



# NJCCIC

*PROTECT, DEFEND,  
RESPOND*



[cyber.nj.gov](http://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.

# Ransomware

## Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity

### Irish health system struggling to recover from cyberattack

By SYLVIA HUI, DANICA KIRKA and FRANK BAJAK May 18, 2021

Stevens Tech struggling to rebound from cyberattack in time for start of school year

Updated Aug 19, 2019; Posted Aug 19, 2019

### Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business

World's largest cruise line operator discloses ransomware attack

Cruise Corp says it suffered a ransomware attack on Saturday, August 15, and that hackers

### THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

### Livingston Public Schools Hacked With Ransomware, Classes Delayed



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.

# Ransomware-as-a-Service



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.

# Ransomware – Q1 2021

Average ransom amount paid in Q1 2021 was between \$220,298 + from Q4

Average downtime is 23 days

Top attack vectors:  
Phishing  
RDP Compromise  
*Software vuln +*

Ransomware costs in 2020 estimated at \$20 billion

77% of cases include data exfiltration

Top Targets:  
Healthcare and professional services

\*According to Coveware and Purplesec



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.

# Ransomware – Q2 2021 - Evolution

Average ransom amount down 38% to \$136,576

Average downtime is 23 days

Top attack vectors:  
Phishing  
RDP Compromise  
Software vuln

Ransomware focus by heads of state, LE, CEOs, & Insurance Co

81% of cases include data exfiltration

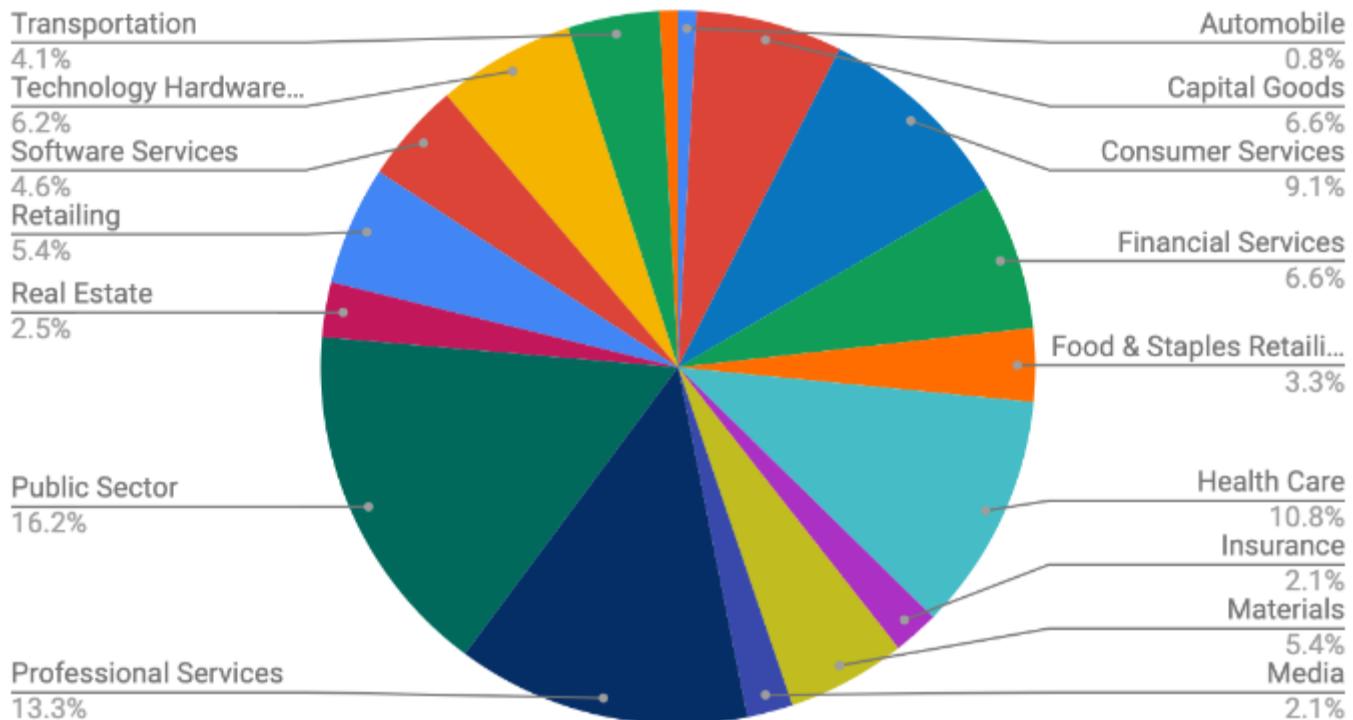
Top Targets:  
Public Sector and Professional Services



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.

