EXECUTIVE BRIEF: THE RANSOMING OF HIGHER EDUCATION

Best practice defenses against ransomware and other cyberattacks

Abstract

Coordinated attacks are hitting higher education institutions across the nation and around the world. Cybercriminals continue to find college and university networks a lucrative target for ransomware. However, there are effective steps you can take to help prevent being a victim.

Introduction

There has been growing concern around ransomware attacks on higher education networks. Academic services have been locked up, and cumulative ransomware costs running in the millions.

A Disturbing Trend

According to the 2020 SonicWall Cyber Threat Report, SonicWall Capture Labs threat researchers recorded 187.9 million in total ransomware volume during 2019, a 6% drop from the record-breaking 2018 volume. But volume shouldn't be confused with effectiveness.

Cybercriminal organizations that leverage ransomware continue to focus on the quality of their attacks over sheer quantity. It's no longer the size of the organization, but rather their likeliness to pay. That is why higher education institutions across the world continue to be targeted with ransomware. And it's very much a global epidemic.

This trend has been particularly damaging for education. According to a recent report, the education sector was the most affected of all U.S. business sectors in 2018 and the first half of 2019. Threats range from nuisance adware to serious malware like trojans, backdoors and, of course, ransomware – a malicious file that encrypts system files and information on endpoints and servers. Universities hit by ransomware attacks are denied access to vital information until they pay a ransom in cryptocurrency (most often Bitcoin).

Apart from the direct financial damage caused by this kind of attack, the inability to access computer systems paralyzes the academic institution. The cost of the damage only accelerates the longer the school is unable to send emails, record working hours or allocate classrooms and study resources, including school computers and Internet access necessary for many learning activities. Schools that refuse to pay can be incapacitated for extended periods of time.

The now-infamous Emotet malware has also been striking schools, with attackers using spearphishing to infect systems with the malware trojan. As many services are now entirely computerized, this can even affect infrastructure like heating and cooling, cafeteria services and security systems.

A Global Concern

Many U.S. universities and colleges have suffered from ransomware attacks, information leaks, and email account compromise in the past year. Universities and academic institutes are being targeted by more sophisticated attackers interested in stealing the intellectual property (IP) and research data that they produce.

The situation in other parts of the world is just as bad. In Australia the head of the local intelligence agency was recruited to inform universities about cyber threats and ways of prevention. This was one of the initiatives put in place after an extremely sophisticated threat actor compromised ANU and persisted within the university's network for months at a time.

In the U.K. in April of this year penetration testing conducted by JISC, the government agency that provides many computerized services to UK academic bodies, tested the defenses of over 50 British universities. The results were unflattering: the pen testers scored 100% success rate, gaining access to every single system they tested. Defense systems were bypassed in as little as an hour in some cases, with the ethical hackers easily able to gain access to information such as research data, financial systems as well as staff and student personal information.

Analysis: Common Threads

SonicWall CEO Bill Conner states, "It is too easy to demand and receive ransom payment without the risks associated with traditional data exfiltration. Until organizations are serious about ransomware protection, these types of wide-reaching ransomware attacks will, unfortunately, continue. As we've witnessed across schools this past year, ransomware attacks are highly disruptive. Today's distributed networks can be compromised in minutes. Everyday operations are then held for ransom at high costs."

It is no coincidence that schools are among the most attacked. Higher education institutions manage substantial sums of money, store personal information for students and teachers and connect with many external bodies and providers and, of course, parents, who primarily communicate with the school via email. This means that the school has a very large attack surface.

Coupled with enticing rewards is the fact that students make for easy victims of phishing scams. Students' lack of experience combined with a tendency to use simple passwords across multiple services makes them prone to credential harvesting and password-spraying attacks. In one incident this past September, over 3000 Kent State student emails were hacked in this way. In addition, the awareness of parents, teachers and faculty regarding cyber risks is often much lower in education than in other sectors.

Ransomware no longer infects a singular device but often multiple devices with the intent to infect the entire network. First made infamous with the WannaCry attack, ransomware authors now try to leverage vulnerabilities like SMB in Windows to spread to other drives. Not all computers are up to date and this leaves an opportunity to not only infect that device but to also infect others.

Some academic institutions are rich in data and poor in security, which makes them a prime target. Colleges have student information, including grades, which are vital to their future endeavors, plus some jurisdictions must keep this data for up to 100 years. Universities that worked to digitize older records and without proper backups in place, may be at risk of losing this data or having to go back and digitize them again. Schools must continually keep everything backed up with those backups off the network whether it is on LTO tape or in the cloud.

Further exacerbating the security situation is that educational establishments typically have limited staff dedicated to security. Unlike banks, schools typically do not have dedicated information security personnel who are engaged in 24/7 protection.

"You've Got Ransomware"

Most ransomware attacks come unsolicited in email. They come in attachments with subject lines such as:

- Here is my resume
- This is an unpaid invoice
- Here is the invoice for your flight/package etc. (in hopes people will be shocked into thinking their credit card info was stolen).

Malicious URLs are also used. They will look like real URLs but lead to other places on the dark web. Common subject lines are:

- Your card has been charged, please review
- Is this you in this video?
- Your package has arrived

Be Prepared with Best Practices

The US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) recommends the following precautions to protect users against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.

- Backup data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when browsing the Internet.

CISA also recommends that organizations employ the following best practices:

- Restrict users' permissions to install and run software applications and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application whitelisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

In addition, SonicWall suggests the following best practice steps:

- Educate users on cyber security best practices
- Use a next-generation firewall to eliminate known threats on the network
- Implement effective sandboxing on those firewalls to identify unknown threats
- Deploy endpoint security with advanced AI to stop attacks before they happen on the endpoint
- Avoid paying ransom; doing so only adds to the problem by encouraging more attacks

Conclusion

Unfortunately, with differing approaches on responding to ransomware demand being driven by budget and resources, cybercriminals have found colleges and universities to be a lucrative target for ransomware attacks. While these ransomware attacks are widespread, there are commonalities to consider. It is critical to be prepared by implementing known best practices and the latest ransomware countermeasures.

Learn more. Read our Solution Brief: 7 Best Practices for Fighting Ransomware.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 28 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com