K2's Ripped From The Headlines

Outrageous Tales Of Cybercrimes

K2 Enterprises

What About Randy?

- 40+ years of technology experience, top-rated speaker for almost 40 years
- Top 25 Thought Leaders in Accounting 2011-2024
- 2004-2023 Accounting Today 100 Most Influential in Accounting for twenty years
- Inducted Accounting Hall of Fame, Feb 2011
- Monthly columns on technology in CPAPractice Advisor, weekly podcasts on technology
- Published author of six books, From Hutchinson, KS
- randy@k2e.com or randyj@nmgi.com
- 620-664-6000 x 112

Major Topics

- Common security weaknesses that occur with hardware and software at home and in the office
- Malware, ransomware, data breach, and incident response tips
- Internal control failures which result in the theft of assets or unauthorized manipulation of data

Learning Objectives

- List at least three major security incidents reported in the headlines in the last year, and explain at least one internal control design or operation flaw that allowed the hack to occur
- Select the correct definitions for security terms such as attack surface, vulnerability, exploit, social engineering, phishing, malware, heuristics, biometrics, and multi-factor authentication (MFA)
- List at least three best practices learned by reviewing the control failures cited in the case studies

FEDERAL BUREAU OF INVESTIGATION
iC3
INTERNET CRIME COMPLAINT CENTER

2023 FBI INTERNET CRIME COMPLAINT CENTER (IC3) ANNUAL REPORT

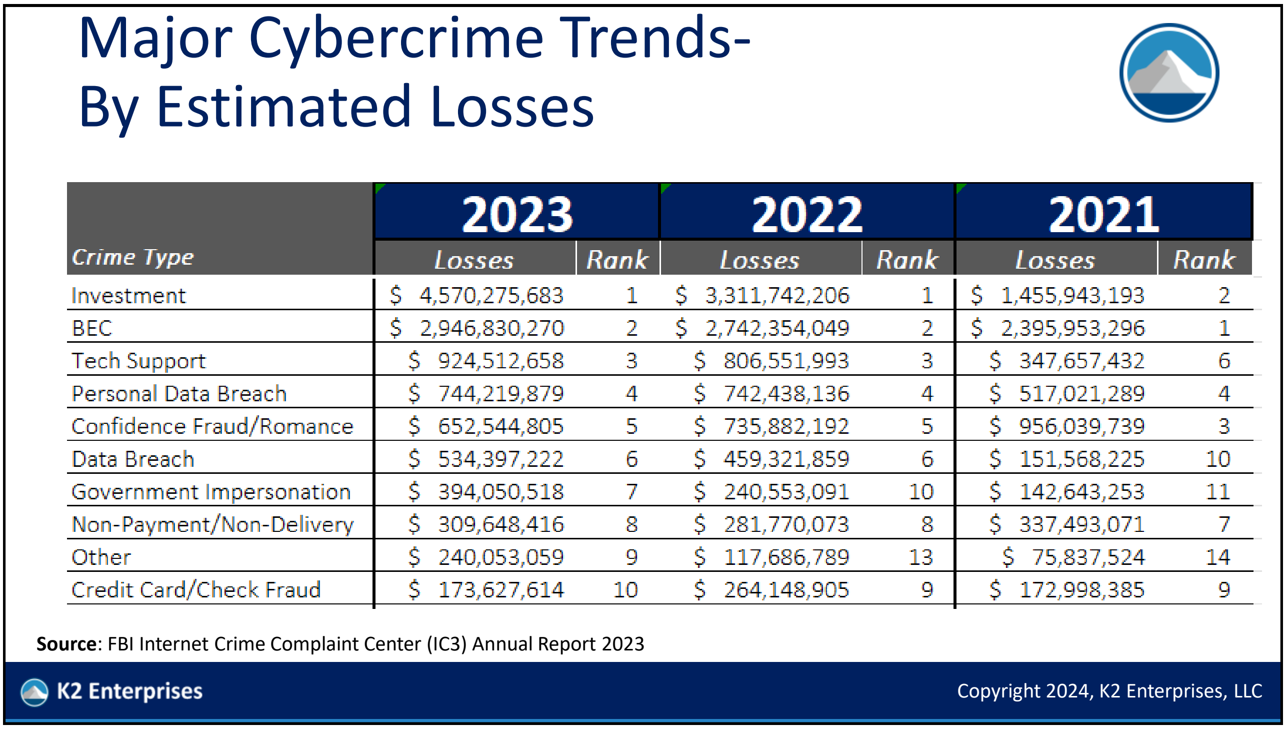
Who Is IC3?

- FBI Internet Crime Complaint Center
- Website: www.ic3.gov
- IC3's annual reports provide tracking on cybercrime trends and insights into how and where these crimes are being committed
- Received **691,701 complaints in 2023**, down from 724,516 in 2022 and 759,165 in 2021
- The **estimated losses** associated with those claims increased to **$12.35 billion in 2023**, up from $10.93 billion in 2022 and $7.69 billion in 2021.

Major Cybercrime Trends- By Number of Complaints

	2023		2022		2021	
Crime Type	*Complaints*	*Rank*	*Complaints*	*Rank*	*Complaints*	*Rank*
Phishing/Spoofing	298,878	1	321,136	1	342,494	1
Personal Data Breach	55,851	2	58,859	2	51,829	3
Non-Payment/Non-Delivery	50,523	3	51,679	3	82,478	2
Extortion	48,223	4	39,416	4	39,360	5
Investment	39,570	5	30,529	6	20,561	8
Tech Support	37,560	6	32,538	5	23,903	7
BEC	21,489	7	21,832	9	19,954	9
Identity Theft	19,778	8	27,922	7	51,629	4
Confidence Fraud/Romance	17,823	9	19,021	10	24,299	6
Employment	15,443	10	14,946	11	15,253	11

Source: FBI Internet Crime Complaint Center (IC3) Annual Report 2023



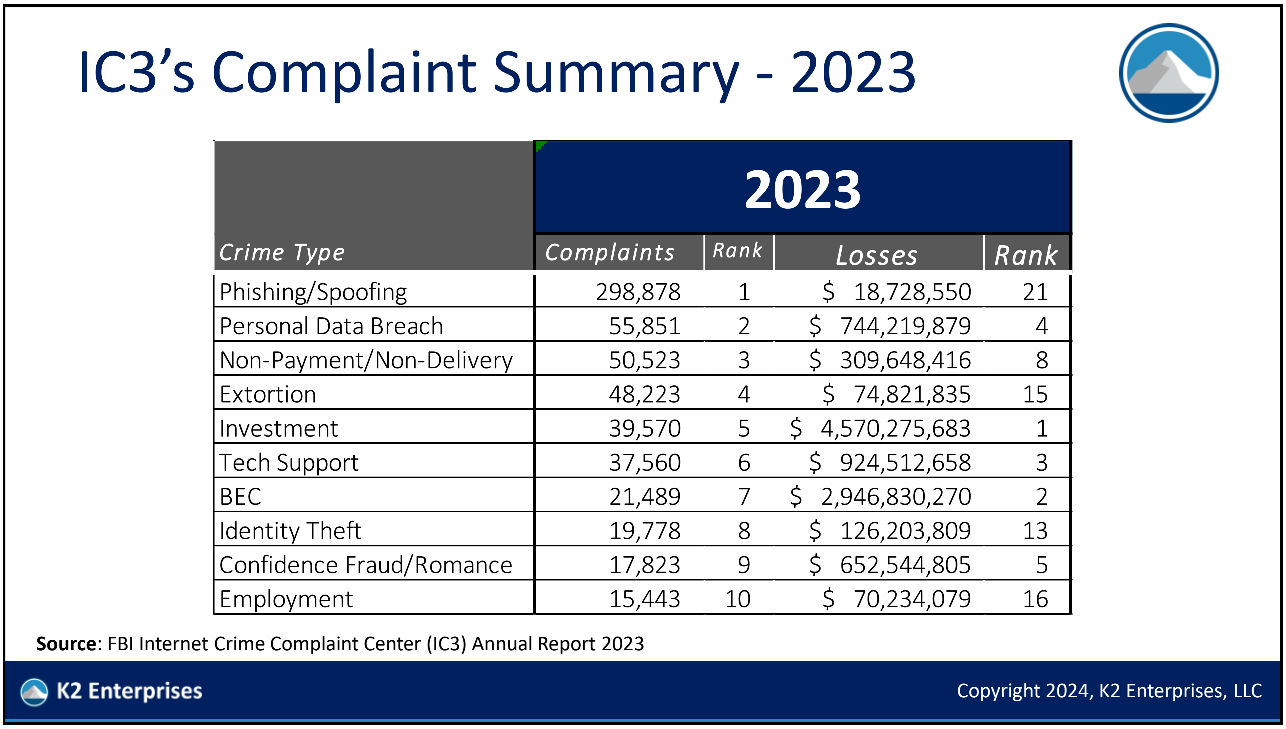
Major Cybercrime Trends- By Estimated Losses

	2023		2022		2021	
Crime Type	*Losses*	*Rank*	*Losses*	*Rank*	*Losses*	*Rank*
Investment	$ 4,570,275,683	1	$ 3,311,742,206	1	$ 1,455,943,193	2
BEC	$ 2,946,830,270	2	$ 2,742,354,049	2	$ 2,395,953,296	1
Tech Support	$ 924,512,658	3	$ 806,551,993	3	$ 347,657,432	6
Personal Data Breach	$ 744,219,879	4	$ 742,438,136	4	$ 517,021,289	4
Confidence Fraud/Romance	$ 652,544,805	5	$ 735,882,192	5	$ 956,039,739	3
Data Breach	$ 534,397,222	6	$ 459,321,859	6	$ 151,568,225	10
Government Impersonation	$ 394,050,518	7	$ 240,553,091	10	$ 142,643,253	11
Non-Payment/Non-Delivery	$ 309,648,416	8	$ 281,770,073	8	$ 337,493,071	7
Other	$ 240,053,059	9	$ 117,686,789	13	$ 75,837,524	14
Credit Card/Check Fraud	$ 173,627,614	10	$ 264,148,905	9	$ 172,998,385	9

Source: FBI Internet Crime Complaint Center (IC3) Annual Report 2023

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC



IC3's Complaint Summary - 2023

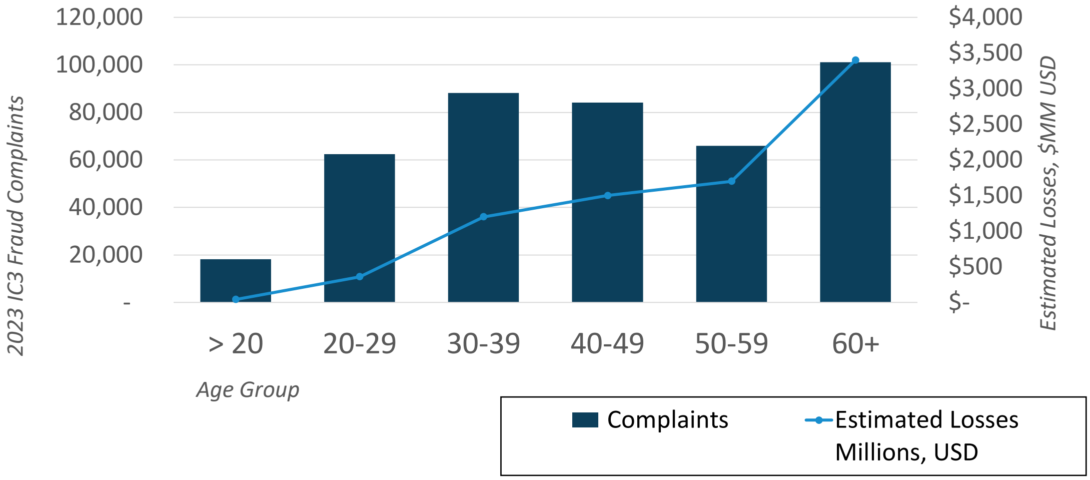
	2023			
Crime Type	*Complaints*	*Rank*	*Losses*	*Rank*
Phishing/Spoofing	298,878	1	$ 18,728,550	21
Personal Data Breach	55,851	2	$ 744,219,879	4
Non-Payment/Non-Delivery	50,523	3	$ 309,648,416	8
Extortion	48,223	4	$ 74,821,835	15
Investment	39,570	5	$ 4,570,275,683	1
Tech Support	37,560	6	$ 924,512,658	3
BEC	21,489	7	$ 2,946,830,270	2
Identity Theft	19,778	8	$ 126,203,809	13
Confidence Fraud/Romance	17,823	9	$ 652,544,805	5
Employment	15,443	10	$ 70,234,079	16

Source: FBI Internet Crime Complaint Center (IC3) Annual Report 2023

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC

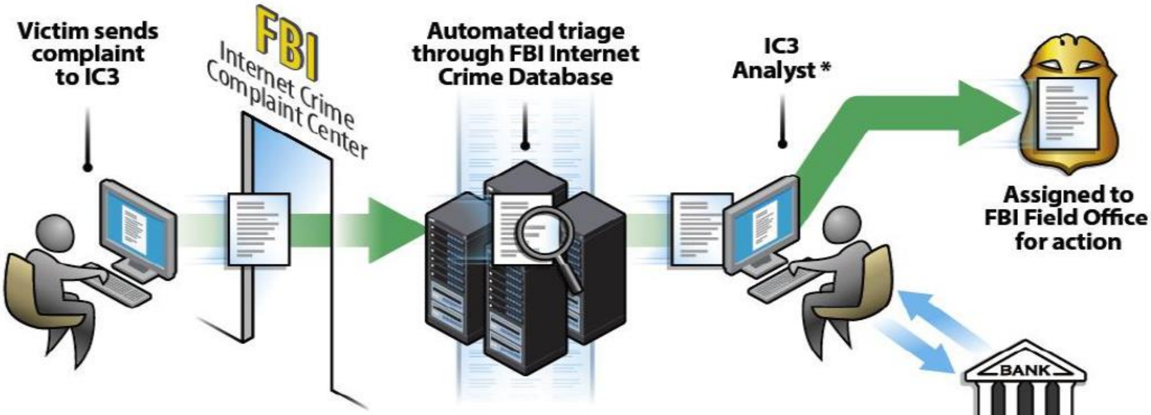
2023 IC3 Complainant Demographics



K2 Enterprises

IC3 Recovery Asset Team Process

Source: FBI Internet Crime Complaint Center (IC3) Annual Report 2023



Victim sends complaint to IC3
FBI
Internet Crime Complaint Center
Automated triage through FBI Internet Crime Database
IC3 Analyst *
Assigned to FBI Field Office for action
BANK
Financial Institution

* If criteria are met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

K2 Enterprises

Guidance For Complainants Who Send Wire Transfers

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Never make any payment changes without verifying the change with the intended recipient; verify email addresses are accurate when checking email on a cell phone or other mobile device.

Source: FBI Internet Crime Complaint Center (IC3) Annual Report 2023

Goals of RAT-Financial Institution Partnership

- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Source: FBI Internet Crime Complaint Center (IC3) Annual Report 2023

Lessons Learned

- The dollars lost to investment scams reported to IC3 tripled between 2021 and 2023
- Although phishing is the most common type of attack reported to IC3, the majority of the loss dollars for 2023 are in investment scams ($4.57B USD) and business e-mail compromises ($2.95B USD)
- FBI/IC3 has a team that works with financial institutions to recover funds from wire transfers and investment scams which can be activated by either FBI or IC3 after a complaint is made at ic3.gov

“What’s a Pig Butchering Scam? Here’s How to Avoid Falling Victim to One”, ProPublica, 9/19/2022

“CFTC Charges Crypto Platform Debiex With $2.3M 'Pig Butchering' Digital Asset Scheme”, Law.com, 1/19/2024

“With ‘Pig Butchering’ Scams on the Rise, FBI Moves to Stop the Bleeding”, NBC News, 2/5/2024

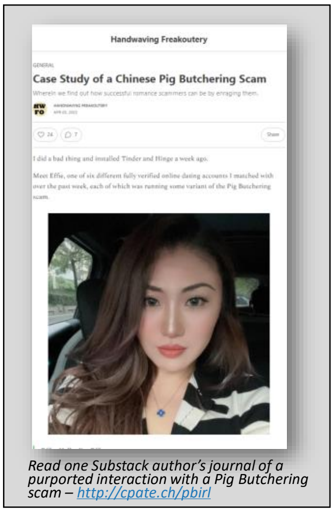
PIG BUTCHERING SCAMS

Last Week Tonight – Pig Butchering

- Excellent (and humorous) 24 minute video on this common scam involving investments with cryptocurrencies and promising romance AND riches which is robbing victims of over $3 billion USD per year
- External Video Link

Pig Butchering

- **A "confidence scam" usually involving cryptocurrency**
- **The Global Anti-Scam Organization (GASO), a non-profit created in 2021 in response to pig butchering scams, reports that the average victim loses $122,000 USD, and two-thirds of victims are women aged 25 to 40**
- Scammers encounter victims on dating services, social media, or through unsolicited messages or calls, often masquerading as a wrong number
- Scammers initiate relationships with victims and slowly gain their trust, eventually introducing the idea of making a business investment using cryptocurrency


Handwaving Freakoutery

GENERAL

Case Study of a Chinese Pig Butchering Scam

Wherein we find out how successful romance scammers can be by enraging them.

HANDWAVING FREAKOUTERY
[illegible]

I did a bad thing and installed Tinder and Hinge a week ago.

Meet Effie, one of six different fully verified online dating accounts I matched with over the past week, each of which was running some variant of the Pig Butchering scam.

Read one Substack author's journal of a purported interaction with a Pig Butchering scam – http://cpate.ch/pbirl

Source: Initial indictment in US Federal court case 2:23-cr-00596-RGK, ProofPoint

Pig Butchering

- Victims are then directed to other members of the scheme operating fraudulent cryptocurrency investment platforms and applications, where victims are persuaded to make financial investments
- Once funds are sent to scammer-controlled accounts, the investment platform often falsely shows significant gains on the purported investment, and the victims are thus induced to make additional investments.
- Ultimately, the victims are unable to withdraw or recover their money, often resulting in significant losses for the victims.

