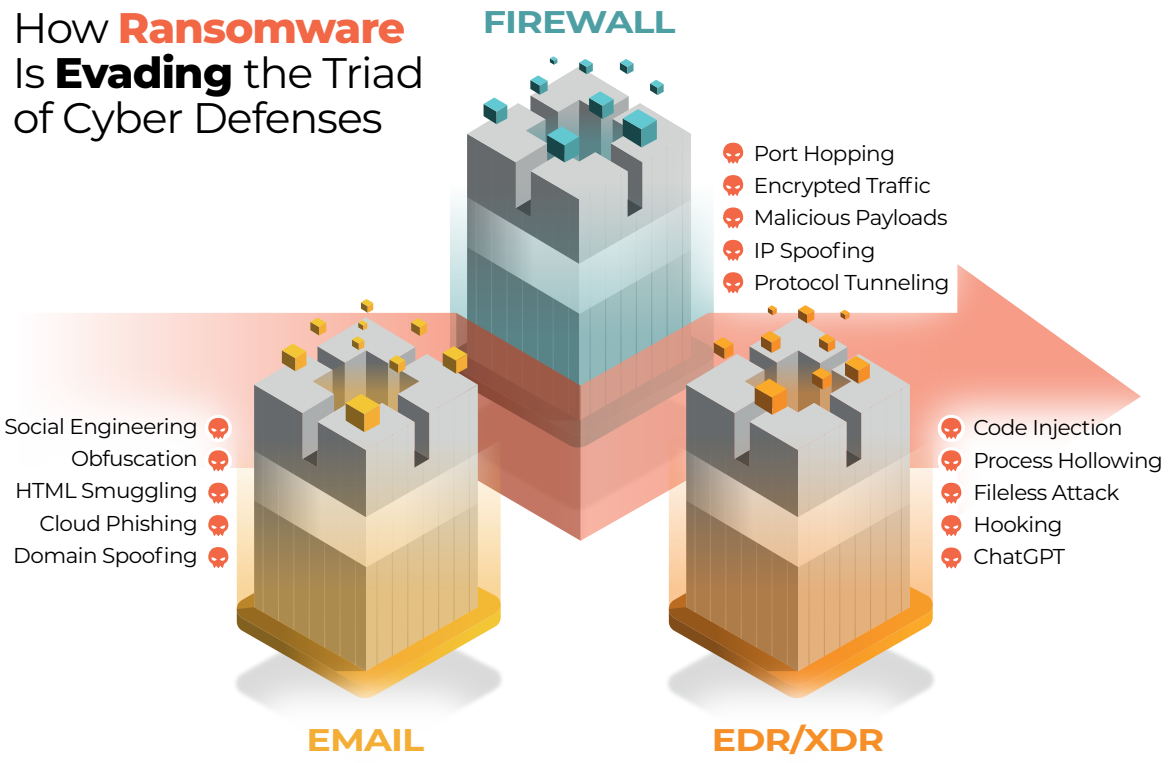
RANSOMWARE FLASHCARD ANALYSIS & OVERVIEW

What the Statistics Tell Us About the State of Ransomware

Index



How Ransomware is Evading Common Cybersecurity Defenses

Cybersecurity architectures are diverse and composed of a wide range of tools ranging from legacy to cutting-edge technologies. However, many organizations from small businesses to service providers and enterprises, rely on this 'triad' of security tools to defend their network infrastructure. Here is a limited list of some new and common ways in which ransomware groups evade these defenses.

- **Email Security**
  - **Social Engineering**

    Social engineering attacks rely on psychological manipulation to coerce or incite users into divulging sensitive information or performing a particular action. For example, a spearphishing attack (Mitre: T1192) impersonates a trusted contact like a manager and leverages the fears and insecurities of a targeted individual to make them grant access to a sensitive system or click on a malicious link.

  - **Obfuscation**

    Obfuscation (Mitre: T1027) is the practice of making malicious code or activities unclear, difficult to understand, and undetectable to email security. Attackers may obfuscate their phishing attempts by blending in with legitimate traffic or spoofing legitimate email addresses.

