Operation Newscaster

en.wikipedia.org/wiki/Operation_Newscaster

Contributors to Wikimedia projects

Logo designed by *iSIGHT Partners*

"**Operation Newscaster**", as labelled by American firm *iSIGHT Partners* in 2014, is a cyber espionage covert operation directed at military and political figures using social networking, allegedly done by Iran. The operation has been described as "creative",[1] "long-term" and "unprecedented".[2] According to *iSIGHT Partners*, it is "the most elaborate cyber espionage campaign using social engineering that has been uncovered to date from any nation".[2]

ISight's perceptions

A screenshot from *NewsOnAir.org*

On 29 May 2014, Texas-based cyber espionage research firm *iSIGHT Partners* released a report, uncovering an operation it labels "Newscaster" since at-least 2011, has targeted at least 2,000 people in United States, Israel, Britain, Saudi Arabia, Syria, Iraq and Afghanistan.[2][3]

The victims who are not identified in the document due to security reasons, are senior U.S. military and diplomatic personnel, congresspeople, journalists, lobbyists, think tankers and defense contractors, including a four-star admiral.[2][3]

The firm couldn't determine what data the hackers may have stolen.[3]

According to the *iSIGHT Partners* report, hackers used 14 "elaborated fake" personas claiming to work in journalism, government, and defense contracting and were active in Facebook, Twitter, LinkedIn, Google+, YouTube and Blogger. To establish trust and credibility, the users fabricated a fictitious journalism website, *NewsOnAir.org*, using content from the media like Associated Press, BBC, Reuters and populated their profiles with fictitious personal content. They then tried to befriend target victims and sent them "friendly messages"[1] with Spear-phishing to steal email passwords[4] and attacks and infecting them to a "not particularly sophisticated" malware for data exfiltration.[2][3]

The report says *NewsOnAir.org* was registered in Tehran and likely hosted by an Iranian provider. The Persian word "Parastoo" (پرستو; meaning *swallow*) was used as a password for malware associated with the group, which appeared to work during business hours in Tehran[2] as they took Thursday and Friday off.[1] *iSIGHT Partners* could not confirm whether the hackers had ties to the Iranian government.[4]

Analysis

According to *Al Jazeera*, Chinese army's cyber unit carried out scores of similar phishing schemes.[4]

Morgan Marquis-Boire, a researcher at the University of Toronto stated that the campaign "appeared to be the work of the same actors performing malware attacks on Iranian dissidents and journalists for at least two years".[4]

Franz-Stefan Gady, a senior fellow at the EastWest Institute and a founding member of the Worldwide Cybersecurity Initiative, stated that "They're not doing this for a quick buck, to extrapolate data and extort an organization. They're in it for the long haul. Sophisticated human engineering has been the preferred method of state actors".[4]

Reactions

References

1. ^ a b c *Nakashima, Ellen (May 29, 2014). "Iranian hackers are targeting U.S. officials through social networks, report says". The Washington Post. Retrieved March 30, 2015.*
2. ^ a b c d e f g h i *Finkle, Jim (May 29, 2014). Tiffany Wu (ed.). "Iranian hackers use fake Facebook accounts to spy on U.S., others". Reuters. Retrieved March 30, 2015.*
3. ^ a b c d *Chumley, Cheryl K. (May 29, 2014). "Iranian hackers sucker punch U.S. defense officials with creative social-media scam". The Washington Times. Retrieved March 30, 2015.*
4. ^ a b c d e f *Pizzi, Michael (May 29, 2014). "Iran hackers set up fake news site, personas to steal U.S. secrets". Al Jazeera. Retrieved March 30, 2015.*

External links

NEWSCASTER – An Iranian Threat Inside Social Media

Cyberwarfare in Iran	
Incidents	• Operation Olympic Games • Operation Ababil • "Operation Newscaster" • "Operation Cleaver"
Groups	• Elfin Team • Charming Kitten
Malware	• Stuxnet • Flame • Duqu • Stars virus • Mahdi • Shamoon
related	• Iranian Cyber Army • Operation Spider

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

- Bad Rabbit
- SpyEye
- Stuxnet

2010

- Alureon
- Duqu
- Kelihos
- Metulji botnet
- Stars

2011

- Carna
- Dexter
- FBI
- Flame
- Mahdi
- Red October
- Shamoon

2012

- CryptoLocker
- DarkSeoul

2013

- Brambul
- Carbanak
- Careto
- DarkHotel
- Duqu 2.0
- FinFisher
- Gameover ZeuS
- Regin

2014

- Dridex
- Hidden Tear
- Rombertik
- TeslaCrypt

2015

- Hitler
- Jigsaw
- KeRanger
- MEMZ
- Mirai
- Pegasus
- Petya (NotPetya)
- X-Agent

2016

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