Chinese Antivirus Firm Was Part of APT41 ?Supply Chain? Attackhola

The U.S. Justice Department this week indicted seven Chinese nationals for a decade-long hacking spree that targeted more than 100 high-tech and online gaming companies. The government alleges the men used malware-laced phishing emails and "supply chain" attacks to steal data from companies and their customers. One of the alleged hackers was first profiled here in 2012 as the owner of a Chinese antivirus firm.

Image: FBI

Charging documents say the seven men are part of a hacking group known variously as "APT41," "Barium," "Winnti," "Wicked Panda," and "Wicked Spider." Once inside of a target organization, the hackers stole source code, software code signing certificates, customer account data and other information they could use or resell.

APT41"s activities span from the mid-2000s to the present day. Earlier this year, for example, the group was tied to a particularly aggressive malware campaign that exploited recent vulnerabilities in widely-used networking products, including flaws in Cisco and D-Link routers, as well as Citrix and Pulse VPN appliances. Security firm FireEye dubbed that hacking blitz "one of the broadest campaigns by a Chinese cyber espionage actor we have observed in recent years."

The government alleges the group monetized its illicit access by deploying ransomware and "cryptojacking" tools (using compromised systems to mine cryptocurrencies like Bitcoin). In addition, the gang targeted video game companies and their customers in a bid to steal digital items of value that could be resold, such as points, powers and other items that could be used to enhance the game-playing experience.

APT41 was known to hide its malware inside fake resumes that were sent to targets. It also deployed more complex supply chain attacks, in which they would hack a software company and modify the code with malware.

"The victim software firm " unaware of the changes to its product, would subsequently distribute the modified software to its third-party customers, who were thereby defrauded into installing malicious software code on their own computers," the indictments explain.

While the various charging documents released in this case do not mention it per se, it is clear that members of this group also favored another form of supply chain attacks " hiding their malware inside commercial tools they created and advertised as legitimate security software and PC utilities.

One of the men indicted as part of APT41 " now 35-year-old Tan DaiLin " was the subject of a 2012 KrebsOnSecurity story that sought to shed light on a Chinese antivirus product marketed as Anvisoft. At the time, the product had been "whitelisted" or marked as safe by competing, more established antivirus vendors, although the company seemed unresponsive to user complaints and to questions about its leadership and origins.

Tan DaiLin, a.k.a. "Wicked Rose," in his younger years. Image: iDefense

Anvisoft claimed to be based in California and Canada, but a search on the company"s brand name turned up trademark registration records that put Anvisoft in the high-tech zone of Chengdu in the Sichuan Province of China.

A review of Anvisoft"s website registration records showed the company"s domain originally was created by Tan DaiLin, an infamous Chinese hacker who went by the aliases "Wicked Rose" and "Withered Rose." At the time of story, DaiLin was 28 years old.

That story cited a 2007 report (PDF) from iDefense, which detailed DaiLin"s role as the leader of a state-sponsored, four-man hacking team called NCPH (short for Network Crack Program Hacker). According to iDefense, in 2006 the group was responsible for crafting a rootkit that took advantage of a zero-day vulnerability in Microsoft Word, and was used in attacks on "a large DoD entity" within the USA.

"Wicked Rose and the NCPH hacking group are implicated in multiple Office based attacks over a two year period," the iDefense report stated.

When I first scanned Anvisoft at Virustotal.com back in 2012, none of the antivirus products detected it as suspicious or malicious. But in the days that followed, several antivirus products began flagging it for bundling at least two trojan horse programs designed to steal passwords from various online gaming platforms. Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/09/chinese-antivirus-firm-was-part-of-apt41-supply-chain-attack/#more-53008

Two Russians Charged in $17M Cryptocurrency Phishing Spreehola

U.S. authorities today announced criminal charges and financial sanctions against two Russian men accused of stealing nearly $17 million worth of virtual currencies in a series of phishing attacks throughout 2017 and 2018 that spoofed websites for some of the most popular cryptocurrency exchanges.

The Justice Department unsealed indictments against Russian nationals Danil Potekhin and Dmitirii Karasavidi, alleging the duo was responsible for a sophisticated phishing and money laundering campaign that resulted in the theft of $16.8 million in cryptocurrencies and fiat money from victims.

Separately, the U.S. Treasury Department announced economic sanctions against Potekhin and Karasavidi, effectively freezing all property and interests of these persons (subject to U.S. jurisdiction) and making it a crime to transact with them.

According to the indictments, the two men set up fake websites that spoofed login pages for the currency exchanges Binance, Gemini and Poloniex. Armed with stolen login credentials, the men allegedly stole more than $10 million from 142 Binance victims, $5.24 million from 158 Poloniex users, and $1.17 million from 42 Gemini customers.

