Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

GoldenJackal's Covert Ops: Stealing Secrets from Air-Gapped Systems

Date of Publication

October 10, 2024

Admiralty Code

A1

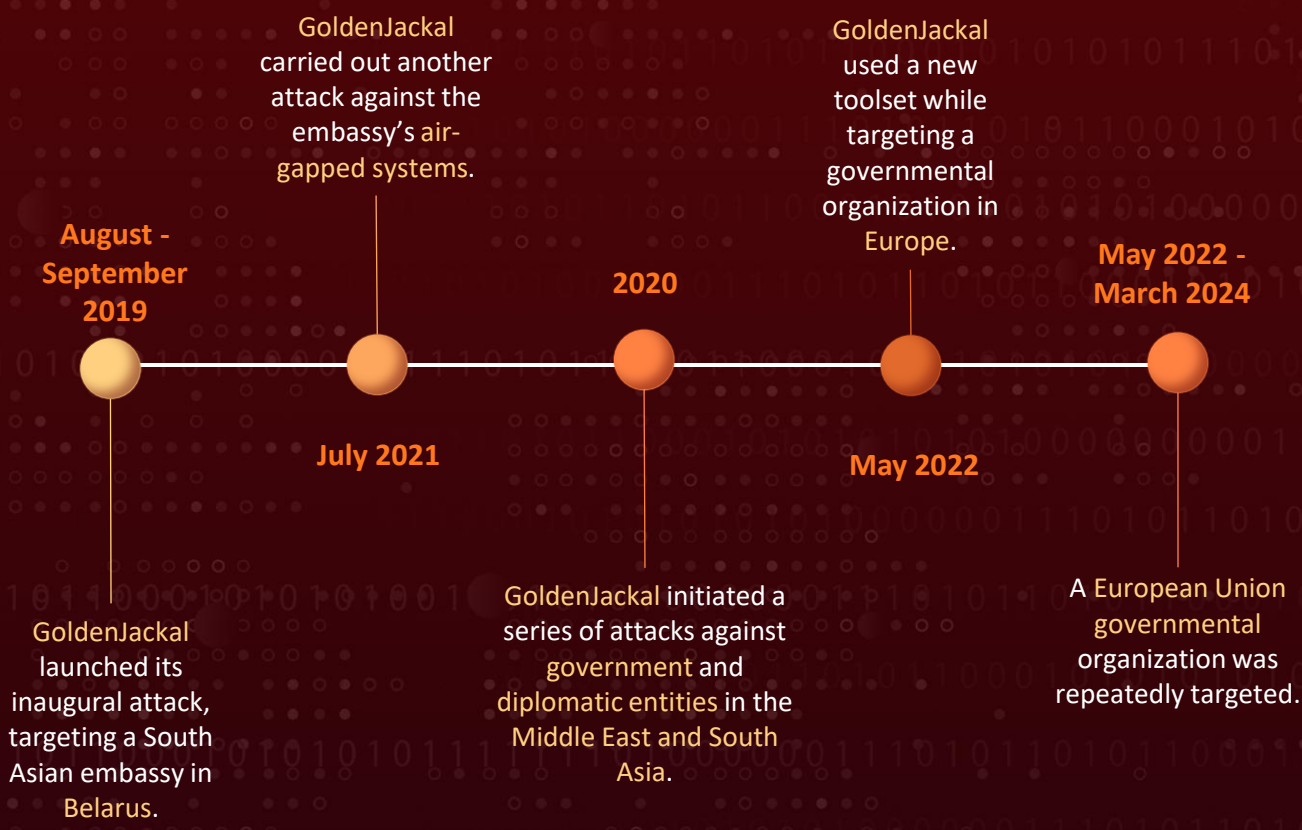
TA Number

TA2024386

Summary

Active Since: 2019
Threat Actor: GoldenJackal
Malware: JackalWorm, GoldenDealer, GoldenHowl, GoldenRobo, GoldenAce, GoldenUsbCopy, GoldenBlacklist, GoldenMailer, GoldenDrive
Attack Regions: Europe, the Middle East, and South Asia
Targeted Industries: Government, Diplomatic Entities, Embassy
Attack: GoldenJackal, a distinguished APT group, masterminded a series of exceptionally sophisticated cyberattacks, primarily directed at government and diplomatic entities across Europe. Utilizing state-of-the-art tools designed to breach air-gapped systems, GoldenJackal seeks to exfiltrate confidential data from high-value machines that are typically isolated from the internet.

