



# Ransomware

“Ransomware is more about manipulating vulnerabilities in human psychology than the adversary’s technological sophistication.”

– James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology

# Ransomware Pandemic

**Massive ransomware cyber-attack hits nearly 100 countries around the world**

More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of 'cyber weapons' from the NSA

**Ransomware attacks hit new high in 2017**

NotPetya takes top spot as Webroot's most damaging attack of 2017, followed by WannaCry and Locky.

**Ransomware damage costs predicted to hit \$11.5B by 2019**

**Ransomware shuts down 1 in 5 small businesses after it hits**

Ransomware hit one third of small-to-medium businesses worldwide last year, and experts say the "human factor" was often to blame.

**"WannaCry" ransomware attack losses could reach \$4 billion**

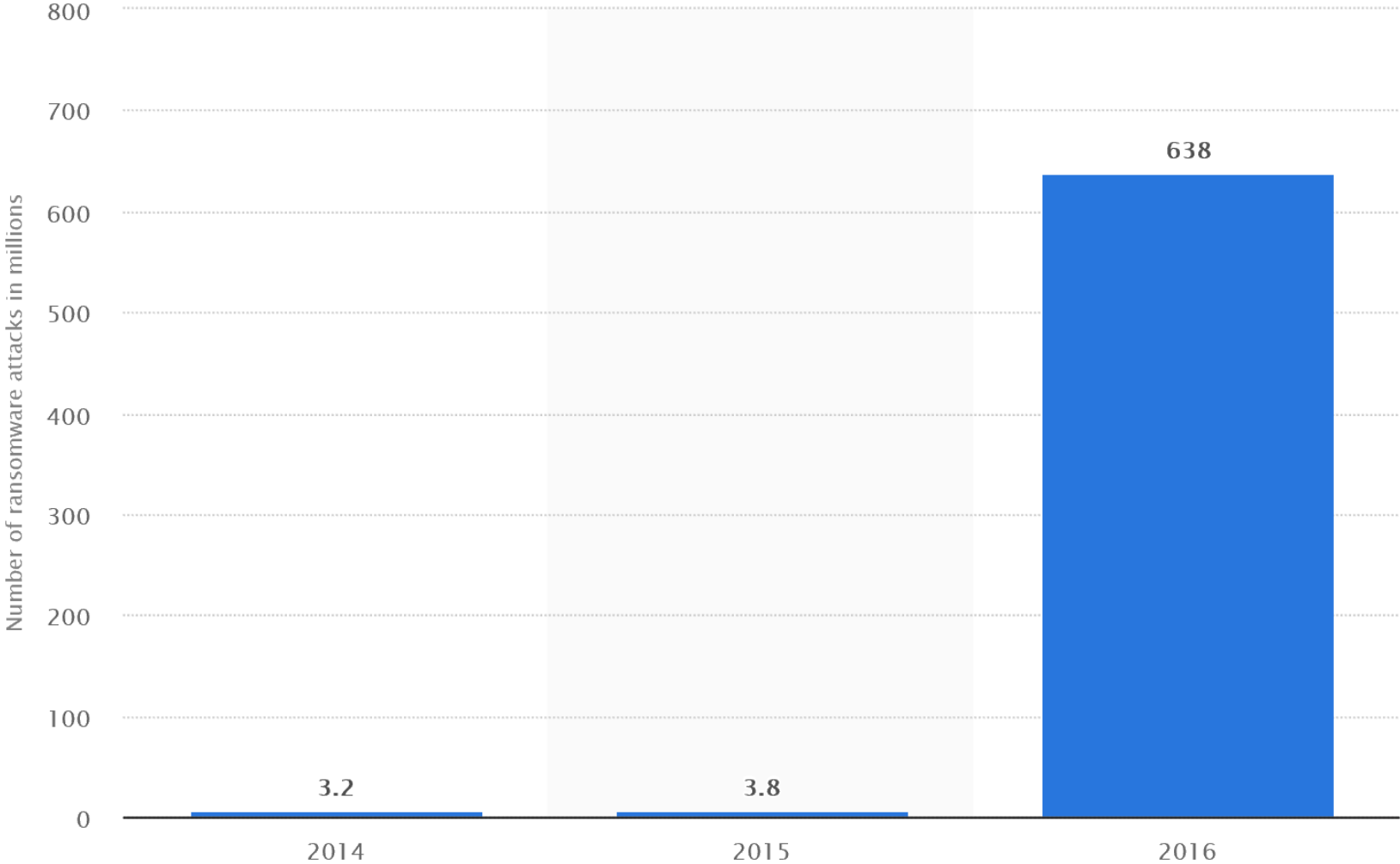
Global ransomware damage costs predicted to exceed \$5 billion in 2017, up from \$325 million in 2015.

**The next ransomware attack will be worse than WannaCry**

**Petya ransomware: Cyberattack costs could hit \$300m for shipping giant**

# Ransomware Pandemic

Number of Ransomware Attacks Worldwide (in millions)



Source: Statista

# Ransomware Pandemic

**The average cost per ransomware attack to businesses was \$133,000 in 2017.**

Sophos | [Tweet this stat](#)

From:  
hgvhgh <hgvhgh@protonmail.com>  
07/09/2018 (4 days ago)

To: [REDACTED]

[Show details](#)

I know you are a big organization. And I have information about your clients. You should pay 290 btc to get decryptor . You can get decryptor after payment.

# What is Ransomware?

- Malware + Extortion Demand
  - Encrypts files and locks victim device
  - Threatened (or partial) destruction
- Ransom demand
  - Attackers deliver decryption tool and/or key after ransom payment
  - Attackers stop destructive attack
- “Destructoware” without a credible demand is not ransomware
  - E.g. NotPetya
  - No way to pay ransom or attackers to decrypt – simply cyber-vandalism



# Who is at Risk?

- Anyone who is connected to the internet
- Every second, the global internet encounters:
  - **15,000** malware sessions hitting victims
  - **15,000** phishing e-mails sent
  - **8,000** scanning attempts
- 29% of internet traffic is harmful botnet traffic
  - Automated systems scanning the web looking for potential victims





