FUSIONTEK

LESSONS TO SHARE:

AN EXPERT'S GUIDE TO RANSOMWARE REMEDIATION

BEFORE WE START

FUSIONTEK

SCAN THE QR CODE TO REQUEST A COPY OF THIS PRESENTATION

BMILLER@FUSIONTEK.COM

WWW.FUSIONTEK.COM

ON THE AGENDA

- Discuss the Evolution of Ransomware
- Review Common Characteristics of Infection
- Layout the Typical Timetable for Resolution
- Share our Recommended Actions

EVOLUTION OF RANSOMWARE

FUSIONTEK

TARGET DATA BREACH

WHEN: Occurred in 2013

HOW: Attackers compromised the network of an HVAC company that was working on projects for Target

WHAT THEY GOT:

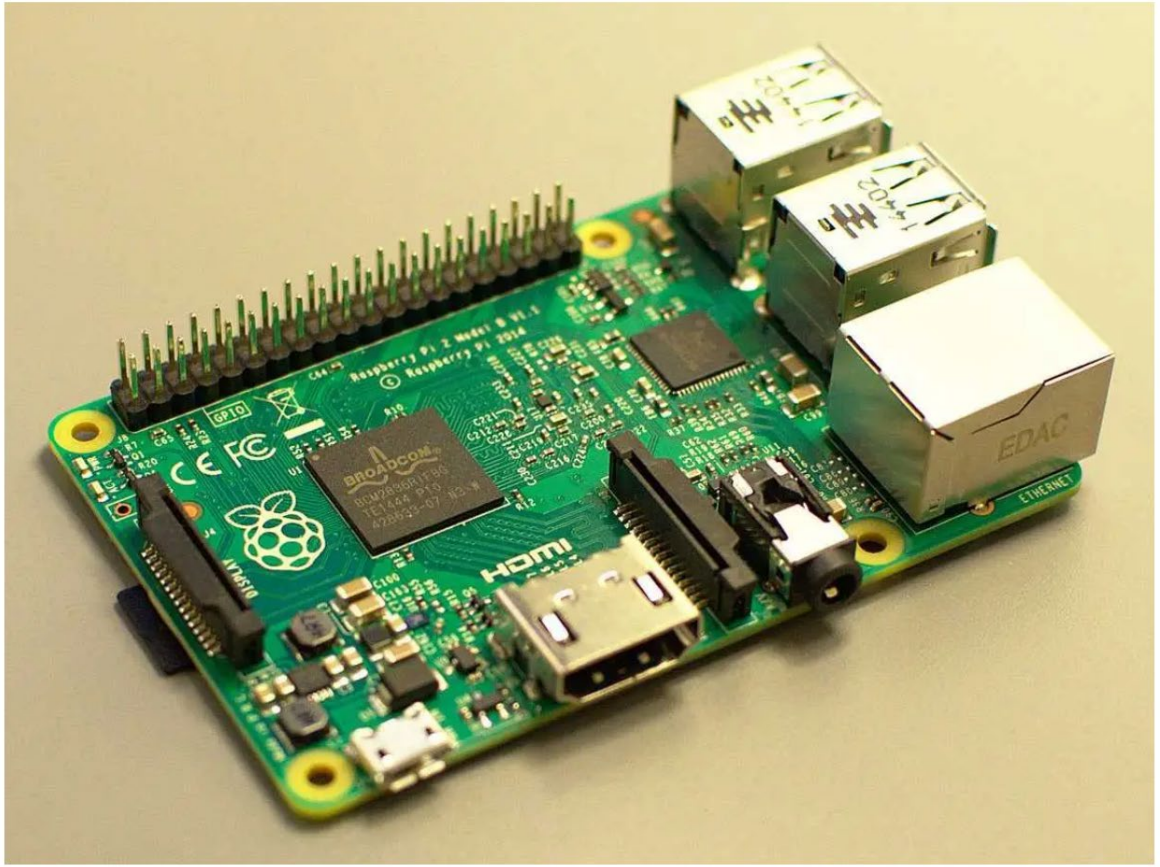
- 40 million payment card accounts
- 70 million customers' personal information

FUN FACT: Catalyst for adoption of chip and pin credit cards

SENSITIVE NETWORKS COMPROMISED

NASA Jet Propulsion Laboratory network was hacked by targeting a Raspberry Pi that wasn't supposed to be connected to it

