Blog for MPA Networks

https://www.mpa.com/blog.aspx?p=ransomware-is-getting-even-worse-and-the-feds-cant-stop-it

Ransomware Is Getting Even Worse …and The Feds Can't Stop It

Posted January 21, 2016

As chaos reigns across much of the Middle East, our government steadfastly insists that "the United States does not negotiate with terrorists—because it will only encourage them in the future." Meanwhile, visitors to our National Parks are warned never to feed bears and other wildlife—because those hungry bears may come to *demand* their next meal from campers!

Yet if cyber-gangsters in Eastern Europe hijack an American company's data with an encryption virus before charging a hefty ransom to remove it, our same government recommends to "go ahead and pay them." What's going on here?

"Don't Say We Didn't Warn You…"

Over two years ago, we first talked about CryptoLocker and other **ransomware**—probably the most dangerous cyber-threat to businesses today.

This isn't just another "nuisance" cooked up by a hacker in his dorm room. International organized crime syndicates have used sophisticated ransomware schemes to extort removal fees—typically between $200 and $10,000, paid in untraceable Bitcoin—from companies in the U.S. and around the world.

The newest strain of ransomware to be spotted "in the wild" is CryptoWall 4. Spread via email attachments and malicious websites, CryptoWall 4 is a "double-whammy"—not

only encrypting vital hard drive data, but also scrambling filenames, making it impossible to tell *which* files have actually been infected.

It's been determined that CryptoWall's source is inside Russia—the malware is cleverly designed to ignore computers using Cyrillic-Russian keyboard language (Russian authorities are quick to prosecute Russian-on-Russian cybercrime, while the rest of the world is apparently "fair game"). **Previous versions of CryptoWall alone have already robbed victims of an estimated $325 million—in Bitcoin ransom payments as well as lost productivity and residual costs (including legal fees).**

Uncle Sam to Victims: Sorry We Can't Help

What can our government do to bring justice to the victims of ransomware? As we've discussed, not much. Given our frosty relations with Vladimir Putin's regime, Russian law enforcement is in no hurry to cooperate. At October's Cyber Security Summit in Boston, Joseph Bonavolonta, Assistant Special Agent in Charge of the FBI's CYBER and Counterintelligence Program, confessed: "The ransomware is that good… to be honest, we often advise people to just pay the ransom."

In other words, imagine being robbed at gunpoint on a busy street corner in broad daylight—while the cops watch and shrug. Yes, it's that scary.

How Can You Protect Yourself?

- Bitdefender is offering a free downloadable CryptoWall 4 "vaccine" to prevent infection.
- Ensure all your PCs are always fully updated (Windows, anti-virus, firewalls, browsers) with the latest security patches.
- Enable pop-up blockers on all browsers, and disable plugins from running automatically.
- Backup *all* your data, all the time. Consider backing up the backups.

For more ideas on how to protect your company from ransomware and other emerging threats, contact us.