deepwatch™

www.deepwatch.com
CIB-23-39

Sep. 21 - 27, 2023

Cyber Intel Brief

Latest Intelligence Analysis on Trending Cyber Threats

Analysis by:
Deepwatch Threat Intelligence

Cyber Intel Brief

Table **of Contents**

Share Your Thoughts

QUICK LOOK

Threat Actors Deliver Knight Ransomware in Phishing Emails

Knight Ransomware | Phishing | No Data Exfiltration | Industries/All

This report unveils the resurgence of Knight ransomware, delivered directly via sophisticated email campaigns targeting diverse sectors, primarily hospitality. Discover the threat actors' adaptability, multifaceted approach, financial motivations, and potential impact on organizational assets and functions. Dive into our comprehensive analysis and tailored recommendations to enhance your organization's cyber resilience against this evolving threat.

Sandman APT Targets Global Telecoms in August Cyber-Espionage Campaign

Sandman | LuaDream | Pass-the-Hash | DLL Sideloading | Data Exfiltration | Information

Discover insights into the elusive Sandman APT group's sophisticated cyber-espionage campaigns, which, so far, primarily targeted telecommunications providers but will likely expand to target other industries. Uncover the intricacies of their advanced LuaDream malware, its multifaceted capabilities, and the meticulous seven-stage infection process. Dive into the report to explore the potential risks, impacts, and tailored mitigation strategies to enhance your organization's cyber resilience against this evolving threat.

3 APTs Conducted Cyber Espionage Against a Southeast Asian Government, Employing Sophisticated Tools and Techniques

Stately Taurus | Alloy Taurus | Gelsemium | Data Exfiltration | Cyber Espionage | Public Administration

Uncover the intricate cyber espionage operations against a Southeast Asian government orchestrated by three distinct APT clusters, including Stately Taurus and suspected Gelsemium. This report delves into their sophisticated tactics, revealing a strategic pursuit of political, economic, and strategic intelligence. Discover the significant risks posed to corporations, the adaptive nature of these threats, and actionable recommendations to improve your cyber resilience.

APT29 Phishing Campaigns Evolve Malware Delivery Methods Between March and July

APT29/Cozy Bear | ROOTSAW | Phishing | Phishing Links & Attachments | Public Administration

Discover the evolving tactics of APT29 in our latest report, "APT29 Phishing Campaigns Evolve Malware Delivery Methods Between March and July." Uncover how this sophisticated cyber-espionage group attributed to Russia's SVR has refined malware delivery, introduced new variants, and strategically balanced infiltration methods, posing a significant risk to high-value entities. Dive into our detailed analysis to understand the potential impact on organizations and explore actionable recommendations to enhance cyber resilience against such advanced threats.

Note: You can share your feedback **here**. Read how Deepwatch approaches cyber threat intelligence **here**.

QUICK LOOK

SSH Fingerprint Leads to the Identification of Extensive Infrastructure Used in Ransomware Attacks

ShadowSyndicate | Ransomware | Cobalt Strike - IcedID - Matanbuchus - Sliver | Industries/All

This report unveils the extensive infrastructure of ShadowSyndicate, a potential emerging Ransomware-as-a-Service (RaaS) affiliate spotlighted by Group-IB. The analysis reveals the group's unique SSH fingerprint, affiliations with multiple ransomware families and the significant risks posed to organizations through loss of confidentiality and availability. The full report explores the intricate details of ShadowSyndicate's operations, the comprehensive risk assessment, and actionable recommendations to enhance your organization's cyber resilience against this evolving threat.

Latest Additions to Data Leak Sites

Manufacturing | Professional, Scientific, and Technical Services | Transportation and Warehousing | Information | Administrative and Support and Waste Management and Remediation Services

This brief analyzes the latest additions to dark web data leak sites, providing timely information for decision-makers. In the past week, ransomware threat groups added 57 victims to these sites, with 30 based in the US. The most targeted industry was Manufacturing, with 12 victims, followed by Professional, Scientific, and Technical Services, Transportation and Warehousing, Information, and Administrative and Support and Waste Management and Remediation Services. It is important to note that while these victims are listed, we cannot confirm the validity of the cybercriminals' claims.

CISA Adds 4 CVEs to its Known Exploited Vulnerabilities Catalog

Apple CVE-2023-41991 | Apple CVE-2023-41992 | Apple CVE-2023-41993 | Trend Micro CVE-2023-41179

This report focuses on known exploited vulnerabilities listed in CISA's catalog, providing timely information for decision-makers. CISA added four CVs to the catalog in the past week, affecting products from Apple and Trend Micro. CISA recommends mitigative action occur between 12 and 16 October 2023.

Note: You can share your feedback **here**. Read how Deepwatch approaches cyber threat intelligence **here**.

Threat Actors Deliver Knight Ransomware in Phishing Emails

Knight Ransomware | Phishing | No Data Exfiltration | Industries/All

Source Material: Proofpoint
Targeted Industries: All

Executive Summary

As part of our initiative to provide intelligence on the latest developments in ransomware deployment, the Adversary Tactics and Intelligence team compiled this report, analyzing the recent blog post by Proofpoint titled "The Return of Direct Ransomware Delivery?"

This report finds that Knight ransomware, an evolution of Cyclops ransomware, has been delivered directly via email through meticulously crafted campaigns, primarily targeting English-speaking users and the hospitality sector. The ransomware exhibits adaptability and a multifaceted approach, with modifications in attack chains and utilizing diverse lures. The threat actors behind this ransomware are primarily motivated by financial gain, demanding ransoms ranging from $5,000-$15,000 in Bitcoin, and exhibit a significant level of adaptability and resourcefulness in their operations. Recommendations include developing and conducting tailored training programs recognizing phishing emails and unsafe links and employing adaptable email filtering solutions to effectively block malicious emails, enhancing an organization's cyber resilience.

Insights & Determinations

- The threat actors' financial motivation, adaptability, and resourcefulness indicate a persistent and evolving threat, emphasizing the need for continuous vigilance and adaptive cybersecurity measures.
- The threat actors behind Knight ransomware will likely continue adapting their tactics, techniques, and procedures in response to the campaign's disclosure, potentially diversifying delivery methods and refining lures to maintain operational efficacy.
- The disclosure of the campaign may serve as a learning opportunity for other threat actors, potentially leading to an increase in the sophistication and diversity of future cyber threats.
- The risk and impact of Knight ransomware on organizations are significant, with potential material implications on net sales, revenues, and operational continuity through various scenarios, including operational disruption and reputation damage.

Introduction

This cyber threat intelligence report's purpose is to provide actionable intelligence that details the resurgence of direct email delivery of Knight ransomware, focusing on a comprehensive analysis of the tactics, techniques, and procedures employed by the threat actors, an assessment of the risk and impact, a short-term outlook and recommended mitigation measures to enhance organizational cyber resilience. The most significant threat highlighted is the ransomware's ability to encrypt critical files and systems, its adaptability, and the potential for diversification in delivery methods. The intelligence presented herein is derived from an in-depth analysis of a blog post published by Proofpoint titled "The Return of Direct Ransomware Delivery?" If you have questions or feedback about this intelligence, you can submit them **here**.

Overview & Background

The blog post from Proofpoint titled "The Return of Direct Ransomware Delivery?" details the resurgence of direct email delivery of Knight ransomware, highlighting several campaigns observed in August 2023. The blog post aims to shed light on the tactics, techniques, and procedures (TTPs) employed by the threat actors behind Knight ransomware and to provide insights into the evolving threat landscape. The blog post analyzes the characteristics of the email campaigns, the modifications in the attack chain, and the behavior of the ransomware upon installation, focusing on its lateral movement and encryption methods.

According to **SentinelOne**, "Knight ransomware emerged in August of 2023 as an evolution or rebrand of Cyclops ransomware. Knight ransomware operates as a multi-extortion group, hosting a TOR-based blog to list victim names and any exfiltrated data. Victims are aggressively coerced into payment to avoid having their data leaked publicly. Knight has been actively advertised and sold on the RAMP forum. Knight ransomware is delivered primarily through phishing and spear phishing campaigns. Some early examples include those masquerading as messages from TripAdvisor." Knight developers also offer affiliates a lite version, or "Knight Lite," for broader, non-targeted spam-based attacks.

Threat Analysis

The threat actors behind Knight ransomware employ a multifaceted approach to deliver the malicious payload via email. The email campaigns observed were predominantly low volume, with fewer than 500 messages, although one contained over 1,000. These campaigns primarily targeted English-speaking users, with additional campaigns in Italian and German. The emails had lures themed around invoices and messages from well-known travel websites, predominantly targeting hospitality organizations. When opened, these lures contained an HTML attachment that loaded a browser-in-the-browser interface spoofing legitimate sites, prompting victims to download a zipped executable or XLL file containing the ransomware. Later, campaigns modified the attack chain to include an interstitial zip file containing either an LNK linking to a WebDAV share or an XLL. Both installed a downloader that then deployed the Knight payload. Once installed, the ransomware initiated lateral movement, scanning for private IP addresses before encrypting networked devices.

