Our Threat Intelligence Journey

September 20th, 2017

Agenda

- Introductions
- BCBSNE Threat Intel Program Background
- Our Goals & Expected Value
- How We Got Started
- Where We Are Now
- Our Unique Advantages
- What Anyone Can Do

INTRODUCTIONS

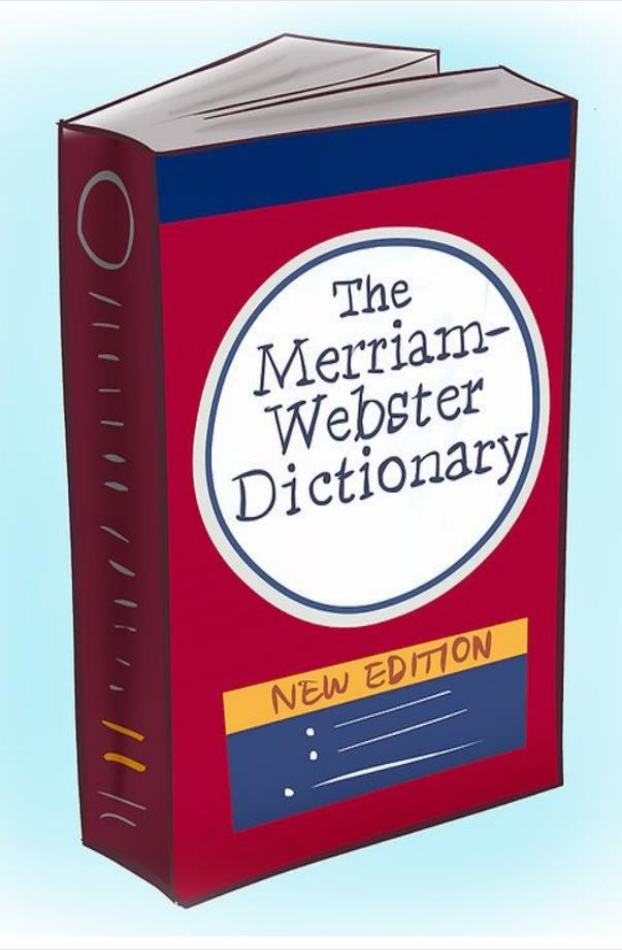
Jeffry Morrissette CISSP
Manager Enterprise Security @ BCBSNE
12+ Years in Info Sec

John Clabaugh
Sr. Threat Intelligence Analyst @ BCBSNE
Intelligence Analyst, USAFR
MS, International Security and Intelligence Studies

BCBSNE THREAT INTEL PROG BACKGROUND

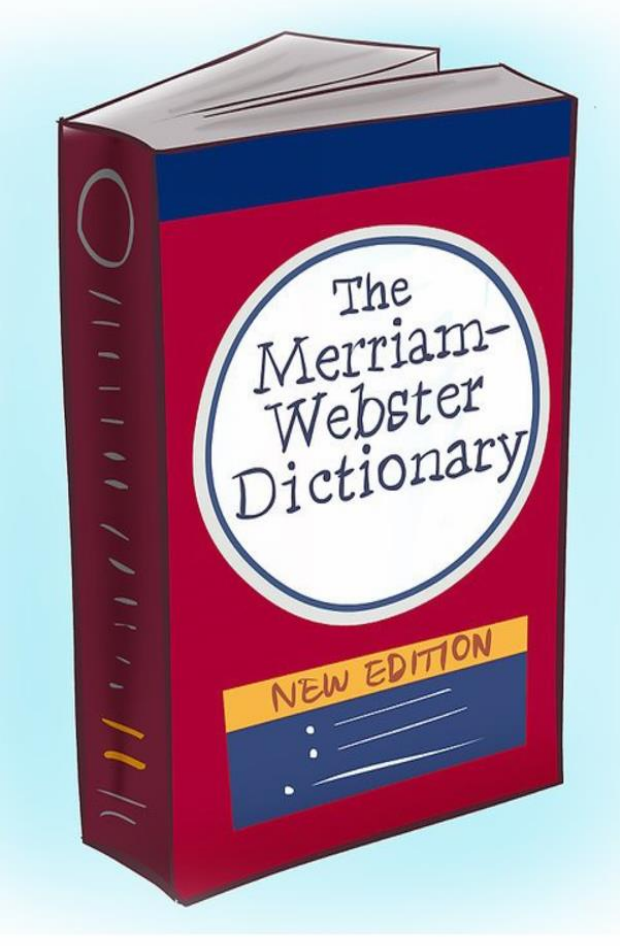
- Why was it a priority for BCBSNE?
  - Defined Security program and organization that works for BCBSNE in place.
  - Popular topic at Security conferences & events, Board meetings, and Vendor conversations.
  - Paranoia of “What we don’t know is going to kill us!”

- Issues with initial research
  - Vendors using “scare” tactics
    - PHI now bigger target than Credit Cards!
    - Medical records selling for much more than CC#!
  - Unclear from industry and vendors what it really meant



WHAT IS THREAT INTELLIGENCE ANYWAY?

- Rely primarily on DoD Joint Publications
  - 2-0: Joint Intelligence
  - 2-1: Joint and National Intelligence Support to Military Operations
- *The PRODUCT resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.*
- There are different aspects and approaches that may make Threat Intel look different in your organization.



WHAT IS THREAT INTELLIGENCE ANYWAY?

