In the Trenches: Dealing with Ransomware and their Attackers

May 2019

Kivu Consulting, Inc.

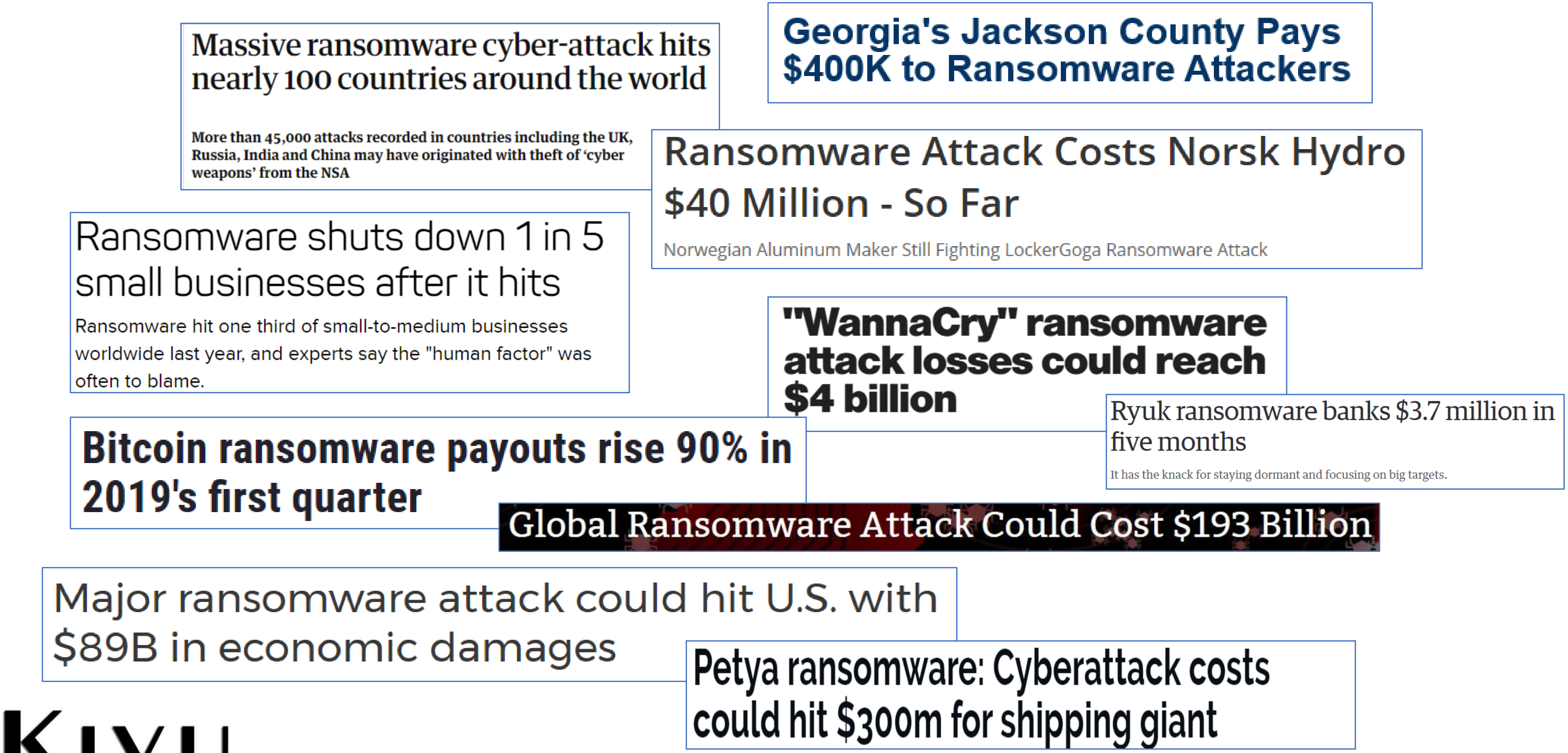
Jaycee Roth

Senior Analyst, Cyber Investigations

The Game Plan

- What is ransomware?
- Mythbusters
- Evolution of ransomware
- Defending against ransomware

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

Georgia's Jackson County Pays $400K to Ransomware Attackers

Ransomware Attack Costs Norsk Hydro $40 Million - So Far

Norwegian Aluminum Maker Still Fighting LockerGoga Ransomware Attack

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

Ryuk ransomware banks $3.7 million in five months

It has the knack for staying dormant and focusing on big targets.

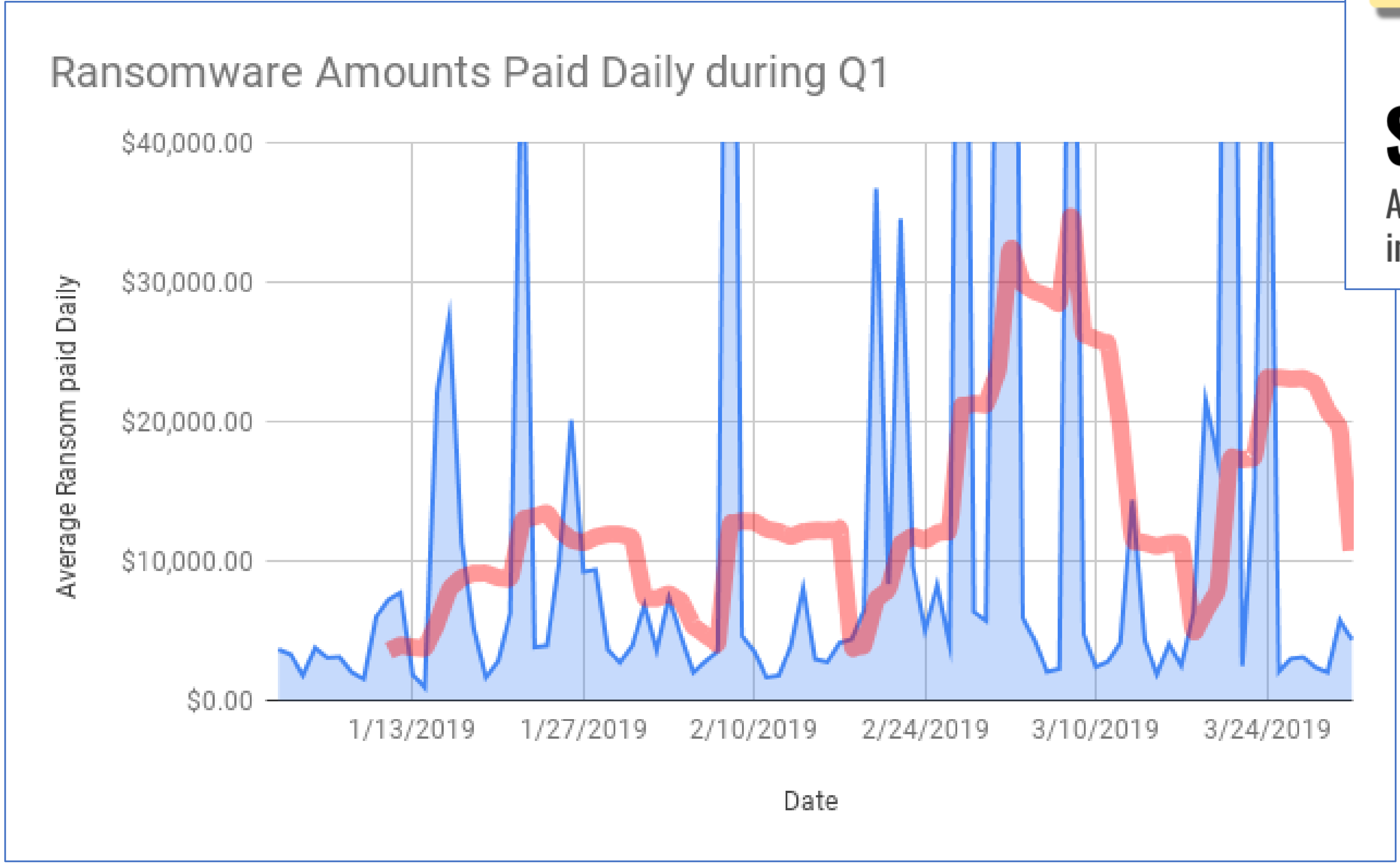
Bitcoin ransomware payouts rise 90% in 2019's first quarter

Global Ransomware Attack Could Cost $193 Billion

Major ransomware attack could hit U.S. with $89B in economic damages

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

Ransomware Pandemic



7.3 days

Average number of days a ransomware incident lasts

$64,645

Average cost of ransomware incident related downtime

www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

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

KIVU

Who is at Risk?

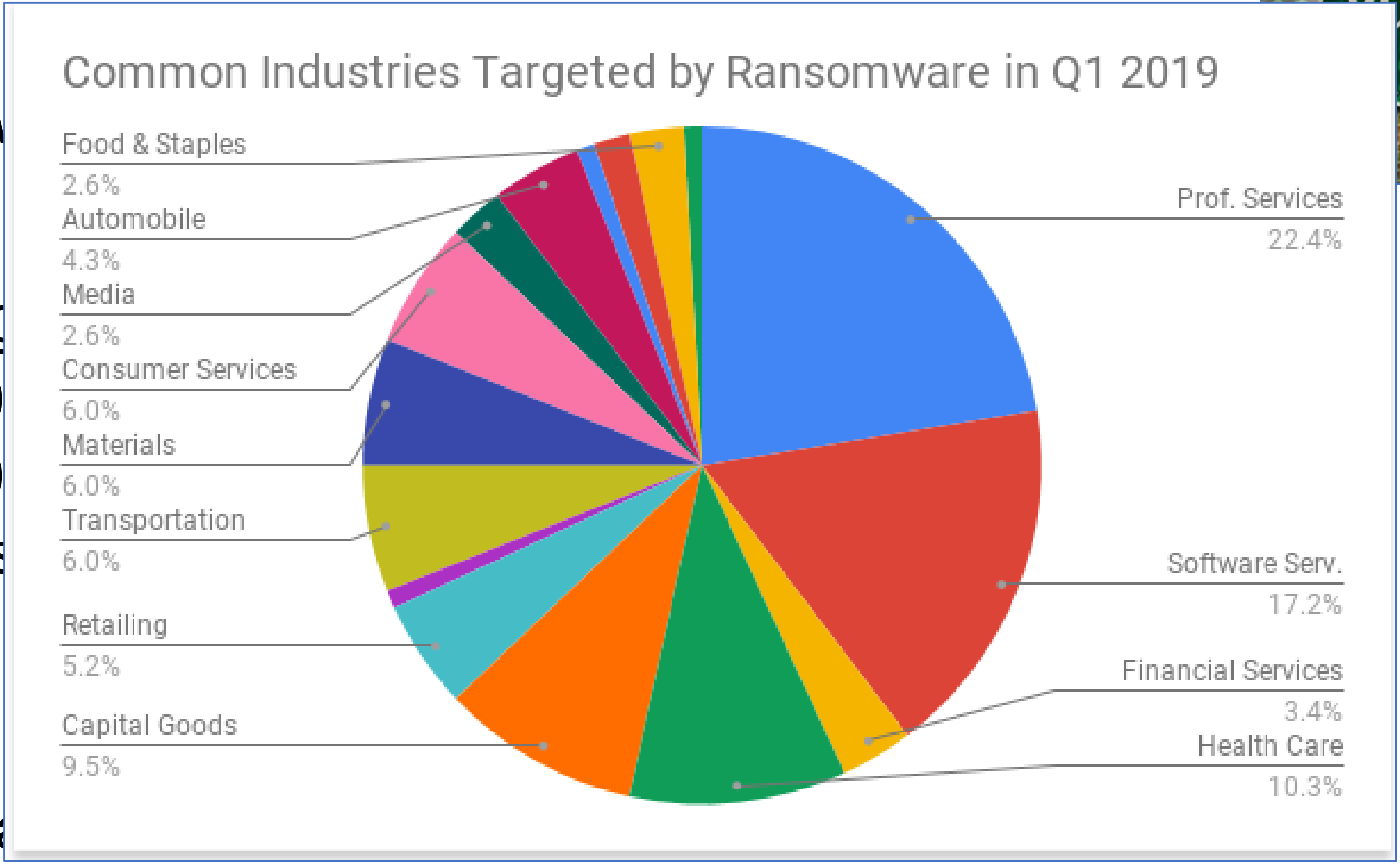
- Anyone who is connected to the internet

- 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

Who is at Risk?

