional signature-based detection tools are inadequate for encrypted traffic. Therefore, modern approaches must focus on metadata analysis, such as checksums, Software Bill of Materials (SBOMs), source and destination addresses, and follow-up traffic. This paper addresses these challenges and outlines strategies for identifying and mitigating threats while ensuring data integrity and privacy.

INTRODUCTION

The rise of encrypted communications, driven by regulatory requirements and heightened security awareness, has transformed the digital landscape. Organizations now prioritize protecting sensitive data in transit and at rest, rendering effective threat intelligence crucial. The widespread adoption of encryption, reported at approximately 80% by Firefox and 95% by Google, complicates the task of inspecting traffic for malicious content.

THE RISE OF ENCRYPTED THREATS

Cybercriminals are exploiting the limitations of traditional security methods that struggle with encrypted traffic. This paper identifies several examples of encrypted threats:

- Malware within encrypted payloads
    - Malicious software can be embedded within encrypted files or communications, effectively evading traditional detection mechanisms that rely on signature-based inspections. This type of threat leverages the privacy provided by encryption to bypass security controls, making it challenging for security teams to identify and mitigate the malware without decrypting the traffic, which may violate privacy policies and regulations.

- Command and control (C2) communications over encrypted channels
    - Attackers often use encrypted channels to establish and maintain command and control over compromised systems. By encrypting their communications, they can hide their activities from detection tools. These encrypted C2 channels allow attackers to issue commands, exfiltrate data, and receive updates from the malware, all while remaining undetected by conventional security solutions that cannot inspect the encrypted traffic.

©Cutting Edge Solutions India Private Limited 2024

- Data exfiltration through encrypted connections
    - Cybercriminals use encryption to conceal the unauthorized transfer of data from compromised systems to external locations. Encrypted data exfiltration can go unnoticed, as the encrypted traffic appears legitimate to monitoring tools. This method allows attackers to steal sensitive information, intellectual property, or personal data without raising immediate suspicion.

- Significant increase in encrypted supply chain attacks
    - Supply chain attacks involve the compromise of third-party vendors or software used by target organizations. The increased use of encryption in these attacks makes detection even more challenging. Attackers embed malicious code within encrypted software updates or dependencies, exploiting the trust relationship between the vendor and the organization. The widespread adoption of open-source software without thorough security vetting exacerbates this threat, as it provides attackers with numerous opportunities to infiltrate target networks.

According to Zscaler, 86% of all cyber threats are now delivered via encrypted channels, with a 186% increase in encrypted attacks, highlighting the urgency for robust threat intelligence solutions.

CHALLENGES IN SECURING ENCRYPTED TRAFFIC

Securing encrypted traffic presents several key challenges:

- Limited Visibility
    - Encrypted traffic conceals payload content, impeding traditional security tools' ability to inspect and analyze data. Security systems that rely on deep packet inspection (DPI) are rendered ineffective, as they cannot decrypt the traffic to view its contents. This limitation necessitates the development of new techniques that can infer potential threats based on metadata and other observable characteristics without compromising encryption.

- Resource Intensity
    - Decrypting and analyzing encrypted traffic requires substantial computational resources, often leading to performance degradation and increased latency. The process of decrypting data, inspecting it for threats, and then re-encrypting it can be resource-intensive, particularly in high-traffic environments. Organizations must balance the need

for thorough inspection with the impact on system performance, often requiring investments in more powerful hardware and optimized software solutions.

- Compliance and Privacy Concerns
    - Decrypting traffic can conflict with privacy regulations and compliance requirements, necessitating a delicate balance between security and legal obligations. Regulations such as GDPR and CCPA mandate the protection of personal data, which can be at odds with security measures that involve decrypting and inspecting traffic. Organizations must navigate these complex legal landscapes to ensure they protect user privacy while maintaining robust security postures.

- Evolving Encryption Standards
    - Continual advancements in encryption technologies can render existing security tools obsolete, demanding ongoing investment in new technologies and expertise. As encryption algorithms and protocols evolve, security solutions must keep pace to remain effective. This dynamic environment requires continuous learning and adaptation by security professionals and investments in state-of-the-art technologies capable of handling new encryption standards.

