



NJCCIC

PROTECT, DEFEND, RESPOND



cyber.nj.gov

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) is known as the Division of Cybersecurity of the New Jersey Office of Homeland Security and Preparedness (NJOHSP). NJOHSP helps to direct prevention, detection, protection, response, and recovery planning, not only at the State level, but also at the regional and national levels with our varied partners. NJOHSP is comprised of four Divisions: Intelligence, Policy and Planning, Cybersecurity, and Administration.



Housekeeping Items

- **Please make sure your line is muted**
- For technical problems, please email Michelle Horowitz Jackson at michelle@njgca.org
- Enter questions in the question box in your dashboard, **you can do this at any point throughout the webinar**
- If your question is not answered today, please email it to michelle@njgca.org

Overview

- Who is the NJCCIC
- Attack Vectors
- Most Prevalent Threats
- Industry-Specific Threats
- Colonial Pipeline Cyber attack review
- Common Shortfalls
- Mitigation Strategies and Resources



The NJCCIC

The State's clearinghouse for information sharing, threat analysis, best practices, and incident reporting.

Information
Technology (OIT)

Federal Partners

NJSP

Homeland Security

Objectives

Promote statewide awareness of the threat landscape

Facilitate the adoption of best practices

Develop public and private sector partnerships with the goal of making NJ more resilient to cyber attacks



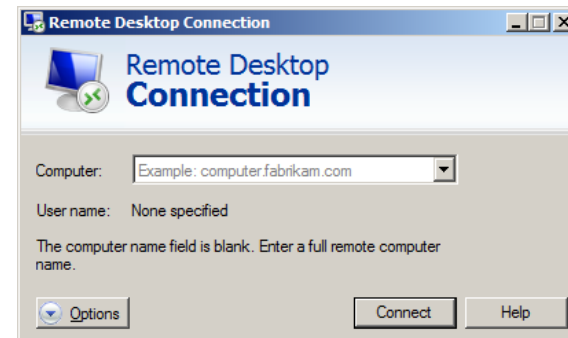
Threat Environment

- Growing dependence on technology and devices/systems results in increased attack surface/grid
- Bar to carry out crippling attacks is low
- Public pressure to pay the ransom – secondary extortion
- Limited funding/budgets
- Legacy systems
- May not have dedicated security teams to help defend their systems



Common Attack Vectors

- Malicious file attachments and links in phishing emails
- Software vulnerabilities
- Remote Access Exploitation (RDP Compromise)



Vulnerabilities



MALWAREBYTES NEWS

Patch now! NSA, CISA, and FBI warn of Russian intelligence exploiting 5 vulnerabilities

Posted: April 16, 2021 by Malwarebytes Labs

The National Security Agency (NSA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) have jointly released a Cybersecurity Advisory called [Russian SVR Targets U.S. and Allied Networks](#), to expose ongoing Russian Foreign Intelligence Service (SVR) exploitation of five publicly known vulnerabilities. The advisories' executive summary reads:

The advisory lists the following CVEs:

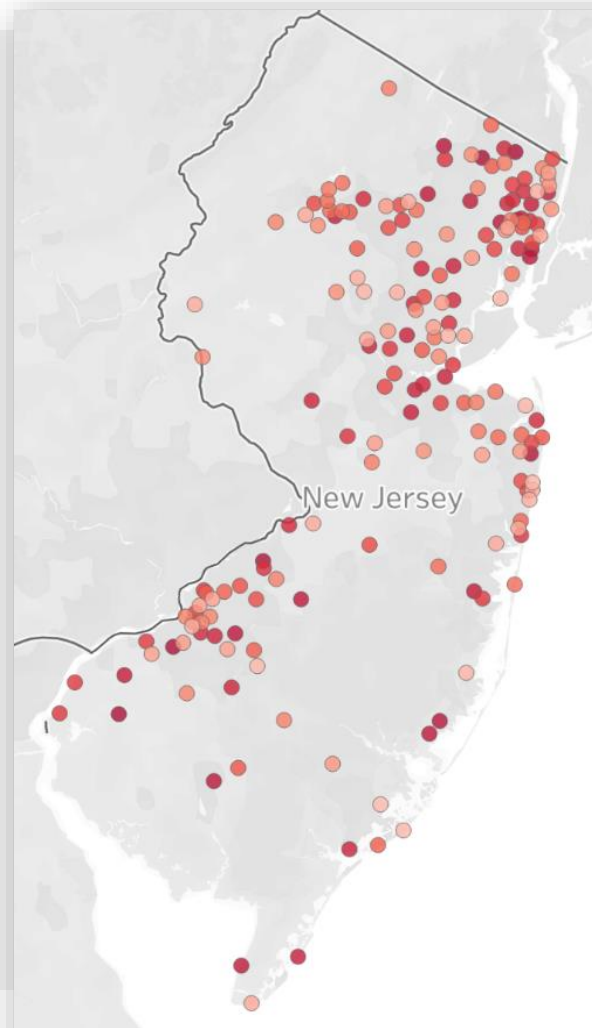
- [CVE-2018-13379](#) as discussed here: [Fortinet FortiGate VPN](#)
- [CVE-2019-9670](#) as discussed here: [Synacor Zimbra Collaboration Suite](#)
- [CVE-2019-11510](#) as discussed here: [Pulse Secure Pulse Connect Secure VPN](#)
- [CVE-2019-19781](#) as discussed here: [Citrix Application Delivery Controller and Gateway](#)
- [CVE-2020-4006](#) as discussed here: [VMware Workspace ONE Access](#)

Image Source: Malwarebytes Blog



Remote Access

- Approximately 31,130 systems in NJ with RDP (port 3389) open to the internet.
- Up from about 25,000 pre-pandemic.



