Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Charon Ransomware Encrypts Files Belonging to Middle East Industries

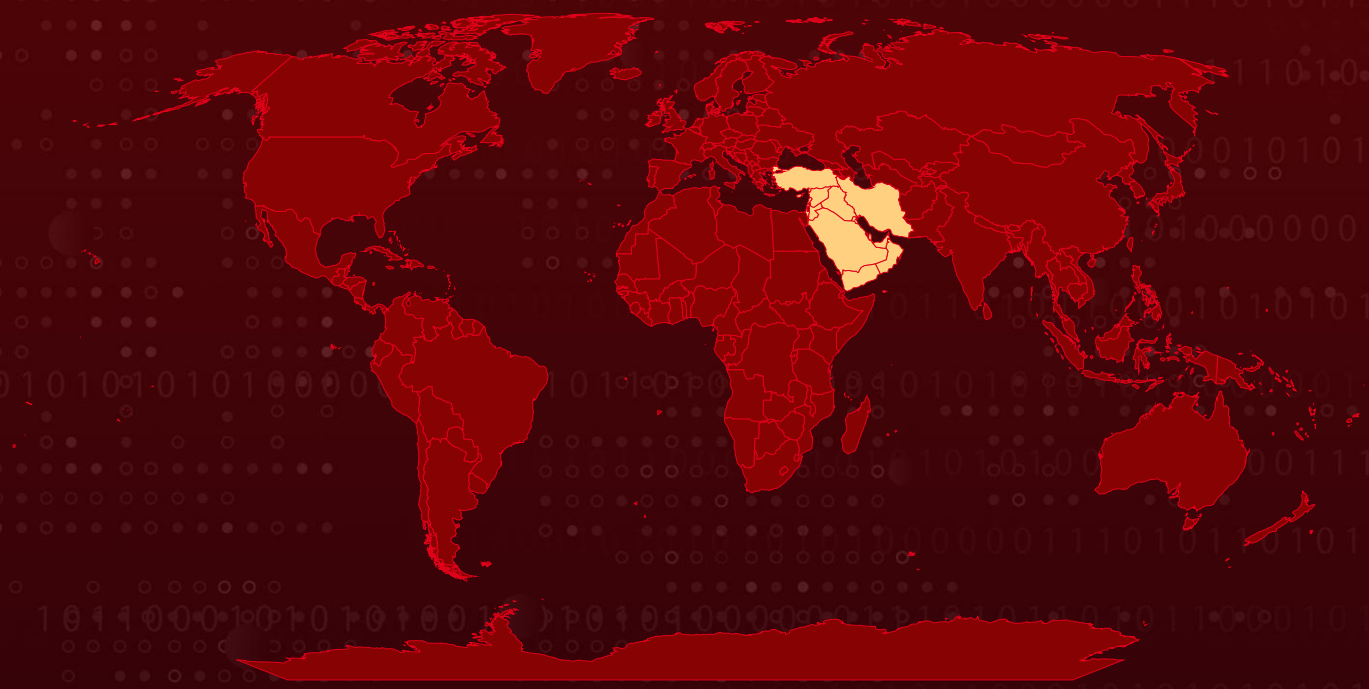
Date of Publication	Admiralty Code	TA Number
August 14, 2025	A1	TA2025250

Summary

Malware: Charon ransomware, SWORDLDR
Affected Platform: Windows
Targeted Region: Middle East
Targeted Industries: Public Sector, Aviation

Attack: Charon is a recently identified ransomware strain associated with sophisticated APT-style attacks targeting the public and aviation sectors in the Middle East. The findings highlight the growing trend of ransomware operators adopting advanced techniques for deployment and defense evasion, further obscuring the boundary between cybercrime and state-sponsored operations.

Attack Regions



Attack Details

#1

Charon is a recently identified ransomware that incorporates advanced techniques often associated with advanced persistent threats (APT). These include dynamic-link library (DLL) sideloading, process injection, and mechanisms designed to evade endpoint detection and response (EDR) solutions. The malware is deployed with customized ransom demands, targeting specific organizations.

#2

A recent campaign involving Charon was observed in targeted attacks against the public sector and aviation industry in the Middle East. The attackers used a DLL sideloading method similar to that employed in **Earth Baxia** campaigns. While DLL sideloading is a common technique, the implementation in this case showed a level of sophistication consistent with high-level threat actors, particularly in its use of coordinated toolchains and encrypted payload delivery.

#3

The intrusion chain leveraged a legitimate browser-related executable, Edge.exe, to sideload a malicious DLL named msedge.dll identified as SWORDLDR. This loader decrypted the embedded ransomware payload and injected it into a newly created svchost.exe process. By impersonating a legitimate Windows service, the malware was able to bypass conventional security controls.

#4

Charon's deployment follows a multistage payload extraction process. The initial payload contained encrypted shellcode that, once decrypted, revealed a secondary payload with embedded configuration data. This configuration specified the use of svchost.exe for process injection, reinforcing its stealth capabilities.

#5

The ransomware is capable of disruptive actions such as terminating security-related services, shutting down active processes, and deleting shadow copies and backups to hinder recovery. It employs multithreading and partial encryption techniques, allowing it to lock files more quickly and efficiently.

#6

A notable feature within Charon is a driver based on the open-source Dark-Kill project, designed to disable EDR solutions through a bring-your-own-vulnerable-driver (BYOVD) attack. Once encryption is complete, the ransomware appends the .Charon extension to affected files and inserts an infection marker reading “hCharon is enter to the urworld!” within them. It also drops a ransom note titled How To Restore Your Files.txt in all affected directories, network shares, and drives.

