Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

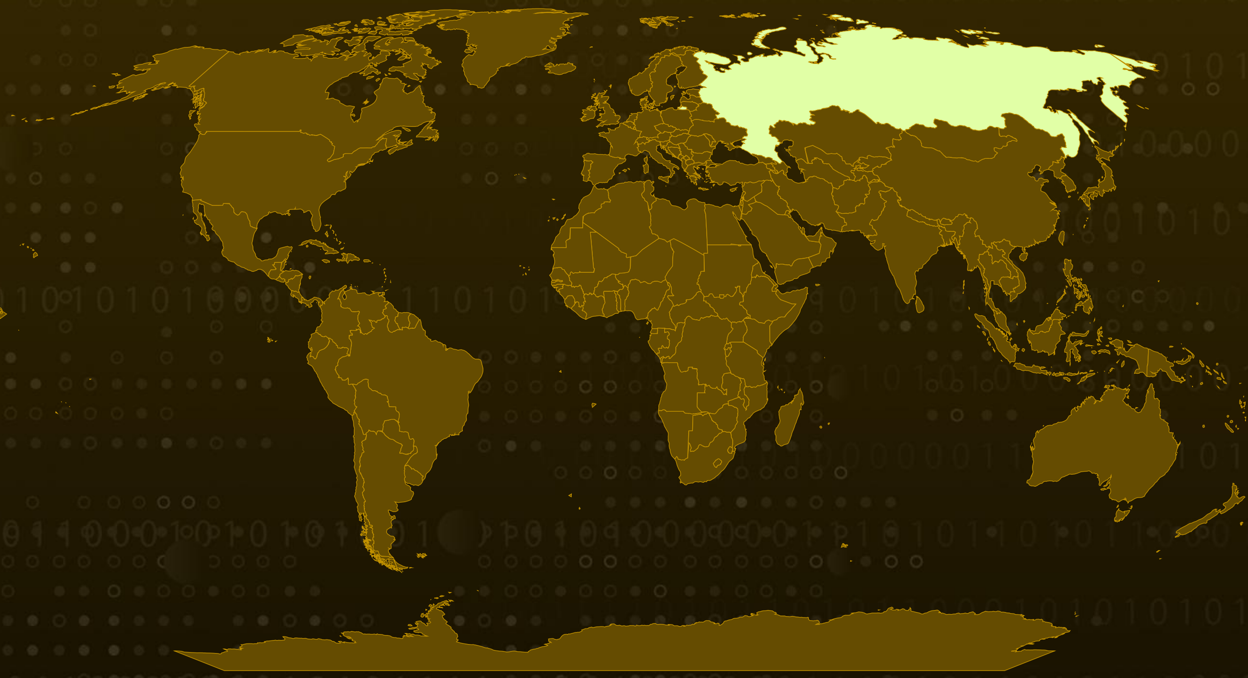
CMoon Worm Emerges: Targets Russia in Data Theft Attacks

Date of Publication	Admiralty Code	TA Number
August 8, 2024	A1	TA2024303

Summary

Attack Discovered: July 2024
Attack Region: Russia
Targeted Industry: Gas supply company
Malware: CMoon
Attack: A new self-spreading worm named 'CMoon' has been actively distributed in Russia since early July 2024. The worm is capable of stealing account credentials and other sensitive data, posing significant risks to infected systems. The distribution vector for CMoon has been identified as a compromised website belonging to a gas supply company.

Attack Regions



Attack Details

#1 In July 2024, cybersecurity researchers identified a highly sophisticated and self-replicating worm called 'CMoon' that has been actively spreading across Russia. This worm is particularly dangerous because it not only steals account credentials and extracts sensitive information, but also facilitates further cyberattacks by gaining remote control over infected systems.

#2 CMoon's initial infection was traced back to a compromised website belonging to a Russian gas supply company. Attackers replaced legitimate document links on the site with malicious executables, tricking users into downloading the worm. The malware was cleverly embedded within a self-extracting archive that contained both the genuine document and the CMoon payload.

#3 Developed using the .NET framework, CMoon is designed to evade detection by modifying file and folder and embedding itself in antivirus directories when possible. It monitors USB drives, replacing files with shortcuts that point back to the worm, allowing it to spread to other systems. The worm also exfiltrates data by searching for files containing sensitive keywords like "secret" or "password" and transmits them to a remote server. This server can send commands back to CMoon, enabling it to download additional malware, capture screenshots, launch DDoS attacks, and gather information about local network resources.

