

APT33 Threat Actors

 branddefense.io/blog/apt-groups/apt33-threat-actors/

August 18, 2022

Introduction

Iran-based APT33 is a cyber threat group known to have been actively engaged in espionage since 2013. The primary targets of APT 33 threat actors, also known as **Elfin**, **Holmium**, **Magnallium**, and **Refined Kitten**, have been institutions/organizations serving in various sectors in Saudi Arabia and the USA. However, it has been observed that other countries, especially South Korea, Belgium, Jordan, and the United Kingdom, were also targeted in the attacks carried out by APT 33 threat actors.

In this context, the campaigns carried out by APT33 threat actors, the malware used, techniques, tactics, and procedures are discussed, and it aims to raise awareness among the readers against possible attacks that the said group may carry out.

Group's Mission and Vision

APT33 is a nation-state-based threat actor whose actions are linked to the targets of the Islamic Revolutionary Guard Corps of Iran (IRGC) and has been conducting espionage-focused operations since at least 2013. Although intelligence gathering is the main focus of APT33 threat actors, attacks with the devastating Shamoon malware are also associated with APT33 threat actors.

APT33 uses both specially developed and open-source remote access tools (RAT) to obtain intelligence from targets. However, recent attacks have also observed that APT33 threat actors use open-source malware families such as PoshC2 and PowerShell Empire.

Countries and Industries Targeted by APT33 Threat Actors

Operations carried out by APT33 threat actors are known to target the following countries/regions;

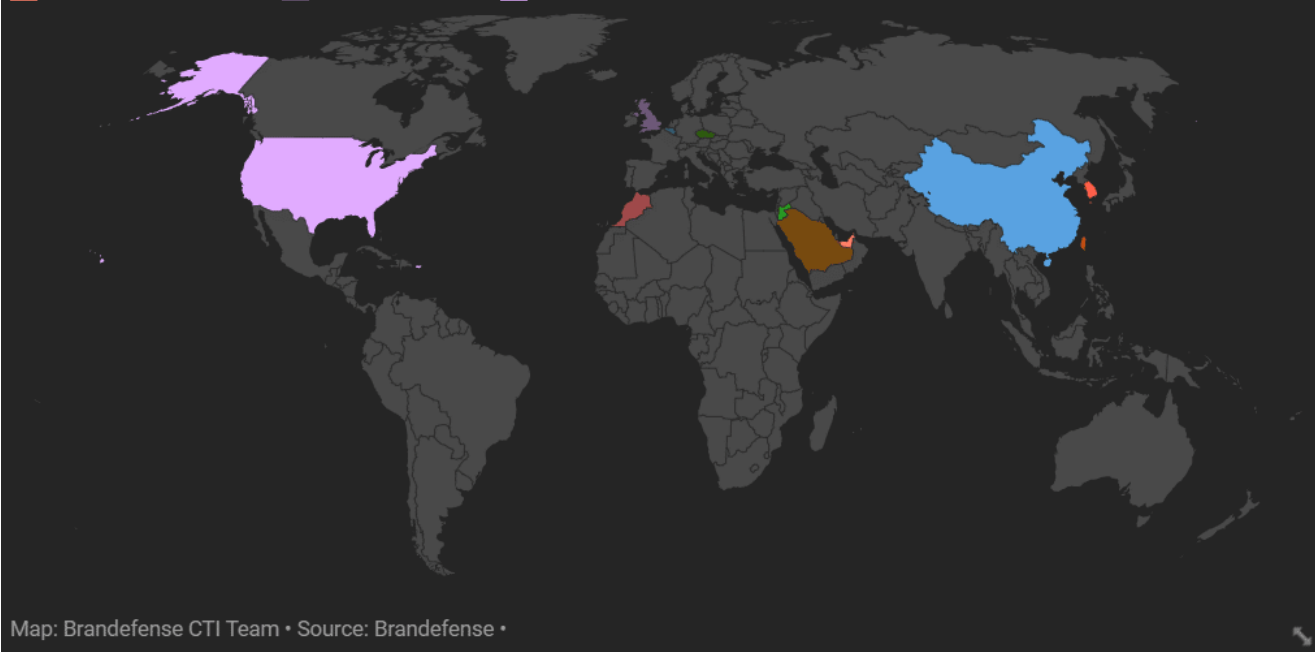
- United States of America,
- UAE,
- Belgium,
- United Kingdom,
- Morocco,
- South Korea,
- Saudi Arabia,
- Thailand,

- Czech Republic,
- Chinese,
- Jordan.

