RELIAQUEST®

The Infostealer Pipeline: How Russian Market Fuels **Credential-Based Attacks**

2025

Executive Summary

Russian Market Reigns Supreme

The scale of Russian Market information-stealing (infostealer) malware logs is staggering. In 2024 alone, ReliaQuest GreyMatter Digital Risk Protection (GreyMatter DRP) raised over 136,000 alerts for customer domains listed on the platform. Russian Market's popularity stems from its simplicity, convenience, and longevity—and with infostealer logs priced as low as $2, it remains a favorite among cybercriminals. However, 85% of the logs we analyzed also appeared in other sources, indicating that Russian Market's content is largely recycled. Despite this lack of exclusivity, its popularity continues to thrive.

Lumma Dominates Infostealers

"Lumma" (aka LummaC2) emerged as the dominant infostealer, accounting for nearly 92% of Russian Market credential log alerts in Q4 2024. Our analysis shows that cybercriminals favor advanced, commercial infostealer tools, which likely drove Lumma's success. In addition, its use of fake CAPTCHA pages for distribution likely further propelled its meteoric rise. But, since Lumma's takedown in May 2025, "Acreed" is the likely next big infostealer threat, surpassing many other established stealers in Q1 2025.

Infostealer Logs Provide Attacker Insights

Infostealers frequently exploit writable directories like Temp, obfuscate filenames, and use living-off-the-land (LotL) techniques to execute payloads, making detection more difficult for defenders. These tactics allow attackers to prolong their presence in compromised systems and steal more sensitive data. Common persistence techniques include registry edits, scheduled tasks, startup folder implants, or abusing legitimate system processes to disguise malicious activity.

Cloud Adoption Broadens the Attack Surface

As more and more businesses adopt cloud services, cybercriminals are drawn to the vast amounts of sensitive data these platforms host. Credentials tied to cloud accounts, particularly software-as-a-service (SaaS) and single sign-on (SSO) credentials, have become key targets. In our analysis, SaaS credentials appeared in 61% of logs and SSO credentials were present in 77%. Compromised cloud accounts afford attackers access to critical systems and present the perfect opportunity to steal sensitive data.

Attackers Set Sights on Password Managers and Mobile Devices

Password managers are expected to become a key focus for attackers in the medium term. The complexity of modern passwords has made password managers indispensable for managing vast credential inventories, turning them into highly lucrative targets. Meanwhile, attackers will highly likely intensify their focus on mobile devices for credential theft. As companies increasingly allow employees to use personal mobile devices to access work systems, attackers will exploit the dual-use nature of these devices to identify and exploit security gaps.

Table of Contents

Crisis of Compromise: The Growing Industry of Stolen Credentials 1

The Dark Economy of Russian Market 3

- Breaking Down Russian Market's Offerings 4
- Success Despite the All-Important Customer Ratings? 5

Infostealers: The Source of Stolen Credentials 6

- Case Study: Vidar 7
- Case Study: Lumma 8
- Countering the Threat with ReliaQuest 9

How Infostealers Compromise Machines: What the Logs Tell Us 11

- 1. Writable Directories Used to Stage and Execute Malware Payloads 11
- 2. Obfuscated Filenames and Compressed Archives 12
- 3. Malware Payloads Hidden in Rarely Monitored Directories 12
- 4. LotL Techniques Turn Trusted Tools into Attack Vectors 13
- 5. Infostealer Malware Persistence Techniques 13
- Countering the Threat with ReliaQuest 14

Cloud Credentials in Cybercriminal Markets 16

- SSO or SaaS Credentials Found in Two-Thirds of Russian Market Logs 16
- PSTS Hit Hardest by SaaS Credential Theft as Education Struggles with SSO 17
- Countering the Threat with ReliaQuest 19

ReliaQuest Reviews: How Does Russian Market Measure Up? 21

- Countering the Threat with ReliaQuest 23

Key Takeaways and What's Next for Infostealers? 25

- The Next Big Infostealer: Acreed 25
- The Growing Risk to Password Managers 26
- Malware Moves to Mobile Devices 26

Endnotes 27

About ReliaQuest 28

Crisis of Compromise: The Growing Industry of Stolen Credentials

Credentials compromised via information-stealing (infostealer) malware are one of today's most pressing cybersecurity threats.

Between January and December 2024 (the reporting period), ReliaQuest's GreyMatter Digital Risk Protection (GreyMatter DRP) service raised over

136,000 alerts

related to potential stolen credentials on Russian Market, indicating that threat actors may already have access to affected domains.

This trend has continued into 2025, with over 50,000 credential theft alerts issued as of May 2025, highlighting the critical need for organizations to stay alert to this tactic.

For victims, the use of stolen credentials to gain initial access can lead to catastrophic consequences.

Once attackers establish a foothold, they can escalate their operations—infiltrating networks, stealing sensitive data, disrupting services, and deploying ransomware.

The scale of this threat is amplified by a growing ecosystem that enables the exploitation of stolen credentials. At the center of this ecosystem are platforms like Russian Market, a notorious Automated Vending Cart (AVC) site launched in early 2019 where infostealer logs are bought and sold, sometimes for as little as $2.

Information-stealing (or "infostealer") malware

is designed to quietly harvest sensitive data from infected systems. These malicious tools target user credentials, browser cookies, credit card data, cryptocurrency wallets, and more.

They typically spread through spam emails, compromised websites, and malicious ads. The stolen data is presented in a text file "log," which buyers can easily download.

The risk of the Russian Market-linked credential threat isn't limited to specific industries or business types or size—any organization with an online presence is a potential target. A notable example is the "Hellcat" ransomware attack on telecommunications giant Telefónica, where the threat actor used an infostealer to obtain credentials and gain initial access.

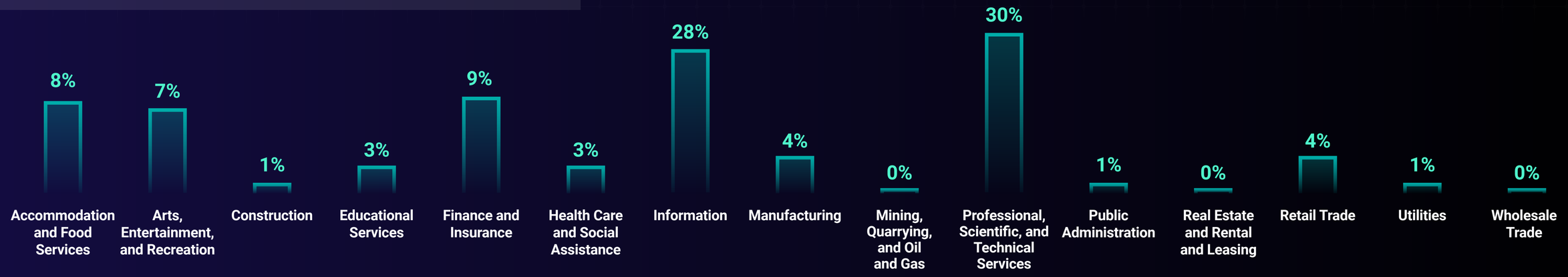
During the reporting period, GreyMatter DRP alerts revealed that every industry faced exposure to this threat. However, the professional, scientific, and technical services (PSTS) and information sectors were disproportionately impacted, accounting for 60% of all alerts.

Here's why

High levels of digital engagement: Employees in these fields rely heavily on the internet for research and daily tasks, often visiting a diverse range of websites. This heightened web activity increases their exposure to drive-by downloads—one of the primary methods used to infect machines with infostealer malware.

Complex supply chains: These industries often operate within intricate supply chains, so employees regularly receive emails from a wide variety of contacts, including unfamiliar senders. This makes them less likely to question unusual emails and increases the risk of falling for spearphishing attempts—a major source of infostealer infections.

Figure 1: ReliaQuest customer alerts stemming from Russian Market, 2024



Cybercriminal marketplaces like Russian Market make credential-based attacks accessible to even low-skilled attackers, fueling waves of breaches across industries. The convenience and affordability of these marketplaces allow attackers to forgo the complexities of developing their own malware and instead focus on exploiting purchased credentials—a minimal investment with potentially devastating results.

The ReliaQuest Threat Research team has spent years studying Russian Market, analyzing how the site functions and helping organizations navigate the risks posed by sensitive domains appearing in its logs. To better understand how Russian Market works and its impact on the credential theft ecosystem, we embarked on a deeper investigation into the forces driving its operations.

This report investigates four critical factors across the credential compromise cycle that we believe contribute to Russian Market's success. Specifically, we'll examine:

The infostealers favored by cybercriminals for attacks.

Whether specific infrastructures, like cloud accounts, are targeted.

How the infostealers represented on Russian Market make their way onto machines in the first place.

