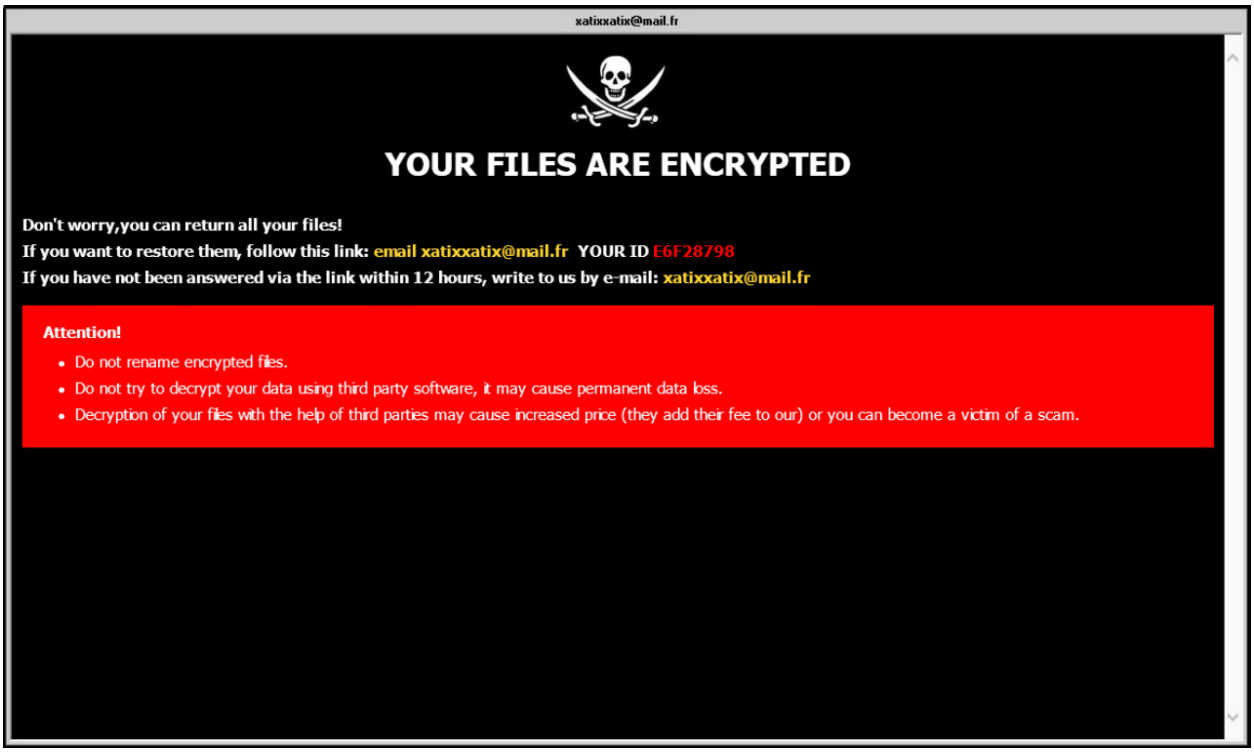
TVCC Ransomware Attack

August 26, 2020



Final Report and Details

TVCC Ransomware Attack

On Wednesday Aug. 26th at 5:05 AM, TVCC was hit with a well-known ransomware known as Dharma. Dharma and its variants have been around for four years and now has taken advantage of the COVID-19 situation by attacking Internet-facing systems using RDP and encrypting SMB files.

How did we get attacked?

On Friday Aug. 21, the IT department put in production a new VMware View server to run our Virtual Desktops (VDI). This single server was designed to replace two older servers which needed upgrades and had an IP address of 198.60.240.105.

This server was put into production without all the system security patches, and without the college endpoint security software system known as “Cortex”.

Unfortunately, at the same time the server was brought online, the college’s firewall was changed to allow the Remote Desktop Protocol (RDP) to connect to internal campus addresses from the outside public Internet.

