LESSONS FROM SURVIVING AN ACADEMIC RANSOMWARE ATTACK

Chad Hogg
Millersville University
chad.hogg@millersville.edu

ABSTRACT
During the Spring 2021 semester Millersville University was the victim of a ransomware attack that disabled all of the university's computational resources. This paper will explain how the department of Computer Science at Millersville University was able to continue its mission without these resources, and how other Computer Science departments could better prepare themselves if they were to face a similar challenge.

1. Introduction

Modern universities depend on information technology to enable their core missions of teaching and research. This is doubly true during a pandemic that has caused a shift to mostly remote learning, with students distributed across a wide geographic region, and triply true for Computer Science departments in this situation.

Sudden and comprehensive loss of information technology infrastructure can thus be devastating. The Computer Science department at Millersville University experienced such a loss on February 28, 2021 resulting from a malicious attack on the university's network. Services were restored gradually over the following six months as a new, more secure network was built from the ground up, but the work of the department, and the university as a whole, needed to continue in the absence of these services.

The Computer Science department had fortunately already been using some services that were wholly disconnected from the university network and thus unaffected by the attack. For other services, we needed to scramble to find appropriate replacements or techniques to do our jobs without them.

It is likely that other Computer Science departments at other universities will suffer similar circumstances due to attacks, natural disasters, or other causes. If so, the lessons that we learned may help them to recover more quickly and completely. Better still, they may allow departments to take proactive steps before such an event occurs that will make them more resilient.

2. Ransomware Attacks

In a ransomware attack, an attacker who has gained unauthorized access to computer system uses that access to sieze control of the system and its data, then demand that the owner pay a ransom to regain access to it. Commonly, data is encrypted with a key that only the attacker knows and promises to reveal in exchange for the ransom. In the case of the attack against Millersville University, the attacker spent a long time exploring a vast network and finding everything valuable that they could access on it before making their presence known.

Universities are a prime target for these types of attacks because by their nature they must manage very large networks accessed by many users in many different ways, because the loss of resources is crippling to them, and because universities have the resources required to pay large ransoms. During the time that Millersville University suffered its attack, attacks were reported on many other universities. [1] The COVID-19 pandemic was an especially lucrative time for cyber criminals to act, because organizations were more dependent on virtualized communication than they would normally be. [2]

3. Related Work

Many authors have written about the policies that university information technology divisions should adopt to decrease the likelihood that they will be victims of an attack and to decrease the level of harm that would result from such an attack. These include multifactor authentication, network segmentation, off-site backups, and other preventative measures. [3, 4]

Other works have examined the reasons why faculty do or do not comply with institutional policies designed to prevent attacks, finding that compliance even among faculty with expertise in information technology or computer science is poor. [5]

This paper, by contrasts describes actions an academic department can take to defend itself, regardless of what institutional policies may be in place.

4. Information Technology Services

The list of ways in which university faculty, especially those teaching Computer Science courses, depend on technology managed by the expert staff at their institutions is vast, including many things one might not think about until they are unavailable.

Email Accounts Email is the most straightforward way that faculty members can communicate with each other and with their students when not physically present in the same location. Typically every member of the campus community has a university-provided email address and most are accustomed to reading it on at least a daily basis. In recent years it has become commonplace for people to receive push notifications on mobile devices whenever an email arrives, making this a very efficient way to reach people. Millersville University uses a Microsoft Exchange server to provide email accounts, which is managed by Microsoft. At the time when the attack was discovered, email accounts were temporarily disabled.

Videoconferencing Classes taught in a synchronous, remote format (which includes all courses offered by the Computer Science department at Millersville University in Spring 2021) require a way for students and faculty to participate in virtual meetings. Millersville University uses Zoom for this purpose, which was temporarily disabled.

Learning Management Systems Universities generally support a learning management system in which faculty members can upload documents that they wish to share with their students and students can submit work to receive grades and other feedback. Millersville University uses Desire2Learn for this purpose, which was temporarily disabled.

