

# RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M03

## FIGHTING A RANSOMWARE BLINDFOLDED

**Renato Marinho**

Chief Research Officer  
Morphus Labs  
@renato\_marinho



#RSAC

# The Incident Report



- Sep 7<sup>th</sup> 09pm
  - The Brazilian branch of a 9,000 employees multinational company with HQ in India and subsidiary in US reported us the incident and asked for help
  - Not much details – apparently yet another Ransomware incident
  - Incident response schedule for the next morning

# Before we begin



- Sep 8<sup>th</sup> 8:00am
  - The “good” news: IT Manager was reported during the night that **the whole company was impacted** – not just the Brazilian branch
  - Management statement: the objective is to **recover the affected assets as soon as possible**
  - Each subsidiary should respond for its own incident and **share the findings** with each other
  - **Do not pay** the ransom

# Before we begin



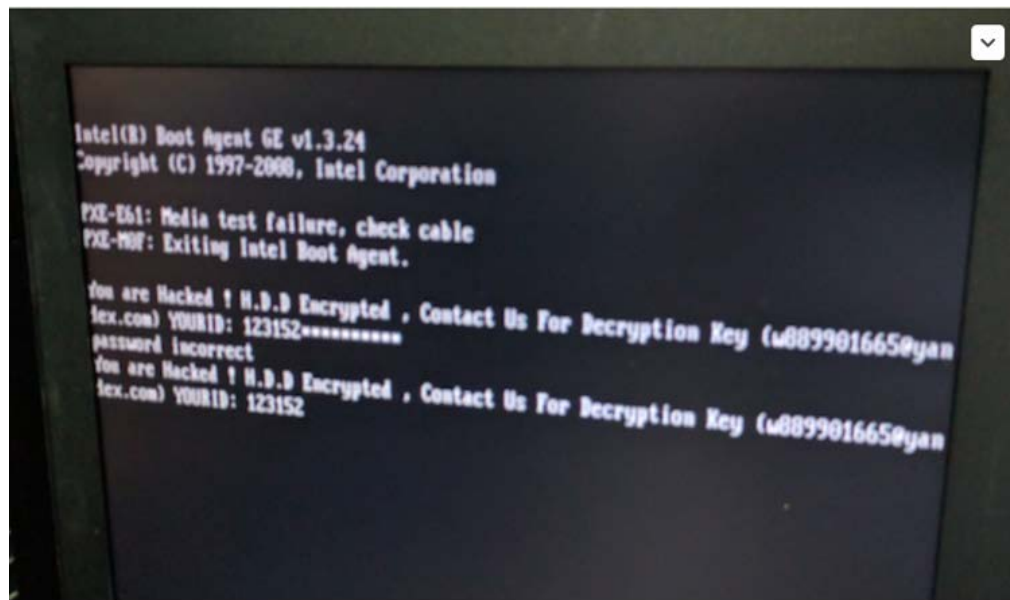
- Sep 8<sup>th</sup> 8:00am
  - Is there a backup?
    - “Just data and not updated. **Better trying to decrypt**”
  - How other subsidiaries are dealing with the problem?
    - India: 8,5 hours time zone difference;
    - They were overwhelmed trying to solve their own problem and **didn't answered our questions**;
  - Our suggestion: **do not start remediation before scope the incident**. Give us time to analyze before start the restauration.



# The odd message



- Sep 8<sup>th</sup> 8:30am



# Web search: what are we dealing with?



- Sep 8<sup>th</sup> 08:30am

## Malwr - Malware Analysis by Cuckoo Sandbox

<https://malwr.com/.../Yzl4ZTl3NjAxYjNmNDNjZDlmZjhiMjlxM...> ▼ Traduzir esta página

29 de ago de 2016 - File Name, 141.exe. File Size, 2415104 bytes. File Type, PE32 executable (console) Intel 80386, for MS Windows.