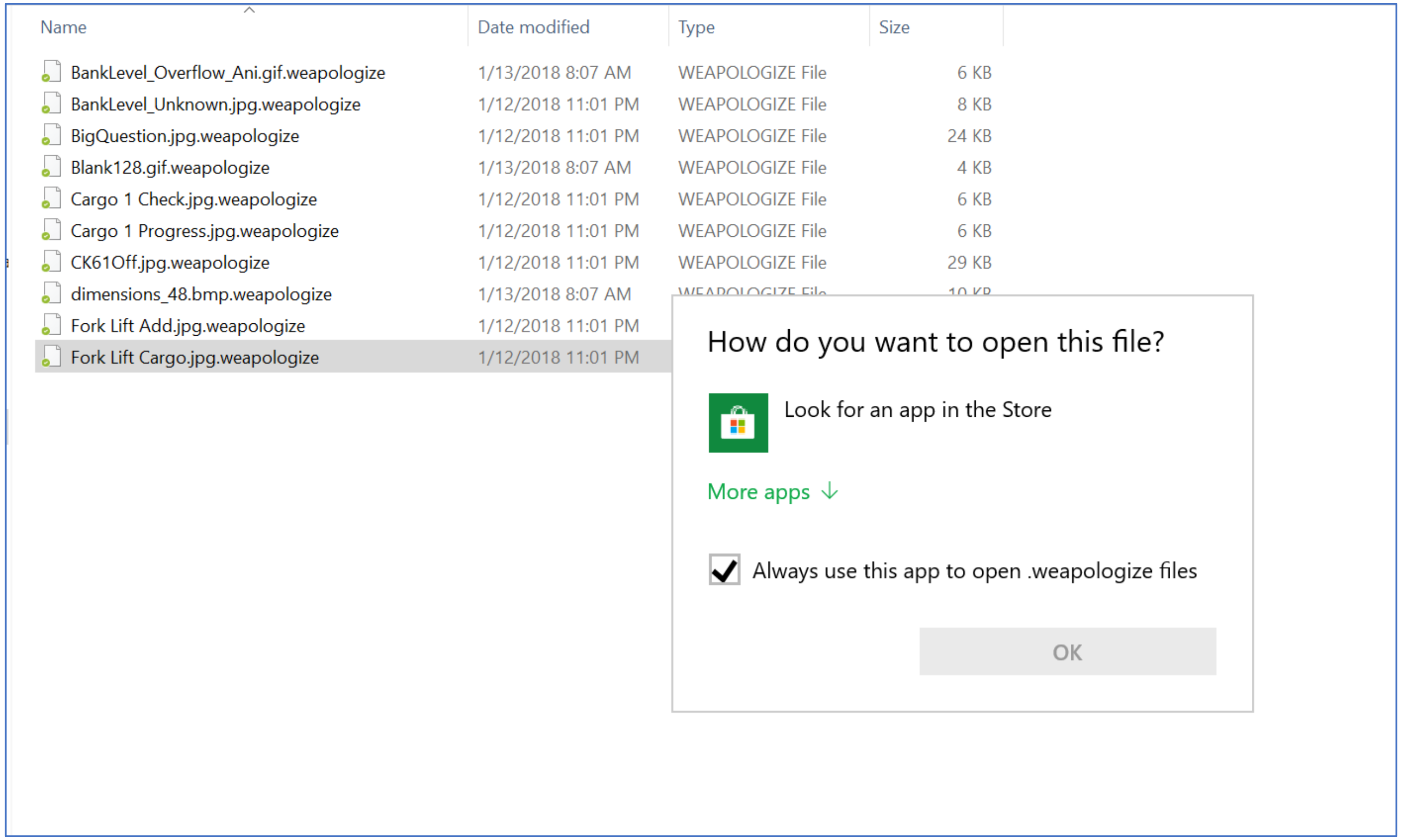
- Anyone w
- Every sec
  - 15,000
  - 15,000
  - 8,000 s
- 29% of in
  - Automa


Common Industries Targeted by Ransomware in Q1 2019

KIVU

What does an attack look like?

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



Name	Date modified	Type	Size
BankLevel_Overflow_Ani.gif.weapologize	1/13/2018 8:07 AM	WEAPOLOGIZE File	6 KB
BankLevel_Unknown.jpg.weapologize	1/12/2018 11:01 PM	WEAPOLOGIZE File	8 KB
BigQuestion.jpg.weapologize	1/12/2018 11:01 PM	WEAPOLOGIZE File	24 KB
Blank128.gif.weapologize	1/13/2018 8:07 AM	WEAPOLOGIZE File	4 KB
Cargo 1 Check.jpg.weapologize	1/12/2018 11:01 PM	WEAPOLOGIZE File	6 KB
Cargo 1 Progress.jpg.weapologize	1/12/2018 11:01 PM	WEAPOLOGIZE File	6 KB
CK61Off.jpg.weapologize	1/12/2018 11:01 PM	WEAPOLOGIZE File	29 KB
dimensions_48.bmp.weapologize	1/13/2018 8:07 AM	WEAPOLOGIZE File	10 KB
Fork Lift Add.jpg.weapologize	1/12/2018 11:01 PM		
Fork Lift Cargo.jpg.weapologize	1/12/2018 11:01 PM		

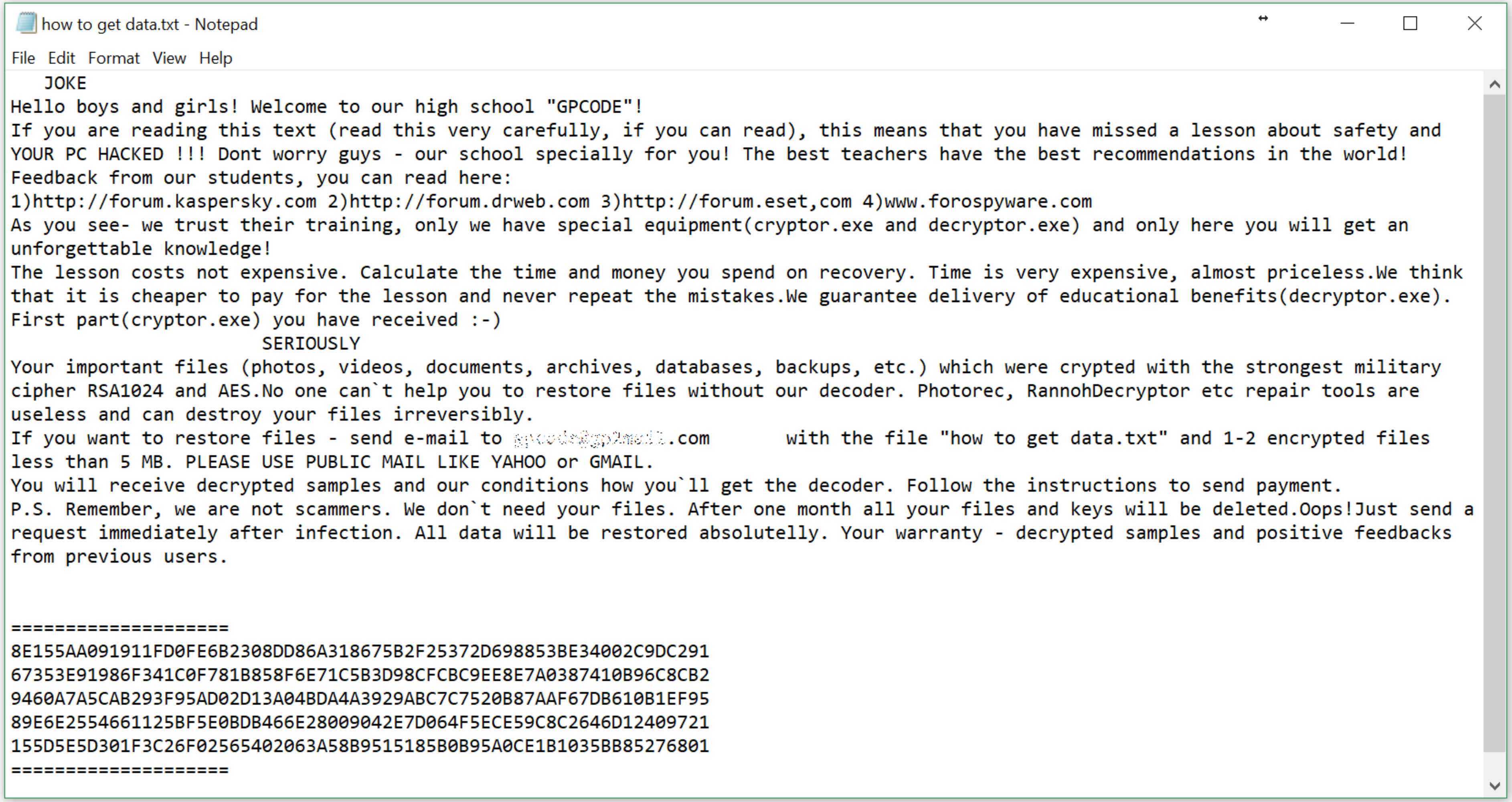
How do you want to open this file?

Look for an app in the Store

More apps ↓

☑ Always use this app to open .weapologize files

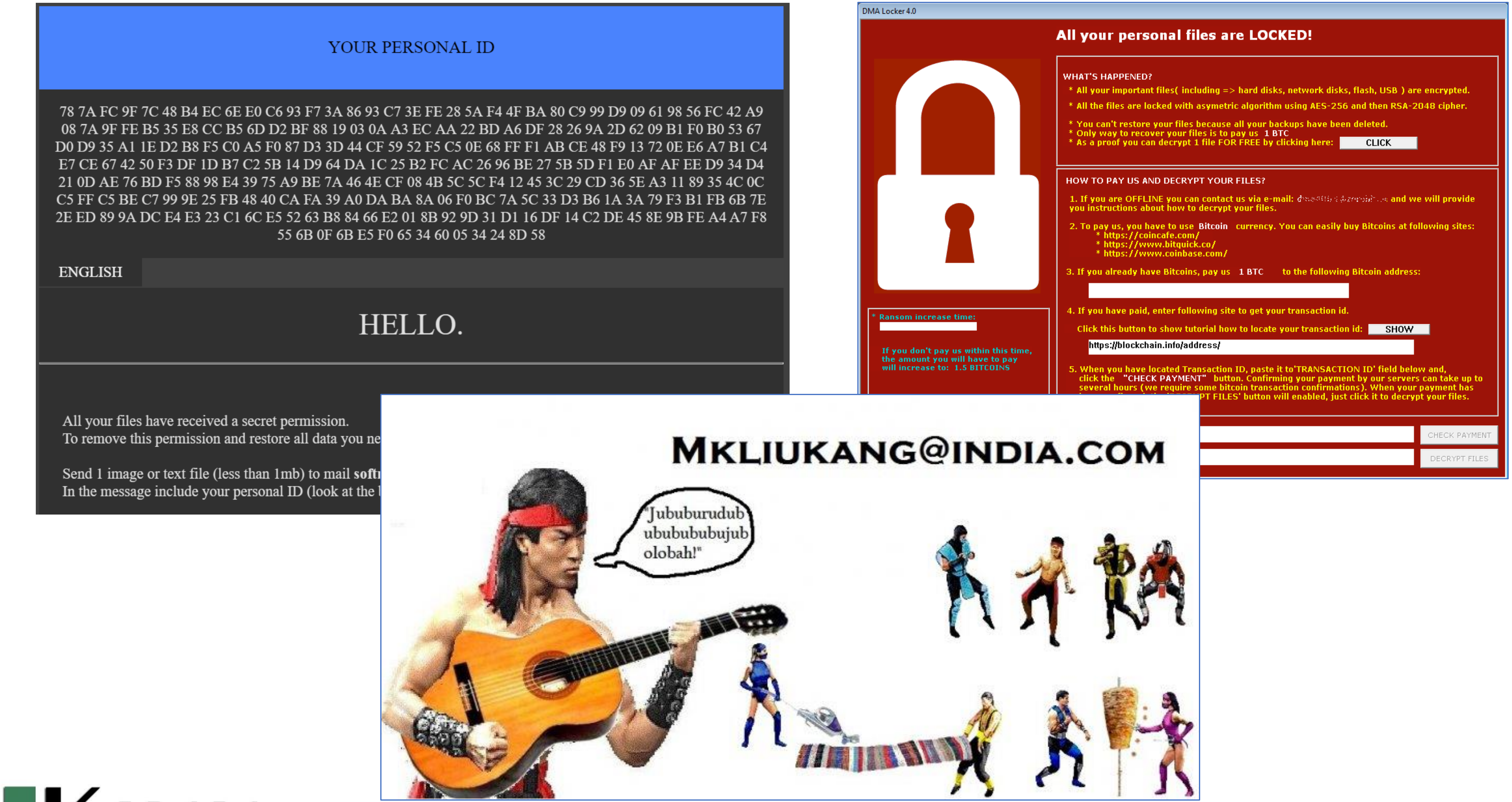
- Ransom note



```
   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 [redacted].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
67353E91986F341C0F781B858F6E71C5B3D98CFCBC9EE8E7A0387410B96C8CB2
9460A7A5CAB293F95AD02D13A04BDA4A3929ABC7C7520B87AAF67DB610B1EF95
89E6E2554661125BF5E0BDB466E28009042E7D064F5ECE59C8C2646D12409721
155D5E5D301F3C26F02565402063A58B9515185B0B95A0CE1B1035BB85276801
====================
```



