



RANSOMWARE

Battling A Rapidly Changing
And Booming Industry

By : Jaaziel Sam Carlos



Ransomware 101



Ransomware Attacks



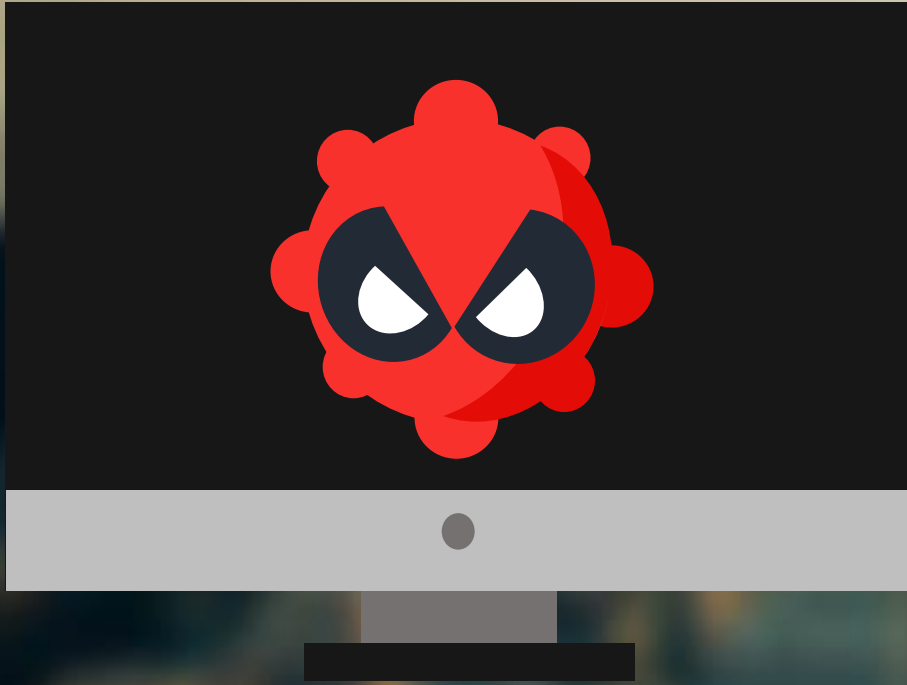
Identifying Ransomware



Solution and Prevention

An aerial photograph of the New York City skyline during the "golden hour" of sunset. The sky is a mix of soft orange, yellow, and pale blue. The city's dense collection of skyscrapers is visible, with the Empire State Building standing out prominently in the center. The Hudson River is visible on the right side of the frame. A solid black horizontal band is superimposed across the lower third of the image, containing the title text.

RANSOMWARE 101



WHAT IS RANSOMWARE?

A type of malware which **limits** or **prevents** users from using a system. It forces its victims to pay **ransom** through certain payment methods. There are at least **110** known Ransomware Family today

OUTSIDE RUSSIA

During 2012, Ransomware variants spread in countries across Europe. Mostly uses Fake Police Notification.

FIRST SIGHTING

The first ransomware was discovered in Russia around 2005. It was detected as PGPCODER

CRYPTOLOCKER

In 2013, CryptoLocker was discovered and the use of military grade encryption and TOR among ransoms wares became common





DAMAGE POTENTIAL HIGH

DISTRIBUTION LOW

UPDATE FREQUENCY HIGH

RANSOMWARE | Ransomware Threat

2014

21

2015

32

2016

60

2014

2015

2016

32

21

60

RANSOMWARE | New Ransomware

FILECRYPTOR

CRYP

CRYP

CRYP



RANSOMWARE | Kinds of Ransomware

ALERT! YOUR COMPUTER HAS BEEN LOCKED

To regain access to your
computer enter the key which
you can have by paying 500\$ in
the following account

LOCKSCREEN



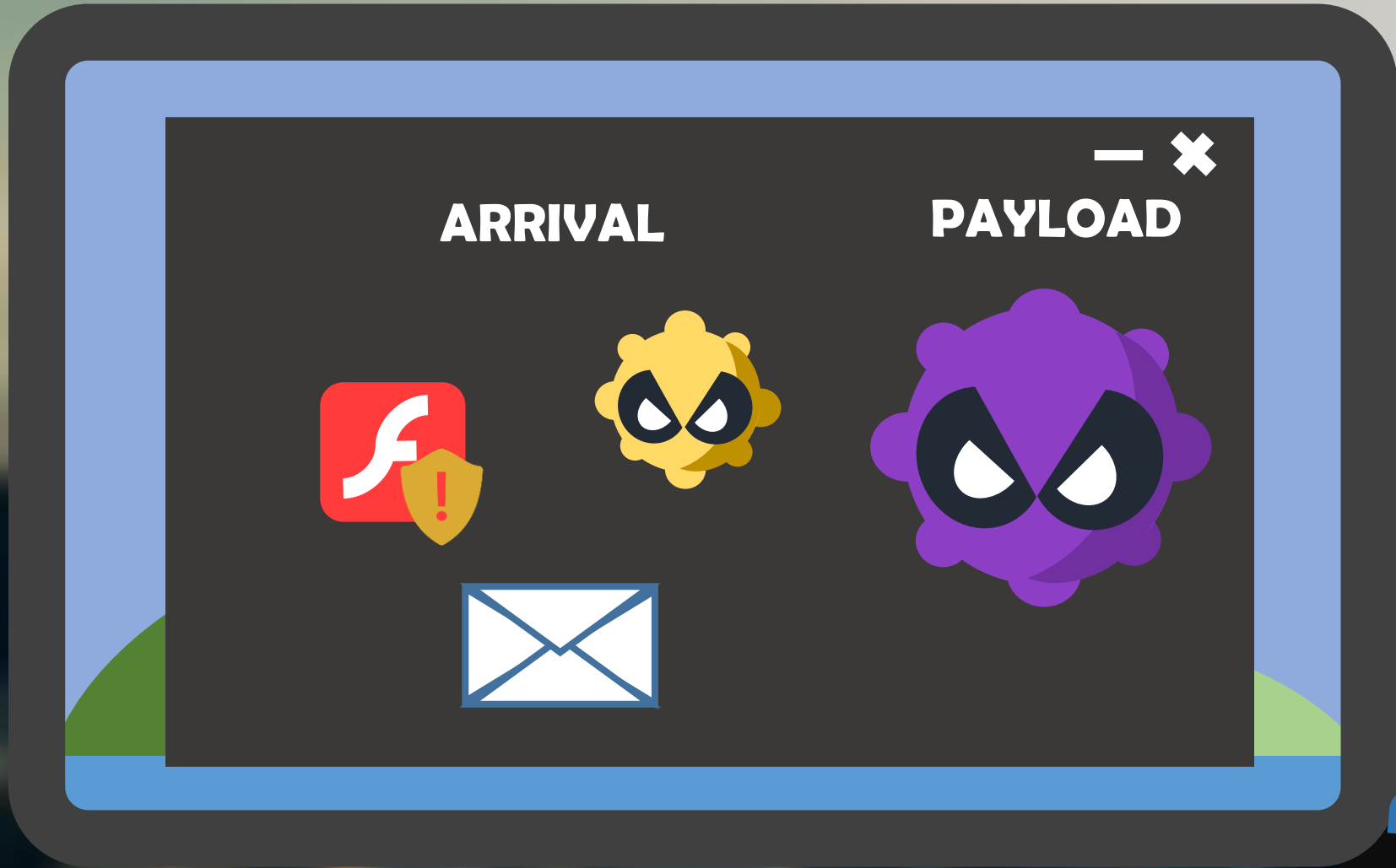
Enter





RANSOMWARE

ATTACKS



RANSOMWARE | Ransomware Attacks

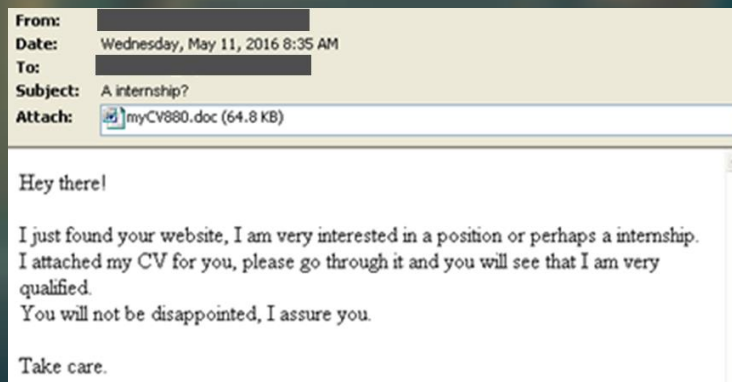
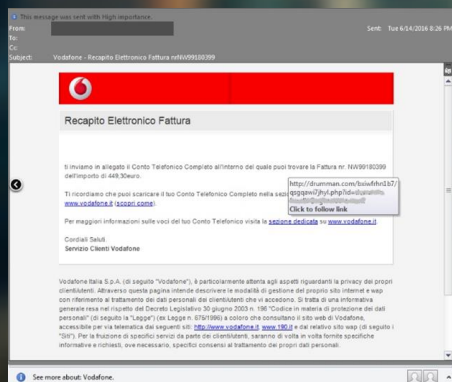


