Emotet malware hits Lithuania's National Public Health Center

bleepingcomputer.com/news/security/emotet-malware-hits-lithuanias-national-public-health-center/

Sergiu Gatlan

By
Sergiu Gatlan

- December 30, 2020
- 11:02 AM
- 0

The internal networks of Lithuania's National Center for Public Health (NVSC) and several municipalities have been infected with Emotet malware following a large campaign targeting the country's state institutions.

"When infected recipients opened infected messages, the virus entered the internal networks of the institutions," NVSC officials said in a statement published today.

"Infected computers, after downloading additional files, began sending fake emails or engaging in other types of malicious activity."

Lithuanian government officials, ministry representatives, and epidemiological diagnostics experts that have previously been contacted by NVSC specialists via email have all received Emotet-infected emails from infected systems.

The NVSC e-mail systems have been temporarily shut down on Tuesday to stop the further spread of the virus.

NVSC information technology specialists, together with experts from the Central State Telecommunications Center and the National Cyber Security Center currently working on cleaning affected systems of the Emotet infection, as well as on recovering NVSC e-mails and restoring email access.

Emails sent as replies to previous conversations

Rytis Rainys, Director of the Lithuanian National Cyber Security Center (NKSC), warned that the Emotet emails sent as replies to previous conversations distributed malicious code using password-protected archives as attachments, with the password shared in the email body.

This prevented anti-malware solutions from detecting the malicious emails which made it possible for the targeted individuals to open the attachment and infect themselves.

Stealing reply-chain emails is a known Emotet tactic used to camouflage malicious emails as parts of existing conversations for higher credibility and better infection rates in future spam campaigns.

The tactic is also being used by the Qbot trojan, and it was previously by the Gozi ISFB banking trojan and the URSNIF information-stealing trojan.

This is the second large Emotet campaign that has targeted Lithuania this year, with a previous one detected by the NKSC in October.

The NKSC published an advisory at the time recommending potential targets (including but not limited to state institutions and companies) to enable and properly configure Sender Policy Framework (SPF) email authentication.

Emotet is back in business

After a break of a month and a half, the Emotet botnet was revived on December 21st [1, 2], and Microsoft spotted an ongoing campaign delivering "a wide range of lures in massive volumes of emails, the use of fake replies or forwarded emails, password-protected archive attachments."

"The new Emotet campaign still uses documents that contain malicious macro that, when enabled, connects to seven malicious domains to download the Emotet payload," Microsoft Security Intelligence tweeted.

Emotet was first spotted in 2014 as a banking Trojan and has now evolved into a botnet used by the TA542 threat group (aka Mummy Spider) to deploy second-stage malware payloads on infected systems.

The payloads Emotet drops on compromised computers include the QakBot and Trickbot (which also deploys both Ryuk and Conti ransomware) trojans.

Before going on a break, Emotet has targeted multiple US state and local governments in potentially targeted campaigns according to an advisory published by DHS-CISA in October.

Related Articles:

Historic Hotel Stay, Complementary Emotet Exposure included

EmoCheck now detects new 64-bit versions of Emotet malware

Emotet botnet switches to 64-bit modules, increases activity

Emotet malware infects users again after fixing broken installer

New ChromeLoader malware surge threatens browsers worldwide