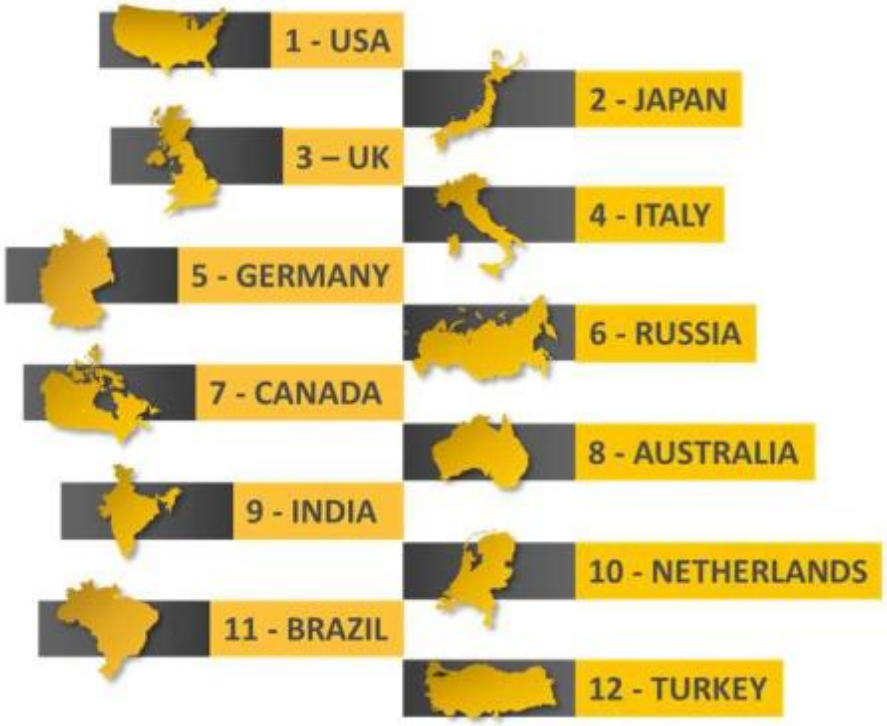
RANSOMWARE

By Prachi Gulihar

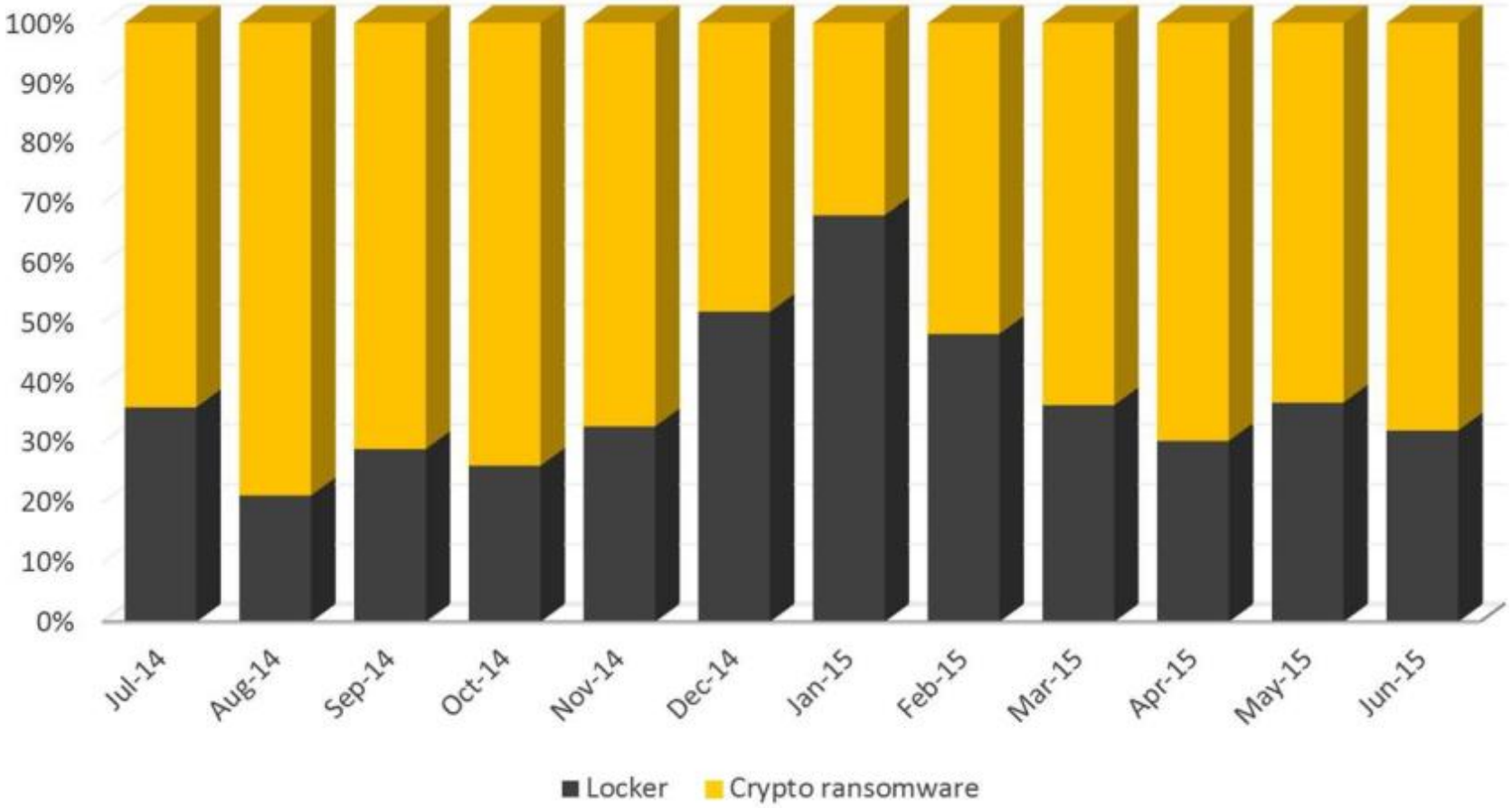
What Is Ransomware?

- Ransomware has been built upon the two words ransom and malware.
- It is a Denial Of Service attack.
- It is a kind of malware which demands a payment in exchange for a stolen functionality.

Motivation



- Ransomware threat has become a global epidemic touching all corners of the world targeting more affluent or populous countries.
- 11 of the top 12 countries impacted by ransomware are members of the G20 organization, representing industrialized and developing economies that make up roughly 85 percent of the worlds GDP.



- Cryptoransomware dominating the ransomware threat landscape for past years.

Types Of Ransomware

Locker Ransomware

- Typically only designed to prevent access to the COMPUTER INTERFACE, leaving the underlying system and files untouched.
- LESS EFFECTIVE at extracting ransom payments compared to its more destructive relative crypto ransomware.
- MASQUERADES as law enforcement authorities and claims to issue fines to users for alleged online indiscretions or criminal activities.
- Particularly be effective on devices that have limited options for users to interact with. This is a potential problem area considering the recent boom in WEARABLE DEVICES and the Internet of Things (IoT).

BUNDESPOLIZEI

[redacted]

TAT

(!)1ro.,,

Fa·l·o

M; U

or..

