



Spring Arbor University Selects Barracuda Sentinel to Stop Office 365 Compromise



Profile

- Spring Arbor University
- Spring Arbor, MI
- 3,800 students, faculty, staff
- 10,000 Office 365 mailboxes
- <http://www.arbor.edu>

Challenges

- Increasing number of Office 365 accounts compromised
- Hijacked accounts blocked for sending spam
- Domain spoofing

Solution

Barracuda Sentinel – AI for Real-Time Spear Phishing and Cyber Fraud Defense

Results

- Real-time protection from targeted attacks
- Office 365 account protection
- Simple, fast set-up and management
- Zero impact on user experience or network performance

About Spring Arbor University

Since 1873, Spring Arbor University has helped students pursue wisdom by offering an education grounded in the Christian faith. What began as a small elementary and secondary school in the late 1800s has evolved into a top-tier, liberal arts, Christian university with more than 3,000 enrolled students. Spring Arbor University now offers more than [70 undergraduate majors and programs, degree completion programs, associate programs and graduate programs](#). With programs presented on campus, online, and on site at 12 locations throughout Michigan and Ohio, the university continues to meet the growing needs of its students.

Increasing Office 365 Account Compromise

Microsoft Office 365 has become so ubiquitous—with more than [100 million monthly active subscribers](#)—that it's almost become part of an identity, particularly among users on the same network. There's an inherent trust when receiving an email from a credible source like a coworker or boss, or even directly from Microsoft Office 365. Cybercriminals have taken notice, and Office 365 has become a breeding ground for highly sophisticated attacks – particularly at educational institutions, who are targeted frequently due to the large number of users, significant financial transactions, and heavy reliance on email communications.

Spring Arbor witnessed this first hand in its Office 365 environment. In mid 2017, just prior to the 2017-2018 school year, cybercriminals targeted Spring Arbor with a massive Office 365 account takeover attempt. The attackers targeted people with an email impersonating Microsoft Office 365, stating that they had reached their email quota and needed to reset their passwords. The criminals also targeted users with fake Dropbox messages trying to solicit credentials.

College campuses are notoriously fast-paced, with students, faculty, and staff managing multiple classes, projects, and relationships. While this pace is great for productivity, it lends itself to significantly increasing the likelihood of one of these types of spear phishing attacks working—with people checking email on mobile devices, running between classes, and quickly clicking on links without analyzing the details. In the case of an Office 365 account compromise, it often takes only one person to fall for the attack before it spreads like wildfire throughout an organization.

That's exactly what happened at Spring Arbor, where a single spear phishing attack was successful, which led to a compromised Office 365 account, which then was used to hijack more than 200 other Office 365 accounts on the network.

About Barracuda Sentinel

Barracuda Sentinel is a cloud service that utilizes AI to stop spear phishing and cyber fraud in real time. The service combines three powerful layers of artificial intelligence, domain fraud visibility and protection using DMARC authentication, and fraud simulation training for high-risk individuals inside an organization. It integrates directly with Office 365 via API, so there is no impact on network performance or user experience, and setup typically takes less than five minutes. Barracuda Sentinel works alongside any existing email security solution, including Barracuda Essentials, Exchange Online Protection, and others.

“We have some three thousand people actively on our network, sending emails every single day at Spring Arbor, which places a very large target on our users and networks,” said Chris Blackstone, CIO at Spring Arbor. “Today’s cybercriminals are increasingly sophisticated, and we quickly found that typical email security solutions were not effective against these highly targeted attacks. We looked at several solutions on the market and selected Barracuda Sentinel. Barracuda Sentinel utilizes cutting-edge artificial intelligence to stop these attacks in real time, and does so in a way that does not impact our network performance or users, which is critical with a large and diverse user base.

“We take pride in knowing that Spring Arbor offers an environment where our students can take advantage of the latest and greatest tools and technologies to further their education,” continued Blackstone. “The same holds true in today’s evolving threat landscape: you have to stay on top of the latest technologies in order to protect your people and your assets. Since implementing Sentinel, we’ve been able to stop several of these targeted attacks in real time.”

“*Since Implementing Sentinel, we’ve been able to stop several of these targeted attacks in real time.*”

Chris Blackstone

CIO

Spring Arbor University

Conclusion

Spear phishing attacks are rapidly becoming the most significant security threat today. These attacks are highly personalized and the results can be devastating to everyone. In fact, spear phishing is the underlying attack that leads to Business Email Compromise (BEC), which has accumulated more than \$5 billion in losses so far, according to the FBI.

Spear phishing can be costly for educational institutions to mitigate, especially as IT budgets continue to shrink. In today’s dynamic threat environment, educational institutions must continue to evaluate and implement leading-edge security platforms to prevent these types of attacks and protect their users, networks, and data.

About Barracuda Networks

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda’s customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda Networks, Barracuda and the Barracuda Networks logo are registered trademarks or trademarks of Barracuda Networks, Inc. in the U.S. and other countries.