Discovered a group of Vietnamese hackers specializing in stealing credit cards for the past 8 years

According to security firm Volexity, a group of suspected Vietnamese hackers has been conducting activities to steal credit card information for the past 8 years.

Security researchers have just discovered a group of unknown Vietnamese hackers with the name XE Group. This group has been involved in hacking and stealing credit card information (skimming) for illegal gain over the past 8 years.

Investigation results show that XE Group exploits publicly available vulnerabilities to compromise external services, notably the Telerik user interface bug. From there, they install malicious code to steal user credentials and payment information.

On average, each day XE Group can steal thousands of credit cards mainly from restaurants, non-profit organizations, arts organizations and travel service platforms.

In 2020, Malwarebytes had its first report on XE Group activity. Recently, security firm Volexity continued to publish more in-depth analysis of this hacker group.

Specifically, Volexity has been mapping the infrastructure used by the XE Group over the past three years and shared all the technical details and IOCs on GitHub. The researchers found that many websites were attacked by the XE Group using the same technique that involved downloading malicious JavaScript scripts.

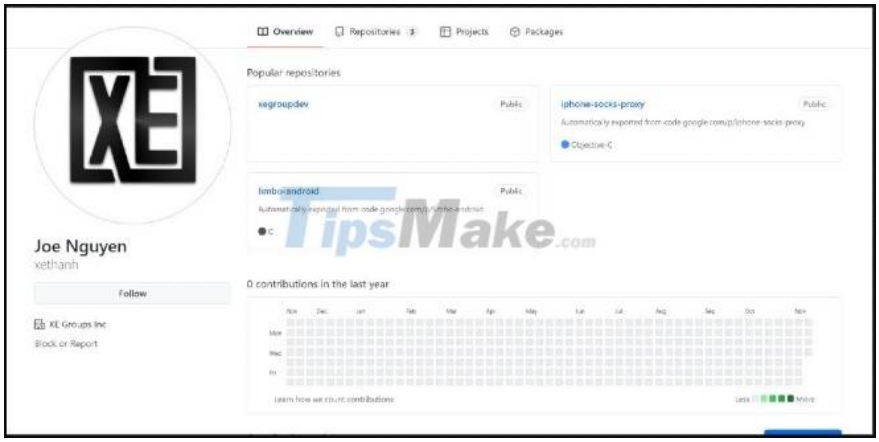
This type of attack is known as Megacart and hackers often add malicious JavaScript code to e-commerce sites to collect customer and payment information as these data are submitted. Stolen data will be sent to a remote server controlled by XE Group.

The lifetime of the attacks depends on how well the malicious code can evade the web before the detection of security products.

According to the test, XE Group's malware achieved a perfect score of 0/57 on VirusTotal. This means that it is completely undetectable by anti-virus software.

Compared to Malwarebytes' 2020 report, Volexity's report shows that XE Group's malware has evolved. Many subtle improvements have been added to increase evasion as well as data mining capabilities.

Volexity said XE Group is run by Vietnamese hackers because some domain names used for command and control servers are registered under a person's name in Vietnam.



Although the domain registration information was forged, the researchers linked the registrant, Joe Nguyen, to a repository created by a user with the same name as the XE avatar.

In addition, the nickname "xethanh" associated with the GitHub repo was also used to register an account on the crdclub[.]su forum, where the hacker group provided the credit card information they had stolen.

Further research has found similar accounts on other specialized credit card forums such as cybercarders[.]su and cardingforum[.]su. This shows that the XE Group hacker group prefers to sell card information rather than exploit it themselves.

According to Volexity, the accounts related to Joe Nguyen have a history of activity since 2013. Therefore, it is likely that the XE Group group has been active in hacking and stealing credit card information for up to 8 years, but only one reports related to them.

Besides detailed reporting, Volexity also provides network indicators and signals so administrators can block XE Group attacks. You can check it out by clicking on the links below:

1. Network indicator
2. Signage VEHICLE Group

Wish you always have a safe solution for your system!

You finished reading the article "**Discovered a group of Vietnamese hackers specializing in stealing credit cards for the past 8 years**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
