JOURNAL OF APPLIED SECURITY RESEARCH
https://doi.org/10.1080/19361610.2021.1874227

Resilient Secured Education System for Online Lectures During the Pandemic

Yoshiyasu Takefuji

Faculty of Environment and Information Studies, Keio University, Fujisawa, Japan

ABSTRACT
Keio is a leading research university where 33,436 students are currently registered with 3,140 faculty members. The university system was cracked in September 2020 by malicious crackers where it is composed of the internet-connected-integrated database across the administrative and academic units. The cracked system was completely down, so that all courses from October 1 to October 7 in 2020 were canceled except my courses. The minimum survival system using private mail servers functioned, and my online courses were successfully held. This article shows my story of how to build a resilient secured education system for online lectures against malicious attacks during the pandemic.

KEYWORDS
Malicious attacks; online lectures; mail server

Introduction

No matter what we do to strengthen security for our organization, there will be no perfectly secured system against malicious attacks. Malicious attacks may come from inside or outside of the campus over the Internet. As long as the faculty member's PC is cracked, it is easy for a malicious cracker to break into the education system. Whenever you click through to a malicious site through your browser or read a malicious emailed message, your PC will become under the control of a malicious cracker. Once your PC is controlled by a cracker, all of the important data including websites, passwords, usernames, and other login information can be breached and shared by the crackers.

A security magazine briefly disclosed the top 10 data breaches in 2020. According to the security magazine (Henriquez, 2020),

1. On January 22, Microsoft disclosed a data breach of 250 million records that took place in December 2019.
2. In June 2020, the user-generated stories website Wattpad suffered a huge data breach that exposed almost 268,745,495 million records.

CONTACT Yoshiyasu Takefuji takefuji@keio.jp Faculty of Environment and Information Studies, Keio University, 5322 Endo, Fujisawa, 252-0882, Japan.

3. Security researcher Bob Diachenko discovered an exposed cluster of databases belonging to the voice over IP telecommunications vendor Broadvoice that contained the records of more than 350 million customers.
4. On January 30, security researcher Jeremiah Fowler discovered a database online that contained what he says was "a massive amount of records." The database belonged to cosmetics giant Estée Lauder and contained a total of 440 million records.
5. In March, news broke that the personal details of more than 538 million users of Chinese social network Weibo were available for sale online.
6. An unprotected database, containing 900 million Whisper posts and all the metadata related to those posts, was found online in March.
7. In June 2020, security researcher Anurag Sen found an unsecured BlueKai database accessible on the open Internet with billions of records.
8. In March 2020, Bob Diachenko reported coming across a leaky Elasticsearch database which appeared to be managed by a U.K.-based security company, according to SSL certificate and reverse DNS records (more than 5 billion records).
9. Security researcher and head of Trust & Safety at Cloudflare Justin Paine discovered an open Elasticsearch database with 8.3 billion records when browsing BinaryEdge and Shodan on May 7.
10. Anurag Sen, at Safety Detectives, discovered a significant data leak of 10.88 billion records belonging to adult live-streaming website CAM4.com.

ZDnet also reported major data breaches in 2020 in which a variety of large defense enterprises, financial organizations, and governments were disclosed (Osborne, 2020). Since 2005, K–12 school districts and colleges/universities across the United States have experienced more than 1,300 data breaches, affecting more than 24.5 million records (Cook, 2020).

During 2005 to 2019 (Seh et al., 2020), data breaches by sector are as follows: business organizations: 17.87%; educational organizations: 10.55%; health service providers: 61.55%; government institutes: 8.82%; and nongovernment organizations: 1.18%.

This article shows the minimum survival system for online lectures during the pandemic. The university academic system is basically composed of course registrations, course communication tools between teachers and students, course grading tools for faculty, and administration tools. We must assume that a malicious cracker can break into our system at all levels anytime.

Event analysis

This section shows why the minimum survival system using private mail servers functioned and three online courses were successfully held while the university academic system was completely down.

