vcpi

November 18, 2019

To Our Valued Client:

We regret to inform you that our business was attacked with Ryuk encryption ransomware spread by TrickBot virus.

Current Status and Next Steps

We have isolated our production systems from the internet. We estimate 20% of our servers are affected by the virus.

We are executing a plan to scan, using a virus-specific software application, individual Microsoft Windows servers to either:

(a) verify the server is not infected; or
(b) verify the server is infected and then restore the server

before installing the servers into newly created network segments, connecting to the internet, and placing into production for your access. We don't currently have an estimate of the time necessary for this work effort, as it will be based on the number of affected servers.

We are prioritizing servers that provide Active Directory access, email, eMAR, and EHR applications.

We will be communicating status updates often and transparently, and, in preparation for service restoration, recommending to you the most efficient manner for your users to regain authenticated access.

Background

We quickly were alerted by our monitoring systems to the spreading of this virus, and we officially invoked our documented Incident Response And Management Process (IRAMP). We contacted our cyber security insurance policy provider, Beazley, and were then connected to Lodestone Security. Lodestone are experienced cyber security incident response experts, and they have been leading our team of engineers with their tools and our IRAMP. We are feverishly working, but careful restoration will take time.

Attached please find detailed notes and Frequently Asked Questions (FAQs) we have prepared thus far.

We appreciate your understanding, patience and collaboration as we get through this unfortunate incident together. We pledge to be transparent and stand ready to communicate with you. Our cellphones and personal email addresses are below. We are working nonstop with our employees, clients and experts to put this incident behind us as soon as possible.

With gratitude,

Karen Christianson
CEO
vcpi
karen.christianson@gmail.com
cell (608) 712-1165

Zachary Koch
President
Zachary.A.Koch@gmail.com
cell (414) 530-6087

We focus on technology so you can focus on care.

November 19, 2019 6AM

Current Situation (as of 6am Tuesday November 19th)

Overnight we identified servers that are not infected and that will be introduced into production, beginning today, for client access.

We are checking the new environment a final time to ensure there is no viral corruption before client access.

The target today is to put as many servers into production for client access as possible, with email and EHR applications the top priority.

We will update again at 10am.

November 18, 2019 10PM

Current Situation (as of 10pm Monday November 18th)

The work detailed in the previous update is progressing at this time and scheduled through the night.

We have work continuing through the day and night on 12-hour shifts of resources.

We will update again at 6am.

<u>November 18, 2019 6PM</u>

Current Situation (as of 6pm Monday November 18th)

The final two core domains are restored and we are working through password resets on those domains at this time.

Once these password resets are made, we will turn on internet connectivity to our Milwaukee datacenter.

We are working diligently to restore hosted Microsoft Exchange email and Microsoft Office/365 with a goal of Office/365 into production by tomorrow morning.

We have successfully restored multiple client system servers in our "sandbox" network segment, including the validation of successful data restoration from our Milwaukee data backup.

For quality and speed of server restoration, we are documenting the process for:

(a) Adding the Lodestone software application as an additional detection mechanism for this virus to each server to be restored; and

(b) running a scan to verify the server is virus-free.

Lodestone Security has been active today in gathering forensic evidence related to this incident to analyze root cause

We will update again at 10pm.

<u>November 18, 2019 2PM</u>

Current Situation (as of 2pm Monday November 18th)

We have 3 core domains in total that need to established to be complete with step #2 below; the principal core domain is successfully complete and that enables us to proceed to step #3; and the other two remain to be completed and will be completed in parallel with step #3 activities, which have begun.

After the other two domains are complete, we will reset all passwords in those three domains.

Internet connectivity to our Milwaukee datacenter is being restored and finishing the other two domains is expected to be complete in the next hour or two.

We have prioritized the client and application restoration work, which has begun. Progress and completion on this aspect will be communicated directly to the restored clients per application. When we understand better the time necessary for this stream of restoration work, we can be more communicative with estimated timeframes.

Progress is being made on our hosted email service restoration; the workload to do so is significant; when internet connectivity to our datacenter is restored we will expand the resources working on this aspect with remote engineers.

We will update again at 6pm.

November 18, 2019 10AM

Current Situation (as of 10am Monday November 18th)

We are on target with our estimated progress from the last update.

The new v-center environment of step #2 below is complete.

Everything with regard to AD and DNS is staged to be restored; we remain confident this step #2 will be completed in its entirety by noon central time.

We have begun step #3 with regard to restoring specific servers in a “sandbox” (i.e. nonproduction) environment for verification that they are virus-free and data has been restored. We anticipate confirmation that our restores are working as expected by the next update (2pm).

We continue to communicate with as many clients as possible through various means.

As our incident response progresses, we will share more estimated timeframes based on our early restoration experiences.