The intentions of the threat actors behind Knight ransomware are financial gain, as evidenced by the ransom demands ranging from $5,000-$15,000 in Bitcoin. The ransomware encrypts files and leaves a ransom note with no current indication of data exfiltration. The lack of data exfiltration suggests that the actors do not seek to sell the data in underground marketplaces or will extort victims by threatening to release the data. The objectives of these actors are to target a variety of users, focusing on English-speaking, aiming for unauthorized access and disruption of systems through encryption. The capabilities of the threat actors are evident in their ability to modify attack chains, utilize different lures, and develop new downloaders, indicating a level of adaptability and resourcefulness in their operations.

Risk & Impact Assessment

The risk posed by Knight ransomware is significant, given its direct email delivery method and affiliates' ability to adapt and modify attack chains. There is a low to moderate risk of organizations being affected by Knight Ransomware, giving organizations time to implement necessary mitigations to prevent an attack. The threat jeopardizes the availability of data and information systems, enabling threat actors to disrupt operations and encrypt critical data. The absence of data exfiltration does not diminish the risk and impact; it only takes one user to open the attachment, impacting the organization. Knight ransomware can have a substantial material impact on affected organizations. This impact can manifest through various means, including operational disruption, reputation damage, ransom payments, regulatory fines, remediation costs, and business downtime, potentially affecting net sales, revenues, and operational continuity. The ransom demands further exacerbate the financial implications, highlighting the tangible consequences of the threat actor's operations on organizational assets and functions.

Outlook

In light of the campaign's disclosure, it is plausible that the threat actors behind this Knight ransomware campaign may adapt their tactics, techniques, and procedures (TTPs) to maintain the efficacy of their operations. The disclosure allows them to assess what is known and not known about their operations and modify their approach to circumvent detection and mitigation measures more effectively. The most likely actions could involve diversifying their delivery methods, refining their lures, and further modifying the attack chain. Additionally, the campaign's disclosure may serve as a learning opportunity for other threat actors. It is not uncommon for threat actors to observe and learn from the successes and failures of their peers. Other groups may analyze the disclosed details to enhance their own campaigns, incorporating successful elements and improving upon the weaknesses identified, leading to an increase in future attacks employing the same tactics, techniques, and procedures.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to the evolving threat landscape posed by Knight ransomware, customers should implement the following actions to mitigate the spam phishing emails delivering this ransomware and improve an organization's cyber resilience:

- Develop and conduct training programs tailored to the organization's varying levels of user knowledge and experience, focusing on recognizing phishing emails and unsafe links.
- Employ email filtering solutions that organizations can adjust to the specific needs and existing systems to block malicious emails effectively.
- Ensure that data backups are conducted regularly, with considerations for secure and isolated storage, particularly for organizations with diverse IT infrastructures.
- Explore and deploy endpoint protection solutions that align with the organization's existing cybersecurity infrastructure and can detect and mitigate ransomware threats.
- Evaluate and implement network segmentation to limit the lateral movement within networks, with adaptability to different network architectures.

Additional threat hunting guidance can be found in Appendix A, and general mitigation guidance in Appendix B.

Sandman APT Targets Global Telecoms in August Cyber-Espionage Campaign

Sandman | LuaDream | Pass-the-Hash | DLL Sideloading | Data Exfiltration | Information

Source Material: SentinelOne
Targeted Industries: Information, but likely impacting all industries in future operations

Executive Summary

As part of our initiative to provide reports on the latest developments in advanced persistent threat groups (APTs), the Adversary Tactics and Intelligence team compiled this report, analyzing the recent blog post by SentinelOne titled "Sandman APT | A Mystery Group Targeting Telcos with a LuaJIT Toolkit."

This report finds that the APT Sandman has conducted sophisticated cyber-espionage campaigns, primarily targeting telecommunications providers across the Middle East, Western Europe, and the South Asian subcontinent. The group utilized a meticulous seven-stage infection process. They deployed the advanced LuaDream malware, characterized by its multi-component and multi-protocol nature, to infiltrate, persist, and gather intelligence. Additionally, LuaDream can manage actor-provided plugins, communicate over various protocols, including TCP, HTTPS, WebSocket, and QUIC, and exfiltrate system and user information, showcasing the group's technical proficiency and adaptability. Recommendations include monitoring and restricting the use of NTLM where possible and securing administrative credentials using best practices such as multi-factor authentication and privileged access management.

Insights & Determinations

- Sandman's adeptness in utilizing various infiltration techniques underscores their meticulous planning and execution. This proficiency in compromising systems and maintaining persistence reveals a significant capability to abuse and manipulate network environments.
- The development and use of LuaDream indicate a high level of sophistication and adaptability. The backdoor's various capabilities showcase Sandman's technical proficiency and the potential for evolving tactics.
- The discernible risk of losing confidentiality due to Sandman's operations and the likely expansion of targeted industries signifies a broadening of the threat landscape, underscoring the imperative for organizations across various industries to enhance their cybersecurity measures to safeguard against the evolving and expanding threat posed by Sandman.
- The short-term outlook suggests that the disclosure of Sandman's campaign may lead to adaptations in their tactics and potential adoption by other threat actors, underscoring the dynamic nature of the threat landscape.

Introduction

This cyber threat intelligence report's purpose is to provide actionable intelligence related to the advanced persistent threat group Sandman and their deployment of LuaDream, focusing on analyzing their activities, primary targets, risk and impact assessment, short-term outlook, and recommended mitigation measures. The combination of LuaDream's advanced capabilities and the meticulous infection process represents the most significant threat, highlighting Sandman's ability to infiltrate, persist, and gather intelligence from targets. The intelligence presented herein is derived from an in-depth analysis of a blog post published by SentinelOne titled "Sandman APT | A Mystery Group Targeting Telcos with a LuaJIT Toolkit." If you have questions or feedback about this intelligence, you can submit them **here**.

Overview & Background

The blog post from SentinelOne titled "Sandman APT | A Mystery Group Targeting Telcos with a LuaJIT Toolkit" details the activities of an advanced persistent threat (APT) group dubbed Sandman conducted in August 2023, which primarily targeted telecommunication providers across the Middle East, Western Europe, and the South Asian subcontinent. The blog post aims to shed light on Sandman's deployment of a novel modular backdoor utilizing the LuaJIT platform, referred to as LuaDream, and to analyze the group's tactics, techniques, and procedures (TTPs). The blog post explores the implementation and architecture of LuaDream, the strategic lateral movements and minimal engagements of the threat actor, and the geographical distribution of the victims.

Sandman is an enigmatic APT group of unknown origin, characterized by its strategic and deliberate approach to minimize detection. Given these providers' sensitive data, the group has focused on targeting telecommunications providers, likely for espionage motivations. LuaJIT, or Lua Just-In-Time Compiler, is a lightweight, high-performance scripting language often used in gaming and embedded applications. It is relatively rare in the context of APT malware, making its use by Sandman notable. The LuaJIT platform allows for the execution of malicious Lua script code, which can be challenging to detect, indicating a well-executed and actively developed project by Sandman.

Threat Analysis

The group employed strategic lateral movements and minimal engagements to achieve its objectives while minimizing the risk of detection. The activities observed suggested a deliberate approach, with the group infiltrating specifically targeted workstations and deploying the necessary folders and files for loading and executing LuaDream, refraining from any further actions that might trigger alarms.

In the initial stages of their campaign, Sandman exhibited adeptness in utilizing various infiltration techniques. The group leveraged the pass-the-hash technique over the NTLM authentication protocol to gain unauthorized access, highlighting their ability to abuse authentication mechanisms. Additionally, the theft of administrative credentials was a pivotal step in their strategy, enabling them to maneuver through the targeted networks with elevated privileges. This approach facilitated the deployment of LuaDream through DLL hijacking, allowing them to execute malicious code by exploiting the loading of legitimate DLLs. These tactics underscored Sandman's meticulous planning and execution, revealing their proficiency in utilizing techniques to compromise systems and maintain persistence.

LuaDream, a novel modular backdoor developed using the LuaJIT platform, stood as the centerpiece of Sandman's arsenal. SentinelOne could not associate LuaDream with any known threat actor at the time of publication. However, they lean towards the possibility of a private contractor or mercenary group. The backdoor is characterized by its multi-component and multi-protocol nature, with the main functionalities revolving around managing actor-provided plugins and exfiltrating system and user information. The architecture of LuaDream indicated an actively maintained and developed project of considerable scale, with the implementation designed to evade detection and hinder analysis. The backdoor employed intricate staging processes, conducted entirely in memory, involving a combination of fully-formed DLL PE images, code, and LuaJIT bytecode. LuaDream communicated over various protocols, including TCP, HTTPS, WebSocket, and QUIC, showcasing its versatility in establishing connections with command and control (C2) servers.

The primary targets of Sandman's campaign were telecommunications providers in the Middle East, Western Europe, and the South Asian subcontinent. The group's focus on this sector suggested a strategic interest in accessing sensitive data, a common target for intelligence collection activities. The geographical distribution of the victims indicated a broad and diversified targeting approach, hinting at the group's extensive capabilities and resources.

