Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

The Zardoor Backdoor's Silent Takeover of Saudi Charities

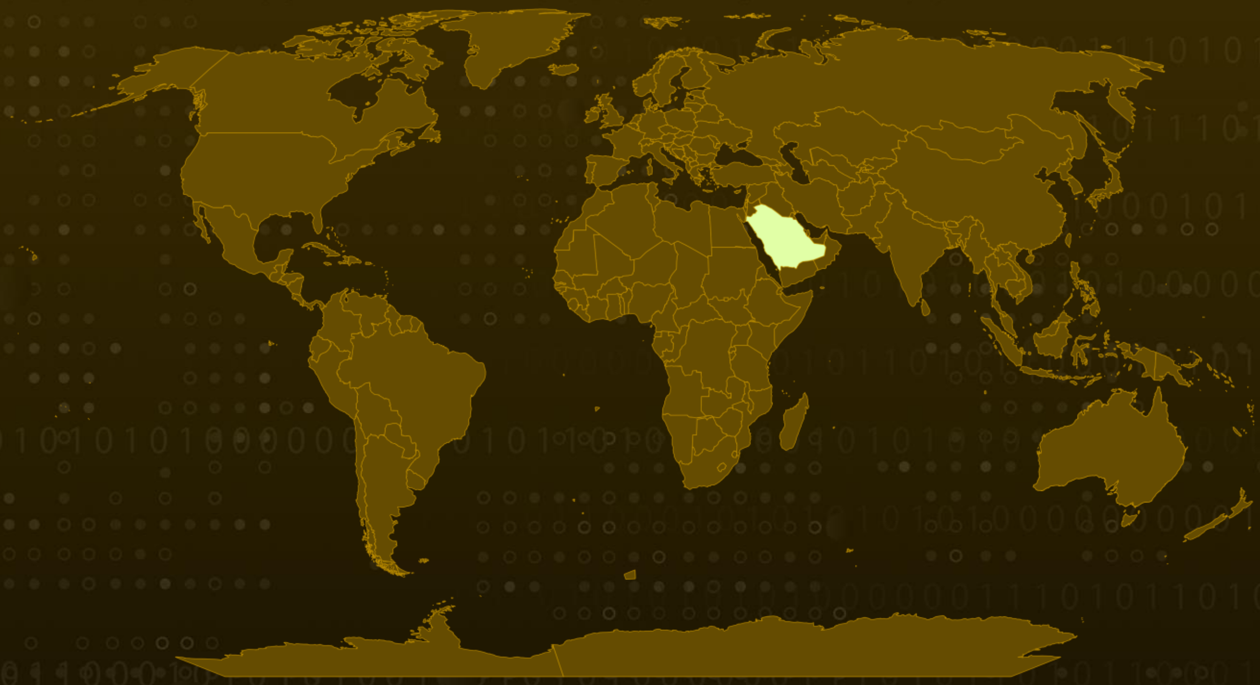
Date of Publication	Admiralty Code	TA Number
February 13, 2024	A1	TA2024055

Summary

First Seen: March 2021
Malware: Zardoor backdoor
Targeted Industries: Non-profit organization
Attack Region: Saudi Arabia

Attack: An espionage operation, designed to distribute a backdoor called Zardoor, was uncovered with evidence suggesting it dates back to March 2021. In May 2023, this meticulously orchestrated campaign specifically targeted non-profit organizations in Saudi Arabia.

Attack Regions



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

Attack Details

#1 A covert espionage campaign was orchestrated to propagate an undisclosed backdoor known as Zardoor, believed to have persisted since at least March 2021. In May 2023, non-profit entities in Saudi Arabia fell victim to this meticulously executed campaign.

#2 The perpetrators employed a sophisticated multi-chain attack methodology, leveraging living-off-the-land binaries (LoLBins) and reverse proxy tools. Additionally, they adeptly tailored open-source instruments, allowing them to maintain persistent access to the targeted network for an extended duration without evoking suspicion.

