Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

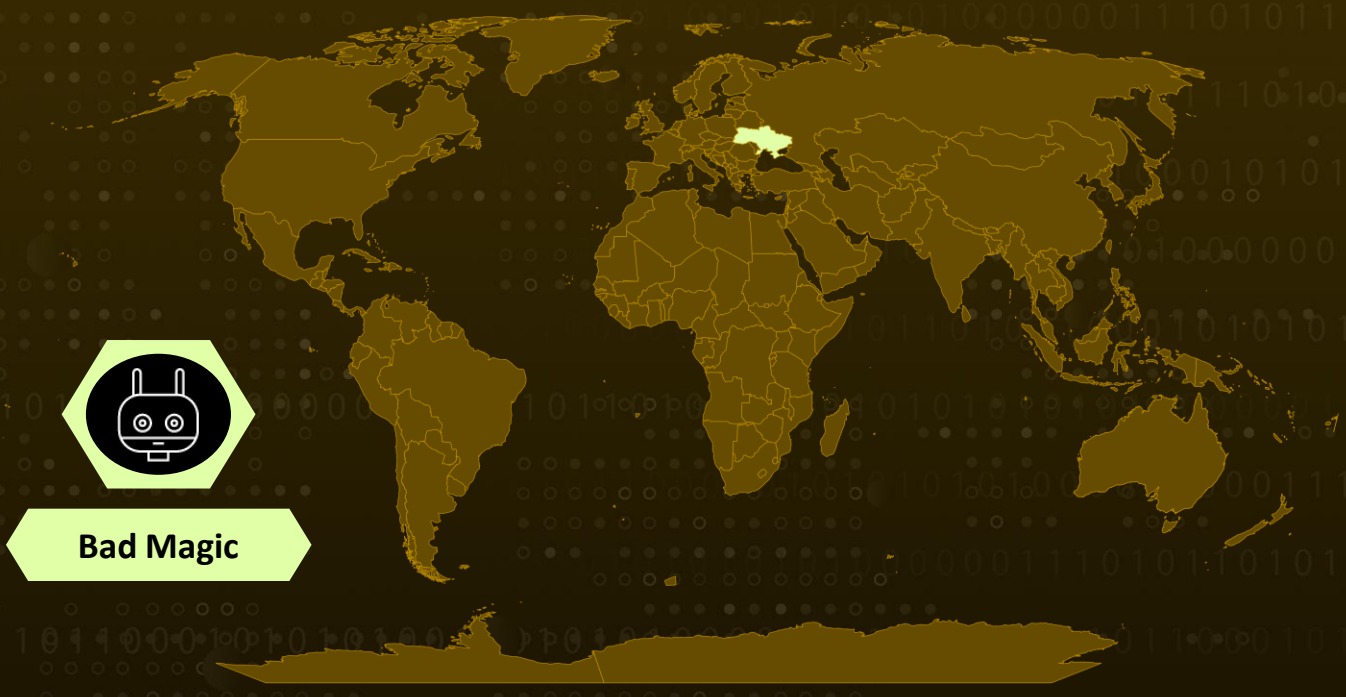
# Bad Magic APT employs new CommonMagic Framework and PowerMagic Backdoor


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| March 22, 2023 | A1 | TA2023151 |

# Summary

**First appeared:** September 2021
**Attack Region:** Donetsk, Lugansk, and Crimea (Cities in Ukraine)
**Actor Name:** Bad magic
**Targeted Industries:** Administrative, Agriculture, and Transportation
**Malware:** PowerMagic
**Attack:** New Bad magic APT was discovered using a new backdoor called PowerMagic and a malicious framework called CommonMagic to target organizations in the administrative, agriculture, and transportation sectors for espionage purposes.

## Attack Regions



# Attack Details

**#1**

A cyber-espionage campaign targeting government, agriculture, and transportation organizations in Donetsk, Lugansk, and Crimea regions that are associated with the Russo-Ukrainian conflict. Victims were navigated to a URL that contained two files, a decoy document and a malicious LNK file with a double extension that leads to infection when opened. When the LNK file is activated, it triggers a chain of events that lead to the infection of the computer with a previously unseen malicious framework that was named CommonMagic.

**#2**

This framework was deployed after the initial infection with the PowerShell backdoor called PowerMagic, which is a loader for the CommonMagic framework. The CommonMagic framework consists of several executable modules, all stored in the directory C:\ProgramData\CommonCommand. The framework uses OneDrive remote folders as a transport and communicates via named pipes. The backdoor created by the PowerShell script communicates with the C&C server every minute, downloads and executes commands, and uploads results in response.