Rosalie Chan Jun 23, 2019, 10:53 AM



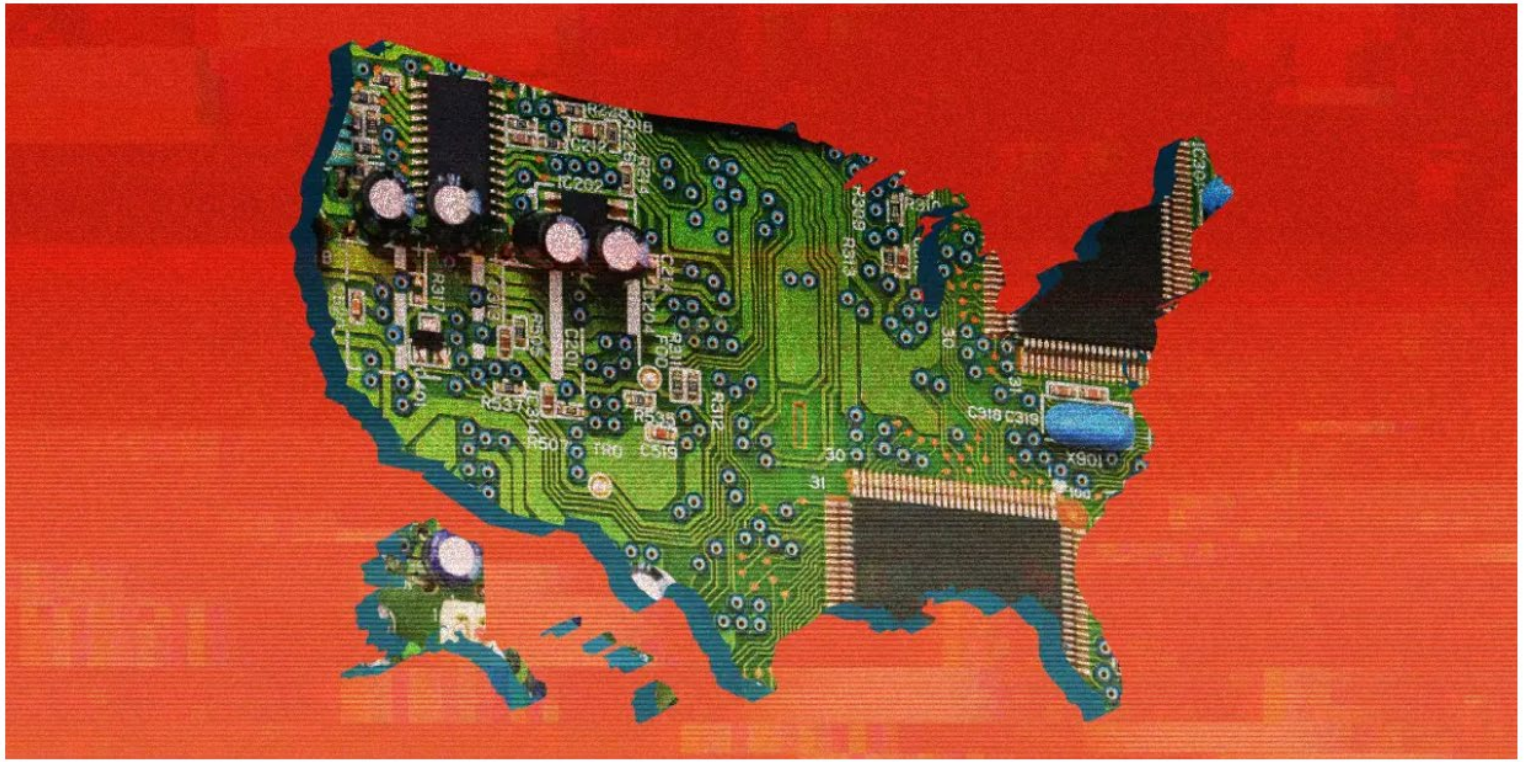
Raspberry Pi Flickr/abuakel

FUSIONTEK

MUNICIPAL NETWORKS INFECTED

A Florida city paid a $600,000 bitcoin ransom to hackers who took over its computers — and it's a massive alarm bell for the rest of the US

Sinéad Baker Jun 20, 2019, 3:01 AM



Samantha Lee/Business Insider

FUSIONTEK

PAYMENTS TO FAKE VENDORS

City of Ellensburg loses $185K to cyber-scammers disguised as vendor

BY NICOLE JENNINGS
AUGUST 21, 2019 AT 9:03 AM

Share

Ellensburg, Washington. (Ellensburg PD)

Less than a month after it was revealed that King County lost $220,000 to cyber criminals posing as vendors, the City of Ellensburg was robbed of over $185,000 in the same way.

Most Popular

- Rep. intros bills to protect driver privacy with Democrats' pay-per-mile plan
- Rantz: Election security bills appear stalled by Washington Democrats
- Chance for another round of snow Tuesday morning

PERSONAL DATA STOLEN

Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank

Oscar Williams-Grut Apr 15, 2018, 12:08 AM

An aquarium at a casino — but not the one in question. Ethan Miller/Getty Images

- **The CEO of the cybersecurity firm Darktrace says hackers are increasingly targeting unprotected "internet of things" devices, such as air-conditioning systems and CCTV, to get into corporate networks.**

HACKERS ACCESS NEST & RING DEVICES

Wisconsin couple describe the chilling moment that a hacker cranked up their heat and started talking to them through a Google Nest camera in their kitchen