Our after-incident research has not established how many individuals may have been attempting to penetrate TVCC’s network – in general, we know that there are always individuals and organizations on the Internet who are consistently testing public networks in an attempt to spread viruses or ransomware, or to gain access to sensitive personal information that can then be sold in some of the shadowy “black markets” which exist on the Internet. There may have been multiple individuals probing TVCC’s networks, or it may have been a single bad actor – we still don’t know. Regardless, at least one individual must have scanned our open network ports and found the open RDP access to the new server.

After several days of testing our systems, the remote hacker discovered a valid username and password to access this new server. They were able to discover the general user account the Security department used for all TVCC security staff to access the college computers. Another service account called

"Quantum" was discovered by the attacker and this was the account used to encrypt the files. The Quantum user account is used by the backup system at TVCC to copy all files every night to the backup systems.

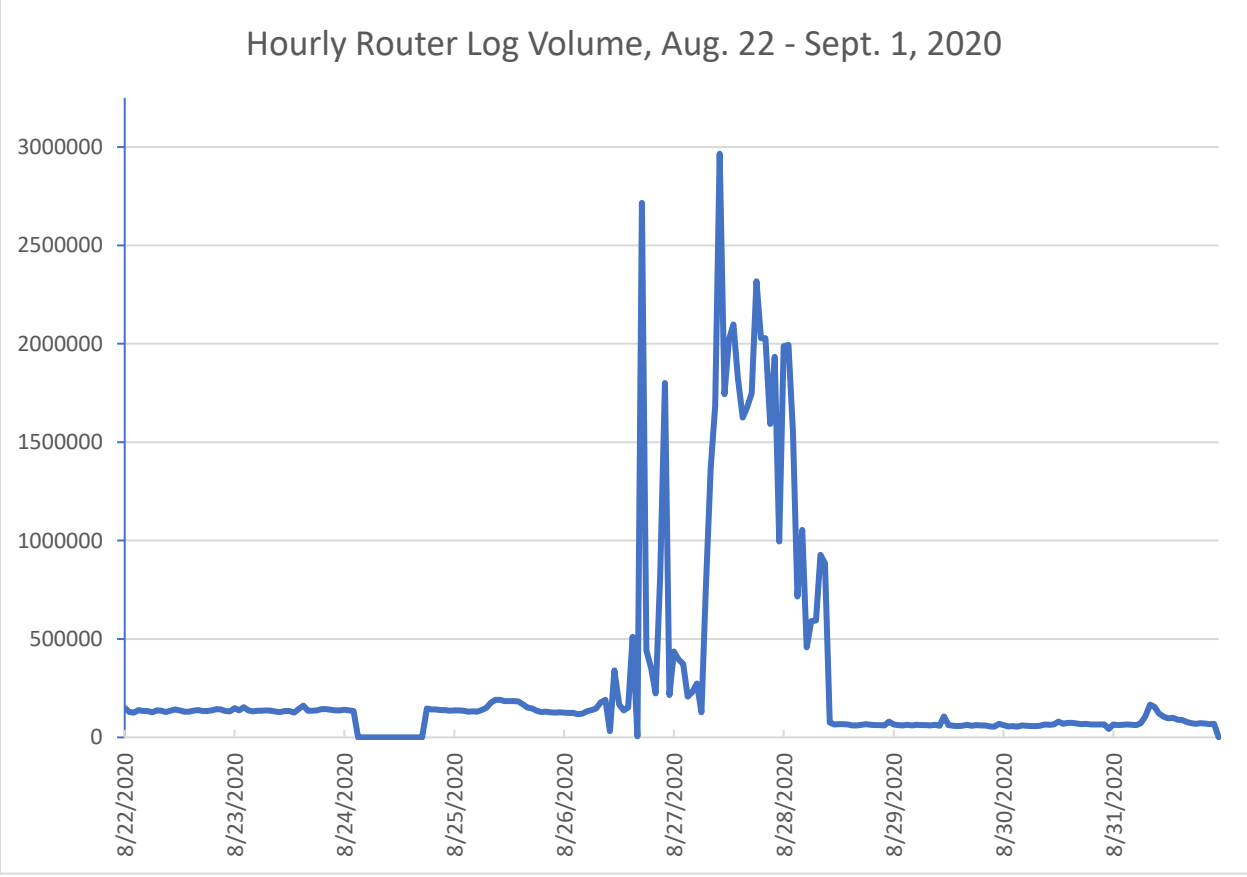
Around 6:00 AM the IT paging system started notifying the IT department that a couple of the webservers had gone offline. This triggered IT staff to research the affected servers and by 6:30 AM we discovered we had been hit with Ransomware. At this point our first reaction was to start disconnecting all servers and workstations from the network, and by 8:00 AM everything had been shut down and we began to follow our drafted Incident Response plan.

