SESSION ID: SEM-M03

FIGHTING A RANSOMWARE BLINDFOLDED

Renato Marinho
Chief Research Officer
Morphus Labs
@renato_marinho
Sep 7th 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 8th 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 8th 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 8th 8:30am
Web search: what are we dealing with?

- Sep 8th 08:30am

Malwr - Malware Analysis by Cuckoo Sandbox
https://malwr.com/.../YzI4ZTI3NjAxYjNmNDNjZDImZjhiMjIxM...

29 de ago de 2016 - File Name, 141.exe. File Size, 2415104 bytes. File Type, PE32 executable (console) Intel 80386, for MS Windows.
Vocês visitaram esta página 2 vezes. Última visita: 07/09/16
Could it be a Petya variant?

- Sep 8th 08:40am – 12:30pm
  - Trying to bypass Ransomware boot block: first try
Carving: anybody in there?

- Sep 8\textsuperscript{th} 1:00pm – 4pm
- Filesystem carving – second try
Carving: anybody in there?

- Sep 8th 1:00pm – 4pm
- Filesystem carving – third try
Feeling like fighting a ransomware blindfolded

- Sep 8th 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 8th 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\textsuperscript{th} 6pm
  ● AV signatures updated
  ● All machines powered on
  ● Full scan started
Contacting the crook

- Sep 9th 00:10am
- “Hey, I got infected”

Computer hacked

Max Wilson  maxwilsonw@yandex.com
1 recipient  09.09.16

Hello,

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

- Sep 9th 00:20am
- Good SLA!

---

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: 1L1nMNMPbxWeMJVtGuabnzWU3WozYs85Bf

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 9th 00:25 am
Suspect file found

- Sep 9th 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\textsuperscript{th} 00:40 am
  - AV, take a nap!
  - Manually looking for the suspect file
Be the full-scan

- Sep 9th 01:00 am
- Suspect file found!
- 152.exe on c:\temp folder
Sleeping is for the weak

- Sep 9th 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?

Symbols 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 9th 01:40 am
  - Samples collected
  - Machine preserved for further analysis
  - Remaining servers released to restoration
Further analysis

- Sep 10th 01pm - 10pm
- Dynamic analysis: let’s poke it a bit
Documenting the findings

- Sep 10th 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\textsuperscript{th} 9am – 12pm
  - I couldn’t delay anymore going to the beach with my family
  - But my thoughts were somewhere else 😊
Writing the article

- Sep 11th 01:00pm
  - Writing the article
  - Mamba: why “Mamba”? 
Getting community involved

- Sep 12th 09:00am
  - Reaching SANS, CERTs and security players (Palo Alto, Fireeye, Trend Micro)
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. Ulrich, Ph.D.
Created: Tuesday, September 13th 2016
Length: 6:15 minutes

MAMBA RANSOMWARE ENCRYPTS HARD DRIVES RATHER THAN FILES

The new malicious program that combines the two is called HDDCryptor, but also known as HDD Cypriot 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 it was featured in a larger campaign.

The number of all Ransomware Mamba Encrypted Crimeware
Mamba ransomware is currently targeting Windows users. In fact, India...

University student targeted for hacking computer and downloading photos
Hacking your school's computers is not only illegal but also...

CYWIRE
Everything You Should About Mamba Ransomware
September 13, 2016; 1:07; 1:07
1 min read

MORPHUS LABS

RSAC 2018
Unfortunately, another big incident
Apply what you have learned today

- Properly scope the incident before start remediation to make sure you got hid 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
- Stablish and exercise an incident communication plan: this may speed up your incident response
QUESTIONS?

rmarinho@morphuslabs.com
@renato_marinho