Alert (AA22-040A)

More Alerts

2021 Trends Show Increased Globalized Threat of Ransomware

Original release date: February 09, 2022

Summary

Immediate Actions You Can Take Now to Protect Against Ransomware: • Update your operating system and software.
• Implement user training and phishing exercises to raise awareness about the risk of suspicious links and attachments.
• If you use Remote Desktop Protocol (RDP), secure and monitor it.
• Make an offline backup of your data.
• Use multifactor authentication (MFA).

In 2021, cybersecurity authorities in the United States,[1][2][3] Australia,[4] and the United Kingdom[5] observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Centre (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities, including in the Healthcare and Medical, Financial Services and Markets, Higher Education and Research, and Energy Sectors. The United Kingdom’s National Cyber Security Centre (NCSC-UK) recognizes ransomware as the biggest cyber threat facing the United Kingdom. Education is one of the top UK sectors targeted by ransomware actors, but the NCSC-UK has also seen attacks targeting businesses, charities, the legal profession, and public services in the Local Government and Health Sectors.

Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors’ growing technological sophistication and an increased ransomware threat to organizations globally.

This joint Cybersecurity Advisory—authored by cybersecurity authorities in the United States, Australia, and the United Kingdom—provides observed behaviors and trends as well as mitigation recommendations to help network defenders reduce their risk of compromise by ransomware.

Click here for a PDF version of this report.

Technical Details

Cybersecurity authorities in the United States, Australia, and the United Kingdom observed the following behaviors and trends among cyber criminals in 2021:

- **Gaining access to networks via phishing, stolen Remote Desktop Protocols (RDP) credentials or brute force, and exploiting vulnerabilities.** Phishing emails, RDP exploitation, and exploitation of software vulnerabilities remained the top three initial infection vectors for ransomware incidents in 2021. Once a ransomware threat actor has gained code execution on a device or network access, they can deploy ransomware. Note: these infection vectors likely remain popular because of the increased use of remote work and schooling starting in 2020 and continuing through 2021. This increase expanded the remote attack surface and left network defenders struggling to keep pace with routine software patching.
- **Using cybercriminal services-for-hire.** The market for ransomware became increasingly "professional" in 2021, and the criminal business model of ransomware is now well established. In addition to their increased use of ransomware-as-a-service (RaaS), ransomware threat actors employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between themselves and other cyber criminals. NCSC-UK observed that some ransomware threat actors offered their victims the services of a 24/7 help center to expedite ransom payment and restoration of encrypted systems or data.

Note: cybersecurity authorities in the United States, Australia, and the United Kingdom assess that if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent. Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model. Additionally, cybersecurity authorities in the United States, Australia, and the United Kingdom note that the criminal business model often complicates attribution because there are complex networks of developers, affiliates, and freelancers; it is often difficult to identify conclusively the actors behind a ransomware incident.

- **Sharing victim information.** Eurasian ransomware groups have shared victim information with each other, diversifying the threat to targeted organizations. For example, after announcing its shutdown, the BlackMatter ransomware group transferred its existing victims to infrastructure owned by another group, known as Lockbit 2.0. In October 2021, Conti ransomware actors began selling access to victims' networks, enabling follow-on attacks by other cyber threat actors.
- **Shifting away from "big-game" hunting in the United States.**
    - In the first half of 2021, cybersecurity authorities in the United States and Australia observed ransomware threat actors targeting "big game" organizations —i.e., perceived high-value organizations and/or those that provide critical services—in several high-profile incidents. These victims included Colonial Pipeline Company, JBS Foods, and Kaseya Limited. However, ransomware groups suffered disruptions from U.S. authorities in mid-2021. Subsequently, the

FBI observed some ransomware threat actors redirecting ransomware efforts away from "big-game" and toward mid-sized victims to reduce scrutiny.
  - The ACSC observed ransomware continuing to target Australian organizations of all sizes, including critical services and "big game," throughout 2021.
  - NCSC-UK observed targeting of UK organizations of all sizes throughout the year, with some "big game" victims. Overall victims included businesses, charities, the legal profession, and public services in the Education, Local Government, and Health Sectors.
- **Diversifying approaches to extorting money.** After encrypting victim networks, ransomware threat actors increasingly used "triple extortion" by threatening to (1) publicly release stolen sensitive information, (2) disrupt the victim's internet access, and/or (3) inform the victim's partners, shareholders, or suppliers about the incident. The ACSC continued to observe "double extortion" incidents in which a threat actor uses a combination of encryption and data theft to pressure victims to pay ransom demands.