- **HTML Smuggling**

  HTML smuggling (Mitre: T1027.006) involves inserting a malicious HTML and javascript code in an email, permitting communications that would typically not be allowed by email security. While the practice is not new, and fairly simple to prevent, it is still a common practice that endusers fall victim to.

- **Cloud Phishing**

  Cloud phishing (Mitre T1586.003) involves taking over cloud-based services like cloud storage, file sharing or collaboration tools. The attackers can then use these formerly legitimate tools to host malicious files or data. Email security can then be tricked into thinking that a link is safe because it is linked to a reputable service.

- **Domain Spoofing**

  This practice (Mitre: T1105) involves setting up a website that impersonates a legitimate page. Often the attackers impersonate the login page of a trusted website, which is then used to capture passwords, personal information, or credit card detail.

• Firewalls

- **Malicious Payloads**

  Malicious payloads include viruses, Trojans, ransomware, and other types of malware. These payloads are typically part of a larger attack and are used to gain access to systems, escalate privileges, move laterally, and steal data. Malicious payloads are delivered mostly through email, but also malicious websites, malvertising, file sharing, and USB drives.

- **Port Hopping**

  Port hopping (Mitre: T1571) is a technique used to evade firewalls and security tools designed to detect and block port scanning activity. This technique involves scanning a range of ports on a target system, but instead of scanning all ports in sequence, the attacker skips around randomly to avoid detection. By hopping around between ports, the attacker can make it more difficult for security tools to detect their activity.

- **Encrypted Traffic**

  Encrypting traffic (Mitre: T1573) is an increasingly common technique used by attackers to bypass firewall defenses by hiding malicious traffic within encrypted packets. Attackers may use techniques such as SSL/TLS encryption to hide their activity and avoid detection by security tools.

- **IP Spoofing**

  In IP Spoofing, attackers modify the IP addresses in their network packages' address bars. In this way, firewalls that rely on knowledge of malicious IP addresses to block or identify malicious traffic are circumvented.

- **Protocol Tunneling**

  Protocol tunneling is used to disguise network traffic and bypass firewall defenses by encapsulating malicious traffic within HTTP, DNS (Mitre: T1071.001), or another legitimate network protocol. Often A VPN can be used to tunnel malicious traffic from an insecure location to the network.

- **EDR/XDR**
  - **Code Injection**

    Code injection allows attackers to insert malicious code through various techniques including process hollowing, creating a remote thread, the 'Early Bird' technique, or 'Atom bombing'. A recent study found 65% of EDRs and EPPs to be vulnerable to the Early Bird Technique, which uses QueueUserAPC() to queue a user mode APC to another threat for code injection.

  - **Control Panel Side-Loading**

    CPL files were created by Microsoft to provide quick access to various tools in the Windows Control Panel. CPL Side-Loading uses these files to hide malicious software. Since EDR solutions look for and block malicious executable files, this method is a reasonably easy way to avoid detection.

  - **DLL Side-Loading**

    DLL Side-Loading tricks an application into loading a malicious DLL (Dynamic Link Library) file instead of a genuine one. Attackers don't just wait until the application is run by a user, but instead use the trusted application to run their malicious DLL code.

  - **API Hooking**

    Windows allows systems like EDRs and EPPS to detect changes to other applications through API hooking, which involves intercepting events, messages, and calls between APIs in the OS. However, 'Userland API Hooking' is a technique where attackers intercept API calls using these permissions to modify applications for their malicious purposes.

  - **ChatGPT**

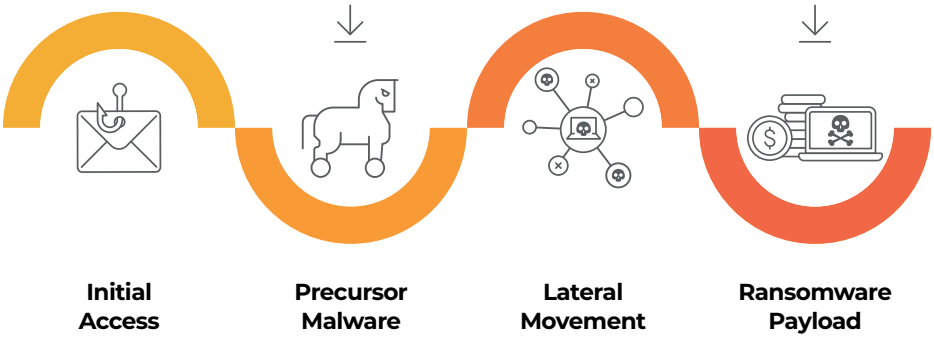
    Cybersecurity researchers recently used ChatGPT to create a proof-of-concept called Black Mamba, a polymorphic keylogger able to dynamically modify its code without command and control infrastructure.