# Recommendations

**Security Leaders**

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

**Security Engineers**

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0007<br>Discovery | TA0004<br>Privilege Escalation | TA0003<br>Persistence | TA0009<br>Collection |
| TA0005<br>Defense Evasion | TA0010<br>Exfiltration | T1070.004<br>File Deletion | T1027<br>Obfuscated Files or Information |
| T1566.001<br>Spearphishing Attachment | T1204<br>User Execution | T1560<br>Archive Collected Data | T1560.002<br>Archive via Library |
| T1112<br>Modify Registry | T1012<br>Query Registry | T1083<br>File and Directory Discovery | T1204.001<br>Malicious Link |
| T1036<br>Masquerading | T1036.007<br>Double File Extension | T1218<br>System Binary Proxy Execution | T1218.007<br>Msiexec |
| T1546<br>Event Triggered Execution | T1546.016<br>Installer Packages | T1027.009<br>Embedded Payloads | T1070<br>Indicator Removal |
| T1053<br>Scheduled Task/Job | T1053.005<br>Scheduled Task | T1059<br>Command and Scripting Interpreter | T1059.001<br>PowerShell |
| T1567<br>Exfiltration Over Web Service | T1567.002<br>Exfiltration to Cloud Storage | T1113<br>Screen Capture | T1140<br>Deobfuscate/Decode Files or Information: |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Domains | webservice-srv[.]online<br>webservice-srv1[.]online |
| SHA256 | 22bb73e97b01be2e11d741f3f4852380b3dae91d9ac511f33de8877a9e7c0534 |
| SHA1 | b63d4c3618b93e362c8fdbda3bf5ab8d65386b5c |

| TYPE | VALUE |
| --- | --- |
| MD5 | fee3db5db8817e82b1af4cedafd2f346<br>ecb7af5771f4fe36a3065dc4d5516d84<br>ebaf3c6818bfc619ca2876abd6979f6d<br>ce8d77af445e3a7c7e56a6ea53af8c0d<br>bec44b3194c78f6e858b1768c071c5db<br>9e19fe5c3cf3e81f347dd78cf3c2e0c2<br>8c2f5e7432f1e6ad22002991772d589b<br>7c0e5627fd25c40374bc22035d3fadd8<br>765f45198cb8039079a28289eab761c5<br>1fe3a2502e330432f3cf37ca7acbffac<br>1de44e8da621cdeb62825d367693c75e<br>1032986517836a8b1f87db954722a33f<br>0a95a985e6be0918fdb4bfabf0847b5a |

## References

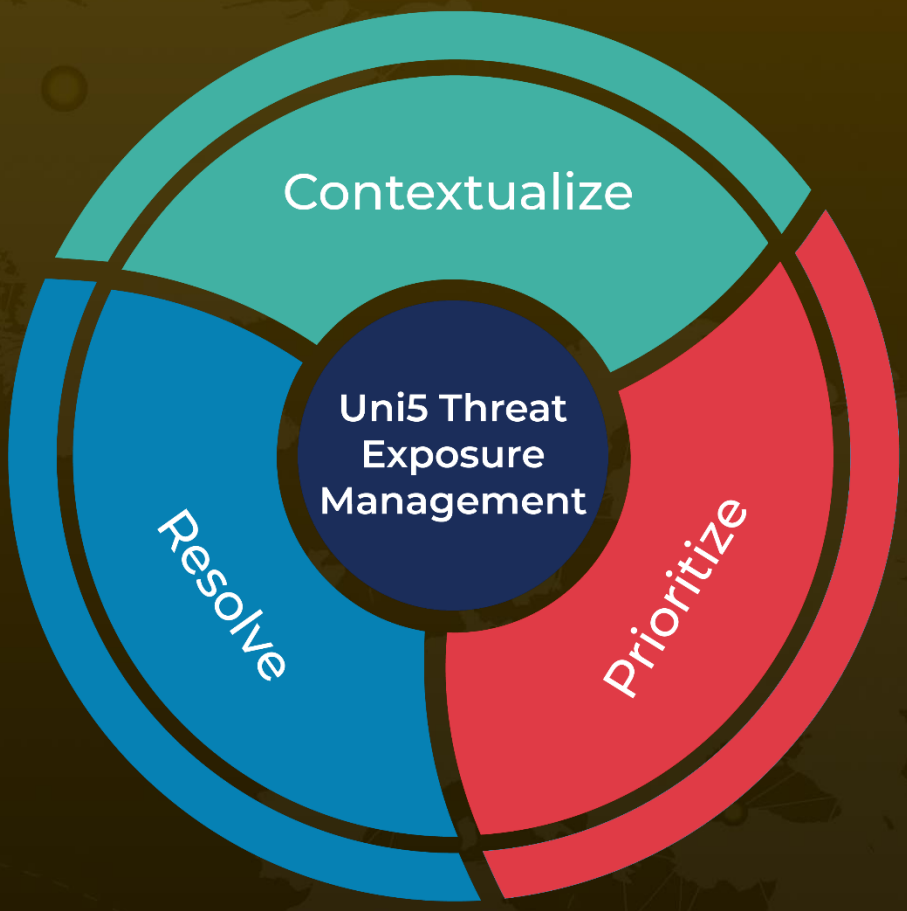

https://securelist.com/bad-magic-apt/109087/

https://securityaffairs.com/143816/apt/apt-uses-commonmagic-framework.html

# What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.




REPORT GENERATED ON

**March 22, 2023 • 1:30 AM**



More at www.hivepro.com