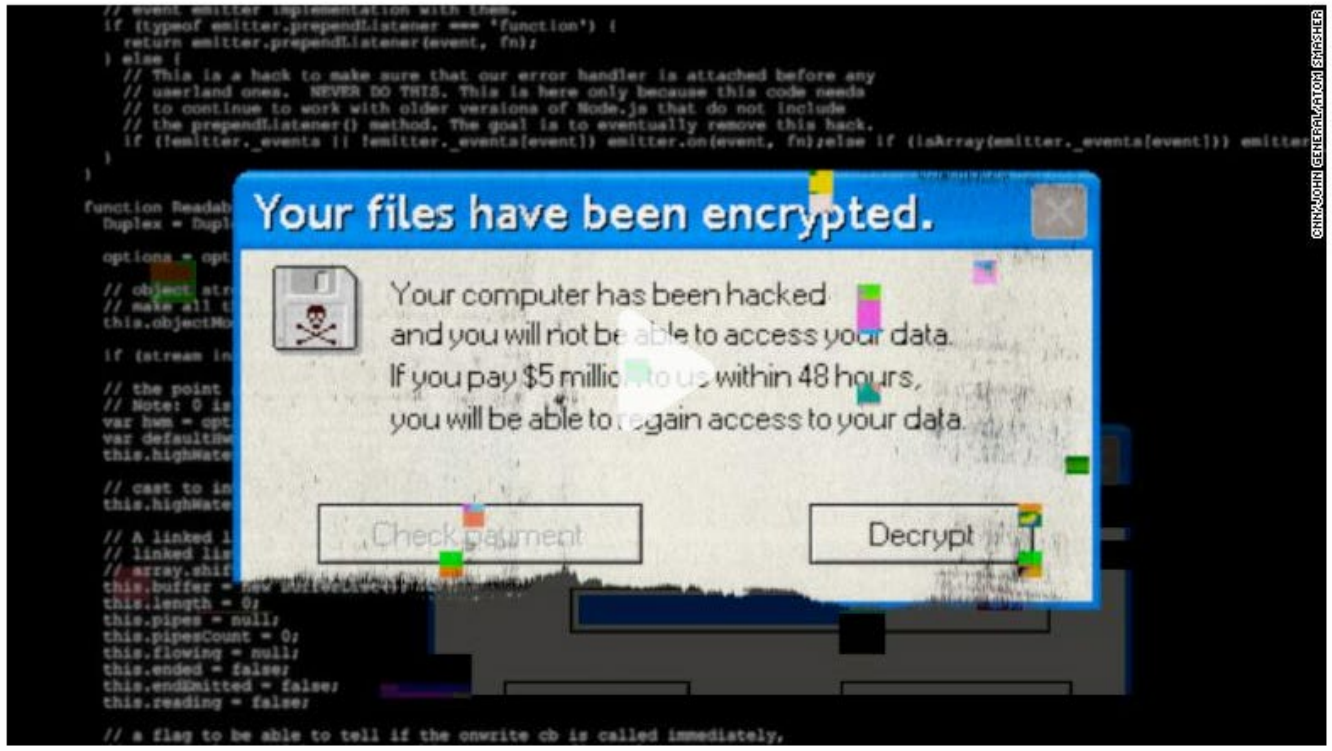
Hayley Peterson Sep 25, 2019, 1:12 PM

COLONIAL PIPELINE SHUTS DOWN GAS ACCESS

Colonial Pipeline says ransomware attack also led to person information being stolen

