CANTELLA & CO., INC.

November 16, 2020

New Hampshire Department of Justice
Att: Gordon MacDonald
33 Capitol Street
Concord, NH 03301

Re: Cantella & Co. Inc. CRD #13905/SEC #801-60841

Dear Mr. MacDonald,

I am writing to notify you of a cyber security incident which occurred at Cantella & Co., Inc. on August 25, 2020. This incident involved email threads which were used to entice recipients to open an attachment containing malware. Recipients of these malicious emails opened the attachments, believing them to be from a credible source, which in turn installed the malware. Unfortunately, this malware is very difficult to detect, and almost none of the antivirus products were able to do so at the time of the infection.

In total, we identified 23 infected computers across our organization. 13 of these computers were those of home office employees with the other 10 belonging to the financial advisors. All computers were wiped and rebuilt. In some cases, the only evidence of compromise was a temporary file. Regrettably though, some client's personal information may have been contained within these infected computers. While we have no evidence of any attempts to misuse private client information thus far, there is a possibility that client name(s), address, social security number, and other identifying information may have been potentially exposed.

We are not able to identify precisely how many clients' information may have been compromised. However, because we believe there is a possibility that at least some clients' information was exfiltrated, we are notifying all clients of the incident. We will be providing clients with complimentary credit monitoring for the next two years through Experian, assuming they opt-in per the instructions they will receive. In addition to this letter I am providing you with our Incident Report detailing the timeline of events. Upon review, if you have any questions please let me know.

Sincerely,

Sheelagh Howett

Sheelagh Howett
Chief Compliance Officer
Chief Risk Officer

Cantella & Co., Inc.
Malware Incident Report
For Events Beginning August 25, 2020
Confidential

Introduction

During this incident, our incident response was supported by two external partners, both of whom are cybersecurity experts well known to us. In both cases, the individuals are highly trusted sources and have government clearance at the highest levels. Both have access to highly sensitive, proprietary and/or confidential information that was shared with us on the condition that they not be attributed as the source. Accordingly, we have redacted certain identifying information in this report.

Timeline

August 25, 2020

3:11PM – The Compliance Department starts to receive suspicious emails, later determined to have a confirmed malware payload. Based on the emails trickling in, it was hypothesized that cMAX might have breached. A number of the emails were quoting exchanges with ComplianceMax, so the initial theory was that they were breached.

3:50PM – Upon further investigation, it became apparent that we had a broader cyber threat incident that was impacting, at a minimum, home office personnel in most or all departments. Discovery efforts were undertaken to determine the extent of threat.

4:10PM – Notification sent to the entire Cantella user base via email and text making them aware of the developing situation and advising against opening .doc attachments. Jay Lanstein, Yu Chu and Jake Bacher were on-site, with other team members off-site collaborating.

4:13PM – Suspicious .doc malware submitted to VirusTotal for analysis (https://www.virustotal.com/gui/file/90f1dd28de4726407f08f32ac09acad0517c8dafc58ab95471e7dbb14a4ec52a). At that time, only 7 of 68 engines flagged it as malware. Although Microsoft was shown as detecting it, a manual update and scan with Defender failed to detect it as malicious.

4:28PM Partner-A engaged for continuous assistance until 8PM when we engaged Partner-B.

5:10PM Suspicion from Partner-A is that the source is a compromise in IMAP, exploiting either a vulnerability in the software or an authentication loophole. This focused the investigation on the server-side, which turned out to be a dead end as it was ultimately found to be a client-side infection.

5:30PM The .doc files seemed to be the only vector for attack, as well as an indication that a message was malicious. Given that .doc is a little-used version of MS Office, we decided to ban .doc files from email gateways as a precautionary measure. This ended up being both the source and the result of the infection, so this step likely mitigated further spread and damage.

6:00PM – Based on the initial assessment, it is determined that none of the Cantella servers have been compromised.

