flare

Infected Devices & Healthcare in 2023

Table of Contents

Infected Devices & Healthcare in 2023 ____ 3
Understanding an Infected Device Listing ____ 3
    A Quick Sidebar on Genesis Market ____ 4
Concluding Thoughts ____ 8

Infected Devices & Healthcare in 2023

Infostealer malware and infected device markets are one of the most critical cybersecurity challenges and opportunities for organizations in 2023. Threat actors are increasingly employing variants of **"stealer malware"** to include RedLine, Raccoon, Vidar, among dozens of others. These remote access trojans (RATs) infect a host, extract sensitive information such as the device's OS, IP address, browser fingerprint (to include saved passwords), and browser history. Data is then exfiltrated to dedicated command and control infrastructure and sold on specialized Dark web marketplaces, **illicit Telegram channels**, and in some cases, clear web sites.

The price of an infected device varies based on several factors including geographic location, number of unique logins saved, and whether the device also has saved financial information like credit card data or banking logins. But one of the most critical aspects in determining pricing is whether the device has saved credentials that include corporate logins such as VPNs, corporate password managers, intranets, websites, and other data that can be used to compromise an organization's environment.

Infected devices are a particularly relevant threat for healthcare organizations. 2021 and 2022 saw healthcare companies ranging from hospitals to elder care facilities increasingly targeted by threat actors given the criticality of their mission and the value of PHI on the dark web. We wanted to conduct a quick investigation into one of the most prominent infected device markets, Genesis Market, to better understand:

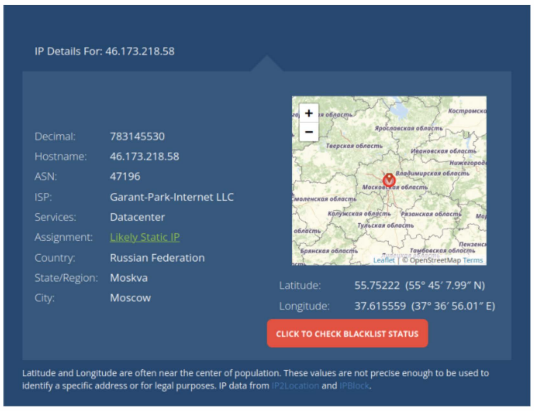
- What percentage of healthcare organizations with more than 500 employees have an infected device for sale on Genesis Market that contains access to a corporate system or service?
- What are the price differences in infected devices for sale (average infected device price with or without corporate healthcare access))?
- What percentage of healthcare organizations have more than one, three, or five, infected devices currently for sale on Genesis Market?

Quick Tip: A browser fingerprint is a 1:1 copy of a browser that includes saved cookies, settings, and other data which allows websites to uniquely identify the user. By mimicking a browser fingerprint, threat actors have the potential to bypass 2FA controls in cases where "remember this browser" has been selected.