Você visitou esta página 2 vezes. Última visita: 07/09/16

# Could it be a Petya variant?



- Sep 8<sup>th</sup> 08:40am – 12:30pm
  - Trying to bypass Ransomware boot block: first try

A screenshot of a terminal window on a Linux system. The prompt is 'root@ubuntu: /tmp'. The output shows 'TestDisk 7.0, Data Recovery Utility, April 2015' by Christophe GRENIER. It lists a partition: '2 P HPFS - NTFS' with size '7711' and other details. An error message states 'Can't open filesystem. Filesystem seems damaged.' Below this, there is a 'Quit' button and a prompt to 'Quit this section'. Finally, several 'mount' commands are shown, all indicating that the specified device is already mounted or busy.

```
root@ubuntu: /tmp
TestDisk 7.0, Data Recovery Utility, April 2015
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

2 P HPFS - NTFS              7711   0  1 70264 254 32  510440640

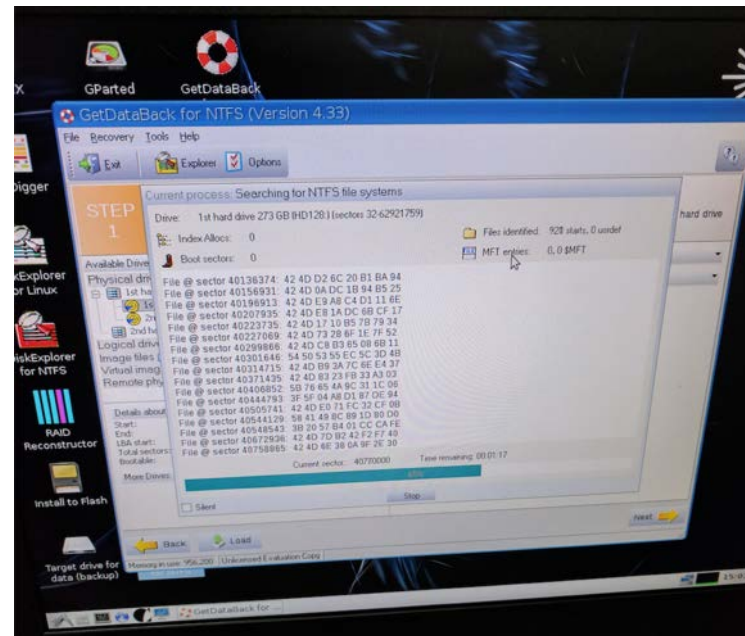
Can't open filesystem. Filesystem seems damaged.

Quit
Quit this section
root@ubuntu:~# mount /dev/sda1 /media/hd
mount: /dev/sda1 is already mounted or /media/hd busy
root@ubuntu:~# mount /dev/sda2 /media/hd
mount: /dev/sda2 is already mounted or /media/hd busy
root@ubuntu:~#
```

