



Crypto Ransomware The Who, What, Why and How

Tyler Moffitt | Senior Threat Research Analyst



Agenda

- **Threat Brief**
 - Insights from Collective Threat Intelligence
 - Android Trends
- **Attack Vectors**
 - Phishing
 - Angler/Neutrino Exploit Kit
- **New Encrypting Ransomware Variants**
 - CryptoMix, Cerber, Chimera, CryptXXX
 - Ransomware Rivalry
- **A Quick Guide to Stopping Ransomware**
 - Five easy-to-follow tips
- Q&A



Insights from Collective Threat Intelligence

So far, Webroot has:



Encountered
millions of instances
of malware
and PUAs



Monitored billions
of IP addresses
and URLs



Analyzed millions of
new/updated mobile
apps for malicious
behavior



Studied major
malware trends
based on millions
of endpoints

Threat Intelligence by the Numbers

BrightCloud® services continuously classify and score 95% of the internet, and monitor the entire IPv4 space and in-use IPv6



9+ Billion

File Behavior
Records



27+ Million

Mobile
Apps



10+ Million

Connected
Sensors

Threat Intelligence by the Numbers

Each day, Webroot discovers...



6,000

Phishing
Sources



80,000

New Malware
& PUAs



51,000

New Mobile
Malware

File Data



More than **97%**
of threats are unique



Less than 50
examples per malware
variant in 2016

Notable Observations

01

Angler Exploit Kit cybergang arrested

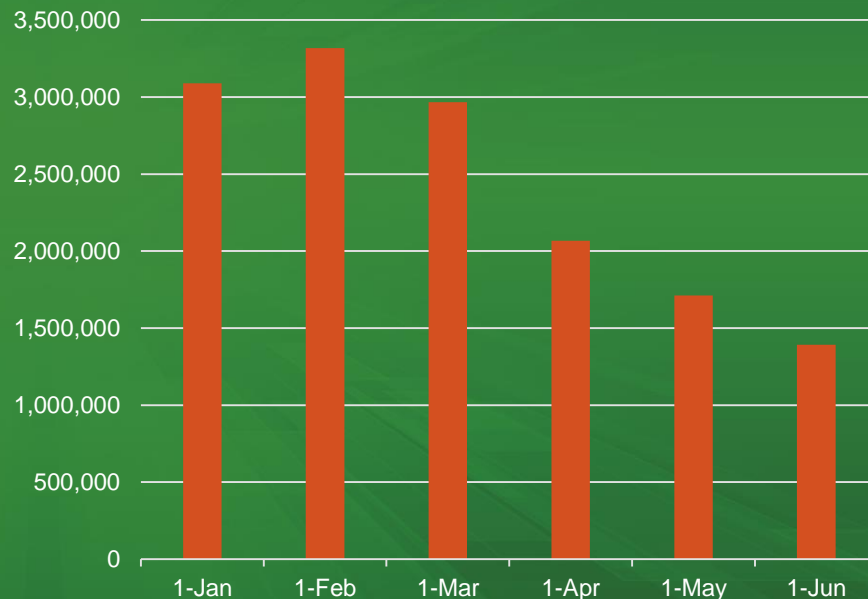
02

Neutrino Exploit Kit eating up Angler market

03

10+ other exploit kits competing for market share

Malware & PUA Monthly Volume



Malware Trends

Angler arrests contributed to:



8.12%
decrease in
malware
volume



15%
decrease in
malware
encounter
rates



53.61%
decrease in
samples per
variant of
malware

PUA Trends

PUAs **36.31% fewer**
examples detected

Encounter rates dropped
by **28.71%**



Examples of per
PUA installer variant
dropped **33.08%**

Android Malware

In the first 6 months of 2016...