- False Positives and Negatives
    - The inability to fully inspect encrypted traffic increases the likelihood of false positives and false negatives, complicating threat detection efforts. False positives, where benign traffic is flagged as malicious, can overwhelm security teams and lead to alert fatigue. Conversely, false negatives, where actual threats go undetected, can result in successful breaches. Developing more accurate detection methods that minimize these errors is essential for effective threat management.

- Complex Threat Landscape
    - The sophistication of attackers exploiting encryption requires advanced threat intelligence and proactive security measures. Attackers continuously develop new techniques to bypass security controls and exploit encrypted channels. Keeping up with these evolving threats demands a proactive approach, leveraging threat intelligence to anticipate and counteract new attack methods. This includes understanding the tactics, techniques, and procedures (TTPs) of threat actors and staying informed about the latest developments in cyber threats.

THE ROLE OF THREAT INTELLIGENCE

Threat intelligence provides critical insights into emerging threats and attacker tactics, enabling the development of effective security strategies for encrypted traffic. By leveraging threat intelligence, security teams can improve incident response times and better understand potential attacker methods. Threat intelligence involves gathering, analyzing, and applying information about current and potential threats, helping organizations to anticipate, prepare for, and respond to cyber incidents more effectively. It includes data on threat actors, their techniques, and indicators of compromise (IoCs), allowing for a more informed and proactive security posture.

Types of Threat Intelligence for Encrypted Traffic

Threat Intelligence Type	Description	Example
Malware signatures for encrypted payloads	Identifies malware within encrypted traffic through specific signatures	Signatures for known malware distributed via encrypted channels.
Indicators of Compromise (IoCs) associated with encrypted attacks	Identifies systems compromised by attackers using encryption	Lists of IP addresses used by attackers for C2 communication over encrypted channels.
Threat actor profiles and their known tactics for exploiting encryption	Information on tactics, techniques, and procedures (TTPs) used by attackers to exploit encryption	Profiles of attacker groups that use encryption to hide malicious activities.

- Malware signatures for encrypted payloads
    - Malware signatures are unique patterns or sequences of bytes that can identify specific types of malware. These signatures can be used to detect malicious software hidden within encrypted traffic. Security tools can compare the signatures against encrypted payloads to identify known malware, even if the content itself remains encrypted. Developing accurate and comprehensive malware signatures requires continuous research and analysis of emerging threats.

- Indicators of Compromise (IoCs) associated with encrypted attacks
    - IoCs are pieces of forensic data that indicate a system has been compromised. These can include IP addresses, domain names, file hashes, and more. For encrypted attacks, IoCs might involve specific patterns of encrypted traffic, known malicious IP addresses used for C2 communications, or other identifiable traits associated with encrypted threats. By monitoring for these IoCs, security teams can detect and respond to compromised systems more effectively.

- Threat actor profiles and their known tactics for exploiting encryption

©Cutting Edge Solutions India Private Limited 2024

- Understanding the profiles of threat actors, including their tactics, techniques, and procedures (TTPs), helps organizations anticipate and defend against attacks. Profiles can include information on the types of encryption methods threat actors use, their preferred tools, and their typical targets. By studying these profiles, security teams can develop more targeted defenses and better anticipate future attacks.

LEVERAGING THREAT INTELLIGENCE FOR ENCRYPTED TRAFFIC SECURITY

- Threat intelligence-driven traffic inspection
  - Using threat intelligence to detect specific patterns or indicators of malicious activity in encrypted traffic, thereby focusing security resources on high-risk traffic. This approach involves correlating threat intelligence data with observed traffic patterns to identify potential threats without decrypting the traffic. Techniques such as analyzing metadata, flow characteristics, and traffic anomalies can help pinpoint suspicious activities.

- Prioritizing security alerts with threat intelligence
  - Utilizing threat intelligence to prioritize alerts that are most likely associated with genuine threats, enhancing the efficiency of incident response. By filtering and prioritizing alerts based on the likelihood and impact of threats, security teams can focus their efforts on the most critical incidents. This reduces alert fatigue and ensures timely responses to high-priority threats.

