Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

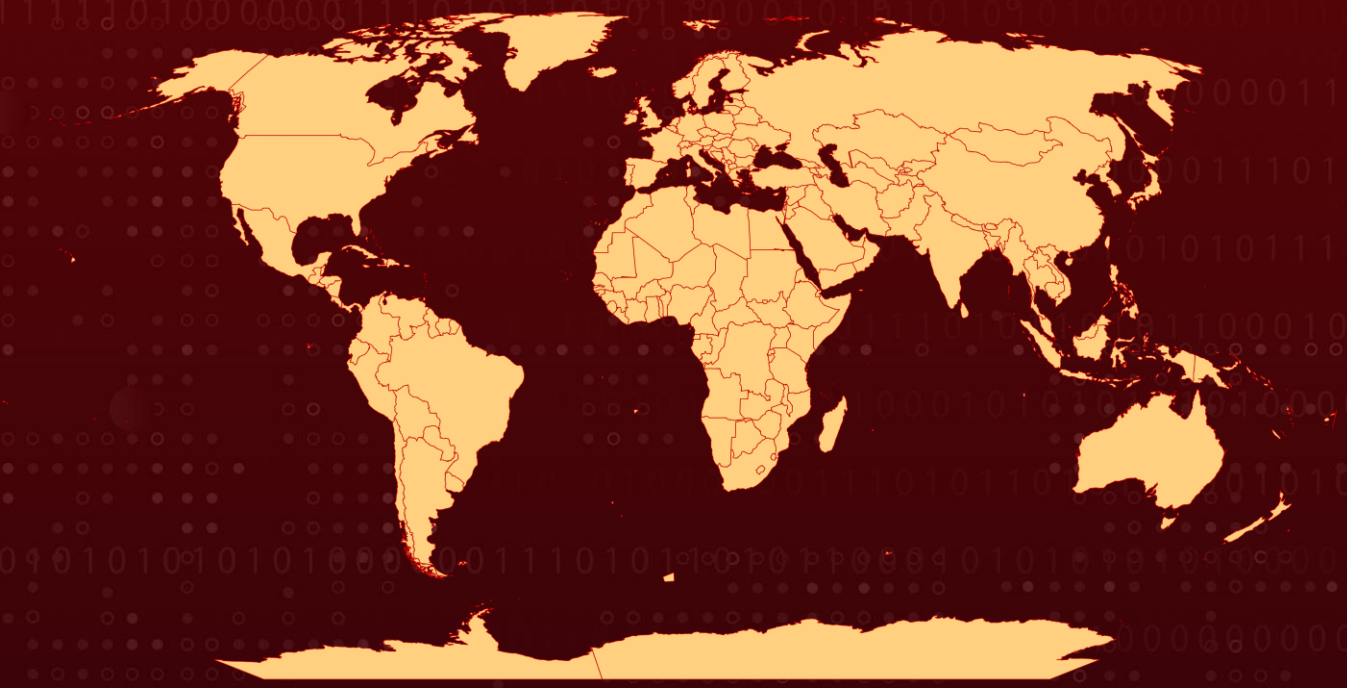
MichaelKors Ransomware Targets Linux and VMware ESXi Systems with Hypervisor Jackpotting

Date of Publication	Admiralty Code	TA Number
May 22, 2023	A1	TA2023239

Summary

First Appearance: April 2023
Malware: MichaelKors
Targeted Countries: Worldwide
Affected Platforms: Windows, Linux and VMware ESXi
Attack: MichaelKors ransomware, a new RaaS operation, has been targeting Linux and VMware ESXi systems since April 2023, utilizing the tactic of "hypervisor jackpotting" to gain unrestricted access and encrypt files, posing a significant threat to organizations' virtualization infrastructure.

Attack Regions



Attack Details

#1 A new ransomware-as-a-service (RaaS) operation called MichaelKors has been targeting Linux and VMware ESXi systems since April 2023. This highlights a trend of cybercriminals shifting their focus to ESXi, a popular virtualization and management system. ESXi's lack of native support for third-party agents or antivirus software makes it an appealing target.

#2 Attackers are using a tactic called "hypervisor jackpotting" to deploy ransomware on ESXi hypervisors, which allows them to gain unrestricted access to the underlying resources of the machine. The absence of security tools, insufficient network segmentation, and in-the-wild vulnerabilities make ESXi hypervisors a rich target environment for threat actors.

#3 The growing adoption of virtualization technology and migration to the cloud contribute to the increasing number of targets. Credential theft and exploitation of vulnerabilities are common attack vectors, and organizations should take steps to secure their ESXi hosts and vCenter server management software.

Recommendations

Harden access controls: Strengthen access controls to ESXi hypervisors by implementing strong passwords, enabling two-factor authentication (2FA), and regularly reviewing and revoking unnecessary privileges. This helps prevent unauthorized access and reduces the risk of credential theft.