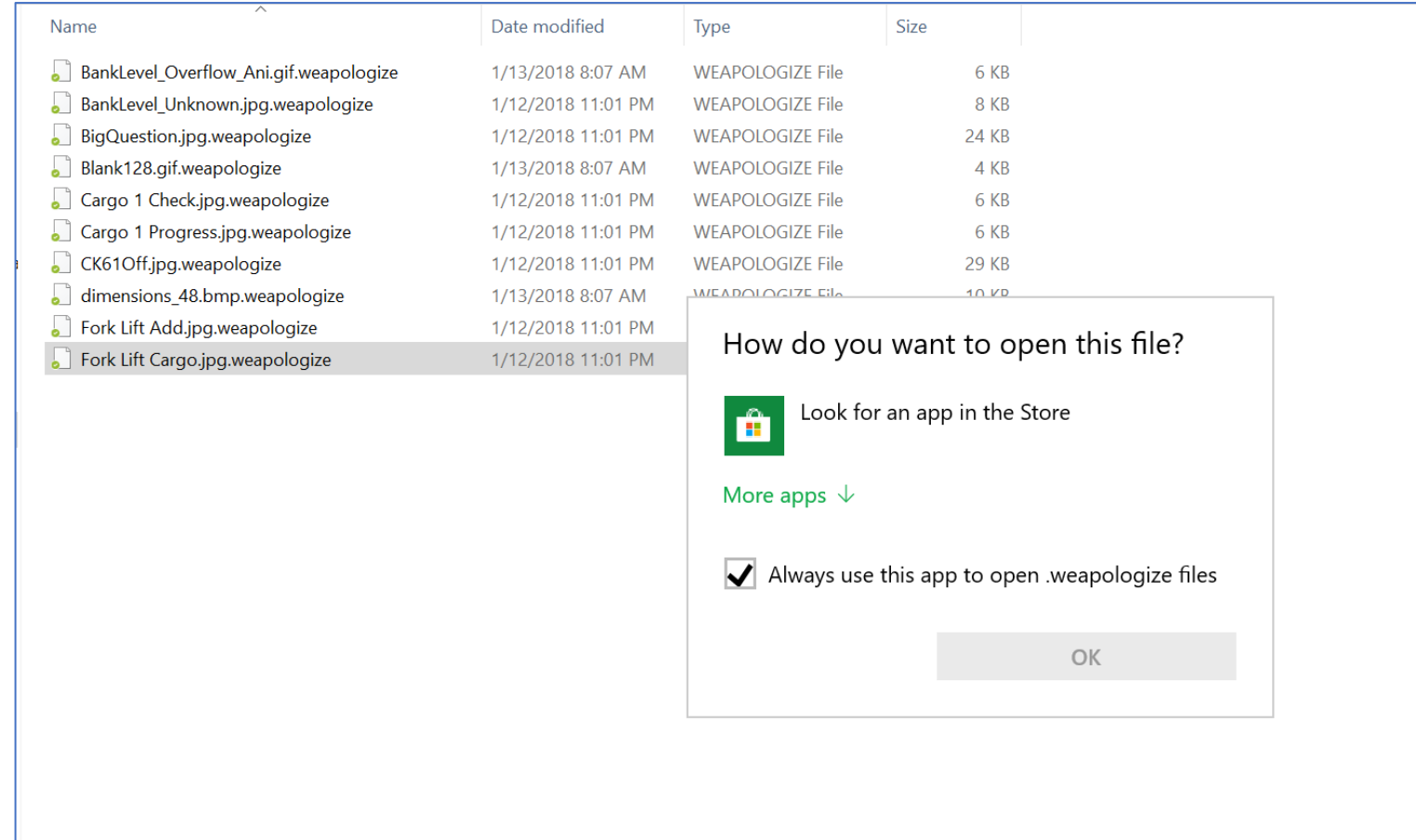
**What does an  
attack look  
like?**

---

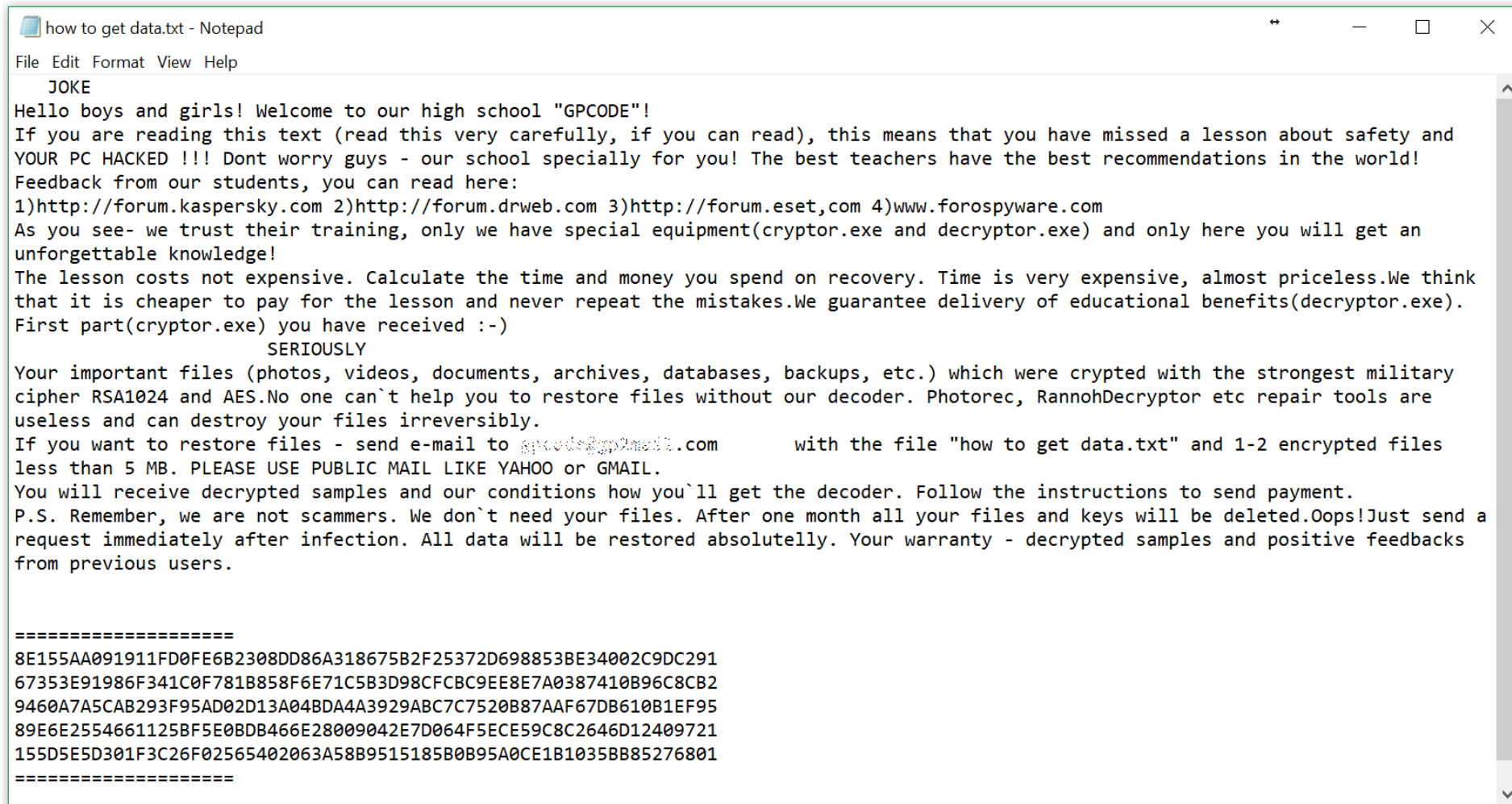




- Symptoms of a ransomware infection:
  - Files have an unrecognizable extension
  - Files can't open



- Ransom note



```
how to get data.txt - Notepad
File Edit Format View Help
      JOKE
Hello boys and girls! Welcome to our high school "GPCODE"!
If you are reading this text (read this very carefully, if you can read), this means that you have missed a lesson about safety and
YOUR PC HACKED !!! Dont worry guys - our school specially for you! The best teachers have the best recommendations in the world!
Feedback from our students, you can read here:
1)http://forum.kaspersky.com 2)http://forum.drweb.com 3)http://forum.eset.com 4)www.forospyware.com
As you see- we trust their training, only we have special equipment(cryptor.exe and decryptor.exe) and only here you will get an
unforgettable knowledge!
The lesson costs not expensive. Calculate the time and money you spend on recovery. Time is very expensive, almost priceless.We think
that it is cheaper to pay for the lesson and never repeat the mistakes.We guarantee delivery of educational benefits(decryptor.exe).
First part(cryptor.exe) you have received :-)
```

SERIOUSLY

Your important files (photos, videos, documents, archives, databases, backups, etc.) which were crypted with the strongest military cipher RSA1024 and AES.No one can't help you to restore files without our decoder. Photorec, RannohDecryptor etc repair tools are useless and can destroy your files irreversibly.

If you want to restore files - send e-mail to [gpcodet@pp2mail.com](mailto:gpcodet@pp2mail.com) with the file "how to get data.txt" and 1-2 encrypted files less than 5 MB. PLEASE USE PUBLIC MAIL LIKE YAHOO or GMAIL.

