CryptoLocker & Ransomware
The “Cop” Version

Presented by

CJIS Solutions

Law Enforcement’s Problem –

In Law Enforcement Terms!

For years Ransomware and the CryptoLocker virus have been out and about infecting computers and costing businesses millions in losses. However as with most things in law enforcement, this too is catching up to agencies and is now becoming a main stream issue.

There are a lot of technical documents that cover this subject however this White Paper is not meant for the technical audience. This document will assist the law enforcement professional in understanding the issue from the cop’s perspective.

Ignoring this issue is like ignoring your dentist. You’ll lose your files just as you could lose your teeth! ***This document will help you save your department’s files, protect your department’s reputation, and keep you out of the news!***

What is Ransomware and CryptoLocker?

Simply put, it’s a virus that enters the user’s computer and encrypts the files so no one can use them. The software runs silently and uses minimal computer power to avoid being detected. It may even take a few days for it to appear. As the virus runs, it scans your computer, as well as any attached storage (such as additional hard drives or even connections to your server) and encrypts files as it goes. The encryption, is what is called AES-256 and some studies have shown that it would take thousands of high powered computers about a million years to break the code (seriously).

A user will normally get a warning message saying that their files are encrypted and then steps needed to pay the “ransom”. In other cases, you’ll go to open a file and it won’t work. When you pay your tech guy 2 hours to look into it, he’ll tell you that there’s instruction files for paying the ransom. So now you have to pay your support guy *and* the ransom!

Sample Warning Message:

Help is on the way!

How is your agency susceptible to the virus?

First know this, if you are connected to the internet, or allow external devices to connect to your computer, you are never 100% protected from viruses. There is no silver bullet antivirus program that will 100% stop everything.

Even with all of your CJIS controls in place, a simple click from an uneducated user is all it takes. Here are the key ways a ransomware/Crypto virus enters your system:

- Opening of attachments – For some reason cops open E-mails that they should know aren’t for them. If you get E-mails telling you that your airline tickets are attached and you didn’t book a flight, then don’t open it! ONLY open attachments on your E-mail from KNOWN senders. You’re a cop, if you feel suspicious, then check with the sender to make sure the E-mail is legitimate. Some extensions to be weary of are .zip, .exe, and even some .doc and .pdf files.

- Opening of a link – Again, maybe it’s the trigger finger but cops love clicking links. As with attachments, if you do not know the sender, or feel the link doesn’t make sense then do NOT click it. Clicking a suspicious link can create actions that will automatically install the virus without anyone knowing.

- Clicking inappropriate ads – Some ads are there to bait you into a click, by the time you realize it the damage is done.

- Permissions – Sorry to say but even Chiefs click a bad link here and there. By giving server or domain permissions to everyone because of their rank and not their technical need is an easy way for a bad link to cause a lot of damage.

Unfortunately 99.9999% of all ransomware or CryptoLocker viruses are installed by user error. So how do you really protect yourself if it’s so easy?

Well – read on.

How to protect yourself?

The do all – end all solution is a proper data backup solution which we'll cover. But before you're restoring files, let's follow these steps first in efforts to prevent the virus first:

- **Domain privileges** – Sorry Chief but if you don't need to have Administrator privledges, please use a regular account. If you get the virus, your Administrator privileges will give the virus a blank check to do what it wants to your system.

- **Installation Restrictions** – Adding restrictions in your domain or user accounts to prevent software installations is a great step. By the nature of the user's logon, they will be prohibited from installing anything on the computer or network.

- **Internet Content Management** – An add in solution such as AVG Cloud Care provided by CJIS Solutions, monitors and regulates the internet activity of specific computers and prevents them from going to known bad sites.

- **Intrusion Prevention** – A portion of your firewall system that monitors your incoming internet traffic for suspicious activity. At CJIS Solutions, everything we use is behind multiple intrusion preventin devices.

- **Aggressive Anti-Spam Software** – A no brainer but keep in mind, more strict + more safe = less convenient. No one likes having their mail held in SPAM to be cleared but remember, this is serious stuff we're talking about and you need to take serious steps. Hosted E-mail from CJIS Solutions employs very strong technology to meet this need.

- **Educate** – Roll call, department E-mail, whatever you have to do, inform your staff at all ranks, the do's and dont's covered here.

Data Backup!

A proper data backup solution is the true way to cover yourself when all else fails. It's inexpensive and works. Data backup from CJIS Solutions comes in all shapes and sizes and CJIS Solutions offers multiple approaches to data backup and can save your files before you're wondering where they went. You can't restore what you don't have so the worst thing you can possibly do is wait.

This white paper was actually created because CJIS Solutions support staff continues to restore agencies from encryption "Crypto" viruses up to this day. We have seen the victory of a restore as we have the anguish of defeat when an agency calls who doesn't have backup.

DO NOT WAIT – CONTACT US TODAY SO WE CAN PROTECT YOUR DEPARTMENT'S FILES!

CJIS Solutions, LLC
P.O. Box 1102
Little Falls, NJ 07424-1102
855-955-CJIS
www.CJISSolutions.com

CJIS Solutions
CJIS Compliant Hosted Solutions for Law Enforcement.

Sales@CJISSolutions.com