The threat actors' intentions behind these operations appeared to be intelligence collection due to the strategic targeting of telecommunication providers and the deployment of advanced malware like LuaDream. The group aimed to gather sensitive information, likely for political, economic, or strategic advantage. The sophistication of the attacks and the targets indicated objectives related to unauthorized access to systems holding valuable information to exfiltrate sensitive data. The capabilities of Sandman, as evidenced by the development and deployment of LuaDream, demonstrated a high level of technical proficiency, resourcefulness, and adaptability, marking them as a significant threat in the cyber landscape.

Risk & Impact Assessment

Given Sandman's known operations and focus on intelligence collection, the discernible risk to customers predominantly pertains to losing confidentiality. If Sandman operates as a contractor or mercenary group or is nation-state sponsored, the breadth of industries targeted will likely expand, especially with shifts in the political landscape, thereby broadening the threat landscape. The loss of confidentiality could cause a material impact on customers due to unauthorized access and exfiltration of sensitive information, leading to the loss of competitive advantage and intellectual property, potentially eroding market share and causing reputational damage.

These factors can have a cascading effect on financial performance as customers and partners lose trust, and the organization faces potential legal liabilities and regulatory fines. While there is no direct evidence of Sandman compromising the integrity and availability of data or systems, the exclusive risk to confidentiality alone can translate to significant financial repercussions. The realization of these risks and impacts underscores the critical need for implementing robust cybersecurity measures to safeguard sensitive information and maintain organizational trust.

Outlook

In the short term, the disclosure of Sandman's campaign will likely prompt a recalibration of their tactics, techniques, and procedures (TTPs) to maintain operational security and evade detection. The threat actors may opt for more covert methods, diversify their toolsets, or shift their focus to different industries or geographical regions. The most likely actions for future campaigns could involve the refinement of LuaDream, the exploration of alternative entry points, and the potential targeting of different sectors that hold valuable information. Other threat actors will likely adapt Sandman's methodologies or launch similar campaigns to avoid attribution and bolster their operations, potentially increasing the overall cyber threat landscape. The anticipation of these developments underscores the importance of continuous vigilance and adaptive cybersecurity strategies to mitigate emerging threats.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to the sophisticated operations of Sandman and their deployment of LuaDream, customers should implement the following specific actions to mitigate the risks associated with this threat actor and enhance cyber resilience:

- Organizations should monitor and restrict the use of NTLM where possible, implementing more robust authentication protocols.
- Organizations should secure administrative credentials using best practices such as multi-factor authentication and privileged access management.
- Monitor for suspicious DLL activity, particularly the creation or modification of ualapi.dll in the C:\Windows\System32\ directory and any unusual interaction with Fax and Spooler Windows services.
- Enhance monitoring for signs of unusual service behavior, as Sandman did not force the execution of LuaDream by restarting services.
- Employ solutions that can inspect memory loading and execution of processes, mainly focusing on detecting LuaJIT bytecode.
- Block and monitor for the presence of known **IOCs** associated with Sandman operations..
- Analyze and secure communication over TCP, HTTPS, WebSocket, and QUIC protocols and monitor for unusual patterns or unauthorized communication.

Additional threat hunting guidance can be found in Appendix A, and general mitigation guidance in Appendix B.

3 APTs Conducted Cyber Espionage Against a Southeast Asian Government, Employing Sophisticated Tools and Techniques

Stately Taurus | Alloy Taurus | Gelsemium | Data Exfiltration | Cyber Espionage | Public Administration

Source Material: Palo Alto Unit 42

- Unit 42 Researchers Discover Multiple Espionage Operations Targeting Southeast Asian Government
- Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda
- Persistent Attempts at Cyberespionage Against Southeast Asian Government Target Have Links to Alloy Taurus
- Rare Backdoors Suspected to be Tied to Gelsemium APT Found in Targeted Attack in Southeast Asian Government

Targeted Industries: Public Administration, but has the potential to impact all industries in future campaigns

Executive Summary

As part of our initiative to provide open-source reports on the latest developments in cyber espionage campaigns, the Adversary Tactics and Intelligence team compiled this report, analyzing a series of blog posts by Palo Alto's Unit 42.

This report finds that three distinct threat actor clusters, identified as CL-STA-0044 (Stately Taurus/Mustang Panda), CL-STA-0045 (Alloy Taurus/GALLIUM), and CL-STA-0046 (suspected Gelsemium), have conducted extensive cyber espionage operations against a Southeast Asian government, employing a variety of sophisticated tools and techniques. The findings reveal meticulous scanning of infected environments, deployment of multiple backdoors and web shells, utilization of credential-stealing techniques, and exfiltration of sensitive information, indicating a strategic focus on intelligence collection for political, economic, or strategic gains. Recommendations include implementing advanced network monitoring to detect specific tools and enhancing credential security through multifactor authentication and regular reviews and updates of access controls.

Insights & Determinations

- The meticulous scanning of infected environments and deployment of multiple backdoors and web shells by clusters CL-STA-0044, CL-STA-0045, and CL-STA-0046 indicate a high level of sophistication and adaptability, highlighting their capability to maintain long-term access for strategic intelligence collection.
- These clusters' exfiltration of sensitive information underscores their strategic focus on acquiring political, economic, or strategic gains, reflecting a persistent threat to the public administration sector and potentially all sectors.
- The potential compromise and disclosure of sensitive data by these threat actor clusters pose a significant risk of reputational damage to corporations, jeopardizing competitive advantages and affecting customer trust and market standing.
- The adaptive responses anticipated from the threat actors following the campaigns' disclosure suggest a likelihood of evolving tactics and techniques, indicating a persistent and escalating threat landscape with a possibility of targeting corporations in the future.

Introduction

Based on our in-depth analysis of a series of blog posts from Unit 42, Palo Alto's intelligence and response team, this report delivers actionable intelligence on espionage attacks against a Southeast Asian government. Focused on three distinct threat actor clusters, CL-STA-0044, CL-STA-0045, and CL-STA-0046, it aims to equip organizations with insights to enhance their cyber resilience against these multifaceted threats. The ensuing sections will delve into each cluster's operations, assess risks and impacts, provide a short-term outlook, and propose mitigation measures. For questions or feedback regarding this intelligence, submissions can be made **here**.

Overview & Background

The blog posts from Unit 42 detail a series of espionage attacks targeting a government in Southeast Asia, executed by separate threat actors grouped into three distinct clusters: CL-STA-0044, CL-STA-0045, and CL-STA-0046. These posts aim to provide details about each cluster's operations, shedding light on the actors' objectives, methods, and the vulnerabilities exploited. The analysis encompasses a variety of systems and data, including the identification of malicious software, network interactions, and the examination of compromised assets, to produce a holistic view of the threat landscape.

The three identified clusters of activity, CL-STA-0044, CL-STA-0045, and CL-STA-0046, represent distinct cyber-espionage campaigns attributed to different Advanced Persistent Threat (APT) groups. CL-STA-0044 is linked to **Stately Taurus** (Mustang Panda), a group known for its focus on intelligence collection, primarily targeting non-profit organizations and entities in the education sector across Southeast Asia. **Alloy Taurus**, associated with CL-STA-0045, has been observed conducting campaigns to establish long-term persistence and obtain access to telecommunications and technology companies, often exploiting vulnerabilities in web servers. CL-STA-0046 is suspected to be tied to the rarely-seen **Gelsemium** APT, a group with a history of sophisticated attacks against governmental institutions, utilizing various tools and techniques to maintain access and perform reconnaissance.

Threat Analysis

CL-STA-0044 (Stately Taurus/Mustang Panda)

The group meticulously scanned infected environments, identifying live hosts, open ports, domain users, and groups, utilizing tools like LadonGo, NBTScan, AdFind, and Impacket. They employed various credential-stealing techniques, deploying tools such as Hdump, MimiKatz, and DCSync and extracting the Ntds.dit file to access Active Directory data.

The group maintained access through multiple backdoors and web shells, notably using an undocumented variant of ToneShell malware, which is distinctive to Stately Taurus. This variant comprises three DLL components, each responsible for persistence, C2 communication, and executing commands. Additionally, the group deployed Cobalt Strike agents and ShadowPad backdoors, a modular malware associated with Chinese threat actors.

Stately Taurus demonstrated a high level of targeting precision, focusing on specific individuals within the victim organizations. They used the utility wevtutil to gather information about particular usernames and pinpoint hostnames of interest, which were later compromised. The group archived and exfiltrated numerous documents and sensitive information, utilizing tools like rar.exe and cloud storage sites, indicating a continuous intelligence-gathering operation.

Stately Taurus focused strategically on intelligence collection, primarily acquiring sensitive governmental information from Southeast Asia for political, economic, or strategic gains. The group demonstrated multifaceted objectives, including unauthorized access, data exfiltration, and establishing a persistent presence in targeted systems, mainly focusing on high-value individuals within organizations. Showcasing advanced technical proficiency, Stately Taurus employed a variety of distinctive tools and malware, such as an undocumented variant of ToneShell, Cobalt Strike, and ShadowPad, reflecting their adaptability, sophistication, and resourcefulness in conducting long-term operations.

