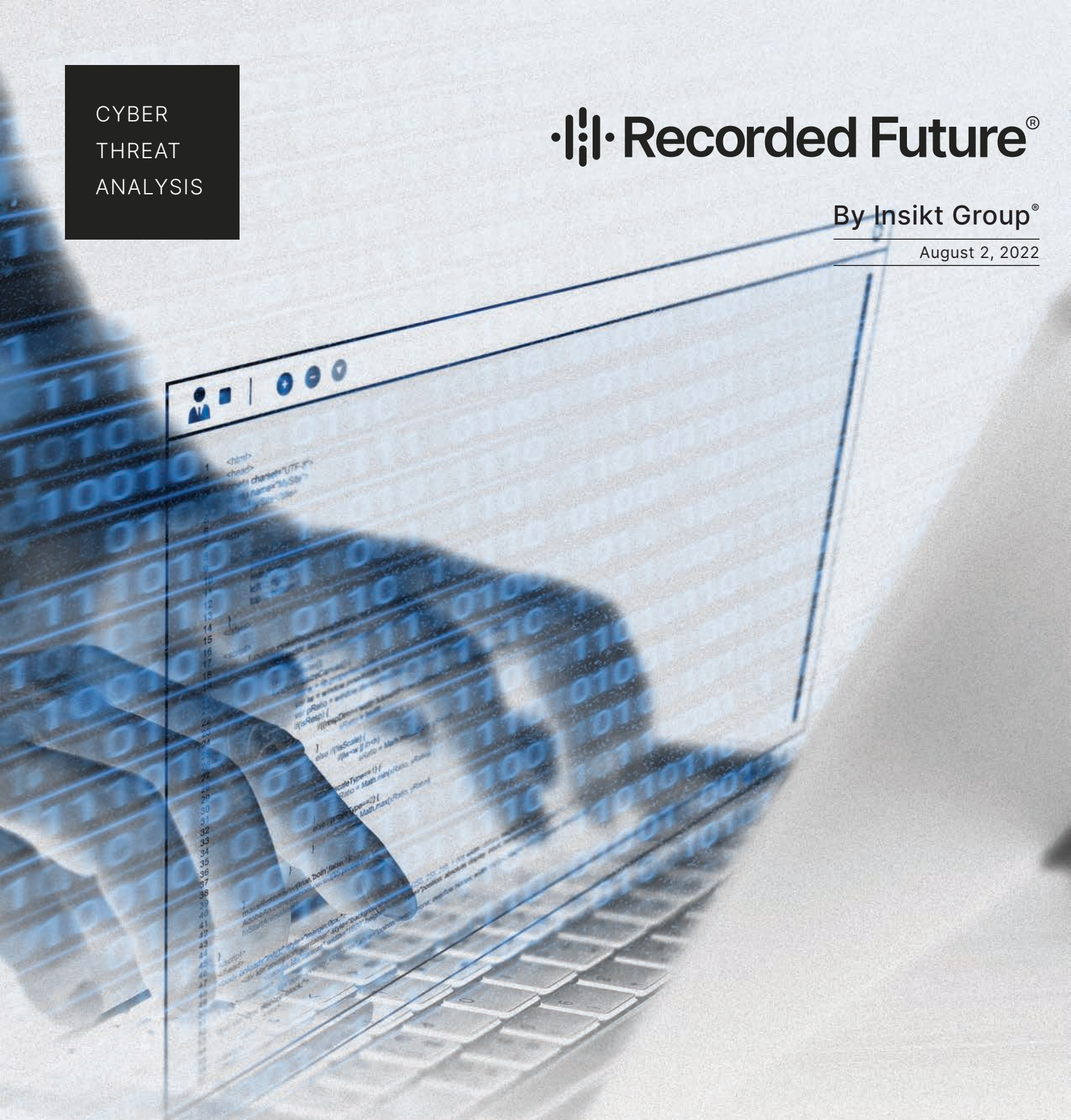
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 2, 2022



Initial Access Brokers Are Key to Rise in Ransomware Attacks

Recorded Future®

This report provides an overview of the tactics, techniques, and procedures (TTPs) used by cybercriminals on dark web and special-access sources to compromise networks, deploy infostealer malware, and obtain valid credentials. These threat actors, dubbed "initial access brokers", represent a specialized industry within the cybercriminal underground that enables a significant majority of ransomware attacks. This report includes information gathered using the Recorded Future® Platform, dark web sources, and open-source intelligence (OSINT) techniques. This is a high-level summary of the chain of events that enable a ransomware attack. It is intended to provide an overview for cybersecurity professionals with non-technical backgrounds or roles.

