

vCISO Threat Intelligence Report

State of Ransomware – November 6, 2023

Contents

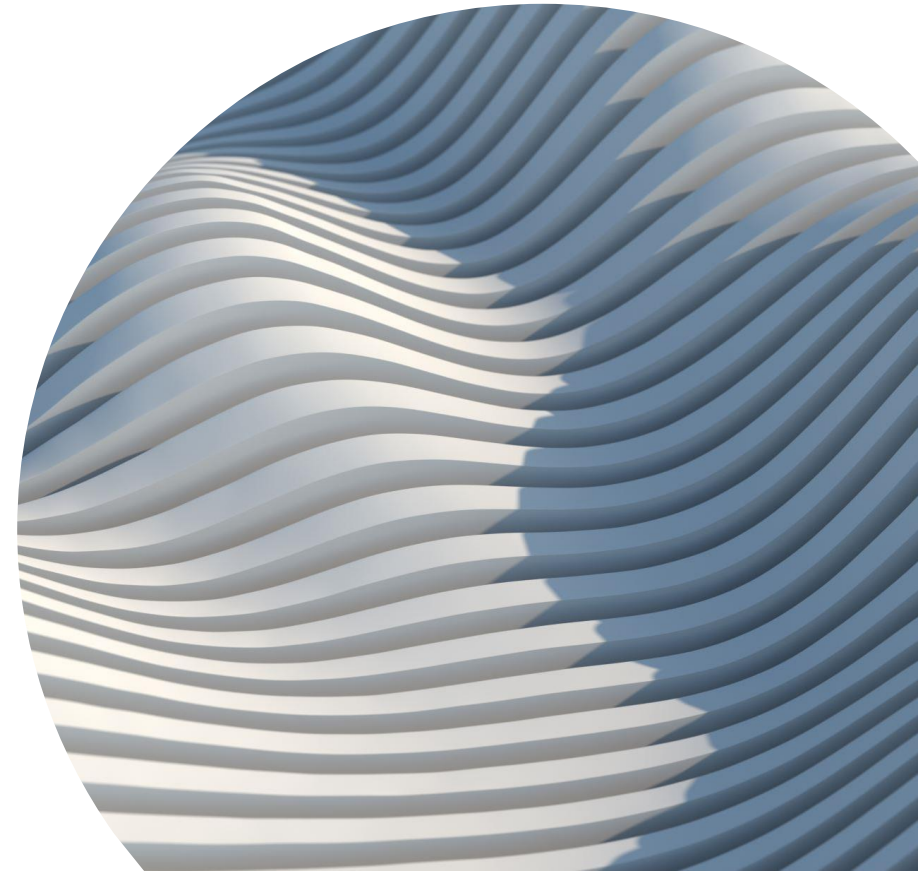
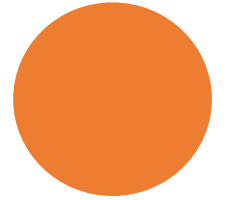
Introduction

Ransomware Threat Intelligence

Ransomware Defense Resources

Knowledge Sharing

 **Riskigy**



Introduction

Riskigy's vCISO threat intelligence reports cover the latest cybersecurity threats, attacks and need-to-know information.

- ✓ **We ingest the latest alerts, reports, articles and podcasts to bring our network the important facts in an actionable easy to consume format.**
- ✓ **Our Threat intelligence reports include information about the tactics, techniques, and procedures (TTPs) used by threat actors, the types of systems and information being targeted, and other threat-related information.**
- ✓ **These reports are designed to provide actionable and contextualized intelligence to increase cyber resilience and help organizations adopt preventive measures before incidents happen.**

It is important to note that our threat intelligence reports are not exhaustive and may not cover all possible threats and vulnerabilities. It is recommended to use multiple sources of threat intelligence and to consult with cybersecurity experts to develop a comprehensive cybersecurity strategy.

Ransomware Threat Intelligence



Second highest ransomware profits expected this year – DHS 2024 Homeland Threat Assessment report

Ransomware operations are poised to achieve the second highest profits by year-end, with at least \$449.1 million already extorted from attacks around the world during the first six months of 2023

The return of ‘big game hunting’ – the targeting of large organizations – as well as cyber criminals’ continued attacks against smaller organizations,” DHS said.