Source: Initial indictment in US Federal court case 2:23-cr-00596-RGK

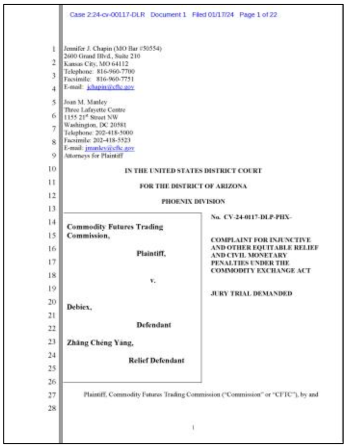
FinCEN reports that scammers commonly communicate with victims using:

- *Instant messaging services and text messages*
- *Professional networking sites*
- *Social media*
- *Dating sites*

Source: FinCEN Alert
FIN-2023-Alert005

Pending Litigation – CFTC vs. Debiex

- The complaint filed in Federal court in Phoenix, Arizona alleges that cryptocurrency exchange Debiex "used popular romance scam tactics" to steal customer funds totaling $2.3 million USD intended for digital asset commodity trading
- The complaint alleges that Debiex was made to look like a live cryptocurrency trading program but no actual trading took place on behalf of customers and all funds submitted were misappropriated



Case 2:24-cv-00117-DLR Document 1 Filed 01/17/24 Page 1 of 22

Jennifer J. Chapin (MO Bar #50554)
2600 Grand Blvd., Suite 210
Kansas City, MO 64112
Telephone: 816-960-7700
Facsimile: 816-960-7751
E-mail: jchapin@cftc.gov

Joan M. Manley
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581
Telephone: 202-418-5000
Facsimile: 202-418-5523
E-mail: jmanley@cftc.gov
Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

PHOENIX DIVISION

Commodity Futures Trading Commission,
Plaintiff,
v.
Debiex,
Defendant
Zhāng Chéng Yáng,
Relief Defendant

No. CV-24-0117-DLP-PHX-

COMPLAINT FOR INJUNCTIVE AND OTHER EQUITABLE RELIEF AND CIVIL MONETARY PENALTIES UNDER THE COMMODITY EXCHANGE ACT

JURY TRIAL DEMANDED

Plaintiff, Commodity Futures Trading Commission ("Commission" or "CFTC"), by and

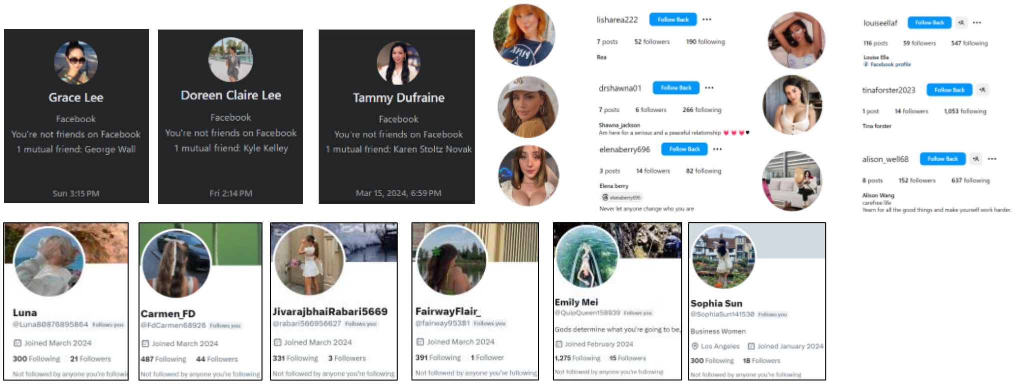
1

Read the original FTC Complaint against Debiex and others

How Pig Butchering Occurs

1. The perpetrator(s) create fake social media and dating profiles using photos of engaging, attractive, and wealthy individuals which will be used to engage with potential scam victims through flirting and not so “random” interactions

How Pig Butchering Occurs



Grace Lee
Facebook
You're not friends on Facebook
1 mutual friend: George Wall
Sun 3:15 PM

Doreen Claire Lee
Facebook
You're not friends on Facebook
1 mutual friend: Kyle Kelley
Fri 2:14 PM

Tammy Dufraine
Facebook
You're not friends on Facebook
1 mutual friend: Karen Stoltz Novak
Mar 15, 2024, 6:59 PM

lisharea222 Follow Back •••
7 posts 52 followers 190 following
Rea

drshawna01 Follow Back •••
7 posts 6 followers 266 following
Shawna_jackson
Am here for a serious and a peaceful relationship 💓💓💓♥

elenaberry696 Follow Back •••
3 posts 14 followers 82 following
Elena berry
elenaberry696
Never let anyone change who you are

louiseellaf Follow Back •••
116 posts 59 followers 547 following
Louise Ella
Facebook profile

tinaforster2023 Follow Back
1 post 14 followers 1,053 following
Tina forster

alison_well68 Follow Back •••
8 posts 152 followers 637 following
Alison Wang
carefree life
Yearn for all the good things and make yourself work harder.

Luna
@Luna80876895864 Follows you
Joined March 2024
300 Following 21 Followers
Not followed by anyone you're followi

Carmen_FD
@FdCarmen68926 Follows you
Joined March 2024
487 Following 44 Followers
Not followed by anyone you're following

JivarajbhaiRabari5669
@rabari566956627 Follows you
Joined March 2024
331 Following 3 Followers
Not followed by anyone you're following

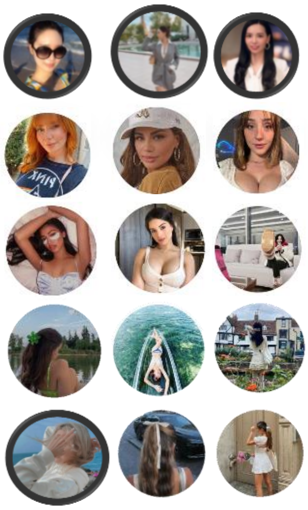
FairwayFlair_
@fairway95381 Follows you
Joined March 2024
391 Following 1 Follower
Not followed by anyone you're following

Emily Mei
@QuipQueen158939 Follows you
Gods determine what you're going to be.
Joined February 2024
1,275 Following 15 Followers
Not followed by anyone you're following

Sophia Sun
@SophiaSun141530 Follows you
Business Women
Los Angeles Joined January 2024
300 Following 18 Followers
Not followed by anyone you're following

2. The young and attractive profile then just happens to contact someone older and less attractive and tries to start dialogue and maybe even an online romance – this is called a “solicitor”

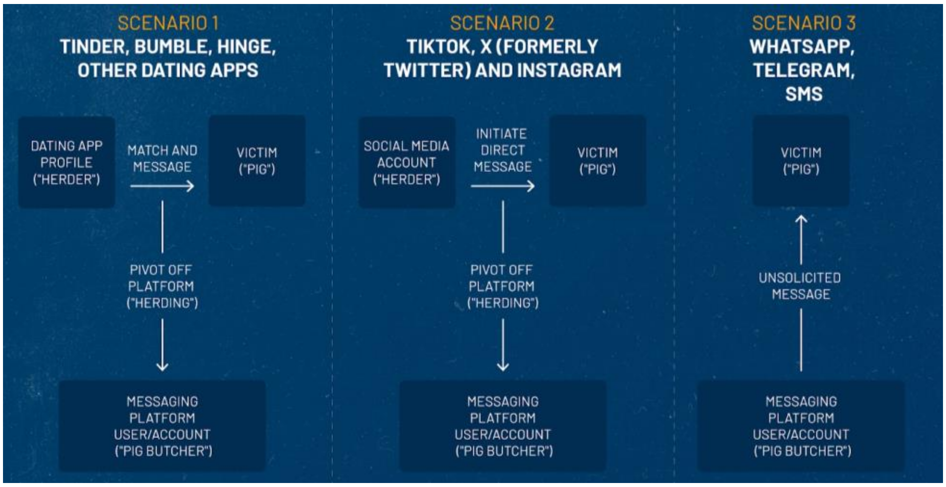
How Pig Butchering Occurs



What do these profiles have in common?

- Attractive profile photos, appear to be young
- All reached out to me via direct messages
- All have low follower counts (only one has more than 100 followers, most are in single digits)
- All follow hundreds of other people who have decided for some reason to not follow them back
- Almost all accounts are less than 90 days old

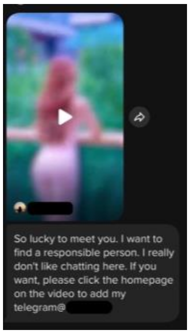
How Pig Butchering Contacts Occur



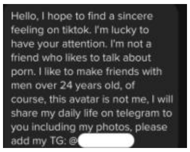
SCENARIO 1
TINDER, BUMBLE, HINGE, OTHER DATING APPS
DATING APP PROFILE ("HERDER")
MATCH AND MESSAGE
VICTIM ("PIG")
PIVOT OFF PLATFORM ("HERDING")
MESSAGING PLATFORM USER/ACCOUNT ("PIG BUTCHER")
SCENARIO 2
TIKTOK, X (FORMERLY TWITTER) AND INSTAGRAM
SOCIAL MEDIA ACCOUNT ("HERDER")
INITIATE DIRECT MESSAGE
VICTIM ("PIG")
PIVOT OFF PLATFORM ("HERDING")
MESSAGING PLATFORM USER/ACCOUNT ("PIG BUTCHER")
SCENARIO 3
WHATSAPP, TELEGRAM, SMS
VICTIM ("PIG")
UNSOLICITED MESSAGE
MESSAGING PLATFORM USER/ACCOUNT ("PIG BUTCHER")

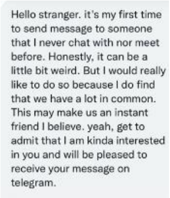
Source: Tenable Blog – Pig Butchering Scam

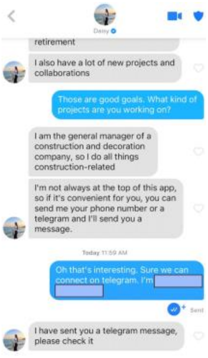
How Pig Butchering Occurs


So lucky to meet you. I want to find a responsible person. I really don't like chatting here. If you want, please click the homepage on the video to add my telegram@[redacted]

[redacted]


Hello, I hope to find a sincere feeling on tiktok. I'm lucky to have your attention. I'm not a friend who likes to talk about porn. I like to make friends with men over 24 years old, of course, this avatar is not me, I will share my daily life on telegram to you including my photos, please add my TG: @[redacted]


Hello stranger. it's my first time to send message to someone that I never chat with nor meet before. Honestly, it can be a little bit weird. But I would really like to do so because I do find that we have a lot in common. This may make us an instant friend I believe. yeah, get to admit that I am kinda interested in you and will be pleased to receive your message on telegram.



retirement

I also have a lot of new projects and collaborations

Those are good goals. What kind of projects are you working on?

I am the general manager of a construction and decoration company, so I do all things construction-related

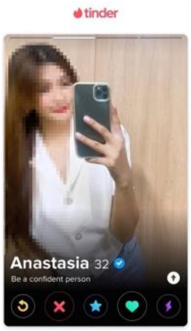
I'm not always at the top of this app, so if it's convenient for you, you can send me your phone number or a telegram and I'll send you a message.

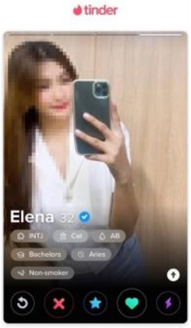
Today 11:59 AM

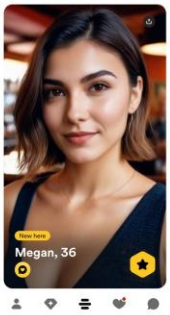
Oh that's interesting. Sure we can connect on telegram. I'm [redacted]

Sent

I have sent you a telegram message, please check it





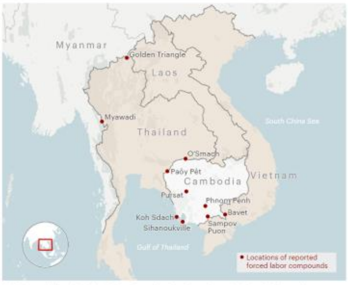


Source: Tenable Blog – Pig Butchering Scam

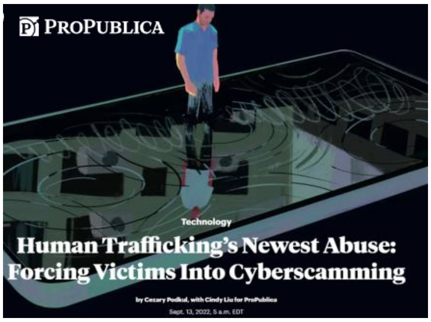
3. Through constant contact, flirting, and flattery, the solicitor makes the target feel that the solicitor is a friend, or maybe even a future love interest – even though you seem to have nothing in common

How Pig Butchering Occurs

Forced Labor Compounds Have Spread Across Cities in Cambodia and Elsewhere in Southeast Asia



Map by Lucas Waldron, ProPublica. © OpenStreetMap Contributors. Research by Danielle Keeton-Olsen.


PROPUBLICA

Technology

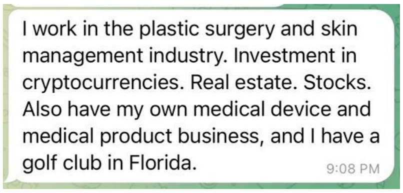
Human Trafficking's Newest Abuse: Forcing Victims Into Cyberscamming

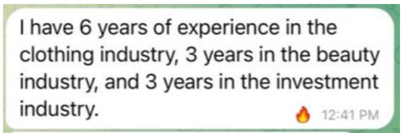
by Cezary Podkul, with Cindy Liu for ProPublica

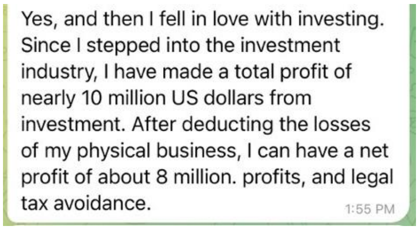
Sept. 13, 2022, 5 a.m. EDT

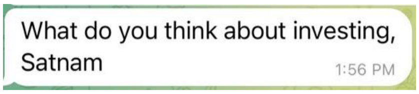
4. Investigative journalists ProPublica even report that many of the scam artists are actually victims of human trafficking, held against their will in forced labor compounds, with serious consequences for those who do not participate in the scams

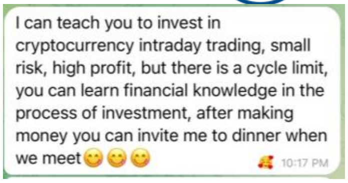
How Pig Butchering Occurs

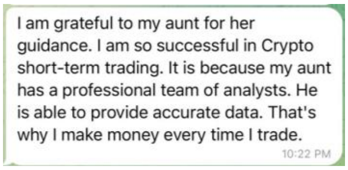

I work in the plastic surgery and skin management industry. Investment in cryptocurrencies. Real estate. Stocks. Also have my own medical device and medical product business, and I have a golf club in Florida. 9:08 PM


I have 6 years of experience in the clothing industry, 3 years in the beauty industry, and 3 years in the investment industry. 🔥 12:41 PM


Yes, and then I fell in love with investing. Since I stepped into the investment industry, I have made a total profit of nearly 10 million US dollars from investment. After deducting the losses of my physical business, I can have a net profit of about 8 million. profits, and legal tax avoidance. 1:55 PM


What do you think about investing, Satnam 1:56 PM

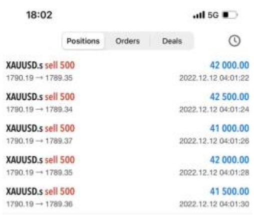

I can teach you to invest in cryptocurrency intraday trading, small risk, high profit, but there is a cycle limit, you can learn financial knowledge in the process of investment, after making money you can invite me to dinner when we meet😋😋😋 10:17 PM


I am grateful to my aunt for her guidance. I am so successful in Crypto short-term trading. It is because my aunt has a professional team of analysts. He is able to provide accurate data. That's why I make money every time I trade. 10:22 PM

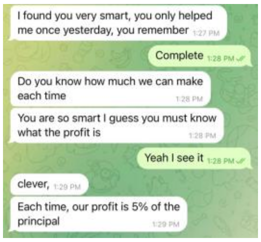
Source: Tenable Blog – Pig Butchering Scam

5. After establishing rapport and getting the target "hooked" on the attention and flirting, the attacker will introduce the idea of investing in cryptocurrencies – where the perp says that they have been making a lot of money with their investments

How Pig Butchering Occurs



```
XAUUSD.s sell 500                 42 000.00
1790.19 → 1789.35       2022.12.12 04:01:22
XAUUSD.s sell 500                 42 500.00
1790.19 → 1789.34       2022.12.12 04:01:24
XAUUSD.s sell 500                 41 000.00
1790.19 → 1789.37       2022.12.12 04:01:26
XAUUSD.s sell 500                 42 000.00
1790.19 → 1789.35       2022.12.12 04:01:28
XAUUSD.s sell 500                 41 500.00
1790.19 → 1789.36       2022.12.12 04:01:30
```


I found you very smart, you only helped me once yesterday, you remember 1:27 PM

Complete 1:28 PM

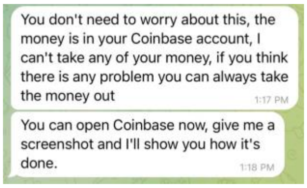
Do you know how much we can make each time 1:28 PM

You are so smart I guess you must know what the profit is 1:28 PM

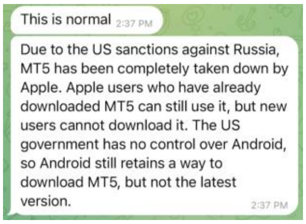
Yeah I see it 1:28 PM

clever, 1:29 PM

Each time, our profit is 5% of the principal 1:29 PM


You don't need to worry about this, the money is in your Coinbase account, I can't take any of your money, if you think there is any problem you can always take the money out 1:17 PM

You can open Coinbase now, give me a screenshot and I'll show you how it's done. 1:18 PM

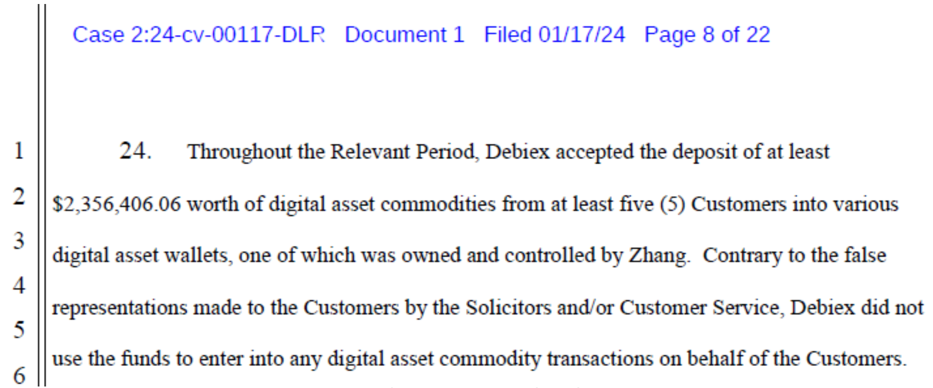

This is normal 2:37 PM

Due to the US sanctions against Russia, MT5 has been completely taken down by Apple. Apple users who have already downloaded MT5 can still use it, but new users cannot download it. The US government has no control over Android, so Android still retains a way to download MT5, but not the latest version. 2:37 PM

Source: Tenable Blog – Pig Butchering Scam

6. The scammers then show "fake returns" from the fake crypto investment website and tries to get the victim to make investments in either a fake exchange or to send crypto to an account controlled by the solicitor so they can show them how to execute the trade

How Pig Butchering Occurs

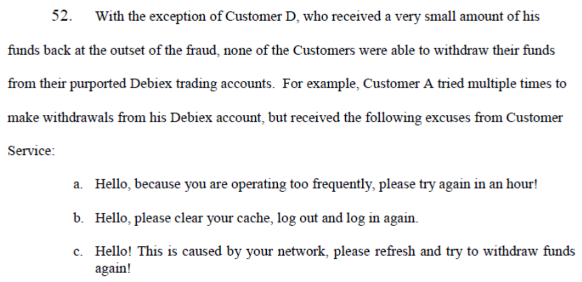


Case 2:24-cv-00117-DLR Document 1 Filed 01/17/24 Page 8 of 22

24. Throughout the Relevant Period, Debiex accepted the deposit of at least $2,356,406.06 worth of digital asset commodities from at least five (5) Customers into various digital asset wallets, one of which was owned and controlled by Zhang. Contrary to the false representations made to the Customers by the Solicitors and/or Customer Service, Debiex did not use the funds to enter into any digital asset commodity transactions on behalf of the Customers.

7. In one case – *CFTC v. Debiex et al*, the US Commodity Futures Trading Commission (CFTC) alleges that over $2.35 million USD of cryptocurrencies were transmitted through a fake exchange called "Debiex"

How Pig Butchering Occurs

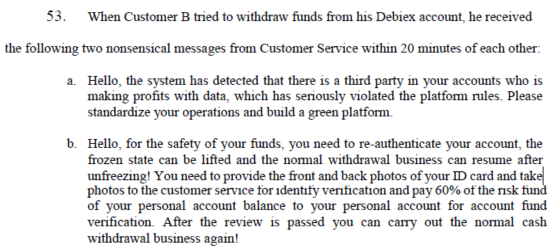


52. With the exception of Customer D, who received a very small amount of his funds back at the outset of the fraud, none of the Customers were able to withdraw their funds from their purported Debiex trading accounts. For example, Customer A tried multiple times to make withdrawals from his Debiex account, but received the following excuses from Customer Service:

a. Hello, because you are operating too frequently, please try again in an hour!

b. Hello, please clear your cache, log out and log in again.

c. Hello! This is caused by your network, please refresh and try to withdraw funds again!



