Fighting Ransomware Blindfolded

Renato Marinho, Morphus Labs
• Chief Research Officer at Morphus Labs;
• Incident Handler no SANS Internet Storm Center (ISC);
• Master and PhD candidate in Applied Informatics;
• 16 years+ of hands-on experience in the field;
• CISSP, CRISC e PMP;
• Computer Forensics professor at Fortaleza University (Brazil);
• Last seen at Ignite Cybersecurity Vancouver 2017; SANSFIRE 2017; Security BSides Vienna, Delaware and São Paulo; Mind the Sec 2017; WSKS Portugal and Brazilian CSIRTs Forum.

@renato_marinho
linkedin.com/in/renatomarinho
Impacted Company

• Multinational with HQ in India and subsidiaries in Brazil and US;
• 9,000 employees worldwide;
• Production and selling goods;
• Network segmented in operation and administrative zones. Operation managed by HQ and administrative managed by each subsidiary;
Management Structure

• Bottom-up management structure:
  – Brazilian IT Manager (the person that first contacted us) Brazilian IT Director, Global Security Officer, Global VP for IT, President.
Incident Detection

- IT Director: September 7\textsuperscript{th} had problem loading e-mails;
- IT team not operational due to the holyday;
- IT Manager went personally to the company’s facility, confirmed the incident and reported IT Director;
Incident Report

• IT Director:
  – Power off all company’s Internet links to avoid data leak;
  – Contact a specialized company to help dealing with the problem;
  – The IT Manager should communicate the problem internally (using a personal E-mail address as the company’s was down);
  – After informed the criminals asked for money in return for the data, he stated that the company should not pay anything, regardless of the problem.
Incident Report

• IT Manager contacted us:
  – September 7\textsuperscript{th} 9PM;
  – Gave us an overview of the incident and its impact (I found quite strange the ransomware message);
  – Scheduled the incident response for the next morning 8am.
Understanding the Incident

• September 8\textsuperscript{th} 8am:
  – Meeting with IT Manager and IT Team before starting the technical activities;
Understanding the Incident

• What we got from this meeting:
  – The Global VP of IT informed that the problem wasn’t just with the Brazilian branch. Subsidiaries in US and India had also been impacted and were trying to recover;
  – Additionally, he oriented that the first objective was to recover the affected assets, establish a group of work and have someone as a point of contact for all efforts in line;
  – The VP for Brazil informed that he tried to contact the special police for digital crimes, which did not respond due to the holiday. He also recommended contacting a specialized attorney;
Additional Guidelines

• The person globally in charge of the Incident Response stated that:
  – Each subsidiary should respond for its own incident;
  – Share their findings;
  – Report the incident extent;
  – Recover the environment without paying the ransom.
Initial Assessment

• 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;
Initial Assessment

• The odd message
Web search: what are we dealing with?

Google search: 1 result

Malwr - Malware Analysis by Cuckoo Sandbox
https://malwr.com/.../Yzl4ZTl3NjAxYjNmNDNjZDlmZjhiMjIxM...
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
In the meantime

• The global VP of IT:
  – Reinforced that the main objective was recover and prevent damage;
  – Global head of Legal oriented to not contact the police and wait for additional guidelines before contacting any external entity – specially media.
Incident Status

• At this point (approx. 1PM), in summary, our situation was:
  – Company’s file e-mail and active directory servers compromised by an unknown malware;
  – No malware sample to analyze as the binary itself was encrypted amongst the company’s data;
  – It was not certain the backup contained all the data – a restore procedure was being tested in parallel;
  – No fast Internet connection to use during the incident response – I was using my 3G/4G smartphone connection;
  – It was not possible to get information from other subsidiaries;
  – Google was not helping much;
  – Pressure from company executives to restore the environment.
Negotiating more time to investigate

• Despite the company pressure to restore the servers, IT Manager asked us about the next move:
  – If we restore all the environment, we will have no chance to identify the infection vector;
  – The recovered servers could be infected by the same threat;
Negotiating more time to investigate

• IT Manager explained the reasons to do not restore to IT Director;
• IT Director agreed and gave us more time – we really don’t know if it was aligned with HQ and how much time we could have;
What are we dealing with?

Could it be a Petya variant?

Bypass Ransomware block: the first try
What are we dealing with?

Carving: anybody in there?
What are we dealing with?

Carving: anybody in there?
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 ok;

Servers released to be restored.
Fully scanning the network

- Looking for evidence on the environment;
- Contact with India again to check for AV signatures update:
  - ”We have a new AV signature to apply. We are going to send you” they told us (cooperation during the crisis not working well);
- 6pm: we manually applied the new signature and started the full scan on local network;
Contacting the crook

• 00:30
”Hey, I got infected”
Contacting the crook

• 00:40

Good SLA!
Contacting the crook

How many victims?
- "Hey Renato: a suspect file was found"
- Great! Where it is?
- "The AV deleted it..."
- Awesome...
Manually scanning the network

AV, take a nap! Be the full-scan again

Who’s your daddy: file found!

152.exe and 141.exe
Initial analysis

• Static and dynamic preliminary analysis

Not only the message was the same, but also the ID (123152). Observe that the “152” part of the ID is exactly equal the name of the binary we found!
Initial analysis

- Suspicious file found on different machines;
- Machines were not logging: no evidence how they arrived;
Report and decision to move forward

• By the next day, we prepared a technical report and shared with other subsidiaries. The objective was to collaborate and try to discover the origin of infection;
• Other subsidiaries just thanked and told us that they were going try to locate the same artifact on their network;
• Our feeling was that they were not interested in discovery the problem’s root cause, but to put operation back online;
• Although it could represent more cost to the Brazilian subsidiary, the IT Director decided to continue with the malware analysis.
Malware analysis
Get community involved

- Although we have obtained many malware details, we couldn’t find how it was initially deployed;
- We decided to write a report and ask for community collaboration;
- 12 September 2016: article published.
- Why ”Mamba”?
Get community involved

• Although we have obtained many malware details, we couldn't find how it was initially deployed;

• We decided to write a report and ask for community collaboration;

12 September 2016: article published.
Get community involved

• Started to interact with SANS ISC and AV players;
What happen next?

Phishing awareness among users

**GAP analysis coordinated with all subsidiaries**

<table>
<thead>
<tr>
<th>S.No</th>
<th>Area</th>
<th>Controls</th>
<th>Current Status</th>
<th>Gaps</th>
<th>Actions</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Policies</td>
<td>Documented Security Policies reflecting Local Privacy Laws</td>
<td>1. Policies are under WIP and yet to be shared</td>
<td>Yes</td>
<td>1. Documentation to be maintained and shared for review</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Policies</td>
<td>IT Policies</td>
<td>1. No update</td>
<td>Yes</td>
<td>1. IT Policies to be documented that address the following areas - Access Control, Backup, Access Management, IT Asset, Network, Backup and etc 2. Base templates shared by InfoSec Team</td>
<td></td>
</tr>
</tbody>
</table>
Get community involved

• Because of this work, we saw that various technologies started to detect Mamba Ransomware within their engines, which probably helped companies worldwide to protect themselves against this threat;
Get community involved

• Unfortunately, by December 2016, Mamba caused another big incident: San Francisco Metro System.