Elevated ransomware profits have been driven by:

- Reemergence of attacks against large organizations
- Persistent intrusions against smaller entities
- AI use in malware and software development is also being explored by nation-states
- New tactics “intermittent encryption” which allows gangs to encrypt systems faster and harder to detect

Takeaway: The DHS found that the average business needs at least 22 days to recover and resume operations after a ransomware attack. Startlingly, ransomware recovery “frequently costs 50 times more than the ransom demand.”

Ransomware boom hits all-time high in September

The uptick represents a year-over-year 153% increase in ransomware attacks.

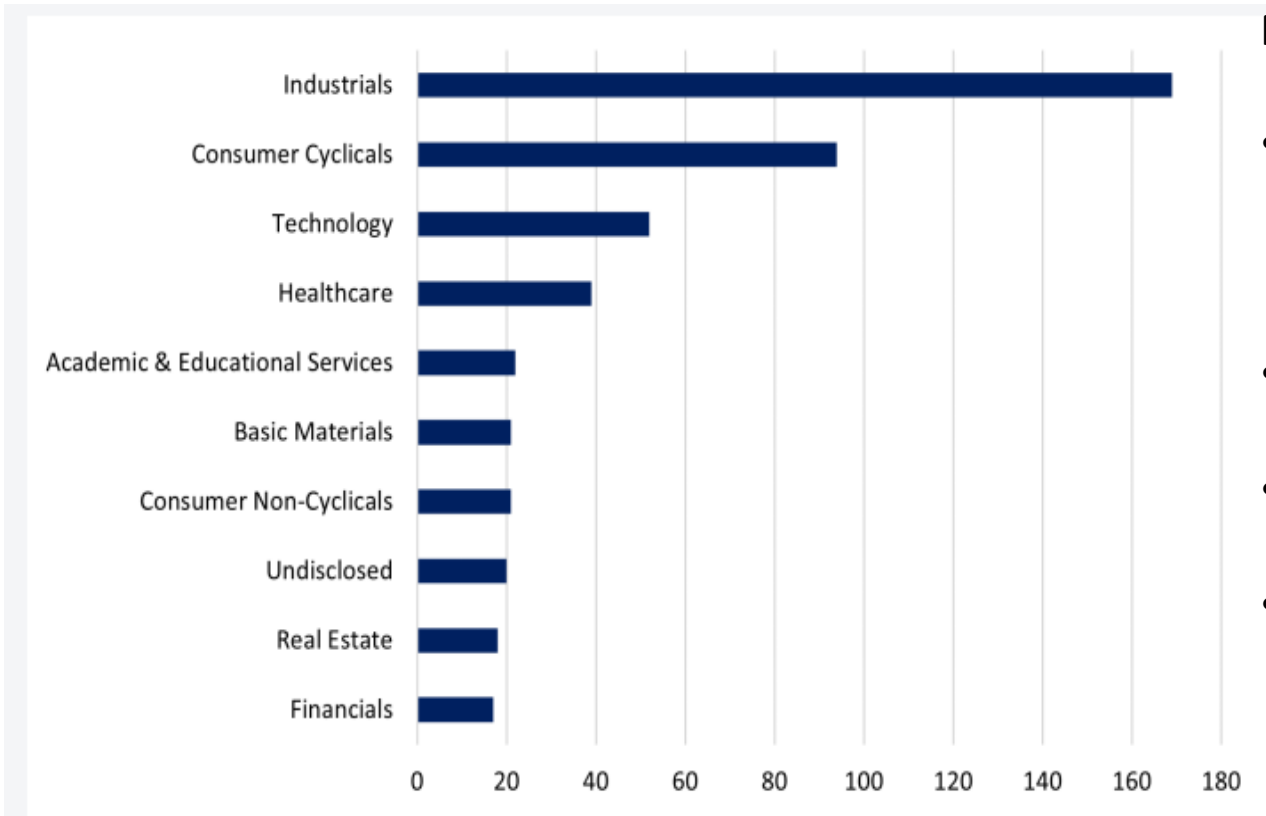


Figure 2: Top 10 Sectors Targeted September 2023

Noted Ransomware Attack Techniques:

