Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

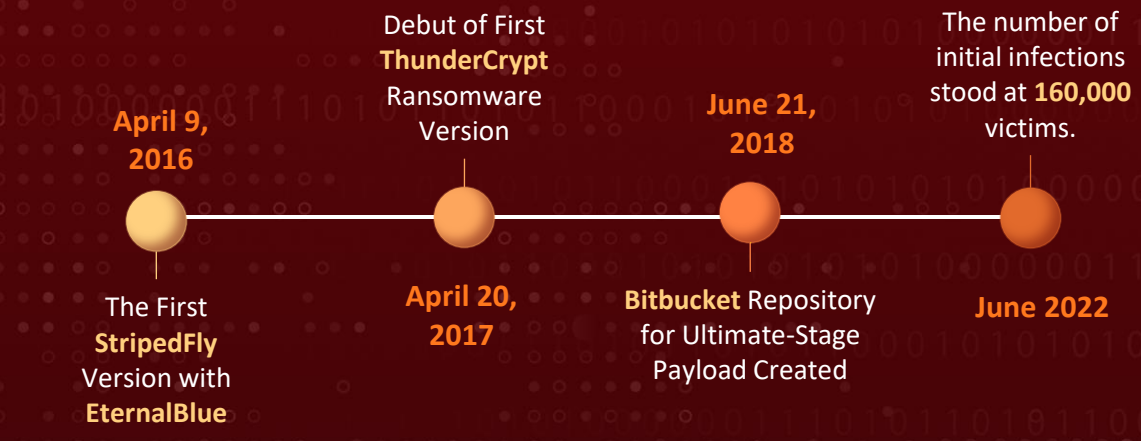
Redefining the StripedFly Malware Framework

Date of Publication	Admiralty Code	TA Number
October 27, 2023	A1	TA2023438

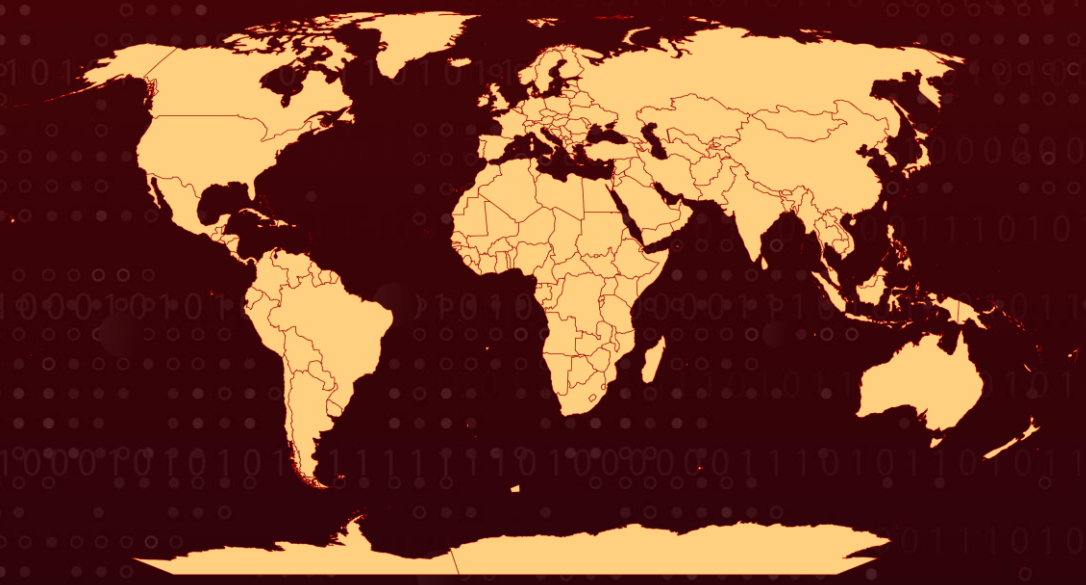
Summary

Active Since: April 2017
Malware: StripedFly, ThunderCrypt
Attack Region: Worldwide
Affected Platforms: Windows and Linux
Attack: An intricate cross-platform malware framework, known as StripedFly, operated discreetly for five years, surreptitiously compromising over a million Windows and Linux systems. It skillfully evaded in-depth analysis and was initially misclassified as a cryptocurrency miner.