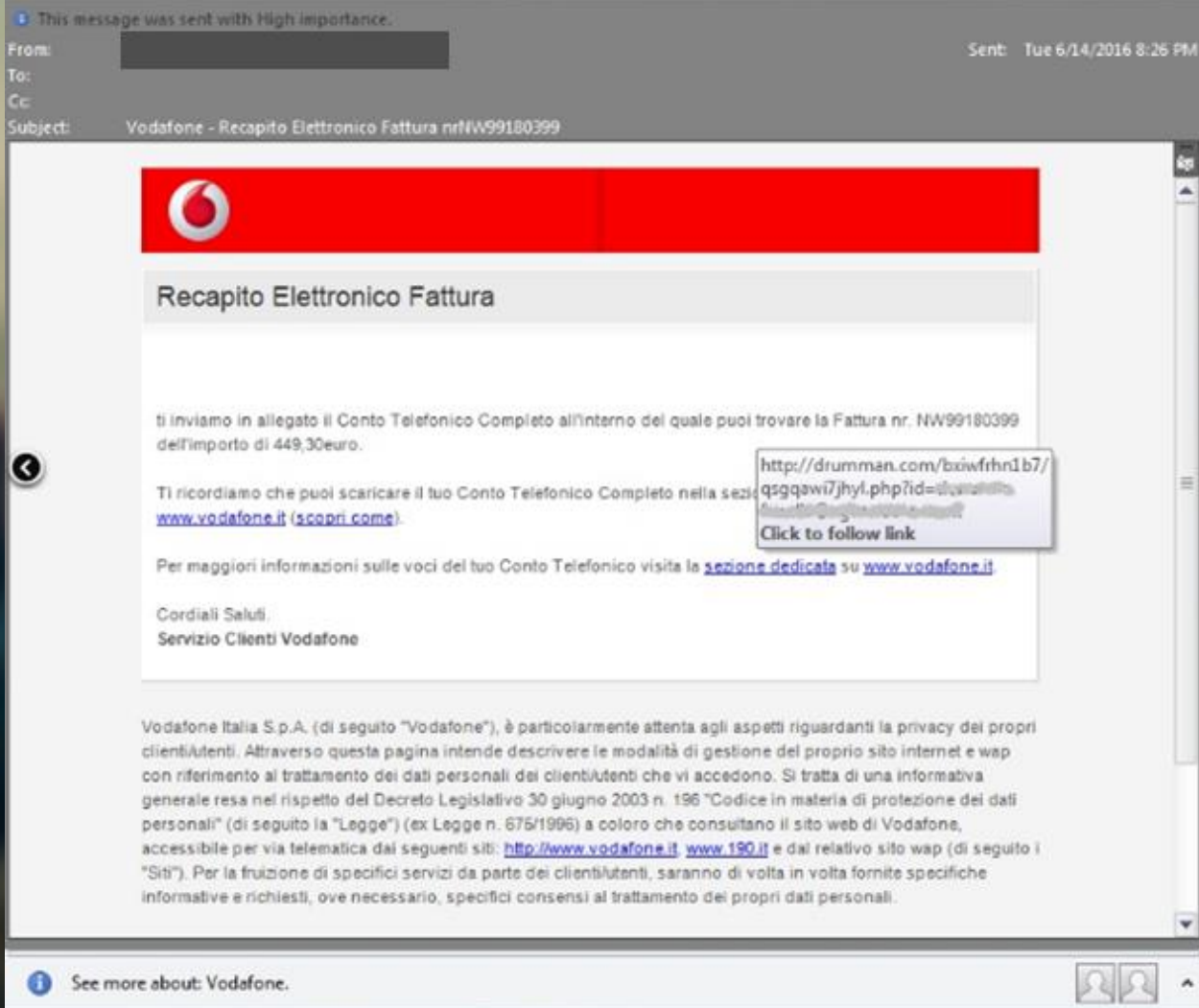
SPAM MAIL



EXPLOIT KITS

RANSOMWARE | Arrival





TYPE 1

A SPAM with a malicious link that redirects to a download site or exploit serve kit

From: [REDACTED]
Date: Wednesday, May 11, 2016 8:35 AM
To: [REDACTED]
Subject: A internship?
Attach:  myCV880.doc (64.8 KB)

Hey there!



I just found your website, I am very interested in a position or perhaps a internship.
I attached my CV for you, please go through it and you will see that I am very qualified.
You will not be disappointed, I assure you.

Take care.

TYPE 2

A SPAM with a malicious document which disguises as a CV

From: [REDACTED] Sent: Thu 11/12/2015 3:36 PM
To:
Cc:
Subject: Cataldi Billing Statement 2243

 Message  Statement.zip (888 B)

