THREAT INTELLIGENCE SUMMARY 2025

OVERVIEW

01 How do threat actors get in?

The **most common attack vectors** involved **stolen credentials** and **exploited software vulnerabilities**. Notably, the majority (over 90 %) of documented exploited vulnerabilities targeted web applications rather than infrastructure elements. While **phishing** has dropped to the third spot, it **remains a significant threat** as attackers increasingly focus on stealing credentials or tokens instead of deploying malware.

02 Once they are in

Attackers are still using malware but are **increasingly relying on** so-called "**living off the land**" (LOTL) **techniques**, leveraging existing tools like Netcat, Telnet and others. Data from analyzed breaches suggest that, on average, 59.5 % of cases (ranging from 44 % to 75 % in various reports) employed LOTL-only techniques.

03 How to protect?

Effective protection requires a **layered security approach**: preventing attackers from getting in, limiting their options if they do, and slowing them down enough for your SOC to detect them. If all else fails, **having backups** of **mission-critical data** and **tested recovery procedures** is essential to quickly resume operations without having to pay a ransom to the attacker.

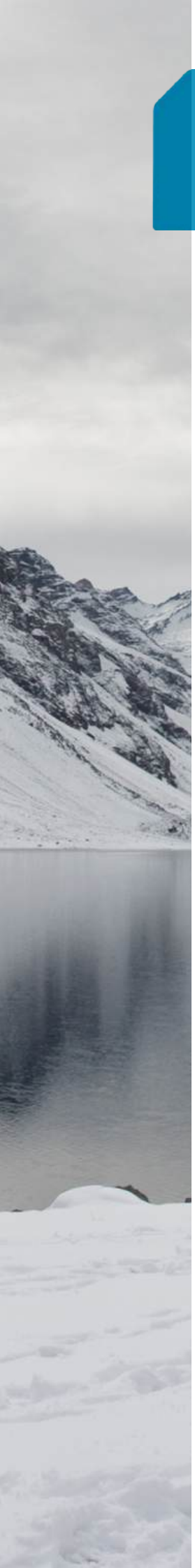
04 Ransomware

Ransomware remains a **major threat**, driven by financial motives. While 67 % of attackers decrypt data after payment, the average ransom demand of $237,500 USD is just part of the cost. Victims also face service disruptions and must invest in security to prevent re-encryption. **Consider** making **investments in security** proactively, **before an attack**. It is far more effective than reacting under pressure.

05 Who is being targeted?

Financial motivation drives most of **attacks**, targeting businesses where disruption leads to monetary gain.
Subscription services, e-commerce, and logistics companies are among the most affected due to their likelihood of paying **ransoms**.

comma_0

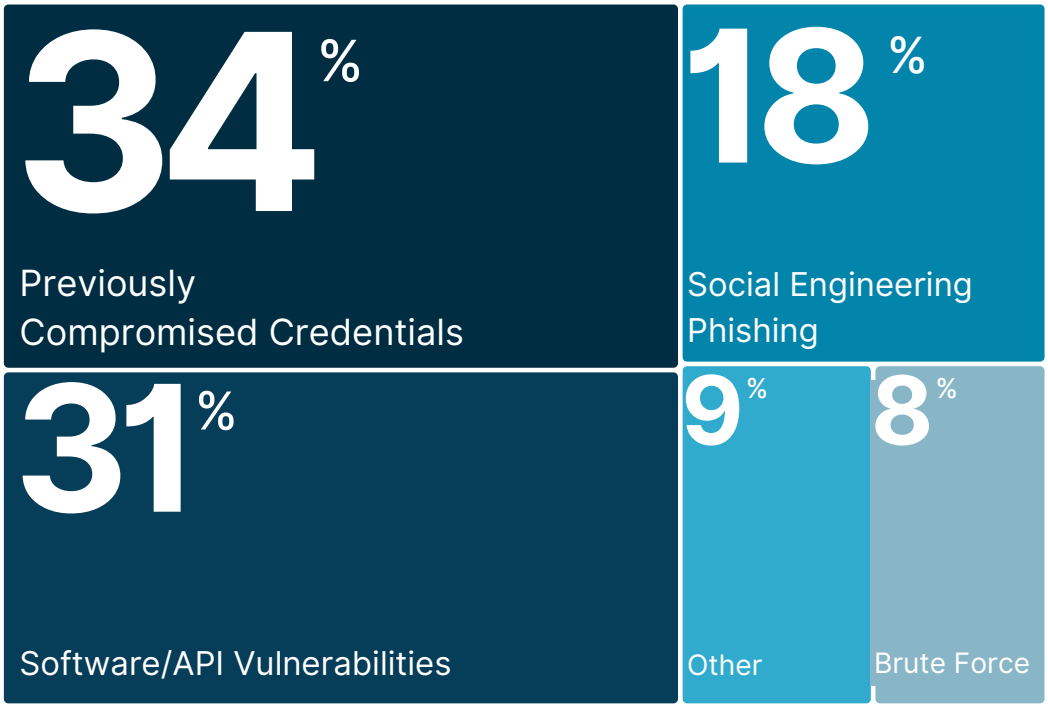


How do attackers get in?

