LUMU

2026

COMPROMISE REPORT

As threats fracture and a new horizon emerges, 2026 demands a pivot in defense. We discover the malware and tactics behind this shift. Understand the enemy, navigate the change.

Executive Summary

If 2025 proved anything, it is that the adversary is no longer a static target. They are a Hydra: cut off one head and two grow back. They become smarter, faster, and harder to see.

The **2026 Lumu Compromise Report** analyzes a year defined not by the malware that the cybersecurity community brought down, but by the resilience of the threats that survived. Major takedowns of gangs like LockBit, Lumma, and Qakbot provided only temporary silence. In their wake, a fractured, decentralized ecosystem emerged, trading brute force for invisibility.

The data reveals a strategic pivot. Attackers have abandoned 'loud' breaches for 'low-and-slow' evasion, mastering Living-off-the-Land (LotL) tactics and hiding within the very tools you trust. They may use VPNs, legitimate traffic distribution systems, or encrypted DNS channels. We no longer look for the enemy at the gate, we have to assume they are already inside.

This document is not just a retrospective, it is a battle plan. We dissect the anatomy of these new, invisible threats, from the 'gatekeepers' like Keitaro to the 'assassins' like DeathRansom. We outline the only defensive posture capable of defeating them: Continuous Compromise Assessment®.

Welcome to the age of the invisible adversary. Here is how you find them.

"

Message From the CEO

The State of Cybersecurity: The Age of Adaptation

The only constant in our industry is change. In 2025, the adversary was not just persistent, but adaptive. When one avenue closes, they do not retreat, they innovate. They shift tactics to bypass the controls we trusted yesterday.

But adaptation is not a one-sided equation. As threats evolve, so must our defense. We are countering their stealth with radical visibility and their speed with automated response. We are moving from static reliance on tools to dynamic operational proficiency.

This report highlights that critical pivot. While the adversary moves fast, we are moving with purpose. Let's prove that when we operate with true proficiency, the future belongs to the defenders, not the disruptors.

Ricardo Villadiego
Founder & CEO, Lumu Technologies

Index

PART I

Four Cybercriminals' Tools in 2025 4

- Anonymizers: The Camouflage 5
- Droppers & Downloaders: The Stealthy Attack 7
- Infostealers: The First Bite 10
- Ransomware: The Deadly Blow 12

PART II

A Closer Look at The Americas 16

- North America 17
- Central America & The Caribbean 19
- South America 21

PART III

The Top MITRE ATT&CK Tactics & Techniques 23

- The Top 10 MITRE ATT&CK Tactics for 2025 24

PART IV

Finding the Footprints of the Invisible Enemy 27

- Data From Lumu's AI-Driven Behavioral Detections 28
- Find the Footprints: Your Battle Plan for 2026 30

PART I

Four Cybercriminals' Tools in 2025

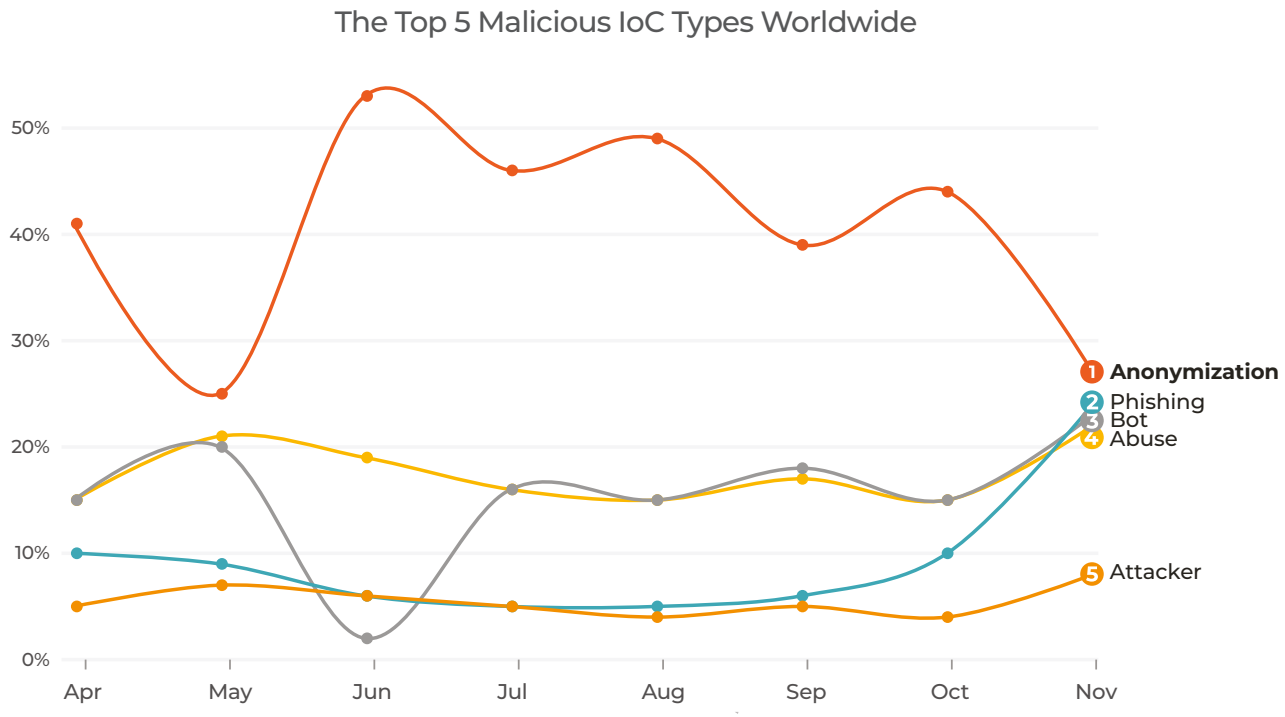
2025 proved that the adversary is resilient. Major takedowns of Lumma and Qakbot provided only temporary relief. The data from 2025 shows the adversary did not just survive, it adapted, and grew stronger.

As we enter 2026, the battle has shifted from high-profile malware to stealth. Attackers mastered **Living off the Land**, camouflaging their activity within legitimate tools and network noise. They traded brute force for behavioral evasion, favoring **anonymizers, DNS tunneling**, and **AI-generated domains**.

This section analyzes the data on the year's top threats: **infostealers, ransomware**, and **droppers**. How they evolved to become more persistent, fragmented, and evasive. Before that, we look at how they hide themselves.

Anonymizers: The Camouflage

According to data gathered by Lumu's threat intelligence service Maltiverse, stealth, deception, and persistent infrastructure are all key components of a modern attack.

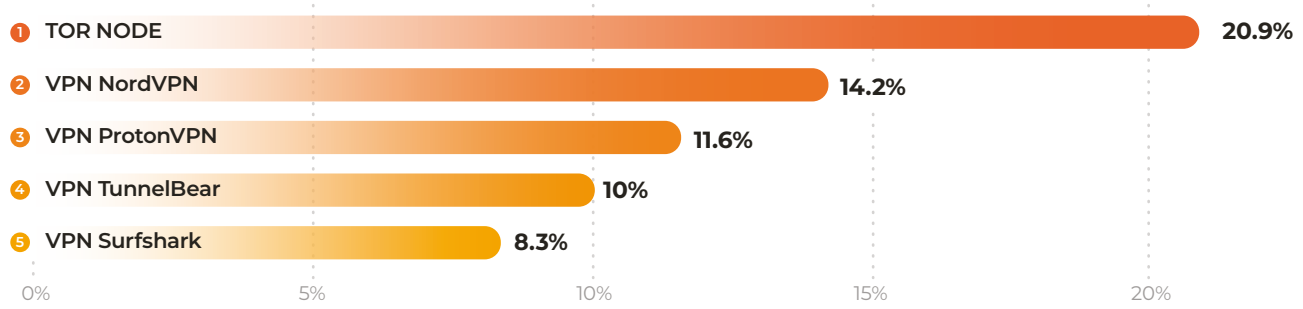


The data shows that **anonymization** remained the most detected IoC type all year, reinforcing it as a foundational tactic.

Not only this, but the IoCs that round out the top five suggest they are building persistent, hidden infrastructure. **Abuse** IoCs are confirmed malicious infrastructure, like malware-hosting sites. **Bots** are a legitimate device that has been compromised and enslaved by an **attacker** to execute remote commands.

They combine this infrastructure with anonymization to maintain their foothold.

Top 5 Anonymizers Detected Worldwide



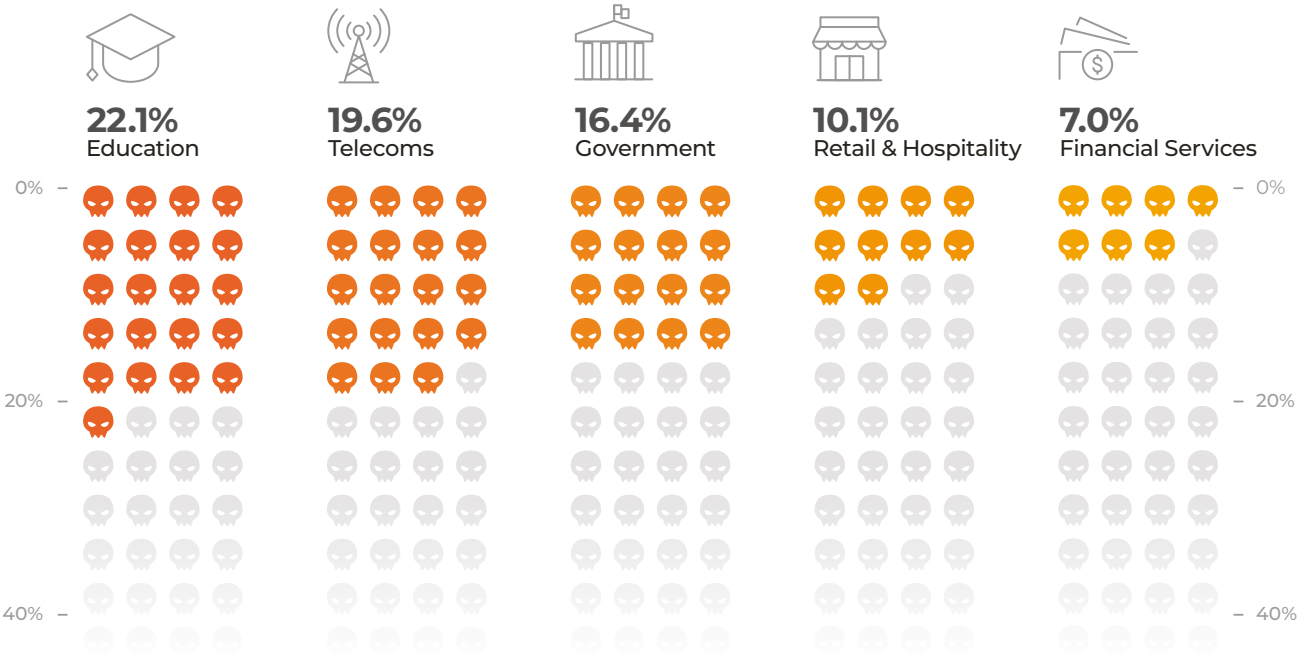
The graph above dives deeper into this 'invisibility' trend. Attackers use anonymization services to establish covert communication channels, mask their true location, and exfiltrate data. While not intrinsically malicious, services like **Tor** and private **VPNs** pose a critical visibility challenge, blinding administrators to potential threats.