Web Pages As an alternative, some faculty use their web pages to distribute documents to students and otherwise manage their courses. The Computer Science department at Millersville University uses Apache for this purpose, self-hosted on a virtual machine in the university's data center, which was temporarily disabled.

Autograding Many Computer Science departments, including the one at Millersville University utilize servers to which students may submit their work and receive immediate feedback from automated tests written by their instructors. The Computer Science department at Millersville University uses AutoLab for this purpose, self-hosted on a virtual machine in the university's data center, which was temporarily disabled.

Shell Servers Computer Science students often need to run specialized software in certain configurations for their courses, which it would be inconvenient or impossible for each student to install on their own personal device. The Computer Science department at Millersville University has a lab of 28 workstations running Linux, which are accessible both from physical terminals in the lab and remotely anywhere in the world through SSH. During the pandemic the lab was not physically open, but the computers were still remotely accessible, and for many of our courses students did their work by connecting to those machines, which were temporarily disabled.

File Storage Students and faculty who are working on University-owned computers need a place to store their work. The Computer Science department at Millersville University uses NFS to mount home directories on our workstations from a file server hosted on a virtual machine in the university's data center, which was temporarily disabled.

Database Servers One of the courses offered by the Computer Science department at Millersville University in Spring 2021 required that students be able to connect to a centralized database server and run SQL queries. We used PostgreSQL hosted on a virtual machine in the university's data center, which was temporarily disabled.

Administrative Document Storage An academic department needs to maintain a collection of historical and current documents: budgets, minutes of meetings, proposals, etc. Millersville University encouraged every department to store these sorts of documents on a shared file server in the university's data center, which was temporarily disabled and then permanently lost.

Registration Records A university needs to maintain records of when courses were offered, who took them, and what grades they received, and have services in which students and advisors can view transcripts and schedules and adjust their registration status. Millersville University uses a Banner system with various frontends, which was temporarily disabled.

Internet Access Students living on campus and all people working on campus depend on access to the general Internet. This was also temporarily disabled.

5. Timeline

On Sunday, February 28, 2021 the university IT staff became aware that their network had been compromised. They responded by immediately shutting all computing services down to prevent further damage and investigate the situation. Within hours access to email was restored, as our email server resided off of the campus network and used Microsoft's authentication services.

On Monday, March 1, 2021 the university cancelled all classes and other non-essential activities for the day, as none of the services necessary to hold them were available. These cancellations were communicated through the university website, a mobile app designed to deliver emergency messages quickly to members of the campus community who had installed it, and by email. During this day access to Zoom and Desire2Learn was restored. Both had already been hosted externally but originally used university resources to authenticate users. Access was restored by switching to using Microsoft cloud authentication. A new unsecured, airgapped wireless network was also set up so that people could access the external Internet from personal devices while on campus.

On Tuesday, March 2, 2021 classes were initially canceled and then un-canceled very confusingly. From that day forward classes resumed. With the ability to communicate asynchronously through email and our learning management system and to communicate synchronously through Zoom, many courses across the university were able to continue much as they had prior to the attack. Most Computer Science courses were still lacking essential resources, however, and required improvisation from instructors. In particular, instructors and students needed to find new ways to run software that they would have run from the shell servers, needed to be able to continue without access to any files that existed only on the NFS share, and needed to submit and receive feedback on assignments without an autograding server.

On Wednesday, March 3, 2021 one of our faculty members set up a version of AutoLab on an external could service. It did not authenticate users, and thus could not be used for submitting work for grading. Students could, however, submit their work to it anonymously to receive automated feedback. This stopgap measure only supported the simplest assignments that do not require any resources beyond a compiler and test scripts.

On Thursday, March 4, 2021 one of our faculty members rented a virtual private server, attempted to configure it as similarly as possible to our existing lab machines, and made it available for students to work on. We set up a replacement database server on the same machine. Students now had a place where they could work on assignments, but any files that had been partially completed and stored only on our NFS share were unavailable to them.