Threat Analysis Continued

CL-STA-0045 (Alloy Taurus/GALLIUM)
Initiated multi-wave intrusions, exploiting vulnerabilities in Exchange Servers to deploy numerous web shells. These shells facilitated the introduction of a variety of tools and malware, including China Chopper, Fscan, WebScan, Reshell, Zapoa, SoftEther VPN, Kerbrute, LsassUnhooker, GoDumpLsass, Mimikatz, LaZagne, Cobalt Strike, HTran, PuTTY, Quasar RAT, HDoor, Gh0stCringe RAT, and a variant of Winnti malware. The group demonstrated a mature approach, employing a combination of credential theft techniques, lateral movement strategies, and the installation of additional tools to maintain persistence and perform malicious activities.

In their operations, Alloy Taurus deployed a diverse array of tools and malware to achieve their objectives. Web shells, particularly China Chopper, were utilized for initial access and control. Scanners like Fscan and WebScan were employed for network scanning, while backdoors like Reshell and Zapoa facilitated remote command execution. The group also used SoftEther VPN software for establishing secure connections and bypassing security measures. They employed various credential theft tools to obtain domain credentials, including Kerbrute, LsassUnhooker, GoDumpLsass, Mimikatz, and LaZagne. For lateral movement across the network, AnyDesk was the tool of choice. Additional malware, including Cobalt Strike, Quasar RAT, HDoor, and Gh0stCringe RAT, were introduced for various malicious capabilities. The group also utilized tunneling tools such as HTran and PuTTY for SSH tunneling, and a variant of Winnti malware was deployed for additional capabilities.

Alloy Taurus is believed to operate with Chinese state interests, focusing on cyber espionage against government entities. The group's intentions likely encompass long-term intelligence collection and establishing a resilient foothold within compromised networks for political, economic, or strategic advantage. The objectives involve targeting critical assets such as web servers and domain controllers, exploiting vulnerabilities, and exfiltrating sensitive information. Alloy Taurus demonstrates a high level of capabilities, utilizing a unique playbook of tools and malware, exhibiting a repetitive attack style, and effectively adapting to different environments and security measures.

CL-STA-0046 (Gelsemium)
Executed a series of stealthy and sophisticated activities over six months between 2022-2023, targeting sensitive IIS servers within a Southeast Asian government entity. The initial infection vector involved the installation of several web shells, including reGeorg, China Chopper, and AspxSpy, on a compromised web server, facilitating access, basic reconnaissance, lateral movement via SMB, and downloading additional tools. The attackers demonstrated adaptability by delivering new tools following unsuccessful installation attempts, highlighting their persistence and advanced capabilities.

The actors deployed a diverse set of additional tools and malware to further their control within the compromised environment. Among these were OwlProxy, a unique HTTP proxy with backdoor functionality previously used against the Taiwanese government, and SessionManager, a custom backdoor allowing command execution and communication with additional network systems. The use of Cobalt Strike, EarthWorm for creating a tunnel for C2 traffic, and SpoolFool, a local privilege escalation tool exploiting CVE-2022-21999, were also observed. These tools and others showcased the group's adaptability, knowledge of diverse tools, and ability to leverage known vulnerabilities.

Gelsemium, operational since 2014, has a history of targeting diverse entities, including governments, universities, and manufacturers, primarily in East Asia and the Middle East. The group's intentions for this operation were focused mainly on intelligence collection from government entities in Southeast Asia, reflecting a strategic interest in governmental operations and sensitive information. The objectives included gaining unauthorized access to sensitive IIS servers and exfiltrating valuable data, leveraging various tools and malware to maintain persistence and adaptability within the compromised environments. The capabilities of Gelsemium were evident in their use of rare and custom tools, adaptability to mitigation efforts, and the execution of a multifaceted and stealthy operation, indicative of a sophisticated and resourceful APT group.

Risk & Impact Assessment

The operations of clusters CL-STA-0044, CL-STA-0045, and CL-STA-0046 pose a significant threat to corporations, particularly regarding the confidentiality of sensitive and proprietary information. The detailed and covert intelligence-gathering activities and the utilization of advanced tools and techniques for unauthorized access highlight the potential for substantial impact on corporate entities and their assets. The compromise and potential disclosure of sensitive data jeopardize corporate competitive advantages and present a considerable risk of reputational damage, which could affect customer trust and market standing. While the exact impact on net sales, revenues, or income from continuing operations can be challenging to quantify, the strategic loss of proprietary information and the potential disruption of business operations emphasize the seriousness of the threat and its extensive ramifications for the corporate sector.

Outlook

In a short-term outlook, the campaigns' disclosure will likely prompt adaptive responses from the threat actors behind the clusters. Historically, threat actors have demonstrated a propensity to evolve their tactics, techniques, and procedures (TTPs) to maintain operational security and avoid detection, suggesting a likelihood of modification in their approach. While they targeted government entities in August, the possibility of targeting corporations in the future cannot be discounted, given that Chinese state-sponsored threat actors are known for their proprietary information theft. The most probable actions in future campaigns may involve the deployment of new or modified malware, exploiting emerging vulnerabilities, and refining intrusion methods to enhance stealth and persistence. Additionally, the disclosure of the campaign could serve as a learning opportunity for other threat actors, potentially leading to the adoption or adaptation of successful TTPs observed in this campaign, thereby diversifying and escalating the threat landscape.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to the evolving threat landscape characterized by the sophisticated Tactics, Techniques, and Procedures (TTPs) employed by clusters CL-STA-0044, CL-STA-0045, and CL-STA-0046, customers should implement the following actions to mitigate the risks posed by these threat actors and enhance an organization's cyber resilience:

- Implement advanced network monitoring to detect the use of tools like LadonGo, NBTScan, AdFind, Impacket, Fscan, WebScan, and the utility wevtutil.
- Enhance credential security by implementing multi-factor authentication and conducting regular reviews and updates of access controls, focusing on mitigating the risk of tools such as Hdump, MimiKatz, DCSync, Kerbrute, LsassUnhooker, GoDumpLsass, and LaZagne.
- Develop and deploy detection signatures for the identified malware variants such as ToneShell, Cobalt Strike, ShadowPad, China Chopper, Reshell, Zapoa, Quasar RAT, HDoor, Gh0stCringe RAT, Winnti malware, OwlProxy, SessionManager, EarthWorm, and SpoolFool.
- Implement Web Application Firewalls to secure the deployment of web shells like reGeorg, China Chopper, and AspxSpy.
- Implement network segmentation to isolate critical systems and sensitive data, limiting lateral movement within the network.
- Deploy advanced endpoint protection and Endpoint Detection and Response (EDR) solutions focusing on the specific tools and malware the clusters use.
- Prioritize and expedite the application of patches and updates, especially for Exchange Servers and other critical systems, to mitigate known vulnerabilities exploited by the threat actors.
- Block the known IOCs (**here**, **here**, and **here**) associated with these clusters.

Additional threat hunting guidance can be found in Appendix A and general mitigation guidance in Appendix B.

APT29 Phishing Campaigns Evolve Malware Delivery Methods Between March and July

APT29/Cozy Bear | ROOTSAW | Phishing | Phishing Links & Attachments | Public Administration

Source Material: Mandiant
Targeted Industries: Public Administration, but has the potential to impact all industries in future campaigns

Executive Summary

As part of our initiative to provide open-source reports on the latest developments in advanced persistent threats, the Adversary Tactics and Intelligence team compiled this report, analyzing the recent blog post by Mandiant titled "Backchannel Diplomacy: APT29's Rapidly Evolving Diplomatic Phishing Operations."

This report finds that APT29, a sophisticated cyber-espionage group attributed to Russia's SVR, has conducted phishing campaigns between March and July 2023, targeting high-value diplomatic and governmental entities. The group demonstrated a consistent evolution in malware delivery methods, shifting from links to attachments to introducing new malware variants, such as ICEBEAT while enhancing the capabilities of existing malware like ROOTSAW. APT29 strategically balanced actor-controlled servers and compromised websites, showcasing adaptability and the persistent pursuit of more covert infiltration methods. The analysis reveals a significant risk of unauthorized access and disclosure of sensitive information, potentially impacting the targeted organizations. Recommendations include implementing advanced email filtering solutions and regular user training and awareness programs to identify and mitigate phishing attempts, enhancing an organization's cyber resilience against such advanced threats.

Insights & Determinations

- APT29 has demonstrated a significant and consistent evolution in their tactics, techniques, and procedures, particularly in malware delivery methods. This evolution indicates a high level of adaptability and a persistent pursuit of more covert and sophisticated infiltration methods, posing an increased threat to high-value targets.
- The strategic balance between using actor-controlled servers and compromised websites, coupled with the meticulous crafting of phishing emails, underscores APT29's commitment to refining their techniques and minimizing the risk of exposure and detection. This adaptability and advanced tradecraft make APT29 a formidable threat to organizations worldwide.
- The meticulous crafting of phishing campaigns, continuous adaptation of malware delivery mechanisms, and targeting high-value entities result in a substantial risk of unauthorized access and disclosure of sensitive information. The potential impact on the targeted organizations could be considerable, leading to material consequences on revenues and operations, highlighting the imperative for robust cybersecurity measures.
- The plausible refinement and enhancement of APT29's existing tactics, techniques, and procedures, mainly focusing on the evolution of ROOTSAW in response to the disclosure of their campaign, indicate a likely continuation of sophisticated cyber-espionage activities.

