You Can Take the Sting Out Of Ransomware

Michael J. Corby, CISSP
Consulting Director, M Corby & Associates, Inc.
Ransomware is rampant across the internet and organizations are paying the criminal hackers who are holding their critical information hostage. Ransomware is a type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid. Attend our June 22 SMP webinar to learn how you can protect yourself from being a victim of ransomware.

Chasing after ransomware components requires constant attention and often yields results that are inconclusive or too late. This session will focus on the protection from the harm threatened by a ransomware attack.
The challenge of security threats is growing and is being recognized as a major risk

Among hundreds of U.S. business and IT managers polled:

- 93% felt vulnerable to security threats
- 53% saw privileged users as their biggest threat
- 44% had a breach or failed a compliance audit

Recent analyses also indicate:

- Remediating a successful attack costs $445,000 per incident
- Consequences of an attack costs $15M in annual company losses
- Only 40% of IT budgets include funding for security threats

*CGI’s 2016 Voice of the Client survey indicated that our clients view Insider Threats as a needed subset of an overall cybersecurity program.*
The spectrum of security threats

- **External Threats**
  - Phishing/Scam Emails/Malicious Websites
  - Malware Detection and Detonation Tools
  - Data Loss Prevention
  - Training and Awareness
  - Privacy Legal/Ethics
  - Industrial Security Programs
  - Behavioral Analytics
  - Coordination with IC: Threat Intelligence Briefings
  - Nation State-Sponsored Industrial Espionage

- **Internal Threats**
  - Fraud
  - Financially Compromised
  - Internal Hacktivist
  - Disgruntled Employee
  - Disgruntled Executive with Insider-Crown Jewels Access
  - Negligent User

**Human Targets of Opportunity**

Increasing Capability, Sophistication & Access
What is Ransomware?

- Ransomware is malicious software that, when installed on a victim computer, has the capacity to remove files, programs and functions, hide or encrypt critical information or capture and publish sensitive data if payment (ransom) is not paid within a certain time period.

- Ransomware infections have recently seen an increase because of the anonymity of the Bitcoin payment method.

- **IN HEALTHCARE:**
  Healthcare has been a primary Ransomware target because of the high cost of a HIPAA privacy violation if private data is publicized, and also because proper medical treatment is highly dependent on the availability of electronic medical records.

- **IN FINANCIAL SERVICES:**
  Financial Services is also a popular target because of its demand for accurate and timely transaction reporting. It is also an industry that is heavily regulated toward protecting personal identity.
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Contact Us
What Are The Effects Of Ransomware For Healthcare (In addition to ransom $$$ if you pay)

Direct Loss of Key Organizational Data
- Patient medical information
- Billing and Insurance information
- Facility and equipment scheduling
- Medical Staff Scheduling

Loss of Processing During Recovery
- Disconnected Computers, Servers, Data Storage devices
- Even if Restoration is possible, it may not be immediate

The Public Relations Disaster
- HIPAA Privacy
- Newsroom and Live Reports
- Social Media and Opinion Sites

Reduced Ability to Conduct Business
- How robust is your Business Continuity Plan?
- What about procedures in progress?
Recent Healthcare Examples

- FBI estimates that in the first quarter of 2016 $209 million was collected by ransomware crooks. Some examples:
  
  Hollywood Presbyterian Medical Center – extortionists demanded $3.6 million from to unlock ransomware. **They paid $17,000.**
  
  Chino Valley Medical Center and Desert Valley Hospital, were infected with ransomware. The owner of the medical center, Prime Healthcare Services, confirmed "**significant disruptions of hospital systems.**"
  
  Methodist Hospital, was recently infected by a ransomware attack. The strain of the ransomware was confirmed as: **Locky**, a new variant of Cryptolocker. **The ransom demand was $1,600.**
  
  Pironti - threatened with a DDoS attack if they didn’t pay $9,000. Instead, they spent more than $200,000 on DDoS technology and consultants. The attack never came.
Significant Wannacry Events

• **UK National Health Service (NHS)**
  – December 2016: “nearly all NHS trusts were using an obsolete version of Windows (Windows XP)”
  – Approximately 40 NHS-connected organizations were affected
  – Operations cancelled, ambulances diverted and patient records unavailable in England and Scotland
  – Told to shut down, take out network cables and unplug the phones. Restoration was eventually completed after much painstaking work.

• **Telefonica (Spanish ISP)**
  – Infected an internal server, from where it spread to employee PCs
  – Employees instructed to disconnect from internal WiFi network. Company blasted warnings through audio speakers to shut down.

• **Federal Express**
  – "experiencing interference with some of our Windows-based systems caused by malware. We are implementing remediation steps as quickly as possible."
Wannacry at rest (it aint over yet)

The halting of the ransomware was by chance

- A 22-year-old U.K. cybersecurity researcher, known online as MalwareTech, has been hailed as an "accidental hero" for halting the spread of the malware bug.
- The researcher reportedly identified a domain name in the malware virus and purchased the site, which acted as a "kill switch", according to ITV News.
- Changes are being made “as we speak” to reissue the ransomware without the “kill switch” oversight.
So What Do We Do About Ransomware?

Best Answer: Treat it Like Rain.

