



Altamaha Bank & Trust

Fraud Awareness and Prevention Forum

www.Altamaha.bank





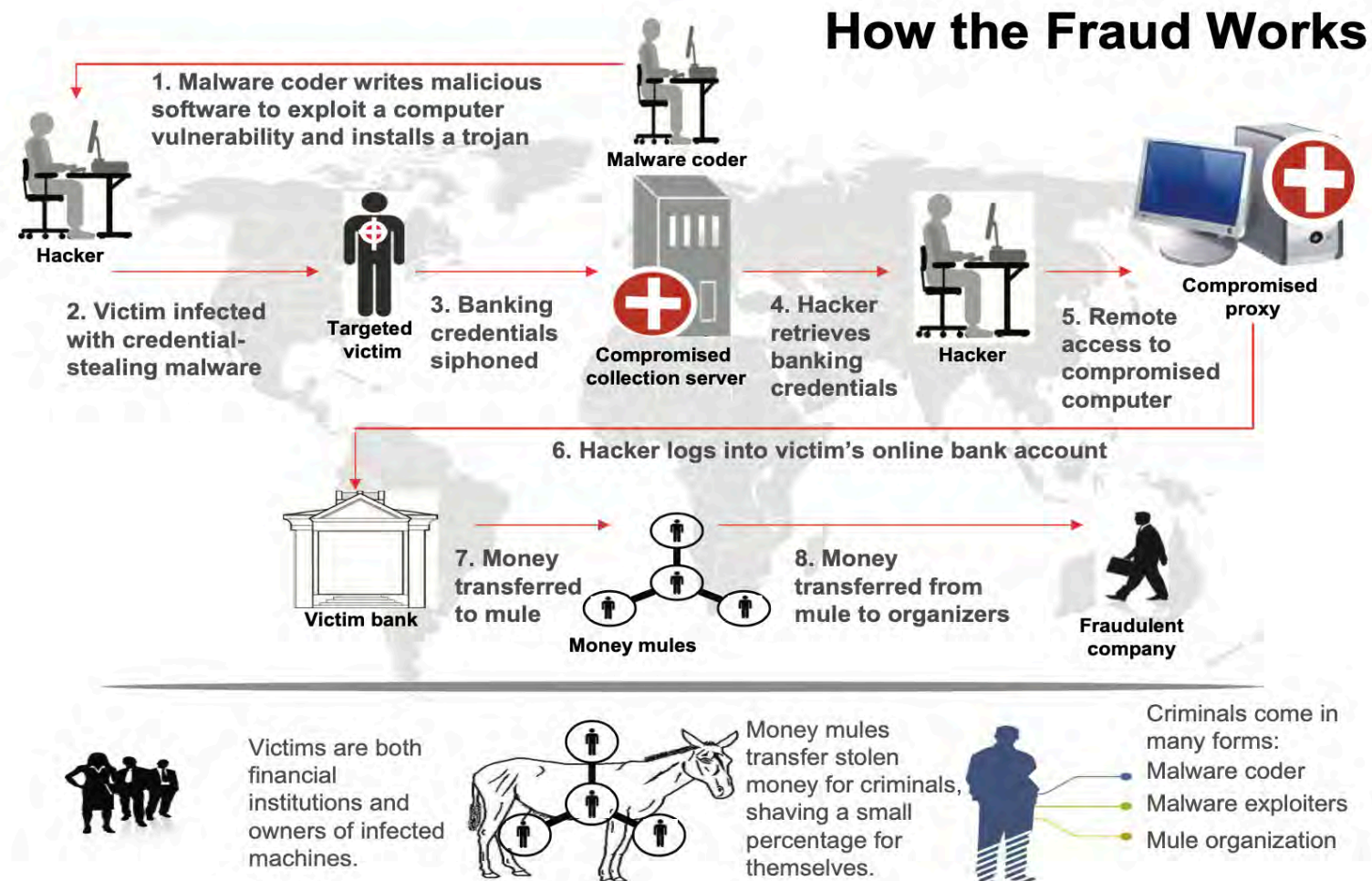
Cyber Risk is Business Risk

Financial Threats – www.ic3.gov

2021 Crime Types continued

By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$2,395,953,296	Lottery/Sweepstakes/Inheritance	\$71,289,089
Investment	\$1,455,943,193	Extortion	\$60,577,741
Confidence Fraud/Romance	\$956,039,740	Ransomware	*\$49,207,908
Personal Data Breach	\$517,021,289	Employment	\$47,231,023
Real Estate/Rental	\$350,328,166	Phishing/Vishing/Smishing/Pharming	\$44,213,707
Tech Support	\$347,657,432	Overpayment	\$33,407,671
Non-Payment/Non-Delivery	\$337,493,071	Computer Intrusion	\$19,603,037
Identity Theft	\$278,267,918	IPR/Copyright/Counterfeit	\$16,365,011
Credit Card Fraud	\$172,998,385	Health Care Related	\$7,042,942
Corporate Data Breach	\$151,568,225	Malware/Scareware/Virus	\$5,596,889
Government Impersonation	\$142,643,253	Terrorism/Threats of Violence	\$4,390,720
Advanced Fee	\$98,694,137	Gambling	\$1,940,237
Civil Matter	\$85,049,939	Re-shipping	\$631,466
Spoofing	\$82,169,806	Denial of Service/TDoS	\$217,981
Other	\$75,837,524	Crimes Against Children	\$198,950
Descriptors**			
Social Media	\$235,279,057	Virtual Currency	\$1,602,647,341

Money Mules



Money Mules

Unwitting or Unknowing

Individuals are unaware they are part of a larger scheme

- Often solicited via an online romance scheme or job offer
- Asked to use their established personal bank account or open a new account in their true name to receive money from someone they have never met in person
- May be told to keep a portion of the money they transferred
- Motivated by trust in the actual existence of their romance or job position