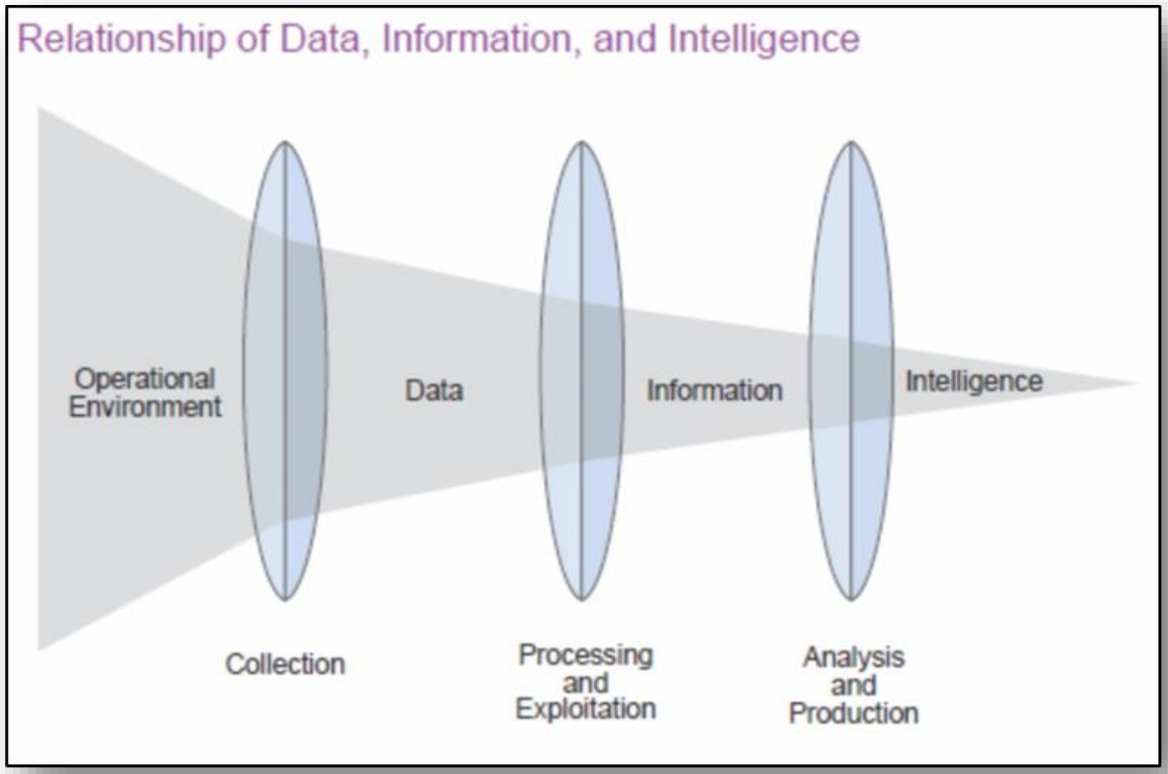
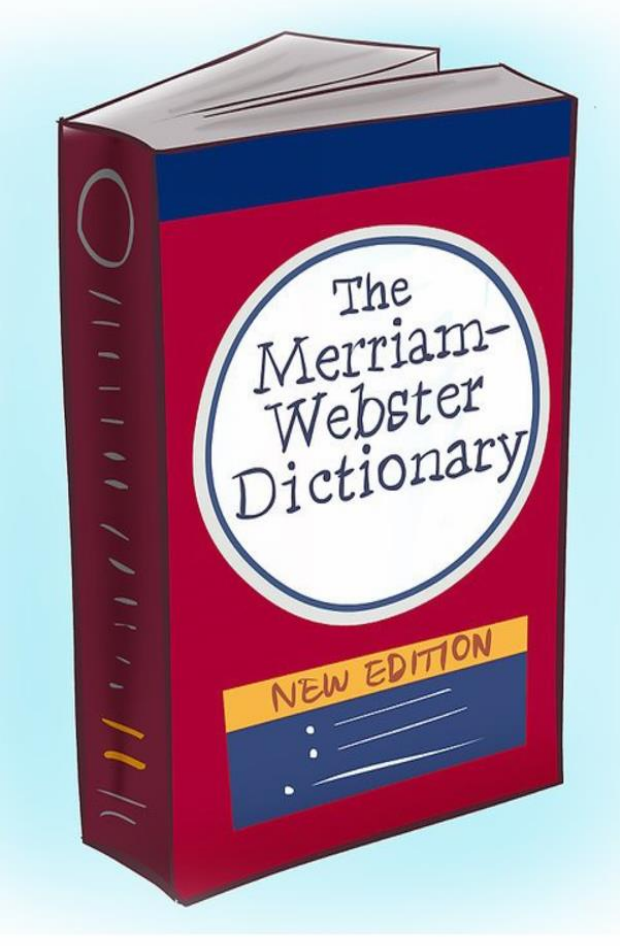


Figure 2. The Intelligence Process

WHAT IS THREAT INTELLIGENCE ANYWAY?