Mistakes which contributed to the attack

- We decommissioned an important gateway server for VDI
- We went live with a new server before it was patched and was configured with proper end point security software
- We opened the firewall with the wrong ports

Review of the Log Data

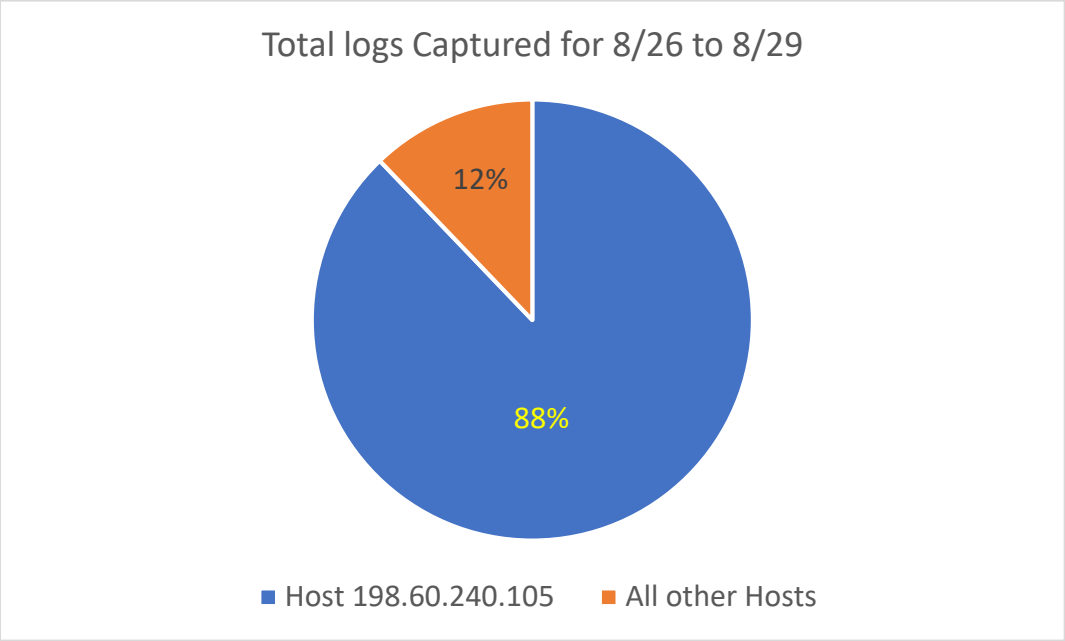
The following graphs give a visual representation of the amount the log traffic generated to our network before, during and after the attack.



Prior to 8/26, logs per hour averaged about 127K per hour. For three-day period from 8/26 – 8/28, we averaged 906K log records per hour. There were two major spikes – 2.7 million in a one-hour period on

8/26, and 2.9 million on 8/27. For the entire period of time, we have 76,833,228 records (and we lost a significant amount of 8/24 records due to a logging failure).

Logs captured for the new server that was deployed compared to all other servers.



During the three-day period from 8/26 to 8/29, the address 198.60.240.105 was the focus of the attack; there were 46,895,200 logs generated from traffic to that address, while there were only 6,490,996 records generated for **all** other destination addresses during the same time frame. During the three-day period from 8/26 to 8/29, 5,501 external addresses tried to talk to 198.60.240.105. The top 10 addresses were from the US, Finland, Singapore, Hong Kong and the United Kingdom.