In a normal work environment there is not often a legitimate need for anonymizers, so we can assume that a high percentage were malicious.

This widespread use of legitimate, encrypted tools to hide malicious activity is a key reason why traditional, signature-based defenses are failing.

Attackers have targeted a wide variety of sectors. Education came top in our records, but telecommunications companies, and state and local government came close behind.

Top 5 Sectors Targeted by Tor and VPNs Worldwide



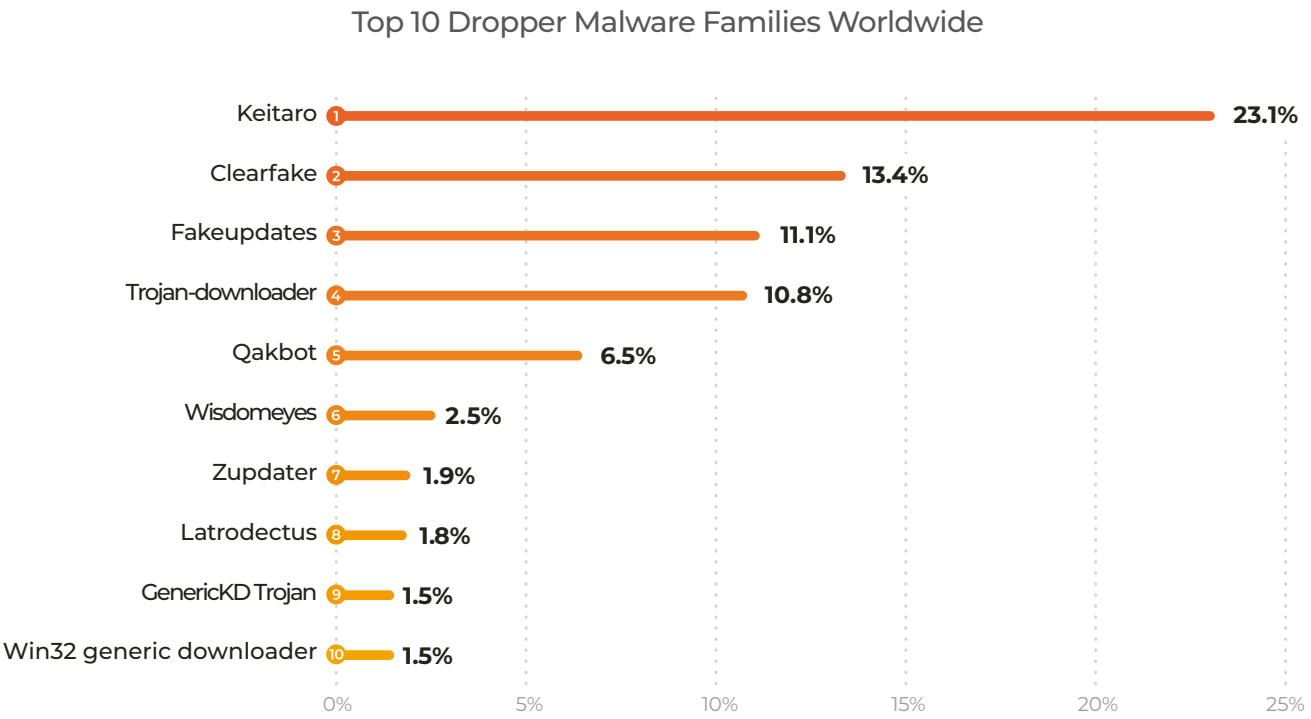
Droppers & Downloaders: The Stealthy Attack

Droppers and downloaders are the invisible beachheads of cybercrime.

Droppers slip past secure gateways, looking like harmless files, but inside they contain hidden malware.

Downloaders are similar, but they automatically download malware from the internet, such as infostealers or ransomware, when activated. This turns a small gap into a massive breach.

Many downloaders have evolved. Rather than downloading the entire malware, they download small pieces that look safe to the gateways. Then the downloaders assemble the pieces at the endpoint level into tools of mass destruction like infostealers or ransomware.



Droppers perfectly illustrate the persistence of criminal gangs. Despite the major Qakbot takedown in the US, residual activity remains, proving that you cannot kill a threat simply by seizing a server. The infrastructure fragments, hides, and continues.

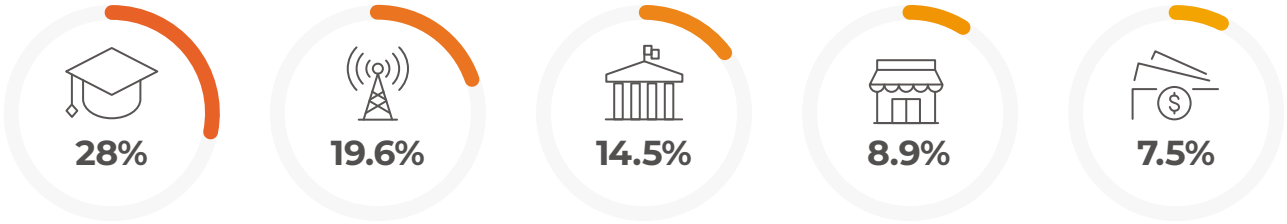
However, the most significant evolution in 2025 is the pivot to **infrastructure abuse**. The top threat, **Keitaro**, isn't malware at all.

Keitaro Breakdown

Keitaro was the Dropper most detected by Lumu in 2025. It is a legitimate **Traffic Distribution System (TDS)** used by marketers to route web traffic. Attackers have weaponized it to create a 'velvet rope' for malware.

Attackers use Keitaro to profile incoming connections. If a user is a security researcher or a bot, Keitaro routes them to a harmless Wikipedia page. If the user is a targeted victim (specific ISP, OS, or geolocation), they are routed to the exploit kit. This is the ultimate form of Living off the Land: using commercial marketing tools to make attacks invisible to automated scanners.

Top 5 Sectors Targeted by Keitaro Worldwide

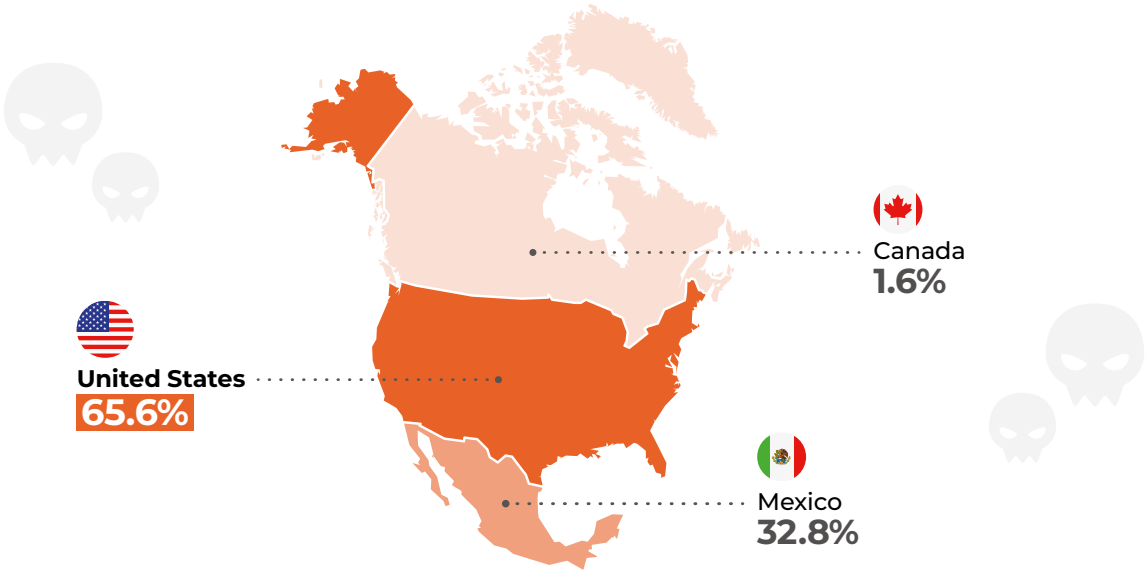


The data reveals a calculated assault on the education sector. Keitaro's prevalence here is not accidental. It exploits the open, Bring-Your-Own-Device (BYOD) nature of university networks. Attackers use these high-bandwidth, low-security environments as testing grounds and launchpads.