Attack Timeline



Attack Regions



Attack Details

#1 Initially, StripedFly was classified and widely dismissed as largely ineffective malware designed for mining Monero cryptocurrency when it was first detected in 2017. StripedFly has revealed itself as a complex modular malware, enabling attackers to establish network persistence, gain a comprehensive insight into network activities, and exfiltrate credentials from approximately one million Windows and Linux systems.

#2 StripedFly boasts advanced features such as TOR-based traffic obscuring methods for communication with command servers, automated update and delivery capabilities through trusted platforms like GitLab, GitHub, and Bitbucket, all while utilizing customized encrypted archives. It also possesses worm-like spreading abilities and a proprietary EternalBlue SMBv1 exploit developed prior to the public disclosure of the vulnerability.

#3 The malware payload is structured as a monolithic binary executable code, allowing for pluggable modules to enhance or update its functionality, a characteristic often found in APT (Advanced Persistent Threat) malware. Initial detection of the StripedFly malware framework involved the injection of its platform's shellcode into the WININIT.EXE process, a legitimate Windows OS component responsible for initializing various subsystems.

#4 The breach likely occurred through the use of a custom EternalBlue SMBv1 exploit targeting internet-exposed computers. The final StripedFly payload, system.img, incorporates a specialized lightweight TOR network client to secure its network communications, the ability to disable the SMBv1 protocol, and the capacity to spread to other Windows and Linux devices on the network using SSH and EternalBlue.

#5 The Bitbucket repository serves as the pipe for delivering the ultimate-stage payload to Windows systems. The malware's command and control (C2) server operates within the TOR network and maintains communication through frequent beacon messages containing the victim's unique identifier. An earlier version of the StripedFly malware framework led to the discovery of a related ransomware variant known as ThunderCrypt.

#6 Notably, both malware strains share the same foundational codebase and communicate with the same C2 server. At the same time, the exact purpose of this malware framework remains uncertain, whether, for profit or cyber espionage, its sophistication marks it as APT malware.

Recommendations

Network Monitoring: Implement robust network monitoring solutions to detect unusual or suspicious traffic patterns. StripedFly used TOR-based traffic concealment mechanisms, making it critical to monitor for anomalies in network communication.

Application Whitelisting: Consider implementing application whitelisting to allow only authorized software to run, which can help prevent the execution of unknown or unauthorized programs.