We use videoconferencing software, which is a vital technology for giving online lectures. Popular videoconference tools such as Zoom Meetings (CVE Details, 2020b), Microsoft Teams (Khalili, 2020; Microsoft, 2020), Google Meet (Tung, 2020), and Cisco WebEx (Bangladesh Government, 2020; CVE Details, 2020a) are all vulnerable against malicious attacks. Therefore, we must prepare for several videoconference tools and Internet access links including Gigabit-Fiber Internet and a high-speed LTE wireless network. The videoconference tools should be regularly updated and upgraded for patching vulnerable security holes.

We need to provide a URL for the videoconference to all registered students during the pandemic. In order to deliver the URL address, a list of email addresses of students is required for a lecturer, which should be securely stored on your mail server.

The minimum survival system for online lectures is composed of stable Internet access, a mail server for delivering a URL, and a videoconference tool.

Three mail servers were actually prepared for coping with emergency incidents in my lectures. Two of them (university official mail server and private mail server) are located at the university campus and one is at my home. The official mail server was completely down from October 1 to October 7 in 2020 while two private servers were successfully running.

The URL of online lectures should be always emailed via BCC (blind carbon copy). As long as a student's PC is cracked, the list of email addresses can be breached without BCC and exploited via the cracked PC. Therefore, an alias list of email addresses of students should be blinded by BCC. When the university mail server is penetrated by a malicious cracker, we need to use non-university email addresses for delivering the URL address to the students. In other words, at least two email addresses per student should be prepared and registered for online lectures.

Important points on your PC:

1. Remember that alias lists of email addresses of students should be always encrypted against the malicious crackers.
2. Start a videoconference for a remote lecture and obtain a videoconference URL address.
3. Use a mail server for sending the URL address to the registered students via BCC.

As a result, all three online lectures were successfully held on October 5 and October 6 respectively by private mail servers while the university campus system was completely down.

With the progress of open-source mail server software, it is straightforward and easy for novice to install a private mail server on your PC. Installation of the mail server is described in the following github site:

https://github.com/ytakefuji/Mail-system

Several recipes to deal with malicious codes:

1. The best way to remove the malicious codes on your PC is to use restore points.
2. In order to cope with ransomware attacks, you need frequent data backup.
3. You should setup your browser on privacy and security as "never remember history."
4. Your operating system running a mail server should be regularly updated and upgraded.

Install the Linux operating system, Ubuntu, or Debian operating system on a $300 laptop. Next, install the mail server on your Linux laptop.

Conclusion

This article shows how the minimum survival system using private mail servers functioned and three online courses were successfully held while the university academic system was completely down. Alias lists of encrypted email addresses for delivering a URL online lecture to registered students and private mail servers play a key role in online lectures; the URL should be emailed to them via BCC. Several mail servers should be prepared and at least two addresses per student should be registered for coping with malfunctioned mail servers. A $300 laptop machine can be used for mail server and web server on a Linux operating system.

ORCID

Yoshiyasu Takefuji http://orcid.org/0000-0002-1826-742X

References

Bangladesh Government. (2020). *CVE-2020-3347: Cisco Webex Meetings desktop app vulnerability*. https://www.cirt.gov.bd/cve-2020-3347-cisco-webex-meetings-desktop-app-for-windows-shared-memory-information-disclosure-vulnerability/

CVE Details. (2020a). *Cisco WebEx security vulnerabilities*. https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-18500/Cisco-Webex.html

CVE Details. (2020b). Zoom security vulnerabilities https://www.cvedetails.com/vulnerability-list/vendor_id-2159/Zoom.html

Cook, S. (2020). *US schools leaked 24.5 million records in 1,327 data breaches since 2005*. https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/

Henriquez, M. (2020). *The top 10 data breaches of 2020*. https://www.securitymagazine.com/articles/94076-the-top-10-data-breaches-of-2020

Khalili, J. (2020). *Microsoft Teams may have downplayed a disastrous security issue*. https://www.techradar.com/news/microsoft-may-have-downplayed-a-disastrous-teams-security-issue

Microsoft. (2020). *Microsoft teams, vulnerabilities*. https://nvd.nist.gov/vuln/detail/CVE-2020-10146

Osborne, C. (2020). The biggest hacks, data breaches of 2020 https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

Tung, L. (2020). *Google: These new data-leaking website attacks are a growing menace*. https://www.zdnet.com/article/google-these-new-data-leaking-website-attacks-are-a-growing-menace/