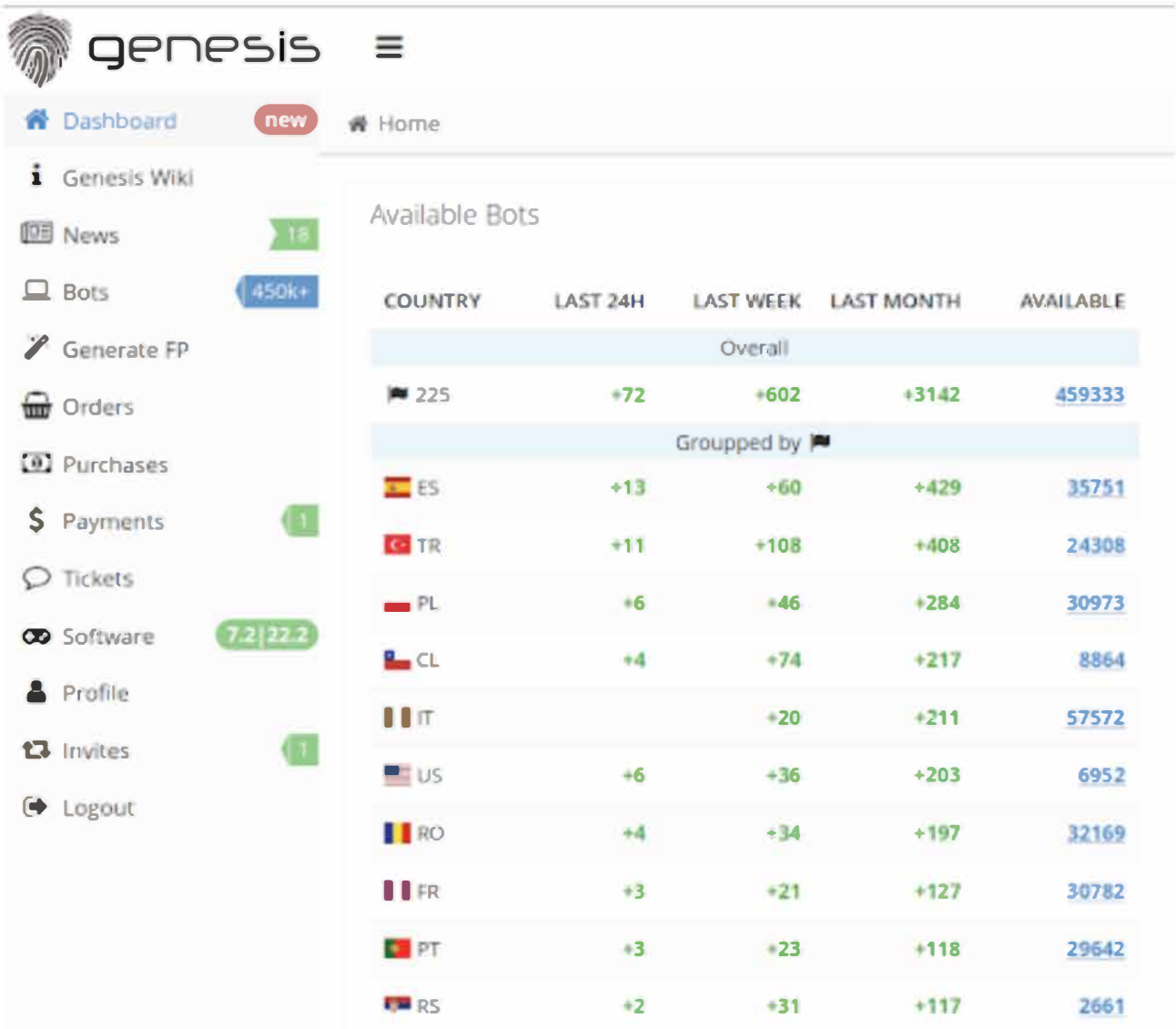
Understanding an Infected Device Listing

Before we dive into statistics, it's worth taking a moment to understand **how infected devices are sold.** The specific data being sold varies based on the marketplace that it is being sold on. For example, some marketplaces may provide a partial IP address while others provide a full IP. For our purposes we will examine a typical listing on Genesis Market:

A Quick Sidebar on Genesis Market



Genesis Market is an illicit market that specializes in selling infected devices, and is hosted in Russia***. The market is set up for usability and includes a simple solution that allows even unsophisticated threat actors to download and mimic the browser fingerprint of a victim. Genesis includes the ability to sort devices by country, contact 24/7 customer support, and has extensive support documentation available. Genesis is a prime example of the increasing commodification of cybercrime, in which highly specialized threat actors each carry out individual, niche roles.