Keitaro: Geography as a Filter

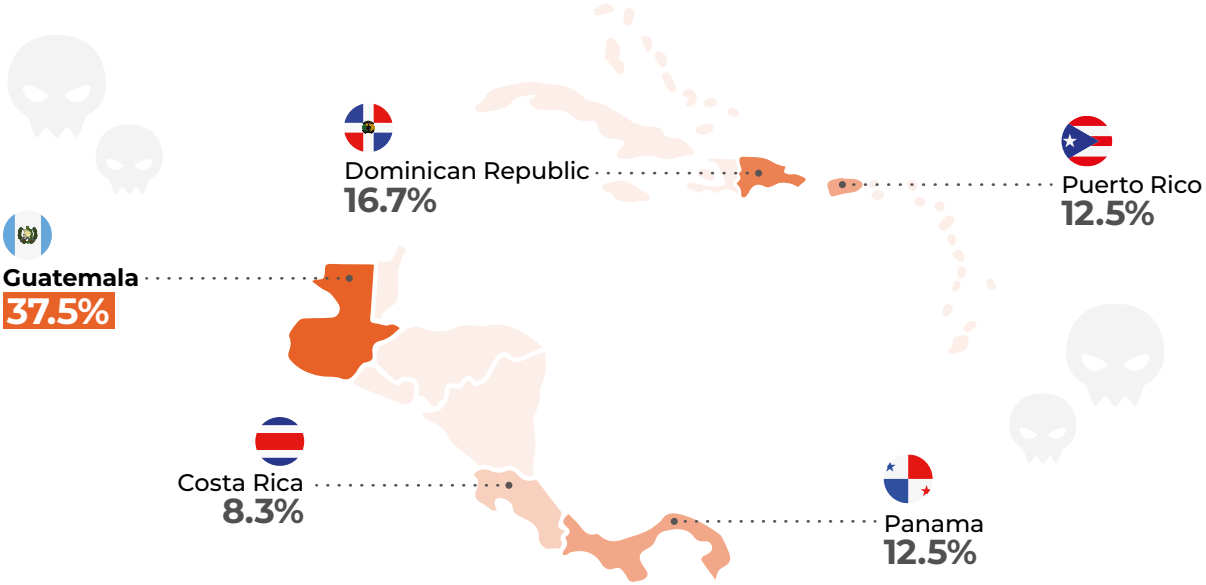
It is worth noting that Keitaro's strong presence in certain countries is not random. Keitaro's strength lies in precision. A banking Trojan designed for Brazilian payment systems is useless in Germany. Keitaro ensures that only valid targets receive the payload, keeping the malware hidden from global threat hunters.

Keitaro in North America



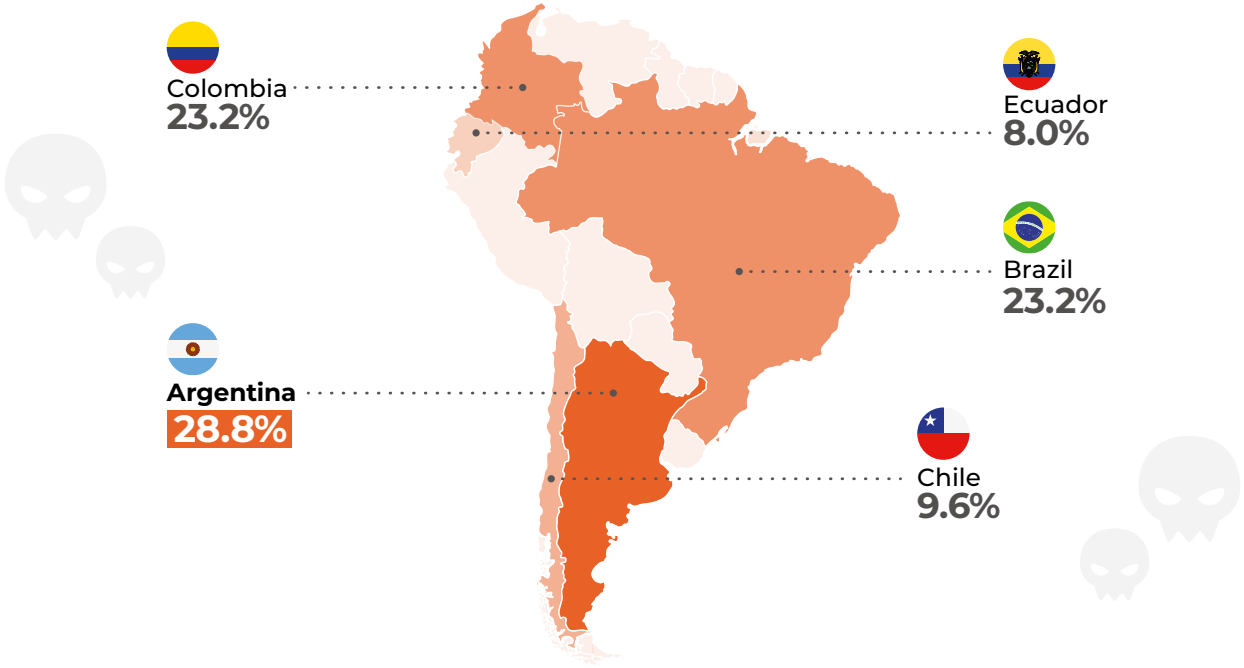
The USA remains the primary target volume-wise, but the filtering is highly specific to corporate environments.

Keitaro in Central America & The Caribbean



Guatemala experienced double the detection volume of its neighbors. As the region's largest economy with a growing reliance on digital services and agriculture, it has become a prime target for regionally-focused campaigns.

Keitaro in South America



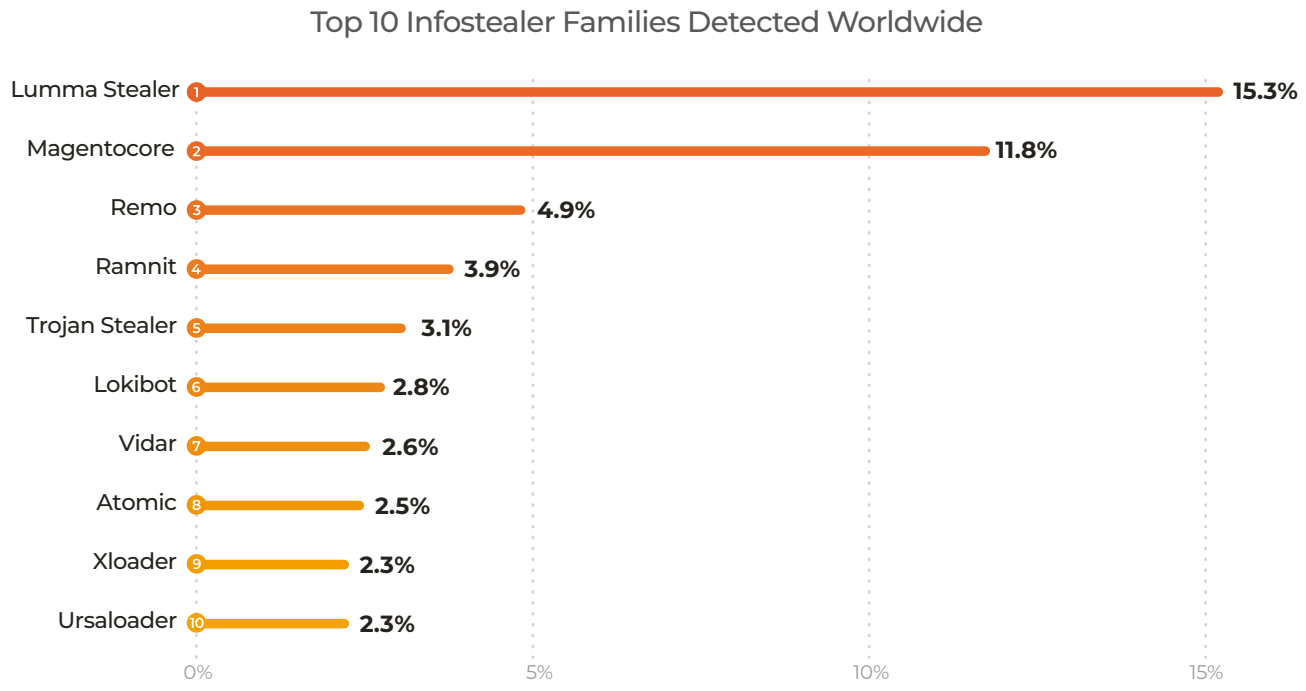
The focus shifts to the economic powerhouses, Argentina, Brazil, and Colombia, where attackers filter for users of specific regional banking platforms.

Defender's Intel: Countering Keitaro

- **Look Beyond the Payload**
  You cannot rely on catching the final malware if the delivery mechanism (the dropper) is whitelisted.
- **Block Known TDS IPs**
  Threat intelligence feeds must include IP ranges of known abused TDS services like Keitaro.
- **Geo-Blocking Is Insufficient**
  Since Keitaro uses legitimate traffic routing, you must inspect the behavior of the connection (e.g., rapid redirects, fingerprinting scripts) rather than just the origin.

Infostealers: The First Bite

Infostealers are the silent precursors to a devastating attack. They harvest credentials and session cookies, grant attackers the ability to bypass Multi-Factor Authentication (MFA) and gain 'legitimate' access. A minor infostealer infection, which a traditional SOC might easily overlook, can quickly turn into a full-scale ransomware breach.

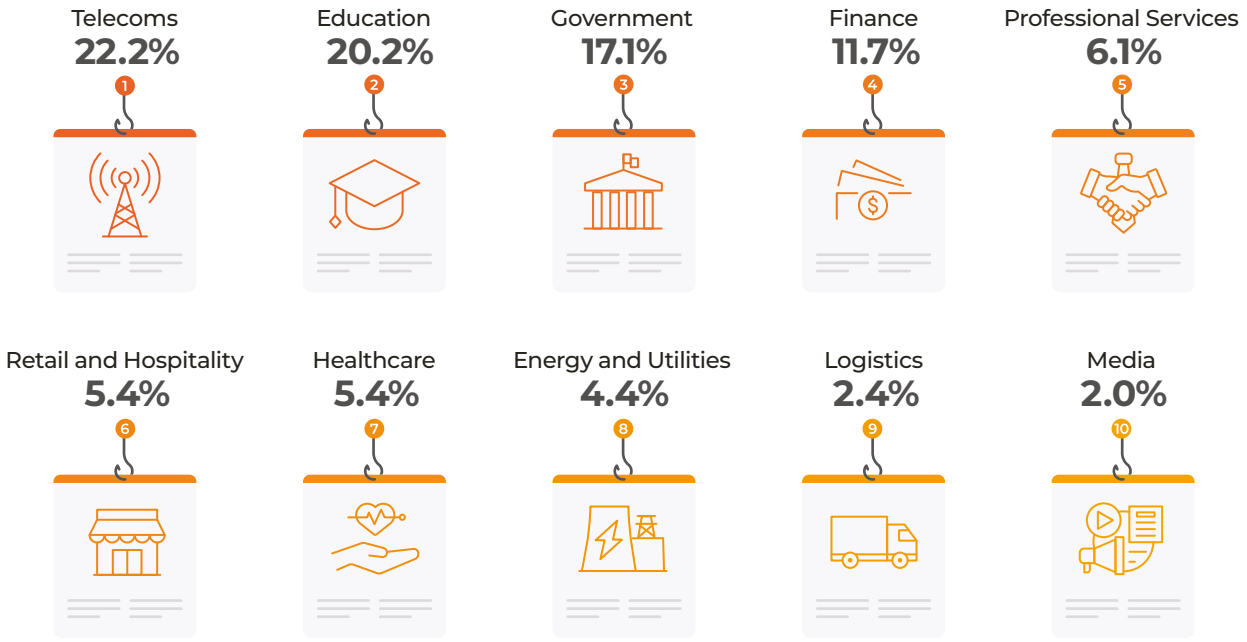


The story of infostealers in 2025 is the story of Lumma. Takedowns, like the FBI's mid-2025 operation, caused immediate, short-term declines in its activity. However, Lumu sensors detected new, more resilient Lumma infections by late July.