# Carving: anybody in there?



- Sep 8<sup>th</sup> 1:00pm – 4pm
  - Filesystem carving – second try





# Carving: anybody in there?



- Sep 8<sup>th</sup> 1:00pm – 4pm
  - Filesystem carving – third try

```
Directory of C:\

08/06/33 06:41p da-h--- 2225935047 0|0ÿtÿ#Ñ.º=€
02/15/96 05:00p d-rhs--- 1782796152 m¹±\6|/€..Y0Δ
01/01/01 12:00a ---h--- 1327671292 fd"⟨z~c|..Ç$¶
≡»Π.¹.gné12:00a d---s--- 177168155 ä
08/03/73 06:48a d--h--- 3490559842 af¹rëaæ¹.

01/01/01 12:00a dar-s--- 826846520 ¶c-¹xô"Δ.Δc¹
06/11/56 01:53p -arhs--- 210861450 æE&|É¶.¹râ
07/27/81 02:32a d---s--- 4216726275 g||xt±^µV..JQ
01/01/01 12:00a dar-s--- 2527542703 kooθlu¹r.τ±
01/01/01 12:00a --r--- 2635697717 Üaj²s#av.¶R
11/16/48 02:14p da----- 3119649718 â|k<ò||9'.!)=
01/01/01 12:00a darhs--- 476270060 -1L||¹æ.θω.
02/11/16 05:47p da----- 612764249 ¶f&|f±r.30i
01/01/01 12:00a -ar-s--- 2438566058 o|e±æâV.n||0
03/13/13 09:01a -a-hs--- 3488058213 µUZH±!!..½jE
10/14/15 10:30a d-rhs--- 3543976326 >úrFΠ θc.f⁴x
06/17/05 02:20a darh---- 4004980456 θ°σMα&?-?..âiM
01/01/01 12:00a da--s--- 2462560808 FíiQ-µη<.j#
07/18/03 11:30a -ar-s--- 4204654839 âDq¹d0k-.ywt
s0$ü.¹j0 09:27p d--hs--- 2270395557 j²
01/01/01 12:00a da--s--- 3641743886 α0¹±+3R&.iP0
12/04/59 05:06p -arh---- 2128257667 '¹¹µ¹Lj+grδ
11/02/33 09:23a -arhs--- 3518669801 Δ-εSS<u.²n¹
01/17/56 05:09p -a----- 1890187249 8s||²²µ||.r<8
01/01/01 12:00a -a-hs--- 3767504727 r¹>pf¹äV.∇α¹
03/04/34 02:03p d---s--- 193661995 r0c

More: ENTER=Scroll (Line) SPACE=Scroll (Page) ESC=Stop
```

# Feeling like fighting a ransomware blindfolded



- Sep 8<sup>th</sup> 5pm
  - No encrypted data to analyze
  - No malware sample
  - No e-mail to look for possible phishing – e-mail server also encrypted
  - No Internet connection – sharing my smartphone 4G
  - No Google results

# More pressure to restore



- Sep 8<sup>th</sup> 5pm
  - It was almost 5pm and the news about the encrypted data augmented the pressure to restore the environment;
  - As the administrative network and systems were down, no business could be done;
  - Almost at the same time, the person verifying the backup assured us that the data was ready;
  - Part of servers released to be restored

# AV Full Scan – Is there a hope?



- Sep 8<sup>th</sup> 6pm
  - AV signatures updated
  - All machines powered on
  - Full scan started



# Contacting the crook



- Sep 9<sup>th</sup> 00:10am
  - “Hey, I got infected”

## Computer hacked



**Max Wilson** maxwilsonw@yandex.com

09.09.16

1 recipient ▾

Hello,

I got a message in my computer informing to contact you. I can't get my files.

# Contacting the crook



- Sep 9<sup>th</sup> 00:20am
- **Good SLA!**



andy saolis <w889901665@yandex.com>

Your HDD Encrypted By AES 2048Bit

send 1BTC Per HOST to My Bitcoin Wallet , then we give you Decryption key For Your **Server** HDD!!

My Bitcoin Wallet Address : **1NlnMNMPbxWeMJVtGuobnzWU3WozYz86Bf**

We Only Accept Bitcoin , it's So easy!

you can use Brokers to exchange your money to BTC ASAP  
it's Fast way!

Here:  
<https://localbitcoins.com/>

if You Don't Have a Account in Bitcoin , Read it First :

<https://bitcoin.org/en/getting-started>

bitcoin Market :  
<https://blockchain.info/>  
<https://www.okcoin.com/>  
<https://www.coinbase.com/>  
<https://bitcoinwallet.com/>

# How many victims?



- Sep 9<sup>th</sup> 00:25 am

**BLOCKCHAIN**  
info

Página InicialchartsEstatísticasmercadosAPICarteira

Portuguê

## Endereço Bitcoin


Endereços são identificadores que pode usar para enviar bitcoins para outras pessoas.

