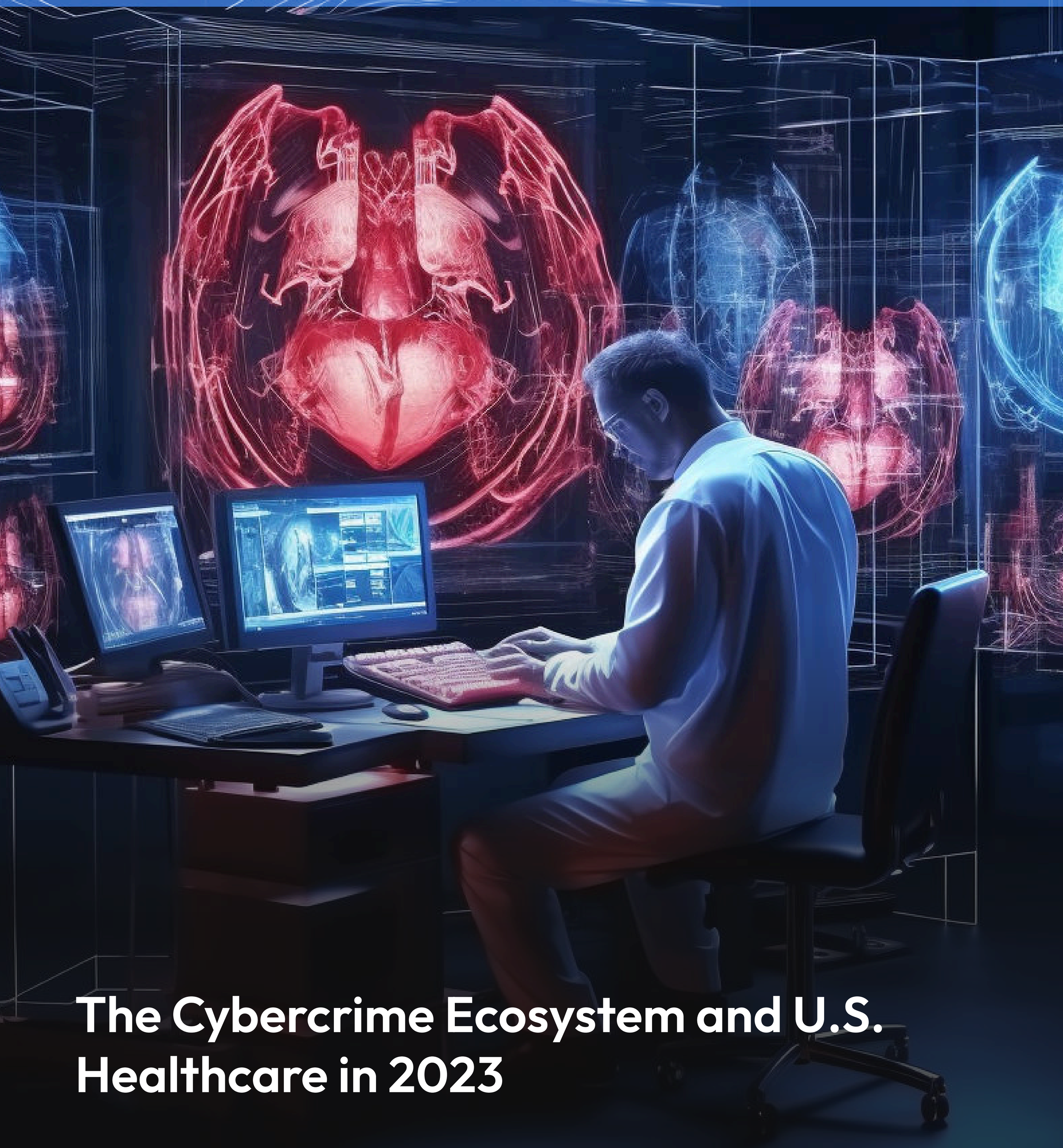
flare



The Cybercrime Ecosystem and U.S. Healthcare in 2023

Table of Contents

The Cybercrime Ecosystem and U.S. Healthcare in 2023

By: Eric Clay, Security Researcher

Introduction: Analyzing Cybercrime Targeting the Healthcare Sector

The cybercrime ecosystem continues to reach new heights of organization, coordination, and sophistication. Every year, cybercriminals develop and use new tools, which are increasingly commoditized and sold in as-a-service business models. The rapid advancement in cybercrime poses significant challenges for healthcare cybersecurity professionals.

