Introduction

MALWARE-TRAFFIC-ANALYSIS.NET

@malware_traffic

InfoSec Handlers Diary Blog
Disclaimer

- Things can and do quickly change
- Personal bias
Overview

• Types of malware
• Distribution methods
• Tech support scams
• Prevention strategies
Types of malware

In wide-scale distribution, we most often find:

• Information stealers / backdoors
• Malware downloaders
• Cryptocurrency miners
• Ransomware
Ransomware

malware that locks your computer or files and holds them for ransom
Ransomware

Boeing

City of Atlanta

Rockport, Maine

Baltimore County

Resurgens

1895

Atlanta, GA.

©

City of

Rockport, Incorporated

1891

OFFICIAL TOWN SEAL

Baltimore County

911

Communications

City of

Atlanta
Ransomware

In March 2018, a report released by the Department of Health and Human Services states that so far this year, at least 8 cyber-attacks employing SamSam ransomware have targeted healthcare and government organizations.
#What happened to your files?
All your files encrypted with RSA-2048 encryption, For more information search in Google "RSA Encryption"

#How to recover files?
RSA is an asymmetric cryptographic algorithm, You need one key for encryption and one key 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?
Bitcoin as payment

2017-01-01
$997

2017-12-31
$13,860
Bitcoin as payment

- 2018-01-01: $13,546
- 2018-04-20: $8,516
WannaCry

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins.
For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am CEST, Monday to Friday.

Send $300 worth of bitcoin to this address:
1Sp7UMM1goJ1pMvKpH1jCJRFdNJXj6LrLn

Check Payment
Decrypt
The image shows a screenshot from VirusTotal, a service used for scanning files for viruses and other types of malware. The screenshot is focused on a search for files related to WannaCry on April 1, 2018. The search term used is "wannacry fs:2018-04-01+". The search results show that over 1000 files were found, indicating a significant number of files infected or associated with the WannaCry attack on that date.
<table>
<thead>
<tr>
<th>Samples</th>
<th>Session</th>
<th>WildFire Verdict</th>
<th>File Size (Bytes)</th>
<th>File Type</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/20/2018 10:19:21am</td>
<td>Malware</td>
<td>348.168</td>
<td>PE</td>
<td>GandCrab</td>
<td>InitialSystemDataEnumeration</td>
</tr>
<tr>
<td>04/20/2018 10:19:15am</td>
<td>Malware</td>
<td>305.168</td>
<td>PE</td>
<td>GandCrab</td>
<td>InitialSystemDataEnumeration</td>
</tr>
<tr>
<td>04/20/2018 10:18:53am</td>
<td>Malware</td>
<td>361.992</td>
<td>PE</td>
<td>GandCrab</td>
<td>InitialSystemDataEnumeration</td>
</tr>
</tbody>
</table>

- **WanaCrypt0r**: Found 3,666 samples
- **GandCrab**: Found 16,992 samples
GandCrab

--- GandCrab V2.1 ---

Attention!
All your files documents, photos, databases and other important files are encrypted and the only method of recovering files is to purchase a private key. It is on our server and

https://www.torproject.org
We are sorry, but your files have been encrypted!

Don’t worry, we can help you to return all of your files!

Files decryptor's price is 1500 USD

If payment isn’t made until 2018-04-15 01:26:20 UTC the cost of decrypting files will be doubled

Time left to double price:

01 days 23h:58m:39s
1 DSH = $350.00

Payment amount: 4.28571429 DSH ( $1,500.00 )

1. Buy cryptocurrency DASH. Here you can find services where you can do it.
2. Send 4.28571429 DSH to the address: XwYcEZpXHS8wigaf7addp7gmJKEYsyVwnb
Gandcrab

1 BTC = $7,864.50

Payment amount: 0.21934007 BTC ($1,500.00 + 15.0%)
A new ransomware called RansSIRIA has been discovered by MalwareHunterTeam that encrypts your files and then states it will donate your ransom payments to Syrian refugees.
In wide-scale distribution, we most often find:

- Information stealers / backdoors
- Malware downloaders
- Cryptocurrency miners
- Ransomware
Up next...

- Types of malware
- Distribution methods
- Tech support scams
- Prevention strategies
How is malware spread?