    The PoC shows how language learning models are creating new challenges for EDRs to detect and block.

Ransomware groups can evade or bypass any one siloed cybersecurity solution in a myriad of different ways.

Whether an EDR, XDR, Firewall, email security, or some other solution in isolation, any single cybersecurity solution provides insufficient defense. This is why most cybersecurity experts will advise a defense-in-depth strategy composed of a stack of tools. More importantly, it shows how important it is that a cybersecurity stack should be integrated so that the tools in such a stack can 'speak' to one another and work together to illuminate blind spots.

Ransomware **Precursor Activity**



Precursor Malware

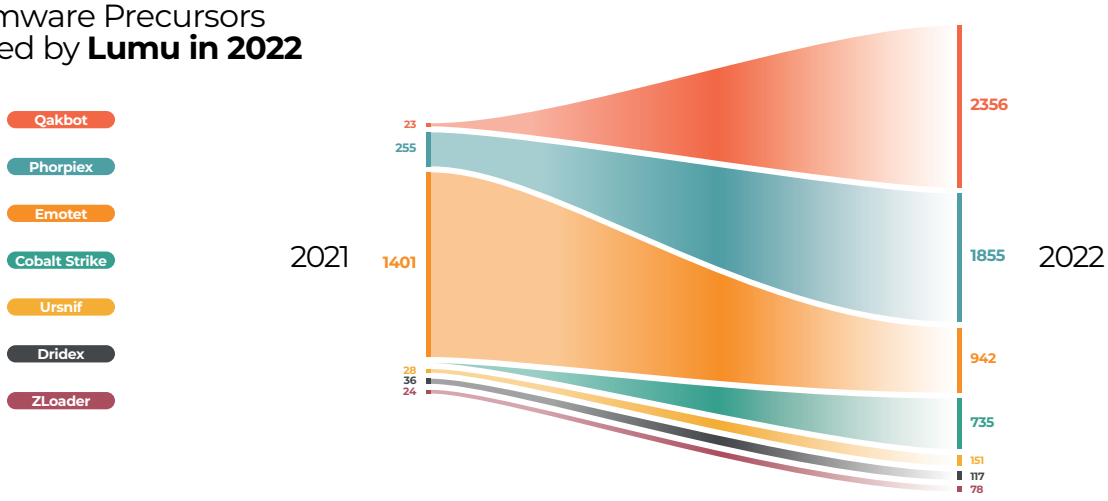
It's important to remember that ransomware doesn't appear out of thin air. Precursor malware is a good indication that ransomware is on the way. Precursor malware's evolution to ransomware involves a few stages.

The first stage in this process typically involves the distribution of an initial malware payload, such as a Trojan horse or a backdoor. This payload is often distributed through phishing emails, social engineering, or other types of malicious activity. Once the payload is installed on a victim's computer, it can begin to collect data and establish a connection with the attacker's command and control (C&C) server.

Next, the attacker can use data collected by the initial payload to customize the attack and select the most effective ransomware strain to use.

The final stage involves the deployment of the ransomware itself. This is typically achieved by using the initial payload to download and execute the ransomware on the victim's computer. Once the ransomware is installed, it quickly takes over.

Ransomware Precursors Detected by **Lumu in 2022**



Source: Precursor malware associated with Ransomware deployment detected by Lumu in 2022. In 2022 Lumu processed 1,307 billion records, up from 430.4 billion in 2021.

The Most Dangerous Precursor Malware Strains

Over the last year, we've noticed a major increase in precursor malware activity associated with Qakbot and Phorpiex. These two malware strains are well known for causing some of the most significant ransomware attacks.