YOUR PERSONAL ID

78 7A FC 9F 7C 48 B4 EC 6E E0 C6 93 F7 3A 86 93 C7 3E FE 28 5A F4 4F BA 80 C9 99 D9 09 61 98 56 FC 42 A9
08 7A 9F FE B5 35 E8 CC B5 6D D2 BF 88 19 03 0A A3 EC AA 22 BD A6 DF 28 26 9A 2D 62 09 B1 F0 B0 53 67
D0 D9 35 A1 1E D2 B8 F5 C0 A5 F0 87 D3 3D 44 CF 59 52 F5 C5 0E 68 FF F1 AB CE 48 F9 13 72 0E E6 A7 B1 C4
E7 CE 67 42 50 F3 DF 1D B7 C2 5B 14 D9 64 DA 1C 25 B2 FC AC 26 96 BE 27 5B 5D F1 E0 AF AF EE D9 34 D4
21 0D AE 76 BD F5 88 98 E4 39 75 A9 BE 7A 46 4E CF 08 4B 5C 5C F4 12 45 3C 29 CD 36 5E A3 11 89 35 4C 0C
C5 FF C5 BE C7 99 9E 25 FB 48 40 CA FA 39 A0 DA BA 8A 06 F0 BC 7A 5C 33 D3 B6 1A 3A 79 F3 B1 FB 6B 7E
2E ED 89 9A DC E4 E3 23 C1 6C E5 52 63 B8 84 66 E2 01 8B 92 9D 31 D1 16 DF 14 C2 DE 45 8E 9B FE A4 A7 F8
55 6B 0F 6B E5 F0 65 34 60 05 34 24 8D 58

ENGLISH

HELLO.

All your files have received a secret permission.
To remove this permission and restore all data you ne

Send 1 image or text file (less than 1mb) to mail **soft**
In the message include your personal ID (look at the t

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 asymetric 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: CLICK

HOW TO PAY US AND DECRYPT YOUR FILES?

1. If you are OFFLINE you can contact us via e-mail: [redacted] 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: SHOW

   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 PT FILES' button will 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

CHECK PAYMENT

DECRYPT FILES

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

SHUTTERSTOCK/CAROLINE MATTHEWS/CNNMONEY

Misconceptions

Myth

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

Misconceptions

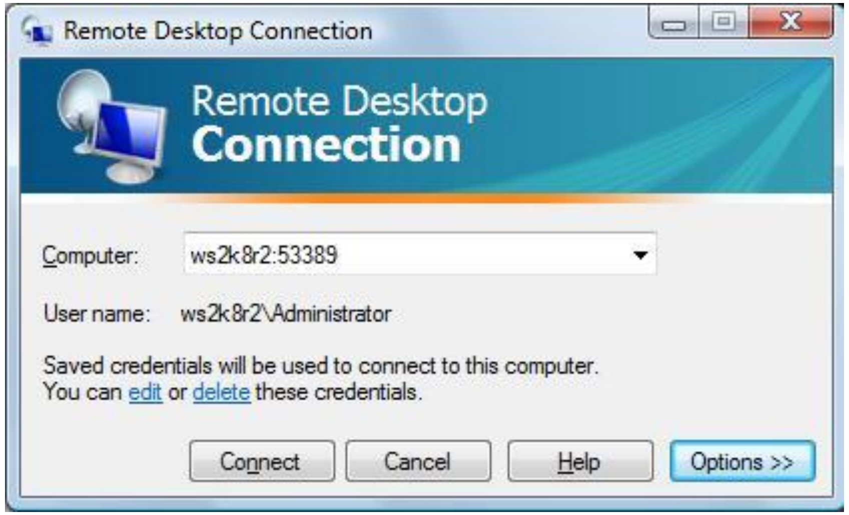
Myth

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**.

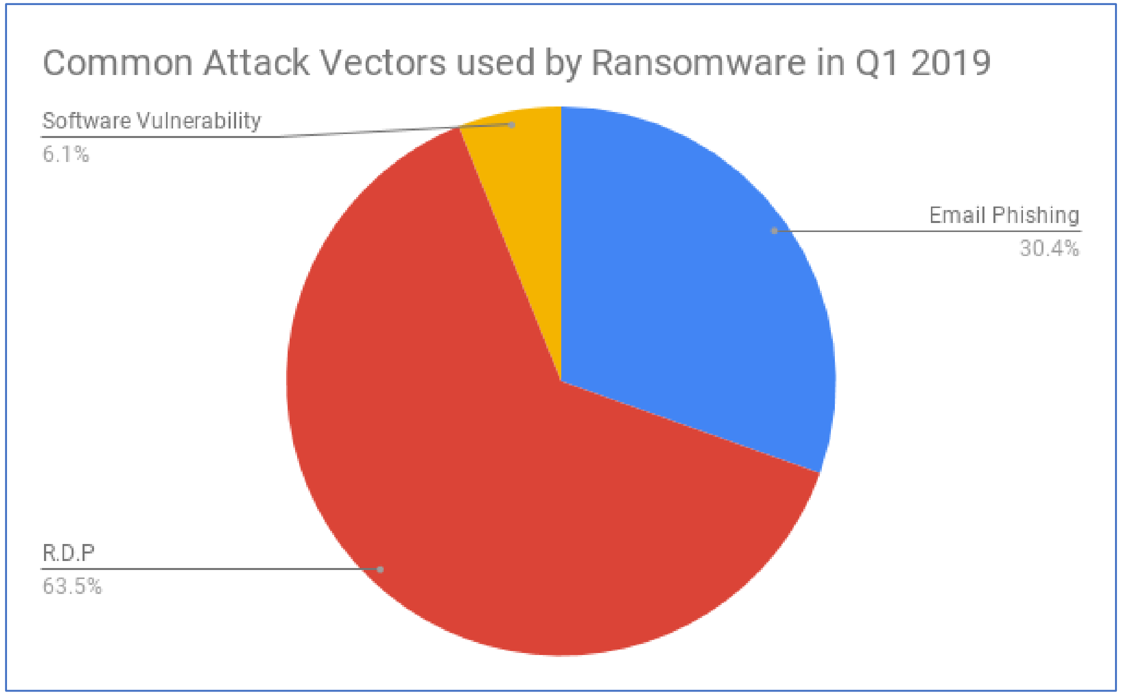
- Remote Desktop Protocol
  - Low-hanging fruit
  - Used to be the intrusion vector in ~95% of ransomware cases, now ~65%
  - More organizations are using VPNs, remoting software, MFA



Computer: ws2k8r2:53389

User name: ws2k8r2\Administrator

Saved credentials will be used to connect to this computer.
You can edit or delete these credentials.

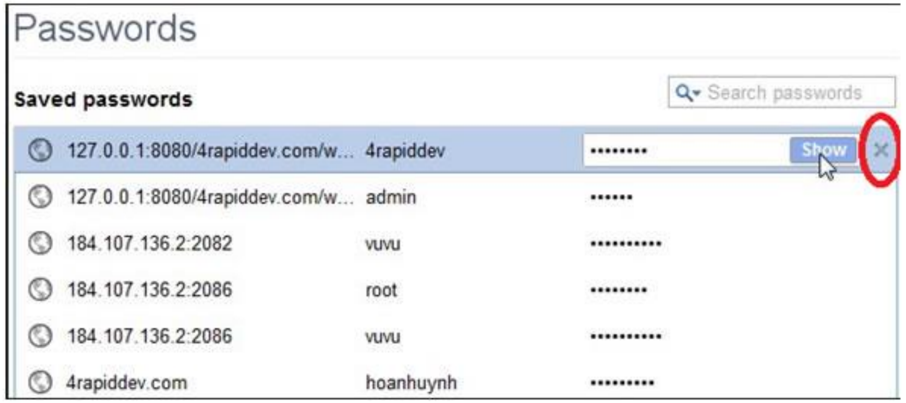

Common Attack Vectors used by Ransomware in Q1 2019

KIVU

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

1040
Department of the Treasury—Internal Revenue Service
U.S. Individual Income Tax Return
the year Jan. 1–Dec. 31, 2011, or other tax year beginning
first name and initial
Last name
spouse's first name and initial
If you have a P.O. box, see



Passwords

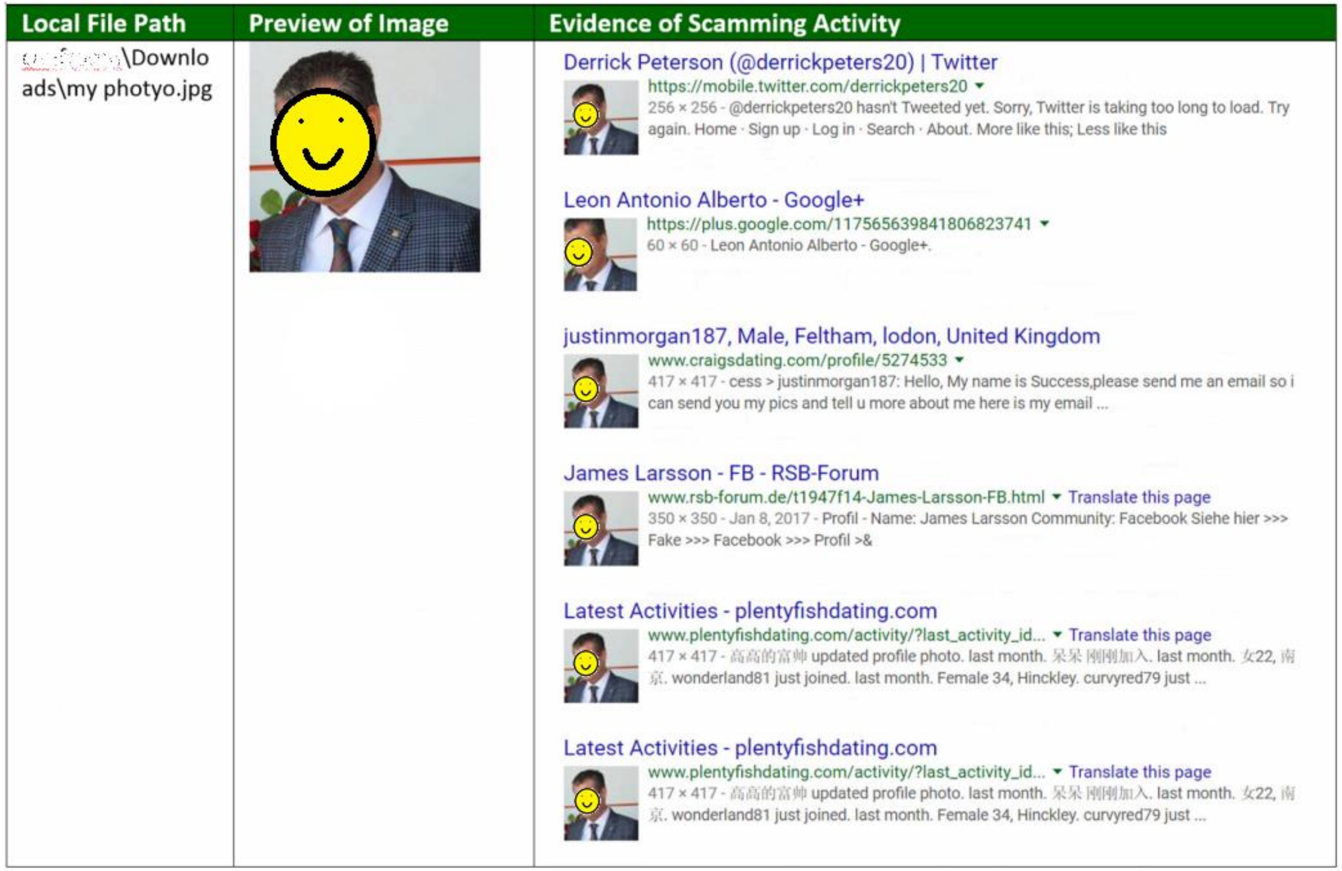
Saved passwords

127.0.0.1:8080/4rapiddev.com/w...	4rapiddev	••••••••
127.0.0.1:8080/4rapiddev.com/w...	admin	••••••
184.107.136.2:2082	vuvu	••••••••••
184.107.136.2:2086	root	••••••••
184.107.136.2:2086	vuvu	••••••••••
4rapiddev.com	hoanhuynh	•••••••••