Executive Summary

Threat actors can gain initial access to networks through infostealer malware infections, initial access brokerage services on dark web and special-access forums, or the purchase of infostealer logs from dark web shops and marketplaces. Other attack vectors, such as phishing, spearphishing, and code injection, are also common on dark web and special-access forums, but their immediate effects are often much less public and visible than the sale of compromised credentials. Using BlackMatter and Conti as examples, we examine the role of credential access in the execution of the attack, from initial access to ransomware deployment. We provide mitigations for credential breaches, infostealer malware infections, and ransomware attacks, as well as our assessment of the future of these tools and the larger ransomware threat landscape.

Key Judgments

- To conduct a successful ransomware attack, threat actors require remote access to compromised networks. The most common method by which threat actors obtain access is through the use of compromised valid credential pairs, which are often obtained via infostealer malware and sold on dark web and special-access sources.
- Compromised credentials are often sold on dark web and special-access forums and shops to ransomware affiliates, who use such access to move laterally through systems, escalate privileges, and use malware loaders to deploy ransomware.

Background

Threat actors require remote access to compromised networks to conduct successful attacks, such as malware loader deployment, data exfiltration, or espionage campaigns. These compromised access methods, often sold on dark web and special-access forums, are the work of specialized threat actors colloquially referred to as "initial access brokers" (IAB). IABs use several tools and TTPs to obtain such access, including obtaining valid credential pairs and session cookies from the successful deployment of infostealer malware, the purchase of infostealer "logs" or "bots" on dark web shops, credential stuffing, adversary-in-the-middle attacks, phishing, remote desktop protocol (RDP) "brute force guessing", and more.

The most common credential pairs that appear for sale or auction on top-tier dark web and special-access sources, such as Exploit and XSS, are for corporate virtual private networks (VPNs), RDP services, Citrix gateways, web applications and content management systems (CMS), and corporate webmail servers (business email compromise, or BEC). Less common, but more sought-after, are ESXi root and Active Directory (AD) access methods, zero-day and n-day vulnerabilities, code injection points (HTML, SQL), and others. This report will outline the typical process by which an initial access broker obtains compromised access methods and sells them on dark web and special-access sources, and the use of such methods to conduct a successful ransomware attack.

Threat Analysis

One of the most effective ways for ransomware operators to gain access to victim networks is by either deploying infostealer malware or obtaining logs exfiltrated by an infostealer on a dark web or special-access source. This malware is deployed through the use of acquired or compromised botnets, phishing, the successful deployment of an obfuscated malware loader or dropper, or through the purchase of compromised credentials on dark web and special access sources.

Compromised Valid Credentials

To easily obtain bulk compromised valid credentials and session cookies, threat actors often rent access to a licensed account for an infostealer malware. These licenses come in many forms, but most often as web panels, source code, builders, or standalone clients. Infostealers are often marketed directly by their developers as a malware-as-a-service (MaaS) offering on top-tier dark web and special-access sources, messaging platforms (such as Telegram), and social media. The information harvested from infostealers, colloquially referred to as "logs" or "bots", is then sold on dark web shops, such as Genesis Store, Russian Market, the now-defunct Amigos Market, and 2easy Shop. The most common infostealers that appear on dark web and special-access sources are RedLine, Vidar, FickerStealer, Taurus, AZORult, and the now-defunct Raccoon.