Qbot, also known as Qakbot, is a type of banking trojan that has been active since 2008. In 2022, we detected 10 143% more contacts from this botnet. It was initially designed to steal sensitive information, such as login credentials and financial data, from infected systems. Qbot has undergone several updates and iterations over the years, making it one of the most persistent and dangerous banking trojans in circulation.

Qbot primarily spreads through phishing emails that contain malicious attachments or links. Once installed on a victim's computer, Qbot establishes persistence by modifying system files and registry keys. It then collects sensitive information by logging keystrokes, capturing screenshots, and monitoring network traffic.

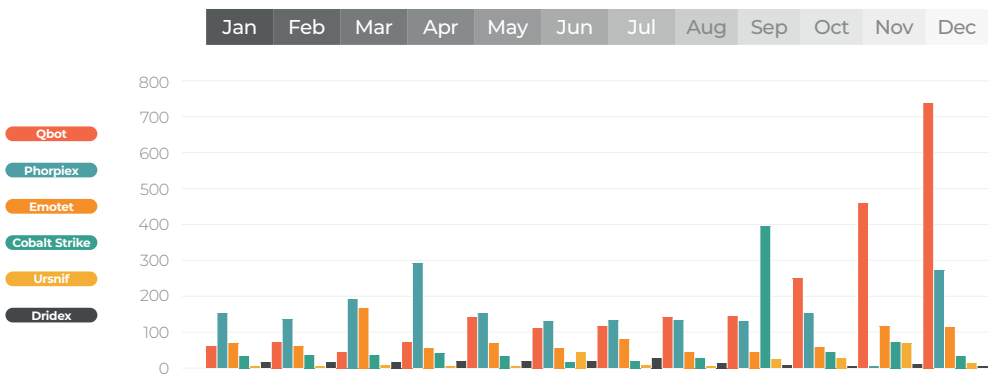
In addition to stealing banking credentials, Qbot can also be used to distribute other types of malware, such as ransomware or remote access Trojans (RATs), to other systems on a network. This allows attackers to use Qbot as a gateway to gain access to a larger number of systems and steal even more sensitive information.

Phorpiex, also known as Trik, also saw a major increase of 627% over the last year. This ransomware precursor typically spreads through spam emails that contain malicious attachments or links. Once installed on a victim's computer, it quickly modifies system files and registry keys. From there Phorpiex connects to a command and control (C&C) server to receive instructions and download additional malware payloads.

One of the distinctive features of Phorpiex is its use of a peer-to-peer (P2P) protocol to communicate with other infected systems. This makes it difficult to block or take down the C&C server as the malware can continue to operate even if the server is shut down.

Phorpiex is also known for its ability to self-propagate and infect other systems on a network. It can also perform various malicious activities, such as sending spam emails, stealing sensitive information, and launching DDoS attacks.

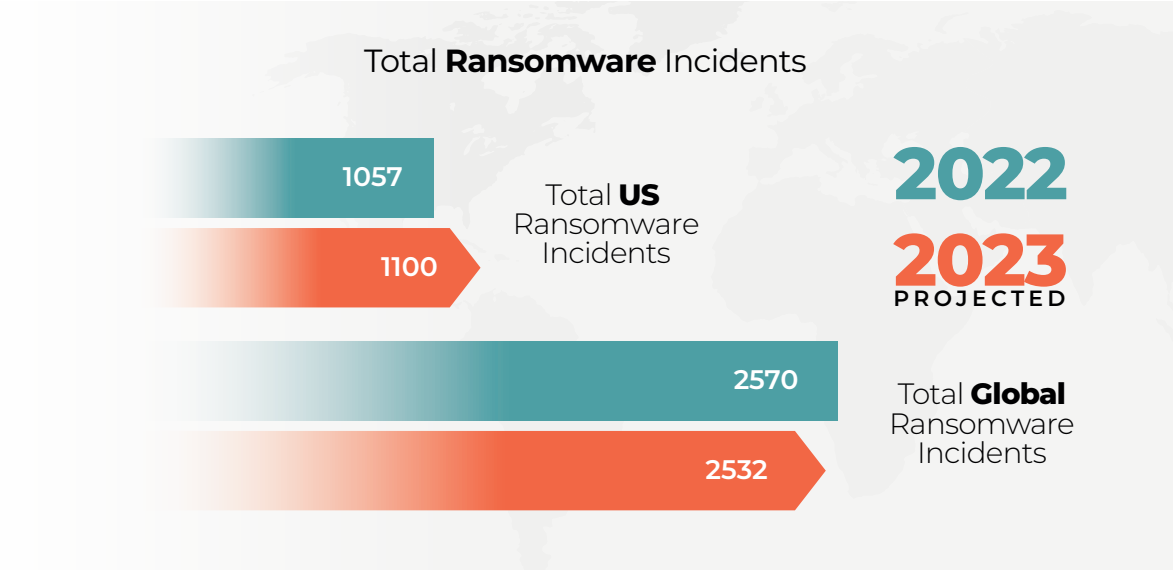
Ransomware attacks can happen at any time of the year, however, it is worth noting that cybercriminals increase their activities during specific periods or events that can provide them with an opportunity to launch successful attacks. Last year, there was a clear surge in ransomware precursor incidents immediately