Witting

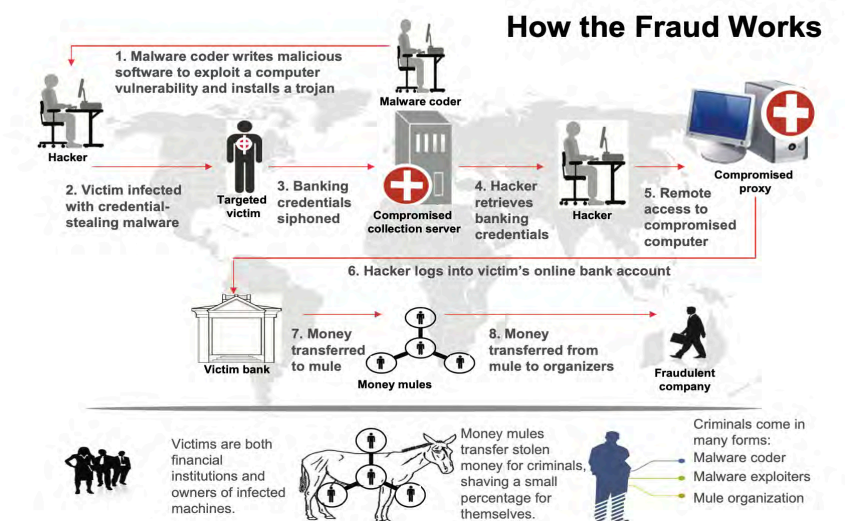
Individuals ignore obvious red flags or act willfully blind to their money movement activity

- May have been warned by bank employees they were involved with fraudulent activity
- Open accounts with multiple banks in their true name
- May have been unwitting at first but continue communication and participation
- Motivated by financial gain or an unwillingness to acknowledge their role

Complicit

Individuals are aware of their role and actively participate

- Serially open bank accounts to receive money from a variety of individuals/businesses for criminal reasons
- Advertise their services as a money mule, to include what actions they offer and at what prices. This may also include a review and/or rating by other criminal actors on the money mule's speed and reliability.
- Travel, as directed, to different countries to open financial accounts or register companies
- Operate funnel accounts to receive fraud proceeds from multiple lower level money mules
- Recruit other money mules
- Motivated by financial gain or loyalty to a known criminal group



#DontBeAMule



FBI FEDERAL BUREAU
OF INVESTIGATION

THINK TWICE

Money Muling is Illegal

#DontBeAMule

Working around Know-Your-Customer Requirements (~11 bank accounts, 7 banks, Shell Companies)

U.S. Attorneys » District of New Jersey » News

Department of Justice

U.S. Attorney's Office

District of New Jersey

SHARE

FOR IMMEDIATE RELEASE

Monday, August 8, 2022

Two Florida Men Charged with Conspiring to Launder Money Obtained from Internet-Enabled Scams

NEWARK, N.J. – Two Florida men were charged with conspiring to launder money taken from victims across the United States, many of whom were elderly, as a part of a series of romance scams and other internet fraud, U.S. Attorney Philip R. Sellinger announced today.

Marlin Perra, 63, of Lake Panasoffkee, Florida, and Leslie Lallande, 65, of Pompano Beach, Florida, were both arrested in Florida and are charged by complaint with one count of money laundering conspiracy. Both defendants are expected to have their initial appearances in the District of New Jersey at a date to be determined.

According to documents filed in this case and statements made in court:

UNITED STATES DISTRICT COURT DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Hon. Leda D. Wettre

v. : Mag. No. 22-13207

MARLIN PERRA, and : **CR**
LESLIE LALLANDE :

I, Heather Hendershot, being duly sworn, depose that the foregoing is true and correct to the best of my knowledge and belief.

SEE ATTACHMENT

I further state that I am a Special Agent in Charge of the Federal Bureau of Investigation, and that this complaint is based on information received from the

SEE ATTACHMENT

continued on the attached pages and made a

c. On or about February 18, 2020, Perra emailed "Nelson Nyarko" with the subject "fidelity wire instructions," in which Perra admonished: "know [sic] more messing around, i dont want to see medical bills, refrigerators, business help. it has to say cars, or automobiles, and no more putting me a he company on the edge, because theres some cheap some of bitch, half asses it, there asses are not on the line, but one more time of any crap, its al over..and i mean it, you people can't play by the united states banking rules. then go do something else[.]"

Based on my training and experience, I know that individuals who launder money are often aware that banks routinely monitor wire transfers to determine whether there is suspicious activity in an account that must be reported to U.S. regulators. Based on my training and experience and my familiarity with this investigation, I believe Perra's email described in the preceding subparagraph reflects that Perra knows that the individuals sending money to his account are sending it for purposes other than investing in car sales, and also knows that such transfers, if observed by a bank investigator, will raise suspicion.

Financial Threats – IC3 - \$1 Billion in reported losses

February 10, 2022

\$1 Billion in Losses Reported by Victims of Romance Scams

HOUSTON, TX—In 2021, some 24,000 victims across the United States reported losing approximately \$1 billion to romance scams.¹ It's likely that many more losses went unreported.

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

The criminals who carry out romance scams are experts at what they do and will seem genuine, caring, and believable. Con artists are present on most dating and social media sites.

The scammer's intention is to establish a relationship as quickly as possible, endear himself to the victim, and gain trust. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money.

Scam artists often say they are in the building and construction industry and are engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they ask for money for a medical emergency or unexpected legal fee.

If someone you meet online needs your bank account information to deposit money, they are most likely using your account to carry out other theft and fraud schemes.

Financial Threats – FTC - \$547 MILLION in reported losses

Reports of romance scams hit record highs in 2021

By: Emma Fletcher | Feb 10, 2022 10:30AM

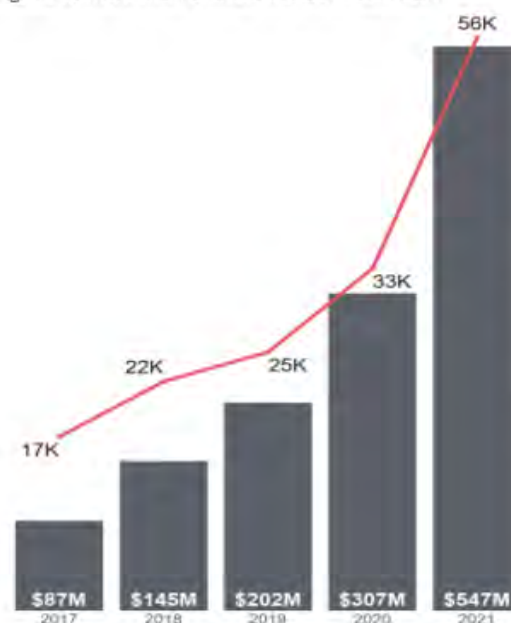
SHARE THIS PAGE



Online dating can be a great way to find lasting love – or even your next fling. But reports to the FTC suggest it also creates opportunities for scammers. In the past five years, people have reported losing a staggering \$1.3 billion to romance scams,[1][2] more than any other FTC fraud category. The numbers have skyrocketed in recent years, and 2021 was no exception – reported losses hit a record \$547 million for the year. That's more than six times the reported losses in 2017 and a nearly 80% increase compared to 2020. The median individual reported loss in 2021 was \$2,400.[3]

Reports about romance scams: Growth over five years

2021 total reported losses were more than 6 times what they were in 2017, and the number of reports grew to more than 3 times the 2017 number.