Recommendations

Defend Against DLL Sideloading and Process Injection: Restrict which executables can run and load DLLs, with a focus on directories often abused for sideloading, such as application folders and temporary locations. Implement alerts for suspicious process activity, including signed binaries like Edge.exe (originally named cookie_exporter.exe), spawning unusual DLLs, or initiating unexpected svchost.exe instances.

Implement the 3-2-1 Backup Rule: Maintain three total copies of your data, with two backups stored on different devices and one backup kept offsite or in the cloud. This ensures redundancy and protects against data loss from ransomware attacks.

Backup & Recovery Preparedness: Maintain offline, immutable, and regularly tested backups. Ensure recovery time objectives (RTOs) and recovery point objectives (RPOs) meet business continuity requirements in the event of ransomware deployment.

Limit Lateral Movement: Restrict access between workstations, servers, and sensitive file shares. Require strong, multifactor authentication for all remote and administrative access. Always verify and authenticate users and devices before granting access to critical resources, even if they are inside the network. Implementing a Zero Trust architecture helps limit the ability of attackers to move laterally within networks.

Improve User Awareness and Privilege Management: Conduct security training to help employees recognize and avoid suspicious emails, attachments, links, and executables that could trigger a ransomware infection chain. Enforce the principle of least privilege, ensuring user and service accounts have only the access necessary for their roles to minimize the potential impact of a compromise.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0008 Lateral Movement	TA0040 Impact	T1204 User Execution
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation	T1070 Indicator Removal
T1070.004 File Deletion	T1027 Obfuscated Files or Information	T1036 Masquerading	T1036.004 Masquerade Task or Service
T1620 Reflective Code Loading	T1055 Process Injection	T1562 Impair Defenses	T1562.001 Disable or Modify Tools
T1562.006 Indicator Blocking	T1082 System Information Discovery	T1486 Data Encrypted for Impact	T1490 Inhibit System Recovery
T1489 Service Stop	T1569.002 Service Execution	T1574 Hijack Execution Flow	T1574.001 DLL

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	80711e37f226ef1dc86dc80a8cbc0b2ec895b361e9ade85da793d94b1d876be8, 739e2cac9e2a15631c770236b34ba569aad1d1de87c6243f285bf1995af2cdc2, e0a23c0d99c45d40f6ef99c901bacf04bb12e9a3a15823b663b392abadd2444e

TYPE	VALUE
SHA1	92750eb5990cdcda768c7cb7b654ab54651c058a, a1c6090674f3778ea207b14b1b55be487ce1a2ab, 21b233c0100948d3829740bd2d2d05dc35159ccb
MD5	dc2d94043269f661bb83f0a0d4a754e7, 966a8a32fee80bba5fcf4f83cd6180fe, a1a0fd18382769745592226f1f652632
Filename	How To Restore Your Files.txt

References

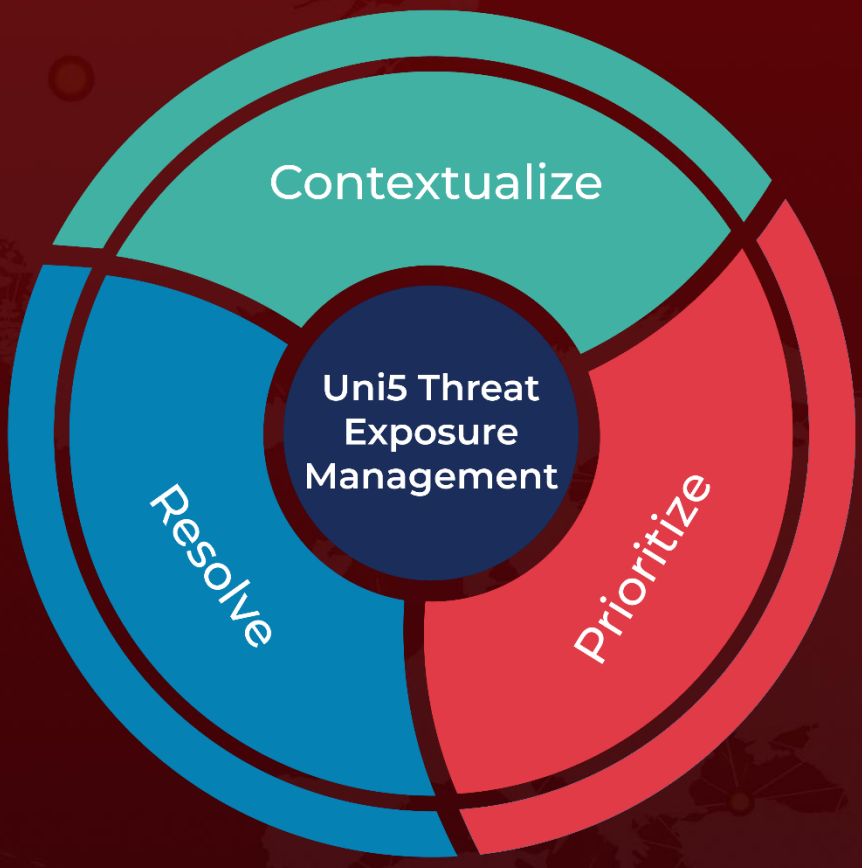
https://www.trendmicro.com/en_us/research/25/h/new-ransomware-charon.html

https://hivepro.com/threat-advisory/earth-baxia-a-new-threat-to-apac-governments/

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 14, 2025 • 5:30 AM

More at www.hivepro.com