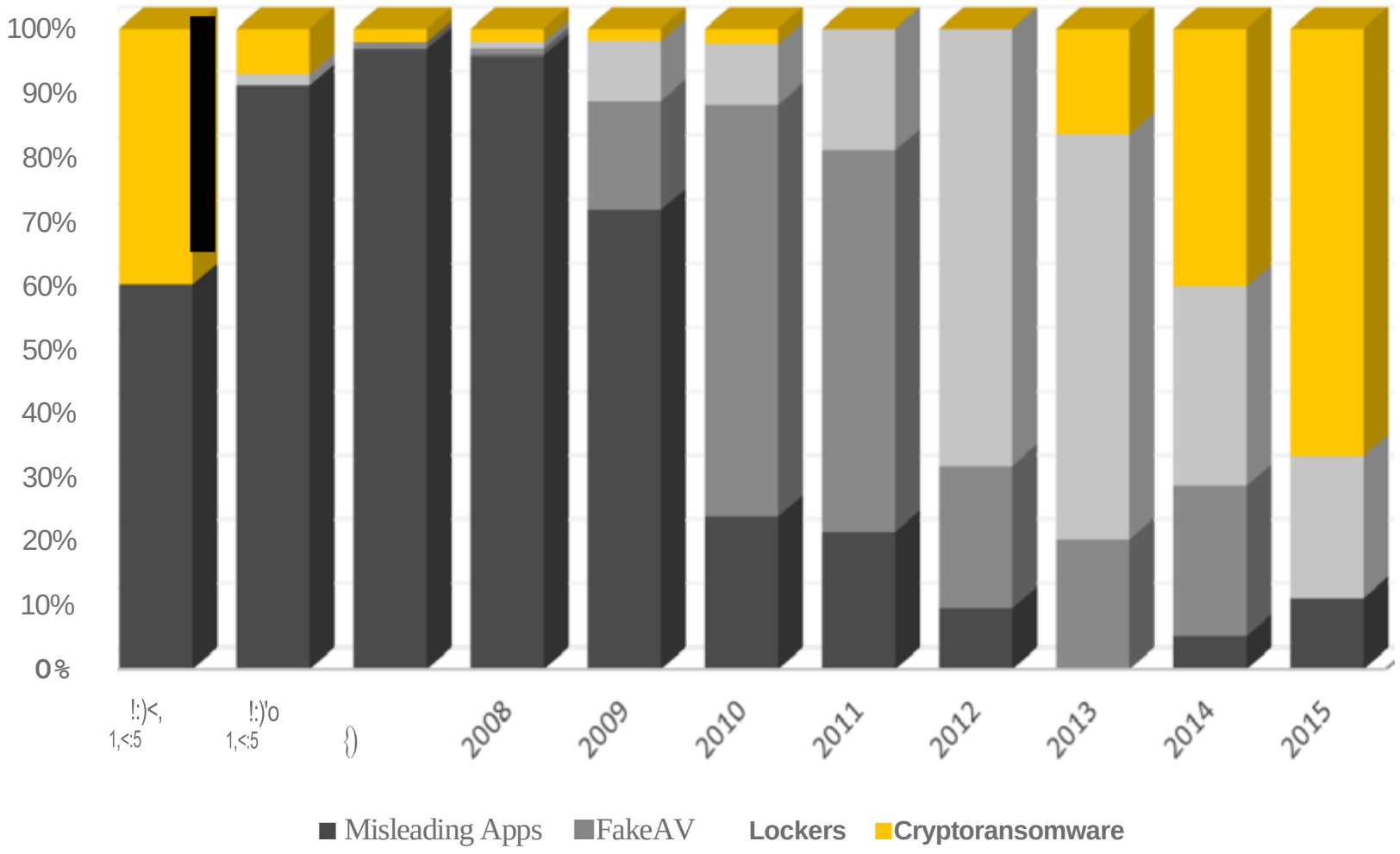
Crypto Ransomware

- Designed to find and ENCRYPT VALUABLE DATA stored on the computer, making the data useless unless the user obtains the decryption key.
- Goal is to stay below the radar until it can find and encrypt all of the files that could be of value to the user.
- The affected computer continues to work normally, as the malware does not target critical system files or deny access to the computers functionality.
- Typical crypto ransomware demand screen is generated.

¥ Threat Finder

Evolution Of Ransomware

- Originated 26 years ago with the appearance of the AIDS Trojan.
- Looking at the recent history of ransomware, ransomware can be divided into four families identified between 2005 and 2015:
  Misleading apps
  Fake AV
  Locker ransomware
  Crypto ransomware


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
!:)<,
1,<:5
!:)'o
1,<:5
{)
2008
2009
2010
2011
2012
2013
2014
2015
Misleading Apps
FakeAV
Lockers
Cryptoransomware

Misleading Apps

- Posed as fake spyware removal tools.
- Performance enhancement tools.
- Exaggerated the impact of issues on the computer.
- Unused registry entries.
- Corrupt files.
- Did not fix anything.

Fake AV

- Mimicked the appearance and functionality of legitimate security software.
- Performed mock scans.
- Claimed to find large numbers of threats.
- The user was asked to pay fees to fix the fake problems.
- Asked to pay for bogus multi-year support services.
- Ignored the alerts.
- Removed the software.
- Resulting in lower return.
- Looked for new ways to make the call-to- action stronger.

The Move To Locker Ransomware

- Disables access and control of the computer.
- Charges around US dollar 150 to US dollar200 payable through electronic cash vouchers.

- Trojan.Randsom.C. Spoofed a Windows Security Center message and asked the user to call a premium-rate phone number to reactivate a license for security software.

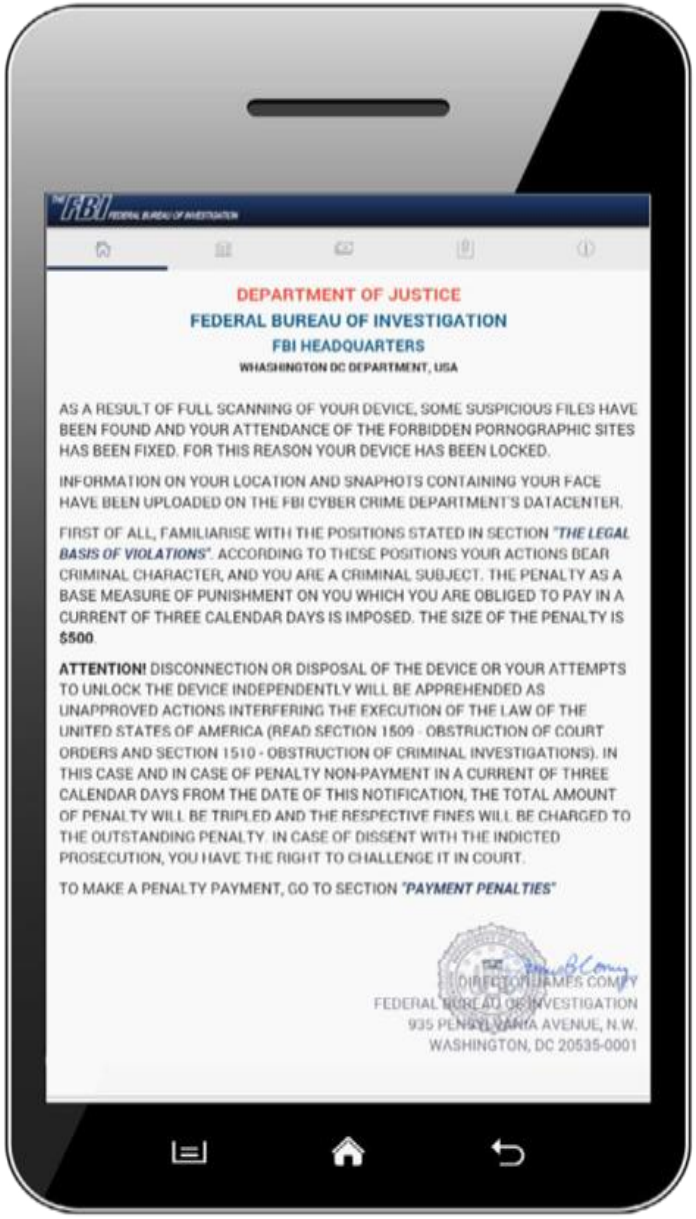
The Move To Crypto Ransomware

- Tends not to use social engineering.
- It is upfront about its intentions and demands.
- Displays an extortion message.
- Offers to return data upon payment of hefty ransoms.
- Requests payment of around US dollar 300 for a single computer.
- The key lessons learnt:
  Proper key management is crucial for success
  Keys stored within the crypto ransomware itself
  Using the same key in all of the variants
  Choosing the right encryption algorithm.
  Development of sophisticated crypto ransomware variants.

Targets And Systems Impacted By Ransomware

- Home users
- Businesses
- Public agencies
- Personal computers
- Mobile devices Servers
- Mobile devices Servers

- False threats found by Android.Fakedefender.



- FBI-themed lock screen from Android.Lockdroid.E, one of the first pure locker ransomware for mobile devices.

How Ransomware Works?

- Propagation: Routes for ransomware to arrive on computer.
- Attackers buy redirected web traffic from a Traffic Distribution Service (TDS) vendor and point it to a site hosting an exploit kit.
- MALADVERTISEMENTS, Malicious advertisements get pushed onto legitimate websites in order to redirect traffic to a site hosting an exploit kit.
- Cybercriminals use REAL-TIME BIDDING to purchase traffic or ad space ofinterest that can allow them to geographically target victims and operate without borders.


