INCIDENT ANALYSIS & MITRE ATT&CK; REPORT

Case ID: TA-SOC-2025-001
Analyst: Jordan Fields (ToddAvery / DAE Project)
Date: 2025-10-13
Classification: Defensive analysis / academic deliverable

Summary: The analyzed file QAe0.exe (SHA-256: 6e13f5c8ca7758d00a49978541775a5c4c6f507b060c473482fbecb190fd0d9c) was flagged by 39 out of 72 security vendors on VirusTotal as a malicious MSIL-based Trojan/Backdoor variant, associated with the Remcos family. This sample exhibits obfuscation, persistence, and remote control characteristics, indicating C2 capabilities.

VirusTotal Detection Summary

- 39 / 72 security vendors flagged this file as malicious

Vendor	Detection
AVG	Win32:MalwareX-gen [Crypt]
Avira	HEUR/AGEN.1376267
CrowdStrike Falcon	Win/malicious_confidence_100% (W)
ESET-NOD32	Variant of MSIL/GenKryptik_A.Gen.BNN
GData	Win32.Backdoor.Remcos.ALE5JQ
Dr.Web	Trojan.KillProc2.38785
Ikarus	Win32.Outbreak
Elastic	Malicious (high confidence)

Behavioral Summary:

- MSIL/.NET executable with macro-create-ole behavior and debug-environment detection.
- Likely uses Remcos RAT functionality: persistence via registry keys, credential theft, and C2 beaconing over HTTP(S).
- Common persistence methods: Run keys, scheduled tasks, and registry modifications.
- Potential impacts: remote control, data exfiltration, lateral movement.

MITRE ATT&CK; Mapping (Remcos Family)

Tactic	Technique (ID)	Description
Initial Access	T1566.001	Phishing Attachment delivering malicious MSIL payload.
Execution	T1059	Execution via PowerShell or .NET runtime invocation.
Persistence	T1547	Registry Run keys, scheduled tasks for autostart.
Defense Evasion	T1027	Packed/obfuscated executable using Crypter.
Credential Access	T1003	Credential dumping via Remcos modules.
Discovery	T1082	System Information Discovery.
Command & Control	T1071.001	C2 communication via HTTP(S).
Exfiltration	T1041	Data exfiltration through encrypted C2 channels.

Indicators of Compromise (IOCs)

- SHA-256: 6e13f5c8ca7758d00a49978541775a5c4c6f507b060c473482fbecb190fd0d9c
- File name: QAe0.exe
- Domains / IPs: (to be populated from sandbox)

- Persistence: Registry Run keys, Scheduled Tasks
- Mutex: Detected during execution (Remcos typical)

Remediation & Containment Recommendations:

1. Isolate infected hosts immediately from the network.
2. Capture memory and disk images for forensics.
3. Remove persistence artifacts and reimage affected systems.
4. Rotate all user and administrative credentials.
5. Block observed C2 domains and IPs at perimeter firewalls.
6. Deploy updated EDR/YARA rules to detect Remcos signatures.
7. Conduct user awareness training to prevent phishing attachment execution.

References:

- MITRE ATT&CK;: https://attack.mitre.org/
- VirusTotal:
https://www.virustotal.com/gui/file/6e13f5c8ca7758d00a49978541775a5c4c6f507b060c473482fbecb190fd0d9c/detection
- Remcos RAT analysis (CISA & CrowdStrike public reports).