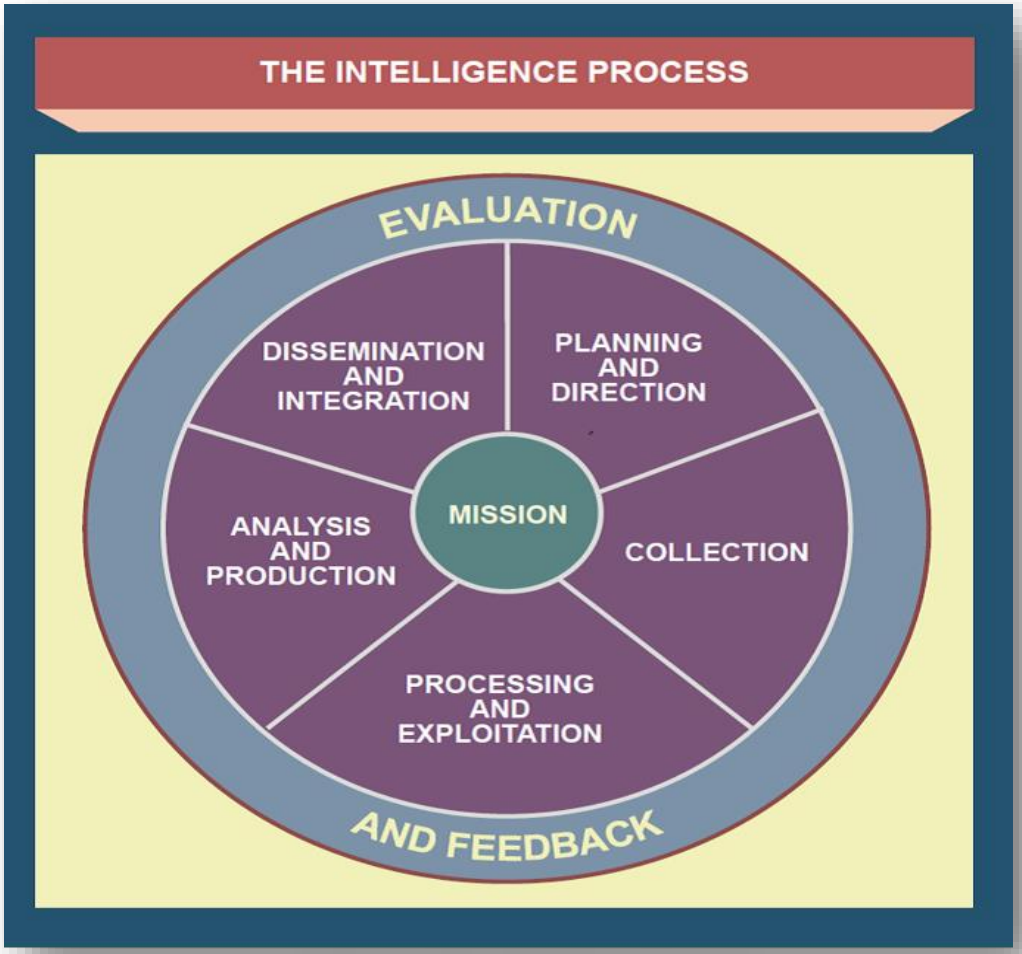
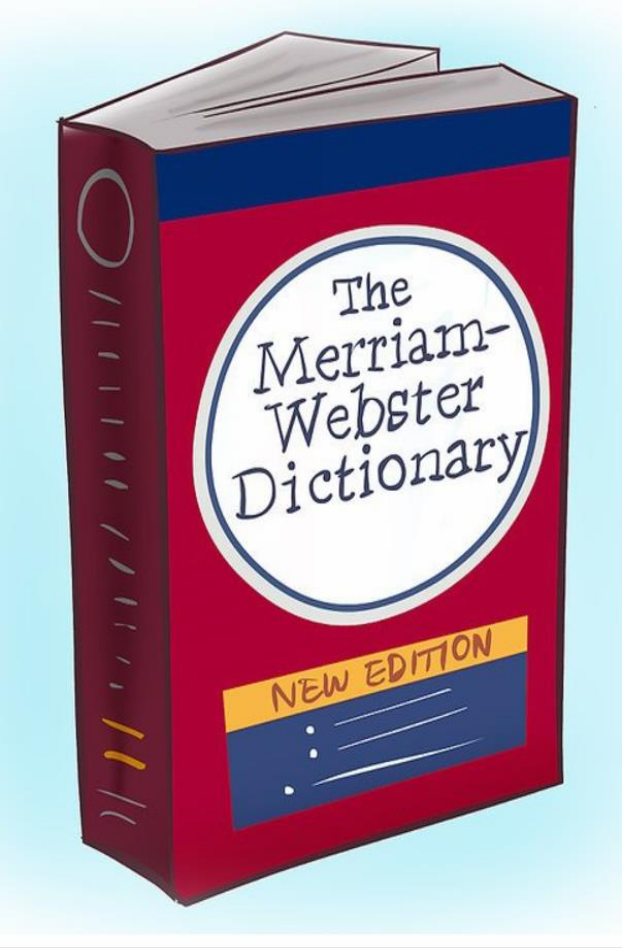


Figure 3. The Intelligence Process



WHAT IS THREAT INTELLIGENCE ANYWAY?

- BCBSNE CTI Program roles and responsibilities

Understand the operational environment
Analysis of current threats, attackers, methods and motivations. Contextualize security events as they relate to BCBSNE. Provide situational awareness

Provide indications and warning (I & W)
Used in the identification and prevention of vulnerabilities from being exploited, as well as informing operations of potential attacks

Support situation development
Intelligence support to incident response in the event of a security incident or breach – key role on IR team

Foster collaboration
Establish and build on relationships internal and external to BCBSNE. Enhance industry security information sharing

OUR GOALS & EXPECTED VALUE

Learn “What we don’t know”

- Who wants to attack us?
- How are they going to attack us? **PREPARE!**
- Do we already have info out there that we don’t know about?
- What is REALLY happening in Healthcare landscape?

Document & trend threats

- Use information for adjusting Security controls and strategy.
- Prioritize efforts & $dollars on REAL threats.
- Support monitoring processes with additional, actionable information.

Proof all the “bad stuff” is real

- Continued support for Security when we haven’t had any “breaches”.
- Justify spending and resources on preventative and monitoring controls.

HOW WE GOT STARTED…

1. Experience counts. Don't re-invent the wheel. Who knows how to do this?

2. Hire or consult with Government/Military SMEs
   - We hired from our military resource in Bellevue.
   - "Tell us what a program looks like."

3. Form **RELATIONSHIPS**:
   - Federal & Local Law Enforcement
   - Community Security/Intel Groups

Blue Cross Unique Advantages

- BCBSA – Blue Cross Blue Shield Association.
- 36 individual Blue Cross Plans cover 100 million people, nearly one-third of all Americans.
- BCBSNE has extremely supportive leadership.
- Legal & Liability assurances for sharing Intel information across plans.
- Support from multiple BCBS security programs and Intel resources…

WHERE ARE WE NOW?

1. Formally codified program and function that is fully integrated in normal business operations

   - Normal business process rather than an additional duty or ad-hoc activity

2. Established Concept of Operations and official procedures for each specific responsibility of the program

   - No single point of failure – program well documented

3. Repeatable operations – moving from reactive to proactive

WHERE ARE WE NOW?

1. Coordination and collaboration within the BCBS system
   - WannaCry and Petya/NotPetya
2. Information sharing both within healthcare and financial sectors
   - NH-ISAC and FS-ISAC
3. Information Security Roundtable (ISRT)
   - Bi-annual meeting sharing experiences and best practices

WHERE ARE WE NOW?

1. CTI Program functions touch every aspect of our business
   - Corporate Communications, Social Media, Customer Service, Patch Management, Desktop Service, Compliance and Ethics, HR
2. Informs decision making at every level
   - Daily updates for firewall blocks and bi-weekly Cyber Security Council reporting
3. Influences company-wide training and awareness
   - Supports creation of internal phishing campaigns and cybersecurity awareness training

WHERE ARE WE NOW?