Reports show that romance scammers are masters of disguise. They create fake online profiles with attractive photos swiped from the web. Sometimes they even assume the identities of real people. They may study information people share online and then pretend to have common interests. And the details they share about themselves will always include built-in excuses for not meeting in person. For example, many reportedly claim to be serving overseas in the military or working on an offshore oil rig.

Many people who've experienced scams report being contacted on dating apps. But you don't have to be looking for love to be courted by a romance scammer. Reports of unexpected private messages on social media platforms are common. More than a third of people who said they lost money to an online romance scam in 2021 said it began on Facebook or Instagram.[4]

Romance scammers weave all sorts of believable stories to con people, but their old standby involves pleas for help while claiming one financial or health crisis after another. The scammers' stories might involve a sick child or a temporary inability to get to their money for a whole range of reasons. People who lost money to a romance scammer often report sending money repeatedly: they believe they're helping someone they care about. But it's all a lie.

In another common twist on the romance scam, people

Pig Butchering



Pig Butchering

support@xtb-market.com

LOGIN

REGISTER


xtb

Markets

HOME

SUPPORT

ACCOUNT



GET ACCESS TO YOUR ACCOUNT

SIGN IN

INVESTMENT PACKAGES

Invest with us and let us invest for you. Let's think, explore and dominate the market, all for you! you don't have to consider the risk of investing in capital market. Choose any investment plan and let us manage all the risk for you and please note that each investment (deposit) lasts for the said number of days as depicted on each investment plan.

STARTER PLAN

WEEKLY 15.7% FOR 4 TIMES

for 4 times

15.7% roi each time

CLASSIC PLAN

MONTHLY 39% FOR 4 TIMES

for 4 times

39% roi each time

PREMIUM PLAN

MONTHLY 40.5% FOR 8 TIMES

for 8 times

40.5% roi each time

PLATINUM PLAN

MONTHLY 45% FOR 6 TIMES

for 6 times

45% roi each time

<https://krebsonsecurity.com/2022/07/massive-losses-define-epidemic-of-pig-butchering/>

12

Financial Threats/Opportunities - Crypto

Russia's 'Gold Standard': What This Means For Gold And Bitcoin

Apr. 13, 2022 11:46 AM ET | SPDR Gold Trust ETF (GLD) | BTC-USD | 36 Comments | 12 Likes

Summary

- Russia has tied the value of its gas to gold, but it is not operating a gold standard.
 - This has helped support the ruble, and it has tremendous consequences on the world.
 - As the world becomes less dependent on the US dollar, Gold and Bitcoin will take its place.
 - I do much more than just articles at Technically Crypto: Members get access to model portfolios, regular updates, a chat room, and more.
- [Learn More »](#)



MEMORANDUM

FROM: FTI Consulting
RE: Summary of White House Executive Order Fact Sheet on Digital Assets
DATE: March 9, 2022

Today, the White House issued an Executive Order ("Order") on "[Ensuring Responsible Development of Digital Assets](#)" outlining the administration's first ever government-wide approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology. The administration also published a corresponding [fact sheet](#).

The intent of the Order is to streamline the administration's approach to regulating digital assets and address the pressing policy issues in this space. The Order acknowledges the rapid growth of the industry and how digital assets can reinforce American leadership on technology and support financial inclusion. However, the Order also outlines the implications of digital assets in the areas of consumer protection, financial stability, national security, illicit financing, and climate risk.

Also today, Treasury Secretary Janet Yellen issued a [press release](#), where she announced she would convene the Financial Stability Oversight Council (FSOC), a multi-agency body led by Treasury, to produce a report on the future of money and payment systems.

The Order's issuance comes as the digital assets industry has faced increased questions about its utility in the aftermath of sanctions against Russia for its invasion of Ukraine. In addition to complying with anti-money laundering (AML) rules, know-your-customer (KYC) regulations, and appropriate sanctions, the industry is facing questions about whether it should go further and restrict users or accounts tied to Russia, or if it could be used to subvert sanctions. During this time, it is more important than ever for the digital asset industry to clearly articulate its value and its responsible regulatory compliance standards.

Below is a compilation of key takeaways from the Order, which also includes sections on definitions that provides further clarity to the industry.

Key Takeaways:

- **Consumer, Business, and Investor Protections:** The Order directs several agencies including the Treasury Department, Commodity Futures Trading Commission (CFTC), Securities and Exchange Commission (SEC), Consumer Financial Protection Bureau (CFPB), and prudential bank regulators to develop digital asset sector policy recommendations. The Order also encourages regulators to ensure sufficient oversight and safeguards against any systemic financial risks posed by digital assets. The Order also points to privacy as an area to focus on in these reports.
- **Illicit Financing:** The Order directs all agencies to take an "unprecedented focus" to mitigate

Financial Threats - Crypto

Case 1:22-mj-00022-RMM Document 1 Filed 02/07/22 Page 1 of 1

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT
for the
District of Columbia

<p>United States of America v. Ilya Lichtenstein (AKA: Ilya "Dutch" Lichtenstein, Ilya Likhtenshteyn) (DOB: XXXXXXXX), and Heather Rhiannon Morgan (AKA: Razzlekhan) (DOB: XXXXXXXX)</p> <p style="text-align: center;"><i>Defendant(s)</i></p>	<p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p>	<p>Case: 1:22-mj-00022 Assigned to: Judge Meriweather, Robin M. Assign Date: 2/7/2022 Description: COMPLAINT W/ ARREST WARRANT</p>
---	---	--