#3 The precise method used to initially breach the targeted entity remains elusive. The unidentified infection pathway sets the stage for the deployment of a dropper component, subsequently installing a malicious dynamic-link library responsible for unleashing two backdoor modules, namely "zar32.dll" and "zor32.dll."

#4 The former serves as the core backdoor element, facilitating Command and Control (C2) communications, while the latter ensures the deployment of "zar32.dll" with elevated administrator privileges. The threat actor utilized Windows Management Instrumentation (WMI) for lateral movement, disseminating the attacker's tools, including Zardoor.

#5 This was achieved by initiating processes on the target system and executing commands received from the C2. Zardoor exhibits capabilities such as data exfiltration, remote execution of fetched executables and shellcode, updating the C2 IP address, and self-deletion from the host.

Recommendations

Continuous Monitoring and Analysis: Establish continuous monitoring and analysis protocols to promptly detect any unusual network behavior, potentially indicating a long-term cyber espionage operation.

Network Segmentation: Employ network segmentation to isolate critical systems and sensitive data, limiting the lateral movement of an attacker within the network in case of a successful infiltration.

Heighten Awareness: Familiarize yourself with common phishing tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0010 Exfiltration	TA0011 Command and Control	T1574.002 DLL Side-Loading	T1018 Remote System Discovery
T1033 System Owner/User Discovery	T1047 Windows Management Instrumentation	T1048 Exfiltration Over Alternative Protocol	T1049 System Network Connections Discovery
T1053.005 Scheduled Task	T1055 Process Injection	T1055.001 Dynamic-link Library Injection	T1057 Process Discovery
T1059.003 Windows Command Shell	T1070.004 File Deletion	T1087.002 Domain Account	T1090.003 Multi-hop Proxy
T1105 Ingress Tool Transfer	T1204.002 Malicious File		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f71f7c68209ea8218463df397e5c39ef5f916f138dc001feb3a60ef585bd2ac2, c6419df4bbda5b75ea4a0b8e8acd2100b149443584390c91a218e7735561ef74, 73c7459e0c3ba00c0566f7baa710dd8b88ef3cf75ee0e76d36c5d8cd73083095, 1480b2038395f9edd2c21dff68eb29a4d6177708b70b687f758af60c8b02f071, 29741f7987ab61b85adb310a7ab2f44405822f1719fa431c8f49007b64f6f5cd, 5226b67b5d49720981841fab64794533fe0530409ba2975e6125a4bc008f2480, 7905bd9bb4d277a81935a22f975a0030faa9e5c9dbb9f6152c2f56ba1cd0cdea, a99a9f2853ff0ca5b91767096c7f7e977b43e62dd93bde6d79e3407bc01f661d,

TYPE	VALUE
SHA256	0058d495254bf3760b30b5950d646f9a38506cef8f297c49c3b73c208ab723bf, d267e2a6311fe4e2dfd0237652223add300b9a5233b555e131325a2612e1d7ef, 5eeab7b795a3303c368c72ef09a345f3a4f02301ec443e98319d600e8287e852, 4b16ea1b1273f8746cf399c71bfc1f5bff7378b5414b4ea044c55e0ee08c89d3, 3adcc81446f0e8ed1a2bc1e815613eb5622afba57941d651faa2b5bc4b2f13c1, 5655a2981fa4821fe09c997c84839c16d582d65243c782f45e14c96a977c594e, 1aea1e7098221f2cc76ccd45078d9a216236b4e7e295dfa68e8a25aab3abe778, d7dfa7009a9d808b744df8ed4f5852bd03ffb82f7a07a258ea8b5e0290fb7d87, 7abf74260ae5b771182e95bc360fefa1b635b56b3aa05922506d55c5d15517c3, d5d16d9bb75d461922eade2597c233255871dc74659f0169f3d3f40f5273ab71, b5b3627606a5c5e720fa32fb9cb90aa813c630673d23c97a81012b832799a897, 0a5aa03e35d6d9218342b2bec753a9800570c000964801cf6bfe45a9bb393c0d
IPv4:PORT	70[.]34[.]208[.]197:10086, 140[.]82[.]33[.]130:14443, 70[.]34[.]194[.]185:14443, 139[.]84[.]232[.]245:37135, 208[.]85[.]20[.]130:37135, 139[.]84[.]229[.]192:443, 70[.]34[.]195[.]221:443, 217[.]69[.]1[.]128:14443, 108[.]181[.]20[.]36:443, 108[.]61[.]189[.]125:443
Domain	lapz[.]ddns[.]net, exchangeupgrade[.]ddns[.]net, exchangeserver[.]zapto[.]org
Mutexes	3e603a07-7b2d-4a15-afef-7e9a0841e4d5, 6c2711b5-e736-4397-a883-0d181a3f85ae, ThreadMutex12453

