مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

FrostyGoop/BUSTLEBERM OT-Centric Malware Threat

Tracking #:432316545

Date:22-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed FrostyGoop, also known as BUSTLEBERM, emerged as a highly impactful operational technology (OT)-centric malware used in a cyberattack targeting critical infrastructure.

TECHNICAL DETAILS:

In July 2024, FrostyGoop, also known as BUSTLEBERM, emerged as a highly impactful operational technology (OT)-centric malware used in a cyberattack targeting critical infrastructure. FrostyGoop uses the Modbus TCP protocol to interact with Industrial Control Systems (ICS), allowing attackers to manipulate or read device data. This marks the malware as one of the most sophisticated ICS-centric threats identified to date. The attack leveraged exposed OT devices and revealed vulnerabilities in widely used protocols like Modbus, which are crucial to critical infrastructure systems globally.
While the malware is primarily used to attack ENCO devices, any Modbus TCP-compatible ICS devices are vulnerable. Threat actors have been observed using FrostyGoop to send commands to ICS devices, triggering errors and operational malfunctions.

Technical Details
Malware Overview

- **Name**: FrostyGoop/BUSTLEBERM
- **Type**: OT/ICS-centric malware
- **Protocol Exploited**: Modbus TCP
- **Initial Compromise**: Suspected exploitation of MikroTik router vulnerabilities (still unconfirmed); could also involve directly exposed OT devices.

Malware Functionality

- FrostyGoop uses the Modbus TCP protocol, a common communication method for ICS devices, to conduct operations like reading and modifying device registers.
- The malware is capable of performing **read**, **write**, and **write-multiple** Modbus operations on compromised ICS devices.
- FrostyGoop is configured using JSON files, which include specific operations for Modbus registers, thus enabling attackers to modify device behavior remotely.
- FrostyGoop is compiled using the Go programming language and leverages a specific open-source Modbus implementation, enhancing its evasion capabilities and making it harder to detect by traditional defense measures.
- A related tool, **go-encrypt.exe**, is used to encrypt and decrypt the configuration files (task_test.json), further obscuring the attackers' actions and intentions.

Exposed Devices and Network Traffic

- The attack vector for FrostyGoop primarily involved devices exposed to the internet, such as ENCO control devices. Over a period of one month in 2024, more than **1 million Modbus TCP devices** were exposed to the internet.
- **Port Exposure**: FrostyGoop leveraged exposed Modbus ports (TCP 502) and other vulnerable ports like Telnet (Port 23) to gain control of OT devices.
- **Network Traffic**: FrostyGoop generates Modbus commands (e.g., function code 3 - read holding registers) to interact with compromised devices, manipulating their data or causing malfunctions.

Indicators of Compromise:

SHA256 hash:

- 5d2e4fd08f81e3b2eb2f3eaae16eb32ae02e760afc36fa17f4649322f6da53fb
- File size: 3.7 MB (3,699,200 bytes)
- File type: PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
- File description: Windows executable file for FrostyGoop malware

SHA256 hash:

- a63ba88ad869085f1625729708ba65e87f5b37d7be9153b3db1a1b0e3fed309c
- File size: 2.4 MB (2,439,680 bytes)
- File type: PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
- File description: Windows executable file for FrostyGoop malware

SHA256 hash:

- 2fd9cb69ef30c0d00a61851b2d96350a9be68c7f1f25a31f896082cfbf39559a
- File size: 3.4 MB (3,359,232 bytes)
- File type: PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
- File description: Windows executable file for FrostyGoop malware

SHA256 hash:

- c64b67c116044708e282d0d1a8caea2360270a7fc679befa5e28d1ca15f6714c
- File size: 2.0 MB (1,951,232 bytes)
- File type: PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
- File description: Windows executable file for FrostyGoop malware

SHA256 hash:

- 91062ed8cc5d92a3235936fb93c1e9181b901ce6fb9d4100cc01167cdc08745f
- File size: 2.5 MB (2,516,480 bytes)
- File type: PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
- File description: Windows executable file for FrostyGoop malware

SHA256 hash:

- a25f91b6133cb4eb3ecb3e0598bbab16b80baa40059e623e387a6b1082d6f575
- File size: 2.5 MB (2,515,968 bytes)
- File type: PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
- File description: Windows executable file for FrostyGoop malware

SHA256 hash:

- 9cf30d82a86a9485f7bbd0786a5de207cf4902691a3efcfc966248cb1e87d5b7
- File size: 1.8 MB (1,773,568 bytes)
- File type: PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows

- File description: Windows executable file for go-encrypt.exe, likely used during previous FrostyGoop activity

SHA256 hash:

- 06919e6651820eb7f783cea8f5bc78184f3d437bc9c6cde9bfbe1e38e5c73160
- File size: 0.4 KB (379 bytes)
- File type: JSON text data
- File description: JSON file named task-test.json likely used to test go-encrypt.exe in July 2024 FrostyGoop attack

RECOMMENDATIONS:

1. **Strengthen Device Exposure Management**
   - **Minimize Internet Exposure**: OT devices should not be directly exposed to the internet. Use firewalls and VPNs to limit external access to ICS systems.
   - **Network Segmentation**: Isolate ICS/OT networks from corporate IT networks to reduce the attack surface. Employ robust segmentation strategies.
   - **Close Unnecessary Ports**: Disable or block all non-essential ports (e.g., Telnet port 23, Modbus port 502) on OT devices.
2. **Patch and Update Vulnerable Devices**
   - Ensure all OT devices, routers, and other network infrastructure are up-to-date with the latest firmware. This includes patching known vulnerabilities in devices like MikroTik routers and TP-Link routers that could be used in attacks.
3. **Implement Robust Authentication**
   - Require multi-factor authentication (MFA) for any remote access to ICS systems and ensure strong passwords for devices accessible via Telnet, SSH, or web interfaces.
4. **Monitor Network Traffic for Anomalies**
   - Utilize intrusion detection systems (IDS) and network traffic analysis tools to monitor for unusual Modbus traffic, such as unauthorized read/write commands.
   - Implement **anomaly detection** to identify suspicious Modbus function codes (e.g., read holding registers or write operations to critical registers).
5. **Regularly Review and Update Incident Response Plans**
   - Establish and test response protocols specifically for OT-related incidents. Ensure that your security team is trained to handle ICS-specific cyberattacks like those involving FrostyGoop.
6. **Leverage Threat Intelligence and Detection**
   - Utilize threat intelligence services to stay updated on the latest malware samples and tactics, techniques, and procedures (TTPs) associated with OT-centric malware like FrostyGoop.
   - Employ **next-generation firewalls** (NGFW) and **endpoint detection & response** (EDR) solutions to provide real-time monitoring and automated defense against known IOCs and malware signatures.
7. **Encryption and File Integrity**
   - Ensure that sensitive configuration files, including JSON files used in malware campaigns, are encrypted.
   - Implement file integrity monitoring (FIM) systems to detect unauthorized changes to configuration files or suspicious file creations on ICS/OT systems.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://unit42.paloaltonetworks.com/frostygoop-malware-analysis/