Ransomware groups have increased their impact by:

- **Targeting the cloud.** Ransomware developers targeted cloud infrastructures to exploit known vulnerabilities in cloud applications, virtual machine software, and virtual machine orchestration software. Ransomware threat actors also targeted cloud accounts, cloud application programming interfaces (APIs), and data backup and storage systems to deny access to cloud resources and encrypt data. In addition to exploiting weaknesses to gain direct access, threat actors sometimes reach cloud storage systems by compromising local (on-premises) devices and moving laterally to the cloud systems. Ransomware threat actors have also targeted cloud service providers to encrypt large amounts of customer data.
- **Targeting managed service providers.** Ransomware threat actors have targeted managed service providers (MSPs). MSPs have widespread and trusted accesses into client organizations. By compromising an MSP, a ransomware threat actor could access multiple victims through one initial compromise. Cybersecurity authorities in the United States, Australia, and the United Kingdom assess there will be an increase in ransomware incidents where threat actors target MSPs to reach their clients.
- **Attacking industrial processes.** Although most ransomware incidents against critical infrastructure affect business information and technology systems, the FBI observed that several ransomware groups have developed code designed to stop critical infrastructure or industrial processes.
- **Attacking the software supply chain.** Globally, in 2021, ransomware threat actors targeted software supply chain entities to subsequently compromise and extort their customers. Targeting software supply chains allows ransomware threat actors to increase the scale of their attacks by accessing multiple victims through a single initial compromise.
- **Targeting organizations on holidays and weekends.** The FBI and CISA observed cybercriminals conducting increasingly impactful attacks against U.S. entities on holidays and weekends throughout 2021. Ransomware threat actors may view

holidays and weekends—when offices are normally closed—as attractive timeframes, as there are fewer network defenders and IT support personnel at victim organizations. For more information, see joint FBI-CISA Cybersecurity Advisory, Ransomware Awareness for Holidays and Weekends.

Mitigations

Cybersecurity authorities in the United States, Australia, and the United Kingdom recommend network defenders apply the following mitigations to reduce the likelihood and impact of ransomware incidents:

- **Keep all operating systems and software up to date.** Timely patching is one of the most efficient and cost-effective steps an organization can take to minimize its exposure to cybersecurity threats. Regularly check for software updates and end of life (EOL) notifications, and prioritize patching known exploited vulnerabilities. In cloud environments, ensure that virtual machines, serverless applications, and third-party libraries are also patched regularly, as doing so is usually the customer's responsibility. Automate software security scanning and testing when possible. Consider upgrading hardware and software, as necessary, to take advantage of vendor-provided virtualization and security capabilities.
- **If you use RDP or other potentially risky services, secure and monitor them closely.**
  - Limit access to resources over internal networks, especially by restricting RDP and using virtual desktop infrastructure. After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require MFA to mitigate credential theft and reuse. If RDP must be available externally, use a virtual private network (VPN), virtual desktop infrastructure, or other means to authenticate and secure the connection before allowing RDP to connect to internal devices. Monitor remote access/RDP logs, enforce account lockouts after a specified number of attempts to block brute force campaigns, log RDP login attempts, and disable unused remote access/RDP ports.
  - Ensure devices are properly configured and that security features are enabled. Disable ports and protocols that are not being used for a business purpose (e.g., RDP Transmission Control Protocol Port 3389).
  - Restrict Server Message Block (SMB) Protocol within the network to only access servers that are necessary, and remove or disable outdated versions of SMB (i.e., SMB version 1). Threat actors use SMB to propagate malware across organizations.
  - Review the security posture of third-party vendors and those interconnected with your organization. Ensure all connections between third-party vendors and outside software or hardware are monitored and reviewed for suspicious activity.
  - Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established.
  - Open document readers in protected viewing modes to help prevent active content from running.