Deploying Stealers

Infostealers, generally considered to be a subgroup of the banking or remote access trojan (RAT) malware category, can capture a great amount of compromised information from an infected device, including keystrokes and peripheral input captures, session cookies, usernames and passwords from browser stores, screen and video captures, local data, browser history and bookmarks, clipboard data, and more. The most common attack vectors by which infostealers spread is through spam campaigns or phishing. Less commonly, but as evidenced by the rapid spread of Mars Stealer in Q1 2022, infostealers can spread via malicious Google Ads and pop-ups. These infostealer payloads can be disguised within Microsoft Office documents through the use of malicious macros; a dropper that encrypts the payload as extra data; or a loader that communicates with its command and control (C2) infrastructure over a web protocol and uses a built-in command and scripting interpreter to remotely execute code. Once an infostealer successfully infects a victim device, it begins to log activities and collect compromised information. These logs are then manually examined by the infostealer operator for credentials that might be profitable (for example, credentials for tools or platforms like RDP, VPNs, or WordPress) on dark web or special-access sources. At this point, an infostealer operator could become an initial access broker for ransomware and data leak groups on dark web forums.

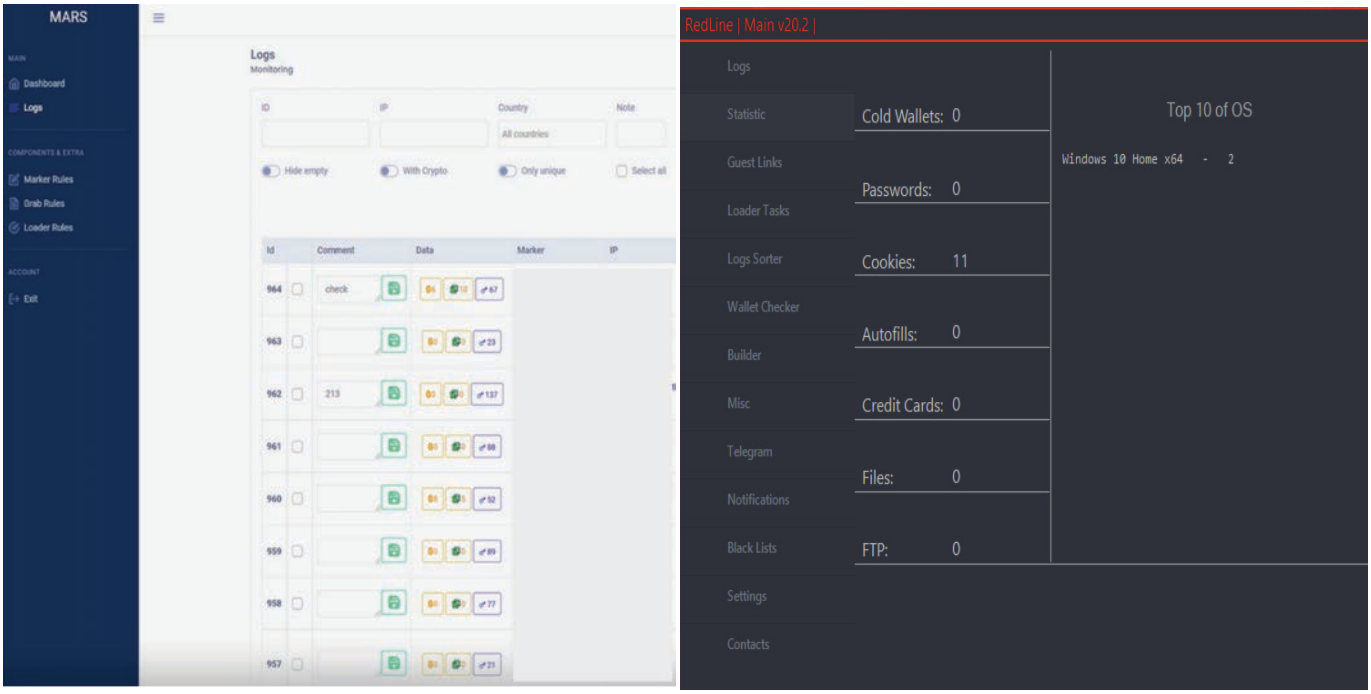


Figure 1: Examples of web panel dashboards for infostealer malware, including Mars (left) and RedLine (right) (Source: Recorded Future)