Healthcare is also one of the most targeted sectors by threat actors. Patient data fetches a premium on the dark web due to its potential use in medical fraud, creating a lucrative target for criminals. In addition, many healthcare organizations may be under additional pressure to pay ransoms in order to maintain the availability of mission-critical systems.

This report will examine the impact of cybercrime on the healthcare sector. We will leverage more than:

- Seven years of archived data from Tor
- 21 million stealer logs
- Thousands of posts on top-tier dark web forums

To better understand how cybercriminals are targeting healthcare and how the threat landscape is shifting for healthcare organizations.

Section I: Stealer Logs, SSO, and the Emerging Threat to Healthcare will focus on infostealer malware infections and healthcare organizations. We'll cover the infostealer lifecycle, stealer logs, and single sign-on credentials before finally analyzing stealer log data from more than 800 healthcare organizations.

Section II: Initial Access Brokers, the Dark Web Hacking Economy, and Healthcare will focus on initial access brokers selling privileged access to healthcare organizations on dark web forums.

Section III: Healthcare and Ransomware: Key Trends 2022 and 2023 will cover key trends involving ransomware and healthcare.

The CISO's Perspective on Cybercrime Risk

Ransomware attacks against healthcare organizations have increased by more than 100% at an annualized rate in 2023. This growth is occurring against the backdrop of an increasingly sophisticated cybercrime ecosystem, with more than 50 ransomware groups operating.

A variant of malware called infostealer is resulting in hundreds of thousands of corporate credentials being distributed on the dark web and Telegram, with an estimated 20% of healthcare organizations affected in the past 6 months. We rate it as highly likely that stealer logs are one of the key drivers of the increase in ransomware attacks. Implementing a continuous threat exposure management platform to automatically detect and remediate high-risk exposure is an essential step in creating a secure environment.

Cybercrime & Healthcare: Major Statistics

- 19.4% of healthcare organizations have had leaked credentials containing corporate access distributed on the dark web and Telegram in the past six months. In many cases, these credentials enabled access to essential services, including secure email, single sign-on environments, active directory, patient records, and even surgery centers.
- Initial access brokers have sold privileged IT access to six healthcare organizations in the past 12 months. Access to three pharmaceutical companies, two undefined healthcare organizations, and a large medical device manufacturer was sold during this time. Threat actors most commonly sell domain admin privileges with VPN or RDP access.
- Stealer logs containing access to corporate single-sign-on applications are a significant and growing risk. Flare identified more than 300,000 credentials to corporate SSO applications in a data set of more than 21 million logs.
- Ransomware attacks against healthcare organizations are up 144% on an annualized basis in 2023, representing a significant and rapid expansion in data extortion ransomware tactics