On average, the **most common way** for attackers to gain access is through the use of **previously compromised credentials**. This technique involves credentials likely **obtained by an initial hacker** during a data breach or identity attack, then **purchased by a second threat actor** from platforms like the **dark web** or **Telegram**.

Closely following compromised credentials were **exploits targeting software vulnerabilities**. Analyzed data suggests that the majority (**over 90 %** [5]) of these **attacks were aimed at web applications rather than infrastructure elements.** Therefore, it may be a good idea to prioritize securing web applications.

In third place, with **18 %** of reviewed breaches, **is phishing**. New types of phishing have emerged, such as voice phishing (vishing), SMS or WhatsApp phishing (smishing), but **email** remains the **most prevalent vector** (in almost all reported cases). Attackers frequently use "business email compromise" (BEC), leveraging existing email threads to appear more legitimate.[1][2][3][4][5]



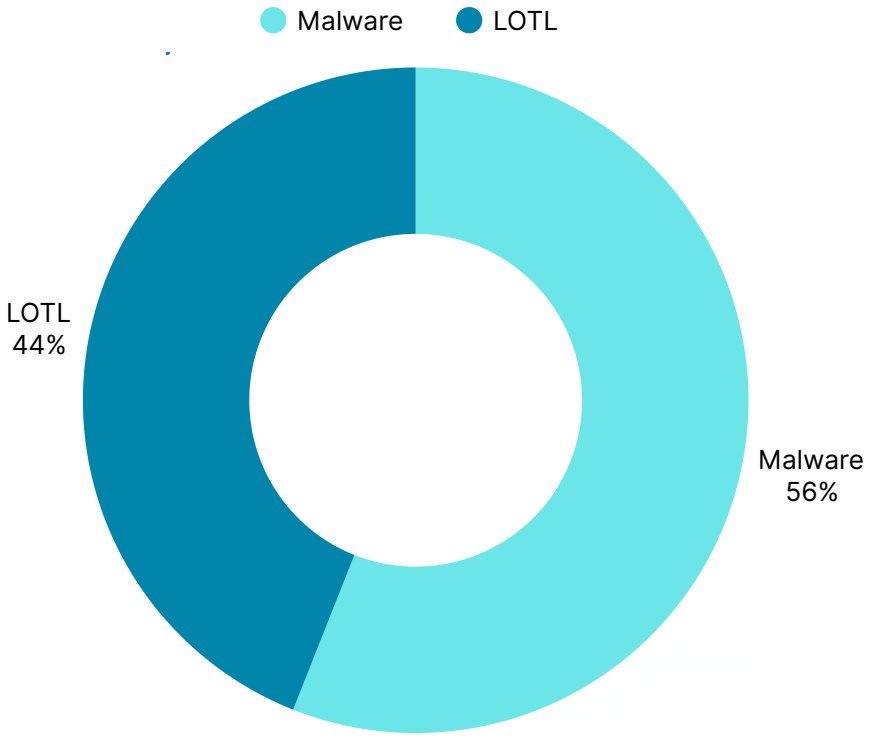
Year 2023

comma_0

Once they are in

Historically, when **attackers** were able to breach a system and "get in," their **first step** was to **deploy** some sort of **custom malware.** This is still true—especially with ransomware attacks.

However, more and more **attackers** have **shifted** to so-called "**living off the land**" (**LOTL**) techniques, where they focus on using **native OS features** or commonly **installed tools** to **avoid detection**.



56 % of attackers **used malware**, rest used **44 % "living of the land"** types of attacks. [4]

comma_0

Once they are in

Another aspect to consider is the time needed to fulfill the attack objectives. **Dwell time** (the period an attacker remains undetected within an infrastructure) is **decreasing**, primarily **due to** the rise in **ransomware attacks**, which tend to be fast.

