BLACKFOG™

The 3 Biggest Cybersecurity Mistakes That Organizations Make:

A FORMER HACKER'S PERSPECTIVE



Contents

Overview 3

Neglecting Comprehensive Attack Surface Management 4

Losing Track of Data Assets and Their Locations 5

Missteps in Cyber Threat Intelligence Practices 6

Frequently Asked Questions 10

In this article, a former hacker provides insightful perspectives on the three biggest cybersecurity mistakes organizations make: neglecting comprehensive attack surface management, losing track of data assets, and missteps in cyber threat intelligence practices. He explains why these oversights occur and how they jeopardize security, offering real-world examples like openly coordinated attacks.

1

Neglecting Comprehensive Attack Surface Management

When discussing an organization's infrastructure, most people typically think of the website and on-site devices. However, the attack surface is often much larger than that, including subdomains, servers, services, web applications, credentials, shared infrastructure like hosting, and employees.

From an attacker's viewpoint, a larger and more varied attack surface is easier to hack. The attack surface frequently includes third-party entities integrated within the organization, and most assets are subject to dynamic content change. For example, server services/daemons may become outdated and need patching, or subdomain codebases may change.

Considering the complexity and size of these assets, manually securing all of them is virtually impossible. So, it's important to implement an attack surface management solution or comprehensive strategy. This strategy should manage all assets, prioritize risks, and identify what requires patching.

To give you an example, if a new vulnerability in Apache2 was discovered tomorrow, could you identify all assets running that service, their versions, and who has access to them? Questions like these are crucial for anyone responsible for an organization's cybersecurity posture.

2

Losing Track of Data Assets and Their Locations

This point somewhat relates to the previous one.

Most organizations have no idea what data they're managing and where it's stored. This lack of data asset inventory and mapping creates significant cybersecurity risks, making organizations vulnerable to data breaches.

For example, a typical organization may utilize on-premises servers and storage, cloud-based infrastructure (IaaS/PaaS/SaaS), bring-your-own-device (BY
OD) policies permitting storage on mobile devices, and local storage on user devices including laptops and desktops, not to mention external hard drives, USB drives, and other removable media.

With such a complex IT environment, many organizations have very limited insight into:

- What types of sensitive data exist across the organization (customer data, financial data, intellectual property, etc.)
- Exactly where that sensitive data is stored and transmitted
- The volumes of this data and how it is growing over time
- Who has permissions and access to that data
- How that data is protected wherever it travels or resides

