2 New Malware Warnings You Should Not Ignore

Millions of merchants are continually at risk for dangerous malwares. Malicious softwares, such as viruses, spyware, and Trojan horses, are created by fraudsters to infect computer systems and perform unwanted actions. When these hackers steal sensitive data, the impact can be detrimental to your business.

“Cyber-attacks, and the fraudsters behind them, have become so sophisticated that they are utilizing any and all information to fool you into opening their malicious documents,” says Rob Kroeger, Infintech director of client services. “If they break into a trusted individual’s data and your contact information is present, they will use that against you and lure you into thinking a communication is safe.”

Here is more information about two malware threats you need to be on the lookout for:

#1 Flokibot – Designed to Steal Your Credit Card Data

This recently identified threat has attacked and compromised POS devices and systems in Brazil but there are reports that countries across the world have been targeted, including the United States. First identified in fall 2016, this financial-oriented malware is designed to bypass fraud detection tools to steal your credit card data. VISA has issued a security alert regarding Flokibot and tips to help protect your business.

- **Related:** ‘TSYS Flokibot Malware Warning Issued’

#2 Carbanak – Creative Phishing Ways Used to Hook You

Carbanak, aka FIN7, is regarded as one of the Internet’s most skilled cyber warfare groups and has upped the ante in their methods of stealing credit cards, banking credentials and other sensitive materials. This group of criminals is financially motivated and uses weaponized office documents to acquire sensitive data, says SC Cybercrime. Carbanak has taken great measures to booby-trap Word and PDF documents and utilize phone calls to further their agenda.

- **Related:** ‘Creative Ways To Trick You Into Opening Malicious Files’

What Can You Do to Prevent a Malware Attack?

- Educate yourself on malwares
- Educate your employees to follow best practices to safely open emails and attachments
- Update operating systems and network equipment like firewalls
- Turn on heuristic and behavior analysis in your anti-malware software
- Monitor network traffic for unusual activity
- Keep your PCI Compliance up-to-date

4455 carver woods drive, suite 110
cincinnati, ohio 45242
p 800.621.8931
f 800.621.9131
infintechllc.com

To Report an Attack or to Learn More about Infintech's Security Measures:

Contact us online or call 1-800-621-8931.

Check out Infintech's newsroom.

Visit this story online.

4455 carver woods drive, suite 110
cincinnati, ohio 45242
p 800.621.8931
f 800.621.9131
infintechllc.com