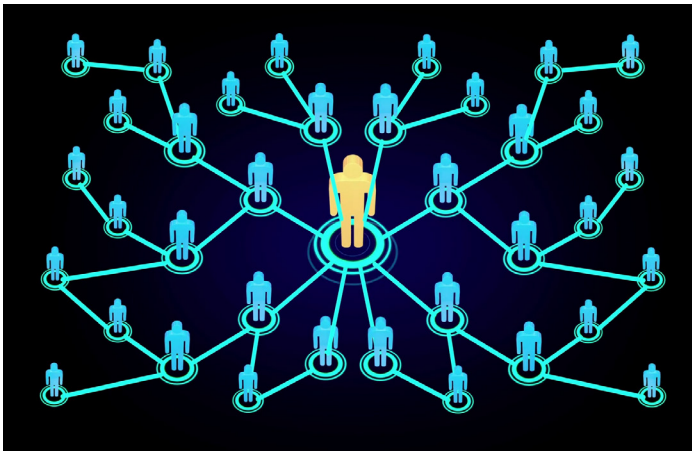
Talk Nerdy To Me

November 2019

THE RISKS OF THIRD PARTY ACCESS

Why third-party remote access is the biggest security threat to networks



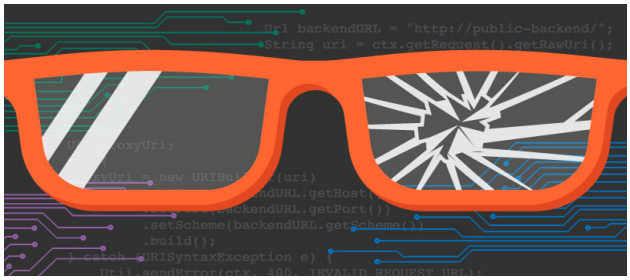
Think back to the Target breach—do you remember how the hacker gained access to the network? Probably not. The hacker was able to get into Target's network from a third-party that Target used for heating and air conditioning. This third-party vendor was not separated from the rest of Target's network, allowing the hackers unfettered access to the point of sale devices. This resulted in millions of credit and debit card information being stolen. Target's reputation took a huge hit that cost them millions of dollars and their profit margins plummeted.

This real-life example speaks volumes for data breaches that affect organizations. It is well known and widely accepted that third-party relationships pose a significant threat. We live in the day-and-age where these relationships are necessary for an organization's success, but they are still risky. The Institute of Internal Auditors report that 80 percent of businesses understand the risks of third-parties, but only devote a small chunk of resources to assessing the risks associated. So where is the disconnect? A company seems to think they're safe until they have gone through a breach and it's too late. All of a sudden they have to contact their customers about the breach, potentially deal with data loss and downtime, and take a hit to their reputation.

So, what can be done to fix this glaring issue? The most immediate fix that will also be beneficial in the long run, is to be preemptive. What third-party vendors have access to your organization's network? Do you have those vendors separated from the rest of your network? Did those vendors go through a vetting proccess before they were given access? Do those vendors keep their own networks up to date and secure?

To learn more about how to protect your network and alleviate the potential threats to your infrastructure, contact us today to attend our FREE Before The Breach lunch and learn at Ruth's Chris Steak House on Friday, December 6th at 12 PM.

Attackers Hide Behind Trusted Domains, HTTPS



Attackers attempting to dodge more advanced security defenses increasingly are adopting more sophisticated techniques to fool victims with their malicious e-mail messages and websites.

A new midyear report from security firm Webroot found that one in four malicious URLs used a legitimate domain in an attempt to improve the success rate of an attack. In the vast majority of cases — 94% — the attacker used a URL shortener to mask a malicious domain in order for it to appear legitimate. In the first half of the year, the company found 1.5 million phishing URLs, accounting for about one in 50 URLs encountered by its customers.

The overall effect is that users are losing one of the most significant signs of a potentially malicious attack: a URL that appears suspicious, says Tyler Moffitt, security analyst for Webroot.

