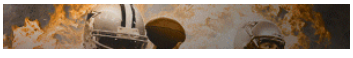
Next →
Chinese Central Bank to Use Blockchain, Competition w...
Explore Menu

Altcoin News Bitcoin Crime Bitcoin Security

Malware Discovered Sending Fake Emails to Steal Bitcoin and Passwords

Lester Coleman on 28/01/2017



A new malware that steals passwords and bitcoin from cryptocurrency wallets has been discovered by Cyren, an Internet security service provider, according to the company's blog. The malware targets banking customers, and according to Cyren, is carrying out a massive campaign.

The emails inform the recipient of a deposit. The emails originate mainly from bots in the United States and Singapore, and are branded as being from various banks, including Emirates, NDB and DBS.

The malware is a keylogger that is carried as an attachment to emails for fake bank transfers. Once the victim opens the attachment, the malware can record everything the victim types on their keyboard and every place they place their mouse.

How It Works

The malware queries the victim's registry for passwords and other information related to various types of software. The subject line usually has financial details like an online wire transfer payment notification.

Recent Posts

Malware Discovered Sending Fake Emails to Steal Bitcoin and Passwords

Chinese Central Bank to Use Blockchain, Competition with Alibaba?

Bank of England Governor: Fintech Brings Great Promise and Risks

BitGo Enhances Its Security With Ledger's Hardware Based Key Storage

The US Postal Inspection Service is Seeking Bitcoin 'Intelligence Gathering Specialists'

Advertisement

The attachments have a SWIFT variation, making the emails look legitimate. SWIFT codes identify financial institutions for fund transfers.

Files that appear to be PDF are really executable files, according to Cyren. Once executed, the file deletes itself and opens a new one called “filename.vbs” in the Windows startup folder. When the computer boots, the software executes itself.

The malware collects passwords and other information, focusing on web browsing software and FTP software. It gathers usernames, passwords, cookies, browsing history and more.

Also read: malware turns servers into cryptocurrency mining engines

Cryptocurrencies Targeted

The malware looks for cryptocurrency wallets and targets a long list of currencies, including bitcoin, Namecoin, Litecoin, Anoncoin, BBQcoin, Bytecoin, Craftcoin, Devcoin, Digitalcoin, Fastcoin, Feathercoin, Florincoin, Freicoin, I0coin, Infinitecoin, Ixcoin, Junkcoin, Litecoin, Luckycoin, Megacoin, Mincoin, Phoenixcoin, Primecoin, Quarkcoin, Tagcoin, Terracoin

Phoenixcoin, Primecoin, Quarkcoin, Tagcoin, Terracoin, Worldcoin, Yacoin and Zetacoin.

Image from Shutterstock.

Posted in: Altcoin News, Bitcoin Crime, Bitcoin Security, News
Tagged in: Cyren, Emirates, SWIFT

Advertisement

Tags

apple Australia bitcoin bitcoin accepted here bitcoin asic miner bitcoin atm bitcoin exchange bitcoin foundation Bitcoin price bitcoin regulation bitfinex bitlicense bitpay bitstamp blockchain block chain Blockchain.info china coinbase cryptocurrency dogecoin Ethereum News fintech gavin andresen IBM india japan litecoin mark karpeles microsoft mtgox mt gox okcoin overstock paypal R3 reddit regulation ripple roger ver Ross Ulbricht russia satoshi nakamoto security silk road

Advertisement