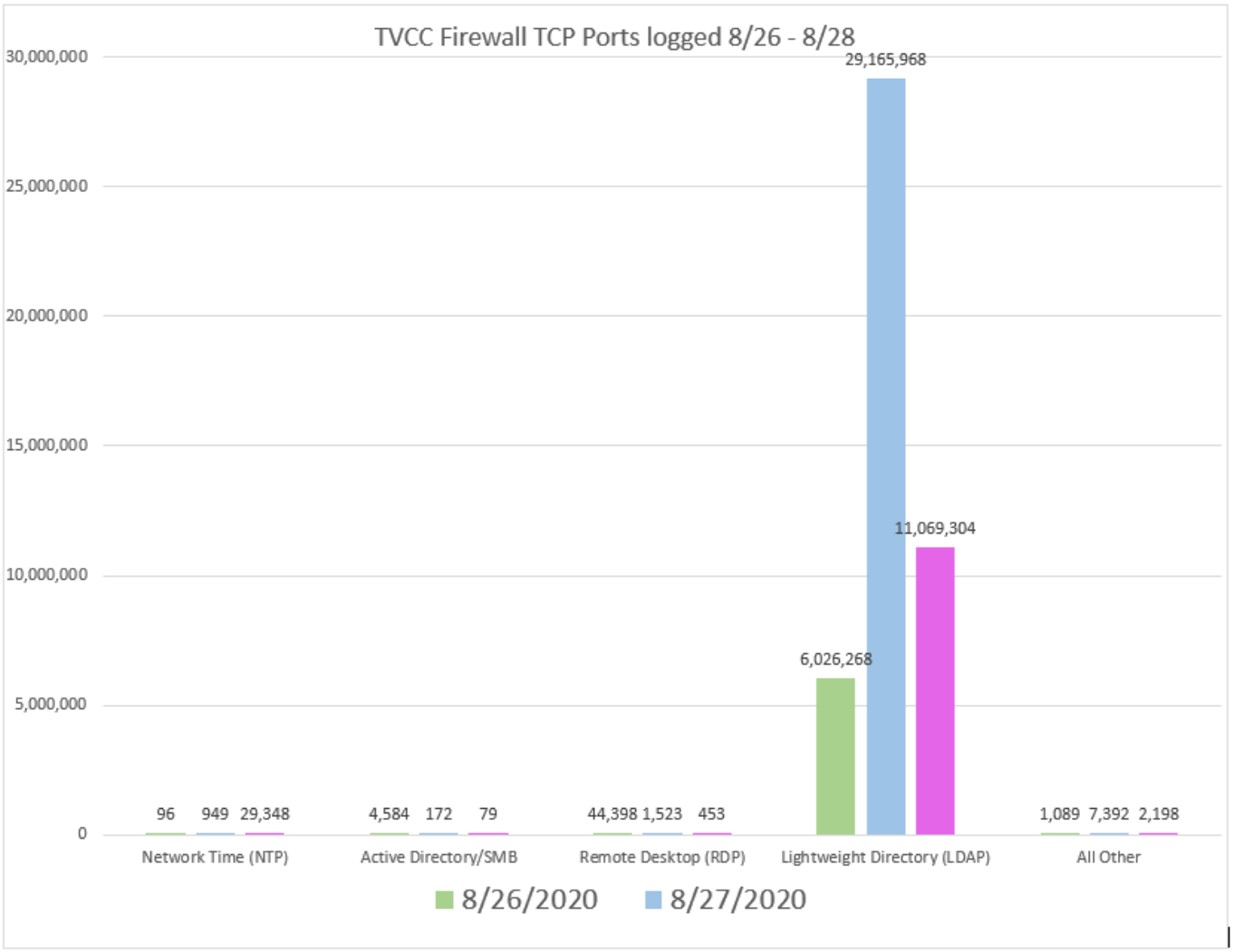
For the three-day period, we averaged about 30,400 distinct IP addresses trying to connect to our network. These requests came from almost every country in the world – there are actually more Internet regions and countries than recognized "sovereign states" (there are 195) - and we got requests from 216 internet regions.

Which ports and protocols were attacked?

One of the common processes used by internet attackers is to run a process to scan for all open ports on a firewall. Ports are rules created in a firewall's configuration to allow outside people to access internal company resources. For example, port 80 is used to allow the outside world to access your company website, so this would be known as an open port. Best practices call for organizations to only open ports that are required, and to disable all other access.