By Brian Fung, CNN Business

Updated 1:10 PM ET, Mon August 16, 2021



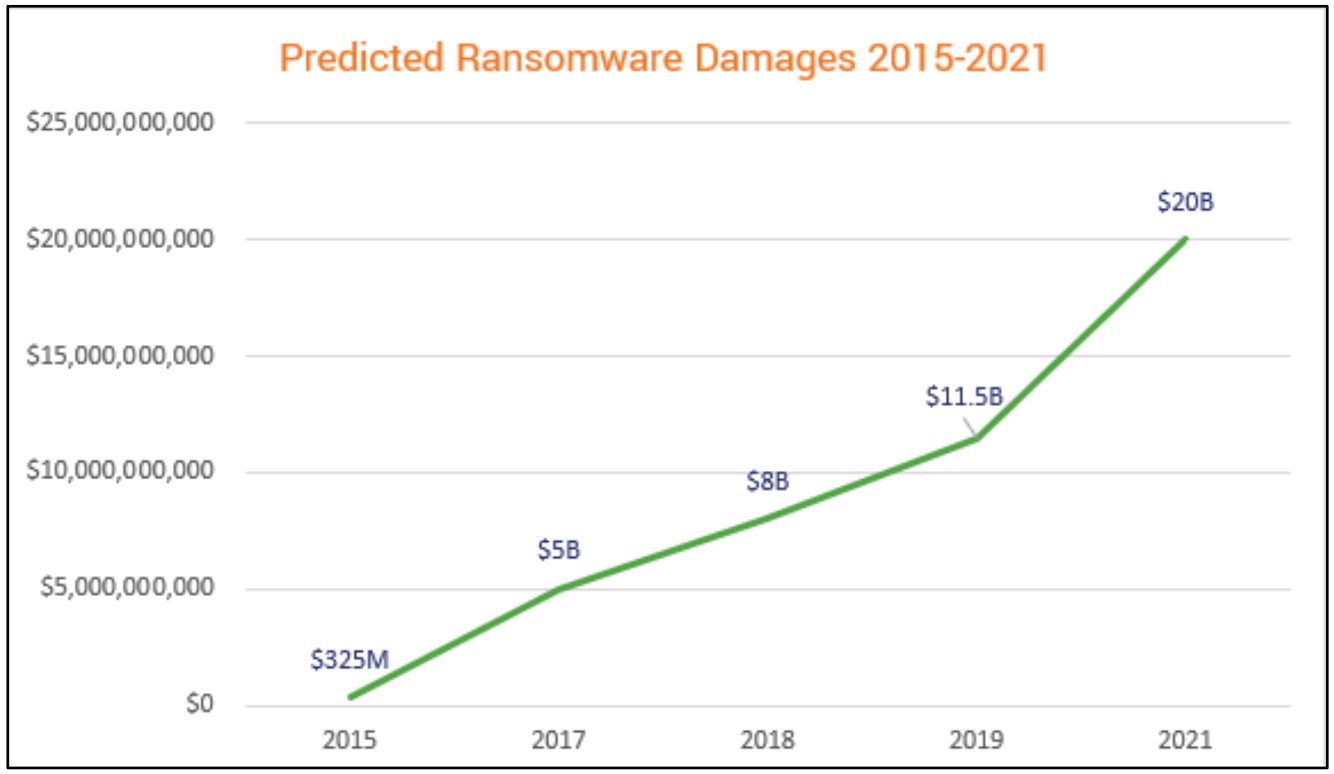
MORE FROM CNN BUSINI

This exec was ce
Trump on Twitte

Democrats plan t
help pay for $1,7

Recomme

ATTACKS INCREASING THROUGHOUT 2021



STAMFORD, CT, October 21, 2021

Gartner Says Threat of New Ransomware Models is the Top Emerging Risk Facing Organizations

Supply Chain Disruptions and Endemic COVID-19 Also in Top Five Risks in 3Q21

Home » Banking industry sees 1318% increase in ransomware attacks in 2021

Cyber | Security Newswire | Cyber Security News

Banking industry sees 1318% increase in ransomware attacks in 2021

threatpost | Cloud Security | Malware | Vulnerabilities | InfoSec Insiders | Webinars

Raccoon Stealer Bundles Malware, Propagates Via Google SEO | Iranian APT Lure

Ransomware Volumes Hit Record Highs as 2021 Wears On

In 2021, the largest ransomware payout was made by an insurance company at $40 million, setting a world record. (Business Insider, 2021)

The average ransom fee requested has increased from $5,000 in 2018 to around $200,000 in 2020. (National Security Institute, 2021)

Experts estimate that a ransomware attack will occur every 11 seconds in 2021. (Cybercrime Magazine, 2019)

FUSIONTEK

https://ww
https://ww
https://www.fusiontek.com/blog/ransomware-statistics-2021/
isk-facing-organizations

COMMON CHARACTERISTICS OF INFECTION

FUSIONTEK

USE OF AN INITIAL ACCESS BROKER

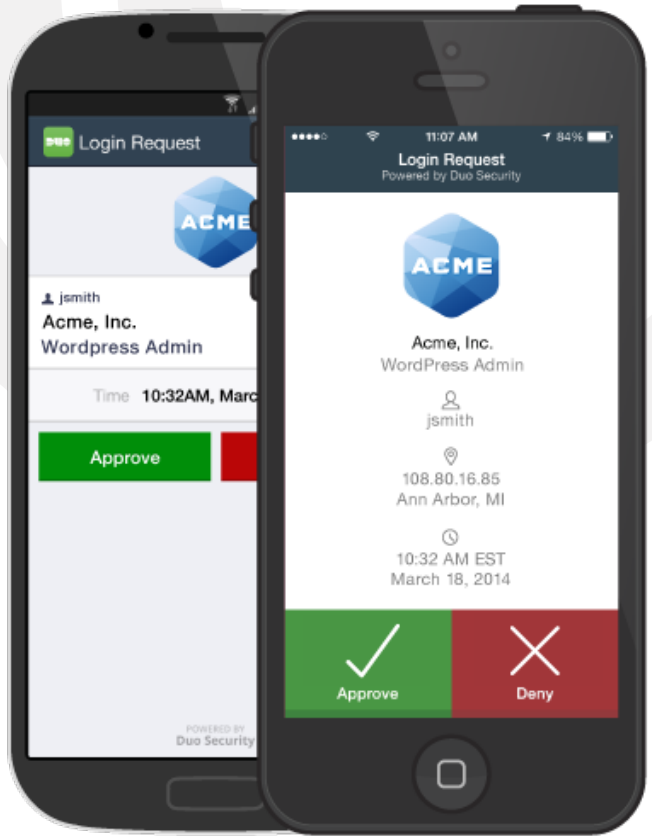
- Initial Access Brokers Gets Credentials and Sells them to the Threat Actor
  - Four Primary Vectors
    - Common Use of Shared Credentials
    - Remote Access without MFA
      - RDP
      - VPN
    - Web Shells / Proxies / Custom Applications
      - Many leverage the Exchange Vulnerabilities of 2021
    - Email
      - Phishing & Dropping of Malware

REUSE OF COMMON OR SHARED PASSWORDS

- Use unique passwords for each site or application
  - Often a compromised password is attempted to be reused in other locations
  - Staples data breach didn’t provide credit card info, but did provide usernames and business contact information that could then be phished

MULTIFACTOR AUTHENTICATION NOT FULLY OR COMPLETELY DEPLOYED

- Fully use MFA anywhere it possibly can be
- Consider removing services that don't fully support or require MFA
- While any MFA is better than no MFA, the recommended type of MFA is app based (i.e. Duo, Okta, or similar platforms)
- TOTP (QR codes) are complex math problems that are a devices solves and generates a code. The authentication information is not logged, and the code can be cloned.
- Text message and email-based authentication can be easily circumvented.



