Contents

[**Magic Hound (G0059)** 2](#_Toc179441735)

[**I. Introduction** 2](#_Toc179441736)

[**II. Tactics** 2](#_Toc179441737)

[**III. Techniques** 2](#_Toc179441738)

[**IV. Procedures** 3](#_Toc179441739)

[**V. Summary** 4](#_Toc179441740)

[**References** 5](#_Toc179441741)

## **Magic Hound (G0059)**

## **I. Introduction**

Magic Hound, which is also known as APT35, Newscaster Team, Charming Kitten, and Phosphorus, is an Iranian state-sponsored advanced persistent threat group that has been active since at least 2011. This group is known for its focus on espionage and data theft. It primarily targets organizations and individuals of strategic interest to the Iranian government, which include government entities, defense contractors, academic institutions, and dissidents.

## **II. Tactics**

This group’s tactical approach is characterized by

1. ***Social Engineering***

It Heavily relies on advanced social engineering techniques to manipulate targets into compromising their security.

1. ***Credential Harvesting***

Its campaigns focus on obtaining login credentials for various services, particularly email accounts and social media platforms.

1. ***Long-term Intelligence Gathering***

Magic Hound continuously tries to collect sensitive information related to geopolitical interests, military capabilities, and rebel activities.

1. ***Impersonation***

This threat group frequently uses of fake personas and impersonates trusted entities to gain victims' trust.

1. ***Multi-platform Targeting***

Its operations span across several platforms, which include Windows, macOS, Android, and iOS devices.

## **III. Techniques**

Magic Hound uses a range of techniques in their operations

|  |  |
| --- | --- |
| Spear-phishing Campaigns (T1566) | Use of highly targeted emails with malicious attachments (T1566.001).  Employment of phishing links leading to credential harvesting pages (T1566.002). |
| Social Media-based Attacks | Creation of elaborate fake personas on platforms like LinkedIn for network building and target engagement. |
| Malware Deployment | Use of custom malware families such as Infy, POWERSTATS, and TURNEDUP.  Deployment of mobile malware for iOS and Android devices. |
| Command and Control (C2) Infrastructure | Use of compromised websites for C2 communication (T1102.002).  Leveraging of legitimate cloud services for C2, including Google Drive and Microsoft OneDrive (T1102.002). |
| Credential Access | Development of convincing phishing pages mimicking legitimate login portals (T1056.003).  Use of keyloggers to capture user credentials (T1056.001). |
| Persistence | Creation of scheduled tasks for periodic malware execution (T1053.005).  Use of Windows Registry run keys for persistence (T1547.001). |
| Defense Evasion | Obfuscation of PowerShell scripts to evade detection (T1027.009).  Use of legitimate services to blend C2 traffic (T1071.001). |

## **IV. Procedures**

Its typical attack chain follows this sequence

***1. Initial Access***

a. Highly targeted spear-phishing emails are sent, often impersonating trusted entities or individuals.

b. Emails contain either malicious attachments or links to credential harvesting sites.

c. In some cases, targets are engaged through fake social media profiles over an extended period.

***2. Execution***

a. If a malicious attachment is opened, it typically exploits vulnerabilities in common software like Microsoft Office.

b. For credential harvesting, victims are directed to convincing phishing sites that mimic legitimate login pages.

***3. Persistence and Privilege Escalation***

a. Once executed, malware establishes persistence through scheduled tasks, registry modifications, or other methods.

b. The group attempts to elevate privileges, often through known vulnerabilities or by exploiting misconfigurations.

***4. Discovery and Lateral Movement***

a. Magic Hound conducts network reconnaissance to identify high-value targets and sensitive data.

b. Lateral movement is achieved using stolen credentials and by exploiting network vulnerabilities.

***5. Collection and Exfiltration***

a. Sensitive documents, emails, and other data of interest are identified and collected.

b. Data is exfiltrated through various channels, often disguised as legitimate traffic to cloud services.

***6. Ongoing Operations***

a. Magic Hound maintains long-term access to compromised accounts and networks for continuous intelligence gathering.

b. They regularly update their tools and techniques to evade detection and maintain persistence.

## **V. Summary**

Magic Hound provides some valuable context around the nation’s cyber espionage priorities and capabilities. Their political operations are similar to Iran's geopolitical interests because this group focuses especially on gathering intelligence about foreign policies, the defense capacity, and internal insurgents.

The group excels at creating detailed fake online personas, and they often maintain these identities for years to build trust with potential targets. This long-term strategy has proven highly effective in compromising high-value targets. In addition, Magic Hound focuses on mobile device compromise by developing malware for both iOS and Android platforms. This includes creating fake secure messaging apps.

The group also exploits legitimate cloud services like Google Drive and Microsoft OneDrive for command and control, which allows its malicious traffic to pop right in front of the user. Instead, the focus of their attention is on side stepping 2FA (two factor authentication) mechanisms through the use of advanced phishing kits that can capture 2FA codes in real time, which reveals the ongoing cat and mouse game between them and the defender in authentication.

## **References**

5. MITRE ATT&CK. (2024). "Magic Hound, G0059." <https://attack.mitre.org/groups/G0059/>