Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Fake Strike Reports, Real Malware: The LOTUSLITE Delivery Chain

Date of Publication	Admiralty Code	TA Number
March 11, 2026	A1	TA2026065

Summary

First Seen: March 04, 2026
Targeted Region: Middle East
Targeted Platform: Windows
Targeted Industries: Government, Defense
Threat Actor: Mustang Panda (aka Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154)
Malware: LOTUSLITE
Attack: Mustang Panda leverages Iran conflict-themed lures delivered through malicious ZIP archives to deploy the LOTUSLITE backdoor via multi-stage DLL sideloading. The campaign exploits geopolitical tensions in the Middle East, using file names referencing Iranian missile strikes against U.S. military facilities to entice victims into executing the payload.

Attack Regions

Attack Details

#1

In March 2026, a cyber campaign used a Middle East conflict–themed lure to spread the LOTUSLITE backdoor. The attack began with a malicious ZIP archive designed to appear related to missile strikes in Bahrain. Its contents were crafted to look credible and timely, exploiting public attention around regional tensions.

#2

Inside the archive was a legitimate KuGou music software executable that had been renamed to "Iran Strikes U.S. Military Facilities Across Gulf Region.exe." Alongside it sat a malicious DLL file, libmemobook.dll. The extracted folder was named "JCPOA," referencing the Joint Comprehensive Plan of Action, further reinforcing the geopolitical theme. This setup relied on social engineering: the file names and folder structure were intended to attract users following developments in the Middle East.

#3

When the executable was launched, it loaded the malicious DLL through DLL sideloading. The DLL, written in 32-bit C++, acted as the first stage of the infection chain. It first checked whether the LOTUSLITE backdoor was already installed by searching for two specific files and verifying their sizes. Persistence was then established through a Windows Run registry key configured to start SafeChrome.exe whenever the system booted.

#4

After persistence was set, the malware checked for additional payload components. If they were missing, it decrypted embedded shellcode and allocated executable memory using VirtualAlloc. The shellcode was copied into this memory and executed indirectly through a callback mechanism using EnumFontsW. This shellcode then contacted a compromised domain and downloaded the next stage of the attack. To blend in with normal traffic, the malware used a Chrome-like User-Agent string in its HTTP requests.

#5

The downloaded files were stored in the system and another Run registry entry was created to launch WebFeatures.exe with a specific argument, ensuring continued execution. In the final stage, WebFeatures.exe, a legitimate KuGou data-import utility, sideloaded a malicious kugou.dll placed beside it. This DLL contained the LOTUSLITE backdoor.

#6 A significant code overlap between this kugou.dll and earlier versions of the LOTUSLITE backdoor was documented in January 2026, including the same command-and-control infrastructure. The campaign highlights how threat actors quickly adapt their lures to current geopolitical events. Earlier operations used narratives tied to tensions between the United States and Venezuela; this wave shifted to Middle East conflict themes to increase the chance that victims would open the files.

Recommendations

Hunt for LOTUSLITE Persistence Artifacts: Search endpoints for the presence of directories C:\ProgramData\CClipboardCm\ and C:\ProgramData\WebFeatures\, as well as Run key entries named ACboardCm and ASEdge under HKCU\Software\Microsoft\Windows\CurrentVersion\Run. Detection of any of these artifacts may indicate an active or prior compromise.

Monitor for DLL Sideloading Activity: Deploy detection rules targeting unsigned or anomalous DLLs loaded by legitimate executables, particularly instances where KuGou software binaries (e.g., SafeChrome.exe, WebFeatures.exe) are loading DLLs from non-standard locations such as ProgramData subdirectories.

Detect Suspicious Use of EnumFontsW for Code Execution: Implement behavioral detection for processes that invoke the EnumFontsW API in conjunction with VirtualAlloc memory allocation, as this callback abuse technique is used by LOTUSLITE to execute decrypted shellcode.

Restrict Execution from ProgramData Directories: Apply application control policies to prevent executables and DLLs from running within C:\ProgramData\ subdirectories that are not associated with approved applications, thereby limiting the attacker's ability to stage and execute payloads.

Enforce Strict Email and File Transfer Controls: Configure email gateways and file-sharing platforms to quarantine or block ZIP archives containing LNK files, renamed executables, or DLLs, especially when file names reference current geopolitical events.