Initial Access Brokers

Stolen credentials are often sold to ransomware affiliates on dark web and special-access forums by specialized cybercriminals called initial access brokers (IABs). While most high-profile accesses are brokered on top-tier Russian-language forums, such as Exploit, XSS, or RAMP, it is still possible to encounter IABs on low-tier or mid-tier English-speaking forums, such as BreachForums or the now-defunct Raid Forums. IABs commonly operate in multiple languages on different forums, often under different monikers (for example, “FuckerZ” connects to “Tokugaw4”, “tokugawa”, “xssisownz”, and “Str0ng3r”), to avoid detection, tracking, and arrest. Many English-language cybercriminal forums, such as Cracked or Nulled, have banned IAB services and ransomware discussions outright, as the risk of law enforcement attention on the forum increases with such activity. Less commonly, ransomware operators and affiliates will work directly with a designated group of IABs that will conduct business off of the forums and in private messaging channels, such as Tox or XMPP (Jabber).

IAB advertisements follow a similar pattern on dark web and special-access forums. The template is loosely as follows: “victim country”, “annual revenue”, “industry”, “type of access”, “rights”, “data to be exfiltrated”, and “devices on local network”. Additional useful information includes the type of antivirus software, IP address ranges, and other details. On top-tier forums, sellers are typically required by the forum’s rules to provide a sale price in the initial advertisement. As many of these deals are negotiable, with price ranges varying widely depending on multiple factors, the most common form of advertisement is the “auction” format. IABs will provide an acceptable starting price (“start”), the minimum price of bid hikes (“step”), and the full or “buy now” price if a threat actor is interested in purchasing immediately (“blitz”). This is often followed by a time range in which the posting will close, which is generally between 4 and 8 hours. The IAB will often indicate if a sale is made in the thread (“sold”, продано), asking the forum’s moderation staff to then close the thread for new replies. IABs, especially those who are working with unknown or low-reputation threat actors on the forums, will often request the use of escrow or middleman services to facilitate transactions.

Below are 3 examples of advertisements from high-credibility IABs” :inthematrix1” ,“nei ,“and” zirochka:“

