REVELE | truenorth

Q4 Healthcare Security Update: Current Emerging Security Threats and Risks

Presenter:

Matt Murren, CISSP-ISSMP
CEO & Founder
True North ITG, Inc.

AGENDA:

- Q4 Healthcare Security Update: Risks and Threats
- State of Healthcare Data Security
- Security Breach #1: Wire Transfer Fraud
  - People & Policy Solutions
  - Security and Technology Solutions
- Security Breach #2: Ransomware Event
  - People & Policy Solutions
  - Security and Technology Solutions
- Q & A + Discussion

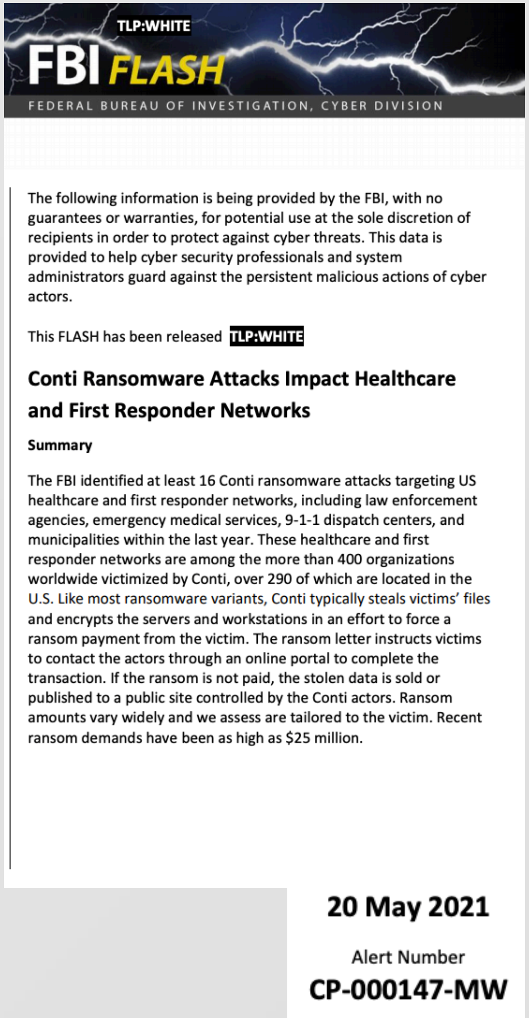
Q4 Security Updates

- First reported Ransomware related death
- Continued FBI Warning: Imminent Ransomware Threat for Healthcare
  - Scripps, Aprima Hosting, Others…
- Phishing and Financial PII Risks
  - Payroll and Supporting Systems
- Healthcare System Interruption
- Supply Chain Attack Preparedness
  - Solarwinds

FBI Warning: Ransomware

- Threat: Conti Ransomware w/ Emotet
- Attack Vector: Phishing, RDP Creds, Infected Word Documents and files. 1-4 weeks of access prior to payload.
- Ransom: $2 million+
- Mitigation: Patching, Training and Awareness, MFA, Endpoint Detection and Response, DNS Blocking and Network Segmentation, EDR, and DR/Business Continuity.

(sneaky tip…in testing)



TLP:WHITE

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP:WHITE**

Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Summary

The FBI identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site controlled by the Conti actors. Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as $25 million.