Every internet attack is unique in the combination of target, network address and network protocol. Some attacks attempt to exploit known weaknesses in website servers, while others attempt to compromise an organization's user authentication system. In this case, TVCC's user authentication system (LDAP) was the initial target, as the attackers attempted to compromise one or more user account, and then once that had been accomplished, the attack shifted its attention to using Remote Desktop Services to encrypt the College's data. Because the attackers needed only one compromised

account to work with, the graphs show the repeated attack on the LDAP system, but a reasonably low set of connection to the RDP protocols once they had accessed the system.



LDAP is a protocol used to authenticate usernames and password. RDP is used to access a system once a username and password are discovered. SMB is used to access files shared on a network. NTP is used to sync date and time.

Reviewing our incident response and recovery efforts

After the IT Department discovered and verified the college network had been breached and that ransomware had been spread throughout the college's servers, the Chief Information Officer activated our draft Incident Response (IR) plan. It should be noted that the IT Department has been working on this plan for most of 2020 as part of a larger cybersecurity review, so this was the first opportunity to see how our work and preparation held up in the face of an actual attack.

The plan for responding to an incident is structured to follow these broad steps:

1. Identification

2. Assessment
3. Classification
4. Notification
5. Eradication
6. Documentation
7. Improvement
8. Communication

The CIO began the process by notifying the college's administrative team members of the breach, and then reaching out to all members of the IT department to make sure they reported to the Ontario offices in order to begin working on issues. Shortly afterward, we also reached out to several key vendors, CompuNet and Palo Alto Networks, to engage their assistance in addressing the incident. Palo Alto's managed threat hunting services was able to access our firewalls and Cortex system to monitor network activity, while CompuNet joined us on multiple support calls and did analysis of network traffic logs.

Assessment and classification generally go hand in hand in incident response. Assessment is a question of evaluating which systems have been affected, and which information may have been accessed or lost, while classification is the process of determining how significant a loss the damage represents. TVCC's IR plan uses a matrix of factors to classify an incident, and in this case, we determined within a matter of minutes that we were dealing with a Data Level 4 (DL4) Emergency, the most severe category and the highest priority to address. It is important to note that loss of data isn't necessarily required to elevate an attack's category and priority – disruption of access to that data can be enough, and in this case, it was clear quickly that we had lost access to significant amounts of TVCC's data, even if we didn't know whether that data had been exfiltrated off the college's network.

Because it became clear in our initial assessment that the ransomware was continuing to spread throughout the college's network even as we tried to understand the extent of the attack, it became critical for us to focus initially on containing and halting its spread. The IT Department began working aggressively to shut down as much of the college's IT infrastructure as possible; not everything could be shut down, though, because the IT support team still needed to be able to look at systems and resources to find the breach and shut down the access the attackers had discovered.

As stated previously, the IT Department became aware of the breach about 6 a.m., and by 8 a.m., most of the college servers had been shut down. Palo Alto Networks had been brought into the response and was evaluating the firewalls and network traffic. A working conference call with Palo Alto and CompuNet was established around 8:30 and would ultimately last most of the day.

By about 10 a.m. the CIO had relocated to the College Boardroom where he worked to notify the appropriate college stakeholders, and guide the response and participate in conference calls with the College's insurance provider. At the same time, other IT Department staff were reviewing access logs and backup files to determine whether ransom would have to be paid.

Through the middle of the afternoon on the 26th, activity on the incident response was split among two major centers – the TVCC Boardroom and the IT Department offices. The CIO and college administrators opened a conversation with the College's insurance provider about the incident and their recommended responses, while the remainder of the IT department focused on making backups of the infected systems in order to provide the opportunity for forensic analysis. The conference call with CompuNet

and Palo Alto Networks also continued through this time, as they worked to find the source of the attack and the protocols that had been exploited.