Regular Security Updates: Ensure that all systems are kept up-to-date with security patches and updates. The StripedFly malware exploited vulnerabilities like the EternalBlue SMBv1 exploit before they were publicly disclosed, underscoring the importance of promptly applying patches.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0011 Command and Control	TA0010 Exfiltration	T1053 Scheduled Task/Job	T1547.001 Registry Run Keys / Startup Folder
T1573 Encrypted Channel	T1059 Command and Scripting Interpreter	T1543 Create or Modify System Process	T1210 Exploitation of Remote Services
T1027 Obfuscated Files or Information	T1211 Exploitation for Defense Evasion	T1212 Exploitation for Credential Access	T1564 Hide Artifacts
T1041 Exfiltration Over C2 Channel	T1204 User Execution		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	gpiekd65jgshwp2p53igifv43aug2adacdebmuuri34hduvijr5pfjad[.]onion, ghtyqipha6mcwxiz[.]onion, ajiumbl2p2mjzx3l[.]onion
URLs	bitbucket[.]org/JulieHeilman/m100-firmware-mirror/downloads/, bitbucket[.]org/upgrades/um/downloads/, bitbucket[.]org/legit-updates/flash-player/downloads, gitlab[.]com/JulieHeilman/m100-firmware-mirror/raw/master/, gitlab[.]com/saev3aeg/ugee8zee/raw/master/, github[.]com/amf9esiabnb/documents/releases/download/, tcp://pool.minexmr[.]com:4444, tcp://mine.aeon-pool[.]com:5555, tcp://5.255.86[.]125:8080, tcp://45.9.148[.]21:80, tcp://45.9.148[.]36:80, tcp://45.9.148[.]132:8080
MD5	b28c6d00855be3b60e220c32bfad2535, 18f5ccdd9efb9c41aa63efbe0c65d3db, 2cdc600185901cf045af027289c4429c, 54dd5c70f67df5dc8d750f19ececd797, d32fa257cd6fb1b0c6df80f673865581, c04868dabd6b9ce132a790fdc02acc14, c7e3df6455738fb080d741dcbb620b89, d684de2c5cfb38917c5d99c04c21769a, a5d3abe7feb56f49fa33dc49fea11f85, 35fadceca0bae2cdcfdaac0f188ba7e0, 00c9fd9371791e9160a3adaade0b4aa2, 41b326df0d21d0a8fad6ed01fec1389f, 506599fe3aecdfb1acc846ea52adc09f, 6ace7d5115a1c63b674b736ae760423b, 2e2ef6e074bd683b477a2a2e581386f0, 04df1280798594965d6fdfeb4c257f6c, abe845285510079229d83bb117ab8ed6, 090059c1786075591dec7ddc6f9ee3eb, 120f62e78b97cd748170b2779d8c0c67, d64361802515cf32bd34f98312dfd40d

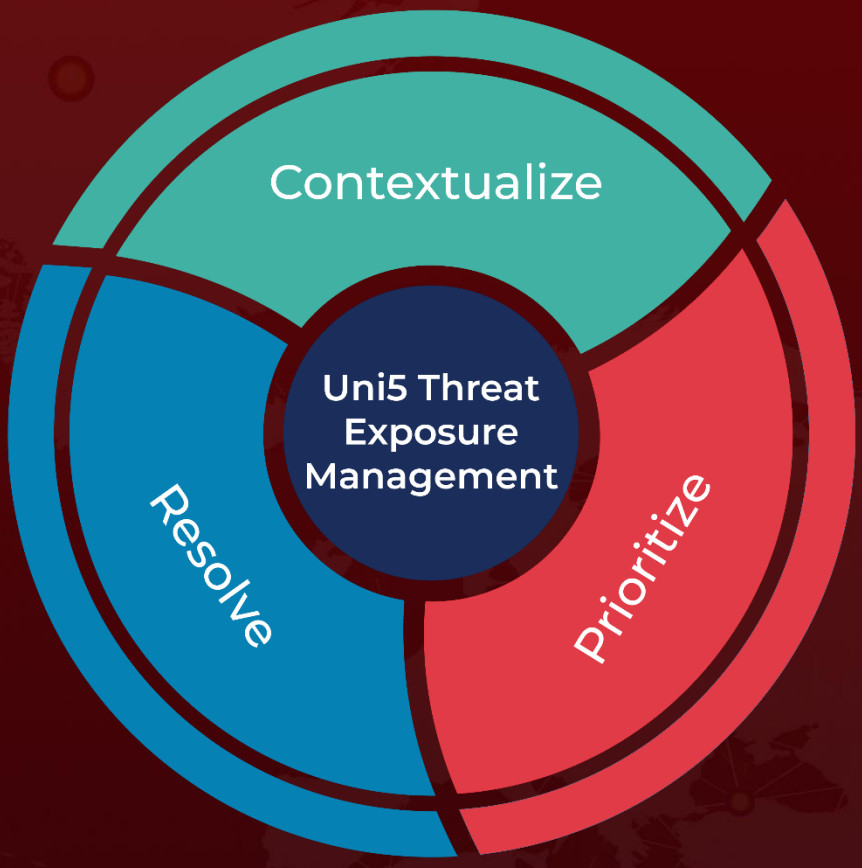
References

https://securelist.com/stripedfly-perennially-flying-under-the-radar/110903/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 27, 2023 . 5:30 AM

More at www.hivepro.com