We will update again at 2pm.

November 18, 2019 6AM

Current Situation (as of 6am Monday November 18th)

The high-level summary of our 3-step incident response critical path is to:

(1) Build a new network (complete);
(2) Restore v-center, Active Directory (AD), and DNS (expected completion this AM);
(3) Restore client application virtual and physical servers (dedicated email team with remaining incident response staff working to restore in priority: Client EHR, eMAR, Citrix, and financial applications)

Overnight we worked to restore our v-center environment; we are not yet done but making steady progress. We are currently, in parallel, restoring Active Directory (AD) and DNS. Those two efforts are necessary in order to begin our other, more visible and client-impactful, restoration efforts.

We have duplicate backup data in Milwaukee and Denver datacenters, and have moved our Milwaukee backup data into the newly created network environment. We have confirmed we have access to this backup data in both locations.

We estimate at this time 20% of our servers have been infected and need to be restored (virtual servers). Approximately 100 physical servers need to be rebuilt, and we are gathering additional resources for that labor-intensive effort. The other servers need to be verified clean by the software application from Lodestone; and brought-up in the new network environment.

As our incident response progress begins to report visible progress of production systems (the 3rd phase above), we will communicate estimated timeframes for client application access.

Our hosted phone system for clients is in production and fully operational. Our vcpi internal wired phones are operational. ServiceNow is operational, but our inbound phone lines are not fully operational, so our third party answering service is taking calls and we are calling back users. All hands (non-engineers) in our company are calling back users and otherwise communicating with our clients.

We have restored internet access to most client corporate networks (client guest networks were unaffected).

We have gathered forensic information and have contacted the FBI, who will be onsite today to begin their investigation.

We will again update at 10am.

November 17, 2019 4PM

Sequence of Initial Events

Monitoring solutions at vcpi observed abnormal activity on our internal network around 1:30 am and alerted the 24/7 support team, who in turn alerted on-call members of the engineering team.

At approximately 3:30 am our engineers determined that the network was being subjected to a ransomware attack, and they began to power down affected servers.

At approximately 6:30 am, we officially invoked the vcpi Incident Response and Management Process (RAMP), which was being followed unofficially.

At around 9am we called our cybersecurity insurer's hotline, and they immediately provided Joshua Dann from Lodestone Security to be our Incident Response Lead. Lodestone Security has been assisting with our team's containment and remediation efforts. Along with Loadstone Security personnel, we are on a 24x7 rotation of personnel, and are working through this incident nonstop. (www.lodestonesecurity.com/about-us).

Current Situation (as of 4pm Sunday November 17th)

While our investigation is ongoing, we believe that multiple servers in our datacenter environment may have been affected by Ryuk ransomware, which may also include the TrickBot virus.

Our Active Directory (AD) servers are included in the affected server number.

We have isolated our datacenter from internet connectivity in an abundance of caution. We are treating every Microsoft Windows server and endpoint as if it is infected. Our networking switches are brand-new, and other networking devices are being checked to affirm the currency of their patching.

We have a segmented network pre-established to act as a staging area in which we will restore Microsoft Windows servers and confirm cleanliness with a tool recommended to vcpi by Lodestone Security. After confirmation in our staging area, our servers will be placed into new network segments and then into production.

We do not know at this time if any client data has been compromised. As part of our Incident Response, Lodestone Security will be performing a forensic analysis to determine if any data was exfiltrated, but at this point our primary concern is mitigating the impact of the incident and getting our clientsfully operational as soon as possible.

Frequently Asked Questions (FAQs)

Q: When will I have access to my systems hosted by vcpi?

A: We do not have an estimate at this time. We are working diligently, nonstop, without resource constraint, according to our documented plan, and with experienced expert leadership. We need to ensure the integrity of the new environment. We are prioritizing critical vcpi infrastructure (including Microsoft Exchange email system) and electronic health record (EHR) software.

Q: Do you know how this happened?

A: We have been learning possible root causes, but our focus has been on restoring client systems. We will be performing root cause analysis with Lodestone Security at the appropriate point in time. We plan to share this information with our clients.

Q: Could this have been prevented?

A: This is part of our root cause analysis to be performed. We take our responsibility for your systems seriously and will be transparent with this information.

Q: Can you promise this type of pervasive incident will not happen again?

A: Unfortunately, no. The potential for this type of incident is revealed by our clear-eyed preparation, documented planning, readiness, investment in experienced experts, and cyber insurance policy.

Q: Has this incident resulted in the access or acquisition of any of our data?

A: We intend to conduct a full forensic investigation that will examine that issue, and we will let you know the results of that investigation. Right now, however, our focus in on mitigating the impact of the incident and getting our clients fully operational as soon as possible.