20 May 2021

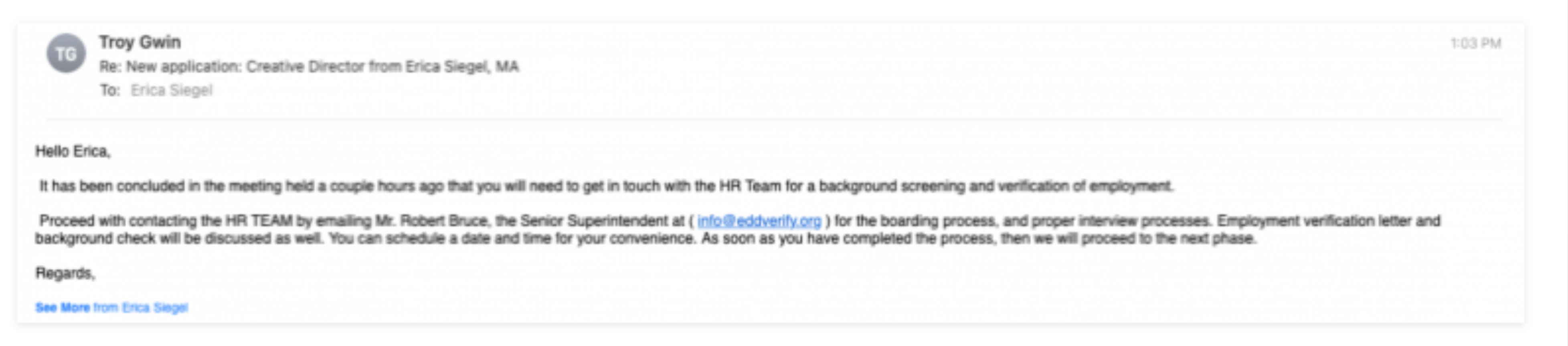
Alert Number

CP-000147-MW

Phishing , HR, and Financial Attacks

- Threat: Fake job interview from Healthcare organizations. Payroll links to employees.
- Attack Vector: Email Phishing leading to password breach. Password breach.
- Impact: Brand + PII Theft by Employee or candidates.
- Mitigation: Inspect email details. Email address, name of sender via Linkedin, Upfront application fees, etc.

Example: Phishing



Troy Gwin

Re: New application: Creative Director from Erica Siegel, MA

To: Erica Siegel

1:03 PM

Hello Erica,

It has been concluded in the meeting held a couple hours ago that you will need to get in touch with the HR Team for a background screening and verification of employment.

Proceed with contacting the HR TEAM by emailing Mr. Robert Bruce, the Senior Superintendent at (info@eddverify.org) for the boarding process, and proper interview processes. Employment verification letter and background check will be discussed as well. You can schedule a date and time for your convenience. As soon as you have completed the process, then we will proceed to the next phase.

Regards,

See More from Erica Siegel

Planning: Healthcare System Interuption

- Threat: Dependent Healthcare systems. Hospitals and Referring Providers. Ransomware and Others.
- Risk: Partners in your Healthcare ecosystem get attacked resulting in lack of diagnostics, referrals, overall workflow.
- Mitigation: Workflow assessment, Critical links, Business Continuity planning. What would break?

Supply Chain and Vendor Attacks

- Threat: Technology tools get breached and downloaded to your network through updates or patches.
- Attack Vector: ”Trusted” software that is embedded with malicious code or intent.
- Mitigation: “No trust” approach, Turn off Auto-updates, EDR, SOC, and SEIM.

Quick Q & A Check…

- We covered a lot there…
- Any questions?

2021 Security Breach #1

- Wire Transfer Fraud: Email phishing attack leading to impersonation attack on Finance team.
- Attack Vector: Email Phishing leading to password breach. Ongoing vendor and invoice fraud leading to ACH payments to false vendors, approved by internal staff.
- Losses: $1 mil.+

Mitigation: Policy and People

- **Training and Awareness:** Build Awareness
  - Identify the originating email address.
  - Scrutinize the request itself.
  - Confirm the request with supervisors.
  - Limit who has access to transfer funds.
- Implement a process to verify transaction approval
- Avoid Executive Email Autoresponders

Mitigation: Security and Technology

- MFA – Multi-Factor Authentication: Use second factor text authentication to validate you are the valid user. Protects in the event a login is detected in another state or Country.
- Geo Filtering: Block access to your network outside of your Geo location. Why does Russia need access to your network? Maybe you do…
- DR + Business Continuity: Daily snapshots with offsite backups that are segmented from your core network.
- Network Segmentation: Limit traffic external to internal and internal to internal.
- EDR + SOC: 24/7 Real time monitoring. Think ADT for data…

2021 Security Breach #2

- Ransomware Attack: Internal employee divulges password to an attacker. Attackers breach internal network on all locations over 3-5 weeks with no impact. In one activation, all sites are infected and all data both offsite and hosted is locked down and encrypted.

2021 Security Breach #2

- Ransomware Attack: Internal employee divulges password to an attacker. Attackers breach internal network on all locations over 3-5 weeks with no impact. In one activation, all sites are infected and all data both offsite and hosted is locked down and encrypted.