Implement Network Segmentation and Zero Trust Access: Restrict lateral movement opportunities by segmenting networks and enforcing least-privilege access controls. Ensure that compromised endpoints cannot freely communicate with internal resources or reach internet-facing C2 infrastructure.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
Defense Evasion	T1574: Hijack Execution Flow	T1574.001: DLL
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1057: Process Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1105: Ingress Tool Transfer	
Resource Development	T1584: Compromise Infrastructure	T1584.004: Server
	T1588: Obtain Capabilities	T1588.002: Tool

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	972585e50798cb5f122f766d8f26637f, 6accd57e48c34cadc998d00594229e42, 8c5a4dafed1586cec48d8eda267d8e42, 722bcd4b14aac3395f8a073050b9a578, 10fb1122079b5ae8e4147253a937f40f, 098bc0dd6a02a777fabb1b7d6f2da505
SHA1	1b3fa84de23c6e789958462e6185e9cf0680ed9c, be34901237c9fa9563e8dc9e71faf3a7e68f983f, b9dfc411699e07343b9b95daa79fe7e4b6811579, e5baecb74c456df26aa7e0fa1661838cd86ccfd7, 7d4e31c8b11be7c970860c4fbc8fe85c70724cb1
SHA256	db40546435a7c42b32493301e333c8c0010e652fecd02463614a386f916055ec, 4fb9b5d115bceee45a89447fb2565faef07452cda6b8e244e53ad91499c3d9b5, 24b11b4b999b385bede48ad9f0570e2e5da4a2054b96738b1e4d4946ece94bc1, 819f586ca65395bdd191a21e9b4f3281159f9826e4de0e908277518dba809e5b, 85647634070641177262l1ff8f89555e5a3b2b70bc9667032abd69cbe53b5216
Domains	www[.]e-kflower[.]com/_prozn/_skin_mbl/home/Kapp[.]rar, www[.]e-kflower[.]com/_prozn/_skin_mbl/home/Kappl[.]rar, media[.]hyperfilevault2[.]mom, arch2[.]maxdatahost1[.]cyou, arch[.]megadatahost1[.]lol, media[.]megafilehost2[.]sbs, media[.]megadatahost1[.]lol, arch2[.]megadatahost1[.]lol, media[.]maxdatahost1[.]cyou, flourishingscreencousin[.]com, holidayslettucecircumvent[.]com
IPv4	172[.]81[.]60[.]97, 80[.]97[.]160[.]190
Filename	Iran Strikes U.S. Military Facilities Across Gulf Region.exe, libmemobook.dll, kugou.dll, WebFeatures.exe, SafeChrome.exe

TYPE	VALUE
File Path	C:\ProgramData\CClipboardCm\, C:\ProgramData\WebFeatures\
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ACboardCm, HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ASEdge

References

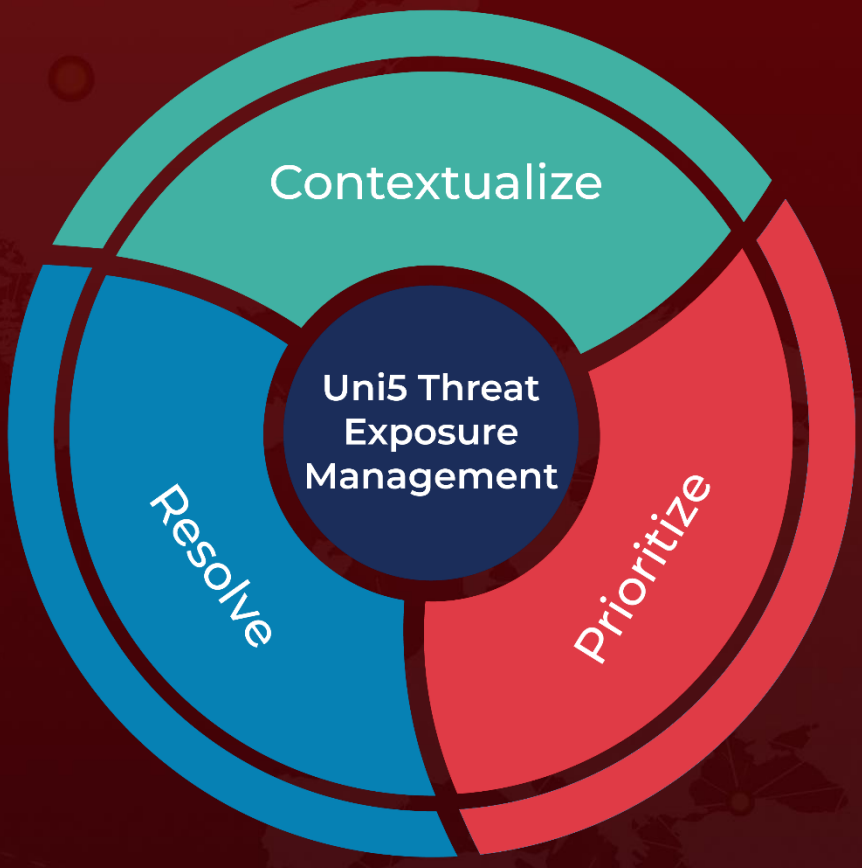
https://www.zscaler.com/blogs/security-research/middle-east-conflict-fuels-opportunistic-cyber-attacks

https://hivepro.com/threat-advisory/geopolitics-as-bait-lotuslite-backdoor-targets-us-entities/

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

March 11, 2026 • 05:00 AM

More at www.hivepro.com