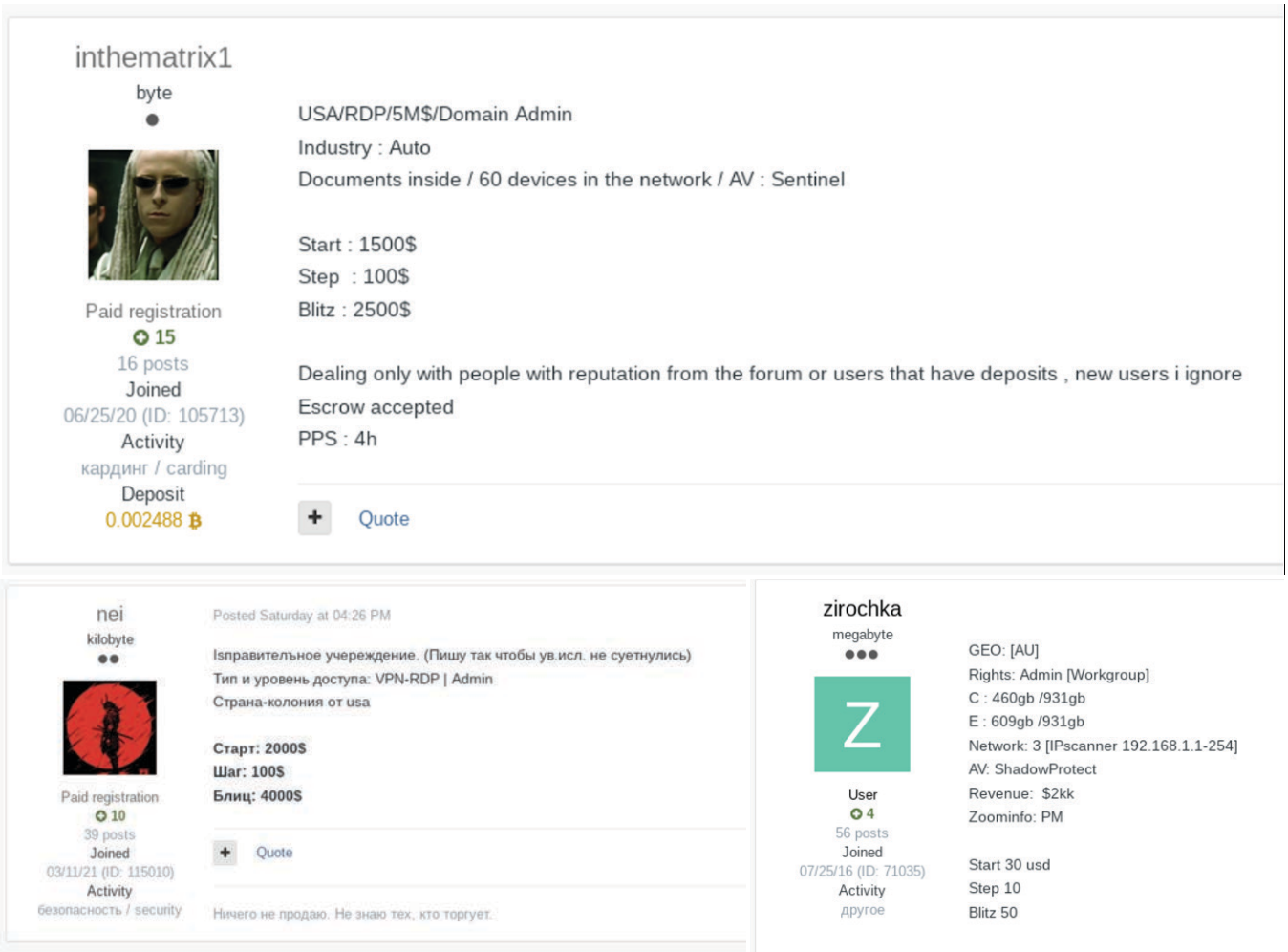


Figure 2: Examples of IAB services on the top-tier Russian-language forum Exploit (Source: Exploit)

Figure 3: Sample of listings on the dark web shop Russian Market (Source: Russian Market)

Dark Web Shops and Marketplaces

Dark web shops and marketplaces are common sources for threat actors to obtain compromised valid credentials, browser and session cookies, RDP and VPN keys, and more. Dark web shops are typically a low-cost method for threat actors to purchase infostealer logs or bots which affect specific domains, IP address ranges, entities, or internet service providers (ISPs). However, one of the drawbacks of dark web shops is that it is difficult to obtain credentials with administrator-level privileges in a single purchase. Threat actors often have to purchase compromised credentials in bulk, expending much more money, time, and energy than working directly with an IAB. Regardless, dark web shops and marketplaces remain a common method by which IABs or ransomware affiliates gain initial access to an entity's network. It is also a common method by which IABs can turn a profit on dark web and special-access forums, via "flipping" low-cost credentials, often purchased for less than $10, to ransomware affiliates for potentially thousands of dollars. The most prevalent dark web shops are Russian Market, Genesis Store, and 2easy Shop.

Russian Market

Russian Market is a criminal shop operated by the threat actor "RussianMarket" that sells database dumps, RDP and SSH accesses, infostealer logs, compromised payment cards, and PayPal accounts. Infostealer logs are primarily harvested from victims infected with popular infostealers, such as Vidar, AZORult, Raccoon Stealer, RedLine, or Taurus. Russian Market is one of the most prevalent dark web shops, offering millions of infostealer logs affecting entities around the world. It is a common destination for threat actors seeking to purchase compromised information related to specific entities, domains, or subdomains, which can then be used for initial access, lateral movement, and privilege escalation.

Genesis Store

Genesis Store is a criminal shop likely created by the threat actor "GenesisStore" in 2018. The store is advertised across multiple Russian- and English-language dark web forums. Genesis Store sells packages ("bots") of compromised account credentials and associated user data designed to allow threat actors to bypass anti-fraud solutions.