CRIMINAL COMPLAINT

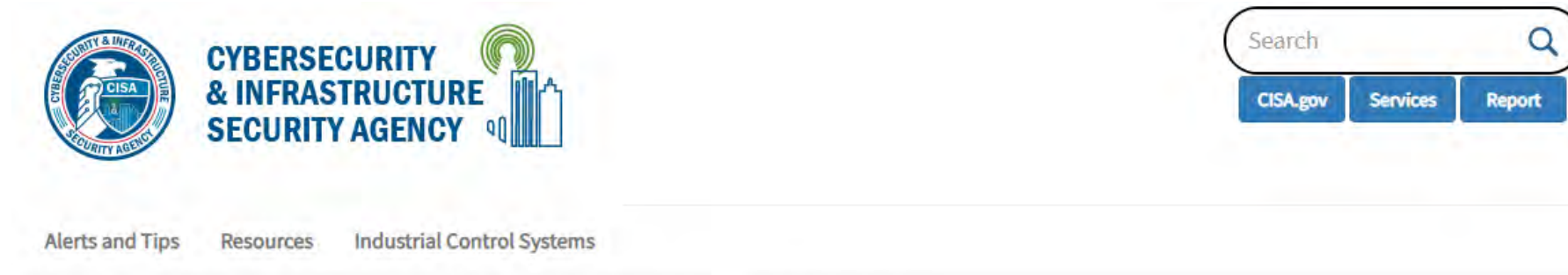
I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of August 2016 to February 2022 in the county of _____ in the
_____ in the District of Columbia, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1956(h) (Money Laundering Conspiracy)	
18 U.S.C. § 371 (Conspiracy To Defraud the United States)	

Self-proclaimed 'Crocodile of Wall Street' and her husband are arrested for 'laundering \$4.5B in Bitcoin stolen in 2016 Bitfinex exchange hack': Authorities recover \$3.6B after seizing private keys to couple's digital wallets

North Korean Threats



North Korea Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the North Korean government's malicious cyber activities. The U.S. Government (USG) refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes a [complete list of related CISA publications](#), many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to North Korean government actors). Additionally, this page provides instructions on how to [report related threat activity](#).

The North Korean government—officially known as the Democratic People's Republic of Korea (DPRK)—employs malicious cyber activity to collect intelligence, conduct attacks, and generate revenue.[1],[2] Recent advisories published by CISA and other unclassified sources reveal that North Korea is conducting operations worldwide. According to the U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment, "North Korea's cyber program poses a growing espionage, theft, and attack threat." Specifically, the Assessment states, "North Korea has conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, potentially stealing hundreds of millions of dollars, probably to fund government priorities, such as its nuclear and missile programs." [3]



Latest U.S. Government Report on North Korean Malicious Cyber Activity

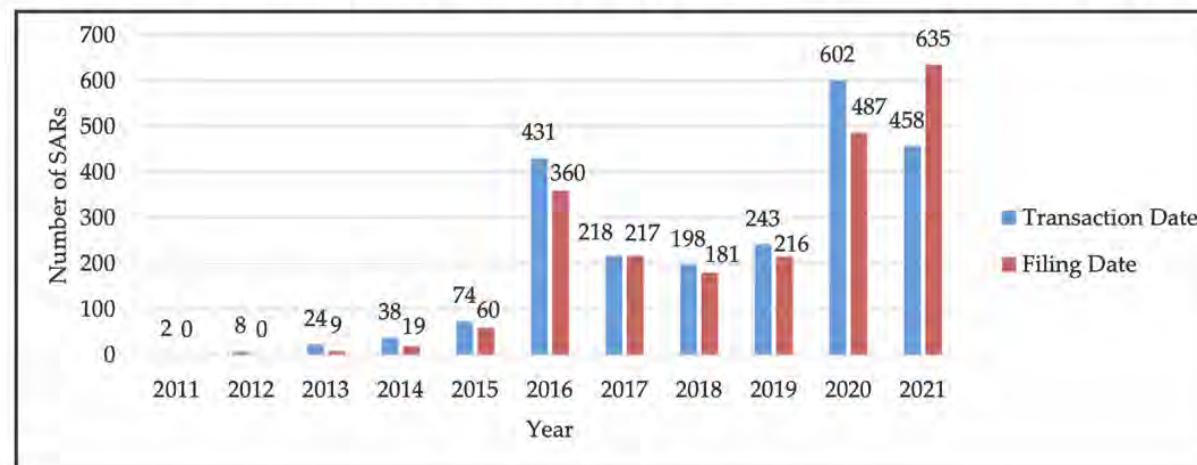
On February 17, 2021, CISA, the Federal Bureau of Investigation (FBI), and the Department of the Treasury identified malware and other indicators of compromise (IOCs) used by the North Korean government to facilitate the theft of cryptocurrency—referred to by the USG as "AppleJeus." See the [Joint FBI-CISA-Treasury Cybersecurity Advisory: AppleJeus: Analysis of North Korea's Cryptocurrency Malware](#) for details, including Malware Analysis Reports (MARs) on AppleJeus malware versions: Celas Trade Pro, JMT Trading, Union Crypto, Kupay Wallet, CoinGoTrade, Dorusio, and Ants2Whale.

The [North Korean Malicious Cyber Activity](#) section below lists all CISA Advisories, Alerts, and MARs on North Korea's malicious cyber activities.

Ransomware Risk

FinCEN analysis of ransomware-related SARs filed during the first half of 2021 indicates that ransomware is an increasing threat to the U.S. financial sector, businesses, and the public. The number of ransomware-related SARs filed monthly has grown rapidly, with 635 SARs filed and 458 transactions reported between 1 January 2021 and 30 June 2021 (“the review period”), up 30 percent from the total of 487 SARs filed for the entire 2020 calendar year.³ The total value of suspicious activity reported in ransomware-related SARs during the first six months of 2021 was \$590 million, which exceeds the value reported for the entirety of 2020 (\$416 million).

Figure 1. Number of Ransomware-Related SARs and Transactions, 2011 to June 2021¹⁷



Ransomware examples

Let's start

10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from no

We received millions of dollars profit by partnering with other well-known cryptolockers.