TRAFFIC DISTRIBUTION SYSTEM
MALVERTISEMENT
EXPLOIT KITS
SOCIAL ENGINEERING
SPAM EMAIL
DOWNLOADER
DATA BREACH
BOT INFECTION
SMS MESSAGE
Your personal files are encrypted!
71 : 03 : 09
Next >>

Downloaders

- Once the downloader infects a computer, it downloads secondary malware onto the compromised system.
- Cybercriminals offer a malware-installation service onto already compromised computers, at a price to other malware authors.
- Botnets have also been known to download ransomware onto computers they have infected.
- Final way of monetizing infected computers that they control.

Affiliate Schemes

- Provide services to those who wish to carry out ransomware attacks.
- No need to have the skills to create a ransomware.
- Offer members a substantial cut of the profits from each ransomware infection.
- All the affiliate member has to do is to spread the ransomware as far and wide as possible to maximize the chances of extracting a ransom.
- Like for each ransom 30-70 percent.

BS Registered Member

Registered Users

Join Date: Sep 2014

Location: blackstuff

Posts: 21

TorLocker Ransomware (Daily BTC inflow)

TorLocker Ransomware
What is this?
An affiliate program.
I provide a password for the control panel of TorLocker, a binary made in assembly for Windows, a builder, and a tor.exe standalone executable.
What is TorLocker?
TorLocker is a ransomware that works using TOR, BitCoin, RSA-2048, AES-256.
Is it similar to CryptoLocker?
Yes and No.
TorLocker encrypts files and demands user for a ransom. So CryptoLocker does.
TorLocker don't need internet connectivity to start encrypting files, CryptoLocker does.
TorLocker has 128 public keys inside the .exe body. Each affiliate receives new different encryption keys already inside the .exe.
After 10 different payments, i generate a new .exe for you, so no repeated keys are going to be used.
TorLocker command and control is hosted behind TOR hidden services. Can't be shutdown easily.
TorLocker accepts BitCoin only (Moneypak,Ukash Already Available for First Set Buyers)
TorLocker process payments and encryption key delivery, automatically. No human intervention is necessary.
How it works?
It will encrypt all files (extensions below) from the computer you send it, connect to TOR, retrieves the amount the user needs to pay (currently 0.380 BTC), the deposit address (a new address for every new client), how many days the user has to pay (currently 9 days counting down to 0 when decryption will not be possible).
After 6 confirmations from the BitCoin network, 70% of the ransom is sent to you. 30% goes to me, and the RSA-2048 decryption key is automatically delivered to the client, who get access to his files again. Each file is encrypted with a random AES-256 key, which is encrypted with the RSA-2048 key and then appended to the encrypted file.
How larger encrypted files become?
512 bytes
Is unicode supported?
Yes
What if I find a bug?
Report and I will correct it.
*Which extensions are currently being used?
".accdb",0,".ai",0,".arw",0,".bay",0,".blend", 0,". cdr",0,".cer",0,".cr2",0,".crt",0,".crw",0,".dbf" ,
0,".dcr",0,".der",0,".dng",0,".doc",0,".docm",0, ". docx",0,".dwg",0,".dxf",0,".dxg",0,".eps",0,".erf"
,0,".indd",0,".jpe",0,".jpg",0,".jpeg",0,".kdc",0 , ".mdb",0,".mdf",0,".mef",0,".mrw",0,".nef",0," .nrw
",0,".odb",0,".odm",0,".odp",0,".ods",0,".odt" ,0," .orf",0,".p12",0,".p7b",0,".p7c",0,".pdd",0,".pdf"
,0,".pef",0,".pem",0,".pfx",0,".ppt",0,".pptm",0, " .pptx",0,".psd",0,".pst",0,".ptx",0,".r3d",0,".raf
",0,".raw",0,".rtf",0,".rw2",0,".rwl",0,".srf" ,0," .srw",0,".wb2",0,".wpd",0,".wps",0,".xlk",0,".xls" ,0,".xlsb",0,".xlsm",0,".xlsx",0,0**
What I need to do to start cashing?
An offline BitCoin wallet. bitcoin-qt is fine. Synchronize the bitcoin wallet with the network (it will take some time).
Download tor browser bundle. Configure TOR as the SOCKS proxy in the bitcoin client (this is a very important step to your safety).
Generate a new address. Get your password for the TorLocker panel from me (buying this listing). Register you BitCoin address in the panel (you will be asked only once, in the first time you login). Spread the .exe, receive the money.
In how many time will you setup my account?
Maximum 4 days.

- Discussion in an underground forum between a ransomware-as-a-service (RAAS) seller and a prospective buyer, offering the buyer a 70 percent cut of potential earnings.

Spam Email

- Use of botnet to send the spam.
- Cybercriminals offer a spamming service to other attackers for a fee.
- Contains a malicious attachment.
- Link to a site hosting an exploit kit.
- Themes:
  Mail delivery notification
  Energy bills
  Job seeker resume
  Tax returns and invoices
  Police traffic offense notifications

