Contents

[**G0090-Wirte** 2](#_Toc179361442)

[**I. Introduction** 2](#_Toc179361443)

[**II. Tactics** 2](#_Toc179361444)

[**III. Techniques** 2](#_Toc179361445)

[**V. Summary** 6](#_Toc179361446)

[**References** 7](#_Toc179361447)

## **G0090-Wirte**

## **I. Introduction**

G0090 Wirte, first identified in 2019 by Kaspersky researchers, is an Advanced Persistent Threat (APT) group primarily targeting the Middle East, with a specific focus on Palestine. This group has demonstrated sophisticated tactics, techniques, and procedures (TTPs) that distinguish it from other threat actors in the region. Its operations have been notable for their use of previously undocumented malware and their ability to maintain long-term persistence in compromised networks.

## **II. Tactics**

1. ***Strategic Target Selection***

The group primarily focuses on government entities, particularly those involved in foreign affairs and national security in the Middle East. This suggests a state-sponsored motivation, likely aimed at intelligence gathering and geopolitical advantages.

1. ***Long-term Persistence***

The group emphasizes maintaining access to compromised networks for extended periods, often remaining undetected for months or even years. This allows for continuous intelligence gathering and potential future exploitation.

1. ***Defense Evasion***

The group employs sophisticated evasion techniques to bypass security controls and avoid detection by antivirus solutions and intrusion detection systems.

1. ***Living Off The Land (LOTL)***

Wirte extensively uses legitimate system tools and processes to blend their activities with normal system operations, making detection and attribution more challenging.

## **III. Techniques**

|  |  |
| --- | --- |
| Techniques | Description |
| Spear-phishing with Tailored Lures (T1566.002) | Wirte crafts highly targeted emails, often impersonating legitimate government agencies or NGOs.  These emails typically contain malicious Microsoft Office documents, particularly Excel files with embedded macros |
| Malware Deployment | Custom Backdoor: "Whisper" - A previously undocumented backdoor written in .NET (T1059.007).  Lightweight First-stage Loaders: Often using PowerShell scripts (T1059.001) to download and execute the main payload |
| Command and Control (C2) Infrastructure | Use of Domain Fronting (T1090.004) to disguise C2 traffic.  Implementation of custom protocols over HTTPS (T1071.001) for covert communication. |
| Persistence Mechanisms | Scheduled Task Creation (T1053.005) for periodic execution of malware.  Modification of Registry Run Keys (T1547.001) to ensure malware runs at system startup. |
| Defense Evasion | Process Hollowing (T1055.012) to inject malicious code into legitimate Windows processes.  Use of Obfuscated Files or Information (T1027), particularly XOR encoding of payloads. |
| Credential Access | Implementation of custom keyloggers (T1056.001) to capture user credentials.    Use of Mimikatz (T1003.001) for dumping LSASS memory to extract passwords and hashes |
| Lateral Movement | Exploitation of Windows Remote Management (WinRM) (T1021.006) for moving between systems.  Use of Valid Accounts (T1078) obtained through initial compromise or credential theft. |

**IV. Procedures**

Wirte's attack chain typically follows this sequence:

***1. Initial Access***

a. Spear-phishing emails are sent to targeted individuals within the organization.

b. These emails contain malicious Excel files with names like "COVID-19 Updates.xlsx" or "Foreign Policy Briefing.xlsx".

c. When opened, the files prompt users to enable macros.

***2. Execution and Persistence***

a. Once macros are enabled, a PowerShell script is executed, which downloads the first-stage loader.

b. The loader then retrieves and executes the Whisper backdoor.

c. Whisper establishes persistence through scheduled tasks and registry modifications.

***3. Command and Control***

a. Whisper initiates communication with its C2 server using a custom protocol over HTTPS.

b. Domain fronting is employed to mask the true destination of the C2 traffic.

***4. Privilege Escalation***

a. The malware attempts to elevate privileges using known Windows vulnerabilities (e.g., CVE-2019-1388).

b. If unsuccessful, it waits for opportunities to capture administrator credentials through keylogging.

***5. Lateral Movement***

a. Once elevated privileges are obtained, Wirte uses WinRM to move laterally within the network.

b. They also leverage Active Directory enumeration to identify high-value targets.

***6. Data Exfiltration***

a. Sensitive documents are identified and compressed using custom routines.

b. Data is exfiltrated in small chunks, often disguised as normal HTTPS traffic.

***7. Operational Security***

a. Wirte employs a "hands-on-keyboard" approach for critical operations to avoid automated detection.

b. They regularly update their tools and infrastructure to evade detection based on known indicators.

## **V. Summary**

G0090 Wirte has emerged as a highly advanced threat actor, particularly in targeting organizations that are in the Middle East. Their operations display some level of complexity and adaptability that poses major challenges to cybersecurity defenders.

Wirte's primary tool, the Whisper backdoor, demonstrates their technical ability. Written in .NET for flexibility across Windows environments, it uses a modular plugin architecture for easy updates and functionality extension. This group uses of a custom encryption algorithm based on a modified RC4 cipher for command and control (C2) communications which demonstrates their commitment to evading detection. Whisper's capabilities, including file operations, screenshot capture, and arbitrary command execution, provide them with extensive control over compromised systems.

The group's infrastructure management is equally impressive. They leverage compromised WordPress sites as initial staging servers and employ multi-layered proxy networks to obscure their true C2 locations. They practice regular rotating of IP addresses and domains, often on a weekly basis, which complicates tracking efforts. Recent observations indicate an evolution in Wirte's tactics, including an increased focus on supply chain attacks, experimentation with zero-day exploits in VPN solutions, and the use of AI-generated content in phishing campaigns to enhance credibility.

## **References**

MITRE ATT&CK. (2024). "WIRTE, G0090." <https://attack.mitre.org/groups/G0090/>