KOVRR
Cyber Risk Modeling

www.kovrr.com

Black Friday & Cyber Monday Cyber Threat Alert

NOVEMBER 2021

This year, Black Friday promises to be a huge win for ecommerce with sales increasing by 15.8% to $10.42 billion as per a new Insider Intelligence | eMarketer report. Cyber Monday is expected to be even bigger at $12.12 billion, up 12.4% from last year.

With all that retail buying, however, cyber criminals will also ramp up their malicious activity. In the midst of the holiday buying frenzy, phishing attacks can increase by up to 400%.

Who can forget Emotet? Until it was recently disrupted by law enforcement and judicial authorities, Emotet was a highly proliferative worldwide Trojan that functioned as a downloader or malware dropper. Emotet botnets dropped Trickbot to deliver ransomware payloads against some victims and Qakbot Trojans to steal banking credentials and data from other targets.

While it has since been dismantled, threats like Emotet-style spear phishing and card skimmers will be unleashed during this holiday shopping season.

What is Spear Phishing?

Spear phishing is an email attack that targets a specific individual or organization. The intent is often to exfiltrate data (credentials, credit card numbers) for malicious purposes. Threat actors may also use phishing tactics to install ransomware onto a victim's PC.

A typical spear phishing attempt takes shape as a highly convincing (but fake) email. Even upon close inspection, the email looks authentic with logos and fonts that match Amazon, PayPal, WalMart, your bank, or any other brand.

The phishing email contains a link that redirects you to a fake website with malware ready and waiting. For example, the email may claim that you have an account problem. The link then directs you to the bogus site where you "login", thus giving away your username and password.

Later, threat actors can then either sell your data or access your account to make unauthorized purchases or empty your bank account.

Other tactics, more specific to the holiday season, might be fake discounts or gift card offers that take you to a rogue site. There you may be asked to login or click on a link that enables malware to be downloaded to your PC.

Some ways to avoid being a victim of spear phishing attacks are;

- Examine URLs closely. If you hover your mouse over the link, you should be able to see it on your browser before clicking.
- Never click on an email link, especially one that suggests you have to login to an account. Always login directly from the company website.
- Examine who is sending the email closely. The email may appear to be from a trusted source. But upon closer inspection, the sender address is typically odd looking or very long containing random characters and numbers.
- Don't click on or open documents, especially ones that promise discounts or rewards.
- Only download apps from official app stores.

Holiday Magecart Skimming Attacks

Another devious trick used by cyber criminals is Magecart data skimming. In these attacks, authentic company websites get infected and are then used to steal data. Magecart is a cybercrime syndicate with dozens of subgroups that specialize in cyberattacks involving digital credit card skimming theft.

One such attack targeted Ticketmaster in 2018. Magecart actors found a way to insert undetected malicious JavaScript into the Ticketmaster website. The malicious code worked as a credit card skimmer or keylogger. This meant any data typed by users on the website was skimmed off to a distant drop server fully visible by attackers.

The ticket-selling giant eventually discovered the malware on a customer chat function for its websites. The infectious code was able to access a user's name, address, email address, telephone number, payment details and Ticketmaster login details.

Eventually, Ticketmaster's UK division was fined $1.65 million by the UK Information Commissioner's Office (ICO) due to the data breach that impacted 9.4 million customers. The ICO determined that Ticketmaster failed to have appropriate security measures in place to thwart the attack.

More Activity, More Risk

Ecommerce was already booming before the COVID-19 crisis. But the pandemic drove even more consumers online, contributing an additional $105 billion in U.S. online revenue in 2020. As mentioned earlier, this holiday season promises to be even bigger than last year.

As more people spend time online, they will be exposed to threats such as spear phishing and skimming scams. With the larger attack surface, we can anticipate a larger number of attacks.

> Kovrr helps organizations gain a clear picture of their financial business exposure due to cyber attacks.

Kovrr's Cyber Risk Quantification (CRQ) begins by collecting data about known and emerging attack vectors. By leveraging global threat intelligence and financial impact data from cyber incidents, companies can execute decisive action regarding their overall cyber risk management. CRQ enables enterprises to assess and manage cyber risk by putting it in clear business terms.

Kovrr's Enterprise Cyber Risk Quantification solution is an efficient and easily repeatable means to quantify cyber risk financially. The platform allows CISOs, CROs and other risk management stakeholders to measure financial exposure for multiple types of cyber events and impact scenarios.

Users receive real-time data to make more informed decisions about managing cyber risk (i.e., whether to accept, mitigate, or transfer the risk), prioritizing new technology investments, and measuring the ROI of those investments in specific controls or programs. The solution leverages the same advanced cyber risk models and technologies trusted by cyber insurance carriers and reinsurers worldwide.

The Author

Avi Bashan

CTO

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models.

To learn more please contact the Kovrr team: contact@kovrr.com