More than
300%
growth in
Android
Apps



Over
500%
growth of
malicious
apps



Over
400%
growth of
PUA

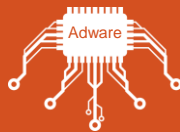
Notable Observations



Fastest
growth of
new
malicious
apps is in
China



Trojans are
still the most
popular
category



More adware
apps have
rooting
functionality



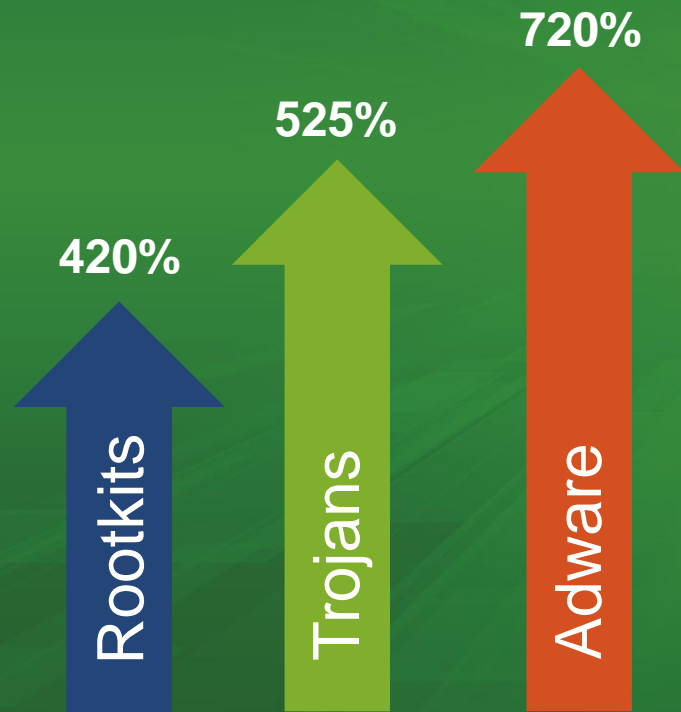
Google Play
isn't 100%
safe



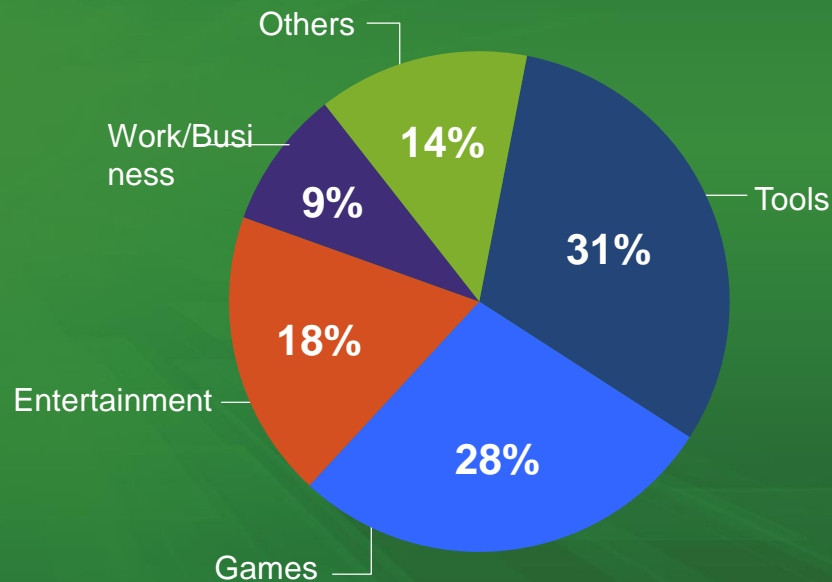
Ransomware
persists

Android Trends

Fastest growing malware categories:



