TechTips Newsletter

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

July 2017

This monthly publication provided courtesy of Richard Lynn, VP Sales & Marketing, Tech Hero

Our Mission: To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

RANSOMWARE PREVENTION: BUCKET LIST OF BEST PRACTICES

Ransomware, for quite some years now, has stopped merely being a part of cyber-fiction and is a dismal reality that has cost billions of dollars to unsuspecting, lethargic, and laggard organizations. Cybercriminals are turning to increasingly complex, savvy, and impenetrable means of cyberattack monetization, and ransomware is right up there at the top. The consequences of a ransomware attack on a business can be catastrophic. Ransomware can paralyze the operations of the entire workplace if it lands in shared locations within wide networks. Of course, in light of all this, being prepared for ransomware is the only option for any organization that uses IT (that's, well, most of them). And as bad as ransomware has been, experts expect it to get worse.

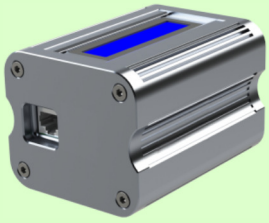
Ransomware, traditionally, has been viewed as a problem that's hard to anticipate and prevent. So, IT experts within organizations have always worked in a "reactive" mode to ransomware. Of course, fighting back after a ransomware attack is important, but only secondary to taking proactive measures for the safekeeping of your organization's IT assets.

Any foiled ransomware attempt implies you save thousands, perhaps millions, of dollars that would be lost in ransomware recovery expert fees, ransom payment, and workplace disruption. This brings us to the idea of learning best practices, tips, and tricks to enable enterprises to prevent ransomware attacks and remove them once they strike.

Keep antivirus updated

Make sure that the antivirus software protecting your enterprise computers is updated to the latest version, across all endpoints. Remember, your enterprise IT network is as vulnerable as the least-protected computer terminal in use. Antivirus applications are based on signatures. Malware can slip in if the version is not updated. However, antivirus packages are your IT department's first line of defense, so implement mechanisms that ensure regular upgrades.

Latest Network Security Device: "NetDefender"



Vulnerability Management Solution

The new NetDefender Vulnerability Management Solution enhances security by proactively identifying, monitoring, and notifying businesses of potential vulnerabilities in their networks—all with breakthrough simplicity and affordability.

Utilizing proprietary software and the compact NetDefender Sensor, NetDefender works in three phases:

1. Identification

The user's network is continuously scanned to locate and identify every connected device with an IP address, from computers and smartphones to printers and smart devices

Includes scanning of external-facing IPs to provide a 360-degree view of network vulnerabilities

2. Monitoring

All connected devices are then scanned 24x7 for vulnerabilities such as missing software patches

3. Notification

All scan information, including vulnerabilities, is displayed in an easy-to-read dashboard, including instructions for remediation

A proprietary "SPF" (Security Protection Factor) scoring system makes it easy to understand the network's health

Users and their IT security providers can be alerted to critical issues via email or text

For more information on this solution please contact your Tech Hero representative at (800) 900-8234 (option 2)

Regular security awareness programs

When was the last time a security awareness campaign was conducted within your enterprise? Most ransomware make their way to computers via phishing, wherein cybercriminals posing as vendors, colleagues, educators, or marketers send out emails with infected documents and other attachments. Because of the pervasive nature of email communication, end users often instinctively open these malicious emails and, in a sense, open the gates for malware and ransomware to rush in. The most effective preventive measure you can rely upon is all about regular education and training of the workforce, enabling them to:

- Identify malicious emails based on known patterns of such phishing mailers.
- Quickly report the receipt of such emails to the organization's IT teams.
- Understand and remember the steps to be taken if they accidently open a suspicious email.

Client Spotlight

FLORIDA HOSPITAL

The skill to heal. The spirit to care.®

Our mission strengthens our commitment to health care. Because of our faith as part of the Seventh-day Adventist Church, we focus on healing the whole person–mind, body and spirit.

In fact, Seventh-day Adventists believe that spiritual and emotional health are vital elements to overall well being. It is this belief that guides us in all we do at Florida Hospital and it has helped us to create one of the finest health care facilities in the U.S., if not the world.

Would you like your company highlighted here in our "Client Spotlight"? Then give us a call today at: 1-800-900-8324 x8840.

