'GhostSec' Claim of First RTU Ransomware Operation Shows No Technical Advancements, but Highlights Expanding Hacktivist Interest in OT

Critical Infrastructure (CI) | Fusion (FS)

January 17, 2023 04:18:02 PM, 23-00001083, Version: 1

Executive Summary

- In January 2023, Mandiant identified the English-speaking actor "GhostSec" claim to have conducted the first ransomware operation against a remote terminal unit (RTU), a type of operational technology (OT) asset.
- The threat actor shared screenshots of the filesystem as proof, which show that they modified the file extensions of an RTU with a Belarus-based IP address allegedly via ransomware.
- While we are unable to verify the claim, we believe the actor likely encrypted files on a legitimate, internet-accessible OT asset in Belarus. However, the targeted asset appears to primarily support OT network communications rather than automation or control functionality.
- The claim highlights low-sophisticated actors' continued interest in OT systems. While the claim is misleading, we rarely observe hacktivists leverage ransomware, particularly against OT assets. OT asset owners should maintain situational awareness of these claims to better prioritize countermeasures.

Threat Detail

On Jan. 11, 2023, Mandiant observed a post on the Telegram channel of the hacktivist group "GhostSec" in which they claimed to have encrypted the filesystem of an RTU in Belarus. GhostSec is an Anonymous-affiliated hacktivist collective that has consistently been targeting various types of IT and OT systems in Russia and allied nations in response to the invasion of Ukraine (22-00004492). Two screenshots shared with the post allegedly show the filesystem of the device before (Figure 1) and after (Figure 2), with the latter showing the files with altered extensions.

