State of the Hack: Spotlight Iran - from Cain & Abel to full SANDSPY

Published: 2020-01-17 · Archived: 2026-04-05 12:38:02 UTC

In response to increased U.S.-Iran tensions stemming from the recent death of Quds Force leader Qasem Soleimani by U.S. forces and concerns of potential retaliatory cyber attacks, we're bringing the latest from our front-line experts on all things Iran. Christopher Glyer and Nick Carr are joined by Sarah Jones (@sj94356) and Andrew Thompson (@QW5kcmV3) to provide a glimpse into Iran-nexus threat groups - including APT33, APT34, APT35, APT39, and TEMP.Zagros - as well as the freshest actionable information on suspected Iranian uncategorized (UNC) groups that are active right now. We get right into it with a picture of Iranian compromise activity from just a few years ago - what we observed and the basic, cookie-cutter approach to their intrusions - and then begin to walk through the stark contrast to their TTPs today. We discuss how and why their Computer Network Operations (CNO) has evolved quickly and provide a detailed walk through all of the graduated Iranian APT groups. Our experts share their experiences with each group, moments in time that surprised or impressed us from Iranian threat actors, and notable shifts in behavior - as well as our standing questions. Iranian intrusion operators have come a long way from DDoS & defacement, basic scanning, Cain & Abel and ASPXspy... to DNS hijacking, social engineering via LinkedIn, information operations, and backdoors like QUADAGENT, SANDSPY, TANKSHELL - then filling in the gaps with the quick adoption of offensive security post-compromise tools and techniques. We close this first episode of season 3 with an overview of actionable mitigations to secure against both Iranian intrusions and several other threats, including disruptive and destructive ransomware attacks. For more information on these mitigations as well as our public source material supporting the discussion from the show, please check out: • APT33 graduation: https://www.fireeye.com/blog/threat-r... https://www.brighttalk.com/webcast/10... • APT33 webinar & examples: https://www.fireeye.com/blog/threat-r... • An example TEMP.Zagros phishing campaign: https://www.fireeye.com/blog/threat-r... • APT35 highlights in MTrends 2018: https://www.fireeye.com/content/dam/c... • Iranian information operations: https://www.fireeye.com/blog/threat-r... • RULER home page usage by Iranian groups & mitigations: https://www.fireeye.com/blog/threat-r... • APT39 graduation: https://www.fireeye.com/blog/threat-r... • Iranian DNS Hijacking (DNSpionage): https://www.fireeye.com/blog/threat-r... • More Iranian influence operations: https://www.fireeye.com/blog/threat-r... • APT34 social engineering via LinkedIn: http://www.fireeye.com/blog/threat-re... • FireEye response to mounting U.S.-Iran tensions: https://www.fireeye.com/blog/products... • U.S.-Iran tensions webinar & mitigations overview: https://www.brighttalk.com/webcast/74...

Source: https://youtu.be/pBDu8EGWRC4?t=2492