Simplified Categories of Malicious Apps



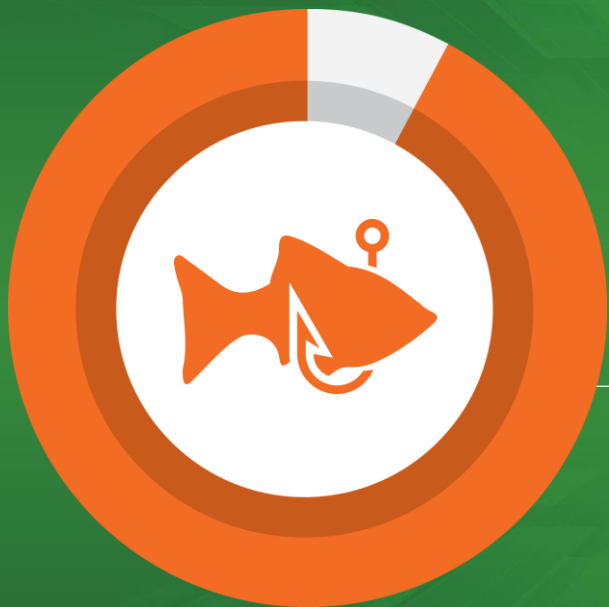
Phishing

Phishing sites are using new tactics to evade detection

JavaScript prevents
leaving a page



Plain text avoids
HTML analysis



92%

chance of visiting a
zero-day phishing site

Notable Observations



Yahoo! displaces
Google, Wells Fargo
displaces PayPal



Canadian Imperial
Bank of Commerce
is #3 financial target



Christian Mingle is
2nd most phished
social networking
site

Threat Brief Conclusions



Angler arrest
had a huge
impact on the
volume of
threats



New exploit
kits are
competing for
market share



Threats
continue
evading
detection
due to
uniqueness



More Android
threats will
make it past
Google Play



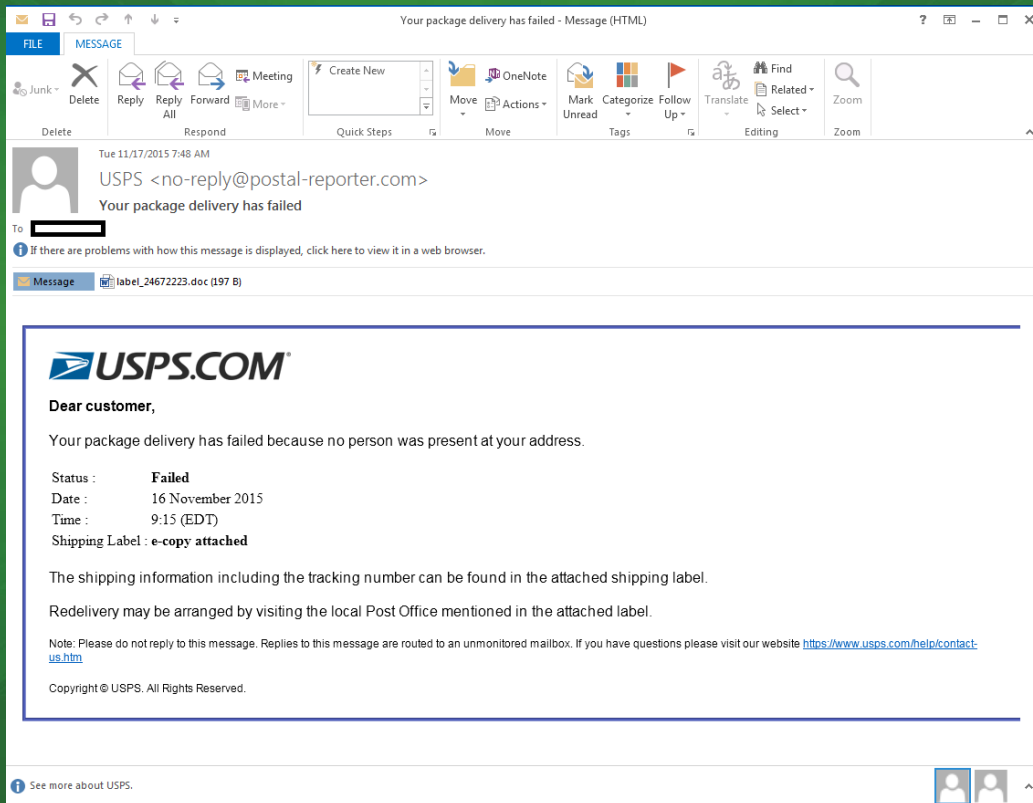
Phishing
remains
effective and
now has
more targets