Attacker Activities

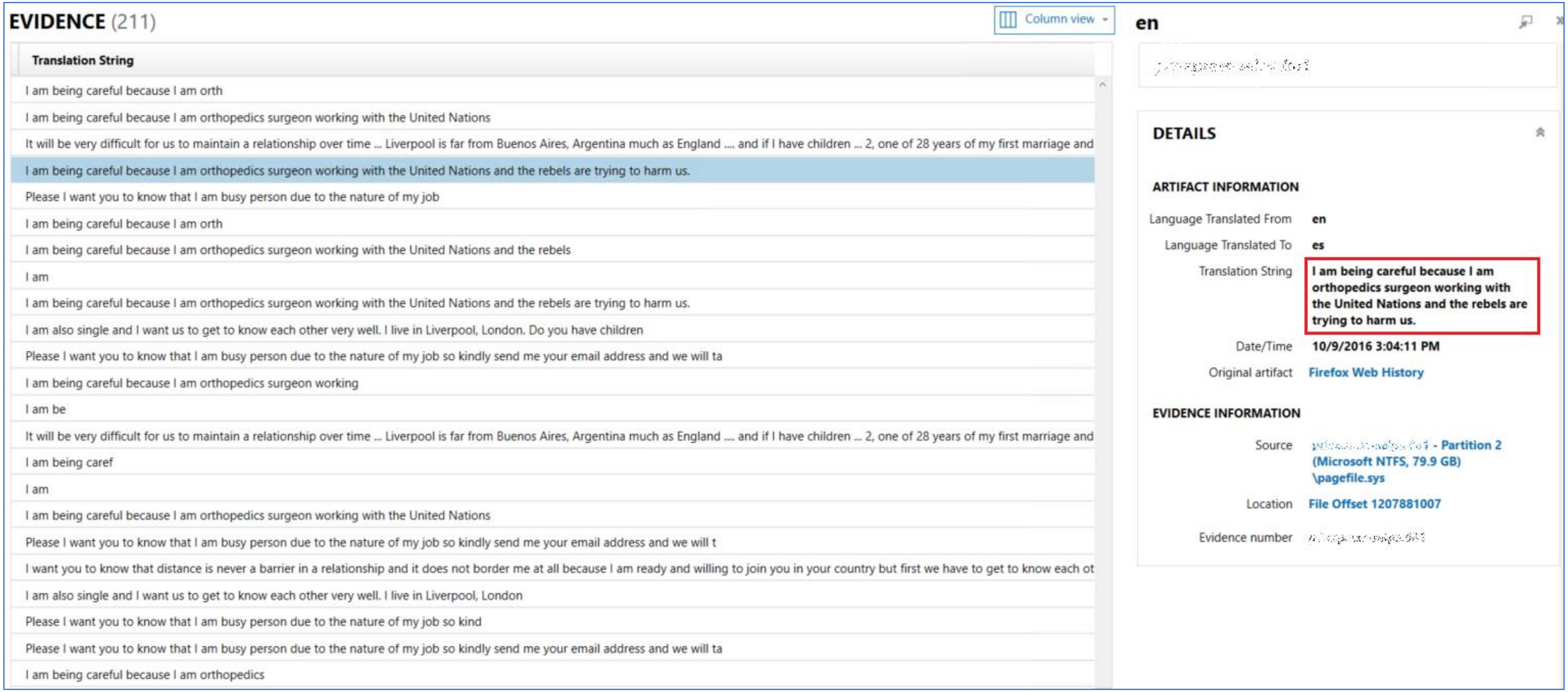
Frequently the victim has been compromised for months – the ransomware attack was just the final insult.

- Activities include:
    - Crytocurrency 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
[redacted]\Downloads\my photyo.jpg		Derrick Peterson (@derrickpeters20) | Twitter https://mobile.twitter.com/derrickpeters20 ▾ 256 × 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 Leon Antonio Alberto - Google+ https://plus.google.com/117565639841806823741 ▾ 60 × 60 - Leon Antonio Alberto - Google+. justinmorgan187, Male, Feltham, lodon, United Kingdom www.craigsdating.com/profile/5274533 ▾ 417 × 417 - cess > 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 ... James Larsson - FB - RSB-Forum www.rsb-forum.de/t1947f14-James-Larsson-FB.html ▾ Translate this page 350 × 350 - Jan 8, 2017 - Profil - Name: James Larsson Community: Facebook Siehe hier >>> Fake >>> Facebook >>> Profil >& Latest Activities - plentyfishdating.com www.plentyfishdating.com/activity/?last_activity_id... ▾ Translate this page 417 × 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 ... Latest Activities - plentyfishdating.com www.plentyfishdating.com/activity/?last_activity_id... ▾ Translate this page 417 × 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 ...

KIVU



EVIDENCE (211)

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

en

[redacted]

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: [redacted] **- Partition 2 (Microsoft NTFS, 79.9 GB) \pagefile.sys**

Location: **File Offset 1207881007**

Evidence number: [redacted]

KIVU

Misconceptions

Myth

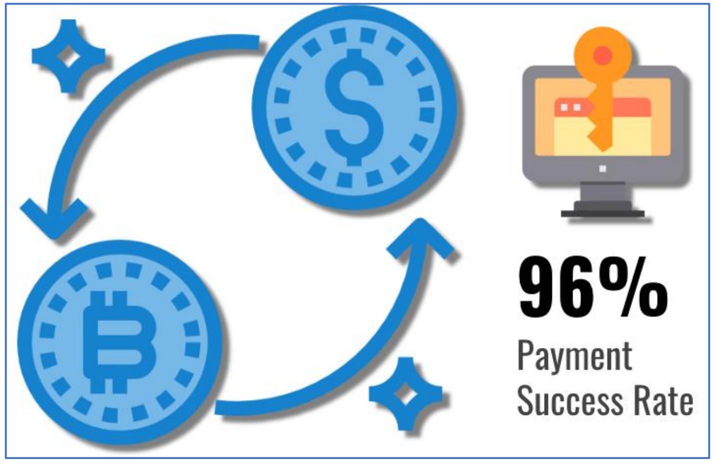
Most attackers take your money and run, without restoring your files.

Misconceptions

Myth

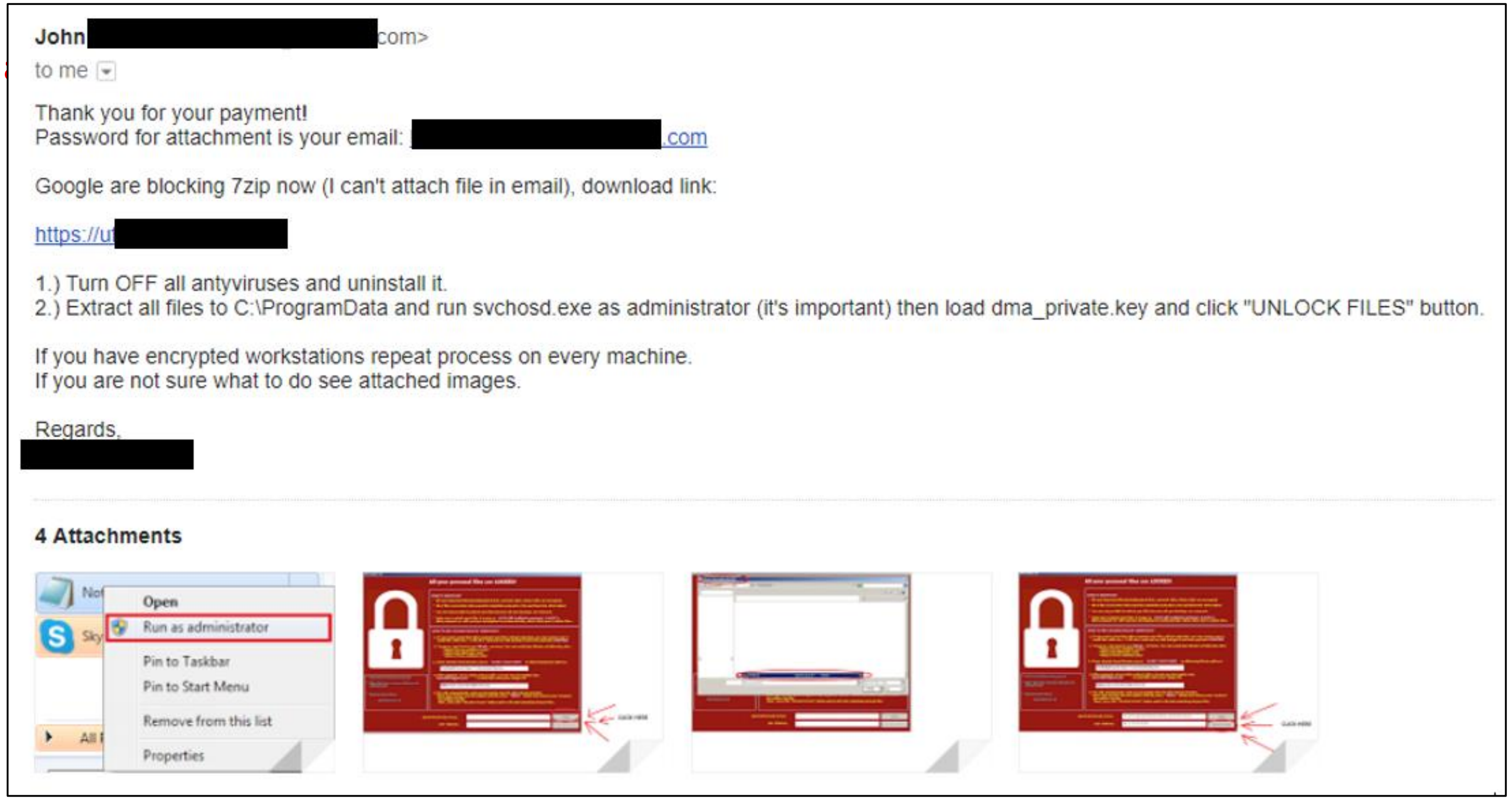
Most attackers take your money and run, without restoring your files.

Reality



Misconceptions

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



John [redacted]com>

to me

Thank you for your payment!
Password for attachment is your email: [redacted].com

Google are blocking 7zip now (I can't attach file in email), download link:

https://u[redacted]

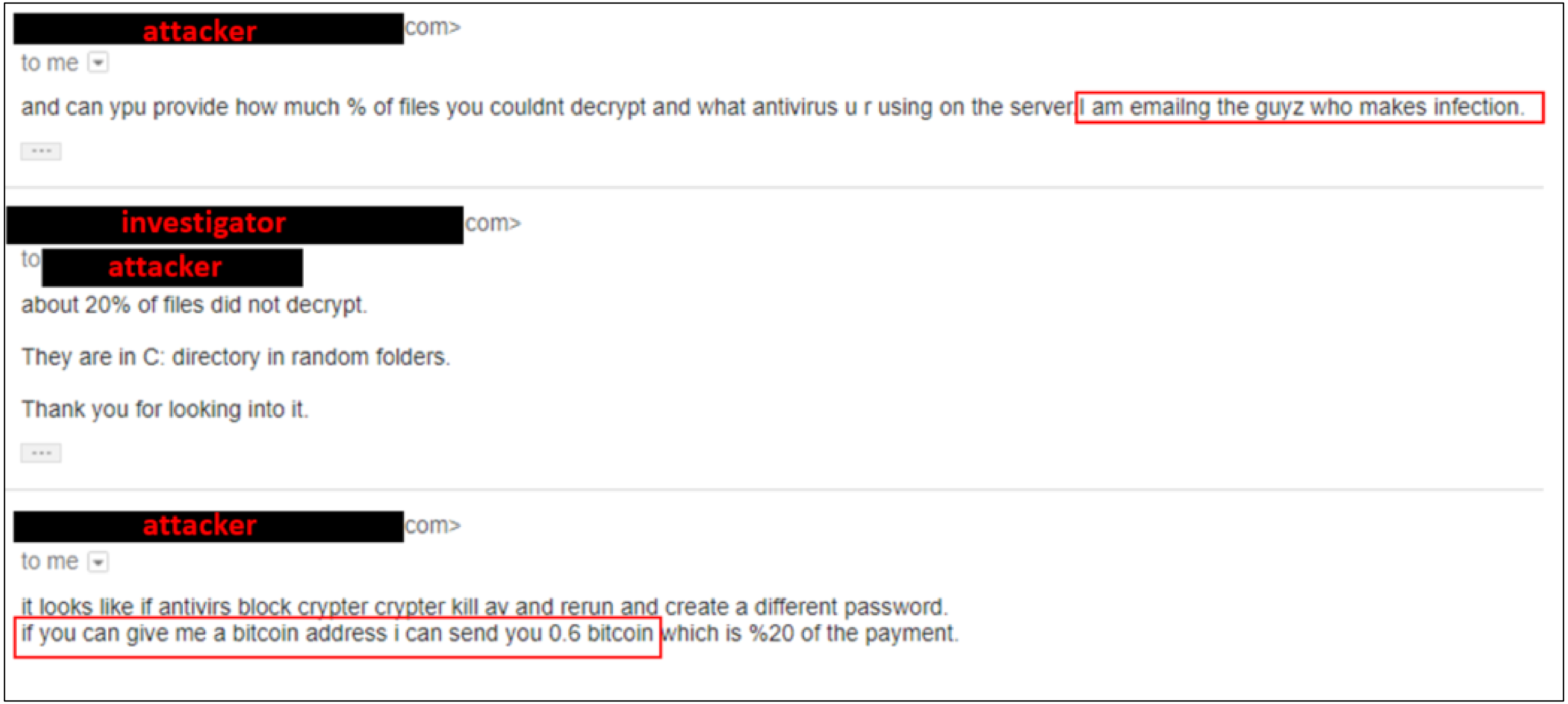
1.) Turn OFF all antyviruses and uninstall it.
2.) Extract all files to C:\ProgramData and run svchosd.exe as administrator (it's important) then load dma_private.key and click "UNLOCK FILES" button.

