Ursnif Trojan has targeted over 100 Italian banks

zdnet.com/article/ursnif-trojan-has-targeted-over-100-italian-banks/

Home Innovation Security

1,700 credentials were stolen from a single payment processor.

Written by Charlie Osborne, Contributor on March 3, 2021

-
-
-
-
-

The Ursnif Trojan has been traced back to attacks against at least 100 banks in Italy.

Security

- My Instagram account was hacked, and two-factor authentication didn't help
- The 5 best browsers for privacy: Secure web browsing
- Stop doing these 10 things that let hackers in, says FBI and NSA

- What is a cybersecurity degree?
- How to delete yourself from search results and hide your identity online

According to Avast, the malware's operators have a keen interest in Italian targets and attacks against these banking institutions have led to the loss of credentials and financial data.

The cybersecurity firm said on Tuesday that at least 100 banks have been targeted, based on information gathered by the researchers.

In one case alone, an unnamed payment processor had over 1,700 sets of credentials stolen.

Avast found usernames, passwords, credit card, banking, and payment information that appears to have been harvested by the malware.

First discovered in 2007, Ursnif began its journey as a simple banking Trojan. The information stealer's code was leaked on GitHub and has since evolved and has become more sophisticated, with its code being developed independently and also appearing as part of the Gozi banking malware.

Ursnif is usually spread via phishing emails -- such as invoice requests -- and attempts to steal financial data and account credentials.

Datktrace researchers documented a 2020 campaign in which the malware was used in an attack against a US bank. A phishing email was sent to an employee who unwittingly opened a malicious attachment and accidentally downloaded an executable file pretending to be a .cab extension.

This file called out to command-and-control (C2) servers registered in Russia only a day prior to the launch of the campaign -- and, therefore, the IPs were not blacklisted at the time of infection. A recent obfuscation technique noted in this attack was the use of User Agents imitating Zoom and Webex to try and hide in network traffic.

Darktrace has also tracked the malware in attacks against organizations in the US and Italy.

Avast has shared its findings with the victim banks the company was able to identify, alongside CERTFin Italy, a financial services data exchange managed by the Bank of Italy and the Italian Banking Association (ABI).

Previous and related coverage

Have a tip? Get in touch securely via WhatsApp | Signal at +447713 025 499, or over at Keybase: charlie0