Most Prevalent Threats

Phishing/Vishing

Business Email Compromise (BEC)

POS Malware

Ransomware/Data Theft/Breach



Phishing

#1 delivery vehicle for ransomware

32% of phishing emails are opened

50% of attacks target financial information

Upwards of 74% of attacks target credentials



Vishing

Tech Support Scams

IRS Phone Scams

Utility Phone Scams

Wire Transfer Scams



Exploiting Public Interest

- COVID-19 Phishing
- Fraudulent Websites
- VTC Targeting
- Stimulus Phishing
- Vaccine Phishing
- Fraudulent Job postings
- Fraudulent Charities or requests for PPE
- Social Unrest
- Political




Urgency/Authority

[EXTERNAL] Training Reminder: Due Date



To

 If there are problems with how this message is displayed, click here to view it in a web browser.

Good morning

Your Security Awareness Training **will expire within the next 24hrs.** You only have 1 day to complete the following assignment:

- **2020 KnowBe4 Security Awareness Training**

Please note this training is not available on the employee training Portal. You need to use the link below to complete the training:
<https://training.knowb.e4.com/auth/saml/4d851fef35c0f>

This training link is also available on [Security Awareness Training](#).

Use the URL: training.knowbe.4.com/login if you like to access the training outside of the network. Please use your email on the initial KnowBe4 login screen. Once the browser directs you to authentication page, please enter your username, password, and click the "Sign in" button to access the training.

Your training record will be available within 30 days after the campaign is concluded.

Thank you for helping to keep our organization safe from cybercrime.

Information Security Office



Threat Actors Capitalize on Unemployment Fears

DocuSign eSignature

DocuSign E-cloud FAQ

These steps are required to open the document, which is stored by DocuSign encrypted Cloud

Click on "Enable Editing" to unlock the editing document downloaded from the Cloud.



Click on "Enable Content" to perform Microsoft decryption tool to start the decryption of the document.



If you are having any issues please contact our support.

Email: elliott.sharpe@michaelpage.co.uk

Telephone: +442072692138

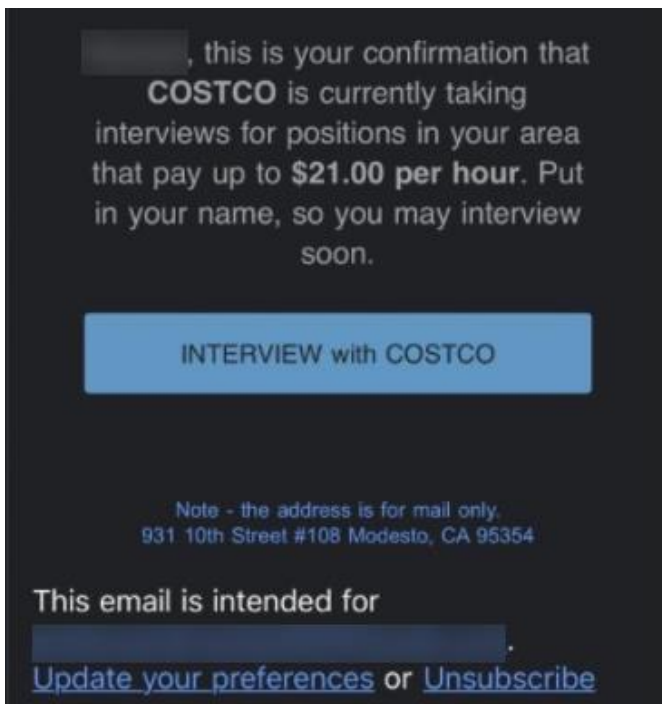
Senior Consultant - Sales at Michael Page



Elliot Sharpe
Talent acquisition Team
Michael Page International

Sec-cloud ID: JN-022021-2172866

Michael Page



Threat Actors Capitalize on Unemployment Fears

[EXTERNAL] Re: NJLWD Division of Unemployment Insurance benefit payment for week ...



barrington702@comcast.net

To [redacted]@dol.nj.gov

Reply

Reply All

Forward



Wed 6/24/2020 2:21 AM

I have made some edits. Please check.

<https://send.firefox.com/download/867c0325a94a42fa/#vLIAFQvJefyXZmh2NHIKqg>

Password for archive: 7777

This e-mail confirms that your claim for weekly Unemployment Insurance benefits, Confirmation# [redacted], has been received.

>

>Your claim is not payable at this time.

>

> If you have a pending appointment or if you have appealed a disqualification and are awaiting a determination, you have been given pended credit for week-ending 11/03/18. If a determination or an appeal decision is in your favor and no other disqualification(s) exist, you will be paid for the week claimed.

>

> If you do not know why your claim is not payable, please call your nearest Reemployment Call Center.