2021 Security Breach #2 cont…

- Attack Vectors: Email, Infected Files, and Network Controls. Lack of Patching.
- Impact: $1 mil. paid by insurance. No Ransom paid.
- Why no Ransom?: Immediately locked down networks. Restored all servers to prior day. Kept networks locked down while all networks, workstations, and servers were cleaned thoroughly. 45 staff working 24/7.

Mitigation: Policy and People

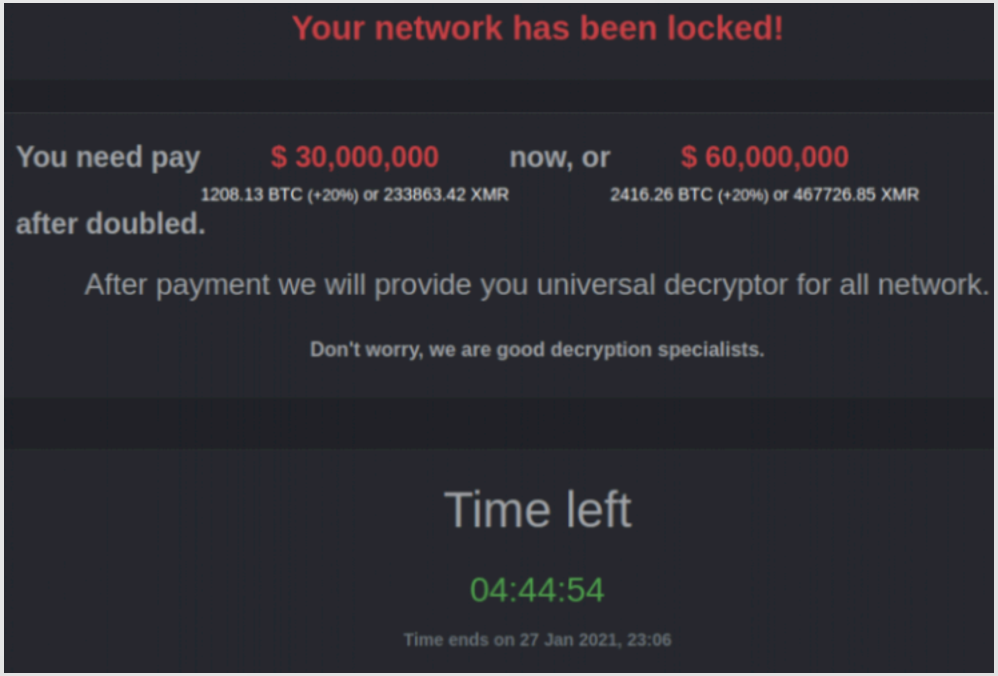
- Backup Procedures
- Security Incident Response: Roles & Tracking
- Training and Awareness: Build Paranoia
    - Unverified links
    - Untrusted email attachments
    - Downloads from untrusted sites
    - Unfamiliar USBs

Mitigation: Security and Technology

- Early Detection: Alerting and Monitoring – SEIM
- Backups: Offsite and On-Prem. Imaging of Servers and Critical Data.
- Incident Response: Plan was in place to sever connection for recovery of EMR. EMR was up and running in 3 hours while onsite recovery commenced.
- Business Continuity: Plan was in place and access was in place to take calls for re-scheduling and access to data for patient notification and re-direction.
- Read Only EMR: Saved the day.

If you ever see this…

- Contact your IT Security provider.
- Contact your Cyberliability Insurance Provider.
- Contact the FBI.
- Start your Business Continuity and Recovery process.



Your network has been locked!

You need pay $ 30,000,000 now, or $ 60,000,000 after doubled.

1208.13 BTC (+20%) or 233863.42 XMR

2416.26 BTC (+20%) or 467726.85 XMR

After payment we will provide you universal decryptor for all network.

Don't worry, we are good decryption specialists.