53. When Customer B tried to withdraw funds from his Debiex account, he received the following two nonsensical messages from Customer Service within 20 minutes of each other:

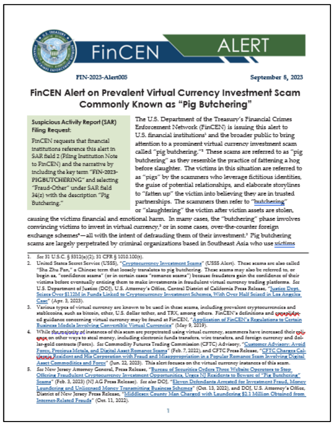
a. Hello, the system has detected that there is a third party in your accounts who is making profits with data, which has seriously violated the platform rules. Please standardize your operations and build a green platform.

b. Hello, for the safety of your funds, you need to re-authenticate your account, the frozen state can be lifted and the normal withdrawal business can resume after unfreezing! You need to provide the front and back photos of your ID card and take photos to the customer service for identity verification and pay 60% of the risk fund of your personal account balance to your personal account for account fund verification. After the review is passed you can carry out the normal cash withdrawal business again!

8. When victims try to withdraw funds, they were greeted with a number of different excuses as to why the funds cannot be withdrawn at this time – all bogus delay tactics. At this point, the funds and/or cryptocurrency is gone – and the solicitor will also disappear without a trace

Behavioral Red Flags

- A customer with no history or background of using, exchanging, or otherwise interacting with virtual currency attempts to exchange a high amount of fiat currency from an existing or newly opened bank account for virtual currency or attempts to initiate high-value transfers to VASPs.
- A customer mentions or expresses interest in an investment opportunity leveraging virtual currency with significant returns that they were told about from a new contact who reached out to them unsolicited online or through text message.



FinCEN ALERT

FIN-2023-Alert005 September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-PIGBUTCHERING" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

[1] See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

[2] United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. See U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).

[3] Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).

[4] While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). See Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.

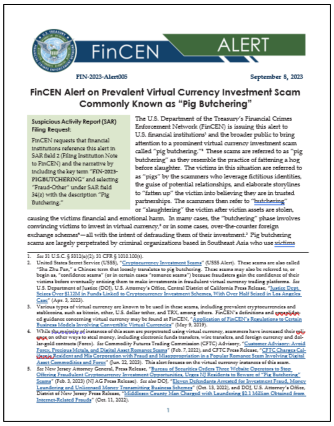
[5] See New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). See also DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

1

Source: FinCEN Alert FIN-2023-Alert005

Behavioral Red Flags

- A customer mentions that they were instructed by an individual who recently contacted them to exchange fiat currency for virtual currency at a virtual currency kiosk and deposit the virtual currency at an address supplied by the individual.
- A customer appears distressed or anxious to access funds to meet demands or the timeline of a virtual currency investment opportunity.



FinCEN ALERT

FIN-2023-Alert005 September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-PIGBUTCHERING" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

[1] See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

[2] United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. See U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).

[3] Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).

[4] While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). See Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.

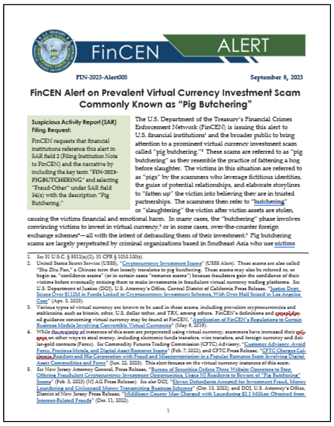
[5] See New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). See also DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

1

Source: FinCEN Alert FIN-2023-Alert005

Financial Red Flags

- A customer uncharacteristically liquidates savings accounts prior to maturation, such as a certificate of deposit, and then subsequently attempts to wire the liquidated fiat currency to a VASP or to exchange them for virtual currency.
- A customer takes out a HELOC, home equity loan, or second mortgage and uses the proceeds to purchase virtual currency or wires the proceeds to a VASP for the purchase of virtual currency.



FinCEN ALERT

FIN-2023-Alert005 September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-PIGBUTCHERING" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

[1] *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

[2] United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. *See* U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).

[3] Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).

[4] While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). *See* Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.

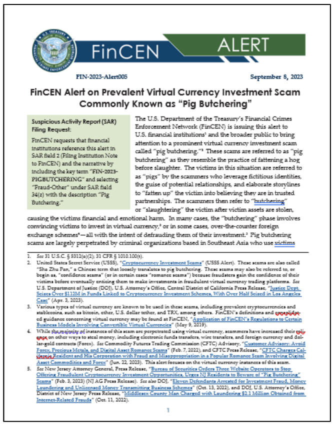
[5] *See* New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). *See also* DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

1

Source: FinCEN Alert FIN-2023-Alert005

Financial Red Flags

- A customer receives what appears to be a deposit of virtual currency from a virtual currency address at or slightly above the amount that the customer previously transferred out of their virtual currency account. This deposit is then followed by outgoing transfers from the customer in substantially larger amounts.
- Accounts with large balances that are inactive or have limited activity begin to show constant, uncharacteristic, sudden, abnormally frequent, or significant withdrawals of large amounts of money being transferred to a VASP or being exchanged for virtual currency.



FinCEN ALERT

FIN-2023-Alert005 September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-PIGBUTCHERING" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

[1] *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

[2] United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. *See* U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).

[3] Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).

[4] While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). *See* Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.

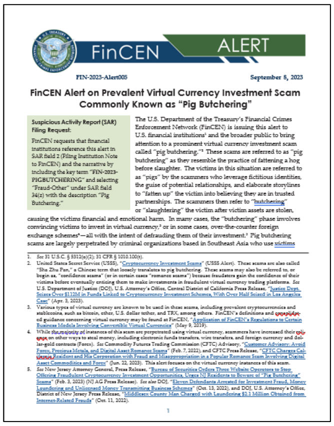
[5] *See* New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). *See also* DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

1

Source: FinCEN Alert FIN-2023-Alert005

Financial Red Flags

- A customer sends multiple electronic funds transfers (EFTs) or wire transfers to a VASP or sends part of their available balance from an account or wallet they maintain with a VASP and notes that the transaction is for "taxes," "fees," or "penalties."
- A customer with a short history of conducting several small-value EFTs to a VASP abruptly stops sending EFTs and begins sending multiple high-value wire transfers to accounts of holding companies, limited liability corporations, and individuals with which the customer has no prior transaction history. This is indicative of a victim sending trial transactions to a scammer before committing to and sending larger amounts.



FinCEN ALERT

FIN-2023-Alert005

September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-PIGBUTCHERING" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

[1] See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

[2] United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. See U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).

[3] Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).

[4] While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). See Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.

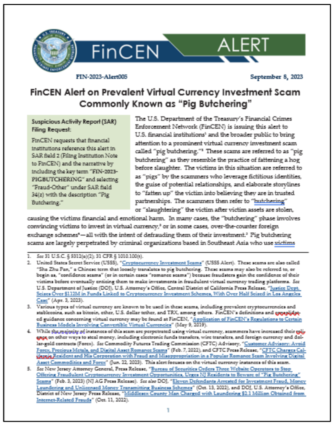
[5] See New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). See also DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

1

Source: FinCEN Alert FIN-2023-Alert005

Technical Red Flags

- System monitoring and logs show that a customer's account is accessed repeatedly by unique IP addresses, device IDs, or geographies inconsistent with prior access patterns. Additionally, logins to a customer's online account at a VASP come from a variety of different device IDs and names inconsistent with the customer's typical logins.
- A customer mentions that they are transacting to invest in virtual currency using a service that has a website or application with poor spelling or grammatical structure, dubious customer testimonials, or a generally amateurish site design.
- A customer mentions visiting a website or application that is purported to be associated with a legitimate VASP or business involved in investing in virtual currency. The website or application shows warning signs such as a web address or domain name that is misspelled in such a manner as to resemble that of another business, a recently registered web address or domain name, no physical street address, international contact information, or contact methods that include only chat or email.



FinCEN ALERT

FIN-2023-Alert005

September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-PIGBUTCHERING" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

[1] See 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).

[2] United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. See U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).

[3] Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).

[4] While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). See Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.

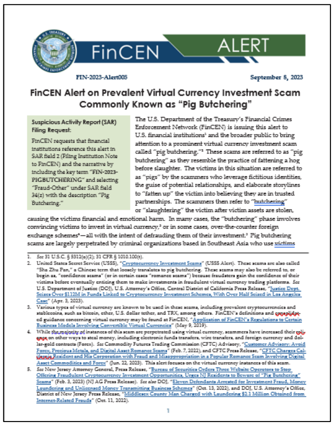
[5] See New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). See also DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

1

Source: FinCEN Alert FIN-2023-Alert005

Technical Red Flags

- A customer mentions that they downloaded an application on their phone directly from a third-party website, rather than from a well-known third-party application store or an application store installed by the manufacturer of the device.
- A customer receives a large amount of virtual currency such as ether at an exchange, subsequently converts the amount to a virtual currency with lower transaction fees such as TRX, and then abruptly sends it out of the exchange.



FinCEN ALERT

FIN-2023-Alert005 September 8, 2023

FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "FIN-2023-PIGBUTCHERING" and selecting "Fraud-Other" under SAR field 34(z) with the description "Pig Butchering."

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this alert to U.S. financial institutions[1] and the broader public to bring attention to a prominent virtual currency investment scam called "pig butchering."[2] These scams are referred to as "pig butchering" as they resemble the practice of fattening a hog before slaughter. The victims in this situation are referred to as "pigs" by the scammers who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to "fatten up" the victim into believing they are in trusted partnerships. The scammers then refer to "butchering" or "slaughtering" the victim after victim assets are stolen, causing the victims financial and emotional harm. In many cases, the "butchering" phase involves convincing victims to invest in virtual currency,[3] or in some cases, over-the-counter foreign exchange schemes[4]—all with the intent of defrauding them of their investment.[5] Pig butchering scams are largely perpetrated by criminal organizations based in Southeast Asia who use victims

1. *See* 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
2. United States Secret Service (USSS), "Cryptocurrency Investment Scams" (USSS Alert). These scams are also called "Sha Zhu Pan," a Chinese term that loosely translates to pig butchering. These scams may also be referred to, or begin as, "confidence scams" (or in certain cases "romance scams") because fraudsters gain the confidence of their victims before eventually enticing them to make investments in fraudulent virtual currency trading platforms. *See* U.S. Department of Justice (DOJ), U.S. Attorney's Office, Central District of California Press Release, "Justice Dept. Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case" (Apr. 3, 2023).
3. Various types of virtual currency are known to be used in these scams, including prevalent cryptocurrencies and stablecoins, such as bitcoin, ether, U.S. dollar tether, and TRX, among others. FinCEN's definitions and consolidated guidance concerning virtual currency may be found at FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019).
4. While the majority of instances of this scam are perpetrated using virtual currency, scammers have increased their reliance on other ways to steal money, including electronic funds transfers, wire transfers, and foreign currency and dollar-gold contracts (Forex). *See* Commodity Futures Trading Commission (CFTC) Advisory, "Customer Advisory: Avoid Forex, Precious Metals, and Digital Asset Romance Scams" (Feb. 7, 2022), and CFTC Press Release, "CFTC Charges California Resident and His Corporation with Fraud and Misappropriation in a Popular Romance Scam Involving Digital Asset Commodities and Forex" (Jun. 22, 2023). This alert focuses on the virtual currency instances of this scam.
5. *See* New Jersey Attorney General, Press Release, "Bureau of Securities Orders Three Website Operators to Stop Offering Fraudulent Cryptocurrency Investment Opportunities, Urges NJ Residents to Beware of "Pig Butchering" Scams" (Feb. 3, 2023) (NJ AG Press Release). *See also* DOJ, "Eleven Defendants Arrested for Investment Fraud, Money Laundering and Unlicensed Money Transmitting Business Schemes" (Oct. 13, 2022), and DOJ, U.S. Attorney's Office, District of New Jersey Press Release, "Middlesex County Man Charged with Laundering $2.1 Million Obtained from Internet-Related Frauds" (Oct. 11, 2022).

1

Source: FinCEN Alert FIN-2023-Alert005

Some Pig Butchering Web Domains

zvip.zone	coinss.pro	mitokenex.com	bitget-tw.com	rkez.xyz
xtfkskpk.buzz	qklyz.com	flyscoin.com	cme-cn.com	acefinex.com
meymytum.xyz	coinline.pro	autoecofxmarkets.com	kucoinusa.com	acefinex.net
vwtryf.xyz	skgroup.vip	ensf.agency	266wrd.com	acefinex[.}vip
eumfpbva.xyz	galaxycoin.vip	shopwse.com	financeaka.cc	eumfpbva.xyz
nhealcoin.cc	nhchain.vip	beybit.com	ettsmc.ltd	meymytum.xyz
zvip.zone	lanbing.club	bihuo.top	bilinkbitex.com	okx-us.net
hitbicvip.com	fwhtoken.com	bn93.com	engiegpg.com	s-coin.vip
hitbic.net	s-coin.vip	sklge.com	aax.news	vwtryf.xyz
oslint.com	walletput.com	tgbone.com	ftxcn99.com	xtfkskpk.buzz
maskexc.com	okx-us.net	hkdbitexchange.com	pinduoyu.com	mitokenex.com

Source: Security provider ProofPoint blog, "Broken Dreams and Piggy Banks: Pig Butchering Crypto Fraud Growing Online", 10/24/2022

Pig Butchering Fraud Reporting

- In addition to filing a SAR, financial institutions are encouraged to refer their customers who may be victims of pig butchering to the FBI's IC3: https://www.ic3.gov/
- Institutions may also refer their customers to the Securities and Exchange Commission's tips, complaints, and referrals (TCR) system to report investment fraud: https://www.sec.gov/tcr
- In the case of elder victims of pig butchering, financial institutions may also refer their customers to DOJ's National Elder Fraud Hotline at 833-FRAUD-11 or 833-372-8311.

Lessons Learned

- Investment scams can use boiler rooms of human trafficking victims to manipulate people emotionally to gain access to their resources
- Most, if not all cryptocurrencies lack the most basic dispute resolution systems and investor protections we take for granted in traditional financial institutions
- Your social media accounts and online dating accounts are a window into your private life that will be used against you if cybercriminals gain access to those profiles and posts
- Online dating and social media has made it possible for scams to be carried out from anywhere in the world with great effect
- If someone with whom you have little to nothing in common with starts flirting and then starts suggesting investment vehicles, they may be a scammer posing as a suitor

"The Chaotic And Cinematic MGM Casino Hack, Explained", Vox 10/6/2023

"The Audacious MGM Hack That Brought Chaos To Las Vegas", The Wall Street Journal, 3/29/2024

INSIDE THE MGM RANSOMWARE ATTACK

About MGM Resorts

MGM RESORTS INTERNATIONAL

Operator of 18 properties in the United States and Macau

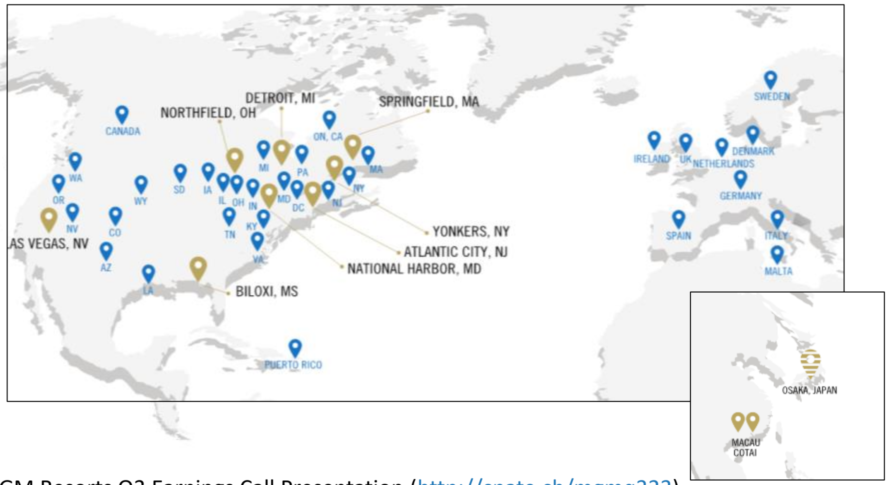
Signed Implementation Agreement an integrated resort in Japan

BETMGM

Sports betting and iGaming brand in 28 North American jurisdictions and Carnival Cruises

LeoVegas MOBILE GAMING GROUP

Online sports betting and iGaming operator in 10 jurisdictions in Europe and Canada



Source: MGM Resorts Q3 Earnings Call Presentation (http://cpate.ch/mgmq323)

MGM Resorts Ransomware

- On Friday, September 8, 2023, the help desk for MGM Resorts received a call from an employee asking for a password reset
- The called shared private information about an employee, and the help desk staffer reset the password without incident
- This casino giant operates some of the biggest properties in the world, including over 37,200 hotel rooms

BELLAGIO LAS VEGAS
PARK MGM LAS VEGAS
Aria RESORT & CASINO LAS VEGAS
Vdara HOTEL & SPA
LUXOR LAS VEGAS
NEW YORK NEW YORK LAS VEGAS HOTEL & CASINO
Excalibur HOTEL•CASINO•LAS VEGAS
Borgata HOTEL CASINO & SPA
DELANO LAS VEGAS
MGM GRAND
THE COSMOPOLITAN of LAS VEGAS
Beau Rivage Resort & Casino • Biloxi
MANDALAY BAY RESORT AND CASINO LAS VEGAS

MGM Resorts Ransomware

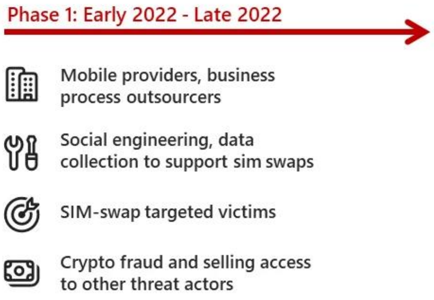
- This actually was a hacker which led to a network compromise, data exfiltration, and ransomware with a requested $30MM ransom which shut down its systems
- Caesar's Entertainment was simultaneously targeted and paid the ransom; Unlike Caesar's, MGM did NOT pay
- We will discuss the tactics employed by the group who was allegedly behind the attack

BELLAGIO LAS VEGAS
PARK MGM LAS VEGAS
Aria RESORT & CASINO LAS VEGAS
Vdara HOTEL & SPA
LUXOR LAS VEGAS
NEW YORK NEW YORK LAS VEGAS HOTEL & CASINO
Excalibur HOTEL•CASINO•LAS VEGAS
Borgata HOTEL CASINO & SPA
DELANO LAS VEGAS
MGM GRAND
THE COSMOPOLITAN of LAS VEGAS
Beau Rivage Resort & Casino • Biloxi
MANDALAY BAY RESORT AND CASINO LAS VEGAS

The Alleged Perps: Octo Tempest

- Financial criminal group
- This hacker group is fluent in English and is believed to consist of British and American hackers
- Also known as 0ktapus, Scattered Spider, and UNC3944
- Activity first noticed in early 2022
- Known to partner with Russian ALPHV/BlackCat hacker group, a ransomware as a service (RaaS) operation starting in mid-2023

Octo Tempest Evolution- 2022-2023



Phase 1: Early 2022 - Late 2022

- Mobile providers, business process outsourcers
- Social engineering, data collection to support sim swaps
- SIM-swap targeted victims
- Crypto fraud and selling access to other threat actors

Source: Microsoft Security Blog (http://cpate.ch/ms8t)

Octo Tempest Social Engineering

Uses one of many social engineering techniques to gain initial access to a network

- Calling an employee and socially engineering the user to either:
  - Install a remote access utility
  - Direct them to a fake corporate login website operated by the hackers
  - Remove their account's use of two-factor authentication
- Calling an organization's help desk and socially engineering the help desk to reset the user's account

Source: *"Octo Tempest Group Threatens Physical Violence as Social Engineering Tactic",* Dark Reading, 10/27/2023 (http://cpate.ch/octhreat)