Advanced data backup mechanisms

Most ransomware attacks work as follows. A malware infects/locks your vital data, and you're asked to pay a ransom to regain access. Think of it – if you already have a couple of updated backups of the "stolen" data, you could get your data back yourself as well as involve cyber policing and investigation experts to track down the hackers without fear. Here are some data backup options you can leverage:

- Daily updates of backup with cloud service providers.
- Periodic archiving of data in local storage devices.
- Using network-attached drives to backup the data.
- High capacity SSDs for physical safekeeping of data.

Leverage Group Policy Object controls

GPO restrictions are surprisingly underused, given their time-tested effectiveness in restricting all kinds of malware. GPO restrictions ensure that there are no unsolicited installations resulting from careless end user activity. GPO settings hand over granular control over endpoint file execution to you. Your IT administrators can add rules to block all kinds of suspicious activities related to file installation and execution. For instance, by blocking all kinds of executables in attachments, you can leverage GPO to effectively neutralize many phishing-origin cybercrimes.

Patching commonly used third-party apps

Adobe-, Flash-, and Java-based applications have been employed an untold number of times to infect computers with ransomware. A preventive measure often ignored by IT experts is patching. When third-party software applications are patched, the attack surface for all kinds of malware infection attempts is minimized.

Restrict endpoint administrator rights

We know that there's a widespread sentiment around letting end users have administrator rights to be able to troubleshoot common IT issues, as a way to reduce workplace disruptions. However, if quick resolution of common computer issues is your goal, do it by making your IT teams more agile. End users are not expected to deal with software installations, system settings tweaks, etc. So restrict administrator rights for end users, and reduce the exposure of your workplace computers to all kinds of malware, including ransomware.

Prevent risks of social engineering and spear phishing

The hit rates of phishing emails are surprisingly high because of the advanced social engineering methods employed by cybercriminals. Enterprise IT teams have to invest time, thought, and money in educating their workforce about how they can balance their social presence and workplace security considerations. Work on a social media policy that lays down the accepted and out-of-bounds social media practices for employees. Identifying spear phishing attempts and neutralizing them is critical for safekeeping of employee identities and their computers' data. Consider hiring a third party to conduct social engineering tests, such as ones offered by LIFARS and Rapid7, to make the employees aware of how loose social media practices can ultimately cause millions of dollars to the company.

Other practices

- Implement data leakage prevention and anomaly detection mechanisms to make sure that no data is being leaked out of the company network.
- Filter out macro-enabled files and restrict the execution of such files, because macros often contain malicious codes that release ransomware into the computer.
- Your backups must start only after complete system scans, so that any malicious files are not backed up!
- Remember the words "least privilege" when devising mechanism of access for end users. Users must only be given the least privileges necessary for them to perform expected tasks.

Fake UPS malspam delivers two malicious packages

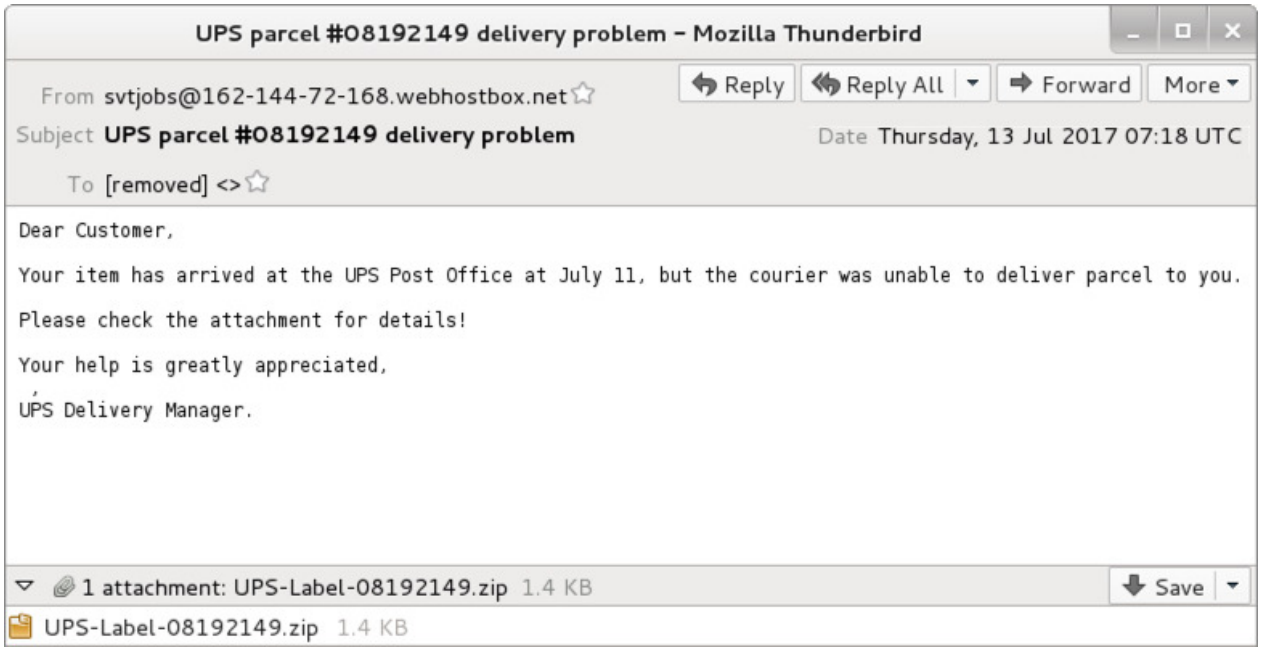
Malspam is a classic hacking technique that still proves successful, especially when the emails in question are made to look quite legitimate. The goal with malspam is to get, as the name infers, malware to infect a machine via spam email. Such is the case with a current malspam campaign that has been monitored by security professionals since late June. According to Brad Duncan, a researcher at SANS Institute, the malspam in question is posing as email from the United Parcel Service and contains a .zip folder with both NemucodAES ransomware and Kovter malware.