We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack:

- Medicine (only: hospitals, any palliative care to a large extent) in the distribution of the
- Funeral services (Morgues, crematoriums)
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the ransom.

Before any attack, we carefully analyze your company.

You can ask all your questions in the chat.

We provide the following guarantees for you:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors.
- We guarantee deletion of all uploaded files.

If you refuse to pay:

- We will publish all your data and store it.
- We will send notification of your leak.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if you don't want to pay, you will add to the

PYSA

Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
[redacted]@protonmail.com
[redacted]@protonmail.com

FAQ:

1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).

2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.

Gentlemen!

Your business is at serious risk.
There is a significant hole in the security system of your company.
We've easily penetrated your network.
You should thank the Lord for being hacked by serious people not some stupid schoolboys or dangerous punks.
They can damage all your important data just for fun.

Now your files are crypted with the strongest millitary algorithms RSA4096 and AES-256.
No one can help you to restore files without our special decoder.

Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.

If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information (Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.
Please don't forget to write the name of your company in the subject of your e-mail.

You have to pay for decryption in Bitcoins.
The final price depends on how fast you write to us.
Every day of delay will cost you additional +0.5 BTC
Nothing personal just business

As soon as we get bitcoins you'll get all your decrypted data back.
Moreover you will get instructions how to close the hole in security and how to avoid such problems in the future
+ we will recommend you special software that makes the most problems to hackers.

Attention! One more time !

Do not rename encrypted files.
Do not try to decrypt your data using third party software.

P.S. Remember, we are not scammers.
We don't need your files and your information.
But after 2 weeks all your files and keys will be deleted automatically.
Just send a request immediately after infection.
All data will be restored absolutely.
Your warranty - decrypted samples.

contact emails
[redacted]@tutanota.com
or
[redacted]@protonmail.com

BTC wallet:
[redacted]

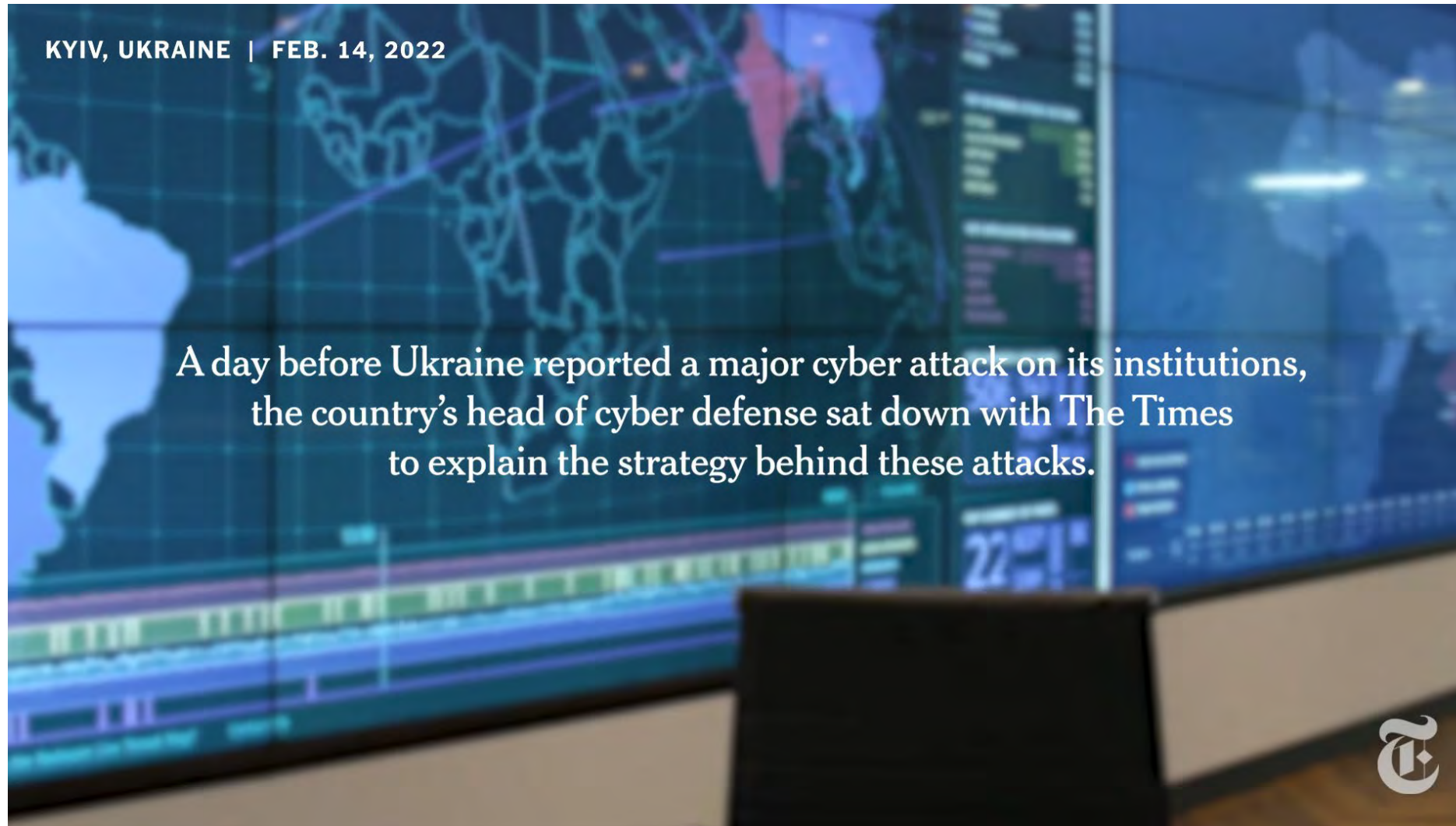
Ryuk
No system is safe

OK

Russia “Arrested” Revil Ransomware Gang: Just before Ukrainian invasion



Financial Threats



CCP Threats

February 1, 2022

[Twitter](#)
[Facebook](#)
[Email](#)

China's Quest for Economic, Political Domination Threatens America's Security

Director Wray Discusses Threats Posed by Government of China

The Chinese government's disregard for global leadership norms, ruthless hunger for economic superiority, and desire to influence American politics make it a threat to U.S. national security, FBI Director Christopher Wray said on January 31.