Octo Tempest Social Engineering

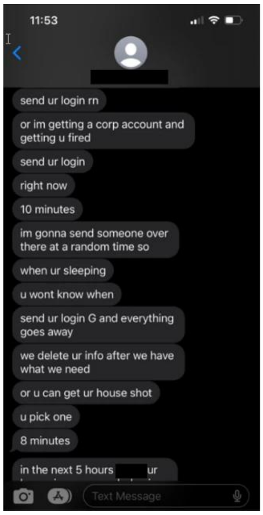
Uses one of many social engineering techniques to gain initial access to a network (continued):

- Purchasing an employee's credentials and/or session token(s) on a criminal underground market
- SMS phishing employee phone numbers with a link to a site configured with a fake login portal
- SIM swap or call forwarding attack against a target employee's cell phone
- *… but sometimes, these techniques are not enough…*

Source: *"Octo Tempest Group Threatens Physical Violence as Social Engineering Tactic",* Dark Reading, 10/27/2023 (http://cpate.ch/octhreat)

Intimidation By Octo Tempest

- In some instances, this perpetrator has been linked to efforts to intimidate users into giving up their credentials
  - Sharing that they know where someone lives and threatening them with violence
  - Threatening to harm an employee's home or family


11:53

[redacted]

send ur login rn

or im getting a corp account and getting u fired

send ur login

right now

10 minutes

im gonna send someone over there at a random time so

when ur sleeping

u wont know when

send ur login G and everything goes away

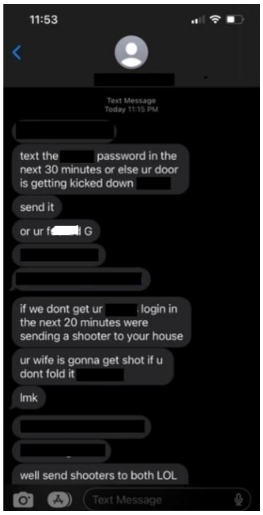
we delete ur info after we have what we need

or u can get ur house shot

u pick one

8 minutes

in the next 5 hours [redacted] ur


11:53

[redacted]

Text Message
Today 11:15 PM

[redacted]

text the [redacted] password in the next 30 minutes or else ur door is getting kicked down [redacted]

send it

or ur f[redacted]l G

[redacted]

[redacted]

if we dont get ur [redacted] login in the next 20 minutes were sending a shooter to your house

ur wife is gonna get shot if u dont fold it [redacted]

lmk

[redacted]

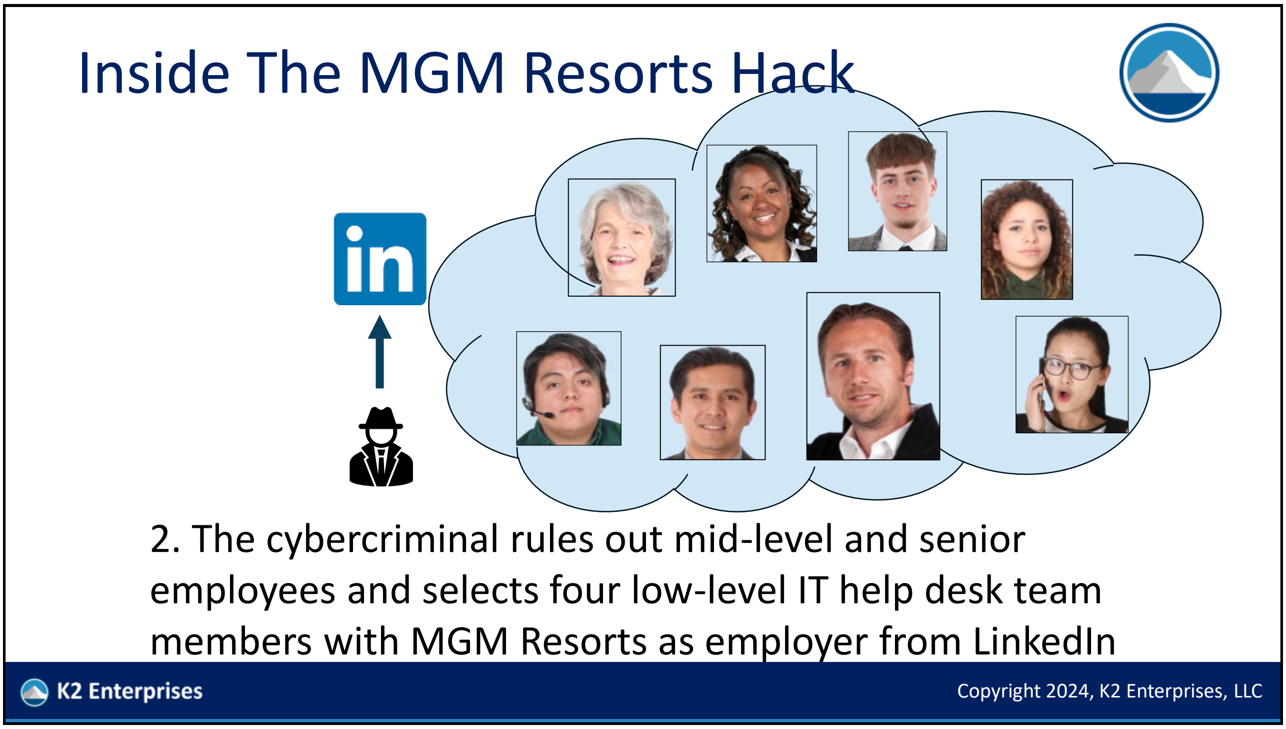
[redacted]

well send shooters to both LOL

Source: *"Octo Tempest Group Threatens Physical Violence as Social Engineering Tactic",* Dark Reading, 10/27/2023 (http://cpate.ch/octhreat)

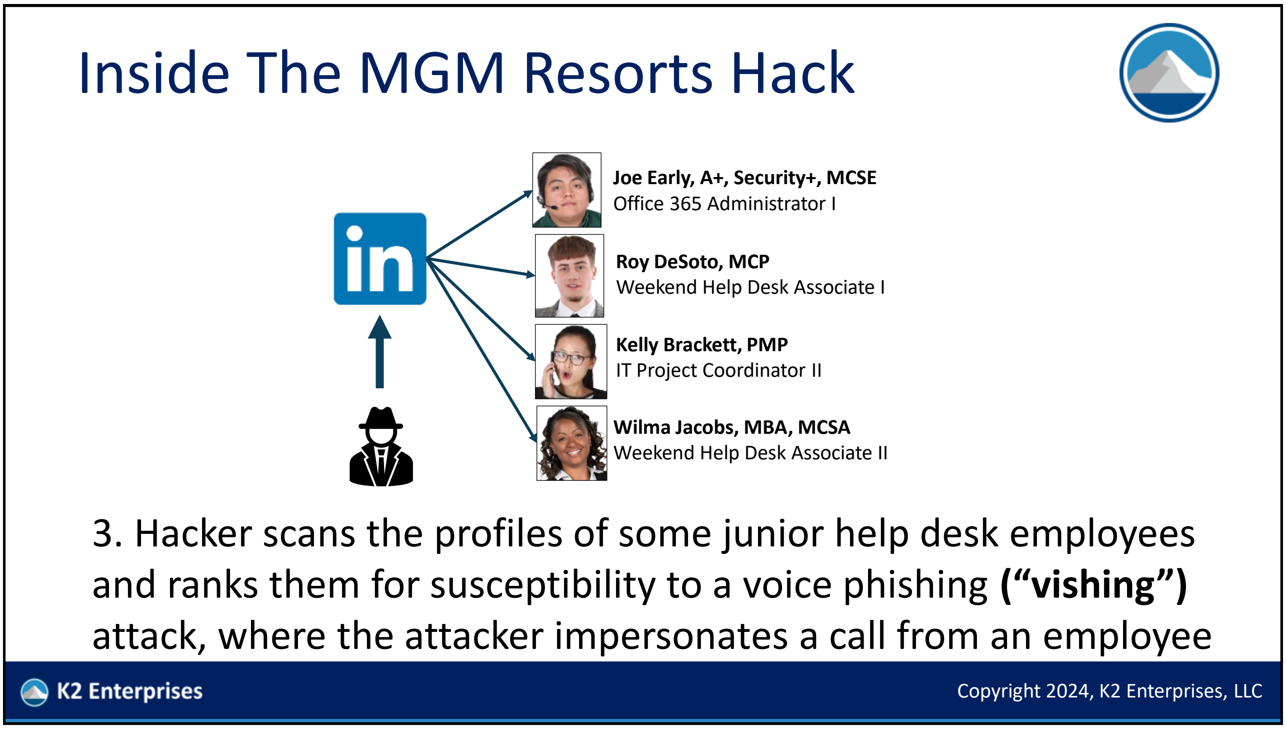
Inside The MGM Resorts Hack

1. Hacking group Octo Tempest scans social networks like **LinkedIn** and **Facebook** as well as **dark web databases** for IT employees at **MGM Resorts**



Inside The MGM Resorts Hack

2. The cybercriminal rules out mid-level and senior employees and selects four low-level IT help desk team members with MGM Resorts as employer from LinkedIn



Inside The MGM Resorts Hack

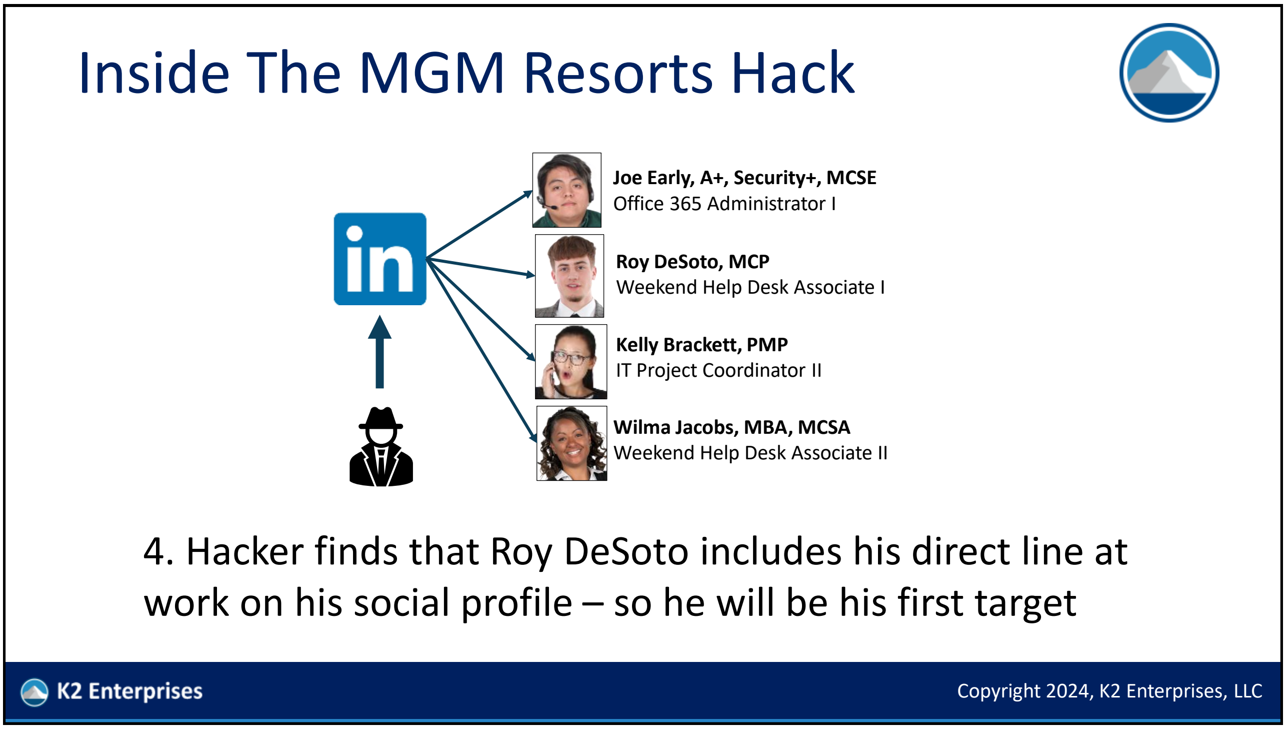
Joe Early, A+, Security+, MCSE
Office 365 Administrator I

Roy DeSoto, MCP
Weekend Help Desk Associate I

Kelly Brackett, PMP
IT Project Coordinator II

Wilma Jacobs, MBA, MCSA
Weekend Help Desk Associate II

3. Hacker scans the profiles of some junior help desk employees and ranks them for susceptibility to a voice phishing **("vishing")** attack, where the attacker impersonates a call from an employee



Inside The MGM Resorts Hack

Joe Early, A+, Security+, MCSE
Office 365 Administrator I

Roy DeSoto, MCP
Weekend Help Desk Associate I

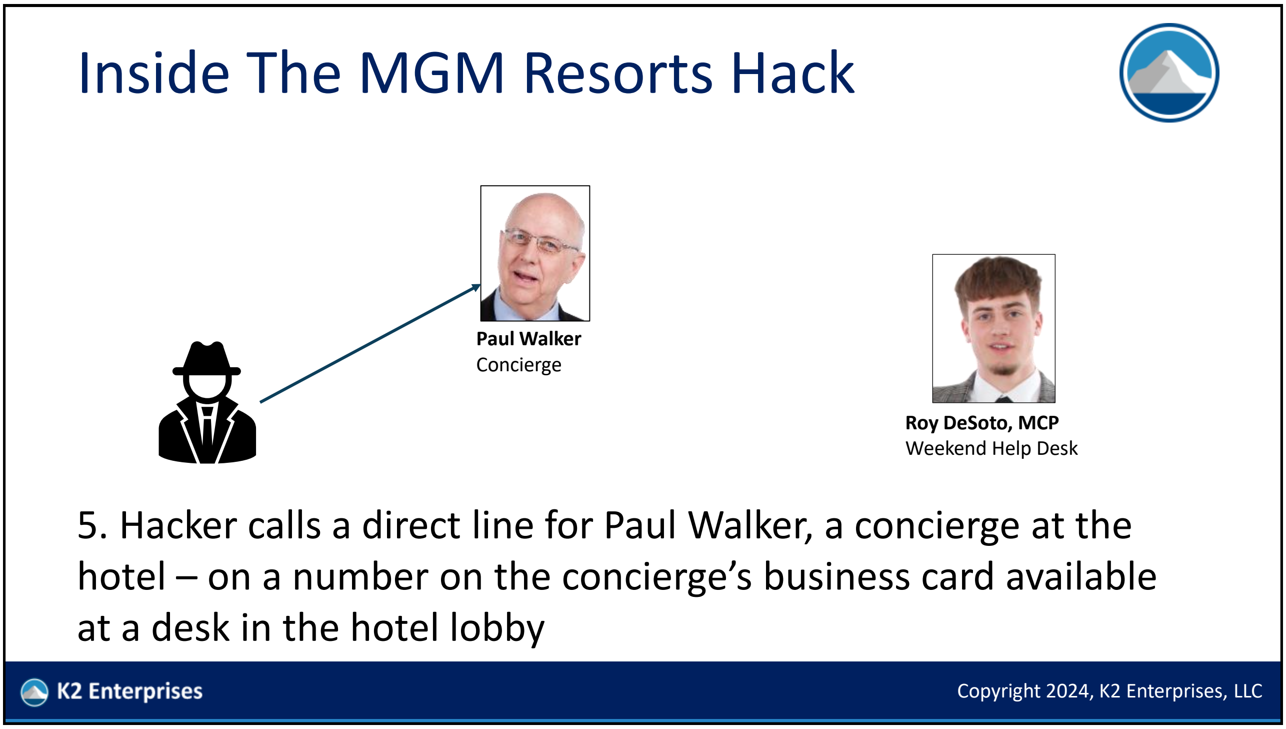
Kelly Brackett, PMP
IT Project Coordinator II

Wilma Jacobs, MBA, MCSA
Weekend Help Desk Associate II

4. Hacker finds that Roy DeSoto includes his direct line at work on his social profile – so he will be his first target

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC



Inside The MGM Resorts Hack

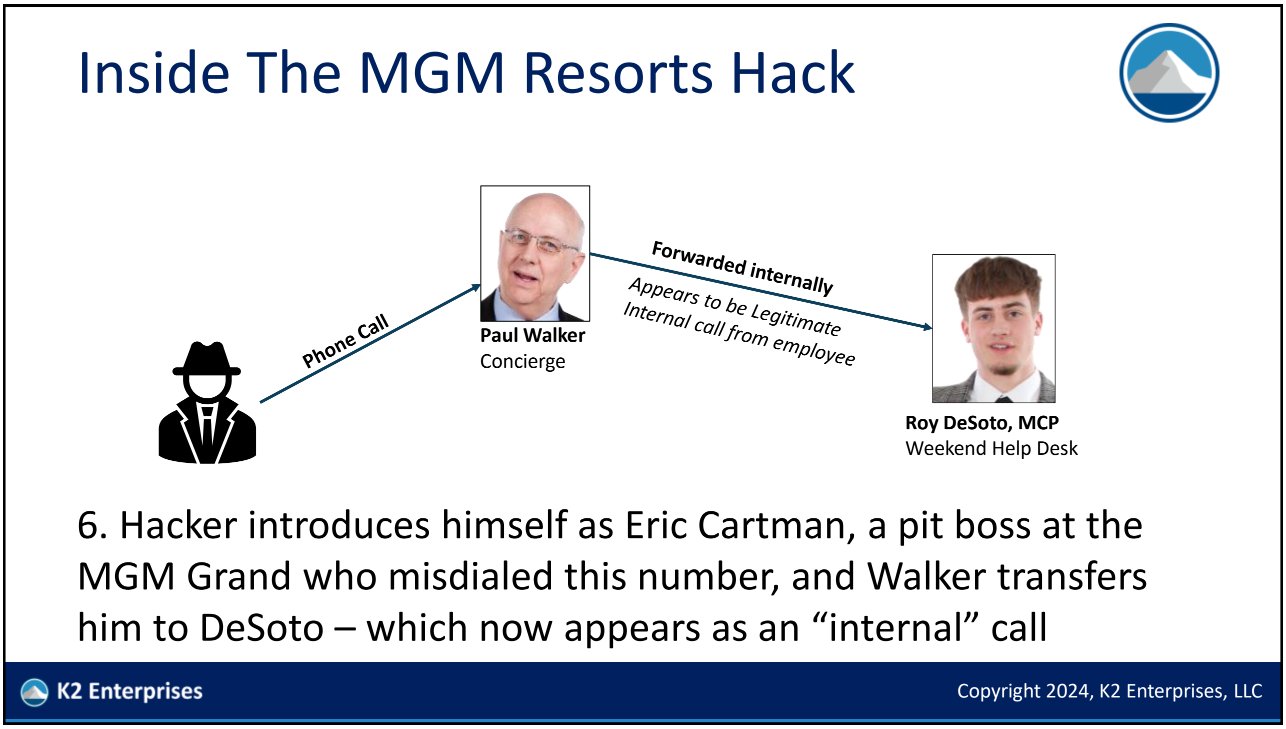
Paul Walker
Concierge

Roy DeSoto, MCP
Weekend Help Desk

5. Hacker calls a direct line for Paul Walker, a concierge at the hotel – on a number on the concierge's business card available at a desk in the hotel lobby