You will receive decrypted samples and our conditions how you'll get the decoder. Follow the instructions to send payment.

P.S. Remember, we are not scammers. We don't need your files. After one month all your files and keys will be deleted.Oops!Just send a request immediately after infection. All data will be restored absolutelly. Your warranty - decrypted samples and positive feedbacks from previous users.

=====

```
8E155AA091911FD0FE6B2308DD86A318675B2F25372D698853BE34002C9DC291
67353E91986F341C0F781B858F6E71C5B3D98CFBC9EE8E7A0387410B96C8CB2
9460A7A5CAB293F95AD02D13A04BDA4A3929ABC7C7520B87AAF67DB610B1EF95
89E6E2554661125BF5E0BDB466E28009042E7D064F5ECE59C8C2646D12409721
155D5E5D301F3C26F02565402063A58B9515185B0B95A0CE1B1035BB85276801
=====
```

#What happened to your files?

All your files encrypted with RSA-2048 encryption, For more information search in Google "RSA Encryption"

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key for decryption So you need Private key to recover your files. It's not possible to recover your files without private key

#How to get private key?

You can get your private key in 3 easy step:

Step1: You must send us 1.7 Bitcoin for each affected PC OR 28 Bitcoins to receive ALL Private Keys for ALL affected PC's.

Step2: After you send us 1.7 Bitcoin, Leave a comment on our Site with this detail: Just write Your "Host name" in your comment

\*Your Host name is:

Step3: We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

\*Our Site Address: <https://bavokn3r741n7a.onion/decrypt/22/>

\*Our BitCoin Address: [18bn5q7vK7upR3GUM8F8anF7qy2Pys](https://blockchain.info/address/18bn5q7vK7upR3GUM8F8anF7qy2Pys)

(If you send us 28 Bitcoins For all PC's, Leave a comment on our site with this detail: Just write "For All Affected PC's" in your comment) (Also if you want pay for "all affected PC's" You can pay 14 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive all keys )

How To Access To Our Site

For access to our site you must install Tor browser and enter our site URL in your tor browser. You can download tor browser from <https://www.torproject.org/download/download.html.en> For more information please search in Google "How to access onion sites"

# Test Decry

Check our site, You can upload 2 encrypted files and we will decrypt your files as de

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 asymmetric 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: [dmasoftware@proton.me](mailto:dmasoftware@proton.me) 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://coinbase.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, 'DECRYPT FILES' button will be enabled, just click it to decrypt your files.

\* Ransom increase time:

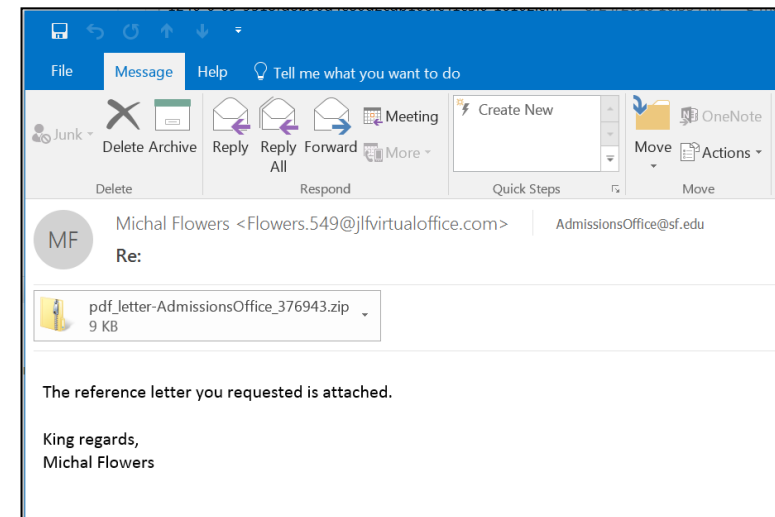
If you don't pay us within this time, the amount you will have to pay will increase to: 1.5 BITCOINS

MKLIUKANG@INDIA.COM



# How to respond to Ransomware

- Active ransomware? That PDF attachment wasn't a PDF after all...
  - Shut down the computer, pull the plug
  - Disconnect the network cable
  - Call insurance carrier



# How to respond to Ransomware

- Everything encrypted?
  - Disconnect internet connectivity
  - Quickly take any notes possible such as details of ransom splash screens, ransom notes, file extensions, etc.
  - Run an AV scan to remove any persistent malware
  - Check if there are valid backups
  - Call insurance carrier



# How NOT to respond to Ransomware

Deciding what  
**not to do**  
is as important  
as deciding  
**what to do.**

Steve Jobs



# How NOT to respond to Ransomware

1. Rebuilding or restoring infected systems from backups without preserving data
  - A forensic conclusion is impossible in the absence of forensic data
  - Was any data accessed or exfiltrated by the attacker?
  - Which device was the source of the intrusion?
  - What vulnerability was exploited to gain remote access?



- Frequently the victim has been compromised for months – the ransomware attack was just the final insult.
- Attackers gain access to:
  - Steal confidential data
  - Misuse computational power (bitcoin mining)
  - Use the compromised servers as bots to launch spam/DDOS/ attacks
  - And of course plant the ransomware malware



- Activities include:

- Cryptocurrency mining
- Hacking other victims
- Running scam campaigns via online dating websites and social media
- Setting up fake seller accounts on online retailers such as Amazon and eBay
- Online shopping using stolen credit cards and PayPal credentials

Local File Path	Preview of Image	Evidence of Scamming Activity
<a href="#">www.fishdating.com</a> \Downloads\my photyo.jpg		<p><b>Derrick Peterson (@derrickpeters20)   Twitter</b>  <a href="https://mobile.twitter.com/derrickpeters20">https://mobile.twitter.com/derrickpeters20</a>            256 x 256 - @derrickpeters20 hasn't Tweeted yet. Sorry, Twitter is taking too long to load. Try again. Home · Sign up · Log in · Search · About. More like this; Less like this</p> <p><b>Leon Antonio Alberto - Google+</b>  <a href="https://plus.google.com/117565639841806823741">https://plus.google.com/117565639841806823741</a>            60 x 60 - Leon Antonio Alberto - Google+.</p> <p><b>justinmorgan187, Male, Feltham, Iodun, United Kingdom</b>  <a href="http://www.craigslist.com/profile/5274533">www.craigslist.com/profile/5274533</a>            417 x 417 - cess &gt; justinmorgan187: Hello, My name is Success,please send me an email so i can send you my pics and tell u more about me here is my email ...</p> <p><b>James Larsson - FB - RSB-Forum</b>  <a href="http://www.rsb-forum.de/t1947f14-James-Larsson-FB.html">www.rsb-forum.de/t1947f14-James-Larsson-FB.html</a>            350 x 350 - Jan 8, 2017 - Profil - Name: James Larsson Community: Facebook Siehe hier &gt;&gt;&gt; Fake &gt;&gt;&gt; Facebook &gt;&gt;&gt; Profil &gt;&amp;</p> <p><b>Latest Activities - plentyfishdating.com</b>  <a href="http://www.plentyfishdating.com/activity/?last_activity_id...">www.plentyfishdating.com/activity/?last_activity_id...</a>            417 x 417 - 高高的富帅 updated profile photo. last month. 呆呆刚刚加入. last month. 女22, 南京. wonderland81 just joined. last month. Female 34, Hinckley. curvyred79 just ...</p> <p><b>Latest Activities - plentyfishdating.com</b>  <a href="http://www.plentyfishdating.com/activity/?last_activity_id...">www.plentyfishdating.com/activity/?last_activity_id...</a>            417 x 417 - 高高的富帅 updated profile photo. last month. 呆呆刚刚加入. last month. 女22, 南京. wonderland81 just joined. last month. Female 34, Hinckley. curvyred79 just ...</p>

