

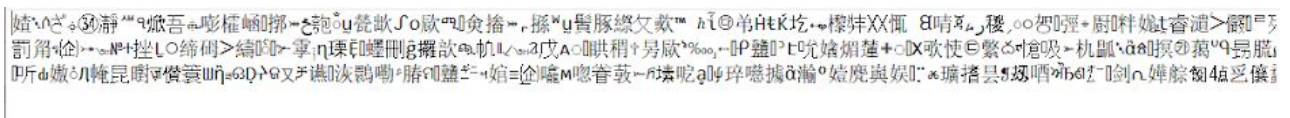
Rans0m - Reversing 100

Descripción:

Un virus de tipo ransomware encriptó los archivos de nuestra Empresa, por suerte obtuvimos el tráfico de red que creemos capturó dicho malware con el nombre svchost.exe.tar.gz

Ayúdanos a desencriptar el archivo "Important_Message.txt.ransm" para obtener la flag!

Important_Message.txt:



El primer paso es utilizar wireshark para analizar los paquetes y seguir la transferencia de paquetes para ver el tipo de comportamiento y si este cuenta con alguna particularidad que pueda ser útil:

Ransmutation.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Display Filters...
Display Filter Macros...
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As...
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Show Packet Bytes... Ctrl+Shift+O
Expert Information

TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-----------------|-----------------|-----------|--------|---------------------------------------|
| 85 | 16.675963 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1293 | FTP Data: 1239 bytes (EPASV) (TYPE I) |
| 43 | 16.674246 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 44 | 16.674284 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 45 | 16.674300 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 46 | 16.674314 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 47 | 16.674328 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 48 | 16.674458 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 49 | 16.674486 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 51 | 16.674497 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 52 | 16.674508 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 53 | 16.674518 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 54 | 16.674794 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 55 | 16.674818 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 56 | 16.674833 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 57 | 16.674846 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 58 | 16.674860 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 59 | 16.674873 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |
| 60 | 16.674888 | 192.168.213.138 | 192.168.213.130 | FTP-DA... | 1514 | FTP Data: 1460 bytes (EPASV) (TYPE I) |

> Frame 43: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
> Ethernet II, Src: Vmware_14:46:33 (00:0c:29:14:46:33), Dst: Vmware_c7:03:07 (00:0c:29:c7:03:07)
> Internet Protocol Version 4, Src: 192.168.213.138, Dst: 192.168.213.130
> Transmission Control Protocol, Src Port: 54334, Dst Port: 49752, Seq: 1, Ack: 1, Len: 1460
FTP Data (1460 bytes data)
[Setup frame: 32]
[Setup method: EPASV]
[Command: TYPE I]
[Command frame: 37]
[Current working directory: /]