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC



Inside The MGM Resorts Hack

Phone Call

Paul Walker
Concierge

Forwarded internally

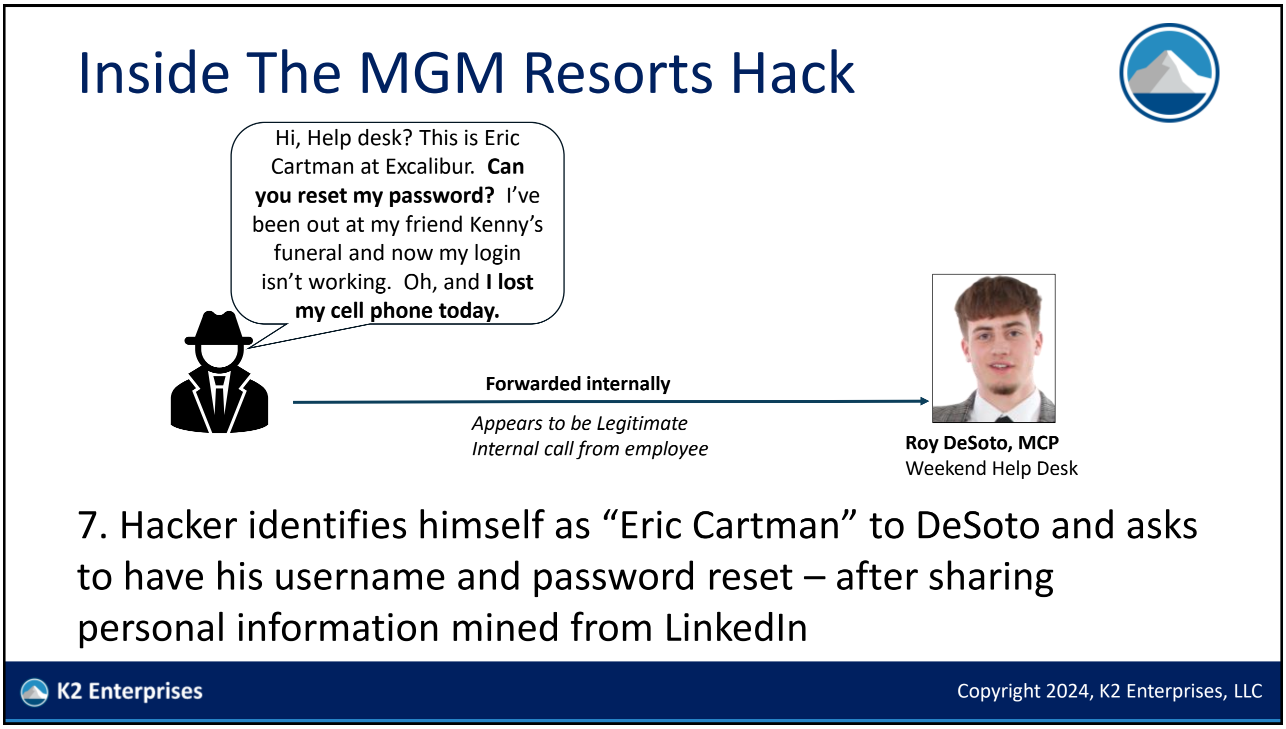
Appears to be Legitimate Internal call from employee

Roy DeSoto, MCP
Weekend Help Desk

6. Hacker introduces himself as Eric Cartman, a pit boss at the MGM Grand who misdialed this number, and Walker transfers him to DeSoto – which now appears as an "internal" call

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC



Inside The MGM Resorts Hack

Hi, Help desk? This is Eric Cartman at Excalibur. **Can you reset my password?** I've been out at my friend Kenny's funeral and now my login isn't working. Oh, and **I lost my cell phone today.**

Forwarded internally

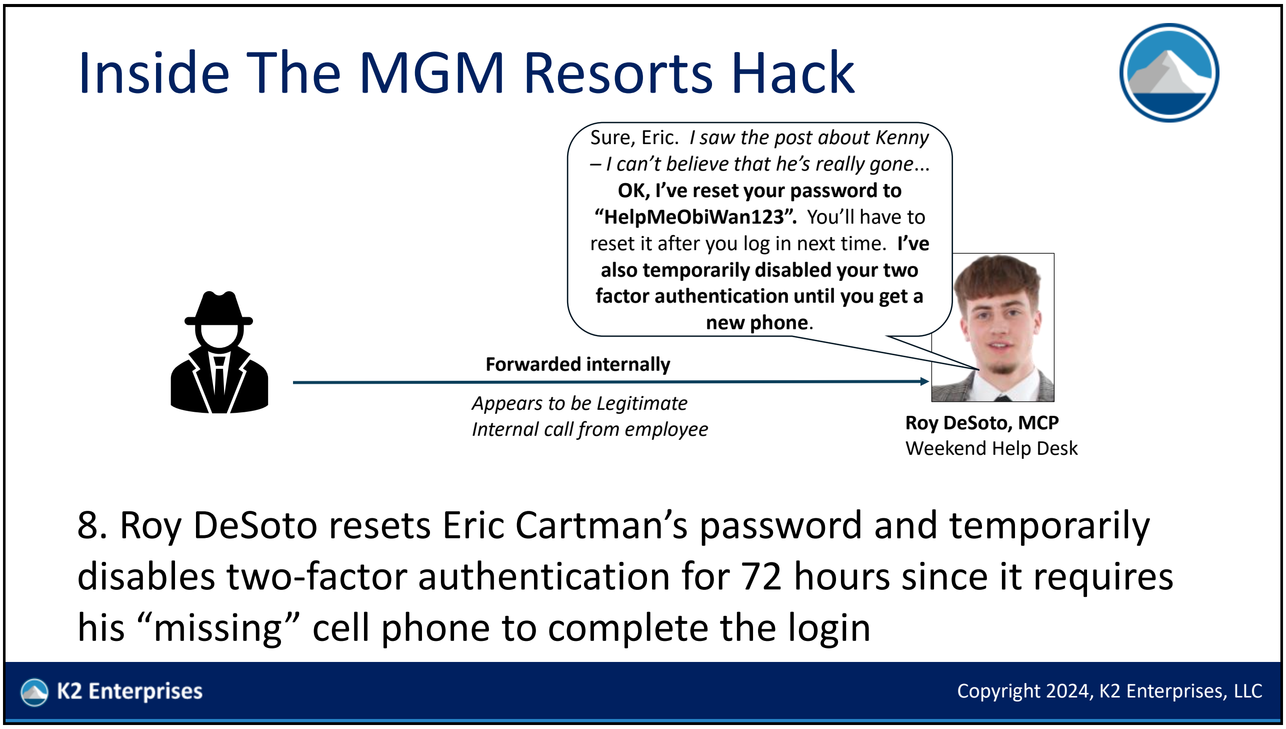
Appears to be Legitimate Internal call from employee

Roy DeSoto, MCP
Weekend Help Desk

7. Hacker identifies himself as "Eric Cartman" to DeSoto and asks to have his username and password reset – after sharing personal information mined from LinkedIn

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC



Inside The MGM Resorts Hack

Sure, Eric. *I saw the post about Kenny – I can't believe that he's really gone…* **OK, I've reset your password to "HelpMeObiWan123".** You'll have to reset it after you log in next time. **I've also temporarily disabled your two factor authentication until you get a new phone**.

Forwarded internally

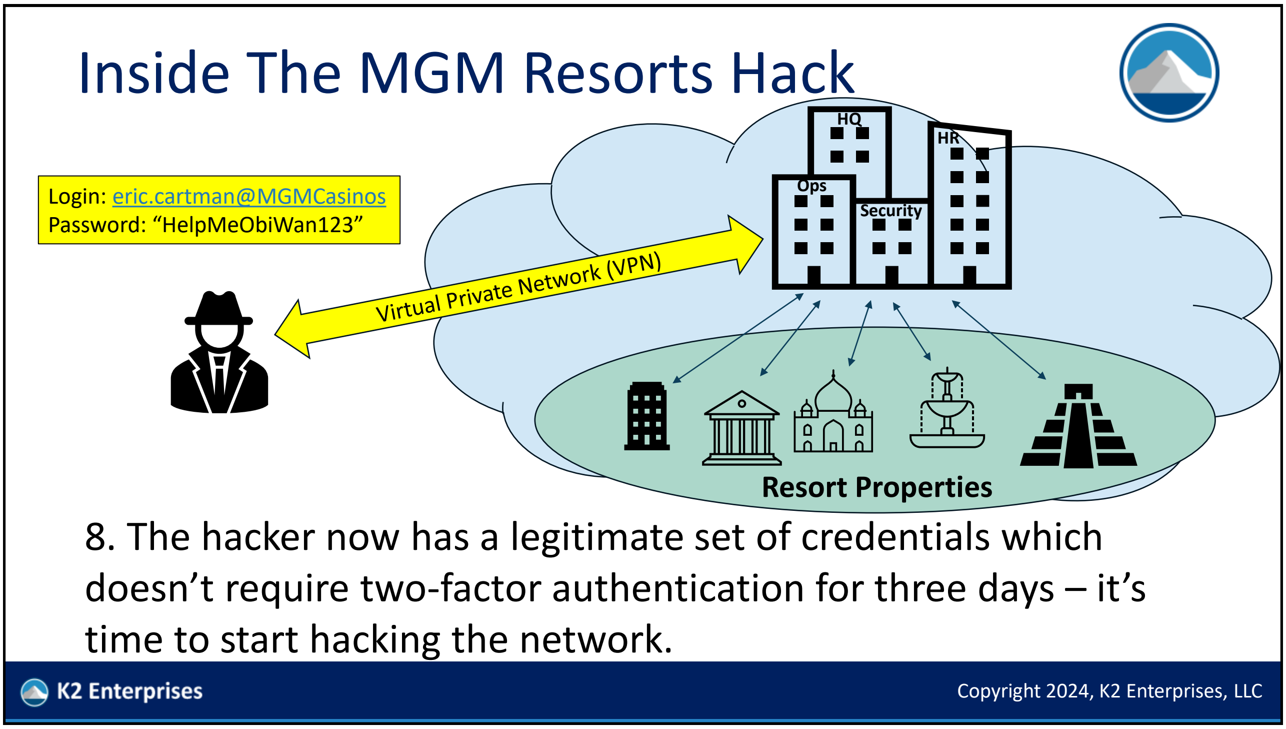
Appears to be Legitimate
Internal call from employee

Roy DeSoto, MCP
Weekend Help Desk

8. Roy DeSoto resets Eric Cartman's password and temporarily disables two-factor authentication for 72 hours since it requires his "missing" cell phone to complete the login

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC



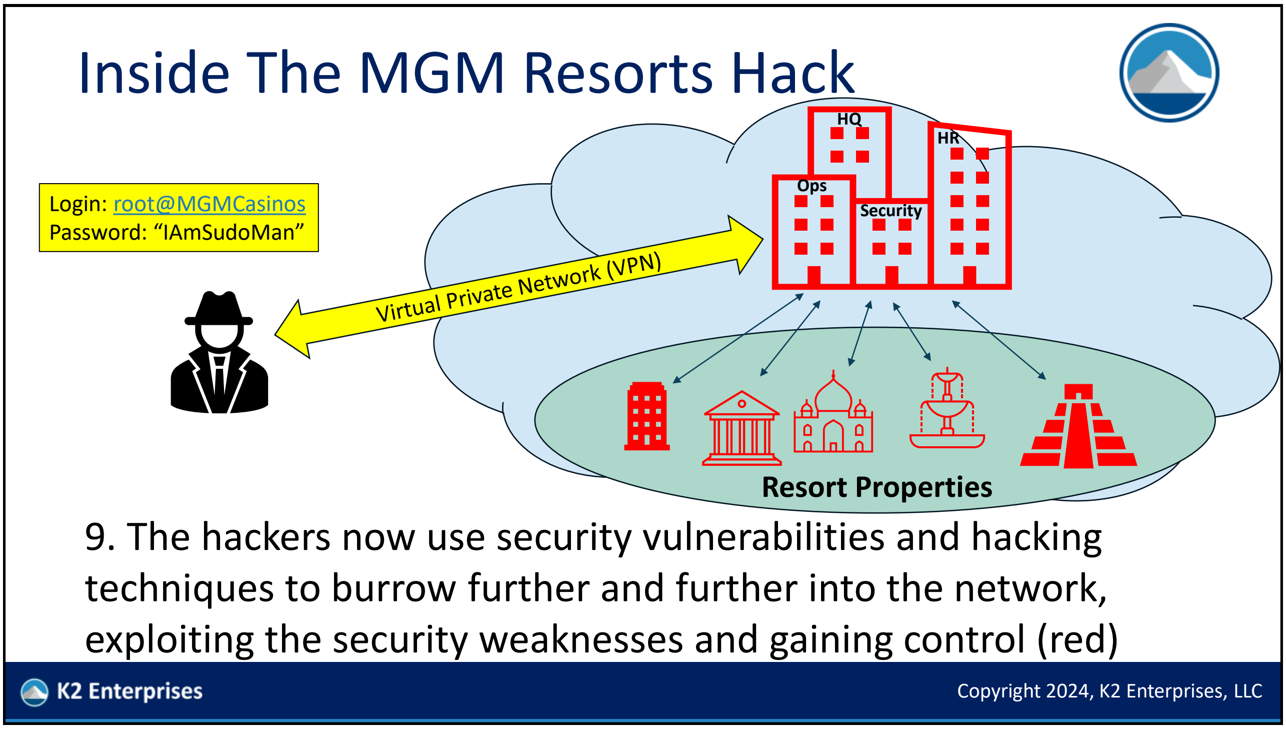
Inside The MGM Resorts Hack

Login: eric.cartman@MGMCasinos
Password: "HelpMeObiWan123"

8. The hacker now has a legitimate set of credentials which doesn't require two-factor authentication for three days – it's time to start hacking the network.

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC

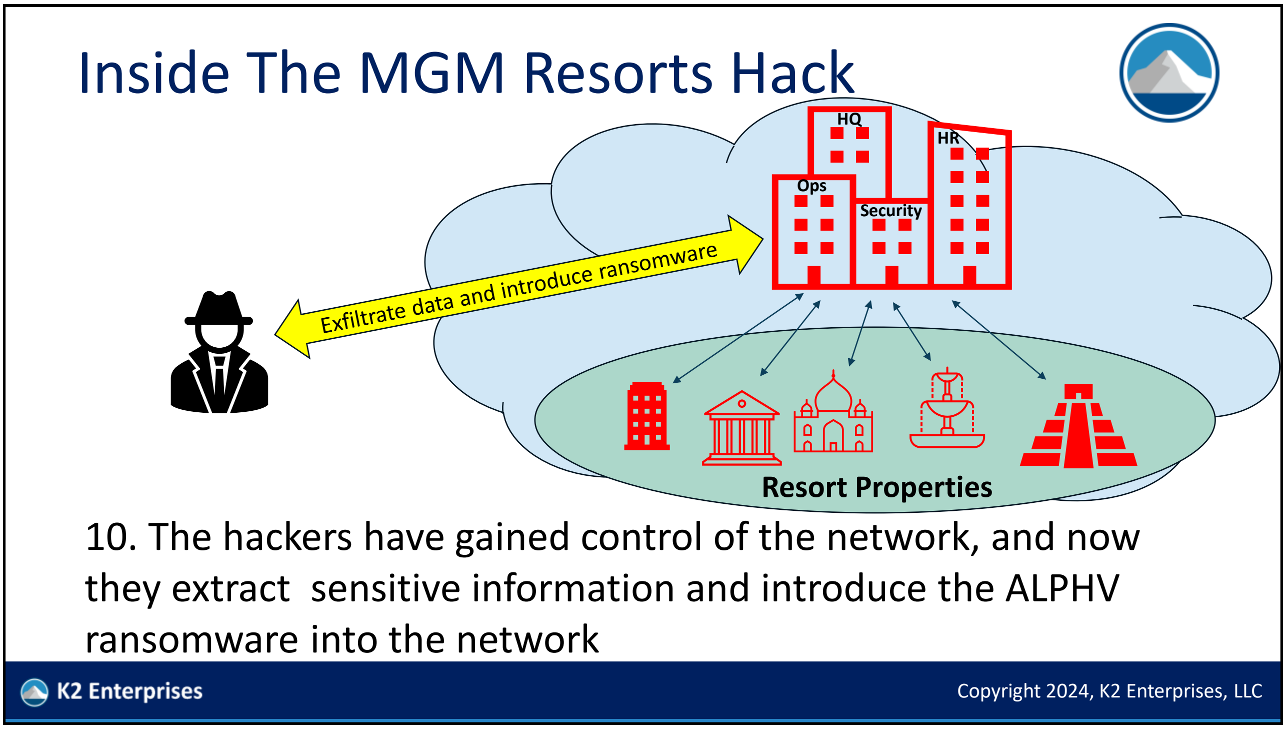


Inside The MGM Resorts Hack

Login: root@MGMCasinos
Password: “IAmSudoMan”

9. The hackers now use security vulnerabilities and hacking techniques to burrow further and further into the network, exploiting the security weaknesses and gaining control (red)

K2 Enterprises



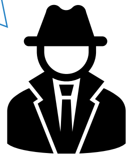
Inside The MGM Resorts Hack

10. The hackers have gained control of the network, and now they extract sensitive information and introduce the ALPHV ransomware into the network

K2 Enterprises

Inside The MGM Resorts Hack

We are Octo Tempest. You must pay $30 million or we will never decrypt your data and release sensitive information. We've locked everything up and you will be living in an analog world until the ransom is paid.



10. Once the data is encrypted on the network and the systems are rendered useless, the cybercriminals ask for $30 million

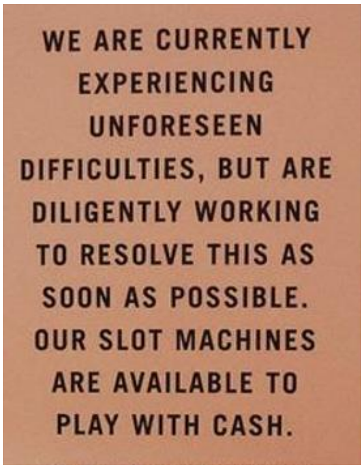
MGM Resorts Ransomware

MGM RESORTS INTERNATIONAL STATEMENT ON CYBERSECURITY ISSUE

September 12, 2023

Las Vegas, Sept. 12, 2023 /PRNewswire/ -- MGM Resorts International (the "Company" or "MGM Resorts") today issued the following statement:

"MGM Resorts recently identified a cybersecurity issue affecting certain of the Company's systems. Promptly after detecting the issue, we began an investigation with assistance from leading external cybersecurity experts. We also notified law enforcement and are taking steps to protect our systems and data, including shutting down certain systems. Our investigation is ongoing, and we are working diligently to resolve the matter. The Company will continue to implement measures to secure its business operations and take additional steps as appropriate."



WE ARE CURRENTLY EXPERIENCING UNFORESEEN DIFFICULTIES, BUT ARE DILIGENTLY WORKING TO RESOLVE THIS AS SOON AS POSSIBLE. OUR SLOT MACHINES ARE AVAILABLE TO PLAY WITH CASH.

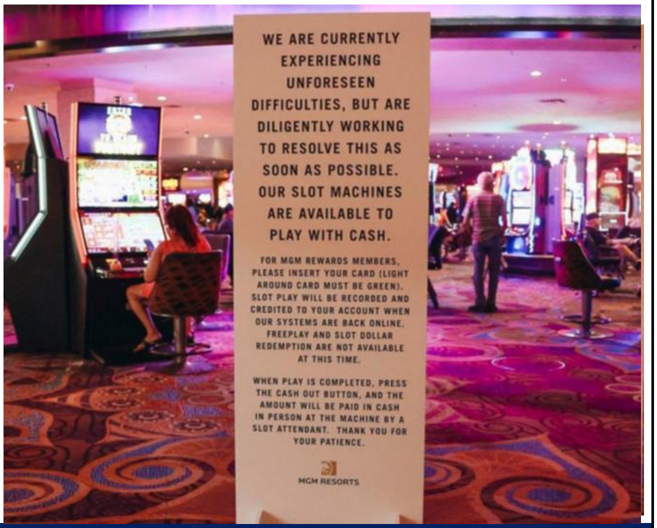
Operational Impacts At MGM

- Hotel room keys no longer worked and tens of thousands were locked out of their hotel rooms
- Dinner reservation systems and online hotel reservation systems were down
- Only cash payments could be accepted at point of sale systems
- ATMs and parking management systems failed

I'm having trouble communicating with the system. When the link is restored, your session will resume.