preceding the holidays. In this way, the ground is prepared for launching ransomware attacks at the most opportune moment. Malicious actors are strategizing, and launching attacks when IT staff may be less available to respond to attacks.

The Impact of Ransomware

The impact of ransomware on organizations and the people that operate cybersecurity is growing in scope and scale. Over the last few years, the world has attempted to quantify the damage of ransomware incidents including its short- and long-term consequences. It is still very hard to quantify the true cost of ransomware but one thing is certain, it is far too great to accept.



Source Darktracer Ransomware Database: https://darktracer.com/ 2023

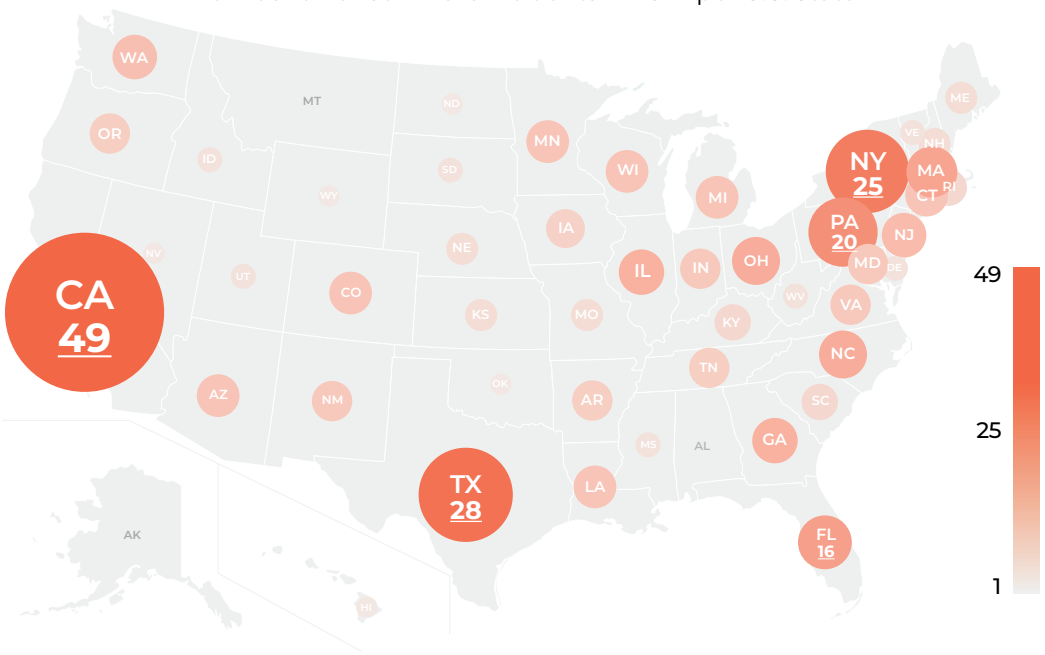
Though not surprising, the projected number of ransomware attacks for 2023 shows yet another increase in the US, while a minor decrease is predicted for 2023 globally. The projected figures are based on ransomware attacks that occurred in Q1 of 2023, so it is likely that the true figure will exceed this one, due to the spike in ransomware attacks we tend to see around the holidays.