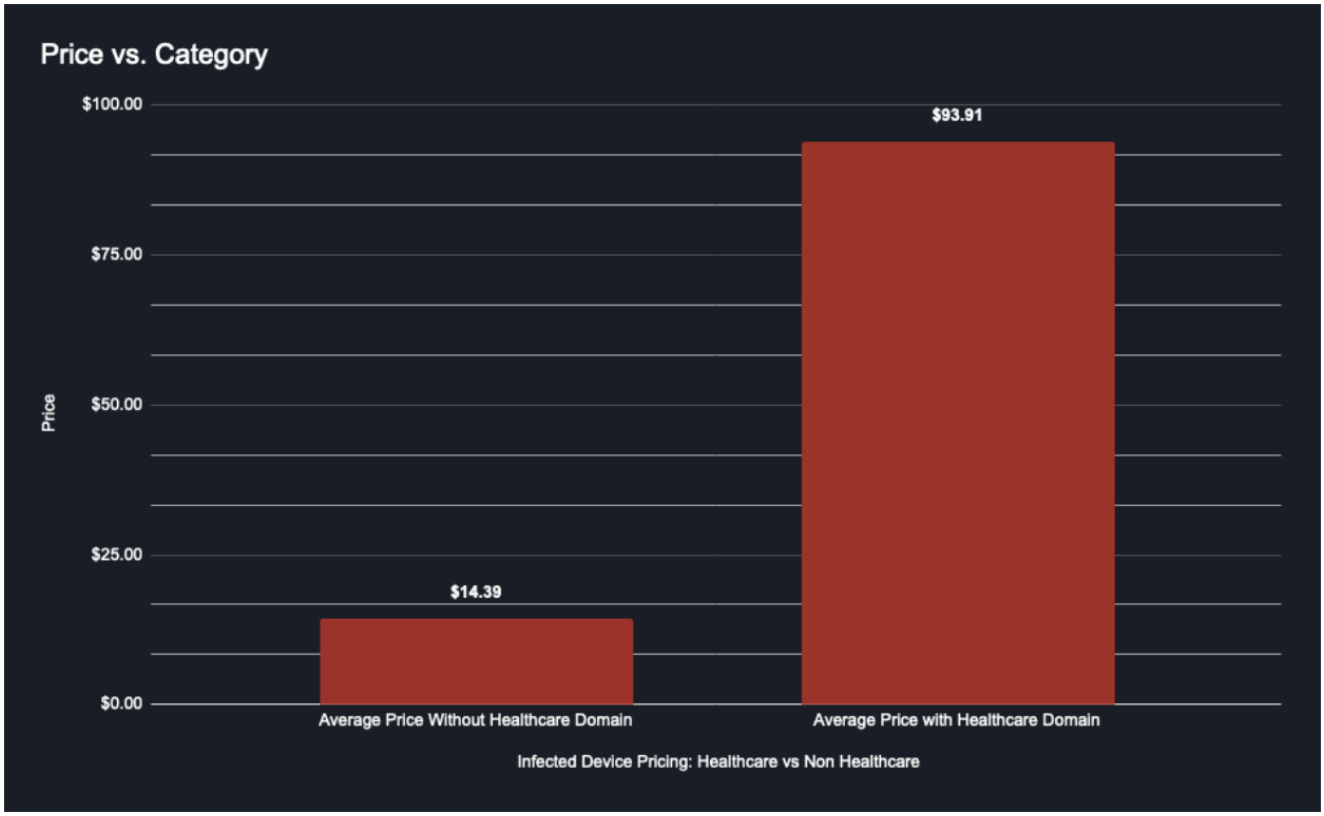


***In 2023, law enforcement seized and shutdown the public-facing clear web site for Genesis Market as well as their public-facing databases. However, research has been found that leads us to believe that this market is still fully operational on the dark web and likely within illicit Telegram channels associated with the market.

To perform this analysis, we identified a random selection of 100 healthcare organizations that have more than 500 employees. We then matched the organization's primary domains (excluding subdomains) against a sample of Flare's database of infected devices listed on Genesis market (88,000 current device listings).