Operational Impacts At MGM

- Many slot machines simply didn't work, and on others, gamers had to wait up to an hour for winnings to be paid out in cash at the machine
- Guests were unable to check in or check out, and when backup systems were deployed, check in and check out often exceeded three hours
- The identity and access management (IAM) systems – Okta and Azure Active Directory – appeared to be compromised
  - (this is according to an excellent detailed analysis by CyberArk's Andy Thompson)



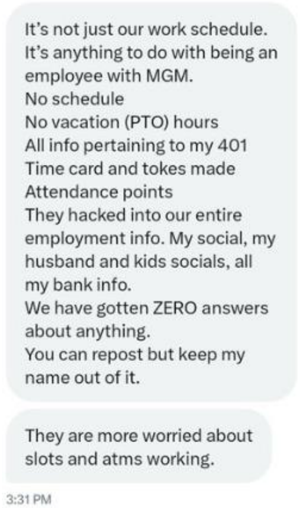
WE ARE CURRENTLY EXPERIENCING UNFORESEEN DIFFICULTIES, BUT ARE DILIGENTLY WORKING TO RESOLVE THIS AS SOON AS POSSIBLE. OUR SLOT MACHINES ARE AVAILABLE TO PLAY WITH CASH.

FOR MGM REWARDS MEMBERS, PLEASE INSERT YOUR CARD (LIGHT AROUND CARD MUST BE GREEN). SLOT PLAY WILL BE RECORDED AND CREDITED TO YOUR ACCOUNT WHEN OUR SYSTEMS ARE BACK ONLINE. FREEPLAY AND SLOT DOLLAR REDEMPTION ARE NOT AVAILABLE AT THIS TIME.

WHEN PLAY IS COMPLETED, PRESS THE CASH OUT BUTTON, AND THE AMOUNT WILL BE PAID IN CASH IN PERSON AT THE MACHINE BY A SLOT ATTENDANT. THANK YOU FOR YOUR PATIENCE.

MGM RESORTS

Operational Impacts At MGM



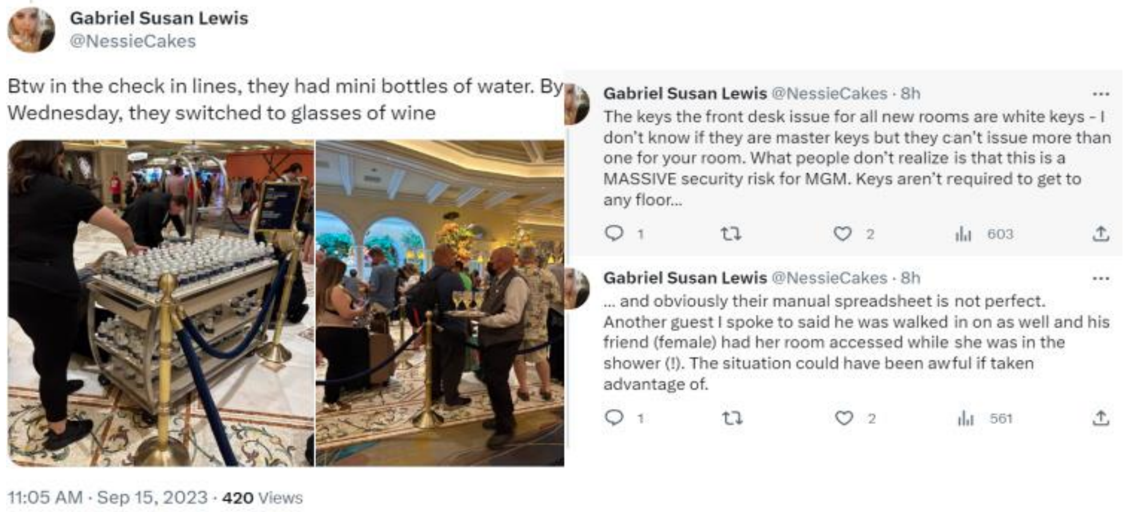
It's not just our work schedule. It's anything to do with being an employee with MGM.
No schedule
No vacation (PTO) hours
All info pertaining to my 401
Time card and tokes made
Attendance points
They hacked into our entire employment info. My social, my husband and kids socials, all my bank info.
We have gotten ZERO answers about anything.
You can repost but keep my name out of it.

They are more worried about slots and atms working.

3:31 PM

- Employees may feel intimidated or ignored in cybercrime situations like this one
- MGM Resorts (and the Aria Resort specifically) had collective bargaining issues with the Culinary Worker's union around this time – and this kind of uncertainty can make it much more difficult to recruit and retail
- When combined with the personal safety threats used by some cybercriminals, the mayhem that can be created on a victim increases exponentially

Operational Impacts At MGM Resorts & Some Bad Press/Social Media Posts



Gabriel Susan Lewis
@NessieCakes

Btw in the check in lines, they had mini bottles of water. By Wednesday, they switched to glasses of wine

11:05 AM · Sep 15, 2023 · 420 Views

Gabriel Susan Lewis @NessieCakes · 8h

The keys the front desk issue for all new rooms are white keys - I don't know if they are master keys but they can't issue more than one for your room. What people don't realize is that this is a MASSIVE security risk for MGM. Keys aren't required to get to any floor...

1 2 603

Gabriel Susan Lewis @NessieCakes · 8h

... and obviously their manual spreadsheet is not perfect. Another guest I spoke to said he was walked in on as well and his friend (female) had her room accessed while she was in the shower (!). The situation could have been awful if taken advantage of.

1 2 561

MGM Resorts Press Release 10/5/2023

MGM RESORTS UPDATE ON RECENT CYBERSECURITY ISSUE

October 5, 2023

LAS VEGAS, Oct. 5, 2023 /PRNewswire/ -- MGM Resorts International ("MGM Resorts" or the "Company") recently disclosed that the Company identified a cybersecurity issue affecting certain of its systems and that its investigation into the issue was ongoing. On or around September 29, 2023, MGM Resorts determined that **an unauthorized third party obtained personal information of some of its customers on September 11, 2023.**

The affected information included name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number. For a limited number of customers, Social Security number and/or passport number was also affected. The types of impacted information varied by individual.

The Company does not believe customer passwords, bank account numbers, or payment card information was affected by this issue.

Source: MGM Resorts Press Release 10/5/2023 (http://cpate.ch/mgmcypr)

MGM Resorts Press Release 10/5/2023

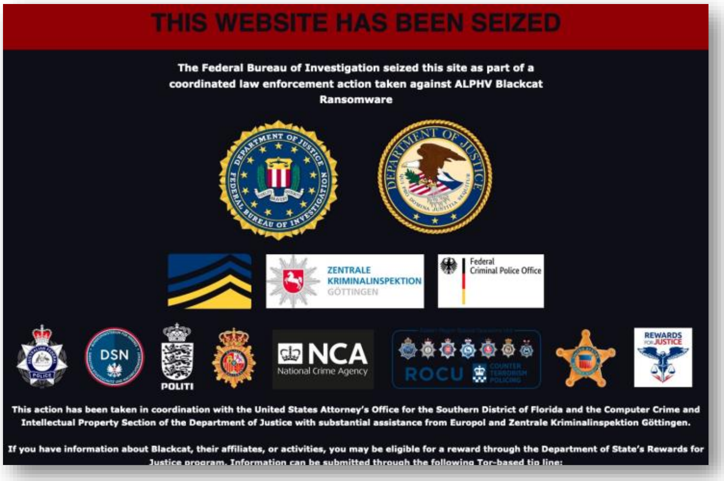
MGM RESORTS UPDATE ON RECENT CYBERSECURITY ISSUE

Promptly after learning of this issue, MGM Resorts took steps to protect its systems and data, including shutting down certain systems. The Company also quickly launched an investigation with the assistance of leading cybersecurity experts and is coordinating with law enforcement. MGM Resorts takes the security of its systems and data very seriously and has put in place additional safeguards to further protect its systems.

MGM Resorts is notifying relevant customers by email as required by applicable law and has arranged to provide those customers with credit monitoring and identity protection services at no cost to them. Individuals who receive an email from MGM Resorts about this issue should refer to that email for additional information and instructions for enrolling in these services.

Source: MGM Resorts Press Release 10/5/2023 (http://cpate.ch/mgmcypr)

Epilogue: Ransomware Site Seized


THIS WEBSITE HAS BEEN SEIZED

The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

ZENTRALE
KRIMINALINSPEKTION
GÖTTINGEN
Federal Criminal Police Office
DSN
POLITI
NCA National Crime Agency
ROCU
COUNTER TERRORISM POLICING
REWARDS FOR JUSTICE

This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

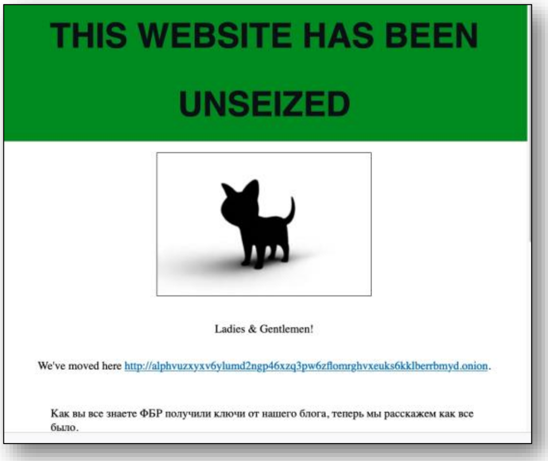
If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line:

Read the PDF affidavit for this raid online at Flashpoint's website

- In late December 2023, the website for the AlphV ransomware was taken down by a coalition of international law enforcement agencies….
- Credentials for the site were obtained from a confidential human source with access to the group

Epilogue: Ransomware Site Seized

- In a bizarre twist, after the site was "seized" by law enforcement, the group launched a new website, claiming that **"this website has been unseized"**
- This site was subsequently shut down by law enforcement


THIS WEBSITE HAS BEEN UNSEIZED

Ladies & Gentlemen!

We've moved here http://alphvuzxyxv6ylumd2ngp46xzq3pw6zflomrghvxeuks6kklberrbmyd.onion.

Как вы все знаете ФБР получили ключи от нашего блога, теперь мы расскажем как все было.

Web graphic for AlphV "unseized" website
Source: Ars Technica 12/20/2023

Lessons Learned

- Voice phishing – or "vishing" is a serious threat to every business and IT personnel should get extra training and monitoring to help prevent successful attacks
- A business continuity plan should be created and periodically tested for all businesses
- Given that the ransom was $30 million and the impact of the disruption was in excess of $100 million in September 2023 alone (before the breach was discovered), paying the ransom (as Caesar's Entertainment reportedly did – for $15MM) should be seriously considered as opposed to having operational chaos

Lessons Learned

- Some cyber criminals today behave more like the gangsters of the early 20th century than the mischievous hackers of the late 20th century
  - Threats against employees, their homes, and their families should be taken seriously and may require 24x7x365 security for the family for a period of time
- The impact of social media to cause fear and panic amidst catastrophic operational failures cannot be underestimated
  - Posts like the Twitter post which cites someone walking in on a woman in the shower can cause trauma that takes years to resolve

Lessons Learned

- Contingencies surrounding all operational issues should be evaluated and updated after each test – including mission critical areas like:
  - Identity/access management systems like OKTA and Ventra ID
  - Gaming operations and payouts
  - Hotel/restaurant point of sale and operations
  - Payment systems, ATMs, and other financial services
  - Reservations and hotel operations
  - Handling social media posts of such failures

"Hackers Backed by Russia and China are Infecting SOHO Routers Like Yours, FBI Warns", Ars Technica, 2/27/2024

"Chinese Malware Removed from SOHO Routers After FBI Issues Covert Commands", Ars Technica, 1/31/2024

ROUTER VULNERABILITIES

A Small Subset Of Critical Updates

Date	Publication	Link
3/26/2024	Bleeping Computer	TheMoon malware infects 6,000 ASUS routers in 72 hours
3/20/2024	Bleeping Computer	New 'Loop DoS' attack may impact up to 300,000
2/27/2024	Ars Technica	Hackers backed by Russia and China are infecting SOHO routers like yours, FBI warns
1/31/2024	Ars Technica	Chinese malware removed from SOHO routers after FBI issues covert commands
1/31/2024	PC Magazine	FBI disrupts Chinese botnet by wiping malware from infected routers
1/31/2024	Bleeping Computer	CISA Vendors must secure SOHO routers against Volt Typhoon attacks
6/19/2023	Bleeping Computer	ASUS urges customers to patch critical router vulnerabilities
6/11/2023	Bleeping Computer	Fortinet fixes critical RCE flaw in Fortigate SSL-VPN devices, patch now
5/19/2023	Ars Technica	ASUS routers knocked offline worldwide by bad security update
5/16/2023	Bleeping Computer	Hackers infect TP-Link router firmware to attack EU entities
5/2/2023	The Register	TP-Link Archer WiFi router flaw exploited by Mirai malware
3/23/2023	Tech Radar	Netgear Orbi routers have some troubling security issues, so patch
3/15/2023	SC Media	Fortinet Govt networks targeted with now-patched SSL-VPN zero
1/20/2023	Bleeping Computer	Over 19,000 end-of-life Cisco routers exposed to RCA Attacks
12/30/2022	Tech Radar	Netgear Wi-Fi routers need to be patched immediately
12/29/2022	Bleeping Computer	Netgear warns users to patch recently fixed WiFi router bug
1/24/2021	Tech Radar	Netgear patches serious bug found in several popular routers
10/16/2017	Bleeping Computer	List of Firmware Driver Updates for KRACK WPA2 Vulnerability

What Happened?

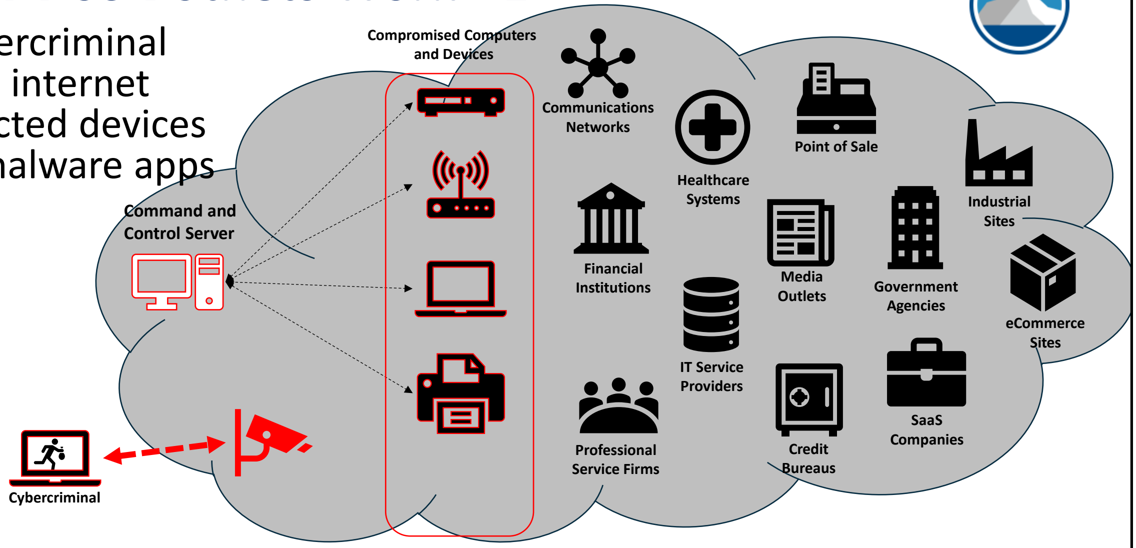
- Even though most everyone has a wireless router at their home, very few people are capable of configuring this router by themselves
  - Fewer users still know how to determine if a router is at its "end of life"
  - And even fewer of them know how to update the firmware/software on the router
- While most of you didn't get any training as a network engineer, it IS critical that you keep up with when your devices are at their end of life.

The Satori Botnet

- Is based on the Mirai malware which compromised internet-connected devices like routers and digital video recorders who had not changed the default passwords
- This kind of botnet is often used to extort money from big websites in exchange for not shutting them down
- Exploits bugs in embedded firmware to take control of internet exposed devices
- Home grade devices are often poorly configured and rarely receive the timely security updates necessary to keep them safe from hackers