>

>For detailed information about unemployment insurance, please visit our website at:

>http://wd.dol.state.nj.us/labor/ui/ui_index.html

>

>

>***** Please do not reply to this message. *****

>

>***** Replies are automatically deleted. *****

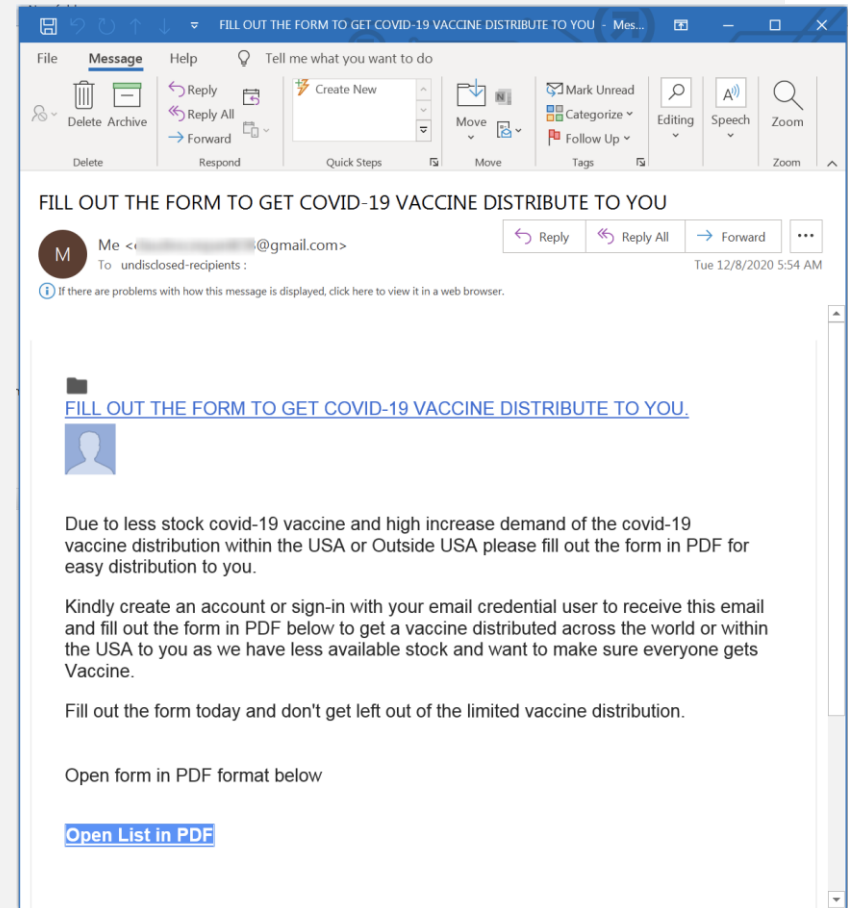
>



New Tactics

Prevalent phishing scams

- COVID vaccine phishing and fake landing pages
- Other current phishing scams:
 - Unemployment Insurance (UI) scams
 - Vishing – (voice phishing)
 - Often target land-lines
 - Claim that they need assistance, request money/gift cards



Business E-mail Compromise

Bogus Invoice Scheme

Wire Fraud

CEO Fraud

Account Compromise

Attorney Impersonation

Data Theft



Reporting

Internet Crime Complaints Soared in 2020

467,361

2019

791,790

2020

**Reports to IC3
up 69.4%**



FBI FEDERAL BUREAU OF INVESTIGATION

Source: 2020 Internet Crime Report, ic3.gov



The information contained in this product is marked Traffic Light Protocol (TLP): WHITE. Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction. This presentation was prepared by the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) pursuant to its authority under Executive Order No. 178 of 20 May 2015.

Invoice Scams



[BEC Scammers Struck Philadelphia Non-Profit Food Bank](#)

Comment: Threat actors took advantage of non-profit food bank, Philabundance, by impersonating contractors that were building the Community Kitchen. The food bank, vital to the local community, fulfilled the fake invoice totaling a loss of \$923,533. Business Email Compromise (BEC) scams are highly-targeted social engineering attacks, unlike generic phishing campaigns. To make messages appear more legitimate, attackers commonly spoof the sender name to display the name of a familiar contact or business associate. Typically, the body of these messages instructs the recipient to transfer funds, fulfill a bogus invoice, buy gift cards, or provide other sensitive information. Users are reminded to be aware of these [red flags](#) and to contact the sender via an alternate means of communication prior to fulfilling any requests.



Gift Card Scams

New Gift Card Scam Claims Funds are for Essential Workers

NJCCIC Alert

Original Release Date: 5/8/2020

Summary

The NJCCIC is aware of a new phishing campaign in which threat actors are impersonating known individuals, likely using display name and/or email address spoofing, and requesting recipients to purchase gift cards for essential workers. The sender asks for the codes on the back of the gift cards after purchase in order to distribute the funds. In an email shared with the NJCCIC, the sender impersonated the town's mayor with a subject line of "FOR OUR ESTEEMED STAFFS:" and requested seven \$100 gift cards. While recipients may ordinarily be suspicious of an email containing grammatical errors and requesting the purchase of gift cards, referencing the recipient by name and claiming the request is for essential workers during the COVID-19 pandemic may make these emails appear more genuine.