"There is so much good we could do with a responsible Chinese government: crack down on cybercriminals, stop money launderers, reduce opioid overdose deaths. But at the FBI, we're focused on the reality of the Chinese government today," Wray said during a keynote address at the Ronald Reagan Presidential Library and Museum in Simi Valley, California.

The threat's complexity is rooted in the intrinsic entanglement of the American and Chinese economies, which is fueled by a high U.S. demand for Chinese-made products and a steady exchange of students between American and Chinese borders. Wray stressed that China has pulled no punches about capitalizing on this interconnectedness to chase economic superiority.



FBI Director Christopher Wray discussed the myriad threats our nation faces from the Chinese government and Chinese Communist Party during a speech at the Ronald Reagan Presidential Library and Museum in Simi Valley, California, on January 31, 2022. (Photo courtesy of Reagan Library)

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, July 19, 2021

Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research

Indictment Alleges Three Defendants Were Officers in the Hainan State Security Department (HSSD), a provincial arm of China's Ministry of State Security (MSS)

A federal grand jury in San Diego, California, returned an indictment in May charging four nationals and residents of the People's Republic of China with a campaign to hack into the computer systems of dozens of victim companies, universities and government entities in the United States and abroad between 2011 and 2018. The indictment, which was unsealed on Friday, alleges that much of the conspiracy's theft was focused on information that was of significant economic benefit to China's companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes. The defendants and their Hainan State Security Department (HSSD) conspirators sought to obfuscate the Chinese government's role in such theft by establishing a front company, Hainan Xiandun Technology Development Co., Ltd. (海南仙盾) (Hainan Xiandun), since disbanded, to operate out of Haikou, Hainan Province.

The two-count indictment alleges that Ding Xiaoyang (丁晓阳), Cheng Qingmin (程庆民) and Zhu Yunmin (朱允敏), were HSSD officers responsible for coordinating, facilitating and managing computer hackers and linguists at Hainan Xiandun and other MSS front companies to conduct hacking for the benefit of China and its state-owned and sponsored instrumentalities. The indictment alleges that Wu Shurong (吴淑荣) was a computer hacker who, as part of his job duties at Hainan Xiandun, created malware, hacked into computer systems operated by foreign governments, companies and universities, and supervised other Hainan Xiandun hackers.

Iranian/Election Threats – “Proud Boys”

Voters in Florida, Arizona, and Alaska received threatening emails earlier this week demanding that they “Vote for Trump or else!” The emails purported to come from the “Proud Boys,” a violent right-wing group. But a Motherboard investigation found the emails were spoofed, suggesting a different type of operation.

SUBSCRIBE

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, November 18, 2021

Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election

An indictment was unsealed in New York today charging two Iranian nationals for their involvement in a cyber-enabled campaign to intimidate and influence American voters, and otherwise undermine voter confidence and sow discord, in connection with the 2020 U.S. presidential election.

According to court documents, Seyyed Mohammad Hosein Musa Kazemi (سید محمد حسین موسی کاظمی), aka Mohammad Hosein Musa Kazem, aka Hosein Zamani, 24, and Sajjad Kashian (سجاد کاشیان), aka Kiarash Nabavi, 27, both of Iran, obtained confidential U.S. voter information from at least one state election website; sent threatening email messages to intimidate and interfere with voters; created and disseminated a video containing disinformation about purported election infrastructure vulnerabilities; attempted to access, without authorization, several states’ voting-related websites; and successfully gained unauthorized access to a U.S. media company’s computer network that, if not for successful FBI and victim company efforts to mitigate, would have provided the conspirators another vehicle to disseminate false claims after the election.

Iranian Threats

Man With Assault Rifle, 66 Ammo Rounds Arrested at Iranian Dissident's NYC Home: FBI

The woman, Masih Alinejad, is a well-known Iranian writer and dissident who last year was the alleged target of a kidnapping plot by Iranian agents, the FBI says

By **Jonathan Dienst**, **Myles Miller** and **Ken Dilanian** • Published July 31, 2022 • Updated on August 1, 2022 at 1:28 pm



Insider Threats



The USS Virginia

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Sunday, October 10, 2021

Maryland Nuclear Engineer and Spouse Arrested on Espionage-Related Charges

Jonathan and Diana Toebe, both of Annapolis, Maryland, were arrested in Jefferson County, West Virginia, by the FBI and the Naval Criminal Investigative Service (NCIS) on Saturday, Oct. 9. They will have their initial appearances on Tuesday, Oct. 12, in federal court in Martinsburg, West Virginia. For almost a year, Jonathan Toebe, 42, aided by his wife, Diana, 45, sold information known as Restricted Data concerning the design of nuclear-powered warships to a person they believed was a representative of a foreign power. In actuality, that person was an undercover FBI agent. The Toebes have been charged in a criminal complaint alleging violations of the Atomic Energy Act.

“The complaint charges a plot to transmit information relating to the design of our nuclear submarines to a foreign nation,” said Attorney General Merrick B. Garland. “The work of the FBI, Department of Justice prosecutors, the Naval Criminal Investigative Service and the Department of Energy was critical in thwarting the plot charged in the complaint and taking this first step in bringing the perpetrators to justice.”