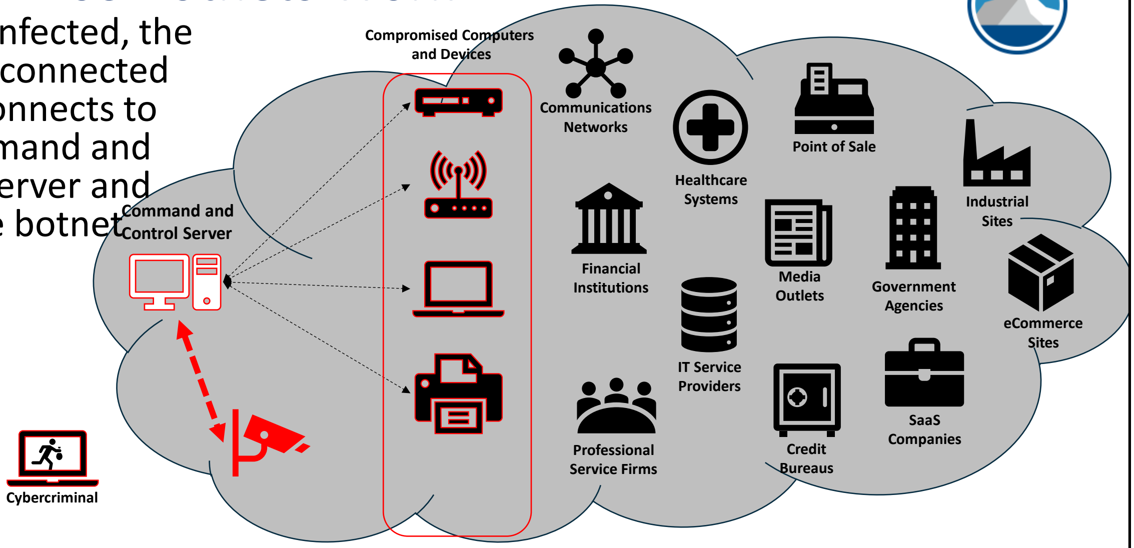
How DDoS Botnets Work - 1

1. Cybercriminal infects internet connected devices with malware apps



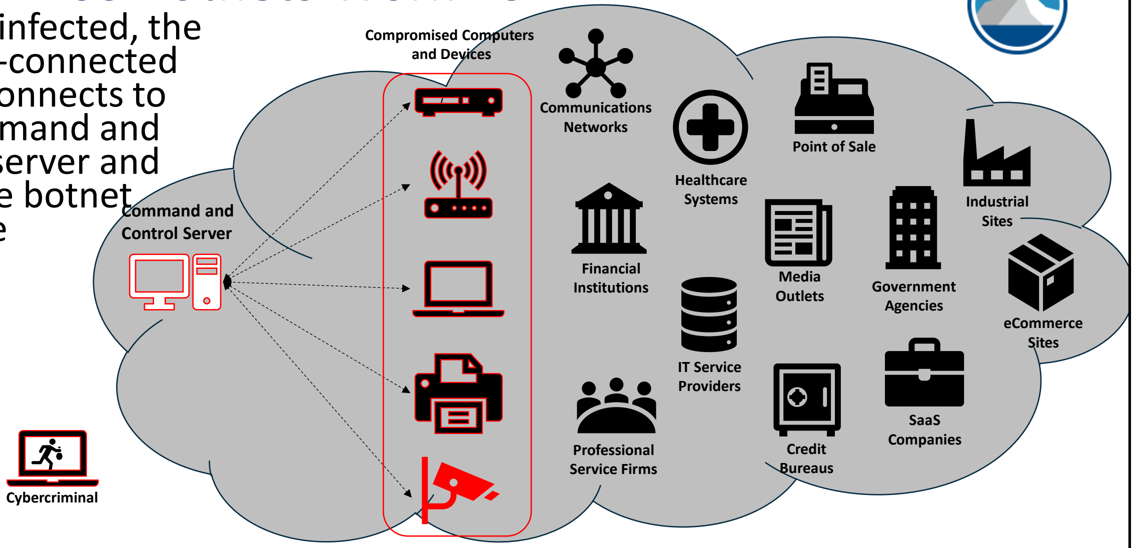
How DDoS Botnets Work - 2

2. Once infected, the internet-connected device connects to the command and control server and loads the botnet software



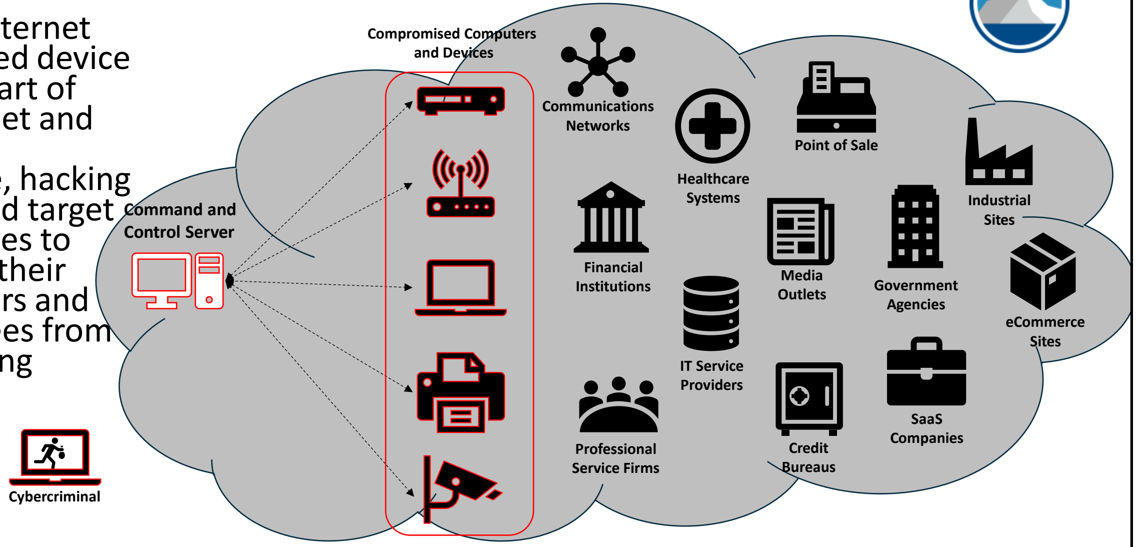
How DDoS Botnets Work - 3

3. Once infected, the internet-connected device connects to the command and control server and loads the botnet software



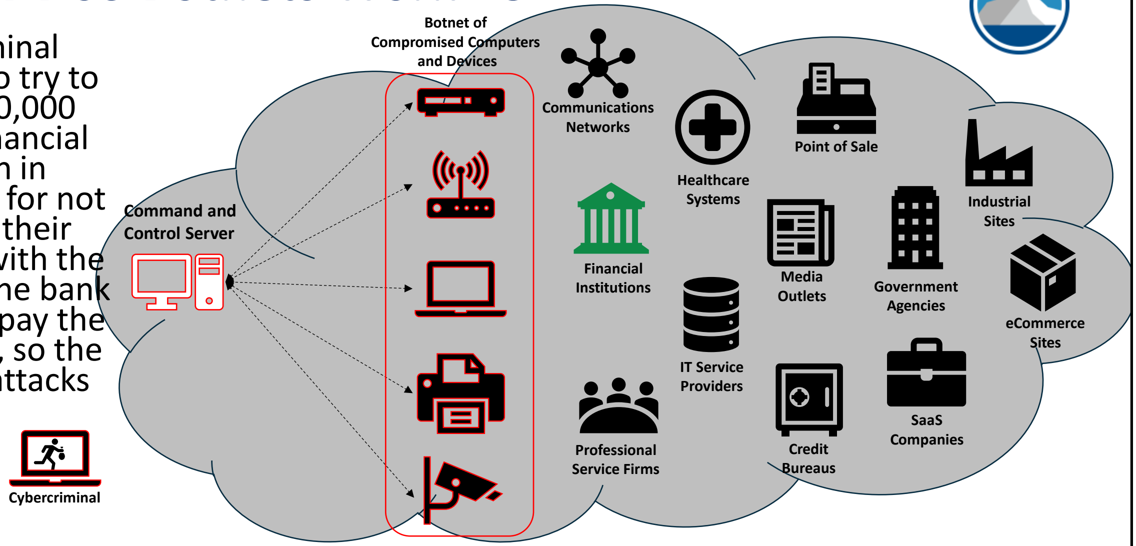
How DDoS Botnets Work - 4

4. The internet connected device is now part of the botnet and can load malware, hacking tools, and target businesses to prevent their customers and employees from interacting



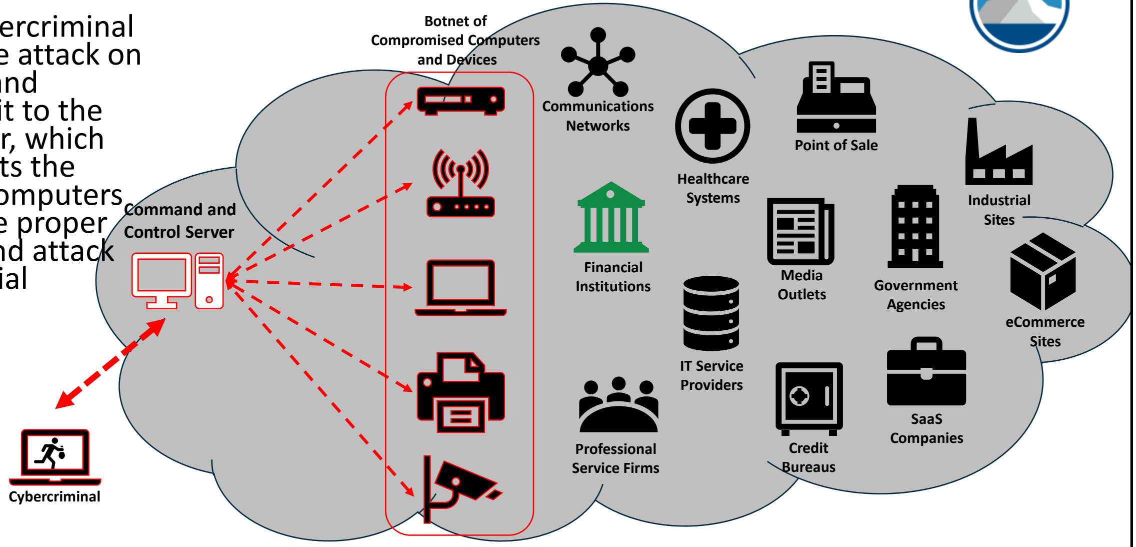
How DDoS Botnets Work - 5

5. The cybercriminal decides to try to extort $90,000 from a financial institution in exchange for not attacking their website with the botnet. The bank does not pay the extortion, so the criminal attacks



How DDoS Botnets Work - 6

6. The cybercriminal sets up the attack on the bank and transmits it to the C&C server, which then directs the infected computers to load the proper exploits and attack the financial institution



Botnet of Compromised Computers and Devices

Command and Control Server

Cybercriminal

Communications Networks

Healthcare Systems

Point of Sale

Industrial Sites

Financial Institutions

Media Outlets

Government Agencies

eCommerce Sites

IT Service Providers

Professional Service Firms

Credit Bureaus

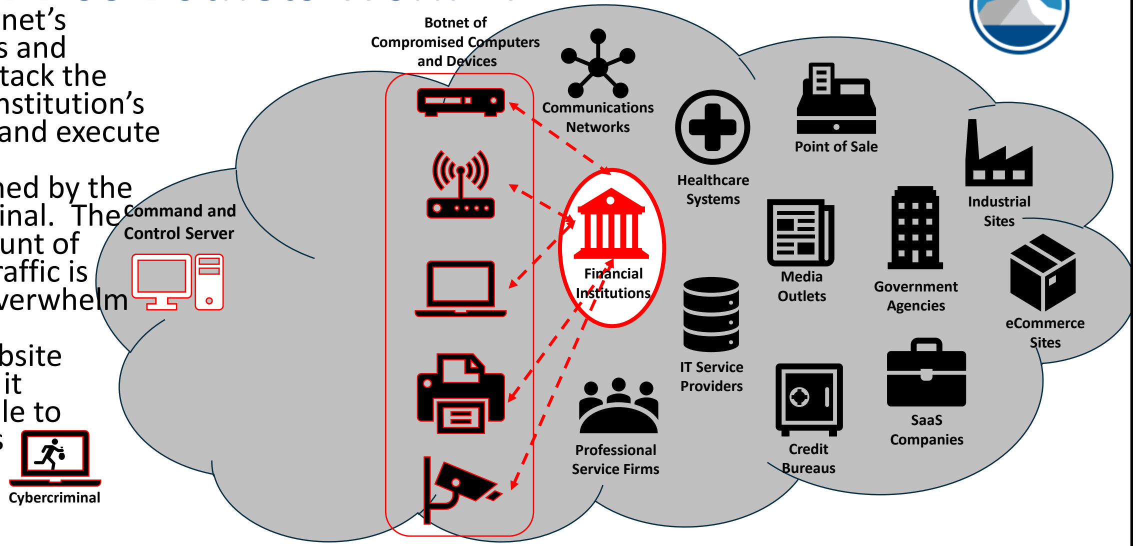
SaaS Companies

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC

How DDoS Botnets Work - 7

7. The botnet's computers and devices attack the financial institution's networks and execute the attack programmed by the cybercriminal. The large amount of internet traffic is likely to overwhelm the bank's website and make it inaccessible to customers



Botnet of Compromised Computers and Devices

Command and Control Server

Cybercriminal

Communications Networks

Healthcare Systems

Point of Sale

Industrial Sites

Financial Institutions

Media Outlets

Government Agencies

eCommerce Sites

IT Service Providers

Professional Service Firms

Credit Bureaus

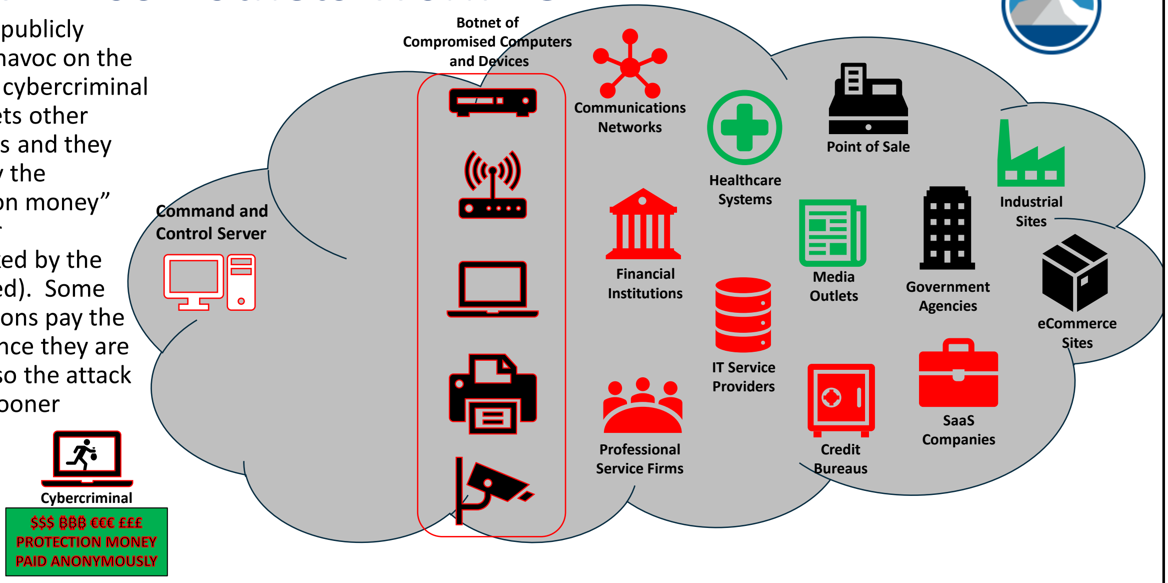
SaaS Companies

K2 Enterprises

Copyright 2024, K2 Enterprises, LLC

How DDoS Botnets Work - 8

8. Having publicly wreaked havoc on the bank, the cybercriminal now targets other businesses and they either pay the “protection money” (green) or are attacked by the botnet (red). Some organizations pay the ransom once they are attacked so the attack will end sooner



Five Reasons Home-Grade Routers And Devices Are Dangerous To Your Office Network

1. Many users do not change the default username and password
2. The firmware is rarely updated; if significant security issues are found and reported, many manufacturers tell you to buy a new device
3. The software and the device itself are designed to be disposable; the business model requires purchasing a new device every 2-3 years
4. The default settings are usually very weak and do not adequately secure the network environment against malicious outsiders
5. There is usually little, if any, opportunity to separate IoT devices like cameras, wi-fi enabled lights, and garage door openers onto a separate subnet so they cannot interact with machines with confidential data

Some Basic Rules For Securing Your IoT Stuff

(Adapted from Krebs on Security, 1/17/2018)

1. Avoid connecting your devices directly to the internet, and use a firewall to block incoming traffic
2. If you can, change the thing's default credentials
3. Update the firmware when you set up and also check for updates periodically
4. Check the default settings and make sure that features like UPnP are disabled
5. Avoid IoT devices that advertise Peer-to-Peer (P2P) capabilities to other devices or online
6. Consider the cost of the device – cheaper is usually not better

KrebsonSecurity
In-depth security news and investigation

17 Some Basic Rules for Securing Your IoT Stuff

JAN 18

Most readers here have likely heard or read various prognostications about the impending doom from the proliferation of poorly-secured "Internet of Things" or IoT devices. Loosely defined as any gadget or gizmo that connects to the Internet but which most consumers probably wouldn't begin to know how to secure, IoT encompasses everything from security cameras, routers and digital video recorders to printers, wearable devices and "smart" lightbulbs.

Throughout 2016 and 2017, attacks from massive botnets made up entirely of hacked IoT devices had many experts warning of a dire outlook for Internet security. But the future of IoT doesn't have to be so bleak. Here's a primer on minimizing the chances that your IoT things become a security liability for you or for the Internet at large.

Rule #1: Avoid connecting your devices directly to the Internet – either without a firewall or in front it, by poking holes in your firewall so you can access them remotely. Putting your devices in front of your firewall is generally a bad idea because many IoT products were simply not designed with security in mind and making these things accessible over the public Internet could invite attackers into your network. If you have a router, chances are it also comes with a built-in firewall. Keep your IoT devices behind the firewall as best you can.

Lessons Learned:

- Don't use home grade hardware anywhere in your business network unless it's segmented onto a separate network which does not carry any confidential information
- Always change the default admin password on your router and other devices to a unique strong password which you store in password management software
- Keep the firmware in your devices updated to the latest versions to protect against known security issues on these devices
- Troubleshoot devices which are not performing properly and reconfigure/replace them promptly when trouble arises

"WormGPT Cybercrime Tool Heralds an Era of AI Malware vs. AI Defenses" **– Dark Reading,** July 13, 2023

"Meet the Brains Behind the Malware-Friendly AI Chat Service 'WormGPT'" – **Krebs on Security**, August 8, 2023

HACKING WITH AI IN THE WILD: WORMGPT AND FRAUDGPT

Hacking With AI In The Wild

- Just as happens with all technologies, what works for good also can be used for evil
- At least two chatbots appeared in mid-2023 to meet the generative AI demands of sophisticated hackers - **WormGPT** and **FraudGPT**
- Public AI engines like ChatGPT have safeguards which prevent socially undesirable queries from being fulfilled – but these tools don't have those kinds of limits

WormGPT

- **WormGPT** is/was an AI engine which analyzes data simultaneously in a non-linear fashion, resulting in more accurate generation of fake e-mail text for phishing and business e-mail compromise (BEC) attacks
- Tested by some security researchers and used by one to create a "business e-mail compromise" (BEC) phishing e-mail
  - *"WormGPT produced an email that was not only remarkably persuasive but also strategically cunning, showcasing its potential for sophisticated phishing and BEC attacks."* – Daniel Kelley of SlashNext

Learn more about WormGPT at the SlashNext blog or at ZDNet

WormGPT

- SlashNext's Kelley also noted:
  - Generative AI can create messages with "impeccable" grammar, which makes the messages more believable
  - This kind of tool makes it much easier for hackers with "limited skills" to create successful attacks against organizations
  - Organizations should update training programs for BEC attacks regularly to include emerging tools like WormGPT

Learn more about WormGPT at the SlashNext blog or at ZDNet

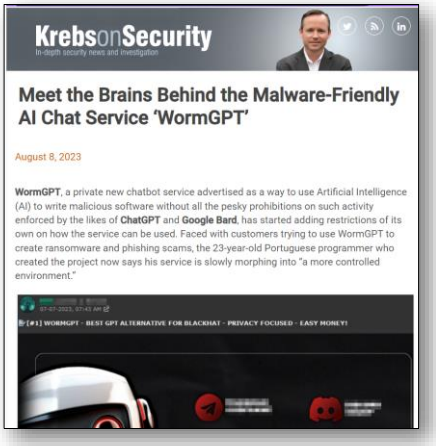
WormGPT

- SlashNext’s Kelley also noted:
  - A possible “fortification” against BEC attacks is to use stringent rules to identify when legitimate employees, customers, or vendors appear to be impersonated in e-mail
  - Another promising approach is to flag messages with keywords linked to BEC attacks like “urgent”, “sensitive”, and “wire transfer” for further scrutiny

Learn more about WormGPT at the SlashNext blog or at ZDNet

Who Was Behind WormGPT?

- According to security investigative journalist Brian Krebs, WormGPT was traced back to a HackForums user going by the handle of “Last”
- This user was traced to an account for a 23 year old Portuguese programmer
- Initially, WormGPT licenses were reportedly sold for **USD** $540-$5,400 / **CAD** $730-$7,300
- Scammers unrelated to WormGPT “sold” subscriptions to WormGPT to victims – who never received access to the tool
- WormGPT shut down in August 2023, shortly after this programmer was publicly identified



KrebsonSecurity
In-depth security news and investigation

Meet the Brains Behind the Malware-Friendly AI Chat Service ‘WormGPT’

August 8, 2023

WormGPT, a private new chatbot service advertised as a way to use Artificial Intelligence (AI) to write malicious software without all the pesky prohibitions on such activity enforced by the likes of **ChatGPT** and **Google Bard**, has started adding restrictions of its own on how the service can be used. Faced with customers trying to use WormGPT to create ransomware and phishing scams, the 23-year-old Portuguese programmer who created the project now says his service is slowly morphing into “a more controlled environment.”

[redacted]
07-07-2023, 07:43 AM

[#1] WORMGPT - BEST GPT ALTERNATIVE FOR BLACKHAT - PRIVACY FOCUSED - EASY MONEY!

[redacted]

[redacted]

Read the detailed profile of WormGPT’s author at Krebs on Security

FraudGPT

- Similar tool to WormGPT
  - Can generate phishing campaigns and business e-mail compromise messages and other fake documents
- Subscription fees range from $200 USD/mo ($271 CAD) to $1,700 USD/yr ($2,300 CAD)
- With more than 3,000 subscriptions sold through July 2023, this product has identified an audience willing to pay for generative AI without limits
- Generative AI is being used more and more by “red teams” which are security analysts charged with finding vulnerabilities in systems

Learn more about FraudGPT at the Cybersecurity News Blog or at Netenrich’s blog

K2 Enterprises

FraudGPT

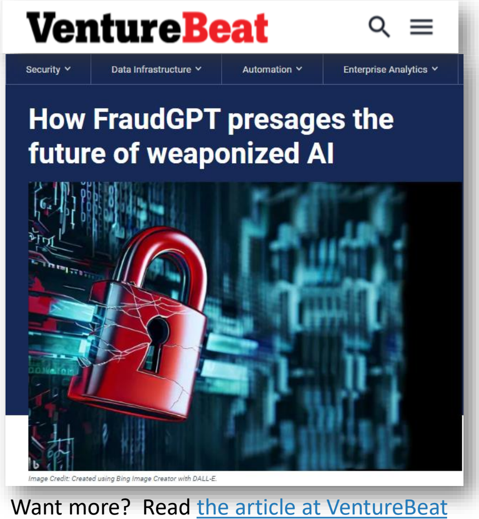
- FraudGPT can reportedly also:
  - write malicious code
  - create undetectable malware
  - create phishing pages
  - build hacking tools
  - identify stolen credit cards numbers which do not require one-time passwords (“non vbv bins”)
  - find leaks and vulnerabilities
  - find hacking groups, sites, and markets

Learn more about FraudGPT at the Cybersecurity News Blog or at Netenrich’s blog

K2 Enterprises

FraudGPT And Weaponized AI

- In a Q3 2023 article, VentureBeat cited five ways in which FraudGPT shows us a troubling future of weaponized AI
  1. Automated social engineering and phishing attacks
  2. AI-generated malware and exploits
  3. Automated discovery of cybercrime resources
  4. AI-driven evasion of defenses is just starting…
  5. Difficulty of detection and attribution



VentureBeat

How FraudGPT presages the future of weaponized AI

Image Credit: Created using Bing Image Creator with DALL-E.

