

Wednesday, August 15, 2018

In This Issue

- **WhatsApp and the Spread of Fake News**
- **Cryptomining/Cryptojacking**
- **Microsoft (MS) Supplier's Supplier Victim of a Supply Chain Attack**

This Month's Tips:

If someone asks you to give them personal information access to confidential information, don't be afraid to be direct and say no. Anyone suspicious should be denied access until you can verify their identity.

Move your mouse over a link without clicking on the link to see the actual address of the site. If the address differs at all from your expectation, you should not click on the link. You can also right click and copy the link and then paste it into a text file to see where the link leads.

Ultimately, common sense is your best protection. If an email, phone call or online message seems odd, suspicious or too good to be true, it may be an attack.

WhatsApp and the Spread of Fake News

Facebook is once again caught up in a fake news controversy, this time with its social messaging service, WhatsApp. The recent spread of false news through the messaging app, WhatsApp, has resulted in violence and even death in India. Recently, a video circulated on the app that appeared to depict child kidnappers. The video was actually an instructional safety video but was shared with a fabricated text warning about kidnappers in the local area. The fear of potential kidnappers running around their community resulted in the killing of two innocent men by an angry mob. This plus other violent incidents have WhatsApp and the Indian government searching for solutions to prevent similar acts of violence.



Because of WhatsApp's end-to-end encryption between its users, it is impossible to track where fake news stories originate. However, the Facebook-owned WhatsApp has taken measures to curtail the spread of fake news by:

- Reducing the number of people a message can be forwarded to from 100 to 5 in India
- Removing the "quick forward" button that had appeared next to messages containing photos, videos, or audio
- Introducing a "suspicious link" label that appears next to links in messages where the app detects something problematic, such as an unusual combination of characters
- Releasing newspaper ads warning people to "question information that upsets you"

These actions are a start to resolving the issue of fake news spreading on WhatsApp, but as well all know by now, fake news is still an issue across any platform that allows for the spread of information. In order to prevent yourself from falling victim to fake news, here are some best practices to follow:

- Beware of stories that might exploit your emotions, especially anger.

- Carefully scrutinize the news you read, regardless the source.
- Familiarize yourself with the author or contributor.

Using these simple strategies can help you avoid the pitfalls of being misled by fake news. Remember, when in doubt, always check it out.

Cryptomining/Cryptojacking

With the growing popularity of cryptomining and large reported cryptocurrency dividends, a hacker is never far behind. Hacker criminals have recently been reported using a ransomware-like strategy to get employees' computers to mine cryptocurrencies on their behalf. Known as cryptojacking, it is the unauthorized use of someone else's computer to mine cryptocurrency.



This is done by tricking an employee to open a malicious link inside an email that in turn uploads cryptomining code onto their computer, or to visit a website or online ad with malicious code that automatically uploads in the victim's browser. The cryptomining code works in the background, often without the employee knowing. A slow-moving computer may be the only sign they notice that something is wrong.

Experts say there is no way to tell how much cryptocurrency is being mined through cryptojacking but that it is nevertheless on the rise and growing fast, because it's easy money, does not require elaborate technical skills, and kits are available on the dark web for as little as \$30.

In January, investigators discovered the Smominru crypto mining botnet, which infected more than a half-million computers, mostly in India, Taiwan, and Russia. The botnet targeted Windows servers to mine Monero, and cybersecurity firm Proofpoint estimated that it had generated as much as \$3.6 million in value as of the end of January.

Prevention Tips:

- Use endpoint protection capable of detecting known cryptominers.
- Keep your web filtering tools up-to-date.
- Maintain browser extensions. Some attackers are using malicious browser extensions or poisoning legitimate extensions to execute cryptomining scripts.

Microsoft (MS) Supplier's Supplier Victim of a Supply Chain Attack

Microsoft recently reported that one of its software supplier's supplier was the victim of a supply chain attack. The attack originated within a company that provides font packages for a PDF editor application to another vendor that supplies these font packages to MS. These packages were



provided as Microsoft Installer (MSI) files that provided escalated system privileges to the installation packages. The attack is believed to have run from January to March of this year.

One of the MSI files was a malicious file containing a cryptocurrency miner. The malicious file was easily recognized, because it was the only software file that did not contain the digital signature from the company creating the file. The malicious file was named *xbox-service.exe* and was automatically installed along with the legitimate MSI files.

The malicious actors were then able to replicate the company's cloud platform and redirect the victim company to the replicated malicious site. From the replicated site, the threat actors were able to install the corrupted MSI files into the Microsoft supply chain.

The attack was first discovered when the Microsoft staff received alerts from the Windows built-in antivirus program Windows Defender. There they found the MSI files missing the required digital signature of the producing company.

This attack could potentially affect other third-party vendors serviced by the victim company. There have been six different companies identified that may receive font software or other potentially malicious software from the victim company. However, there is currently no evidence that they have been impacted by the malicious code.

Inspired eLearning | 613 NW Loop 410 | Suite 530 | San Antonio, TX 78216

[Forward this email](#) to a friend.

© 2018 Inspired eLearning, LLC. All Rights Reserved.

All organizations with an active Security Awareness license are granted permission to republish any or all of the content in our Security Awareness Newsletter, as long as distribution of that content is limited to employees within the organization.