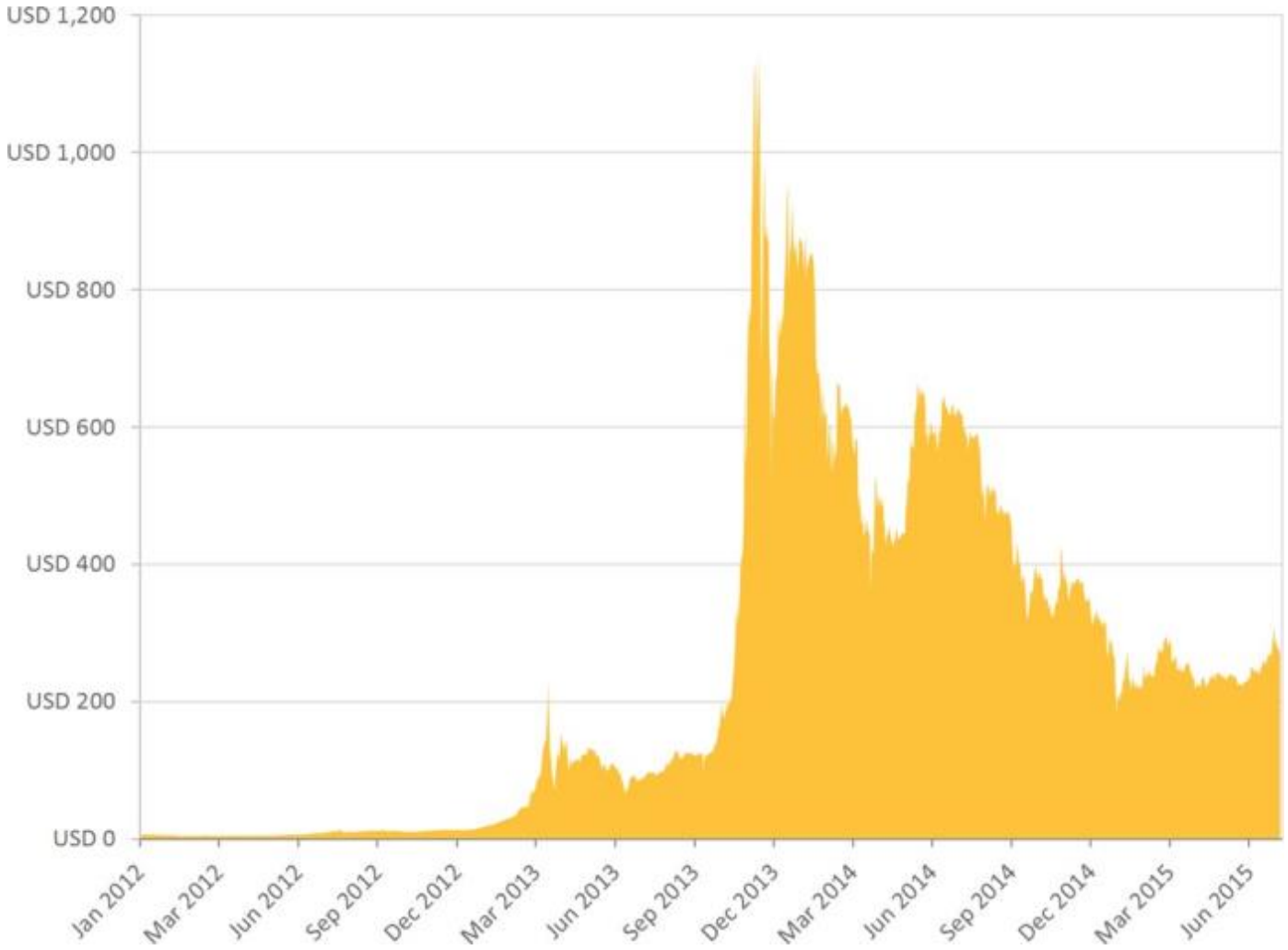

AFP
AUSTRALIAN FEDERAL POLICE
You could have recently been given with a drive
Purpose: irresponsible driving a car
intrusion number: 2839335832290
Time frame associated with problem: 27/06/
Amount owing: $186.58 AUD
Due date: 26/06/2015
To discover more info please
see your
have to be created within 11 d
violation info as well as your
You may apply for the ex
penalty, or contest the
It is automatically pro
See more about: Australian Federal Police.
POST eParcel
The mailman did not deliver package
The courier did not redeem the item to your home bec
Download sh
Just in case the box isn't received within 30 servi
settlement from you for it's helping to keep in th
This is an automatically generated message
See more about: Australia Post.
EnergyAustralia
Electricity bill
Dear Valued Customer
Your electricity bill is ready
Service: Electricity
Bill Amount: $462.37
Due Date: 05/31/2014
The bill amount listed below does not include payments made after the bill period ended.
There you can view your bill details
Opening balance$63.79
Balance carried forward$32.09
Current charges$462.37
Total amount due$462.37
3% discount if you pay this bill by the due date$13.87
Total amount due with discount$448.49
Due date: 31 may 2014
Total amount if paid after due date $462.37
Total amount with 3% discount if paid by due date $448.49

Pricing

- The most important criteria for the chosen payment system is that it must provide anonymity.
- Users are given a different ransom demand amount depending on their location.
- When a computer is compromised, Cryptowall reports back to a command-and-control (CC) server with the IP address of the infection.
- The server performs a lookup of the IP address and determines the country that the infected computer is located in.
- Based on various factors the price returned to the infected computer is adjusted to suit the location.

Payment Systems

- Use of payment voucher systems such as Paysafecard etc.
- The arrival of cryptocurrencies like Bitcoin.
- They provided anonymity, making it easier for cybercriminals to launder their ill-gotten gains.
- Payments are made through sites hosted on the dark web (often accessed through Tor), making it more difficult for law enforcement to track down the cybercriminals.
- Despite its advantages for cybercriminals, holding bitcoins for long is not favorable Bitcoin exchanges are hacked.
- Impacted by high-volume DDoS attacks.
- Leading to bitcoin breaches so they should be quickly.
- Favored payment systems.
- Crypto ransomware tends to favor cryptocurrencies.
- Locker ransomware prefer to use payment voucher systems.



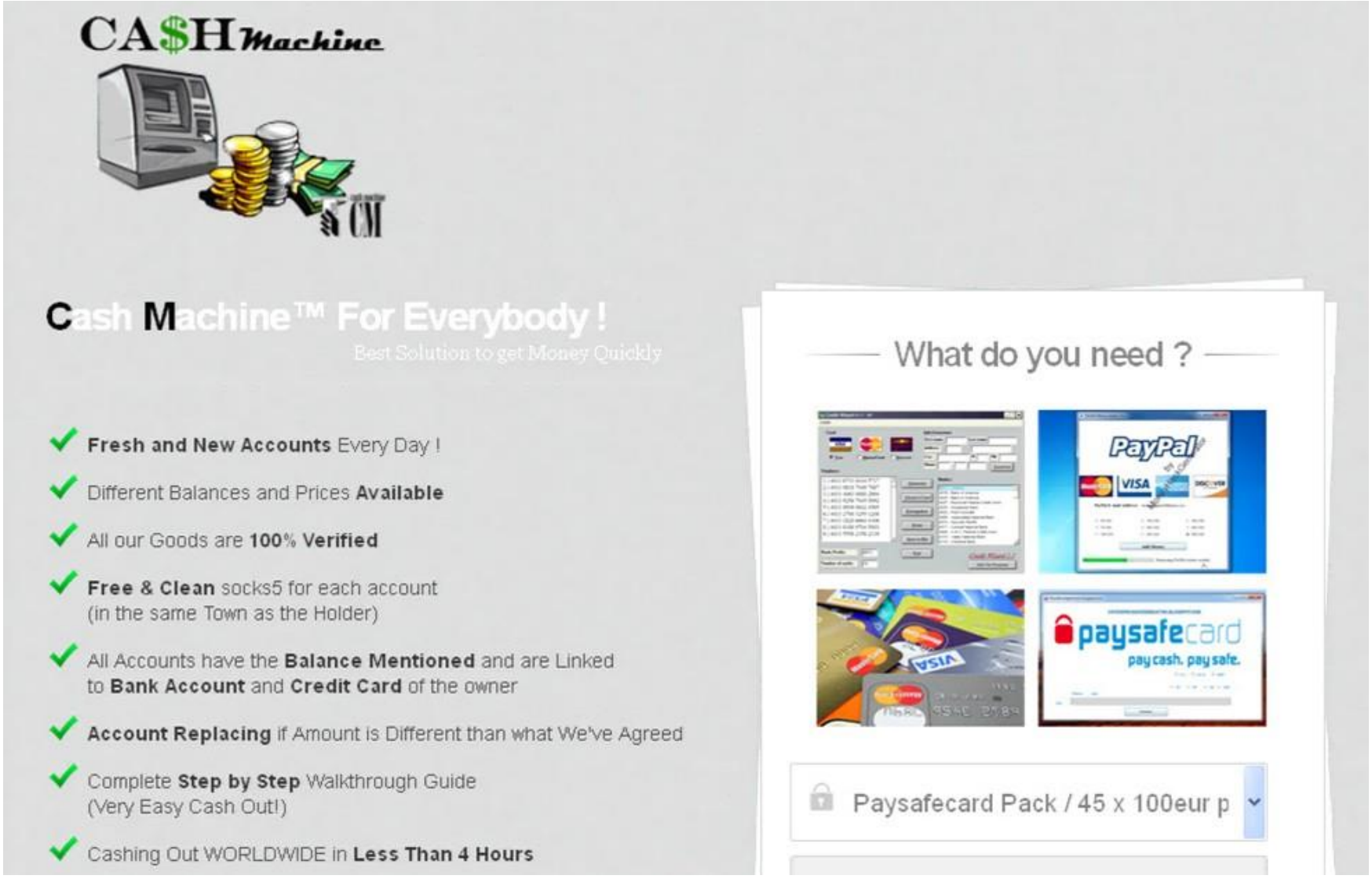
- Bitcoin versus US dollar exchange rate from 2012 to 2015, showing the wild movement in the exchange rate.

- Ransom note demanding payment of US dollar 500 in bitcoins for decryption of files.

- To build trust, some crypto ransomware allows the victim to decrypt five randomly chosen files for free. This is a trust-building exercise to show victims that the cybercriminals can and are willing to decrypt filesif the ransom is paid.

How Cybercriminals Cash Out?

- Depends on how the ransom payment was made.
- For Vouchers specialized money-laundering services are used like online betting and casino that accept voucher codes for payment.
- These sites are hosted in different geographical and legal jurisdictions, making it difficult for law enforcement to track the money.
- Once laundered, the money is transferred to fraudulently obtained debit cards and the money is withdrawn from ATMs.
- An agreed percentage of the payment vouchers value is sent to the ransomware cybercriminals.



- A website accessed through Tor offers cash-out services, allowing cybercriminals to quickly convert illicit gains into hard cash.

Bitcoins

- Laundering services mix up bitcoins from legitimate sources as well those from ill-gotten gains
- By transferring them through multiple Bitcoin block transaction wallets
- Then it becomes very difficult to differentiate between legitimate transactions and cybercrime payments in the bitcoin transaction history.
- By the time the bitcoins are cashed out, no link to criminal activity is found.

ANONYMIZE BITCOIN

BITCOIN MIXER

... the perfect bitcoin mixing service...

Powerful tools to launder your bitcoins.

Our bitcoin mixing service will fully anonymize bitcoin.

Features include:

Quick Launder - We scramble your bitcoins with the coins of other users, obscuring their origins. Fast and automated, but not 100% untraceable.