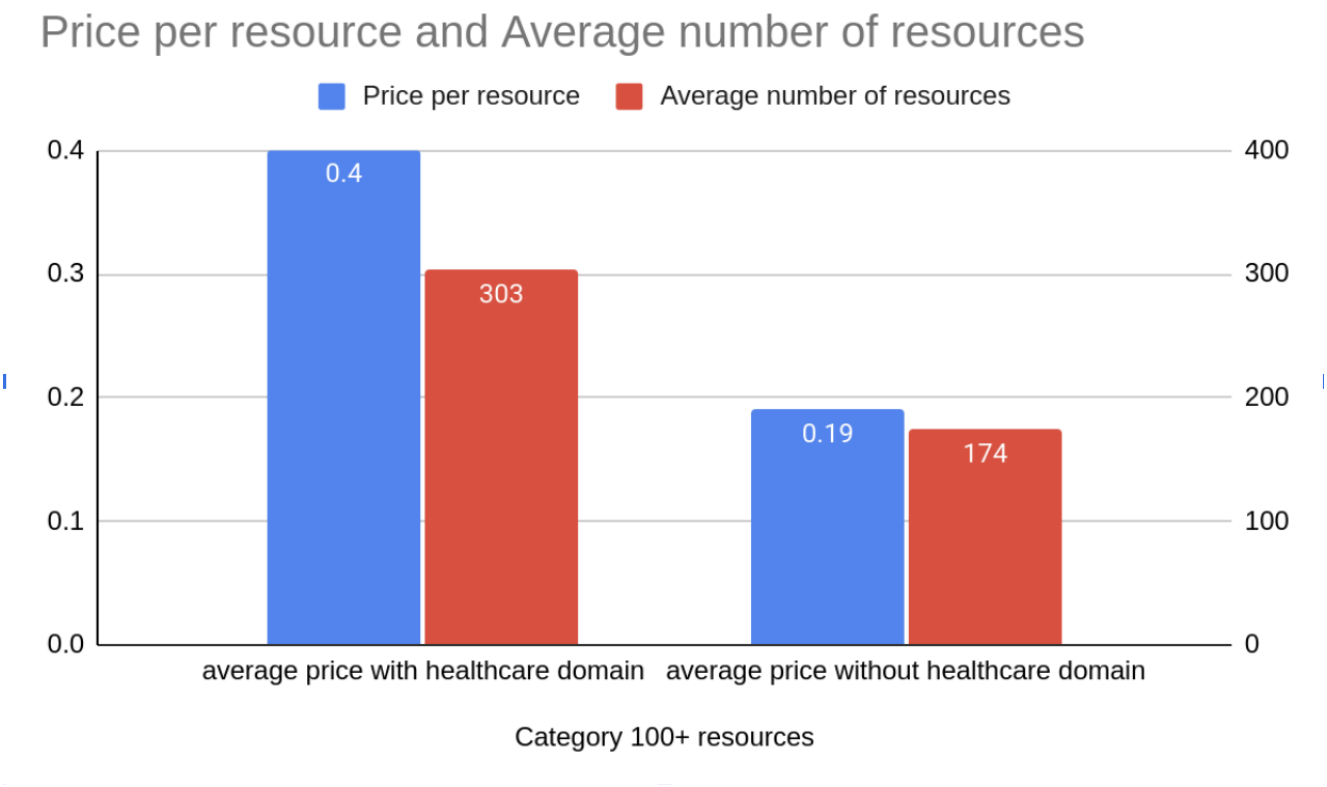
The first and most interesting data point that emerges is that threat actors **clearly place a high-value on domains with access to corporate healthcare environments.** Genesis market listings that contained high-value healthcare access were sold for an average of **$93.91** compared with a global average of market listings without high-value healthcare access at $14.47.

With only this information, it would seem that infected devices with access to healthcare domains were an average of 648% more valuable than those without. However, the number of domains for sale (referred to as "resources") also heavily impacts their price; we wanted to consider the possibility that devices for sale with access to healthcare specific domains might just have more resources, artificially making it look like the price was higher.



