LUMU

COMPROMISE

REPORT 2024

Hackers are sidestepping traditional defenses. As the threat landscape rapidly evolves, we reveal cybercriminals' latest tactics, where they are targeting, and vulnerabilities they're exploiting. Discover the proactive steps you need to take to protect your organization from the most up-to-date cyber threats.

Executive Summary

The year 2024 has brought a surprising variety of cyberattacks, making for interesting reading. We have seen everything from the Snowflake incident to the exposure of nearly three billion personal records in the National Public Data breach. The worrying trend of ransomware attacks on government and education has continued.

The cybercrime ecosystem is concerningly vibrant and diverse. To have success, there is one key factor that remains important to note – that cyberattacks continue to bypass the standard, traditional cybersecurity defenses in place at most organizations.

Lumu's Compromise Report 2024 hones in on those cyberattacks that have evaded cybersecurity stacks and provides insights into the attacks most likely to harm organizations.

Key Findings

Phishing

Phishing remains one of the most persistent and evolving threats, continuing to bypass traditional defenses. 13.6% of all phishing attempts that Lumu detected had targeted the financial sector, closely followed by government institutions, at 13.5%.

Infostealer Malware

According to the most recent cybersecurity incident reports, infostealer malware continues to be one of the most common malwares detected and is growing in sophistication. Infostealer malware steals credentials that can, then provide initial access for launching secondary attacks.

Ransomware

When a cyberattack reaches later stages in the chain, the delivery of ransomware has the potential to create a devastating impact on an organization. The most detected families in this report, such as Cuba and Blacksuite (Royal) Ransomware, have targeted high-value sectors including finance and IT services.

Other Malware Tools

Lumu identified over 8,800 distinct malware families, with Droppers, Remote Access Trojans (RATs), and Backdoors being particularly noteworthy. These tools are crucial in later stages of the attack chain, facilitating the deployment of additional malicious payloads or enabling persistent access to compromised systems.

MITRE ATT&CK® Techniques

We observed several common adversarial techniques through the MITRE ATT&CK® framework for identifying and responding to cyberattacks. The insights provided by MITRE's tactics, techniques, and procedures (TTPs) are critical for organizations to adapt their cybersecurity posture, although they must be tailored to the threats seen by each network.

Index

Initial Access Trends

The trends in 2024 have underscored the persistent threat of phishing and infostealer malware as sources of initial access. The following sections delve into the specifics of these threats, their impact, and their evolving tactics.

Phishing

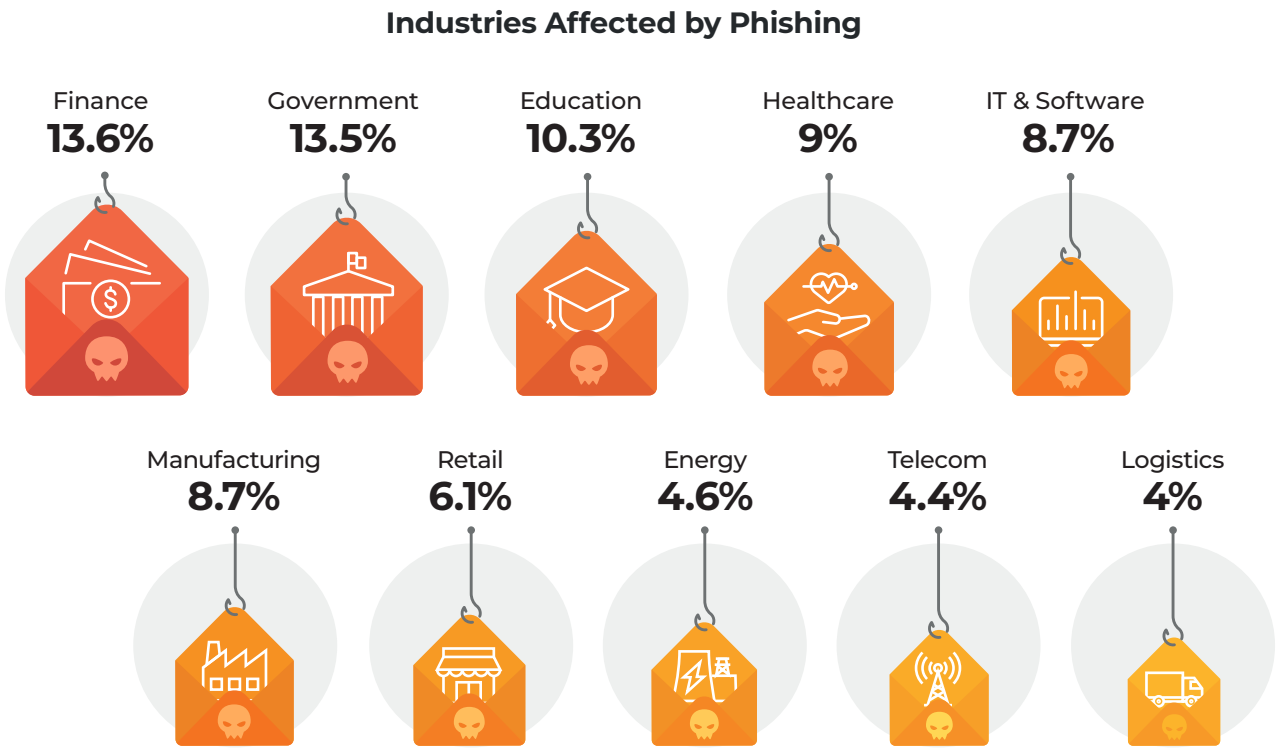
Phishing, including all forms of malicious emails seeking to obtain sensitive data from the victim, remains one of the leading initial-access threat vectors, with a significant number of sub-techniques continually being deployed in the wild.

Additionally, the use of social engineering is a key factor in facilitating very specific, handcrafted phishing attacks that can bypass common defenses like email security solutions, and endpoint security tools.

The Lumu platform has detected a significant number of phishing attempts, highlighting its status as a persistent and widespread problem.

Top Industries Affected by Phishing

In 2024, the primary target for phishing campaigns was the financial sector, followed closely by government institutions. These sectors are prime targets for phishing due to their wealth and sensitive data. The geopolitical importance of these sectors also makes them especially attractive to foreign actors.



