Motivation of APT33: Iranian Cyber Operations

By Kieren Gregory

4/27/2025

Cyber War Gaming

Dr.Dustin Mink

Abstract

The Iranian government is known for creating the advanced persistent threat known as APT 33. APT33 is related and associated with espionage and destruction targeting defense, energy, and the critical infrastructure of other nations. This case study looks at the driving forces and motivation behind APT33's malicious capability, reviewing the stages of a well organized cyber operation using the MITRE ATT&CK framework.Through analysis of Iranian motivation it is discovered APT33's activities help Iran achieve its political goals of disruption, retaliation, and advantageous gains in the Middle East. The below findings help establish Iran's use of APT33 is classified as digital statecraft showcasing how each stage of a cyber operation, from initial access through the outcome is created with strategic goals to disrupt infrastructures of other nations.

Introduction

APT33, also known as Refined Kitten, is one of the most active Iranian threat organizations. APT33 has been active since 2013 and has mostly targeted organizations in the US, Saudi Arabia, and South Korea. The APT33 strictly focuses on concentrating industries vital to national security such as defense contracts, chemicals, and aviation. High-profile attacks attributed to APT33, such as those using the Shamoon disk wipe virus, have shown Iran’s capacity to partake in harmful cyber campaigns alongside more traditional espionage operations [1]. This case study evaluates the reason foreign cyber campaigns exist and their motivations, moving from technical analysis to Iranian geopolitics rooted in their motive.

Literature Review

APT33 is identified as G0064 in the MITRE ATT&CK threat group database [1]. The group engages in damaging attacks, spear-phishing tactics, and developing proprietary malware. The operational endurance and technological properties of APT33 efforts are extensive in reports from Palo Alto's Unit 42 and FireEye [2][3]. Based on malware samples, targeting patterns, and command and control infrastructure, FireEye's first profile of APT33 in 2017 linked the group to Iran. The group's emphasis on companies engaged in oil production, essential infrastructure, and aviation was described further in depth within later studies. Although a large section of material lists the group's tactics, techniques, and procedures, there exists a lack of information of the strategic motivations behind APT33's operation. Most studies explain how APT33 carries out the cyberattack, but don't look into why specific targets are chosen or how the cyber strategies support Iran's larger military, political, and economic objectives. Therefore, the following is the research question for this study: What drives APT33's cyber operations, and how do their objectives come to fruition at each stage of a well organized cyber operation as defined by MITRE ATT&CK? A close up examination of this issue provides information about APT33's activities along with Iran's usage of cyberspace as a national strategic tool.

Methodology

Based on document analysis of publicly accessible intelligence reports, MITRE ATT&CK data, and studies on Iranian cyber activity, this study employs a qualitative case study methodology. The steps in the research process are outlined in Figure 1. The first step is determining APT33 campaigns by reviewing the literature. The second step is looking at matching APT33 actions to MITRE ATT&CK strategies. The final step is examining how each strategy supports an Iranian strategic objective. The objectives are espionage, revenge and sabotage.

The hypothesis in question asks how APT33's efforts have a purposeful framework for a cyber operation. Each MITRE ATT&CK phase is chosen to directly support Iranian goals rather than exploring the technical side of things. With its concentration on intrusion steps, the Lockheed Martin Cyber Kill Chain differs from the MITRE ATT&CK framework, which delivers a more thorough, practical perspective of threat behavior spanning 14 operational methods, from first access to ultimate impact.

