Pengeretur.dk Cautions Finnish Consumers Following Massive Malware Attack & Offers Advice to Impacted Mobile Phone Users

NEW YORK, UNITED STATES, December 17, 2021 /EINPresswire.com/ -- Finland's Transport and Communications Agency (Traficom) has reported that a major malware attack has infected mobile telephones throughout the country. According to Traficom. fake SMS messages urged recipients to click on a link ostensibly sent by their service providers. The malware, known as FluBot, which steals data from its victims, was then installed automatically on users' devices.

> Pengeretur urges the public throughout the Nordic countries to take precautions to protect against malware. If a device has been infected with malware, it should be reset, preferably by a professional"
>
> *Judith Persson*

As a result of this data theft, cybercriminals gained access to the personal accounts of all mobile phone users who clicked the nefarious link, enabling them to commit identity theft, and charge transactions to their victims. Once installed, FluBot immediately begins to steal information from the recipient. In many cases, victims will require professional fund recovery assistance.

Why FluBot Is Dangerous

The messages were received by an estimated 70,000 Finnish mobile users, according to the National Cyber Security Center. They were written in Finnish but did not include certain Finnish diacritical marks. One red flag was that these messages were interspersed with strange characters such as %, /, + and @, apparently to make it difficult to filter them.

The messages were composed to look like a typical SMS from the mobile service provider and claimed to be a follow-up to communications customers had already received in a voice message. The SMS contained a few sentences, along with the link that led the customer to a request to install the software.

The Increase in Malware Attacks

The FluBot incident in Finland is one of many malware attacks that hit every country and sector. Ransomware, a type of malware that holds the consumer's services hostage until and unless the victim pays the attackers, usually in cryptocurrency, is the latest trend in cyber-attacks.

In fact, the banking industry has seen a 1,138% rise in ransomware attacks, according to Security

magazine. According to the Center for Cybersecurity, the threat of cybercrime is “very high” for government services, private companies and individuals in Denmark.

Danish authorities, however, have had some success in cracking down on internet fraud. In December 2020, the Danish Eastern High Court sentenced a 38-year-old man to three years in prison for stealing 22.4 million DKK through online casino games. Similar to the Finnish FluBot attack, the fraudulent casino games installed malware on customer devices. Also in 2020, the Danish police arrested 11 people for installing keyloggers on library computers to track data, like passwords, with the aim of committing financial fraud.

Experts strongly recommend never to take the contents of SMS messages at face value. Consumers, therefore, should research all information in the messages they receive before acting on them. If the message appears to be from a company, call or message them to confirm its authenticity.

“We urge the public throughout the Nordic countries to take all necessary precautions to protect against malware, and be especially careful about requests to click on links, install software or download a document,” states Judith Dayan Persson, Vice President of European Operations and Business Development at MyChargeBack, the parent company of Pengeretur, a one-stop shop for consumers in the Nordic countries to recover funds lost related to credit/debit card and cryptocurrency transactions. “If a device has been infected with malware, it should be reset, preferably by a professional,” she adds. “Install a backup, but make sure it has been acquired before the malware attack to ensure it was not infected,” she advises. “And then prevent additional infection by installing anti-virus software and ensuring it is updated regularly.”

About Pengeretur
Pengeretur is the Nordic service of https://MyChargeBack.com, the global leader in complex dispute resolution involving card-not-present transactions for goods and services that were not provided by the merchant as contracted. Having built relationships with over 800 banks in more than 100 countries and 450 law enforcement agencies as well, MyChargeBack has successfully recovered millions in disputed claims and put that money back into its clients’ wallets, where it belongs.

Reuben Eliaz
MyChargeBack.com
+1 917-920-6749
email us here

in today's world. Please see our Editorial Guidelines for more information.