As Duncan writes in his report, "Malspam with zip archives containing JavaScript files are easy for most organizations to detect" but, for many organizations, "investigating blocked emails is pretty low on their list of priorities." This is problematic as this particular malspam contains two rather powerful strains of malware.

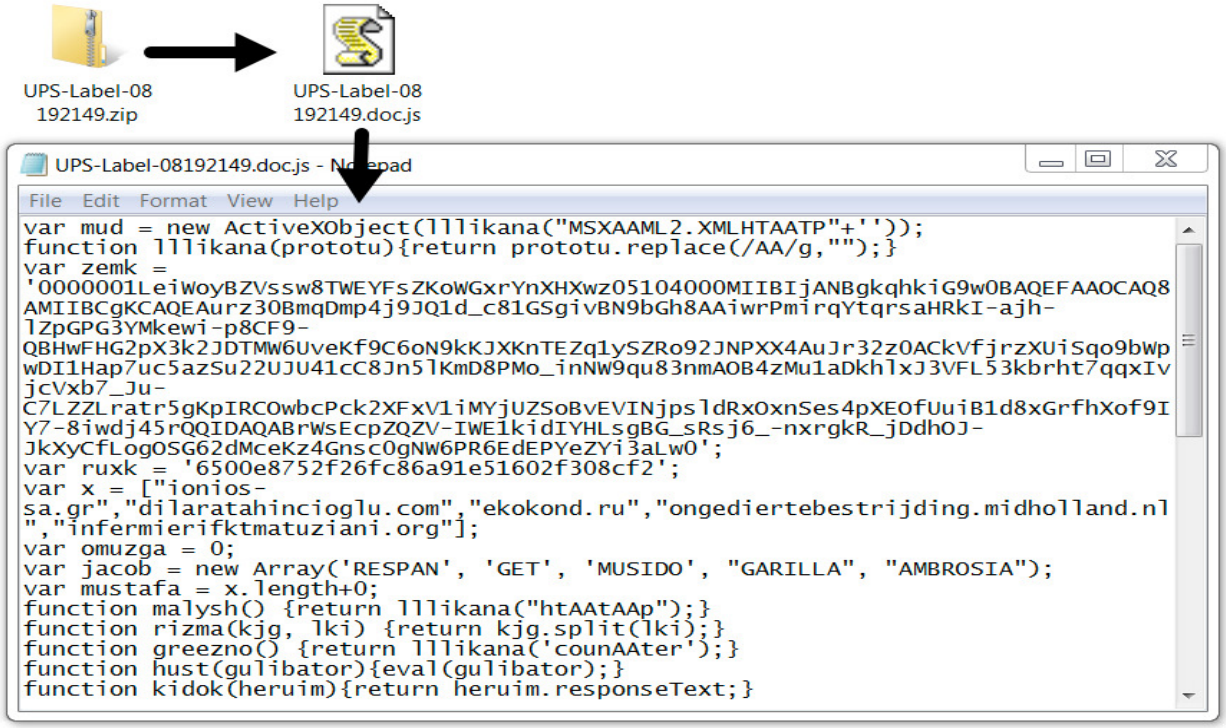
The first of these, NemucodAES, is a ransomware that is written in JavaScript and PHP. It is able to, in addition to encrypting your files with TeslaCrypt (or other ransomware binaries), download other malware. This is the most up-to-date version of Nemucod ransomware strains, and while decryptors exist, the addition of another malware make this attack more complex as it assaults the machine in two ways, both on the machine level as well as the client-side level.