- Outsourcing initial access to target IT environments to **Access Brokers** to gain access to target networks through phishing, exploit kits or stolen credentials so they can deploy their ransomware.
- Exploiting **zero-day vulnerabilities** in target security controls and applications to gain access.
- Using **legitimate penetration testing tools**, such as Cobalt Strike, to deliver the payloads.
- **Compromising websites** and using them to distribute exploit kits to site visitors. Which allows attackers to exploit vulnerabilities in visitors' web browsers and operating system.

Why Ransomware victims can't stop paying off Hackers!

Paying is often the easiest option, but don't expect to get let off the hook so easily!



According to a survey of hundreds of security leaders published by Splunk, some **83% of organizations admitted to paying hackers following a ransomware attack**, and more than half paid at least \$100,000, either through cyber insurance or a third-party.

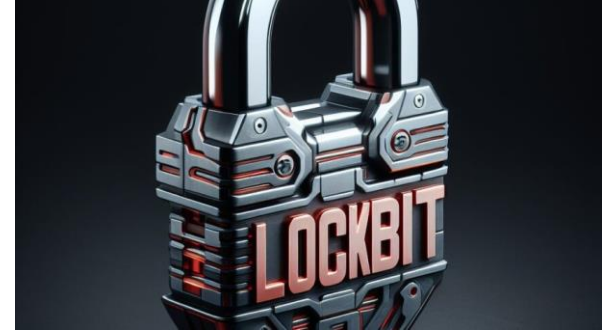


No guarantee that paying up will ensure the safe return of stolen data — or that all copies have been erased. After all, any data stolen by cybercriminals is compromised whether a ransom is paid or not, and you can't trust a criminal's word that they actually deleted your data.



According to a study by Cybereason, **80% of ransomware victims who paid the ransom were hit by a subsequent ransomware attack**, with 68% of compromised organizations saying that the second attack came less than a month later and that the hackers demanded a higher ransom.

Lockbit Ransomware Group

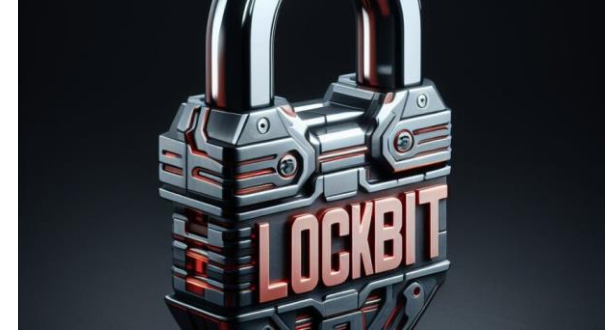


The ransomware group is known for its ransomware-as-a-service.

- Boeing is the latest victim of LockBit ransomware.
- LockBit was the most deployed ransomware in 2022 in the UK.
- UK targeted, Scottish law firm Raeburn, Christie, Clark and Wallace.
- The Royal Mail rejected the US\$80 million ransom demand from the hackers.
- UK's Ministry of Defense. Information stolen included British military intelligence sites as well as high-security prisons.
- The FBI has recorded around **1,700 LockBit incidents in the US**. Victims in the US have paid approximately **US\$91 million** since LockBit activity was first observed on January 5, 2020.

What you need to know about Lockbit Ransomware cont.

Here's a look at the different variants of the LockBit Ransomware



- ❑ **LockBit** – The first variant that succeeded the original .abcd extension used by the ransomware group gained notoriety for its ability to deploy its encryption process in under five minutes.
- ❑ **LockBit 2.0** – LockBit 2.0 evolved from the original LockBit variant by improving its ability to decode strings and codes faster to avoid detection. Once the variant has established administrative privileges, the encryption process begins.
- ❑ **LockBit 3.0** – Launched in late June 2022, LockBit 3.0 continues the trend of increasing encryption speed to avoid security detection. The malware uses anti-analysis techniques, password-only execution, and command line augmentation. LockBit 3.0 also introduces the first recorded ransomware bug bounty program, calling for users and security researchers to report any bugs to the ransomware group in exchange for financial reward.
- ❑ **LockBit Green** – The latest variant was revealed by VX-underground and appears to be a standard ransomware variant targeting Windows environments.
- ❑ **Lockbit for Mac** – In May 2023, Flashpoint discovered that LockBit had begun developing a macOS version of LockBit ransomware.

