



X by Invincea

Responding To Ransomware



X by Invincea

Ransomware Nightmares

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 [REDACTED] 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.

This email invites you to download invoice-order.zip.
The ZIP file contains the ransomware as invoice-order.exe.

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 DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTIONS.



X by Invincea

Ransomware Nightmares

SNSLOCKER

Your personal files are encrypted!


SNSLocker

Welcome To SNS world

Your personal files have been crypted and locked by a very strong algorithmes : AES and RSA

And the only way to get your files back is to pay me for 300 USD

Dont try to remove me because if u do u ll lose ur files forever

If u re ready to pay click next

11:41:12

<< Back

Next >>

DMA Locker 4.0

All your personal files are LOCKED!

WHAT'S HAPPENED?

- * All your important files(including => hard disks, network disks, flash, USB) are encrypted.
- * All the files are locked with asymeric algorithm using AES-256 and then RSA-2048 cipher.
- * You can't restore your files because all your backups have been deleted.
- * Only way to recover your files is to pay us 1 BTC
- * As a proof you can decrypt 1 file FOR FREE by clicking here:

HOW TO PAY US AND DECRYPT YOUR FILES?

1. If you are OFFLINE you can contact us via e-mail: dma4004@zerobit.er and we will provide you instructions about how to decrypt your files.
2. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
 - * <https://coincafe.com/>
 - * <https://www.bitquick.co/>
 - * <https://www.coinbase.com/>
3. If you already have Bitcoins, pay us 1 BTC to the following Bitcoin address:
4. If you have paid, enter following site to get your transaction id.
Click this button to show tutorial how to locate your transaction id:
<https://blockchain.info/address/>
5. When you have located Transaction ID, paste it to 'TRANSACTION ID' field below and, click the "CHECK PAYMENT" button. Confirming your payment by our servers can take up to several hours (we require some bitcoin transaction confirmations). When your payment has been confirmed, the 'DECRYPT FILES' button will enabled, just click it to decrypt your files.

TRANSACTION ID:

CHECK PAYMENT

PAYMENT STATUS:

DECRYPT FILES

To Pay Or Not To Pay?

Your money or your files?





X by Invincea

Argument for paying

“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

A RANSOMWARE ANECDOTE



X by Invincea

Argument against paying

- We don't negotiate with terrorists
- Paying incents attackers to keep using ransomware





X by Invincea

Argument against paying

"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**



X by Invincea

Criminals Are Unreliable

"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

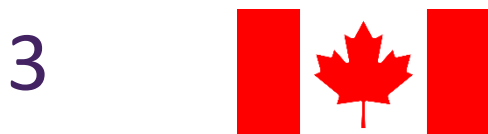
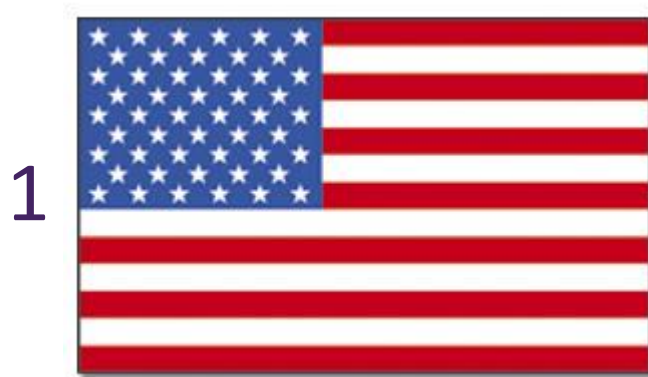
Amount extorted by CryptoWall since 2015

\$1M+

True cost of a large ransomware attack

Ransomware Trends

Targets



Critical Infrastructure:

- Healthcare
- Government
- Law Enforcement
- Energy
- Financial

Top Infection Methods

1

Weaponized Office documents

2

Malicious email links

3

Malvertising

4

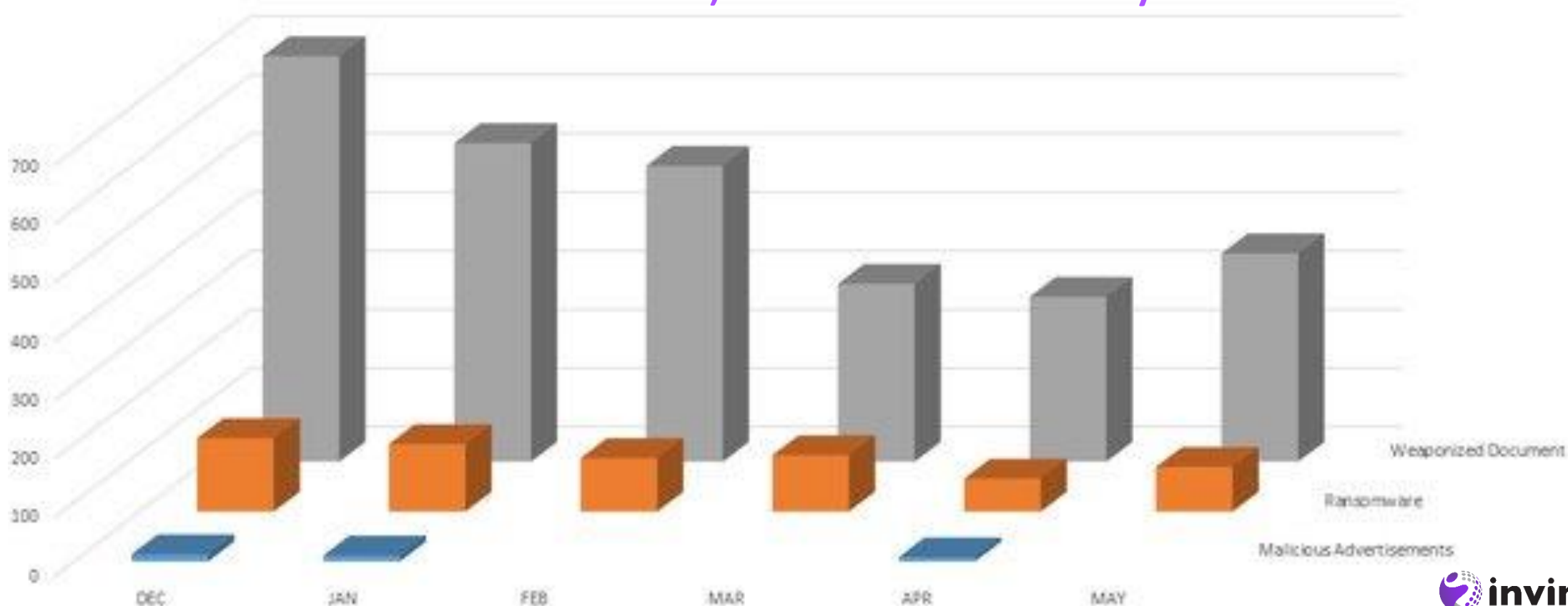
Unauthorized programs



X by Invincea

Trends

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



X by Invincea

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

KIM ZETTER SECURITY 05.13.16 1:00 PM

4 WAYS TO PROTECT AGAINST THE VERY REAL THREAT OF RANSOMWARE





X by Invincea

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

KIM ZETTER SECURITY 05.13.16 1:00 PM

4 WAYS TO PROTECT AGAINST THE VERY REAL THREAT OF RANSOMWARE





X by Invincea

Business Continuity & Disaster Recovery

- Develop a business continuity plan for what happens if you lose 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 recover files
- Have an IR plan in place with access to 3rd parties that can assist



X by Invincea

Final Recommendation

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

**-Yours truly
Quote from ... today**



THANK YOU



www.invincea.com