Hello Please see enclosed a copy of the billing statement for Nov 2015

Best regards
Sherika Oney

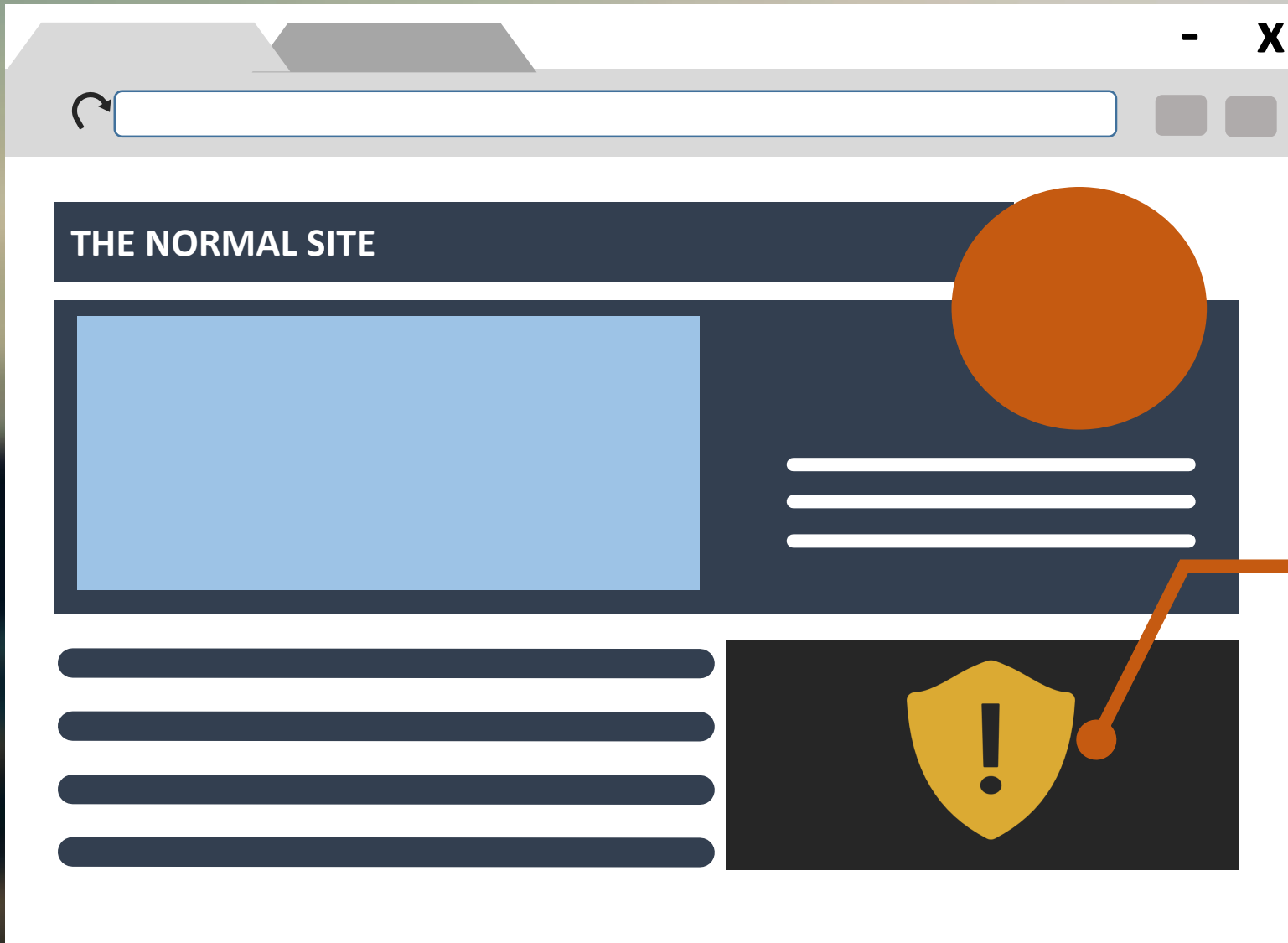
TYPE 3

A SPAM with a malicious script file which downloads the ransomware

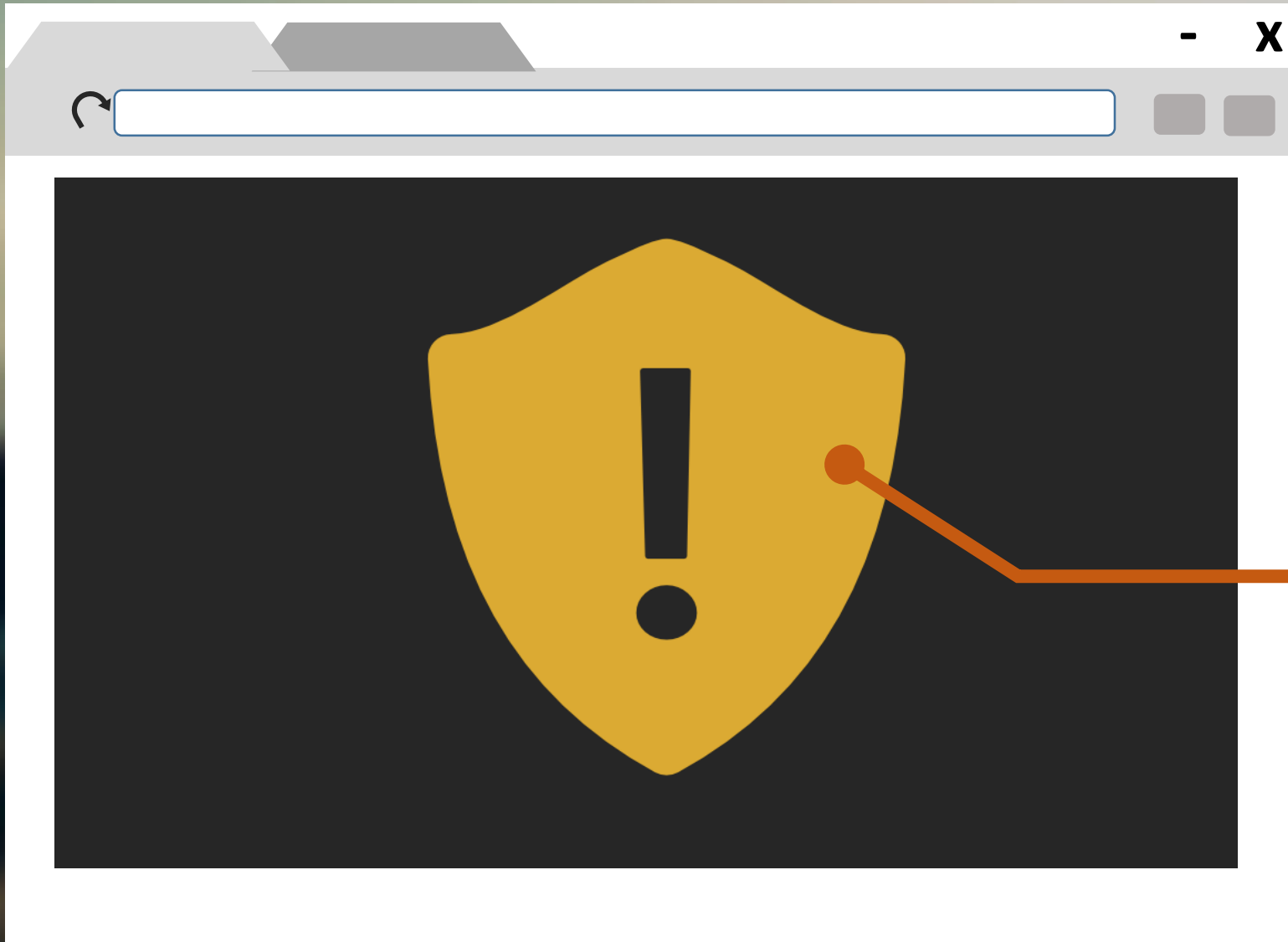


EXPLOIT KITS

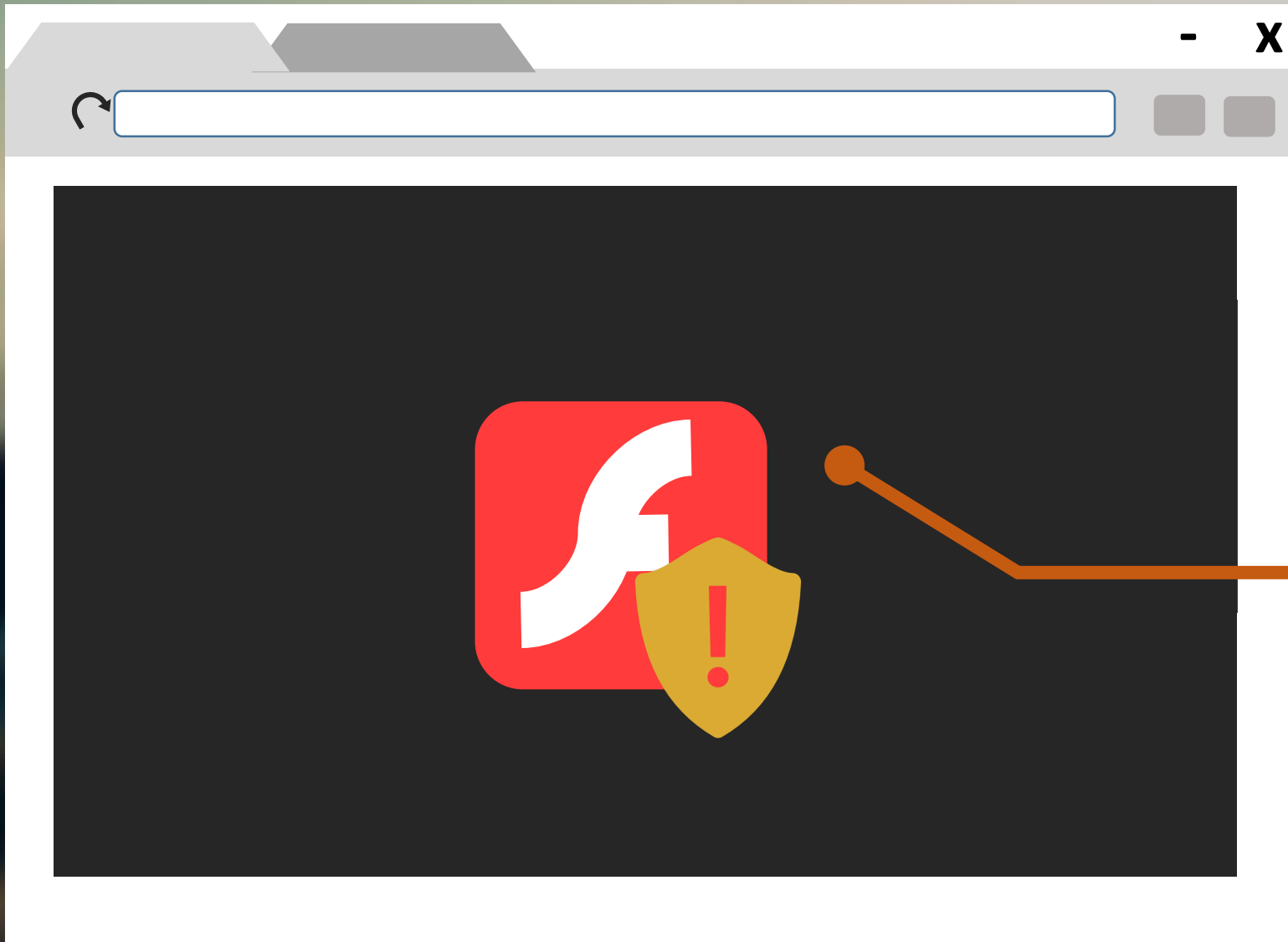
RANSOMWARE | Exploit Kits



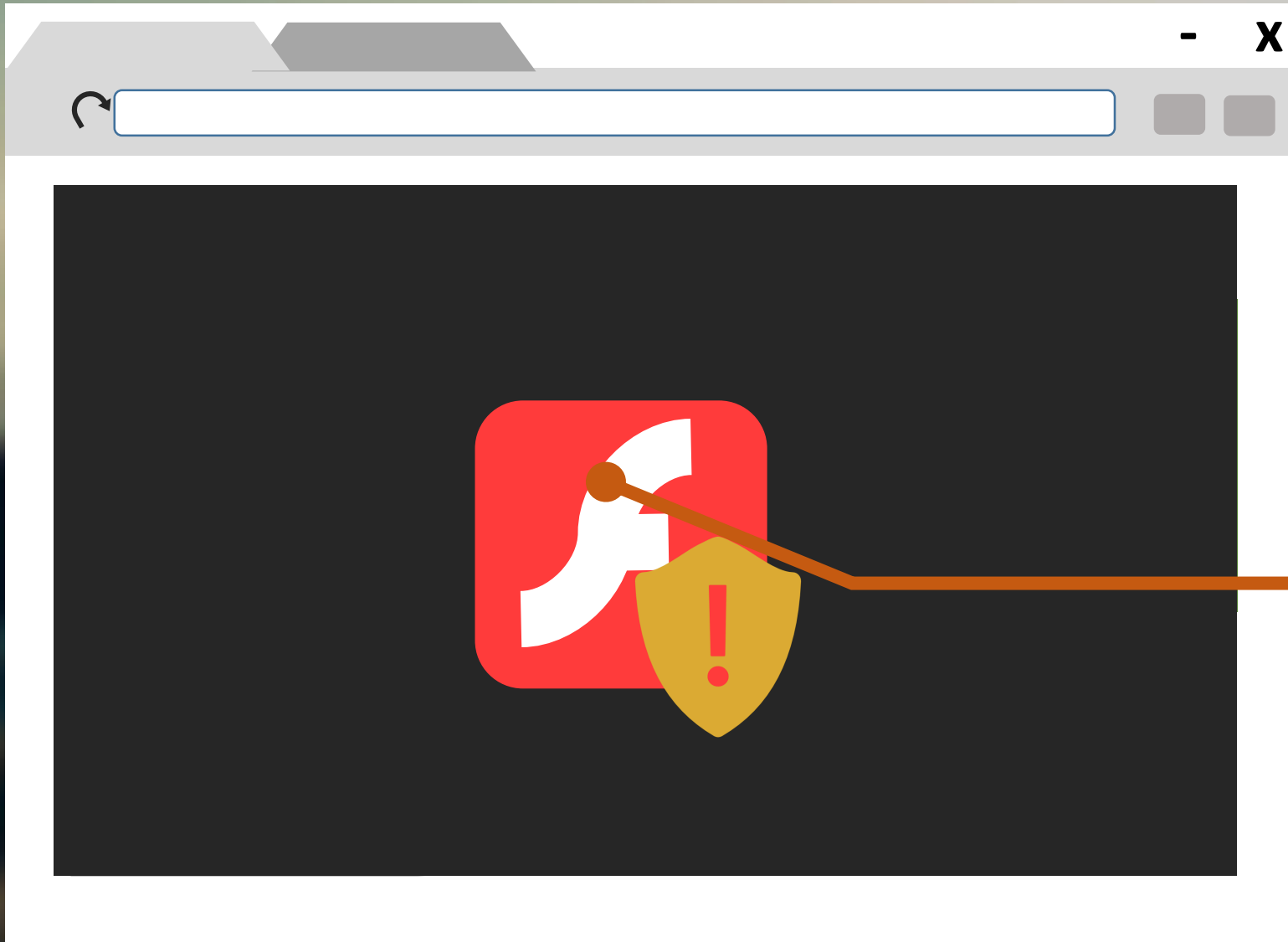
A normal site can redirect to an exploit server kit with the use of “Malvertisement”



The **malvertisement** will redirect the network traffic to an **Exploit Server Kit**



The **Exploit Kit** will be responsible for checking the system for **vulnerability** that will be exploited and using it to download the **Ransomware**

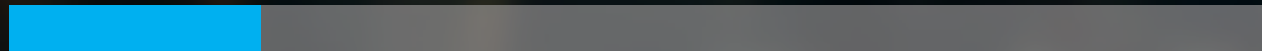