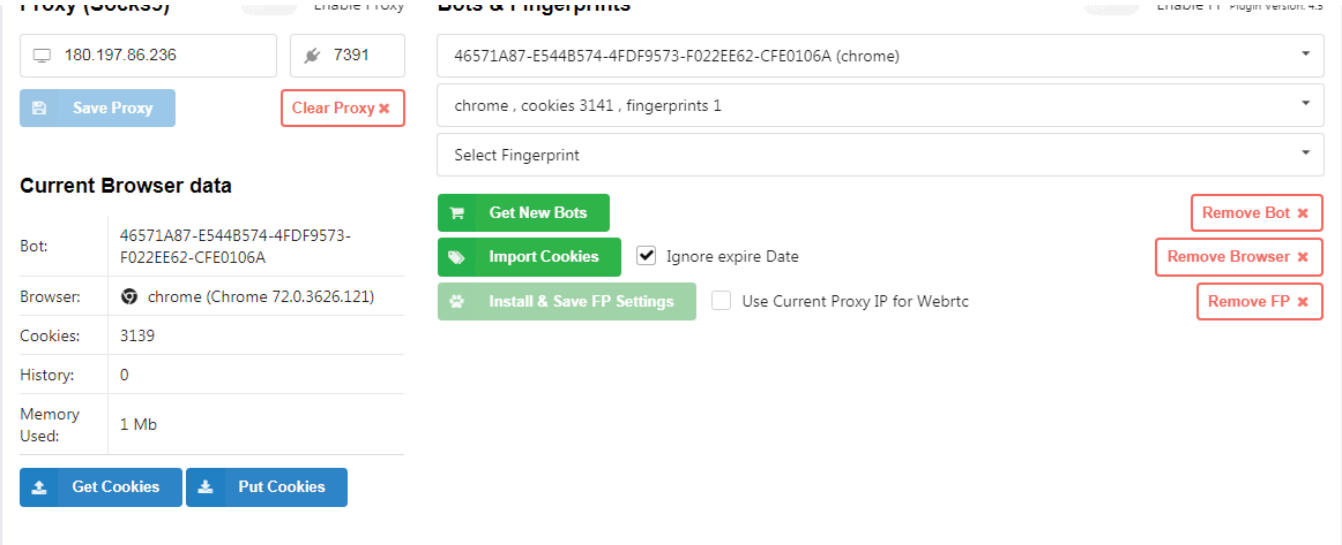


Figure 4: Import cookies with the Chrome browser plugin "Genesis Security" (Source: Genesis Store)

Victim data is sold in a single package referred to as a bot or log, which includes account credentials, IP address, browser fingerprint (system information), and cookies. After a bot is purchased by a threat actor, victim data can be imported into a browser plugin called Genesis Security, as shown in Figure 4 below. This feature allows the attacker to masquerade as the victim and perform account takeover and session hijacking attacks. The price for each bot varies depending on the number of account credentials, types of accounts, and geographical location of the victim.

2easy Shop

2easy Shop is a Russian and English-language dark web shop that has been in operation since at least 2021 and was founded by the threat actor "2easy". The shop sells logs harvested from unspecified infostealers, but likely Vidar, RedLine, and Raccoon Stealer, among others. The prices for logs range between $3 and $200 per listing and include compromised user logs and accounts from hundreds of organizations around the world. The price point for victim data on the shop varies depending on the content and date of the listing.

When compromised data is purchased on 2easy Shop, a buyer typically receives a victim's browser cookie data, browser history, screenshots, general system information about compromised machines, and other data. The compromised account credentials and associated user data is commonly used by threat actors to bypass targeted organizations' defenses and anti-fraud solutions, which can be used for initial access, lateral movement, or privilege escalation.

Using Access/Credentials to Deploy Ransomware

Case Study: BlackMatter Ransomware

Figure 5 below shows "BlackMatter", a user representing the BlackMatter ransomware affiliate program, looking for targets located in specific countries, excluding medical and government entities, with revenues at a certain profit threshold. This gives insight into the way that ransomware groups get access to networks and how they recruit affiliates, and it suggests that financial gain is a primary motivator.