In addition to the financial and government sectors, attackers also focused on two areas of society that directly influence the daily lives of millions: education and healthcare. Again, in part, due to the value and sensitive nature of data stored by these sectors, they have become high-value targets.

In particular, local government and education have been targeted due to weaker or less joined-up defenses and their need to embrace rapid technological advancements. These sectors were significantly impacted by ransomware attacks in 2023 and the first quarter of 2024, highlighted in our Local Government and Education Cybersecurity Advisory.

These phishing attacks can leverage initial access by using different techniques. However, one of the most concerning trends is the use of phishing to deploy infostealer malware.

Infostealer Malware

Infostealers are a type of malware that is primarily designed to breach computer systems and steal sensitive information. Infostealers are frequently deployed through phishing and malvertising campaigns, then the information they steal is sold on the dark web and used in a variety of attacks.

Infostealers have seen a notable rise in prevalence and sophistication in recent years. According to our data, this form of malware has disproportionately targeted organizations in the USA.

Why Is Infostealer Malware Considered an Initial Attack Vector?

Infostealers can be considered an initial vector for adversaries as attackers often tend to buy information stolen through this method to save efforts in creating malicious campaigns. There are two main uses for this type of malware that are important to highlight.

Firstly, the credentials stolen by this malware can be sold and provide a way for threat actors to gain access to networks. In this way, the infostealer becomes the initial attack vector for a multitude of attacks.

Secondly, while infostealers were, originally, only designed to steal credentials, they have evolved to be capable of much more. Certain types of infostealers can now deploy additional capabilities to conduct privilege escalation as well as deploy other types of malware. As a result, once an infostealer has completed its initial goal of stealing credentials, it becomes the beachhead from which a secondary attack, like ransomware, can be launched. For more detail about Infostealers, The Silent Threat Compromising the World One Password at a Time.

The Credential Marketplace: Driving Demand for Infostealers

The underground economy surrounding infostealer malware has created a thriving market for stolen credentials. As well as ransomware attacks, the availability of high-privilege and organization-specific credentials fuels a wide range of cybercriminal activities, including credential-stuffing attacks and targeted intrusions.

On top of this, the marketplace significantly lowers the barrier for attackers, enabling even less sophisticated actors to purchase access to valuable accounts and launch further attacks with relative ease.

The credential market not only drives the demand for infostealers but also perpetuates a cycle of continuous compromise, where stolen credentials from one breach lead to further infiltrations.

The credential marketplace, therefore provides the financial incentive for infostealers and is also the reason they have become a significant threat to organizations worldwide.

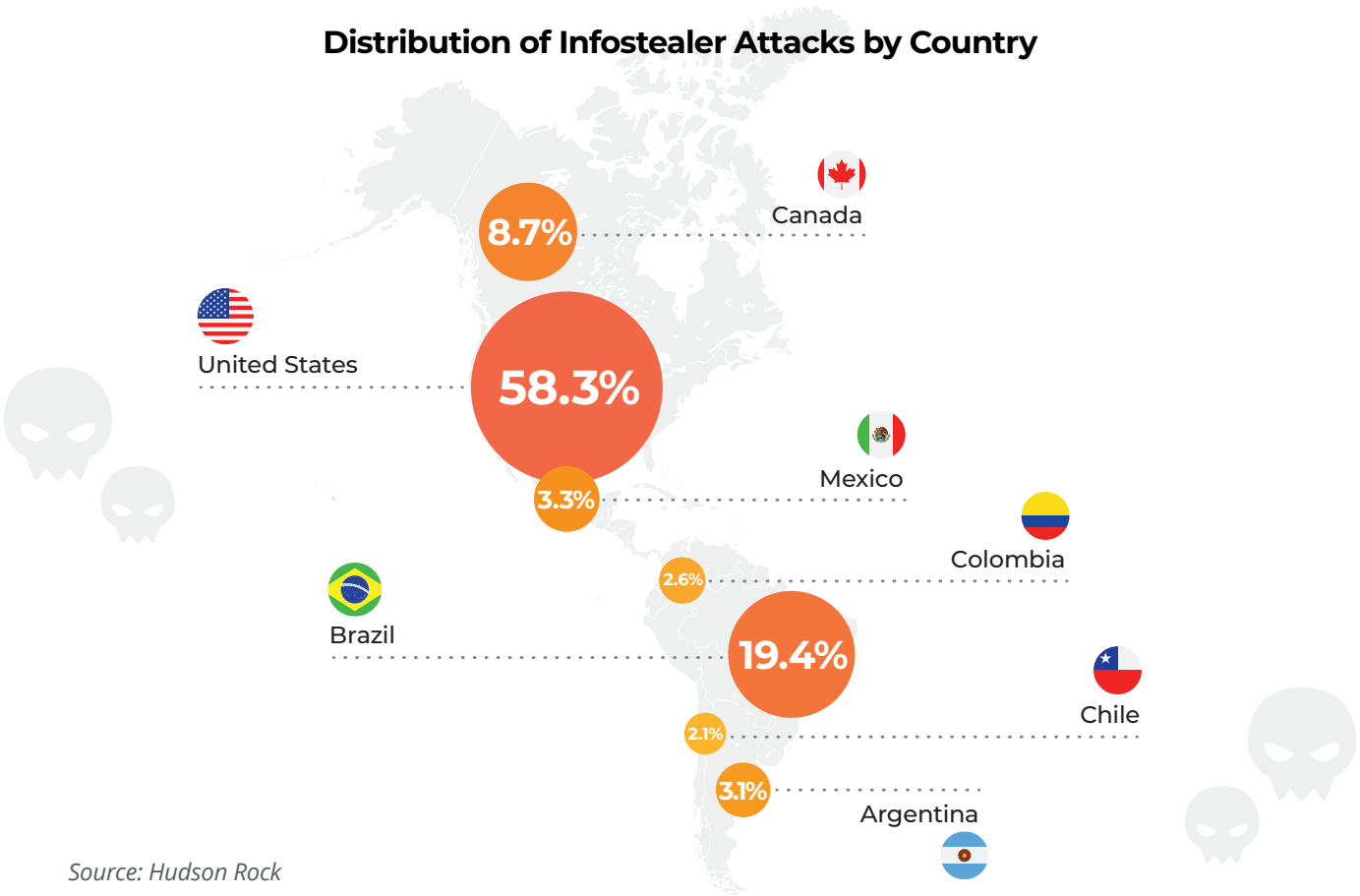
Case Highlight: Snowflake Incident

Infostealers are a significant headache for many in cybersecurity. The most public case this year was the cyberattack compromising Snowflake accounts in several companies, where infostealer malware was used to acquire credentials that were then used in a large number of subsequent attacks.