Targeted Countries by APT 33

Countries targeted in attacks by APT 33

■ Belgium ■ China ■ Czech Republic ■ Jordan ■ Morocco ■ Republic of Korea ■ Saudi Arabia ■ Taiwan
■ United Arab Emirates ■ United Kingdom ■ United States of America



Sectors/Industries Targeted by APT33 threat actors;

- Research Institutions,
- Information Technology,
- Consultancy,
- Education,
- Aviation,
- Government Institutions,
- Chemical,
- Logistics,
- Engineering,
- Finance,
- Retail,
- Defense,
- Health,
- Telecommunications,
- Production Technologies.

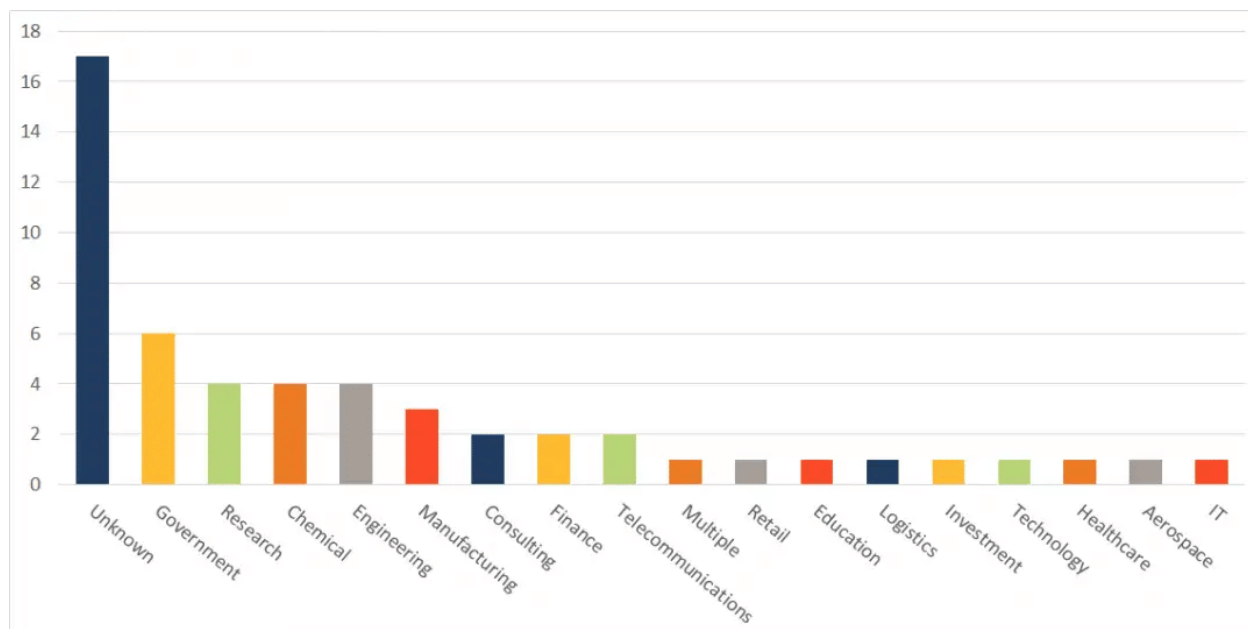


Figure 2: Sectors/Industries Targeted by APT33

Operations/Campaigns Performed by APT33

Most attacks by APT33 focus on organizations located in Saudi Arabia. However, many US-based organizations, including numerous Fortune 500 companies, have also been targeted by threat actors.

Between 2016-2017, APT33 targeted various aerospace-related organizations. At the same time, the group also sought to endanger organizations in the petrochemical sector. The primary vector in attacks involves the distribution of spear phishing emails with a malicious file attachment. The possible reason behind aviation and space targeting is the assumption that Iran's aviation capabilities are enhanced.

Another campaign that took place during this time targeted Saudi Arabian government agencies using two different attack vectors, both phishing and waterhole attacks.

In the operations carried out between 2017-2018, APT33 threat actors targeted the engineering sector. In these operations, the e-mail client of the targets was manipulated through compromised credentials and an open source tool. The identity information of the targets is obtained through third-party breaches, credential collection scams or weak password usage. Additionally, threat actors use an open-source tool that exploits the vulnerability CVE-2017-11774 to download and execute malware used in campaigns on targeted systems.