As with the mythological Hydra, Lumma has simply regrown two serpentine heads in place of one. While the malware group's operations changed, the malware continued. On a positive note, this means that core identification techniques for Lumma malware remain valid.

While Lumma is still dominant, the landscape shifted to include new financial credential stealers like **MagentoCore, Remo**, and **Ramnit**. The infostealer market is quick to fill any vacuum.

Top 10 Sectors Where Infostealers Detected Worldwide



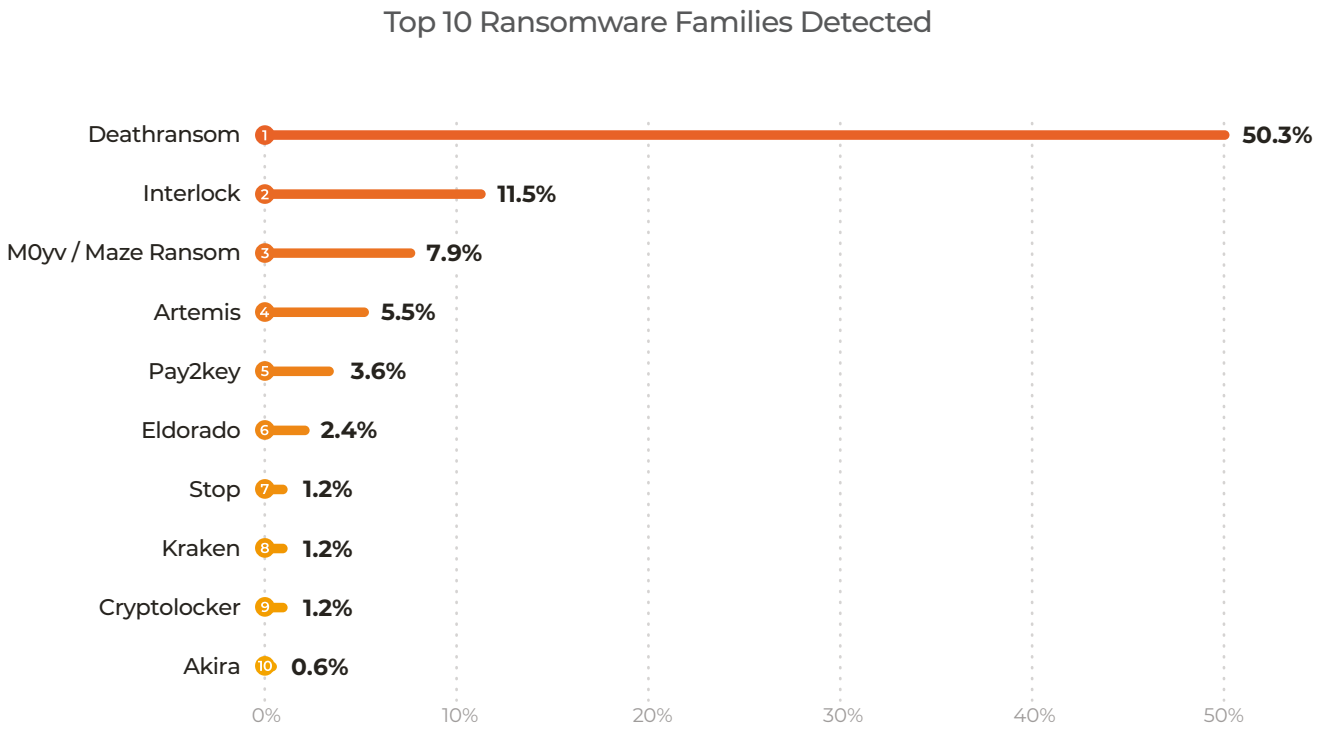
It is worth taking note that infostealers statistics were not uniform across all countries. For example, in the USA over 60% of detections were in the education sector.

With the rise of Living-off-the-Land tactics, true resilience must be built on layers, starting with total network visibility. The first priority is defending against credential and data theft at the network level to immediately detect any exfiltration attempts. However, security teams must also accept the reality that perimeters can be breached.

To ensure a single slip at the entry point is not fatal, you must also monitor for internal threats. This could be detecting strange **Command and Control traffic**, flagging **malicious scripts**, or identifying **attempts to disable antivirus software**. In other words, ensure defense in depth.

Ransomware: The Deadly Blow

Ransomware paralyzes organizations in minutes. It is no longer just about data recovery, it is a high-stakes extortion racket where your own sensitive data is the weapon used against you.

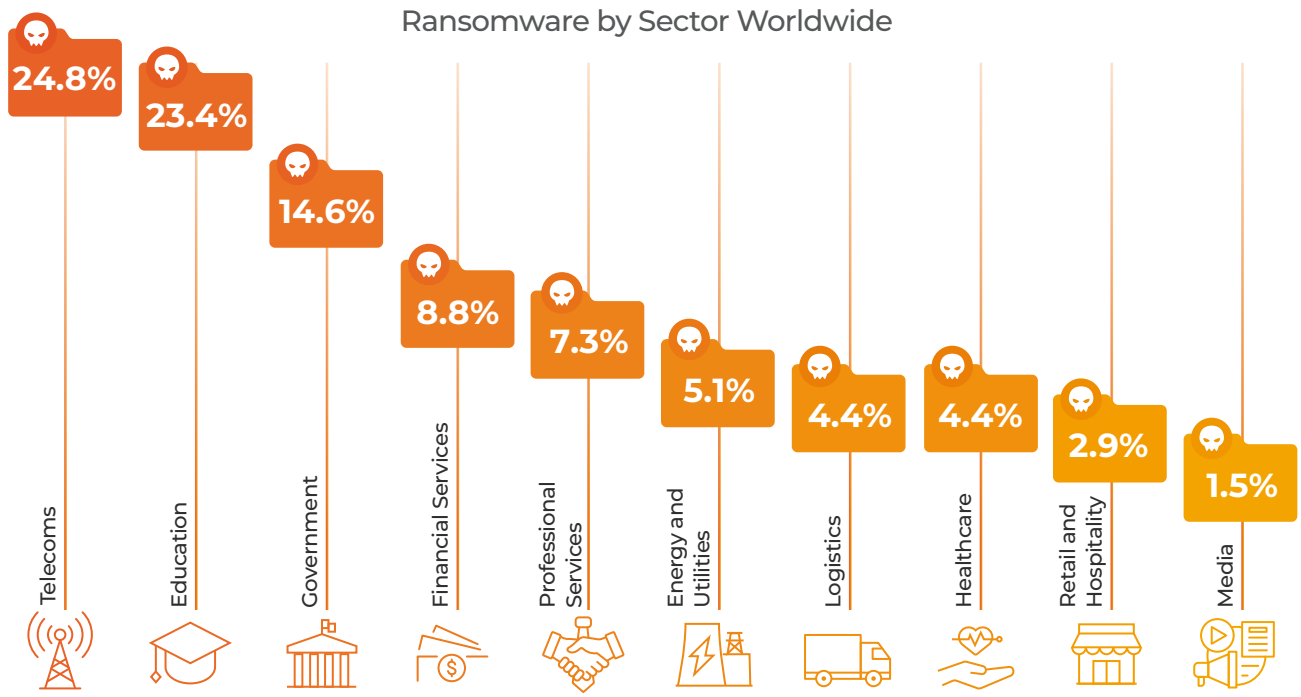


The 2025 landscape is dominated by fragmented groups that split from larger, well-known gangs. This decentralization aids their persistence and evasion of authorities.

DeathRansom, far above all others, thrives in this chaos. As a volatile Ransomware-as-a-Service (RaaS) strain, it empowers unskilled affiliates with lethal tools, fluctuating between sophisticated encryption and simple data theft to keep defenders constantly off-balance. This makes it the perfect tool for attackers across the world.

Despite international takedown efforts, **LockBit** remains a top threat, while other groups like the state-targeting Interlock are resurging.

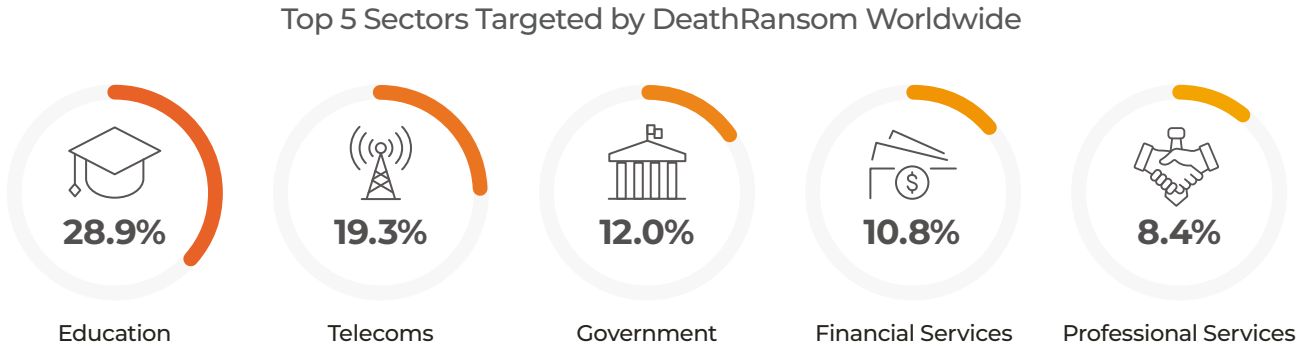
Crucially, attack chains have prioritized speed and stealth. Gangs are Living off the Land, using legitimate tools to bypass security and camouflage traffic. This shift to evasion techniques is a key theme we will explore in Parts III and IV.



