Somnia Malware Detection: UAC-0118 aka FRwL Launches Cyber Attacks Against Organizations in Ukraine Using Enhanced Malware Strains

socprime.com/blog/somnia-malware-detection-uac-0118-aka-frwl-launches-cyber-attacks-against-organizations-in-ukraine-using-enhanced-malware-strains/

Veronika Telychko

Veronika Telychko

Somnia Malware Detection

Since the outbreak of the global cyber war, cyber attacks against Ukraine and its allies leveraging info-stealers and malicious payloads have been causing a stir in the cyber threat arena. In the latest cyber attack on the Ukrainian organization, threat actors have applied a diverse offensive toolkit, including the Vidar info-stealer and the notorious Cobalt Strike Beacon, which have been frequently used in a set of malicious campaigns against Ukraine since February 2022.

On November 11, 2022, CERT-UA researchers provided insights into the cybersecurity incident of damaging the information integrity and availability due to the ongoing cyber attack against organizations in Ukraine leveraging the advanced version of Somnia malware and a set of other malicious strains. The adversary activity responsible for unauthorized intrusion into targeted automated systems and computers has been attributed to the hacking collective FRwL aka Z-Team also tracked as UAC-0118.

Detecting the UAC-0118 Malicious Activity Covered by CERT-UA#5185 Alert

In view of the escalating volume and sophistication of cyber attacks against Ukraine and its allies, cybersecurity practitioners should timely detect emerging threats to proactively defend their organizations from potential intrusions. SOC Prime Platform aggregates a batch of high-fidelity alerts and relevant hunting queries to identify the malicious activity associated with the UAC-0118 actor and covered by the CERT-UA#5185 alert. All detections are tagged with "UAC-0118" ("UA#5185") to simplify the content selection for SOC team members:

Sigma rules to detect the malicious activity covered in the CERT-UA#5185 alert

Press the **Explore Detections** button to reach the dedicated Sigma rules filtered by the corresponding UAC-0118 tag based on the group identifier. Detection algorithms are aligned with MITRE ATT&CK® and are accompanied by detailed cyber threat context, including relevant CTI links, mitigations, executable binaries, and more relevant metadata. Sigma rules are packed with translations to 25+ SIEM, EDR, and XDR solutions to match any environment cybersecurity practitioners need.

Explore Detections

To streamline threat hunting efforts and boost the efficiency of SOC operations, security experts can search for IOCs associated with the latest UAC-0118 attack using Uncoder CTI. Just paste the text containing relevant IOCs from CERT-UA#5185 alert and get custom IOC queries ready to run in a chosen environment.

IOCs Provided by Activity Covered by CERT-UA#5185 Alert

UAC-0118 Activity Spreading Somnia Malware: Attack Analysis

The latest CERT-UA#5185 alert provides research into the ongoing targeted cyber attack against Ukraine by the FRwL group also known as Z-Team or UAC-0118 spreading Somnia malware on the compromised systems. The investigation has revealed that the infection chain has been triggered by downloading and launching the malicious file disguised as Advanced IP Scanner software. The file masquerading as legitimate software has actually contained the Vidar information stealer.

Cybersecurity researchers assume that the attacker tactic, which involves creating copies of official web resources disguised as widespread software, belongs to the offensive toolkit of initial access brokers. In the case of the latest incident, initial access brokers were in charge of a data breach, and then they shared the compromised data with the FRwL hacking group, so they can proceed with a cyber attack.

Notably, the Vidar malware is also capable of stealing Telegram session data. If a potential victim has no two-factor authentication and a passcode turned on, it enables attackers to gain unauthorized access to the compromised user account. In the ongoing cyber attack, the victim’s Telegram account has been used for submitting configuration files of the VPN connection, including certificates and authentication data. Due to the disabled two-factor authentication during the VPN connection, adversaries were capable of accessing the corporate network. After gaining unauthorized access via VPN, threat actors applied Netscan for reconnaissance, launched Cobalt Strike Beacon, and performed data exfiltration via Rclone. In addition to the above-mentioned malware strains, the FRwL group was observed deploying Anydesk та Ngrok on the compromised systems.

The malware strain applied in the ongoing cyber attack dubbed Somnia has significantly evolved. The initial malware version used the 3DES algorithm, while the current version applies the AES encryption algorithm and doesn’t include data decryption capabilities for enhanced defense evasion.

MITRE ATT&CK® Context

To dive into the context behind the latest cyber attacks by the UAC-0118 threat actor, all dedicated Sigma rules are aligned with MITRE ATT&CK® framework addressing the corresponding tactics and techniques:

Tactics	Techniques	Sigma Rule
Command and Control	Remote Access Software (T1219)	Remote Access Software Doman Communication Attempt (via dns)
Protocol Tunneling (T1572)	Possible Ngrok Configuration File Creation (via file_event)	
Possible Command and Control by Use of ngrok RDP Tunnel (via network_connection)		
Exfiltration	Exfiltration Over Web Service (T1567)	Possible Data Exfiltration over Non-Corp Service (via dns)
Possible Data Exfiltration via Third Party Services/Tools (via proxy)		
Transfer Data to Cloud Account (T1537)	Possible Data Exfiltration via Third Party Services/Tools (via proxy)	
Persistence	Boot or Logon Autostart Execution (T1547)	Possible Persistence Points [ASEPs - Software/NTUSER Hive] (via registry_event)
Lateral Movement	Remote Services (T1021)	Possible Hidden AnyDesk Install (via cmdline)

Also, you can download the ATT&CK Navigator file below in the JSON format that provides the relevant MITRE ATT&CK context based on both Sigma rules from the SOC Prime Platform and IOCs provided by the CERT-UA#5185 alert:

Download JSON file for ATT&CK Navigator