Section 1: Stealer Logs, SSO, and the Emerging Threat to Healthcare

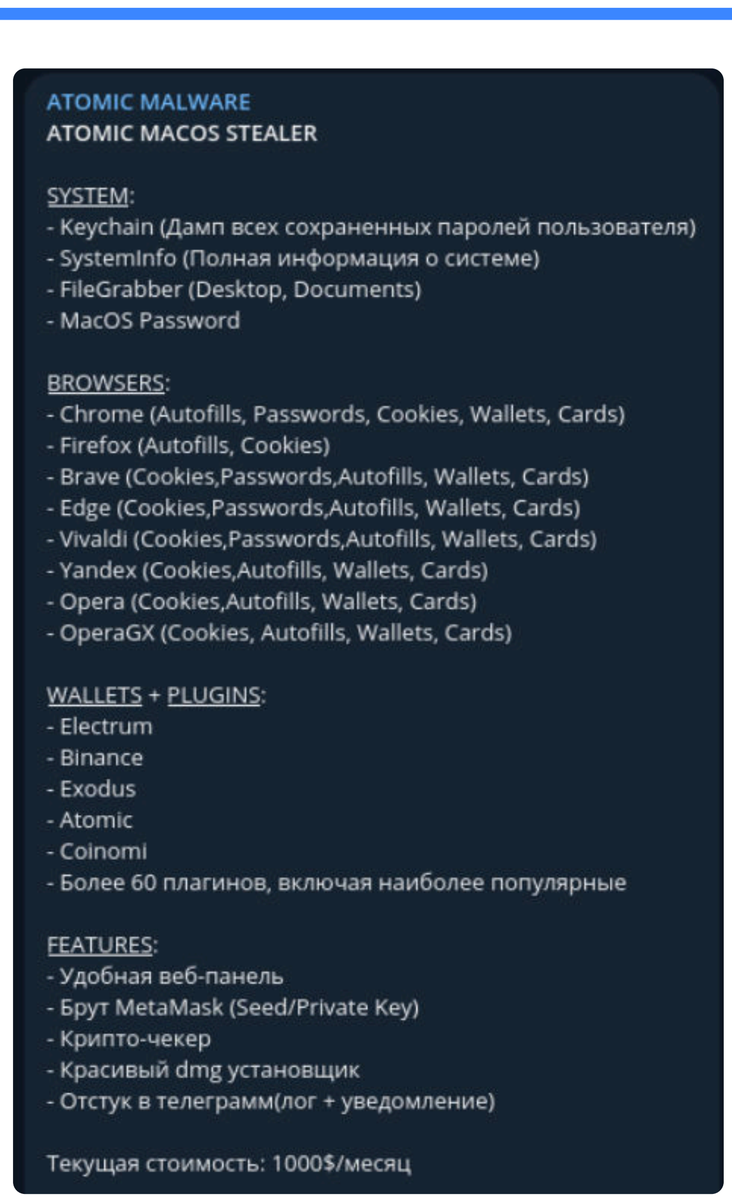
Stealer logs represent one of the most high-risk vectors for organizations today. Infostealer malware infects computers and extracts the browser fingerprint with all of the saved passwords in the browser including active session cookies. Threat actors then package thousands of individual logs together in “log files” which are distributed across public and private paid illegal telegram channels.

Key Findings on Stealer Logs and Healthcare

- **19.4%** of healthcare organizations surveyed had an infostealer infection with access to corporate credentials in the past 6 months. **9.6%** of organizations had two or more stealer logs with unique corporate access posted.
- Access found in the logs included credentials and session cookies to **ADFS, SSO Applications, Citrix, VPN, RDP,** and dozens of other internal resources.
- We rate it as **highly likely** that stealer logs with access to corporate environments are a primary vector for ransomware groups and initial access brokers.

These findings were particularly alarming due to the dramatic increase we are seeing in ransomware and cybercrime year over year. Creating an efficient internal solution for the rapid detection and remediation of stealer logs with corporate access is likely one of the highest ROI activities a security team can undertake in 2023.

These findings also closely parallel results from a research report we did several months ago, in which we found thousands of corporate credentials in a stealer log sample of 21,000,000.



Threat actor advertises for Atomic Malware

Public Telegram Channels

Threat actors share hundreds of thousands of new logs in public channels every week, containing millions of unique credential pairs. (Each log contains all of the credentials saved on a single host.) Threat actors post these logs directly to public Telegram in order to "advertise" private paid rooms.

Private Telegram Channels

In private paid-access Telegram channels, threat actors offer exclusive access to more extensive and valuable logs containing a higher volume of logs with access to corporate IT environments. These channels often require a subscription fee or membership, attracting individuals who are willing to pay for more targeted and specialized information.

Threat actor on Telegram advertises two forms of accessing RedLine stealer malware

Russian Market

Russian Market operates as a dark web marketplace with automated purchasing and listing of logs. Threat actors can browse for logs with specific credentials and purchase a log that looks promising for as little as $10.

Most infostealer malware infections are targeted at individuals rather than companies. Infostealers are primarily distributed through cracked software, malvertising, and phishing. Threat actors are looking for easy ways to steal banking credentials, saved credit card numbers, VPN accounts, Netflix accounts, and other easily accessible SaaS applications.

However, in many cases, threat actors end up picking up **corporate credentials as part of their distribution, and these can be extremely high-risk.** To better understand the presence of corporate healthcare credentials in stealer logs, we manually sorted through stealer logs with access to almost 1,000 healthcare organizations to identify logs that likely contain corporate access.

Urgent Recommendations for Healthcare Organizations

We recommend that healthcare organizations adopt the following policies and measures immediately.

- Monitor Russian Market and Telegram for stealer logs that may contain access to corporate IT environments and SaaS applications.
- Place significant restrictions on BYOD policies.
- Utilize a password manager and create a policy against saving credential sets in the browser.
- Reduce TTL for session cookies for corporate applications in order to reduce the risk of logs bypassing 2FA controls present.