WEB SHELLS / PROXIES / CUSTOM APPLICATIONS

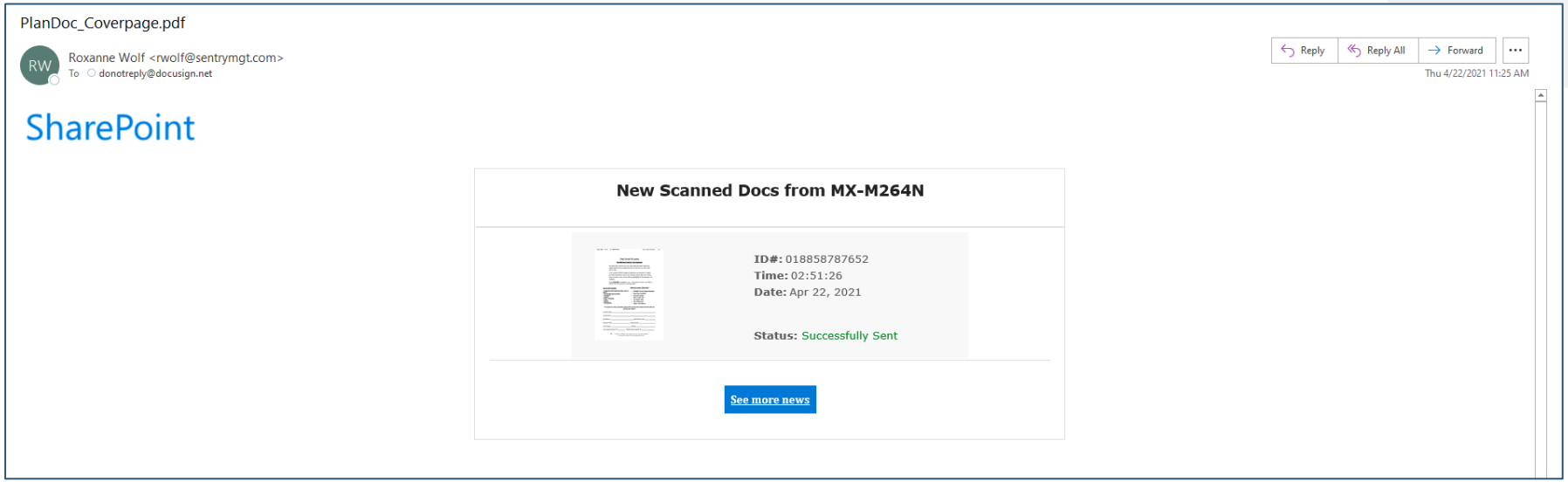
- Exchange Vulnerabilities First Appearing in March 2021 are a common example
- Patching the vulnerability does not remove the threat
  - Threat Actors often use it for initial access before installing alternate access methods
- Custom Web Apps and similar code are a higher risk, due to smaller install base

PHISHING EMAILS – DIRECT RESPONSE EMAILS

- Typically impersonating someone and getting either bank account info or gift cards
- Commonly targeted at newer hires who might not understand an organizations processes / procedures after then post about a nee job on LinkedIn, Facebook, Instagram, etc.…