Resumo	
Endereço	1NLnMNMPbxWeMJVtGuobnzWU3WozYz86Bf
Hash 160	ea1866e8a64f7f5062abd73e345c0050c7729ebe
Ferramentas	<a href="#">Análise de Correlação</a> - <a href="#">Tags similares</a> - <a href="#">não gastos</a> <a href="#">Saídas</a>

transações	
Nro. de Transações	6
Total Recebido	4 BTC
Saldo final	0 BTC

Solicitar Pagamento

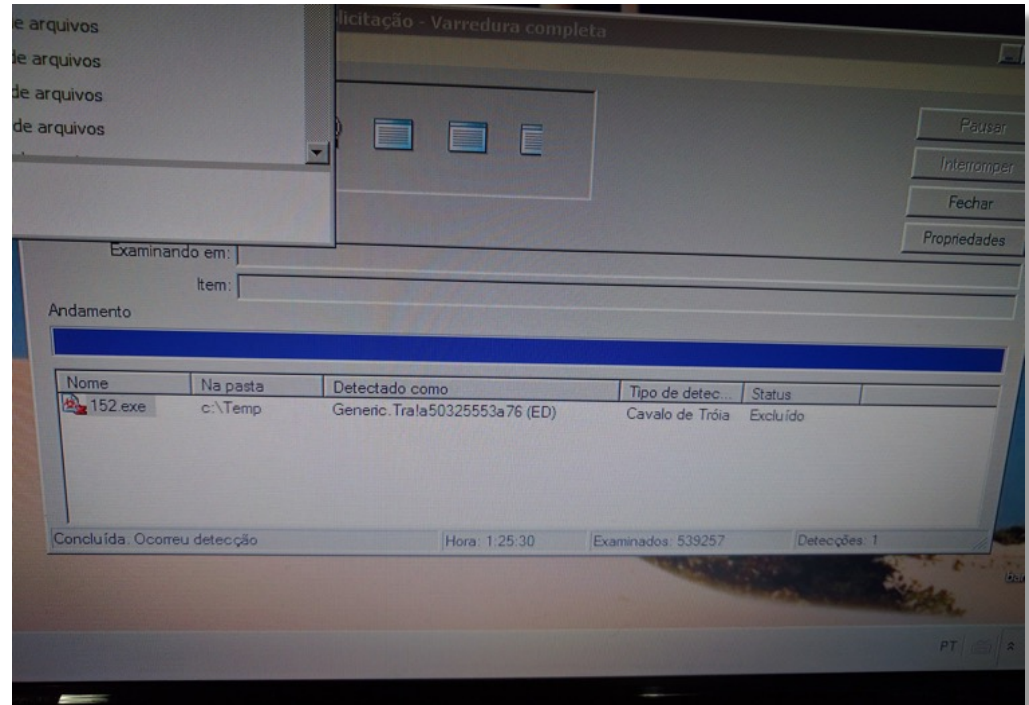
botão de doação



# Suspect file found



- Sep 9<sup>th</sup> 00:30 am
  - - "Hey Renato: a suspect file was found"
  - - "Great! Where it is?"
  - "The AV deleted it..."
  - "Awesome..."