By mid-afternoon, TVCC IT staff had determined that backup systems located at the College's Caldwell Center were intact. Because the timing of the attack at 5 a.m. came after the nightly backup routine had been completed, the offsite backups had a complete replication of the College's server infrastructure pre-attack, and not enough time elapsed between the start of the breach and its discovery for the attackers to find and corrupt the backup systems. IT staff began to restore data from the offsite location, but this proved to be a difficult process. Because of the speed of the network infrastructure, it was determined it would be faster to make copies of the backup systems and drive them to Ontario instead of using the network. Ultimately this process took almost 48 hours to retrieve all the backup and data and to restore to production servers.

It should be noted here that the time period between 10 a.m. and 4 p.m. was when the team of individuals responding to the incident was at its largest, and as will be discussed in the "lessons learned" section below, was also the time when communications between stakeholders were challenged the most. This was especially noted in the challenge encountered in getting current information from the IT staff doing the damage and recovery assessments in the IT offices to the CIO and administrative officers in the Boardroom.

By the conclusion of the business day on the 26th, the response team had generally shrunk to just the IT Department staff. Forensic evaluation of the College's network by CompuNet and Palo Alto Networks had moved from an emergency phase to one of less immediate urgency. Backups had been identified and were being prepared for recovery from Caldwell to the Ontario campus; a number of portable storage devices were quickly procured from Staples to facilitate this movement. IT staff were focused on preparing the server infrastructure to receive and restore the backups.

Friday, Aug. 27 was mostly devoted to restoring data and servers, a task which was largely completed by 4 p.m. At that time, all servers had been restored and the college IT infrastructure was back in full operation. Copies of the corrupted servers had been made and delivered to BlueVoyant (an external partner of TVCC's insurance partner) for their forensic analysis, and the CIO had begun discussions with BlueVoyant about their request to install additional monitoring solutions on the College network. While the learning and improvements from this incident will continue, at the end of Friday, the incident was over, and operations had returned to a normal state.

Lessons learned from this incident

First, it should be acknowledged that a lot went right in this incident which made the recovery quicker and the sustained damage much less. We were lucky the ransomware was detected within three hours of the breach. If the attacker had had more time, all systems including our backups would have been encrypted. Additionally, the investments the College administration and IT Department have made over the years to establish multiple data centers and backup systems gave us the capacity to recover data, rather than the less palatable and riskier option of negotiating with the attackers. Other organizations have found themselves unable to recover their encrypted data even after making a ransom payment to attackers – we avoided that particular outcome because of preparation ahead of time. Additionally, the IT Department has been engaged in a project of cybersecurity review and preparation for more than a year, and it happened we'd spent the Spring Quarter working with several students to develop a proposed cybersecurity incident response plan – the department was well aware of our intended

response plan, and was able to quickly move into action, rather than construct some sort of response under the pressure of an attack. Even so, there was much we learned from the experience.

- Vendor Relationships: Maintaining our vendor relationships with CompuNet and Palo Alto Networks was key to having a successful support team. Because of these relationships they were able to drop their daily activities and help TVCC immediately work on the cybersecurity breach. Having access to skilled cybersecurity professions helped the IT Department respond quickly to the attack. Without their support, the damage could have been much worse and possibly could have led to having to pay the ransom.
- Backup Systems: Even though our backup system design was out of date, the College was able to recover all data by having an offsite copy at the Caldwell data center. If the attacker had been given more time to access our network, they would have eventually discovered the Caldwell backups and corrupted those files. As a result of this attack the IT department will need to change their backup strategy.
- Backup Restoration: In practice, we learned the restoration process from our backups is very slow. This was due to several factors – the network speed between Caldwell and Ontario is not high, and our backup systems in Caldwell were slow to read and copy data to our portable storage devices. We also learned that while our server and storage infrastructure was adequate to run our campus needs during a normal operating condition, it was inadequate to both keep a copy of the contaminated servers and restore older uncontaminated servers from the backup. We spent a lot of time trying to clear space and create resources to get back online, even while we were wanting to do forensic investigation of the corrupted network.
- Forensics: After having gone through this process of recovering from a ransomware attack, we discovered how important it will be to provide enough resources to keep all the compromised servers and data. Our first reaction was to just restore everything and overwrite the corrupt data, but after talking to the insurance team and forensics team, they requested we retain the corrupt data to determine whether we'd need to pay the ransom for unrecoverable data or to do some forensic investigation to determine if data was stolen. In general, the College does not have enough resources to keep two copies of its servers and data on hand – it is a level of capacity TVCC has not been able to afford or support.
- Incident Response Team: During the event it became very clear we need to have a small team of decisionmakers to call out the orders of dealing with the attack and how to recover from the attack. For small organizations such as TVCC, we rely on a single individual, the Chief Information Officer, to manage and supervise the IT support team while also working with College leadership, outside agencies like insurance, FBI and law enforcement, and outside vendors. The duties of an IR Team need to be divided up so a team of people can be in multiple places/meetings at once. In an event like this breach, time is of the utmost importance as we look for ways to stop, contain and repair the attack. Containment necessarily needs to be of higher priority than moving on to forensics and investigation, but we also know College leaders need access to the best and most current information as possible. We suffered somewhat from not having enough qualified individuals to fill all our needs and be in all locations during some of the overlapping conversations and decision-making processes.
- Change Control Process: As we discovered the avenue of how the attacker was able to breach the college security systems, it has become clear we need to consider developing a process for how to manage adds, edits and deletes to the college technology – especially when we are dealing with the core network infrastructure which underpins the entire College. Because we are a small IT department, we've believed the internal communication between a small group