The reasons for the overall increase are a combination of the following:

- Increased ability to evade protection mechanisms, as described above.
- The rise of stealth attacks, where ransomware organizations use zero days and seek to covertly infiltrate and silently obtain payment.
- More people online represents countless avenues for cybercriminals to enter the network of an organization.
- Ransomware ecosystems became more diverse after the decline of large ransomware groups like Conti and REvil, allowing smaller groups to operate in stealth by focusing on volume rather than size.

The Impact

Number of ransomware incidents in 2022 per U.S. State



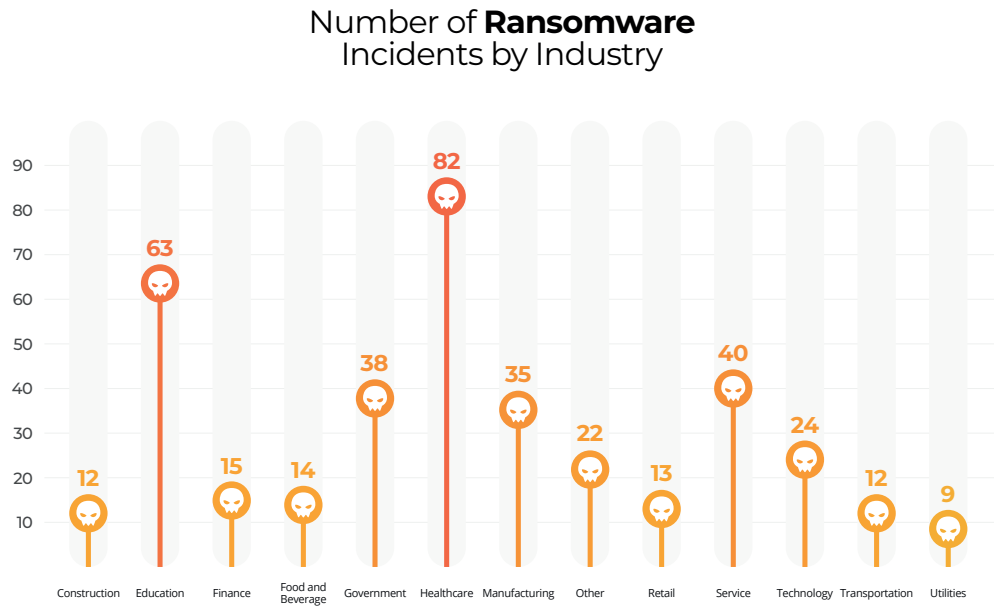
Source: Comparitech Ransomware Database: https://www.comparitech.com/ransomware-attack-map/

	2021	2022
ALABAMA	8	0
ARIZONA	11	8
ARKANSAS	5	6
CALIFORNIA	69	49
COLORADO	6	8
CONNECTICUT	7	8
DELAWARE	1	2
DISTRICT OF COLUMBIA	7	2
FLORIDA	35	16
GEORGIA	24	12
HAWAII	3	1
IDAHO	6	2
ILLINOIS	36	12
INDIANA	14	7
IOWA	8	5
KANSAS	5	3
KENTUCKY	4	4
LOUISIANA	3	8
MAINE	9	3
MARYLAND	15	7
MASSACHUSETTS	46	15
MICHIGAN	13	8
MINNESOTA	8	8
MISSISSIPPI	5	2
MISSOURI	18	3

	2021	2022
MONTANA	3	0
NEBRASKA	6	3
NEVADA	5	1
NEW HAMPSHIRE	5	3
NEW JERSEY	26	10
NEW MEXICO	3	7
NEW YORK	50	25
NORTH CAROLINA	15	13
NORTH DAKOTA	2	1
OHIO	17	13
OKLAHOMA	13	1
OREGON	6	6
PENNSYLVANIA	30	20
RHODE ISLAND	2	4
SOUTH CAROLINA	9	4
TENNESSEE	14	6
TEXAS	43	28
UTAH	8	2
VERMONT	2	2
VIRGINIA	19	7
WASHINGTON	21	9
WEST VIRGINIA	2	2
WISCONSIN	12	8
SOUTH DAKOTA	12	2
WYOMING	0	1

Source: Comparitech Ransomware Database: https://www.comparitech.com/ransomware-attack-map/

The distribution of reported incidents across the United States aligns with the population density of each state. The most populous states have the largest "business" opportunities for cybercriminals. It's worth noting that according to Comparitech, there was a decline in the overall number of ransomware attacks in the United States. Other sources, such as Darktracer, showed a marginal increase.



