CCS Technologies

August 2017
Volume 12, Issue 8

"Local Support • Personal Service • Since 1976" www.ccstech.net "Relax...we're on IT"

300 Main Street, Coopersville, MI 49404
616.997.TECH(8324)
Fax 616.997.9317

206 Washington, Grand Haven, MI 49417
616.842.TECH(8324)

3489 Kelly Street, Hudsonville, MI 49426
616.669.TECH(8324)

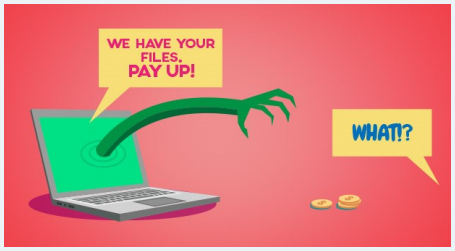
Caught in the Crossfire: Our World is a Very Dangerous Place

by Jeff Verry

When elephants fight, it is the grass that suffers. So goes the old proverb, and so goes the current state of cybersecurity in 2017. We've already seen worldwide infections via multiple versions of so-called ransomware – malicious software that holds a computer's stored documents, pictures, and now even accounting files and backups hostage until a price is paid to unknown criminals under the table using online currency like Bitcoin.

"Who makes this stuff?" It's a question we get with some frequency. Why would anybody go through the trouble of creating a computer virus? It used to just be bored kids living in their brother's basement just doing it for kicks or bragging rights (some of you may remember Melissa97). Oh weren't those the days…

Now it is presumed that most attacks found in the wild are the product of organized crime syndicates in a ploy to make money. "Criminal organizations have always found innovative ways to extort money," says digital forensics expert Lesley Carhart, and ransomware is lucrative because it "plays on people's emotional and financial reliance on their computers." Security firm Symantec reports that the average money made in a ransomware attack has gone up 266% since last year.



So the shady business of virus writing has gone from glorified hobby to professionalized extortion. The latest forms of attacks we are seeing are even worse – it is all out war. The latest "ransomware" that proliferated across the Internet last month had an interesting feature, it had no way of actually giving you your files back. The conclusion held by most is that it was not ransomware at all, but rather a cyberweapon designed by professional software developers to deliberately target and disrupt computers at the operating system level.

FedEx has already reported that they will need to lower their next quarter earnings due to being "unable to fully restore all of the affected systems and recover all of the critical business data that was encrypted by the virus" in its Ukraine based operations. They cite over a dozen points of damage including:

- loss of revenue resulting from the operational disruption immediately following the cyber-attack;
- loss of revenue or increased bad debt expense due to the inability to invoice properly;
- loss of revenue due to permanent customer loss;
- remediation costs to restore systems

Like any good business person or concerned user, you are undoubtedly asking yourself the question, so what now? Here are three critical takeaways you can take into consideration immediately:

If it can happen to FedEx, it can happen to you. There is no system that can guarantee total security. Just like no car, however safe, can keep you from being hurt if the accident is bad enough, no computer security is 100% effective. By all means, take all of the precautions we have recommended in the past: firewall, anti-virus, user training, regular updates and backups.

This has become a (virtual) shooting war. The NotPetya virus described above was of North Korean origin, using tools created by the CIA, and targeted the Ukraine's infrastructure (it successfully shut down one of their airports). We are living in very dangerous times. Taking out identity theft insurance might not be a bad idea. Watching your credit score and your bank accounts doesn't hurt either.

Did I mention backups? This cannot be said adamantly enough: when the crisis hits, nothing beats having a restorable backup. If you are not sure how to back up your computer or what kind of system is best for your business, please give us a call and we can help you.

Our reliance on our computers and the data they contain and transmit has never been greater. At the same time, threats have escalated steadily over the past months and the danger has also never been greater. If you have any questions or concerns about your security, your computer's health or even how at risk your employees' behavior might be, schedule a consultation with a *CCS Technologies* technician today.

"Relax...we're on IT"

Contact Information

Information	Info@ccstech.net
Tech Support	Support@ccstech.net
Sales	Sales@ccstech.net
Greg Slater	Gslater@ccstech.net
Ellen Slater	Eslater@ccstech.net
Drew Rowe	Drowe@ccstech.net
Jeff Verry	Jverry@ccstech.net
Joe Halstead	Jhalstead@ccstech.net
Jorge Arias	Jarias@ccstech.net
Karen Strickland	Kstrickland@ccstech.net
Mark Kowitz	Mkowitz@ccstech.net
Ryan McMillen	Rmcmillen@ccstech.net
Eric Ruzek	Eruzek@ccstech.net
Tammy Sanders	Tsanders@ccstech.net

CCS Technologies Store Hours

Coopersville Store

Mon-Fri 8:00 am - 5:30 pm, Sat 9:30 am - 12:00 pm

Grand Haven Store & *Hudsonville Store*

Mon-Thu 9:00 am - 6:00 pm, Fri 10:00 am - 6:00 pm

Sat 10:00 am – 3:00 pm