Recommendations

The NJCCIC reminds users to never purchase gift cards and send the codes to someone without verifying the request first via a separate means of communication. This is an unusual request and should be handled with increased suspicion.



Point of Sale Malware



Point-of-Sale Malware



Point-Of-Sale Malware

For a list of known POS malware variants, click [here](#).

[Learn More About PoS Malware+](#)

What is POS Malware?

PoS malware is malicious software designed to steal credit and debit card data from payment processing systems, known as point-of-sale (PoS) terminals.

What Data Does POS Malware Steal?

PoS malware targets consumers' personal and financial data stored on one of up to three 'tracks' on the magnetic strip located on the back of a payment card. The majority of payment cards in the U.S. contain two tracks of data used by financial institutions to store a customer's information; some cards contain a third track.

<https://www.cyber.nj.gov/threat-center/threat-profiles#other-malware>



Vulnerabilities



Vulnerabilities Found in PoS Devices – Patches Available

NJCCIC Advisory

Original Release Date: 12/17/2020

Summary

Researchers disclosed vulnerabilities affecting widely used point-of-sale (PoS) terminals manufactured by Verifone and Ingenico.

How does the threat actor get in?

- Vendor vulnerabilities and equipment updates
- Bad management of third-parties
- Bad security hygiene
- Unprotected WI-FI network
- No/weak data encryption



Threats and Consequences



Visa Security Alert

SEPTEMBER 2020

NEW MALWARE SAMPLES IDENTIFIED IN POINT-OF-SALE COMPROMISES

Distribution: Public

Summary:

In May and June 2020, respectively, Visa Payment Fraud Disruption (PFD) analyzed malware samples recovered from the independent compromises of two North American merchants. In these incidents, criminals targeted the merchants' point-of-sale (POS) terminals in an effort to harvest and exfiltrate payment card data. Subsequent to analysis, the first attack was attributed to the malware variant [TinyPOS](#), and the second to a mix of POS malware families including [RtPOS](#), [MMon \(aka Kaptoxa\)](#), and [PwnPOS](#). The recent attacks exemplify threat actors' continued interest in targeting merchant POS systems to harvest card present payment account data. PFD is providing the analysis of these malware variants and the corresponding indicators of compromise (IOCs) to assist in the identification, prevention, and mitigation of attacks using the malware.



Threats and Consequences



NJCCIC

Breached Wawa Customer Data Available on Dark Web

NJCCIC Alert

Original Release Date: 2020-02-03

Last month, Wawa disclosed a payment breach that affected more than 850 locations, impacting over 1.5 million purchases between March 4, 2019 and December 2019. The breach was caused by malware infecting Wawa's payment processing system. Threat intelligence firm Gemini Advisory Group identified a data dump, promoted as BIGBADABOOM-III, on the underground marketplace "Joker's Stash." The dump contained

POS Malware at Gas Stations Across North America

NJCCIC Alert

Original Release Date: 2019-12-23

In security alerts published in November and December 2019, VISA detailed incidents of POS malware at gas pump and gas station operators across North America. Cyber-criminals are installing POS malware on fuel



Mitigations



Office Devices That Are Vulnerable To Cyberattacks And How To Protect Them

May 4, 2021

Are you protecting POS system security?



Point-Of-Sale System Security (POS)

April 30, 2021

[Learn More](#)



How do you clean your POS Devices?

IMPLEMENT BEST PRACTICES TO IMPROVE THE LONGEVITY OF YOUR INVENTORY.

Options For Disinfecting Your Point-Of-Sale (POS) Devices

April 13, 2021

Source: [BLM Technologies](#)

Do your research! Educate yourself on current threats, vulnerabilities, available updates, and appropriate mitigations.



Ransomware

Malicious software that extorts money from victims by restricting access to files, systems, or devices.

- Impacts desktops, laptops, mobile devices
- Paying does NOT guarantee file restoration



Ransomware

Average ransom amount paid in Q3 2020 was over \$233,000, up from \$110,500 in Q1.

Top attack vectors are RDP compromise (57%) and phishing (26%)

Ransomware damages estimated at \$8.9 billion in 2019.

Ransomware incidents last about 16 days, up from 7 days in Q1.

Top industries targeted: Professional Services, Healthcare, Govt, and Edu.

Avg ransom for top 3:
Sodinokibi ~\$300k
Ryuk +\$1M million
Netwalker Thou-Mil

Evolving Tactics - Low Barrier to Entry

Source: Coveware



PII, PHI, IP, Financial Data

Attackers hack into networks, siphon data through back doors, or install malware designed to capture information

If valuable data is insecure & accessible, it is a matter of when, not if, it is located and exploited.



Data breaches

Data Breaches in 2019 – 2021 – An Alarming Timeline

- 533 Million Users – Facebook, April 03, 2021. ...
- 5 Billion – Keepnet Labs, June 9, 2020. ...
- 47.5 Million – Truecaller, May 27, 2020. ...
- 26.3 Million – LiveJournal, May 27, 2020. ...
- 8.3 Billion – AIS, May 25, 2020. ...
- 25 Million – Mathway, May 25, 2020. ...
- 2.3 Million – Indonesia, May 22, 2020. ...
- 9 Million – EasyJet – May 19, 2020.