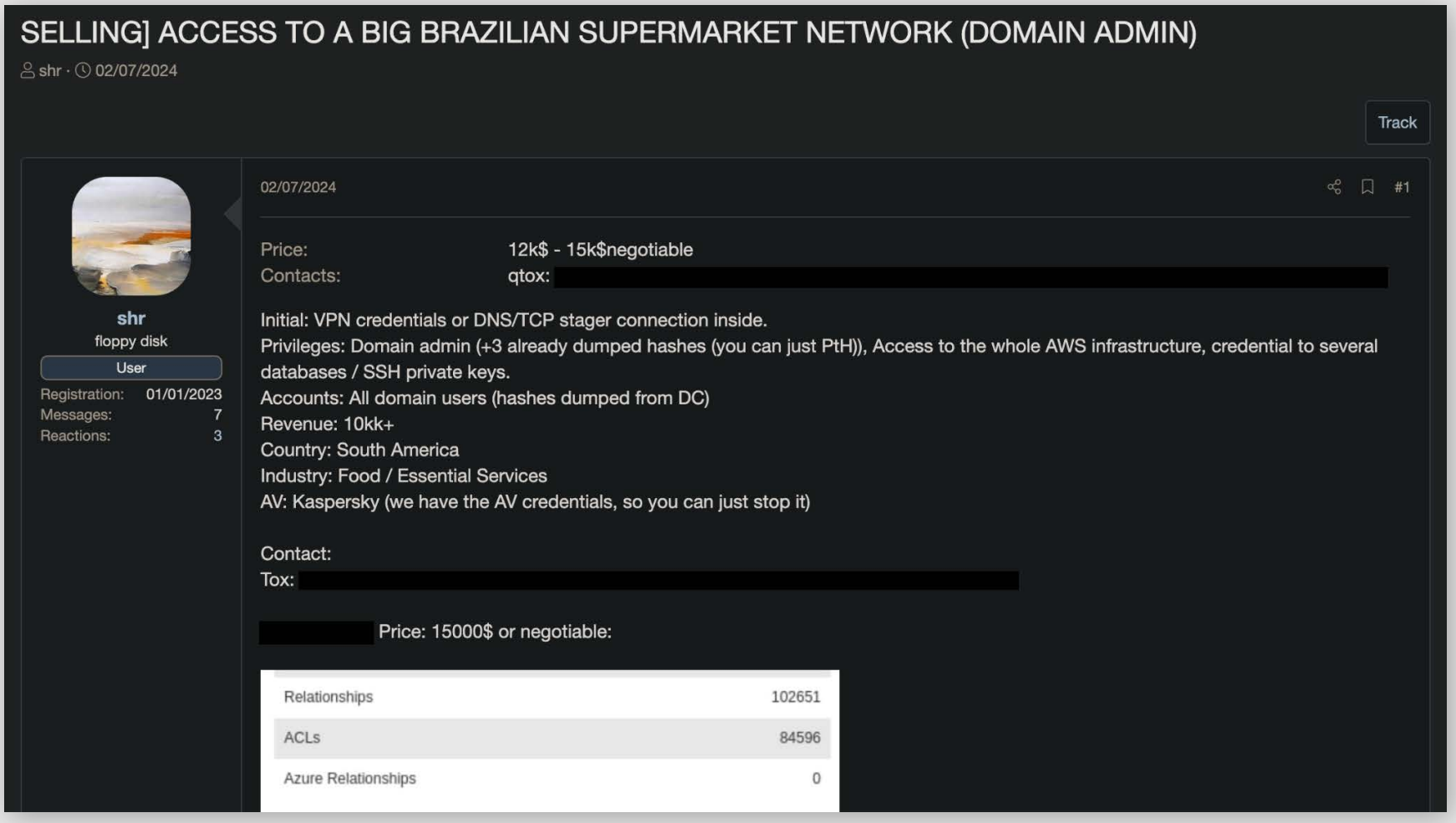
Because of this, it becomes extremely difficult to implement cybersecurity controls like access restrictions, activity monitoring, encryption, etc., when the organization itself lacks clarity on what data exists and where it is located at any given time.

3

Missteps in Cyber Threat Intelligence Practices

A lot of organizations invest heavily in cyber threat intelligence (CTI), but their approach is often misguided. The first step to effective CTI is a realistic evaluation of your risk profile and most likely attack vectors.

Most organizations focus on researching advanced threats such as advanced persistent threats (APTs), which are typically relevant to large corporations. However, smaller organizations are more susceptible to ransomware and opportunistic types of cybercrime. Additionally, many CTI teams prioritize monitoring obscure hacking forums on the dark web, overlooking openly coordinated attacks on platforms like Telegram, Discord, and Clearnet sites. However, for meaningful intelligence, organizations need insiders embedded on these platforms that are frequented by cybercriminals.

