Science Translations
Established 1990
PC410.COM™

Managed Services,
PC Consulting, Sales, & Service in Central Maryland

The latest Ransomware isn't Ransomware

The Petya Ransomware that has been leading news headlines for a few weeks is a little different from other ransomware. Petya enrypts hard drives, and then connects to other computers on the local network to encrypt them as well, and it asks for a ransom. But Petya is not ransomware, according to an independent researcher, and confirmed by Homeland Security's CERT, also known as the United States Computer Emergency Readiness Team. While the software claims to encrypt files, what the code analysis shows is that the hard drive boot sectors are overwritten and the files are essentially wiped. There's no way to go back to the original files. So paying the ransom is pointless; no one will get their files back from this one.

More on Petya at CERT:

https://www.us-cert.gov/ncas/alerts/TA17-181A

". . . there is no evidence of a relationship between the encryption key and the victim's ID, which means it may not be possible for the attacker to decrypt the victim's files even if the ransom is paid."

And to add more complexity: The antivirus industry names these things based on similarity to other malware they've seen, which isn't much more than a category. The result is that there are multiple malware programs known as 'Petya'; some are broken, at least one is a wiper, and some are ransomware.

Why create such a thing? Eventually, we'll know more, but as of now, it's likely that it's political and that the author of this particular Petya is a nation-state, possibly targeting the Ukraine.

So far, this mis-labeled disk wiping software is mostly clearing hard drives in the Ukraine, and on computers running Windows versions that use old network communications methods for talking to each other, basically Windows 7 systems missing the March security patch (number KB4012215), and older systems, especially Windows XP. Microsoft has made an exception to their security patching calendar and provided a patch for Windows XP in this case, but this doesn't change the basic rules for running computers safely:

- Don't open attachments from unknown sources. Most of these are new versions of malware, too new for antivirus software to recognize as bad.
- Windows versions older than Windows 7 should be retired or taken offline, no exceptions. These Windows versions are obsolete, and no longer patched: XP, Vista, and Windows 8. Windows 8 qualifies for an upgrade to 8.1, which can still be patched.
- Windows 7 & 8.1 need patching monthly. Windows 10 patches can't be turned off, but should be checked regularly to make sure they're up-to-date.
- Patches include updates for Adobe products, as well as Apple, Firefox & Thunderbird, Google Chrome, and Java. Microsoft Office has security patches too, but they'll end later this year for Office 2007; it's time to move to something newer.
- Local backups should have versions; keep at least the last three backup sets, spread over at least a month.
- Cloud backups should have versions. 30 days of old versions of files is generally adequate.

I have automatic patch monitoring and updating available for managed service plans and cloud backups available at $50/pc/year. Call for recommendations.

Local Tech News is Fake News

Petya was mis-reported as if it were ransomware, and it is news that should be compared to most product safety recalls; that really describes it best. Petya is opportunistic and malicious software, that takes advantage of old errors in Microsoft Windows to wipe hard drives, and some users of Windows have to get repairs or stop using the product.

But yes, it's fake news; it follows the normal pattern in local technology news reporting of reading the network news feed from days earlier and treating it as still-newsworthy filler, while newer information has contradicted the original headline. All of the Baltimore television and radio stations are consistently guilty of mangling tech news by editing week-old tech news down to three sentences that fail to answer basic questions, and then they pair it with stock footage or a one-sentence quote from a "security" expert not involved in finding the problem, and rerun it in every newscast for 24 hours, without updates. It's misleading; the action points for consumers are wrong.

If you hear a news story report about a tech topic, computers, phones, the latest ransomware, the best plain-English place to look up what's really happening is c|net, run by CBS Interactive. (And yet CBS news isn't immune to bad reporting on tech issues. Hmmm.)

c|net is online here:

https://www.cnet.com/news/

Or you can just type in their old web address; it still works: ‘news.com’

c|net has more than just tech news–there are product reviews, tech tips, and information on tech that isn’t all computers: cell phones, cars, smart homes, and movie reviews that would appeal to anyone who likes technology. (Basically any movie with any of these terms in the description: Star Wars, Star Trek, Marvel, or DC.)

Contact

Address all editorial and unsubscr be requests to:
Jerry Stern, Editor, Science Translations, P.O. Box 1735, Westminster MD 21158

Phone (410) 871-2877