Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

9 February 2021

PIN Number
20210209-001

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 PIN has been coordinated with DHS-CISA.

This PIN has been released **TLP: GREEN**. The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Cyber Actors Compromise US Water Treatment Facility

Summary

On 5 February 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a US water treatment plant. The unidentified actors accessed the SCADA system's software and increased the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the drinking water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal. The cyber actors likely accessed the system by exploiting cyber security weaknesses including poor password security, and an outdated Windows 7 operating system to compromise software used to remotely manage water treatment. The actor also likely used the desktop sharing software TeamViewer to gain unauthorized access to the system.

The FBI has observed cyber actors targeting and exploiting desktop sharing software and computer networks running operating systems with end of life status to gain unauthorized access to systems. Desktop sharing software has multiple legitimate uses such as enabling telework, remote technical support, and file transfers, but can also be exploited through malicious actors' use of social engineering tactics and other illicit measures. Windows 7 became more susceptible to exploitation due to a lack of security updates and well known vulnerabilities discovered. Microsoft, the FBI, and other industry professionals strongly recommend upgrading computer systems to an actively supported operating system. Continuing to use any operating system within an enterprise beyond the end of life status presents vulnerabilities for cyber actors to exploit.

Threat Overview

Desktop Sharing Software

The FBI has observed corrupt insiders and external cyber actors using desktop sharing software to victimize targets in a range of organizations, including those in the critical infrastructure sectors. In addition to adjusting system operations, cyber actors also use the following techniques:

- Use access granted by desktop sharing software to perform fraudulent wire transfers.
- Inject malicious code, which allows the cyber actors to hide desktop sharing software windows, protect malware files from being detected, and control desktop sharing software startup parameters to obfuscate their activity.
- Move laterally across a network to increase the scope of activity.

TeamViewer, a desktop sharing software, is a legitimate popular tool used by cyber actors engaged in targeted social engineering attacks, as well as large scale, indiscriminate phishing campaigns. Desktop sharing software can also be exploited by employees who pose an insider threat against their employers.

Beyond its legitimate uses, TeamViewer allows cyber actors to exercise remote control over computer systems and drop files onto victim computers, making it functionally similar to Remote Access Trojans (RATs). TeamViewer's legitimate use, however, makes anomalous activity less suspicious to end users and system administrators compared to typical RATs.

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Windows 7 End of Life

On 14 January 2020, Microsoft ended support for the Windows 7 operating system, which includes security updates and technical support unless certain customers purchased an Extended Security Update (ESU) plan. The ESU plan is paid per-device and available for Windows 7 Professional and Enterprise versions, with an increasing price the longer a customer continues use. Microsoft will only offer the ESU plan until January 2023. Continued use of Windows 7 creates the risk of cyber actor exploitation of a computer system.

Cyber actors continue to find entry points into legacy Windows operating systems and leverage Remote Desktop Protocol (RDP) exploits. Microsoft released an emergency patch for its older operating systems, including Windows 7, after an information security researcher discovered the RDP vulnerability in May 2019. Since the end of July 2019, malicious RDP activity has increased with the development of a working commercial exploit for the vulnerability. Cyber actors often use misconfigured or improperly secured RDP access controls to conduct cyber attacks. The xDedic Marketplace, taken down by law enforcement in 2019, flourished by compromising RDP vulnerabilities around the world.

Recommendations

The following measures may help protect against this scheme:

- Use multiple factor authentication;
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials;
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured, and secure;
- Audit network configurations and isolate computer systems that cannot be updated;
- Audit your network for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts;
- Audit logs for all remote connection protocols;
- Train users to identify and report attempts at social engineering;
- Identify and suspend access of users exhibiting unusual activity;
- Keep software updated.

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: GREEN. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.
For comments or questions related to the content or dissemination of this product, contact CyWatch.

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