## EVIDENCE (211)

Column view

Translation String
I am being careful because I am orth
I am being careful because I am orthopedics surgeon working with the United Nations
It will be very difficult for us to maintain a relationship over time ... Liverpool is far from Buenos Aires, Argentina much as England .... and if I have children ... 2, one of 28 years of my first marriage and
I am being careful because I am orthopedics surgeon working with the United Nations and the rebels are trying to harm us.
Please I want you to know that I am busy person due to the nature of my job
I am being careful because I am orth
I am being careful because I am orthopedics surgeon working with the United Nations and the rebels
I am
I am being careful because I am orthopedics surgeon working with the United Nations and the rebels are trying to harm us.
I am also single and I want us to get to know each other very well. I live in Liverpool, London. Do you have children
Please I want you to know that I am busy person due to the nature of my job so kindly send me your email address and we will ta
I am being careful because I am orthopedics surgeon working
I am be
It will be very difficult for us to maintain a relationship over time ... Liverpool is far from Buenos Aires, Argentina much as England .... and if I have children ... 2, one of 28 years of my first marriage and
I am being caref
I am
I am being careful because I am orthopedics surgeon working with the United Nations
Please I want you to know that I am busy person due to the nature of my job so kindly send me your email address and we will t
I want you to know that distance is never a barrier in a relationship and it does not border me at all because I am ready and willing to join you in your country but first we have to get to know each ot
I am also single and I want us to get to know each other very well. I live in Liverpool, London
Please I want you to know that I am busy person due to the nature of my job so kind
Please I want you to know that I am busy person due to the nature of my job so kindly send me your email address and we will ta
I am being careful because I am orthopedics
I am also single and I want us to get to know each other very well. I live in Liverpool, London. Do you have children?
I am being careful because I am orthopedics surgeon working
I am bee
Please I want you to know that I am busy person due to the nature of my job so kin
Please I want you to know that I am busy person due to the nature of my job so kindly send me your email address and we will take it from there.
I am being careful because I am orthopedics surgeon working with the United Nations and the rebels are trying to harm us
Please I wa
Please I want you to know that I am busy person due to

en

pagefile.sys

### DETAILS

#### ARTIFACT INFORMATION

Language Translated From **en**

Language Translated To **es**

Translation String **I am being careful because I am orthopedics surgeon working with the United Nations and the rebels are trying to harm us.**

Date/Time **10/9/2016 3:04:11 PM**

Original artifact **Firefox Web History**

#### EVIDENCE INFORMATION

Source **pagefile.sys - Partition 2 (Microsoft NTFS, 79.9 GB) \pagefile.sys**

Location **File Offset 1207881007**

Evidence number **pagefile.sys**

# How NOT to respond to Ransomware

## 2. Running a bunch of free online decryptors

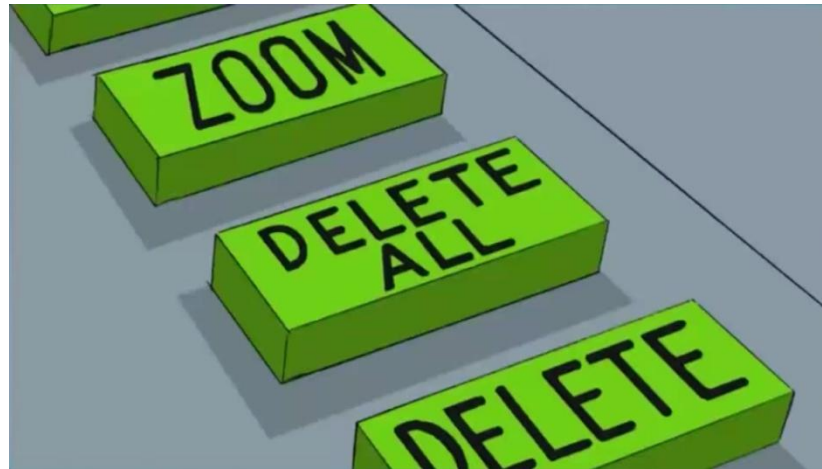
- Decryptor tools are not one-size-fit-all, most do not work
- Free decryptor software may wipe critical data required for forensic analysis



# How NOT to respond to Ransomware

## 3. Delete all ransom notes

- Ransom notes contain important information such as the attacker's contact information and victim ID numbers
- Different attacking entities may use the same ransomware variant



# How NOT to respond to Ransomware

## 4. Reach out to the attacker yourself

- Using company e-mail
- Informing the hacker you are hiring outside assistance
- Revealing your desperation
- Revealing the number of affected devices
- Revealing the identities of the most critical devices/files
- Using long sentences or fancy words that could be misconstrued when put through an online translator
- Insulting, antagonizing or threatening the attacker

When victims try to engage themselves, they may accidentally antagonize the attacker, or give up information that reveals their identity

My supervisor says that you try to f<sup>8\$!#%</sup> us when you ask passwords from

**10.0.12.221**

**10.0.12.13**

So he want 0.5 bitcoins more for this 2 servers

Please send 0.5 btc to the same address

My supervisor said not waste time with this case because you hold us for idiots and ask most critical servers including HYPER-V host with more then 10 VM

From:

hgvhgh <hgvhgh@protonmail.com>

09/09/2018 (2 days ago)

To:



[Show details](#)

you know why we did not give you the decryptor for the first time, because you thought we were children, we ask 300 bitcoins you tell us 7, I appreciate my time and yours, so I made you a discount, very big, if your boss does not want believe me on the word is his problem, I will start a further conversation with 293 bitcoins

Talking to attackers can be a mercurial task – leave it to the experts

21.12.2016 13:50 -- LET ME KNOW WHEN YOU ARE READY TO PAY MY RANSOM,  
BITCHES ! WHOESONS

LET ME KNOW WHEN YOU ARE READY TO PAY MY RANSOM, BITCHES !  
WHOESONS LET ME KNOW WHEN YOU ARE READY TO PAY MY RANSOM,  
BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY TO PAY MY  
RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY TO PAY  
MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY TO  
PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY  
TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE  
READY TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU  
ARE READY TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN  
YOU ARE READY TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW  
WHEN YOU ARE READY TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME  
KNOW WHEN YOU ARE READY TO PAY MY RANSOM, BITCHES ! WHOESONS LET  
ME KNOW WHEN YOU ARE READY TO PAY MY RANSOM, BITCHES ! WHOESONS  
LET ME KNOW WHEN YOU ARE READY TO PAY MY RANSOM, BITCHES !  
WHOESONS LET ME KNOW WHEN YOU ARE READY TO PAY MY RANSOM,  
BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY TO PAY MY  
RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY TO PAY  
MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY TO  
PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE READY  
TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU ARE  
READY TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN YOU  
ARE READY TO PAY MY RANSOM, BITCHES ! WHOESONS LET ME KNOW WHEN  
YOU ARE READY TO PAY MY RANSOM, BITCHES ! WHOESONS



- Ransomware attackers frequently market themselves as security professionals, IT experts, and even children's charities – don't be fooled
- Ransomware attackers are criminals, they are not providing you a service

File Edit Format View Help

And now most important information:

We are the International Children Charity Organisation! Your money will be spent for the children charity. So that is mean that You will get a participation in this process too. Many children will receive presents and medical help!

And We trust that you are kind and honest person! Thank You very much! We wish You all the best! Your name will be in the main donors list and will stay in the charity history!

Remember You can save many children destinies! Money for You is just a paper (You will earn money again in the next month), but for many children is a real chance to change their life!