The exclusivity of stolen logs and whether they're sold elsewhere.

These insights are crucial for enterprises, where the stakes couldn't be higher.

Preventing credential theft before it occurs is far more effective than managing the fallout once stolen credentials are in circulation. By understanding how infostealers work and the infrastructure that enables their exploitation, businesses can implement proactive strategies to safeguard their systems and reduce their vulnerability to this growing threat.

This report provides organizations with the knowledge needed to take action—read on to explore the hidden mechanics of Russian Market and learn how to stay ahead of cybercriminals.

The Dark Economy of Russian Market

Russian Market has emerged as a leading force in the stolen credential trade.

After gaining traction through extensive promotion on cybercriminal forums, it gained widespread popularity by 2022.

Since then, it has outlasted Genesis Market, which was taken down in 2023, and beat out new competitors like Exodus Market, solidifying its position as a key platform in the cybercriminal ecosystem.

What sets Russian Market apart from its competitors is its simplicity, convenience, and longevity. It's like the Amazon for cybercriminals, offering a streamlined, one-click purchase experience and fast, hassle-free transactions. Signing up is straightforward—users only need an email address and password—making the platform highly accessible to those looking to tap into its offerings. To deter potential scams, the site carefully advertises its active domains on the homepage, further enhancing its appeal.

In a cybercriminal ecosystem where reputation is everything and regulation is nonexistent, Russian Market's perceived reliability and longevity have been critical to its success. Unlike Telegram channels, which now make up its primary competition for infostealer logs, Russian Market offers buyers the ability to filter logs based on their specific needs. This level of precision and convenience gives it a significant edge over its competitors.

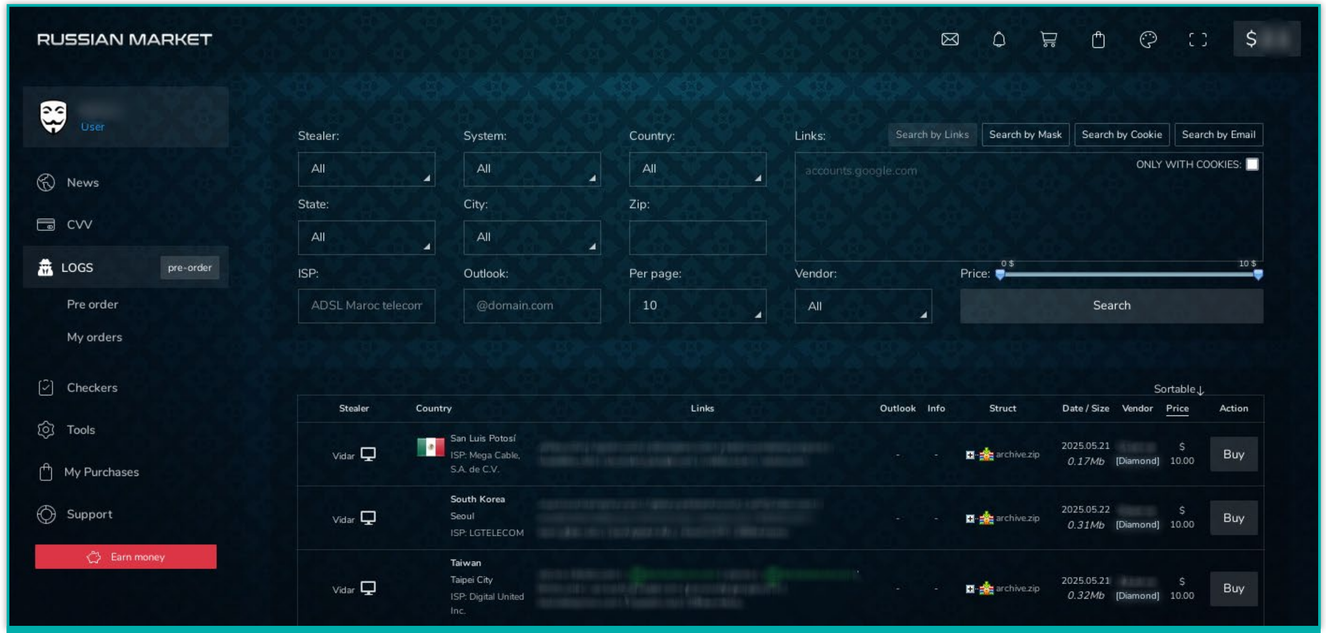


Figure 2: Russian Market "LOGS" page

The sheer volume of logs available on Russian Market is staggering. Although logs are constantly sold, removed, and replenished, it was estimated that by February 2023, the marketplace had over five million logs for sale. Since then, uploads have continued to increase, with each log containing tens or even hundreds of individual credentials. This puts the total number of credentials available for purchase easily into the hundreds of millions, if not billions.

Breaking Down Russian Market's Offerings

Russian Market is divided into various subsections, each advertising different products:

CVV For buying and selling stolen card verification values (CVVs), the security codes printed on credit and debit cards.

LOGS For buying and selling stolen credentials, cookies, and other information obtained through infostealer malware.

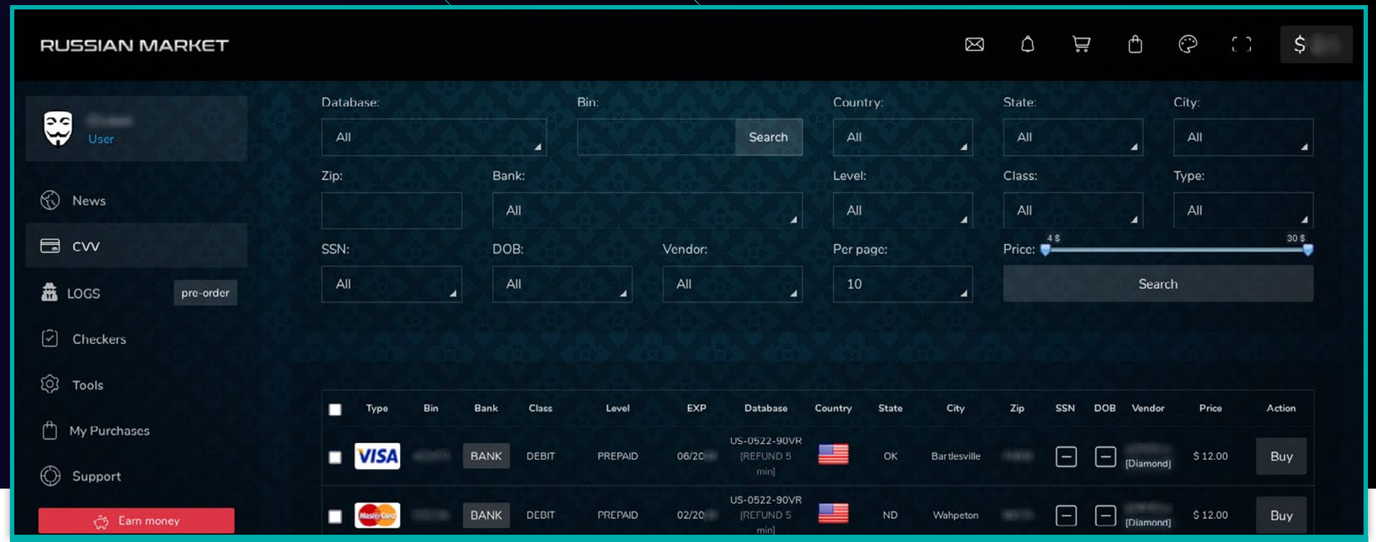


Figure 3: Russian Market "CVV" page

At its core, Russian Market thrives on selling stolen credentials.

When choosing which credential logs to buy, threat actors can filter by country, city, system, malware, internet service providers (ISPs), and domains, often zeroing in on internal domains to infiltrate organizational networks. With prices ranging from $2 to $10 per log, even amateur attackers with limited resources can wreak havoc. It's a no-brainer for attackers—why go to the effort of running infostealer campaigns when someone else has already done the dirty work? Small investments, big consequences.

Once logs are purchased on Russian Market, the buyer downloads a zip file containing several folders depending on the infostealer used. The folders are typically:

All Passwords: Contains all credentials found within the compromised machine.

Brute: Contains passwords, likely used to brute-force more accounts and domains.

Processes: Contains all the processes running on the compromised machine.

Software: Contains a list of all the software captured on the compromised machine.

System: Contains the version of the infostealer used, as well as system details about the compromised machine such as antivirus, graphics processing unit (GPU), and machine name.

While the passwords folder is undoubtedly the centerpiece for most buyers, as it directly enables account compromise, the other folders also hold valuable information.

In this report, we'll look into their significance in more detail.

Success Despite the All-Important Customer Ratings?

