[redacted]

[redacted] Issues Arising from Sustained Iranian Cyber Attack Campaigns Against U.S. and Global Financial Sector Targets

Between 2010 and at least 2016, a series of sustained cyber attacks attributed to Iran disrupted U.S., Saudi, regional Middle Eastern, and other global financial sector networks.

The core of the campaign, between 2012 and 2014, was dubbed "Operation Ababil" as a result of significant hostile information operations messaging.

Multiple response options were employed to remediate the effects of the attacks, including intelligence & information sharing, incident response efforts, unattributed third party offensive cyber operations against attackers' botnet infrastructure, and eventual delayed criminal indictment of Iranian nationals involved in the attacks.

USG response was reportedly constrained by other national policy priorities, but at the cost of imposing the bulk of defensive responsibility directly on the private sector.

Overview

In the early part of this decade, a sustained disruptive campaign targeting US, Middle East region, and global networks through intermittent distributed denial of service (DDOS) cyber attacks known commonly as "Ababil."[1] These attacks resulted in significant impact to the financial sector, with additional victimization of energy, oil & gas and other extractive, and aviation sector enterprises. The campaign has been attributed by the US government to the government of the Islamic Republic of Iran.

Context

It has been argued that the Ababil campaign was intended as retaliation against alleged US and allied sabotage against the Iranian nuclear and missile programs disclosed in Western press reporting following the discovery of the malware known as Stuxnet. However, attack incidents predate this disclosure. When viewed in totality, it may instead be hypothesized that the Iranian government pursued these cyber attacks to push back on increasing attempts to isolate the Islamic republic from the international financial system - particularly given the rising domestic costs of the then ongoing effects of economic sanctions.

Private sector enterprises continue to believe that they were forced to respond to these attacks almost entirely alone, with limited if not ineffective assistance provided by the US government. While some observed interventions by unknown third parties may have contributed to degradation of adversary botnet infrastructure used in the attacks, the private sector's own capacity for resilience and defensive innovation was almost certainly the decisive factor leading to the eventual defeat, and strategic irrelevance, of the Iranian campaign. US policymakers were thus able to reportedly de-prioritize response to the Ababil attacks in favor of continued pursuit of wider regional diplomatic objectives, including the then ongoing P5+1 negotiations that eventually led to the Joint Comprehensive Plan of Action (JCPOA).

[1] This summary case study is adapted directly from prior academic analysis, in JD Work. "Echoes of Ababil: Re-examining formative history of cyber conflict and its implications for future engagements". Society of Military History Annual Conference, Columbus, Ohio. 9-12 May 2019.

[redacted]

[redacted]

Significant events

A series of DDOS attacks were first noted against a range of Saudi Arabian business entities in late April and early May 2010. These targets were unlikely to have been selected for extortion demands, and no other monetization options appear to have existed that would have driven criminally motivated attacks. The targeted enterprises were led by some of the most prominent businessmen in the Kingdom, and had close connections with Saudi royal family figures. Ongoing DDOS attacks would continue and escalate against a variety of Saudi targets through late 2010, including targeting firms involved energy, mining, oil & gas, and construction projects on behalf of the Kingdom's sovereign wealth investments. The attack campaign would subsequently quickly expand to include these investment entities, as well as other financial sector targets in the country, and intermittently continue through September 2011. The incidents were initially unattributed. Although the botnet infrastructure used to deliver attack effects had been tracked by commercial cyber intelligence services, the infrastructure was known to be run by a suspected Russian contract DDOS service operator offering "hacker for hire" services to underground customers on paid basis. Contemporaneous assessment indicated that these incidents were intended for political objectives, in the absence of criminal monetization options. The government of Saudi Arabia was reportedly initially unaware of these events due to its limited national cybersecurity capacity, and when warned treated the matter as a topic of political sensitivity. This likely attenuated the signaling value of the offensive operation and blurred any messaging objectives sought by adversary operators. As a result, no reaction – official or informal – is known during this period.

New DDOS attacks directly against Saudi government targets would be identified in the summer of 2012. These incidents differed in tooling and techniques, and were publicly claimed under the Anonymous hacktivist brand. However, Anonymous operations in this period were executed by loosely affiliated independent hackers that could claim any action under the wider (and generally inchoate) ideology of the group. The ability to make such claims without prior coordination and using only a simple anti-authoritarian narrative was abused by Iranian hackers, including individuals that had been arrested and subsequently recruited by Iran's Ministry of Intelligence and Security (*Vezarat-e Ettela'at Jomhuri-ye Eslami-ye*, MOIS) in connection with events during the Green Movement unrest (or, as it was known in Iran, the 1388 sedition). Several of the individuals involved in these operations would allegedly later emerge as key contractors, providing further offensive cyber capabilities to the Iranian Revolutionary Guards Corps. These operators would naturally leverage prior understanding of the Anonymous collective, and its global hacktivist allies, in developing social engineering and deception tradecraft to hide their activities under hacktivist personas as a (mis)attribution front when executing intrusion and attack against neighboring countries, including Israel and Saudi Arabia.

IRGC offensive cyber operators would acquire new DDOS implant tooling from the Russian criminal underground marketplace, and deploy this new malware in a global infection campaign targeting weakly secured enterprise servers with high bandwidth internet connections. The resulting botnet infrastructure has been dubbed Brobot / Toxin / Kamikaze by Western security industry researchers. The Brobot framework would encompass multiple specific attack scripts deployed at varying points throughout the campaign, as the adversary continued to develop new capabilities and continued to attempt to defeat countermeasures deployed by security services supporting industry targets. Servers compromised for the aggregated Brobot infrastructure were exploited through contemporaneously disclosed vulnerabilities in common content management systems. Specific vulnerabilities targeted would shift throughout the ongoing campaign as operators sought new ways

[redacted]

[redacted]

to refresh and sustain infrastructure, developing additional 1-day exploit options throughout the period to target unpatched victims.

This new infrastructure would be used in initial small scale attacks, assessed to be live fire testing, targeting Iranian information technology and telecom infrastructure (likely as a controlled operational test and evaluation), and then against a major Saudi oil and energy sector firm in August 2012 (which may be seen as a live fire demonstration). Concurrent ongoing attacks from legacy hacker for hire infrastructure continued to be observed during this time. Operators would begin larger scale attacks in September 2012 across multiple Saudi financial sector targets, leveraging both legacy and newer Brobot capabilities.

From September 2012, the campaign would expand to target major US and global financial institutions – predominantly relying on the Brobot infrastructure. Credit for the ongoing DDOS attacks would be under the name "martyr Izz ad-Din al-Qassam Cyber Fighters Group" claimed through multiple social media channels. The group would call its actions "Operation Ababil," in a reference to the warning by fifth Abbasid Caliph Harun al Rashid (766-809 AD) against "crusader" states of Byzantium. The attackers sought to deliberately invoke an Islamic tradition for their actions, in reference to the legendary *tairan ababil* (flocks of birds) that are said to have protected Mecca from an advancing Christian army in 570 AD by dropping hellfire stones of clay and brimstone on the heads of the attackers. The multi-year core Ababil campaign resulted in more than 350 separate attacks against over 50 financial institutions. Initial attacks leveraging the Brobot infrastructure were highly successful, and reportedly resulted in continuing disruption of multiple targets based on the then-exceptionally high malicious traffic volumes directed against victim networks.

US officials later estimated the cost of the attacks to be in the "tens of millions of dollars," although the estimates to date are generally not as reliable as might be expected, making the full costs difficult to quantify.

[redacted]