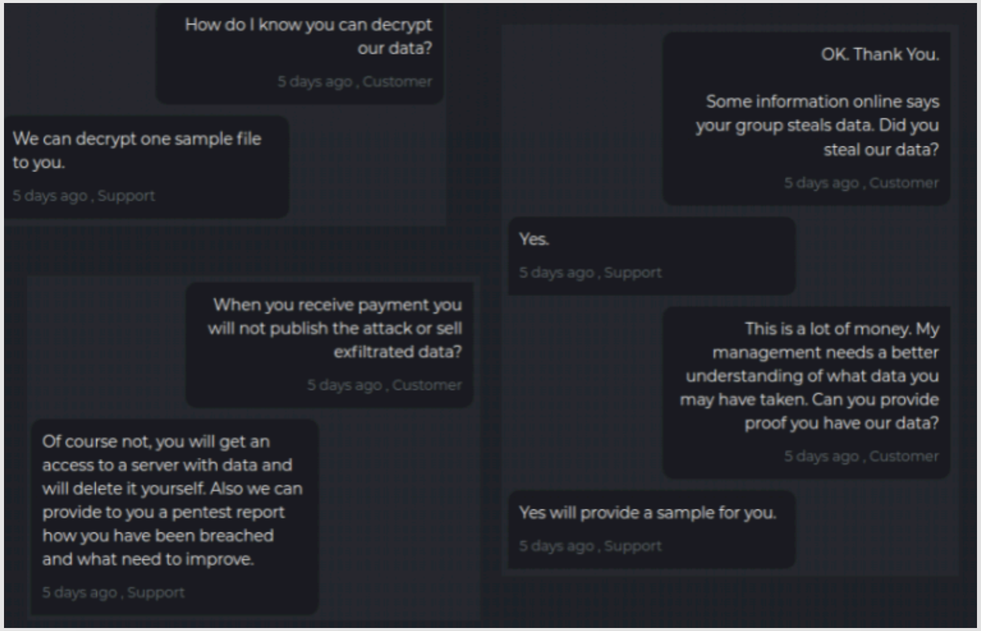
Time left

04:44:54

Time ends on 27 Jan 2021, 23:06

Don’t ever do this…

- Never start negotiations without FBI, Security Expert, or Insurance assistance.
- Divulge additional information or terms.
- Start any process without a lead incident manager and documenting EVERYTHING.



How do I know you can decrypt our data?
5 days ago , Customer

We can decrypt one sample file to you.
5 days ago , Support

When you receive payment you will not publish the attack or sell exfiltrated data?
5 days ago , Customer

Of course not, you will get an access to a server with data and will delete it yourself. Also we can provide to you a pentest report how you have been breached and what need to improve.
5 days ago , Support

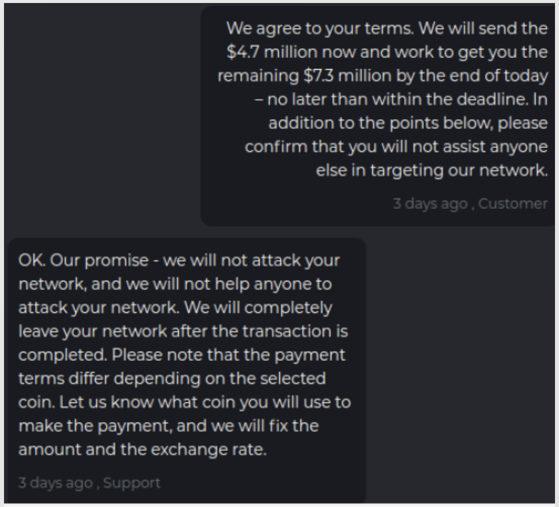
OK. Thank You.

Some information online says your group steals data. Did you steal our data?
5 days ago , Customer

Yes.
5 days ago , Support

This is a lot of money. My management needs a better understanding of what data you may have taken. Can you provide proof you have our data?
5 days ago , Customer

Yes will provide a sample for you.
5 days ago , Support



We agree to your terms. We will send the $4.7 million now and work to get you the remaining $7.3 million by the end of today – no later than within the deadline. In addition to the points below, please confirm that you will not assist anyone else in targeting our network.
3 days ago , Customer

OK. Our promise - we will not attack your network, and we will not help anyone to attack your network. We will completely leave your network after the transaction is completed. Please note that the payment terms differ depending on the selected coin. Let us know what coin you will use to make the payment, and we will fix the amount and the exchange rate.
3 days ago , Support

What’s wrong here!?

Q & A + Open Conversation

- General Questions?
- Real World Scenario Questions?
- Resources or follow-up. Please Matt.

REVELE | truenorth

Thank You!

We are here to help.

Presenter:

Matt Murren, CISSP-ISSMP
CEO & Founder
True North ITG, Inc.
Tel. 425.870.9305
matt@truenorthitg.com