Introduction

This report synthesizes insights derived from Mandiant's detailed examination of APT29's activities, aiming to deepen understanding and awareness of the evolving threats posed by this formidable cyber-espionage group. Focusing on their campaigns conducted between March and July 2023, we dissect APT29's sophisticated phishing campaigns, adaptive strategies, and the potential ramifications of their operations. The purpose is to explain the group's modus operandi and equip organizations with actionable mitigation measures to enhance cyber resilience against such advanced threats. This analysis anticipates the possible trajectories of APT29's evolving tactics and the broader implications for the global cybersecurity landscape by offering a forward-looking outlook. If you have questions or feedback about this intelligence, you can submit them **here**.

Overview & Background

The blog post from Mandiant titled "Backchannel Diplomacy: APT29's Rapidly Evolving Diplomatic Phishing Operations" provides an in-depth examination of the evolving threat posed by APT29, a cyber-espionage group associated with the Russian government. The blog post highlights APT29's latest tactics, techniques, and procedures (TTPs), focusing on their sophisticated phishing operations targeting diplomatic entities. By analyzing compromised communication channels, phishing emails, and malicious payloads, the blog post offers valuable insights into APT29's modus operandi and its implications for diplomatic cybersecurity.

APT29, also known as Cozy Bear, is a highly sophisticated and well-resourced Advanced Persistent Threat (APT) group attributed to Russia's Foreign Intelligence Service (SVR). The group has been active since 2008 and is known for its extensive cyber espionage campaigns targeting government networks, research institutes, think tanks, and various industries in Europe, the United States, and Asia. APT29 has been involved in several high-profile cyber attacks, including the 2016 Democratic National Committee (DNC) hack and the SolarWinds supply chain attack in 2020. The group uses a variety of tactics, techniques, and procedures (TTPs) to gain access to target networks, including spearphishing, social engineering, and the exploitation of software vulnerabilities. Once inside a network, APT29 deploys custom malware and tools to maintain persistence and exfiltrate sensitive data. The group is known for its advanced tradecraft, adaptability, and ability to blend into regular network traffic to evade detection. APT29 has a history of using trusted and legitimate cloud services for their attacks, such as social media platforms and cloud storage services. Overall, APT29 is considered one of the world's most sophisticated and persistent APT groups, and its activities have been a significant concern for governments and organizations globally.

Threat Analysis

In response to Ukraine's early planning and counteroffensive in June 2023, APT29 has been notably active, conducting phishing campaigns between March and July 2023 to gain initial access to targets, exhibiting a rapidly evolving approach. The group has demonstrated a shift in malware delivery methods, opting for more sophisticated and covert techniques to infiltrate their targets. The phishing emails sent by APT29 were meticulously crafted, often impersonating diplomatic entities, to lure the victims into interacting with malicious content. Various infection chains attributed to APT29 have coincided within a single campaign, suggesting that distinct initial access operators or subteams may be operating in parallel to service different regional targets or espionage objectives.

Decisions about which malware delivery approach to use or when to introduce new later-stage malware variants are unknown. However, mission-specific parameters such as targets or operational objectives may influence these decisions. Typically, APT29 reserves the first use of new capabilities for targets inside Ukraine or diplomatic entities associated with the North Atlantic Treaty Organization (NATO) or European Union (EU) member states. Then, these capabilities are incorporated into its broader operations with minimal changes, pointing to the group's possible changing risk calculus after first exposure.

Throughout the phishing campaigns conducted from March to July 2023, APT29 exhibited a consistent pattern of evolution and adaptation in their malware delivery methods and tactics. In March, the group initiated campaigns using links, sometimes generated by URL shortening service, to direct victims to compromised websites hosting a new version of ROOTSAW with user-agent-based anti-analysis to filter out non-compatible victim devices. This approach was further refined in subsequent campaigns, shifting the anti-analysis guardrails server-side and introducing additional filtering layers, including IP filtering facilitated by public API services.

April saw a departure from using ROOTSAW and a shift towards using attachments, with victims directly receiving malicious ISO or ZIP files if they passed server-side checks, a tactic likely adopted to minimize forensic artifacts. The campaigns in May and June demonstrated a further evolution in delivery mechanisms, incorporating Scalable Vector Graphics (SVG) and introducing new variants of ROOTSAW, indicative of APT29's continuous efforts to enhance their techniques. These months also witnessed a strategic balance between using actor-controlled servers and compromised websites, allowing for more controlled operations, including profiling victim information and delivering tailored next-stage downloaders. By July, they introduced ICEBEAT, a new downloader utilizing the Zulip messaging platform for C2, and the incorporation of ROOTSAW within PDFs marked a further evolution in APT29's operations, showcasing their persistent pursuit of more sophisticated and covert infiltration methods.

Threat Analysis Continued

APT29's progression underscores their commitment to refining their techniques, ensuring the successful profiling of victims, and minimizing the risk of exposure and detection through the evolution in links and attachments, the variety in dropped files, and the strategic use of command and control servers.

APT29 has also made a concerted effort to update and evolve their later-stage malware, increasing the quantity and quality of tooling used across its campaigns. At least six distinct downloaders have been identified during the first half of 2023: BURNTBATTER, DONUT, SPICYBEAT, MUSKYBEAT, STATICNOISE, and DAVESHELL. BURNTBATTER is an in-memory loader observed loading the SPICYBEAT downloader through a shellcode dropper named DONUT, a public tool for creating position-independent shellcode. SPICYBEAT, written in C++, downloads the next-stage payload from DropBox or OneDrive. MUSKYBEAT is an in-memory dropper decoding and executing next-stage payloads. STATICNOISE, another downloader written in C, handles the final-stage payload. DAVESHELL, based on a publicly available repository, operates as an in-memory dropper using reflective injection to execute its embedded payload.

APT29's intentions behind these sophisticated campaigns are multifaceted. Primarily, the group seeks to gain initial access to facilitate a centralized exploitation team's collection of sensitive information, trade secrets, intellectual property, and government secrets for political, economic, or strategic advantage. The current targeting of diplomatic entities and government institutions indicates a focus on obtaining information concerning the current pivotal phase of the Ukraine/Russia war. The objectives of APT29 are clear: to infect systems from a diverse range of high-value targets with the ROOTSAW malware to deliver follow-on payloads. In terms of capabilities, APT29 is highly skilled and resourceful. The group's ability to evolve their tactics, techniques, and procedures (TTPs), consistently update ROOTSAW, and use a diverse range of follow-on payloads showcases their advanced knowledge and skills in cyber espionage. The continuous adaptation and evolution demonstrate the significant resources available to them, making them a formidable threat to organizations worldwide.

Risk & Impact Assessment

Given the group's sophisticated and evolving tactics to obtain unauthorized access to sensitive data and systems, there is a significant likelihood of losing confidentiality. The meticulously crafted phishing campaigns, the continuous adaptation of malware delivery mechanisms, and the targeting of high-value targets underscore the substantial risk of unauthorized access and disclosure of sensitive information. The impact of APT29's operations on organizations could be considerable, potentially leading to a material impact on net sales, revenues, or income from continuing operations. The unauthorized access and likely exfiltration of proprietary information compromise the business operations of targeted organizations and could have cascading effects on revenue. The intentions behind APT29's campaigns further amplify the potential damage, underscoring the imperative for robust cybersecurity measures to mitigate the risks and safeguard confidentiality.

Outlook

It is plausible that APT29 will respond to the disclosure of their campaign by further refining and enhancing their existing tactics, techniques, and procedures, mainly focusing on the evolution of ROOTSAW. The group will likely implement additional filtering mechanisms to this malware to improve user and system profiling while minimizing exposure and detection risks. Given their historical behavior, APT29 will probably continue to employ phishing emails as their primary initial access vector, with a potential variation in the use of links and attachments based on the campaign's objectives and targeted entities. The type of attachments used may also vary, reflecting the group's adaptability and the continuous effort to optimize their infiltration success.

Considering APT29's strategy of initially deploying new capabilities against specific targets related to Ukraine, NATO, or EU member states, we anticipate that any significant advancements or modifications in their arsenal will first be observed in operations targeting these entities. Subsequently, these enhanced capabilities will likely be integrated into their broader global operations, reflecting Russia's extensive geopolitical interests and ambitions. Observing APT29's evolving tactics, other threat actors may attempt to learn from and adapt some of these sophisticated methods, potentially leading to a shift in the threat landscape. The anticipation of enhanced cybersecurity responses post-disclosure will also shape APT29's future strategies as they navigate an environment of increased vigilance and improved defenses.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to the evolving tactics and techniques of APT29, customers should implement the following actions to mitigate the risks posed by APT29's phishing campaigns and improve an organization's cyber resilience:

- Implement advanced email filtering solutions to identify and block phishing emails, preventing initial access through spearphishing links and attachments.
- Conduct regular training and awareness programs to educate users on recognizing phishing attempts and the risks associated with clicking suspicious links or opening unknown attachments.
- Enable Multi-Factor Authentication (MFA) across all possible systems, especially for external remote services, to add a layer of security, reducing the risk of unauthorized access.
- Implement application control policies using solutions like Microsoft's **AppLocker** to prevent the execution of unauthorized and malicious executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers.
- Implement advanced network monitoring solutions to detect unusual traffic, connections to virtual private servers, non-standard ports, and any signs of command and control communication. Employ anomaly detection to identify unusual user behavior or system interactions.
- Utilize Data Loss Prevention (DLP) solutions to monitor and prevent unauthorized data exfiltration, thereby mitigating the risk of data loss during the exfiltration stage.
- Limit user privileges, apply the principle of least privilege, and monitor account activities to detect and respond to any unauthorized or suspicious activities.
- Block the known **IOCs** associated with this threat.