Prosecutors say the men then laundered the stolen funds through an array of intermediary cryptocurrency accounts " including compromised and fictitiously created accounts " on the targeted cryptocurrency exchange platforms. In addition, the two are alleged to have artificially inflated the value of their ill-gotten gains by engaging in cryptocurrency price manipulation using some of the stolen funds.

For example, investigators alleged Potekhin and Karasavidi used compromised Poloniex accounts to place orders to purchase large volumes of "GAS," the digital currency token used to pay the cost of executing transactions on the NEO blockchain " China"s first open source blockchain platform.

"Using digital crurency in one victim Poloniex account, they placed an order to purchase approximately 8,000 GAS, thereby immediately increasing the market price of GAS from approximately $18 to $2,400," the indictment explains.

Potekhin and others then converted the artificially inflated GAS in their own fictitious

Poloniex accounts into other cryptocurrencies, including Ethereum (ETH) and Bitcoin (BTC). From the complaint:

"Before the Eight Fictitious Poloniex Accounts were frozen, POTEKHIN and others transferred approximately 759 ETH to nine digital currency addresses. Through a sophisticated and layered manner, the ETH from these nine digital currency addresses was sent through multiple intermediary accounts, before ultimately being deposited into a Bitfinex account controlled by Karasavidi."

The Treasury"s action today lists several of the cryptocurrency accounts thought to have been used by the defendants. Searching on some of those accounts at various cryptocurrency transaction tracking sites points to a number of phishing victims.

"I would like to blow your bitch ass away, if you even had the balls to show yourself," exclaimed one victim, posting in a comment on the Etherscan lookup service. Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/09/two-russians-charged-in-17m-cryptocurrency-phishing-spree/#more-52989

Due Diligence That Money Can?t Buyhola

Most of us automatically put our guard up when someone we don"t know promises something too good to be true. But when the too-good-to-be-true thing starts as our idea, sometimes that instinct fails to kick in. Here"s the story of how companies searching for investors to believe in their ideas can run into trouble.

Nick is an investment banker who runs a firm that helps raise capital for its clients (Nick is not his real name, and like other investment brokers interviewed in this story spoke with KrebsOnSecurity on condition of anonymity). Nick"s company works primarily in the mergers and acquisitions space, and his job involves advising clients about which companies and investors might be a good bet.

In one recent engagement, a client of Nick"s said they"d reached out to an investor from Switzerland " The Private Office of John Bernard " whose name was included on a list of angel investors focused on technology startups.

"We ran into a group that one of my junior guys found on a list of data providers that compiled information on investors," Nick explained. "I told them what we do and said we were working with a couple of companies that were interested in financing, and asked them to send some materials over. The guy had a British accent, claimed to have made his money in tech and in the dot-com boom, and said he"d sold a company to Geocities that was then bought by Yahoo."

But Nick wasn"t convinced Mr. Bernard"s company was for real. Nick and his colleagues couldn"t locate the company Mr. Bernard claimed to have sold, and while Bernard said he was based in Switzerland, virtually all of his staff were all listed on LinkedIn as residing in Ukraine.

Nick told his clients about his reservations, but each nevertheless was excited that someone was finally interested enough to invest in their ideas.

"The CEO of the client firm said, "This is great, someone is willing to believe in our company"," Nick said. "After one phone call, he made an offer to invest tens of millions of dollars. I advised them not to pursue it, and one of the clients agreed. The other was very gung ho."

When companies wish to link up with investors, what follows involves a process

known as "due diligence" wherein each side takes time to research the other"s finances, management, and any lurking legal liabilities or risks associated with the transaction. Typically, each party will cover their own due diligence costs, but sometimes the investor or the company that stands to benefit from the transaction will cover the associated fees for both parties.

Nick said he wasn"t surprised when Mr. Bernard"s office insisted that its due diligence fees of tens of thousands of dollars be paid up front by his client. And he noticed the website for the due diligence firm that Mr. Bernard suggested using " insideknowledge.ch " also was filled with generalities and stock photos, just like John Bernard"s private office website.

"He said we used to use big accounting firms for this but found them to be ineffective," Nick said. "The company they wanted us to use looked like a real accounting firm, but we couldn"t find any evidence that they were real. Also, we asked to see an investment portfolio. He said he"s invested in over 30 companies, so I would expect to see a document that says, "here"s the various companies we"ve invested in." But instead, we got two recommendation letters on letterhead saying how great these investors were."

KrebsOnSecurity located two other investment bankers who had similar experiences with Mr. Bernard"s office.

"A number of us have been comparing notes on this guy, and he never actually delivers," said one investment banker who asked not to be named because he did not have permission from his clients. "In each case, he agreed to invest millions with no push back, the documentation submitted from their end was shabby and unprofessional, and they seem focused on companies that will write a check for due diligence fees. After their fees are paid, the experience has been an ever increasing and inventive number of reasons why the deal can"t close, including health problems and all sorts of excuses."

