

Christmas and Cybercrime

Presented by:
Trevor Dierdorff



AMNET[®]
The IT Department for Your Business[™]

CFMA 11/18/2021

Why do hackers attack more during holidays?



In a joint advisory, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) said they "observed an increase in highly impactful ransomware attacks occurring on holidays and weekends — when offices are normally closed in the United States.

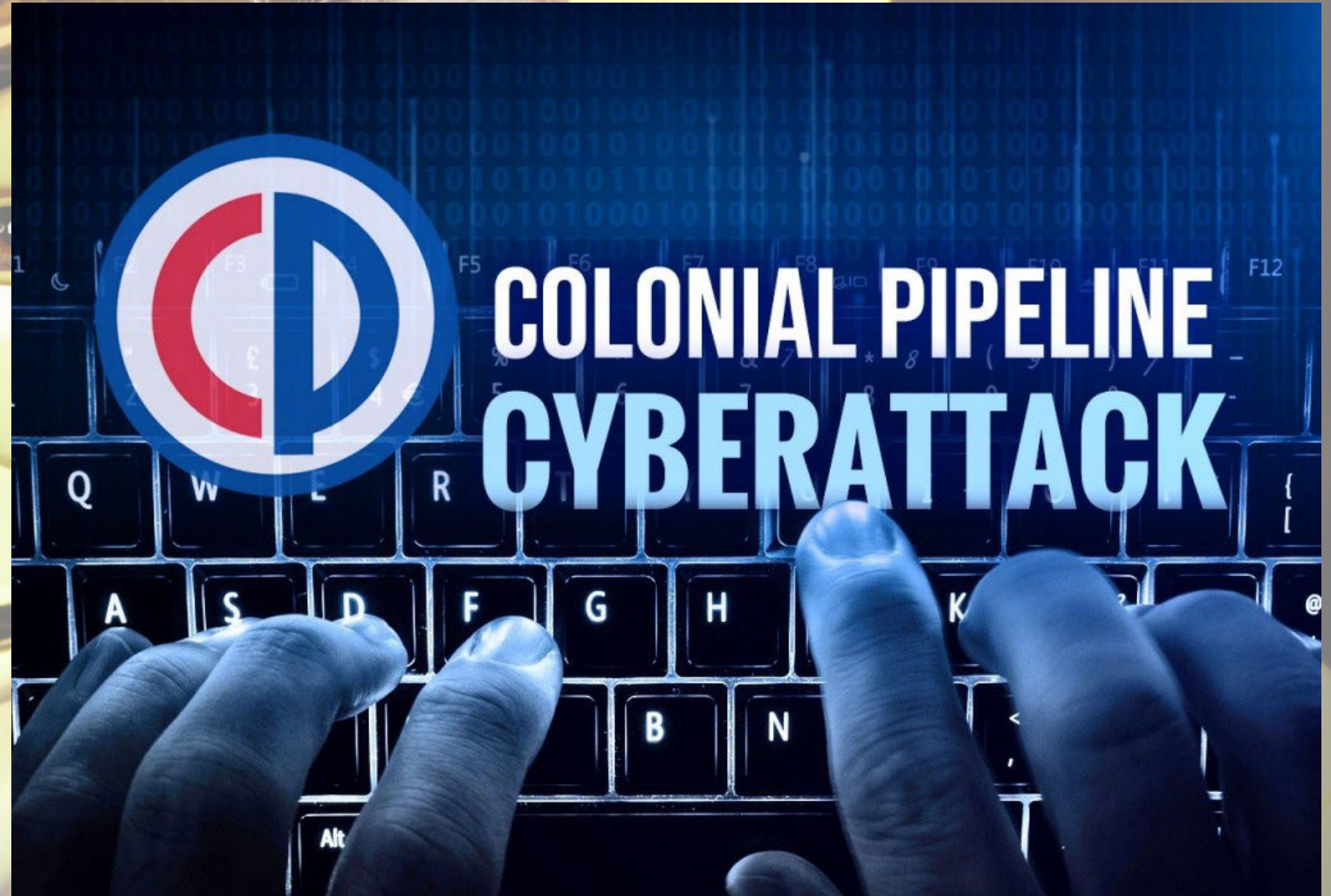
We have no specific threat information regarding attacks. But what we do have, is history.

