

PicassoLoader and Cobalt Strike Beacon Detection: UAC-0057 aka GhostWriter Hacking Group Attacks the Ukrainian Leading Military Educational Institution

socprime.com/blog/picassoloader-and-cobalt-strike-beacon-detection-uac-0057-aka-ghostwriter-hacking-group-attacks-the-ukrainian-leading-military-educational-institution/




WRITTEN BY

Veronika Telychko

Technical Writer

[post-views]

June 16, 2023 · 3 min read

 PicassoLoader and Cobalt Strike Beacon Detection: UAC-0057 aka GhostWriter Hacking Group Attacks the Ukrainian Leading Military Educational Institution

On June 16, 2023, CERT-UA researchers issued a new alert covering the recently discovered malicious activity targeting the National Defense University of Ukraine, named after Ivan Cherniakhovskyj, the country's leading military educational institution. In this ongoing campaign, threat actors spread PicassoLoader and [Cobalt Strike Beacon](#) on the compromised systems via a malicious file containing a macro and a lure image with the university emblem. The malicious activity is attributed to the hacking collective tracked as UAC-0057 aka GhostWriter.

UAC-0057 aka GhostWriter Attack Analysis

The onset of the summer of 2023 has intensified the activity within the cyber threat landscape. Early June, CERT-UA warned the worldwide community of cyber defenders about the ongoing cyber-espionage operations against Ukrainian and Central Asian organizations linked to the UAC-0063 group. In mid-June, another wave of cyber attacks caused a stir in the cyber threat arena covered in the corresponding [CERT-UA#6852 alert](#).

Cybersecurity researchers have recently uncovered a PPT file containing a malicious macro and an emblem image of the National Defense University of Ukraine named after Ivan Cherniakhovskiy luring the targeted representatives of the corresponding educational institution into opening the document. The infection chain starts by opening the document and activating the malicious macro that leads to generating a DLL file along with a shortcut file to launch the former. The malicious DLL file is identified as PicassoLoader malware, which is commonly used by the UAC-0057 hacking group, also known as GhostWriter. PicassoLoader downloads and launches a .NET malware dropper, which in turn, decrypts and launches another DLL file. The latter is used to decrypt and launch the infamous [Cobalt Strike Beacon](#) malware on compromised systems. Threat actors maintain the persistence of the above-referenced DLL file via a scheduled task or by creating an LNK file in the autostart folder.

According to the CERT-UA research, the malware remote access servers are located in Russia, however, the domain names are hidden via Cloudflare capabilities.

Detecting the Malicious Activity of UAC-0057 Group Covered in the CERT-UA#6852 Alert

In the face of the relentless surge in cyber attacks against Ukraine and its allies, cybersecurity defenders are making concerted efforts to raise awareness and swiftly mitigate the associated risks. In response to the novel CERT-UA#6852 alert covering the malicious activity of the UAC-0057 hacking group also tracked as GhostWriter, SOC Prime Platform has released curated Sigma rules available by the link below:

[Sigma rules to detect adversary activity by UAC-0057 covered in the CERT-UA#6852 alert](#)

Detection algorithms are aligned with the [MITRE ATT&CK® framework v12](#), enriched with intelligence and relevant metadata, and can be applicable across dozens of SIEM, EDR, and XDR technologies. To streamline the search for the above-mentioned Sigma rules, security engineers can apply the custom filter tags based on the group ID ("UAC-0057") or the corresponding CERT-UA alert ("CERT-UA#6852").

To reach the entire collection of Sigma rules for GhostWriter activity detection, click the **Explore Detection** button below. Check out ATT&CK links, CTI, and more cyber threat context to always stay in the know.

[Explore Detections](#)

Cybersecurity experts can also seamlessly hunt for indicators of compromise related to the UAC-0057 adversary activity and provided in the latest [CERT-UA research](#). Rely on [Uncoder AI](#) to instantly generate custom IOC queries ready to run in the selected SIEM or EDR environment and timely identify the PicassoLoader or Cobalt Strike Beacon infection in your infrastructure.

 Hunt for IOCs covered in the CERT-UA#6852 alert using Uncoder AI

MITRE ATT&CK Context

To explore the context behind the latest UAC-0057 malicious campaign reported in the CERT-UA#6852 alert, all dedicated Sigma rules are automatically tagged with ATT&CK addressing the corresponding tactics and techniques:

Tactics	Techniques	Sigma Rule
Initial Access	Phishing (T1566)	MSOffice Drops Files to Suspicious Location (via file_event)
		MSOffice Drops Suspicious Files (via file_event)
Execution	Command and Scripting Interpreter (T1059)	Environment Variables in Command Line Arguments (via cmdline)
Persistence	Boot or Logon Autostart Execution (T1547)	Suspicious Sctipts in Autostart Location (via file_event)
Defense Evasion	System Binary Proxy Execution (T1218)	Rare DLL Exports Invocation by Rundll32 (via cmdline)
		Execution of a Payload with a Spoofed Extension using Rundll32 or Regsvr32 (via cmdline)
		LOLBAS rundll32 (via cmdline)
		LOLBAS regsvr32 (via cmdline)

Table of Contents



Join SOC Prime's Detection as Code platform to improve visibility into threats most relevant to your business. To help you get started and drive immediate value, book a meeting now with SOC Prime experts.

[Join for Free Book a Meeting](#)