Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

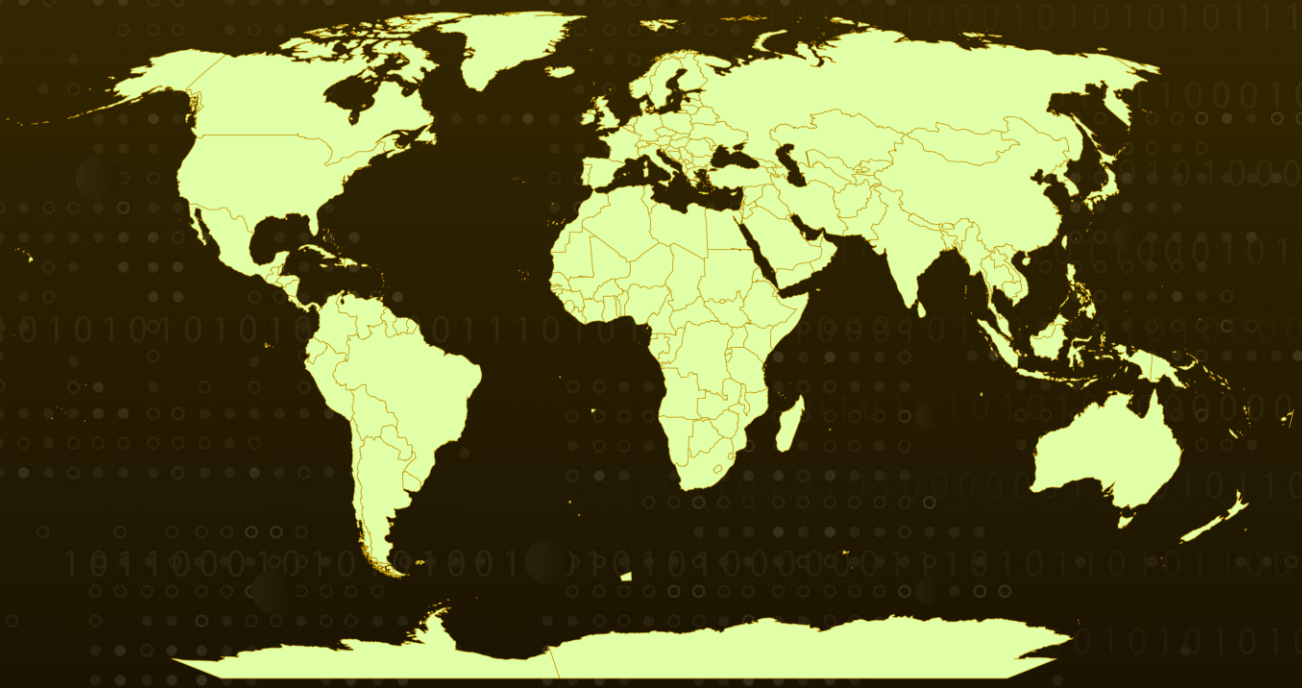
LOLKEK Ransomware Evolving New Tactics to Evade Detection

Date of Publication	Admiralty Code	TA Number
August 10, 2023	A1	TA2023328

Summary

First appeared: May 2023
Attack Region: Worldwide
Affected Platform: Windows
Malware: LOLKEK ransomware (also known as GlobeImposter)
Attack: LOLKEK ransomware is still being actively developed and uses new tactics to evade detection, including code obfuscation, legitimate tools usage and targeting network shares. It encrypts all drives, including network shares, and demands 0.1 Bitcoin in ransom.

Attack Regions



Attack Details

#1

LOLKEK is a ransomware family that has been around since 2016. It is still being actively developed, and new samples have been observed in the wild in May 2023. These samples use a number of new tactics to evade detection, including obfuscation of the code, use of legitimate tools and services, and encryption of network shares in addition to local drives.

#2

The newly observed samples use obfuscation of the code to make it more difficult to analyze. They also use legitimate tools and services to evade detection, for example, the Windows Management Instrumentation (WMI) service to enumerate all of the drives on the system. They can then encrypt all of the drives, including network shares. The encryption keys are generated using the victim's computer name and the current date and time.

#3

The ransom note is a text file called README.txt. The ransom note demands 0.1 Bitcoin in exchange for the decryption key. The note also includes a link to a TOR website where the victim can contact the ransomware operators. LOLKEK's evolution showcases its potential for larger, more sophisticated attacks, emphasizing the need for robust defenses.

Recommendations

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that adversaries can exploit.

Conduct Regular Data Backups: Implement a robust data backup strategy that includes regular backups of critical data and systems, ad hoc and periodic backup restoration test. In the event of a ransomware attack, having up-to-date backups will allow organizations to restore their systems and data without paying the ransom.