Attack Vectors

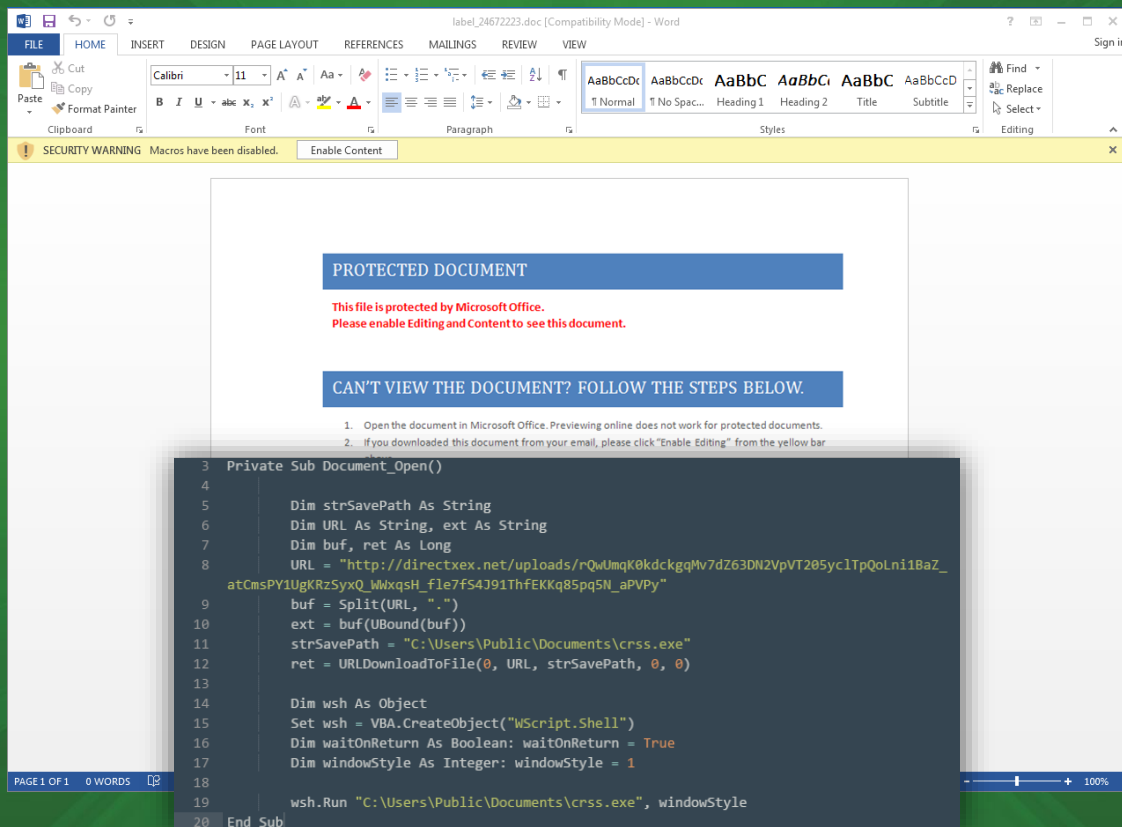
Phishing & Exploit Kits



Social Engineering – Phishing Macro infection



Social Engineering – Phishing Macro infection



Angler/Bedep/Neutrino Exploit Kits

01

Been around since late 2013

*Took over for the demise of
Blackhole Exploit Kit*

04

**Bedep helps stifle the
research process**

Prevents payloads from being dropped on VMs

02

**80% of all Drive-by-Attacks
this year**

Most are deploying CryptXXX

05

**Cyber Criminals using Angler
generate \$3M/month**

Almost exclusively from Ransomware

03

**Attack Flash Player, Java, word and
Silverlight vulnerabilities**

*Hack into legit website then simple
IFRAME injection*

06

**Neutrino just recently took
over Angler**

*Also has many prevention checks for
research environments*

Malvertising Explained

Attack that uses online ads to spread malicious code

01

Cyber criminals submit booby-trapped advertisements to ad networks for real time bidding process

02

Malicious ads rotate with normal ads on legitimate, highly reputable sites

03

Users visits site with an infected ad

04

Invisible iframe redirects to exploit landing page where malicious code attacks the system

05

Malicious software is installed - usually Encrypting Ransomware

Encrypting Ransomware

Newest Variants



CryptXXX

01

**From the Creators
Of the Reveton FBI
lock**

*Very dedicated and
always updating*

02

**Exclusively uses
Exploit Kits**

*Malvertising and
Hacked websites
only way to get it*

03

**Default
Payment is \$500**

04

**Now uses Neutrino
after Angler was
shut down**

05

**Is also known to
drop Dridex**

*So this ransomware
will also try and
steal credentials*

CryptXXX

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 price 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: D7[REDACTED]E87

□

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

□

□1 - <http://rp4roxehucf2vgft.onion.to>

□2 - <http://rp4roxehucf2vgft.onion.cab>

□3 - <http://rp4roxehucf2vgft.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 - Video instruction: <https://www.youtube.com/watch?v=NQrUZdsw2hA>