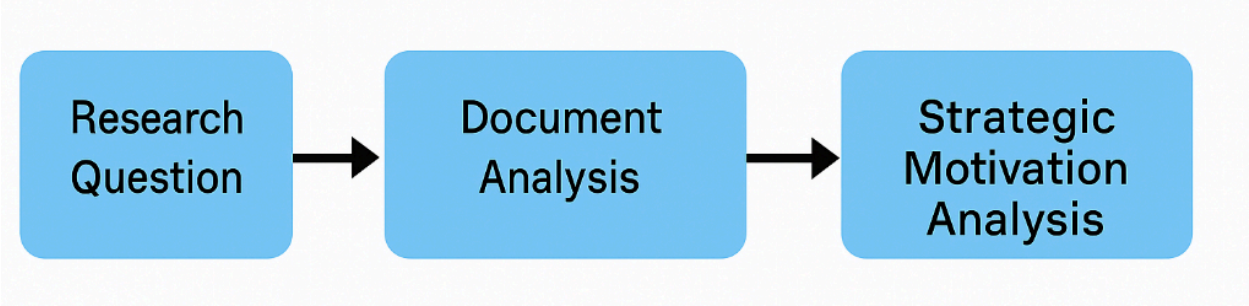

Figure 1. Research Process Model for Analyzing APT33 Cyber Operations.

The case study methodology involves a four step approach. The study starts by forming a research topic on the driving motive behind APT33's cyber operation. Second, information gathered via academic research, cybersecurity frameworks via MITRE

ATT&CK, and document analysis of intelligence reports. Third, looking at the perspective on APT33's strategies within the cyber operation stages, the methods and behaviors map to the MITRE ATT&CK framework. When understanding how each phase contributes to Iranian national security, the data becomes analyzed for strategic premeditation. In regards to nation state cyber operations, this methodology guarantees a thorough comprehension of technical aspects along with nation goals.

Results

The analysis below looks at how APT33's strategies fit into the MITRE ATT&CK framework at various stages of their cyber operations. APT33 first enters target environments by utilizing advanced spear-phishing techniques. These communications are designed to mimic human resources departments in the aviation industry with the intention of misleading workers in core industries essential to the economies of geopolitical competitors like Saudi Arabia [2]. After successful delivery, APT33 uses macro-enabled files to reduce the chance of early detection during initial infiltration by running malicious scripts contained within Microsoft Office documents. APT33 creates registry keys for autorun execution, implants custom malware like TurnedUp, and creates implants that can survive system reboots to remain persistent in infiltrated situations [1]. By taking advantage of flaws in widely used programs, such as Adobe Flash Player and Microsoft Office, privilege escalation enables the gang to increase its access and control within victim networks [3]. Throughout operations, defense evasion is a top priority. To get beyond endpoint security, APT33 hashes payloads utilizing techniques such as Base64 encoding. Another major goal of APT33 is establishing

access to elevated credentials to gain unauthorized access. Iranian cyber operations obtain present employee passwords utilizing keyloggers such as DropShot. This program allows secretive evasive movements within the targeted network environment [2]. After initial entry, APT33 maps the internal network architecture by performing system and network discovery. Within the discovery, the presence of important data such as data repositories or critical files can be leaked and dumped by using specific commands. In efforts to lessen and minimize detection, APT33 establishes persistence while spreading across the target network using stolen credentials and tools like PsExec [3]. When it comes to command and control, APT33 uses HTTPS encryption to help establish links to Iranian officials and websites. The high standard of operational security is made using remote access entry, facilitating longer times of entry unlike channels that are dependent on elements often seen in IRC [1]. After APT33 completes network mapping and reconnaissance, private information of the targeted network is sought after. This information includes confidential documents, trade secrets, aviation secrets, and defense strategies. To evade detection and information transmission to Iran backed servers, the dumped files are compressed and use encryption via secret communication channels. APT33 also utilizes destructive malware tools like Shamoon to corrupt and destroy as much of the target network infrastructure as possible. The destruction was evident when Saudi Arabian companies disclosed substantial financial losses from the nature of an APT33 cyberattack. The cyberattack left the targeted company's hard drives fried and employee computers were left unusable [2]. It is important to note every stage of APT33 cyber operation shows a methodical approach with Iranian goals of achieving economic imbalance, destruction and retaliation.

