Responding To Ransomware
Ransomware is getting more sophisticated, and shifting to an enterprise threat

Hello,

Thank you for your order. We’ll be informing you once item(s) have dispatched.

You can check the invoice number by downloading Your Order Invoice to this mail. Download Invoice.

The City keeps a copy of all E-mails sent and received for a minimum of 2 years. All retained E-mails will be treated as a Public Record per the California Public Records Act, and may be subject to disclosure pursuant to the terms, and subject to the exemptions, of that Act.

ALL YOUR PERSONAL FILES ARE ENCRYPTED

All your data (photos, documents, database, ...) have been encrypted with a private and unique key generated for this computer. It means that you will not be able to access your files anymore until they’re decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.

The payment has to be done in Bitcoin to a unique address that we generated for you. Bitcoins are a virtual currency to make online payments. If you don’t know how to get Bitcoins, you can google “How to Buy Bitcoins” and follow the instructions.

YOU ONLY HAVE 4 DAYS TO SUBMIT THE PAYMENT! When the provided time ends, the payment will increase to 5 Bitcoins. Also, if you don’t pay in 7 days, your unique key will be destroyed and you won’t be able to recover your files anymore.

To recover your files and unlock your computer, you must send 1.2 Bitcoin (500$), to the next Bitcoin address:

Click Here to Show Bitcoin Address

WARNING!

DO NOT TRY TO GET RID OF THIS PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRIPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTIONS.
To Pay Or Not To Pay?

Your money or your files?
“The ransomware is that good... To be honest, we often advise people just to pay the ransom.”

-Joseph Bonavolonta
FBI Assistant Special Agent in Charge of the Cyber and Counterintelligence Program
Quote from 2015
Money or Files?

50%

50% of ransomware victims have paid
40% said they would pay if they were hit with ransomware

Source: BitDefender
A RANSOMWARE ANECDOTE
Argument against paying

• We don’t negotiate with terrorists
• Paying incents attackers to keep using ransomware
"The FBI doesn’t support paying a ransom in response to a ransomware attack."

-James Trainor
FBI Cyber Division Assistant Director
Quote from April 2016
"Paying a ransom doesn’t guarantee an organization that it will get its data back—we’ve seen cases where organizations never got a decryption key after having paid the ransom."

-James Trainor
FBI Cyber Division Assistant Director
Quote from April 2016
True Cost

$600
Average price of ransomware

$50K
Some ransom demands are as high as $50K

$325M
Amount extorted by CryptoWall since 2015

$1M+
True cost of a large ransomware attack
Critical Infrastructure:
- Healthcare
- Government
- Law Enforcement
- Energy
- Financial
Top Infection Methods

1. Weaponized Office documents
2. Malicious email links
3. Malvertising
4. Unauthorized programs
Ransomware and Weaponized Docs (which can spread ransomware) increased in May
Constant State of Innovation

- 2-for-the-price-of-1 Ransomware: Ransomware + DDOS
- Hash Factory: Ransomware changes hash every 15 seconds
- Server-side Ransomware: Beyond the desktop
- Viral Ransomware: Spreads like a virus
Recommendations
Limited Decryption Ability

• TeslaCrypt (v3.0-v4.2)
  – ESET was able to get the decryption key by ASKING attackers for it. Seriously.

• Decryption tools are available for:
  – 777
  – Xorist
  – 8Lock8
  – GhostCrypt
Common Advice Only Helps So Much

- Keep Your AV up-to-date
- Filter your email
- Patch everything all the time
- Careful what you click

"Users will open attachments, they will visit sites that are infected, and when that happens, you just need to make sure that your security technology protects you."

-Anup Ghosh
CEO, Invincea
Wired Magazine, May 2016
Our Recommendations

• Deploy anti-malware prevention
• Behavioral monitoring
• Isolation
• Back it up!!!!

"network shares are as at risk as your desktop system in a ransomware infection. If the backups are done offline, and the backup is not reachable from the machine that is infected, then you’re fine."

-Anup Ghosh
CEO, Invincea
Wired Magazine, May 2016
Business Continuity & Disaster Recovery

• Develop a business continuity plan for what happens if you loose access to your data or systems

• Backup your data and airgap it from your primary network
  – Put controls in place that will allow you to rapidly your recover files

• Have an IR plan in place with access to 3rd parties that can assist
Final Recommendation

“Don’t pay unless you absolutely have to!”

- Yours truly

Quote from ... today
THANK YOU

www.invincea.com