SECURITY REPORT:

How Ransomware and Malware Affect SMBs

This report has been written and provided by:

Veltec Networks

Veltec Networks, Inc.
408-849-4441
info@veltecnetworks.com

Many SMBs are having to re-think their disaster recovery and business continuity strategies due to the recent spike in ransomware attacks in recent years, but also because of malware infection in general and how it operates. Many enterprise owners and staff don't even know what a ransomware attack looks like. And, with its covert ability to sneak into IT networks virtually undetected, organizations and enterprises have to make cybersecurity and disaster recovery a main priority, right alongside sales, productivity, and accounting.

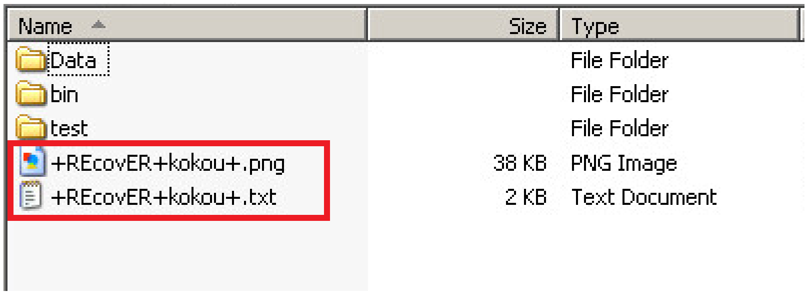
For those of you still getting familiarized with it, ransomware is a type of malware that encrypts the files on a computer, and then holds them hostage for a ransom fee in order to regain access. It normally spreads through email phishing attacks, exploit kits, removable drives or external network shares. New strains have appeared online with alarming frequency, and traditional antivirus programs cannot prevent these attacks until they have been identified – too late, in most cases, leaving many small and medium-sized businesses open to a data loss disaster.

Here, we aim to investigate and advise on the preparedness of decision-makers at small-to-midsize businesses (SMBs), so they may better protect their ventures against malware cyberattacks, and provide advice from IT security experts on how to avoid disaster. One of the most salient pieces of advice given by experts – and the FBI alike – is to never pay the ransom fee. Instead, consult with an IT services expert, who will generally be able to go in and bypass the malware program's link to a C&C server, and thus halt the efficacy of the attack.

What Ransomware Looks Like

Because many business owners still have no basic working understanding of what ransomware even looks like or how it operates, here is some graphic evidence for your edification. Ransomware uses encryption to lock-up your database in a very aggressive way. It uses a public-private key encryption interface or procedure to do so. With great stealth, it uploads its file "payload" onto hard drives.

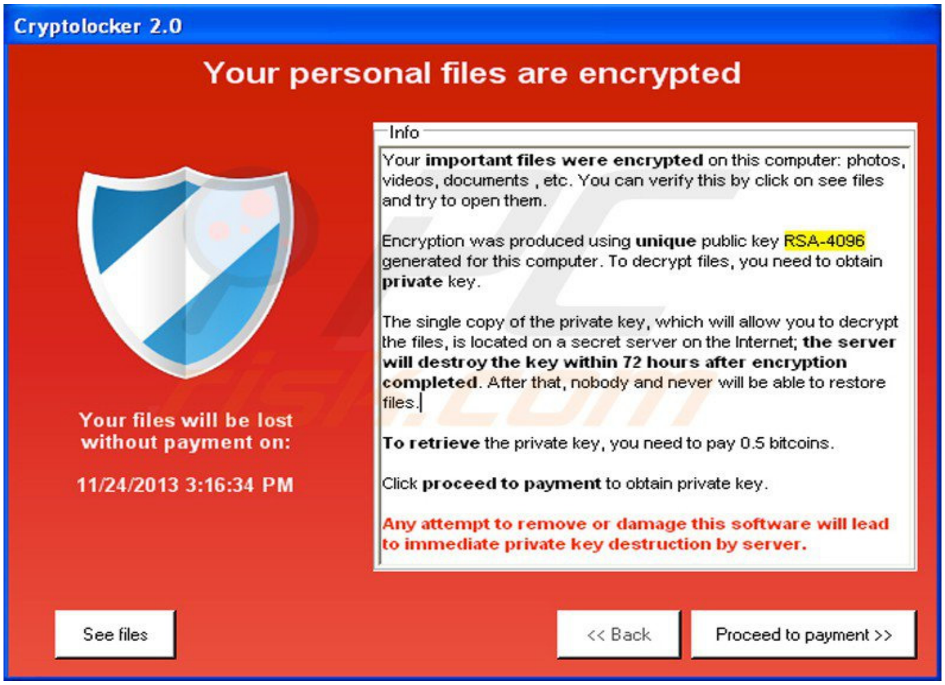
One such example looks like this:



Name	Size	Type
Data		File Folder
bin		File Folder
test		File Folder
+REcovER+kokou+.png	38 KB	PNG Image
+REcovER+kokou+.txt	2 KB	Text Document

The ransomware files are in red, where the file-encrypting and "ransom note" files, respectively, sit in your system cache. Ransomware works so fast to encrypt and lock up your files now that total file encryption of your entire database can happen within a few minutes of you inadvertently clicking on a "mimic" email link. The ransom note will demand a certain amount of money – generally requested in Bitcoins – in order to obtain the private decryption key housed on a command and control (C&C) server which is running the operation remotely.

Here's a graphic of what a CryptoLocker attack looks like:



Cryptolocker 2.0

Your personal files are encrypted

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

To retrieve the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Facts on Malware Attacks and SMBs:

- 67% of SMB executives claim they would never pay a ransom to regain access to company files if their systems were infected with ransomware.
- Only 23% of SMBs in one sample say they are "very confident" their data is secure from a ransomware attack.
- A mere 31% of SMBs have irregular or non-existent file backup, meaning they would forfeit their files in an attack.
- Only 34% of SMBs test their file backups regularly to ensure that their data has been properly saved and is retrievable.
- Almost one-quarter, or 23% of SMBs say they currently do not have a disaster recovery plan for restoring backed-up data.

(Facts on Malware Source: SoftwareAdvice.com)

These are troubling statistics to be sure. Ideally, closer to 100% of respondents would say they would **never pay a ransom fee** to cybercriminals to unlock their files. Especially since new strains of ransomware will still kill your files anyway, even after you've paid. And, those low numbers on file backup and disaster recovery readiness need to be much higher as well, as just one day of downtime can cause great financial harm, let alone permanent data loss.

Some Other Interesting Information:

- **Hollywood Presbyterian Medical Center attack that cost the hospital $17,000 and took its network offline for days**

- **Researchers at IBM Security's X-Force team released data showing that 70 percent of businesses infected by ransomware have paid to get their information back**

- **Twenty percent of companies have paid more than $40,000 in ransom**

What can you do to save yourself from being a victim?

- Patch Management
- Anti-Virus and Anti-Malware
- Invest in a good firewall
- Backups
- Anti-SPAM for your emails
- Web Filtering
- Strong passwords
- Employee training

Get Expert Help for Ransomware Readiness

If you have questions regarding better disaster recovery planning and preventing ransomware attacks, Veltec Networks, Inc. is a proven leader in providing IT consulting and cybersecurity in San Jose.

Contact one of our expert IT staff at (408) 849-4441 or send us an email at info@veltecnetworks.com today, and we can help you with all of your data defense and disaster recovery planning needs.