would adequately inform all IT members. This incident exposed that thinking as a mistake – it's still possible for a technician to fail to share planned changes or get a second opinion on a proposed solution. We need a process that will more formally prompt those conversations, and document the changes so that others in the department will be aware of what has been altered.

- Campus Communication: This incident highlighted the challenges of keeping the campus stakeholders informed in the middle of a rapidly shifting set of facts. In general, the IT Department was able to keep the College administrators informed, but staff and faculty were largely uninformed during the event; there were several proposed mass communications prepared for distribution on the 26th, but they were never sent. While this incident happened to fall in a non-instructional period, we did not do a good job of communicating broadly as we would have liked. We need to have future discussions about how long is acceptable to pass before some sort of communication is sent to all campus stakeholders, even if that notification is non-specific and potentially vague.

Next steps and planned changes

The IT Department has identified a number of changes to make or investigate. Some of these represent improvements to existing technical systems, while others would require new systems, and yet others are more procedural than technical.

- Continue to train all college employees on steps they can take to be more effective participants in the College's cybersecurity efforts. While the IT Department had already begun the process of rolling out the Proofpoint security training system before this incident occurred, the Proofpoint training is designed to help end users spot social engineering attempts to gain access to sensitive data and systems.
- The IT Department has moved quickly to harden the College firewalls' configuration and to find and patch computers on campus which may have failed to have the TRAPS endpoint security software installed. Both Palo Alto Networks and CompuNet have been engaged to review and harden the firewall configurations, and we feel there has been significant improvement made as a result.
- The IT Department received funding after the incident to improve the College's backup solution. These funds were used to expand the College's primary SAN device (called the "PUR"), and to implement a new backup solution from Exagrid to replace the aging Quantum storage devices. A major selling point for the Exagrid solution is that it specifically helps protect data from the sort of ransomware attack used in our incident. Ultimately the plan is to also install another Exagrid device in the Caldwell Center datacenter to recreate the replicated backup devices we had with the Quantums.
- The IT Department is engaged in research for two or three potential software solutions to help with cybersecurity. Primary among these packages are software to help detect security vulnerabilities, as well as security information and event management (SIEM) solutions which would expand the ability to centralize system logs and recording events for forensic research.
- The IT Department is also exploring whether the emergent "Security Operations Center as a Service" solutions are a potential fit. Historically, SOCs have served as a centralized function within an organization that was designed to monitor and improve security while preventing and detecting security incidents. Unfortunately, this sort of work usually requires multiple trained

personnel as well as an array of software tools. Recently, however, vendors have begun to offer these sorts of expertise as a contracted service. It represents a significant partnership to enter into, since it requires a customer to expose multiple systems to outside administration and monitoring, and so far, the economic cost has been significant. The IT Department still is evaluating, however – it may prove to be a feasible option for the College to consider.