Regional Impact of Infostealers

This chart shows the countries most affected by the infostealers across the Americas. The outlook has remained stable since early 2024, with the USA at the top, followed by Brazil and Canada.

Distribution of Infostealer Attacks by Country

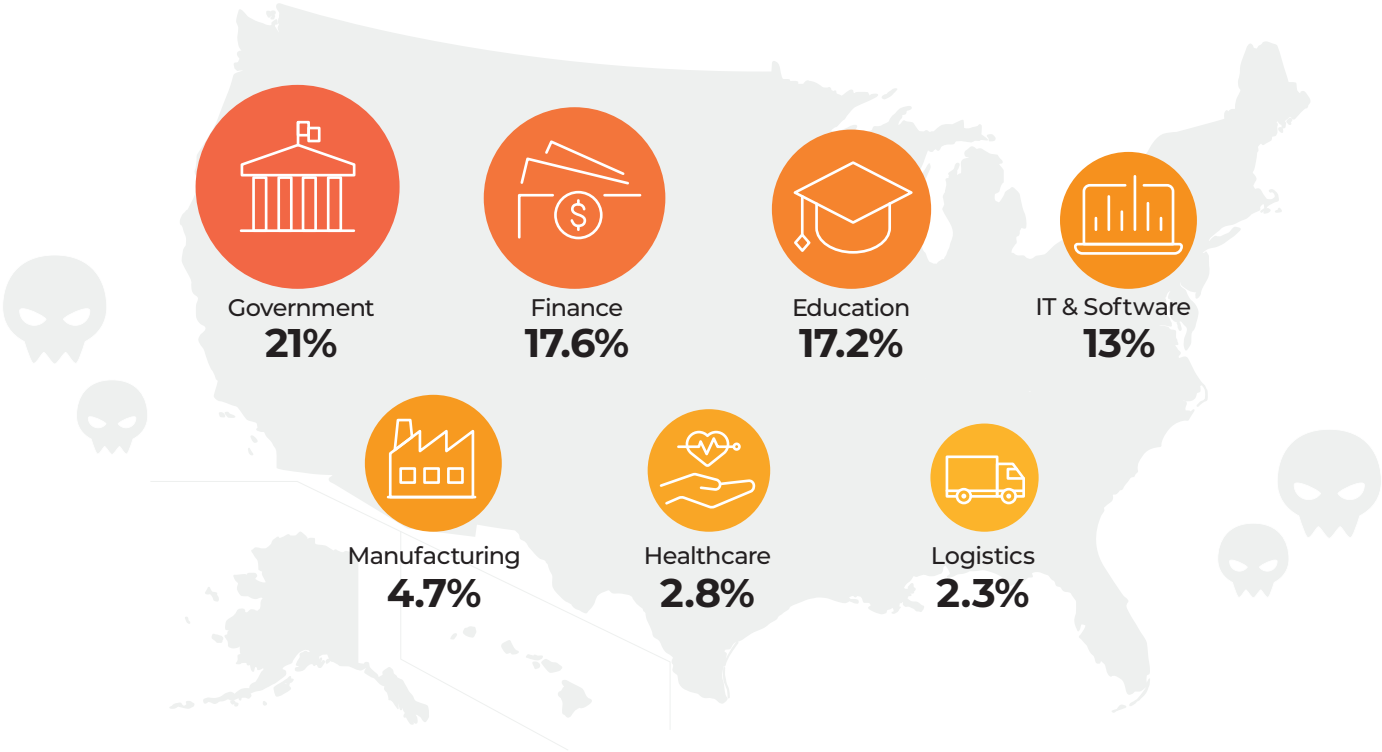


Source: Hudson Rock

The Sectors Most Impacted by Infostealers

In the USA, the sectors that are most targeted by infostealers are government, finance, and education.

Sectors Affected by Infostealers in the USA



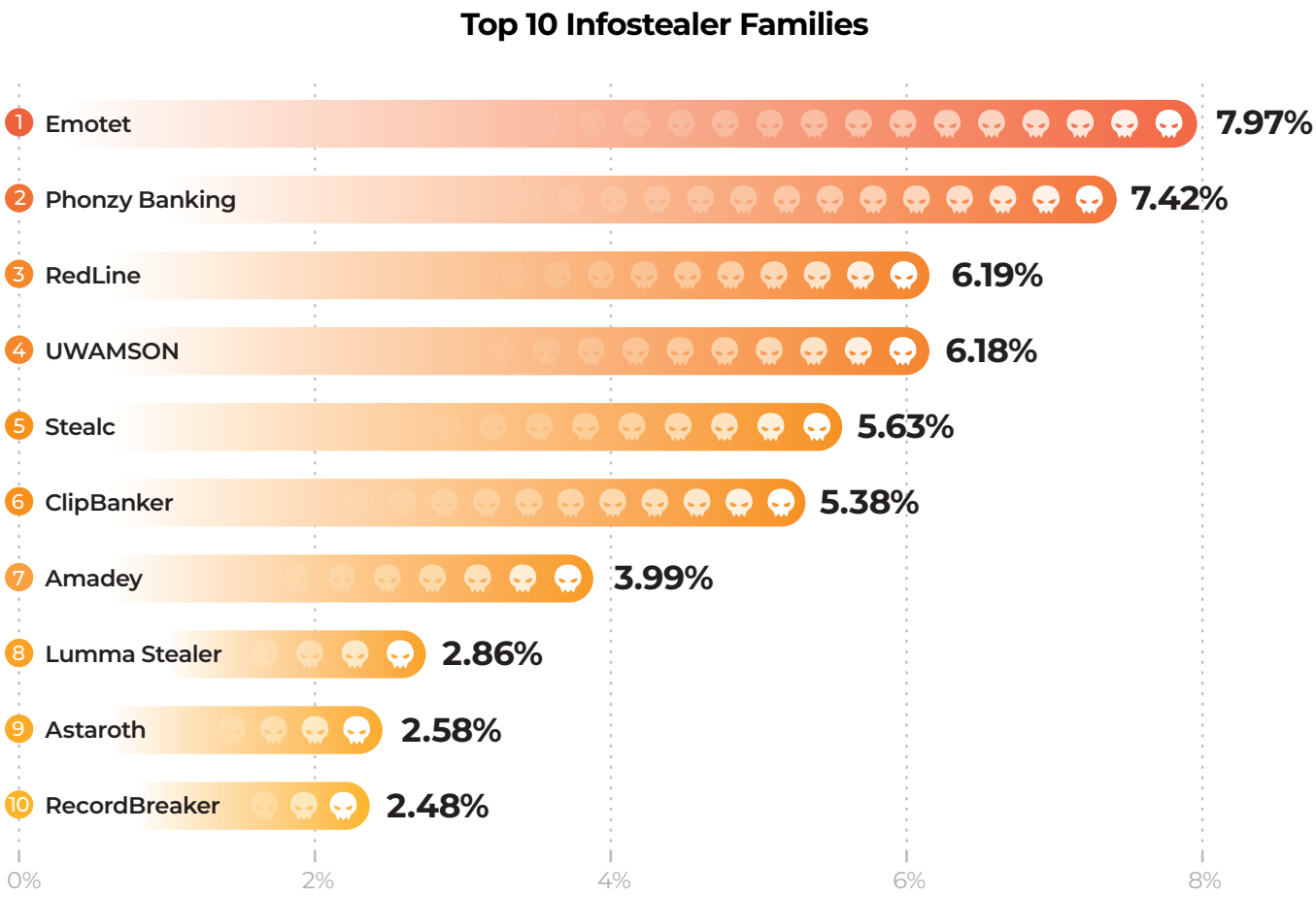
Local and state governments frequently face significant cyberattacks due to the value of their assets, the resources available to them, and their access to sensitive national security information.

