Warning: The malware campaign hides the shadow of gift emails from Amazon

Traditionally, the holidays and year-end shopping holidays are always a golden opportunity for bad actors to launch a series of malicious campaigns on cyberspace to gain illegal profits from those who are fickle and gullible.

This year is no exception when there have been a series of cyber attack campaigns recently discovered. The latest is a case of spreading Dridex malicious code in the form of gift emails from Amazon, which has been discovered by international security researchers.

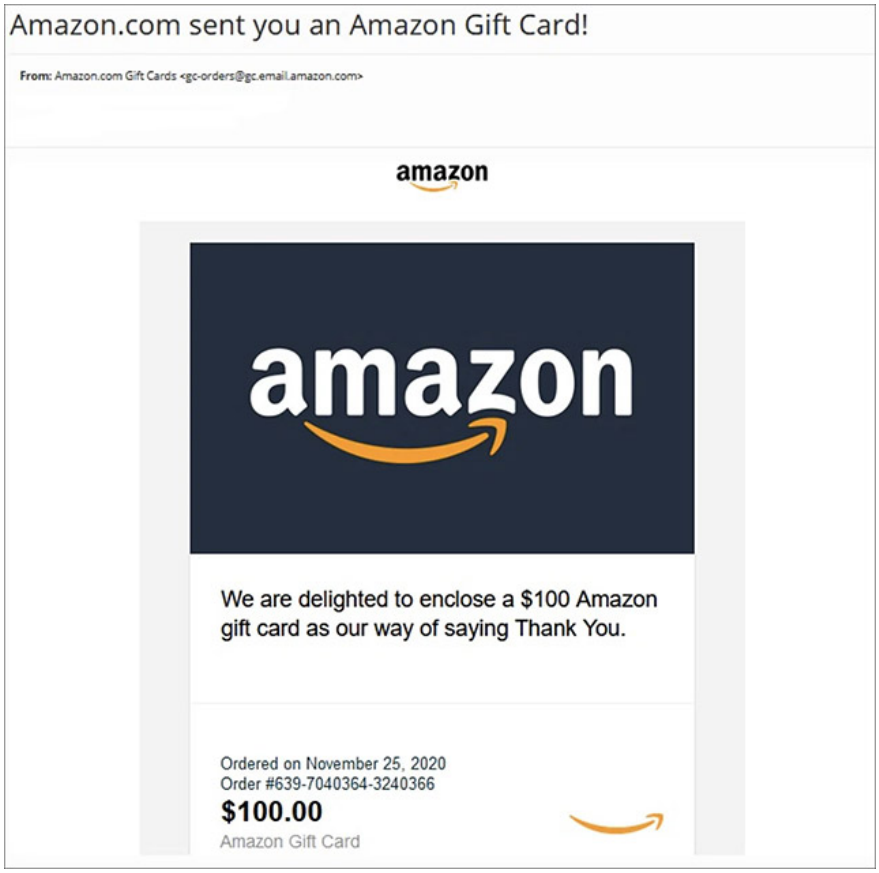
Dridex is a modular banking trojan. When successfully infecting a victim's system, the malicious code can perform various malicious activities, including stealing login credentials, keylogging, screen capture, as well as downloading. and install additional malware… All of this was done in a stealthy manner without the knowledge of the system owner. Dridex is being spread publicly through a phishing email campaign that disguises itself as an Amazon Gift Card to deceive people who do not have much knowledge or security knowledge.

Dridex is considered particularly dangerous because it can provide DoppelPaymer and BitPaymer malicious agents with access to compromised networks. Thereby paving the way for ransomware attacks that can cause enormous damage.

Dridex scam campaign

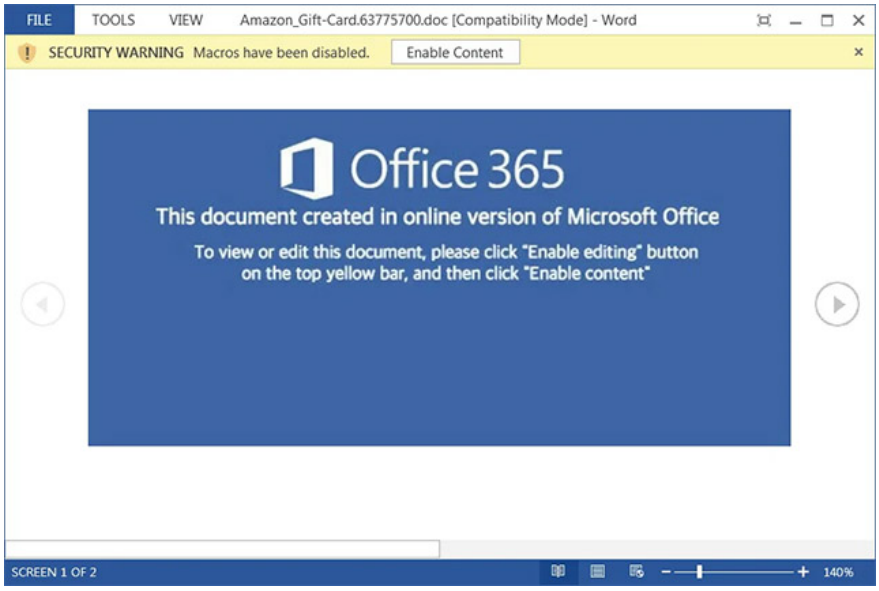
When spreading malicious code, hacker gangs tend to take advantage of hot ongoing events or holidays as the subject of fraudulent campaigns. This makes it easier for victims to open up malicious attachments. That's exactly what's going on with the Dridex distribution campaign - with malicious email attachments disguised as gift vouchers from Amazon.

These emails are nicely designed, disguised as a message sending a $ 100 gift voucher from Amazon. If you want to accept the gift, the victim will have to click on the malicious attachment.



After just one click, malicious Word documents with names similar to 'Amazon_Gift_Card', 'Order_Gift_Cart' and 'Amazon_eGift-Card' are immediately downloaded to the victim's machine.

These attachments indicate that they were created in the online version of Microsoft Office, and prompt the recipient to click the 'Enable Content' button. If you do, the malicious macros will be downloaded. Soon, Dridex and possibly other types of malware will be present on the victim's system.



During today's year-end shopping rush, the gift card is clearly a popular tribute gift. However, it's important to remember that Amazon and most other e-commerce websites will never ask you to download something in exchange for a gift voucher. Instead, the legitimate email will contain a snippet that you can redeem right on the Amazon site quickly.

If you receive any emails that say gift certificates and prompt you to download attachments, avoid them immediately.