Section 2: Initial Access Brokers, the Dark Web Hacking Economy, and Healthcare

Initial access brokers specialize in gaining and selling access to corporate IT environments. They operate across multiple dark web forums, including Exploit, XSS, Ramp, and Breach Forums, and list corporate IT access in auction-style format.

These brokers play a significant role in the dark web hacking economy by facilitating unauthorized access to sensitive information. The healthcare industry is particularly vulnerable to these attacks, as healthcare companies hold valuable patient data that can be exploited for financial gain.

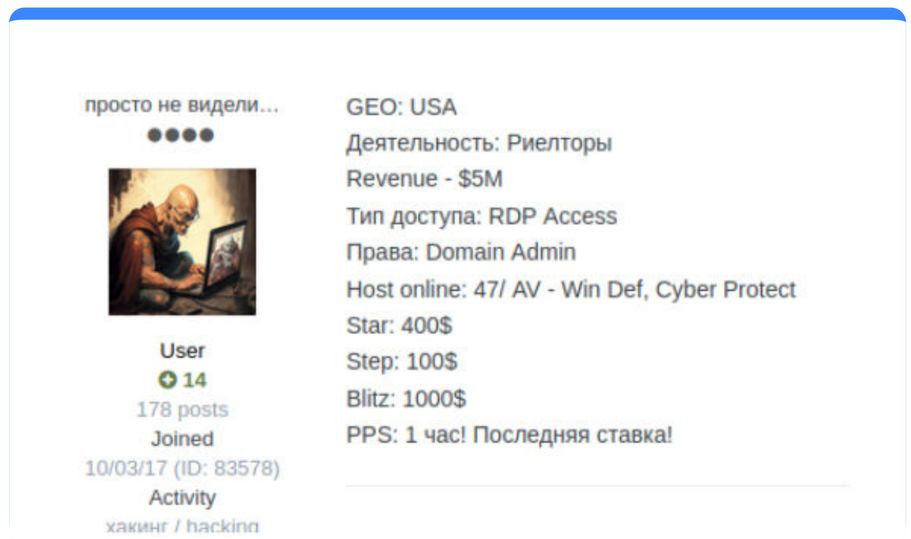
Key Findings about Initial Access Brokers

- Across a limited sample size of access broker posts, we found access to six healthcare organizations being sold in the past six months.
- Access was sold to three pharmaceutical companies, two undefined healthcare companies, and one medical practice organization.
- RDP and VPN access are the most common types of access sold, with domain admin being the most common level of access.
- The U.S. was the most targeted country, with 36% of IAB posts containing access to U.S. companies.
- We rate it as highly likely that IAB access is routinely used by **ransomware groups.**

The Anatomy of an Initial Access Broker Post

Many initial access broker posts follow an extremely similar format, creating a consistent set of features that we can measure to better understand the IAB economy.