That said, while an **average dwell time** of **10 days** may seem short, **advanced Red Teams** often **achieve** most of their **objectives** within a timeframe of **5–7 days**. Therefore, when facing an advanced attacker, security teams need to act quickly. [4]

10 D

Average dwell time

5-7 D

Red Teams achieve most of their objectives

comma_0

Once they are in

Analyzed data shows that the **average ransomware campaign** takes around **48 hours** to complete—from the start of the phishing campaign to the encryption of data.

48 H

Average campaign duration

Furthermore, there is evidence that some **APT** (**Advanced Persistent Threat**) groups can carry out a successful **campaign** in under **13 hours**. [4]

13 H

APT campaign duration

comma_0

How to protect - Breach

There are **three** main **ways** attackers **gain access,** each requiring **different strategies** to address effectively:

01

Phishing

Unsurprisingly, **almost all phishing campaigns** are still **delivered via email**. To combat this, **invest in** a **mail gateway** — preferably one that **integrates AI** to detect threats beyond static patterns — and conduct regular **cybersecurity awareness training** to keep employees vigilant.

02

Using Stolen Credentials

Attackers often use stolen credentials to access systems. **To protect internal systems, strong authentication** mechanisms and **monitoring for abnormal user behavior** are essential, as they can detect when attackers attempt to use stolen credentials. For **externally** facing **B2C systems**, this is more challenging but can be addressed through **application monitoring** and proactive **dark web searches** for leaked data.

03

Exploitation of Vulnerabilities

The approach to **mitigating** this **vector involves:**

Proactive Measures: Secure the development process, **minimize** the use of **vulnerable third-party components**, and follow best practices for **secure coding**.

Reactive Measures: Implement robust **vulnerability management** by prioritizing **patching** in **production systems**. When resources are limited, teams should focus on vulnerabilities that are actively being exploited or have a **publicly available proof of concept** (PoC), as these are more easily exploited even by unskilled attackers.

comma_0

How to protect - Post breach

XDR

As discussed earlier, attackers are increasingly shifting from malware to native tools ("**living off the land**" or **LOTL**). Traditional antivirus solutions are not equipped to handle this shift effectively. To **stop attackers** from **exploiting native OS tools**, we need modern **XDR** (**Extended Detection and Response**) solutions with **behavioral profiling**, such as **User and Entity Behavior Analytics** (**UEBA**).

SOAR

Having the capability to **automatically detect** and **respond** to attackers **24/7** is **crucial**. As we saw in the dwell-time analysis, some **ransomware campaigns** were able to **achieve** their **objective** (**encrypting** data) within just **13 hours**. **Relying** on a **human-operated SOC** to respond with accuracy at **3 AM** on a **Sunday** is **not** the **best** approach.

It is essential to have a **system** that can **autonomously stop or** significantly **slow down** an attacker **by isolating** compromised **endpoints**, **removing** affected users from **privileged groups**, **resetting session** tokens, and taking other defensive actions in real time.

How to protect - Governance

01

Have an IR (Incident Response) plan

Having an **IR plan** is a must-have, but it also **needs** to be **practiced**. Conduct regular **table top exercises**.

02

Attack surface visibility

Manage vulnerabilities of your **exposed services**, or they will eventually be exploited.

03

Strong segmentation on network and identity level

Even after breach, the attackers will have a **hard time traversing** around the **network**. This will either **stop them** or at least **slow them down** and give you more time to respond. If nothing else, at least it will **limit the impact** of the attack due to limited resources which can be attacked.

Lastly, it's crucial to build everything with modern security architecture principles in mind. Buzzwords like "**Assume the Breach**" and "**Zero Trust**" are more than just marketing terms.