Limited Resources to Battle Ransomware

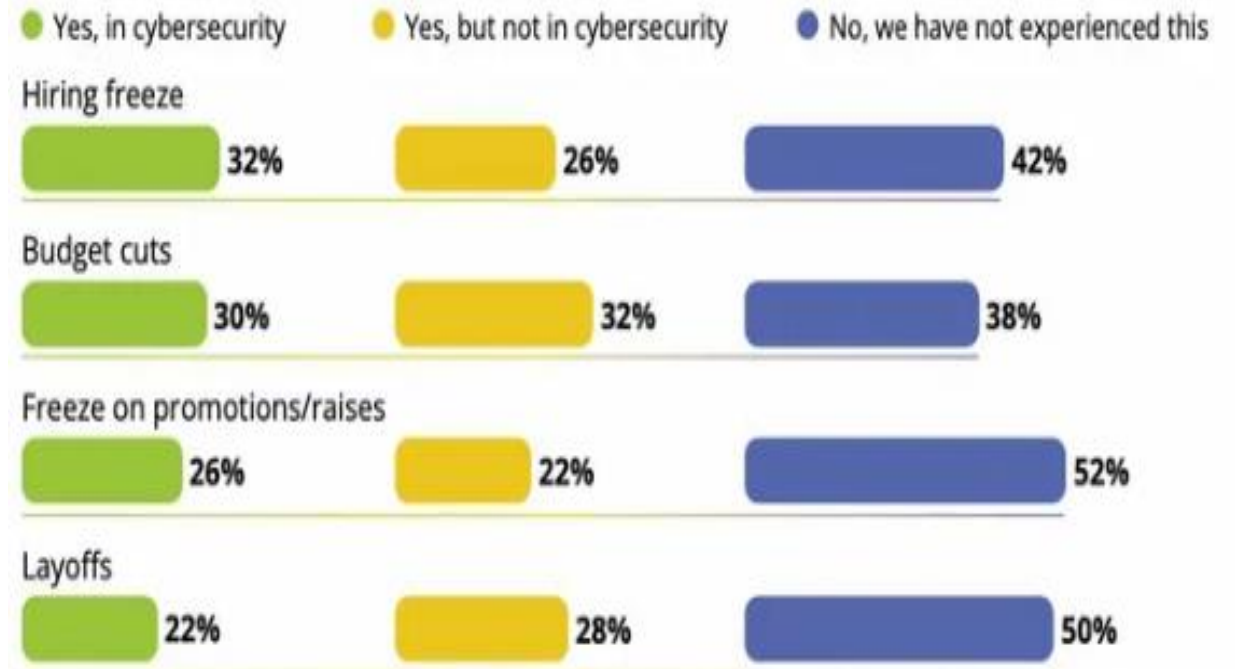
ISC2 Reports: Nearly 1.5 million people work in cybersecurity in North America, but even with a growing gap in skilled specialists, they bear a higher chance of hiring freezes and layoffs.

"You can't hire your way out of the skills shortage, which impacts both staff size and advanced skills".

Actions to take include more:

- Process automation
- Buying more intelligent solutions
- Use AI and advanced analytics
- Offloading some tasks or processes to managed services providers
- All of these should be part of an enterprise security strategy

Has your organization experienced the following cutbacks in the past 12 months?



Base: 11,656-12,200 global cybersecurity professionals

Note: "Don't know/does not apply" responses were removed from the sample base.