7:50PM Partner-B engaged. Principal is not immediately available, but requested raw message source samples, IP address information, and a network tap so that he can investigate.
8:11PM We were still uncertain of whether it was client or server side, and we were looking for the root cause and/or indicia of infection. Called for more manpower from the IT team to investigate client machines. Matt O'Brien came into the office.
8:30PM – Backtracking from the emails being received, we observed commonalities in the emails to identify the most likely users who were infected. For example, if a malicious email contained a snipped of a prior legitimate thread sent by A to B, C and D, we came to suspect that one or more of those 4 users were infected. If we then found a malicious email quoting a thread between only B and C, we focused on B and C first.
9:00PM – I.T. Department reaches out to the first suspected users – [redacted] As of this time, the malware was undetected by Windows BitDefender. Recommendation from Partner-B was to make use of the Microsoft Autoruns tool to identify any suspicious entries.
9:35PM [redacted] machines were both found to have a suspicious task in Task Scheduler at almost the same time. This was the first definitive information that we had found evidence of the malware.
9:45PM – After researching the task, we determined that the computers were infected by the Emotet malware.
10:50PM – Reviews of computers belonging [redacted] are completed. Only [redacted] computer did not show signs of infection.
10:53PM [redacted]) contacted. His assistant, [redacted], was identified as potentially infected. As[redacted] machine was in the branch and turned off, plans were made to scan her machine first thing in the morning.
11:20PM – Documentation related to the Emotet malware indicates that it has the ability to steal credentials. Even though the primary distribution method is through emails, it can gain the ability through "command and control" servers to spread itself across the network utilizing brute force attacks.

Partner-B advises that:

1. The malware may be able to spread machine-to-machine over SMB in certain environments.
2. It steals every credential it can find.
3. Infected machines should be wiped – don't attempt to clean it.

11:25PM Neither Windows Defender nor Malwarebytes are detecting the malware. At this time, manually looking at Autoruns is the only reliable way to find it.
11:27PM Reaction to SMB spread is to take Windows shares offline. If the malware is able to spread this way, our shared drives could be infected, subject to ransomware, etc. Other network volumes only mounted on Linux-based systems are able to be left online because the Windows network has no access to those volumes.
11:30PM – Access to network shares is disabled for everyone.
11:50PM – Passwords for all home office personnel, outside of the I.T. Department is changed. Passwords are not shared with users until they are cleared. At this point, most users are not

going to be available, and our focus shifted to development of a remediation plan to be put into action for the morning.

8/26
1:02AM Detection and remediation plan distributed to IT team.
1:30AM Operations conclude for the night
6:00AM Operations resume
6:45AM Triage order of home office scanning established – Trading, Operations, Compliance, then other departments
7:45AM Email policy to block macro documents implemented
It is determined that Windows Defender now correctly identifies the malware. Scanning protocol is revised to reflect use of this tool as it is faster and does not depend on a detailed review of every item in Autoruns.
8:00AM – All hands I.T. Department meeting is held to layout tasks and responsibilities
8:20AM – I.T. staff initiates calls to Home Office to scan and identify compromised computers. Action plan includes use of Windows Defender to identify the malware, an update prior to running the scan, and that infected machines should be completely wiped and Windows reinstalled. Any infected users' passwords should be immediately reset as the assumption is that the passwords were stolen.
3:55PM Partner-A confirmed that their commercial product was failing to detect the malware.

Over the ensuring days, we reached out to every user and scanned every machine. This involved reliance on our internal asset tracking system, Reacher. We also built a custom report to identify which machines had been scanned and which remained outstanding. Finally, we received numerous tickets from users with screenshots of their scans, which needed to be reconciled with Reacher to ensure full coverage. We leveraged several home office employees outside of IT to assist our response by getting users connecting via remote assistance. Our response time was greatly assisted by these team members.

Damage Assessment

The attack involved exfiltration of legitimate historical email strings from Outlook users, which were used to entice others to download and run the malware. For example, if a user sent a message to 3 others, the malware would extract that and re-deliver it to one or more of the recipients with a malicious attachment.

We are unable to determine if attachments were also exfiltrated from the original email strings, but it is reasonable assume that they were. It is reasonable to assume that PII was in at least some of the emails, as many of the emails were internal and therefore deemed to be secure. While we are not aware of any attempts to misuse this PII, it is possible.

Our intelligence sources indicate that the malware's initial payload is to spread laterally, and to steal credentials. In other instances where the malware was not rooted out, victims had other

malware installed, including ransomware. We did not find any evidence suggesting that this occurred in our case.

There were a total of 23 infected machines - 10 home office computers and 13 advisors. All were wiped and rebuilt. In some cases, the only evidence of compromise was a temporary file. While we suspected that was the result of a user forwarding a suspect email to IT for review, we nonetheless wiped those machines out of an abundance of caution.

