Analysing Malware Traffic

Alföldi Mátyás

May 30, 2020

Contents

Introduction

Source: http://www.malware-traffic-analysis.net/2020/01/30/index.html
Basic info:
LAN segment data:

- LAN segment range: 10.20.30.0/24 (10.20.30.0 through 10.20.30.255)
- Domain: sol-lightnet.com
- Domain controller: 10.20.30.2 - Sol-Lightnet-DC
- LAN segment gateway: 10.20.30.1
- LAN segment broadcast address: 10.20.30.255

Interesting Alerts

First few interesting Alerts:

- ET POLICY exe download via HTTP - Informational
- ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile
- ET POLICY Binary Download Smaller than 1 MB Likely Hostile
- ET POLICY PE EXE or DLL Windows file download HTTP

The IP related to this is: 49.51.133.162 The virustotal link shows that 2 detected files communicate with this IP.
(https://www.virustotal.com/gui/ip-address/49.51.133.162/details)
The abuse.ch lookup for this shows that the downloaded sv.exe is the Pony Trojan (https://urlhaus.abuse.ch/host/gengrasjeepram.com/), but looking into the virustotal link multiple AV names it Hancitor, which explains the later Hancitor related alerts.
(https://www.virustotal.com/gui/file/995cbbb422634d497d65e12454cd5832cf1b4422189d9ec06efa88ed56891cda)

ET POLICY External IP Lookup api.ipify.org
This seems mostly like this service is used by the malware, but is not necessarily malicious.

ETPRO TROJAN Tordal/Hancitor/Chanitor Checkin
The IP address: 81.177.6.156 is also reported to have been malicious.
This one is related to the Hancitor malware.

ETPRO TROJAN Hancitor encrypted payload Jan 17 (1)
Here we can see communication with 148.66.137.40, which when looking up virustotal 10+ known malicious files communicate with it.

ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile
49.51.133.162 also seems to be related to gengrasjeepram.com

Pcap Analysis

Information about the infected host:

- Host: DESKTOP-4C02EMG
- User: alejandrina.hogue
- IP: 10.20.30.227
- Mac: 58:94:6b:77:9b:3c
- Windows version: win 8 most likely from the data exfiltration

Communications mentioned in the alerts:

0.1 49.51.133.162

The only communication with this server is during the sv.exe download.

0.2 81.177.6.156

Seems like the communication starts with data exfiltration. The following info is exfiltrated:

- Some Guid
- Build Version of a software
- hostname@domain\user
- Windows version
- External IP
- Type (integer)

What is interesting is that during the HTTP OK message from the server, something that looks like base64 is sent back.
Most likely the application that communicates with this ip (probably sv.exe) can understand it.
Later on it seems that more data is exfiltrated and again an encoded messages is passed back with the HTTP OK.
Although it seems as if the malware exfiltrates the same data multiple times, might be a bug in it.

0.3 148.66.137.40

Two pictures are gathered with get requests, which result in encrypted data being returned.