Mr. Bernard"s investment firm did not respond to multiple requests for comment. The one technology company this author could tie to Mr. Bernard was secureswissdata.com, a Swiss concern that provides encrypted email and data services. The domain was registered in 2015 by Inside Knowledge. In February 2020, Secure Swiss Data was purchased in an "undisclosed multimillion buyout" by SafeSwiss Secure Communication AG.

SafeSwiss co-CEO and Secure Swiss Data founder David Bruno said he couldn"t imagine that Mr. Bernard would be involved in anything improper.

"I can confirm that I know John Bernard and have always found him very honourable and straight forward in my dealings with him as an investor," Bruno said. "To be honest with you, I struggle to believe that he would, or would even need to be, involved in the activity you mentioned, and quite frankly I"ve never heard about those things." Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/09/due-diligence-that-money-cant-buy/#more-52428

Microsoft Patch Tuesday, Sept. 2020 Editionhola

Microsoft today released updates to remedy nearly 130 security vulnerabilities in its Windows operating system and supported software. None of the flaws are known to be currently under active exploitation, but 23 of them could be exploited by malware or malcontents to seize complete control of Windows computers with little or no help from users.

The majority of the most dangerous or "critical" bugs deal with issues in Microsoft"s various Windows operating systems and its web browsers, Internet Explorer and Edge. September marks the seventh month in a row Microsoft has shipped fixes for more than 100 flaws in its products, and the fourth month in a row that it fixed more than 120.

Among the chief concerns for enterprises this month is CVE-2020-16875, which involves a critical flaw in the email software Microsoft Exchange Server 2016 and 2019. An attacker could leverage the Exchange bug to run code of his choosing just by sending a booby-trapped email to a vulnerable Exchange server.

"That doesn"t quite make it wormable, but it"s about the worst-case scenario for Exchange servers," said Dustin Childs, of Trend Micro"s Zero Day Initiative. "We have seen the previously patched Exchange bug CVE-2020-0688 used in the wild, and that requires authentication. We"ll likely see this one in the wild soon. This should be your top priority."

Also not great for companies to have around is CVE-2020-1210, which is a remote code execution flaw in supported versions of Microsoft Sharepoint document management software that bad guys could attack by uploading a file to a vulnerable Sharepoint site. Security firm Tenable notes that this bug is reminiscent of CVE-2019-0604, another Sharepoint problem that"s been exploited for cybercriminal gains since April 2019.

Microsoft fixed at least five other serious bugs in Sharepoint versions 2010 through 2019 that also could be used to compromise systems running this software. And because ransomware purveyors have a history of seizing upon Sharepoint flaws to wreak havoc inside enterprises, companies should definitely prioritize deployment of

these fixes, says Alan Liska, senior security architect at Recorded Future. Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/09/microsoft-patch-tuesday-sept-2020-edition/#more-52959

The Joys of Owning an ?OG? Email Accounthola

When you own a short email address at a popular email provider, you are bound to get gobs of spam, and more than a few alerts about random people trying to seize control over the account. If your account name is short and desirable enough, this kind of activity can make the account less reliable for day-to-day communications because it tends to bury emails you do want to receive. But there is also a puzzling side to all this noise: Random people tend to use your account as if it were theirs, and often for some fairly sensitive services online.

About 16 years ago " back when you actually had to be invited by an existing Google Mail user in order to open a new Gmail account " I was able to get hold of a very short email address on the service that hadn"t yet been reserved. Naming the address here would only invite more spam and account hijack attempts, but let"s just say the account name has something to do with computer hacking.

Because it"s a relatively short username, it is what"s known as an "OG" or "original gangster" account. These account names tend to be highly prized among certain communities, who busy themselves with trying to hack them for personal use or resale. Hence, the constant account takeover requests.

What is endlessly fascinating is how many people think it"s a good idea to sign up for important accounts online using my email address. Naturally, my account has been signed up involuntarily for nearly every dating and porn website there is. That is to be expected, I suppose.

But what still blows me away is the number of financial and other sensitive accounts I could access if I were of a devious mind. This particular email address has accounts that I never asked for at H&R Block, Turbotax, TaxAct, iTunes, LastPass, Dashlane, MyPCBackup, and Credit Karma, to name just a few. I"ve lost count of the number of active bank, ISP and web hosting accounts I can tap into.

I"m perpetually amazed by how many other Gmail users and people on similarly-sized webmail providers have opted to pick my account as a backup address if they should ever lose access to their inbox. Almost certainly, these users just lazily picked my account name at random when asked for a backup email " apparently without fully

realizing the potential ramifications of doing so. At last check, my account is listed as the backup for more than three dozen Yahoo, Microsoft and other Gmail accounts and their associated file-sharing services.