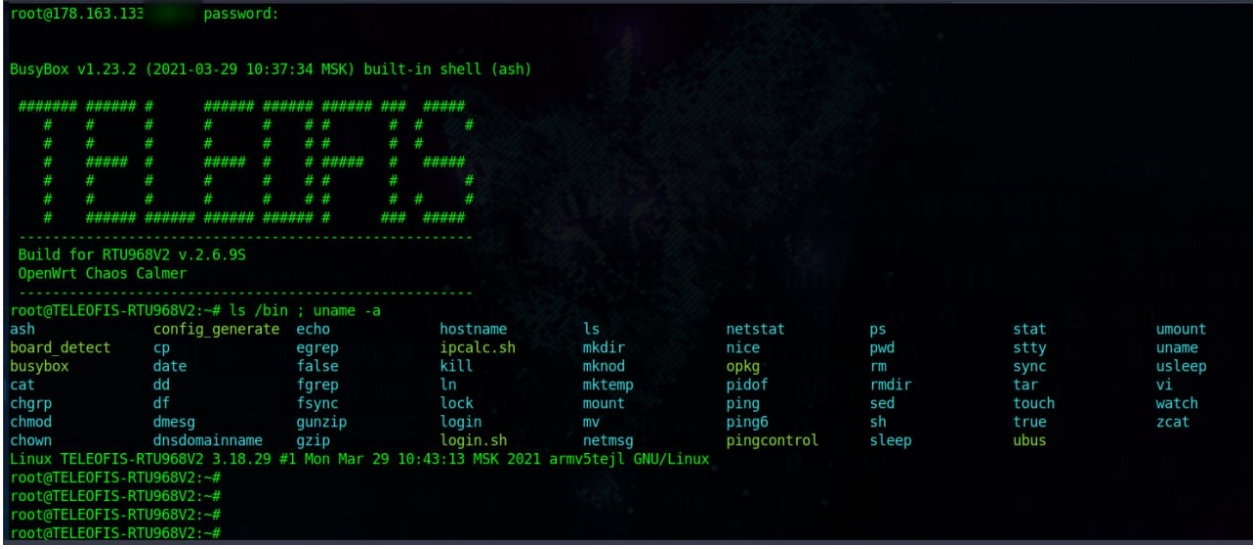

Figure 1: Alleged screenshot of RTU filesystem before encryption

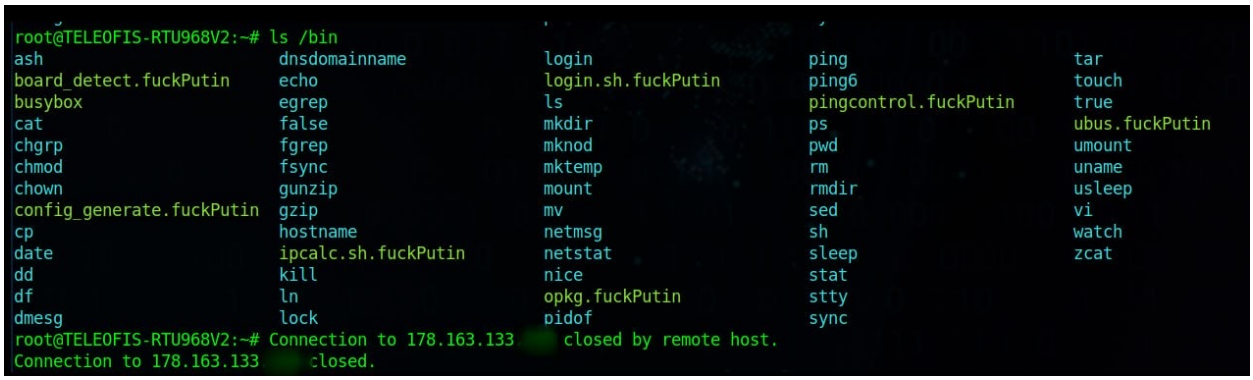

Figure 2: Alleged screenshot of RTU filesystem after encryption

- The screenshots included in the post indicate that the device targeted is a TELEOFIS RTU968 V2 located in Belarus and show several key pieces of system information meant to prove that the filesystem of the device was encrypted by the threat actor and that the threat actor has the capability to compromise RTUs.
  - *TELEOFIS RTU968 V2 and Belarus geolocation*
    - Per the manufacturer, the TELEOFIS RTU968 V2 is a 3G router featuring RS-232 and RS-485 serial interfaces, i[.]MX287 ARM9 processor, and OpenWrt operating system. The operating system is open source and available publicly on the project website. Bootloader, firmware, and SDK files for this device are available publicly on GitHub.
      - The banner of Figure 1 indicates TELOFIS as the device vendor, RTU968V2 firmware version 2.6.9S, and OpenWrt 15.05 "Chaos Calmer."
      - The terminal prompt indicates the hostname of the device is "TELEOFIS-RTU968V2".
      - The returned result of the command "uname -a" indicates the device is running on the "armv5tej" architecture. This architecture is not the one implemented in the manufacturer's advertised processor (ARM926EJ-S), but as the product line was debuted in 2016, it could indicate an older hardware version.
    - While the last octet of the IP address pictured is blurred, 178[.]163[.]133[.]0/24 is indeed an IP address block operated by Belarussian telecom provider A1. We fingerprinted a TELEOFIS RTU968 V2 asset operating in that IP range, which suggests that the victim asset was a legitimate device.
  - *Filesystem Encryption*

        - Figure 2 shows several filenames modified with appended ".fuckPutin" extensions. Modification of filenames and extensions is common in ransomware attacks, but the actor offered no further proof to validate that the modification was caused by ransomware.
        - The extension of the file "busybox" was not modified presumably because it is necessary to operate BusyBox, an open-source project often utilized in embedded systems, to provide common Linux functionality such as the "ls," "mv," "mkdir," "tar," and "grep" commands as well as a shell to run them.
- While we are unable to verify the actor's claim entirely, it is plausible that they encrypted the filesystem of an OT asset in Belarus.
    - Through open-source information and internet search engines, we have identified 42 devices that appear to be TELEOFIS RTU698 V2 systems. Most are located in Russia; however, three are located in Belarus and potentially include the device allegedly compromised by the threat actor. While most of these devices appear to have more robust security controls, such as VPNs, in place to prevent unauthorized remote access, the threat actor was likely able to gain access via SSH directly via brute forcing credentials or a similar technique.
    - This is consistent with current trends in hacktivist claims of OT asset compromises as these groups often gain malicious access to internet-accessible OT assets by leveraging internet-device search engine tools, such as Shodan and Censys (22-00022003).