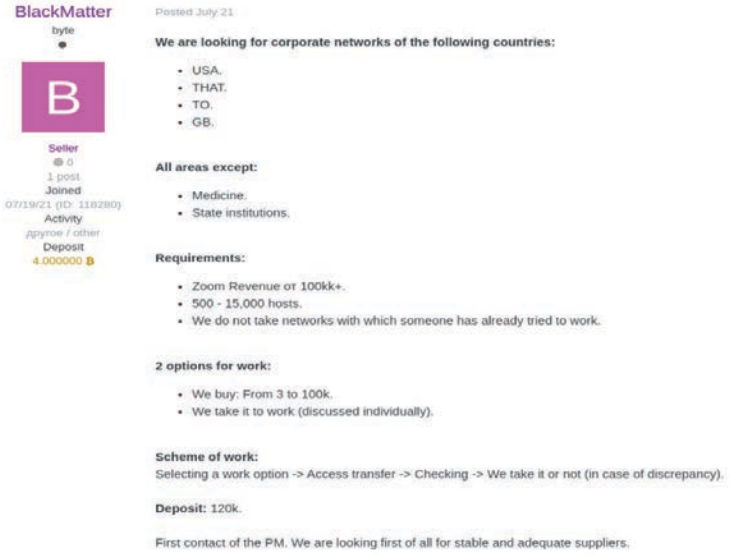


Figure 5: BlackMatter representative advertisement looking for target networks (Source: Exploit)

Once access to a compromised network or domain is obtained, threat actors then leverage several tools and TTPs to move laterally in a system, escalate privileges, exfiltrate or destroy data, and deploy ransomware. According to the FBI, affiliates associated with the BlackMatter ransomware-as-a-service (RaaS) group have used previously compromised user credentials as an initial access vector to compromise organizations. After gaining access, threat actors compromise Active Directory to gain additional user and administrator privileges, then modify Group Policy Objects (GPOs) to deploy ransomware.

Case Study: Conti Ransomware

Like the threat actors associated with BlackMatter, Conti Gang, the operators of Conti Ransomware, and their affiliates also typically begin compromising a network using stolen credentials. According to CISA, Conti affiliates use a variety of initial access vectors including phishing, compromised credentials, malware distribution, and exploiting vulnerabilities. CISA and the FBI have observed Conti's operators using Router Scan, a tool to scan and brute-force network devices. The attackers would also use kerberoasting to discover and crack administrator hashes. Once they successfully achieve Domain Administrator rights, they begin exfiltrating sensitive data using Rclone and mega[.]nz. When the threat actors are satisfied with the data they captured and the network defenses have been removed, they begin preparing the network to deploy the ransomware. As we saw with the BlackMatter case study, Conti will place the ransomware executable in a location such as SYSVOL on the Domain Controller and then set up a domain-wide scheduled task to execute the ransomware under the highest privileges achieved.

Mitigations

Credential Leaks

Credential leaks and email exposure amplify the risks associated with ransomware attacks, as the data can be used to devise tailored spearphishing lures and serve as initial points of compromise via credential stuffing and account takeover. Recorded Future clients can surface exposed credentials in the Recorded Future Platform and should force password resets for those users whose leaked credentials are still active.

Infostealer Malware

Given the role that infostealers play in underground marketplaces and in enabling ransomware attacks, mitigation strategies against infostealer malware should be incorporated:

- Keep all systems current with the latest security patches and updates.
- Invest in a solution that offers patch posture reporting. This type of solution can provide insight into the vulnerabilities that have received remediation measures as well as the machines that have received those patches.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on any malicious activity.
- Deploy a spam filter used to detect indicators of phishing, such as viruses, blank senders, and keyword text triggers.
- Deploy a web filter to block malicious websites.
- Monitor for suspicious changes to system file drives and Registry that focus on the interception of keystrokes.
- Educate your employees and conduct training sessions with mock phishing scenarios.
- Develop a password security policy that includes but is not limited to password expiration and complexity.
- Require encryption for employees, especially employees working remotely. This includes whole-disc, such as 256-bit AES, and network encryption via SSL or TLS.
- For enterprises, Recorded Future can monitor for potential typosquat domains weaponized in phishing attacks. This includes not only the domains belonging to one organization, but third-party partners and vendors with enterprise network access.

- The Recorded Future Platform can also assist with the detection of compromised credential information linked to valid accounts to assist in providing context surrounding suspicious user behavior that may include keylogging activity. Recorded Future Platform users can continue to monitor underground sources to identify the spyware and keylogging tools that are likely to be the most harmful to their immediate infrastructure or supply chain.