This list is not all inclusive – these are just *some* of the most publicized breaches

***Haveibeenpwned.com* →**



';--have i been pwned?

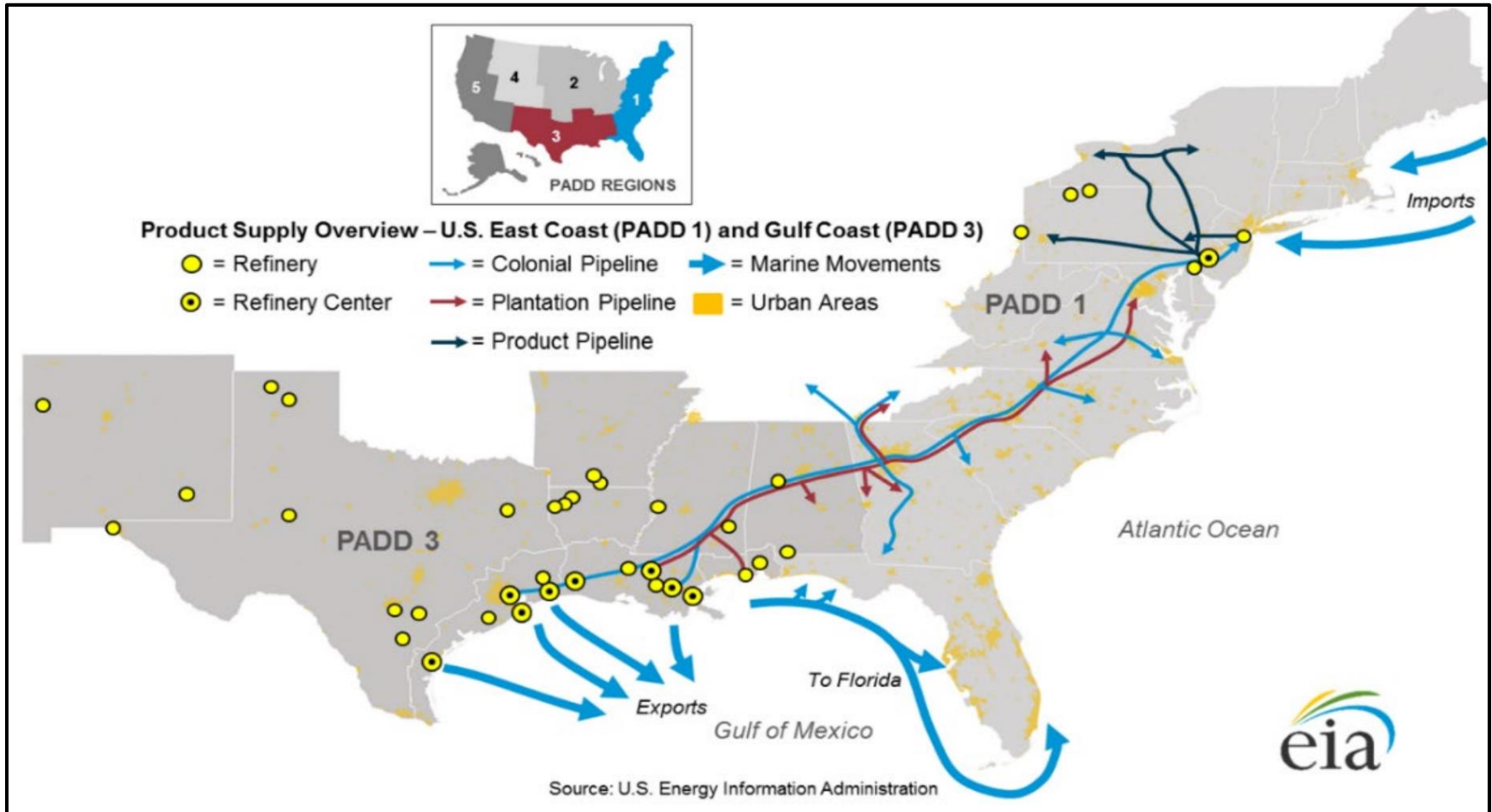
Check if your email or phone is in a data breach

pwned?

Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)