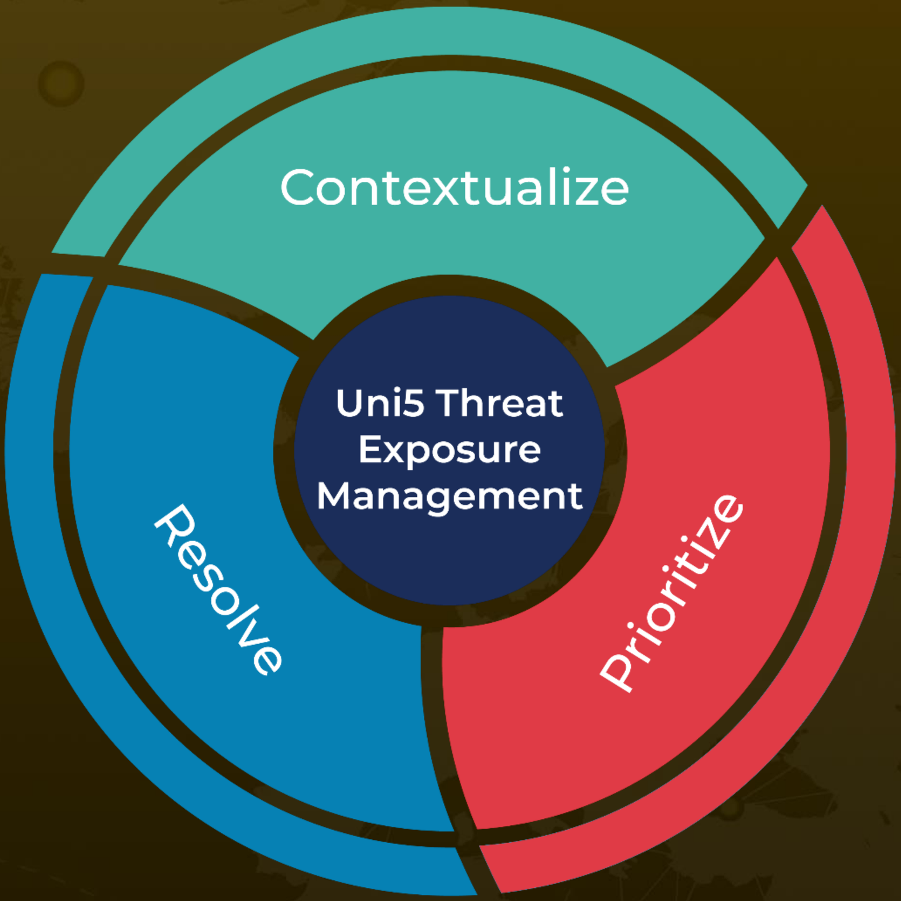
References

https://blog.talosintelligence.com/new-zardoor-backdoor/

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

February 13, 2024 • 4:00 AM

More at www.hivepro.com