“Attackers’ tactics are reducing (consumers’) ability to tell the difference between what is a scam and what is not,” he says. “Attackers know that many consumers do a mental check on any domain, and they are trying to fool them.”

As companies continue to improve the security of modern operating systems and applications, cybercriminals and online attackers are likewise searching for ways to defeat both software security and fool targeted users. Using trusted domains is one way that attackers are attempting to limit the ability to victims to discern an attack. Another method: employing secure HTTP to give visitors a false sense of security, and nearly a third of phishing domains use HTTPS now.

“When you see that little lock icon in your browser, it just means that the information you transmit on that site is encrypted and securely delivered to where it’s going,” Hal Lonas, chief technology officer at Webroot, said in the report. “There’s no guarantee that the destination is safe.” In addition, attackers are targeting older operating systems, with malware targeting Windows 7 rising 71%, according to Webroot.

Over the past decade, attackers have created ways of camouflaging their malware using techniques that create variants to evade signature-based antivirus scanning. The strategy has now become ubiquitous, with 95% of all malware samples encountered by Webroot’s software having a unique signature, up from 92% last year, the company said.

Other companies have seen similar trends. Network security firm WatchGuard, for example, saw a significant increase — 64% — in the number of malware variants blocked by its two detection services. The company also saw attacks using content delivery networks (CDNs) to host malware on legitimate-seeming domains. Two previously popular attacks, cryptojacking and cryptomining malware, have largely subsided as the value of cryptocurrency remains off its peak, but Webroot continues to see attackers attempt to install the payloads as a passive way to monetize otherwise low-value compromises.

“Because they can make money off people’s computers by mining, and most people have no idea their system is infected, it continues to be a popular attack,” Moffitt says. “It may only be 60 cents a day, but over tens of thousands of compromised systems — that adds up.”

Source: InformaTech

BEFORE THE BREACH

HACKERS ARE HERE!

NEW SKILLS FOR A NEW FIGHT

- 1 in 5 businesses will suffer a cyber breach this year
- 81% of all breaches happen to small/medium sized businesses
- 66% of companies do NOT test their backups
- 60% of companies that lose their data will go out of business within 6 months
- 92% of malware is delivered via email
- 97% of breaches could have been prevented with today's technology

Want to learn more about how to protect your business?

Sign up TODAY for our FREE Cybersecurity Lunch and Learn

December 6th, 2019
12 PM to 2 PM
At Ruth's Chris Steak House
(Limited Seating)

RUTH'S CHRIS STEAK HOUSE

www.preferreditgroup.com/beforethebreach

talk nerdy to me

PREFERRED IT EMPLOYEE SPOTLIGHT

Meet Cole Smith! Cole started with us about a month ago and has picked things up really fast! He has his Bachelor of Science in Criminal Justice from Ball State University but decided he wanted to pursue a career in IT instead.

He was a D1 swimmer at Ball State University and was team captain his senior year. Cole enjoys building and shooting guns, spending time with his dog Gunner, and spending time with his family and girlfriend.

Cole has shown us that he is a hard worker and eager to learn all that he can about IT. We are hopeful that with some time and training, he becomes a permanent technician with Preferred IT Group!

Welcome to the team Cole!

Socktober Success!!

Every October, we collect socks of all colors and sizes to donate to the local homeless shelters. This year, we were able to collect 756 pairs of socks! We also had 12 pairs of gloves donated as well! Huge THANK YOU to all of our customers who helped us collect this year! Every bit helps and we are very grateful!

TREND MICRO VISITS PITG

The Trend Micro team came to our office to meet with our Director of Operations, Matt Carpenter this month.

Preferred IT Group has been a long time partner of Trend Micro and we look forward to the next step of that partnership with the release of Trend Micro XDR Worry-Free Business Services!

preferred IT group

CONTACT US

Fort Wayne
260.440.7377
Warsaw
574.306.4288
Columbia City
260.213.4266
Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.