Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

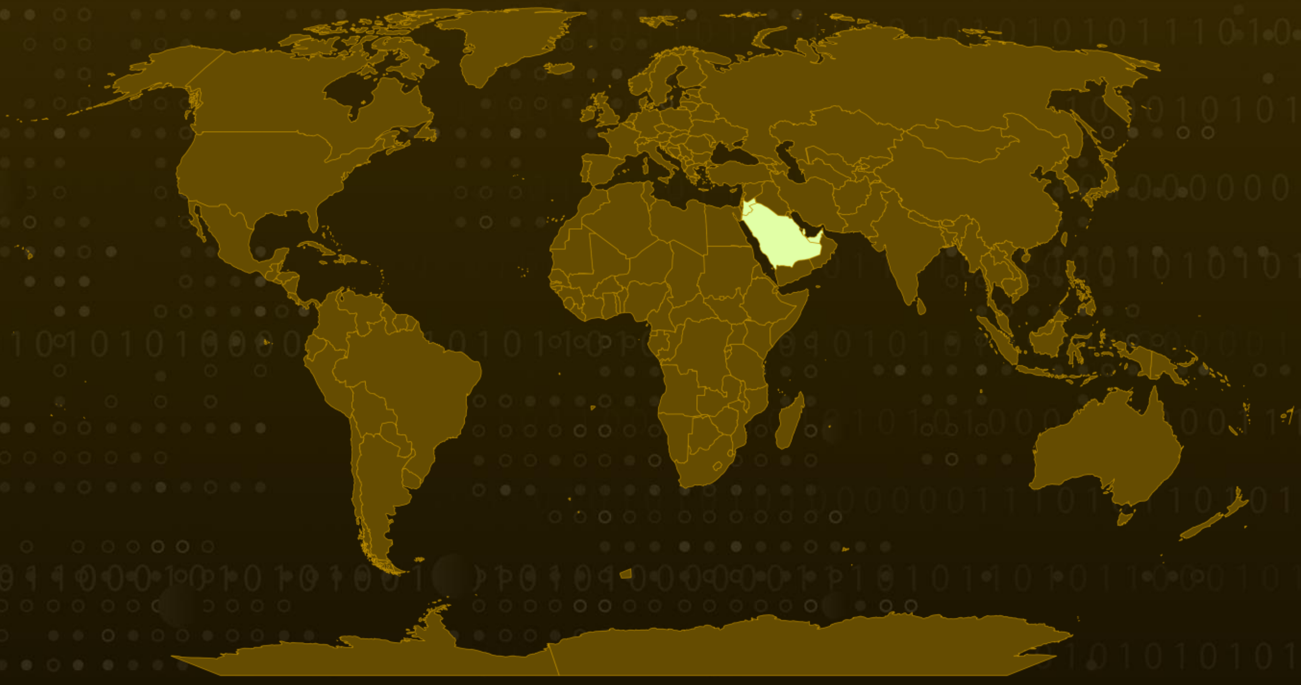
WINTAPIX Kernel Driver Targeting Middle Eastern Nations

Date of Publication	Admiralty Code	TA Number
May 23, 2023	A2	TA2023242

Summary

First seen: December 2021
Malware: Donut
Attack Region: Saudi Arabia, Jordan, Qatar, and the United Arab Emirates
Attack: The WINTAPIX driver, protected by VMProtect, targets Saudi Arabia and other Gulf countries, possibly linked to Iranian threat actors exploiting Exchange servers for malware deployment.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 Donut is a publicly available in-memory injector/loader, meticulously crafted to facilitate the execution of a kernel driver known as WINTAPIX (Wintapix.sys). The WINTAPIX driver, carefully compiled in June 2021, surfaced in the public domain for the first time in December 2021. It is worth noting that approximately 65% of the inquiries for this driver originated from Saudi Arabia, indicating its significant target audience.

#2 Moreover, instances of its detection have been reported in Jordan, Qatar, and the United Arab Emirates, which are widely recognized as primary targets for Iranian threat actors. Notably, Iranian threat actors have a track record of exploiting Exchange servers to deploy additional malware, thus raising the possibility that this driver has been employed in conjunction with Exchange attacks.

#3 WINTAPIX benefits from partial protection provided by VMProtect, an advanced software protection tool that leverages virtualization to safeguard software applications against reverse engineering and unauthorized usage.

#4 Its principal objective revolves around generating and executing the subsequent phase of the attack. This process entails the utilization of a shellcode, which is embedded directly into the binary without any form of obfuscation. Additionally, an integral function of WINTAPIX involves establishing persistence through the creation of registry keys.

Recommendations

Implement robust security measures, including network monitoring and intrusion detection systems, to detect and mitigate potential threats the WINTAPIX driver poses, particularly in regions with high inquiry rates such as Saudi Arabia, Jordan, Qatar, and the United Arab Emirates.

