Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 December 2020

PIN Number
20201210-001

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

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

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

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.

DoppelPaymer Ransomware Attacks on Critical Infrastructure Impact Critical Services

Summary

Since late August 2019, unidentified actors have used DoppelPaymer ransomware to encrypt data from victims within critical industries worldwide such as healthcare, emergency services, and education, interrupting citizens' access to services. Since its emergence in June 2019, DoppelPaymer ransomware has infected a variety of industries and targets, with actors routinely demanding six- and seven-figure ransoms in Bitcoin (BTC). Prior to infecting systems with ransomware, the actors' exfiltrate data to use in extortion schemes and have made follow-on telephone calls to victims to further pressure them to make ransom payments.

Threat Details

DoppelPaymer ransomware attacks since June 2019 have negatively impacted the provision of healthcare, emergency, and education services to citizens worldwide.

Healthcare

In September 2020, a DoppelPaymer attack against an identified hospital in Germany left emergency service personnel unable to communicate with the hospital. At least one individual requiring emergency services was re-routed to a hospital 20 miles away. This individual later died, though German authorities ultimately did not hold the ransomware actors responsible because the German authorities felt the individual's health was poor and the patient likely would have died even if they had not been re-routed. After German authorities contacted the actors through the provided communication accounts, the actors withdrew the extortion attempt and provided a digital decryption key upon learning patients' lives were endangered, according to open source reporting about the German investigation.

In July 2019, DoppelPaymer actors infected 13 out of 380 servers used by an identified US medical center with ransomware. The actors demanded a 50 bitcoin ransom, which, at the time of infection, was worth approximately $600,000. The medical center required several weeks to restore their systems from offsite backups following the ransomware attack.

Emergency Services

In September 2020, DoppelPaymer actors compromised an identified county's E911 Center and made changes, preventing officials from accessing the county's computer-aided dispatch (CAD) system. The actors reset passwords, removed accounts from the domain administrators group, and created an admin account called "AD." In a separate attack on a different county, the actors encrypted servers used by the county responsible for emergency dispatch, patrol, jail, and payroll departments.

In summer 2020, a DoppelPaymer attack disrupted police and emergency services as well as other government functions for an identified US city, forcing them to revert to manual operations to continue essential services to the community. The ransomware was introduced via an Internet Explorer/Edge browser after an employee viewed a cryptocurrency website. The city's system was infected by a Dridex malicious advertisement campaign through the browser's temporary internet files. The ransomware was successful in encrypting files stored on the following platforms: Windows 7, Windows 10, Server 2008, Server 2012, and Server 2016.

Educational Institutions

In September 2020, DoppelPaymer actors targeted an identified community college, resulting in school officials' limiting physical access to the campus for several days, impacting in-person classes. The actors claimed to have exfiltrated files, and provided the victim a TOR site, contact email, and BTC wallet for

contact and payment. During remediation efforts, malicious file “rdel.exe” was found on multiple machines. If the file were run in the command line with a corresponding CRC32 hash, the “rdel.exe” file would execute.

In July 2020, DoppelPaymer actors infected networks used by a different identified community college. Due to the infection, the college restricted network access to all but IT and maintenance staff. The malware infected servers at three of the college’s campuses but did not infect cloud-based applications.

Additional Tactics, Techniques, and Procedures

Doppelpaymer is one of the first ransomware variants where actors have called the victims to entice payments. As of February 2020, in multiple instances, DoppelPaymer actors had followed ransomware infections with calls to the victims to extort payments through intimidation or threatening to release exfiltrated data. In one case an actor, using a spoofed US-based telephone number while claiming to be located in North Korea, threatened to leak or sell data from an identified business if the business did not pay the ransom. During subsequent telephone calls to the same business, the actor threatened to send an individual to the home of an employee and provided the employee's home address. The actor also called several of the employee’s relatives.

Recommended Mitigations

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or 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 field office or the FBI’s Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

- Ensure backups are secure and are disconnected from the network at the conclusion of each backup session.
- Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible. Patch operating systems, software, firmware, and endpoints.
- Monitor inbound and outbound network traffic; set alerts for data exfiltration.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

- Apply two-factor authentication to user login credentials, receiving responses by text rather than email as actors may be in control of victim email accounts.
- Implement least privilege for file, directory, and network share permissions.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 CyberWatch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. 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. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

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

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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