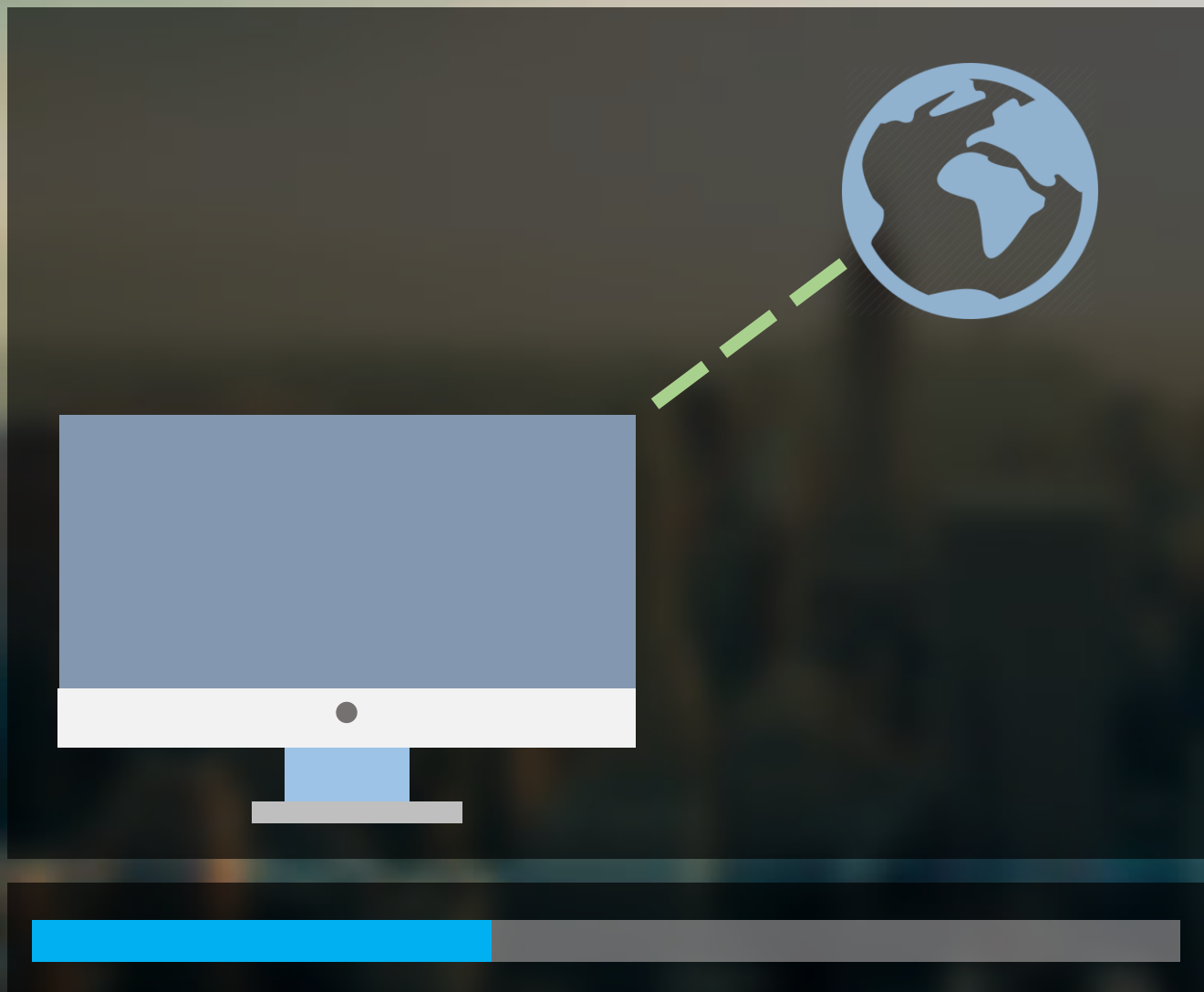
A **Compromised Site** is a site which is **hacked/stolen** by a cybercriminal. This can be used to redirect a user to a **Exploit Server Kit**

Exploits	Delivered Ransomware (2015)	Delivered Ransomware (2016)
Angler Exploit Kit	CryptoWall, TeslaCrypt, CryptoLocker	CryptoWall, TeslaCrypt, CryptoLocker, CryptXXX
Neutrino Exploit Kit	CryptoWall, TeslaCrypt	CryptoWall, TeslaCrypt, Cerber, CryptXXX
Magnitude Exploit Kit	CryptoWall	CryptoWall, Cerber
Rig Exploit Kit	CryptoWall, TeslaCrypt	Ransom_GOOPIC
Nuclear Exploit Kit	CryptoWall, TeslaCrypt, CTB-Locker, Troldesh	TeslaCrypt, Locky
Sundown Exploit Kit		CryptoShocker
Hunter Exploit Kit		Locky
Fiesta Exploit Kit	TeslaCrypt	

ARRIVAL

Ransomware is downloaded or dropped onto the system.