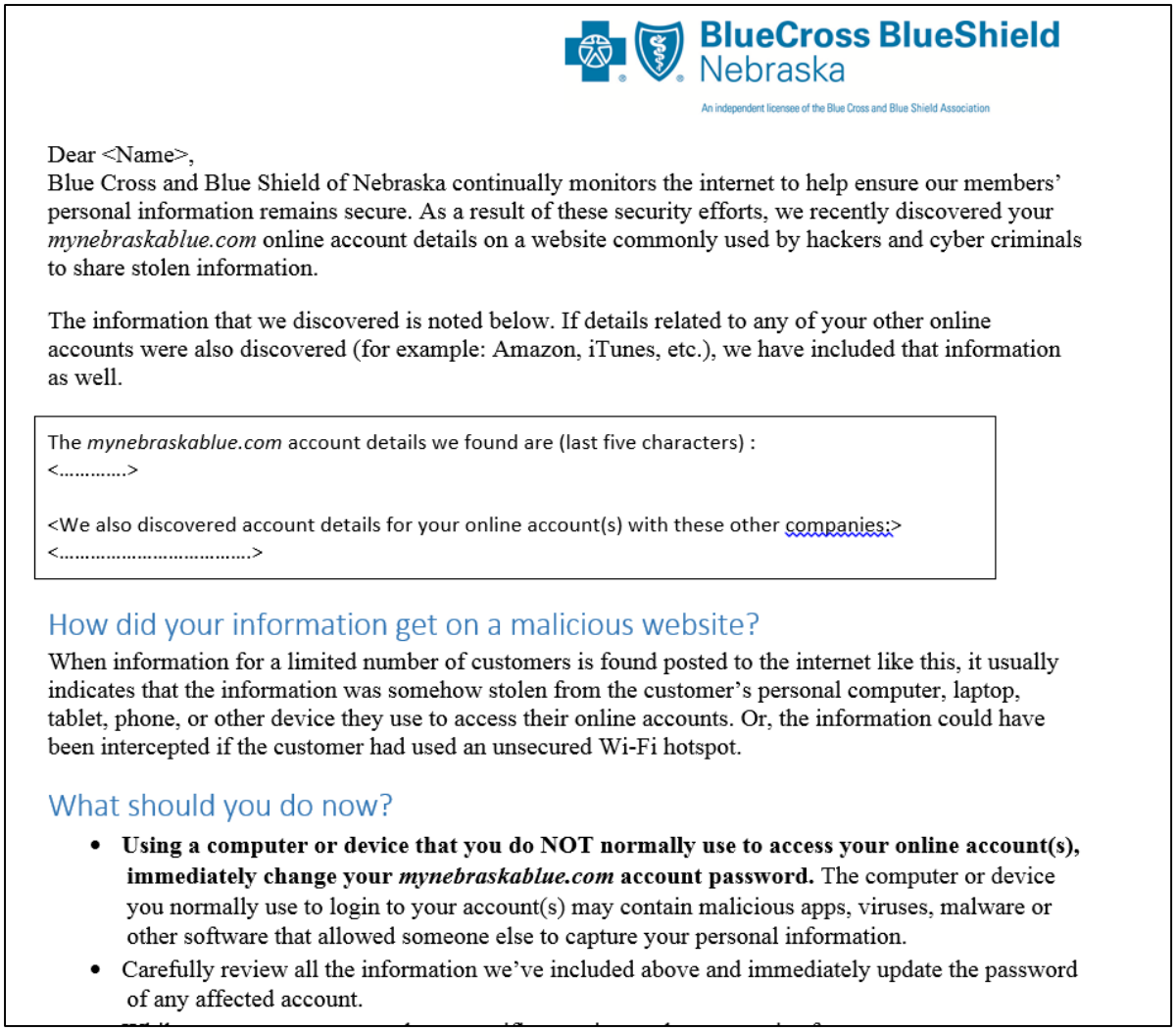
1. Capabilities and production

2. Domain and credential monitoring, web scraping and alerting, dark web monitoring

3. Threat notifications, critical advisories, intelligence summaries, and bi-weekly strategic reporting

WHERE ARE WE NOW?

Credential monitoring



BlueCross BlueShield Nebraska

An independent licensee of the Blue Cross and Blue Shield Association

Dear <Name>,
Blue Cross and Blue Shield of Nebraska continually monitors the internet to help ensure our members' personal information remains secure. As a result of these security efforts, we recently discovered your *mynebraskablue.com* online account details on a website commonly used by hackers and cyber criminals to share stolen information.

The information that we discovered is noted below. If details related to any of your other online accounts were also discovered (for example: Amazon, iTunes, etc.), we have included that information as well.

The *mynebraskablue.com* account details we found are (last five characters) :
<……>

<We also discovered account details for your online account(s) with these other companies:>
<……>

How did your information get on a malicious website?

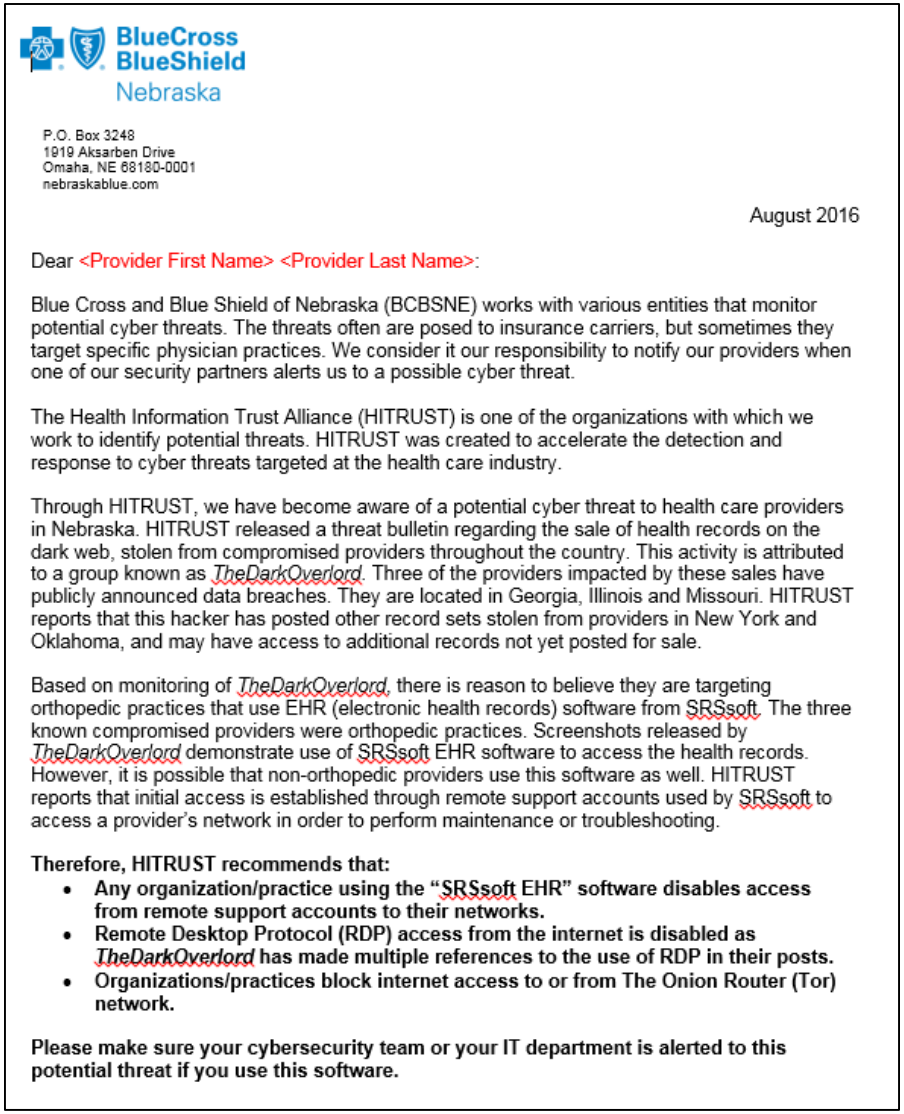
When information for a limited number of customers is found posted to the internet like this, it usually indicates that the information was somehow stolen from the customer's personal computer, laptop, tablet, phone, or other device they use to access their online accounts. Or, the information could have been intercepted if the customer had used an unsecured Wi-Fi hotspot.

