CYBER SECURITY

OCTOBER 2017

INTERVIEW WITH CYBER SECURITY EXPERT NICK CASILLAS – INTRODUCTION FROM PARKER, SMITH & FEEK'S TIM SCHMIDT

Tim Schmidt | Account Executive, Parker, Smith & Feek

We all remember the first email we received from a "foreign dignitary" offering us a ridiculous sum of money in exchange for paying a small amount of taxes, claiming the funds had come from an unknown distant relative. Needless to say, the online threat landscape has evolved into a much more sophisticated, global issue, affecting people and companies of all shapes and sizes. If you are a client of Parker, Smith, & Feek, then you have likely heard us speak on the importance of cyber and social engineering coverage to help indemnify you after an attack. Today, I'd like to give you more guidance on prevention and the current threats that may affect you.

After hearing my clients' common questions and concerns regarding the increasingly sophisticated threat landscape, I thought it would be beneficial to get answers directly from a cyber security professional. Nick Casillas is a territory account manager for Barracuda Networks, a global leader in security and data protection solutions for more than 150,000 customers worldwide. He lives and breathes content security, networking application delivery, and data storage/disaster relief response.

TIM: What is the top cyber threat a business owner faces today?

NICK: The threat landscape is sophisticated and ever changing. New headlines pop up daily about the latest security breach or data theft. These attacks leave business owners scrambling to determine the best way to cost effectively keep their users, networks, and data safe.

Ransomware is top of mind with everyone today, with ransomware profits expected to reach $1 billion in 2017. Innovative, entrepreneurial criminals who look to profit from infecting a victim are fueling this activity, using media such as email links, email attachments, website exploits, social media campaigns, compromised business applications, and USB drives for offline infection.

Additionally, spear phishing and cyber fraud are rapidly becoming significant security threats. Countless individuals and organizations have unwittingly wired money, sent tax information, and emailed credentials to criminals who were impersonating their boss, colleague, or a trusted customer. These attacks are highly targeted and personalized. They work because they are built on trust and typically do not contain any

continued >

malicious links or attachments that might get stopped with existing email security solutions. This latest type of attack takes an equally novel approach in order to effectively protect an organization.

TIM: Could you walk us through a recent real life scenario and how the business was affected?

NICK: In May of 2017, the world experienced a well-coordinated ransomware attack known as WannaCry. This attack infected hundreds of thousands of individuals and businesses alike, including hospitals, government entities, and everyday users in more than 100 countries across the globe. In a period of 48 hours, attackers managed to encrypt all the data stored on victims' hard drives with the promise of decrypting the data upon the receipt of a monetary payment via the e-currency platform Bitcoin. This attack targeted aging computer operating systems and exposed the vulnerabilities of using outdated software.

> ...smaller businesses face the same security risks as large enterprises, and often do so with fewer people and technology resources to appropriately handle.

We're also seeing a sharp increase in the number of attacks on Office 365. One in particular is an Office 365 account compromise, or account takeover attacks, where attackers attempt to steal login credentials and ultimately gain access to launch attacks from within an organization. If the spear phishing attack is successful and the attacker is able to get control of the account, we've seen a few different scenarios for what happens next. First, the attackers can set up forwarding rules to observe the user's communications patterns to use as leverage in future attacks such as ransomware. Another common scenario is where attackers use the compromised account to send messages to other employees inside the organization in an attempt to collect additional credentials or other sensitive information, or attempt to get a fake wire transfer sent to a fraudulent account.

TIM: Do smaller businesses face the same risks today as the larger companies we are seeing being hacked in the headlines?

NICK: Absolutely, smaller businesses face the same security risks as large enterprises, and often do so with fewer people and technology resources to appropriately handle. The recent WannaCry ransomware attack is a great example, where hundreds of thousands of businesses, large and small, were impacted. While the use of cloud applications and the internet as a whole has tremendously benefitted businesses looking to efficiently scale, it's also leveled the playing field and created much easier access to business infrastructure through a multitude of threat vectors. The amount of information we make available online combined with the readily available exploitation kits sold on the dark web (complete with dedicated sales and support), promise that anyone can instantly launch an attack without sophisticated coding.

TIM: What are best practices for today and how can businesses avoid cyber threats such as ransomware, phishing attacks, etc.?

NICK: At Barracuda, we recommend a layered approach in stopping advanced threats from reaching your users and data – across every threat vector.

Email

Email remains the top business communications tool and, thus, one of the most easily exploitable areas.

continued >

With ransomware and spear phishing on the rise, businesses must take steps to keep email secured. This includes a comprehensive security strategy designed to prevent ransomware attacks from infiltrating your network. Any effective strategy will include a plan for data protection and backup – particularly important with today's rampant ransomware attacks and making sure you can easily and quickly recover without having to pay the ransom.

For the more targeted and personalized spear phishing attacks, businesses should look to solutions that leverage advanced technologies like artificial intelligence rather than rules-based detections. Barracuda Sentinel's artificial intelligence engine learns organizations' unique communications patterns to predict future attacks. Using AI, we're able to identify and block real-time spear phishing attempts, offer domain fraud visibility and protection, and provide simulation training to high-risk individuals within the organization to protect against monetary and data fraud.

We also offer free powerful detection tools to run scans across customer networks looking for vulnerabilities already lurking on your systems. Upon diagnosis, remediation tools are available to secure the network and clean up the expressed threats.

Network

We advise implementing a cloud-ready next-generation firewall, designed to secure on-premises, cloud-hosted, SaaS-based, and mobile elements, as well as third-party applications. They enable secure network connections for your remote workers, improve site-to-site connectivity, and ensure secure, uninterrupted access to cloud-hosted applications.

Web

Web traffic requires web security gateways leveraging advanced threat protection to let you safely use online applications and tools without exposure to web-borne ransomware and other threats. Granular access policies give you maximum control, and powerful reporting tools provide total visibility.

Applications

Web applications secured via a web application firewall continuously monitor your outward-facing websites and applications. By automating security audit procedures, it can dramatically accelerate your application development cycles while removing risks.

Barracuda's global threat intelligence network includes massive amounts of diverse threat information – across every threat vector – from more than 50 million collection points around the world, giving us the most comprehensive view of the global threat landscape in the world. We're able to leverage this intelligence to create actionable data that protects more than 150,000 organizations from the most sophisticated security threats.

Each and every day, these threats grow and evolve, making enhanced online and network security a must to avoid a catastrophic breach. Staying up to date on the current climate and changes will help you mitigate these risks by preparing your network while properly insuring your cyber risk in the event of a breach.

As always, should you have any questions, please contact your Parker, Smith & Feek Team. While every effort has been taken in compiling this information to ensure that its contents are totally accurate, neither the publisher nor the author can accept liability for any inaccuracies or changed circumstances of any information herein or for the consequences of any reliance placed upon it.