Rocket Kitten

Rocket Kitten or the **Rocket Kitten Group** is a hacker group thought to be linked to the Iranian government.[1] The threat actor group has targeted organizations and individuals in the Middle East, particularly Israel, Saudi Arabia, Iran as well as the United States and Europe.

Origins

Cybersecurity firm FireEye first identified the group as **Ajax Security Team**,[2] writing that the group appears to have been formed in 2010 by the hacker personas "Cair3x" and "HUrr!c4nE!". By 2012, the threat actor group turned their focus to Iran's political opponents.[3] Their targeted attack campaigns, dubbed "Rocket Kitten", have been known since mid-2014.[4] By 2013 or 2014, Rocket Kitten had shifted its focus to malware-based cyberespionage.[3]

Security firm Check Point describes Rocket Kitten as an "attacker group of Iranian origin."[1]

Rocket Kitten's code uses Persian language references. The group's targets are involved in defense, diplomacy, international affairs, security, policy research, human rights, and journalism. According to Check Point, the group has targeted Iranian dissidents, the Saudi royal family, Israeli nuclear scientists and NATO officials. Security researchers found that they carried out a "common pattern of spearphishing campaigns reflecting the interests and activities of the Iranian security apparatus."[4] Other researchers determined that Rocket Kitten's attacks bore a similarity to those attributed to Iran's Revolutionary Guards.[4] Intelligence officials from the Middle East and Europe linked Rocket Kitten to the Iranian military establishment.[2] Rocket Kitten favours a Remote Access Trojan,[5] and by 2015, researchers found it was using customised malware.[2]

History

Operation Saffron Rose

Cybersecurity firm FireEye released a report in 2013 finding that Rocket Kitten had conducted several cyberespionage operations against United States defense industrial base companies. The report also detailed the targeting of Iranian citizens who use anti-censorship tools to bypass Iran's Internet filters.[3]

Operation Woolen-Goldfish

Trend Micro identified the Operation Woolen-Goldfish campaign in a March 2015 paper. The campaign included improved spearphishing content.[1]

Oyun

In November 2015, security errors by Rocket Kitten allowed the firm Check Point to gain password-less root access to "Oyun", the hackers' back-end database. They discovered an application that was able to generate personalized phishing pages and contained a list of over 1,842 individual targets.[2][6] Among Rocket Kitten's spearphishing targets from June 2014 to June 2015, 18% were from Saudi Arabia, 17% were from the United States, 16% were from Iran, 8% were from the Netherlands, and 5% were from Israel.[2] Analysts used credentials to access key logs of the group's victims and found that Rocket Kitten had apparently tested their malware on their own workstations and failed to erase the logs from the data files.[6] Check Point identified an individual named Yaser Balaghi, going by Wool3n.H4t, as a ringleader of the operation.[5]

Telegram hack

In August 2016, researchers identified Rocket Kitten as being behind a hack of Telegram, a cloud-based instant messaging service. The hackers exploited Telegram's reliance on SMS verification, comprising over a dozen accounts and stealing the user IDs and telephone numbers of 15 million Iranians who use the software. Opposition organizations and reformist political activists were among the victims.[4]

References

1. ^ *a b c "Rocket Kitten: A Campaign With 9 Lives" (PDF). Check Point. 2015.*
2. ^ *a b c d e Jones, Sam (April 26, 2016). "Cyber warfare: Iran opens a new front". Financial Times.*
3. ^ *a b c "Operation Saffron Rose" (PDF). FireEye. 2013. Retrieved 26 December 2016.*
4. ^ *a b c d Menn, Joseph; Torbati, Yeganeh (2 August 2016). "Exclusive: Hackers accessed Telegram messaging accounts in Iran - researchers". Reuters.*
5. ^ *a b Carman, Ashley (9 November 2015). "Supposed mastermind behind 'Rocket Kitten' APT identified in research paper". SC Magazine US.*
6. ^ *a b Muncaster, Phil (10 November 2015). "Opsec Blunders Expose Rocket Kitten Masterminds". Infosecurity Magazine.*

External links

The Spy Kittens Are Back: Rocket Kitten 2, Trend Micro.

Hacking in the 2010s

Timeline

Major incidents

2010	• Operation Aurora • Australian cyberattacks • Operation ShadowNet • Operation Payback
2011	• DigiNotar • DNSChanger • HBGary Federal • Operation AntiSec • Operation Tunisia • PlayStation • RSA SecurID compromise
2012	• LinkedIn hack • Stratfor email leak • Operation High Roller
2013	• South Korea cyberattack • Snapchat hack • Cyberterrorism Attack of June 25 • 2013 Yahoo! data breach • Singapore cyberattacks
2014	• Anthem medical data breach • Operation Tovar • 2014 celebrity nude photo leak • 2014 JPMorgan Chase data breach • Sony Pictures hack • Russian hacker password theft • 2014 Yahoo! data breach
2015	• Office of Personnel Management data breach • Hacking Team • Ashley Madison data breach • VTech data breach • Ukrainian Power Grid Cyberattack • SWIFT banking hack

2016	• Bangladesh Bank robbery • Hollywood Presbyterian Medical Center ransomware incident • Commission on Elections data breach • Democratic National Committee cyber attacks • Vietnam Airport Hacks • DCCC cyber attacks • Indian Bank data breaches • Surkov leaks • Dyn cyberattack • Russian interference in the 2016 U.S. elections • 2016 Bitfinex hack
2017	• 2017 Macron e-mail leaks • WannaCry ransomware attack • Westminster data breach • Petya cyberattack 2017 cyberattacks on Ukraine • Equifax data breach • Deloitte breach • Disqus breach
2018	• Trustico • Atlanta cyberattack • SingHealth data breach
2019	• Sri Lanka cyberattack • Baltimore ransomware attack • Bulgarian revenue agency hack • Jeff Bezos phone hacking

Hacktivism
Advanced persistent threats
Individuals
Major vulnerabilities publicly disclosed
Malware

2010	• Bad Rabbit • SpyEye • Stuxnet
2011	• Alureon • Duqu • Kelihos • Metulji botnet • Stars
2012	• Carna • Dexter • FBI • Flame • Mahdi • Red October • Shamoon
2013	• CryptoLocker • DarkSeoul
2014	• Brambul • Carbanak • Careto • DarkHotel • Duqu 2.0 • FinFisher • Gameover ZeuS • Regin
2015	• Dridex • Hidden Tear • Rombertik • TeslaCrypt
2016	• Hitler • Jigsaw • KeRanger • MEMZ • Mirai • Pegasus • Petya (NotPetya) • X-Agent

2017	• BrickerBot • Kirk • LogicLocker • *Rensenware* ransomware • Triton • WannaCry • XafeCopy
2019	• Grum • Joanap • NetTraveler • R2D2 • Tinba • Titanium • Vault 7 • ZeroAccess botnet

Retrieved from "https://en.wikipedia.org/w/index.php?title=Rocket_Kitten&oldid=1071589841"