What should you do now?

- **Using a computer or device that you do NOT normally use to access your online account(s), immediately change your *mynebraskablue.com* account password.** The computer or device you normally use to login to your account(s) may contain malicious apps, viruses, malware or other software that allowed someone else to capture your personal information.
- Carefully review all the information we've included above and immediately update the password of any affected account.

WHERE ARE WE NOW?

Threat notifications



BlueCross BlueShield Nebraska

P.O. Box 3248
1919 Aksarben Drive
Omaha, NE 68180-0001
nebraskablue.com

August 2016

Dear <Provider First Name> <Provider Last Name>:

Blue Cross and Blue Shield of Nebraska (BCBSNE) works with various entities that monitor potential cyber threats. The threats often are posed to insurance carriers, but sometimes they target specific physician practices. We consider it our responsibility to notify our providers when one of our security partners alerts us to a possible cyber threat.

The Health Information Trust Alliance (HITRUST) is one of the organizations with which we work to identify potential threats. HITRUST was created to accelerate the detection and response to cyber threats targeted at the health care industry.

Through HITRUST, we have become aware of a potential cyber threat to health care providers in Nebraska. HITRUST released a threat bulletin regarding the sale of health records on the dark web, stolen from compromised providers throughout the country. This activity is attributed to a group known as *TheDarkOverlord*. Three of the providers impacted by these sales have publicly announced data breaches. They are located in Georgia, Illinois and Missouri. HITRUST reports that this hacker has posted other record sets stolen from providers in New York and Oklahoma, and may have access to additional records not yet posted for sale.

Based on monitoring of *TheDarkOverlord*, there is reason to believe they are targeting orthopedic practices that use EHR (electronic health records) software from SRSsoft. The three known compromised providers were orthopedic practices. Screenshots released by *TheDarkOverlord* demonstrate use of SRSsoft EHR software to access the health records. However, it is possible that non-orthopedic providers use this software as well. HITRUST reports that initial access is established through remote support accounts used by SRSsoft to access a provider's network in order to perform maintenance or troubleshooting.

Therefore, HITRUST recommends that:

- **Any organization/practice using the "SRSsoft EHR" software disables access from remote support accounts to their networks.**
- **Remote Desktop Protocol (RDP) access from the internet is disabled as *TheDarkOverlord* has made multiple references to the use of RDP in their posts.**
- **Organizations/practices block internet access to or from The Onion Router (Tor) network.**

Please make sure your cybersecurity team or your IT department is alerted to this potential threat if you use this software.

WHERE ARE WE NOW?

Bi-weekly strategic reporting

BlueCross BlueShield Nebraska

Traffic Light Protocol: Green

Threat Intel Update 10 AUG 2017

- **Two dark web markets taken offline**
  - On 4 July, AlphaBay (AB) went offline and its creator Alexandre Cazes was arrested in Thailand
    - Largest online dark market in the world (servers located in Quebec)
      - 200,00 users and 40,000 vendors (10x size of Silk Road)
    - Existed for 2 years, totaling more than $2 Billion in transactions – major source of heroin and fentanyl
      - Sales from AB are linked to fentanyl overdose deaths in US
    - Cazes was found dead in his Thai jail cell a week after his arrest – "suicide" by hanging with a towel
  - On 20 July, Hansa Market went offline
    - US FBI coordinated with Dutch and other European authorities – waited to take down AlphaBay until Hansa servers were cloned on 20 June (located in Lithuania)
      - Dutch government operated Hansa for a month
      - Authorities rightly presumed a flood of users from AlphaBay to Hansa (AlphaBay Refugees)
        - Total number of users increased 8x after AB take down
  - Significantly limits dark web monitoring

Green - Recipients may share TLP: Green information with peers and partner organizations within their sector or community, but not via publicly accessible channels

Slide # 1

WHERE ARE WE NOW?

Intelligence report

BlueCross BlueShield Nebraska

Cyber Threat Intelligence Report

16-004 | 6/28/2016 | Traffic Light Protocol: **AMBER**

More Than 10 Million Healthcare Records for Sale

Executive Summary

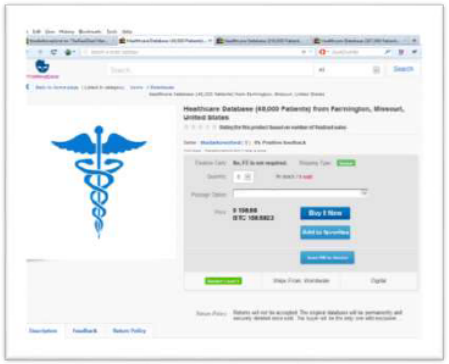
Recently, a hacker known as *TheDarkOverlord* placed 650,000 patient records for sale on the Dark Web. These records came from 3 separate medical clinics: one in Missouri, one in Georgia, and one in "Central/Midwest United States". The information available within the records varies, however all 3 contain PII. On 28 June, the same actor posted a database of 9.3 million records stolen from a healthcare insurance company in which the actor exploited the same RDP flaw. This database also includes PII. Based on our current analysis, we assess that Blue Cross Blue Shield of Nebraska was not targeted.

Key Points

- It is currently unknown if the RDP 0-day[1] used is one already exposed but not patched or if it is new
- Based on our firewall policies we do not have inbound RDP to any BCBSNE resources exposed to the internet.
- The actor is selling the records for 158 bitcoins (BTC), 635 BTC, and 317 BTC[2], respectively. The price for the data is significantly higher than most large record sales; actor states they are only selling to one buyer per data set
- *TheDarkOverlord* provided samples of data in an interview with deepdotweb, and based upon analysis of the samples, we determined with high confidence the identity of one provider
- We do not know the identities of the remaining two providers and the healthcare insurance company

Threat Detail

1. Healthcare database of 48,000 from Farmington, Missouri.



AMBER - Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.