The education sector faced several incidents in late 2023, and this trend has continued into 2024. As schools and universities increasingly rely on digital platforms for remote learning and data storage and management, they become attractive targets for cybercriminals.

Additionally, IT and software service companies, despite having robust cybersecurity infrastructures, have been heavily affected. This category includes Managed Service Providers (MSPs), software vendors, software solutions, tech devices vendors, networking companies, and more. It is important to note that, in these statistics, MSP incidents are recorded independent of their clients, who could be in other types of industries.

Top Infostealer Malware Families

To effectively combat infostealer attacks, it is important to understand the tools and techniques used, including the specific types of malware. We have collated our data to rank the top ten infostealers observed, dividing them into groups or families.



The infamous malware infostealer Emotet remains the predominant family group at 7.97% of all detections, even after being on the scene for over a decade. Mid-2023, Emotet experienced a notable resurgence, and data indicates it continues to have significant prevalence.

It is worth noting that, due to recent law-enforcement operations targeting their leaders, it is expected that Emotet's activity will sharply decrease in the second half of the year.

Common infostealers, such as RedLine, Stealc, and Amadey, follow Emotet in continuing the strengthening trend we discussed in early 2024.

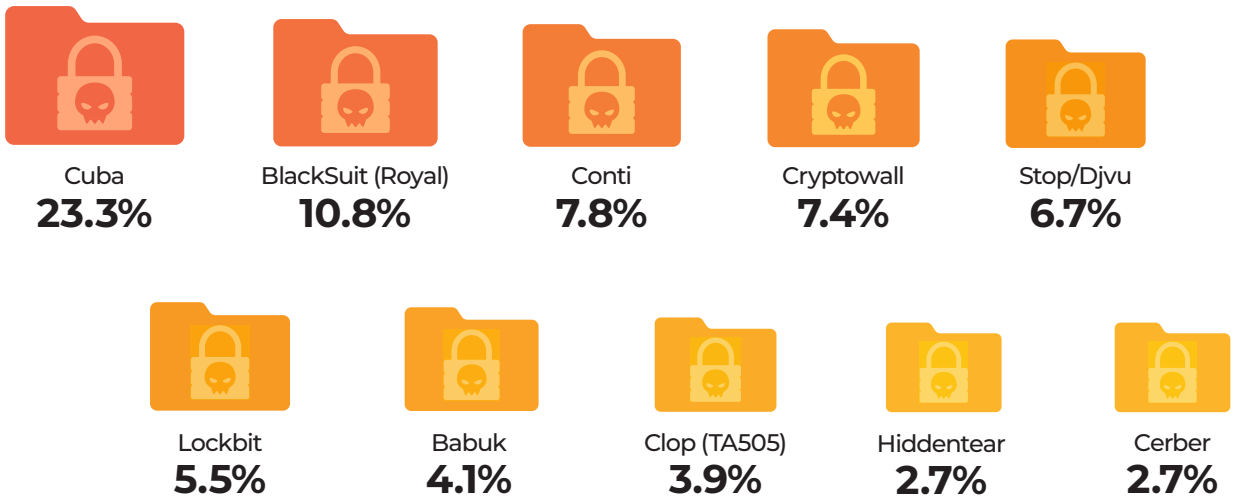
There are several banking trojans in the top ten, and, in fact, they make up 25.59% of the infostealers that we encountered. Banking trojans specialize in stealing credentials from financial entities and include Phonzy Banking, the number two in the list at 7.42%, and ClipBanker, in sixth place.

Ransomware

Ransomware poses a high level of risk and has significant implications for companies if successfully deployed. For this reason, we are going to highlight, and examine in more detail, the most prevalent ransomware families detected by Lumu this year.

Our cyber threat intelligence team mapped 65 major ransomware families (each with their own variations).

Ransomware Families 2024



By a notable margin, Cuba Ransomware has been the most detected ransomware, with a significant rise in activity, and accounts for 23.3% of incidents. In second and third place are Blacksuite (Royal) Ransomware and Conti Ransomware, which continue to be persistent threats.

A positive trend has been recorded, however, as Lockbit sees a decrease in detections after it was taken down in early 2024, dropping to sixth position.

Cuba Ransomware

The most prevalent malware on this list is Cuba Ransomware. The ransomware gang known as Cuba first came to the attention of cybersecurity analysts in late-2020 under the name Tropical Scorpius. It primarily targets organizations across the Americas and Europe, focusing on industries such as oil, financial services, government, and healthcare.