Attack Timeline



Attack Regions

Attack Details

#1 GoldenJackal masterminded a series of highly advanced cyberattacks between May 2022 and March 2024, targeting a governmental organization in Europe. The group deployed cutting-edge tools capable of breaching air-gapped systems. GoldenJackal, a prominent cyber espionage APT group, strategically targets government and diplomatic entities.

#2 It aims to exfiltrate confidential data from high-priority machines that are typically isolated from the internet. GoldenJackal's impressive arsenal features several C#-based implants, including JackalWorm. Notably, the group deployed custom tools during its attack on a South Asian embassy in Belarus.

#3 These tools comprised three key components: GoldenDealer, which delivers executables via USB monitoring; GoldenHowl, a sophisticated modular backdoor; and GoldenRobo, a robust file collection and exfiltration tool. In 2022, GoldenJackal unveiled a new modular tool, GoldenAce, developed in Go, specializing in USB infections.

#4 Additionally, file-stealing tools like GoldenUsbCopy and GoldenUsbGo were employed to transfer stolen files to the attackers. Another noteworthy component, GoldenBlacklist, and its Python-based variant GoldenPyBlacklist, filters, and archives specific email messages before exfiltration. The group also utilizes GoldenMailer to send stolen data via email, and GoldenDrive to upload information to Google Drive.

#5 GoldenJackal's sophisticated toolsets provide the group with extensive capabilities. They enable it to infiltrate and maintain long-term persistence within targeted networks. Compromised systems are exploited to gather, process, and exfiltrate sensitive data while distributing files, configurations, and commands across other systems.

Recommendations

- **Implement USB Device Control Policies:** Enforce strict policies on the use of USB devices within government networks. Use endpoint security solutions to control and monitor USB access, ensuring only authorized devices can connect to systems.
- **Regular Software Updates and Patch Management:** Ensure that all software, especially critical applications and operating systems, are up-to-date with the latest security patches. This includes monitoring for zero-day vulnerabilities that could be exploited by GoldenJackal.
- **Implement Data Loss Prevention (DLP) Solutions:** Deploy DLP tools that monitor and control data transfers, particularly for sensitive information. Configure rules to prevent unauthorized data from being copied to USB devices or external storage.
- **Set Up Automated Alerts for Anomalous Behavior:** Configure systems to automatically alert security teams for anomalous activities, such as large file transfers or unexpected process executions, particularly those resembling GoldenJackal's tactics.
- **Integrate Endpoint Detection and Response (EDR):** Utilize EDR solutions that provide real-time monitoring, threat detection, and response capabilities. Configure these tools to alert on indicators of compromise (IOCs) associated with GoldenJackal's known tools like JackalWorm and GoldenHowl.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0011 Command and Control	TA0010 Exfiltration	T1583 Acquire Infrastructure	T1583.003 Virtual Private Server
T1583.004 Server	T1584 Compromise Infrastructure	T1584.006 Web Services	T1587 Develop Capabilities
T1587.001 Malware	T1585 Establish Accounts	T1585.003 Cloud Accounts	T1588 Obtain Capabilities
T1588.002 Tool	T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell
T1059.006 Python	T1106 Native API	T1569 System Services	T1569.002 Service Execution
T1204 User Execution	T1204.002 Malicious File	T1543 Create or Modify System Process	T1543.003 Windows Service
T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1053.005 Scheduled Task	T1564.001 Hidden Files and Directories
T1070.004 File Deletion	T1036.005 Match Legitimate Name or Location	T1036.008 Masquerade File Type	T1112 Modify Registry
T1027.013 Encrypted/Encoded File	T1552.001 Credentials In Files	T1552.004 Private Keys	T1087.001 Local Account