COMPLIANCE AND ETHICS

Accomplishments

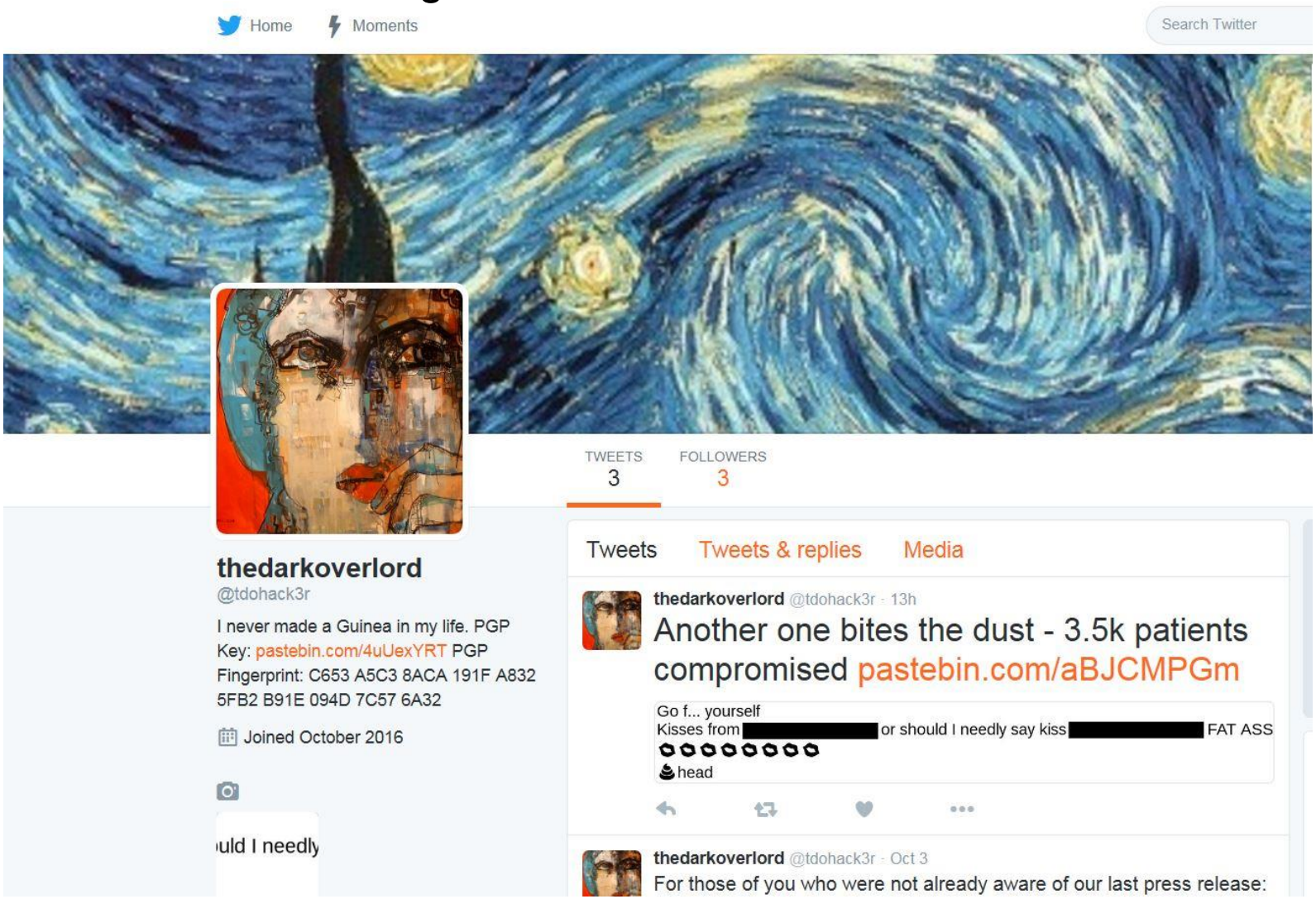
1. Provided intel that has started or assisted multiple Federal investigations, including confirmed arrests and prosecution

2. Identification of credentials for members and employees – also for several local businesses – allowing individuals to be notified