Using sophisticated tactics like exploiting software vulnerabilities, social engineering, and compromised Remote Desktop Protocol (RDP) connections [T1563.002], the group encrypts victims' files and demands ransom for decryption keys.

Cuba Ransomware stands out for its use of tools such as SystemBC, a SOCKS5 backdoor, capable of communicating through TOR to anonymize their activity and make post-incident investigations more difficult.

Lumu detected several attempts of this type of connection associated with this actor. In our dataset, most activity registered was in Mexico, 27.5%, followed by Argentina, 17.8%.

BlackSuit (Royal) Ransomware

Royal, now known as the BlackSuit Hacking Group, is a relatively new threat actor that has profited significantly from targeting healthcare organizations, private companies, and local governments. Initially known as Zeon when it first emerged in 2022, the group rebranded to Royal in September of that year. Most recently, in August 2024, they rebranded once again, this time adopting the name BlackSuit.

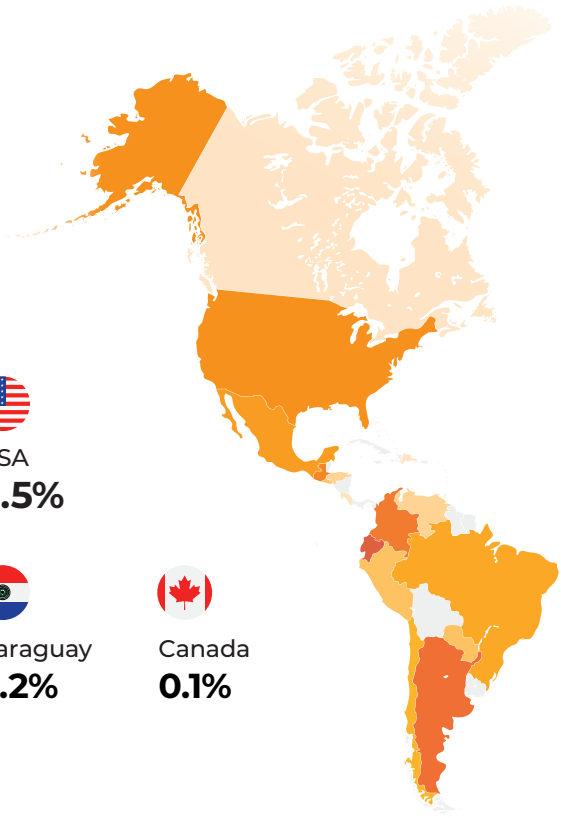
One of the most notable attacks by this group was the city of Dallas, Texas, in May 2023. The incident had a major financial impact, with direct mitigation costs estimated at $8.5 million and 39,590 man-hours spent on remediation efforts.

Another significant attack by Royal occurred in late 2022, targeting the Silverstone Formula One circuit. Silverstone only became aware of the breach when Royal posted the announcement on their leak site.

BlackSuit, like many prominent new ransomware gangs, employs techniques to bypass and disable EDR systems [T1562.001]. Its primary attack vectors often involve RDP and SMB credentials, typically obtained through infostealers [T1021.001].

Distribution of Ransomware Attacks by Country

These ransomware attacks have been recorded across North and South America. Ecuador, Argentina, Colombia, Guatemala, the USA and Mexico were the six countries where most ransomware attacks were detected.



Ecuador **16.9%**

Argentina **16.7%**

Colombia **14.5%**

Guatemala **10.6%**

USA **9.5%**

Mexico **9.5%**

Brazil **8.8%**

Chile **4.7%**

Peru **3.9%**

Paraguay **2.2%**

Canada **0.1%**

RansomHub Ransomware

RansomHub, a Ransomware-as-a-Service (RaaS) operation that surfaced in February 2024, has quickly gained notoriety by compromising over 210 organizations across key sectors, including healthcare, government services, and critical infrastructure.

In this business model, RansomHub receives a fee to provide the ransomware and tech support. Affiliates use the software to carry out attacks, encrypting and exfiltrating their victims' data.

The group has drawn affiliates from groups like ALPHV (BlackCat) and LockBit, broadening the reach of RansomHub's Ransomware. During the period under review, both BlackCat and LockBit were detected in significant incidents, highlighting the widespread nature of this threat across various sectors.

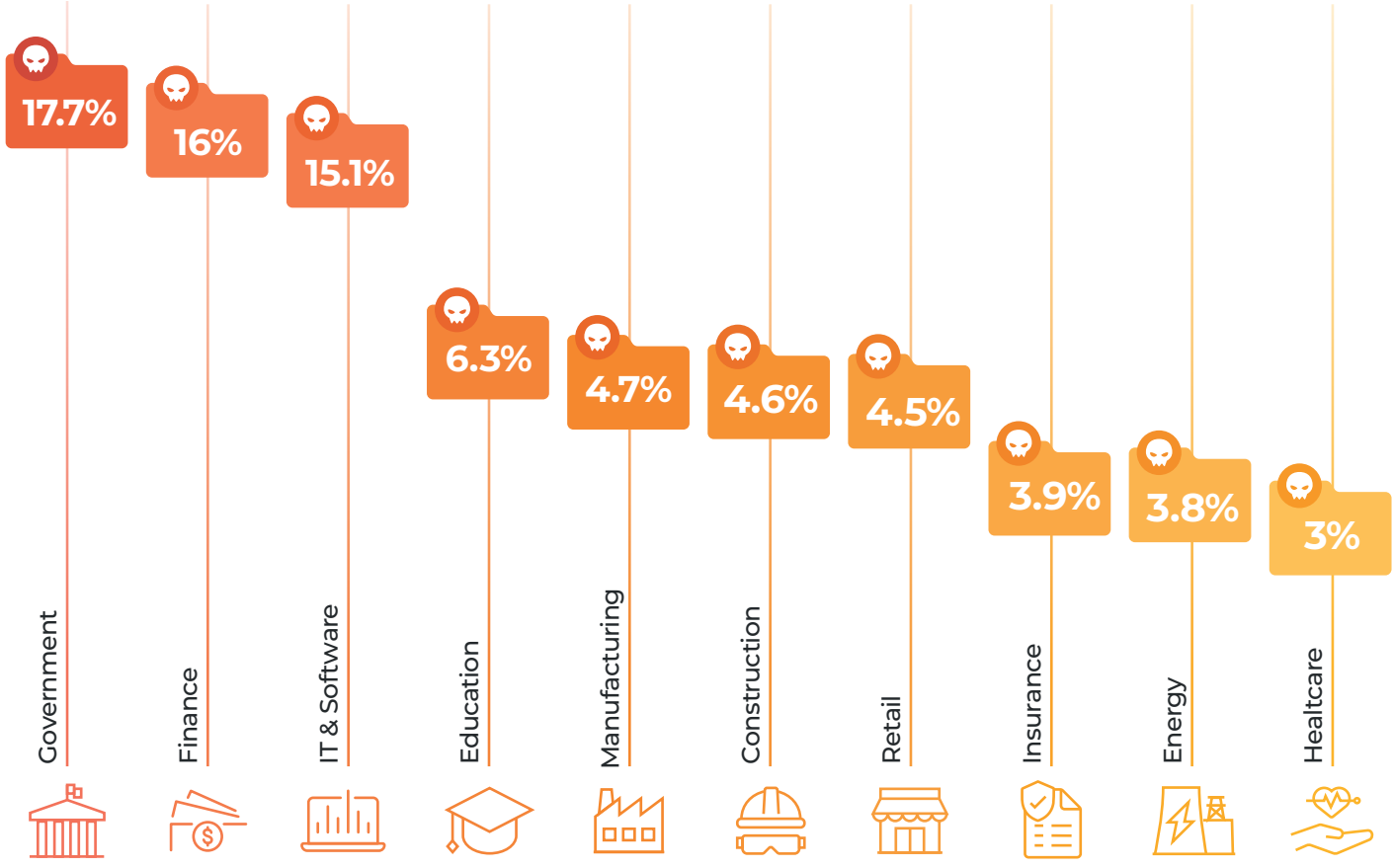
To read more about RansomHub, read our advisory: CISA Releases Advisory on RansomHub Ransomware Attacks.