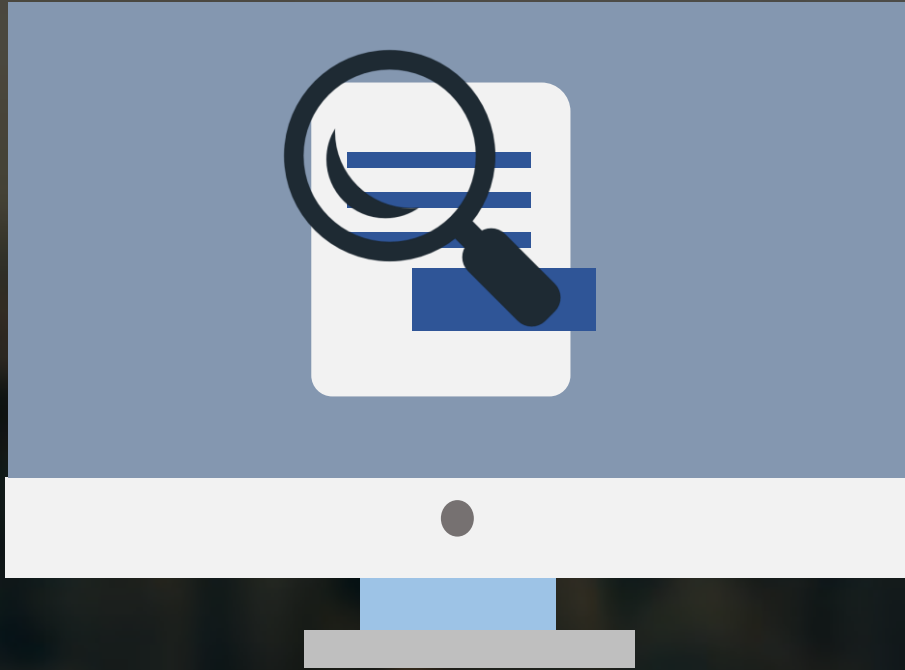


CONTACT

The Ransomware will connect the C&C to receive a Key and send victim information

SEARCH

The ransomware will now start searching the system for target file types and directories



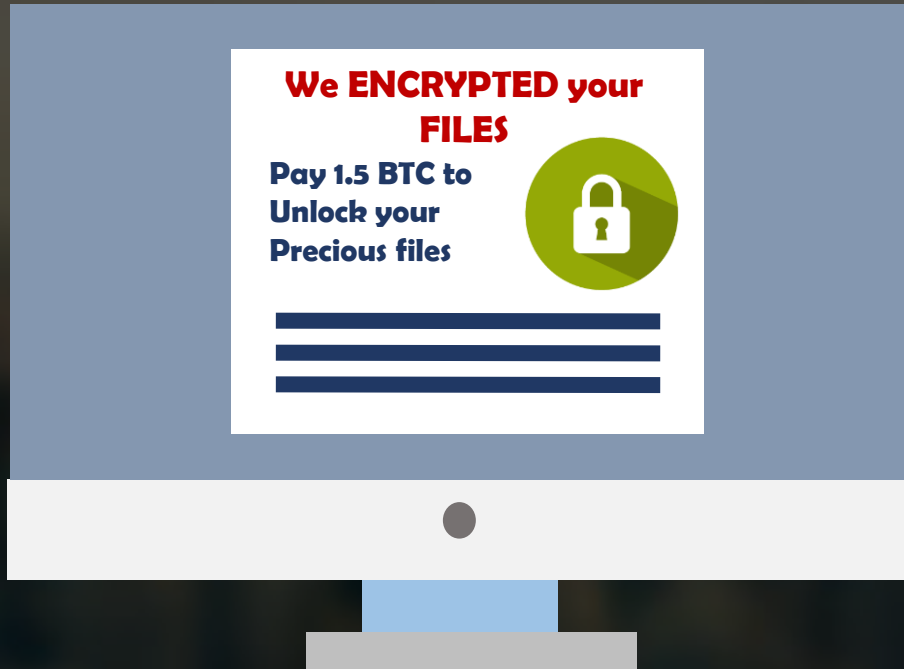
ENCRYPT

Once the ransomware finds a target it will encrypt the said files



RANSOM

The ransomware will now display a ransomnote that instructs the victim on how to pay the ransom



WHAT IS ITS IMPACT TO THE VICTIMS?

ALERT! YOUR FILES ARE NOW ENCRYPTED

To regain access to your
computer enter the key which
you can have by paying 500\$ in
the following account



Enter

Permanent or
temporary lost of
important files



RANSOMWARE | Impact of Ransomware Infection

Financial loss
when paying the
ransom



RANSOMWARE | Impact of Ransomware Infection



Average payed ransom by victim

\$30M every **100 days** collected by CryptoLocker threat actors



A Hospital from L.A. payed a ransom amounting to **17,000\$**



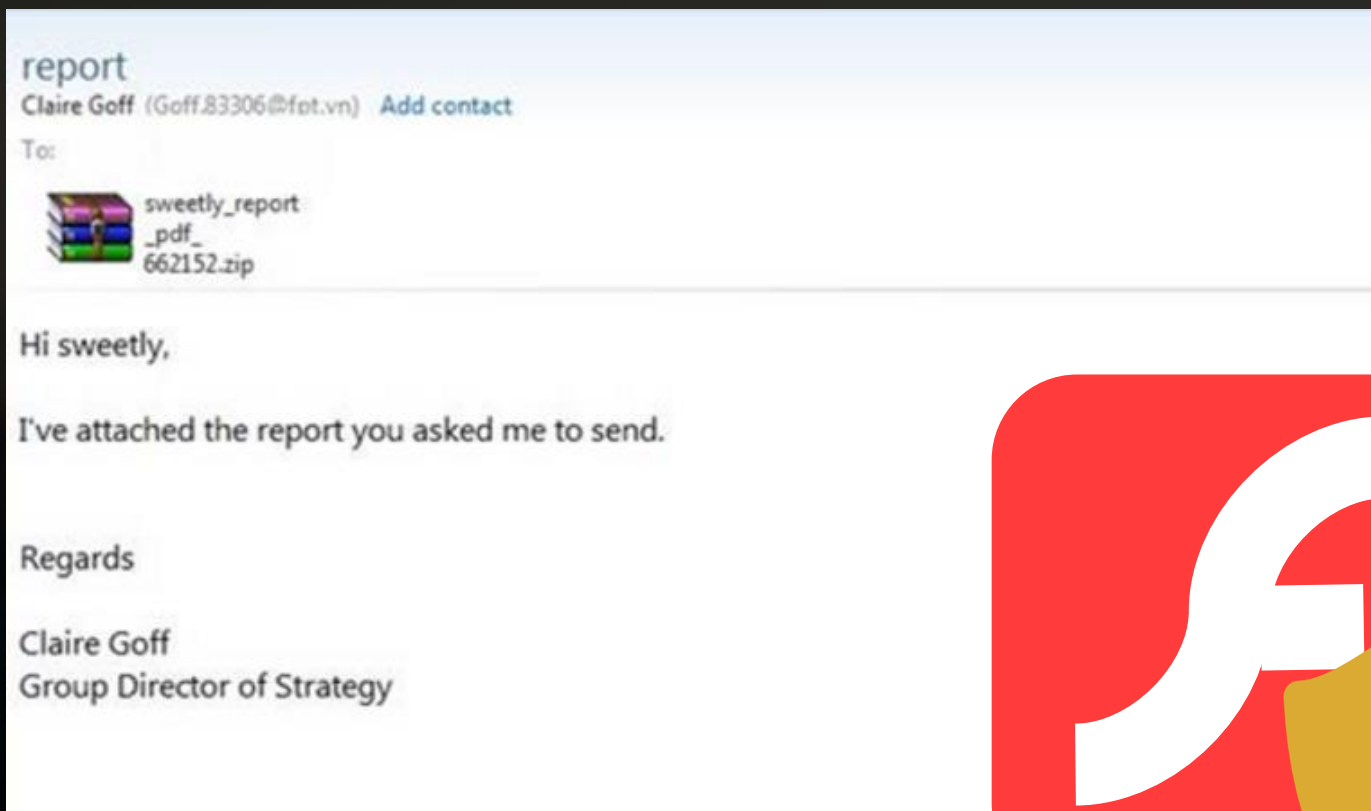
IDENTIFYING

RANSOMWARE

RANSOMWARE | Identifying Ransomware



LOCKY

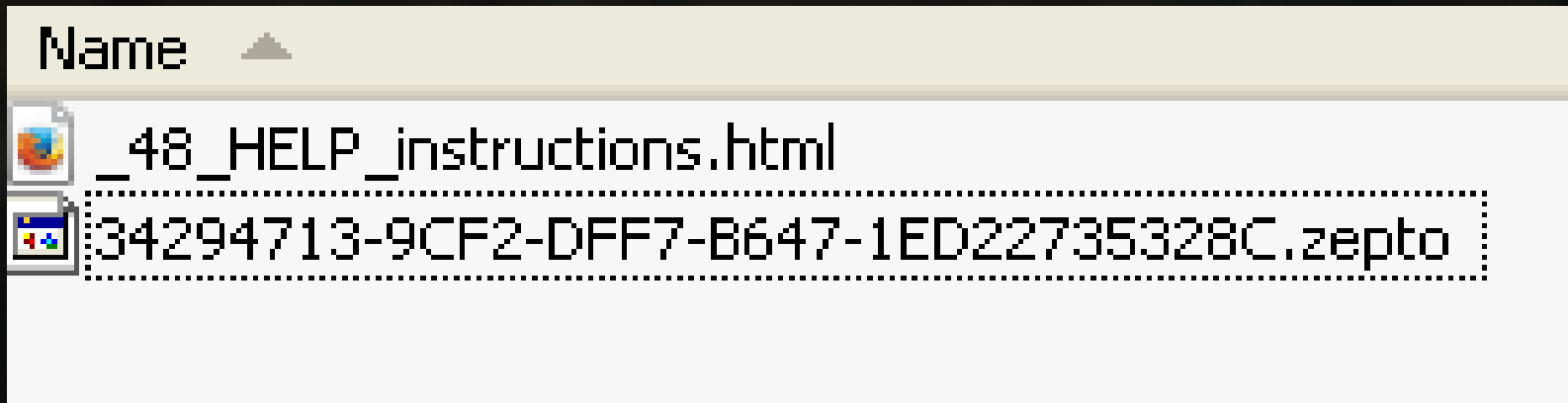


LOCKY's
arrival vector
is either
through SPAM
mail or
through
Nuclear
Exploit Kit

```
set registry value      key: HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Setting
set registry value      key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell F
set registry value      key: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell F
set registry value      key: HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache value:
new process              "C:\DOCUME~1\DYITUS~1\LOCALS~1\Temp\1837aWEGHS2.exe" 321
```

LOCKY needs an **argument** to run properly

Encrypts the file name and
adds “.locky” or “.zepto”



!!! IMPORTANT INFORMATION !!!

$$\begin{array}{l} \$_{-}++ \\ |_{-}^{*}\$ \\ - =^{*}.\$. \$ \\ | \$_{-} - = \end{array}$$



CryptProjectXXX

RANSOMWARE | CryptXXX



CrypXXX_sample.dll
Application Extension
373 KB



explorer.exe
Run a DLL as an App
Microsoft Corporation

Latest variants **lock the screen** after encrypting the files on the system

Copies legitimate **rundll32.exe** to its **current folder** use it to load the malware (some variants rename the rundll32)

NOT YOUR LANGUAGE? USE <https://translate.google.com>

What happened to your files ?