Like many criminal platforms, Russian Market has drawn its share of criticism from users. For example, on the popular carding site crdpro, complaints have surfaced with comments such as, “Russianmarket too don’t ever use that site” and “Russianmarket not good for me.” Even prominent figures in the cybercriminal world have weighed in. In September 2024, a well-known initial access broker (IAB) operating under the alias “SGL” (formerly “Sganarelle”) shared their frustrations on the Russian-language cybercriminal forum XSS, warning:

> I can’t recommend you anything, but I can say [tell] you for sure: don’t lose your money on Russian Market. It’s full of public logs, which they sell as private.

Despite these complaints, Russian Market continues to dominate its niche. It’s hardly flawless—cybercriminal spaces often face accusations of being scams, honeypots, or both—but the competition is seen as even less reliable. This is summed up by a user on the cybercriminal forum Exploit, who criticized Russian Market for selling the same logs “several times” but still referred to themselves as a “topbuyer” on the platform. The same user dismissed other marketplaces like 2easy for having a limited selection and Genesis for being too expensive.

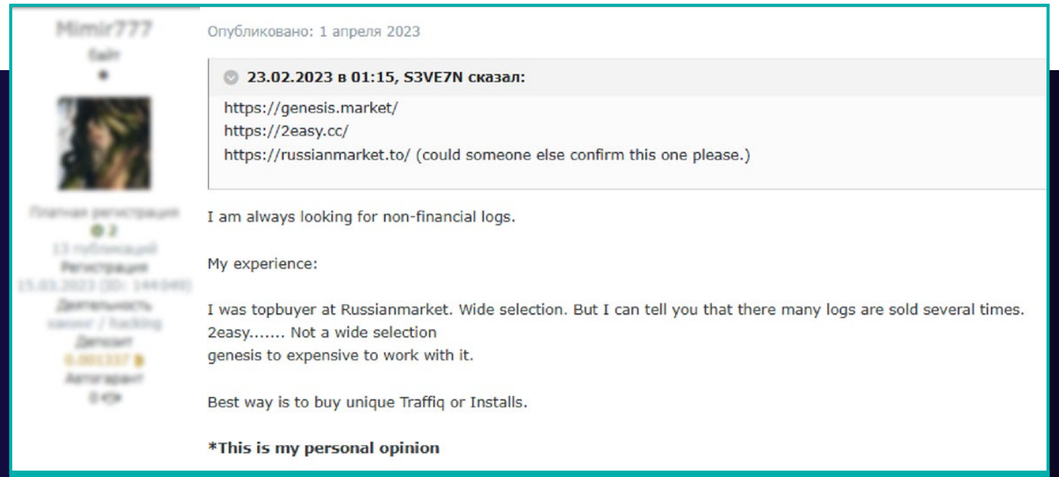


Figure 4: User of cybercriminal forum Exploit praises the selection on Russian Market, but claims that logs are sold multiple times

This dynamic explains why Russian Market remains the leader:

It’s simply the best of a bad bunch. Despite its flaws, the platform offers a broader selection of logs, smoother transactions, and better pricing than its competitors, making it the go-to choice for many threat actors.

However, Russian Market’s prominence also makes it a more likely target for law enforcement. If the platform were taken down, cybercriminals would likely have to choose an alternative marketplace. But this could inadvertently increase risks for businesses, as stolen credentials might be distributed more widely across platforms.

For defenders, the accessibility of Russian Market blows open the threat landscape, empowering everyone from seasoned hackers to low-skilled opportunists to buy and weaponize stolen credentials. For businesses, this presents a serious challenge: even attackers with minimal technical expertise or resources can use stolen data. Instead of developing their own malware campaigns, they can simply purchase ready-to-use credential logs for a few dollars, enabling them to launch phishing scams, commit fraud, infiltrate networks, or manipulate financial transactions with ease. This accessibility drastically increases the volume and frequency of attacks, as even amateurs can exploit vulnerabilities, disrupt operations, and carry out a variety of damaging attacks.

Infostealers: The Source of Stolen Credentials

Every credential theft attack begins with a critical decision: selecting the infostealer.

This choice lays the foundation for the entire operation, shaping its effectiveness and scope. We set out to examine whether the popularity of specific infostealers had fluctuated over time and pinpoint the factors that drove these shifts—whether through technical innovation, law enforcement intervention, or changes in distribution tactics.

Examining trends in infostealer popularity is essential for understanding which tools dominate the credential theft landscape and how attackers evolve their tools and strategies.

Our analysis of 1.6 million-plus posts on Russian Market dating back to 2022 reveals clear trends in the rise and fall of specific infostealers. In this section, we'll also share case studies that illustrate how we've tackled infections involving these infostealers in real-world customer incidents.

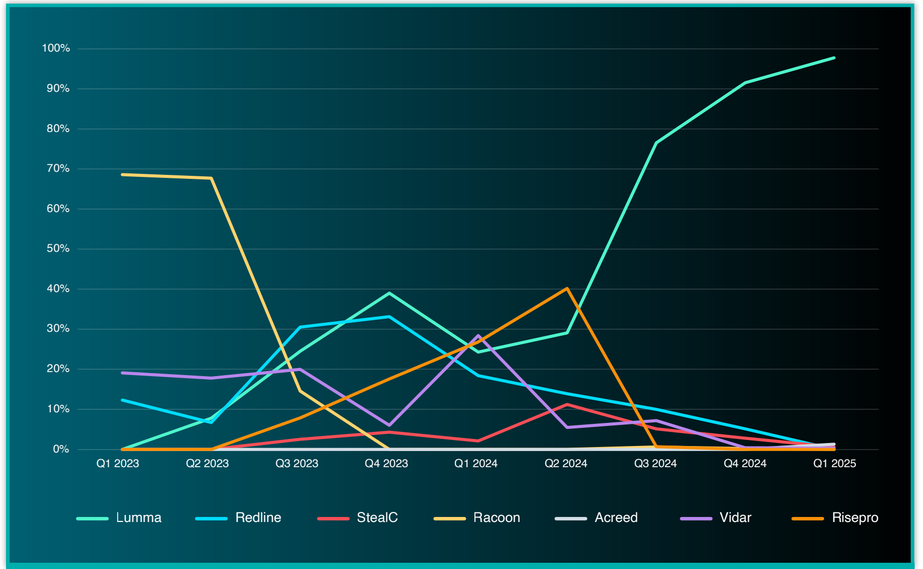


Figure 5: Percentage of Russian Market alerts attributed to different infostealers by quarter

The infostealer market shifts frequently, as the most dangerous cybercriminal services are consistently the target of law enforcement operations.

This leads to takedowns of established groups and paves the way for new variants to emerge and quickly gain traction.

Crunching the numbers revealed two major stories:

Raccoon Stealer's Demise: In March 2022, the operator of "Raccoon Stealer" was arrested, and its digital infrastructure was dismantled by law enforcement. Although a new version was released in August 2023, the number of alerts we observed continued to decrease, suggesting that criminals shifted to other infostealers. However, in the aftermath of Raccoon's downfall, no single infostealer emerged as a dominant replacement.

Lumma Stealer's Rise: Our findings show that cybercriminal forum users prefer infostealers with advanced, commercial operations, like Lumma. In Q3 2024, Lumma began distribution via fake CAPTCHA pages, which likely helped catapult its market domination.

Case Study: Vidar

ReliaQuest GreyMatter is built to rapidly detect and respond to emerging threats, including infostealer incidents, by leveraging advanced detection tools and processes to combat credential theft. In February 2025, after identifying credential listings on Russian Market linked to a customer, ReliaQuest initiated a comprehensive hunt to uncover potential “Vidar” infostealer activity and provided recommendations to strengthen defenses.

Vidar infostealer typically propagates through phishing and social engineering techniques, tricking victims into executing malicious PowerShell commands. The malware operates by convincing the user to run a malicious file that appears legitimate. Once installed, the malware communicates with malicious domains to exfiltrate credential data, enabling attackers to sell it on underground forums.

Actions Taken

During our four-month hunt to uncover Vidar activity and assess potential compromises tied to the malware, we deployed the following detections:

Suspicious Mshta Command Execution: Configured to detect abnormal command lines linked to Vidar’s initial payload delivery. This detection was active during both the initial 30-day hunt and extended four-month investigation.

Encoded PowerShell Execution: Focused on identifying obfuscated PowerShell commands used by the malware to load malicious binaries and maintain persistence.

Anomalous Network Connections: Monitored for suspicious network connections targeting newly created domains and social media platforms including Telegram, Mastodon, and Steam.

Key Findings

Hunt Results: Our investigation into suspicious Mshta commands, suspicious PowerShell executions, and LotL techniques did not return any evidence of Vidar payloads or indicators of compromise (IOCs). Detection rules for malicious Mshta commands and encoded PowerShell activity didn’t fire throughout the investigation, which reinforces that Vidar wasn’t present.