Want more? Read the article at VentureBeat

Lessons Learned

- The best tool against offensive AI tools is likely to be a whole new class of defensive AI tools which use real time information to respond to emerging threats
- The days of signature-based antivirus tools as an effective solution are over since novices can use AI tools to create new strains of malware which will run amok for the 2-3 days it takes for the malware signatures for new threats to be incorporated into these tools

Lessons Learned

- The AI arms race has only begun, and will make both the "good guys" and the "bad guys" more effective
- Every revolutionary tool can be used for good and evil, and those who do not keep up with the rapid evolution of threats and defenses will experience unprecedented attacks in the coming years

Lessons Learned

- Like the dawn of the atomic age at the end of World War II, there is no way to go back to the "good old days" before AI technology existed - it's here forever
- Generative AI tools like WormGPT and Fraud GPT will make it possible for entry level hackers ("script kiddies") and non-technical organized crime to create very effective cyber attacks without having the technical skills and experience once needed to design, launch, and execute these hacks

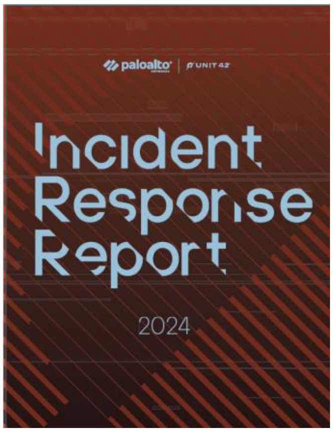
UNIT 42™
BY PALO ALTO NETWORKS

UNIT 42 2023 INCIDENT RESPONSE REPORT

K2 Enterprises

2024 Unit 42 Incident Response Report

- Enterprise IT hardware vendor Palo Alto Networks operates a top tier forensic and incident response team called “Unit 42”
- Unit 42’s annual incident response report details the major themes and lessons learned from its 2024 engagements
- Its observations detail the trends and threats used by cybercriminals to attack targets, and serve as a roadmap for expected future trends in cybercrime


paloalto | UNIT 42

Incident Response Report

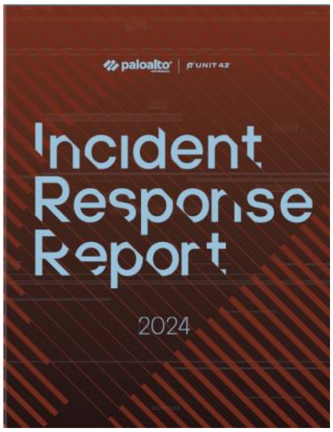
2024

Obtain and review the 66-page detailed report from Unit 42

K2 Enterprises

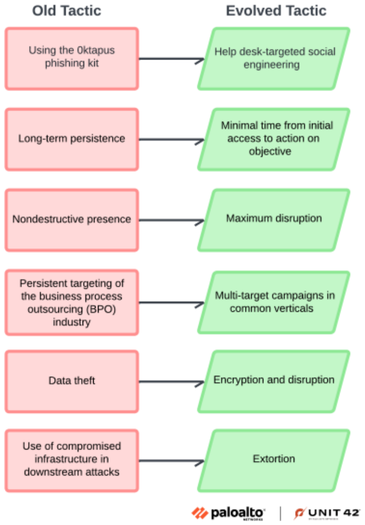
Key Findings – 2024

- Attackers are compromising systems and exfiltrating data faster than ever
  - Defenders need to speed up to remain effective
- Software vulnerabilities were how attackers compromised systems in all of the largest scale attack campaigns in 2023
- Threat actors are becoming more specialized and sophisticated, and can use IT, cloud, and security tools very effectively as offensive weapons against targets



Obtain and review the 66-page detailed report from Unit 42

Muddled Libra / Scattered Spider

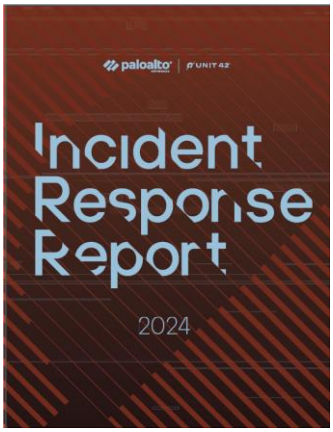


Old Tactic	Evolved Tactic
Using the Oktapus phishing kit	Help desk-targeted social engineering
Long-term persistence	Minimal time from initial access to action on objective
Nondestructive presence	Maximum disruption
Persistent targeting of the business process outsourcing (BPO) industry	Multi-target campaigns in common verticals
Data theft	Encryption and disruption
Use of compromised infrastructure in downstream attacks	Extortion

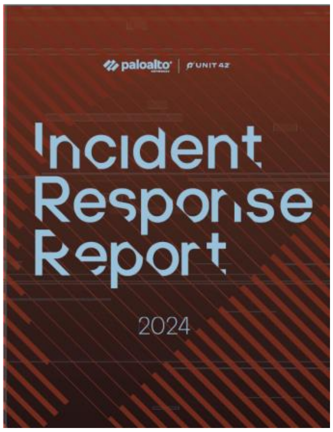
- Much of the 2024 Unit 42 incident response report is concerned with 2023's most active hacker group, "**Muddled Libra**"
- This group is know by many other names, including Scattered Spider, 0ktapus, Starfraud, UNC3944, Scatter Swine, and Octo Tempest
- In 2023, Muddled Libra was responsible for attacks on **Caesar's Entertainment, MGM Resorts**, identity/access management vendor **Okta**, and a late 2022 attack on telecommunications firm **Twilio**

Vulnerabilities Enabling Attacks

- Three key security weaknesses were at the core of 2023’s major cybersecurity incidents
  - **Unpatched software** and configuration vulnerabilities gave attackers openings to exploit
  - **Inconsistent and incomplete deployment of endpoint detection and response tools** allowed attackers to operate from undefended parts of victim networks
  - **Identity and access management (IAM)** compromises and credential thefts allow attackers to function as privileged users on victim networks



Obtain and review the 66-page detailed report from Unit 42



Vulnerabilities Enabling Attacks

- Three key security weaknesses were at the core of 2023’s major cybersecurity incidents
  - **Unpatched software** and configuration vulnerabilities gave attackers openings to exploit
  - **Inconsistent and incomplete deployment of endpoint detection and response tools** allowed attackers to operate from undefended parts of victim networks
  - **Identity and access management (IAM)** compromises and credential thefts allow attackers to function as privileged users on victim networks

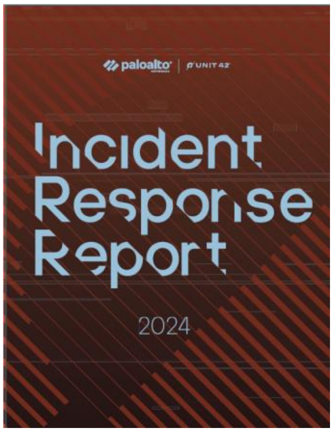
Obtain and review the 66-page detailed report from Unit 42

K2 Enterprises
Copyright 2024, K2 Enterprises, LLC

Industries Targeted In 2023

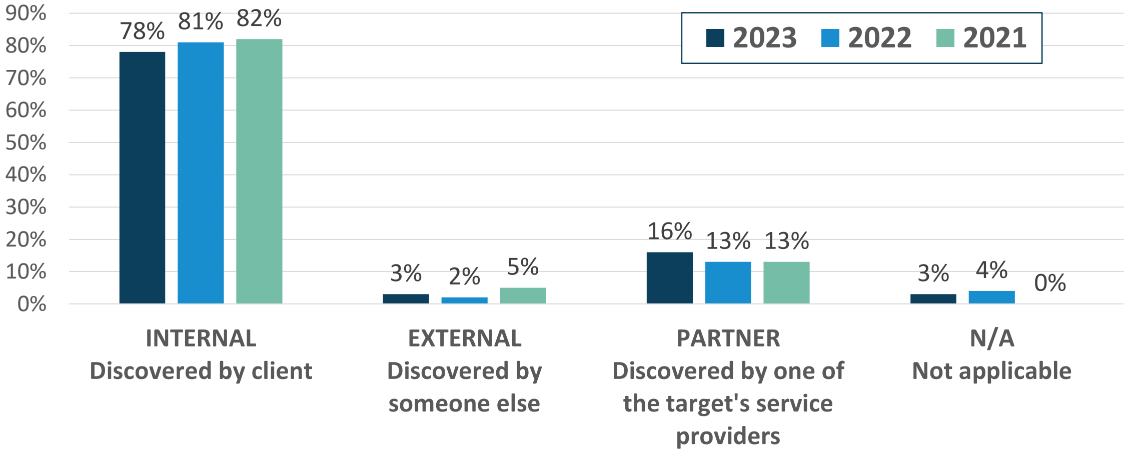
The industries most commonly targeted by attackers in 2023 were:

- Professional and legal services
- High technology
- Manufacturing
- Healthcare
- Finance
- Wholesale and retail



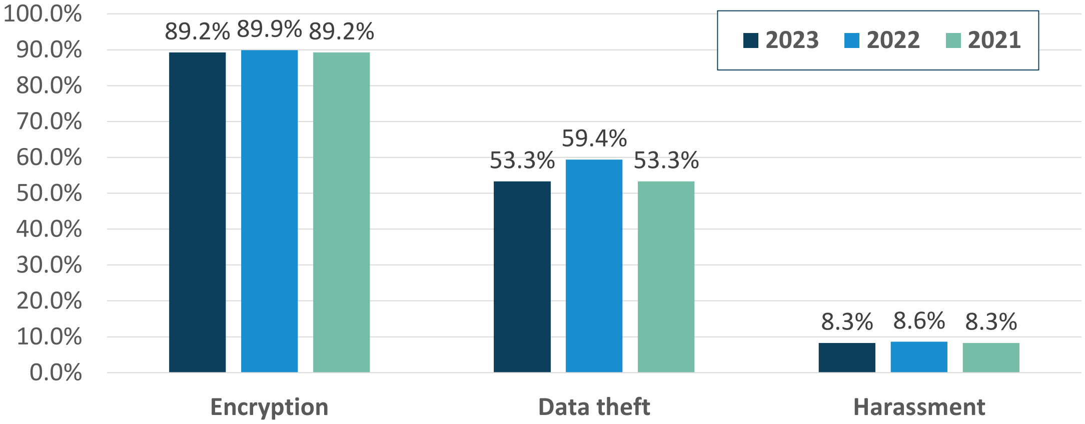
Obtain and [review the 66-page detailed report from Unit 42]

Who Discovered The Attack?



Source: Unit 42 2023 IRR, pg. 21

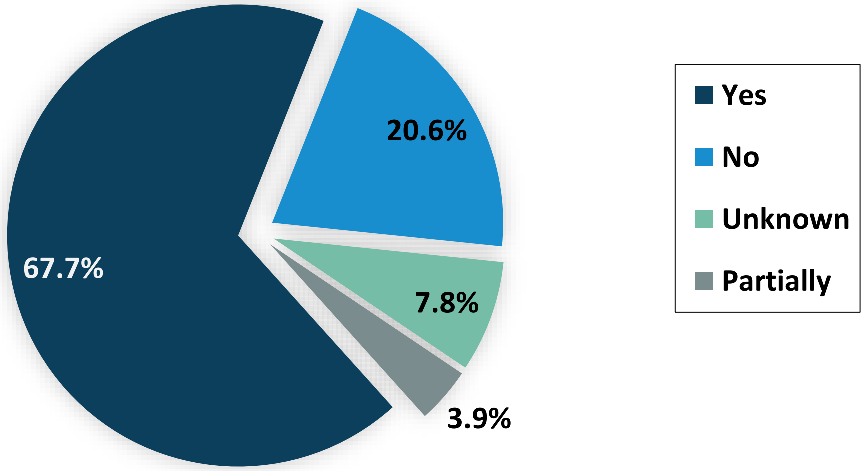
Extortion Techniques – All Cases



Source: Unit 42 2023 IRR, pg. 21

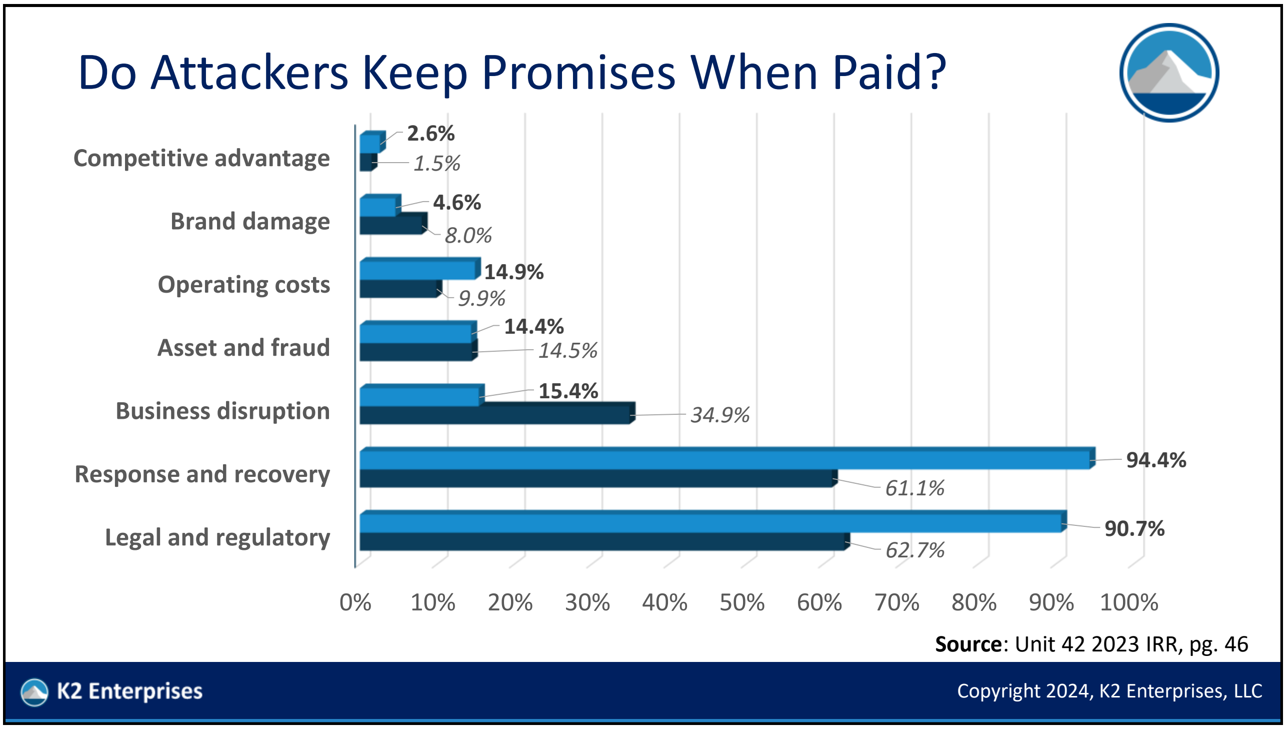
K2 Enterprises

Do Attackers Keep Promises When Paid?



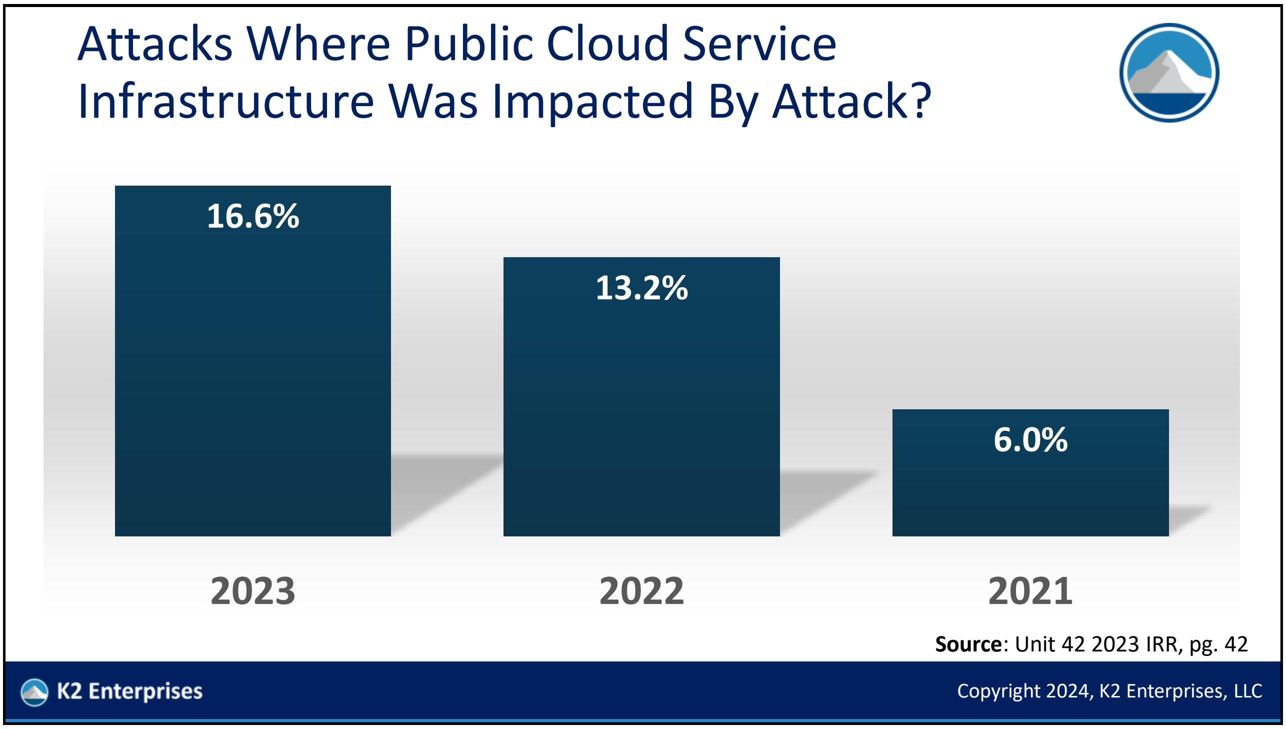
Source: Unit 42 2023 IRR, pg. 21

K2 Enterprises



Do Attackers Keep Promises When Paid?

Source: Unit 42 2023 IRR, pg. 46



Attacks Where Public Cloud Service Infrastructure Was Impacted By Attack?

Source: Unit 42 2023 IRR, pg. 42

Lessons Learned

- Extortionists who run ransomware scams are becoming more ruthless in how they execute their scams
- Just as public cloud services have become part of every company's infrastructure, hackers are increasingly compromising the identity and access management systems like Okta and Microsoft Ventra ID which make single sign-on access to these services by employees possible
- Although the majority of scammers kept their promises when ransoms were paid, there are certainly no guarantees

K2 Enterprises

Conclusion

- Threats and threat actors will change more rapidly in the future
- AI will be used for both good and evil purposes, so you must use it to defend your data and devices
- Ransomware attacks are becoming more vicious and cybercrime is starting to have many features that are similar to organized crime, like physical threats against people
- Although phishing is a serious problem and the most common complaint to FBI's IC3, the dollars involved pale in comparison to business e-mail compromises and investment scams
- Your home hardware devices are your front door to the internet – and MUST be both supported and on the latest hardware to reduce your risks to anything approaching an acceptable level

K2 Enterprises