Industies Targeted by Ransomware

In our ransomware statistics, government institutions occupy the top spot, consistent with the initial vector trends. Again, both the financial and geopolitical incentives make government, whether at state or local level, an especially attractive target.

The finance sector, IT and software services, education, and manufacturing round off the top five most targeted industries. The high-value targets, sensitive data, and critical nature of these five sectors make them especially attractive to ransomware attackers.

Ransomware by Sector



Top Malware Tools Used by Threat Actors

Lumu's threat intelligence team reported detections for over 8,800 distinct malware families. These families were categorized into several groups, based on behavioral and functional similarities.

Infostealer malware, dropper malware (trojans designed to install malware), and RATs (Remote Access Trojans) dominate the detection statistics. However, all the malware families, tools, and malicious behavior mentioned below remain relevant and significant threats across the cybersecurity landscape.

24.6%

Droppers: used later in the cyber kill chain to download, deliver, and install additional malicious payloads onto a victim's system. Predominantly observed in North America.

11.3%

PUA: a Potentially Unwanted Application (PUA) is a type of software that may not be malicious, but can negatively affect the performance or security of a user's system. PUAs include adware or toolbars.

5.9%

Backdoors: malware that allows unauthorized access to a victim's system by bypassing normal authentication mechanisms.

3.6%

Mining: exploits a victim's computing resources for unauthorized cryptocurrency mining.

2.6%

Ransomware: encrypts or exfiltrates a victim's files, or locks down their system, then a ransom payment is demanded for decryption, non-disclosure, or restoration of access.

1.5%

Botnets: network of compromised devices controlled remotely by an attacker for malicious purposes.

11.7%

Infostealers: primarily designed to collect sensitive information from the victim's system, such as passwords, financial data, and personal information.

9.2%

RATs: Remote Access Trojans (RATs) are often deployed in focused campaigns, designed to covertly take remote, unauthorized control of a victim's system.

4.6%

Hack Tools: designed to assist in penetration testing or security auditing activities, such as exploiting vulnerabilities, cracking passwords, or bypassing security measures, but ultimately, also for malicious attacks. Examples include Cobalt Strike, Sliver, and Mimikatz.

3.1%

Android-Specific Malware: designed specifically to operate on Android platforms.

1.6%

Sinkholes: a security technique used to redirect malicious traffic to a controlled environment for analysis and mitigation process. *Not a malware, but an indicator of unclassified malware.

20.3%

Others: including spam campaigns, malvertising domains, and generic malware lacking a specific purpose.

MITRE ATT&CK® Matrix Techniques & Trends

The MITRE ATT&CK® Matrix is a knowledge base that organizes the tactics, techniques, and procedures (TTPs) taken by threat actors in real-world attacks.

Administered by the non-profit MITRE Corporation, this repository helps cybersecurity professionals to understand what threat actors are trying to achieve with each action and how it can be countered.

The Matrix is categorized into fourteen tactics that follow each stage of an attack, beginning from Initial Access through to Exfiltration and Impact. Over 300 techniques and sub-techniques are allocated to these tactics.

The Top 10 Most Common MITRE ATT&CK® Techniques

Lumu's threat intelligence team has compiled a list of the ten attack techniques seen most often this year.

Malicious File – T1204.002 Execution

The attacker delivers a malicious file, often disguised as a legitimate document or executable file, and tricks the user into opening it, usually through social engineering or phishing. Once opened, the file executes malicious code, enabling the attacker to gain initial access or further compromise the system.

Windows Command Shell – T1059.003 Execution

The attacker utilizes the Windows Command Shell to execute commands, and control the compromised system. This may involve spawning new command shell processes or leveraging existing tools like PowerShell to carry out malicious actions.

Obfuscated Files or Information – T1027 Execution

The attacker disguises malicious files, code, or information to evade detection by security tools and analysts. This might involve encrypting, encoding, or otherwise obscuring content, making it difficult to identify or understand the true purpose of the data.

User Execution – T1204 Execution

The attacker tricks the user into executing malicious code or opening a harmful file, often through social engineering, phishing, or exploiting vulnerabilities in legitimate software. This allows the attacker to gain a foothold on the system and carry out further malicious activities.

PowerShell – T1059.001 Execution

The attacker leverages PowerShell, a built-in scripting language in Windows, to execute malicious commands and automate tasks. This grants the attacker significant control over the compromised system, allowing them to perform various actions like downloading malware, stealing data, or manipulating system settings.

