MTSi Micro Technology Solutions, Inc. The Computer Systems People™

Tech Times Monthly Newsletter

Micro Technology Solutions, Inc. P: (508)324-9475 F: (508)324-4477 www.mtsolutions.net

September 2019 **Vol. VIII Issue VIIII**

IT NEWS:

- Microsoft Issues New Windows 10 Update Warning (more)
- MTSi Employee Appreciation Dinner (more)
- 15 Upcoming Business-Changing Tech Trends (And How To Prepare For Them) (more)
- You Should Update LastPass Right Now (more)

Follow

Review us on facebook

"Don't limit your challenges. Challenge your limits."

In this issue:

Phishing: what it is, how to prevent it and how to respond to an attack

Phishing is a scam conveyed via the Internet, where attackers try to deceive their victims in order to gain access to sensitive information such as usernames, passwords or bank details. Generally, the cybercriminal sends false communications to the victim, posing as a well-known company, or as someone with whom it is possible to have conversations and relationships, using plausible excuses to obtain the victim's personal data.

The phenomenon of phishing is a current and frequent threat. In its latest report, Kaspersky Lab has revealed a two-fold increase in the number of attacks blocked, with 44 per cent of attacks detected aimed at banks, payment systems and online shops. (more)

Fake PayPal Site Spreads Nemty Ransomware

A web page pretending to offer an official application from PayPal is currently spreading a new variant of Nemty ransomware to unsuspecting users.

It appears that the operators of this file-encrypting malware are trying various distribution channels as it was recently observed as a payload from the RIG exploit kit (EK).

The latest occurrence of Nemty was observed on a fake PayPal page that promises to return 3-5% from purchases made through the payment system.

Several clues point to the fraudulent nature of the page, which is also flagged as dangerous by major browsers, but users may still fall for the trick and proceed with downloading and running the malware, which is conveniently named 'cashback.exe'.

Security researcher nao_sec found the new Nemty distribution channel and used AnyRun test environment to deploy the malware and follow its activity on an infected system. (more)

Just An SMS Could Let Remote Attackers Access All Your Emails, Experts Warn

Beware! Billion of Android users can easily be tricked into changing their devices' critical network settings with just an SMS-based phishing attack.

Whenever you insert a new SIM in your phone and connects to your cellular network for the very first time, your carrier service automatically configures or sends you a message containing network-specific settings required to connect to data services.

While manually installing it on your device, have you ever noticed what configurations these messages, technically known as OMA CP messages, include?

Well, believe me, most users never bother about it if their mobile Internet services work smoothly.

But you should worry about these settings, as installing untrusted settings can put your data privacy at risk, allowing remote attackers to spy on your data communications, a team of cybersecurity researchers told The Hacker News. (more)