If you have encrypted workstations repeat process on every machine.
If you are not sure what to do see attached images.

Regards,
[redacted]

4 Attachments

Misconceptions



[redacted] attacker com>

to me

and can ypu provide how much % of files you couldnt decrypt and what antivirus u r using on the server I am emailng the guyz who makes infection.

[redacted] investigator com>

to [redacted] attacker

about 20% of files did not decrypt.

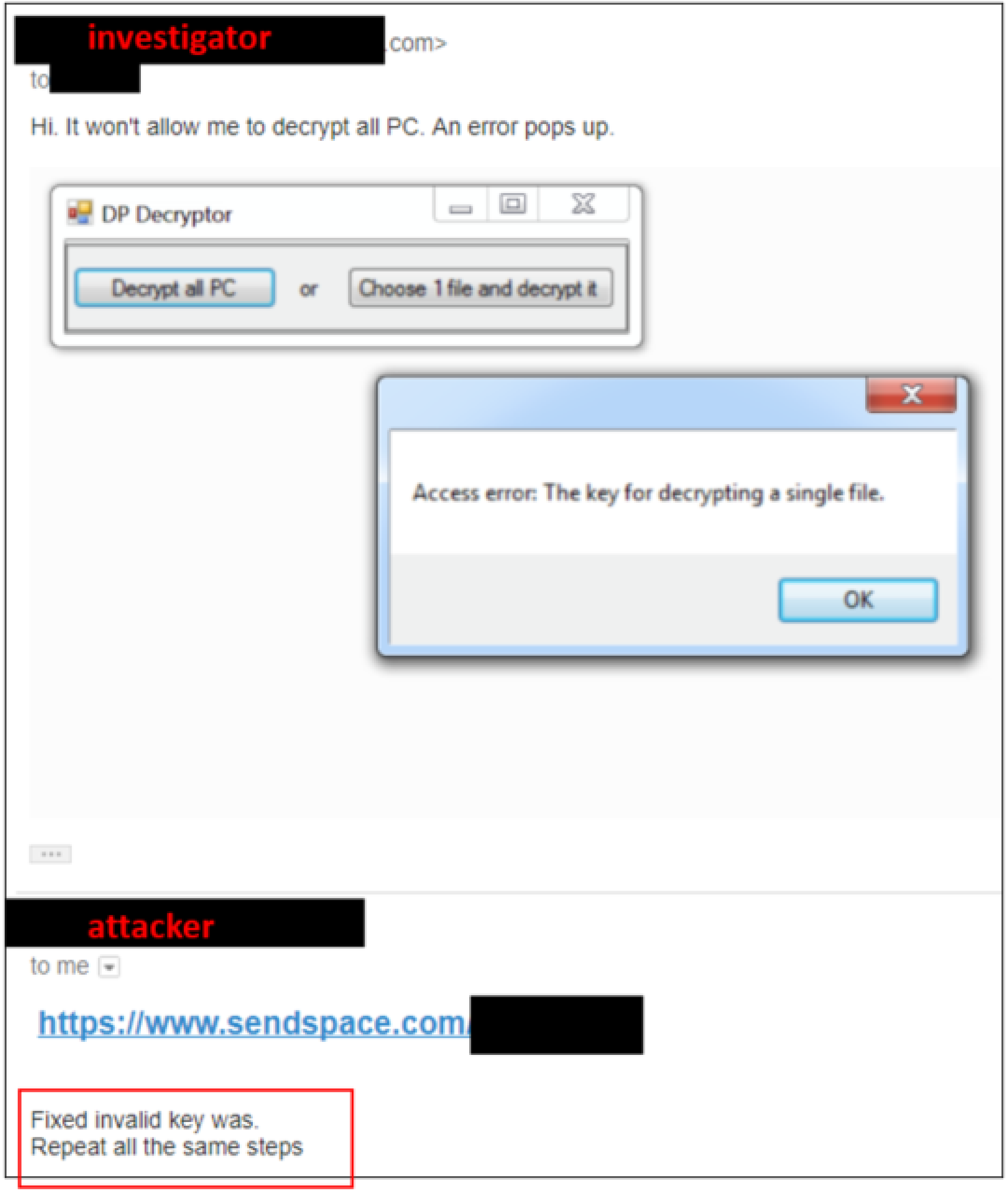
They are in C: directory in random folders.

Thank you for looking into it.

[redacted] attacker 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.

Access error: The key for decrypting a single file.

attacker [redacted]

to me

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

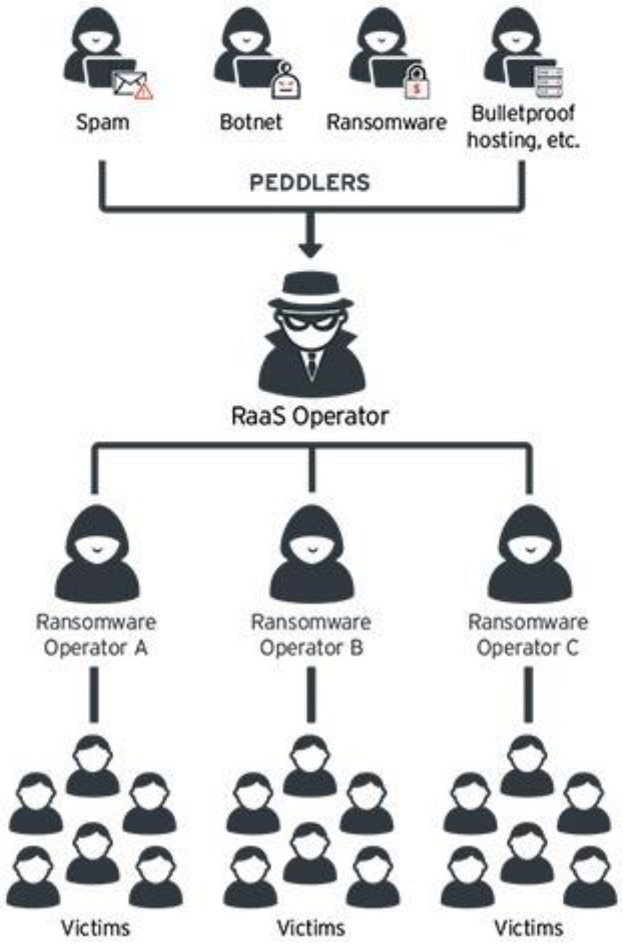
Myth

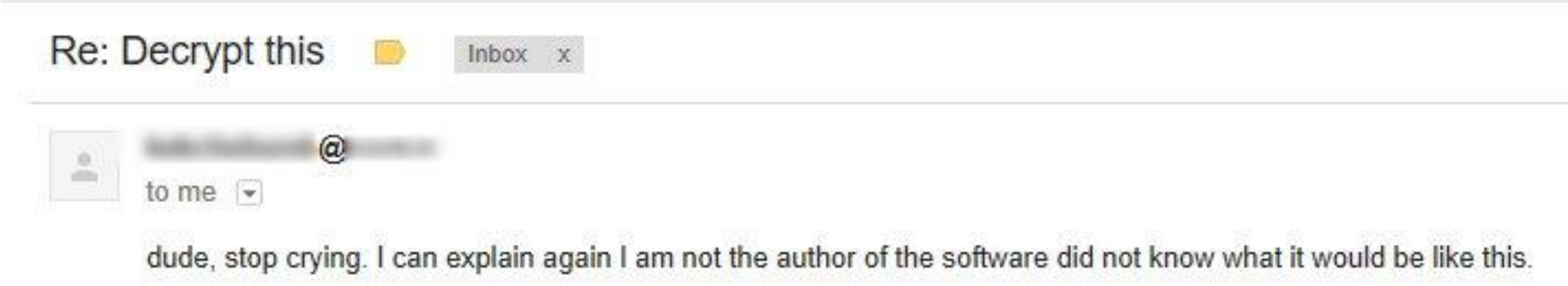
Ransomware attackers are technologically-savvy.

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.


Spam
Botnet
Ransomware
Bulletproof hosting, etc.
PEDDLERS
RaaS Operator
Ransomware Operator A
Ransomware Operator B
Ransomware Operator C
Victims
Victims
Victims



Re: Decrypt this

[redacted]@[redacted]

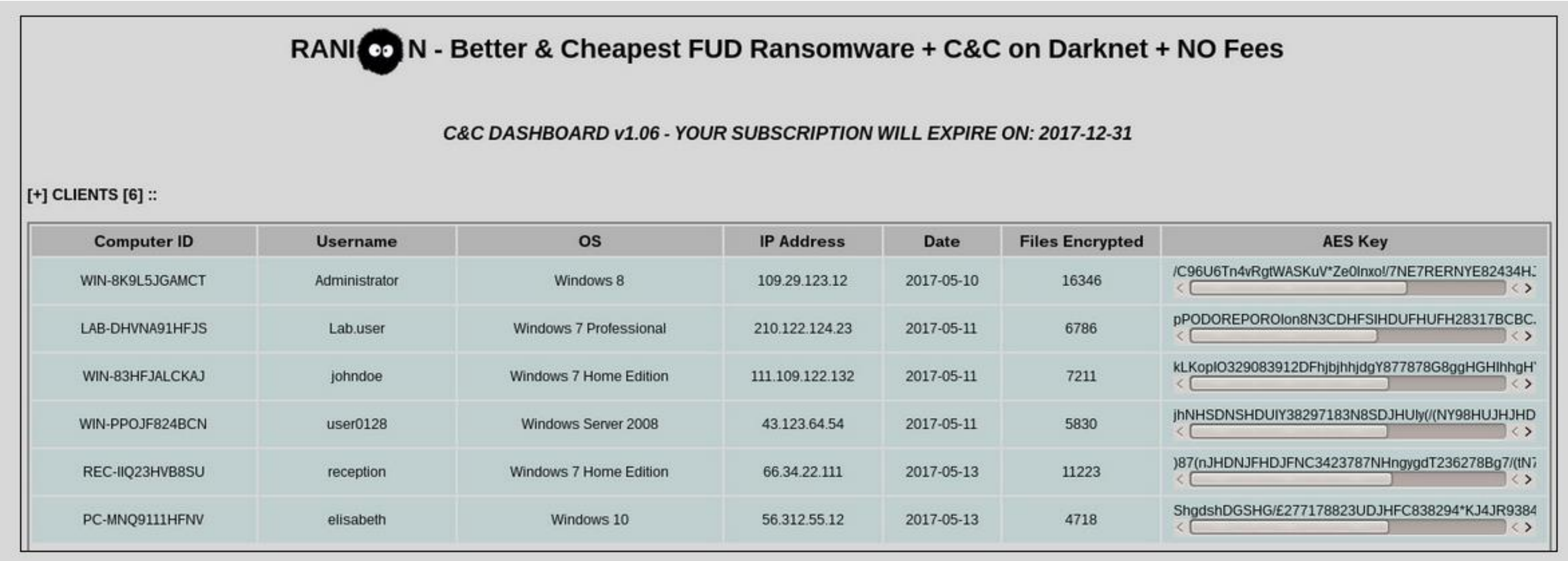
to me

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

Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS)

- RaaS has been gaining traction since the end of 2016
- The profit-sharing model is attractive for subscribers and developers
- Instead of paying a flat fee for a single piece of malware, **the user can sign up for a free** or inexpensive platform that provides:
  - Access to ransomware
  - A user-friendly dashboard to monitor victims
  - Customizable features (demand amount, email address, wallet, extension)