Also ONLY WE can give to our customers very important benefits:

- 1) You will restore all Your data immediately
- 2) Your network vulnerabilities will be closed
- 3) You will protect Your system from the main attack in the future! It's a very important option!  
Only our community can give You this opportunity! All other anti-malware companies just promise it, but in fact they cannot protect You! It's very terrible!
- 4) Main idea - many children will receive a donation and medical help from Your name!
- 5) You will have a free tech support for solving any PC troubles! Just ask a support and support will help You!

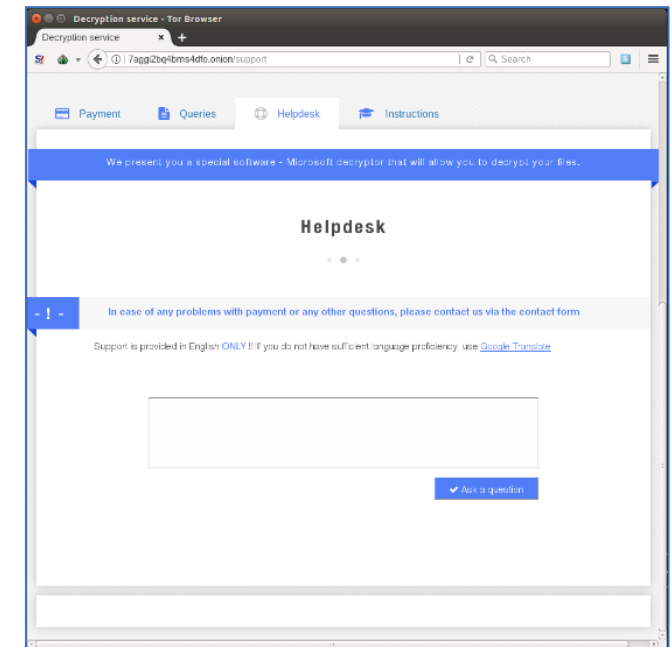
P.S> When your payment will be delivered you will receive your software with private key IMMEDIATELY!

P.P.S> In the next 24 hours your price may be doubled by the Main Server automatically.

So now you have a chance to restore your PC at low price!

Best regards,  
Charity Team

Also You will have a FREE tech support for solving any PC troubles for 3 years!



The image features a solid yellow background. Scattered across it are four black silhouettes: a beret in the upper left, a mustache in the lower left, a pair of glasses in the upper right, and a beard in the lower right. The text 'MythBusters: Ransomware Edition' is centered in white, bold font, with the 'MythBusters' part on the top line and 'Ransomware Edition' on the bottom line.

# MythBusters: Ransomware Edition

# Misconceptions

- Misinformation about ransomware and ransomware attackers can be found in all corners of the internet
- Unless you are dealing with ransomware infections and threat actors on a regular basis, it can be difficult to know which information is accurate



# Misconceptions

## Myth

Training employees on phishing awareness will protect you from most ransomware attacks.

# Misconceptions

## Myth

Training employees on phishing awareness will protect you from most ransomware attacks.

## Reality

Phishing was once a popular attack vector, but since late 2016, attackers have overwhelmingly favored other vectors for ransomware, such as **Remote Desktop Protocol (RDP) intrusion.**

# Implications of RDP Intrusions

- Once inside, an attacker can snoop around to see if there's **anything worth taking** before he kicks off the ransomware infection
  - Financial information and/or accounting data
  - Healthcare information
  - Stored account credentials



# Misconceptions

## Myth

Most attackers take your money and run, without restoring your files.

# Misconceptions

## Myth

Most attackers take your money and run, without restoring your files.

## Reality

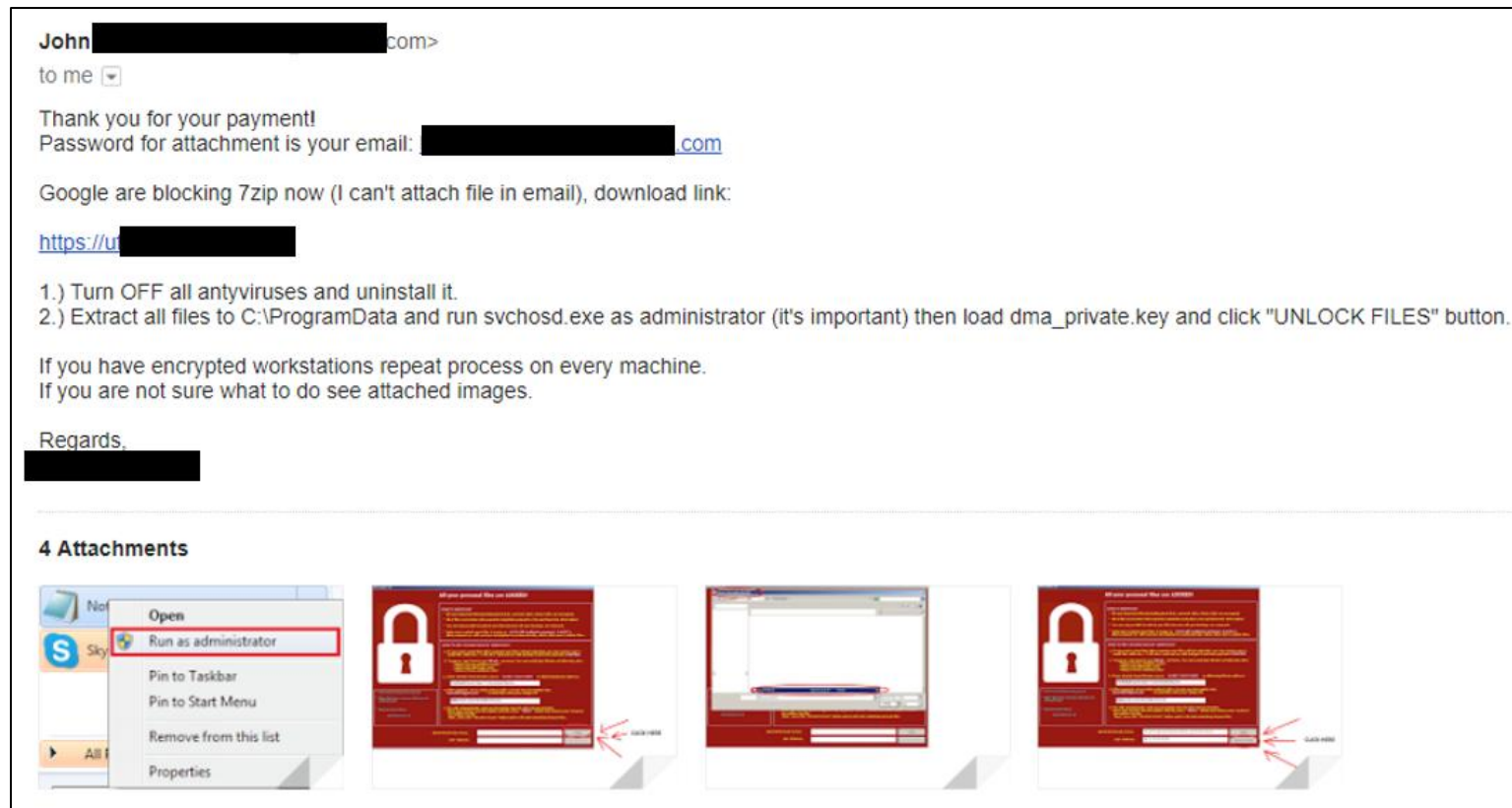
To date, we have never had an attacker refuse to turn over the decryption software.

We **have** had attackers request additional payments; in those cases, the tool was always provided following the additional payments.



# Misconceptions

- Most of the time, the attackers are responsive and cooperative (sometimes even helpful)



# Misconceptions

**attacker** [redacted] com>  
to me ▾  
and can you provide how much % of files you couldnt decrypt and what antivirus u r using on the server **I am emailing the guyz who makes infection.**  
...