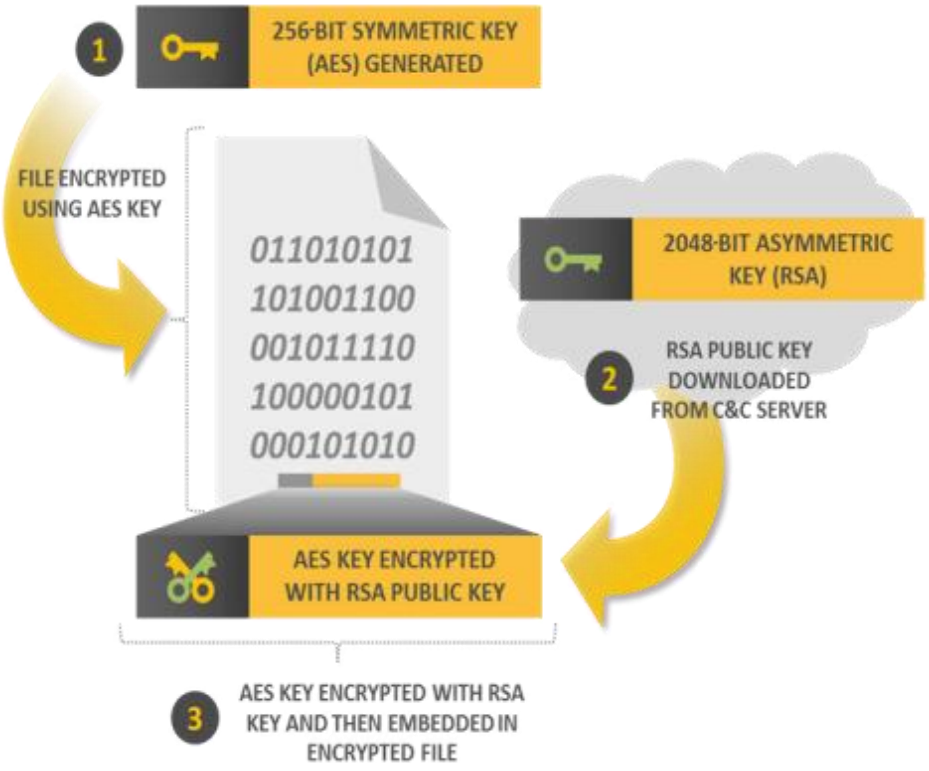
Secure Launder - We completely randomize your bitcoins, sending them back to you from a separate 'onionland' wallet, ensuring their is absolutely no connection between your old coins

- A bitcoin-laundering service offers to mix bitcoins from different sources to make it harder for investigators to track the bitcoins.

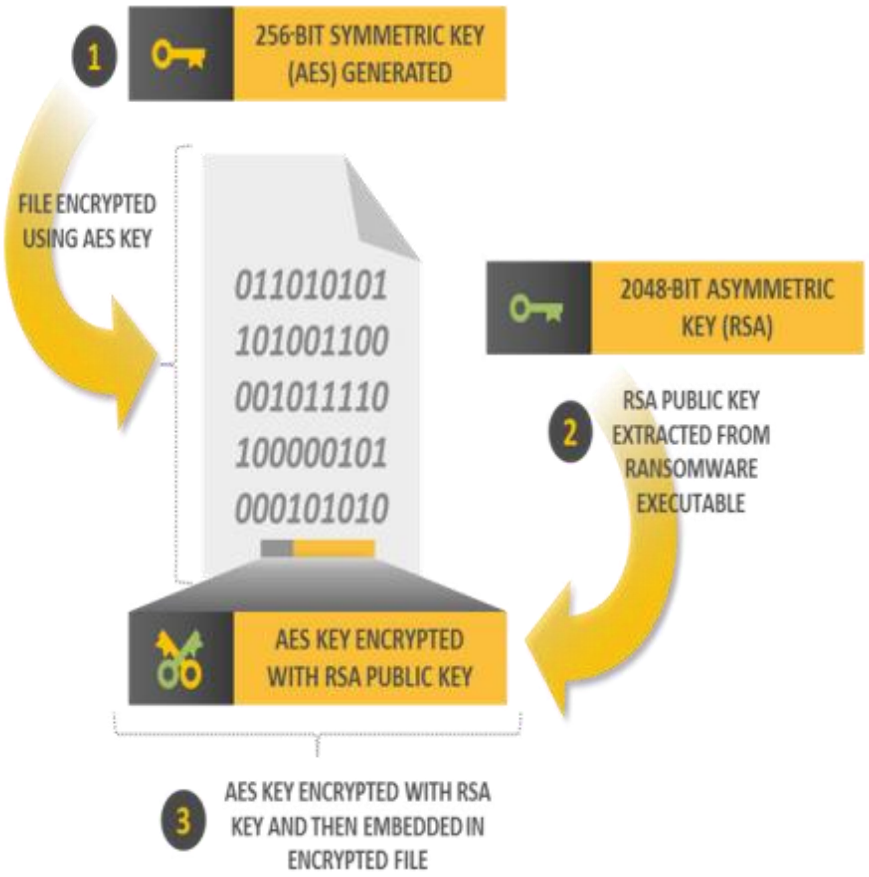
Ransom Techniques

- Modern crypto ransomware typically uses both symmetric and asymmetric encryption techniques.
- Symmetric encryption-
  A single key is used to encrypt the data and the same key is used to decrypt the encrypted data.
- Knowing the key allows the user to decrypt data that has been encrypted with the same key.
- Either a key is generated on the infected computer and send this to the attacker.
- Or request a key from the attacker before encrypting the user files.
- Advantage:
  They are generally much faster than asymmetric algorithms use small keys (typically 256-bit).
- A typical crypto ransomware has to quickly search and encrypt a large number of files, so performance is essential to encrypt files before the victim can discover the threats activities.

- Asymmetric encryption-
- Uses two keys:
  The public key is used to encrypt the data.
  The private key is used to decrypt the encrypted data.
- Advantage:
  The attacker does not need to be as protective of the public key as they would need to be with the symmetric encryption
- Drawbacks:
  Much slower than symmetric key encryption. could risk exposing the operation before the encryption is fully completed.
- The variants that use asymmetric encryption may also generate specific public-private key pairs for each infected computer.
- The location of the keys have a fundamental impact in both the schemes.



- CryptoDefense has to download a public key before encryption begins.



- CTBLocker can begin encrypting without contacting a server first as it already has a public key embedded.

Browlock Ransomware

- Browlock is different as it does not block access to the underlying operating system. To become infected, the user must navigate to a server hosting Browlock through their web browser.
- Browlock is implemented entirely using client-side web technology. The ransom page contains HTML code and images that are used to display the ransom page contents to the user.
- The page contains JavaScript code that defines an onbeforeunload function. This function is called when the user attempts to exit the page and allows web developers to ask the user to confirm that they want to exit or display final messages.

---- All activities of this computer have been recorded

A Allyour flies are enc:rypted Don't try to unloek your computer! ,A

Vouhaiv• b••n subjecr•d to vlolaitlon ot Cop)lrlght aind Rslat•d Rights Law 1v1a•o. Mus:ic. sortw:,,r•1 aina lll•gainy u'"1ng or cu,nriDuting copyr1g1>r•<l contenu., mu, lnrnnglng ArtJc1e, , Section 8, Clause 8. a1so knO'Nll as 1ne Copyright or tne Cnm1na1Cocie or unlreo States o1America
Ar1lc1e 1, Secw;,n 8, C:;,1,.1,;ie 8 or tne cr1m1n.-1 Cooe pro-,t..,ies ror a nne or lWQ tQ hundred mlnlmal wages or a deprlv1:1tlon or liberty for twOto eight year3

Vou """• 1>••n v,ewlng or e11srr1butlng prohibited Pornoor:,ptuc eor,t•nt" (Chllci Porno photos and etc were round on your computer) Thus "1olatlng article 20:2 or 1ne Crimln:,11Co,;1e or vniteCl Sl=i.lteo' or Amenta, Artti;:le '202 or 1ne Crlmma1 Code provides for a deprhratlon or liberty for four to twelve year.,

111•8"' ::,,ec•sc h:u 1>••n 1n1tt::,t•<1 trom your PC wtTnout vour .,.,,.,w,•<19• or cons•nt. your re m"y be Int•ct•d by malw;or•. thus you are "1olatlng the law on Ne,g1ect1U1use orPersonal Computer Arliere 210 ot tne Cr1m1na1 Code prov!Cles Tor a fine or up10 $100.000 anator Cleprtvatlon or 111:,eny for four 10 nine yeal"!l.
Pursuant to tne amencimenl to Cnm!n<111Cooe or Unlteo States or America or Ma,y 28, 2011, 1n1oa1:;,w 1nrnngement (IT it lo' not r·epeateo - tir:,t time) m::,y i;,e con Hde.-e<J as condltlonal In case you paytile fine of the States

To unlock your cow,puter ..ne1 :i,.,,..old ou,er 1•:111 .eons•qu•nc•s. you ....-. 01>1iq;ot•C1 t'o P"'Y '" r•••a-s• r•• or '$300, P"V"l>I• throuqn Gr••nOor MoneyP:1., tyou .....,.,. to purcn:ot:e Mon•yP::,tc .e,,,-e1. 10:sd It' wtTh S oo snd ·ntar th• cod•l,,.You c'"n buy tha cod• '"t any shop or uas sr·,.tlon Monay.-;ok is bl• .., tt•• ctor•s n;,tlonw1aa.