All of your files were protected by a strong encryption with RSA4096

More information about the encryption keys using RSA4096 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

How did this happen ?

!!! Specially for your PC was generated personal RSA4096 Key , both public and private.

!!! ALL YOUR FILES were encrypted with the public key , which has been transferred to your computer via the Internet.

!!! Decrypting of your files is only possible with the help of the private key and decrypt program , which is on our Secret Server

What do I do ?

So , there are two ways you can choose: wait for a miracle and get your money doubled, or start obtaining BITCOIN NOW! , and restore your data easy way

If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment

Your personal ID: **7011C7D82F91**

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

- 1 - <http://hn5fbbc4pyz77xfa.onion.to>
- 2 - <http://hn5fbbc4pyz77xfa.onion.cab>
- 3 - <http://hn5fbbc4pyz77xfa.onion.city>

If for some reasons the addresses are not available, follow these steps:

- 1 - Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
- 2 - After a successful installation, run the browser
- 3 - Type in the address bar - <http://hn5fbbc4pyz77xfa.onion>
- 4 - Follow the instructions on the site

Be sure to copy your personal ID and the instruction link to your notepad not to lose them.

Version	File Extension	Loader	Note Filename(s)
1	.crypt	none	de_crypt_readme
2	.crypt	use of svchost.exe	{unique ID}
3	.crypt	use of svchost.exe	!Recovery_{ID} {unique ID}
3	.cryp1	use of rundll32.exe	!{unique ID}
3.2	.crypz	use of explorer.exe	!{unique ID}
3.205	.[Random]	use of rundll32.exe	@{unique ID}



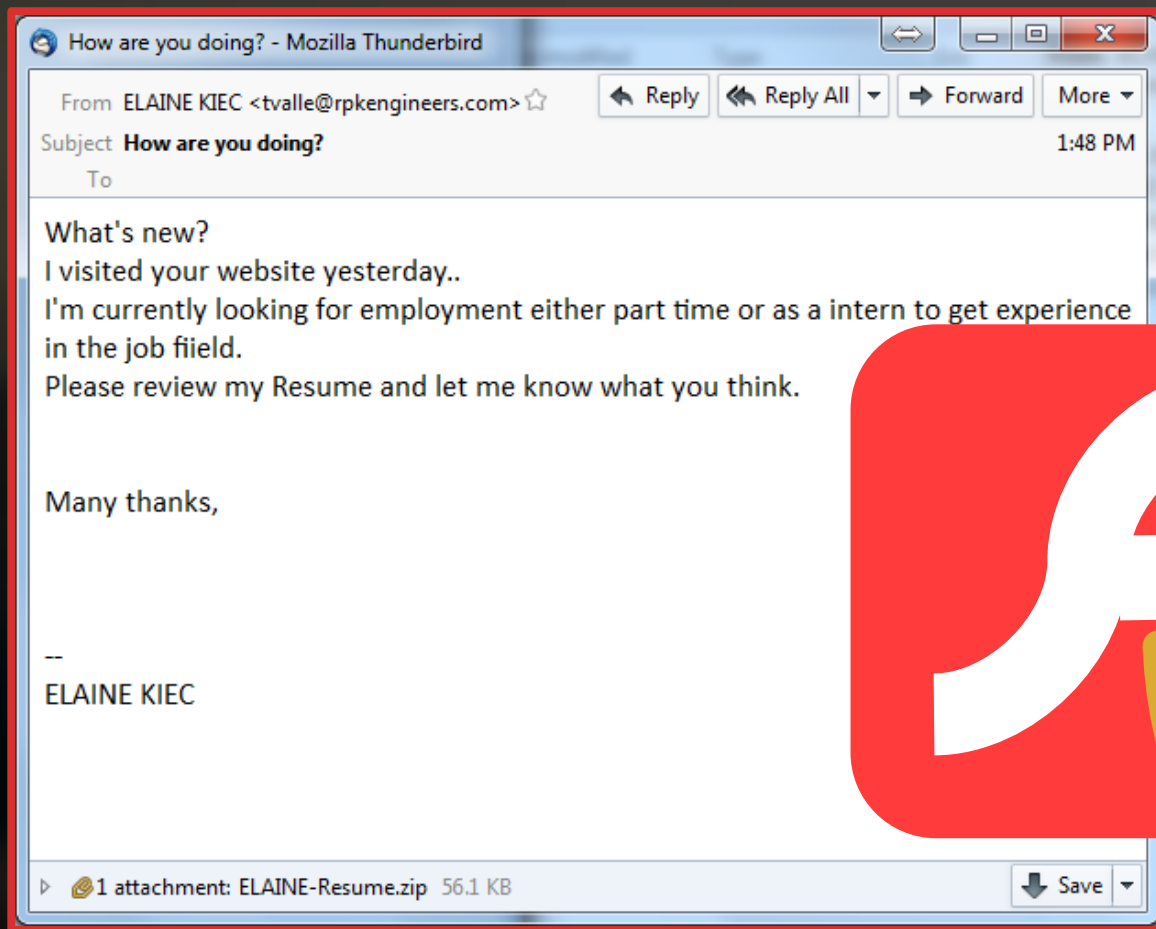
Petya is a type of lockscreen.
And is able to encrypt, not
the files, but the Master File
Table














Cerber

RANSOMWARE | Cerber



CERBER's
arrival vector
is either
through SPAM
mail or
through
Neutrino
Exploit Kit

 # DECRYPT MY FILES #	1 KB
 # DECRYPT MY FILES #.html	13 KB
 # DECRYPT MY FILES #.txt	11 KB
 # DECRYPT MY FILES #.vbs	1 KB
 __init__.py	0 KB
 h1N8hyQ_jE.cerber	1 KB
 iWN3mY5A5w.cerber	2 KB
 JkK'WH_usUa.cerber	1 KB
 TAtK-OvIPy.cerber	1 KB

Encrypts the
file name and
adds
“.cerber” also
drops a
speaking
ransomnote

C E R B E R R A N S O M W A R E

#####

Cannot you find the files you need?
Is the content of the files that you looked for not readable?

It is normal because the files' names, as well as the data in your files
have been encrypted.

Great!!!
You have turned to be a part of a big community #CerberRansomware.

#####

!!! If you are reading this message it means the software
!!! "Cerber Ransomware" has been removed from your computer.

#####

Opens a
ransomnote
containing
the name of
the
ransomware
“CERBER”

