Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

30 March 2022

PIN Number

20220330-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Ransomware Attacks Straining Local US Governments and Public Services

Summary

The FBI is informing Government Facilities Sector (GFS) partners of cyber actors conducting ransomware attacks on local government agencies that have resulted in disrupted operational services, risks to public safety, and financial losses. Ransomware attacks against local government entities and the subsequent impacts are especially significant due to the public's dependency on critical utilities, emergency services, educational facilities, and other services overseen by local governments, making them attractive targets for cyber criminals. Victim incident reporting to the FBI between January and December 2021 indicated local government entities within the GFS were the second highest victimized group behind academia.

Threat

In 2021, local US government agency victims were primarily among smaller counties and municipalities, which was likely indicative of their cybersecurity resource and budget limitations. "The State of Ransomware in Government 2021" survey of 30 countries, conducted through an

independent research group commissioned by a UK-based company, found rectifying a ransomware attack on a local government often included financial liabilities related to operational downtime, people time, device costs, network costs, lost opportunity, and, in some cases, paid ransoms. Further, the survey found local governments were the least able to prevent encryption and recover from backups, and had the second highest rate of paying the ransom compared to other critical infrastructure sectors. According to a US-based media source reporting on state and local government matters, underfunded public sector organizations' understaffed and outdated systems often put them in the position to pay ransoms simply to get the data back.

Recent reporting indicates ransomware incidents against local governments resulted in disruptions to public and health services, emergency and safety operations, and the compromise of personal data. These types of attacks can have significant repercussions for local communities by straining financial and operational resources and putting residents at risk for further exploitation.

- In January 2022, a US county took computer systems offline, closed public offices, and ran emergency response operations using "backup contingencies" after a ransomware attack impacted local government operations. The attack also disabled county jail surveillance cameras, data collection capabilities, internet access, and deactivated automated doors, resulting in safety concerns and a facility lockdown.

- In September 2021, cyber actors infected a US county network with ransomware, resulting in the closure of the county courthouse and the theft of a substantial amount of county data (to include personal information on residents, employees, and vendors). The actors posted the data on the Dark web when the county refused to pay the ransom.

- In May 2021, cyber actors infected local US county government systems with PayOrGrief ransomware, making some servers inaccessible and limiting operations. The attack disabled online services, including scheduling of COVID-19 vaccination appointments, and the attackers claimed to have 2.5 gigabytes of data, including internal documents and personal information.

- In January 2021, cyber actors infected local US county government systems with ransomware that compromised jail and courthouse computers in addition to election, assessment, financial, zoning, law enforcement, jail management, dispatch, and other files. The attack impacted the sheriff department's records management program and county clerk, treasurer, and supervisor of assessment and public defender office computers. The ransomware note stated files would be deleted after two weeks if the ransom was not paid.

Ransomware tactics have and will continue to evolve as noted in the February 2022 Joint Cybersecurity Advisory (CSA) by government agencies in the United States, Australia, and the United

Kingdom.[1] The top three initial infection vectors in 2021 were phishing emails, remote desktop protocol exploitation, and software vulnerability exploitation. These were likely exacerbated by the continued remote work and learning environments which expanded the attack surface and challenged network defenders. In 2021, actors expanded their targeting tactics and widened the scope of victimization potential by implementing service-for-hire business models, sharing victim information among actor groups, diversifying extortion strategies, and attacking upstream/ downstream accesses and data sources such as cloud infrastructure, managed service providers, and software supply chains.

In the next year, local US government agencies almost certainly will continue to experience ransomware attacks, particularly as malware deployment and targeting tactics evolve, further endangering public health and safety, and resulting in significant financial liabilities. The FBI has an opportunity to disrupt some of this activity by leveraging partnerships with domestic and foreign governments, as well as the private sector, to more effectively identify actors, finances, and infrastructure.

Recommendations

The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees, and customers. Regardless of whether your organization decides to pay the ransom, the FBI urges you to report ransomware incidents as soon as possible to your local FBI field office (www.fbi.gov/contact-us/field-offices). Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law, when possible.

The FBI encourages local government agencies to proactively initiate contingency planning, to the degree possible, for operational continuity in the event of a ransomware attack and systems are inaccessible. For example, re-routing emergency communications of local dispatch centers, alternative communication mechanisms for residents and personnel (if systems typically rely on electronic communications or VoIP), or alternative methods to conduct administrative services (such as bill pay, reporting on utility issues, etc.).

In addition to the items above, the FBI recommends GFS organizations consider the following:

[1] Reference the 9 February 2022 Joint Cybersecurity Advisory "2021 Trends Show Increased Globalized Threat of Ransomware," published by the FBI, Cybersecurity & Infrastructure Security Agency, National Security Agency, Australian Cyber Security Centre, and the National Cyber Security Centre (GCHQ) at ic3.gov/media/news/2022/220209.pdf.

- **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, server-less 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.
- **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 strong, unique passwords for all accounts with password logins** (e.g., service account, admin accounts, and domain admin accounts). 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 that requires strong, unique passwords for each admin account.
- **Require multi-factor authentication** (MFA) for as many services as possible—particularly for webmail, VPNs, accounts that access critical systems, and privileged accounts that manage backups.
- **Maintain offline (i.e., physically disconnected) backups of data, and regularly test backup and restoration** to safeguard 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 separating 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.
- **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 security policy.
  - Open document readers in protected viewing modes to help prevent active content from running.

- **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.
- **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).

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.
- **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.
- **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.

- **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.
- **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.
- **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, use tools that log and report 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.
- **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.

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the US Government's new, official one-stop location for resources to tackle ransomware more effectively.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.