Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

30 March 2020

PIN Number

20200330-001

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.

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

www.fbi.gov/contact-us/field | **E-Mail:** cywatch@fbi.gov | **Phone: 1-855-292-3937**

Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector

Summary

Since at least 2016, the FBI has observed an Advanced Persistent Threat (APT) actor conduct a global network exploitation campaign using the Kwampirs Remote Access Trojan (RAT) and is providing additional, non-technical information in an effort to highlight key objectives of the actor campaign. This information, along with previously released FBI Liaison Alert System (FLASH) messages, is intended to enhance the network defense posture of public and private partners.

The Kwampirs RAT is a modular RAT worm that gains system access to victim machines and networks, with the primary purpose of gaining broad, yet targeted, access to victim companies to enable follow-on computer network exploitation (CNE) activities. Through victimology and forensic analysis, the FBI found heavily targeted industries include healthcare, software supply chain, energy, and engineering across the United States, Europe, Asia, and the Middle East. Secondary targeted industries include financial institutions and prominent law firms.

The FBI has not seen the Kwampirs RAT incorporating a wiper or destructive module components; however, through comparative forensic analysis, several code-based similarities exist with the data destruction malware Disttrack (commonly known as Shamoon).

Kwampirs Targeting the Healthcare Sector

Kwampirs operations against global healthcare entities have been effective, gaining broad and sustained access to targeted entities. Targeted entities range from major transnational healthcare companies to local hospital organizations. The scope of infections has ranged from localized infected machine(s) to enterprise infections. During these campaigns, the Kwampirs RAT performed daily command and control communications with malicious IP addresses and domains that were hard-coded in the Kwampirs RAT malware.

The FBI assesses Kwampirs actors gained access to a large number of global hospitals through vendor software supply chain and hardware products. Infected software supply chain vendors included products used to manage industrial control system (ICS) assets in hospitals.

Kwampirs Campaign Overview

This campaign employs a two-phased approach. The first phase establishes a broad and persistent presence on the targeted network, to include delivery and execution of secondary malware payload(s). The second phase includes the delivery of additional Kwampirs components or malicious payload(s) to further exploit the infected victim host(s).

For technical indicators of compromise (IOCs) and YARA rules related to the Kwampirs RAT, please see previous TLP: WHITE FBI FLASH messages CP-000111-MW: *"Kwampirs Malware Indicators of Compromise Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries"* and CP-000118-MW: *"YARA Rules to Identify Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries,"* released on 6 January 2020, and 5 February 2020, respectively.

Kwampirs actors have successfully gained, then sustained persistent presence on victim networks for a time period ranging from three to 36 months, and deployed a targeted secondary module, which performed detailed reconnaissance. The following are examples of targeted network assets of the secondary module:

- Primary domain controllers;
- Secondary domain controllers;
- Engineer servers which are used to develop and test ICS products and instruments;
- Software development servers which maintain source code for software applications;
- File servers which are used as shared repositories for research and development (R&D).

Targeted software supply chain vendors share some of the following business and operations attributes:

- Global imaging business products/services that are multi-industry;
- Product co-development and corporate alliances with worldwide software companies;
- Product co-development and corporate alliances with companies in the Enterprise Resource Planning (ERP) industry;
- Products and services supporting ICS maintenance functions, with strong business presence in the Healthcare and Energy sectors.

Significant intrusion vectors include the following:

- During mergers and acquisition(s), infections from one company have moved laterally into the acquiring company once the networks are connected;
- During the software co-development process, malware has been passed between multiple entities through shared resources;
- During the software co-development process, shared internet facing resources have infected co-development participants;
- Software supply chain vendors infected device(s) installed on the customer/corporate LAN or customer/corporate cloud infrastructure.

Kwampirs campaign actors have targeted companies in the imaging industry, to include networked scanner and copier-type devices, with domain access to customer networks. The FBI assesses these imaging vendors are targeted to gain access to customer networks, including remote or cloud management access, which could permit lateral CNE movement within victim networks.

The FBI emphasizes, due to the modular nature of the Kwampirs RAT, secondary module(s) are capable of being downloaded to the victim network, which would provide access to enable further CNE activities. Secondary module(s) downloaded would be separate and different from the Kwampirs RAT IOCs, and may not have been remediated by anti-virus end point protection.

Residual Kwampirs RAT host artifacts may still reside on victim networks and be valuable in assisting a company to determine if they were a victim of the Kwampirs RAT. The artifacts include the following four .pnf files:

Post AV - Possible Residual Artifacts Created by the Kwampirs RAT Found in: %SystemRoot%/inf/	
mtmndkb32.pnf	digirps.pnf
mkdiawb3.pnf	ie11.pnf

Another method of identifying historical artifacts associated with a previous Kwampirs RAT intrusion, post AV remediation, is to examine **System 7045** Events, with a service name of **WMI Performance Adapter Extension**. This is actually a legitimate Windows service and the location

should be **C:\Windows\System32\wbem\WmiApSrv.exe** for Windows 10, 8, 7, XP, and Windows Server OS. Eliminating the legitimate services would identify remaining services that are Kwampirs. This can be confirmed by correlating with AV logs or, if still present, scanning the binary with AV.

Recommendations:

Recommended Actions Post-Infection:

If a Kwampirs RAT infection is detected, contact your IT mitigation and remediation company and coordinate your mitigation efforts with your local FBI field office. The following information is helpful in assisting the FBI's investigation of this malware:

- Full capture of network traffic in PCAP format from the infected host(s) (48 hour capture);
- Full image and memory capture of infected host(s);
- Web proxy logs capture, to include cache of the Web proxy;
- DNS and firewall logs;
- Identification and description of host(s) communicating with the C2 (ex: server, workstation, other);
- Identification of patient zero and attack vector(s), if able.

Best Practices for Network Security and Defense:

- Employ regular updates to applications and the host operating system to ensure protection against known vulnerabilities.
- Establish, and backup offline, a "known good" version of the relevant server and a regular change-management policy to enable monitoring for alterations to servable content with a file integrity system.
- Employ user input validation to restrict local and remote file inclusion vulnerabilities.
- Implement a least-privileges policy on the Web server to:
    - Reduce adversaries' ability to escalate privileges or pivot laterally to other hosts;
    - Control creation and execution of files in particular directories.
- If not already present, consider deploying a demilitarized zone (DMZ) between the Web-facing systems and corporate network. Limiting the interaction and logging traffic between the two provides a method to identify possible malicious activity.
- Ensure a secure configuration of Web servers. All unnecessary services and ports should be disabled or blocked. All necessary services and ports should be restricted where feasible. This can include whitelisting or blocking external access to administration panels and not using default login credentials.

- Use a reverse proxy or alternative service to restrict accessible URL paths to known legitimate ones.
- Conduct regular system and application vulnerability scans to establish areas of risk. While this method does not protect against zero-day attacks, it will highlight possible areas of concern.
- Deploy a Web application firewall and conduct regular virus signature checks, application fuzzing, code reviews, and server network analysis.

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 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. 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.

Administrative Note

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