3. Research and analysis of 3rd party vendor risk above and beyond security evaluation

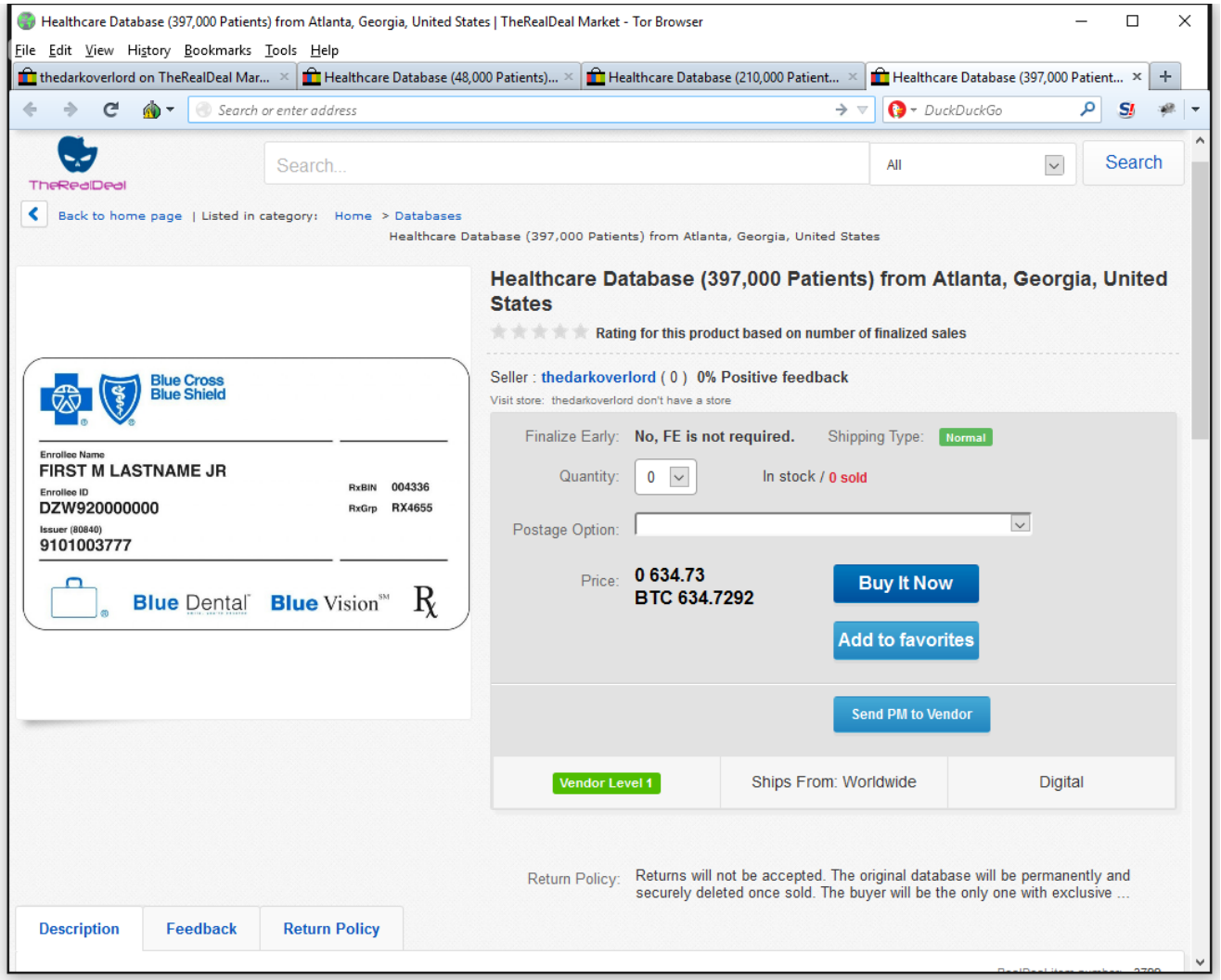
Accomplishments

TheDarkOverlord monitoring

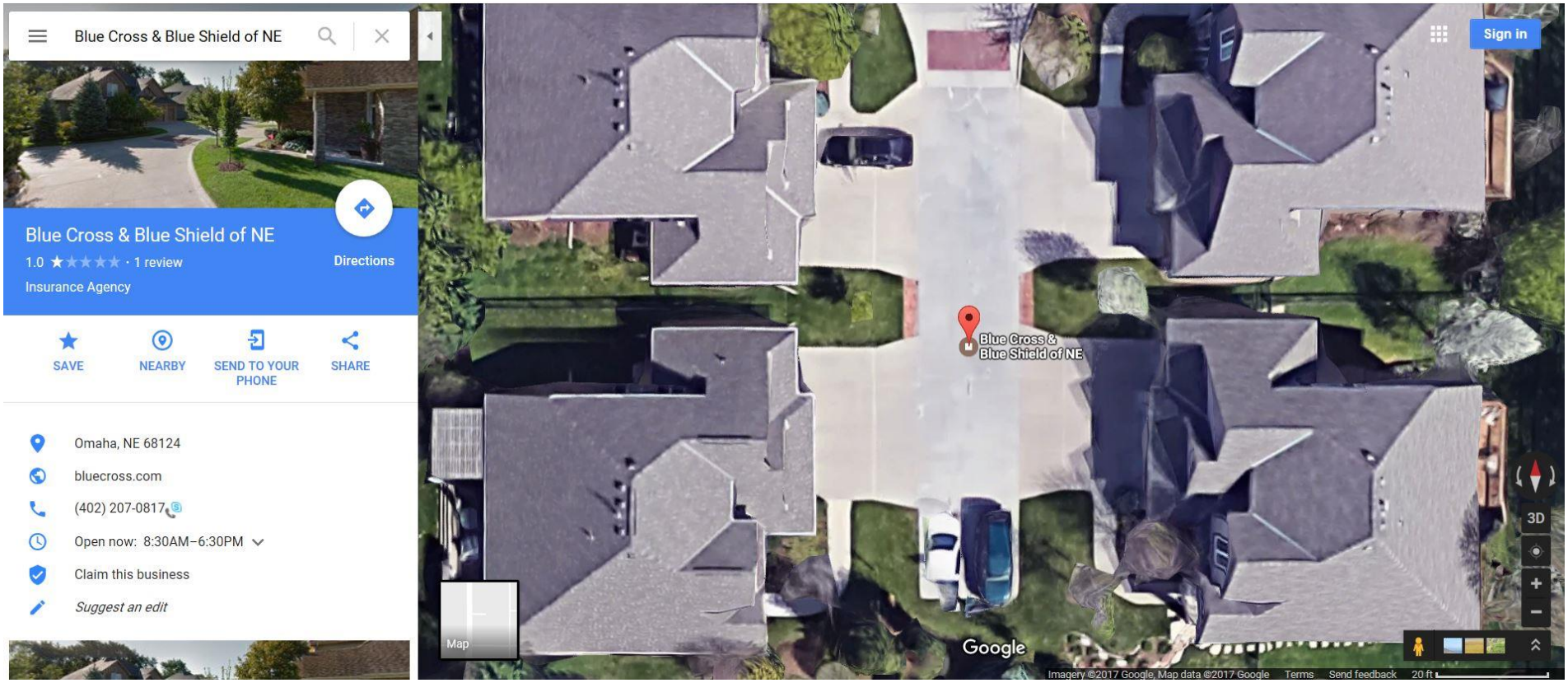


Accomplishments

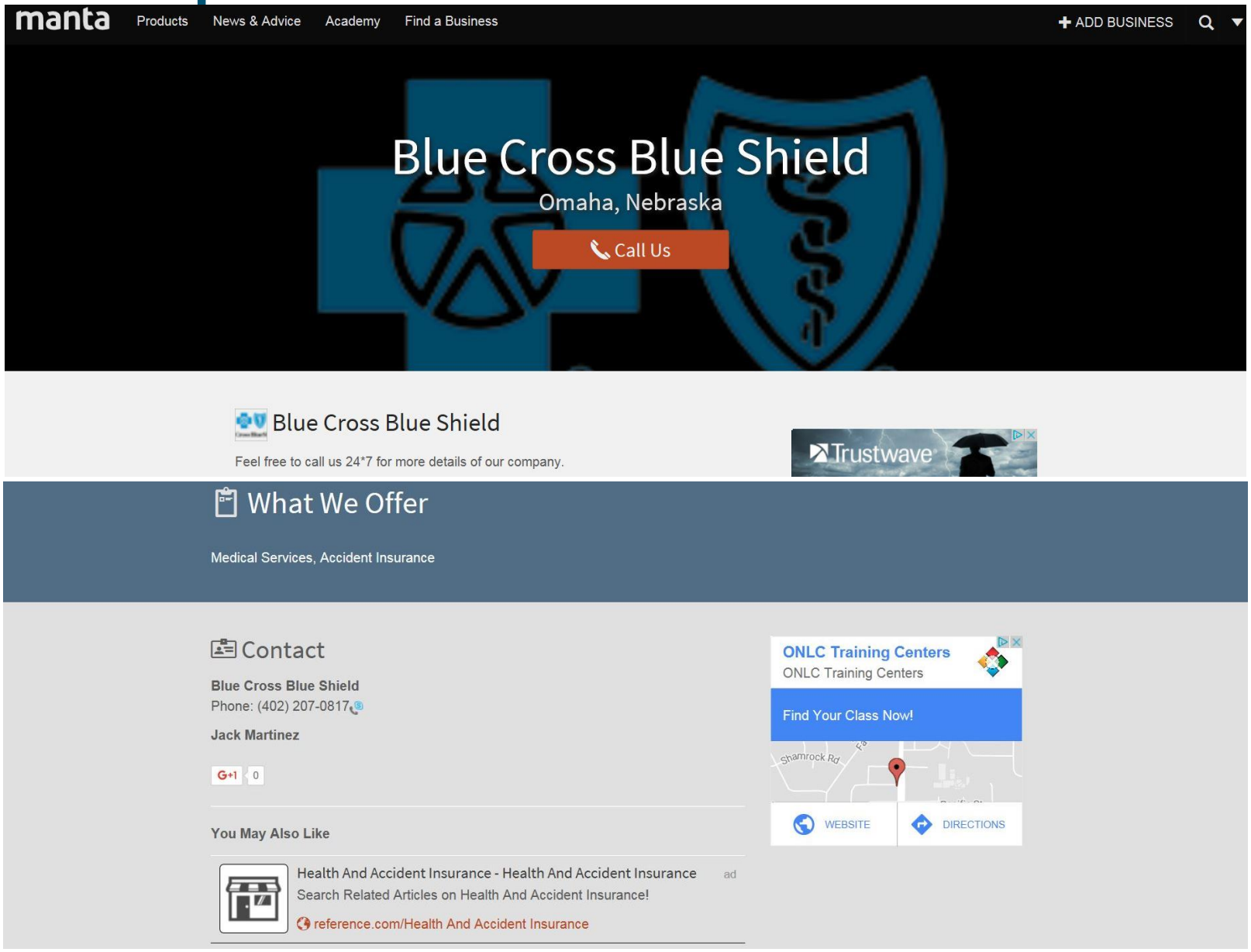
TheDarkOverlord monitoring



Accomplishments



Accomplishments



Accomplishments

Official Nebraska Government Website

NEBRASKA.GOV

All State Agencies | All State Services | Select Language |

PROTECT THE GOOD LIFE

Report Fraud

Home | About Us | Learn to Protect | Consumer News | Charities | Resources | Contact Us | Custom Searcl

Home / Consumer News / Blue Cross Blue Shield Imposter Scam

Blue Cross Blue Shield Imposter Scam

July 10, 2017

Lincoln–The Attorney General's Office received notice this morning that scam artists based in Florida are posing as Blue Cross and Blue Shield of Nebraska ("BCBSNE"). The scam artists are using fake Google and Manta listings bearing Blue Cross's logo and web address, along with bogus physical addresses in Omaha. Investigators employed by BCBSNE believe the scam is affiliated with an entity called Simple Health based out of Hollywood, Florida. When contacted by phone, the scam artists collect personal information and offer insurance plans well below market value. Simple Health victims have reported online that the company charges their credit card monthly, but never provides insurance cards or proof of coverage. They also make it difficult to cancel service.

Nebraska consumers should be wary of calling any telephone number other than one available on BCBSNE's official webpage in order to purchase insurance.

WANT TO GROW YOUR OWN PROGRAM?

Even without the Blue Cross Blue Shield family resources, there are pieces any organization can implement.

HOW DO YOU PROCEED?

- Understand your business and your risks.
  - Develop your CTI goals based on company business risks & culture.

- Don’t try to boil the ocean…
  - Don’t feel you have to figure it out on your own
    - Talk to as many peers, security community organizations, vendors, consultants to start understanding the concepts and methodologies.