Insider Threats



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, November 21, 2019

Chinese National Who Worked at Monsanto Indicted on Economic Espionage Charges

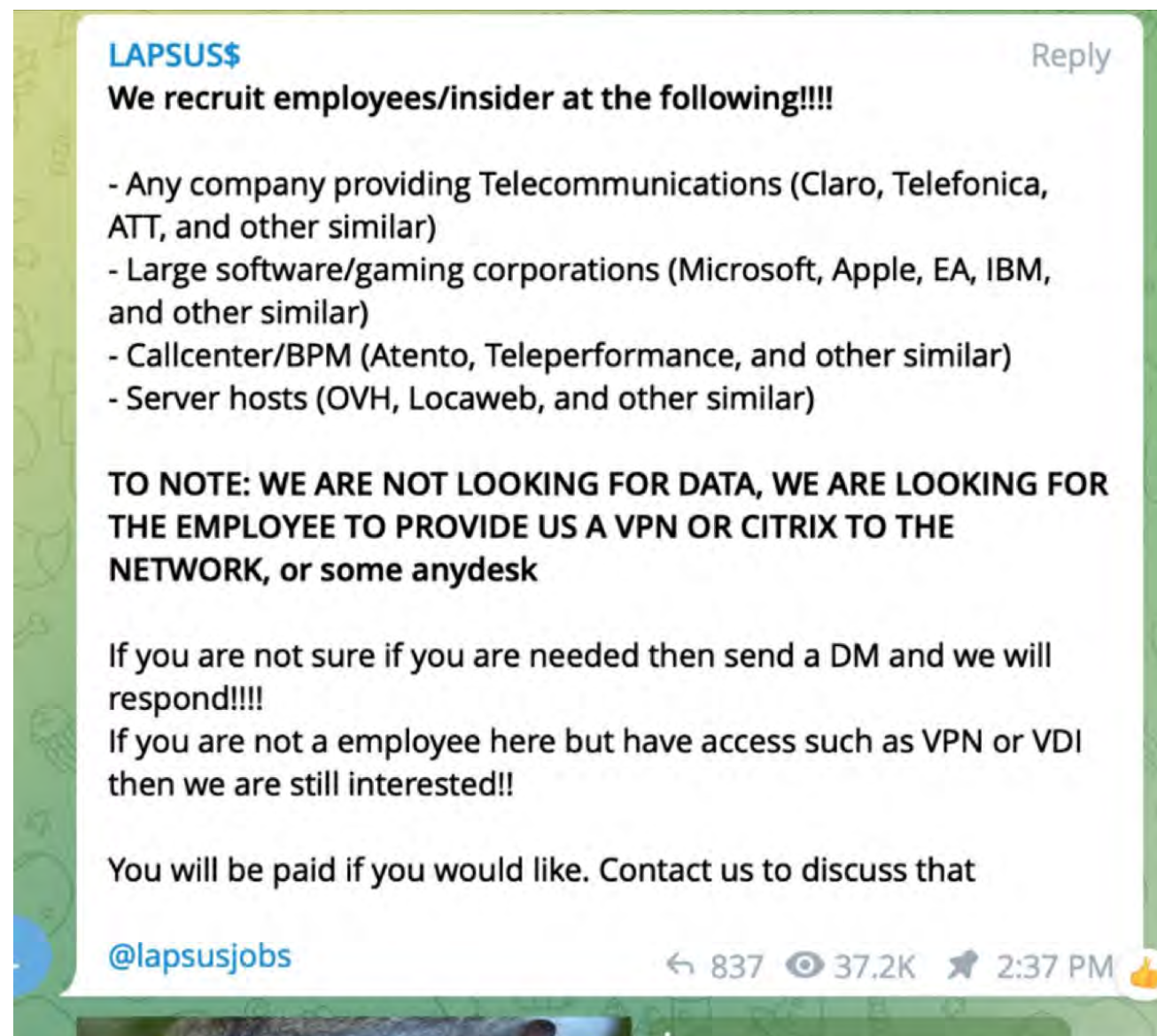
Haitao Xiang, 42, formerly of Chesterfield, Missouri, was indicted today by a federal grand jury on one count of conspiracy to commit economic espionage, three counts of economic espionage, one count of conspiracy to commit theft of trade secrets and three counts of theft of trade secrets.

According to the indictment, Xiang was employed by Monsanto and its subsidiary, The Climate Corporation, from 2008 to 2017, where he worked as an imaging scientist. Monsanto and The Climate Corporation developed a digital, on-line farming software platform that was used by farmers to collect, store, and visualize critical agricultural field data and increase and improve agricultural productivity for farmers. A critical component to the platform was a proprietary predictive algorithm referred to as the Nutrient Optimizer. Monsanto and The Climate Corporation considered the Nutrient Optimizer a valuable trade secret and their intellectual property.


“The indictment alleges another example of the Chinese government using Talent Plans to encourage employees to steal intellectual property from their U.S. employers,” said Assistant Attorney General for National Security John C. Demers. “Xiang promoted himself to the Chinese government based on his experience at Monsanto. Within a year of being selected as a Talent Plan recruit, he quit his job, bought a one-way ticket to China, and was caught at the airport with a copy of the company’s proprietary algorithm before he could spirit it away.”

“The revolutionary technology at the core of this case represents both the best of American ingenuity and why the Chinese government is so desperate to steal it for themselves,” said Assistant Director John Brown. “The FBI is committed to working with a host of partners to stop individuals, like the defendant in this case, from engaging in economic espionage to acquire information and technology for a foreign government that is either unable or unwilling to compete on a level playing field. Our country’s economic security is our national security, and the FBI will always do everything in our power to protect it.”


Insider Threats/Emerging Threats



Insider Threats/Emerging Threats



[Our Company](#)
[News](#)
[Responsibility](#)
[Investors](#)
[Careers](#)



SIM Swapping

Stay a step ahead of the scammers. Educate yourself on some of the most common frauds and scams.

[Identity Theft](#)
[Account Take Over](#)
[Phishing](#)
[Spoofing](#)
[Pre-texting](#)
[Slamming & Cramming](#)
[Malware](#)
[Smishing & Spam Text Messages](#)
[SIM Swapping](#)

What is a SIM swap?

SIM swapping, sometimes called a SIM hijacking attack, occurs when the device tied to a customer's phone number is fraudulently manipulated. Fraudsters usually employ SIM swapping as a way to receive one-time security codes from banks, cryptocurrency exchanges, and other financial institutions.

How does SIM swapping work?

Fraudsters typically perpetuate SIM hijacks after a customer's personal information has been obtained via phishing attacks or by purchasing compromised account credentials through dark web marketplaces. Victims of hijacking attacks frequently have their email accounts compromised prior to the SIM change, allowing fraudsters to intercept communications from providers like Verizon. Phishing occurs when criminals send fraudulent requests for personal information to victims, usually posing as a company or government agency.



Case studies

Examples of Cybersecurity Incidents



Organization Breach

Following a state-sponsored breach, we were appointed to conduct a full forensic clean-up following the investigation by firm

This involved multiple locations and devices to ensure all traces of the malware deployed were eradicated. This was conducted over a 2-month period, 24 hours-a-day, and involved mobile devices, desktop computers, and laptops



Financial Institution Hack

One of the largest public sector banks in India

Hackers gained access to the bank's SWIFT system and transferred \$170m from the Bank's account in the US to accounts in Cambodia.