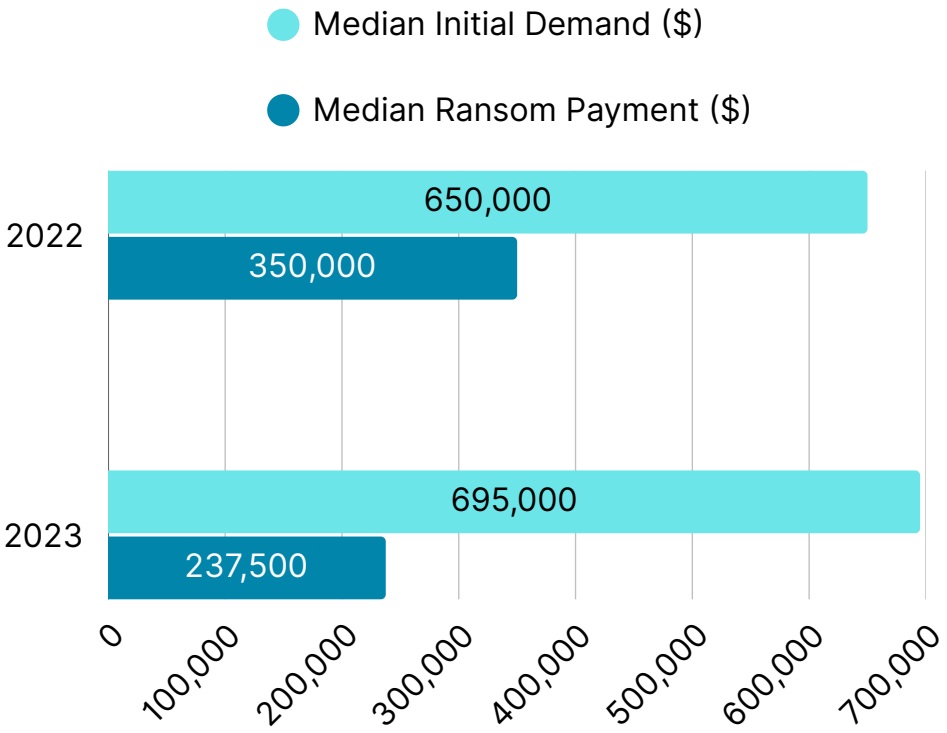
Zero Trust enables **granular control over permissions** and identities, significantly **reducing the potential** for attackers to **move laterally** within your infrastructure.

In a worst-case scenario where all defenses are breached, Zero Trust principles enforce **strict segmentation**, **limiting** the attacker's **reach** and **minimizing** potential **damage**.

comma_0

Ransomware

How much does it cost?



The **median ransom** for 2023 was **$237,500 USD** (5,000,000 CZK). It's important to remember that the **overall cost** of a ransomware attack can **significantly exceed** the ransom amount.[4]
Typical costs associated with ransomware include:

- **Penalties for non-compliance** with regulations (e.g., NIS2, DORA).
- **Fines for GDPR** violations related to leaked data.
- **Reputational damage**.
- **Costs** related to **business continuity** and **disruption**.

However, the most important aspect to consider is that the first step when attacked by ransomware is to **fix** the **root cause** — otherwise, the attackers can encrypt your data again. Once you are attacked, you will inevitably need to **invest in cybersecurity** and **protect** your **infrastructure**. So why not do it beforehand, when you have time to plan, rather than during an attack when you're under pressure?

comma_0

Ransomware

Ransomware attacks are among the **most publicized cyber threats**. You've likely heard of multinational corporations being targeted, as well as smaller entities like government agencies and hospitals. Historically, ransomware focused on disrupting operations, but **attackers** now also **exfiltrate PII** (**protected under GDPR**) and threaten to publish it if ransoms aren't paid. **Defense** requires a **two-pronged approach**:

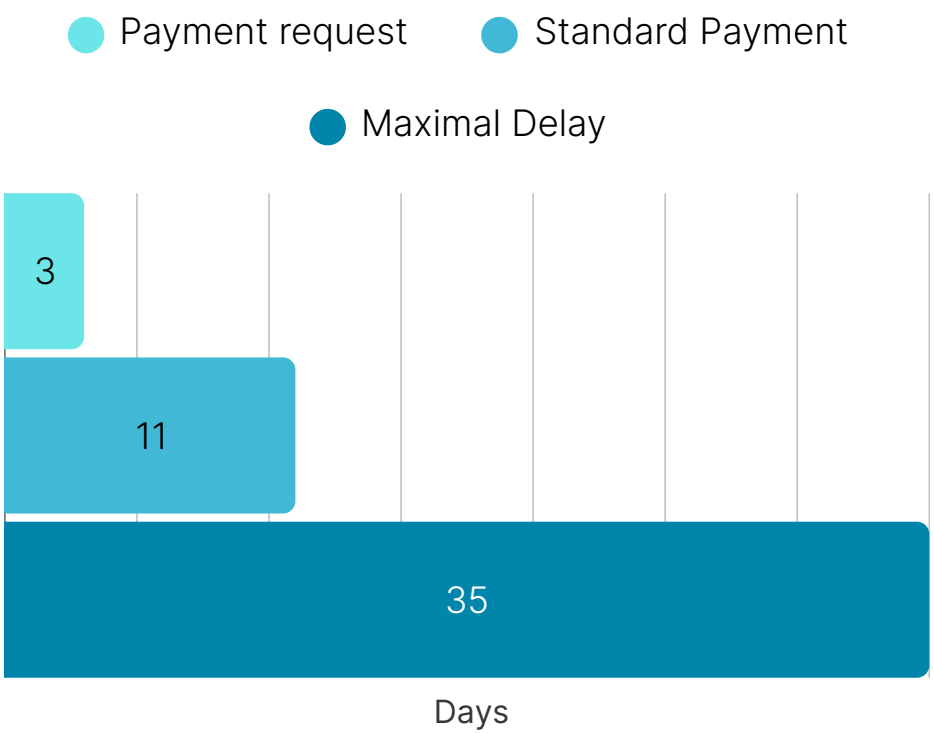
Preventing Access and **Slowing Attackers Down**: Follow best practices to block initial access and delay attackers long enough for your security team to respond.