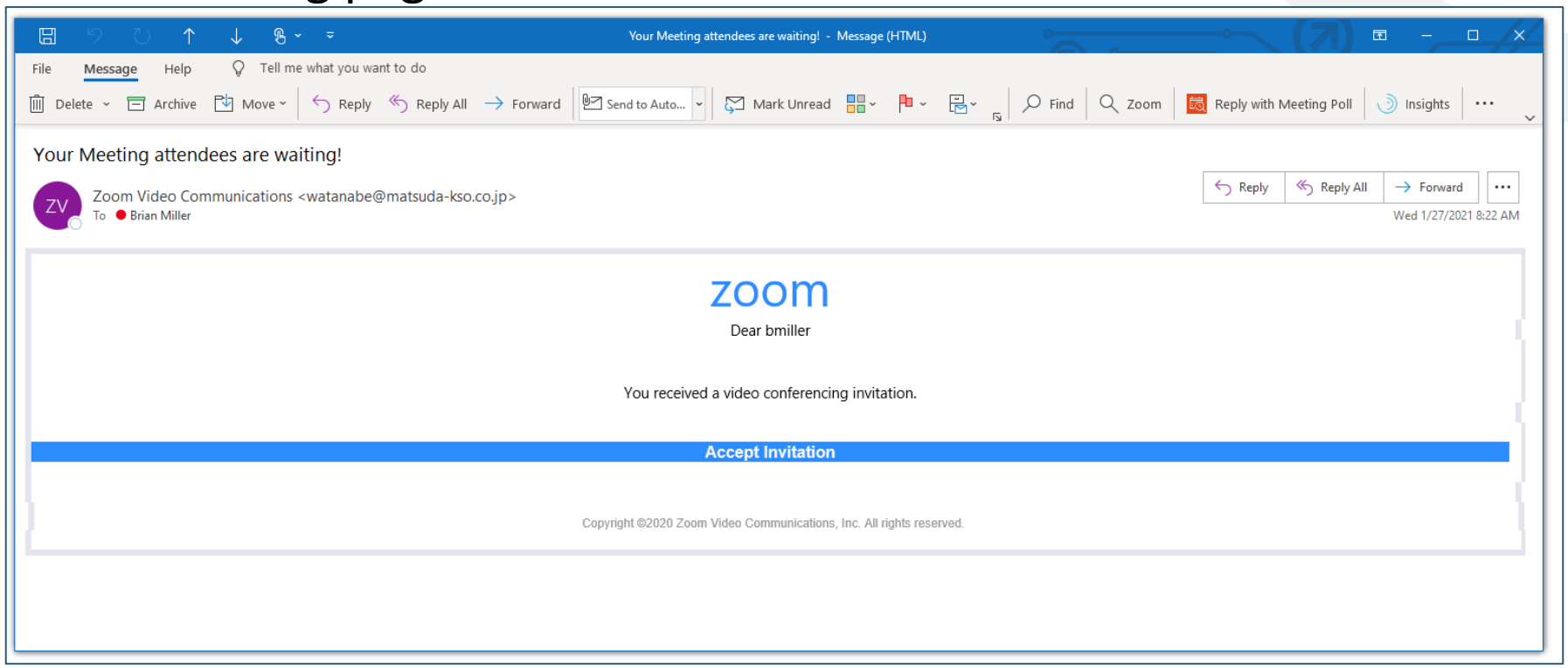
PHISHING EMAILS – FAKE NOTIFICATION EMAILS

- Fake SharePoint, Zoom or Voicemail notifications
  - Embedded link will attempt to scrape credentials or take you to a fake landing page



PHISHING EMAILS – FAKE NOTIFICATION EMAILS

- Fake SharePoint, Zoom or Voicemail notifications
  - Embedded link will attempt to scrape credentials or take you to a fake landing page



PHISHING EMAILS – MALICIOUS LINKS HIDDEN IN DOCUSIGN OR SIMILAR PLATFORMS

- Will either mimic the e-signing platform or be the real platform
- If the real platform, the attached file to “review or sign” will be loaded with malware

SUPPLY CHAIN OR ZERO DAY VULNERABILITY ATTACKS

- Very common with software vendors, especially legacy software platforms
- Equally risky for on-prem and cloud solutions
- Targeted by larger ransomware organizations and nation-state threat actors
- Impacted products over the past year
  - Microsoft
  - Cisco
  - SolarWinds
  - Kaseya

LACK OF A SECURITY FOCUSED IT CULTURE

- Security tools aren’t fully or completely deployed
- Exceptions made to not activate items such as MFA, or security tools on the computer because it is too complex or inconvenient
- Depending only on one security product (i.e. we’ve got product X so we don’t need to do anything else)

TYPICAL TIMETABLE

FUSIONTEK

INITIAL INFECTION

- Access to the network obtained
- Backdoor software installed to allow future access in multiple ways
- Reconnaissance of the network and review of typical file types to monetize
  - Backups and security software in use
  - Insurance documents and policy limits
  - Sensitive internal or industry data
- Escalation of privileges using a compromised administrative account
- Exfiltration of data to external location
- This process can be as short as 12-24 hours, but typically the threat actors are in the network for weeks prior to detection or launching the ransomware payload

DEPLOYMENT OF RANSOMWARE

- Typically launched overnight or on a weekend.
  - Holiday weekends are more popular as they allow for a longer infection time prior to discovery
- Goal is to infect as many systems as possible
- Some ransomware strains completely stop the machines from functioning, however, most just encrypt work product (databases, word documents, PDF files, etc.…)
- During the deployment phase, security software will typically be disabled, and backups destroyed