We conducted end-to-end incident response, identifying chain of events, conducting malware reverse engineering, working with law enforcement, and helping with remediation



Ransomware

Multiple clients

Developed ransomware tool – Radar – and delivered seven engagements. Radar was able to prevent and remediate ransomware infections



YAHOO!

Search engine breach impacting 3 billion users

We were brought in to provide technical counsel, perform complex investigations, and analyze harm related to plaintiffs

We provided expert testimony in the case

Examples of Cybersecurity Incidents



Ransomware

E-commerce billing and finance platform

Weak customer credentials led to a highly successful, laterally moving attack that was able to successfully encrypt servers in a matter of hours

We assembled a cross-segment team to deploy to the client site immediately, and successfully negotiated with the malicious actor to get the client back up and running



Cyber Breach Communications

Consumer credit reporting agency

After an earlier data breach, the agency discovered that additional consumers had some portion of their personally identifiable information stolen

We arranged an embargoed media story, media-trained a C-suite executive to prepare for background interviews, and developed communications materials for customers, policymakers, employees, and investors



Cyber Vulnerabilities Discovery

Multi-billion dollar energy sector business

In connection with an unrelated internal investigation, we identified several cyber vulnerabilities, as well as employees engaged in suspicious activity

We prepared and presented a cybersecurity assessment and a remediation plan to the company's CEO and Board of Directors, and identified two employees who were actively stealing trade secrets



Security Breach

Large healthcare entity

A security breach resulted in an investigation by the Office of Civil Rights (OCR)

We were engaged to help manage breach communication and documentation and to develop a robust privacy and security program to protect against future compliance risk



Fraud Protection = “Have a plan”

“Cyber” is in Everything! Fraud can Effect Everyone!!

- It is necessary to have a plan which includes input from multiple business segments
 - Your LEGAL Team is your friend!
 - COMMUNICATIONS TEAM (for Companies)
 - INFORMATION TECHNOLOGY/FORENSIC TEAM (Corporate/Best Buy)
 - Outside vendors/assistance (Friends and Family?)
 - Help educate each other – have these conversations with other co-workers and family members



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**

- cisa.gov/uscert
- [Report Cyber Issue](#)
- [Subscribe to Alerts](#)



CYBERSECURITY



INFRASTRUCTURE
SECURITY



EMERGENCY
COMMUNICATIONS



NATIONAL RISK
MANAGEMENT



ABOUT
CISA



MEDIA



SHIELDS UP

LEARN MORE →

4 STEPS TO KEEP YOU CYBER SAFE

1



TURN ON
MULTI-FACTOR
AUTHENTICATION

2

UPDATE YOUR
SOFTWARE



THINK BEFORE
YOU CLICK


3

USE STRONG
PASSWORDS



4




National Cyber Security Centre

[ABOUT NCSC](#)
[CISP](#)
[REPORT AN INCIDENT](#)
[CONTACT US](#)

[Home](#)
[Information for...](#)
[Advice & guidance](#)
[Education & skills](#)
[Products & services](#)
[News, blogs, events...](#)

[Home](#)

Information for...

[Individuals & families](#)
[Self employed & sole traders](#)
[Small & medium sized organisations](#)
[Large organisations](#)
[Public sector](#)
[Cyber security professionals](#)


Cyber Aware and staying secure online

From banking to shopping, and streaming to social media, people are spending more time than ever online. Cyber Aware is the government's advice on how to stay secure online.

[Visit Cyber Aware](#)

As well as our six Cyber Aware actions, the NCSC has provided further guidance for those looking to stay secure online.


- Use a strong and separate password for your email +
- Install the latest software and app updates +
- Turn on 2-Step Verification (2SV) +
- Password managers: using browsers and apps to safely store your passwords +
- Backing up your data +
- Three random words +



CyberSprinters

Exciting new interactive online security resources for 7-11 year olds.

[Game and activities](#)



Cyber Security for Schools

Practical advice, resources and



MOBILE SECURITY

A study by Pew Research Center found that almost all Americans, 90%, now have a cell phone and 58% own a smartphone.

Almost all aspects of our life are now connected to the Internet and our mobile devices. Americans are increasingly using their phones for banking, online shopping, and social media. The more we travel and access the Internet on the go, the more risks we face on our mobile devices.

Tips for Securing Mobile Devices

Think Before You Connect. Before you connect to any public Wi-Fi hotspot, confirm the name of the network and exact login procedures to ensure that the network is legitimate.

- **Guard Your Mobile Device.** In order to prevent theft, unauthorized access and loss of sensitive information, never leave your mobile devices unattended in a public place.
- **Keep It Locked.** Always lock your device when you are not using it. Use strong PINs and passwords to prevent others from accessing your device.
- **Update Your Mobile Software.** Keep your operating system software and apps updated, which will improve your device's ability to defend against malware.
- **Only Connect to the Internet if Needed.** Disconnect your device from the Internet when you aren't using it and make sure your device isn't programmed to automatically connect to Wi-Fi.
- **Know Your Apps.** Be sure to thoroughly review the details and specifications of an application before you download it. Delete any apps that you are not using to increase your security.



FRAUD & PHISHING

Fraud is the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right. **Phishing** is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.

Tips

- Most organizations – banks, universities, companies, etc. - don't ask for your personal information over email. Beware of requests to update or confirm your personal information.
- Do not open attachments, click links, or respond to email messages from unknown senders or companies.
- Don't access your personal or banking accounts online from a public computer or kiosk.
- Beware of "free" prizes; if you think an offer is too good to be true, then it probably is.
- Make sure you change your passwords often and avoid using the same password for multiple accounts.
- Install and regularly update software firewall, antivirus, and anti-spyware programs. These software programs can help to protect the data on your computer, and can easily be purchased on the web or at your local office supply store.

<https://www.ic3.gov/>



If the Director of the FBI and the CIA can be targeted...





Experts with Impact™

Todd Renner, Senior Managing Director

Todd.Renner@FTIConsulting.com

Mobile: +1 404.791.2881

LinkedIn: www.linkedin.com/in/todd-renner-fbi