Marketplace Listings: Credential logs containing potential customer credential data and tied to Lumma and Vidar compromises were found on Russian Market. These listings spanned from September 2023 to February 2025. However, no active malware activity was found within the customer’s environment. It’s realistically possible that the credentials listed were recycled and not linked to recent compromises.

Case Study: Lumma

In January 2025, ReliaQuest responded to a critical alert signaling suspicious activity within a customer's environment. The alert flagged a high-severity malware signature linked to the execution of a suspicious PowerShell command, which had downloaded a payload identified as Lumma malware. Evidence of malicious domains and activity consistent with Lumma's known behavior prompted ReliaQuest to launch a thorough investigation aimed at confirming the malware's presence and mitigating its potential impact.

Lumma is an infostealer malware known for targeting browser-stored credentials, cryptocurrency wallets, and other sensitive data. It typically propagates through phishing campaigns and obfuscated scripts, using compromised domains and PowerShell commands to execute its payloads. Once active, Lumma communicates with malicious infrastructure to exfiltrate stolen data, which is often sold on underground marketplaces.

Actions Taken

Our investigation focused on threat detection, containment, and the identification of IOCs tied to Lumma activity. The following actions were implemented:

Host Isolation: The compromised host was isolated using SentinelOne to prevent further malware execution or lateral movement within the environment.

Credential Rotation: Passwords were reset, and all active sessions for the affected user were terminated to mitigate potential abuse of stolen credentials.

IOC Blocking: Malicious domains ("ferrydero[.]com," "iplogger[.]co," and "rolyreno[.]com") were added to the blocklist, along with the hash of the downloaded payload ("gojeks[.]exe"), to prevent further communication or execution.

Key Findings

Our investigation of the compromised network host confirmed that the Lumma infostealer was successfully downloaded and executed. However, due to existing controls, outbound connections to the C2 infrastructure were successfully blocked. Logs verified that no outbound communication occurred between the compromised host and the Lumma-related infrastructure, and there was no evidence of data exfiltration.

Given the constantly evolving nature of infostealers, the top infostealer today is likely not tomorrow's problem.

As such, it's important to have broad detections in place that identify the typical initial access patterns used by infostealers—phishing emails, fake CAPTCHA pages, drive-by downloads—rather than focusing on the tactics, techniques, and procedures (TTPs) of individual variants.

RELIAQUEST GREYMATTER®

Countering the Threat with ReliaQuest

It's far more effective to address infostealer activity at its root—when infostealers are infiltrating your environment—than waiting for the consequences of credential abuse to play out. By stopping infostealers early, organizations can significantly reduce the downstream risks associated with stolen credentials.

ReliaQuest has developed specific detections and GreyMatter Automated Response Playbooks designed to target infostealer activity at multiple stages of the attack lifecycle.

The detections focus on identifying suspicious behaviour associated with credential theft, while the Automated Response Playbooks enable rapid responses to mitigate risks.

By combining the detections with the Playbooks, organizations can reduce their mean time to contain (MTTC) threats from hours to just minutes.

Recommended Detection Rules

Suspicious Process Launching Shell: Identifies unexpected shell launches triggered by compromised processes, often associated with Lumma activity. The malware exploits vulnerabilities by injecting malicious code into Office documents or using Windows utilities to execute shell commands. These methods enable credential theft and system compromise, allowing attackers to exfiltrate sensitive data or disrupt operations.

Malware Not Cleaned: Detects instances where infostealer malware, such as Lumma and Vidar, avoids removal due to factors like low antivirus detection confidence or system-level obstacles (e.g., missing files or insufficient permissions). These situations allow attackers to retain access and exfiltrate credentials for further misuse, heightening the risk of account compromise or lateral movement.

Suspicious PowerShell Command Execution: Detects fileless attacks in which infostealers like Lumma and Vidar execute malicious scripts directly via PowerShell, bypassing traditional file-based detection mechanisms. This technique allows the malware to steal credentials, load payloads into memory, and maintain persistence, enabling attackers to exploit compromised accounts and systems while evading detection.

RELIAQUEST GREYMATTER®

Recommended Automated Response Playbooks

Reset Password: Automatically resets the password of a compromised account after detecting suspicious activity (e.g., failed login attempts or unusual logins). This prevents attackers from accessing the account and launching further attacks.

Terminate Session: Ends all active sessions of a compromised account, forcing attackers to reauthenticate. When combined with Reset Password, it locks attackers out and prevents reuse of stolen credentials.

Block IOC: Adds IOCs to a blocklist based on suspicious activity (e.g., remote logins from risky locations). Blocking these IOCs mitigates threats and prevents further interaction with known malicious entities.

Fortify Your Security Posture

To mitigate risks associated with infostealers like Vidar and Lumma, we recommend the following steps:

Enforce strict network policies or Group Policy Objects (GPOs) to prevent the storage of credentials in web browsers, as infostealers often target browser-stored data for exfiltration.

Reduce session durations to limit the risk of session hijacking and force users to reauthenticate more frequently, minimizing the attack window for compromised cookies.

Implement certificate-based authentication to strengthen access controls and reduce susceptibility to phishing attacks while protecting sensitive accounts.

How Infostealers Compromise Machines: What the Logs Tell Us

Analyzing Russian Market logs gives us direct visibility into how infostealers operate, providing valuable insights into their techniques straight at the source.

By studying these logs, ReliaQuest equips organizations with a deeper understanding of how infostealer infections occur and the specific attack paths used to steal credentials and compromise systems.

These logs reveal critical details such as the targeted operating systems, file paths exploited by malware, and the evasive techniques attackers use to avoid detection. Armed with this intelligence, organizations can take informed, proactive steps to neutralize these threats early in the attack lifecycle.

Drawing on the techniques observed in Russian Market logs, we identified five primary attack paths and developed actionable recommendations to help organizations defend against infostealer threats.

1. Writable Directories Used to Stage and Execute Malware Payloads

What? The Temp directory is a frequent target for malware due to its writable permissions across user accounts, eliminating the need for admin access. AutoIt scripts appeared heavily in the samples we investigated, indicating that the malware actively uses automation to stage operations and execute payloads.

How? Files with randomly generated names like “RelishKitchen.a3x” and subdirectories like “000066001/stealc_default2.exe” suggest that the malware creates temporary working folders to stage operations before executing or exfiltrating stolen data. The diversity of file types found in the Temp directory—including .exe, .au3, .a3x, and .pif—indicates a degree of flexibility in execution methods, enabling it to run compiled scripts, standalone executables, and shortcut files.

Why? Malware authors favor AutoIt for its obfuscation capabilities, while temporary staging folders complicate detection and analysis for defenders. This tactic means that businesses may suffer multiple credential thefts before identifying a compromise, paving the way for further attacks.

Fortify Your Security Posture

- **Monitor the Temp Directory:** Track suspicious file creation, execution, and deletion in the Temp directory, paying special attention to unusual file extensions such as .au3, .a3x, and .pif.
- **Restrict Write Permissions:** Limit write access for non-essential processes or untrusted applications to prevent malware from staging payloads.
- **Implement Behavior-Based Detections:** Deploy threat detection solutions to identify abnormal patterns in the Temp directory, such as frequent creation of subdirectories or execution of AutoIt scripts.

2. Obfuscated Filenames and Compressed Archives

What? Infostealers use obfuscated filenames and compressed archives to evade detection and complicate analysis.

How? Filenames include special characters, making them difficult for traditional signature-based antivirus tools to flag, e.g. @!#newest_software_7878_p@ssw0rd_/setup.exe and Rar/setup.exe*and*RarEXb4772.40717/Setup.exe. Malware is often bundled inside compressed archives, disguising itself as legitimate software to lure victims into executing the payload.

Why? This is another method by which attackers can prolong their presence in a compromised system, increasing the risks for businesses.

Fortify Your Security Posture

- **Detect Obfuscated Filenames:** Use heuristic-based detection systems to flag files with suspicious naming conventions, including randomness or special characters.
- **Archive Scanning:** Deploy automated tools to scan compressed archives (.rar, .zip) for embedded executables before allowing users to open them. Flag archives containing executables in unusual directories or with suspicious naming conventions.
- **Restrict Execution from Downloads Folder:** Prevent files from being executed directly from download directories to reduce the risk of accidental execution of compressed malware payloads.

3. Malware Payloads Hidden in Rarely Monitored Directories

What? Infostealers use unusual directories to hide malware payloads, increasing their chances of evading detection.

How? For example, we uncovered the executable MavInject32.exe in a directory typically reserved for font files, C:/Windows/Fonts/OFFSYMB.TTF/16.0.15128.20178/. Mavinject32.exe is a legitimate Windows utility used to inject code into other processes. Attackers use this tool to inject malicious code into running processes. Additionally, we have seen these binaries placed in folders such as “C:/Windows/Fonts/” to bypass static detections.