- Automating threat detection and response
  - Implementing automated systems to detect and respond to threats based on threat intelligence, thereby improving security operations' effectiveness. Automation can streamline the process of threat detection, analysis, and response, reducing the time and effort required from security personnel. Automated systems can quickly apply threat intelligence to identify and mitigate threats, enhancing overall security posture.

STRATEGIES FOR USING THREAT INTELLIGENCE - COMMON INDICATORS OF COMPROMISE

- Unusual network traffic

- An unexpected increase in data usage may signal data exfiltration. This could include large volumes of outbound data transfers that are inconsistent with normal usage patterns. Monitoring for significant deviations in network traffic can help identify potential data breaches.

- Unexpected system reboots or shutdowns
  - Such anomalies may indicate unauthorized access. Attackers may force system reboots to install malicious updates or to cover their tracks. Frequent or unexpected reboots can be a red flag for security teams to investigate further.

- Slow or malfunctioning devices
  - A sudden slowdown or repeated crashes may suggest malware presence. Malware often consumes significant system resources, leading to performance issues. Monitoring system performance and investigating unexplained slowdowns can help detect and mitigate malware infections.

- Suspicious emails or messages
  - Phishing attempts often come through email or messaging platforms. These communications may contain malicious links or attachments designed to compromise systems. Educating users about recognizing and reporting suspicious messages is crucial for preventing successful phishing attacks.

- Unauthorized changes
  - Unexpected modifications to system settings, files, or software installations may indicate an intrusion. Attackers may alter configurations to establish persistence or to facilitate further exploitation. Regularly auditing system changes and verifying their legitimacy can help detect unauthorized modifications.

- Irregular user activity
  - Unusual access patterns, such as logging in at odd hours or accessing unauthorized areas, can indicate compromised accounts. Monitoring user behavior and identifying deviations from normal activity can help detect and respond to potential account compromises.

- Increased failed login attempts
  - This may indicate a brute force attack. Attackers often use automated tools to repeatedly attempt logins with various password combinations. Monitoring for an unusual number of failed login attempts can help detect and mitigate brute force attacks.

©Cutting Edge Solutions India Private Limited 2024

- Unusual outbound communications
    - Devices communicating with a threat actor's C2 server can be a sign of compromised systems. These communications often involve encrypted traffic to external IP addresses known to be associated with malicious activities. Monitoring outbound traffic for such patterns can help identify compromised devices and take appropriate actions to isolate and remediate them.

ENCRYPTED TRAFFIC ANALYSIS

- Initial Data Packet (IDP)
    - Allows extraction of critical data such as URI, DNS, and metadata like TLS version and ciphers. By analyzing the initial data packets of encrypted connections, security tools can gather valuable information about the connection's nature without decrypting the entire traffic. This can include identifying the server being accessed, the type of encryption used, and other contextual data that can help assess the connection's legitimacy.

- Sequence of Packet Lengths and Times (SPLT)
    - Conveys application payload byte counts and interarrival times for several packets in a flow. By examining the sequence and timing of packet lengths, security tools can identify patterns consistent with known malicious activities. For instance, certain types of malware exhibit distinct communication patterns that can be detected through SPLT analysis.

- Byte Distribution
    - Represents the probability of specific values appearing in a flow's payload packet, including full byte distribution, byte entropy, and mean/standard deviation of bytes. Analyzing byte distribution helps detect anomalies in encrypted traffic that may indicate the presence of malicious payloads. Unusual byte patterns can be a sign of encrypted malware or other threats, prompting further investigation.

CATEGORIES OF THREATS DETECTED BY ETAS

- Illicit crypto mining
    - Unauthorized use of an organization's resources to mine cryptocurrency. This activity can significantly degrade system performance and increase operational costs. By monitoring

for signs of crypto mining, such as unusual CPU or GPU usage, organizations can detect and prevent unauthorized mining activities.

- Android OS Trojans
    - Malicious software targeting Android devices, often distributed through deceptive apps. These Trojans can exfiltrate sensitive data, monitor user activity, or install additional malware. Detecting and mitigating Android OS Trojans requires monitoring for suspicious app behavior and unusual traffic patterns associated with compromised devices.