□3 - After a successful installation, run the browser

□4 - Type in the address bar: <http://rp4roxehucf2vgft.onion>

CryptoMix

01

No payment on the DarkNet

One of the few ransomware that doesn't have this

02

All communication is done via emailed links to encrypted messages

03

Encrypted messages are only displayed once and then lost forever

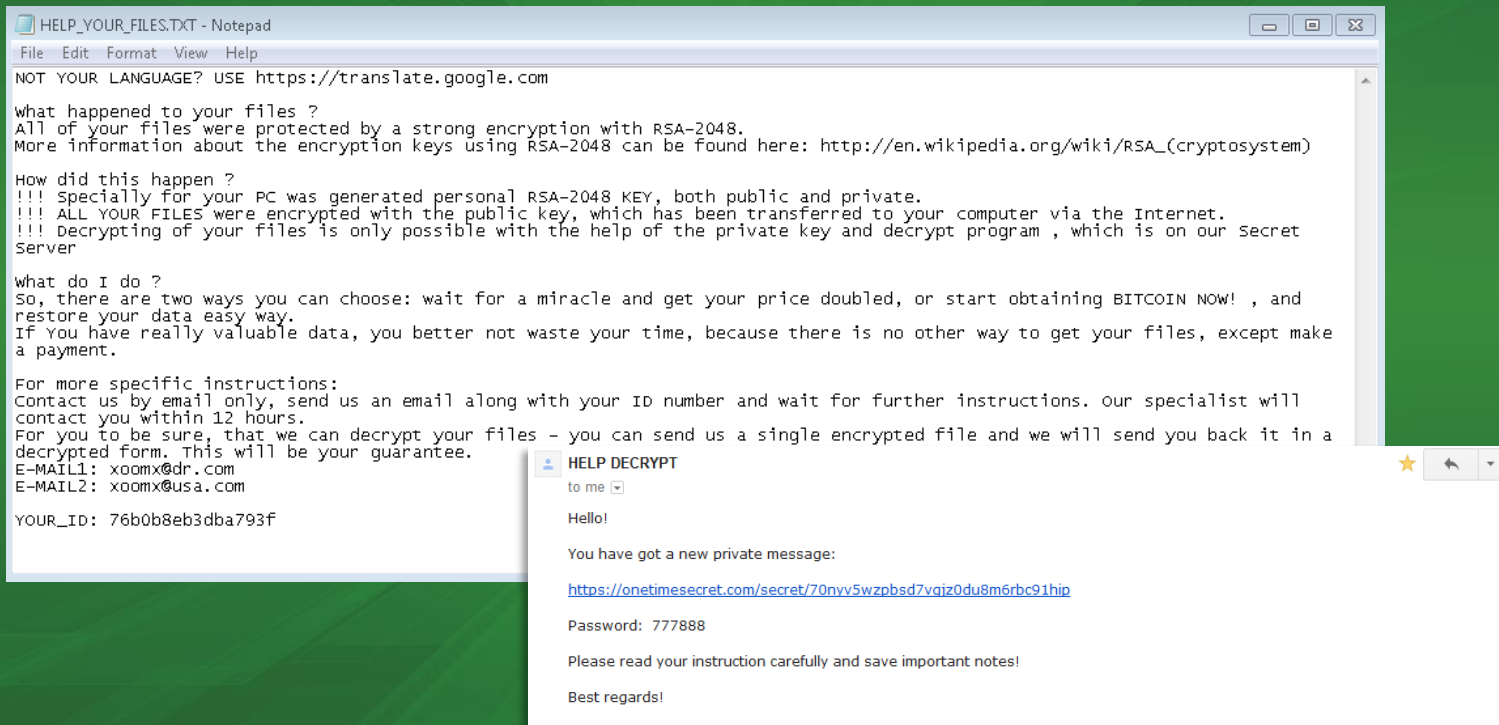
04

**Extremely expensive at 5BTC
~ \$2900**

05

Claim that you'll receive free tech support and all your ransom money goes to children charity

CryptoMix



CryptoMix

Dear User,

to decrypt your files You will need a special software with your special unique private key.

Price of software and your private key is 5 bitcoins. With this product you can decrypt all your files and protect Your system!!!! Protect!!!! Your system will be without any vulnerability.

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

You can buy bitcoins through this bitcoin web site <https://localbitcoins.com/>

Register there and find a nearest Bitcoin seller. It's easy! Choose more comfortable payment method for buying Bitcoin!

After that You should send 5 bitcoins to the bitcoin wallet address:

2FH7sjkh83JH8fVh810DhrBg85HJwAg

All this process is very easy! It's like a simple money transfer.

And now most important information:

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!

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 will be doubled by the Main Server automatically. So now you have a chance to restore your PC with low price!

Best regards,

Charity Team

Cerber

```
#DECRYPT MY FILES#.txt - Notepad
File Edit Format View Help

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 #Cerber+Rans0mware.

#####

!!! If you are reading this message it means the software
!!! "Cerber Rans0mware" has been removed from your computer.

#####

what is encryption?
-----

Encryption is a reversible modification of information for security
reasons but providing full access to it for authorized users.
```


Cerber Decryptor

cerberhhyed5frqa.onion/9713-5138-6AE7-0063-7ETC

Home page FAQ Support Decrypt 1 file for FREE Reload current page

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».

All transactions should be performed via  **bitcoin** network only.

Within 5 days you can purchase this product at a special price: **\$2.000 (≈ \$1316)**.

After 5 days the price of this product will increase up to: **\$4.000 (≈ \$2632)**.

The special price is available:

04 . 23:59:33

Ransomware Rivalry

Chimera® Ransomware

You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file. Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get your unique key file.

Address:

Amount: 0,93945085 Bitcoins

RAW Paste Data

Like the analysts already detected, Mischa uses parts of the Chimera source. We are NOT connected to the people behind Chimera. Earlier this year we got access to big parts of their deveolpment system, and included parts of Chimera in our project.