# Be the full-scan

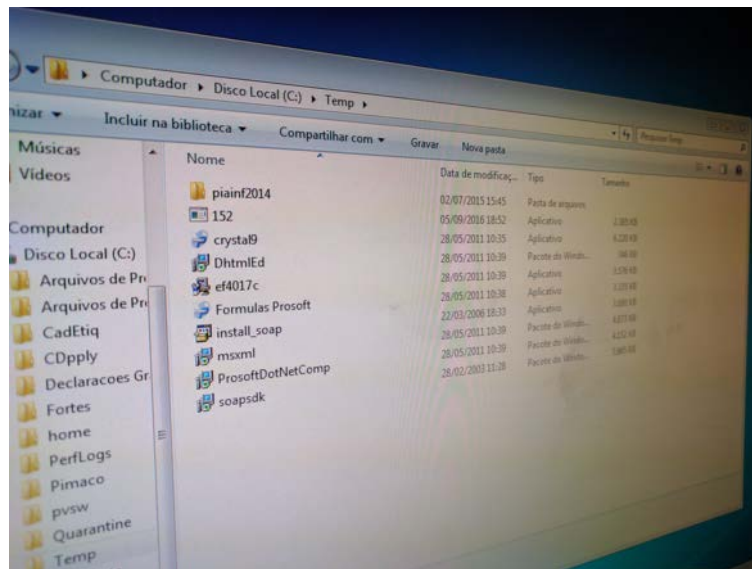


- Sep 9<sup>th</sup> 00:40 am
  - AV, take a nap!
  - Manually looking for the suspect file

# Be the full-scan



- Sep 9<sup>th</sup> 01:00 am
  - Suspect file found!
  - 152.exe on c:\temp folder



# Sleeping is for the weak



- Sep 9<sup>th</sup> 01:10 am
- **Static and dynamic** preliminary sample analysis
- Wow, there is a match: same ransom message found!

```
Add this file to the keyfiles list?  
ymbols on this layout  
You are Hacked ! H.D.D Encrypted , Contact Us For Decryption Key (w889901665@yandex.com)  
YOURID: 123152  
You must restart your computer before the new settings will take effect.  
  
Do you want to restart your computer now?
```

# Let's call it a day



- Sep 9<sup>th</sup> 01:40 am
  - Samples collected
  - Machine preserved for further analysis
  - Remaining servers released to restoration



# Further analysis



- Sep 10<sup>th</sup> 01pm - 10pm
  - Dynamic analysis: let's poke it a bit

The screenshot shows a debugger window with assembly instructions on the left and a command prompt window in the center. The command prompt shows the execution of `dcccon.exe -enum` and `dcccon.exe -info pt0`, displaying disk information for `pt0`.

```
401000: push ebp
401001: mov ebp, esp
401003:
401006:
401009:
40100a:
40100f:
401012:
401015:
401018:
40101b:
40101c:
401021:
401024:
401027:
40102a:
40102b:
401030:
401033:
401036:
40103d:
40103f:
401042:
401045:
401048:
40104b:
40104e:
401050:
401053:
401056:
401059:
40105c:
40105f:
401062:
401064:
401066:
401069:
```

Command Prompt Output:

```
C:\DC22>dcccon.exe -enum
volume | mount point | size | status
-----|-----|-----|-----
pt0 | C: | 39.9 GB | mounted, boot, system
pt1 | D: | 0 bytes | unmounted

C:\DC22>dcccon.exe -info pt0
Device: \Device\HarddiskVolume1
SymbolicLink: \??\Volume{11788658-88c2-11e5-bf9c-806e6f6e963}
Mount point: C:
Capacity: 39.9 GB
Status: mounted, boot, system
Cipher: AES
Encryption mode: XTS
Pfcns.2 prf: HMAC-SHA-512
Encrypted portion: 100.000%

C:\DC22>
mov eax, [ebp+0x10]
add eax, [ebp+0x4]
movss ecx, byte [eax]
add ecx, [ebp+0xc]
mov edx, [ebp+0x8]
add edx, [ebp+0x4]
mov [edx], d
jmp 0x0103f
mov eax, [ebp+0x8]
mov eax, ebx
```

The screenshot shows the 'DefragmentService Properties (Local Computer)' dialog box. The 'General' tab is selected, showing the service name 'DefragmentService', display name 'DefragmentService', and description. The path to the executable is 'C:\D\152.exe 123456'. The startup type is set to 'Automatic'. The service status is 'Stopped'. There are buttons for 'Start', 'Stop', 'Pause', and 'Resume'. The 'Start parameters' field is empty.