---

**investigator** [redacted] com>  
to **attacker** [redacted]  
about 20% of files did not decrypt.  
They are in C: directory in random folders.  
Thank you for looking into it.  
...

---

**attacker** [redacted] com>  
to me ▾  
**it looks like if antivirs block crypter crypter kill av and rerun and create a different password.**  
**if you can give me a bitcoin address i can send you 0.6 bitcoin which is %20 of the payment.**

**investigator** [redacted] com>

to [redacted]

Hi. It won't allow me to decrypt all PC. An error pops up.



The screenshot shows the DP Decryptor application window with two buttons: "Decrypt all PC" and "Choose 1 file and decrypt it". An error dialog box is overlaid on top, displaying the message "Access error: The key for decrypting a single file." with an "OK" button.

...

---

**attacker** [redacted]

to me [redacted]

<https://www.sendspace.com> [redacted]

Fixed invalid key was.  
Repeat all the same steps

# Misconceptions

## Myth

Ransomware victims are usually targeted attacks.

# Misconceptions

## Myth

Ransomware victims are usually targeted attacks.

## Reality

Most ransomware victims become infected because they have a common system vulnerability currently being exploited by attackers e.g. open RDP port, weak/default passwords on specific applications.

Attackers utilize tools that scan the Internet for open ports, and if they happen to identify one, they would attempt to gain access.

# Misconceptions

## Myth

Ransomware attackers are technologically-savvy.

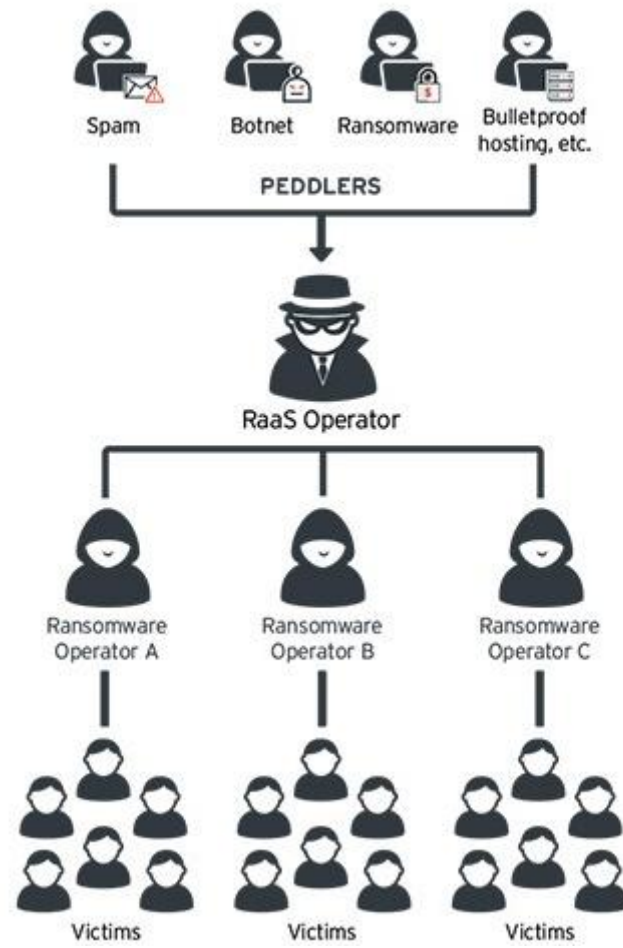
# Misconceptions

## Myth

Ransomware attackers are technologically-savvy.

## Reality

Modern ransomware variants are commonly sold on the black market in easy-to-use, all-inclusive packages – this is called Ransomware-as-a-Service. Attackers do not require advanced technical skills to deploy ransomware. In fact, the most damaging attacks experienced by Kivu have been caused by amateur hackers who are unable to respond to victims or lose control of their own attack.





---

Re: Decrypt this



Inbox x

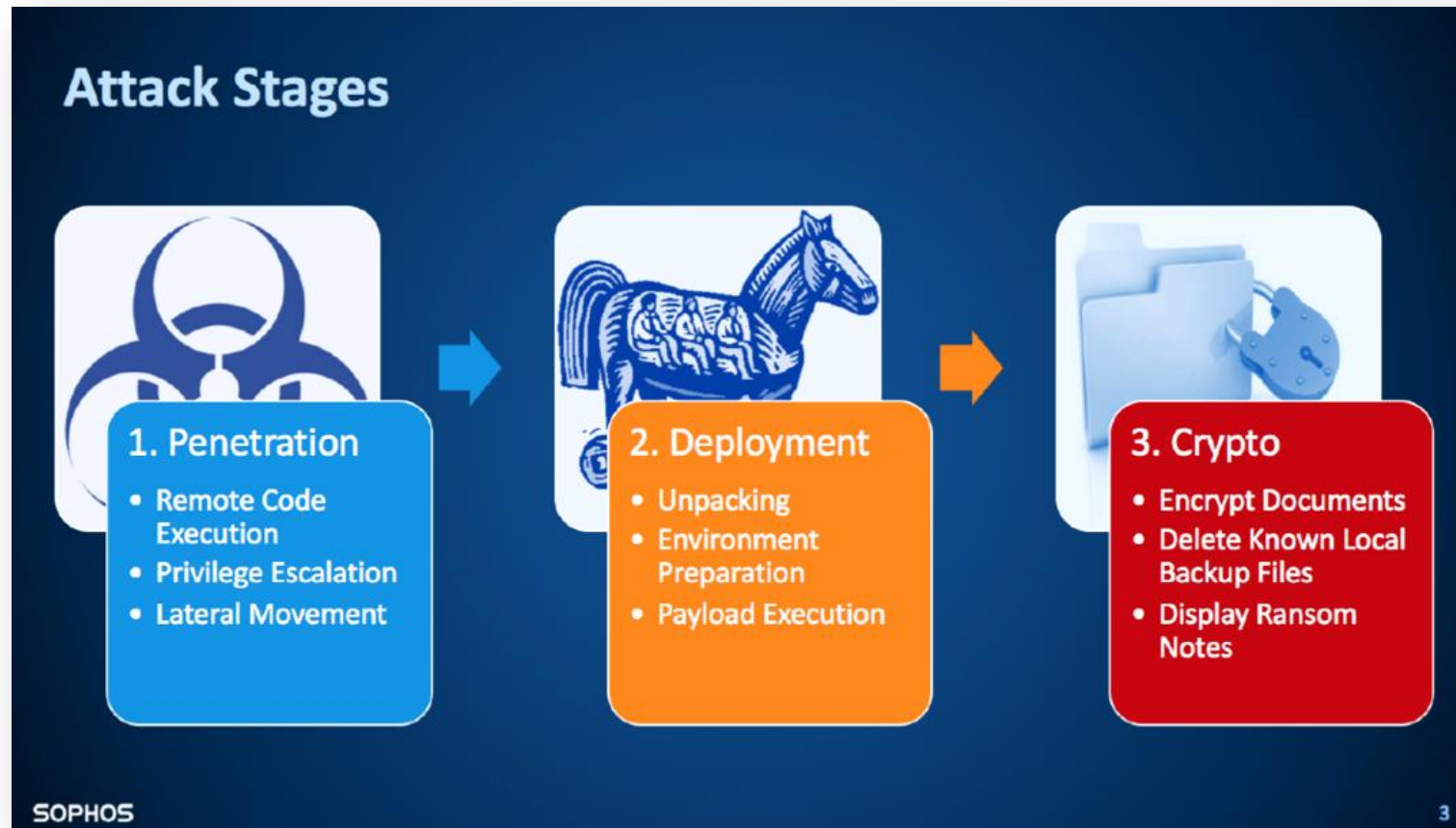


[Redacted]@ [Redacted]