The fragmented, hit-and-run model that is associated with RaaS ransomware means attackers can be less selective. This data shows the industry breakdown, revealing a wide spread of victims as these smaller groups hunt for any vulnerable target.

DeathRansom Breakdown

Unlike the disciplined, corporate-style operations of groups like LockBit, **DeathRansom** represents the fractured nature of the 2026 threat landscape. It is a chaotic **Ransomware-as-a-Service** strain that empowers unskilled affiliates to strike hard and fast.

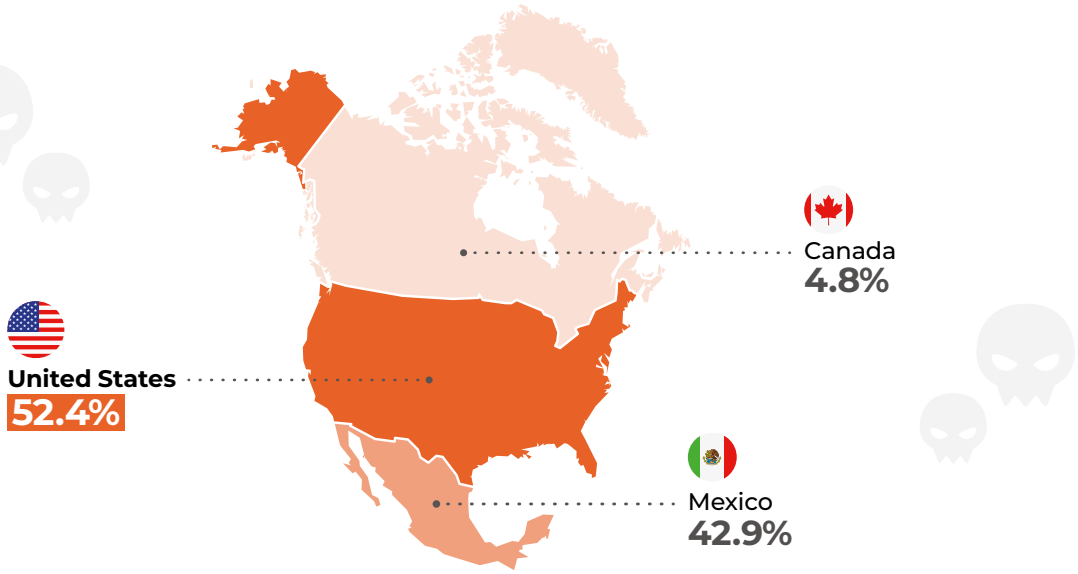


DeathRansom has zeroed in on **education**. Why? It is the path of least resistance. Schools and universities manage vast networks with limited security staff. More importantly, they operate under extreme pressure to remain open. DeathRansom affiliates exploit this urgency, betting that a school district will pay a smaller ransom quickly to avoid public scrutiny and classroom shutdowns, rather than engaging in a drawn-out negotiation.

DeathRansom: Geography as a Filter

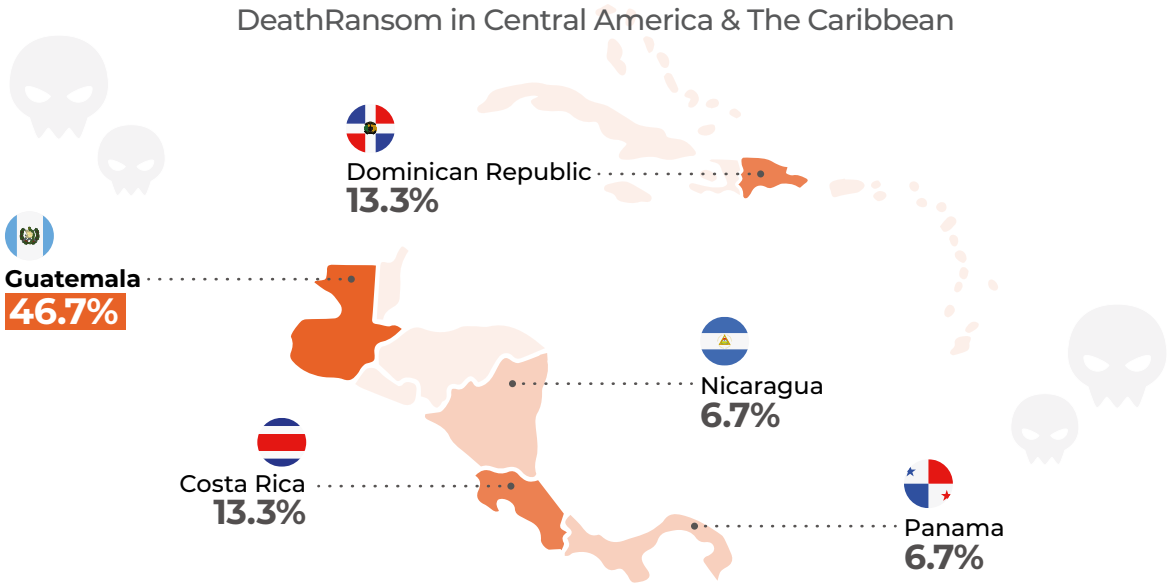
DeathRansom does not use a spray and pray approach. Its affiliates favor a personalized, targeted methodology. The data shows a clear correlation between the region's dominant industry and infection rates.

DeathRansom in North America



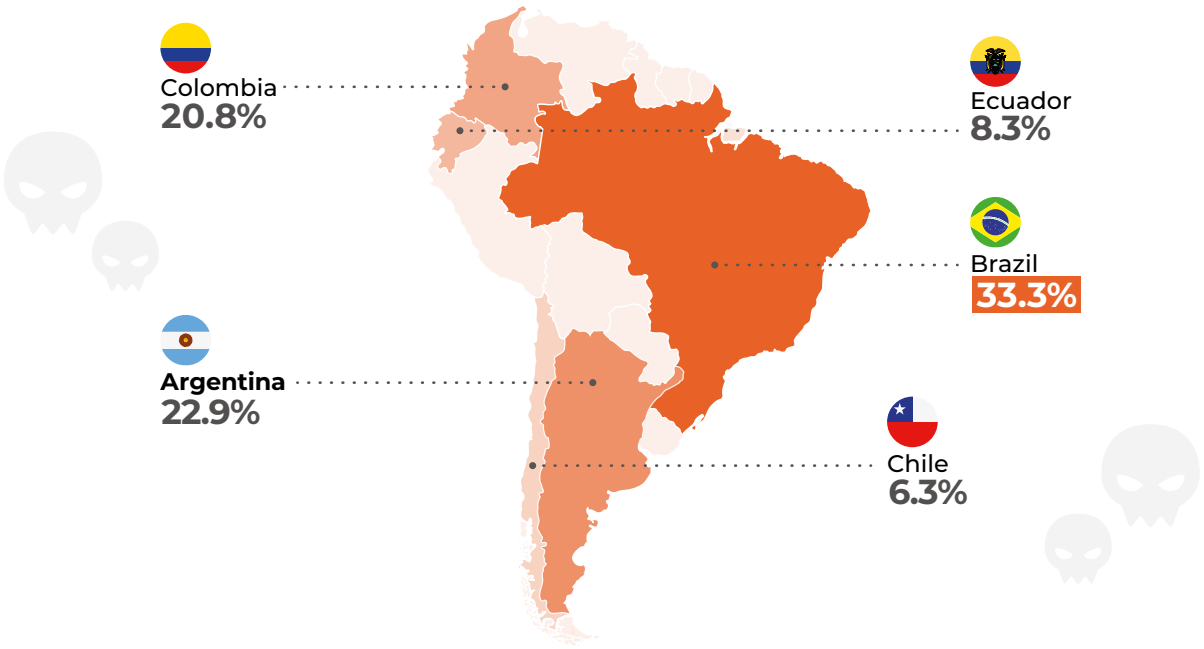
DeathRansom affiliates often target mid-sized organizations in North America. These organizations often lack the resources of the Fortune 500 but have enough cash flow to pay a moderate ransom.

DeathRansom in Central America & The Caribbean



The high detection rates here align with the region's manufacturing and logistics hubs. DeathRansom targets the uptime pressure. In export economies, if the factory floor stops, the losses mount instantly, forcing a quick payout.

DeathRansom in South America



The targets in South America are the regional economic engines. The attack profile suggests these are not random hits, but calculated strikes against the supply chain and production sectors where operational downtime is catastrophic.

Defender's Intel: Defeating DeathRansom

- **Don't Rely on Decryptors**
  DeathRansom is historically buggy. It started as a fake ransomware that couldn't actually decrypt files. Even if you pay, there is a high statistical chance you will not get your data back.
- **Behavior Over Signatures**
  Because DeathRansom is used by many paying affiliates, the delivery method changes constantly (phishing, RDP brute force, software vulnerabilities). You cannot block it by looking for a specific file hash.
- **Watch for Pre-Encryption Activity**
  Since they rely on extortion, look for massive file read operations (data exfiltration) occurring before the encryption event. This is your window to stop the breach.

PART II

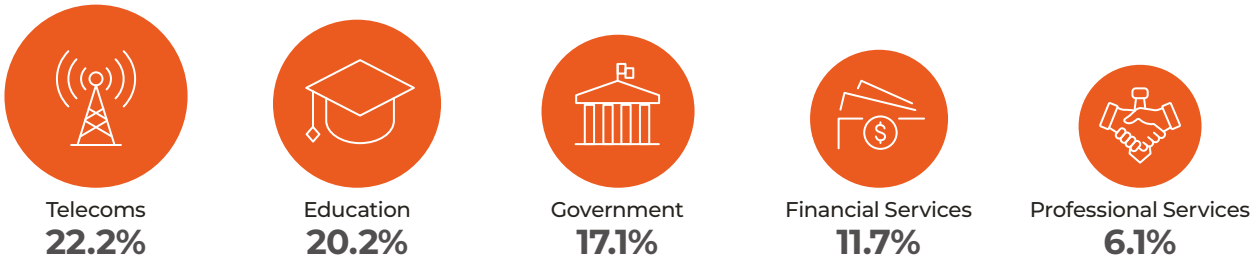
A Closer Look at The Americas

While tactics may be global, the targets are local. The 2025 data reveals that the impact of these threats is not uniform. It is shaped by regional economies, digital maturity, and specific vulnerabilities. This section zooms in on the distinct threat profiles of North America, South America, and the Caribbean to show exactly where, and how, the adversary is striking.