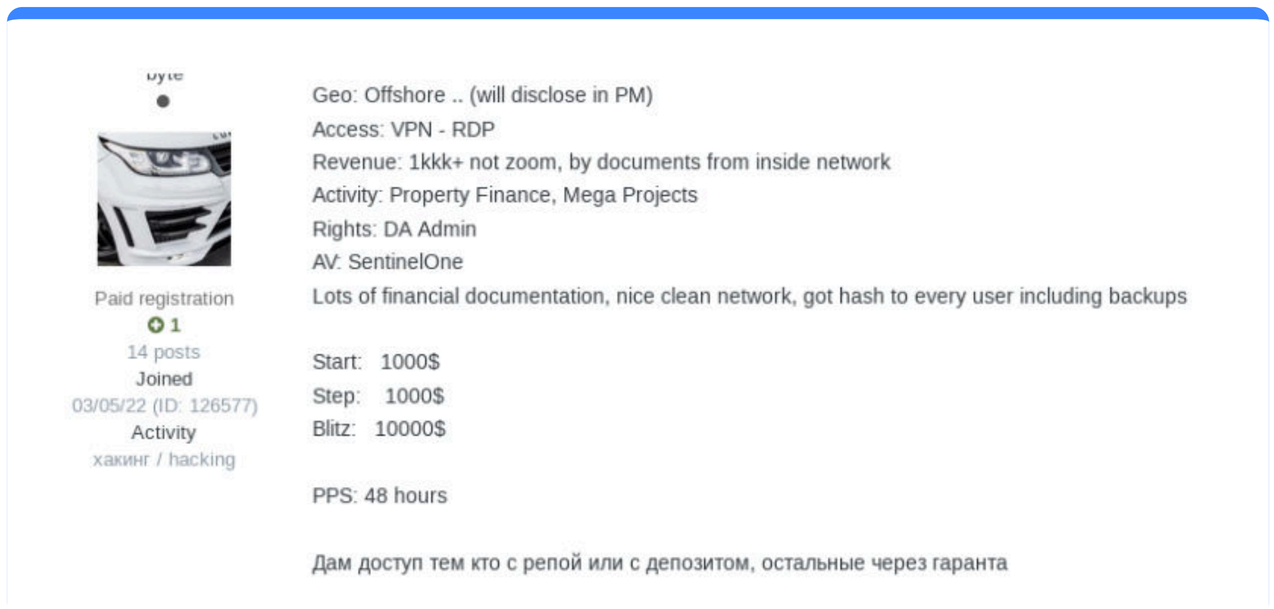
- **Access Type/Тип доступа:** Describes the type of access obtained, most commonly RDP or VPN access.
- **Activity/Деятельность:** Describes the industry or activity of the victim company. Finance, Retail, and Manufacturing are the three most common targets.
- **Rights/Права:** Describes the level of privileges obtained.
- **Revenue:** Describes the revenue of the victim company, often obtained from U.S. based data providers publicly available online.
- **Host Online:** Often describes the number of hosts from the victim and sometimes includes antivirus and security systems in place.
- **Start:** The starting price of the auction.
- **Step:** The bid increments.
- **Blitz:** The buy it now price.



IAB post advertising RDP access for a U.S.-based organization

We rate it as highly likely that ransomware groups are using initial access broker posts as a key method for gaining access and persistence to corporate healthcare IT systems. We've seen many examples like that pictured on the right where threat actors have specifically called out the absence or compromise of backup and recovery systems in initial access broker posts.

This is a telling indicator that the access broker likely expects the access being sold to be used for data encryption ransomware attacks.



IAB post advertises RDP access to an organization along with financial documentation

Section 3: Healthcare and Ransomware: Key Trends 2022 and 2023

Ransomware has been a scourge for healthcare organizations in recent years, but the past 12 months has seen a particularly precipitous increase. To measure the number of ransomware victims, we chose to focus on victims that had their data published from January 1, 2022 to the end of June 2023.

What is Data Extortion Ransomware?

Data extortion ransomware is a recent innovation in which the ransomware group exfiltrates data and demands a ransom. These ransomware attacks involve threats of publishing or selling the stolen data if the ransom is not paid. This tactic adds an additional layer of pressure on victims, particularly in industries like healthcare where sensitive patient information is at stake. If the victim doesn't pay, their files are leaked on dedicated ransomware blogs.

Key Findings about Ransomware and Healthcare Organizations

- Ransomware attacks against healthcare organizations increased at an annualized rate of 144% from 2022 to 2023.
- Lockbit and Cl0p continue to be two of the most prolific groups through the end of June 2023.
- Some ransomware groups claim that they won’t attack healthcare organizations out of principle, although the existence of affiliates make it challenging to abide by this in practice.