Why? Its unusual location means it’s less likely to be detected, as security software is typically trained to focus on common executable locations, such as Program Files or SysWOW64. This tactic gives attackers more time to identify and steal credentials for valuable accounts, including domain admins, before defenders can identify the threat.

Fortify Your Security Posture

- **Monitor Non-Standard Directories:** Implement file system monitoring to track the creation and modification of executables in non-standard directories such as C:/Windows/Fonts.
- **Restrict Write Access to Non-Standard Directories:** Prevent non-admin processes from writing to system directories that are not typically associated with application executables.
- **Investigate Process Injections:** Analyze processes for suspicious injection behaviors that could indicate attempts to bypass security controls or execute malicious payloads, focusing on the use of LOLBAS tools.

4. LotL Techniques Turn Trusted Tools into Attack Vectors

What? Infostealers employ living-off-the-land (LotL) techniques to execute payloads by exploiting legitimate tools already present on the system.

How? For example, we identified files such as MSBuild.exe and NETFXSBS10.exe within the .NET Framework directory, indicating that malware is leveraging pre-installed .NET utilities for execution. MSBuild (Microsoft Build Engine) is commonly abused to load malicious scripts or execute inline code, minimizing the need for standalone executables and enhancing stealth.

Why? LotL techniques enable infostealers to seamlessly blend malicious activity with normal system processes, making detection significantly more difficult and increasing the risk of a full-scale attack for businesses.

Fortify Your Security Posture

- **Monitor .NET Utilities:** Track unusual usage of .NET Framework executables like MSBuild.exe, flagging attempts to load non-standard or external scripts for compilation or execution.
- **Restrict MSBuild Usage:** Limit the use of MSBuild and other .NET utilities to trusted applications and developers. Block their execution from untrusted processes or users.
- **Behavioral Analysis:** Implement solutions to detect LotL attacks by monitoring legitimate tools for abnormal behavior like accessing external servers or executing non-standard scripts.

5. Infostealer Malware Persistence Techniques

What? Infostealer malware often employs persistence mechanisms to maintain access on compromised systems, ensuring it can survive reboots or user interventions. Common persistence techniques include registry edits, scheduled tasks, startup folder implants, or abusing legitimate system processes to disguise malicious activity.

How? The persistence mechanisms we identified could serve multiple purposes:

- Creating registry keys or scheduled tasks to automatically execute malicious payloads upon system startup.
- Leveraging legitimate system processes or utilities to camouflage malicious activity, reducing the likelihood of detection.
- Implanting files in startup directories to ensure malware execution during every boot cycle.

Why? These activities pose a significant risk to organizations because they enable the malware to operate undetected for longer periods, increasing the likelihood of data theft, unauthorized system access, or further compromise of the network.

Fortify Your Security Posture

- **Monitor System Changes:** Deploy solutions to detect suspicious modifications to registry keys, scheduled tasks, and startup directories.
- **Investigate Persistence Indicators:** Use forensic tools to analyze changes in system processes or files that suggest persistence mechanisms are in place.
- **Restrict Access to Critical System Areas:** Enforce strict access controls to prevent unauthorized modifications to sensitive system components.

By employing these tactics to evade detection for as long as possible, cybercriminals can use infostealers to harvest a greater volume of credentials, especially those tied to high-value accounts with administrative privileges.

These accounts can then be exploited in future attacks to steal sensitive data like intellectual property, financial records, and customer information. For businesses, the consequences of a leak are severe: reputational damage, regulatory fines, and significant operational disruption.

RELIAQUEST GREYMATTER®

Countering the Threat with ReliaQuest

When an infostealer successfully compromises a device in your network, swift action to find the compromise as quickly as possible is critical to minimize dwell time and prevent the escalation of a full-blown attack. However, as outlined above, these tactics are specifically designed to help infostealer malware evade detection for as long as possible. To address this, a multi-pronged approach is essential.

ReliaQuest has developed an extensive suite of detections to identify and mitigate infostealer activity. Though too numerous to outline in full, the following example rules provide a snapshot of the comprehensive detection capabilities we offer. For a deeper look, visit GreyMatter Detect.

GreyMatter Automated Response Playbooks immediately contain threats upon detection, reducing MTTC to under five minutes and minimizing potential damage. Combined with GreyMatter detection rules and preconfigured hunts that proactively identify vulnerabilities and establish baselines for normal activity to detect anomalies, GreyMatter delivers comprehensive protection against infostealer threats.

Recommended Detection Rules

Service Installation in Suspicious Directory: Infostealers commonly exploit writable directories like the Temp directory to stage and execute malicious payloads, including the installation of unauthorized services. This detection identifies attempts to install services in high-level or temporary directories, allowing organizations to detect and respond to potential infostealer activity early in the attack lifecycle. This rule excludes known legitimate services to reduce false positives while maintaining focus on malicious behavior.

Non-standard Process Launching Windows Process: Infostealers often manipulate legitimate Windows processes to evade detection and execute malicious payloads. This technique is frequently coupled with tactics like installing services in suspicious directories, allowing attackers to abuse trusted processes for persistence and execution. This detection monitors instances where default Windows processes are launched by non-standard parent processes, signaling potential tampering or hijacking attempts.

Suspicious CSC .NET Compiler Execution: Infostealers often exploit legitimate frameworks like .NET to execute malicious code and evade detection. This detection flags suspicious use of the CSC .NET compiler, which attackers may leverage to load malware, perform in-memory attacks, or compile malicious scripts. By identifying unusual behavior .NET processes, organizations can detect infostealer activity tied to phishing campaigns and drive-by compromises, allowing for rapid response to prevent further intrusion.

RELIAQUEST GREYMATTER®

Recommended Hunt Packages and Automated Response Playbooks

Cleartext Passwords in Document: Infostealer malware harvests credentials from various sources on compromised hosts, including documents containing passwords. This Hunt helps organizations identify unencrypted passwords within documents and remove them to prevent infostealers from accessing sensitive credentials.

Password Manager Access to Sensitive Secrets – Credential Access: While password managers are generally more secure than other storage solutions, they're not immune to infostealer attacks. This Hunt allows organizations to establish a baseline of normal password manager usage within their environment, providing a reference point to detect abnormal activity and identify infostealers operating within the network.

Isolate Host: If infostealer malware is detected on a host, immediate isolation is vital to prevent the exfiltration of sensitive files and credentials. Automating this Response Playbook allows security teams to quickly contain threats, giving defenders the time needed to reimage the host and eliminate the malware.

Cloud Credentials in Cybercriminal Markets

In our 2025 Annual Threat Report, we revealed that 9% of intrusions in 2024 involved access gained through cloud accounts or trusted relationships.

As businesses across all industries increasingly adopt cloud services to boost resilience and operational efficiency, attackers have adapted to this shift. Lured by the expansive attack surface and wealth of sensitive data these platforms offer, threat actors have made credentials tied to cloud services a key target. When compromised, these credentials can grant attackers access to critical systems, escalate privileges, and exfiltrate sensitive data—posing significant risks to organizational security.

This prompted us to investigate whether cloud infrastructure was extensively represented in Russian Market logs. Our analysis of cloud logs and infostealer incidents focused on software-as-a-service (SaaS) and single sign-on (SSO) login credentials. These credentials pose some of the most significant risks to organizations because of their widespread use and the potentially damaging consequences that exploitation can bring.

SSO or SaaS Credentials Found in Two-Thirds of Russian Market Logs

SaaS credentials can be potentially dangerous to organizations if stolen, particularly for cloud-based apps, which attackers frequently target.

- These apps, especially those outside the purview of company IT departments, may not always comply with corporate security policies, making them easier for attackers to exploit.
- On Russian Market, the demand for SaaS logins is reflected in the high volume of fake credentials observed for key services like Google Workspace and Zoom, further highlighting their attractiveness as targets for cybercriminals.

SSO logins, widely used in modern organizations for their convenience, introduce unique security challenges:

- A single credential can grant access to multiple connected applications, exposing a wide range of systems and data.
- Although SSO logins are often protected by multifactor authentication (MFA), threat actors have developed ways to bypass these measures. Our 2025 Annual Threat Report revealed that session hijacking—via adversary-in-the-middle (AiTM) phishing attacks—bypassed MFA in every successful business email compromise (BEC) incident in 2024. This highlights that while MFA is an important security layer, it's not foolproof.