RANI●N - Better & Cheapest FUD Ransomware + C&C on Darknet + NO Fees

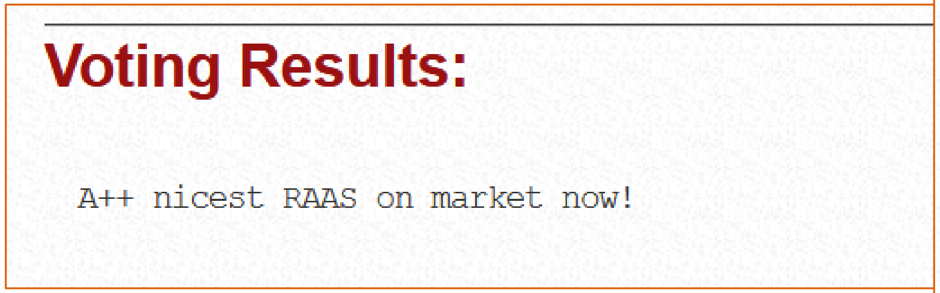
C&C DASHBOARD v1.06 - YOUR SUBSCRIPTION WILL EXPIRE ON: 2017-12-31

[+] CLIENTS [6] ::

Computer ID	Username	OS	IP Address	Date	Files Encrypted	AES Key
WIN-8K9L5JGAMCT	Administrator	Windows 8	109.29.123.12	2017-05-10	16346	/C96U6Tn4vRgtWASKuV*Ze0lnxo!/7NE7RERNYE82434H
LAB-DHVNA91HFJS	Lab.user	Windows 7 Professional	210.122.124.23	2017-05-11	6786	pPODOREPOROlon8N3CDHFSIHDUFHUFH28317BCBC
WIN-83HFJALCKAJ	johndoe	Windows 7 Home Edition	111.109.122.132	2017-05-11	7211	kLKoplO329083912DFhjbjhhjdgY877878G8ggHGHIhhgH
WIN-PPOJF824BCN	user0128	Windows Server 2008	43.123.64.54	2017-05-11	5830	jhNHSDNSHDUIY38297183N8SDJHUly(/(NY98HUJHJHD
REC-IIQ23HVB8SU	reception	Windows 7 Home Edition	66.34.22.111	2017-05-13	11223	)87(nJHDNJFHDJFNC3423787NHngygdT236278Bg7/(tN
PC-MNQ9111HFNV	elisabeth	Windows 10	56.312.55.12	2017-05-13	4718	ShgdshDGSHG/£277178823UDJHFC838294*KJ4JR9384

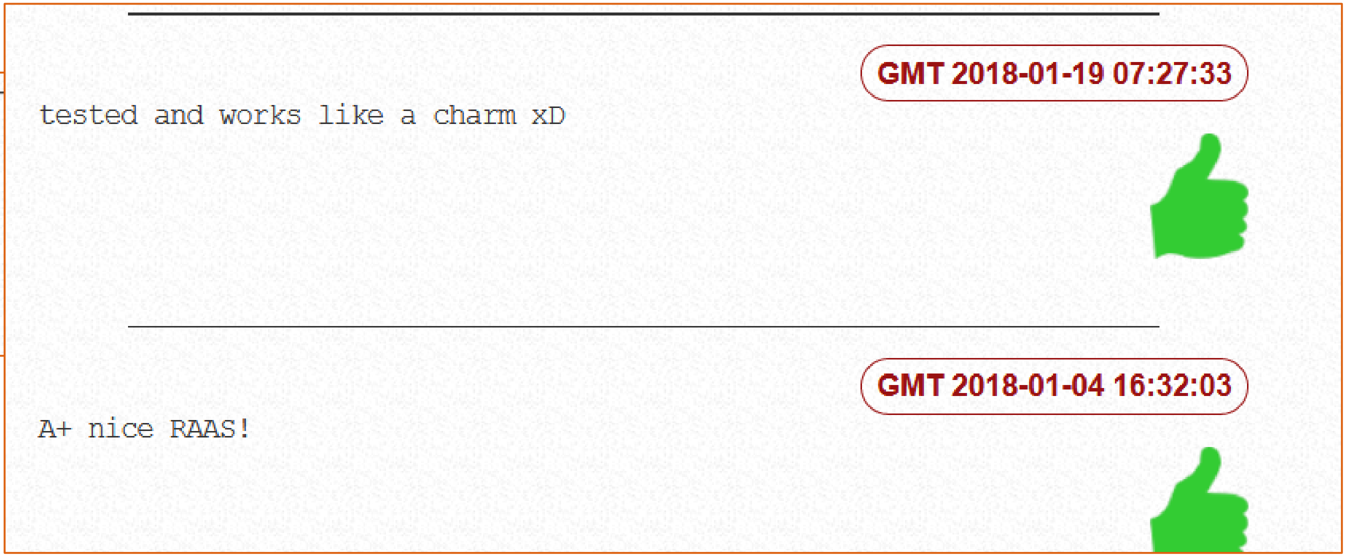
RaaS Update

- RaaS platforms vary in terms of what they offer
- Some offer a range of packages from “basic” to “platinum”
- Pricier subscriptions ensure access to additional features, like customer support, a malware downloader, and longer access to the server



Voting Results:

A++ nicest RAAS on market now!



GMT 2018-01-19 07:27:33

tested and works like a charm xD

👍

GMT 2018-01-04 16:32:03

A+ nice RAAS!

👍

RaaS Update

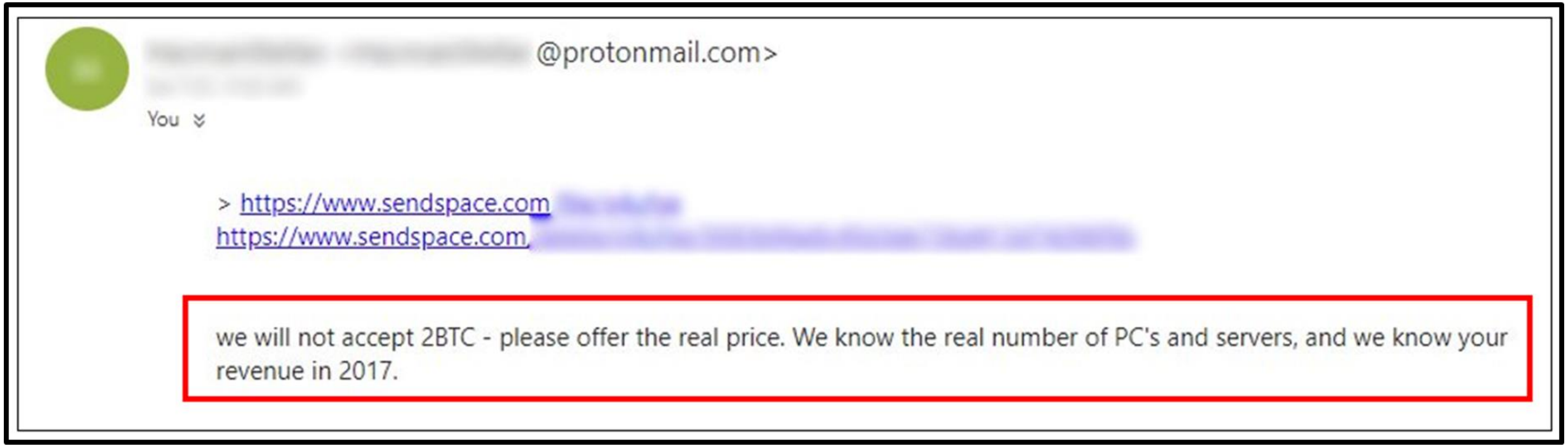
- The bad RaaS:
  - Platform does not screen their subscribers
  - Subscribers may have **little to no technical knowledge**
  - Subscribers tend to be hostile, **disorganized**
  - Malware samples are **not updated or improved** overtime
  - Developer provides **little to no customer support**

- The good RaaS:
  - Developers tightly control their pool of subscribers
  - Subscribers are **rigorously vetted** and must have prior hacking/ransom experience
  - Malware samples and decryption tools are **updated every few days** or weeks
  - Developers provide **robust customer support**

Ransomware is Evolving

Variant	Active	Demand Range
BitPaymer/iEncrypt	Apr 2018 – present	$62,000 - $1,300,000 for all
Ryuk	Aug 2018 – present	$45,000 - $2,000,000 for all
Target777/Defray	Dec 2018 - present	$100,000 - $740,000 for all
GandCrab	Jan 2018 - present	$1,500 - $4,000 per device

- Attackers are doing reconnaissance on victims before proceeding with the ransomware attack

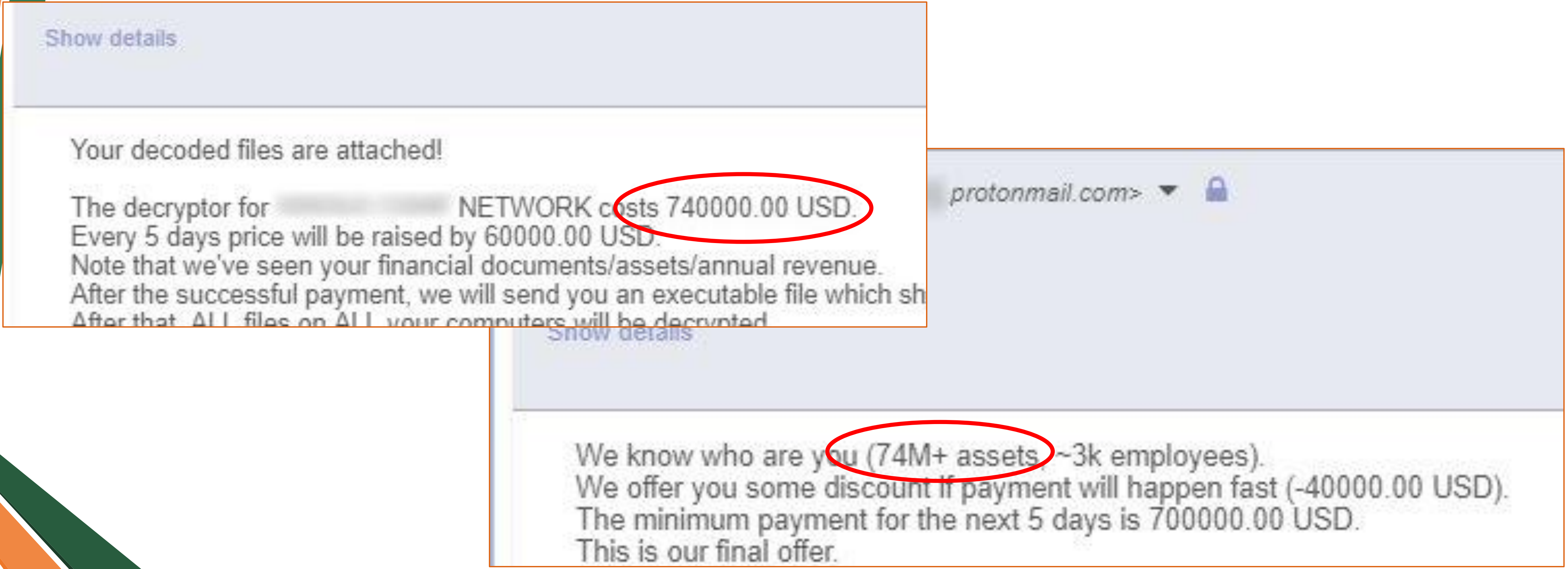


[redacted] @protonmail.com>
[redacted]
You

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

we will not accept 2BTC - please offer the real price. We know the real number of PC's and servers, and we know your revenue in 2017.

- Attackers are doing reconnaissance on victims before proceeding with the ransomware attack
- A clue to how the attackers generate the unique price per victim



Your decoded files are attached!

The decryptor for [redacted] NETWORK costs 740000.00 USD.
Every 5 days price will be raised by 60000.00 USD.
Note that we've seen your financial documents/assets/annual revenue.
After the successful payment, we will send you an executable file which sh
After that, ALL files on ALL your computers will be decrypted.

We know who are you (74M+ assets, ~3k employees).
We offer you some discount if payment will happen fast (-40000.00 USD).
The minimum payment for the next 5 days is 700000.00 USD.
This is our final offer.

