Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

8 January 2021

PIN Number
20210106-001

Please contact the FBI with any questions related to this Private Industry Notification at your local **Cyber Task Force**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

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 product was coordinated with DHS-CISA.

This PIN has been released **TLP: WHITE**: Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Egregor Ransomware Targets Businesses Worldwide, Attempting to Extort Businesses by Publicly Releasing Exfiltrated Data

Summary

The FBI first observed Egregor ransomware in September 2020. To date, the threat actors behind this ransomware variant claim to have compromised over 150 victims worldwide. Once a victim company's network is compromised, Egregor actors exfiltrate data and encrypt files on the network. The ransomware leaves a ransom note on machines instructing the victim to communicate with the threat actors via an online chat. Egregor actors often utilize the print function on victim machines to print ransom notes. The threat actors then demand a ransom payment for the return of exfiltrated files and decryption of the network. If the victim refuses to pay, Egregor publishes victim data to a public site.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

The FBI assesses Egregor ransomware is operating as a Ransomware as a Service Model. In this model, multiple different individuals play a part in conducting a single intrusion and ransomware event. Because of the large number of actors involved in deploying Egregor, the tactics, techniques, and procedures (TTPs) used in its deployment can vary widely, creating significant challenges for defense and mitigation. Egregor ransomware utilizes multiple mechanisms to compromise business networks, including targeting business network and employee personal accounts that share access with business networks or devices. Egregor ransomware may use phishing emails with malicious attachments to gain access to network accounts. Egregor can also exploit Remote Desktop Protocol (RDP) or Virtual Private Networks to gain access. Adversaries may also leverage Egregor's RDP exploitation capability to laterally move inside networks.

Once Egregor gains access to the network, Egregor ransomware affiliates use common pen testing and exploit tools like Cobalt Strike, Qakbot/Qbot, Advanced IP Scanner, and AdFind to escalate privileges and move laterally across a network, and tools like Rclone (sometimes renamed or hidden as svchost) and 7zip to exfiltrate data.

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom emboldens adversaries to target additional organizations, encourages other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local FBI field office. Doing so provides the FBI with the critical information they need to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law.

Recommended Mitigations

- Back-up critical data offline.
- Ensure copies of critical data are in the cloud or on an external hard drive or storage device.
- Secure your back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
- Install and regularly update anti-virus or anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks.
- Use two-factor authentication and do not click on unsolicited attachments or links in emails.

- Prioritize patching of public-facing remote access products and applications, including recent RDP vulnerabilities (CVE-2020-0609, CVE-2020-0610, CVE-2020-16896, CVE-2019-1489, CVE-2019-1225, CVE-2019-1224, CVE-2019-1108).
- Review suspicious .bat and .dll files, files with recon data (such as .log files), and exfiltration tools.
- Securely configure RDP by restricting access, using multi-factor authentication or strong passwords.

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 PIN has been released **TLP: WHITE**: Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey