Bellevue Bank and Trust Cybersecurity Incident Report

Reported By: Lathan Birmingham **Date of Report:** 12/4/2022

Title/Role: Senior Cybersecurity Analyst **Incident No:** 123456789

Incident Severity: **Negligible:** □ **Minor:** ☒ **Severe:** 🟨 **Critical:** 🟥

TLP: **White:** □ **Green:** 🟩 **Amber:** 🟨 **Red:** 🟥

CYBERSECURITY INCIDENT INFORMATION

Date of Incident: September 17th, 2021 **Time of Incident:** 9:48 am

Incident Manager: Bruce Edwards **Title/Role:** SOC/CSIRT manager

Phone: (123) 456-7890 **Email:** edwardsb@bbtrust.com

Location: Bellevue Bank and Trust

Specific Area: Midwest

Incident Type: Ransomware

No. of Hosts Affected: 3 **Source IP Addresses:**

IP Address: 10.103.14.47
10.103.52.55
10.104.25.6 **Computer/Host:**

Operating Systems: Unknown **Other Applications:**

Incident Background

Bellevue Bank and Trust is a small credit union based in the midwest. BB&T uses Proofpoint for external email security. BB&T's SOC has been alerted by the FS-ISAC that several American and Canadian banks had seen an uptick in phishing related attacks with a few banks and other financial instituions reportedly suffering from a new variant of ransomware that so far had limited spread. The SOC and Threat Intelligence convened a conference call with server engineering, desktop services, the Bank's help desk, and business technology units to discuss the details of the FS-ISAC alert and ask for cooperation and vigilance in looking for and preparing for a ransomware attack.

Incident Description

10 employees of BB&T received an email with a malicious document. Of those 10 employees, 5 downloaded the file, 3 opened the file, and 2 reported the file. The Word document took advantage of CVE-2021-4044 MSHTML zero day. Patching had been disabled on the CIO laptop including EDR and Anti-virus updates. A new vulnerability in Proofpoint allowed the email to evade detection. Files stored locally on the laptops were unrecoverable as the bank would not be paying a ransom for the files. Some work was lost but the loss was not devastating to the employees or bank.

Events Timeline (2021)

Wednesday, September 15th

Evening	SOC detected phishing emails from crownpension@rosemoreinc.com to 150 employees. The email was a generic email asking the bank employee to click on the link to update their retirement account information. The email was not personally addressed to the employee and the link contained a drive-by download that attempted to exploit CVE-2021-30598 and CVE-2021-30599 which caused Chrome to download and attempted to get the user to open a word document that contained a malicious document containing an exploit against CVE-2021-40444.
4:30 pm – 6:00 pm	Emails received and blocked by Proofpoint. Security case is opened and closed after investigation reveals no infection or impact

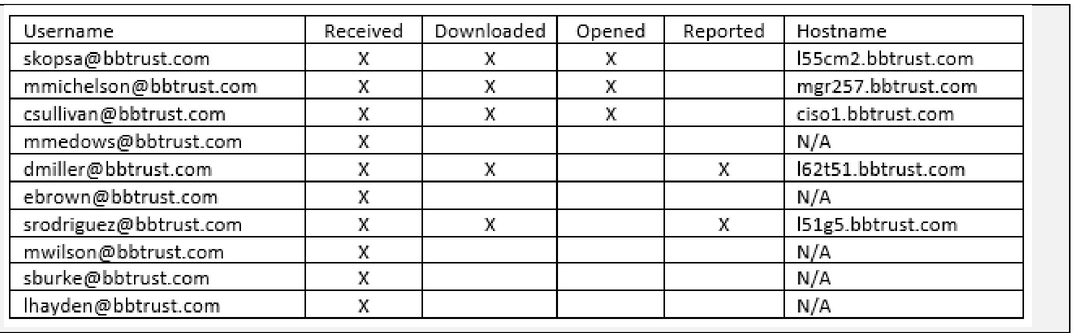
Thursday, September 16th

9:30 am	SOC recieves alert from FS-ISAC that there is a new variant of ransomware with limited spread targeted to financial instutitons
11:00 am	SOC and Threat Intelligenced had a call with server enginerring, desktop services, help desk, and business technology units to discuss FS-IAC alert and prepare for ransomware attak
10:00 pm	SOC recieves two EDR alerts from virtual desktop and back-office computer alerting for execution of .docx file named • **ATTN: Bank COVID-19 Response Update.docx** EDR tool blocked file from executing on both computers. SOC noted alerts and forwarded information to MSSP, who monitors bank from 11 pm – 8 am. Junior Analyst Sandra Williams opens a case with the following information: • **Word Document MD5 Hash: 5cb9cff7e12b6c1d8724ab8f8a10555e** She also records the following 2 events:
10:55 pm	vdi15a22.bbtrust.com 10.45.16.32 asmith
11:02 pm	lincolnbackoffice15.bbtrust.com 10.105.127.134 Jgarcia

Friday, September 17th

9:48 am	Mike Simms opns case and finds that MSSP scanned systems for docs matching MD5 hash with no avail. MSSP found email containing malicious documents sent to 10 bank emails from **phishing@uottawa.ca.** Only **asmith** and **jgarcia** opened the file before MSSP deleted hishing emails from user inboxes.

	Junior Analyst Mike Simms takes call from help desk employee Jordan Brands. Jordan reports 2 calls fom employees who have experienced a ransomware attack. They cannot access their email, local docs, internet, or corprate intranet.
	Proofoint did not block email, so all 10 recipients received the email
	The following information was recorded: l55cm2.bbtrust.com 10.103.14.47 skopsa mgr257.bbtrust.com 10.103.52.55 mmichelson
	Mike finds **skopsa** and **mmichelson** received the email from **lisa.trudell@genworth.com** with the attachment • **ATTN: Updated Bank COVID-19 Response Update.docx.**
	Mike hashes the file: • **Word Document MD5 Hash: dcc43f6872da3da500be2562cd0b2789**
	Mike asks Josh Pierce (SOC malware expert) to inspect file
10:26 am	Help desk calls SOC reporting multiple users cannot access important docs on the file system. Many file types have been renamed with .enc extension but when they are named back to their original extensions, they are corrupted.
10:45 am	CIO's secretary calls SOC because CIO's laptop is infeted with ransomware. CIO Charles Sullivan is demanding answer from SOC manager Bruce Edwards. The following information is logged: cio1.bbtrust.com 10.104.25.6 csullivan
10:52 am	SOC manager Bruce Edwards declares incident and convenes CSIRT and takes on role of incident manager. Phone conference call with CIO, CISO, and other important managers join call. Bruce asks SOC to join call as they are the expert of the CSIRT. Mike carries out the below tasks.
10:57 am	Mike runs command on EDR to disable the following computers from accessing the network: l55cm2.bbtrust.com 10.103.14.47 skopsa mgr257.bbtrust.com 10.103.52.55 mmichelson cio1.bbtrust.com 10.104.25.6 csullivan
11:01 am	Mike Simms delivers the following list of email addresses to JA Sandra Williams. skopsa@bbtrust.com, mmichelson@bbtrust.com, csullivan@bbtrust.com, mmedows@bbtrust.com, dmiller@bbtrust.com, ebrown@bbtrust.com, srodriguez@bbtrust.com, mwilson@bbtrust.com, sburke@bbtrust.com, lhayden@bbtrust.com
11:10 am	Sandra works with Exchange admin Kevin Silkwood to delete any email from lisa.trudell@genworth.com from all user inboxes. Sandra makes notes of the following table:



Username	Received	Downloaded	Opened	Reported	Hostname
skopsa@bbtrust.com	X	X	X		l55cm2.bbtrust.com
mmichelson@bbtrust.com	X	X	X		mgr257.bbtrust.com
csullivan@bbtrust.com	X	X	X		ciso1.bbtrust.com
mmedows@bbtrust.com	X				N/A
dmiller@bbtrust.com	X	X		X	l62t51.bbtrust.com
ebrown@bbtrust.com	X				N/A
srodriguez@bbtrust.com	X	X		X	l51g5.bbtrust.com
mwilson@bbtrust.com	X				N/A
sburke@bbtrust.com	X				N/A
lhayden@bbtrust.com	X				N/A

11:15 am	Mike finishes running query in bank’s endpoint visibility platform to search for files named • **ATTN: Bank COVID-19 Response Update.docx** • **ATTN: Updated Bank COVID-19 Response Update.docx** or hashes on endpoints matching • **5cb9cff7e12b6c1d8724ab8f8a10555e** • **dcc43f6872da3da500be2562cd0b2789** Mike hands off results to JA Lee Mullin.
11:25 am	Lee Mull deletes all files found.
11:28 am	Mike finishes querying Data Insights tool to find that cio1.bbtrust.com at 10.104.25.6 has accessed many files on the shares. This indicates that the CIOs laptop has been exclusively responsible for encrypting files. No activity since his laptop was isolated from network. **File shares report:** **Path...................................... # of files encrypted** **\\bankshare01\Finance........... 11380** **\\bankshare01\Architects .... 20342** **\\bankshare01\Executives ...... 9842** **\\bankshare01\IT................... 40376** **\\bankshare01\Sales.............. 2078** **Hostname: bankshare01.bbtrust.com** **IP Address: 10.15.0.25**
11:45 am	Mike updates CSIRT Manager Bruce. Mike works with Don Sanders from backup team to delete and restore directories/shares that were encrypted. This consists of completely deleting the directory from the file server and then restoring using the online backup system.
12:05 pm	Josh pierce finishes malware analysis and produces the following Indicators of Compromise (IOC): • **Domains** ○ yoursuperservice.com ○ zapored.com ○ arcnew.com ○ aerodx.com ○ avetoo..com ○ banolik.com ○ fangulf.com

	○ kuxizi.com ○ rosemoreinc.com ○ genworth.com ○ uottawa.com • **Email** ○ crownpension@rosemoreinc.com ○ phishing@uottawa.ca ○ lisa.trudell@genworth.com • **IP Addresses** ○ 142.234.157.164 ○ 108.52.12.100 ○ 104.244.154.112 ○ 102.195.100.204 ○ 192.111.149.58 ○ 205.221.186.24 • **MD5 Hashes** ○ 5cb9cff7e12b6c1d8724ab8f8a10555e ○ dcc43f6872da3da500be2562cd0b2789 ○ 0615d36031bf3da7ec68c5f2d46d4c04 ○ 784c7b3c4131cf0f8ac3d38feb1f378b ○ 0dedfa96043208167f8deb5cc652909a ○ 06122d9d3f5fd498c75e1894684d7659 ○ 7e7023a81ca8f0d86211899ca85a5ba8
1:36 pm	Mike finishes working with network services to add IOCs to DNS blocklists and temporary IP address firewall block rules using IOCs after an approval of an emergency change request.
2:35 pm	Analyst Sylvester Jones finishes forensic images of 3 compromised laptops and turns over laptops for reimaging by desktop services
5:45 pm	Server engineering finishes restoring directoires on the file share that were encrypted by the CIOs laptop.
9:27 pm	CSIRT closes incident WebEx and conference call
Monday, September 20th	
8:00 am	Desktop servces return laptops with a new image to the CIO and two employees who opened malcious file
11:00 am	CSIRT holds after-action conference call to share the following: • No new ransomware activity or phishing emails detected over the weekend • The Word document took advantage of CVE-2021-4044 MSHTML zero day • Patches for the MSHTML are available and were in the process of being deployed but KB5005573 had not been deployed to the three endpoints suffering the attack • Patching had been disabled on the CIO laptop including EDR and Anti-virus updates • A new vulnerability in Proofpoint allowed the email to evade detection. The vulnerability was fixed by Proofpoint over the weekend.

- Files stored locally on the laptops were unrecoverable as the bank would not be paying a ransom for the files. Some work was lost but the loss was not devastating to the employees or bank.
- No sensitive information, including customer information was exfiltrated or accessed as part of this attack.

Impact Assessment

The Word document took advantage of CVE-2021-4044 MSHTML zero day. Files stored locally on the laptops were unrecoverable as the bank would not be paying a ransom for the files. Some work was lost but the loss was not devastating to the employees or bank. No sensitive information, including customer information was exfiltrated or accessed as part of this attack.

Path	**# of files encrypted**
\\bankshare01\Finance	11380
\\bankshare01\Architects	20342
\\bankshare01\Executives	9842
\\bankshare01\IT	40376
\\bankshare01\Sales	2078

Hostname: bankshare01.bbtrust.com
IP Address: 10.15.0.25

Network Infrastructure Overview

Since the CIO downloaded and opened the malcious file, the hacker likely accessed the **Headquarters Distribution and Access Network**, where he then accessed the file server **bankshare01** and used the administrator privelages on the CIO's account to encrypt many files.