Additionally we now release about 3500 decryption keys from Chimera. They are RSA private keys and shown below in HEX format. It should not be difficult for antivirus companies to build a decrypter with this informations.

Please also check our RaaS system, which now has its registration opened: <http://janusqqdo2zx75el.onion/>

LINK: <https://www.sendspace.com/file/0fk7wj>

Tweets

Tweets & replies

Media



JANUS @JanusSecretary · Jul 26

Now publishing leaked #chimera
#ransomware keys:
pastebin.com/7HrZCsmT • @hasherezade



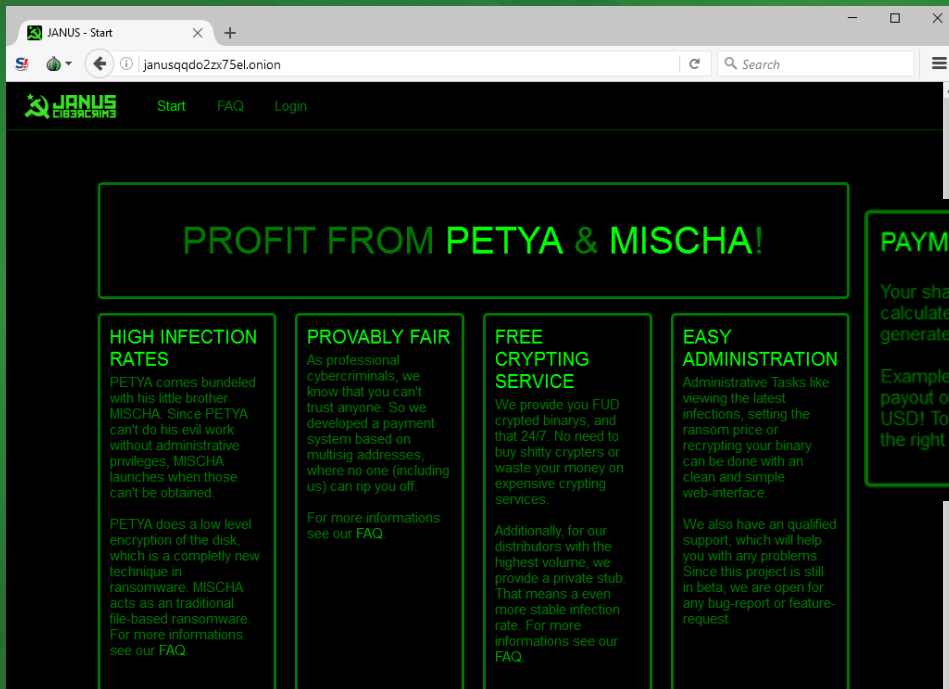
12



7



Ransomware Rivalry



The screenshot shows a web browser window with the address bar displaying 'janusqdo2zx75el.onion'. The page has a dark theme with a green header bar containing the 'JANUS' logo and navigation links for 'Start', 'FAQ', and 'Login'. The main content area features a large green box with the text 'PROFIT FROM PETYA & MISCHA!'. Below this, there are four columns of text, each with a green header and a light green background. The columns are titled 'HIGH INFECTION RATES', 'PROVABLY FAIR', 'FREE CRYPTING SERVICE', and 'EASY ADMINISTRATION'. Each column contains a paragraph of text describing the service's features and benefits.

PROFIT FROM PETYA & MISCHA!

HIGH INFECTION RATES
PETYA comes bundled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.

PETYA does a low level encryption of the disk, which is a completely new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.

PROVABLY FAIR
As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.

For more informations see our FAQ.

FREE CRYPTING SERVICE
We provide you FUD crypted binaries, and that 24/7. No need to buy shitty crypters or waste your money on expensive crypting services.

Additionally, for our distributors with the highest volume, we provide a private stub. That means a even more stable infection rate. For more informations see our FAQ.

EASY ADMINISTRATION
Administrative Tasks like viewing the latest infections, setting the ransom price or recrypting your binary can be done with an clean and simple web-interface.

We also have an qualified support, which will help you with any problems. Since this project is still in beta, we are open for any bug-report or feature-request.