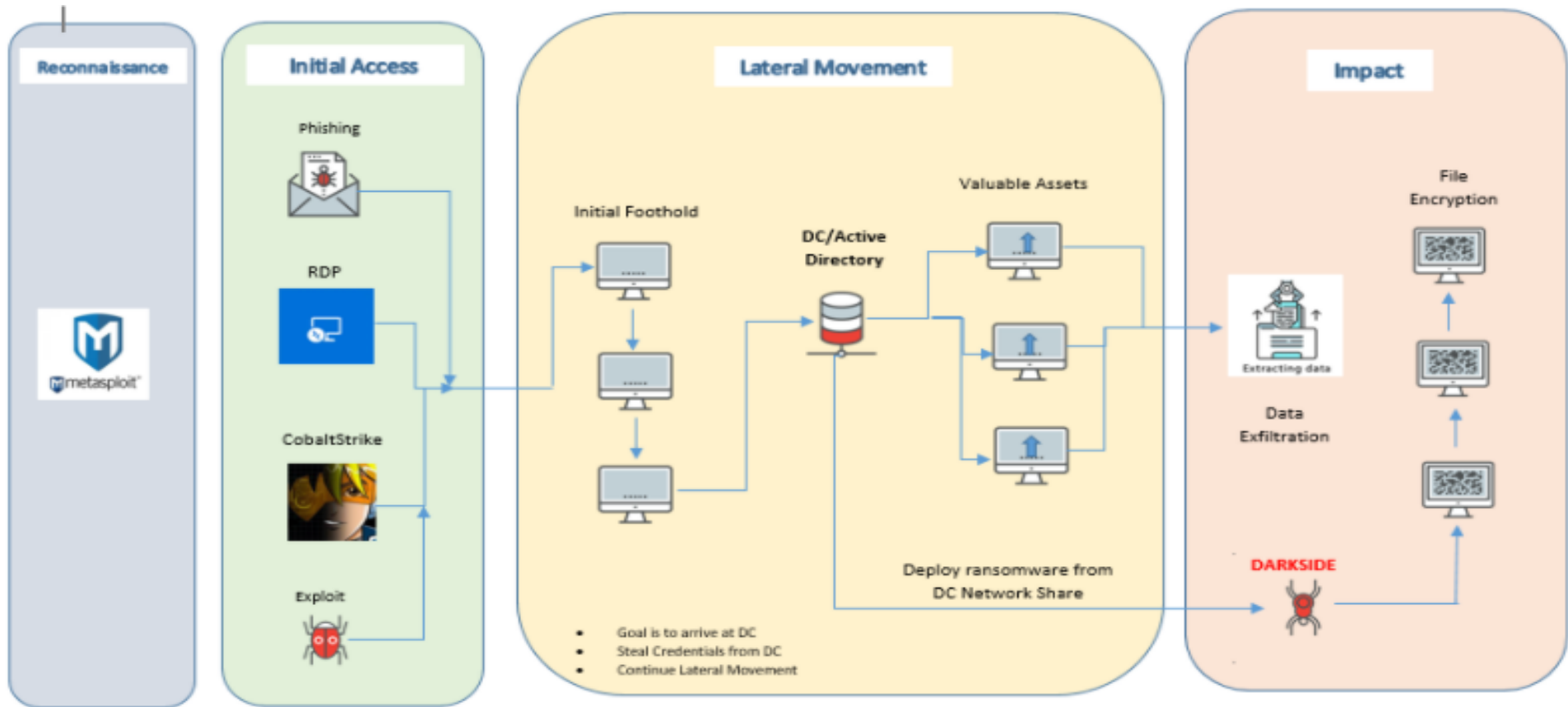
Colonial Pipeline Cyber Attack



Fallout



DarkSide



DarkSide Infection Process *Image Source: Trend Micro*



Top 3 Ransomware Threats

Dharma/Phobos

RDP; Particularly aggressive ransomware, as it continues to encrypt files after the initial ransom note appears and can be run repeatedly, with or without internet.

Ryuk – 2018-Present

Used by profit-motivated criminals. Often accompanies Emotet or Trickbot trojans. Ransoms are very high and target large corporations.

Sodinokibi/REvil– 2019-Present

Often targets managed service providers (MSPs) and IT service providers and infect their clients via RDP.



Your computer have been infected!



Your documents, photos, databases and other important files **encrypted**



To decrypt your files you need to buy our special software - *2r6s1t3-Decryptor*



You can do it right now. **Follow the instructions below.** But remember that you do not have much time

2r6s1t3-Decryptor costs

You have **2 days, 23:59:30**

* If you do not pay on time, the price will be doubled

* Time ends on **May 1, 19:48:07**

Current price

0.47217028 btc
≈ 2,500 USD

After time ends

0.94434056 btc
≈ 5,000 USD



Ransomware as a Service

Satan

Login

Register

What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

How to make money with Satan?

First of all, you'll need to **sign up**. Once you've sign up, you'll have to log in to your account, create a new virus and download it. Once you've downloaded your newly created virus, you're ready to start infecting people.

Now, the most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will keep a 30% fee of the income, so, if you specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the number of infections and payments you have.



Fancy Lazarus Returns in Another Ransom DDOS Campaign

NJCCIC Alert

Original Release Date: 6/17/2021

Summary

Threat actors, who previously claimed to be notorious threat groups APT28 and the Armada Collective, have been observed in a new campaign threatening organizations with DDOS attacks. Recently taking the moniker, "Fancy Lazarus," the threat group sends targeted emails to various sectors, including energy, financial, insurance, manufacturing, public utilities, and retail. Fancy Lazarus appears to be attempting to capitalize on recent high-profile ransomware attacks. The extortion attempt begins with a threatening email warning of a future DDOS attack against their organization if a ransom is not paid. Ransom demands begin with two bitcoin (about \$75,000), doubling if demands are not met by the deadline and increasing daily if not paid. According to Proofpoint researchers, the extortion emails are tailored to the intended target organization and are often sent to email aliases such as help desk, administrative, or customer service. While some threats were easily mitigated, organizations have indicated that operations were impacted.



Extortion Scams

From: Elizabeth Arduino <isirwinvri@outlook.com>
Sent on: Thursday, April 9, 2020 3:55:11 PM
To: [REDACTED]@mkzd.state.nj.us
Subject: [EXTERNAL] [REDACTED]: [REDACTED]

From Outlook.com email addresses
Subject line is *username : password*

Your password is [REDACTED] I know a lot more things about you than that.