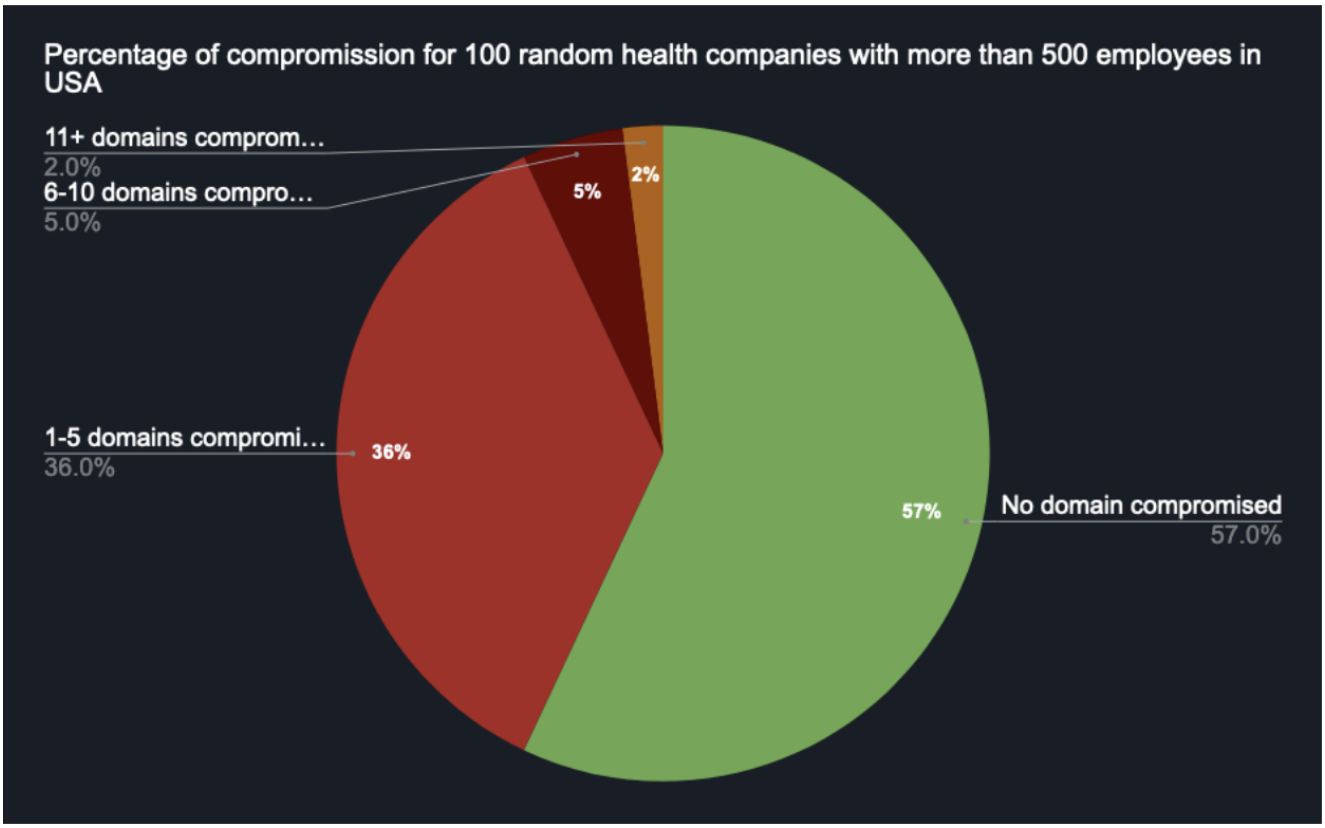
This major difference could only be caused by the number of resources available in bots that contain healthcare domains. In the 85 bots with one of our 100 healthcare domains included, the average number of resources included in the listing was 256. In the 81,769 bots without healthcare domains, the average number of resources is 60. By only looking at the number of resources, the factor of four would explain the price difference. However, this doesn't paint the whole picture.

The next graph illustrates the price per resource and the average number of resources for bots with more than 100 resources for two categories: with healthcare domains and without healthcare domains.



Interestingly, the price per resource is slightly over twice as much for bots with healthcare domains than those without. This reinforces the findings from the global price analysis presented earlier. Therefore, although bots with healthcare domains have more resources, the price per resource is higher suggesting that threat actors (both buying and selling) understand the value of having access to healthcare credentials.

The next analysis we wanted to perform was to identify what percentage of our randomly selected healthcare companies' access to corporate domains are currently for sale on Genesis Market. This can help us contextualize the threat that the infected devices pose, particularly since the ease of use of Genesis Market makes it easy for threat actors to bypass 2FA and MFA controls thanks to browser fingerprinting and the following impersonation.



43% of our sample of 100 healthcare organizations either had an active compromise affecting a corporate account or customer account.

Even more concerningly, 5% of healthcare organizations had between 5-10 bots with access to domains indicating high-risk access with 2% of organization's having more than 10. Having an infected device for sale with access to corporate resources indicates that threat actors have potential access to your organization's environment, and should be considered an Indicator of Compromise.

Concluding Thoughts

Genesis Market and infected device markets more broadly represent both a critical threat and opportunity for information security teams in 2023 and beyond. We see hundreds of thousands of new devices being listed on a monthly basis across dozens of sources including illicit Telegram channels, 2easy market, Russian Market, and Genesis Market, with many containing privileged logins to corporate resources.

The proliferation of stealer malware and commoditization of infected device listings also represents a significant opportunity for companies to disrupt the dark web supply chain. Defenders can:

- Detect attack infrastructure such as lookalike domains being set up
- Automatically monitor markets & Telegram channels devices for sale that have access to corporate domains and subdomains
- Monitor Initial Access Broker forums where access to your organization may be sold off.

About Flare

Flare's SaaS platform sets up in 15 minutes and automates monitoring for high-risk exposure across the clear and dark web. Our platform can be easily configured to automate monitoring across dozens of illicit Telegram channels and infected device markets to detect devices for sale with access to corporate subdomains. H-ISAC Members can access Flare for free for 1 year through our community services offering.

Want to learn about how Flare can support dark web monitoring for leaked credentials?

Free Trial **Book a Demo**

flare.systems
hello@flare.systems