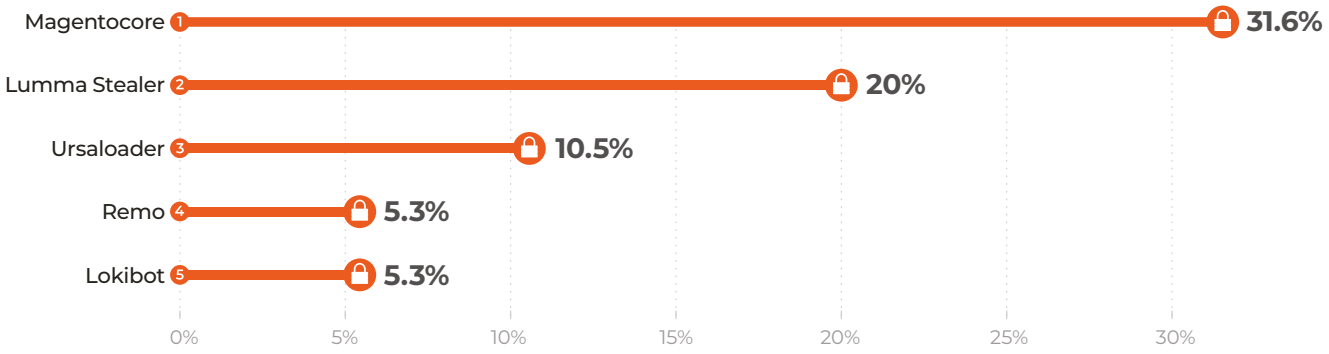
North America

North America remains the global epicenter for high-value targets. The region's mature digital infrastructure makes it the primary playground for sophisticated Ransomware-as-a-Service (RaaS) operations that prioritize high payouts over volume.

Top 5 Sectors Affected by Infostealers in North America



Top 5 Infostealer Families in North America

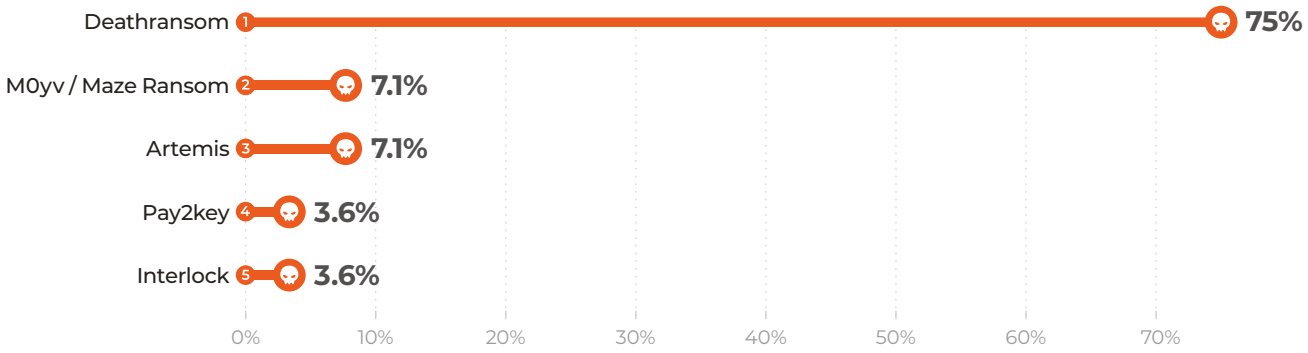


The dominance of **Magentocore** signals a war on E-commerce. Unlike other regions where banking credentials are king, North American attackers target the high volume of automated online transactions, injecting scripts to skim payment data at checkout.

It leads a landscape that includes **Lumma Stealer**, a Malware-as-a-sService (MaaS) specialized in harvesting cryptocurrency wallets and browser credentials, and **Ursaloader**, a Trojan designed to stealthily download and deploy additional malicious payloads onto infected systems.

Top 5 Sectors Affected by Ransomware in North America

Top 5 Ransomware Families in North America



The prominence of **DeathRansom** and **Maze (M0yv)** here highlights a trend toward double extortion. This is when data is both locked and threatened to be released by the attackers. North American companies have robust backups, making simple encryption less effective. Consequently, attackers have pivoted to data theft and the threat of public leakage.

Regional Defense Priority: North America

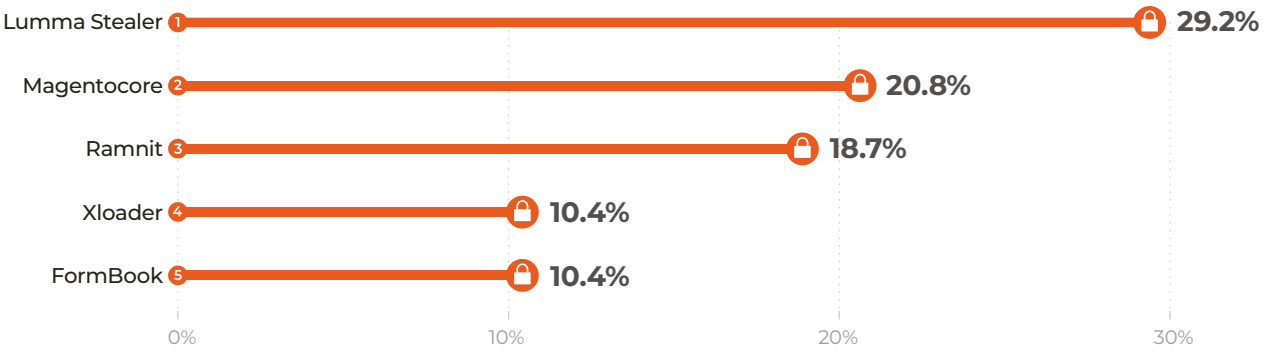
Data Exfiltration Monitoring. Backups will not save you from extortion. North American defenders must prioritize monitoring and controlling outbound traffic from the network to stop data from leaving the network.

Central America & The Caribbean

This region faces a highly specific threat profile. With economies heavily reliant on tourism, offshore finance, and logistics, the attacks are quieter. The goal here is not to disrupt operations (which causes immediate alarms), but to siphon assets unnoticed.

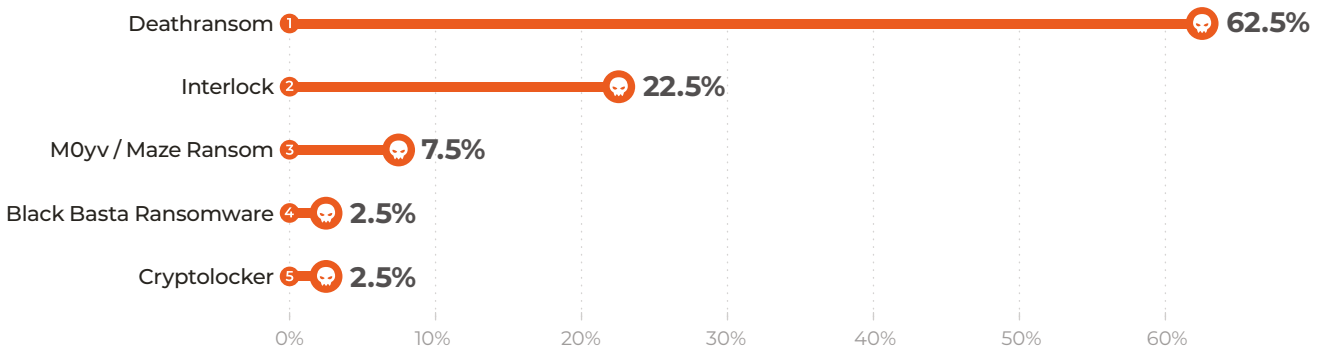
Top 5 Sectors Affected by Infostealers in Central America & The Caribbean

Top 5 Infostealer Families in Central America & The Caribbean



Lumma Stealer's dominance here is directly linked to the prevalence of cracked or pirated software in developing economies. Attackers hide Lumma inside free versions of business software. Once installed, it silently harvests crypto-wallets and credentials.

Top 5 Ransomware Families in Central America & The Caribbean



DeathRansom is again the main player in the region. Government agencies and large organizations are frequent targets.

Top 5 Sectors Affected by Ransomware in Central America & The Caribbean

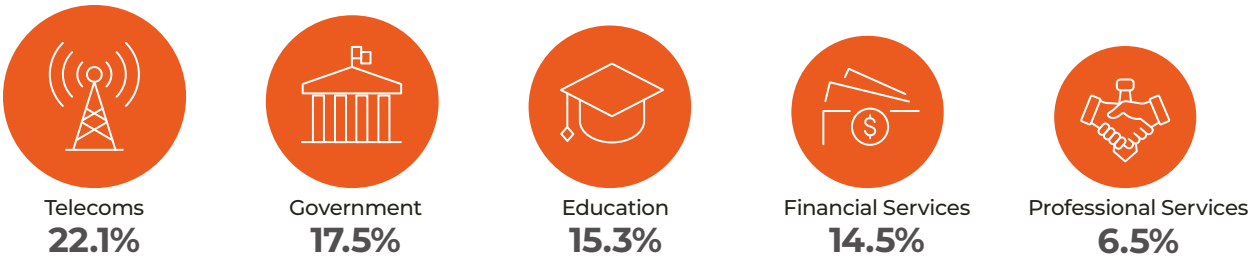
Regional Defense Priority: Central America & The Caribbean

Software Supply Chain. The vector is often internal. Organizations must enforce strict software licensing policies to prevent employees from downloading compromised cracked tools.

