Cybercriminals Need Shopping Money in 2017, Too!

December 28, 2016
by SentinelOne

Oh, the ransomware outside is frightful, and the amounts are not delightful...

If you've been out in the world lately, there's a chance holiday music is stuck in your head too. You might have noticed that our tune is a little different from the original. That's because along with "let it snow, let it snow, let it snow," our minds are full of information on cybercriminals.

As we move past the season of gift giving, we are cheering that there haven't been any documented breaches. But wait..., we shouldn't celebrate just yet. It's reported that more than 50% of the biggest holiday retailers may not be PCI-compliant.

That's not good news. Especially with all those distracted employees that used their personal devices on company networks to find the next great purchase. It's possible that attackers have been out there all along, collecting information, just to be used later. So, while it's past the largest flux of shopping, now is a good time to learn some lessons before President's Day.

What to Expect in 2017 from Cybercriminals During Peak Shopping Times

There is seemingly an endless amount of holidays that retailers use to advertise a good sale. As employees are shopping online, they need to be vigilant when opening emails and providing credentials. Cybercriminals are highly active at times when there is an emphasis on purchasing. They are focused on sending malware-ridden emails advertising holiday "sales," just waiting for an unsuspecting shopper to fall into their trap. If that isn't enough, they go as far as to hide malware in websites and fake shipping notifications.

While identity theft has always been a concern around holidays, phishing has added fuel to the fire. Attackers are taking aim by sending out false urgent messages from merchants, asking for credentials and saving credit card information. By doing this, shoppers open themselves up for extortion and credit card fraud for criminal shopping.

Cerber ransomware is the latest documented threat of this kind. Through a spam campaign, it prompts victims to open a password protected Word document containing instructions to cancel a seemingly fraudulent purchase. Preying on the fear of credit card theft, victims quickly open the file, only to find they have downloaded the Cerber ransomware.
The healthcare, retail, and financial sectors are prime targets. With an abundance of personally identifiable information and strict regulations like HIPAA, malicious actors understand the value of holding their data ransom. Extortion to unlock patients' information, ecommerce fraud, and data breaches aren't the only concerns lingering from compliance issues this season.

Cybercriminals are now leveraging social media as a ransomware tactic and have all businesses in mind. Using the "ImageGate" attack vector for the Locky ransomware, malicious actors can post on social media sites for quick and impactful access. Exploiting misconfigurations on sites allows for actors to post what seems like a standard image, only to have someone click to find they've gotten a Scalable Vector Graphic with ransomware code embedded. In seconds, files are encrypted and inaccessible, leaving the company to pay the ransom.

The dangers of social media are difficult to contain since these sites are normally whitelisted. Assuming this remains standard protocol, companies will need to make the effort to inform employees of safe practices while browsing platforms. That includes warnings around downloading files with extensions such as SVG, JS, or HTA. Anything that automatically downloads is ripe for exploiting the way that Windows masks file extensions by default.

Don't Bankroll Criminal Shopping Sprees

The sad reality is that we are watching company after company pay ransoms that could have been avoided. With the threat of being unavailable to customers or having their reputation damaged for leaking data, they quickly pay without a second thought.

While the final 2016 holiday shopping is behind us, we need to continue to be vigilant as the threat actors are still out there. 2017 will hopefully be a more secure year. Let's take the time to learn from other victims and work now to protect all of mankind. If you're ready to learn more about safeguarding against ransomware, download our free white paper, Ransomware Is Here: What Can You Do About It?.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Cybersecurity Jobs Outlook is Bleak News for Businesses
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- Why Your Operating System Isn't Your Cybersecurity Friend
- SentinelOne's Cybersecurity Predictions 2022: What's Next?
- 12 Months of Fighting Cybercrime & Defending Enterprises | SentinelLabs 2021 Review
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022