#4 The worm targets a wide range of applications, including web browsers, email clients, cryptocurrency wallets, and messaging platforms. It terminates any processes that interfere with its operations, ensuring that it can continue to exfiltrate data or carry out other malicious activities. CMoon communicates with its remote server using a distinct header (`CMOON $`) in its outgoing packets, which helps to maintain control and facilitate its various functions.

#5 Despite efforts to mitigate the threat by removing the malicious files from the gas company's website, CMoon's self-replicating capabilities mean it could continue to spread independently, even in the absence of the original infection sources. This ongoing risk highlights the worm's potential for causing widespread damage.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1189 Drive-by Compromise
T1059 Command and Scripting Interpreter	T1036 Masquerading	T1592 Gather Victim Host Information	T1592.002 Software
T1547 Boot or Logon Autostart Execution	T1547.009 Shortcut Modification	T1041 Exfiltration Over C2 Channel	T1573 Encrypted Channel

T1113 Screen Capture	**T1498** Network Denial of Service	**T1016** System Network Configuration Discovery	**T1555** Credentials from Password Stores
T1555.005 Password Managers	**T1217** Browser Information Discovery	**T1539** Steal Web Session Cookie	**T1071** Application Layer Protocol
T1071.001 Web Protocols			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4:Port	93[.]185[.]167[.]95:9899
MD5	132404f2b1c1f5a4d76bd38d1402bdfa
SHA256	a4be526be5359ad2981f439457fe652895731ad56c10c113c22a7836a9591e5d

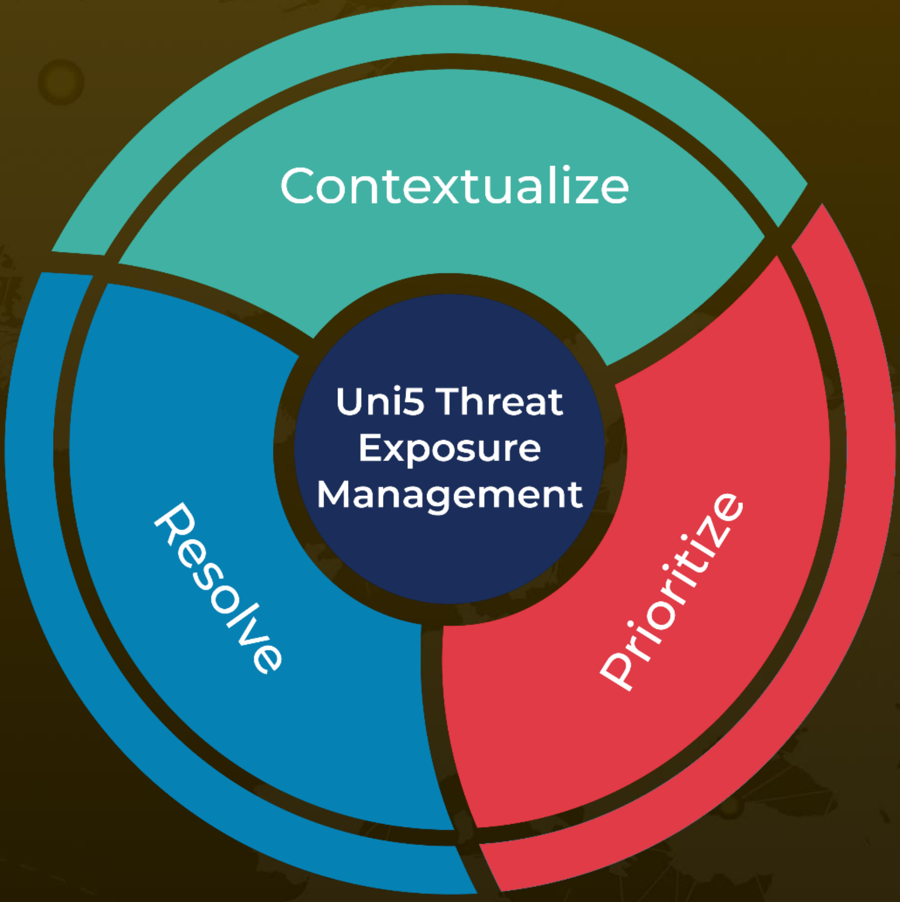
References

https://securelist.ru/how-the-cmoon-worm-collects-data/109988/

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

August 8, 2024 • 7:00 AM

More at www.hivepro.com