If for some reason I ever needed to order pet food or medications online, my phantom accounts at Chewy, Coupaw and Petco have me covered. If any of my Weber grill parts ever fail, I"m set for life on that front. The Weber emails I periodically receive remind me of a piece I wrote many years ago for The Washington Post, about companies sending email from [companynamehere]@donotreply.com, without considering that someone might own that domain. Someone did, and the results were often hilarious.

It"s probably a good thing I"m not massively into computer games, because the online gaming (and gambling) profiles tied to my old Gmail account are innumerable.

For several years until recently, I was receiving the monthly statements intended for an older gentleman in India who had the bright idea of using my Gmail account to manage his substantial retirement holdings. Thankfully, after reaching out to him he finally removed my address from his profile, although he never responded to questions about how this might have happened.

On balance, I"ve learned it"s better just not to ask. On multiple occasions, I"d spend a few minutes trying to figure out if the email addresses using my Gmail as a backup were created by real people or just spam bots of some sort. And then I"d send a polite note to those that fell into the former camp, explaining why this was a bad idea and ask what motivated them to do so.

Perhaps because my Gmail account name includes a hacking term, the few responses I"ve received have been less than cheerful. Despite my including detailed instructions on how to undo what she"d done, one woman in Florida screamed in an ALL CAPS reply that I was trying to phish her and that her husband was a police officer who would soon hunt me down. Alas, I still get notifications anytime she logs into her Yahoo account.

Probably for the same reason the Florida lady assumed I was a malicious hacker, my account constantly gets requests from random people who wish to hire me to hack into someone else"s account. I never respond to those either, although I"ll admit that sometimes when I"m procrastinating over something the temptation arises.

Losing access to your inbox can open you up to a cascading nightmare of other

problems. Having a backup email address tied to your inbox is a good idea, but obviously only if you also control that backup address. Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/09/the-joys-of-owning-an-og-email-account/#more-45506

Sendgrid Under Siege from Hacked Accountshola

Email service provider Sendgrid is grappling with an unusually large number of customer accounts whose passwords have been cracked, sold to spammers, and abused for sending phishing and email malware attacks. Sendgrid"s parent company Twilio says it is working on a plan to require multi-factor authentication for all of its customers, but that solution may not come fast enough for organizations having trouble dealing with the fallout in the meantime.

Image: Wikipedia

Many companies use Sendgrid to communicate with their customers via email, or else pay marketing firms to do that on their behalf using Sendgrid"s systems. Sendgrid takes steps to validate that new customers are legitimate businesses, and that emails sent through its platform carry the proper digital signatures that other companies can use to validate that the messages have been authorized by its customers.

But this also means when a Sendgrid customer account gets hacked and used to send malware or phishing scams, the threat is particularly acute because a large number of organizations allow email from Sendgrid"s systems to sail through their spam-filtering systems.

To make matters worse, links included in emails sent through Sendgrid are obfuscated (mainly for tracking deliverability and other metrics), so it is not immediately clear to recipients where on the Internet they will be taken when they click.

Dealing with compromised customer accounts is a constant challenge for any organization doing business online today, and certainly Sendgrid is not the only email marketing platform dealing with this problem. But according to multiple emails from readers, recent threads on several anti-spam discussion lists, and interviews with people in the anti-spam community, over the past few months there has been a marked increase in malicious, phishous and outright spammy email being blasted out via Sendgrid"s servers.

Rob McEwen is CEO of Invaluement.com, an anti-spam firm whose data on junk email trends are used to improve the spam-blocking technologies deployed by several Fortune 100 companies. McEwen said no other email service provider has come

close to generating the volume of spam that"s been emanating from Sendgrid accounts lately.

"As far as the nasty criminal phishes and viruses, I think there"s not even a close second in terms of how bad it"s been with Sendgrid over the past few months," he said.

Trying to filter out bad emails coming from a major email provider that so many legitimate companies rely upon to reach their customers can be a dicey business. If you filter the emails too aggressively you end up with an unacceptable number of "false positives," i.e., benign or even desirable emails that get flagged as spam and sent to the junk folder or blocked altogether.

But McEwen said the incidence of malicious spam coming from Sendgrid has gotten so bad that he recently launched a new anti-spam block list specifically to filter out email from Sendgrid accounts that have been known to be blasting large volumes of junk or malicious email.

"Before I implemented this in my own filtering system a week ago, I was getting three to four phone calls or stern emails a week from angry customers wondering why these malicious emails were getting through to their inboxes," McEwen said. "And I just am not seeing anything this egregious in terms of viruses and spams from the other email service providers." Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/08/sendgrid-under-siege-from-hacked-accounts/#more-52812

Confessions of an ID Theft Kingpin, Part IIhola

Yesterday"s piece told the tale of Hieu Minh Ngo, a hacker the U.S. Secret Service described as someone who caused more material financial harm to more Americans than any other convicted cybercriminal. Ngo was recently deported back to his home country after serving more than seven years in prison for running multiple identity theft services. He now says he wants to use his experience to convince other cybercriminals to use their skills for good. Here"s a look at what happened after he got busted.