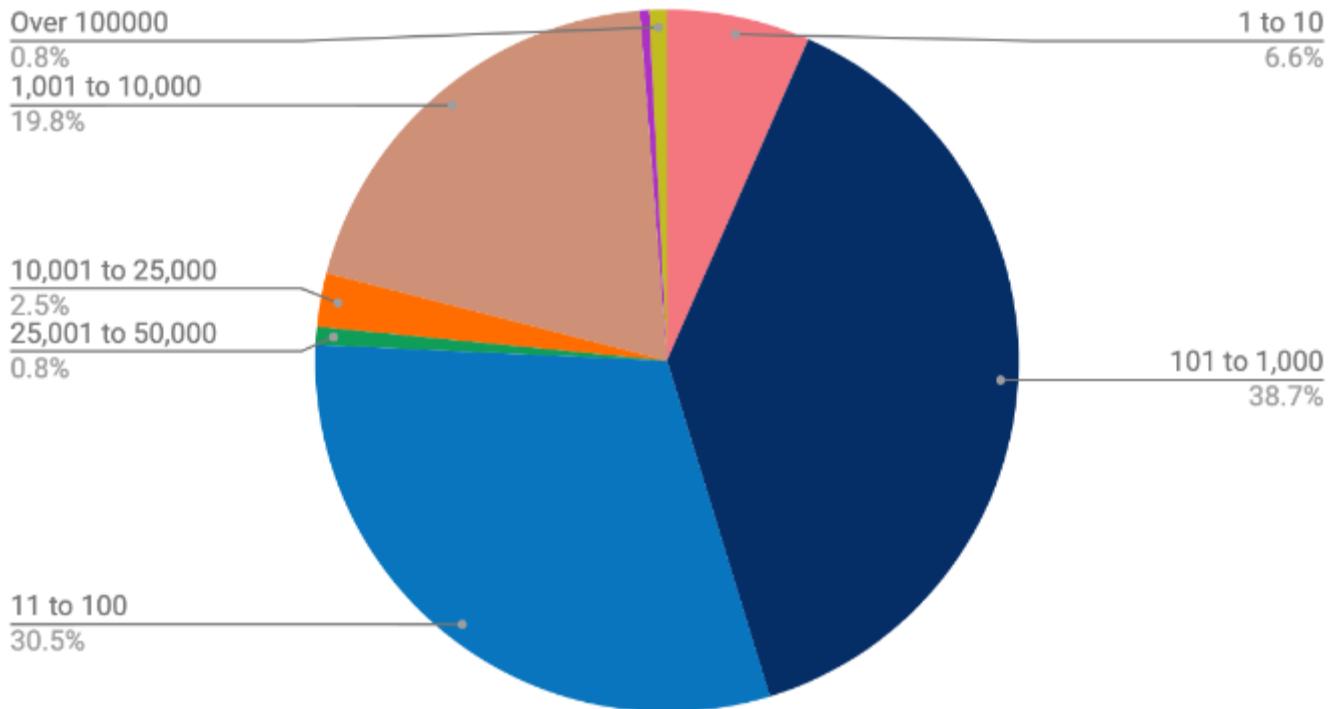
# Ransomware targets

## Common Industries Targeted by Ransomware Q2 2021



# Ransomware Targets

Distribution by Company Size (Employee Count)



# Credential Compromise



ryryry ryryry  
huskielauren sunshine 6kk7do6s  
iloveyou School karen1234 yankees  
aaron431 maggie 59mile  
linkedin 1234 penguin password1  
trenton andrewmoose2156 summer  
reset family 59trick viking  
pepperprincess mystic  
19weed monkey PBKDF1  
monkey pass1 paterson  
simpsons laronda snickers  
fling

splat ginger soccer  
thomas matthew samantha abc123 football  
kitten 20100728  
newpass hello eagles teacher  
michael1 michael r1A93c5x  
123456 thehatch tigger  
SPARKY 30media 66bob  
nicolejordan

Why are credentials the keys to the kingdom?