How?

I placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger, which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account.

What exactly did I do?

I made a split-screen video.

The first part recorded the video you were viewing (you've got an exceptional taste haha), and the next part recorded your webcam (Yep! t's you \doing nasty things!).

What should you do?

Well, I believe, \$2000 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy bitcoin" in Google).

Bitcoin Address:

bc1q6nv2ly80v0q9mtl0aevagn4auw6l4f3zemdahv
(It is cAsE sensitive, so copy and paste it)

Important:

You have 24 hours to make the payment. (I have a unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts, including relatives, coworkers, and so forth. Nonetheless, if I do get paid, I will erase the video immediately. If you want evidence, reply with "Yes!" and I will send your video recording to your five friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Elizabeth Arduino





Achieving Digital Resilience



Who's Responsible?

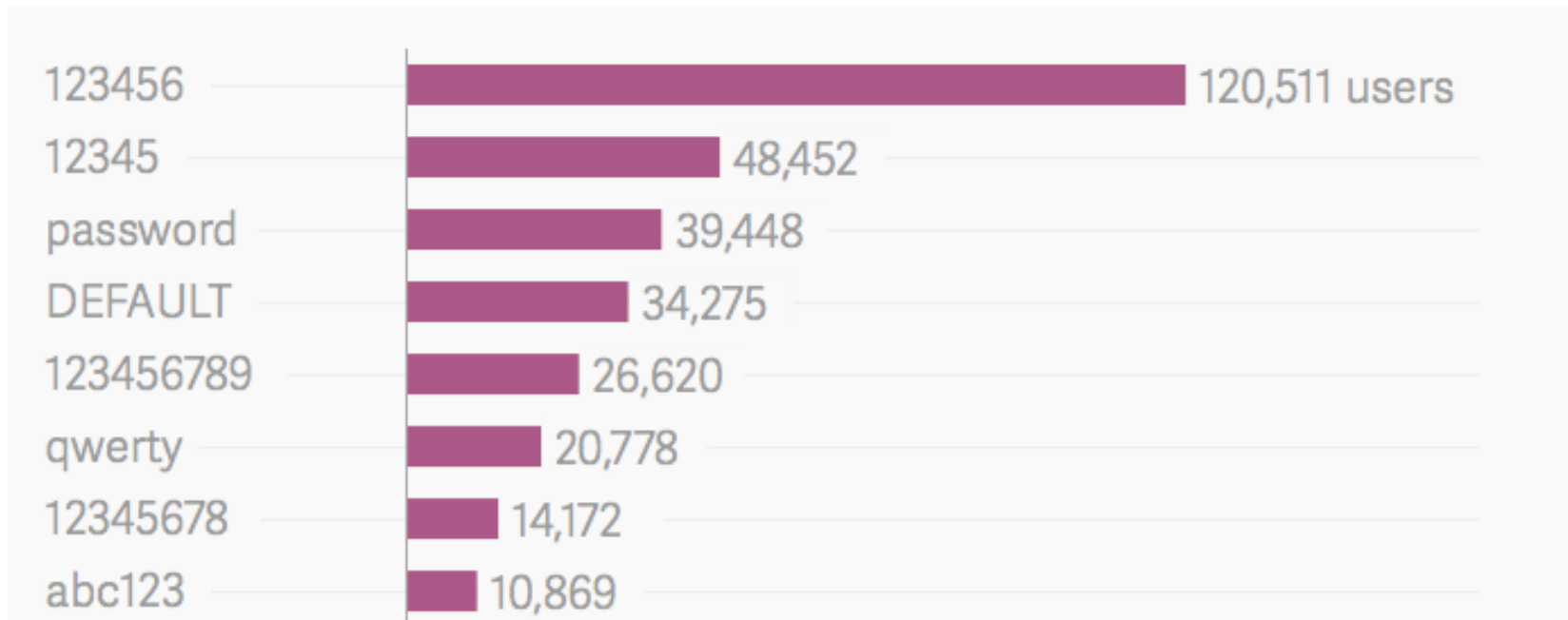
Cybersecurity is everyone's responsibility

- Board of directors
- C-Suite
- Management
- Full-time
- Part-time/temp
- Contractors/Third-parties
- Interns
- Anyone w/network access



Passwords

Most common passwords from a highly-publicized data breach



Credentials are the “keys to the kingdom”



So, What Do We Do?

Change default credentials

Enable MFA

Keep hardware/software updated – verify 3rd party vendors and equipment

Think before you click links/open attachments

Verify requests for sensitive information or transfer of money

Navigate to sites directly, not via links

Segment networks (IT from OT)

Create strong passwords and don't reuse them

Encrypt important data when sending electronically

HAVE A RESPONSE PLAN – PRACTICE!

Educate! Ensure all employees know how to respond!