In another campaign carried out in February 2019 and attributed to APT33, a chemical company serving in Saudi Arabia was targeted. In the detected spear phishing attempt, threat actors sent users a compressed file that would exploit a known security vulnerability

(CVE-2018-20250) when opened. This file led to the execution of additional code that would include downloading malware from an external location.

A password spraying, otherwise known as Brute Force, campaign associated with APT33 has been observed targeting cloud-hosted infrastructure of various industries from mid-June 2019 to October 2019. Industrial control system vendors were among the most targeted sectors in these campaigns.

Two more targeted phishing campaigns were observed in June 2019. The first targets various US entities in the federal government. The second targeted phishing campaign targets financial institutions in the Middle East and the USA. In these campaigns used documents containing malicious macros responsible for distributing malware used by APT33 in the past.

Most recently, in August 2019, APT33 manipulated domain names associated with US defense contractors in phishing attacks to infect targeted systems with malware.

Malware and Tools Used by APT33

In the campaigns carried out by APT33, spear-phishing e-mails are generally used as a malware delivery method. These phishing emails contain malicious documents and links to malicious files hosted on the threat actors' infrastructure. However, in more recent campaigns, it has been observed that APT33 threat actors use tools that allow manipulation of email clients through the captured credentials of the targets. APT33 has an extensive arsenal of malware to exploit for their operations. Some of these malicious software are:

TURNEDUP: It is a backdoor capable of downloading and uploading files, collecting information about the target system and creating a Reverse Shell.

SHAPESHIFT (STONEDRILL): It is a backdoor capable of downloading additional files and deleting disks, volumes, and files depending on its configuration.

DROPSHOT: A malware responsible for dropping and executing tools like TURNEDUP and SHAPESHIFT on the targeted system.

POWERTON: It is a special PowerShell-based back door, first observed in 2018.

In addition to the special malware they developed, APT33 threat actors also use much malware available from underground platforms such as **Remcos RAT**, **Quasar RAT**, **DarkComet RAT**, **Pupy RAT**, **NetWeird**, and **PoshC2** in their campaigns.

Technicals, Tactics and Procedures (TTP's) Used by APT33

MITRE ATT&CK is an open knowledge base of threat actors' techniques, tactics, and procedures. By observing the attacks that occur in the real world, the behavior of threat actors is systematically categorized.

MITRE ATT&CK aims to determine the risks against the actions that the threat actors can take in line with their targets and make the necessary improvements and plans.

The table below details the technical tactical procedures (Mitre Att&ck) used by APT33 threat actors.

Tactic	Technic ID	Technic Name
Initial Access	<u>T1078</u>	Valid Accounts
Execution	<u>T1203</u>	Exploitation for Client Execution
Persistence	<u>T1078</u>	Valid Accounts
Privilege Escalation	<u>T1480</u> <u>T1078</u>	Execution Guardrails Valid Accounts
Defense Evasion	<u>T1562</u> <u>T1027</u>	Impair Defences Obfuscated Files or Information
Credential Access	<u>T1555</u> <u>T1040</u>	Credentials from Password Stores Network Sniffing
Discovery	<u>T1040</u>	Network Sniffing
Command & Control	<u>T1544</u> <u>T1571</u>	Ingress Tool Transfer Non-Standard Port

Mitigations && Recommendations

In this content, the methods used by APT33 threat actors in their initial access to target systems and in the processes after gaining access are discussed. When the encountered cases were examined, it was seen that the group mostly used phishing attacks to gain first access and took advantage of the vulnerabilities in the existing systems. In this context, precautions should be taken by considering the attack vectors used in order to be protected from attacks that may be carried out by APT33.

Important recommendations to be implemented to protect assets in the digital world and to minimize the risk of exploitation arising from security vulnerabilities and device configuration are shared below.

- Suspicious emails and links from unknown sources should not be trusted.
- Regular backups of systems, programs and files should be made.
- In many campaigns, it is seen that intrusions provided by threat actors are caused by security vulnerabilities existing in the system. Operating systems, applications and programs used in this context should be kept up to date.
- Institution/organization personnel should be aware of the social engineering or phishing threats used in these campaigns so that they do not put themselves and the institutions they belong to at risk.
- The login information should be created using strong policies, and MFA/2FA features should be enabled and used on all possible platforms.
- It is important to download files or programs from legitimate and reliable sources.
- Signature-based security solutions should be used to identify network traffic generated by malicious software. (IDS/IPS)
- Where remote access is required, secure methods such as VPN should be used.
- Finally, it is recommended that IoC findings associated with the APT group in question be blocked from security devices in use.