Figure 6: Percentage of Russian Market logs investigated that contained either SSO or SaaS credential pairs

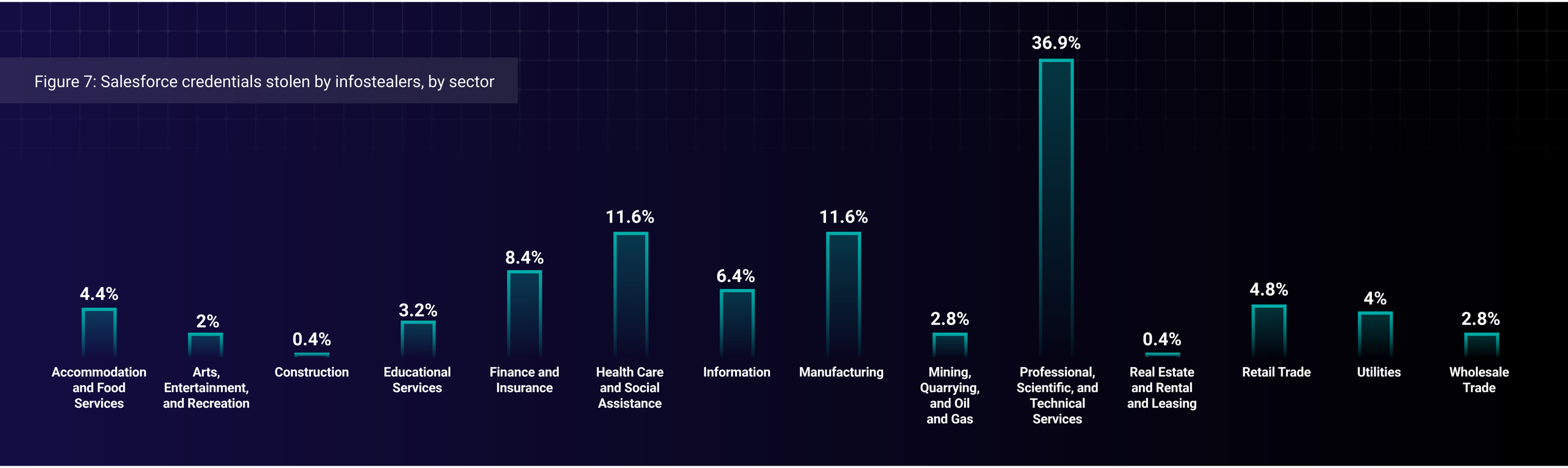
Infostealer compromises often include SaaS credentials, particularly in tech-heavy sectors like PSTS. As shown in our data, SaaS credentials are heavily prevalent in logs, suggesting their significant value to attackers. SaaS credentials provide access to critical systems and sensitive data, making them integral to enabling further compromises and lateral movement within victim organizations.

Our investigation of Russian Market logs shows how frequently SaaS credentials are targeted and exposed in infostealer logs. However, it's worth noting that these statistics include logs with credentials usable in both personal and corporate contexts. For instance, the SaaS credentials often related to software like Microsoft Teams or Google Workspace, which are widely used in both environments. This overlap makes it harder to measure the full corporate impact but nonetheless underscores the broad exposure of cloud credentials.

PSTS Hit Hardest by SaaS Credential Theft as Education Struggles with SSO

To better understand the risks associated with SaaS credentials, we analyzed their prevalence in our dataset, focusing on credentials tied to various SaaS providers being sold on cybercriminal marketplaces. This included infostealer incidents targeting companies that depend on Salesforce—a widely used software that serves as a clear example of the scale and severity of the cloud credential threat.

Figure 7: Salesforce credentials stolen by infostealers, by sector



Infostealer incidents disproportionately impacted the PSTS sector, with the data revealing three times as many incidents affecting companies using Salesforce in PSTS compared to the next most affected sector. This highlights the sector's heightened vulnerability to compromised SaaS credentials.

In contrast, analysis of incidents involving SSO credentials revealed that educational services was the most impacted sector, followed closely by PSTS.

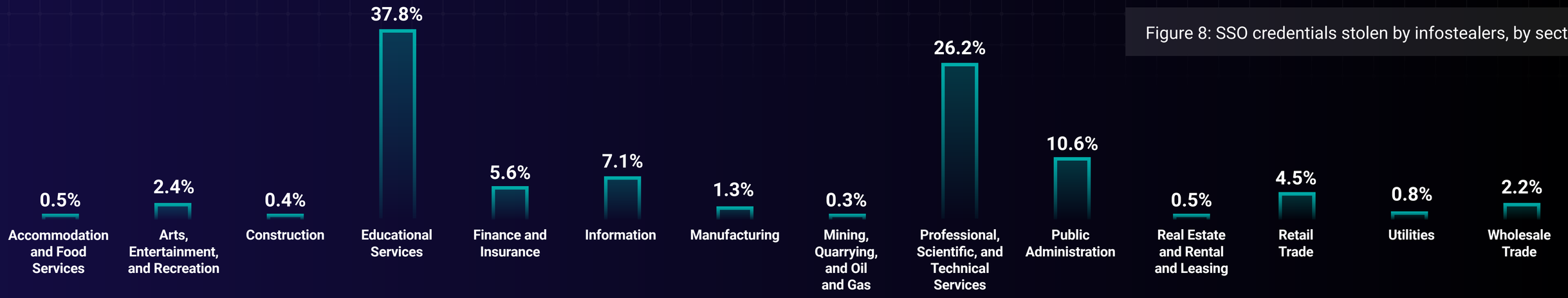


Figure 8: SSO credentials stolen by infostealers, by sector

The heightened risk faced by educational institutions can be attributed to their large user bases, which often include students accessing their accounts through SSO from personal devices. These devices are also frequently used to access potentially compromised websites, such as those offering music or movie downloads, further increasing the likelihood of exposure to infostealer malware.

Unlike corporate-managed devices, personal devices generally lack robust security measures, making them more susceptible to compromise. This vulnerability, in turn, increases the overall risk for educational institutions.

Figure 9: Russian Market listing offering credentials captured via mobile devices

For defenders, the targeting of SaaS and SSO credentials exposes a weak spot in modern cloud-based environments. Attackers often exploit these credentials to access multiple systems, escalate privileges, and exfiltrate sensitive data, which significantly expands the attack surface and facilitates lateral movement within organizations.

The prevalence of compromised cloud credentials in Russian Market logs demonstrates the importance of securing both corporate-managed and personal devices, especially in high-risk sectors like PSTS and education.

To mitigate these threats, defenders must prioritize proactive measures, including robust credential management, monitoring for infostealer activity, and implementing security controls that address both SaaS and SSO vulnerabilities before attackers can capitalize on them.

RELIAQUEST GREYMATTER®

Countering the Threat with ReliaQuest

The purchase of credentials associated with your organization on Russian Market significantly heightens the risk of compromise attempts.

ReliaQuest provides a robust set of detection rules designed to identify and block the use of stolen credentials, helping organizations safeguard accounts and secure their environments.

By combining these detection rules with recommended Automated Response Playbooks and preconfigured Hunts, organizations can proactively uncover vulnerabilities, mitigate risks, and stay ahead of potential threats.

Recommended Detection Rules

Azure AD Suspected Compromised Access: If infostealer malware compromises credentials for an Azure Active Directory (AD) account (now known as Microsoft Entra ID), threat actors may attempt to access the account to achieve their objectives. This detection monitors and alerts on successful logins that exhibit unusual patterns or behaviors strongly associated with account compromise.

Suspicious Command Executed on Cloud Resource: Stolen cloud credentials can allow attackers to gain unauthorized access to an organization's cloud environment. This alert identifies suspicious command executions following unauthorized access, including activities like pivoting between cloud resources, such as Azure virtual machines (VMs) or Kubernetes clusters, and executing malicious scripts.

Malware Detection in Cloud Storage: Threat actors may exploit cloud accounts to deploy malware to cloud storage, posing a risk of infecting other users within the environment. This rule activates when cloud storage antivirus tools detect malware within the cloud storage environment.

RELIAQUEST GREYMATTER®

Recommended Hunt Packages and Automated Response Playbooks

Amazon Web Services Enumeration: Compromised cloud accounts can be exploited for enumeration and discovery within cloud environments. This Hunt is designed to detect commands related to user and policy enumeration, group and role identification, infrastructure discovery, and account or bucket listing. By monitoring these activities, the Hunt Package can uncover unauthorized access and reconnaissance efforts, enabling security teams to respond swiftly and safeguard sensitive cloud resources.

Suspicious Azure Enterprise OAuth Applications Login Events: When Azure Enterprise account credentials are stolen by infostealers, threat actors often exploit legitimate Azure Enterprise OAuth applications to achieve persistence and exfiltrate data in Microsoft 365. This Hunt focuses on detecting login events to commonly abused applications, which may signal a potential compromise.

Reset Credentials: This Automate Response Playbook automatically initiates password resets for compromised accounts as soon as unusual activity like failed login attempts or abnormal login patterns has been detected. This action blocks unauthorized access and prevents attackers from leveraging the account for additional attacks, such as enumeration, persistence, or malware deployment.