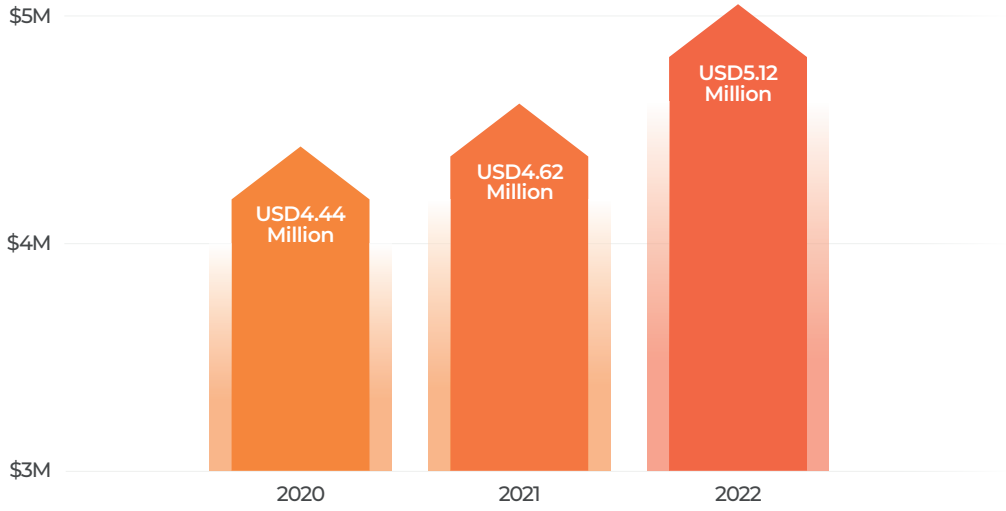
Source: Comparitech Ransomware Database: https://www.comparitech.com/ransomware-attack-map/

A trend that has been observed over the last few years is ransomware's diversification across different sectors. Whereas before, the financial sector took the reign as the most targeted industry, that is no longer the case. The financial sector has been investing in protection which is efficiently deterring cybercriminals. However, this over-emphasis on defense is resulting in their cybersecurity operations maturity and response capabilities becoming outdated.

The healthcare sector has undergone a digital transformation that makes it easier to share data between different healthcare systems and deliver better care for patients. However, this benefit comes at a cost: cyber attacks exploit patient privacy, and vulnerabilities in legacy healthcare systems to profit through ransomware schemes.

Education is the second most victimized industry. The education sector has long underinvested in cybersecurity—including protection and defense mechanisms—which puts them in a particularly vulnerable position. Low cybersecurity operation maturity makes them an easy target while they also have to deal with a large attack surface. An average school has as many devices connected to the network as a large corporation, with the budget of a small enterprise. The combination of low maturity, large attack surface, and lower budgets make the education sector a true paradise for a cybercriminal organization.

Cost of a **Ransomware Attack**



Source: IBM Cost of a Data Breach Report: https://www.ibm.com/reports/data-breach

The cost of a ransomware attack does not only include the amount of the ransomware payment but also the loss of critical data, system downtime, and reputational damage. We've seen that ransomware attacks have become more complex, difficult to remediate, and expensive to respond to. Alongside the increased use of cryptocurrencies to extract payment, all this has caused a gradual increase in the cost of a ransomware incident. In short, ransomware actors have been able to maximize the monetization of network access as well as the damage they inflict.

The Future of Ransomware

A ransomware incident is never one attack. It is a combination of targeted threats that successfully bypass protection giving the cybercriminal freedom to move unsupervised within the network until reaching valuable data that will cause operational disruption for the victimized business. It is undeniable that ransomware attacks cannot be ignored by any organization or any sector of the economy. Those verticals that used to be ignored are now relevant and attractive targets.

www.lumu.io

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