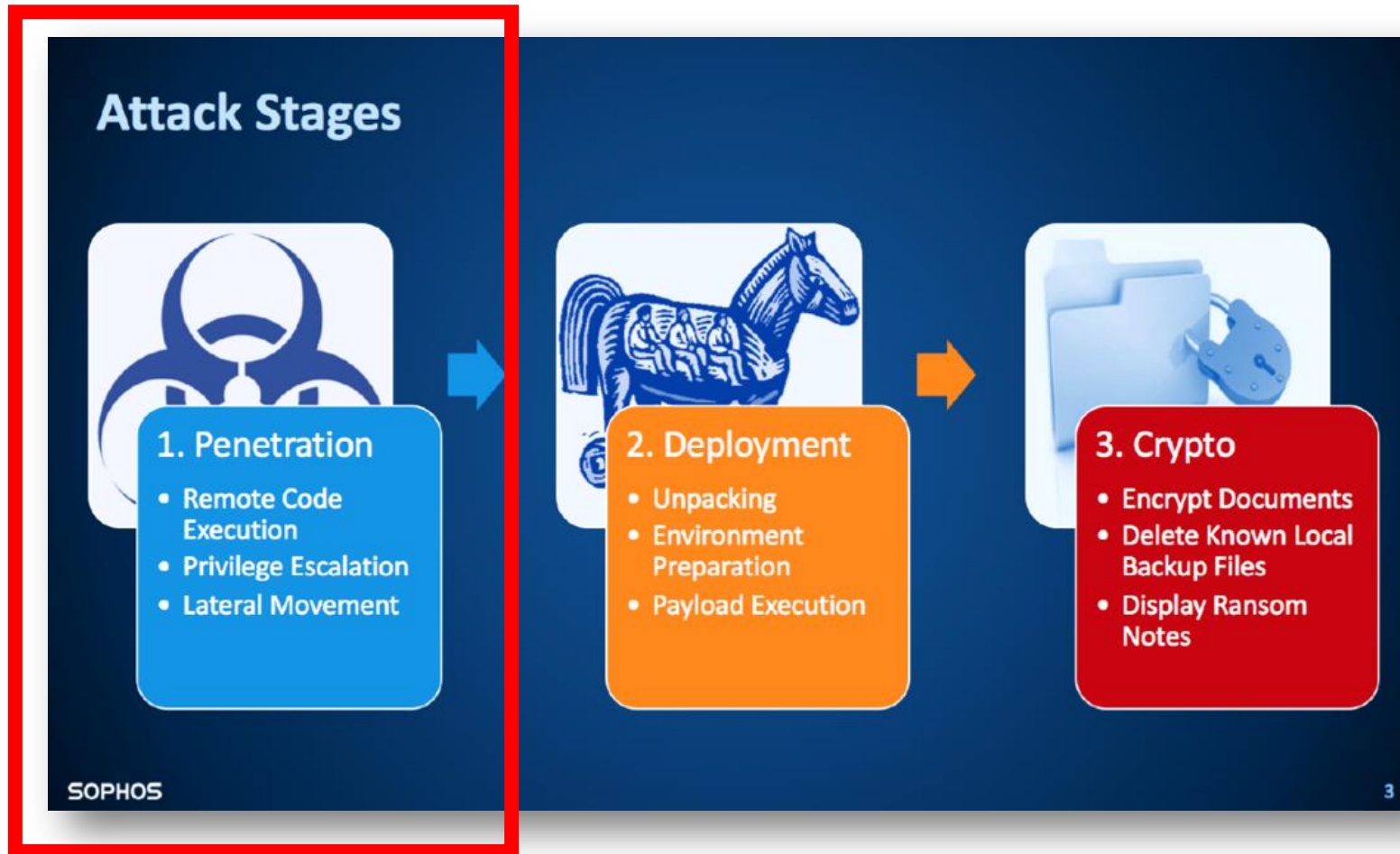
to me ▾

dude, stop crying. I can explain again I am not the author of the software did not know what it would be like this.

# Defending Against Ransomware



# Defending Against Ransomware



# Defending Against Ransomware

## 1. Close RDP, use a Virtual Private Network (“VPN”)

- Close RDP (or other remote access protocols) unless strictly required
- If you must use RDP, either whitelist IP's on a firewall or do not expose it to the Internet
- Put RDP behind a firewall, only allow RDP from local traffic
- Setup a VPN to the firewall and enforce strong password policies, especially on any admin accounts or those with RDP privileges



# Defending Against Ransomware

## 2. Implement an account lockout policy

- Implement a lockout policy whereby a user who has made more than three failed logon attempts will be “locked out” for a period of time, preferably 5-8 hours



# Defending Against Ransomware

## 3. Develop an effective password strategy

- Create passwords that include a combination of uppercase and lowercase letters, along with number and symbols, at least 12 characters in length
- Alternatively, a lengthy password with a long string of memorable words like “happy go lucky cats and dogs” have shown to be the most resistant against brute-force attacks

Password:

