Carbanak

en.wikipedia.org/wiki/Carbanak

Contributors to Wikimedia projects

Carbanak is an APT-style campaign targeting (but not limited to) financial institutions,[1] that was discovered in 2014[2] by the Russian cyber security company Kaspersky Lab.[3] It utilizes malware that is introduces into systems running Microsoft Windows[4] using phishing emails,[3][5] which is then used to steal money from banks. The hacker group is said to have stolen over 900 million dollars, from the banks as well as from over a thousand private customers.

The criminals were able to manipulate their access to the respective banking networks in order to steal the money in a variety of ways. In some instances, ATMs were instructed to dispense cash without having to locally interact with the terminal. Money mules would collect the money and transfer it over the SWIFT network to the criminals' accounts, Kaspersky said. The Carbanak group went so far as to alter databases and pump up balances on existing accounts and pocketing the difference unbeknownst to the user whose original balance is still intact.[6]

Their intended targets were primarily in Russia, followed by the United States, Germany, China and Ukraine, according to Kaspersky Lab. One bank lost $7.3 million when its ATMs were programmed to spew cash at certain times that henchmen would then collect, while a separate firm had $10 million taken via its online platform.

Kaspersky Lab is helping to assist in investigations and countermeasures that disrupt malware operations and cybercriminal activity. During the investigations they provide technical expertise such as analyzing infection vectors, malicious programs, supported command and control infrastructure and exploitation methods.[7]

FireEye published research tracking further activities, referring to the group as FIN7, including an SEC-themed spear phishing campaign.[8] Proofpoint also published research linking the group to the Bateleur backdoor, and expanded the list of targets to U.S.-based chain restaurants, hospitality organizations, retailers, merchant services, suppliers and others beyond their initial financial services focus.[9]

On 26 October 2020, PRODAFT (Switzerland) started publishing internal details of the Fin7/Carbanak group and tools they use during their operation.[10] Published information is claimed to be originated from a single OPSEC failure on the threat actor's side.[11]

On March 26, 2018, Europol claimed to have arrested the "mastermind" of the Carbanak and associated Cobalt or Cobalt Strike group in Alicante, Spain, in an investigation led by the Spanish National Police with the cooperation of law enforcement in multiple countries as well as private cybersecurity companies. The group's campaigns appear to have continued, however, with the Hudson's Bay Company breach using point of sale malware in 2018 being attributed to the group.[12]

Controversy

Some controversy exists around the Carbanak attacks, as they were seemingly described several months earlier in a report by the Internet security companies Group-IB (Russia) and Fox-IT (The Netherlands) that dubbed the attack Anunak.[13] The Anunak report shows also a greatly reduced amount of financial losses and according to a statement issued by Fox-IT after the release of *The New York Times* article, the compromise of banks outside Russia did not match their research.[14] Also in an interview conducted by Russian newspaper *Kommersant* the controversy between the claims of Kaspersky Lab and Group-IB come to light where Group-IB claims no banks outside of Russia and Ukraine were hit, and the activity outside of that region was focused on Point of Sale systems.[15]

Reuters issued a statement referencing a Private Industry Notification issued by the FBI and USSS (United States Secret Service) claiming they have not received any reports that Carbanak has affected the financial sector.[16] Two representative groups of the US banking industry FS-ISAC and ABA (American Bankers Association) in an interview with *Bank Technology News* say no US banks have been affected.[17]

References

1. ^ *Kaspersky Labs' Global Research & Analysis Team (GReAT) (February 16, 2015). "The Great Bank Robbery: the Carbanak APT". Securelist. Archived from the original on February 17, 2015.*
2. ^ *"Carbanak_APT Analysis" (PDF). Kaspersky. Archived from the original (PDF) on 19 March 2017. Retrieved 12 June 2017.*
3. ^ *a b David E. Sanger and Nicole Perlroth (14 February 2015). "Bank Hackers Steal Millions via Malware". The New York Times.*
4. ^ *Fingas, Jon (February 14, 2015). "Subtle malware lets hackers swipe over $300 million from banks". engadget. Archived from the original on February 15, 2015.*
5. ^ *"Carbanak Ring Steals $1 Billion from Banks". Threatpost. 15 February 2015.*
6. ^ *"The Great Bank Robbery: the Carbanak APT". Securelist. 16 February 2015.*
7. ^ *"FIN7 Evolution and the Phishing LNK". FireEye.*
8. ^ *"FIN7/Carbanak threat actor unleashes Bateleur JScript backdoor | Proofpoint US". www.proofpoint.com. July 31, 2017.*
9. ^ *"OpBlueRaven: Unveiling Fin7/Carbanak - Part I : Tirion". Prodaft.com.*
10. ^
11. ^ *Newman, Lily Hay. "THE BILLION-DOLLAR HACKING GROUP BEHIND A STRING OF BIG BREACHES". Wired.*

12. ^ *"Anunak APT against Financial institutions" (PDF). Fox-IT. 22 December 2014. Archived from the original (PDF) on 22 March 2015. Retrieved 4 March 2015.*
13. ^ *"Anunak aka Carbanak update". Fox-IT. 16 February 2015.*
14. ^ *"Group-IB and Kaspersky have conflicting views". Kommersant. 23 February 2015.*
15. ^ *"FBI, Secret service, no signs of Carbanak". Reuters. 18 February 2015. Archived from the original on 24 September 2015. Retrieved 30 June 2017.*
16. ^ *"Carbanak overhyped, no US banks hit". BankTechnologyNews. 19 February 2015.*

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=Carbanak&oldid=1052356275"