Home office users: [redacted]

Field users: [redacted]

Damage Control

During this incidence, the following technical process were implemented and/or existing technical policies were adjusted. Most of these policies are permanent to prevent Office macros from being used as an attack vector in the future:

- Firewall policies were modified to drop traffic to email systems that contained attachments with the ability to execute code.
- Firewall was configured to decrypt SSL/TLS-based email traffic to further analyze traffic for malicious content
- Temporarily, the configuration for email systems was changed to drop all .doc attachments regardless of content.
- The macro detection module within the anti-spam software was enabled to identify and drop files containing macros

Challenges Experienced

- We implemented an email block on Microsoft Office macro documents in June 2020, but the mail server software did not properly identify these documents as containing macros.
- We did not have the technical ability to identify compromised machines initially. We were unable to find any reliable tools in the early hours of the attack, and had to perform manual reviews.
- We initially requested screenshots of Windows Defender scan results from remote users. We did not receive consistent screenshots (e.g. some users just emailed to state their scan was clean), and did not receive consistent results (e.g. some users did not treat the request as urgent, or pushed back on using Windows Defender as opposed to other anti-virus software).
- Not having everyone available in a physical war room led to some instances of members following outdated processes. This was especially in the early hours when the plans

were quickly evolving in response to new information. The physical separation led to some disconnect in communication within the team.

- Internal strategy to handle and make calls could have been better structured.
- Utilizing multiple effort tracking tools (Trac, Reacher and Portal) was confusing and led to too much time determining next steps rather than completing scans.
- Raymond James imposed a mandatory password change on Friday, August 28 with very short notice. On Friday at 3PM ET, they then locked out all users, even those who had changed their passwords. They required a screenshot from each user in order to unlock the accounts, which required the team to redo work. In instances in which an IT member viewed scan results through screensharing, we had not been collecting screenshots. This new requirement led to confusion among users who though they were cleared, and additional work.
- Not everybody's cell phone numbers were populated in the database. In addition, some users had not provided updates when their cell phone numbers changed. This reduced the rapid response to text message alerts. In addition, we had launched the text message alert system on the morning of August 25, and had not yet notified users that we would leverage text messages for alerts. This caused some users to doubt the legitimacy of messages we sent.
- Existing efforts to warn email recipients with in-body alerts ("CAUTION: This email originated from outside the Cantella Organization. Exercise care with message content. Do not click on links or open attachments you were not specifically expecting unless you validate with the sender and know the content to be safe"). These warnings were overlooked or ignored and would have prevented infections had that not been the case. However, several users reported that the warning deterred them from clicking on the attachments.
- Various legitimate companies employ automated process to send out subscription emails. The attackers also employed similar automated process of sending out emails over Non-RFC compliant SMTP. We could not block all attacks without impacting legitimate email traffic.

Areas identified for Improvement

- Review our email systems' antivirus configuration
- Enhance existing password reuse testing to include reuse of characters e.g. August01! and August02!, and to utilize dictionary checks. Prohibit common terms such as Cantella from appearing anywhere in the password.
- Have an internal policy requiring everyone to share their cell phone numbers and to make I.T. aware of any changes in the number, similarly to updating information with HR.
- Test the text message system regularly to ensure that users are aware of it, and will respond appropriately to any alerts of any kind.
- Conduct regular cyber security training for home office and advisors
- Disable MS Office macros on computers as a standard policy, and add this verification to annual checkups

- Feature enhancements to Reacher :
    - Add a check for macros being disabled
    - Add more verbose audit trail (log deleted assets, date/time stamp each change)
    - Modify MAC address fields to be mandatory (to ensure reliable identification of assets)
    - Flag incomplete Reacher profiles
    - Add machine location (e.g. home, seasonal home, office, etc.) - we encountered cases where we were trying to get an advisor to scan a machine that was located in a seasonal location and had not even been used. We could have saved time had we known this information.
    -
- Investigate third party technologies and tools to identify and/or block compromised users (i.e Cortex, Palo Alto, Mimecast)
- Review enhancing cybersecurity posture by having anti-virus, anti-malware endpoint software that would allow insight into the remote computer system, as well as enforcing standardized software.
- Review extending log retention period from four weeks to eight weeks across all email systems.
- Investigate impact of dropping Non-RFC compliant SMTP traffic on the firewall
- Add additional documentation of infection protocol
    - Remove ethernet cable
    - Place machine in airplane mode
    - Hold off on wiping machine until all evidence is collected
    - Process to ensure full wipe is completed
    - Reset passwords for all user accounts, as well as any group/department accounts the user had access to
- Create documentation for emergency changes
    - Macro documents
    - Decrypting email traffic
    - Breaking backup mirroring relationship
    - Taking Windows shares offline