Forensic Analysis Overview

Analyst Sylvester Jones took forensic images of the 3 comprimised laptops.

Locations where malicious documents were found:

Hostname	**IP**	**Username**	**Path**
l55cm2.bbtrust.com	10.103.14.47	skopsa	C:\Users\skopsa\Documents
mgr257.bbtrust.com	10.103.52.55	mmichelson	C:\Users\\Documents
cio1.bbtrust.com	10.104.25.6	csullivan	C:\Users\csullivan\Desktop

After querying the data insights tool, Mike finds that the CIOs laptop was responsible for encrpying files in the file share **bankshare01.**

Josh pierce analyzes the malware and produces the following Indicators of Compromise (IOC):

- **Domains**
    - yoursuperservice.com
    - zapored.com
    - arcnew.com
    - aerodx.com
    - avetoo..com

    - banolik.com
    - fangulf.com
    - kuxizi.com
    - rosemoreinc.com
    - genworth.com
    - uottawa.com
- **Email**
    - crownpension@rosemoreinc.com
    - phishing@uottawa.ca
    - lisa.trudell@genworth.com
- **IP Addresses**
    - 142.234.157.164
    - 108.52.12.100
    - 104.244.154.112
    - 102.195.100.204
    - 192.111.149.58
    - 205.221.186.24
- **MD5 Hashes**
    - 5cb9cff7e12b6c1d8724ab8f8a10555e
    - dcc43f6872da3da500be2562cd0b2789
    - 0615d36031bf3da7ec68c5f2d46d4c04
    - 784c7b3c4131cf0f8ac3d38feb1f378b
    - 0dedfa96043208167f8deb5cc652909a
    - 06122d9d3f5fd498c75e1894684d7659
    - 7e7023a81ca8f0d86211899ca85a5ba8

Containment Actions

Mike runs command on EDR to disable the following computers from accessing the network:

l55cm2.bbtrust.com	10.103.14.47	skopsa
mgr257.bbtrust.com	10.103.52.55	mmichelson
cio1.bbtrust.com	10.104.25.6	csullivan

Sandra and Kevin delete the malicious emails from the 10 recipients.

Mike runs a query to search for files named

- **ATTN: Bank COVID-19 Response Update.docx**
- **ATTN: Updated Bank COVID-19 Response Update.docx**

or hashes on endpoints matching

- **5cb9cff7e12b6c1d8724ab8f8a10555e**
- **dcc43f6872da3da500be2562cd0b2789**

Mike hands off these results to Junior Analyst Lee Mullin.

Lee deletes all files found.

Findings/Root Cause Analysis:

Mike queries data insights tool to find that cio1.bbtrust.com at 10.104.25.6 has accessed many files on the shares. This indicates that the CIOs laptop has been exclusively responsible for encrypting files. This is not surprising as someone has given the CIO access to nearly all shares and directories on the file server.

Remediation:

Mike works with Don Sanders from backup team to delete and restore directories/shares that were encrypted. This consists of completely deleting the directory from the file server and then restoring using the online backup system.

Mike works with network services to add IOCs to DNS blocklists and temporary IP address firewall block rules using IOCs after an approval of an emergency change request.

Final Recommendation:

Since there are many different domains, IPs, file hashes and emails that were deployed to attack our network, the mandatory phishing awareness training will be impleneted for all employees. Eduating our employees is the only way to prevent this from happening again.

Our CIO will no longer have administrative privileges, as this is how all the files were able to be encrypted.

Definitions:

All definitions are taken from the NIST Glossary.

CSIRT (Computer Security Incident Response Team)
A capability set up for the purpose of assisting in responding to computer security-related incidents
NIST SP 800-61 Rev. 2

Encryption
The process of changing plaintext into ciphertext using a cryptographic algorithm for the purpose of security or privacy.
NIST SP 800-175B Rev. 1 under Encryption

Ransomware
A type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.
NIST IT Laboratory – Small Business Center | Ransomware

Phishing
A digital form of social engineering that uses authentic-looking—but bogus—e-mails to request information from users or direct them to a fake Web site that requests information.
NIST SP 800-115 under Phishing