APT18 Threat Group Report

Overview

- **APT18** is a cyber threat group active since at least **2009**, known for targeting various industries such as:
  - Technology
  - Manufacturing
  - Human Rights Groups
  - Government
  - Medical Sectors
- **Aliases**: TG-0416, Dynamite Panda, Threat Group-0416
- **ID**: G0026
- **First Identified**: May 31, 2017
- **Last Updated**: April 11, 2024

Tactics, Techniques, and Procedures (TTPs)

Domain	Technique ID	Name	Details
Command & Control	T1071.001	Application Layer Protocol: Web Protocols	APT18 uses **HTTP** for Command and Control (C2) communication.
Command & Control	T1071.004	Application Layer Protocol: DNS	APT18 uses **DNS** for C2 communication.
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Establishes persistence via the registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Uses **cmd.exe** to execute commands on victim systems.
Persistence	T1133	External Remote Services	Leverages legitimate credentials to access remote services.
Discovery	T1083	File and Directory Discovery	Lists file information in specific directories.
Defense Evasion	T1070.004	Indicator Removal: File Deletion	Deletes tools and batch files from victim systems.
Execution	T1105	Ingress Tool Transfer	Transfers files to victim systems.
Defense Evasion	T1027.013	Obfuscated Files or Information: Encrypted/ Encoded File	Obfuscates payload strings to avoid detection.
Execution	T1053.002	Scheduled Task/Job: At	Uses the **Windows Task Scheduler** (`at.exe`) to execute scheduled tasks on victim networks.
Discovery	T1082	System Information Discovery	Collects system information from victim systems.
Defense Evasion	T1078	Valid Accounts	Leverages legitimate credentials to access external remote services.

Software Used by APT18

ID	Name	Capabilities
S0106	**cmd**	Executes commands, discovers files, transfers tools, deletes indicators, collects system information.
S0032	**gh0st RAT**	Keylogging, system discovery, registry modification, file discovery, DLL side-loading, encrypted communications.
S0071	**hcdLoader**	Executes Windows commands and creates/modifies system processes.
S0070	**HTTPBrowser**	Supports DNS/Web protocols for C2, file discovery, obfuscation, and indicator removal.
S0124	**Pisloader**	Supports DNS C2, task scheduling, obfuscation, and system discovery.

Key Observations

- **C2 Mechanisms**:
  - Reliance on **HTTP** and **DNS** protocols for covert communication.
  - DNS requests are particularly leveraged as a stealth mechanism.
- **Persistence Techniques**:
  - Uses registry run keys and startup folders for consistent access.
  - Scheduled tasks are employed for repeated execution.
- **Defense Evasion**:
  - Deletes artifacts and uses obfuscation techniques to evade detection.
  - Legitimate credentials are abused for external services, blending malicious activity with normal behavior.

References

1. Carvey, H. (2014). Indicators of lateral movement using `at.exe`.
2. Shelmire, A. (2015). Evasive maneuvers by Wekby group.
3. Grunzweig, J. et al. (2016). DNS requests as command and control mechanisms.
4. Adair, S. (2017). Advanced threats in Exchange environments.
5. Grunzweig, J. et al. (2016). Fast flux DNS tactics by APT18.

Conclusion

APT18 is a sophisticated threat group that employs advanced tactics and custom tools to target critical sectors. Its ability to blend into normal network activity and evade detection highlights its advanced capabilities. Organizations should prioritize monitoring DNS communications, registry modifications, and use of scheduled tasks to detect and mitigate threats from APT18 effectively.