The second of the .zip download is an older malware called Kovter. It was known initially as a ransomware, but eventually was formatted to be a "click-fraud" malware. Basically this creates a situation in which a malicious script generates clicks for numerous websites (which are also malicious) for obvious monetary reasons. During the infection, a hacker can infiltrate and gain control of your machine. Even if the machine becomes decrypted and the ransomware is removed, you still have to deal with the reality that your computer has been used as a hub for click-fraud or worse. The amount of malicious traffic that will have flooded your machine by this point is significant.

Victims are baited to download the .zip file containing NemucodAES and Kovter as the email (shown below) claims the attachment is related to an undelivered package from UPS.



In actuality, the .zip file contains the following malicious code:



THECHANNELCO.
CRN®
MSP 500
2017

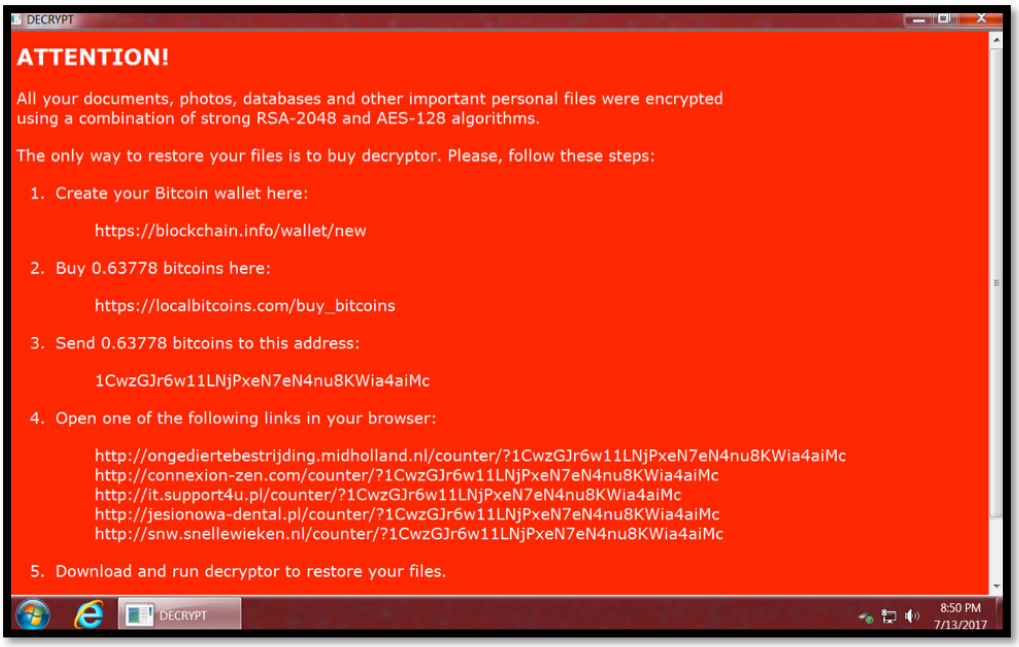
Tech Hero

has made the Pioneer 250 list of CRN's 2017 Managed Service Provider 500 List!

The 2017 MSP 500 list recognizes companies in North America whose approach to delivering managed services is one innovative step ahead.

The MSP Pioneer 250 is a list of channel companies with business models weighted toward managed services and largely focused on SMB market.

The victim is then met with the following message:



The strategy for preventing an infection from this malspam is two -fold. Firstly, Duncan states that "with proper network monitoring, traffic from an infection is easily detected. But some of these messages might slip past your filtering, and some people could possibly get infected." As such, one must educate themselves on the nature of malspam and how not to fall for download requests. If these two countermeasures are deployed, there is a chance that, as this campaign evolves, you can keep yourself and your network safe.