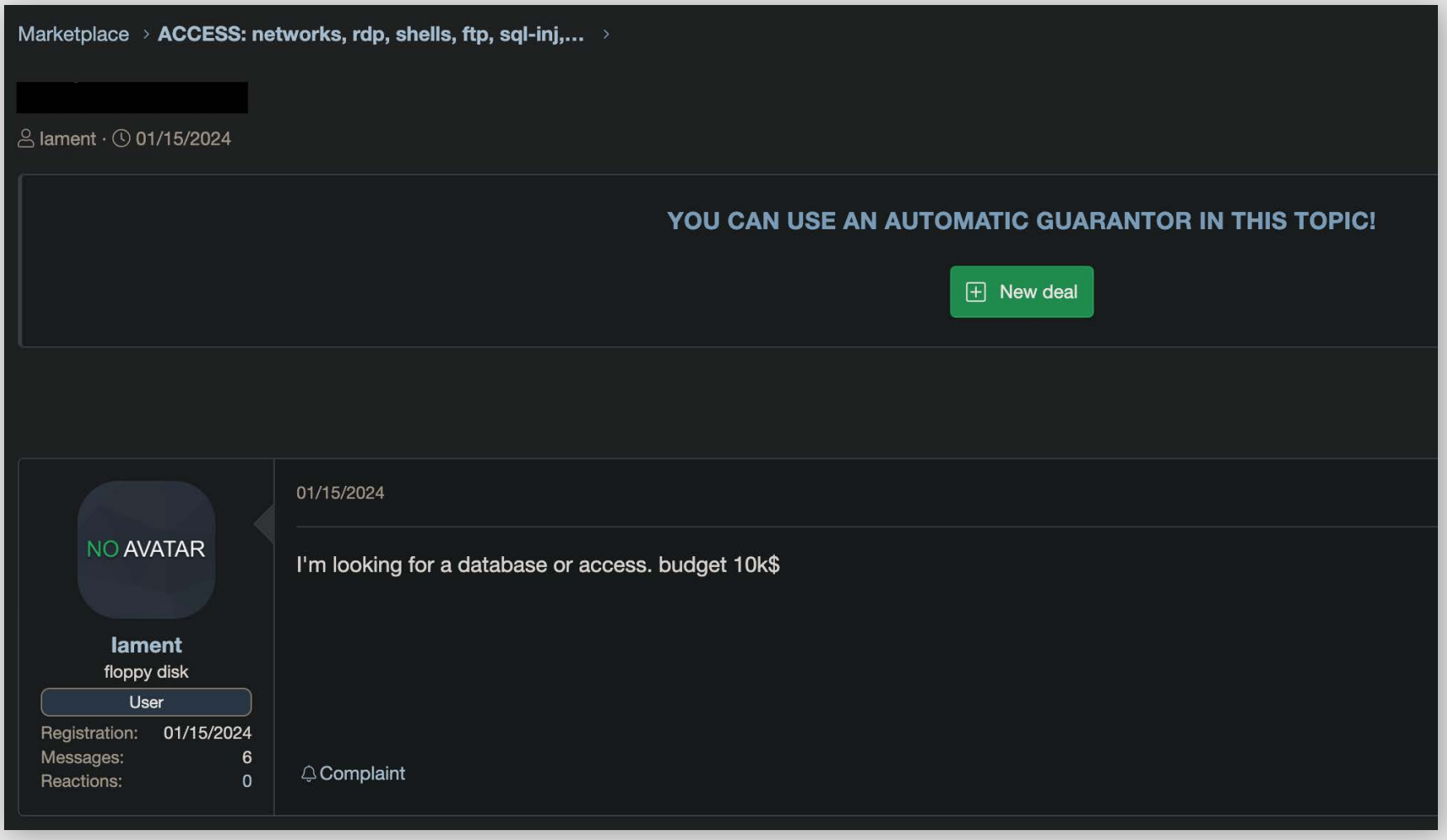


To give you an example, take a look at this thread that I found on a Clearnet cybercrime forum. It's an access broker selling access to a Brazilian supermarket's network.

In the thread, they have posted many screenshots with internal information. By looking at all the information that they've made publicly available, it's possible to narrow the possibilities down to fewer than five potential organizations.

The point I'm trying to make here is that access brokers and cybercriminals openly sell data and access to organizations, sometimes even posting the name of the organization they've compromised.

Does the Brazilian supermarket in question know that someone has breached their network and is selling it on a cybercrime forum? Probably not.



Here's another example. A cybercriminal is looking to purchase access to a major defense contractor, which we'll refrain from naming for privacy purposes.

Now, I don't know about you, but if I were part of the cybersecurity team at this organization, I would be engaging with this individual and trying to coax additional information out of them to see what they plan to do with the database or access they're seeking. It could open up a whole investigation.