Table 1. APT33's Techniques Mapped to MITRE ATT&CK

Tactic	Technique	Behavior
Initial Access	Phishing (T1566.001)	Fake job offers
Execution	Scripting (T1059)	PowerShell macros
Persistence	Autostart Execution (T1547)	TurnedUp backdoor
Defense Evasion	Obfuscated Files (T1027)	Base64 payloads
Credential Access	Keylogging (T1056.001)	DropShot malware
Lateral Movement	Remote Services (T1570)	PsExec usage
Impact	Disk Wipe (T1561.002)	Shamoon malware

Conclusion

The results of this case study provide compelling evidence that APT33 does not act opportunistically but with intentional, strategic intent. APT33's attacks clearly show long term planning, sector-specific targeting, and a strong understanding of operational security, in contrast to financially driven threat groups that prioritize short-term benefits. Their behaviors are consistent with Iranian geopolitical goals when their conduct maps across the MITRE ATT&CK framework. Every stage of APT33's cyber operation, spear-phishing for initial access and escalating movement utilizing authentic credentials to data exfiltration, is a coordinated effort to accomplish national strategic objectives. The actions of APT33 benefit the Iranian government in several interconnected ways. Iran's espionage operations make it possible to obtain confidential technical data, which aids Iran in catching up with its regional and western competitors in terms of technology. Iran can respond against enemies like Saudi Arabia without resorting to military warfare

by using harmful software like Shamoon for economic disruption. This study emphasizes a critical aspect of cyberwarfare. This aspect is the necessity of assessing nation state cyber threats utilizing more than solely a technical analysis approach. For national defense and policy planning, the best approach is learning how to comprehend organizations like APT33 infiltrate networks, it is even more important to comprehend why. Defenders who react to the newest malware signatures or zero day exploits run the risks of failing to see the bigger strategic picture, in which cyber operations are becoming increasingly used within the military, economics, and geopolitical competition. Technical activities are also driven by strategic intent and when technical aspects are properly understood, underlying objectives become clear. Furthermore, operational security can become compromised from credential harvesting and escalation attempts. These attempts leave long lasting weaknesses Iran can eventually take advantage of. The initiatives above symbolize the role in the Iranian cyber attack methodology within their operations. Understanding their methodology is important in light of Iran's continued sanctions from the international community and military limitations within the country itself. In conclusion, APT33 is a well round example of how a nation state sponsored cyber operation has become effective in utilizing tools in aims of disrupting other countries. The cyber campaign of APT33 was planned to project the power of Iran and their capabilities to protect their nation, punish adversaries, gather foreign intelligence and employ strategic advancements any way possible. It is important to understand the level of intent of cyber terrorist organizations utilizing methods like APT33. Through understanding the intent and function of such threats, it will help other nations defend and protect their assets in the international world. APT'S of all

backgrounds are an increased risk in the world of cyberspace. This case study emphasizes the importance of a strategic approach to assessing threats such as APT33, combining technical detection backed by strategic intelligence.

References (IEEE)

[1] MITRE ATT&CK, "APT33," MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org/groups/G0064/

[2] FireEye, "Iranian APT33 Targets Aviation and Energy Sectors," FireEye Threat Research, Sep. 2017. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/09/apt33-threat-group.html

[3] Palo Alto Networks Unit 42, "OilRig and Iranian Threat Landscape," Unit42 Blog, 2019. [Online]. Available: https://unit42.paloaltonetworks.com/tag/apt33/

[4] U.S. Department of Homeland Security, "Alert (AA19-339A): Iranian Cyber Threats," CISA, Dec. 2019. [Online]. Available: https://www.cisa.gov/news-events/alerts/2019/12/05/iranian-cyber-threats

[5] Mandiant, "APT33: The Iranian Threat Group's New Infrastructure & Evasion Tactics," Mandiant Intelligence, 2021. [Online]. Available: https://www.mandiant.com/resources/blog/apt33-infrastructure-evasion