- **Implement a user training program and phishing exercises** to raise awareness among users about the risks of visiting suspicious websites, clicking on suspicious links, and opening suspicious attachments. Reinforce the appropriate user response to phishing and spearphishing emails.
- **Require MFA** for as many services as possible—particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- **Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords**. Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access. **Note**: devices with local admin accounts should implement a password policy, possibly using a password management solution (e.g., Local Administrator Password Solution [LAPS]), that requires strong, unique passwords for each admin account.
- **If using Linux, use a Linux security module (such as SELinux, AppArmor, or SecComp) for defense in depth.** The security modules may prevent the operating system from making arbitrary connections, which is an effective mitigation strategy against ransomware, as well as against remote code execution (RCE).
- **Protect cloud storage by backing up to multiple locations, requiring MFA for access, and encrypting data in the cloud.** If using cloud-based key management for encryption, ensure that storage and key administration roles are separated.

Malicious cyber actors use system and network discovery techniques for network and system visibility and mapping. To limit an adversary's ability to learn an organization's enterprise environment and to move laterally, take the following actions:

- **Segment networks.** Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement. Organizations with an international footprint should be aware that connectivity between their overseas arms can expand their threat surface; these organizations should implement network segmentation between international divisions where appropriate. For example, the ACSC has observed ransomware and data theft incidents in which Australian divisions of multinational companies were impacted by ransomware incidents affecting assets maintained and hosted by offshore divisions (outside their control).
- **Implement end-to-end encryption.** Deploying mutual Transport Layer Security (mTLS) can prevent eavesdropping on communications, which, in turn, can prevent cyber threat actors from gaining insights needed to advance a ransomware attack.
- **Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a network-monitoring tool.** To aid in detecting the ransomware, leverage a tool that logs and reports all network traffic, including lateral movement on a network. Endpoint detection and response tools are particularly useful for detecting lateral connections as they have insight into unusual network connections for each host. Artificial intelligence (AI)-enabled

network intrusion detection systems (NIDS) are also able to detect and block many anomalous behaviors associated with early stages of ransomware deployment.

- **Document external remote connections.** Organizations should document approved solutions for remote management and maintenance. If an unapproved solution is installed on a workstation, the organization should investigate it immediately. These solutions have legitimate purposes, so they will not be flagged by antivirus vendors.
- **Implement time-based access for privileged accounts.** For example, the just-in-time access method provisions privileged access when needed and can support enforcement of the principle of least privilege (as well as the zero trust model) by setting network-wide policy to automatically disable admin accounts at the Active Directory level. As needed, individual users can submit requests through an automated process that enables access to a system for a set timeframe. In cloud environments, just-in-time elevation is also appropriate and may be implemented using per-session federated claims or privileged access management tools.
- **Enforce principle of least privilege through authorization policies.** Minimize unnecessary privileges for identities. Consider privileges assigned to human identities as well as non-person (e.g., software) identities. In cloud environments, non-person identities (service accounts or roles) with excessive privileges are a key vector for lateral movement and data access. Account privileges should be clearly defined, narrowly scoped, and regularly audited against usage patterns.
- **Reduce credential exposure.** Accounts and their credentials present on hosts can enable further compromise of a network. Enforcing credential protection—by restricting where accounts and credentials can be used and by using local device credential protection features—reduces opportunities for threat actors to collect credentials for lateral movement and privilege escalation.
- **Disable unneeded command-line utilities; constrain scripting activities and permissions, and monitor their usage.** Privilege escalation and lateral movement often depend on software utilities that run from the command line. If threat actors are not able to run these tools, they will have difficulty escalating privileges and/or moving laterally. Organizations should also disable macros sent from external sources via Group Policy.
- **Maintain offline (i.e., physically disconnected) backups of data, and regularly test backup and restoration.** These practices safeguard an organization's continuity of operations or at least minimize potential downtime from an attack as well as protect against data losses. In cloud environments, consider leveraging native cloud service provider backup and restoration capabilities. To further secure cloud backups, consider separation of account roles to prevent an account that manages the backups from being used to deny or degrade the backups should the account become compromised.
- **Ensure all backup data is encrypted,** immutable (i.e., cannot be altered or deleted), and covers the entire organization's data infrastructure. Consider storing encryption keys outside the cloud. Cloud backups that are encrypted using a cloud key management service (KMS) could be affected should the cloud environment become compromised.

