Threat Intelligence Report

Emerging Threat: Threat Actors Deploying FOG Ransomware Exfiltrated Data from Victims, Suggesting Previously Unobserved Double Extortion Tactic

"FOG," a new ransomware family, has been targeting organizations in the academic and recreation sectors of the United States since May 2024. Until now, open-source reports on FOG ransomware have only described data encryption. Once victim files were encrypted by the ransomware payload, FOG ransom notes directed victims to a dedicated chat site to discuss payment in exchange for decryption. In June 2024, however, FTI Cybersecurity investigated FOG ransomware infections in which threat actors also exfiltrated data from victim environments, a previously unobserved tactic. Based on these findings, FTI Cybersecurity assesses that threat actors deploying FOG ransomware will almost certainly begin to employ double extortion tactics against victims who do not engage in ransom negotiations.[1]

THREAT ACTIVITY

FOG ransomware infections have generally exhibited consistent elements, though specific indicators of compromise have varied. FTI Cybersecurity observed threat actor behavior consistent with past-reported FOG infections, with one notable exception: data exfiltration.

- FTI Cybersecurity determined the threat actor gained unauthorized access to the victim's Virtual Private Network (VPN) using compromised credentials available on the dark web.
- Once a connection had been established via VPN, the threat actor pivoted to a backup server and leveraged a domain administrator account to run various reconnaissance operations. FTI Cybersecurity subsequently observed the threat actor create a new user, granting the new account local administrative privileges.
- From there, the threat actor established a connection to a suspected command and control (C2) server and began conducting network and host-based enumeration of target systems and system passwords.
- After several days of reconnaissance, the threat actor gained access to the victim's underlying virtualization infrastructure and dropped the ransomware payload.
- After the payload was dropped, the threat actor exfiltrated data from the victim's virtual datastores before initiating encryption. Based on FTI Cybersecurity analysis, exfiltration likely occurred via Secure File Transfer Protocol (SFTP). Within hours of exfiltration, several commands were issued to prepare and escalate the permissions of the ransomware binary. Once the actor obtained execution permissions on the virtualization host, they initiated encryption on the datastore volumes. Notably, encryption targeted underlying datastores within the virtual machine infrastructure, rather than specific hosts.
- Once encryption was complete, FTI Cybersecurity observed the threat actor enumerating all virtual machines and powering them down.
- FTI Cybersecurity identified a ransom note left by the threat actors, which contained a link to a unique chat room for ransom negotiations.

[1] Double extortion refers to a ransomware tactic in which threat actors exfiltrate victim files before encrypting them, then threaten to leak sensitive data if a ransom is not paid.

RECOMMENDED ACTIONS

Based on knowledge of the FOG ransomware group, and threat actors generally, FTI Cybersecurity recommends the following preventative actions:

- Monitor dark and deep web sources for leaked credentials.
- Use Multifactor Authentication (MFA) on VPN services and other externally facing resources.
- Limit service and administrative accounts using the "no trust" model. Assign permissions granularly, or only as needed.
- Rotate service and administrative account passwords every 30-45 days.
- Generally limit the risk of ransomware by employing next-generation anti-virus and endpoint detection solutions, implementing network segmentation, and maintaining secure offline data backups in case of encryption.
- Consider retaining a dedicated third-party Incident Response firm to ensure seamless and rapid response to a cybersecurity incident.

THREAT ASSESSMENT

FTI Cybersecurity assesses threat actors deploying Fog ransomware will almost certainly leverage exfiltrated data to increase financial payouts from victims. Threat actors will likely threaten victims with exposure of sensitive data if they do not engage in ransom negotiations with threat actors. To date, FTI Cybersecurity has not yet identified a dedicated leak site for FOG ransomware victims on the clear or dark web. This could indicate the threat actors are privately selling the data on the underground, or simply have yet to set up a formal leak site. More information is required to determine the threat actors' method for exploiting exfiltrated data.

SOURCES

- Lost in the Fog: A New Ransomware Threat
- *Information in this report is partially derived from FTI Cybersecurity investigations. Some information may be redacted or generalized for client privacy.*

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)

FTI Cybersecurity Global Offices

AMERICAS

Atlanta	Los Angeles	Sao Paulo
Boston	Mexico City	Seattle
Chicago	Miami	Toronto
Houston	New York	Washington, DC
Irvine	San Francisco	Wayne

EMEA

Berlin	Dusseldorf	Mumbai
Brussels	Frankfurt	Munich
Cape Town	Johannesburg	Paris
Dubai	London	Zurich
Dublin	Madrid	

APAC

Brisbane	Perth	Sydney
Hong Kong	Shanghai	Tokyo
Melbourne	Singapore	

FTI CONSULTING