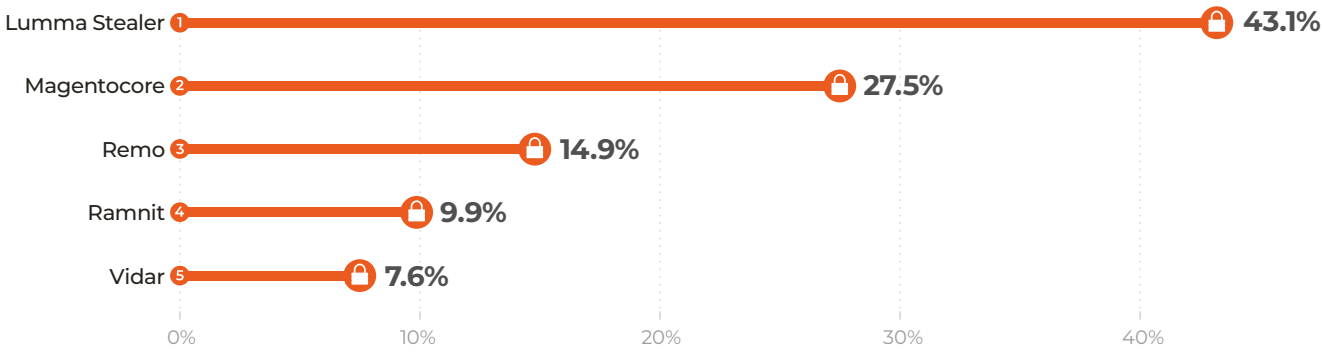
South America

South America is the fastest-growing attack surface in 2025. The data shows a sharp pivot toward financial fraud and aggressive ransomware campaigns. Cyber criminals are targeting critical infrastructure and government services, particularly in Brazil, Colombia, and Argentina. Often in this region, the rapid digitization of banking has outpaced security adoption, creating a fertile ground for financial fraud.

Top 5 Sectors Affected by Infostealers in South America

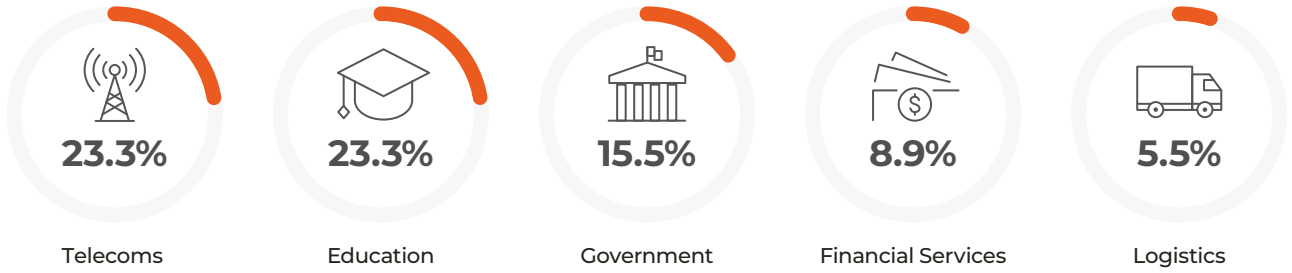


Top 5 Infostealer Families in South America

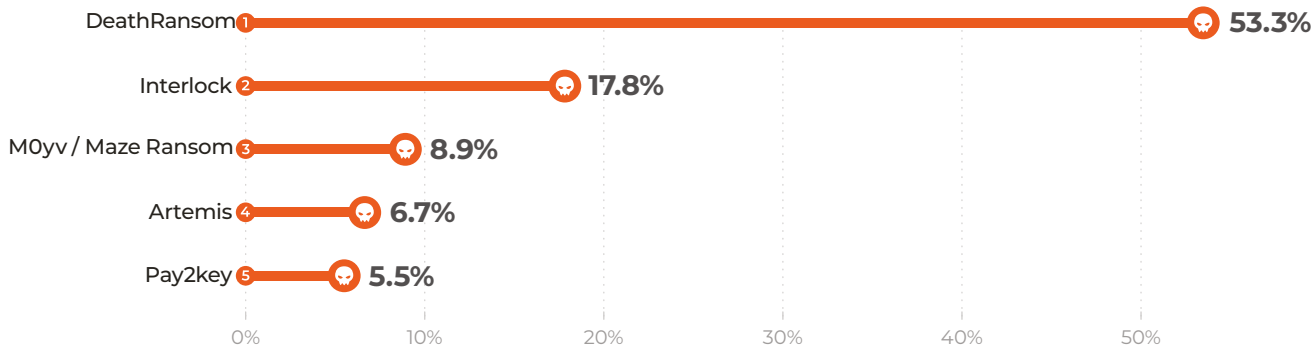


Lumma Stealer and **MagentoCore** appear again here, attacking crypto assets and e-commerce data respectively. They are joined by **Remo**, a threat family often associated with remote data theft, and **Ramnit**, a resilient banking worm that infects files to steal financial credentials. This indicates a widespread campaign against the consumer banking sector.

Top 5 Sectors Affected by Ransomware in South America



Top 5 Ransomware Families in South America



DeathRansom dominates the region as a data-theft-focused threat that often skips complex encryption in favor of pure extortion.

Groups like **Interlock** are using aggressive double-extortion tactics against state utilities and government services, betting that political pressure will force quick payments.

Regional Defense Priority: South America

Identity Confidence. With banking **Trojans** and credential theft rampant, simple MFA is being bypassed. Defenders must move to behavioral identity monitoring to detect when a valid user account is acting suspiciously.

PART III

The Top MITRE ATT&CK Tactics & Techniques

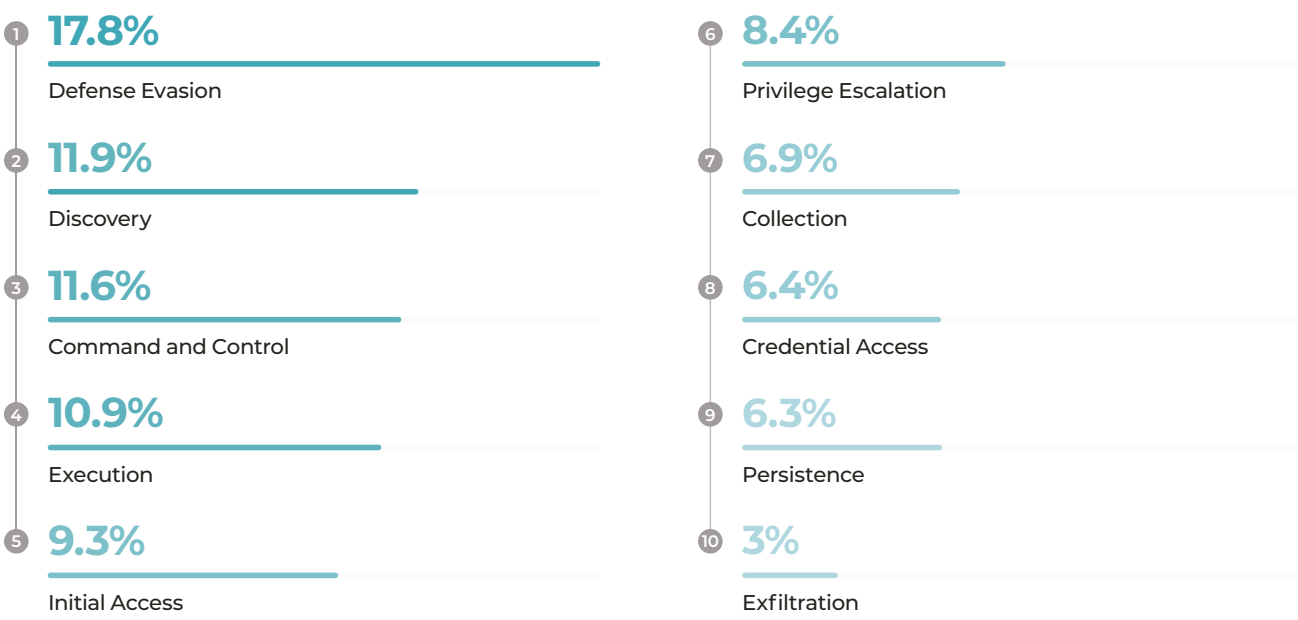
The 2025 data proves that the threat story is no longer about what the malware is, but how it arrives. Attackers are mastering the art of blending in. They are abandoning loud, disruptive entrances in favor of low-and-slow infiltration, cloaking their movements inside legitimate traffic.

The Top 10 MITRE ATT&CK Tactics for 2025

The clearest evidence of this shift is in the TTPs (Tactics, Techniques, and Procedures). The MITRE ATT&CK framework data shows a distinct trend: attackers are prioritizing evasion above all else.

Notably, **Command and Control (C2)** has replaced **Execution** in the top three tactics. This signals a change in priority: the adversary is less concerned with running destructive code immediately and more focused on maintaining a persistent, silent lifeline to your network without tripping alarms.

Top 10 MITRE ATT&CK Tactics



Let's look at how they achieve this silence across the top three categories.

#1 MITRE Tactic: Defense Evasion

Defense Evasion remains the single most dominant tactic. This includes the evasion of Endpoint Detection and Response (EDR) and firewalls.

The techniques used in 2025 reveal an adversary that is not just hiding, but actively 'wearing the skin' of legitimate software.

Top 5 Defense Evasion Techniques

1. **Process Injection (T1055)** 6.6%
   The ultimate camouflage. Attackers inject malicious code into the memory of legitimate processes (like web browsers or system tools). They don't just hide among your applications. They hide inside them.
2. **File Deletion (T1070.004)** 6.3%
   A disciplined enemy cleans up. They actively wipe files, such as malware payloads or staged data. A sub-technique of Indicator Removal.
3. **Indicator Removal on Host (T1070)** 6.0%
   The broader technique extends beyond just files to the system itself. Attackers clear event logs and command history to scrub the timeline. They are wiping their fingerprints to prevent reconstruction of the attack.
4. **Modify Registry (T1112)** 5.7%
   Attackers manipulate the registry to hide configuration settings, disable security controls, or establish persistence without dropping files.
5. **System Checks (T1497)** 5.5%
   Before acting, the malware checks the environment (time, user activity, system specs) to ensure it isn't inside a security sandbox or analysis tool. If it senses a trap, it stays dormant.

#2 MITRE Tactic: Discovery

Before they strike, they map. The techniques in this phase show an adversary acting less like a hacker and more like a sysadmin.

Top 5 Discovery Techniques

1. **System Checks (T1497.001)** 8.3%
   The top technique is an act of self-preservation. The malware checks the environment (time, mouse movement, hard drive size) to determine if it is inside a real victim machine or a security analyst's sandbox.
2. **System Information Discovery (T1082)** 8.2%
   The malware catalogs the OS version and environment details. They are analyzing the specific build to pinpoint missing patches and identify vulnerabilities ripe for exploitation.
3. **File and Directory Discovery (T1083)** 7.9%
   This is the quiet hunt for value. Attackers scan the file system to locate sensitive data or credentials, ensuring that when they exfiltrate data, they take only what is valuable.