T1083 File and Directory Discovery	**T1046** Network Service Discovery	**T1120** Peripheral Device Discovery	**T1057** Process Discovery
T1018 Remote System Discovery	**T1518** Software Discovery	**T1082** System Information Discovery	**T1016.001** Internet Connection Discovery
T1135 Network Share Discovery	**T1210** Exploitation of Remote Services	**T1091** Replication Through Removable Media	**T1560.002** Archive via Library
T1119 Automated Collection	**T1005** Data from Local System	**T1025** Data from Removable Media	**T1074.001** Local Data Staging
T1114.001 Local Email Collection	**T1071.001** Web Protocols	**T1092** Communication Through Removable Media	**T1132.001** Standard Encoding
T1572 Protocol Tunneling	**T1090.001** Internal Proxy	**T1041** Exfiltration Over C2 Channel	**T1052.001** Exfiltration over USB
T1132 Data Encoding	**T1567.002** Exfiltration to Cloud Storage	**T1048.002** Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	**T1016** System Network Configuration Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	da9562f5268fa61d19648dff9c6a57fb8ab7b0d7, 5f12ffd272aabc0d5d611d18812a196a6ea2faa9, 6de7894f1971fdc1df8c4e4c2edcc4f4489353b6, 7cb7c3e98cab2226f48ba956d3be79c52ab62140, 8f722eb29221c6eaea9a96971d7fb78dab2ad923, 24fbcec23e8b4b40fea188132b0e4a90c65e3ffb, a87ceb21ef88350707f278063d7701bde0f8b6b7, 9cbe8f7079da75d738302d7db7e97a92c4de5b71, 9083431a738f031ac6e33f0e9133b3080f641d90, c830efd843a233c170285b4844c5960ba8381979, f7192914e00dd0ce31df0911c073f522967c6a97, b2baa5898505b32df7fe0a7209fc0a8673726509

TYPE	VALUE
File Name	winaero.exe, 1102720677, OfficeAutoComplete.exe, prinntfy.dll, zUpdater.exe, fc.exe, upgrade, fp.exe, cb.exe, GoogleUpdate.exe
IPv4	83[.]24[.]9[.]124, 196[.]29[.]32[.]210
Domain	assistance[.]uz, thehistore[.]com, xgraphic[.]ro
Email	mariaalpane[@]outlook[.]com, katemarien087[@]outlook[.]com, spanosmitsotakis[@]outlook[.]com

References

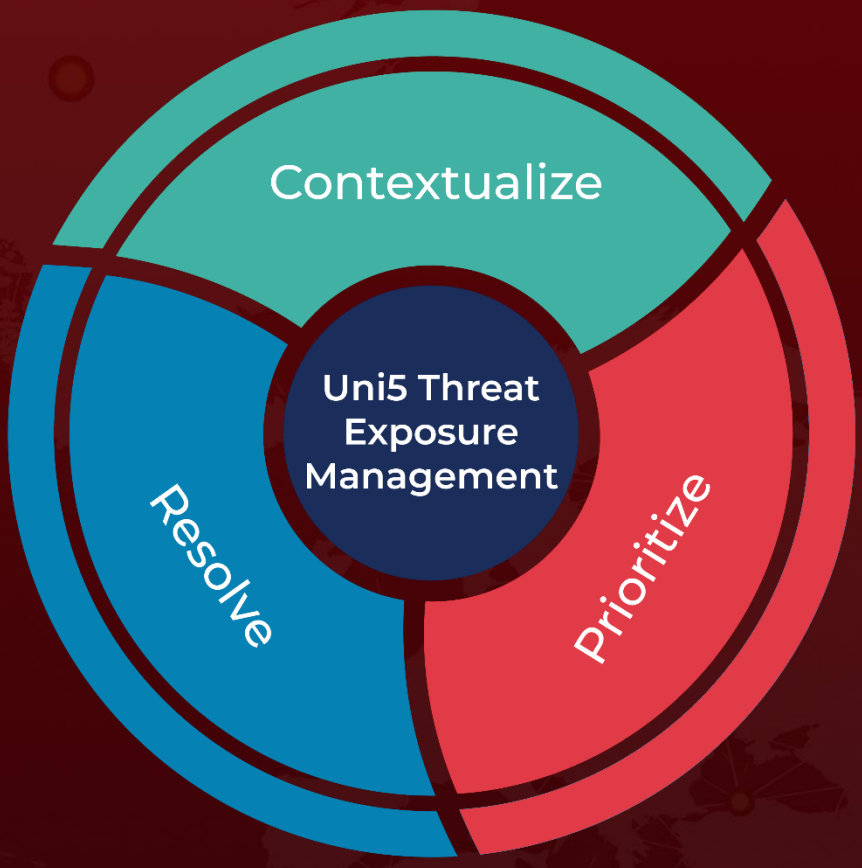
https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/

https://hivepro.com/threat-advisory/unveiling-the-stealthy-operations-of-goldenjackal-apt-group/

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

October 10, 2024 . 5:00 AM

More at www.hivepro.com