Network segmentation: Implement network segmentation to isolate ESXi hypervisors from other systems and limit lateral movement in the event of a breach. By segmenting the network, attackers will find it more difficult to move laterally and compromise critical systems.

Regular backups and testing: Maintain regular backups of critical data and ESXi datastore volumes. Ensure that backups are securely stored and regularly tested for reliability, so that in the event of a ransomware attack, data can be restored without paying the ransom. Regularly testing the restoration process helps ensure the effectiveness of the backup strategy.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0008 Lateral Movement	TA0004 Privilege Escalation
TA0011 Command and Control	TA0042 Resource Development	TA0005 Defense Evasion	TA0040 Impact
TA0001 Initial Access	T1588 Obtain Capabilities	T1569 System Services	T1027 Obfuscated Files or Information
T1078 Valid Accounts	T1505 Server Software Component	T1021 Remote Services	T1068 Exploitation for Privilege Escalation
T1021.007 Cloud Services	T1564 Hide Artifacts	T1564.006 Run Virtual Instance	T1588.005 Exploits
T1210 Exploitation of Remote Services	T1486 Data Encrypted for Impact		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5 cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849 a32b7e40fc353fd2f13307d8bfe1c7c634c8c897b80e72a9872baa9a1da08c46 855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808 7095beafff5837070a89407c1bf3c6acf8221ed786e0697f6c578d4c3de0efd6 3339ba53e1f05f91dbe907d187489dbaba6c801f7af6fd06521f3ba8c484ec6c
SHA1	c7fcbaedf6b077b3d9bfc4720c3860a5d848bcb4 c7b28fe059e944f883058450d5c77b03076b0ea1 b033a146de147d97db6f8dadbe2141df2f0192be 91ad089f5259845141dfb10145271553aa711a2b 228239d1bf7020ecdc4021f3c20a14041b210d78 0f5457b123e60636623f585cc2bf2729f13a95d6

TYPE	VALUE
MD5	c159afb7d2111690326cad610776db34 b0fd45162c2219e14bdccab76f33946e aa1ddf0c8312349be614ff43e80a262f 99549bcea63af5f81b01decf427519af 546af2069c28f794dc918958a80ac17b 40c9dc2897b6b348da88b23deb0d3952

References

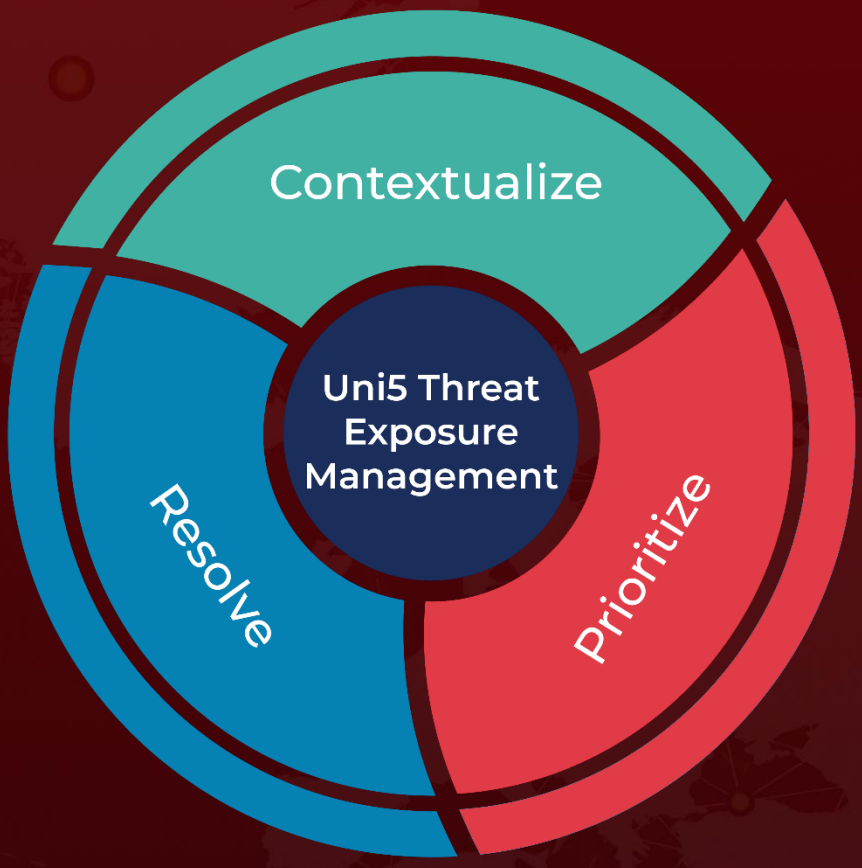
https://www.blackhatethicalhacking.com/news/michaelkors-ransomware-takes-aim-at-linux-and-vmware-esxi/

https://www.crowdstrike.com/blog/hypervisor-jackpotting-lack-of-antivirus-support-opens-the-door-to-adversaries/

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

May 22, 2023 • 6:30 AM

More at www.hivepro.com