Banking Trojan + Ransomware

- **Banking trojan** infections precede **BitPaymer and Ryuk** ransomware infections
- The banking trojan is introduced **days, weeks, or months** in advance of the ransomware attack
- The device where the banking trojan is introduced is usually *not* the device where **the ransomware is later introduced**
- Attacker uses **credentials harvested by the banking trojan** to later gain access to the victim network to deploy the ransomware

Banking Trojan + Ransomware

Banking Trojan is known to have five primary functions:

1. Harvest all **network passwords** stored on a system for the current logged-on user
2. Captures **passwords** stored by **Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera**
3. **Captures passwords and account details for various email clients** such as Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail, and Gmail
4. **Enumeration of network resources** and spreads like a worm
5. Intercepts network traffic from the browser to **steal banking details** entered by the user

Banking Trojan + Ransomware

- Banking Trojans are **polymorphic** – evade antivirus detection
- Recovery and restoration can be time-consuming and expensive
  - Complete sanitization involves rebuilding entire network, servers and computers

The Irony of Better Security

The Irony of Better Security

- **Industries responded** to the top cybersecurity risks of the past few years
  - Increase in use of **multi-factor authentication** (MFA)
  - Retire vulnerable operating systems
  - Update and secure **remote access** solutions
- As industry adapts, so do our adversaries
  - More **reconnaissance**
  - Varied attack vectors
  - More **sophistication** in attack methods

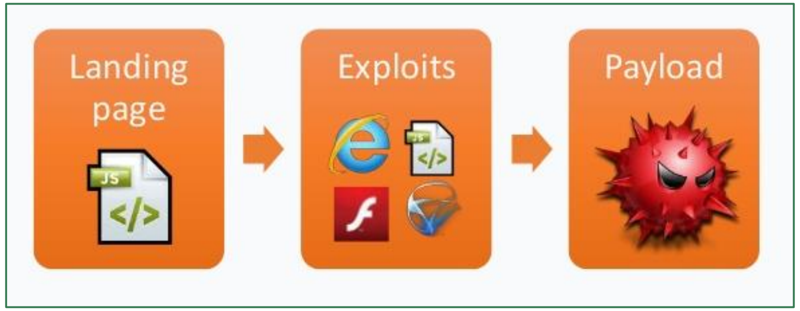
Evolution of Ransomware Intrusion Vectors

2016: Phishing

2017: RDP

2018: Phishing + RDP

2019: Phishing + RDP + Exploit Kits

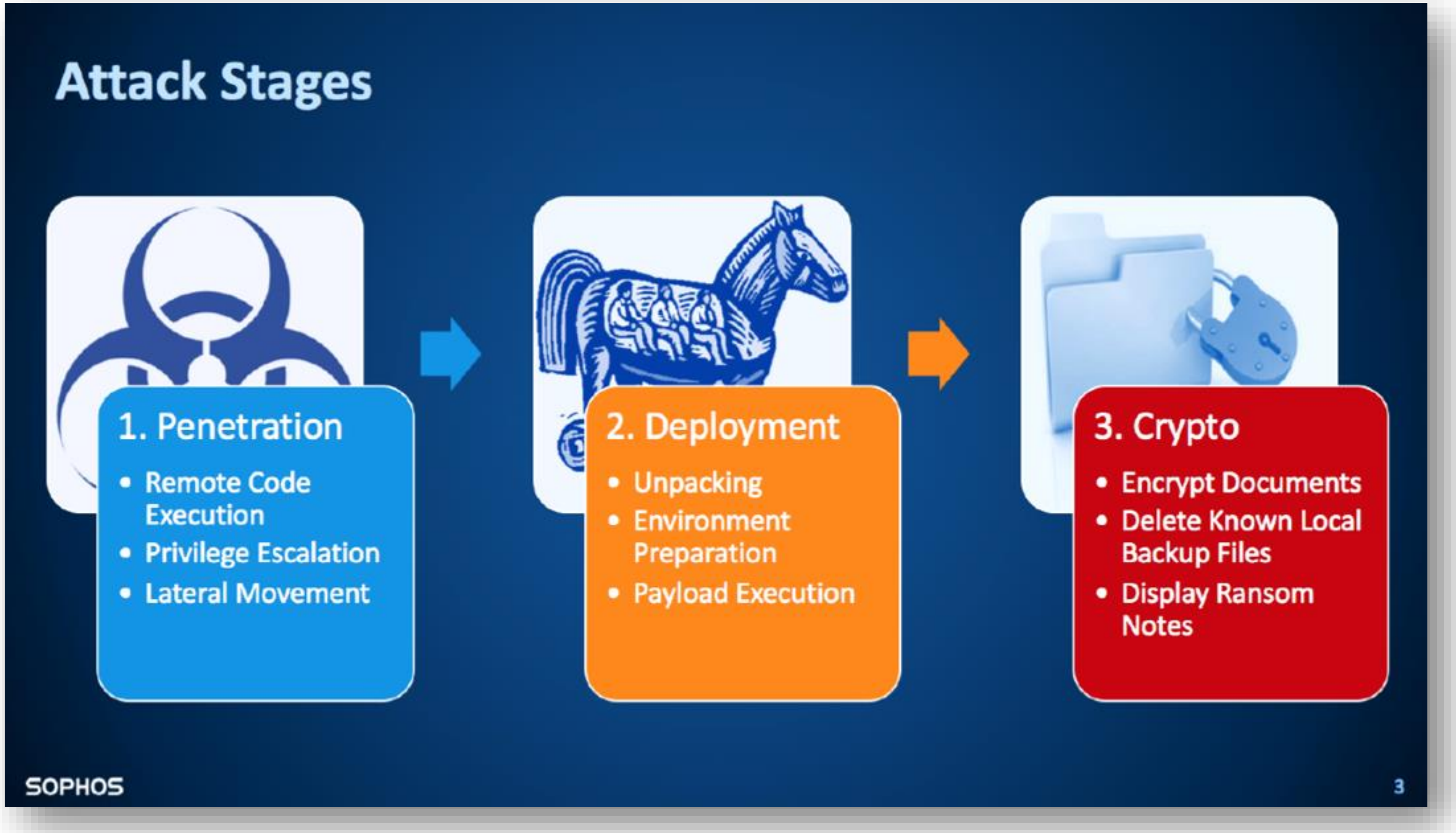


Victimization of MSPs

- Increase in MSP-related ransomware attacks since mid-2018
  1. MSPs reporting compromise of their customers directly
  2. Customers reporting compromise and later discovering it was a result of their MSP being initially compromised

Defending Against Ransomware

Defending Against Ransomware



Attack Stages

1. Penetration

- Remote Code Execution
- Privilege Escalation
- Lateral Movement

2. Deployment

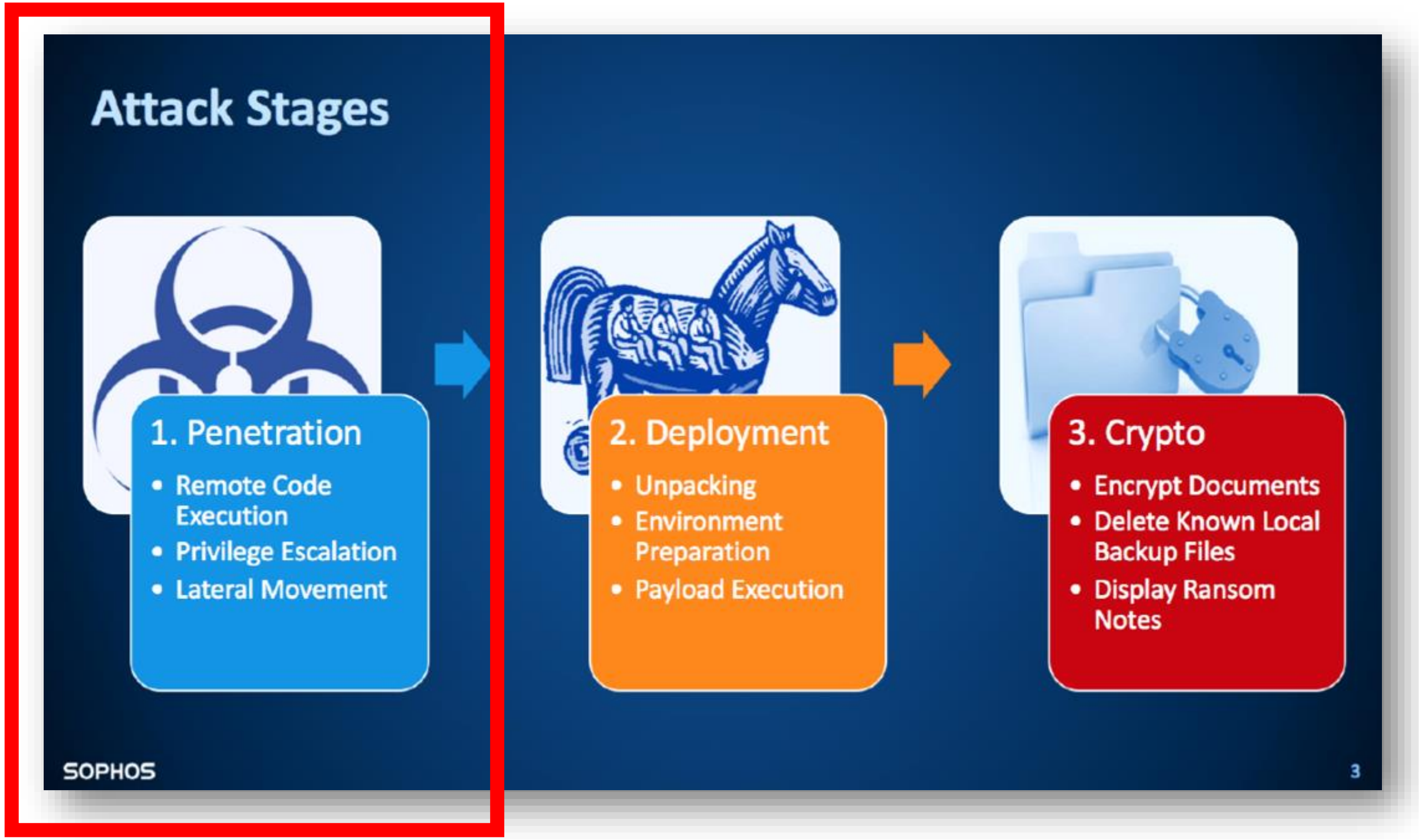
- Unpacking
- Environment Preparation
- Payload Execution

3. Crypto

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

SOPHOS

Defending Against Ransomware



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

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

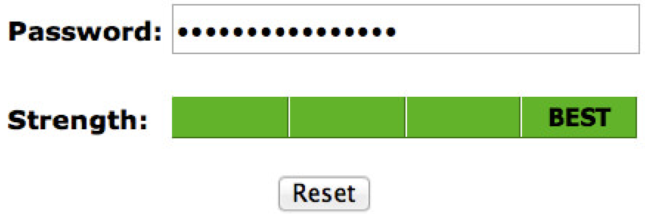
KIVU

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 16 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: ••••••••••••••••