Additional threat hunting guidance can be found in Appendix A and general mitigation guidance in Appendix B.

SSH Fingerprint Leads to the Identification of Extensive Infrastructure Used in Ransomware Attacks

ShadowSyndicate | Ransomware | Cobalt Strike - IcedID - Matanbuchus - Sliver | Industries/All

Source Material: Group-IB
Targeted Industries: All

Executive Summary

As part of our initiative to provide reports on the latest developments in threat actor infrastructure, the Adversary Tactics and Intelligence team compiled this report, analyzing the recent blog post by Group-IB titled "Dusting for fingerprints: ShadowSyndicate, a new RaaS player?."

This report finds that ShadowSyndicate, a potentially emerging Ransomware-as-a-Service (RaaS) affiliate, is leveraging an extensive and diverse infrastructure, all using a single unique SSH fingerprint. The detailed analysis reveals the group's affiliations with various ransomware families, including high-confidence attributions to Quantum, Nokoyawa, and ALPHV and low-confidence attributions to Royal, Cactus, and Play. The group's operations pose significant risks to organizations, primarily through the loss of confidentiality and availability, leading to substantial financial and reputational repercussions. The report also uncovers the geographical preferences of ShadowSyndicate's server locations, with Panama being a notable hotspot, and highlights potential links between ShadowSyndicate and Cl0p infrastructure. In light of these findings, recommendations include blocking the known IOCs associated with ShadowSyndicate's infrastructure enhancing organizations' cyber resilience.

Insights & Determinations

- Using a unique SSH fingerprint across an extensive and diverse infrastructure indicates a deliberate effort to maintain connectivity among a large number of malicious servers, enhancing their ability to launch and manage ransomware attacks.
- ShadowSyndicate's affiliations with Quantum, Nokoyawa, ALPHV, Royal, Cactus, and Play ransomware families underscore the group's potential reach and versatility in ransomware operations.
- The primary risks posed by ShadowSyndicate's operations stem from the loss of confidentiality and availability. The potential unauthorized access and disclosure of sensitive information, coupled with the encryption of sensitive data and systems, can lead to severe financial and reputational repercussions for affected organizations.
- The plausible responses to the disclosure of their operations and the potential for other threat actors to leverage the disclosed information suggest a dynamic and evolving cyber threat landscape. Organizations should remain vigilant and proactive in anticipating and countering the evolving tactics of ShadowSyndicate and similar threat actors.

Introduction

This report delves into the potentially emerging Ransomware-as-a-Service (RaaS) affiliate ShadowSyndicate to provide actionable intelligence related to the group's extensive infrastructure. The scope of our analysis is centered on Group-IB's blog post, offering a concise yet detailed examination of ShadowSyndicate's infrastructure, assessing the associated risks and impacts, and projecting a short-term outlook. Readers can expect to gain a comprehensive understanding of ShadowSyndicate's infrastructure, affiliations with various ransomware families, and the implications of their activities on organizational security. By acting on the intelligence presented, organizations will be better equipped to enhance their cyber resilience, implement effective mitigation strategies, and anticipate potential threats associated with ShadowSyndicate's evolving tactics. If you have questions or feedback about this intelligence, you can submit them **here**.

Overview & Background

The blog post from Group-IB titled "Dusting for fingerprints: ShadowSyndicate, a new RaaS player?" provides an in-depth overview of the infrastructure leveraged by ShadowSyndicate, a potentially new and notable Ransomware-as-a-Service (RaaS) affiliate. The blog post aims to present preliminary conclusions about the group, offering insights into ShadowSyndicate's infrastructure while leaving avenues for further research into the group's identity open for exploration. Group-IB's analysis focuses on SSH servers, all with the same SSH fingerprint, attributed to ShadowSyndicate, tools and malware identified, SSH server characteristics (like server owners and locations), and the SSH server's links to various ransomware families.

Threat Analysis

In Group-IB's report, they stated that it's "incredibly rare for one Secure Shell (SSH) fingerprint to have such a complex web of connections with a large number of malicious servers." Due to this rarity, Group-IB decided to track the use of this SSH fingerprint to a single threat actor, ShadowSyndicate. Every intelligence report aims to answer one or more questions. For Group-IB's report, they ultimately sought to determine whether ShadowSyndicate is a hoster, DevOps engineer, a bulletproof hosting provider, an initial access broker, or a Ransomware-as-a-Service affiliate. Group-IB's analysis points to ShadowSyndicate working as an affiliate for various Ransomware-as-a-Service (RaaS) operations. However, additional data and analysis are needed to confirm this hypothesis.

Group-IB's detailed research reveals 85 servers have the same Secure Shell (SSH) fingerprint, with at least 52 servers used as a Cobalt Strike C2 framework. With high confidence, Group-IB attributed ShadowSyndicate to Quantum ransomware activity in September 2022, Nokoyawa ransomware activity in October and November 2022, and March 2023, as well as to ALPHV activity in February 2023. Group-IB attributed ShadowSyndicate to Royal, Cactus, and Play ransomware activity with low confidence.

ShadowSyndicate's connection to CL0P is less conclusive. However, Group-IB's research uncovered several potential links between ShadowSyndicate and Cl0p infrastructure. Several IP addresses attributed to Cl0p now use the ShadowSyndicate SSH key, suggesting a possible link to ShadowSyndicate. These servers are now used as C2 infrastructure for Cobalt Strike or Metasploit.

Group-IB also identified evidence that a small set of servers are being used as command and control (C2) servers or connected to Sliver. Sliver is an open-source penetration testing tool developed in the programming language Go. Like Cobalt Strike and Metasploit, Sliver can be used by threat actors in real-life attacks. Additionally, two servers have been linked to IcedID infection chains, leading to Quantum and Nokoyawa ransomware families. Group-IB also potentially identified two servers linked to Matanbuchus, a Malware-as-a-Service (MaaS) loader. Matanbuchus is used to execute .exe payloads and for loading and executing shellcodes and malicious DLL files. Finally, one server was detected as a Meterpreter C2 in March 2023.

Group-IB's research also revealed that 18 entities own SSH servers linked to ShadowSyndicate. The following owners accounted for almost 50% of the total owners.

- Flyservers S.A.
- Channelnet
- Reliable Communications s.r.o.
- DATASOLUTIONS S.A.
- Alviva Holding Limited

The servers' locations are based in 13 different territories, with Panama being their preferred country of choice, followed by Cyprus, Russia, Seychelles, and Costa Rica.

Risk & Impact Assessment

Organizations face a pronounced threat due to the loss of confidentiality and availability caused by ransomware attacks linked to ShadowSyndicate's infrastructure. The likelihood of an incident occurring is elevated due to the group's extensive infrastructure and association with various Ransomware-as-a-Service (RaaS) operations. The primary risks are the unauthorized access and disclosure of sensitive information and the encryption of sensitive data and systems, allowing threat actors to extort victims for financial gain. The material impact of such risks on organizations is substantial. Ransomware operations can lead to significant service disruptions and access to critical information, affecting an organization's mission and functions. The potential unauthorized access and disclosure of sensitive information and encryption of sensitive data and systems can have severe financial repercussions, resulting in the loss of net sales, revenues, or income from continuing operations. Moreover, the reputational damage incurred from such breaches can have long-lasting effects on an organization's standing and customer trust.

Outlook

It's plausible that ShadowSyndicate may respond to the disclosure by adapting and evolving their infrastructure to mitigate the impact of the revealed information. The group might seek to diversify their infrastructure, employ new tools, and explore alternative methods of operation to maintain anonymity and continue their activities. Other threat actors will likely analyze the details to identify gaps in operational security and opportunities, potentially leading to an increase in the adaptation of successful strategies, thereby potentially enhancing their capabilities and posing an elevated threat to organizations. The cyber threat landscape is expected to remain dynamic, with both ShadowSyndicate and other threat actors continually adjusting their approaches in response to the disclosure of malicious operations.

Actions & Recommendations

The Adversary Tactics and Intelligence team has added evaluated observables to our indicator feeds. Additionally, we use this intelligence report to improve our correlation rules and detections and conduct threat hunting. However, due to limitations in log sources received by Deepwatch, not all activity can be monitored.

To withstand, recover, and adapt to ransomware attacks linked to ShadowSyndicate's infrastructure, customers should implement the following actions to improve an organization's cyber resilience:

- Block the known **IOCs** associated with ShadowSyndicate's infrastructure.

Additional threat hunting guidance can be found in Appendix A and general mitigation guidance in Appendix B.