DefragmentService Properties (Local Computer)

General Log On Recovery Dependencies

Service name: DefragmentService

Display name: DefragmentService

Description:

Path to executable: C:\D\152.exe 123456

Startup type: Automatic

Service status: Stopped

Start Stop Pause Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK Cancel Apply

# Documenting the findings



- Sep 10<sup>th</sup> 10pm – 2am
  - We prepared a technical report, with Indicators of Compromise and malware modus operandi, and shared with other subsidiaries
  - Other subsidiaries thanked and told us that they were going try to locate the same artifact on their network – no feedback received

# Beach: coconuts with ransomware



- Sep 11<sup>th</sup> 9am – 12pm
  - I couldn't delay anymore going to the beach with my family
  - But my thoughts were somewhere else ☺



# Writing the article



- Sep 11<sup>th</sup> 01:00pm
  - Writing the article
  - Mamba: why “Mamba”?

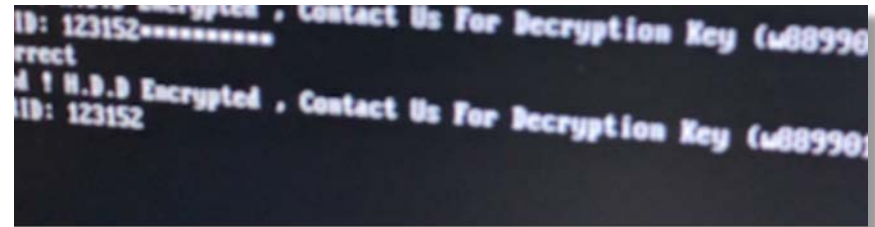




# Getting community involved



- Sep 12<sup>th</sup> 09:00am
  - Reaching SANS, CERTs and security players (Palo Alto, Fireeye, Trend Micro)



## Mamba: The new Full Disk Encryption Ransomware Family Member

Published on September 12, 2016



**Renato Marinho**  
Director at Morphis Segurança da Informação



108



13



56



Renato Marinho, Morphis Labs

# Media coverage



## ISC StormCast for Tuesday, September 13th 2016

A daily summary of network and system security news from the SANS Internet Storm Center

Author: [Johannes B. Ullrich, Ph.D.](#)

Created: Tuesday, September 13th 2016

Length: 6:15 minutes



threatpost

CATEGORIES

FEATURED

PODCASTS

VIDEOS



Welcome > [Blog Home](#) > [Malware](#) > Mamba Ransomware Encrypts Hard Drives Rather Than Files



MAMBA RANSOMWARE ENCRYPTS HARD DRIVES RATHER THAN FILES

cyberwire about issues interviews events podcasts videos glossary sponsors

### The CyberWire Daily Podcast 9.21.16

Russian hackers hit German political targets. Vulnerability Cisco discovered while investigating Shadow Brokers' leaks exploited in the wild. New strains of ransomware are out. The Air Force Association is taking up cyber in its annual meetings. The Internet-of-moving things. And North Korea parts the curtain in front of its domains.

In today's podcast, we hear about Russian hackers turning their attention to German political targets as well as politicians in the US. The son-of-Shadow Brokers vulnerability Cisco discovered is being exploited in the wild. New strains of ransomware are out—Mamba is as dangerous to networks as its namesake is to human tissue. The Air Force Association is taking up cyber in its annual meetings. The Internet-of-moving things handles disclosures. Matthew Green from Johns Hopkins University's Information Security Institute discusses the disclosures of backdoors. University of Maryland's Jonathan Katz talks about new security standards adopted by Google. And North Korea parts the curtain in front of its domains.

[Download](#)

Recorded Future

Get trending information on hackers, exploits, and vulnerabilities every day for FREE with the Recorded Future Cyber Daily. [Sign up today.](#)

October 5-6, 2016, Washington, DC The fifth annual RSAC (Ransomware Summit) is a must-attend event.