Hackers love to hack when they know we're distracted and not ready to respond.

The "REvil" Cyber Gang Targeted Meat Processor JBS Over Memorial Day Weekend



Colonial Pipeline paid a \$4.4 million in ransom to the DarkSide group after being forced to shut down its operations during Mother's Day weekend






The “Total Global Impact of Cyber Crime [has risen to] \$3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined. ”

Europol Serious & Organized Threat Assessment

2013!

Cybercrime To Cost The World \$10.5 Trillion Annually By 2025

United States GDP is \$21.5 trillion



Ransomware payments reached over \$400 million in 2020 in the US, the FBI reported. 2021, the average ransom payment is up more than 500% over 2020, amounting to \$5.3 billion, according to Cybereason.

Top 50 Cyber Threats

- **Account Takeover**
- **Advanced Persistent Threat**
- **Application Access Token**
- **Bill Fraud**
- **Business Invoice Fraud**
- **Brute Force Attack**
- **Compromised Credentials**
- **Credential Dumping**
- **Credential Reuse Attack**
- **Credential Stuffing**
- **Cloud Access Management**
- **Cloud Cryptomining**
- **Command and Control**
- **Cross-Site Scripting**
- **Cryptojacking Attack**
- **Data From Information Repositories**
- **DoS Attack**
- **DDoS Attack**
- **Disabling Security Tools**
- **DNS Amplification**
- **DNS Hijacking**
- **DNS Tunneling**
- **Drive-by Download Attack**
- **Host Redirection**
- **Insider Threat**
- **IoT Threats**
- **IoMT Threats**
- **Macro Viruses**
- **Malicious Powershell**
- **Man-in-the-Middle Attack**
- **Masquerade Attack**
- **Meltdown and Spectre Attack**
- **Network Sniffing**
- **Pass the Hash**
- **Phishing**
- **Phishing Payloads**
- **Ransomware**
- **Shadow IT**
- **SIM jacking**
- **Social Engineering Attack**
- **SQL Injection**
- **Spear Phishing**
- **Spyware**
- **System Misconfiguration**
- **Typosquatting**
- **Watering Hole Attack**
- **Web Session Cookie**
- **Whale Phishing**
- **Wire Attack**
- **Zero Day Exploit**



NIST Cybersecurity Framework

The Cybersecurity Framework assesses security measures beyond what's in the IT infrastructure to the critical policies, processes, and procedures of an organization.

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
<ol style="list-style-type: none">1. Asset Management2. Business Environment3. Governance4. Risk Assessment5. Risk Management Strategy	<ol style="list-style-type: none">1. Access Control2. Awareness & Training3. Data Security4. Info Protection Process & Procedures5. Maintenance6. Protective Technology	<ol style="list-style-type: none">1. Anomalies & Events2. Security Continuous Monitoring3. Detection Processes	<ol style="list-style-type: none">1. Response Planning2. Communications3. Analysis4. Mitigation5. Improvements	<ol style="list-style-type: none">1. Recovery Planning2. Improvements3. Communications



U.S. Small Business
Administration

“...regardless of size, degree of cyber risk or cybersecurity sophistication—apply the principles and best practices of (NIST CSF) to improve the security and resilience of critical infrastructure.”

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

- 
- Defense in Depth
 - Patched systems
 - 24/7 monitoring/alerting
 - Annual compliance auditing
 - Experienced IT/Security team



User clicks on an email



**So what if our company gets ransomware?
We have cyber insurance!**

What do ransomware hackers charge?

Why your IT provider may put you at risk.





**We're too small
to be attacked.**

FALSE!



The cybercriminals
behind
ransomware do
not particularly
care who their
victims are, as long
as they are willing
to pay the ransom.