Strengthen defenses against Exchange server vulnerabilities, as Iranian threat actors have a history of exploiting such servers to deploy additional malware, potentially in conjunction with the WINTAPIX driver. Regularly update and patch Exchange servers to minimize the risk of compromise.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0003** Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion
TA0008 Lateral Movement	**TA0011** Command and Control	**TA0010** Exfiltration	**T1021** Remote Services
T1021.001 Remote Desktop Protocol	**T1027** Obfuscated Files or Information	**T1027.009** Embedded Payload	**T1036** Masquerading
T1036.001 Invalid Code Signature	**T1041** Exfiltration Over C2 Channel	**T1055** Process Injection	**T1059** Command and Scripting Interpreter
T1059.003 Windows Command Shell	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1090** Proxy
T1105 Ingress Tool Transfer	**T1140** Deobfuscate/Decode Files or Information	**T1205** Traffic Signaling	**T1543** Create or Modify System Process
T1543.003 Windows Service	**T1562** Impair Defenses	**T1569** System Services	**T1569.002** Service Execution
T1573 Encrypted Channel	**T1573.001** Symmetric Cryptography	**T1562.009** Safe Mode Boot	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f6c316e2385f2694d47e936boac4bc9b55e279d530dd5e805f0d963cb47c3c0d 8578bff36e3b02cc71495b647db88c67c3c5ca710b5a2bd539148550595d0330 aae9c8bd9db4e0d48e35d9ab3b1a8c7933284dcbeb344809fed18349a9ec7407 27a6c3f5c50c8813ca34ab3b0791c08817c80387766577495489088484 2973ed 1485cOed3e875cbdfc6786a5bd26d18ea9d31727deb8df290a1cOOc780419a4e

References

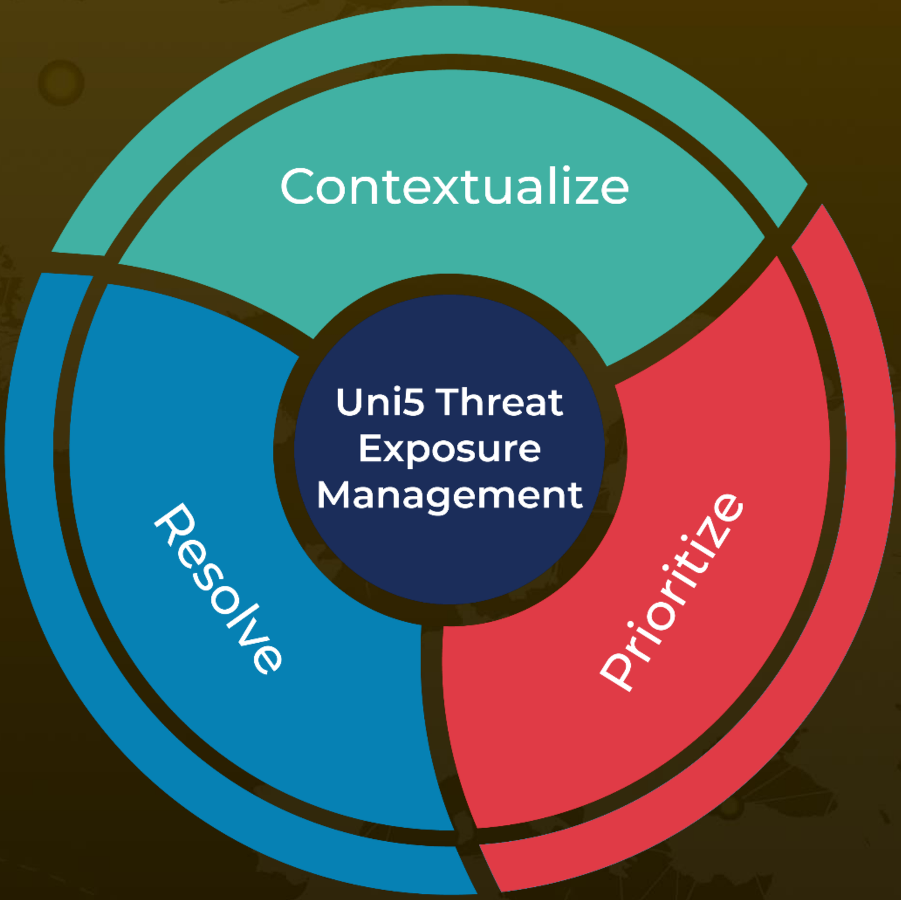
https://www.fortinet.com/blog/threat-research/wintapix-kernal-driver-middle-east-countries

https://attack.mitre.org/software/S0695/

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 23, 2023 • 6:07 AM

More at www.hivepro.com