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.

# HaveIBeenPwned.com



The page shows a search bar with the text '@yahoo.com' and a 'pwned?' button. Below the search bar, the text 'Oh no — pwned!' is displayed, followed by 'Pwned on 9 breached sites and found no pastes (subscribe to search sensitive breaches)'. A '3 Steps to better security' section is shown with three icons: a person using a magnifying glass on a password, a person at a computer, and a person at a computer with a lock icon. Below these are the steps: 'Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.', 'Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.', and 'Step 3 Subscribe to receive notifications for other breaches. Then use a unique password.' A 'Why 1Password?' link is also present. A 'Start using 1Password.com' button is located at the top right of the main content area. The main content area has a dark red background.

**LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords

**Houzz:** In mid-2018, the housing design website Houzz suffered a data breach. The company learned of the incident later that year then disclosed it to impacted members in February 2019. Almost 49 million unique email addresses were in the breach alongside names, IP addresses, geographic locations and either salted hashes of passwords or links to social media profiles used to authenticate to the service. The data was provided to HIBP by dehashed.com.

**Compromised data:** Email addresses, Geographic locations, IP addresses, Names, Passwords, Social media profiles, Usernames

**Lumin PDF:** In April 2019, the PDF management service Lumin PDF suffered a data breach. The breach wasn't publicly disclosed until September when 15.5M records of user data appeared for download on a popular hacking forum. The data had been left publicly exposed in a MongoDB instance after which Lumin PDF was allegedly been "contacted multiple times, but ignored all the queries". The exposed data included names, email addresses, genders, spoken language and either a bcrypt password hash or Google auth token. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

**Compromised data:** Auth tokens, Email addresses, Genders, Names, Passwords, Spoken languages, Usernames

**MyFitnessPal:** In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.im".

**Compromised data:** Email addresses, IP addresses, Passwords, Usernames



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.