RANSOMWARE IDENTIFICATION TOOLS





SOLUTION AND

PREVENTION

RANSOMWARE | Solution and Prevention

FREE DECRYPTION TOOLS

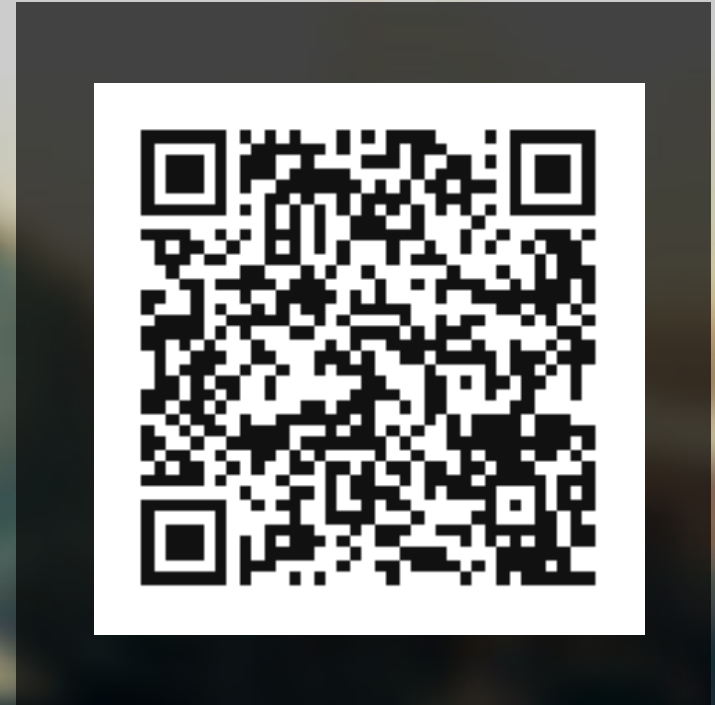


RANSOMWARE INFO



Ransomware Overview

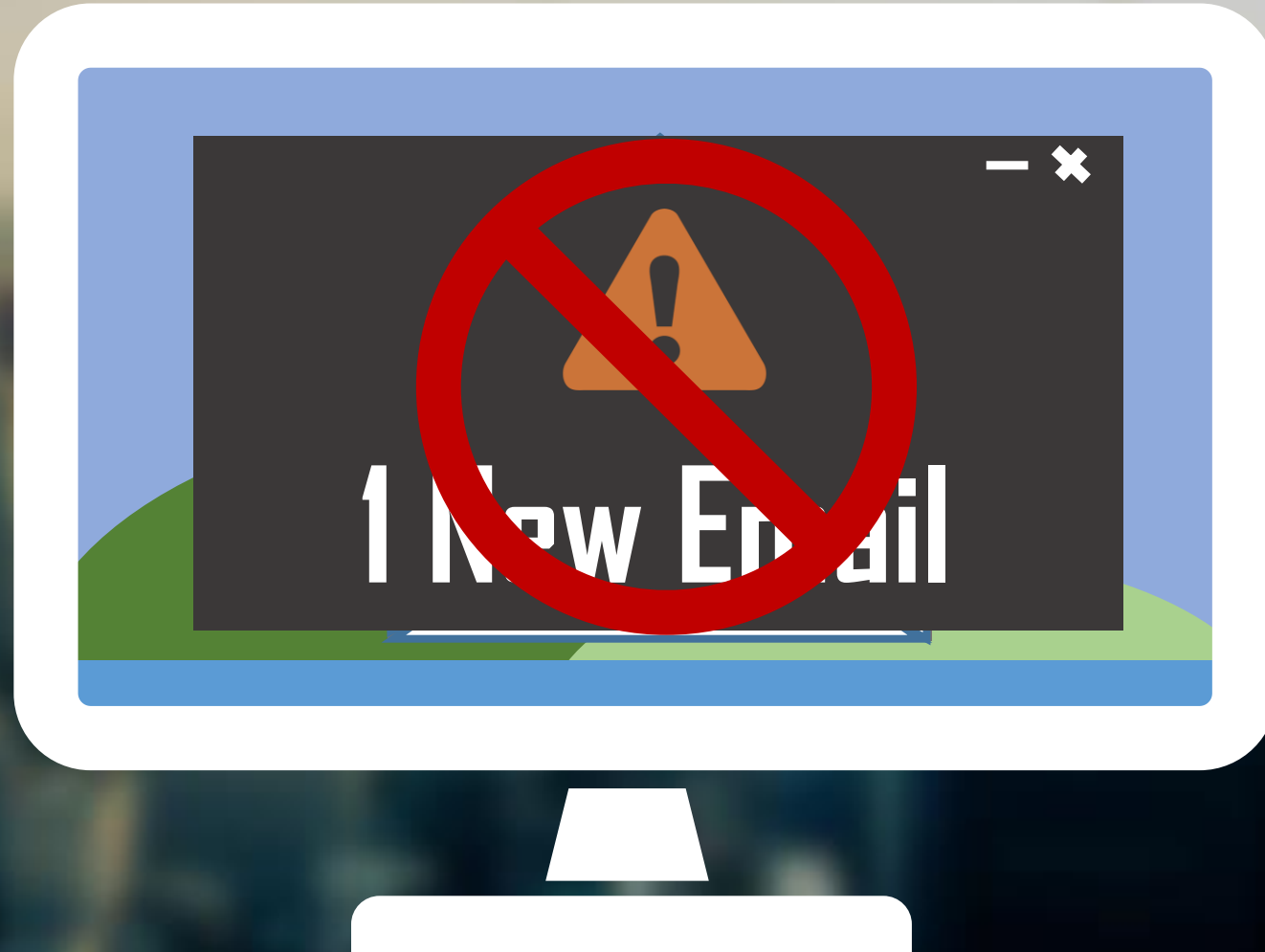
Ransomware Overview							
Ransomware Unidentified Detection Prevention Infographics Download Sources and Contributors							
Name	Extensions	Extension Pattern	Ransom Note Filename(s)	Comment	Encryption Algorithm	Also known as	Decryptor
.CryptoHasYou.	.enc		YOUR_FILES_ARE_LOCKED.txt		AES(256)		
777	.777	._[timestamp]_[email]\$.777 e.g. ._14-05-2016-11-59-36_	read_this_file.txt		XOR	Sevleg	https://decrypter.emsis
7ev3n	.R4A .R5A		FILES_BACK.txt			7ev3n-HONE\$T	https://github.com/has
7h9r	.7h9r		README_.TXT				
8lock8	.8lock8		READ_IT.txt	Based on HiddenTear	AES (256)		http://www.bleepingco
Alpha Ransomware	.encrypt		Read Me (How Decrypt) !!!!!.txt		AES(256)	AlphaLocker	http://download.bleepi
Apocalypse	.encrypted		How_To_Decrypt.txt	decryption@service@mail.ru			https://decrypter.emsis
AutoLocky	.locky		info.txt info.html				https://decrypter.emsis
BadBlock			Help Decrypt.html				https://decrypter.emsis
Bandarchor		.id-[ID]_[EMAIL_ADDRESS]		Files might be partially encrypted	AES(256)	Rakhni	
BitCryptor	.clf			Has a GUI. CryptoGraphic Locker family. Newer CoinVault variant.			https://noransom.kasp
BlackShades Crypter	.Silent		Hacked_Read_me_to_decrypt_files.html YourID.txt		AES (256)	SilentShade	
Blocatto	.blocatto			Based on HiddenTear	AES (256)		http://www.bleepingco
Booyah				EXE was replaced to neutralize threat		Salam!	
Brazilian	.lock		MENSAGEM.txt	Based on EDA2	AES(256)		
BrLock					AES		
Browlock				no local encryption, browser only			
Bucbi				no file name change, no extension	GOST		
BuyUnLockCode		(*) encoded (IA-Z0-9I(9))	BUYUNLOCKCODE.txt	Does not delete Shadow			



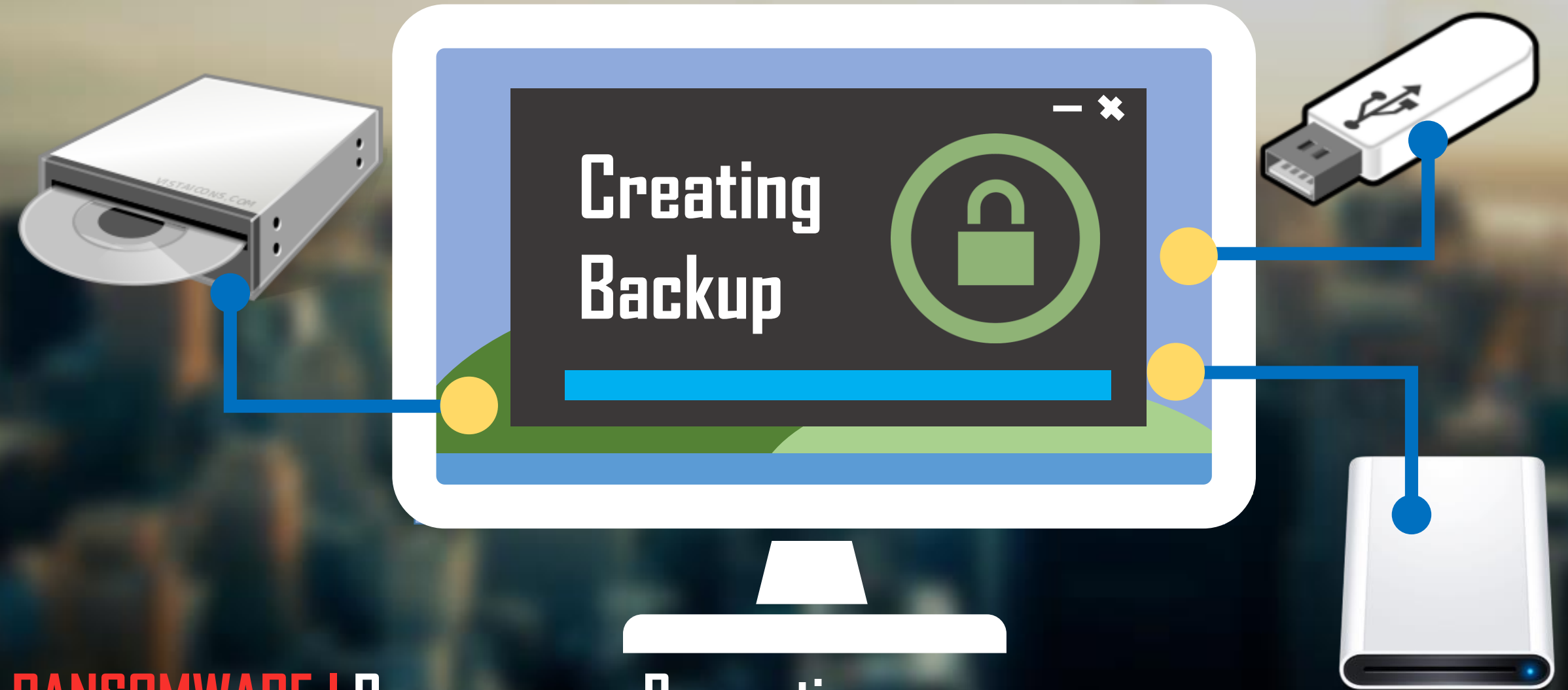
<https://docs.google.com/spreadsheets/d/1TWS238xaccAto-fLKh1n5uTsdijWdCEsGIM0Y0Hvmc5g/pubhtml#>