Hieu Minh Ngo, 29, in a recent photo.

Part I of this series ended with Ngo in handcuffs after disembarking a flight from his native Vietnam to Guam, where he believed he was going to meet another cybercriminal who"d promised to hook him up with the mother of all consumer data caches.

Ngo had been making more than $125,000 a month reselling ill-gotten access to some of the biggest data brokers on the planet. But the Secret Service discovered his various accounts at these data brokers and had them shut down one by one. Ngo became obsessed with restarting his business and maintaining his previous income. By this time, his ID theft services had earned roughly USD $3 million.

As this was going on, Secret Service agents used an intermediary to trick Ngo into thinking he"d trodden on the turf of another cybercriminal. From Part I:

The Secret Service contacted Ngo through an intermediary in the United Kingdom " a known, convicted cybercriminal who agreed to play along. The U.K.-based collaborator told Ngo he had personally shut down Ngo"s access to Experian because he had been there first and Ngo was interfering with his business.

"The U.K. guy told Ngo, "Hey, you"re treading on my turf, and I decided to lock you out. But as long as you"re paying a vig through me, your access won"t go away"," the Secret Service"s Matt O"Neill recalled.

After several months of conversing with his apparent U.K.-based tormentor, Ngo agreed to meet him in Guam to finalize the deal. But immediately after stepping off of the plane in Guam, he was apprehended by Secret Service agents.

"One of the names of his identity theft services was findget[.]me," O"Neill said. "We

took that seriously, and we did like he asked."

In an interview with KrebsOnSecurity, Ngo said he spent about two months in a Guam jail awaiting transfer to the United States. A month passed before he was allowed a 10 minute phone call to his family and explain what he"d gotten himself into.

"This was a very tough time," Ngo said. "They were so sad and they were crying a lot."

First stop on his prosecution tour was New Jersey, where he ultimately pleaded guilty to hacking into MicroBilt, the first of several data brokers whose consumer databases would power different iterations of his identity theft service over the years.

Next came New Hampshire, where another guilty plea forced him to testify in three different trials against identity thieves who had used his services for years. Among them was Lance Ealy, a serial ID thief from Dayton, Ohio who used Ngo"s service to purchase more than 350 "fullz" " a term used to describe a package of everything one would need to steal someone"s identity, including their Social Security number, mother"s maiden name, birth date, address, phone number, email address, bank account information and passwords.

Ealy used Ngo"s service primarily to conduct tax refund fraud with the U.S. Internal Revenue Service (IRS), claiming huge refunds in the names of ID theft victims who first learned of the fraud when they went to file their taxes and found someone else had beat them to it.

Ngo"s cooperation with the government ultimately led to 20 arrests, with a dozen of those defendants lured into the open by O"Neill and other Secret Service agents posing as Ngo.

The Secret Service had difficulty pinning down the exact amount of financial damage inflicted by Ngo"s various ID theft services over the years, primarily because those services only kept records of what customers searched for " not which records they purchased.

But based on the records they did have, the government estimated that Ngo"s service enabled approximately $1.1 billion in new account fraud at banks and retailers throughout the United States, and roughly $64 million in tax refund fraud with the states and the IRS.

"We interviewed a number of Ngo"s customers, who were pretty open about why they were using his services," O"Neill said. "Many of them told us the same thing: Buying

identities was so much better for them than stolen payment card data, because card data could be used once or twice before it was no good to them anymore. But identities could be used over and over again for years."

O"Neill said he still marvels at the fact that Ngo"s name is practically unknown when compared to the world"s most infamous credit card thieves, some of whom were responsible for stealing hundreds of millions of cards from big box retail merchants.

"I don"t know of anyone who has come close to causing more material harm than Ngo did to the average American," O"Neill said. "But most people have probably never heard of him."

Ngo said he wasn"t surprised that his services were responsible for so much financial damage. But he was utterly unprepared to hear about the human toll. Throughout the court proceedings, Ngo sat through story after dreadful story of how his work had ruined the financial lives of people harmed by his services.

"When I was running the service, I didn"t really care because I didn"t know my customers and I didn"t know much about what they were doing with it," Ngo said. "But during my case, the federal court received like 13,000 letters from victims who complained they lost their houses, jobs, or could no longer afford to buy a home or maintain their financial life because of me. That made me feel really bad, and I realized I"d been a terrible person."

Even as he bounced from one federal detention facility to the next, Ngo always seemed to encounter ID theft victims wherever he went, including prison guards, healthcare workers and counselors.