Claim of First "RTU" Ever Encrypted Misleading

While the evidence provided by the threat actors appears to demonstrate that the device is a TELEOFIS RTU698 V2 and that the filesystem was compromised, we believe the actor's claim of the "first RTU ever encrypted" is misleading.

- Whereas most RTUs operating in industrial control environments are highly specialized devices engineered for specific applications and often running on real-time operating systems (RTOS), the TELEOFIS RTU968 V2 is essentially a small form factor computer not unlike a Raspberry Pi, which runs on a generic version of Linux with hardware modules to add 3G and serial connectivity.
- Attacks against Linux systems are not new or novel, nor is encrypting Linux filesystems (20-00023423, 21-00017909). The primary novel feature of a theoretical encryption attack against RTUs would be the encryption of control logic, but the targeted device appears to essentially function as a router and not a controller.
- The actor does not provide evidence of connected serial devices, commonly used ports in control systems, or other indication the device is being used as part of a control system network. However, per the manufacturer's website, the device appears primarily marketed for OT environments.

'GhostSec' Shows Traditional Hacktivist Capabilities and Limitations, but Unusual Interest in OT

GhostSec is an Anonymous-affiliated hacktivist group founded in 2014. The group began by mostly conducting distributed denial-of-service (DDoS) attacks against websites of groups, organizations, and countries they profess ideological opposition to. However, in response to the invasion of Ukraine and the targeting of ICS/OT systems by Russian cyberattacks, various groups, including GhostSec, have developed an increasing interest in targeting ICS/OT systems (22-00014563). GhostSec's activity has marginally deviated from baseline hacktivist activity against OT as the group has repeatedly leveraged multiple ICS-oriented exploitation frameworks, which we rarely observe deployed in the wild (22-00014563 and 22-00027178).

Outlook

Mandiant has previously reported on hacktivist claims of OT compromises, specifically noting that the majority of such attacks leverage internet-accessible systems and unsecure configurations. While this threat activity largely appears to fall into this category, it is important to note the ongoing interest of hacktivists in targeting ICS/OT environments. While GhostSec's latest claim is misleading, we rarely observe hacktivists leverage ransomware, particularly against low-level OT assets. We assess this claim and broader hacktivism trend's targeting OT will likely continue due to factors like publicly available ICS attack tools and Russia's invasion of Ukraine (22-00022003).

We recommend asset owners and operators maintain situational awareness of trends in hacktivist capability and intent to target ICS/OT systems and motivational factors, such as the ongoing conflict in Ukraine. Furthermore, we recommend best practices for remote access to critical and internet-accessible systems, such as using a VPN solution configured to use multi-factor authentication (MFA) to access an ICS/OT demilitarized zone (DMZ), followed by initiating a remote desktop connection to a dedicated jump host in the ICS/OT network that uses a separate authentication domain.

Please rate this product by taking a short four question survey

First Version Publish Date

January 17, 2023 04:18:02 PM

Threat Intelligence Tags

Actors

- GhostSec
  Aliases
  - GhostSec

Affected Industries

- Construction & Engineering

Affected Systems

- Users/Application and Software
- Industrial Network Protocols

Intended Effects

- Disruption
- Interference with ICS

Motivations

- Ego
- Ideological/Religious

Tactics, Techniques And Procedures (TTPs)

- Malware Propagation and Deployment
- Web Application Attacks

- Ransomware

Target Geographies

- Belarus

Version Information

Version:1, January 17, 2023 04:18:02 PM

german[.]simkin@mandiant.com