Does the buyer already have someone lined up who's interested in the database or access? Who knows?

The point that I'm trying to make is that this isn't a rare occurrence. If you position yourself on the correct forums and networks, hundreds or even thousands of

these transactions are taking place on a daily basis, and the information is already out there to be gathered as intelligence.

Effective CTI relies less on technical measures and more on proactive social engagement, such as directly interacting with and influencing cybercriminals on their own platforms. This is similar to undercover policing, rather than merely reacting to crimes.

However, quantifying the value of such engagement is challenging. Teams might wait indefinitely to disrupt potential attacks that meet their criteria. Nevertheless, realistic threat models tailored to specific organizations can help direct resources toward likely attack vectors.

The key aspects of CTI, in my opinion, involve alignment with specific risk profiles, direct infiltration of cybercrime ecosystems for insight, and a balance of technical skills with soft skills. Most organizations still overlook these elements, favoring universal tech solutions and passive dark web monitoring.

FREQUENTLY ASKED QUESTIONS

Here’s some frequently asked questions that provide additional context:

1

Are smaller businesses actually easier to target or do large scale enterprises present more “holes” in their defenses?

There are two answers to this:

1. Smaller businesses can often be more vulnerable because they have less to invest in cybersecurity.

2. At the same time, large scale enterprises have massive attack surfaces which can sometimes span hundreds or even thousands of servers and applications.

If I had to choose based on one or the other, I would say that large scale enterprises are a lot easier to hack because there’s so much that has to be secured. Although contextual, sometimes small businesses might have a single website and less than 10 applications facing the internet which is really not that much at all.

2

What industry always falls short when it comes to cybersecurity and why do you think that is?

There are many industries that get targeted frequently. Healthcare, for example, faces ample attacks due to the valuable data managed within organizations. However, in terms of vulnerability, I would argue that government entities (e.g. .gov domains) are the most prominently exposed industry.

This stems from the expansive attack surface governments often possess combined with the talent and skill gap of the private sector. The private sector often offers larger salaries, drawing away top cybersecurity talent from the public sector.

Just touching on my previous point, if you search “site:gov ext:php” on Google, you will find millions of web pages running PHP. This single example demonstrates the sheer size of the government’s attack surface, encompassing tens if not hundreds of millions of potential entry points across their digital landscape. This massive landscape, coupled with talent shortages, leaves government systems profoundly exposed.

3

Will new reporting regulations help in the long term, or will they merely cause headaches and provide more opportunities for extortion from cybercriminals? For example, consider the case of BlackCat reporting MeridianLink to the SEC last year.

New reporting regulations will undoubtedly prove beneficial. I believe they will prompt key decision-makers in organizations to view cybersecurity as a necessity rather than an option. In the past, it was somewhat possible to conceal data breaches, but that is no longer viable. Incidents like the one involving BlackCat ransomware have always existed. We saw similar situations arise when GDPR was introduced a few years ago. However, the SEC ruling appears much clearer and more concise in its requirements, so enforcement is likely to increase.

Overall, I believe these regulations do more good than harm. Transparency allows consumers to take protective action at an individual level. It also places liability on breached organizations and, in cases of negligence, exposes them to legal consequences that they arguably deserve if they fail to follow proper security measures. While jolting at first, these regulations will cultivate a culture where cybersecurity receives the priority status it warrants moving forward.

BLACKFOG™

ABOUT BLACKFOG

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Our behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. Our cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

All contents copyright © 2024 BlackFog, Inc. All rights reserved. The BlackFog logo and name are trademarks of BlackFog, Inc. All other trademarks are the property of their respective owners.

Except as specifically stated herein, none of the material may be copied, reproduced, distributed, republished, downloaded, displayed, posted, or transmitted in any form without authorized, prior written permission from BlackFog, Inc. Permission is granted for you to make a single copy of this document solely for informational uses within your organization, provided that you keep intact all copyright and other proprietary notices. No other use of the information provided is authorized.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The information contained in this document represents the current view of BlackFog, Inc. on the issues discussed as of the date of publication.