"When I was in jail at Beaumont, Texas I talked to one of the correctional officers there who shared with me a story about her friend who lost her identity and then lost everything after that," Ngo recalled. "Her whole life fell apart. I don"t know if that lady was one of my victims, but that story made me feel sick. I know now that what I was doing was just evil."

Ngo"s former ID theft service usearching[.]info.

Link para leer mas

https://krebsonsecurity.com/2020/08/confessions-of-an-id-theft-kingpin-part-ii/#more-52861

Confessions of an ID Theft Kingpin, Part Ihola

At the height of his cybercriminal career, the hacker known as "Hieupc" was earning $125,000 a month running a bustling identity theft service that siphoned consumer dossiers from some of the world"s top data brokers. That is, until his greed and ambition played straight into an elaborate snare set by the U.S. Secret Service. Now, after more than seven years in prison Hieupc is back in his home country and hoping to convince other would-be cybercrooks to use their computer skills for good.

Hieu Minh Ngo, in his teens.

For several years beginning around 2010, a lone teenager in Vietnam named Hieu Minh Ngo ran one of the Internet"s most profitable and popular services for selling "fullz," stolen identity records that included a consumer"s name, date of birth, Social Security number and email and physical address.

Ngo got his treasure trove of consumer data by hacking and social engineering his way into a string of major data brokers. By the time the Secret Service caught up with him in 2013, he"d made over $3 million selling fullz data to identity thieves and organized crime rings operating throughout the United States.

Matt O"Neill is the Secret Service agent who in February 2013 successfully executed a scheme to lure Ngo out of Vietnam and into Guam, where the young hacker was arrested and sent to the mainland U.S. to face prosecution. O"Neill now heads the agency"s Global Investigative Operations Center, which supports investigations into transnational organized criminal groups.

O"Neill said he opened the investigation into Ngo"s identity theft business after reading about it in a 2011 KrebsOnSecurity story, "How Much is Your Identity Worth"" According to O"Neill, what"s remarkable about Ngo is that to this day his name is virtually unknown among the pantheon of infamous convicted cybercriminals, the majority of whom were busted for trafficking in huge quantities of stolen credit cards.

Ngo"s businesses enabled an entire generation of cybercriminals to commit an estimated $1 billion worth of new account fraud, and to sully the credit histories of countless Americans in the process.

"I don"t know of any other cybercriminal who has caused more material financial harm to more Americans than Ngo," O"Neill told KrebsOnSecurity. "He was selling the

personal information on more than 200 million Americans and allowing anyone to buy it for pennies apiece."

Freshly released from the U.S. prison system and deported back to Vietnam, Ngo is currently finishing up a mandatory three-week COVID-19 quarantine at a government-run facility. He contacted KrebsOnSecurity from inside this facility with the stated aim of telling his little-known story, and to warn others away from following in his footsteps.

Ten years ago, then 19-year-old hacker Ngo was a regular on the Vietnamese-language computer hacking forums. Ngo says he came from a middle-class family that owned an electronics store, and that his parents bought him a computer when he was around 12 years old. From then on out, he was hooked.

In his late teens, he traveled to New Zealand to study English at a university there. By that time, he was already an administrator of several dark web hacker forums, and between his studies he discovered a vulnerability in the school"s network that exposed payment card data.

"I did contact the IT technician there to fix it, but nobody cared so I hacked the whole system," Ngo recalled. "Then I used the same vulnerability to hack other websites. I was stealing lots of credit cards."

Ngo said he decided to use the card data to buy concert and event tickets from Ticketmaster, and then sell the tickets at a New Zealand auction site called TradeMe. The university later learned of the intrusion and Ngo"s role in it, and the Auckland police got involved. Ngo"s travel visa was not renewed after his first semester ended, and in retribution he attacked the university"s site, shutting it down for at least two days.

Ngo said he started taking classes again back in Vietnam, but soon found he was spending most of his time on cybercrime forums.

"I went from hacking for fun to hacking for profits when I saw how easy it was to make money stealing customer databases," Ngo said. "I was hanging out with some of my friends from the underground forums and we talked about planning a new criminal activity."

"My friends said doing credit cards and bank information is very dangerous, so I started thinking about selling identities," Ngo continued. "At first I thought well, it"s just information, maybe it"s not that bad because it"s not related to bank accounts directly.

But I was wrong, and the money I started making very fast just blinded me to a lot of things."

His first big target was a consumer credit reporting company in New Jersey called MicroBilt.

"I was hacking into their platform and stealing their customer database so I could use their customer logins to access their [consumer] databases," Ngo said. "I was in their systems for almost a year without them knowing."

Very soon after gaining access to MicroBilt, Ngo says, he stood up Superget[.]info, a website that advertised the sale of individual consumer records. Ngo said initially his service was quite manual, requiring customers to request specific states or consumers they wanted information on, and he would conduct the lookups by hand.