- **Collect telemetry from cloud environments.** Ensure that telemetry from cloud environments—including network telemetry (e.g., virtual private cloud [VPC] flow logs), identity telemetry (e.g., account sign-on, token usage, federation configuration changes), and application telemetry (e.g., file downloads, cross-organization sharing)—is retained and visible to the security team.

Note: critical infrastructure organizations with industrial control systems/operational technology networks should review joint CISA-FBI Cybersecurity Advisory DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks for more recommendations, including mitigations to reduce the risk of severe business or functional degradation should their entity fall victim to ransomware.

Responding to Ransomware Attacks

If a ransomware incident occurs at your organization, cybersecurity authorities in the United States, Australia, and the United Kingdom recommend organizations:

- **Follow the Ransomware Response Checklist** on p. 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- **Scan backups.** If possible, scan backup data with an antivirus program to check that it is free of malware. This should be performed using an isolated, trusted system to avoid exposing backups to potential compromise.
- **Report incidents** to respective cybersecurity authorities:
    - **U.S. organizations** should report incidents immediately to the FBI at a local FBI Field Office, CISA at us-cert.cisa.gov/report, or the U.S. Secret Service at a U.S. Secret Service Field Office.
    - **Australian organizations** should report incidents to the ASD's ACSC via cyber.gov.au or call 1300 292 371 (1300 CYBER 1).
    - **UK organizations** should report incidents to NCSC-UK via report.ncsc.gov.uk and/or Action Fraud, the United Kingdom's fraud and cyber reporting centre, via actionfraud.police.uk.
- **Apply incident response best practices** found in the joint Cybersecurity Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

Note: cybersecurity authorities in the United States, Australia, and the United Kingdom strongly discourage paying a ransom to criminal actors. Criminal activity is motivated by financial gain, so paying a ransom may embolden adversaries to target additional organizations (or re-target the same organization) or encourage cyber criminals to engage in the distribution of ransomware. Paying the ransom also does not guarantee that a victim's files will be recovered. Additionally, reducing the financial gain of ransomware threat actors will help disrupt the ransomware criminal business model.

Additionally, NCSC-UK reminds UK organizations that paying criminals is not condoned by the UK Government. In instances where a ransom paid, victim organizations often cease engagement with authorities, who then lose visibility of the payments made. While it continues to prove challenging, the NCSC-UK has supported UK Government efforts by identifying needed policy changes—including measures about the cyber insurance industry and ransom payments—that could reduce the threat of ransomware.

Resources

- For more information and resources on protecting against and responding to ransomware, refer to StopRansomware.gov, a centralized, U.S. whole-of-government webpage providing ransomware resources and alerts.
- CISA's Ransomware Readiness Assessment is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.
- CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.
- The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.
- The ACSC recommends organizations implement eight essential mitigation strategies from the ACSC's Strategies to Mitigate Cyber Security Incidents as a cybersecurity baseline. These strategies, known as the "Essential Eight," make it much harder for adversaries to compromise systems.
- Refer to the ACSC's practical guides on how to protect yourself against ransomware attacks and what to do if you are held to ransom at cyber.gov.au.
- Refer to NCSC-UK's guides on how to protect yourself against ransomware attacks and how to respond to and recover from them at ncsc.gov.uk/ransomware/home.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The FBI, CISA, NSA, ACSC, and NCSC-UK do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation.

References

[1] United States Federal Bureau of Investigation
[2] United States Cybersecurity and Infrastructure Security Agency
[3] United States National Security Agency
[4] Australian Cyber Security Centre
[5] United Kingdom National Cyber Security Centre

Revisions

February 9, 2022: Initial Version