SECURITYWEEK NETWORK: Information Security News | Infosec Island | Suite and Spooks

## SECURITYWEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 20

The new malicious program that combines the two is called HDDCryptor, but also known as HDD Cryptor or Mamba ransomware. The threat was spotted for the first time in the beginning of this year, although it caught the attention of researchers in the past several weeks after was featured in a larger campaign.

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Manage

Home > Malware

### HDDCryptor Leverages Open Source Tools to Encrypt MBR

By [Isaac Arghire](#) on September 21, 2016

[Tweet](#)

HACKREAD SECURITY IS A MYTH

HACKING NEWS • TECH • CYBER CRIME • HOW TO • CYBER EVENTS • SECURITY • SURVEILLANCE • GAMING • SCIENCE • VIRAL

YOU ARE 40% HACKED

CYBER CRIME [BYPASSING CENSORS](#)

CYBER CRIME [BYPASSING CENSORS](#)

SUBSCRIBE TO OUR NEWSLETTER

Enter your email... [SUBSCRIBE](#)

The host of all Ransomware Mamba Encrypts Entire Hard Drive

Mamba ransomware is currently targeting Windows users in Brazil, India...

University Student Arrested for hacking computer and changing grades

Hacking your school's computers is no ordinary feat and it...

CYWARE

CYBER SECURITY

## Everything You Should Know About Mamba Ransomware

September 23, 2016 • 0 Comment • Sidarth Trisal • 1 min read

MORPHUS LABS

RSAC Conference 2018

# Unfortunately, another big incident



**PCWorld**  
FROM MSN

Home / Security

## San Francisco's Muni transit system slammed by ransomware

The ransomware attacker is said to be demanding \$73,000.

**International Business Times**

## San Francisco's transport system held to ransom in cyberattack giving passengers free rides for Thanksgiving

Over 2,000 systems were reportedly hit by a variant of the H20Crypt ransomware.

**threatpost**

## HACKERS MAKE NEW CLAIM IN SAN FRANCISCO TRANSIT RANSOMWARE ATTACK

**Forbes**

## Ransomware Crooks Demand \$70,000 After Hacking San Francisco Transport System

San Francisco Metro System Hacked with Ransomware, Resulting in Free Rides

**CNBC**

## Hackers are holding San Francisco's MUNI light-rail system for ransom

Andrew Lipsitz  
12 hours ago

**The Hacker News**  
Security in a serious way

## San Francisco Metro System Hacked with Ransomware, Resulting in Free Rides

Les transports en commun de San Francisco rançonné

**THE VERGE**

## Hackers are holding San Francisco's system for ransom

"You Hacked, ALL Data Encrypted"

by Andrew Lipsitz | @AndrewLipsitz | Nov 27, 2016, 4:16pm EST

**Ransomware-angreb holder San Franciscos transportsystem som gidsel for en halv million**

Et ransomware-angreb netop mod San Franciscos transportbetjeb Muni gjorde, at brugerne rejste gratis i weekenden. Hackerne kræver, at Muni betaler en løsesum på over en halv million kroner for igen at få fuld adgang til deres system.

**CBS SF Bay Area**

## Cyber Attackers Hack Muni's Fare System In San Francisco

"You Hacked, ALL Data Encrypted," was the message at SF Muni stations across the city. Cate Caughran reports passengers were getting free rides all day on Saturday.

**FORTUNE**

## Hackers Threaten to Release 30GB of Stolen Data From San Francisco's Municipal Railway



# Apply what you have learned today



- Properly scope the incident before start remediation to make sure you got rid of the threat
- Look around during an incident response: there is always a trace on the environment
- Collect and retain operating system and service logs out of your servers: you may not have access to them during a crisis
- Back up your system and application configuration additionally to data: rebuilding and back them online may consume lots of time
- Establish and exercise an incident communication plan: this may speed up your incident response



**RSA**®Conference2018



#RSAC

**QUESTIONS?**

[rmarinho@morphuslabs.com](mailto:rmarinho@morphuslabs.com)

[@renato\\_marinho](https://twitter.com/renato_marinho)