  - Start with a foundation and build upon small successes.
    - Start with **relevant** information sharing organizations:
      - FREE…
        - » USCERT (United States Computer Emergency Readiness Team)
        - » Infragard (FBI and members)
        - » CISCP (Cyber Information Sharing and Collaboration Program from DHS)
        - » NIAC (Nebraska Information Analysis Center)
        - » MRAR (Midwest Regional Analyst Roundtable)

PROCEED TO NEXT STEPS…

- More focused/Automated information
  - Paid services:
    - ISACs (Information Sharing & Analysis Center)
      - FS-ISAC (Financial)
      - NH-ISAC (Health Care)
      - SIEM integration of feeds (STIX, TAXI, etc…)

- Commercial Products Utilizing Intel Input
  - If you have budget for **technology**:
    - Mandiant FireEye
    - CrowdStrike
    - Carbon Black
    - Ask your solutions provider about products and services!!!

STILL CLIMBING…

- Brand/Industry Monitoring Services/Processes
  - Internet Monitoring
    - Recorded Future$/IntSights – monitor internet and dark web for key words/phrases related to your business
    - Domain Registration monitoring
    - Pastebin (Pro service includes monitoring and take down)
    - Virus Total (Pro service includes intel reporting)
    - With the right talent, create your own!

- INTEGRATION!!!
  - SIEM Consolidates CTI Feeds and Services with Other Input
    - eMail, Proxys, Security Event logs, access logs, endpoint, vuln scan results, firewall events, etc.

WHAT ARE THE COMMON HURDLES?

COMMON HURDLES YOU MAY ENCOUNTER

- Legal departments freak out until you can educate them!!!
  - Concerns about information sharing with outside entities
  - Fear of liability if information appears to be advice or instruction

- May have difficulty with Sr. Mgmt/Exec support
  - Some of the value may be perceived as subjective
  - Some risks may be more image and reputation based than Cyber related.
  - CTI **consumption** and **action** takes budget for either **resources** or **technology** and often **both**.

Questions??