Cybercrime Can Be Fatal



promo
m marketing
Magazine
COMPUTER & ELECTRONICS

Colorado Timberline Abruptly Closes, Cites Ransomware Attack

By **Brendan Menapace**

-  FACEBOOK
-  TWITTER
-  LINKEDIN
-  EMAIL
-  1 COMMENTS

Colorado Timberline, the supplier based in Denver, posted an announcement on its website yesterday announcing that the company was closing abruptly. Here's the full text of the message:

COLORADO
TIMBERLINE

Dear valued customers and suppliers of Colorado Timberline:

It is with great difficulty and a heavy heart that we must inform you that effective immediately Colorado Timberline has ceased all operations indefinitely.

We have recently been plagued by several IT events, unfortunately we were unable to overcome the most recent ransomware attack and this unfortunate and difficult decision was made.

Thank you for your support and loyalty from each of you over

- ~100 employees
- Ransomware Attack August 14th, 2018
- Out of Business September 12th, 2018



An iceberg floating in the ocean, used as a metaphor for the layers of the web. The tip of the iceberg is above the water line, representing the Surface Web. The much larger part of the iceberg is submerged below the water line, representing the Deep Web and Dark Web. The background is a blue sky with clouds above the water and a dark blue ocean below.

Surface Web

YAHOO!

Google

reddit

CNN.com

bing

Deep Web

Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Some organization-specific
repositories

Dark Web

TOR
Political protest
Drug trafficking
and other illegal activities

96%

of content on the
Web (estimated)

What is the Dark Web?

It is a black market for
cyber criminals.

Your personal data is for
sale today on the Dark
Web

Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:



Social security number



\$1

Online payment services login info
(e.g. PayPal)



\$20-\$200

Credit or debit card
(credit cards are more popular)



\$5-\$110

With CVV number
\$5

With bank info
\$15

Fullz info*
\$30

Drivers license



\$20

Loyalty accounts



\$20

General non-financial institution logins



\$1

Diplomas



\$100-\$400

Passports (US)



\$1000-\$2000

Subscription services

\$1-\$10

Medical records

\$1-\$1000**



Physical Security



QuickBooks®



MAXIMUM SECURITY ENTRANCE.



Human Firewall



- **95% of cyber attacks are the result of human error**
- **Cybersecurity Awareness Training**
- **MFA**
- **Password Locker With Randomly Generated 9+ Character Passwords**
- **Be Skeptical. Of EVERYTHING!**

Top 20 Passwords of 2021



- 1) 123456
- 2) 123456789
- 3) qwerty
- 4) password
- 5) 1234567
- 6) 12345678
- 7) 12345
- 8) iloveyou
- 9) 111111
- 10) 123123



- 11) 987654321
- 12) qwertyuiop
- 13) mynoob
- 14) 123321
- 15) 666666
- 16) 18atcskd2w
- 17) 7777777
- 18) 1q2w3e4r
- 19) 654321
- 20) 555555

I changed all my passwords to "incorrect".

A meme featuring Steve Carell as Michael Scott from the TV show 'The Office'. He is smiling broadly and holding a banana. The image is framed by a thick black border.

**So whenever I forget, it will
tell me "Your password is incorrect."**

Time It Takes For A Hacker To Crack Your Password



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



Questions?

Bottom Line: Security is Inconvenient



Personal Action Items



- Update your computer and anti-virus software **TONIGHT!**
- Get a password locker
- Update ALL passwords
- Use 2-Factor Authentication
- Backup your data
- Purchase ID Theft Service
- Stay Informed



Business Action Items

- Get Management's Unwavering Commitment
- Cybersecurity Awareness Training
- Harden Network/Systems
- Create and Enforce Policies
- Cybersecurity Audit
- Purchase Cyber Insurance
- Stay Informed
- Engage with Amnet



Merry Christmas

**Free Dark Web Scan and Basic Security
Assessment for CFMA members who
book before January 1.**

Amnet.net
(719) 442-6683



Confidential Information of Amnet