- Ad injectors
    - Malicious programs that inject unwanted advertisements into web pages. These can degrade user experience, expose users to further malware, and undermine trust in legitimate websites. Identifying ad injectors involves monitoring for unexpected modifications to web content and analyzing traffic for known ad-injection patterns.

- SALITY malware
    - A family of polymorphic file infectors that spread by infecting executable files. SALITY can disable security tools, steal sensitive information, and create backdoors for further exploitation. Detecting SALITY requires advanced threat intelligence to recognize its polymorphic nature and monitor for signs of file infection.

- Malware using SMB (Server Message Block) service discovery
    - Attackers exploit SMB services to spread malware across networks. This technique was infamously used in the WannaCry ransomware attack. Monitoring SMB traffic for unusual activity and ensuring proper SMB configuration and patching can help mitigate this threat.

- Potentially unwanted applications such as Tor and BitTorrent
    - Applications like Tor and BitTorrent can be used for legitimate purposes but also pose security risks. Tor can anonymize malicious activities, and BitTorrent can facilitate the distribution of pirated or malicious content. Monitoring for the use of these applications and enforcing appropriate usage policies can help manage their risks.

WEIGHING THREATS AGAINST ENCRYPTED FILES AND COMMUNICATIONS

When assessing risks associated with encrypted files and communications, organizations must consider the following.

- Threat Potential
    - Evaluating the likelihood of threats exploiting encrypted channels and understanding specific attacker methods. This involves analyzing historical data, threat intelligence reports, and industry trends to gauge the potential risks associated with encrypted traffic.

- Impact Assessment
    - Assessing potential damage, including data loss, financial loss, reputational damage, and operational disruptions. Organizations must evaluate the potential consequences of a successful attack on their operations, considering both direct and indirect impacts.

- Resource Allocation
    - Allocating resources effectively to mitigate threats, including investments in technology, personnel, and processes. This includes budgeting for advanced security tools, training for security personnel, and developing robust incident response plans to address encrypted threats.

- Risk Tolerance
    - Balancing security needs with operational efficiency and user privacy based on the organization's risk tolerance. Each organization must determine its acceptable level of risk, taking into account its specific industry, regulatory environment, and business objectives.

- Regulatory Compliance
    - Ensuring security measures align with relevant regulations and industry standards, often mandating specific actions for protecting encrypted communications. Compliance with standards such as GDPR, HIPAA, and PCI DSS is critical to avoiding legal penalties and maintaining customer trust.

BENEFITS OF USING THREAT INTELLIGENCE

- Improved Threat Detection Accuracy

- Enhanced ability to identify a broad range of threats, including those within encrypted traffic. Threat intelligence provides the necessary context to recognize sophisticated attacks that traditional methods may miss, improving overall detection capabilities.

- Faster Incident Response Times
  - Prioritizing security alerts and automating threat detection and response to enable quicker incident responses. With real-time threat intelligence, security teams can respond to incidents more efficiently, reducing the time attackers have to inflict damage.

- Proactive Threat Mitigation
  - Equipping security teams with the knowledge to proactively mitigate threats, fostering preparedness and reassurance. By staying informed about emerging threats and attacker tactics, organizations can implement preventive measures and enhance their security posture.

CLOSING SUMMARY

Threat intelligence is indispensable for securing encrypted traffic. As cybercriminals evolve their methods for exploiting encryption, the necessity of advanced threat intelligence becomes paramount. Future developments will require even more sophisticated threat intelligence solutions to address the complexities of securing encrypted communications effectively. The ongoing evolution of encryption standards and attacker tactics demands a proactive and informed approach to threat detection and response, ensuring that organizations remain resilient against emerging threats.

References

1. Cisco Encrypted Traffic Analytics: Necessity Driving Ubiquity - Cisco Blogs. Cisco Encrypted Traffic Analytics
2. Future-Proof Your Encrypted Traffic Through Analytics. Yates Communicates
3. AI-Based Video Analytics is Revolutionizing Surveillance - Intozi | Innovation through AI. Intozi
4. Testing Archives - FreeAPIData.com. FreeAPIData

©Cutting Edge Solutions India Private Limited 2024