- Email
- Social media
- The web
- Attackers breach networks and drop malware
Email is the most common method criminals use to send malware.
Distribution through Email

These emails contain:

- Archives with malware executables
- Microsoft Office documents
- RTF documents that exploit Microsoft Office
- Archives with other types of files
- Links to malware
Dear Customer,

You have received a HelloFax

Date and Time: 04/19/2018 08:44 AM
Number of pages: 4

Personal reference number: MGH757448K.

Download Your Fax
http://ilovepatchouli.com?eit4i=SQVVXUNZHQSH3LUw
Distribution through Email

What do you want to do with invoice_319872.doc?

Size: 219 KB
Type: Microsoft Office Word 97 - 2003
From: 16646.com

- Open
  The file won’t be saved automatically.
- Save
- Save as

Cancel
Distribution through Email

Security Warning: Macros have been disabled. Options...

This document is protected

2. If this document was downloaded from your email, please click "Enable Editing" from the yellow bar above.

3. Once you have enabled editing, please click "Enable Content" from the yellow bar above.
Distribution through Email

CVE-2017-0199
CVE-2017-8759
CVE-2017-11882
Enviada do meu iphone via whatsapp
Hora: 07:40 mn

Em anexo segue histórico de conversas e Fotos.

WhastApp.zip
Distribution through Email

WhastApp.zip → HistoricoDeConversacao.PDF.vbs
Distribution through Email
<table>
<thead>
<tr>
<th>Time</th>
<th>Sender (spoofed)</th>
<th>Subject</th>
<th>Attachment name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:38 UTC</td>
<td>&lt;Emily2018@</td>
<td>Photo from Emily</td>
<td>SCN-20180404-3E90CC.zip</td>
</tr>
<tr>
<td>10:41 UTC</td>
<td>&lt;Lee2018@</td>
<td>Photo from Lee</td>
<td>JPG-20180404-1FF786.zip</td>
</tr>
<tr>
<td>10:53 UTC</td>
<td>&lt;Madge2018@</td>
<td>Photo from Madge</td>
<td>JPG-20180404-394ED1.zip</td>
</tr>
<tr>
<td>11:01 UTC</td>
<td>&lt;Mae2018@</td>
<td>Photo from Mae</td>
<td>SH-20180404-C1CE36.zip</td>
</tr>
<tr>
<td>11:15 UTC</td>
<td>&lt;Louise2018@</td>
<td>Photo from Louise</td>
<td>JPEG-20180404-EEF832.zip</td>
</tr>
<tr>
<td>11:46 UTC</td>
<td>&lt;Alexandria2018@</td>
<td>Photo from Alexandria</td>
<td>PIC-20180404-C2D648.zip</td>
</tr>
<tr>
<td>11:54 UTC</td>
<td>&lt;Sofia2018@</td>
<td>Photo from Sofia</td>
<td>SCN-20180404-E02418.zip</td>
</tr>
<tr>
<td>11:58 UTC</td>
<td>&lt;Rebecca2018@</td>
<td>Photo from Rebecca</td>
<td>SH-20180404-706CAE.zip</td>
</tr>
<tr>
<td>12:01 UTC</td>
<td>&lt;Minerva2018@</td>
<td>Photo from Minerva</td>
<td>SH-20180404-DDAC8F.zip</td>
</tr>
<tr>
<td>12:04 UTC</td>
<td>&lt;Michelle2018@</td>
<td>Photo from Michelle</td>
<td>JPG-20180404-2CD499.zip</td>
</tr>
</tbody>
</table>
Subject: Photo from Emily
From: Emily Sofiano <Emily2018@[recipient's email domain]>
Date: Wednesday, 04 Apr 2018 10:38 UTC

SCN-20180404-3E90CC.zip
Distribution through Email

SCN-20180404-3E90CC.zip  SH-20180404-BBDBAA-url
Distribution through Email

URL=file://169.239.129.25/stream/SH-20180404-BBDBAA.vbs
### Distribution through Email

```text
file://169.239.129.25/stream/
```
Distribution through Email

2014-04-13 03:42 – 3:53 UTC
92.53.77.184 port 80
rowrotatable.in
Distribution through Email

• Many different types of files used by criminals to install malware.
• Malicious spam with links to malware is harder to catch.
• Some types of malware have defense mechanisms and will act differently if analyzed.
Distribution through Social Media
My printer is about to be thrown through a window if this pic won't come out right. You see anything wrong with it? http://p12-ac.tinyfilehost.com/userfiles/96856/NewPhoto.JPG
Opening NewPhoto.JPG.scr

You have chosen to open:

**NewPhoto.JPG.scr**

which is: scr File

from: p12-ac.tinyfilehost.com

Would you like to save this file?