Ngo"s former identity theft service, superget[.]info

But Ngo would soon work out how to use more powerful servers in the United States to automate the collection of larger amounts of consumer data from MicroBilt"s systems, and from other data brokers. As I wrote of Ngo"s service back in November 2011:

"Superget lets users search for specific individuals by name, city, and state. Each "credit" costs USD$1, and a successful hit on a Social Security number or date of birth costs 3 credits each. The more credits you buy, the cheaper the searches are per credit: Six credits cost $4.99; 35 credits cost $20.99, and $100.99 buys you 230 credits. Customers with special needs can avail themselves of the "reseller plan," which promises 1,500 credits for $500.99, and 3,500 credits for $1000.99.

"Our Databases are updated EVERY DAY," the site"s owner enthuses. "About 99% nearly 100% US people could be found, more than any sites on the internet now."

Ngo"s intrusion into MicroBilt eventually was detected, and the company kicked him out of their systems. But he says he got back in using another vulnerability.

"I was hacking them and it was back and forth for months," Ngo said. "They would discover [my accounts] and fix it, and I would discover a new vulnerability and hack them again."

This game of cat and mouse continued until Ngo found a much more reliable and stable source of consumer data: A U.S. based company called Court Ventures, which aggregated public records from court documents. Ngo wasn"t interested in the data

collected by Court Ventures, but rather in its data sharing agreement with a third-party data broker called U.S. Info Search, which had access to far more sensitive consumer records.

Using forged documents and more than a few lies, Ngo was able to convince Court Ventures that he was a private investigator based in the United States.

"At first [when] I sign up they asked for some documents to verify," Ngo said. "So I just used some skill about social engineering and went through the security check."

Then, in March 2012, something even more remarkable happened: Court Ventures was purchased by Experian, one of the big three major consumer credit bureaus in the United States. And for nine months after the acquisition, Ngo was able to maintain his access.

"After that, the database was under control by Experian," he said. "I was paying Experian good money, thousands of dollars a month."

Whether anyone at Experian ever performed due diligence on the accounts grandfathered in from Court Ventures is unclear. But it wouldn"t have taken a rocket surgeon to figure out that this particular customer was up to something fishy.

For one thing, Ngo paid the monthly invoices for his customers" data requests using wire transfers from a multitude of banks around the world, but mostly from new accounts at financial institutions in China, Malaysia and Singapore.

O"Neill said Ngo"s identity theft website generated tens of thousands of queries each month. For example, the first invoice Court Ventures sent Ngo in December 2010 was for 60,000 queries. By the time Experian acquired the company, Ngo"s service had attracted more than 1,400 regular customers, and was averaging 160,000 monthly queries.

More importantly, Ngo"s profit margins were enormous.

"His service was quite the racket," he said. "Court Ventures charged him 14 cents per lookup, but he charged his customers about $1 for each query."

By this time, O"Neill and his fellow Secret Service agents had served dozens of subpoenas tied to Ngo"s identity theft service, including one that granted them access to the email account he used to communicate with customers and administer his site. The agents discovered several emails from Ngo instructing an accomplice to pay Experian using wire transfers from different Asian banks. Continue reading "

Link para leer mas
https://krebsonsecurity.com/2020/08/confessions-of-an-id-theft-kingpin-part-i/#more-52808

FBI, CISA Echo Warnings on ?Vishing? Threathola

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) on Thursday issued a joint alert to warn about the growing threat from voice phishing or "vishing" attacks targeting companies. The advisory came less than 24 hours after KrebsOnSecurity published an in-depth look at a crime group offering a service that people can hire to steal VPN credentials and other sensitive data from employees working remotely during the Coronavirus pandemic.

"The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate virtual private networks (VPNs) and elimination of in-person verification," the alert reads. "In mid-July 2020, cybercriminals started a vishing campaign"gaining access to employee tools at multiple companies with indiscriminate targeting " with the end goal of monetizing the access."

As noted in Wednesday"s story, the agencies said the phishing sites set up by the attackers tend to include hyphens, the target company"s name, and certain words " such as "support," "ticket," and "employee." The perpetrators focus on social engineering new hires at the targeted company, and impersonate staff at the target company"s IT helpdesk.

The joint FBI/CISA alert (PDF) says the vishing gang also compiles dossiers on employees at the specific companies using mass scraping of public profiles on social media platforms, recruiter and marketing tools, publicly available background check services, and open-source research. From the alert:

"Actors first began using unattributed Voice over Internet Protocol (VoIP) numbers to call targeted employees on their personal cellphones, and later began incorporating spoofed numbers of other offices and employees in the victim company. The actors used social engineering techniques and, in some cases, posed as members of the victim company"s IT help desk, using their knowledge of the employee"s personally identifiable information"including name, position, duration at company, and home address"to gain the trust of the targeted employee."

