FOG RANSOMWARE: A NEW STORM IN THE THREAT LANDSCAPE

Fog ransomware began as a minor extortion threat but has rapidly turned into a global operation using legitimate tools and hybrid encryption to outpace defenses

40%

of Fog incidents began with credentials harvested from infostealer logs circulating on criminal marketplaces

When Fog ransomware first emerged in mid-2024, it appeared to be just another throwaway ransomware release. Its early code was basic, and its first victims were small manufacturers and logistics firms in Central Europe, the kind of targets that usually do not make headlines.

Less than a year later, things have changed. Fog has become one of the most adaptable and elusive ransomware families on the scene, spreading across continents and industries faster than most defenders can react.

FROM SMALL JOBS TO GLOBAL REACH

Fog's expansion has been rapid. The group behind it has moved well beyond its original manufacturing and logistics targets into healthcare, education, and critical infrastructure across North America and Asia.

Its developers have built a modular payload that can be tailored to different victims, combining traditional file encryption with data theft and lateral movement.

Fog relies heavily on living-off-the-land (LOTL) tactics, whereby it uses built-in system tools instead of custom malware to evade signature-based defenses. In recent attacks, the gang has relied on PowerShell scripts for persistence and legitimate remote-management applications, such as AnyDesk and ConnectWise, to maintain access long after the initial breach.

The European Union Agency for Cybersecurity (ENISA) notes that Fog is one of several newer ransomware operations that favor legitimate administrative utilities to "blend into normal network activity" and bypass behavioral analytics. Once inside, attackers often attempt to disable or uninstall endpoint protection tools before detonating the encryption payload.

A LINEAGE HIDING IN PLAIN SIGHT

Fog's lineage is still debated. Some analysts have identified overlaps in its code and infrastructure that point back to Eastern European crime forums that emerged after the fall of Conti and LockBit, suggesting that a few of Fog's developers may be veterans from those crews. Others suggest it is more of a copycat or spinoff, borrowing tactics from the old cartels but running as its own independent outfit.

Whatever its origins, Fog has quickly learned from the mistakes of its predecessors. By early 2025, newer Fog samples had stepped up their game, using a combination of Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption and introducing self-modifying scripts that

change every time they run, making static analysis challenging. Even the ransomware's configuration files are built on the fly, so each infection acts a little differently—an unwelcome twist for anyone trying to write reliable detection signatures.

The group's leak-site activity mirrors the professionalization of the broader ransomware economy. Victims are named, shamed, and their identities sometimes auctioned on data leak forums. Negotiation chat logs suggest that Fog maintains a customer-support-style interface for ransom payments, offering decryption "proofs" and file samples to establish credibility.

ENTRY POINTS AND EXPOSURE

Most Fog attacks begin in the old-fashioned way—through stolen VPN logins or holes in unpatched edge devices.

Analysis found that over 40% of Fog incidents began with credentials harvested from infostealer logs circulating on criminal marketplaces.[‡] In other cases, the gang broke in by exploiting outdated firewalls and remote access gear, taking advantage of the slow patching pace common in mid-sized organizations.

Once inside, the attackers move quickly. Researchers have documented Fog's ability to detect and terminate popular endpoint protection processes before launching encryption, and to exfiltrate key files to temporary cloud storage locations to support double-extortion demands. The malware's internal scheduler can trigger encryption during off-hours, minimizing the chance of interruption. These methods are by no means groundbreaking, but their combined use is highly effective.

CONTAINMENT OVER CLEANUP

As Fog's operators broaden their reach, the practical question is how defenders can contain an adaptable adversary that relies on legitimate tools as much as malicious code. Traditional signature-based or heuristic detection cannot reliably distinguish Fog's activity from that of legitimate administrators.

The answer lies in implementing Zero Trust principles across both endpoints and internal network traffic. When admin tools are needed, they should be tightly approved, carefully monitored, and kept separate from the rest of the environment.

ThreatLocker® Application Control enforces a strong allowlisting approach, allowing only known and verified applications to execute. Even trusted applications are strictly managed through Ringfencing™, tightly controlling their behavior to prevent unauthorized actions such as accessing sensitive data, launching unexpected processes, or communicating outside their intended scope.

On top of that, ThreatLocker Network Control precisely restricts which devices can communicate with specific systems, dramatically reducing lateral movement and minimizing the blast radius of any attempted compromise.

Good identity and access hygiene is also key. Most Fog attacks could have been blocked with a few simple steps: enforcing multi-factor authentication (MFA), regularly changing VPN credentials, and monitoring for leaked logins online. Staying on top of audit logs and spotting unusual behavior matters just as much: If a new remote-access tool, PowerShell script, or admin share pops up out of nowhere, it is a sign something has gone wrong.

Regular patch management—particularly for externally facing infrastructure—remains one of the simplest yet most overlooked defenses. The exploitation of known vulnerabilities in edge devices remains one of Fog's most consistent entry points.

LESSONS FOR THE NEXT WAVE

Fog's rapid rise shows just how much the ransomware playbook has evolved. Hackers do not need cutting-edge exploits or bespoke malware anymore—they succeed by moving fast, staying flexible, and twisting legitimate tools to do their bidding.

Defending against that means shifting focus from chasing indicators to tightening the rules on what users and processes can actually do once they are inside the network.

Zero Trust, when extended across every endpoint and communication path, offers a framework for doing just that. By verifying every process, restricting movement between systems, and containing the spread of any intrusion, organizations can shrink the impact of even a successful breach.

Stopping Fog and the next wave of copycats will depend less on perfect detection and more on the kind of disciplined control that ThreatLocker offers—verifying everything that runs, connects, or communicates inside the network.

THREATLOCKER TIP

Fog ransomware's hackers can evade typical breach indicators by staying fast and fluid. Prevent a breach by taking the Zero Trust approach with ThreatLocker Application Control and Network Control