Latest Additions to Data Leak Sites

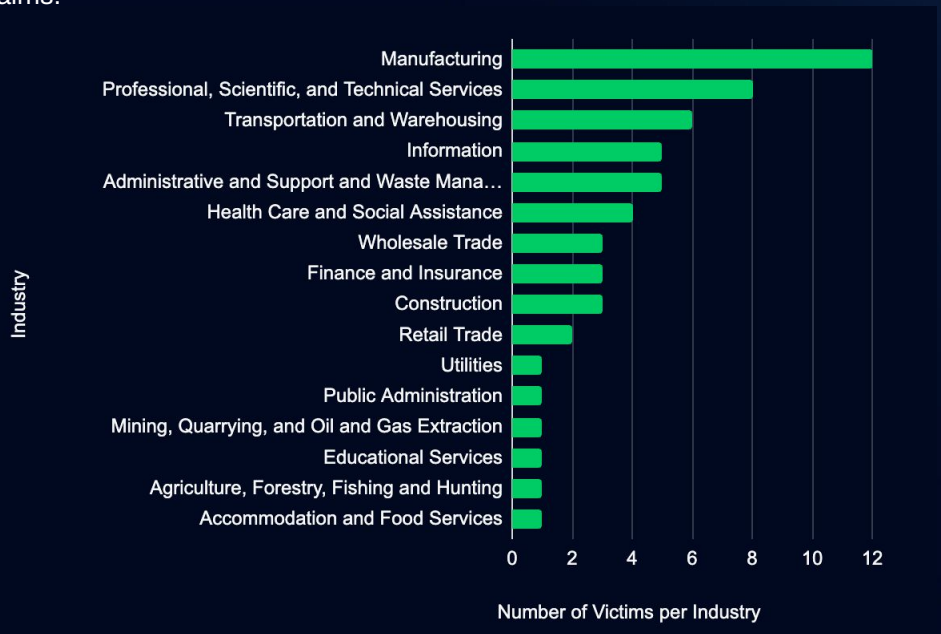
Manufacturing | Professional, Scientific, and Technical Services | Transportation and Warehousing | Information | Administrative and Support and Waste Management and Remediation Services

Introduction

This report analyzes the latest additions to dark web data leak sites, aiming to provide timely and relevant information, enabling decision-makers to anticipate and respond effectively. The report's scope encompasses identifying the victims, the country where they are headquartered, and the industry they operate in. The primary objectives of this report are to provide decision-makers with knowledge of which industries ransomware operators are targeting. If you have questions or feedback about this intelligence, you can submit them **here**.

Analysis

In the past week, monitored data extortion and ransomware threat groups added 57 victims to their leak sites. Of those listed, 30 are based in the US. **Manufacturing was the most popular industry listed,** with 12 victims. This industry is followed by eight in **Professional, Scientific, and Technical Services,** six in **Transportation and Warehousing**, five in **Information**, and **Administrative and Support and Waste Management and Remediation Services**. This information represents victims whom cybercriminals may have successfully compromised but opted not to negotiate or pay a ransom. However, we cannot confirm the validity of the cybercriminals' claims.



Threat Actor	Targeted Organization	Country	Industry
8base	J.T. Cullen Co., Inc.	USA	Manufacturing
	Springer Eubank	USA	Transportation and Warehousing
	The Envelope Works Ltd	UK	Administrative and Support and Waste Management and Remediation Services
Akira	CLX Logistics	USA	Transportation and Warehousing
	Fuji Seal International (US branch)	Japan	Manufacturing
	Glovis America	USA	Transportation and Warehousing
ALPHV	Al Ashram Contracting	United Arab Emirates	Construction
	American University of Antigua	Antigua and Barbuda	Educational Services
	Arail Construction & Industrial Co. Ltd	Saudi Arabia	Construction
	Clarion	USA	Manufacturing
	Angola's Electricity Distribution Company (ENDE)	Angola	Utilities
	MNGI Digestive Health	USA	Health Care and Social Assistance
	Mole Valley Farmers	UK	Retail Trade
	NOVEXCO	Canada	Wholesale Trade
	PainCare	USA	Health Care and Social Assistance
	Phil-Data Business Systems	Philippines	Professional, Scientific, and Technical Services
	Pik Rite	USA	Manufacturing
	Progressive Leasing	USA	Finance and Insurance
	Ruko	Germany	Manufacturing
	SAGAM Groupe	France	Manufacturing
	TAOGLAS	Ireland	Manufacturing
	Unique Engineering	USA	Professional, Scientific, and Technical Services
	Yusen Logistics	Japan	Transportation and Warehousing
Bianlian	F. Hinds	UK	Retail Trade
	Road Safety Inc.	USA	Administrative and Support and Waste Management and Remediation Services
	Smartfren Telecom	Indonesia	Information
BlackByte	Hoteles Xcaret	Mexico	Accommodation and Food Services
CL0P	Bluefin Payment Systems	USA	Information
	Ferguson	USA	Wholesale Trade
Karakurt	Hospice of Huntington	USA	Health Care and Social Assistance
	Yakima Valley Radiology	USA	Health Care and Social Assistance

Threat Actor	Targeted Organization	Country	Industry
Lockbit	Altman Plants	USA	Agriculture, Forestry, Fishing and Hunting
	BauscherHepp, Inc	USA	Manufacturing
	Compass Health Analytics	USA	Information
	Constantine Cannon	USA	Professional, Scientific, and Technical Services
	Hutchinson Whitehead Wealth Management	USA	Finance and Insurance
	Marshall Industrial Technologies Inc.	USA	Administrative and Support and Waste Management and Remediation Services
	Messner Reeves	USA	Professional, Scientific, and Technical Services
	Payroll Select Services	USA	Professional, Scientific, and Technical Services
	Pelmorex Corp	Canada	Information
	Precision Practice Management	USA	Administrative and Support and Waste Management and Remediation Services
Medusa	Auckland Transport	Australia	Transportation and Warehousing
	Chait & Company	USA	Professional, Scientific, and Technical Services
	Franktronics, Inc	USA	Administrative and Support and Waste Management and Remediation Services
	Gulf American Lines	USA	Transportation and Warehousing
	Philippine Health Insurance	Philippines	Finance and Insurance
Play	First Line Ltd.	UK	Wholesale Trade
	PASCHAL-Werk G. Maier GmbH	Germany	Manufacturing
	Rea Magnet Wire	USA	Manufacturing
	RTA Fleet Management	USA	Information
	TSC Group Holdings Limited	USA	Mining, Quarrying, and Oil and Gas Extraction
	Košice Region	Slovakia	Public Administration
Ragnar	COMECA Group	France	Manufacturing
	Groupe Fructa	France	Manufacturing
	Skatax Accounting	UK	Professional, Scientific, and Technical Services
	Stratesys Solutions	Spain	Professional, Scientific, and Technical Services
	Retail House	UK	Construction

CISA Adds 4 CVEs to its Known Exploited Vulnerabilities Catalog

Apple CVE-2023-41991 | Apple CVE-2023-41992 | Apple CVE-2023-41993 | Trend Micro CVE-2023-41179

Source: CISA
Targeted Industries: All

Introduction

This report aims to provide knowledge into known exploited vulnerabilities and provide timely and relevant information, enabling decision-makers to anticipate and respond effectively. The report's scope encompasses identifying the CVEs, vendors, and products added to CISAs Known Exploited Vulnerabilities Catalog. The primary objectives of this report are to provide decision-makers with knowledge of which vulnerabilities CISA has added to the catalog and the recommended mitigation due date. If you have questions or feedback about this intelligence, you can submit them **here**.

Analysis

Within the past week, CISA added four CVEs to the catalog, affecting products from Apple and Trend Micro. Threat actors can exploit these vulnerabilities for code execution, privilege escalation, or bypass signature validation. It is crucial to promptly apply updates or follow vendor instructions to mitigate these vulnerabilities, with CISA recommending mitigative action occur between 12 and 16 October 2023.

Recommendations

ATI recommends mitigative action occur according to the mitigation “Due Date” recommended by CISA.

CVE ID	Vendor/ Project	Product	Description	CISA Due Date
CVE-2023-41991	Apple	Multiple Products	Apple iOS, iPadOS, macOS, and watchOS contain an improper certificate validation vulnerability that can allow a malicious app to bypass signature validation.	10/16/23
CVE-2023-41992	Apple	Multiple Product	Apple iOS, iPadOS, macOS, and watchOS contain an unspecified vulnerability that allows for local privilege escalation.	10/16/23
CVE-2023-41993	Apple	Multiple Products	Apple iOS, iPadOS, macOS, and Safari WebKit contain an unspecified vulnerability that can allow an attacker to execute code when processing web content.	10/16/23
CVE-2023-41179	Trend Micro	Apex One and Worry-Free Business Security	Trend Micro Apex One and Worry-Free Business Security contain an unspecified vulnerability in the third-party anti-virus uninstaller that could allow an attacker to manipulate the module to conduct remote code execution. An attacker must first obtain administrative console access on the target system in order to exploit this vulnerability.	10/12/23

BOLO and Relevant Detections Guidance

Threat Actors Develier Knight Ransomware in Phishing Emails

Source Material: Proofpoint

We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the threat hunting guidance provided below.