Fortify Your Security Posture

To address the risks posed by stolen SaaS and SSO credentials, organizations should implement the following proactive measures:

Monitor Unusual Login Activity: Deploy monitoring solutions to detect signs of infostealer-linked credential abuse, such as geographically anomalous logins, repeated login failures, or logins from unfamiliar devices.

Audit and Adjust User Privileges and Unused Accounts: Regularly review user permissions to ensure they align with assigned roles, removing excessive privileges to limit the risk of lateral movement or data exfiltration. Identify and remove dormant or unused accounts and tokens to prevent their exploitation by threat actors.

Restrict Personal Devices: Enforce policies requiring employees to use only company-provided devices equipped with proper security protocols and provide regular training on cybersecurity best practices so employees understand the importance of secure device use.

ReliaQuest Reviews: How Does Russian Market Measure Up?

To better understand Russian Market's popularity among cybercriminals, we investigated the quality of the credentials it offers.

Does it provide unique information that other platforms don't?

Evaluating the quality of the logs enables us to help businesses quantify their risks associated with credential compromise. And by understanding these risks, businesses can make more informed decisions about mitigation strategies.

Our analysis of over 300 malware logs containing tens of thousands of stolen credentials revealed that much of Russian Market's inventory is recycled rather than unique.

However, the presence of duplicated credentials across Telegram channels and other cybercriminal forums doesn't necessarily mean that Russian Market is being deliberately deceptive. Nor does it suggest that the platform relies entirely on recycling credentials from other leaks—or that it's worse than other stolen credential marketplaces.

Figure 10: Post by XSS user SGL claiming Russian Market is full of public logs

The situation is more of a "chicken-and-egg" problem: Russian Market's straightforward registration process for sellers makes it easy for cybercriminals to upload their logs to multiple platforms simultaneously. Additionally, threat actors who buy logs on Russian Market are likely reselling them elsewhere—and vice versa—further muddying the waters.

Unlike cybercriminal forums where buyers can publicly call out scammers in arbitration sub-sections, Russian Market lacks a system for users to rate or review sellers. This absence of accountability likely erodes trust among individual buyers over time. However, new buyers continuously emerge, allowing unscrupulous sellers to operate with relative impunity, confident that the risk is worth the reward.

The prevalence of recycled logs raises questions about the uniqueness of Russian Market's inventory, while the widespread presence of fake credentials casts further doubt on its overall quality.

Some sellers pad their listings with blatantly fake entries of generic email addresses like "example[at]gmail[.]com", especially for high-demand domains like "gmail." Buyers can only see the domain name (e.g., "gmail") before purchase, so they don't discover the fake entries until the transaction is complete.

The prevalence of fake credentials also reflects another critical reality:

Some domains are far more valuable than others. High-demand domains like "gmail" are particularly prized by buyers because they're often used to register for multiple other services, such as financial platforms, entertainment services, or online shopping accounts.

This means a single compromised Gmail account can grant attackers access to an entire chain of connected services, significantly increasing their potential profit.

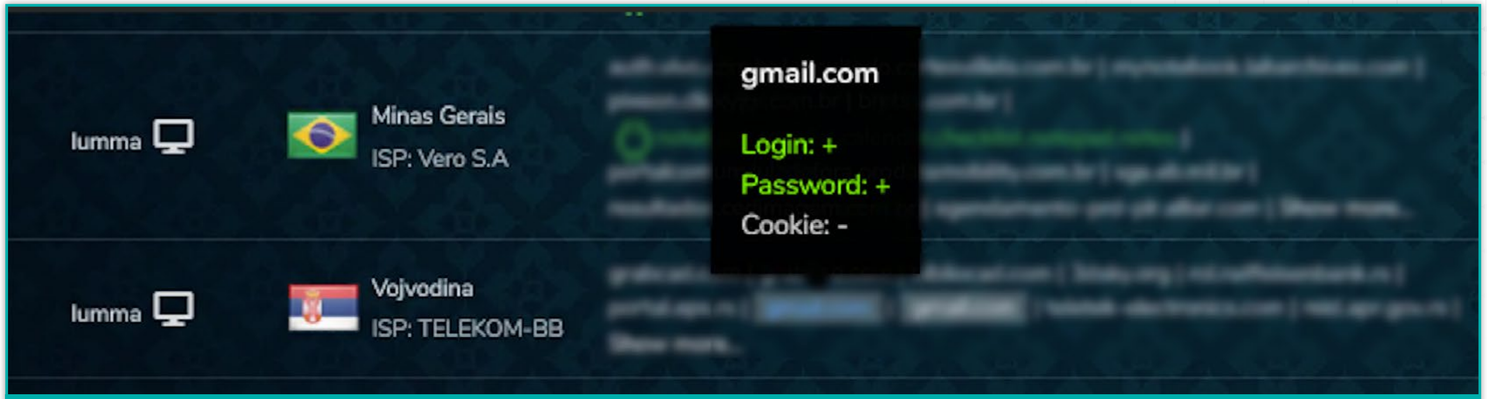


Figure 11: Gmail log listed on Russian Market

In some cases, legitimate businesses buy credentials from Russian Market to identify accounts at risk of compromise. While this approach can yield valuable information, it also carries the unintended consequence of driving up demand for stolen credentials. This dynamic highlights the delicate balance organizations must strike when considering such actions, as they risk inadvertently fueling the very ecosystem they're trying to defend against.

For defenders, this emphasizes a critical vulnerability: When employees use personal email accounts like Gmail to register for corporate services, they unintentionally expand their organization's attack surface. Purchasing credential logs for defensive purposes also introduces its own set of risks. Repeated purchases can inadvertently sustain and grow the marketplace for stolen credentials, increasing the likelihood that similar domains will be targeted and exploited.

This creates a dangerous feedback loop, where defensive actions unintentionally reinforce the ecosystem driving these threats. To break this cycle, organizations must prioritize proactive defenses—stopping infostealer malware at its source—rather than relying on reactive, after-the-fact measures. By addressing the root cause of credential theft, defenders can significantly reduce their exposure to these escalating risks.

RELIAQUEST GREYMATTER®

Countering the Threat with ReliaQuest

Organizations that have credentials sold on Russian Market face a greater risk of compromise attempts using those stolen credentials.

ReliaQuest has developed a range of detections to help identify and prevent attempts to use stolen credentials, enabling organizations to actively protect accounts and environments from compromise.

Enable these detection rules with the recommended Automated Response Playbooks to ensure your organization stays ahead of potential threats and reduces the risk of credential abuse.

Recommended Detection Rules

Geographically Anomalous Remote Login – Signature Detected: Stolen credentials harvested by infostealers are often used by attackers to access accounts from unfamiliar regions, enabling further compromise or lateral movement. This rule detects remote logins from locations previously unused by the legitimate user, identifying potential malicious activity.

Successful Remote Brute Force: Infostealers often provide attackers with partial credentials, which are then exploited in brute-force attacks to gain unauthorized access to systems, escalate privileges, and compromise additional accounts. This rule flags successful remote logins following such credential abuse.

Multiple Lockouts on a Single Account: Malicious activities like password guessing or credential stuffing can cause repeated account lockouts in Microsoft Windows, disrupting operations and compromising security. This detection monitors for five consecutive lockout events from the same user within a 10-minute window, enabling security teams to identify potential brute-force attacks or credential abuse attempts and take swift action to protect accounts.

RELIAQUEST GREYMATTER®

Recommended Hunt Packages and Automated Response Playbooks

Insider Threat - Non-corporate Email Domains: The use of personal accounts and emails within an organization introduces unnecessary risk. This proactive Hunt identifies when a personal email has been used, enabling defenders to educate users and address the issue before it can be exploited by a threat actor.

Reset Password: This Automated Response Playbook immediately updates the password for compromised accounts when suspicious activity like failed login attempts or unauthorized access has been detected. This action ensures that passwords captured by infostealers cannot be reused by threat actors, preventing further exploitation of the account.

Terminate Sessions: This Playbook ends all active sessions for compromised accounts, ensuring that any sessions captured by an infostealer cannot be used to access the account. Pairing this action with a password reset prevents attackers from reusing stolen credentials and blocks unauthorized access.

Fortify Your Security Posture

Organizations should take proactive steps to mitigate the risks posed by using personal email accounts on corporate networks.

Disable Personal Accounts: Prevent the use of personal accounts for business operations, account registration, and logins. Disable domains outside of your organization across your environment.

Audit For Personal Accounts: Audit for employees using personal accounts on company devices to identify if standard operating procedures (SOPs) have been bypassed and pinpoint areas that may require stricter policies or enhanced controls.

