FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

06 January 2020

Alert Number

CP-000111-MW

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the **Reporting Notice** section of this message.

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

**Note: This information is being provided by the FBI to assist cyber security specialists protect against the persistent malicious actions of cyber criminals. The information is provided without any guaranty or warranty and is for use at the sole discretion of the recipients.*

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

This FLASH 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.

Kwampirs Malware Indicators of Compromise Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries

Summary:

Since at least 2016, an ongoing campaign using the Kwampirs Remote Access Trojan (RAT) targeted several global industries, including the software supply chain, healthcare, energy, and financial sectors. The FBI assesses software supply chain companies are a key interest and target of the Kwampirs campaign. This campaign has two phases. 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).

Technical Details:

Propagation, Persistence, Backdoor (Module 1):

Upon successful infection, the Kwampirs RAT propagates laterally across the targeted network via `SMB port 445`, using hidden admin shares such as `ADMIN$` and `C$`. The malware maintains persistence on the infected Windows host by dropping a binary to the hard drive and creating a malicious Windows system service set to auto start upon reboot. The new malicious service scans and catalogs the host configuration, encrypts the data, and transmits it to an external Command and Control (C2) server via an `HTTP GET` request on `port 80`.

Secondary Payload (Module 2):

Module 2 executes additional Kwampirs RAT modular components on the infected host(s). These malicious components can allow for additional detailed collection of system and network interface configuration. This information is encrypted and transmitted to the C2 server via `HTTP`. The FBI has observed secondary module commands, to be highly targeted and executed on critical business and/or network hosts, to include the following:

- Primary Domain Controllers
- Secondary Domain Controllers
- Engineering & Quality Assurance / Testing workstations
- Primary Source Code servers

Secondary Modules executed on the victim host(s), include the following additional commands being executed, resulting in much deeper and thorough reconnaissance on the targeted entity.

Command Prompt	Command Description
`cmd.exe /c "hostname" 2>nul`	Query infected system's hostname
`cmd.exe /c "getmac" 2>nul`	Query infected system's MAC address
`cmd.exe /c "ver" 2>nul`	Query infected system's version number
`cmd.exe /c "arp -a" 2>nul`	View the current ARP cache
`cmd.exe /c "systeminfo" 2>nul`	Display detailed configuration information, product ID, and hardware properties
`cmd.exe /c "tasklist /v" 2>nul`	Display the currently-running tasks in a verbose format
`cmd.exe /c "tasklist /svc" 2>nul`	Display the currently-running tasks with services hosted in each process
`cmd.exe /c "netstat -nab" 2>nul`	Deliver basic statistics on all network activities. (-n=Numerical display of address and port numbers, -a=Display all active ports, -b=Display executable file of a connection or listening port)

Command Prompt WMIC Command	Command Description
`cmd.exe /c "wmic nic get caption,AdapterType, Manufacturer" 2>nul`	Query infected system's network interface card type and manufacturer
`cmd.exe /c "wmic timezone get caption" 2>nul`	Query infected system's timezone
`cmd.exe /c "wmic IRQ get caption, IRQNumber" 2>nul`	Query the infected system's Interrupt ReQuest setting in the system's BIOS
`cmd.exe /c "wmic port get StartingAddress, EndingAddress" 2>nul`	Identify open and closed ports on an infected system
`cmd.exe /c "wmic csproduct" 2>nul`	Aquire the computer model of the infected system
`cmd.exe /c "wmic computerSystem" 2>nul`	Aquire the computer manufacturer and model, to include (32bit/64bit) architecture information
`cmd.exe /c "wmic baseboard" 2>nul`	Aquire motherboard manufacturer, model number, and serial number
`cmd.exe /c "wmic cpu" 2>nul`	Aquire the current CPU settings for the infected system
`cmd.exe /c "wmic partition" 2>nul`	Identify disk partitions on the infected system
`cmd.exe /c "wmic bios" 2>nul`	Determine the current BIOS configuration for the infected system
`cmd.exe /c "wmic startup" 2>nul`	List programs that run on startup on the infected system
`cmd.exe /c "wmic netlogin" 2>nul`	Display login sessions on an infected system
`cmd.exe /c "wmic portconnector" 2>nul`	Identify open ports on the infected system
`cmd.exe /c "wmic memphysical" 2>nul`	Display the amount of physical memory that the infected system has
`cmd.exe /c "wmic share" 2>nul`	Display all shared resources
`cmd.exe /c "wmic logon" 2>nul`	Display what username is currently logged onto the infected system
`cmd.exe /c "wmic OS" 2>nul`	Determine the current operating system type for the infected system
`cmd.exe /c "wmic logicaldisk get caption,description,size, providername" 2>nul`	Determine the current disk space, type, and manufacturer
`cmd.exe /c "wmic desktop" 2>nul`	Query desktop configuration settings through the infected system's desktop management software
`cmd.exe /c "wmic process get caption,commandline" 2>nul`	Generate process list of current infected system

The FBI has discovered that the Kwampirs RAT establishes persistence on the victim host by creating a service with the following configuration:

Kwampirs RAT Created Service	
Service name:	`WmiApSrvEx`
Service display name:	`WMI Performance Adapter Extension`
Registry key:	`SYSTEM\CurrentControlSet\Services\WmiApSrvEx`
Service image path:	`%SystemRoot%\system32\**Executable Filename**`

The FBI has identified the following Kwampirs RAT executable filenames:

Kwampirs RAT Executable Files - Found in: `c:\windows\system32\`		
`wmiaprvse.exe`	`wmiapsrve.exe`	`wmiapsvrce.exe`
`wmiapsrvce.exe`	`wmiApSrvEx.exe`	`wmiapsvre.exe`
`wmiapvsre.exe`	`wmipsvrce.exe`	`wmipvsre.exe`
`wmipsrvce.exe`	`wmiprvse.exe`	`wmipsvre.exe`

The FBI has identified additional Kwampirs RAT DLL files, utilized by the malware:

Kwampirs RAT DLL files dropped to disk		
Files identified in `c:\windows\syswow64\`		
`wmipadp.dll`	`wmiassn.dll`	`wmipdpa.dll`
`wmiamgmt.dll`		
Files identified in `c:\windows\system32\`		
`wmiadrv.dll`	`wmipadp.dll`	`wmiassn.dll`
`wmipdpa.dll`	`wmiamgmt.dll`	

Other files created by the Kwampirs RAT Found in: `%SystemRoot%/inf/`	
`mtmndkb32.pnf`	`digirps.pnf`
`mkdiawb3.pnf`	`ie11.pnf`

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 would assist 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.
- Utilize 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). With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

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. 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.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.