"The actors then convinced the targeted employee that a new VPN link would be sent and required their login, including any 2FA [2-factor authentication] or OTP [one-time

passwords]. The actor logged the information provided by the employee and used it in real-time to gain access to corporate tools using the employee"s account."

The alert notes that in some cases the unsuspecting employees approved the 2FA or OTP prompt, either accidentally or believing it was the result of the earlier access granted to the help desk impersonator. In other cases, the attackers were able to intercept the one-time codes by targeting the employee with SIM swapping, which involves social engineering people at mobile phone companies into giving them control of the target"s phone number. Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/08/fbi-cisa-echo-warnings-on-vishing-threat/#more-52783

Voice Phishers Targeting Corporate VPNshola

The COVID-19 epidemic has brought a wave of email phishing attacks that try to trick work-at-home employees into giving away credentials needed to remotely access their employers" networks. But one increasingly brazen group of crooks is taking your standard phishing attack to the next level, marketing a voice phishing service that uses a combination of one-on-one phone calls and custom phishing sites to steal VPN credentials from employees.

According to interviews with several sources, this hybrid phishing gang has a remarkably high success rate, and operates primarily through paid requests or "bounties," where customers seeking access to specific companies or accounts can hire them to target employees working remotely at home.

And over the past six months, the criminals responsible have created dozens if not hundreds of phishing pages targeting some of the world"s biggest corporations. For now at least, they appear to be focusing primarily on companies in the financial, telecommunications and social media industries.

"For a number of reasons, this kind of attack is really effective," said Allison Nixon, chief research officer at New York-based cyber investigations firm Unit 221B. "Because of the Coronavirus, we have all these major corporations that previously had entire warehouses full of people who are now working remotely. As a result the attack surface has just exploded."

A typical engagement begins with a series of phone calls to employees working remotely at a targeted organization. The phishers will explain that they"re calling from the employer"s IT department to help troubleshoot issues with the company"s virtual private networking (VPN) technology.

The employee phishing page bofaticket[.]com. Image: urlscan.io

The goal is to convince the target either to divulge their credentials over the phone or to input them manually at a website set up by the attackers that mimics the organization"s corporate email or VPN portal.

Zack Allen is director of threat intelligence for ZeroFOX, a Baltimore-based company that helps customers detect and respond to risks found on social media and other

digital channels. Allen has been working with Nixon and several dozen other researchers from various security firms to monitor the activities of this prolific phishing gang in a bid to disrupt their operations.

Allen said the attackers tend to focus on phishing new hires at targeted companies, and will often pose as new employees themselves working in the company"s IT division. To make that claim more believable, the phishers will create LinkedIn profiles and seek to connect those profiles with other employees from that same organization to support the illusion that the phony profile actually belongs to someone inside the targeted firm.

"They"ll say "Hey, I"m new to the company, but you can check me out on LinkedIn" or Microsoft Teams or Slack, or whatever platform the company uses for internal communications," Allen said. "There tends to be a lot of pretext in these conversations around the communications and work-from-home applications that companies are using. But eventually, they tell the employee they have to fix their VPN and can they please log into this website."

The domains used for these pages often invoke the company"s name, followed or preceded by hyphenated terms such as "vpn," "ticket," "employee," or "portal." The phishing sites also may include working links to the organization"s other internal online resources to make the scheme seem more believable if a target starts hovering over links on the page.

Allen said a typical voice phishing or "vishing" attack by this group involves at least two perpetrators: One who is social engineering the target over the phone, and another co-conspirator who takes any credentials entered at the phishing page and quickly uses them to log in to the target company"s VPN platform in real-time.

Time is of the essence in these attacks because many companies that rely on VPNs for remote employee access also require employees to supply some type of multi-factor authentication in addition to a username and password " such as a one-time numeric code generated by a mobile app or text message. And in many cases, those codes are only good for a short duration " often measured in seconds or minutes.

But these vishers can easily sidestep that layer of protection, because their phishing pages simply request the one-time code as well.

A phishing page (helpdesk-att[.]com) targeting AT&T employees. Image: urlscan.io

Allen said it matters little to the attackers if the first few social engineering attempts fail. Most targeted employees are working from home or can be reached on a mobile device. If at first the attackers don"t succeed, they simply try again with a different employee.

And with each passing attempt, the phishers can glean important details from employees about the target"s operations, such as company-specific lingo used to describe its various online assets, or its corporate hierarchy.

Thus, each unsuccessful attempt actually teaches the fraudsters how to refine their social engineering approach with the next mark within the targeted organization, Nixon said.

"These guys are calling companies over and over, trying to learn how the corporation works from the inside," she said. Continue reading "

Link para leer mas

https://krebsonsecurity.com/2020/08/voice-phishers-targeting-corporate-vpns/#more-52718