How do I p:,,y th• ttn• to un1oa:1<; my PC?
1 Fll"ICI :a re1:a11 1ocat1on or MoneyPak riear to you:

OO u.bl'.9-... §!

2 Pick up the MoneyPak at prepaid selection :and load It with cash at the register
A-<>-QI¥M$4.g:iwil1 1/
3 Enter your hlOneyF'ak cooe ano submit "UNLOCK YOUR PC NOW"

-.,,ucbccrwser...-lllo.. unOlockeClwinin3-12hou,,.atlerlh., mon•vlsou1in1om•81i11a·• ..ccoun1

J>1.. ase,..,.e:F1nemus11>e1>:a111wt1n1n12nou,s.Assoon ,...,:.i-110111• ol•P•o,tn• pos.,bH11')1top...,,lhenneo,cplM" All PC dat• wl!l - d•l••n•d •nd ,rtmm•l proco<l..,,•• will oeln1!la1uo .. 1ns1-,,oull'metlne1sno1oa111

Message from webpage

ALL IPC DATA WIl.I BE D£TAIlIEI) AM> CRIMINAL PROCEDURES WILL BE INITIATED AGAINS"T YOU If THE FINE WltL NOT BE PAID.

OK

Windows Internet Ewplorer

Are you sure you want to leave this page?

Message from :

AU PC DATA Will BE OCTAll'ED PH) CRIMINAL PROCEDURES Will BE INITIATED AGAINST YOU IF THE FINE Will NOT BE PAID.

Leave this page

+ tay on this page

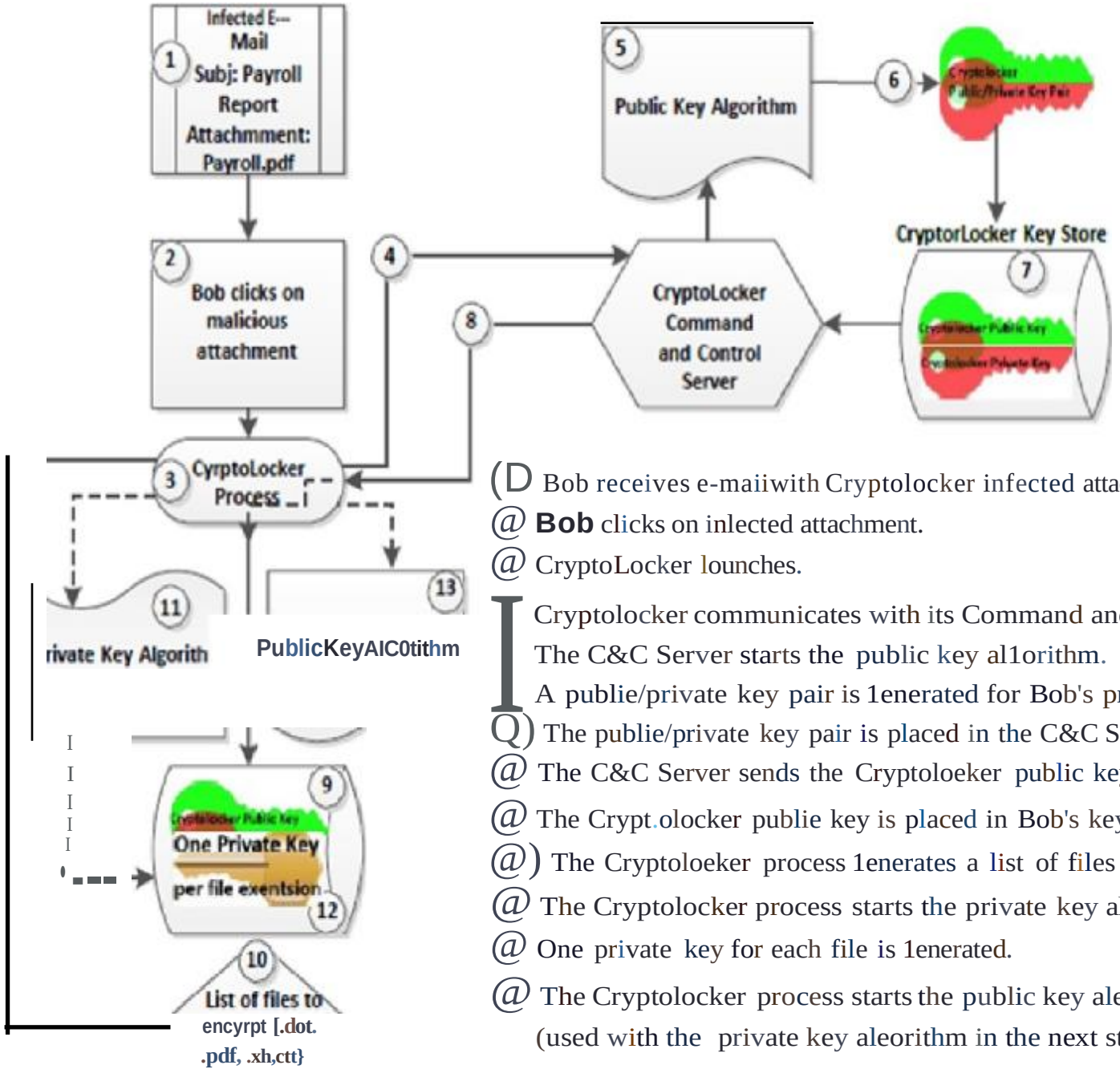
- The main Browlock page also contains multiple iframes that point to another page on the same Browlock server. This page also defines an onbeforeunload JavaScript function that displays the same message to the user.
- As the number of iframes is in the hundreds in most Browlock samples, the user may believe that they cannot exit the main Browlock page.
- The reality is that the user can actually exit if they persist in selecting Leave this page or if they close the browser process Windows Task Manager.

```
▼<html xmlns="http://www.w3.org/1999/xhtml">
  ▶<head>…</head>
  ▼<body onkeypress="return catchControlKeys(event);">
    ▼<iframe class="frame" width="0" height="0" src="us/close.html">
      ▼#document
        ▼<html>
          ▶<head>…</head>
          ▼<body style="margin:0px;padding:0px;width:100%;height:100%;">
            ▼<script type="text/javascript">
                        window.onbeforeunload = function(env){
                        var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WILL BE D
                            alert(str);
                            return str;
                        }

            </script>
          </body>
        </html>
    </iframe>
    ▼<iframe class="frame" width="0" height="0" src="us/close.html">
      ▼#document
        ▼<html>
          ▶<head>…</head>
          ▼<body style="margin:0px;padding:0px;width:100%;height:100%;">
            ▼<script type="text/javascript">
                        window.onbeforeunload = function(env){
                        var str = 'YOUR BROWSER HAS BEEN LOCKED.\n\nALL PC DATA WILL BE D
                            alert(str);
                            return str;
                        }

            </script>
          </body>
        </html>
    </iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
    ▶<iframe class="frame" width="0" height="0" src="us/close.html">…</iframe>
```

- Source code from Browlock showing multiple iframes containing functions to display ransom message popups.



(D Bob receives e-maiiwith Cryptolocker infected attachment.

@ **Bob** clicks on inlected attachment.

@ CryptoLocker lounches.

I Cryptolocker communicates with its Command and Control (C&C) Server.
The C&C Server starts the public key al1orithm.
A publie/private key pair is 1enerated for Bob's proeess.

Q) The publie/private key pair is placed in the C&C Server key stora1e.

@ The C&C Server sends the Cryptoloeker public key to Bob's Cryptolocker pro

@ The Crypt.olocker publie key is placed in Bob's key store.