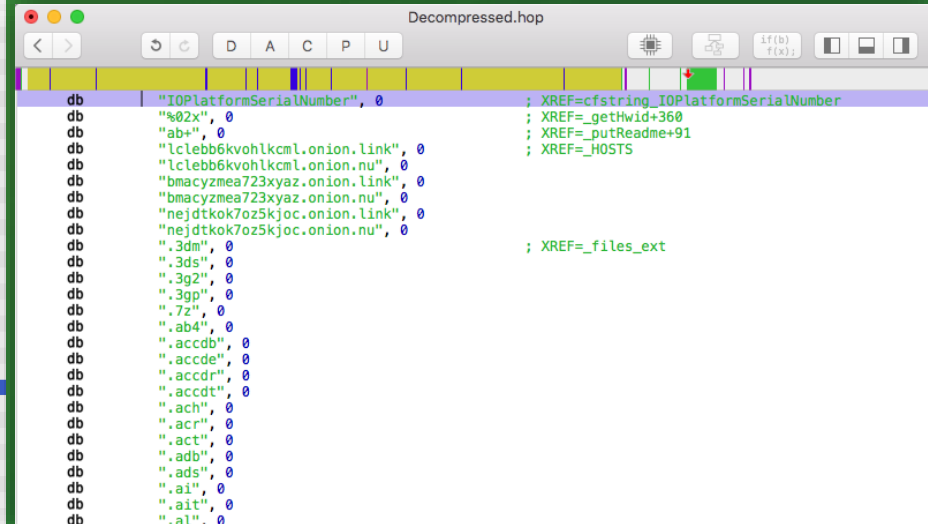
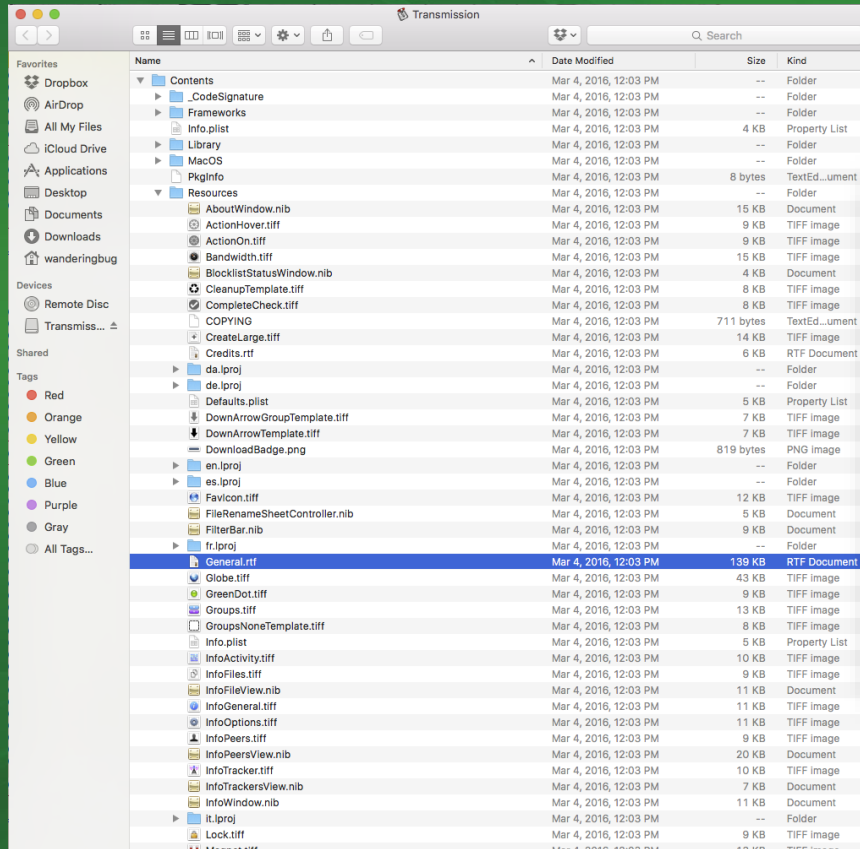
PAYMENT SHARE

Your share on the payments you have generated is calculated with the following table. The more volume you generate in one week, the more share on the profit you get.

Volume/Week	Share
<5 BTC	25%
<25 BTC	50%
<125 BTC	75%
>=125 BTC	85%

Example: If you generate a volume of 125 BTC, you get a payout of 106.25 BTC. That are at the moment about 45,000 USD! To get a volume over 100 BTC is not a big deal with the right technique!

KeRanger – Mac OS Encrypting Ransomware



Ransomware for Thermostats



The Advantages of Bitcoins



How To Clean Your Coins

Step 1
Deposit
Bitcoin



Step 2
Withdraw
Bitcoin

Confused? Questions? Check our FAQ or contact us

NEED TO LAUNDER YOUR BITCOINS? Need a Bitcoin Mixer?

Bitcoin transactions can be viewed publicly in the blockchain, meaning anyone can analyze your bitcoin transactions and figure out their origins, potentially tracing them back to your exchanger where you bought the coins, thereby unmasking your real identity. Bitcoins are decentralized and peer-to-peer, but not anonymous by default. BitLauder cleans your Bitcoins, removing all traces of previous ownership and transactions, thus completely 'washing' them to obscure their origins.