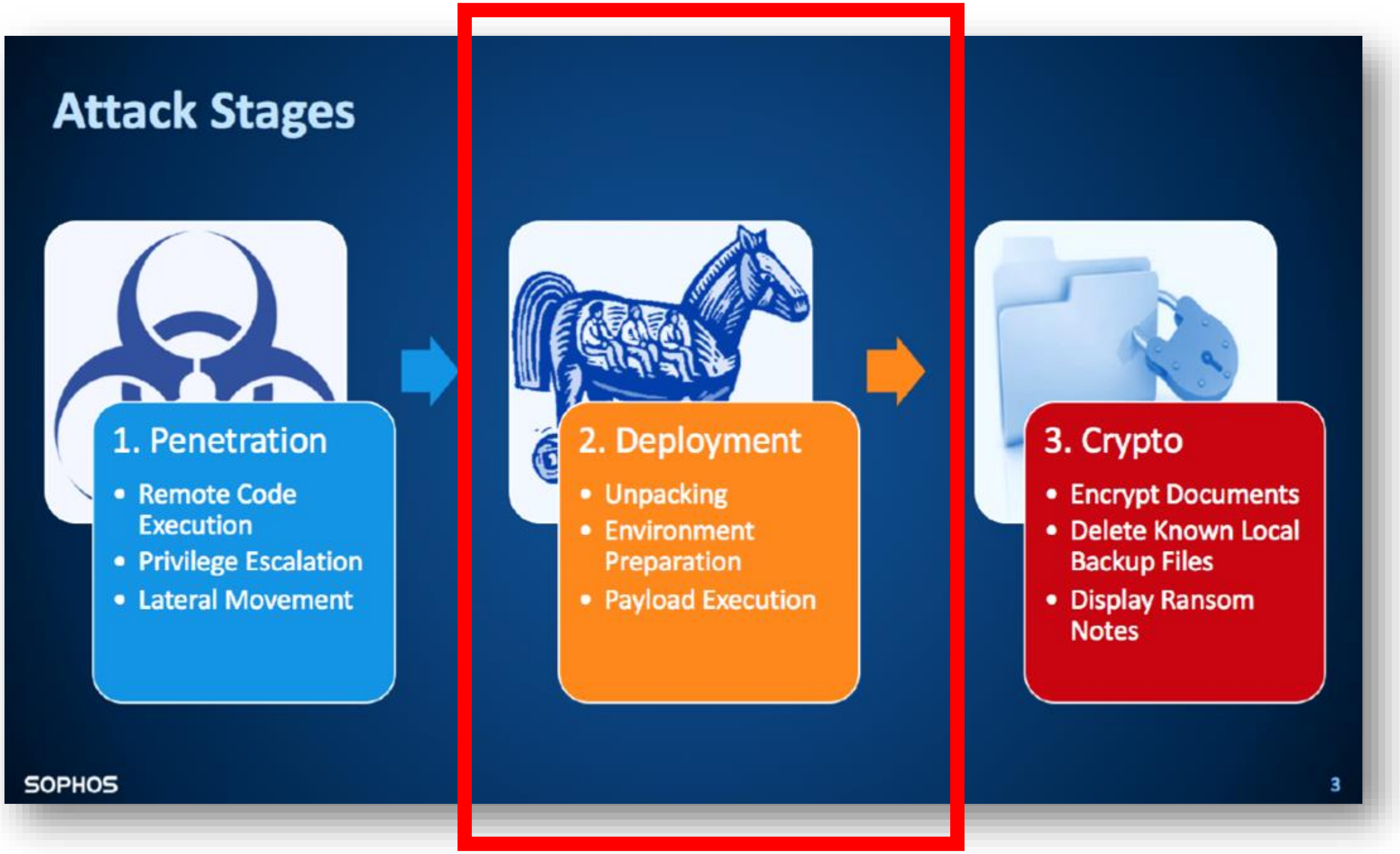
Strength: BEST

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

KIVU

Defending Against Ransomware



Attack Stages

1. Penetration

- Remote Code Execution
- Privilege Escalation
- Lateral Movement

2. Deployment

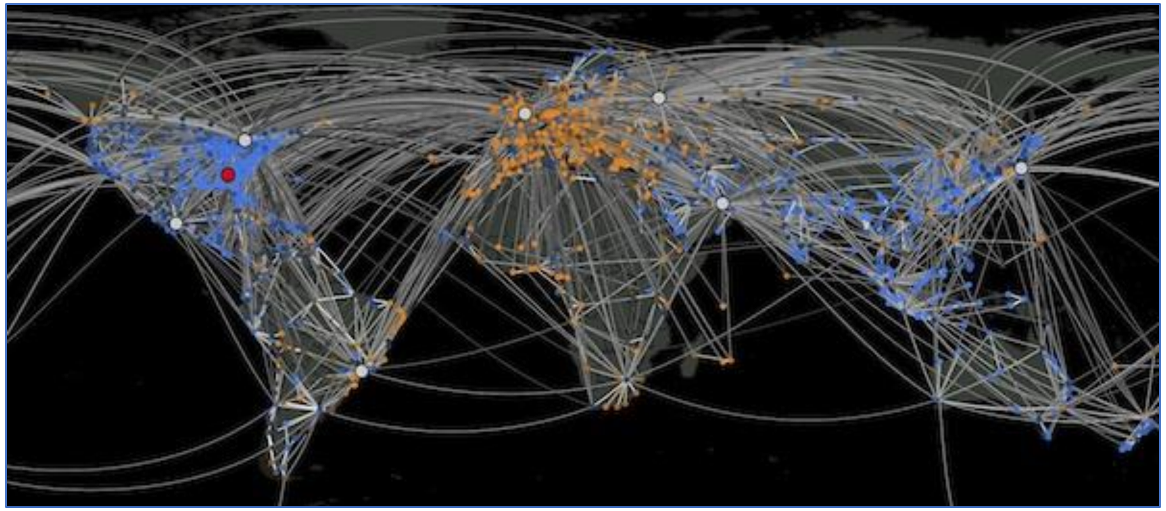
- Unpacking
- Environment Preparation
- Payload Execution

3. Crypto

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

Defending Against Ransomware

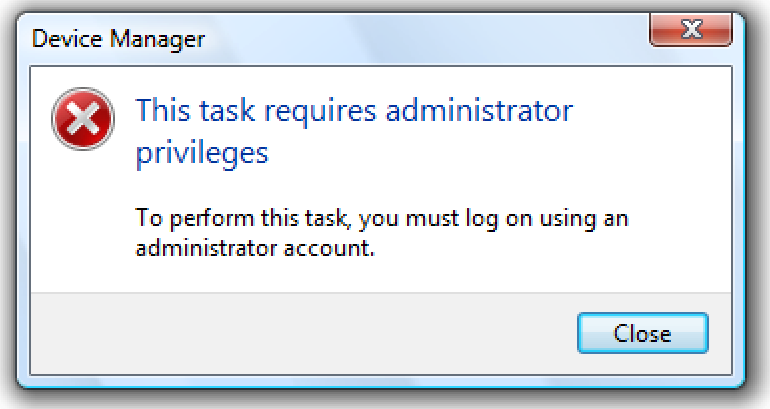
5. **Segregate your networks**
   - Separate your network into smaller, independent networks
   - If a ransomware infection occurs, it will be limited to the isolated network instead of propagating across the entire enterprise



KIVU

Defending Against Ransomware

6. **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

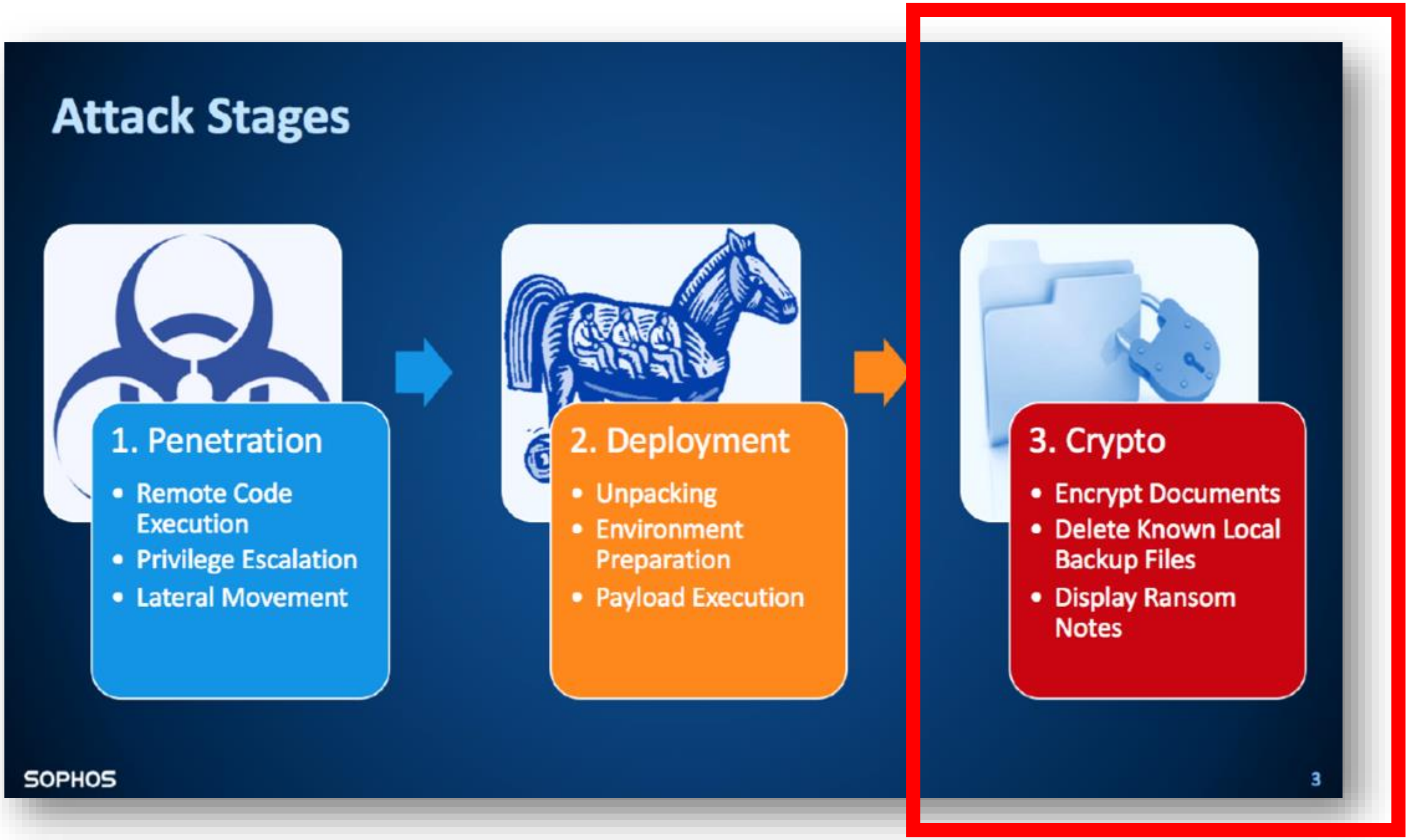


Device Manager

This task requires administrator privileges

To perform this task, you must log on using an administrator account.

Defending Against Ransomware



Attack Stages

1. Penetration

- Remote Code Execution
- Privilege Escalation
- Lateral Movement

2. Deployment

- Unpacking
- Environment Preparation
- Payload Execution

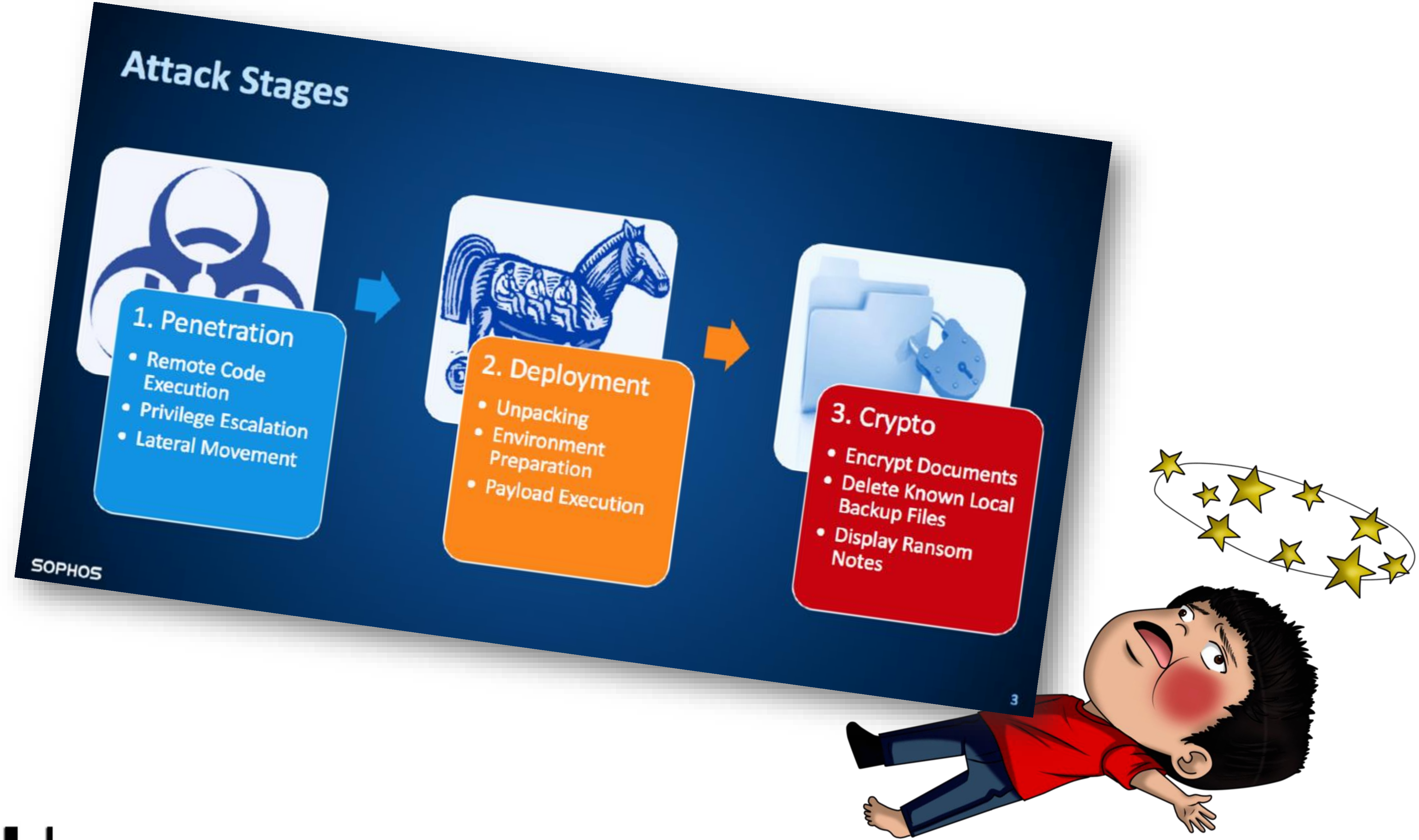
3. Crypto

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

SOPHOS

Defending Against Ransomware

7. **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

Kivu

Questions?