Strength:  **BEST**

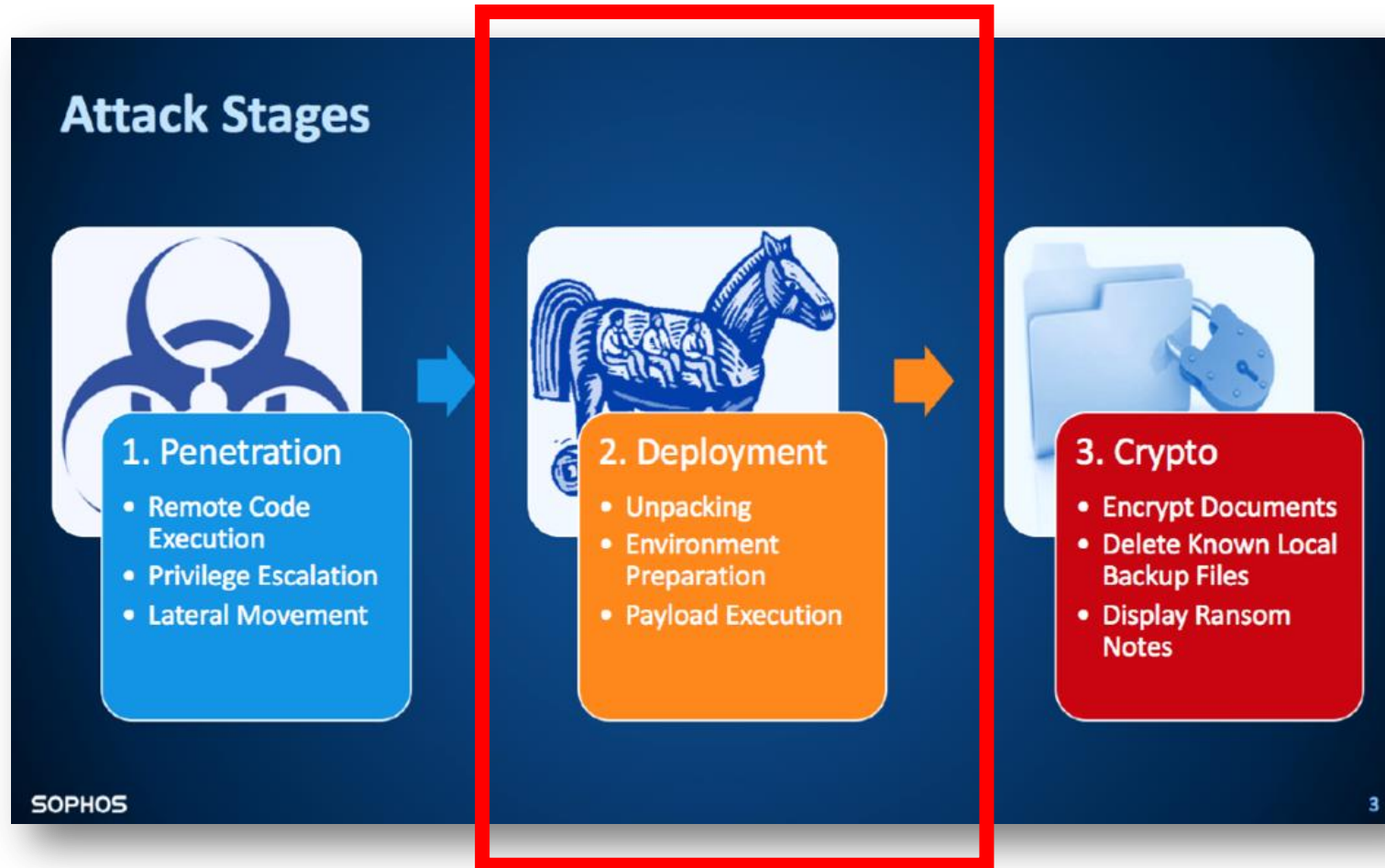
# Defending Against Ransomware

## 4. Employee training

- Anti-phishing training won't stop advanced ransomware attacks that are perpetrated by infiltrating the network. They may however prevent low-grade attacks – IF the training is sufficient and repeated
- Better to re-think employee authorization/permissions and monitor employees for dangerous/negligent activities (personal Internet use)
- Training works best when it empowers employees, not scolds them



# Defending Against Ransomware





# Defending Against Ransomware

## 6. Segregate your networks

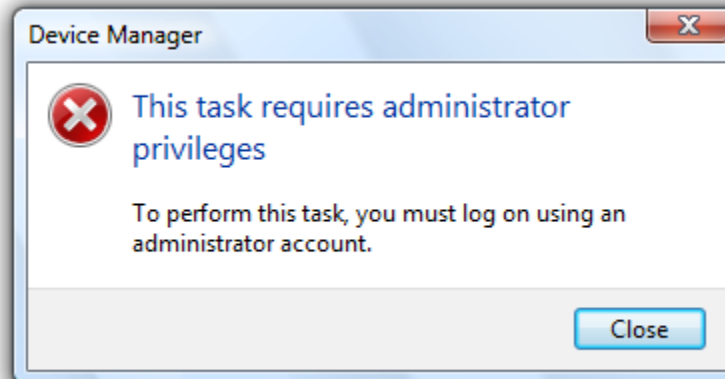
- Separate your network into smaller, independent networks
- If a ransomware infection occurs, it will be limited to the isolated network instead of propagating across the entire enterprise



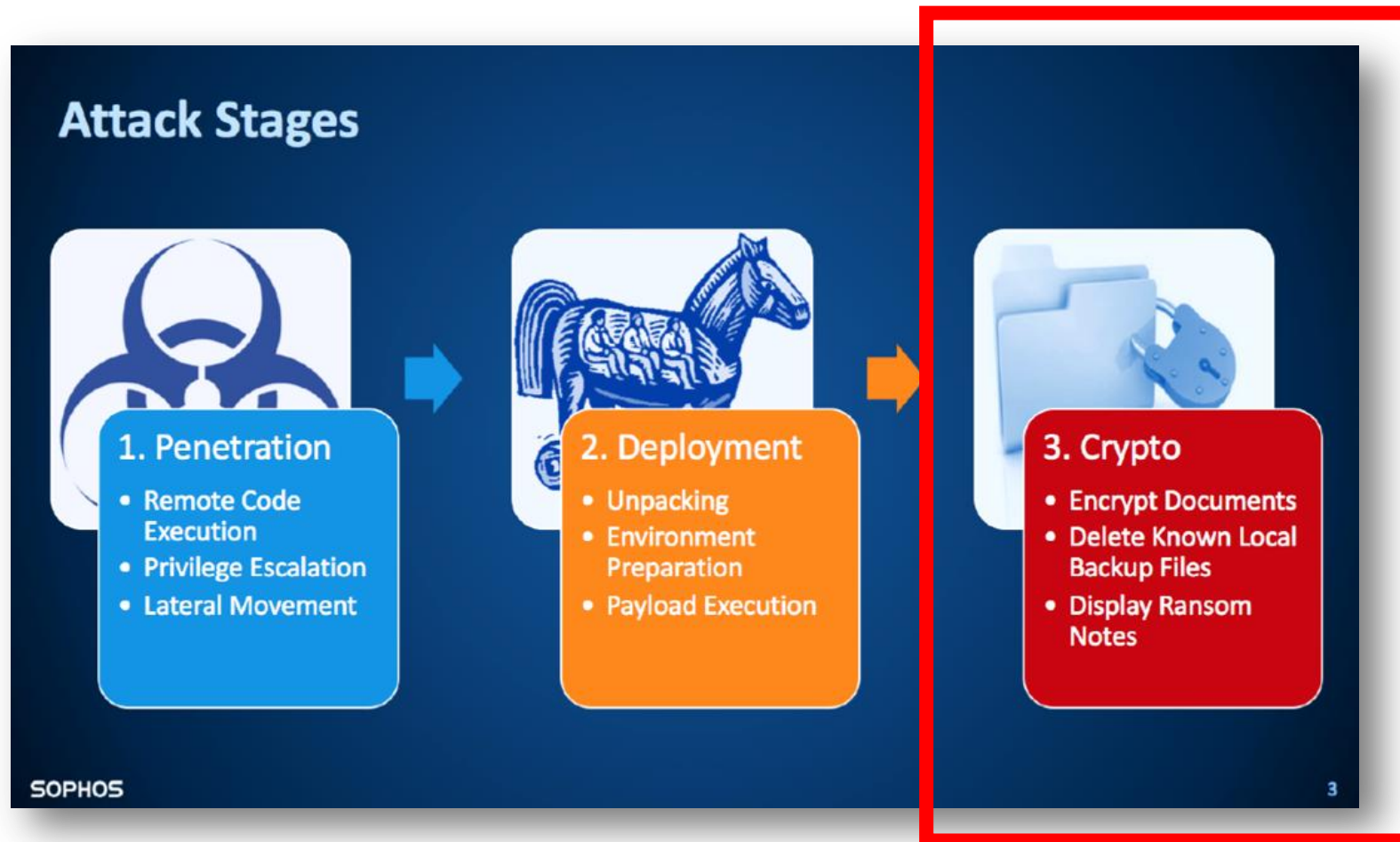
# Defending Against Ransomware

## 7. Ensure end users are not administrators

- Ransomware generally requires administrative permissions to execute and spread laterally
- Limit the number of administrative accounts on the network



# Defending Against Ransomware



# Defending Against Ransomware

## 8. Offline backups!

- Regularly back-up any files stored on your devices – how often depends on internal risk assessments and educated review
- Test the restoration of data on a minimum quarterly basis
- Ensure your backups are NOT connected to the rest of your critical network, otherwise your backups will also be infected with ransomware if an incident does occur
- Using online cloud backups that auto-sync your data is NOT enough – as files are undergoing encryption during an active ransomware infection, the newly encrypted files will be synced to the cloud thus overwriting any functional copies of those files stored in the backup

# Attack Stages



## 1. Penetration

- Remote Code Execution
- Privilege Escalation
- Lateral Movement



## 2. Deployment

- Unpacking
- Environment Preparation
- Payload Execution



## 3. Crypto

- Encrypt Documents
- Delete Known Local Backup Files
- Display Ransom Notes

SOPHOS

3