Ransomware

Maintain offline backups of your organization's data and ensure that these backups stay up to date to prevent data loss in the event of a ransomware infection. Additionally, Recorded Future recommends the following mitigations to reduce overall risk:

- Ransomware often follows a specific pattern of behavior that can be detected with a robust threat intelligence system, integrated with SIEM platforms.
    - Implement YARA rules like the ones found in Recorded Future Hunting Packages to identify malware via signature-based detection or SNORT rules for endpoint-based detections.
    - The IOCs provided throughout this report can be used to proactively query or scan environments for items such as file hashes, registry keys, and IP traffic associated with ransomware.
- Network segmentation can halt the propagation of ransomware through an organization's network. This solution involves splitting the larger network into smaller network segments and can be accomplished through firewalls, virtual local area networks, and other separation techniques.
- If remote access solutions are crucial to daily operations, all remote access services and protocols, such as Citrix and RDP, should be implemented with two-factor or multi-factor authentication.
    - Exposed Remote Desktop Protocol (RDP) servers are also abused by threat actors to gain initial access into a target's network. Threat actors will look for networks that have internet-facing servers running RDP and then exploit vulnerabilities in those servers or use brute-force password attacks. Once inside the network, the threat actors move laterally and install ransomware on target machines, often disabling backups and other protections.
- Through the use of process monitoring, monitor for the execution and command of binaries involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit.
- Monitor for the creation of suspicious file modification activity, particularly large quantities of file modifications in user directories.
- Consider keeping sensitive client information on systems disconnected from the internet or segmented from the rest of the corporate network. Since ransomware will encrypt all files on a victim system and often will search for directories on the network (such as networked file shares) to also encrypt, moving highly sensitive customer data to a system with no internet access or access to the rest of the network will minimize the access ransomware would have to those files.

Outlook

Infostealer malware and exfiltrated logs will remain popular among threat actors as a means to obtain credentials to gain access to victim networks. While some infostealer variants, such as RedLine, FickerStealer, and AZORult have endured, new variants like Mars Stealer, MetaStealer, and Eternity will continue to emerge. Dark web shops and marketplaces will also remain an attractive source of infostealer logs for threat actors. However, the most effective method by which a ransomware affiliate can gain initial access to a compromised network is through the use of an IAB on dark web and special-access forums. Other attack vectors by which initial access is gained is through the use of a RAT, phishing, spearphishing, and other social engineering attacks. The process by which ransomware operators and affiliates infect networks following initial access can be very quick and often undetectable.

Appendix A :MITRE ATT&CK

RESOURCE DEVELOPMENT		
Enterprise	T1584	Compromise Infrastructure
Enterprise	T1587	Develop Capabilities
INITIAL ACCESS		
Enterprise	T1566	Phishing
Enterprise	T1078	Valid Accounts
Enterprise	T1190	Exploit Public-Facing Application
Enterprise	T1189	Drive-by Compromise
EXECUTION		
Enterprise	T1059	Command and Scripting Interpreter
Enterprise	T1204	User Execution
PERSISTENCE		
Enterprise	T1133	External Remote Service
Enterprise	T1137	Office Application Startup
PRIVILEGE ESCALATION		
Enterprise	T1055	Process Injection
DEFENSE EVASION		
Enterprise	T1027	Obfuscated Files or Information
CREDENTIAL ACCESS		
Enterprise	T1557	Adversary-in-the-Middle
Enterprise	T1110	Brute Force
Enterprise	T1555	Credentials From Password Stores
Enterprise	T1056	Input Capture
Enterprise	T1539	Steal Web Session Cookie
DISCOVERY		
Enterprise	T1217	Browser Bookmark Discovery
LATERAL MOVEMENT		
Enterprise	T1021	Remote Services
COLLECTION		
Enterprise	T1115	Clipboard Data
Enterprise	T1005	Data From Local System
Enterprise	T1114	Email Collection
Enterprise	T1113	Screen Capture
Enterprise	T1125	Video Capture

COMMAND AND CONTROL		
Enterprise	T1071	Application Layer Protocol
EXFILTRATION		
Enterprise	T1041	Exfiltration Over C2 Channel
IMPACT		
Enterprise	T1485	Data Destruction
Enterprise	T1486	Data Encrypted For Impact

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,400 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.