Be On the Lookout (BOLO)

- .html email attachments from external/untrusted sources
- Presence of/reference to .knight_l file extension
- Sharp increases in internal network destinations from one host that may indicate internal scanning

Relevant Detections

- dwa_enda_00096: Suspicious Process Chain
- dwa_enda_00053: Suspicious Process Execution on Host
- dwa_neta_00027: Internal Scanning on High-Risk Ports
- dwa_neta_00008: Suspicious Port Scanning Activity
- dwa_inta_00044: Threat Intel Outbound IP Match
- dwa_inta_00046: Threat Intel - Outbound Domain Match

Sandman APT Targets Global Telecoms in August Cyber-Espionage Campaign

Source Material: SentinelOne

We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the threat hunting guidance provided below, and the observables listed **here**.

Be On the Lookout (BOLO)

- AV/EDR alerts for Pass-The-Hash
- Presence of/reference to the following files and directories
    - C:\Windows\System32\ualapi.dll
    - C:\ProgramData\FaxConfig\fax.dat
    - C:\ProgramData\FaxConfig\fax.cache
    - C:\ProgramData\FaxConfig\fax.module
    - C:\ProgramData\FaxConfig\fax.Application
    - C:\ProgramData\FaxLib\

Relevant Detections

- dwa_enda_00096: Suspicious Process Chain
- dwa_enda_00053: Suspicious Process Execution on Host
- dwa_inta_00044: Threat Intel Outbound IP Match
- dwa_inta_00046: Threat Intel - Outbound Domain Match

BOLO and Relevant Detections Guidance

3 APTs Conducted Cyber Espionage Against a Southeast Asian Government, Employing Sophisticated Tools and Techniques

Source Material: Palo Alto Unit 42

- **Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda**
- **Persistent Attempts at Cyberespionage Against Southeast Asian Government Target Have Links to Alloy Taurus**
- **Rare Backdoors Suspected to be Tied to Gelsemium APT Found in Targeted Attack in Southeast Asian Government**

We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the threat hunting guidance provided below, and the observables listed **here**, **here**, and **here**.

Be On the Lookout (BOLO)

- AV/EDR alerts relating to possible DcSync attacks
  - Also visible via "lsadump::dcsync" in the command line as shown in **Figure 5**
- Usage of NBTScan.exe, adfind.exe, or renamed copies matching known hash signatures
- Presence of/reference to the follow files
  - Domain_users_light.txt, Domain_computers_light.txt, or Domain_groups_light.txt
- Cmd.exe spawning "a.logs" as shown in **Figure 2**
- Usage of Impacket loopback UNC paths with "ADMIN$" and "2>&1" as shown in **Figure 3**
- Presence/execution of "Hdump.exe" or "h64.exe" (credential stealing utility)
  - Additional command line arguments used with this tool can be seen in **Figure 4**
- Usage of mimikatz or LaZagne to dump credentials
- Usage of "vssadmin create shadow" to create a volume shadow copy in order to retrieve the Ntds.dit file (see **Figure 6**)
- Creation of "DISMsrv" service, or "TabletPCInputServices," or "TabletInputServices" scheduled tasks
- Addition of "TabletPCInputServices" or "TabletInputServices" registry run keys
- Rare/anomalous usage of "libcurl.dll"
- DLL sideloading alerts relating to "GUP.exe"
- Curl being used to upload files to Dropbox as shown in **Figure 14**
- Creation of "Admin$", "Back$", "infoma$", or "testuser" user accounts
- Usage of fscan or traffic relating to Softether VPN
- Alerts relating to Kerbrute, LsassUnhooker, or GoDumpLsass
- Usage of the arguments "--dc" and "bruteforce" in command line logs as shown in **Figure 6**
- Creation of "updatevmtoolss" scheduled task that runs a .bat file
- Usage of procdump with lsass.exe in the command line as shown **here** **or** the usage of "cmdkey /l" to list stored usernames and passwords
- Usage of the reg commands shown in **Figure 7** to downgrade the NTLM version
- Presence of "J9kzQ2Y0qO" in command line data or anydesk.exe command pipe structure as shown **here**
- C:\Windows\Help in sc commands as shown in **Figure 9**
- Usage of .111 files in command line or presence of the "slave" argument and localhost address as shown in **Figure 10** (Reverse RDP Tunnel)
- Execution of C:\Recovery\I.exe or "regsvr32.exe Loader.any as shown in **Figure 11**
  - Or single character exe files in root of C:\Recovery or .any files being run with regsvr32.exe

BOLO and Relevant Detections Guidance

3 APTs Conducted Cyber Espionage Against a Southeast Asian Government, Employing Sophisticated Tools and Techniques

Source Material: Palo Alto Unit 42

Be On the Lookout (BOLO) Continued

- Usage of Hdoor (chinese backdoor) arguments “-hbs”, “/m”, and “/t” as shown **here**
- Rare .exe files being run in root of C:\upload, rsssocks in command line data with an IP, or usage of AddUser.dll as shown in **Figure 2**

Relevant Detections

- dwa_enda_00096: Suspicious Process Chain
- dwa_enda_00053: Suspicious Process Execution on Host
- dwa_enda_00078: Suspicious Registry Modification
- dwa_enda_00100: Windows Service Install Watchlist Match
- dwa_enda_00013: Suspicious Service Installed
- dwa_auda_00041: Risky Scheduled Task Created or Modified
- dwa_inta_00044: Threat Intel Outbound IP Match
- dwa_inta_00046: Threat Intel - Outbound Domain Match

APT29 Phishing Campaigns Evolve Malware Delivery Methods Between March and July

Source Material: Mandiant

We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the threat hunting guidance provided below, and the observables listed **here**.

Be On the Lookout (BOLO)

- .html email attachments from external sources
- Alerts for YARA rules shown in Detection section

Relevant Detections

- dwa_enda_00096: Suspicious Process Chain
- dwa_enda_00053: Suspicious Process Execution on Host
- dwa_inta_00044: Threat Intel Outbound IP Match
- dwa_inta_00046: Threat Intel - Outbound Domain Match

BOLO and Relevant Detections Guidance

SSH Fingerprint Leads to the Identification of Extensive Infrastructure Used in Ransomware Attacks

Source Material: Group-IB

We recommend that all customers retrospectively hunt for malicious activity, which will likely indicate compromise, using the threat hunting guidance provided below, and the observables listed **here**.

Be On the Lookout (BOLO)

- Traffic to hosting providers shown in the article that have no business use

Relevant Detections

- dwa_inta_00044: Threat Intel Outbound IP Match
- dwa_inta_00046: Threat Intel - Outbound Domain Match

General Mitigation Guidance

Perimeter (Internet Edge)

- Regularly scan systems for vulnerabilities and patch systems as soon as possible. Prioritization should be placed on those systems that are internet-exposed with a focus on known exploited vulnerabilities like those featured in CISA's **Known Exploited Vulnerabilities Catalog**.
- Assets on the public internet expose exploitable services, such as RDP. Where these services must be exposed, appropriate compensating controls should be implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols should be disabled on internet-facing assets.
- Integrating a secure email gateway as part of the organizational technology stack can significantly reduce the risk of phishing emails arriving in end-user's inboxes.
- Prevent users from launching embedded files in Microsoft OneNote files, like .hta, .bat, .com, .cmd, .exe, .js, .jse, ps1, .scr, .vbs, and .wsf, through Group Policy settings by using the "Embedded Files Blocked Extensions" template available from Microsoft **here**.

Accounts

- Integrating **phishing-resistant multi-factor authentication** (MFA) as part of the organizational policy can significantly reduce the risk of a cybercriminal gaining control of valid credentials for additional tactics such as initial access, lateral movement, and collecting information. Organizations can also use phishing-resistant MFA to restrict access to cloud resources and APIs.
- An enforced organization-wide policy and process that requires changing default passwords for all hardware, software, and firmware before being deployed on any network. Organizations have a system-enforced policy requiring a minimum password length of 15 or more characters for all password-protected IT assets, and all OT assets are technically possible.
- No user accounts have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g. for business email, web browsing, etc.)—Disable remote PowerShell execution for non-administrative users where possible.

General Mitigation Guidance

Network & Host

- Determine if certain websites or attachment types (such as Telegram, Discord, .lnk, and .iso.) are necessary for business operations and block access if security analysts cannot monitor the activity well or if it poses a significant risk.
- Prevent users from opening scripts, like .hta, .jse, .js, .vbs, and .wsf, through Group Policy settings and prevent the execution of script interpreters (MSHTA.exe and WSCRIPT.exe) through Group Policy or Application Control.
- A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.
- Employ an anti-virus or EDR solution that can automatically quarantine suspicious files.
- Security applications that look for behavior used during exploitation can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.
- Security applications that look for behavior used during exploitation can be used to mitigate some exploitation behavior. Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring.

Disaster Recovery

- Customers are highly encouraged to establish an incident response plan and frequently test it. These plans should include the calculation for the amount of time it would take to restore from backups and the overall cost. Customers should restore data from backups when testing their plans.
- Customers with encrypted off-site backups should ensure that the digital decryption key or the applications needed to restore are not stored on a local file-sharing network and access is tightly controlled.

deepwatch™

Share Your Thoughts

Please take a moment to share your thoughts and ideas by clicking the button below. You can read how Deepwatch approaches cyber threat intelligence **here**.

Your feedback submission can be anonymous. However, we read each submission carefully, and your feedback is valuable to the Deepwatch Adversary Tactics and Intelligence team and enables Deepwatch to make quick and continuous improvements to these products.

Share Your Thoughts