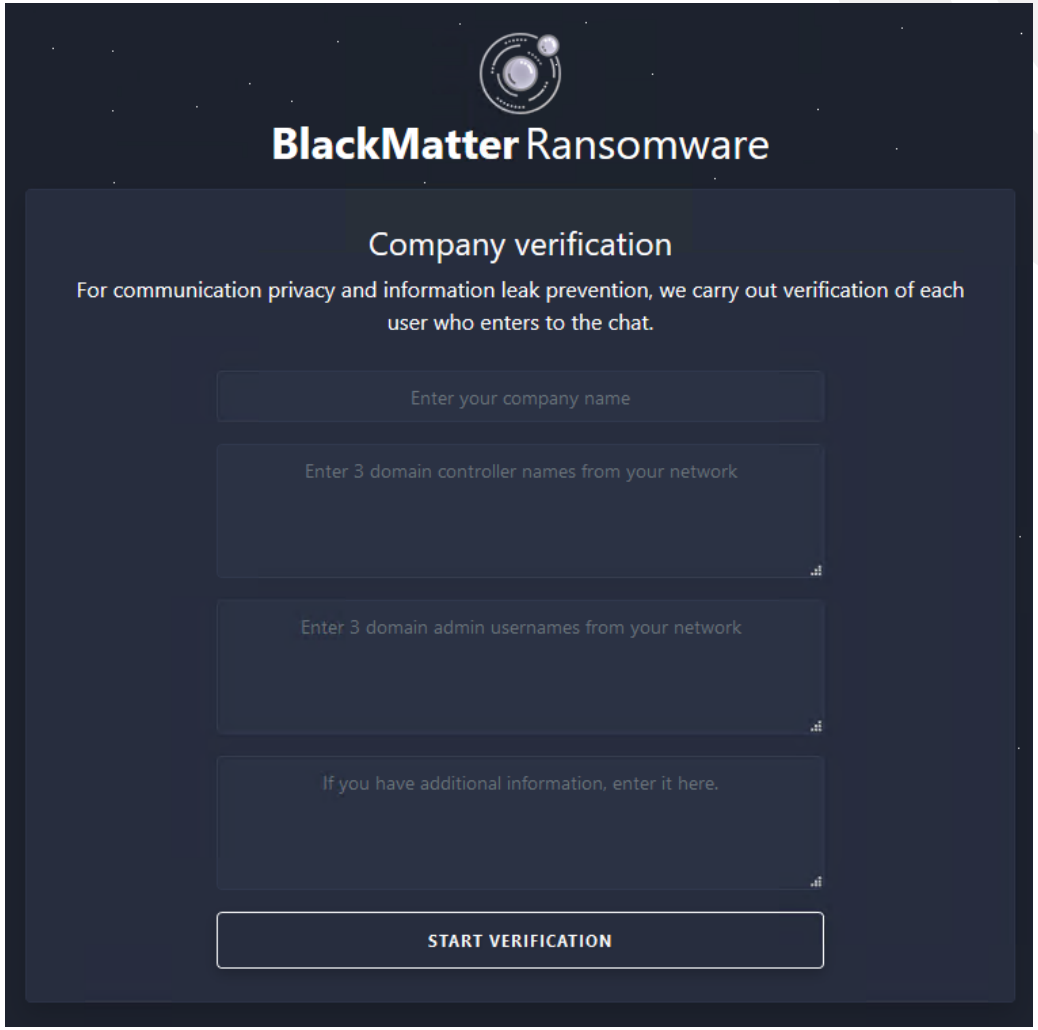
COMMUNICATING WITH THE THREAT ACTORS

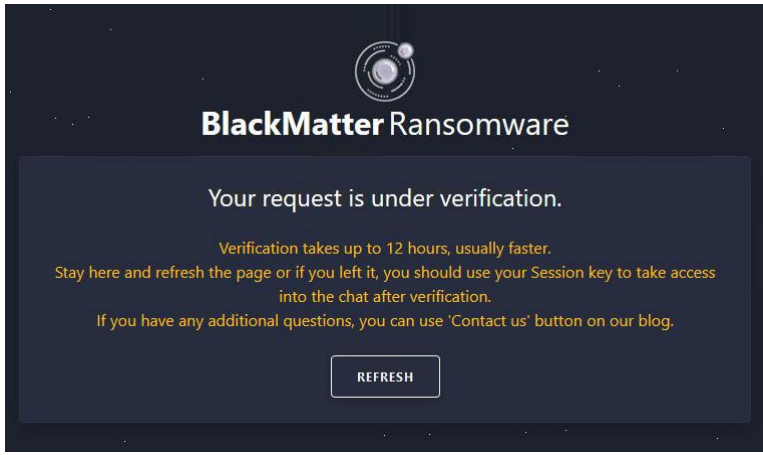
- In each encrypted folder, they typically leave a notepad document with a dark web address to obtain the ransomware amount

```
   We know that you will try to restore your systems, but in addition to the encrypted computers, we have
collected a lot of confidential and critical information from your network, which we will be ready to
release in 2 days after you read this note, I recommend that you get in touch as soon as possible. In
order to keep the incident under wraps, you need to take care of the problem yourself. Uploading the
executable file to virustotal will inevitably alert dozens of people and thus give publicity to your
compromise, we advise you to avoid this.

>>> What happens?
   Your network is encrypted, and currently not operational.
   We need only money, after payment we will give you a decryptor for the entire network and you will
restore all the data.

>>> What guarantees?
   We are not a politically motivated group and we do not need anything other than your money.
   If you pay, we will provide you the programs for decryption and we will delete your data.
   If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this
does not comply with our goals.
   We always keep our promises.

>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open http://supp24maprinktc7uizgfyqhisx7lkszb6ogh6lwdzpac23w3m

>>> Warning! Recovery recommendations.
   We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.
```