4. **Process Discovery (T1057)** 6.8%
   The malware surveys the battlefield by listing running processes. It is hunting for threats to its own survival, specifically scanning for EDR agents or Antivirus software to avoid or disable.
5. **Remote System Discovery (T1018)** 6.7%
   Finally, they look outward. By identifying other endpoints and servers on the network, they map the path for lateral movement. This ensures the infection doesn't stop at a single machine.

#3 MITRE Tactic: Command and Control

This tactic represents the lifeline of the attack. The top techniques reveal that adversaries are no longer building new roads. They are driving on the highways you already use.

Top 5 Command and Control Techniques

1. **Application Layer Protocol (T1071)** 25.5%
   Attackers hide commands inside standard application layer protocols to bypass perimeter defenses. By wrapping malicious data in common traffic like DNS, their communications look like routine network noise to security controls.
2. **Ingress Tool Transfer (T1105)** 9.4%
   Once the silent channel is established, they use it. This technique marks the moment the Dropper (discussed in Part I) pulls down the next stage of the attack, transferring tools or files from an external server to the compromised victim.
3. **Asymmetric Cryptography (T1573.002)** 9.4%
   Even if you catch the traffic, you cannot read it. Attackers use robust SSL/TLS encryption, often with valid certificates, to blind defenders to the content of the communication.
4. **Multi-hop Proxy (T1090.003)** 9.3%
   This is the anonymizer connection. Traffic is routed through a maze of proxies (like Tor) to obscure the true destination.
5. **Web Protocols (T1071.001)** 9.0%
   Attackers leverage HTTP/HTTPS to mask their tracks. To a traditional firewall, this malicious traffic looks identical to a user browsing the web, allowing it to exit the network unchallenged.

Defender's Intel

This data confirms a harsh reality. Traditional tools cannot see what looks like normal business activity. The adversary is no longer at the gate, they are inside, cloaked in legitimate traffic.

If your defense relies on blocking 'bad' files, you will miss the 'good' files acting badly. To defeat the invisible enemy, we must stop hunting for the malware and start hunting for the behavior. Their footprints.

PART IV

Finding the Footprints of the Invisible Enemy

The era of 'keeping them out' is over. When the adversary uses legitimate credentials, encrypted channels, and commercial marketing tools (like Keitaro) to enter your network, the perimeter becomes irrelevant.

If the enemy is invisible, building higher walls is a waste of resources. The only winning strategy for 2026 is radical visibility.

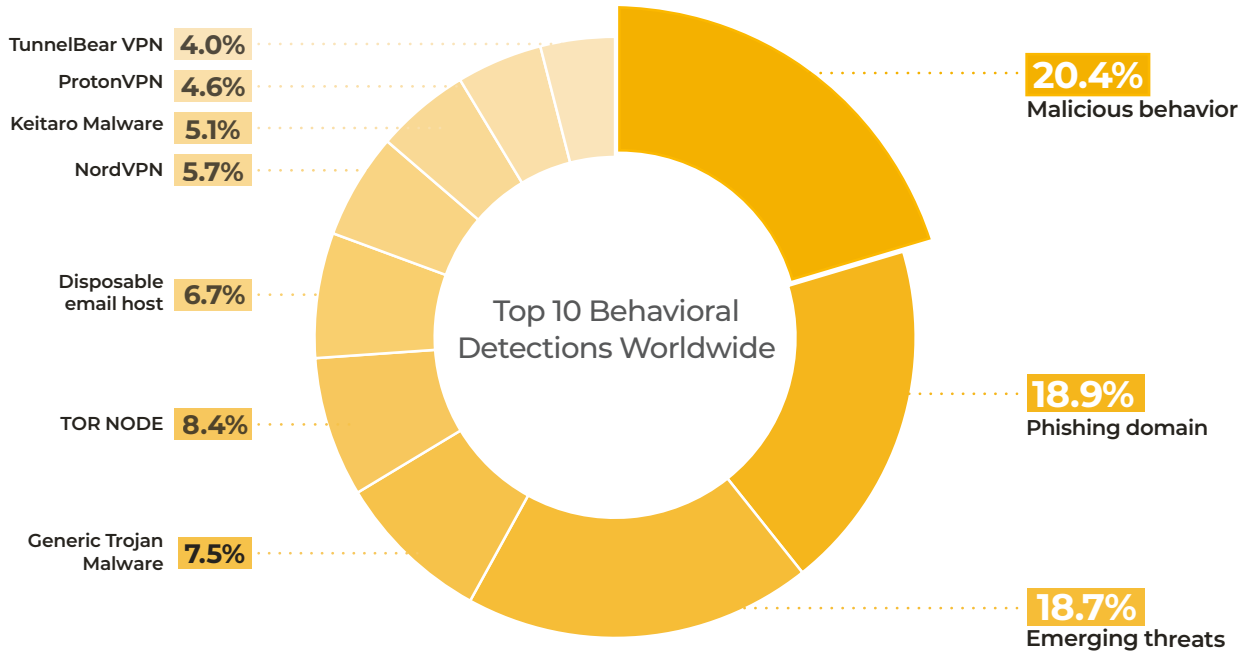
We must shift our philosophy from prevention to 24/7 behavioral observation across the network. This means operating under a single, uncomfortable assumption: we are already compromised.

In a world where attacks gain a foothold in a millisecond with AI, you don't have the luxury to respond in hours or days. Both visibility and response must be automated and immediate.

If you cannot see the malware, you must look for the evidence of its operation. Every digital asset leaves a trace. No matter how stealthy the enemy becomes, it must communicate to survive. It must call home.

Data From Lumu's AI-Driven Behavioral Detections

The following data represents not what we stopped at the gate, but what we found already inside. Threats that had bypassed firewalls, EDRs, and secure gateways.



The prevalence of **Malicious Behavior** (specifically **DNS Tunneling** and **DGAs**) at the top of this list is the smoking gun. It confirms that while endpoints were reporting 'All Clear', the network layer tells the truth.

Malicious Behavior

Lumu's AI-driven behavioral detections system's top alert was for **Malicious Behavior**. This represents a critical finding. Not a specific malware but an **active**, **ongoing compromise** inside the network.

This category combines two of the most evasive tactics:

- **DNS Tunneling:** The silent exfiltration highway. Attackers encode stolen data into complex DNS queries. To a standard filter, it looks like web traffic. To a behavioral engine, it looks like a distinct, rhythmic pulse of data leaving the building.
- **Domain Generation Algorithm (DGA):** The evasion engine. When a C2 server is blocked, the malware automatically generates thousands of new random domain names to find a new path out. Lumu detects this not by knowing the domains in advance, but by seeing the pattern of rapid, failed queries. It sees the desperation of the malware trying to phone home.

What is the takeaway from this? You cannot block what you don't know. But you can detect the behavior of the unknown. If an asset is querying 5,000 random domains in a minute, it is compromised. Regardless of what your antivirus says.

Phishing Domain

The second most common detection is when the fish has taken the bait. In Part I, we identified Phishing as a top tool, and this data confirms it is breaking through defenses.

These are not just phishing links. These are **active connections** to domains specifically crafted for credential theft or malware delivery **that have already bypassed other security filters**. This detection finds the point-of-entry, catching the threat at the very beginning of a successful breach.

Emerging Threats

This category identifies the infrastructure the attacker is building for future attacks. **Emerging Threats** are Newly Registered Domains (NRDs) that Lumu's validation algorithm flags as malicious. This judgment is based on their registration, infrastructure, and other high-risk metrics.

Adversaries bulk-register thousands of cheap domains to use for a single campaign. A mature defense strategy treats recency as a risk factor. If a corporate laptop is communicating with a domain that was registered ten minutes ago, that is an immediate anomaly.

Adversaries bulk-register thousands of these domains to be used for DGA, tunneling, or phishing campaigns. They conceal malicious traffic as legitimate DNS queries and direct it to NRDs.

These NRDs, often created by DGAs, have no negative reputation and thus bypass static blacklists. Sophisticated attackers also use 'domain warming', a technique for artificially inflating a new domain's reputation.

The malware on a compromised system then uses DNS tunneling to contact a C2 server hosted on one of these prepared domains. A proactive defense requires correlating the malicious behavior (tunneling) with the high-risk infrastructure (NRDs).

Find the Footprints: Your Battle Plan for 2026

1 See the Unseeable (Behavioral Detection)

You cannot hunt a shapeshifting enemy by looking for its old forms. You must look for its footprints. This means Network Detection and Response (NDR), like Lumu Defender.

- **Watch for DNS Tunneling:** Behaviorally model legitimate DNS traffic to instantly spot the subtle anomalies of a tunnel used for Command and Control.
- **Be Alert to DGA:** Detect the rapid, algorithmic generation of domains to block attack infrastructure before it activates.

2 Map Your Battlefield (Threat Surface Management)

You cannot protect what you cannot see. The attacks of 2025 thrived in unmanaged corners like shadow IT and forgotten IoT devices.

- **Eliminate Blind Spots:** Move beyond static asset inventory. Use tools (like Lumu Discover) to gain real-time visibility into every asset communicating on your network to reduce the attack surface. Ensure your NDR is designed for a hybrid world where traffic flows directly to the cloud from endpoints in coffee shops or homes.

3 Build an Active Defense (Operationalizing Intelligence)

Visibility without action is just organized negligence. Intelligence must be instantly operationalized.

- **The Watchman (NDR):** Ensure high-fidelity behavioral detections trigger immediate, automated blocking of malicious connections (Lumu Defender).
- **The Fortress (Zero Trust):** Assume the breach has happened. Use rigorous segmentation to ensure that if the enemy gets in, they cannot move laterally.
- **The Scout (External Intelligence):** Integrate advanced threat intelligence (like Maltiverse) to spot new attacker infrastructure before it targets you.
- **The Patrol (Threat Hunting):** Shift from alert-chasing to proactive hunting, using behavioral data to root out dormant threats.

The lesson of this report is not that we are losing. It is that the game has changed.

The data from 2025 serves as a stark wake-up call. The adversary is resilient, adaptive, and largely invisible to traditional defenses. But invisibility is not invincibility.

If your security strategy for 2026 relies solely on blocking known threats, you are as good as compromised. Your battle plan requires a fundamental shift in posture. We must move from passive defense to active, continuous vigilance.

You must assume the adversary is already inside.

By shifting your focus from the malware, which constantly changes, to the behavior, which cannot be hidden, you strip the adversary of their greatest advantage. The battle for 2026 will not be won by building higher walls, but by turning the lights on inside the fortress.

www.lumu.io