Registry Run Keys / Startup Folder – T1547.001 Persistence

The attacker modifies the Windows Registry to add malicious entries under Run Keys or the Startup Folder. These entries automatically execute code or launch programs whenever the system boots up, allowing the attacker to gain persistence on the compromised machine.

Process Injection – T1055 Defense Evasion

The attacker forces a legitimate process to execute malicious code, effectively hiding the malicious activity within a trusted context. This can evade detection by security tools and allow the attacker to gain greater control over the compromised system.

System Information Discovery – T1082 Discovery

The attacker actively gathers information about the compromised system, including hardware, software, network configurations, and user accounts. This reconnaissance helps the attacker understand the environment, identify potential vulnerabilities, and plan further malicious activities tailored to the specific target.

Application Layer Protocol – T1071 Command and Control

The attacker utilizes legitimate application layer protocols, such as HTTP, HTTPS, or DNS, to blend malicious traffic with normal network activity. This can help evade detection and allow the attacker to communicate with compromised systems, exfiltrate data, or deliver additional malware.

It is important to note that half of the top-ten observed MITRE ATT&CK techniques are Execution techniques. This suggests that once attackers gain initial access, their primary focus is on executing malicious code within the compromised environment.

Observations and Threat-Informed Defense

The MITRE ATT&CK® Matrix provides critical strategic insights into the real-life threats being faced by organizations and networks. This threat information should be used to adapt cybersecurity stacks and postures to address the threats faced by organizations and shore up potential weaknesses.

Correlations between the identified threat trends and the most common MITRE ATT&CK techniques highlight the evolving strategies of cyber adversaries.

To effectively combat these threats, a threat-informed defense approach is essential. This strategic approach to cybersecurity combines company-specific threat intelligence with traditional security measures and threat analysis. Given feedback from our user base, we gathered observations to inform strategic changes to a cybersecurity stack under a threat-informed defense practice.

- **Infostealer Malware and Data from Local System (T1005)**

  The connection between infostealer malware and the Data from Local System technique emphasizes the evolving capabilities of infostealers to extract large volumes of private data without being detected.

  The ability of these malware types to bypass traditional defenses and operate covertly makes them a significant threat that requires advanced detection and response capabilities.

  Effectively combating infostealer malware requires a well-integrated cybersecurity stack. By ensuring that advanced endpoint detection, network monitoring, and threat intelligence systems work together seamlessly, organizations can quickly identify and respond to abnormal data access patterns. This integration enhances the overall defense, making it more difficult for infostealers to exfiltrate sensitive information undetected.

- **Command and Control (C2) via Application Layer Protocol (T1071)**

  The use of legitimate application layer protocols, such as HTTP and DNS, for Command and Control (C2) purposes presents a significant challenge for defenders. By blending malicious traffic with normal network activity, attackers can maintain control over compromised systems while evading detection and further developing their attack.

  This correlation between C2 tactics and the Application Layer Protocol technique underscores the importance of stopping attacks before they can cause significant damage or reach a stage where ransomware is deployed.

  Organizations should invest in continuous network traffic analysis solutions like Network Detection and Response (NDR) or Network Analysis and Visibility (NAV). These tools can distinguish between normal and malicious traffic, enabling faster detection and disruption of C2 channels. Integrating threat intelligence feeds into these systems will further enhance their ability to detect the novel behaviors associated with C2 activities, allowing for proactive containment before significant damage occurs.

- **Phishing and User Execution (T1204)**

  Phishing's success is driven by social engineering tactics that trick users into executing malicious code. Phishing remains a popular way of compromising systems because it continues to successfully evade defenses like email security and employee phishing training.

  While both of these security measures remain important, it is crucial to recognize that because of the volume of attacks involved, they will eventually fail. Recognizing this, it's crucial to adopt a defense-in-depth strategy that layers additional security controls, such as AI-driven phishing detection and user behavior analytics. This will catch what initial defenses might miss and stop these attacks before they cause significant harm.

It is important to reiterate that threat-informed defense requires cybersecurity defenses to be adapted to the threats that are specific to the individual organization or its peers. The observations made above are extracted from a wide group of organizations and should only be considered as general guidance and not as part of an organization-specific threat-informed defense strategy.

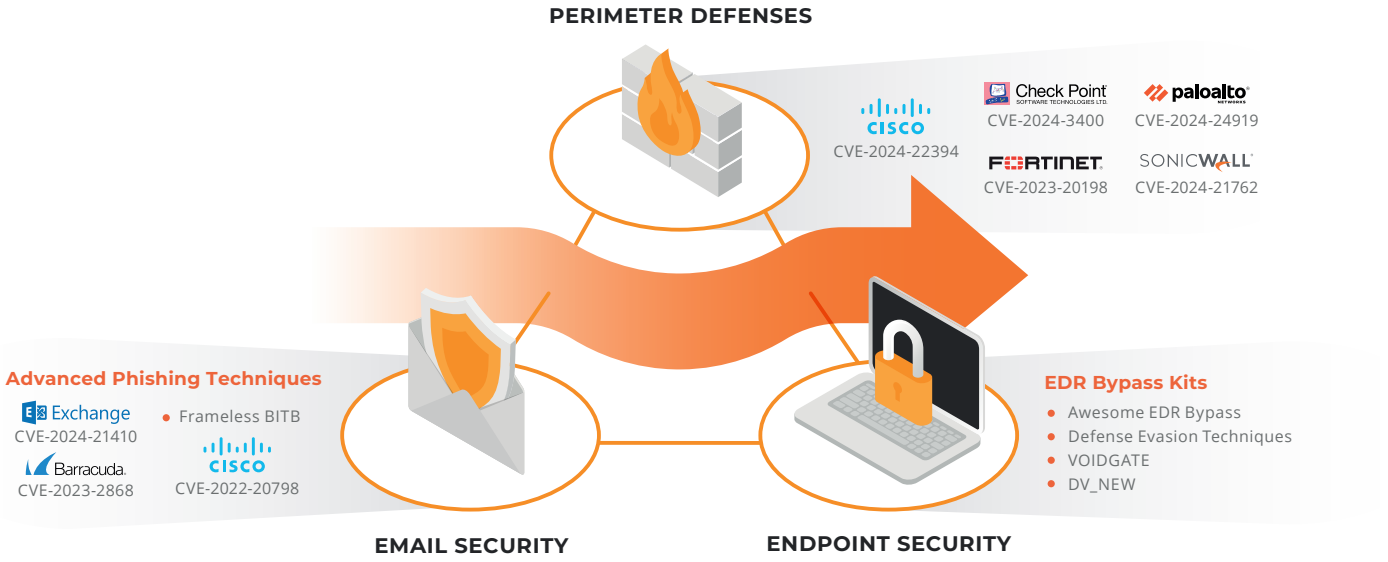
How Lumu Automates the MITRE ATT&CK® Matrix

For every compromise incident detected, the Lumu portal highlights the specific techniques associated with the attack. This association allows cybersecurity professionals to quickly understand what the threat actor is trying to achieve and respond accordingly.