# Credential Compromise

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**

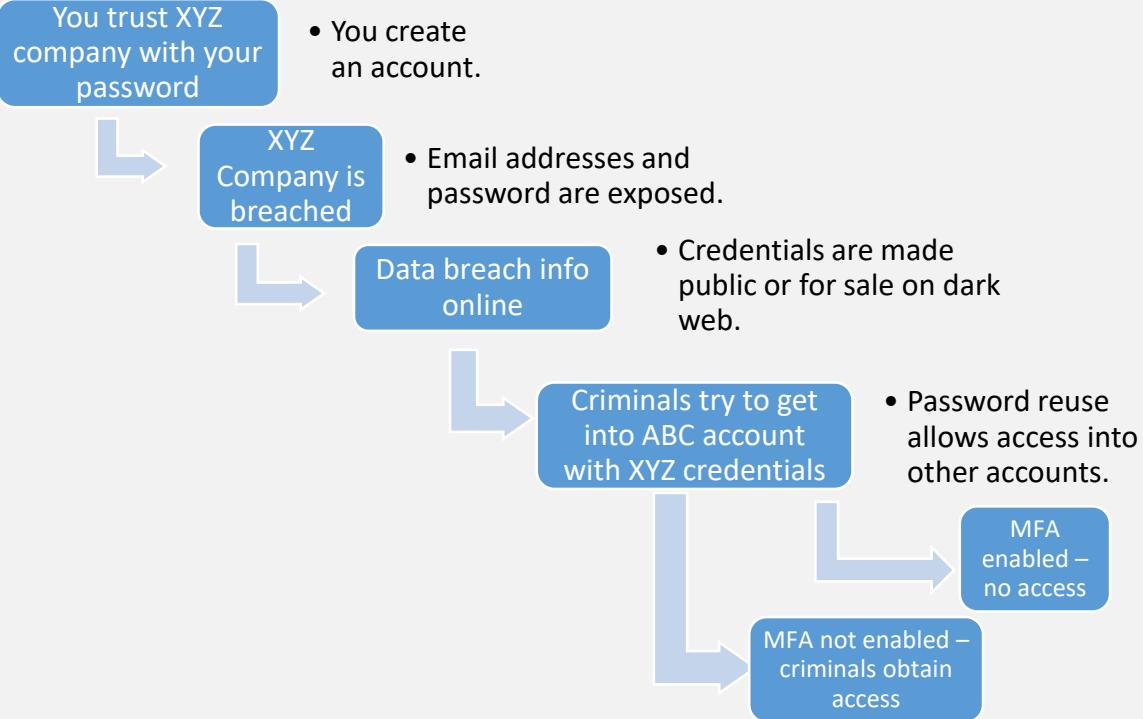
**Something  
you are**

**Something  
you know**



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.

# Why Multi-Factor Authentication Matters



# Increase resiliency



## Data Backups

- Keep backups OFF the network
- Store in separate and secure location
  - Test backups regularly
  - Keep multiple copies

## Encrypt Data

- Encrypt sensitive data at rest and in transit
- Exfiltration of data prior to ransomware is increasingly common

## Business Continuity

- Establish COOPs and Incident Response
  - Test these plans
  - Modify plans



# What Can We Do?

Separate IT and OT networks

Enable MFA for ALL users

Keep hardware/software updated

Employ security technologies and manage them

Close unnecessary connections (ports)

Educate!



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.

## Ransomware



### Ransomware

To view a complete list of all known ransomware variants, click [here](#).

[Learn More About How Ransomware Works +](#)

#### What is Ransomware?

Ransomware is a type of malicious software (malware) that attempts to extort money from victims by restricting access to a computer system or files. The most prevalent form of this profit-motivated malware is crypto-ransomware, which encrypts files into encoded messages that can only be decrypted (decoded) with a key held by the malicious actor.

#### How Does Ransomware Work?

- Ransomware infections occur when a user opens a malicious email attachment, clicks on a malicious link, or visits a website infected with malicious code, known as a drive-by download.
- Once a system is infected, the ransomware contacts a command and control (C2) server to generate an encryption key and begins encrypting files on the victim's machine.
- The ransomware runs quietly in the background performing in-depth searches of all disk folders, including removable drives and network shares, and encrypts as many files as it can.
  - Ransomware may also delete Shadow Volume Copies, destroy restore points, and overwrite free disk space to prevent victims from recovering their files and systems without paying the ransom.
  - If a system is powered off as files are being encrypted, some ransomware variants resume where they left off when the system or device is powered on again.
- After files are encrypted, a ransom note is displayed on the screen with instructions on how and where to pay the ransom and the length of time before the hacker or software destroys the decryption key.
  - Some recent variants offer victims a 'second chance' to pay after the initial timer expires; however, the 'second chance' is often at least double the original ransom amount.
  - If the victim pays the ransom, the malware is supposed to contact the C2 server for the decryption key and begin decrypting the victim's files; however, in many cases, the files are never decrypted.
  - Some ransomware files can delete themselves in order to avoid detection and analysis by security researchers or law enforcement.

[READ FULL THREAT ANALYSIS REPORT HERE >](#)

#### Ransomware Mitigation Strategies

For many organizations, preventing ransomware entirely is nearly impossible, however, the impact of a successful infection can be greatly reduced if a robust data backup process is in place. Comprehensive data backups should be scheduled as often as possible and must be kept offline in a separate and secure location. The most effective method to prevent ransomware infections is to conduct regular training and awareness exercises with all employees to ensure users are proficient in safe Internet-browsing techniques and the ability to identify phishing emails. For specific recommendations for data protection, systems management, network management, mobile device management, and post-infection remediation click below:

[RECOMMENDATIONS >](#)



# Connect With Us



[NJCCIC@CYBER.NJ.GOV](mailto:NJCCIC@CYBER.NJ.GOV)



[1-833-4-NJCCIC](tel:1-833-4-NJCCIC)  
[\(1-833-465-2242\)](tel:1-833-465-2242)



[@NJCYBERSECURITY](https://twitter.com/NJCYBERSECURITY)



[CYBER.NJ.GOV](http://CYBER.NJ.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.