COMMUNICATING WITH THE THREAT ACTORS

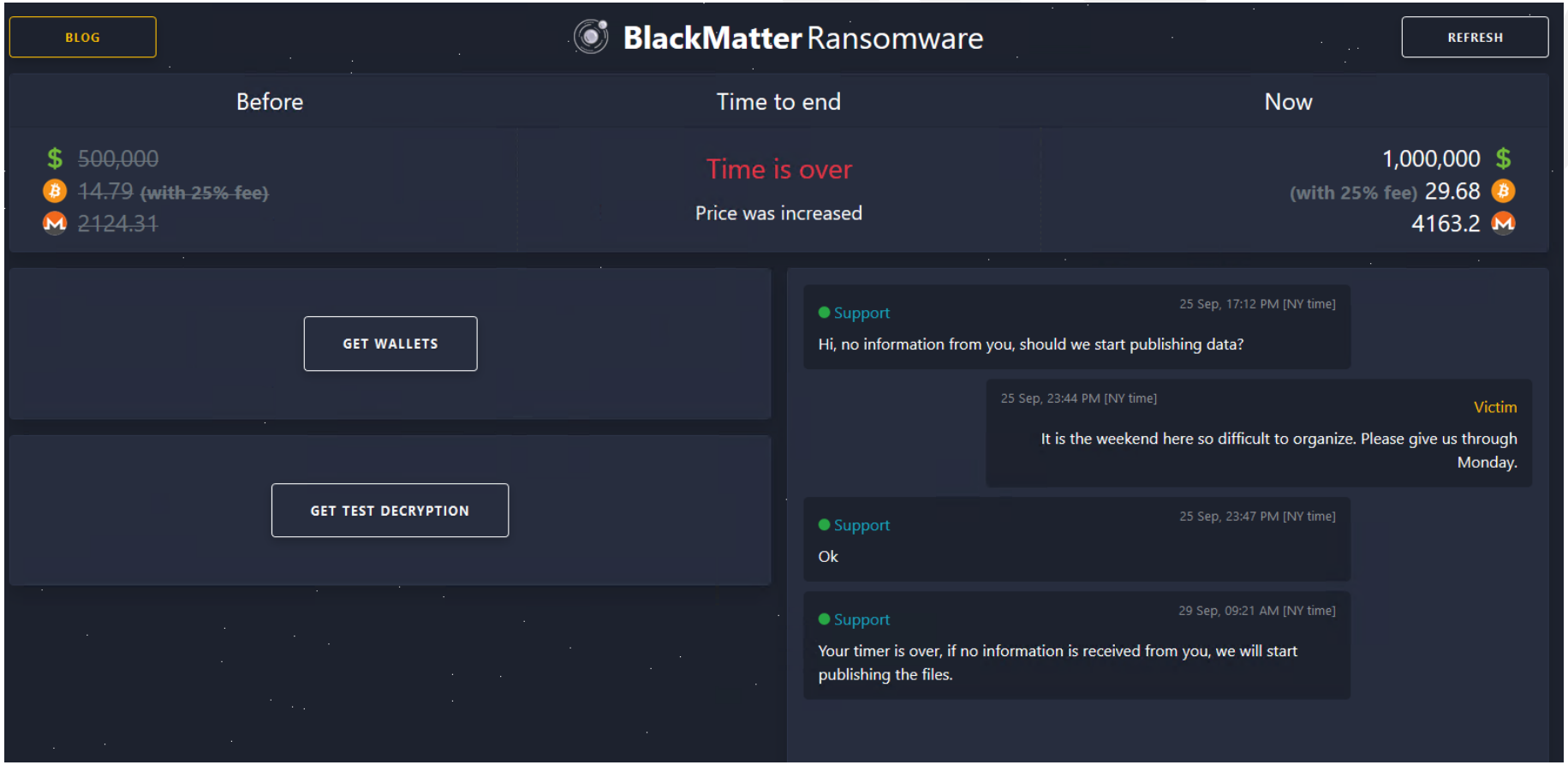
- Using a tor browser, we then connect to the threat actors “help desk”.
- The “help desk” asks you to verify information on the compromised network





COMMUNICATING WITH THE THREAT ACTORS

- Typically, two prices are provided for the files.
  - A 50% discount if paid in 3 days is common
- The “blog” is where they post files for folks who don’t pay.



REMEDIATION PROCESS

- In parallel to the ransomware negotiations, the process can begin to restore necessary files and folders from backups or rebuild.
- It is important to complete a root cause analysis prior to restoration so compromised data isn’t restored causing a reinfection.
- Several hundred hours of work is not uncommon depending on the size and scope of the infection.

RECOMMENDED ACTIONS

FUSIONTEK

UNDERSTAND YOUR INSURANCE REQUIREMENTS AND COVERAGE

- Many carriers either have carveouts or riders related to ransomware breaches
- Check your specific policy and be aware of the process they may require you to follow when this occurs to your organization
- Many riders require you to attest to items such as MFA fully deployed to all users

REQUIRE MFA ON ALL LOGINS FROM ALL SOURCES

- Fully and correctly deployed MFA is the number one prevention tool
- In all ransomware cases we have worked MFA has not been fully and correctly deployed
- Evaluate it for “non-IT” items as well (i.e. access to your Business Checking Accounts or HR management tools)

DEPLOY NEXT GENERATION CLOUD SECURITY TOOLS

- Talk to your IT team (external partner, in house team, etc..) about
  - Air gapped backups
  - Zero Trust Tools
  - MFA deployment process / standards
  - Plan for what happens when this occurs

THANK YOU

FUSIONTEK

SCAN THE QR CODE TO CONNECT WITH OUR TEAM

BMILLER@FUSIONTEK.COM

WWW.FUSIONTEK.COM