[Save File] [Cancel]
Targeting through Social Media

YOU

SOCIAL MEDIA

MALWARE
Stop calling it a ransomware "attack"

Published: 2016-08-07
Last Updated: 2016-08-07 19:49:47 UTC
by Brad Duncan (Version: 1)

3 comment(s).
Targeting through Social Media

Comment by SarahTheEnthusiast

I would beg to differ. I think that this type of malware is becoming so increasingly popular that even the careful internet users can get tricked into downloading and opening a link.
Targeting through Social Media

SarahTheEnthusiast (continued...)

I was a victim of ransomware attack just two days ago, and the hoax was so elaborate that it got me simply because I was thinking that this was too much of a trouble for someone to get me to download a virus.
Distribution through the Web
Distribution through the Web

Unexpected web pages or pop-up windows

Exploit kits
Distribution through the Web
Distribution through the Web
Distribution through the Web

This type of file can harm your computer. Do you want to keep Chrome_68.9.39.js anyway?

You are using an older version of Chrome

Update now to keep your Chrome browser running smoothly and securely.

Your download will begin automatically. If not, click here:

Update Chrome

This type of file can harm your computer. Do you want to keep Chrome_68.9.39.js anyway?
Distribution through the Web

You are using an older version of Firefox

Update now to keep your Firefox browser running smoothly and securely.

Your download will begin automatically. If not, click here:

Update Firefox
Distribution through the Web

Opening Firefox_63.9.39.js

You have chosen to open:

Firefox_63.9.39.js

which is: JavaScript File (38.6 KB)

from: https://dl.dropboxusercontent.com

Would you like to save this file?

Save File  Cancel
Exploit Kits

criminal's malware

behind the scenes

user's computer
Exploit Kits

Exploit kits are web servers that use exploits to take advantage of vulnerabilities in browser-based applications to infect a Windows computer without the user's knowledge.
Exploit Kits

- Flash player
- Web browser
- Silverlight
- Java, PDF
Up next...

- Types of malware
- Distribution methods
- Tech support scams
- Prevention strategies
** Windows Warning Alert **
Malicious Spyware/Riskware Detected
Error # 0x80072ee7

Please call us immediately at: 800-721-3515
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.
Your computer has alerted us that it has been infected with a Spyware and riskware. The following information is being stolen...
Financial Data
Facebook Logins
Credit Card Details
Email Account Logins
Photos stored on this computer
You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity.
Windows Defender Alert: Zeus Virus Detected In Your Computer!!

Please Do Not Shut Down or Reset Your Computer.

The following data will be compromised if you continue:
1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.
Windows Defender Alert: Zeus Virus Detected In Your Computer!! Please Do Not Shut Down or Reset Your Computer.

The following data will be compromised if you continue:
1. Passwords
2. Browser History
3. Credit Card Information
4. Local Hard Disk Files.

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks.

Call Microsoft Technical Department: 800-721-3515 (Toll Free)
00deabhsupport.tk/news/?number=800-721-3515

Authentication Required

http://00deabhsupport.tk is requesting your username and password. The site says: “Security Update Error 0x81983959 Help Desk: 800-721-3515 (TOLL-FREE)”

User Name: 
Password: 

OK Cancel

Please Do Not shutdown or Reset Your Computer.

Waiting for 00deabhsupport.tk...
Up next…

• Types of malware
• Distribution methods
• Tech support scams
• Prevention strategies
Prevention Strategies

• Keep regular backups of critical data and test them.
• Training and awareness.
• Keep your systems up-to-date and fully patched.
• Browsing restrictions.
• Threat detection, prevention and protection solutions.
Summary

• Types of malware
• Distribution methods
• Tech support scams
• Prevention strategies
Thank you!

Brad Duncan
Threat Intelligence Analyst