The IT Department has also been reviewing College policies and its own procedures. This effort had been underway for more than a year at the time of the incident – the IT Department had commissioned a cybersecurity gap analysis from CompuNet in 2019, and among the findings of that process was a need to develop and improve some of the technical governance. Ultimately these policies will need to be reviewed and approved by the College's administrative team, as well as the Board of Education. The documents and policies needed include the following:

- Information Security Policy - This is an overarching Board policy which usually is adopted to direct College leadership, and the IT Department, to establish a number of internal policies and procedures covering a range of information security issues such as appropriate use, user authentication and passwords, data classification, and end-user training. This policy has not been developed yet.
- Cybersecurity Incident Response policy – this document would be a board policy directing the development of an IR Plan by the College's administrators and the IT Department. This policy has been developed but not adopted.
- Incident Response Plan – this document outlines the composition of an Incident Response team, as well as how to classify an incident and who should be notified in the case of an incident. As was noted before, the IT Department has developed this plan and tested it during the recent incident; while it generally held up, some modifications have been suggested.
- Incident Response procedures – These are processes which are specific to the IT Department's internal operations and generally are guidelines for how to respond to a suspected incident and who to notify and when. This document has been drafted but not adopted yet.
- Security training and awareness policy – The College is rolling out security training, but there is no HR policy in place which makes such training a part of an employee's essential duties. While many employees do engage positively with security training, it probably shouldn't be left as an optional component of being a TVCC employee. A draft of a policy has been developed for this.
- Data classification and stewardship policy – An important part of data security is determining what sort of sensitive data is owned and maintained by the College, and identifying who is primarily responsible for caring for that data. Codifying this is known as "data classification and stewardship", and there is an associated training process of making sure the various "Data stewards" on campus know their responsibilities for protecting the data and notifying the correct individuals if they suspect a breach. This policy has not been developed yet.
- A policy governing the College's SAAS relationships – Software as a Service creates a data relationship between the College and an external vendor, and adds complexity to the College's information security responsibilities. The IT Department has been researching potential documents or covenants that might be deployed with any external vendor who wants to provide SAAS services to TVCC that would require appropriate Infosec practices and notification if they suffered a data breach. This policy has not been developed yet.
- A user authentication and password policy – This policy outlines how often passwords will be changed, and who will be considered eligible to use College IT assets. There is an existing policy in place which needs review and updating.

Conclusion

No organization would wish for a cybersecurity incident to determine its own readiness to respond, but the Aug. 26 incident has offered us a significant set of beneficial learning opportunities. Just as a summary, these are among the lasting takeaways from the incident:

- For an organization of its size, TVCC was more prepared to deal with this incident than most comparable peer institutions. Employees from both Palo Alto Networks and CompuNet commented in the aftermath of this incident that TVCC's recovery speed was notable and unusual. This should be seen as a compliment to the entire College and not for any specific individual or department – the College's investment over time in security and backup systems put us in a position to recover quickly, and that's something we should collectively celebrate.
- We continue to need expanded staff capacity in the case of an incident. A question the IT Department grappled with was "where was it more effective to have Scott – in the IT Department or the Boardroom?" The fact this is a key question for our response suggests we still have a ways to go to eliminate the bottleneck of the CIO's role in any incident response.
- The College Board and Administration need to spend some time reviewing and revising the procedural and policy documents which guide the IT Department's future response to any incidents. This incident didn't highlight a failure of policy or process so much as it pointed out that we haven't broadly discussed these sorts of challenges, and we haven't formalized some of the work that has been happening in the IT Department around cybersecurity over the past two years. It's always the case that our daily work load usually takes precedence over thinking about things like policy or procedure, but we should take this opportunity to reflect on what this incident, which was a major breach, meant for the College and its stakeholders.
- Both as individuals and as a group, the IT Department staff performed admirably during this incident. The workload was distributed quickly and the internal communications were good. The three days of the incident were not marked by panic so much as a collective commitment to working through aspects of the problem until we fully recovered from the breach.
- The support from the TVCC President and administrative team demonstrated a real understanding of the incident's severity, and their commitment to preventing repeat incident. Even in a time of budget challenges, the commitment to finding additional resources to support backup and security effort is notable.