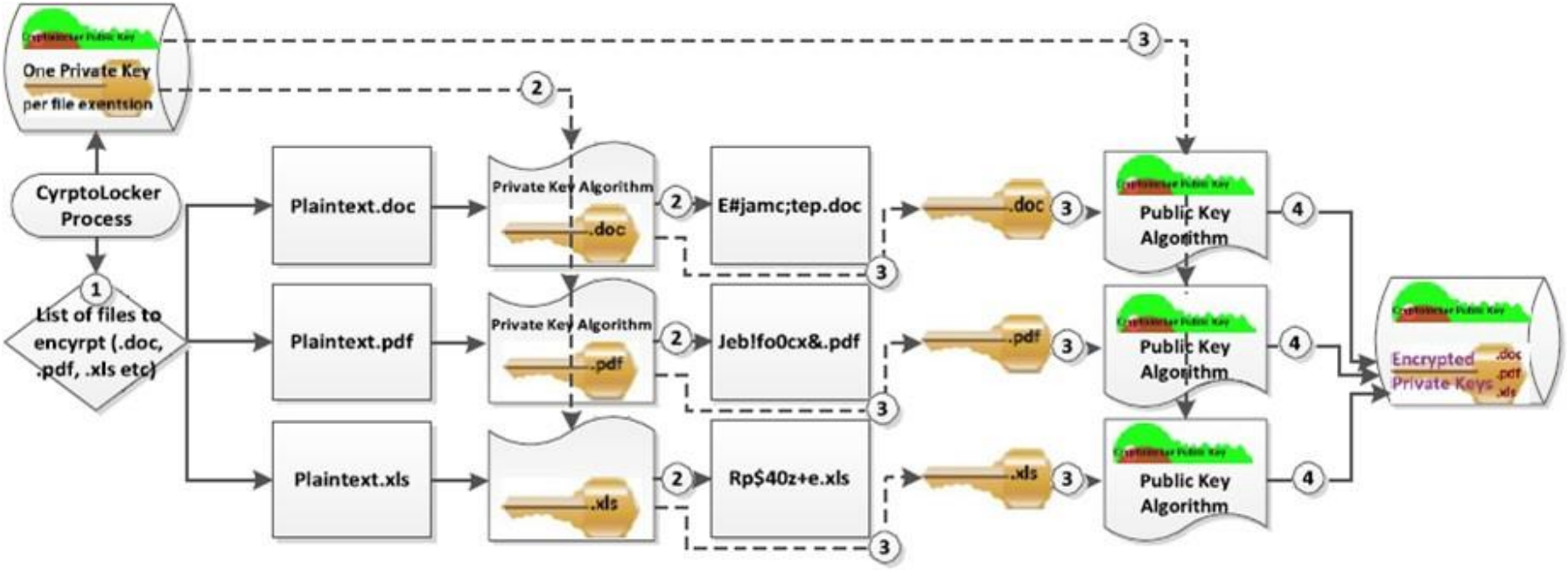
@) The Cryptoloeker process 1enerates a list of files (by extension) *to* encrypt.

@ The Cryptolocker process starts the private key al1orithm.

@ One private key for each file is 1enerated.

@ The Cryptolocker process starts the public key aleorithm
(used with the private key aleorithm in the next step.)

Cryptolocker Encryption



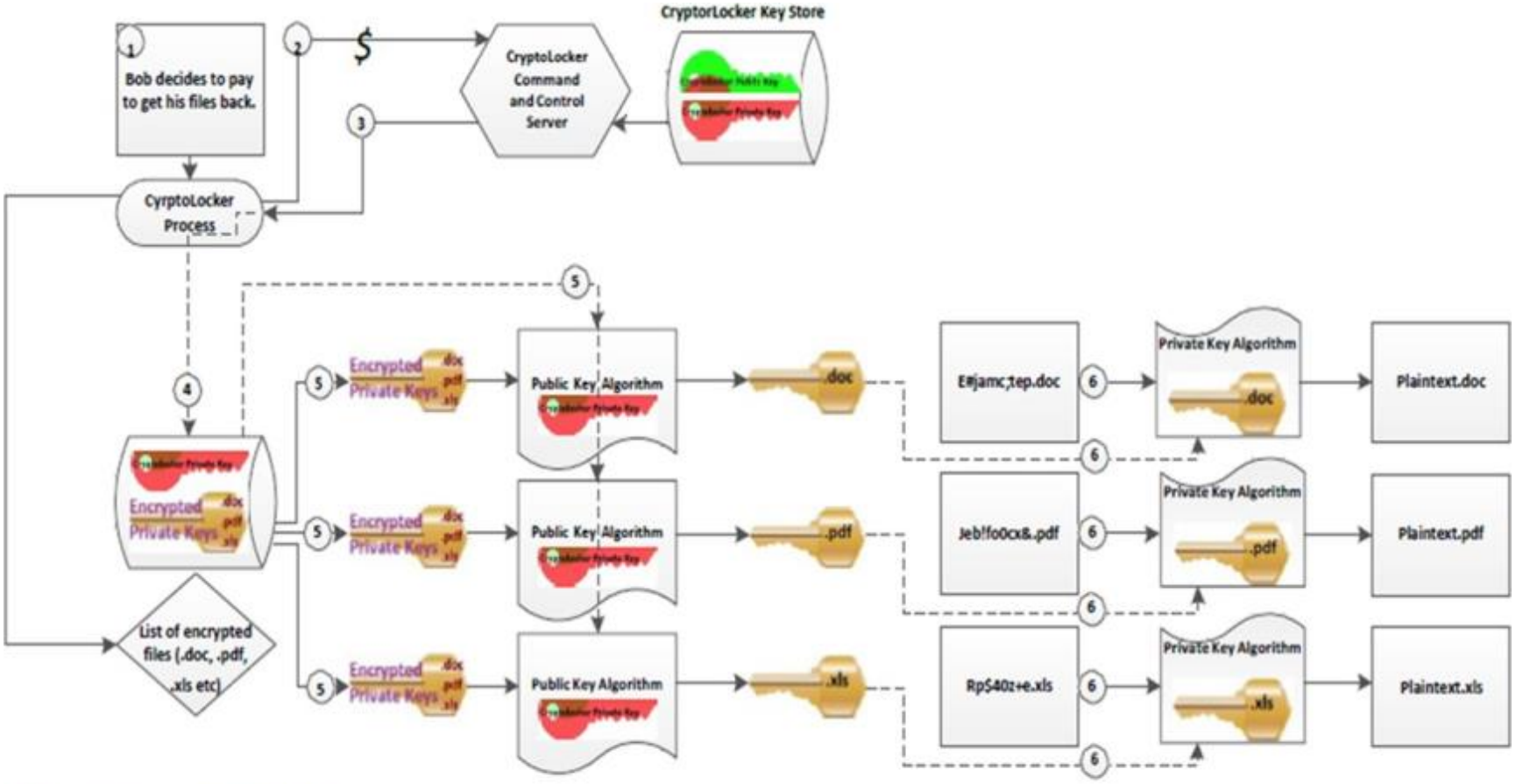
① The files to be encrypted are identified by extension.
② Each file is encrypted using the private key algorithm and the private key for the specified extension.
③ After all of the files are encrypted, each extension's private key is encrypted using the public key algorithm and the CryptoLocker C&C public key.
④ The encrypted keys are stored in the local key store.

Cryptolocker Infection

- When CryptoLocker infects a computer, it attempts to connect with one of several preconfigured malicious websites (generically known as a Command and Control (C2) server).
- The C2 server generates an RSA public/private key pair, and passes the public key to the CryptoLocker malware on the infected computer.
- CryptoLocker then generates the AES private key algorithm to encrypt files on the target computer, targeting specific, common extensions (e.g. .exe, .doc, .jpg, .pdf, etc.), generating a different 256-bit private key for each group of files per file extension.
- Aftereach group of files is encrypted, CryptoLocker uses the RSA public key it received from the C2 server to encrypt the AES private key that was used to encrypt the files.

- When all of the files have been encrypted, the ransomware generates a page to be displayed to the victim that indicates the price, method, and time period for payment to be made.
- If the ransom is made within the indicated time, the victim will be presented with a download screen that links to the RSA private key that will be used to decrypt the AES private keys encrypted by the RSA public key. The decrypted private keys will then be used to decrypt the associated files.

Cryptolocker Decryption



① Bob decides to get his files back.
② Bob sends the specified amount to the CryptoLocker C&C Server.
③ The C&C Server send the CryptoLocker Private Key to Bob's CryptoLocker process.
④ The CryptoLocker Private Key is placed in Bob's Key Store.
⑤ The encrypted Private Keys are decrypted using the CryptoLocker C&C Private Key and the Public Key algorithm.
⑥ The files are decrypted using the decrypted file extension Private Keys and the Private Key algorithm.