Additionally, the Lumu Portal offers the Global MITRE ATT&CK® Matrix, which shows the aggregate of the most common techniques observed across all attacks targeting a specific enterprise. These insights allow SecOps teams to adjust their cybersecurity posture according to the threats and techniques they are facing most often.

Conclusions

The threat intelligence gathered by Lumu underscores a persistent reality: threat actors are able to bypass traditional elements of the cybersecurity stack to compromise networks. Phishing and infostealers, in particular, are adept at initial access, escalating their attacks by bypassing traditional defenses, such as firewalls, VPN, SASE or ZTNA tools, email security, and EDRs.



While traditional defenses remain crucial, given the observations in this report, it is clear that real-time network detection and response remains the best way to have complete visibility and stop cyberattacks that have bypassed defenses. The network, as the ultimate source of truth, provides critical evidence for identifying and mitigating compromises that evade other security measures.

It bears repeating that in all cases, the compromises reported here were detected by Lumu through the analysis or real-world network metadata. By continuously monitoring network traffic and analyzing metadata, organizations gain early-stage visibility into sophisticated attacks. This allows for proactive cybersecurity and the ability to take action before attacks escalate.

The broader insights from these attacks allow for better strategic defense. A proactive, threat-informed defense approach requires insight into the threats and adversarial techniques that organizations are facing 'in the wild', and aligning cybersecurity investments accordingly. Ultimately, the goal should be that security measures are responsive, dynamic, and able to detect the latest threats.

Defending against future threats requires more than just technology; it demands adaptability, resilience, and above all vigilance. And that vigilance is impossible without real-time network visibility.

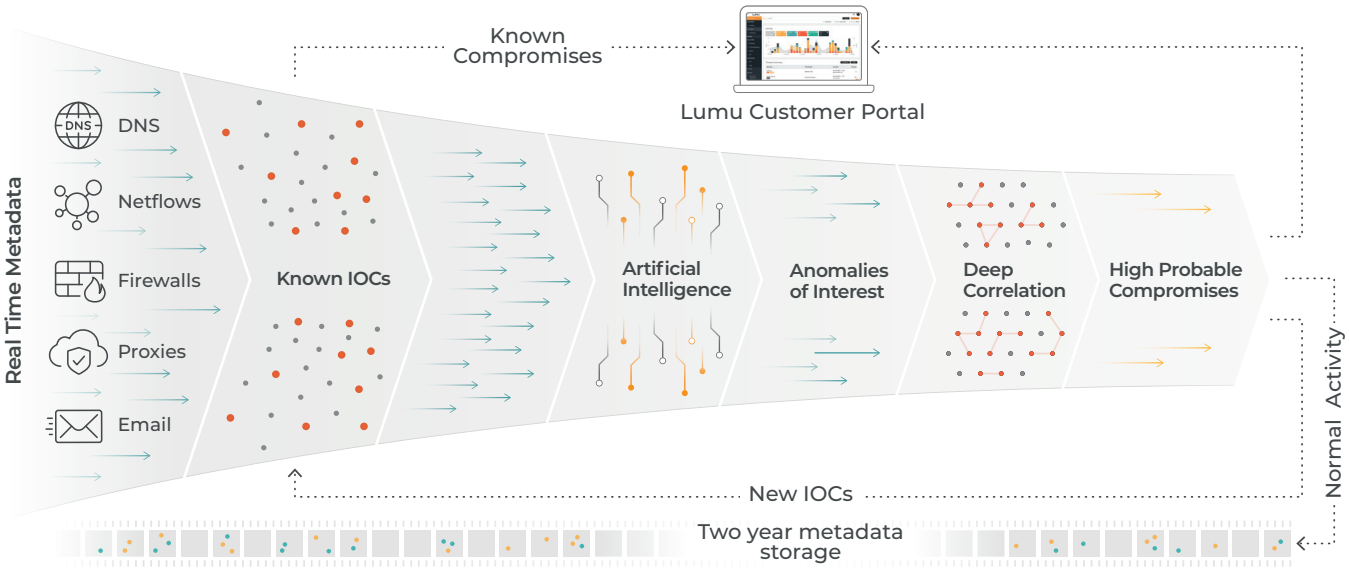
Methodology

Scope of the Report

Data in this report represents original findings from Lumu, based on detections made during the first half of 2024, unless noted otherwise. These statistics are the aggregate of detections made by Lumu across our customer base, which extends across the Americas. As a result, the data represented here shows the compromises that have been able to bypass traditional elements of the cybersecurity stack, primarily email security, perimeter defenses like firewalls, and endpoint protection like antivirus, EDR and XDR solutions.

How Lumu Detects Compromises and Responds to Threat Actors in Real Time

Lumu detects threats that are attempting to bypass, or have bypassed, traditional elements of the cybersecurity stack in real time, relying on the network as the ultimate source of truth.



The Illumination Process begins by analyzing real-time network metadata against hundreds of sources of known Indicators of Compromise (IOCs). Any identified matches are immediately reported, while the remaining metadata advances to the next phase. In this stage, artificial intelligence (AI) models establish a baseline of normal network behavior, enabling the detection of anomalies.

Any deviations from the norm are further investigated to determine if they represent genuine threats. By effectively filtering out false positives, the Illumination Process ensures that analysts' attention is focused on confirmed compromises.

When a threat actor is identified, Lumu triggers an automated response in milliseconds by orchestrating the defense with the existing cybersecurity stack. The end result is an autonomous threat-detection and response platform that increases cyber resilience without the complexity of traditional models based on SIEMs.

www.lumu.io

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