Cryptowall Virus

A friend of mine's law firm down in Florida just got hit with the Cryptowall Virus. He was extorted for $1000 to have his files un-encrypted (apparently after the virus takes control a window pops up allowing you to pay $500 by bitcoin or $1000 by PayPal gift card). Just thought I'd pass it along. He paid because another attorney in his town was hit and didn't pay. Subsequently, the other attorney missed the SOL on a PI case. Judge down there said he wasn't sure if he could extend the SOL and it's pending. Here in NY, it's written into the statute that a judge cannot extend the SOL on any case.

If it was just the virus, my buddy would have been ok, turns out the IT guy screwed up by allowing the secretary to have administer rights which she should have never had and also that his back up failed. Anyway, just thought I'd share that.

I'll add that the virus only gives you something like 24 or 48 hours to pay, after that you cannot pay even if you want to.

Michael A. Huerta, New York

This is terrifying. I'm paranoid about getting hit by something like this.

William Chuang

Kinda makes you want to review your opinion on the death penalty.....

James P. Moriarty, Iowa

I just want to point out that one of the first things anyone should do after purchasing a new computer is create a user account which does not have administrator rights and add a password <-this is the account you sign on and use on a daily basis.

You also need to change the default password on the administrative account. When you need to administrative rights (as in you have purchased a new something and want to install it) - you switch users; but you always work in the non-administrative rights account.

The point being, the IT guy should have done this on all firm machines, not just the secretary's PC.

Regards,

Andrea Cannavina, not a lawyer

Thx Andrea. Good to know. What if I have an Admin account on my PC that was created by my IT guy years ago, but he has retired and I don't know what his password is/was? I think I too have full rights using my regular non-Admin login, but would like to be able to switch, as you have suggested. Thx.

Lyza Sandgren, not a lawyer, Georgia

I've posted on computer security a few years ago. I cut and pasted it and expanded topics a bit.

(1) Computers should not be run on an administrator account. Use a user account to reduce the risk of bad things happening. Use Firefox or Chrome with an adblock plugin. There are instances where a website is secure but the ad server is infected and will infect you.

(2) Use a good anti-virus/anti-malware program with an integrated software firewall
on every computer. I use Norton Internet Security but you can search for other products.
Scan your computers constantly because just one bad computer on the network can compromise the entire network.

(3) Put your network on OpenDNS,
which will block known malware servers transparently. You can also selectively block objectionable material such as pornography and the like.

(4) Patch all of your software. Keep up with Windows Updates, Microsoft Office Updates, etc.
Bad guys review patches to see what security flaws are fixed, then come up with exploits. A patch thus becomes a race between the users to install the update and the hackers to take advantage.

(5) Don't open attachments from emails unless you know the sender. Even if you know the sender, don't open "spammy" emails with extensions.

(6) Create backups. My information is stored on a file server, which is

then backed up onto a hard drive, then backed up using CrashPlan. My work documents are stored using Google Drive. Don't rely on just a hard drive, or just Google Drive/DropBox/OneDrive. You need to keep your data in at least two places.

(7) Use a password manager. I personally use LastPass. Others use KeepPass. You can make your own decision but do not use the same password on multiple sites. A password manager will generate unique and complex passwords for each website, so that if one website gets hacked, the bad guys can't simply use the same login information for all the other sites.

(8) Use two-factor authentication. I use Google Authenticator in connection with LastPass. So even if someone can guess/hack my LastPass password, they still can't get in unless they have my cellphone and guess the PIN, then use GA. For Gmail and now DropBox, you can use a FIDO U2F USB key that costs about $20, and makes that login essentially unbreakable.
â€‹
Most banks and other financial institutions has some form of two-factor authentication such as texting or emailing a key each time you login. It's a pain, but you should enable two-factor for each website that supports it.

(9) Encrypt everything. I use Bitlocker and TPM to encrypt my computers, laptop, and file server. My tablets and cell phone is also encrypted. The NSA or the CIA or the FBI can perhaps hack into my stuff but the average thief probably wouldn't be able to do so. He'll just be forced to wipe the data off and reinstall the operating system, which is okay with me.

William Chuang

William Chuang, thanks for sharing these great ideas. What about those of us without a typical cellphone? How do we do two-factor authentication if we don't have a cellphone?

Thanks for this thread of emails.

Roberta Fay, California

Cell phone or dongle are the two main methods of two factor authentication. You can also do iris scans and fingerprint recognition. All require some extra equipment. Of them all, a cell phone is least expensive and most versatile for most consumers and small businesses.

Darrell G. Stewart, Texas

I don't know about two-factor without a cell phone. Some websites (such as Chase) will send you an email or call you. However, most will require a smartphone to run an app, a cell phone for tests, or a FIDO U2F USB key.

William Chuang

Good reminder - if you haven't tested your backups then you haven't backed up.

We got a call from a company a couple of years ago that had a server crash on them. They'd been running nightly backups so they got a new server, installed the operating system and went to restore the most recent backup. At that point they discovered that their nightly backups hadn't actually worked in over a year.

Lots of painful (and expensive) data recovery and rebuilding ensued.

Testing backups is not difficult. Create a dummy file - it can be a Word document, a Text file or whatever. Name it "Dummy Backup Test File" if you want to. Store that file among your important files.

Then, every now and then (I recommend quarterly but your mileage may vary) delete that dummy test file and then go to your backups and see if you can restore it. If you can't then you know one of two things:

1) You don't know how to restore files in your system. That's easily fixed but should be fixed.

2) Your backups aren't working properly. That needs to be fixed ASAP.

If you have any databases (like QuickBooks or a practice management system) run on-site then you should confirm with the vendor if there are any special backup/restore procedures for that. Sometimes restoring a database isn't quite as simple as restoring a file.

And yes...try not to run your daily operations using an account with admin privileges. We've seen firms where even the RECEPTIONIST account even had domain admin privileges - simply because the IT guy who set it up either didn't know any better or was too lazy to lock it down.

Disclaimer: Still never been a lawyer.

Ben M. Schorr, Arizona