On Tuesday, March 16, 2021 it was announced that both current data and all backups of the shared drive used for administrative document storage were unrecoverable. This meant that we lost the primary copies of our budgets, meeting minutes, accreditation self-studies, and other important historical documents and records.

On Friday, March 19, 2021 the server on which AutoLab had traditionally run became available to again accept submissions of student work, provide them with instantaneous feedback, and accept manual feedback on student work by instructors.

On Monday, March 22, 2021 limited access to registration records became available. Full access that would allow us to properly advise students would have to wait several more weeks, and the registration period for the following semester needed to be postponed.

On Tuesday, March 23, 2021 Computer Science faculty web sites and general access to the file server for faculty members were restored. Instructors who were accustomed to distributing documents through their web sites were able to do so again, and faculty members who stored important files on the NFS share were able to read and copy them for the first time.

Access to the computer labs / shell servers for anyone, and student access to the file server, did not become available until late in the summer, when the department worked with IT staff to redesign the way that users authenticate with them to use multi-factor authentication combining SSH with Duo.

6. Mitigation

The Computer Science department faculty were able to work around the lack of services due to a combination of luck in policies they already had in place and alternative resources that they were able to build as needed.

Discord Discord is a free messaging and videoconferencing service that was originally developed for communcation between players of multiplayer games but has become widely popular among college-aged people. Slack is a similar product used more frequently in professional contexts.

When the COVID-19 pandemic first forced Millersville University to suspend face-to-face classes the Computer Science department made a decision to set up a Discord server and strongly encourage all of our students to join it. The original intention was to replace the face-to-face interactions that our students would be missing out on and provide a unified platform for virtual communication and social interaction among members of the department.

By the time of the ransomware attack the server had been in use for approximately one year and our students were already in the habit of communicating with their peers and instructors through it. We were already using it for department-wide announcements, course-specific announcements, tutoring, hosting social events, and general chatter.

It proved invaluable as a communication link that was never severed because it was not associated with the university network or authentication in any way. If email access had not been restored quickly it would have been even more useful, and while they ended up not being necessary we had contingency plans to teach our courses through its videoconferencing capability if Zoom access had not been made available within a few days.

GitHub Git is a distributed version control system in which a document repository stores all historical versions of files that have been added to it along with metadata about the files and the changes that have been made to them. GitHub is a website that serves as a convenient way to host repositories and manage who has access to them. GitLab, BitBucket, and SourceForge are popular competitors to it.

Several years before the attack, the Computer Science department created a private organization on GitHub and a repository for each course, asking instructors to add their course materials to those repositories each semester. The original intention of this was to make it easier for instructors to collaborate and share materials, producing better and more consistent delivery of those courses. When files stored in faculty members' home directories became inaccessible, faculty members who had been diligent about keeping these repositories up to date, or were privately using some other form of distributed file management were very glad to have done so. Those who had been lulled into a false sense of security that the contents of the file server would always be accessible found themselves in a difficult situation.

We also had a repository that stored copies of many of the administrative documents the department had generated over the last few years. This was especially useful, as the university's official location for storing such documents and all of its backups were deemed unrecoverable. Unfortunately we had only created this a few years in the past and had added only documents created since that point to it.

Furthermore, instructors in several of our courses had created repositories for students and encouraged or required them to keep them up to date with their work for the course. When student home directories became inaccessible and remained that way for the entire semester, students in those courses still had access to their work in progess and completed assignments. Students in other courses lost access to their files, effectively permanently.

Virtual Private Server A virtual private server is a virtual machine rented from a cloud provider such as DigitalOcean, Hostinger, or AWS. When it became clear that our lab machines would not be made available for the remainder of the semester, faculty members selected a vendor, rented a server, and began configuring it. This would have been easier if all of the documentation of how our lab machines were configured were not locked away on our inaccessible filesystem.