Evaluate Russian Market Listings: Evaluate exposed credentials on AVCs like Russian Market before purchasing them to verify whether the listed domains belong to sensitive areas of your organization, such as employee portals or administrator consoles, rather than customer-facing portals.

Key Takeaways and What's Next for Infostealers?

This report shines a light on the pivotal role Russian Market plays in the stolen credential economy, providing threat actors with easy access to infostealer logs at scale.

It emphasizes the importance of preventing infostealer compromises during the initial stages of an attack to stop stolen credentials from appearing on platforms like Russian Market, where they can be exploited further.

When initial access is achieved, swift and effective detection and mitigation of infostealer threats become essential to minimizing downstream risks and preventing attackers from leveraging compromised credentials in future campaigns.

Looking ahead, emerging trends in the infostealer landscape are introducing new challenges that organizations must prepare for. Below, we explore key developments, including the rise of "Acreed" infostealer and the increasing prominence of password managers and mobile devices, which are likely to shape the future of infostealer threats.

The Next Big Infostealer: Acreed

Our analysis of Russian Market logs spotlights Acreed as a newly emerged infostealer, which we anticipate will become a major force in credential theft. In Q1 2025, Acreed surpassed every established infostealer in terms of Russian Market alert attribution, ranking second only to giant Lumma.

> Since the law enforcement takedown of Lumma in mid-May 2025, Acreed is perfectly positioned to rapidly gain traction as cybercriminals seek alternatives.

Should Acreed hit the same heights as Lumma and the two begin competing for business, the scale of credential theft incidents is highly likely to boom. Businesses may even fall victim to simultaneous compromises by multiple infostealers or successive attacks in short intervals. While Acreed's specific TTPs are currently unknown, it's highly likely that it employs similar strategies as other infostealers. In the short term (up to three months), generic detections can help mitigate Acreed's impact.

However, until its attack pathways are fully understood and targeted defenses are developed, businesses may face difficulties mitigating the risks associated with this emerging threat.

The Growing Risk to Password Managers

We predict with high confidence that infostealers will focus on targeting password managers in the medium-term future (3–12 months).

The growing need for complex passwords to prevent brute-force attacks using rainbow tables has directly led to greater reliance on password managers. These centralized repositories of sensitive credentials—essential for both individual users and enterprises managing vast credential inventories—are a highly lucrative vector for attackers seeking mass credential access.

A successful compromise of a password manager could give attackers access to a vast array of accounts and services, enabling large-scale data breaches, operational disruptions, and further lateral movement within organizational networks.

To mitigate these risks:

Organizations should prioritize the security of password management platforms and implement additional monitoring to detect unusual activity.

Malware Moves to Mobile Devices

Companies are increasingly allowing employees to use personal mobile devices to access work systems like email, messaging apps, and sometimes additional key software.

As such, mobile devices are rapidly becoming prime targets for threat actors. Future developments in infostealer malware will highly likely focus on exploiting these devices more aggressively, leveraging their dual-use nature (personal and professional) to identify and exploit security gaps. Even in organizations with policies restricting mobile access to specific tools—such as email—malware targeting these devices could still harvest enough information to enable broader attacks, including BEC.

For businesses, this trend presents significant risks, including the potential exposure of sensitive corporate data, unauthorized access to critical systems, and disruption of key operations. The lack of direct control over personal devices further complicates security efforts, leaving gaps that attackers can exploit.

To mitigate these risks:

Organizations must carefully manage what employees can access through their mobile devices and adopt robust security measures to ensure sensitive systems and data remain protected from compromise.

Endnotes

1. hxxps://www.securityweek[.]com/infostealer-infections-lead-to-telefonica-internal-ticketing-system-breach/

2. A drive-by download is a type of cyber attack in which malicious software is automatically downloaded onto a device when a user simply visits a compromised website or views malicious content, often exploiting browser or software vulnerabilities.

3. hxxps://www.securitymagazine[.]com/articles/101404-us-agencies-and-defense-contractors-infected-with-infostealer-malware

About ReliaQuest

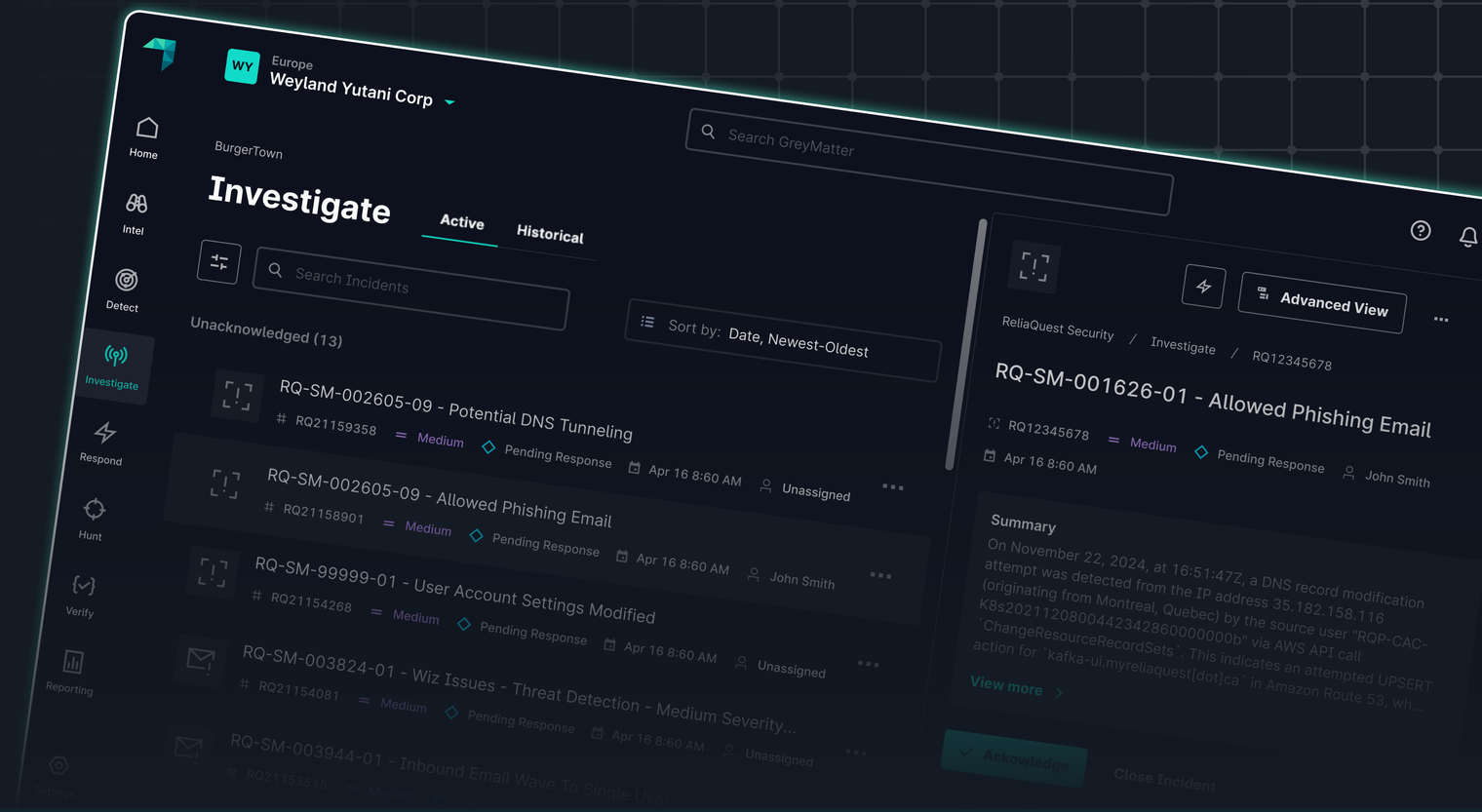
ReliaQuest exists to Make Security Possible.

Our agentic AI-powered security operations platform, GreyMatter, allows security teams to detect threats at the source, and contain, investigate, and respond in less than 5 minutes—eliminating Tier 1 and Tier 2 security operations work.

GreyMatter uses data-stitching, detection-at-source, AI, and automation to seamlessly connect telemetry from across cloud, multi-cloud, and on-premises technologies.

ReliaQuest is the only cybersecurity technology company that delivers outcomes specific to each organization's unique architecture, technology, and business needs.

With over 1,000 customers and 1,200 teammates across six global operating centers, ReliaQuest Makes Security Possible for the most trusted enterprise brands in the world.



Learn more at www.reliaquest.com →

[ReliaQuest's ShadowTalk](#) is a weekly podcast featuring discussions on the latest cybersecurity news and threat research.

Listen to the latest episodes on your favorite podcast channels.

RELIAQUEST®

reliaquest.com

800.925.2159

info@reliaquest.com