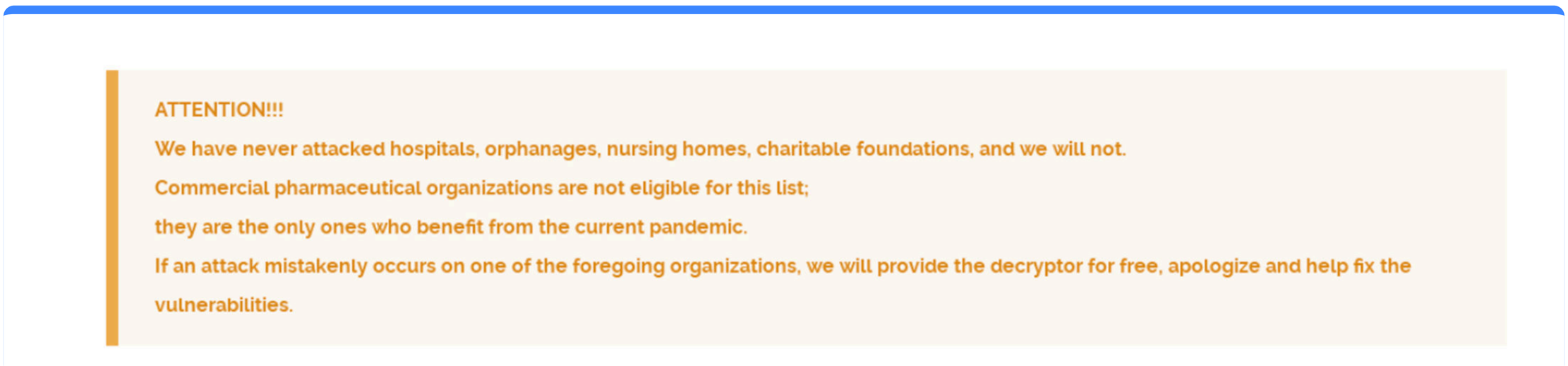
In our analysis of ransomware attacks against healthcare organizations for the years 2022 and the first half of 2023, specific ransomware groups have been identified as particularly active. These groups not only disrupt healthcare services but also put patient data at risk. The top five ransomware groups most responsible for these attacks are:

- **LockBit**: With 27 documented attacks, LockBit stands out as the most active group targeting healthcare organizations. The group is known for its sophisticated attack techniques and has been a significant threat to healthcare providers.
- **CL0P Leaks:** Accountable for 10 attacks, CL0P Leaks is another group that has focused its efforts on healthcare entities. Their attacks often involve leaking sensitive information if the ransom is not paid.
- **Royal:** Royal has been involved in eight attacks against healthcare organizations. Their modus operandi typically includes encrypting critical files and demanding a ransom for the decryption keys.
- **ALPHV:** This group has executed seven attacks against healthcare organizations. ALPHV often exploits vulnerabilities in healthcare systems to deploy their ransomware.

- **Karakurt:** Also responsible for seven attacks, Karakurt is known for its targeted approach. They often use spear-phishing campaigns to gain initial access to healthcare networks.

Group Variance and the Ethics of Ransomware

Data extortion ransomware continues to be a significant challenge for healthcare organizations in 2023. One of the most interesting aspects of doing research on ransomware groups is just how much they vary in their approaches. For example the group CL0P claims that they don't target healthcare organizations and charities out of a sense of ethical obligation.



Post from CL0P that states they will not and have not attacked hospitals, orphanages, nursing homes, and charitable foundations

Other groups such as BianLian make absolutely no distinction between victims and have been known to directly target children's hospitals, medical clinics and other critical infrastructure.

In some examples we've seen ransomware groups describe themselves as "pentesters," "ethical hackers" and their activities as "pentesting after the fact" in an effort to create a veneer of respectability and ethical consideration to their activities.

Cybercrime and Healthcare: Conclusions from Analysis

Healthcare is one of the most at-risk industries from threat actors. Malicious actors have enormous motivation to target healthcare companies given the wealth of data that they hold and the value of that data. In many cases healthcare companies may be incentivized to pay ransoms and deal with cybercriminals rather than accept weeks of downtime or loss and exposure of sensitive patient data.

The trends are clear; infostealer malware infections containing access to SSO credentials and healthcare organizations are a significant threat vector, at the same time ransomware groups and initial access brokers specifically target healthcare. Worryingly, all signs point to these trends continuing to worsen in 2024.

Continuous Threat Exposure Management as an Opportunity

Implementing robust external monitoring can help mitigate a significant degree of risk. Continuous threat exposure management represents an opportunity for organizations to proactively detect and remediate high-risk exposure that leaves them vulnerable from threat actors.

Preventing infostealer malware infections is a key part of the battle, but building and integrating a security program focused on the principle of defense in depth is even more important. Organizations that build comprehensive approaches to prevent large scale loss of confidentiality, integrity, or availability will find the most success in risk mitigation.

About Flare

Flare is the proactive external cyber threat exposure management solution for organizations. Our AI-driven technology constantly scans the online world, including the clear & dark web, to discover unknown events, automatically prioritize risks, and deliver actionable intelligence you can use instantly to improve security. Our solution integrates into your security program in 30 minutes to provide your team with actionable intelligence and automated remediation for threats across the clear & dark web.

Want to learn about how Flare can support your organization with monitoring for external threats?

Free Trial **Book a Demo**

flare.io

hello@flare.io