In the labs we had depended on the same central authentication mechanism as everything else at the university, which was no longer an option. Instead, we wrote scripts to create local accounts for each student and email them temporary credentials. As students discovered unmet needs more packages were installed. Eventually, the server became a place where students could compile and test code written in C, C++, Java, Python 3, OCaml, and R, with various libraries needed for different assignments. It also hosted a database server to which students could submit queries.

It would be prohibitively expensive to rent equivalent computing power to the 28 machines we were used to, so we needed to manage with significantly fewer resources. The change from having our student population load-balanced among many workstations to having everyone using a single virtual server brought its own additional challenges, as did switching from having expert administrators responsible for running things to a non-expert (me) doing so. A number of students, especially in our Operating Systems course, accidentally wrote programs that overwhelmed the system with resource requests, and we did not initially have safeguards in place to prevent this. Instead it required manual notification and response when people were unable to log in. Often, by this time, it was too late to do anything but reboot the machine.

We did not investigate the option deeply, but it may have been better to use a cloud system in which each login gets its own independent sandbox to work in. Another alternative that we did not consider is to build a virtual machine image that students could download and run on their own personal computers.

While the virtual private server provided students with a place to do their work, it did not restore access to the filesystem on which any work they had done prior to the attack was saved.

7. Conclusion

While Spring 2021 was an especially challenging time for the Computer Science department at Millersville

University, we were able to achieve the objectives for our courses and otherwise serve our students adequately. We learned some valuable lessons from the experience.

First, having a method of communication that is in no way dependent on university resources is extremely valuable. Even in the absence of a disaster such as this paper describes it is an effective way of building comaraderie among students. In the presence of such a disaster it provides a way to continue making announcements, holding meetings, and even teaching virtual classes if necessary. Waiting until a disaster has already occurred to begin setting up an alternative communication channel would be too late, as you would have no way to inform students and colleagues of its existence. We were very fortunate to already have something in place.

We have found Discord to be such a valuable communication tool that we have continued to use it now that our campus has returned to residential living, face-to-face classes, and mostly functional technology, and plan to continue its use indefinitely. Student and faculty activity on the server peaked during our emergency and has declined substantially now that we see each other on a daily basis, but it is still the fastest, least intrusive way to communicate important news to each other and to socialize.

Second, no document of any importance should exist at only one place, and no organization should be entrusted with both the current version and all backups of a document. Distributed version control systems are an ideal solution here because even if only a single person regularly uses it they are likely to have copies on several different machines. While they work better with textual documents than binary files, version control systems are not only useful for source code and should be used for important documents of any type. External cloud storage providers can also work, but if they store the only copy of a document this is no better than storing the only copy on a campus network.

It is not enough to only update central repositories at the end of a semester, because data can be lost in the middle of a course. Just as students would be encouraged to commit their code often, we too must commit our documents often.

Third, having someone on staff with significant experience in administering systems makes it more likely that you will be able to successful build and maintain systems as they are needed. Thoroughly documenting the systems that you have, and making sure that that documentation counts as documents that do not exist in only one place, makes it much more likely that you will be able to successfully replicate those systems. Neither of these things were true for our department, and they limited our effectiveness in quickly building mitigations.

References

[1] Federal Bureau of Investigation, Cyber Division. *FBI FLASH: CP-000142-MW*. `https://www.ic3.gov/Media/News/2021/210316.pdf`.

[2] Harjinder Singh Lallie, Lynsay A. Shepherd, Jason R.C. Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, Xavier Bellekens, Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks During the Pandemic. *Computers & Security 105*, 2021, 102-248.

[3] Noran Shafik Fouad, Securing Higher Education Against Cyberthreats: from an Institutional Risk to a National Policy Challenge. *Journal of Cyber Policy, 6*(2), 2021, 137-154.

[4] Ross Brewer, Ransomeware Attacks: Detection, Prevention, and Cure. *Network Security 2016*(9), 2016, 5-9.

[5] Sofia Dyrendahl, Faculty Reflections on University Information Security Policy. Master's Thesis. University of Gothenberg, 2021.