Tested DRP and **Immutable Backups**: Ensure disaster recovery plans are tested, so you can rebuild infrastructure without paying a ransom or decrypting lost data. Last but not least, assure mission-critical data is backed up securely.

comma_0

Ransomware

How long do the negotiations with attackers last?



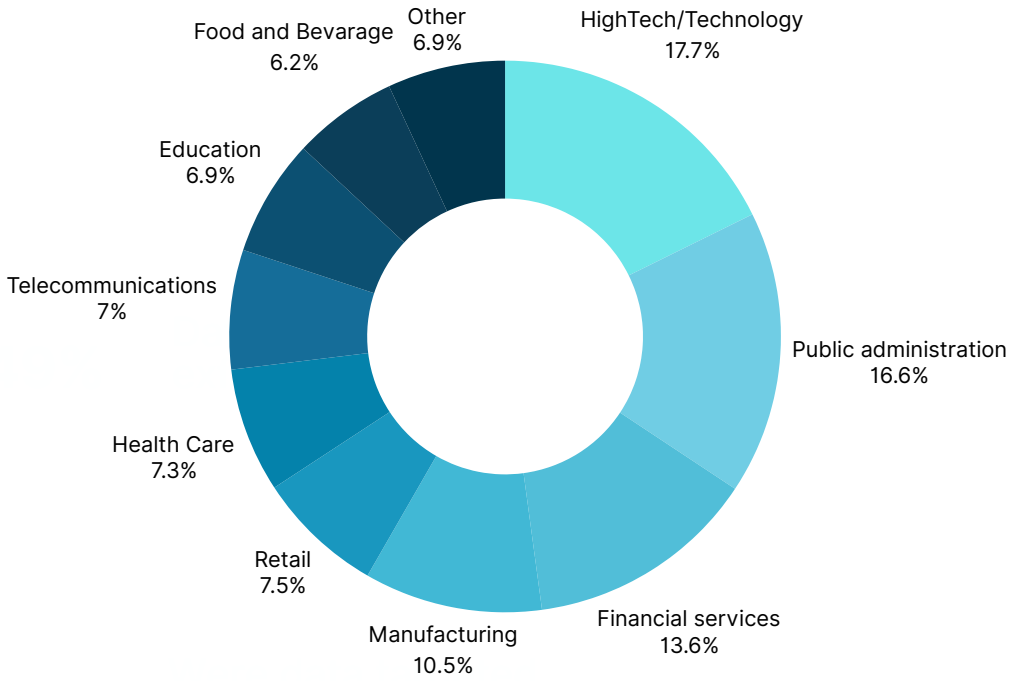
Negotiations with threat actors often extend their original deadlines, typically **set at 72 hours**. These discussions usually **last up to 11 days**, giving organizations time to respond. Some choose to pay the ransom on the first day, while others delay **payment for up to 35 days**. [4]

This variability highlights the importance of strategic decision-making during ransomware incidents. Negotiation timelines play a **crucial role in business continuity and disruption.**

Who is being targeted?

Almost **ALL (95+ %)** attacks are financially motivated, so basically, everyone able to pay ransom is a target. [4]
This applies the most for companies whose disturbed operations would cause financial loss (like SaaS services, e-commerce, logistics ..) as they are most likely to pay a ransom.

In 2023, the **most affected** industries were **HighTech/Technology, Public administration (Government), Financial services, Manufacturing, Retail, Healthcare** and **Telecommunications.** [1][2][3][4][5]



Does not matter which field you are from, if you can pay ransom or you have valuable information → you are the target.

comma_0

References

1 Cisco Systems, Talos IR trends, 2024

2 Mandiant, M-Trends, 2024

3 Crowdstrike, Global Threat Report, 2024

4 Palo Alto Networks, Unit 42 - Incident response, 2024

5 DBIR, Verizon, 2024

Contact Us

Contact us today to take the first step towards a secure future for your business.

www.comma0.io

info@comma0.io