Threat Bulletin

Amazon Black Friday Phishing Attack

January 2022

What is the Amazon Black Friday phishing attack?

Scammers frequently pretend to be from Amazon. According to the US Federal Trade Commission, between July 2020 and June 2021 one-third of people reporting a business impersonator said the scammer was from Amazon.

One such attack was recently seen by Allot security researchers among our European customers. It took place between November 16 and November 30. It was spread through WhatsApp and SMS text messages. The target was asked to fill out a survey in exchange for a gift from Amazon. After completing the survey, the target was asked to fill in their credit card information.

Phishing, a type of social engineering attack, is frequently used to steal information such as login details or credit card details. It occurs when the attacker tricks a victim into clicking a malicious link.

In November 2021, Allot Secure blocked 1.7 million instances of this attack.

Figure 1 - Popup offering user a gift after completing survey

How were users infected?

After clicking on the phishing link, the user was asked to fill in a short survey. Once the survey was completed, a message appeared saying that the person won a prize, but that to claim the prize, the survey needed to be shared with twenty friends. This is a common social engineering tactic. The victim was also prompted to enter their credit card details.

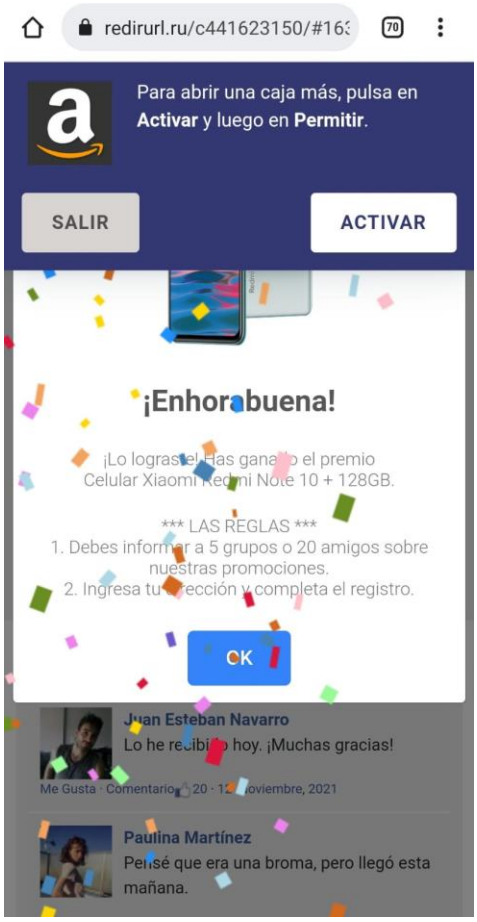

Figure 2 - Popup congratulating user for winning a new cell phone

Compromising credit card data was not the only consequence of the attack. After entering credit card details, another pop up appeared prompting the user to click on “Allow” (“Activar” in Spanish). Subsequently, the device was infected with adware.

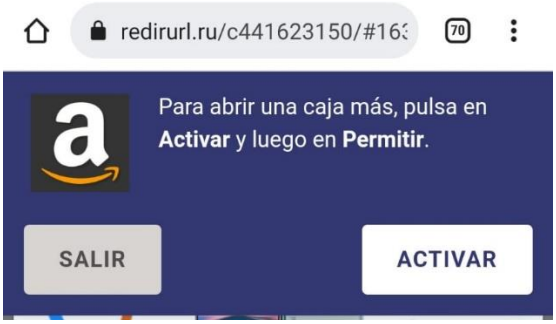

Figure 3 - Upon clicking "Accept" user's device is infected with adware

However, subscribers to Allot NetworkSecure were protected from this attack. Allot NetworkSecure blocked communication with the URLs that hosted the fake promotion, relieving those protected of the need to decide whether to click on a dangerous link.

"This was one of the largest phishing attacks that we've seen in recent history. Fortunately for people subscribed to CSP cybersecurity services based on Allot NetworkSecure no damage was incurred as a result of this attack," said Itay Glick, Vice President Security Products for Allot. "Though we did not have prior knowledge of this attack, the solution kicked in and blocked a serious threat, keeping regular people safe with no manual intervention."

Conclusion

To protect their customers, many communication service providers are turning to network-based security which stops the attacks on the network-level before they even reach their customers' devices.

Protect Subscribers with Allot Secure

Allot Secure is the world's largest network-based telco security-as-a-service solution, protecting more than 23 million subscribers worldwide. It delivers effortless, device-independent security, achieving adoption rates over 50%. Allot Secure merges network-based, gateway, and client security into a unified service offering a seamless customer experience for event handling, policy setting, and reporting. It is the only platform protecting end-user and IoT devices simultaneously in the core network, home network, and off-network with a transparent and unified end-user experience. Allot Secure protects mobile, fixed, and converged customers at home, at work and on the go.

Want to learn more about Security as a Service?
We can assist.

Contact Allot.