Multi-Factor Authentication (MFA)

Best method to protect against account compromise as a result of credential theft

Choose authentication apps or hardware tokens over SMS or email codes

Multi factor authentication



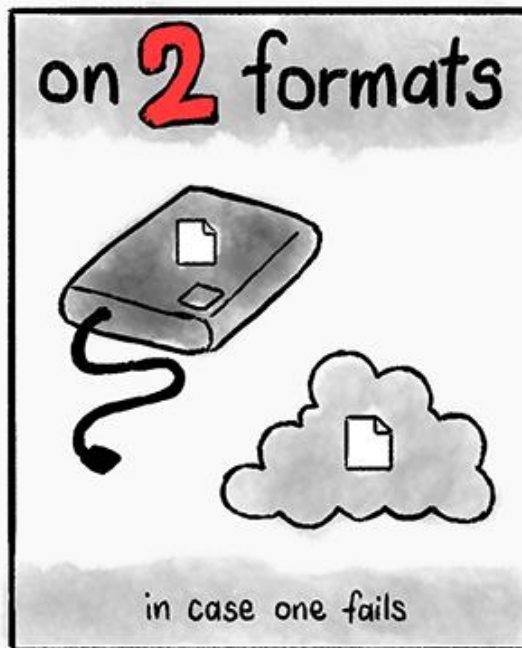
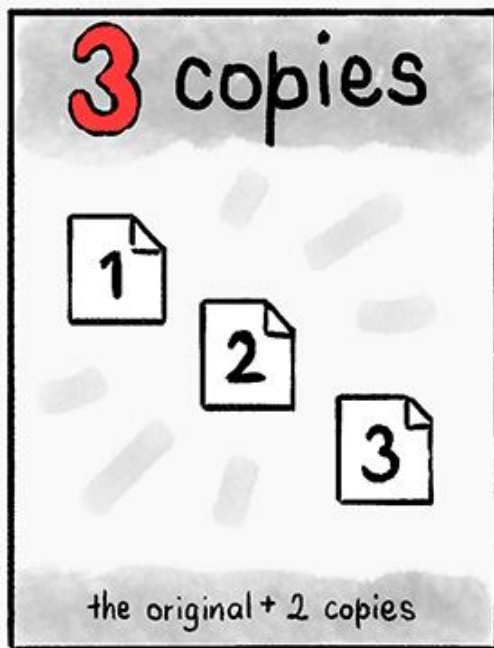
**Something
you have**

**Something
you are**

**Something
you know**



Backup, Backup, Backup



Who Do I Report Incidents To?

- Follow your Incident Response Policy/Plan
 - IT department
 - 3rd Party Vendor/Supplier
 - Depending on severity, may also contact NJCCIC, Local PD, and FBI for assistance
- **Report money losses to FBI/LE within 48 hours*
- Greater chance of recovering funds*



Reporting Incidents to NJCCIC

NJCCIC Cybersecurity Incident Reporting System

The NJCCIC Incident Reporting System provides a secure web-enabled means of reporting cyber security incidents to the NJCCIC. The information you submit allows us to provide timely handling of your security incident as well as the ability to conduct improved analysis.

If you would like to report a cybersecurity incident, please complete the following form providing as much detail as possible. Incomplete information may limit the NJCCIC's ability to process or act on your report.

Impacted Individual/Organization Information

First Name *	Last Name *
<input type="text"/>	<input type="text"/>
Phone Number *	Extension
<input type="text"/>	<input type="text"/>
Email *	Confirm Email *
<input type="text"/>	<input type="text"/>
County *	Zip Code *
<input type="text" value="--None--"/>	<input type="text"/>
Organization Reporting *	
<input type="text" value="--None--"/>	

cyber.nj.gov/report



Useful Resources

- **Government Organizations**

- [NIST](#)
- [MS-ISAC](#) - must be a member to get alerts
- [Local Fusion centers \(NJCCIC/ROIC\)](#)
 - [SISM \(NJ Statewide Information Security Manual\)](#)
- [DHS/CISA](#) (Cybersecurity and Infrastructure Security Agency)
- [FINCEN.gov](#)

- **Vendor/Supplier notifications and alerts**

- [Verifone](#)
- [Ingenico](#), etc.

- **Technical cybersecurity sources**

- [ZDNet](#)
- [Bleeping Computer](#)
- [VMWare](#)
- [PlexTrac](#), etc.



Additional NJCCIC Resources

- [Tips for Teleworkers, Remote Access Security](#)
- [Don't Be Fooled: Ways to Prevent BEC Victimization](#)
- [Impersonation Scams](#)
- [Protecting Against Tech Support Scams](#)
- [Ransomware: The Current Threat Landscape](#)
- [Instructional Guides](#)
- [Mitigation Guides](#)
- [How Big is Your Footprint?](#)
- [Compromised PII: Facilitating Malicious Targeting and Fraudulent Activity](#)



Weekly Bulletin

Presentations and Training

Threat analysis

Threat profiles

Be Sure to Secure

Cyber Risk Self-Assessment

Incident Reporting/Response



Questions?

Any Questions?



Connect With Us



Theresaa Barker-Figueroa

Main: 1-833-4-NJCCIC, 1-833-465-2242

24/7 Incident Hotline: 1-866-4-SAFE-NJ

Website: www.cyber.NJ.gov

Email: njccic@cyber.nj.gov

FOLLOW ON SOCIAL MEDIA:

@NJCYBERSECURITY



Michelle Horowitz Jackson

732-256-9646

Website: www.njgca.org

Email: michelle@njgca.org