Three options if it's raining on you:

- Stop it from raining.
- Go someplace where it isn’t raining.
- Use an umbrella.
How to Recover If You Are Attacked

• **Recovery potential:**
  • Restore a “clean” copy of affected data files and programs
  • Must have backups that are recent, but prior to infection (not synchronous)
  • Backups Must Be Offline and Secured

• **Immediate actions if you are attacked:**
  • Disconnect and Isolate the device(s)
  • Organize a Response Team including PR/Legal/HR/Executives and IT
  • Don't pay the ransom
    • it may not result in restoration
    • your site will most likely be sold to others
  • Contact FBI
  • Remember that if you call the law, you relinquish control, but don’t let that stop you

You must have remembered to bring the umbrella!
Best chances for prevention

• Repeated Awareness/training sessions
  • Inform people about ransomware and the advanced attempts to fool them
  • “Decriminalize” ransomware victims and focus on recovery/restoration
  • Describe a simple, yet effective, series of steps to minimize risk

• Software Patches up-to-date
  • Exploits can enter through known software vulnerabilities as well as e-mail
  • Rapid proliferation of malware is facilitated by outdated software

• Auto update Anti-virus
  • Antivirus software lags behind advanced ransomware but it is an improvement
  • Update as frequently as possible and keep multiple A/V product active

• Manage administration accounts
  • Many products have built-in administrator accounts that were never changed or removed
  • The best day for a ransomware criminal is to compromise an administrator account
  • Administration privilege removes all defenses to the spread of data imprisonment
• **Enforce least privilege**
  • Similar to administration accounts, this limits the data that is exposed
  • Easier to assert different protection mechanisms based on risk and organization mission

• **Disable office macros on email**
  • Easy to do, but difficult to implement across the enterprise
  • Deemed as an “unfriendly” IT Security gesture.

• **Implement software restriction policies**
  • Also unpopular, but necessary in an environment that is under threat
  • BYOD benefits the budget line at the cost of extreme increase of risk
Advanced attacks are becoming normal

• **Targeted data based on the individual (spear phishing)**
  • The perpetrators do their research ("I was at your presentation...")

• **Multifactor attack: email plus phone call**
  • Successful ransomware is driven manually ("Did you just receive the invoice ...")

• **Extract bitcoin from wallet directly**
  • If you have ever used bitcoin, your risk increases substantially
  • The ransom can be paid by you without you ever knowing

• **Threat to reveal personal data if not paid**
  • Remember the Sony Pictures news stories

• **Use of your IT as a host for DDOS or botnet site**
  • Once you open your door for communication, all defenses can be disabled and you may become part of the problem
Plan to have a better program

- **Improve your Backup Architecture**
  - Do not back up sensitive data to an external hard drive that’s always connected because Ransomware will encrypt the files hosted in those locations too.
  - Use the 3-2-1 rule: at least three copies of the data, two frequencies online (continuous and daily), and at least one copy stored off-site or offline (weekly).

- **Join an Information sharing and analysis center (ISAC)**
  - ISAC’s provide significant technical information that can help identify and possibly neutralize Ransomware. Industry specific organizations exist for:
    - **Multi state**
    - Financial services
    - National health
Enhance Technology Barriers

• Five reasonably simple technical barriers:

1. **Consider installing Office ADMX template for disabling macros.** The template kills the non-executable variants of ransomware that are starting to gain in popularity among criminals. One of the reasons such variants exist is because they load directly into RAM and bypass most restriction policies.

2. **Avoid mapping your drives and hide your network shares.** `WNetOpenEnum()` will not enumerate hidden shares. This is as simple as appending a $ to your share name.

3. **Work from the principle of least permission.** Very few organizations need a share whereby the Everyone group has Full Control. Delegate write access only where it’s needed, don’t allow them to change ownership of files unless it’s a must.

4. **Be vigilant and aggressive in blocking file extensions via email.** If you’re not blocking .js, .wsf, or scanning the contents of .zip files, you’re not done. Consider screening ZIP files outright. Consider if you can abolish .doc and .rtf in favor of .docx which cannot contain macros.

5. **Install the old CryptoLocker Software Restriction Policies** which will block some rootkit-based malware from working effectively. You can create a similar rule for `%LocalAppData%\*.exe and `%LocalApp- Data%\*\*.exe as well. If it’s at all feasible, run on a whitelist approach instead of a blacklist. It’s more time-intensive but much safer.
The Joy of Tech — by Nitrozac & Snaggy

The Internet of ransomware things...

- Hungry? Pay up and I'll unlock my door!
- On strike until you send money to my hackers.
- 20 bucks in my PayPal account or I'll only brew decaf!
- I'll be burning the toast if you don't get me some dough!
- The next time you leave, it'll cost you $100 bucks to get back into the house, unless you give me $75 now!
- 30 bucks in Bitcoin, or next time I smell smoke, I might just let you sleep.
- My alarm system is going to go off randomly throughout the night, unless you “donate.”
- Wire my hacker $100 or I'll reverse my motor and blow dirt all over this place!
- Your dirty dishes can wait, I'm busy mining bitcoins.
- Excuse us while we participate in a DDoS attack.
- I'll start your car, but only to take you to your bank to make a transfer.
- Send me $25 or I'll tell everyone on your social network that you were stupid enough to buy an Internet-connected broom!
- I'm turning off the heat until you warm up my bank account!
THANK YOU!
Whether you are in the cybersecurity planning stage, or have been a victim of a cybercrime, please feel free to contact me:

Michael Corby  
Consulting Director  
M Corby & Associates, Inc.  
65 Fairview Drive  
Leicester, Massachusetts 01524  
MCorby@mcorby.com  
Office: 508-892-2980  
Cell: 508-873-7488

Try this for more information  
https://www.nomoreransom.org/