More than a fifth of cybersecurity workers have experienced layoffs in their group. (Source: ISC2)

Ransomware Defense Resources



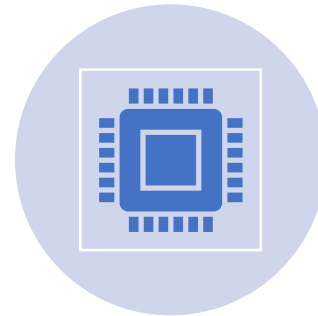
International Counter Ransomware Initiative 2023 Joint Statement

White House seeks more international cooperation to combat ransomware

Developing Capabilities | Sharing Information | Fighting Back



Ransomware attacks are expected to grow from \$20 billion globally in 2021 to \$71.5 billion in 2026



The United States is the target of 46% of ransomware attacks, according to the National Security Council



48 countries that are part of the Counter Ransomware Initiative will meet to collaborate on ways to combat the growth of ransomware




The Biden Administration established the CRI in 2021 to disrupt and defend against malicious cyber attacks


Bad Practices that are exceptionally Risky according to CISA and #StopRansomware


CISA Bad Practices Github discussion page to engage with administrators and IT professionals.

- Use of unsupported (or end-of-life) software is dangerous.
- Use of known/fixed/default passwords and credentials is dangerous.
- The use of single-factor authentication for remote or administrative access to systems is dangerous.

These practices significantly elevate risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.

 High Severity (8-10) Vulnerabilities being unpatched for longer than X # of Days.
[MattInfoSec21](#) started on Jan 5, 2022 in [Ideas for new Bad Practices](#)

 Prohibiting password pasting / password managers
[richlv](#) started on Jun 28 in [Ideas for new Bad Practices](#)

 Providing too much AD access to a Tier 1 support
[mchahusgithub](#) started on Jul 7 in [Ideas for new Bad Practices](#)

 Allowing Critical Servers Unfiltered Internet Access
[ErsatzLogic](#) started on Sep 1, 2021 in [Ideas for new Bad Practices](#)

And many more!

DHS #StopRansomware Guide 3.0 Released in October

In the new version of the guide, the agencies added a bullet list to initial access vectors for Internet-facing vulnerabilities and misconfigurations.

The best practices for these flaws include avoiding exposure of services, such as

- Remote desktop protocol (RDP) on the web; limiting the use of RDP and other remote desktop services
- Disabling Server Message Block (SMB) protocol version 1, upgrading to version 3 (SMBv3)
- Hardening SMBv3 after mitigating existing dependencies.
- Ransomware operators impersonating IT staff in phone calls or SMS messages to steal credentials from employees and access the organization's network.
- Common advanced forms of social engineering, like search engine optimization, drive-by-downloads, and malvertising.
- Abnormal amounts of data outgoing over any ports in the ransomware and data extortion response.
- Initiating threat-hunting activities, organizations should check for potential signs of data being exfiltrated from the network.
- Data outgoing over any ports and the presence of common tools for data exfiltration like Rclone, Rsync, various web-based file storage services, and FTP/SFTP.

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

The NSA and CISA strongly encourage network defenders to implement their recommendations and software manufacturers to incorporate secure-by-design and -default principles and tactics.

Top Ten Misconfigurations:

1. Default configurations of software and application
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or configured MFA methods
8. Insufficient ACLs on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

CISA's Ransomware Readiness Assessment (RRA)

Schedule a Walkthrough “Assessment” of the RRA:

- ❑ Helps organizations evaluate their cybersecurity posture, with respect to ransomware, against recognized standards and best practice recommendations in a systematic, disciplined, and repeatable manner.
- ❑ Guides asset owners and operators through a systematic process to evaluate their operational technology (OT) and information technology (IT) network security practices against the ransomware threat.
- ❑ Provides an analysis dashboard with graphs and tables that present the assessment results in both summary and detailed form.

Connect with Us and Get Social with the Riskigy Team

Teamwork makes the dream work! There is strength in numbers! Together we stand and the countless other reasons to connect with us!



Information & Intelligence Sharing – e: soc@riskigy.team

Mike Marrano - e: mike@riskigy.team

LinkedIn: <https://www.linkedin.com/company/riskigy>

Twitter: twitter.com/riskigy

Newsletter & Alerts: <https://riskigy.com/blog>