Protect your Backups: Ensure backups are adequately protected, employ 3-2-1-1 back up principle and Deploy specialized tools to ensure backup protection.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0007 Discovery	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1490 Inhibit System Recovery
T1005 Data from Local System	T1202 Indirect Command Execution	T1486 Data Encrypted for Impact	T1070.004 File Deletion
T1070 Indicator Removal	T1112 Modify Registry	T1012 Query Registry	T1083 File and Directory Discovery
T1027.002 Software Packing	T1027 Obfuscated Files or Information	T1082 System Information Discovery	T1566 Phishing
T1566.001 Spearphishing Attachment	T1204.002 Malicious File	T1204 User Execution	T1059 Command and Scripting Interpreter
T1059.007 JavaScript	T1047 Windows Management Instrumentation		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	Ed247b58c0680b7c92632209181733e92f1b0721, 768b8d81a6b0f779394e4af48755ca3ad77ed951, 88baff4e1751bd364cdb1a4bb5fda4a37ee127c4, 456b0bda3f6d9ec9a874daac050b75fc28174510
SHA256	08029396eb9aef9b413582d103b070c3f422e2b56e1326fe318bef60bdc382ed, 58ac26d62653a648d69d1bcaed1b43d209e037e6d79f62a65eb5d059e8d0fc3f, 2c66e5f96470526219f40c6adfd6990cc28d520975da1fdb6bb5497d55a54117, 0b179973dc267d9c300e9b7d3c27c67a18d7c79b2cc34927cbe5a465f83c6190

TYPE	VALUE
Domains	Mmcbkgua72og66w4jz3qcxkkhefax754pg6iknmtfujvkt2j65ffraad[.]onion, filessupport@onionmail[.]org
URL	https[:]//yip[.]su/2QstD5
MD5	518a38b47292b1e809c5e6f0bb1858be

References

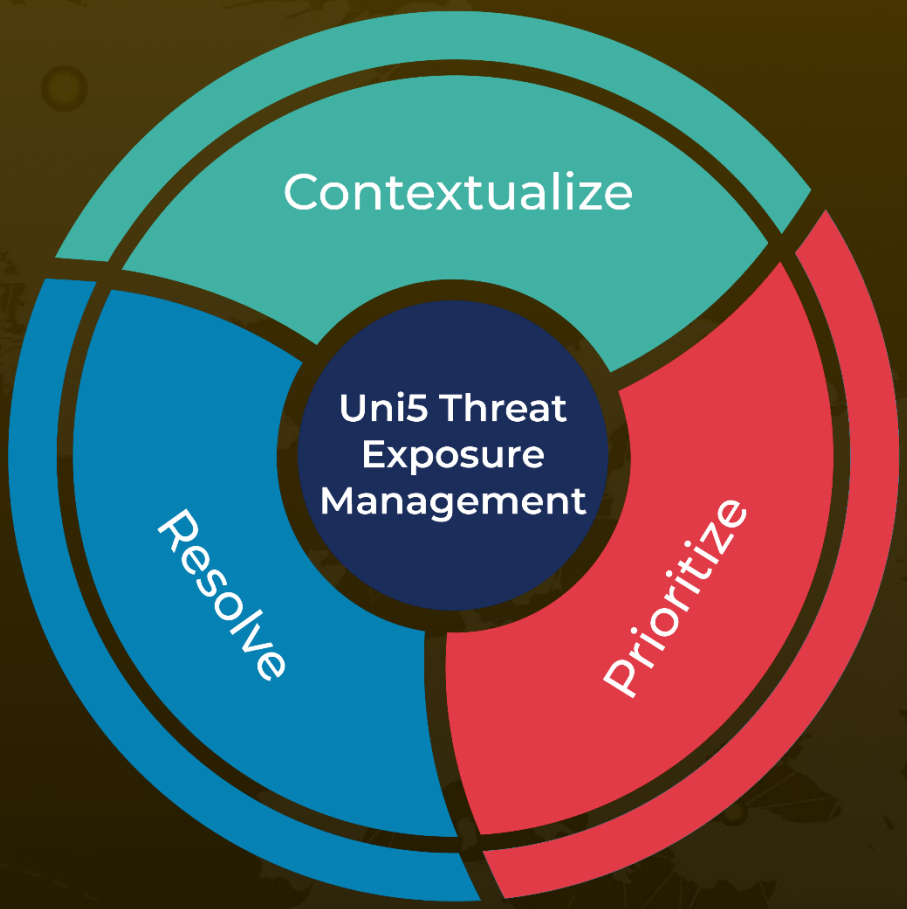
https://www.sentinelone.com/blog/lolkek-unmasked-an-in-depth-analysis-of-new-samples-and-evolving-tactics/

https://www.hivepro.com/new-ransomware-campaign-tzw-linked-to-globeimposter-targets-south-korean-organizations/

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 10, 2023 • 4:00 AM

More at www.hivepro.com