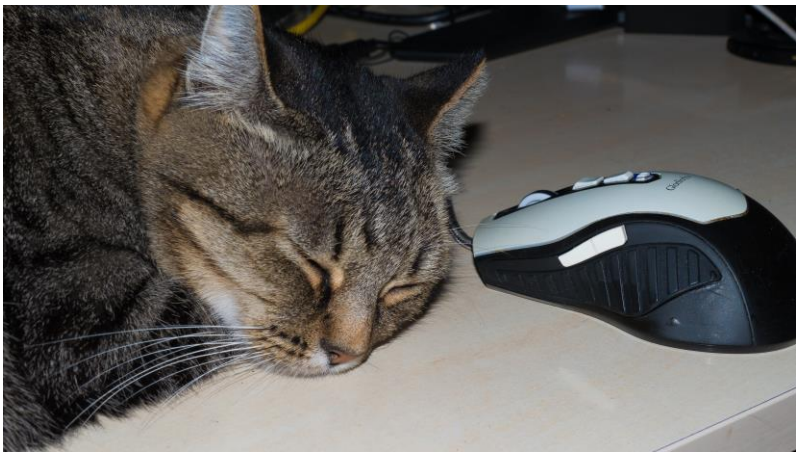
The Felismus RAT: Powerful Threat, Mysterious Purpose



This week, my colleagues and I furiously investigated the mystery of Felismus, a sophisticated, well-written piece of malware discovered recently by researchers at Forcepoint Labs. The malware's modular, self-updating construction is a nod to the apparent skill of its creators and the severe risk it poses to victims.

While little has been uncovered so far about Felismus's creators or their intentions, a different puzzle captivated my team. Inquiring minds had to understand the malware's name, which supposedly relates to the Tom & Jerry reference in its only human-readable encryption key: "Tom&Jerry@14here."

What episode did the term "Felismus" come from? *Why couldn't we find a connection?*

As it turns out, the answer had been staring us in the face all along. In Latin, *felis* means cat; *mus* means mouse. Tom & Jerry, cat and mouse. Of course.

One mystery solved, a dozen more to go. Although researchers believe Felismus plays a role in a targeted campaign due to its scarcity, its creators' targets and intent remain murky. Still, the significant power that Felismus grants to its operators makes it a potentially devastating threat to victims. Security and IT professionals should be aware of how it works and how it could affect their organizations.

Felismus is a Remote Access Tool (RAT), a type of malware that allows malicious actors to take complete control of an infected system. Like most RATs, it allows attackers to communicate with a remote server, download files, and execute shell commands.

Felismus appears to infiltrate systems by posing as an Adobe Content Management System file, as evidenced by the "AdobeCMS.exe" filename present in samples of the malware found in the wild. A malicious actor might fool unsuspecting users into downloading the file by presenting them with an update notice through a compromised

ad network or phishing email campaign: “To view this media content, click here to update to the latest version of Adobe.”

When the Felismus executable is run, it deposits two Dynamic Link Library (DLL) files in the file system. The DLLs provide functions for the executable to call, allowing the original executable file to take up less disk space. The malware creates an invisible window when it is run, camouflaging it as a Windows process by registering a WindowProc function to it. This enables the window to accept and process messages, which is how the malware communicates with its C2 server.

The original process sends encrypted commands through the invisible window to a domain, disguising the activity as normal browsing and shopping behavior. Because the activity is designed to look like normal, whitelisted behavior, antivirus products are unlikely to pick it up. Although the contents of these commands have not been deciphered, they appear to be related to the malware’s setup process. In response, the server sets up a UUID for the victim, which is a unique identifier that is used later as part of the encryption process. Once communication has been established, the attacker can execute a shell command, save the results of the shell command, upload those results to a remote server, download a file from a remote server, execute a file, and create and save a text file.

On their own, these functions already pose a significant threat. What makes Felismus particularly dangerous is its modular construction, which can help it hide or extend its capabilities. Once Felismus has compromised a system, an attacker can easily add a new functional module designed to accomplish whatever they want within the environment. This could be a keylogger, a network traffic analyzer, a tool to automate exploration of the system, or anything else the attacker might want. Felismus is also capable of self-updating, which means it can be updated to strengthen itself, fix bugs, or even change what it looks like to evade antivirus products.

Not much has been uncovered about Felismus’s creators or their motives, who appear to be quite skilled at hiding their tracks. Not only are the malware’s executables and DLL files written in a way that makes analysis difficult, but most communications with its C2 server are twice-encrypted—using different keys. Felismus appears to detect processes associated with popular antivirus programs, presumably to avoid them. The attackers’ care not to reuse identifiers like email addresses also means there’s no evidence linking it to known campaigns. While the malware’s C2 infrastructure is active, very little has been uncovered about how it’s currently being used.

Still, the malware’s construction offers a few hints about the attackers. First, a couple of spelling errors indicate that English might not be their first language. Another clue is that the antivirus processes that the malware detects include one vendor that primarily serves customers in China and another vendor primarily used in Korea. Of the five domains that have been associated with the malware, three are named in ways that may indicate a connection to the financial sector. However, the other two don’t fit that pattern.

Although researchers uncovered Felismus recently, it appears to have been operating under the radar for at least six months. Unfortunately, that's not atypical. Most compromised systems go undetected for months before they're uncovered, which is why the security industry has shifted its focus from prevention to detection.

How AlienVault Can Help

Felismus is carefully constructed to avoid discovery. Fortunately, AlienVault Unified Security Management (USM) provides the security capabilities your organization needs to detect the malware within your environments and respond quickly.

AlienVault USM provides network intrusion detection (NIDS), host intrusion detection (HIDS), and cloud intrusion detection capabilities to help you detect intrusions like Felismus across the breadth of your critical infrastructure.

Correlation rules within USM offer additional functionality, alerting you when a series of events suggests that malicious activity might be taking place. This pre-built library of rules addresses a wide range of events that can occur when a system has been compromised by a RAT like Felismus, along with a wide variety of other threats.

New threats like Felismus emerge constantly as malicious actors spin out new malware and iterate on existing threats. For organizations without the resources to devote an entire team to threat intelligence research, it's impossible to keep up with the rate of change within the security landscape, let alone incorporate that information into a security and response plan.

The AlienVault Labs Security Research Team investigates emerging threats so you don't have to, providing continuous threat intelligence updates to your USM deployment in the form of new correlation directives, intrusion signatures, vulnerability signatures, response templates, and more. Because these actionable updates are built directly into the USM platform, your security plan is always up-to-date and ready to detect the latest threats as they emerge. To see an example of the threat intelligence the Security Research Team provides, including updates related to Felismus, see their recent Threat Intelligence Update summary posted in the AlienVault Forums.

The Security Research Team informs their research with threat data from the AlienVault Open Threat Exchange (OTX), the world's first open threat intelligence community. More than 53,000 participants from 140 countries around the world contribute 10 million indicators of compromise to OTX every day. By incorporating diverse threat data from OTX into their own research, the Security Research Team strengthens your security plan from every angle.