ANONYMIZE BITCOIN

Our Bitcoin laundry completely anonymizes your Bitcoin, masking their origins and obscuring their history.

BITCOIN MIXER

BitLauder provides a full-featured Bitcoin Mixer, such as a 'quick and instant' method and a longer, more secure algorithm which completely scrambles your Bitcoin history.

FAST AND EASY

LAUNDERING BITCOIN

We are experts at laundering bitcoins. We use the most sophisticated methods available to completely anonymize your bitcoins and obscure their history from forensic tracing. Almost all Bitcoins are tainted by illegal activity. Find out why you should use our Bitcoin tumbler

TIME RELEASE

Schedule your bitcoins to be released over a period of time to one address OR multiple addresses

Bitcoin

A Quick Guide to Stopping Ransomware

5 Easy to follow Tips



Deploy Reputable, Multi-Layered Endpoint Security

Having endpoint security that prevents malware infections in the first place is vital. Look for security that protects web browsing, controls outbound traffic, protects system settings, proactively stops phishing attacks, and continuously monitors individual endpoints.



Deploy Backup and Business Continuity Recovery



Disable Macros and Autorun

Lots of crypto ransomware infect systems using macros. Macros can easily be disabled in the Trust Center of every version of Microsoft® Office. It is also possible to enable individual macros, should they be used for a particular task. While autorun is a useful feature, it is often used by malware to propagate. For instance, USB sticks will use autorun to proliferate, as do commonly used by Visual Basic Script (VBS) malware and worms. It is best to Policy disable autorun.



Create Strong Windows Policies



When it comes to crypto ransomware, consider using Windows Policies to block certain paths and file extensions from running. Policies can be set up in groups, which is useful if varying levels of access are required. (Note: Test any policies on a test PC.) Examples of useful policies include: blocking executables in temp or temp+appdata and the creation of startup entries. The following file types shouldn't be run in the following directories: .SCR, .PIF, and .CPL in users' temp, program data, or desktop.

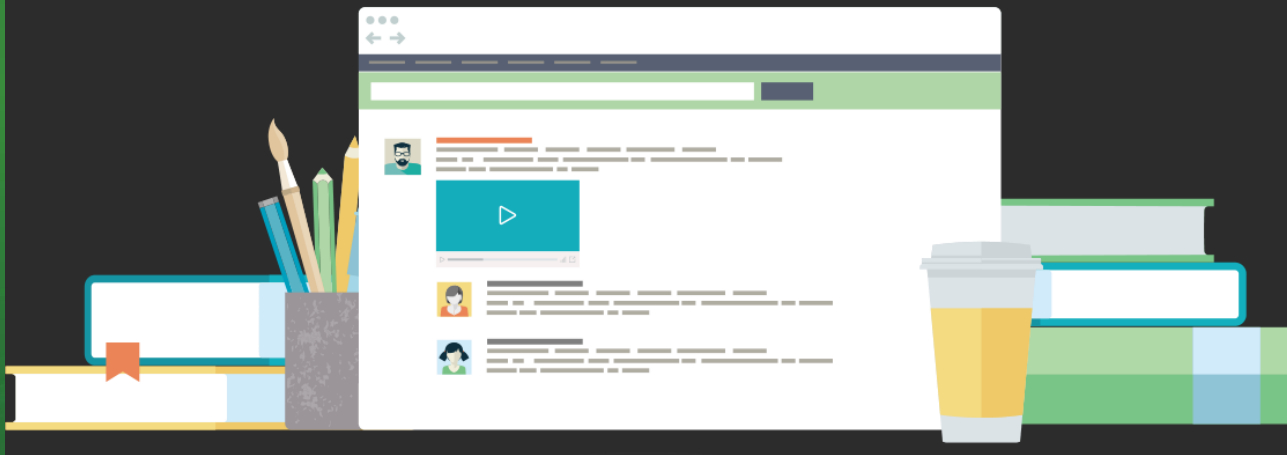
Use Policies to Block Volume Shadow Copy Service

Windows creates local copies of files using the VSS copy service. Ransomware like CryptoLocker will encrypt this area because it holds VSS copies for the local drive (normally the C:\ drive). Using Windows Policies to block access to the service helps stop ransomware like CryptoLocker from erasing local drive file backups. Policies should point to the VSSAdmin executable. Any attempt to access or stop the service will result in a block.



Educate Users

As always with security, users are often the weakest link. Malware will continue to thrive and be a viable business as long as staff are unaware and uneducated on the risks of the Internet. Providing the basics will protect users at home and in the office.



Thank you.

Questions?
tmoffitt@webroot.com