RANSOMWARE | Ransomware Overview Public Document

Never open unverified email

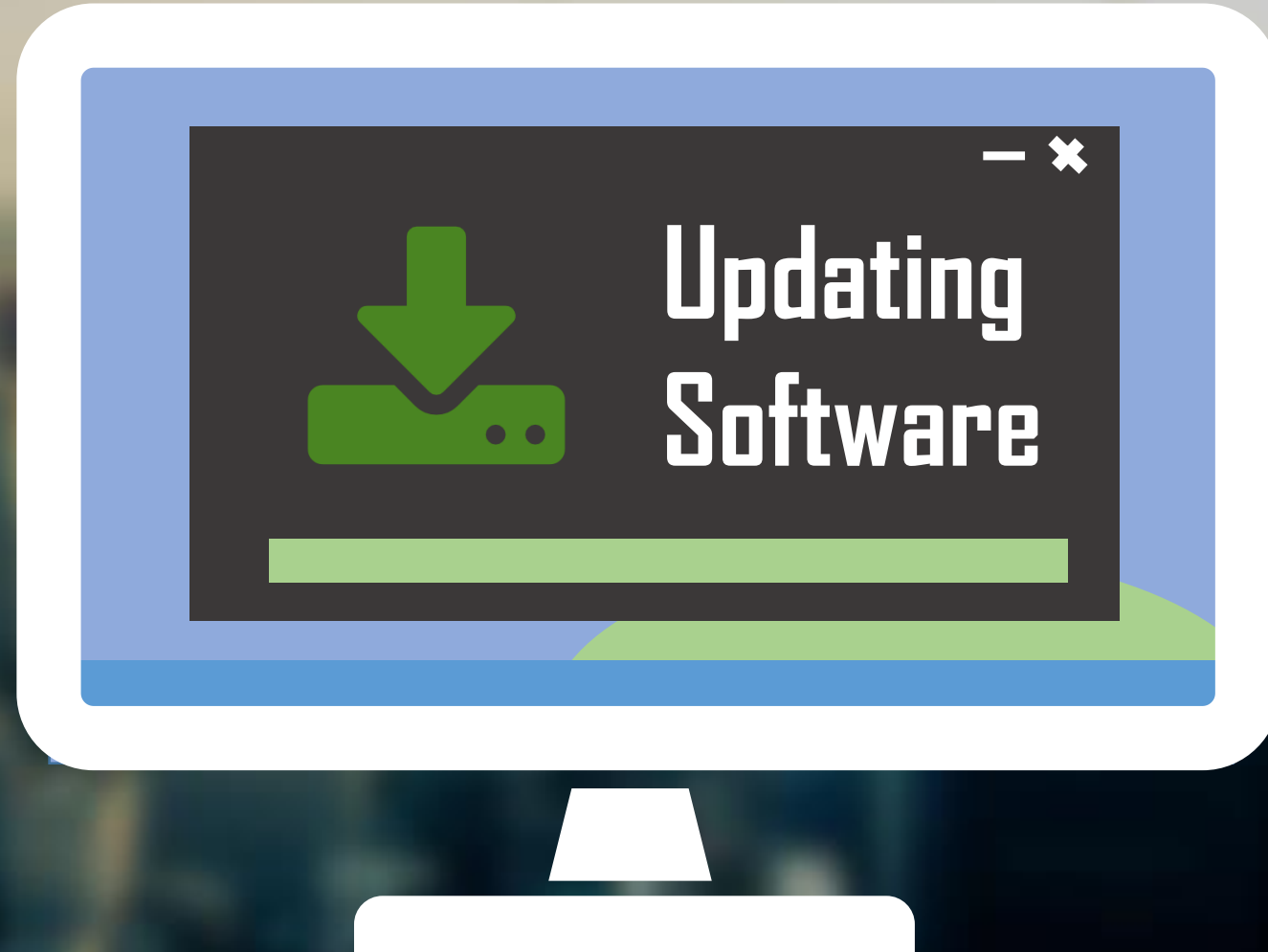


Follow the 3-2-1 Rule

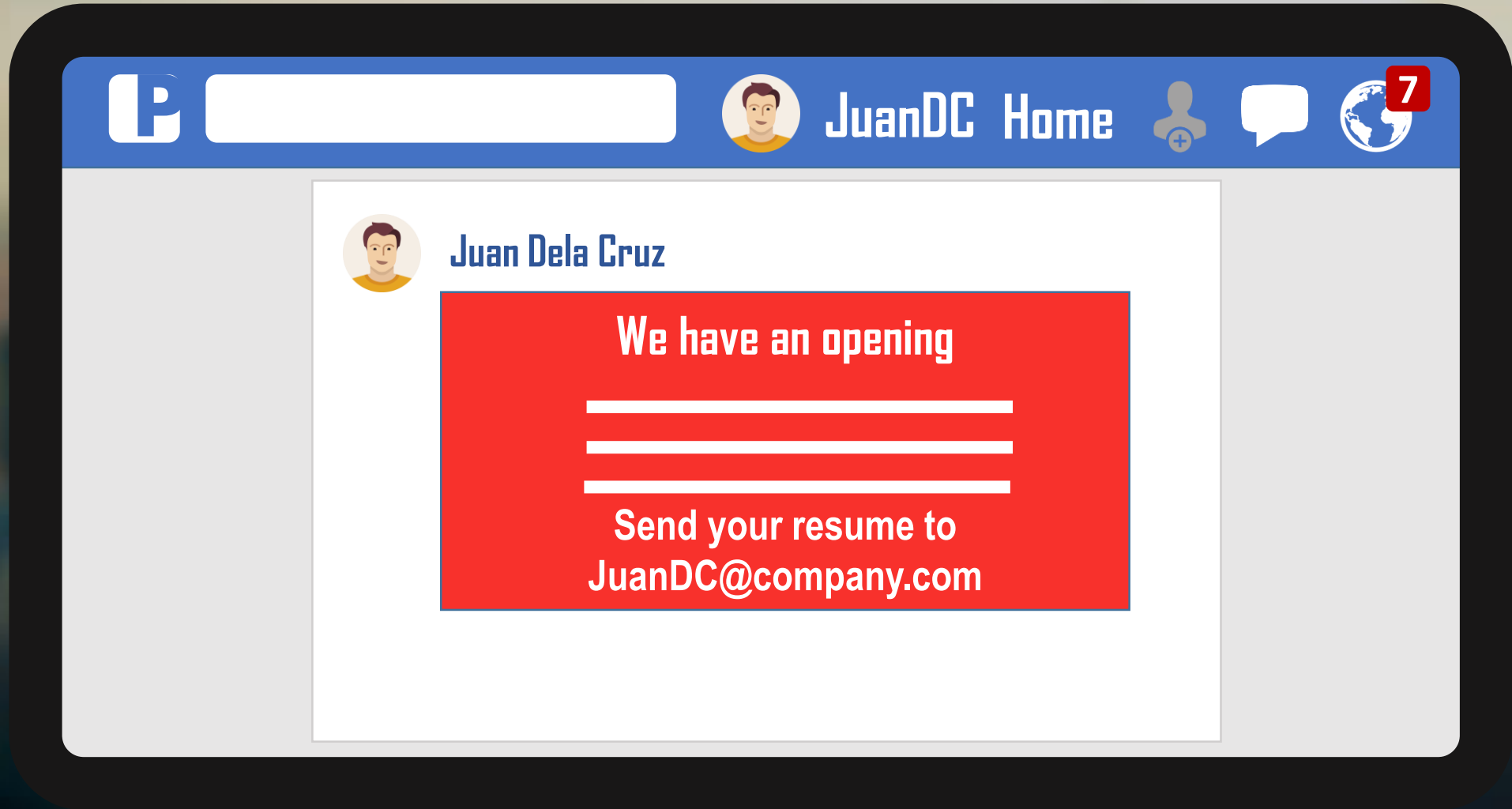


RANSOMWARE | Ransomware Prevention

Update OS & Applications Regularly



Avoid posting your company email online



Q & A



Ransomware



Threat Actor



THANK YOU