Dissecting Cryptolocker

- Analysis Overview

Type	Description
Evasion	Checking for specific image filename
Evasion	Trying to detect analysis virtual environment (guest mo
Evasion	Trying to detect analysis virtual environment (malware a
File	Modifying executable in Windows directory
File	Searching for files across mounted drives
File	Searching for files iterating over directories
Memory	Search for API functions in memory (possible shellcode)
Network	Hide network activity through code injection
Packer	Loading an embedded PE image (potential unpacking)

- Loaded libraries...

c:\wfndows\syswo'IN64\tnsvcrt.dll

c:\windows\syswow64\snsclf.dll

c:\ 'lindows\syswow64\lpk.dll

c:\windows\syswow64\kernelbase.dll

c:\windcws\syswow64\kernel32.dU

c:\windaws\svswow64\odi32.dll

c:\windows\syswow64\cryptbase

c:\windcw \sySt!lm32\wcw64,r;pu.dU

c:\windows\system32\wow64.dll

c:lwindows\system321ntdll.dll

c:\windows\system32\imm32.dll

Properties

CieneR,I | ibiiy | Securiy | Details | l'levious V<nions

Property	Vu
De ription	
Product name	M<:m«>/t® IMndow"® Open,bng s-,.t,,m
VJFTip,arryname	rlIQ'Q5Qll;l,,,,OrJ)Ql1IOQl1
File desaiption	Booe crypmgraphic API DU
In1Emal name	ayplbase.dll
Original fil<nome	a -,plbase.dll
ProduclversKlfl	6.1.7057.0
Fila W!lrlion	6.1.7057.0 (wifVTlllirL090J05-2000)

□x742100□□

0x74280000

0x77910000

0x76f7000'.l

Mitigation strategies And Solutions

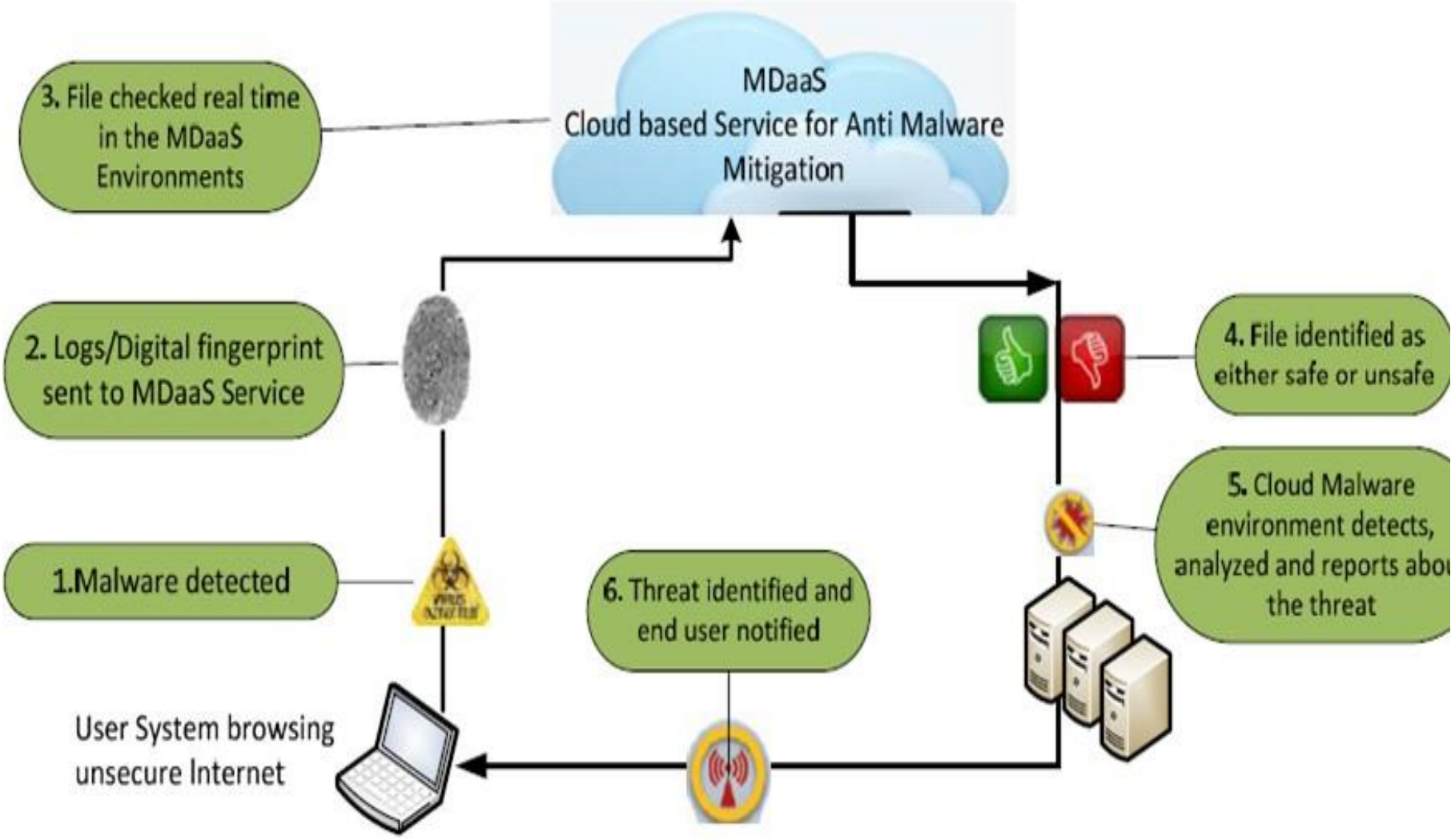
- Educate and inform.
- Patching software:
  You dont have to enter in the URL of the malicious website yourself. Your browser could be redirected to the malicious site by a malvertisement or hidden iframe even by simply visiting well-known and legitimate sites.
- Some of the most common software is also the most targeted through exploit kits so use automatic updates if possible.
- Adobe:
  Users of Adobe Acrobat/Reader, Flash Player, and Shockwave Player.
- Microsoft: Users of Microsoft products such as Windows, Office, and Internet Explorer.

- Use a layered defense approach.
- A multi-layered defense strategy addresses each of these attack vectors at various points in an organizations infrastructure.
- For example, using a messaging protection solution could provide protection against many messaging-based attacks before the malicious message could even reach a user at the endpoint.
- Network protection could help prevent users from visiting malicious websites and file-based protection could block malicious code from executing at the endpoint computer.
- Eachlayer creates an extra obstacle for the malware to overcome, making it much more difficult for the ransomware attack to be successful.

- Advice for mobile/tablet device users:
  Install suitable mobile security solution.
- Be wary of installing apps from untrusted sources such as unofficial markets and messages or websites offering free apps for installation.
- When installing a new app, check the list of permissions to see if it is appropriate for the app that you are installing.
- Enable a remote-wipe facility to allow you to delete all data and perform a full factory reset on the mobile/tablet device even if it is locked by ransomware. This feature will also come in handy should the device be lost or stolen.
- Use network protection:
  Ransomware infections today are a result of malicious network traffic.
  Prevents drive-by-download attack.
  Prevents users from accessing malicious websites.
  Prevents network encryption.
- Make backups.

- Shadow Copies:
  Sometimes crypto ransomware can have weaknesses in their implementation which could allow victims to recover at least some of their files without paying.
- For example, Windows can be set up to make recovery points at regular intervals. These backups are called shadow copies. If this service is enabled and if a crypto ransomware has not interfered with this feature, it is possible recover some files using this method.
- File recovery software:
  Another point worth noting is that when a file is deleted in Windows, the contents of the file are not scrubbed from the physical disk itself.
- Instead, the entries defining the file are removed from the disk allocation tables, freeing up the space. The original data in the freed space is not overwritten until a new file is written to the same space on the disk.
- No bullet-proof solution.

New Malware Solution Proposed



Advantages Of Cloud Based Malware Scanner System

- The cloud based malware scanner system has pay-as-you-use services running over virtual platforms over the internet.
- Global reach anywhere remotely.
- Not being limited by hardware or computing power.
- Ensuring highly scalable setup.
- Provide antimalware services when required over periods of time, indexing and analyzing huge database and malware logs.
- Service can be further made customizable for the end users.
- Provides them the ability to upload and update logs and even grab image of the infected systems.
- Inform each user as soon as a new malicious payload is detected.