dword 4:24:38 PM

Sore semua, kita akan mulai kulgram, pembahasannya tentang code signing.
mas @xathrya bisa jelaskan sedikit tentang code signing, dan kenapa harus membahas itu?

om @rhmtnf 4:25:24 PM

dword 4:27:44 PM

kita mulai sekarang aja deh, disini saya sebagai moderator. Diharapkan ketika pemateri sedang menjelaskan jangan ada yang memotong. Nanti kita akan buka sesi pertanyaan,.

dword 4:28:31 PM

Ok mas @xathrya dan @rhmtnf bisa dimulai sekarang

Satria Ady Pradana 4:30:22 PM

oke, kulgram kali ini mengenai code signing. Kita akan membahas tentang apa itu code signing, apa efeknya, dan bagaimana kisah malware meng-abuse code signing untuk mengelabui AV.
kali ini pematerinya ada 2 yaitu saya dan @rhmtnf . Di awal kita akan bahas dulu dasarnya secara singkat terus dilanjutkan oleh rahmat untuk bagian abusing-nya

secara sederhana code signing artinya memberikan tanda bahwa sebuah aplikasi itu benar dibuat oleh pihak yang tepercaya 4:31:29 PM

kalo formalnya. 4:32:57 PM
code signing adalah proses untuk menandatangani secara digital sebuah program executable ato script untuk menjamin bahwa kode tidak berubah ato corrupt semenjak ditandatangani. Signature ini hanya menjamin bahwa program dikeluarkan oleh pihak yang benar, tidak menjamin bahwa program ini tidak malicious

apa saja yang bisa di-sign? executables biasa dan drivers 4:34:23 PM

nah code signing ini prinsipnya sama seperti digital certificate biasa (x509 certificate). Dia memanfaatkan yang namanya PKI (Public Key Infrastructure) 4:35:42 PM

seseorang yang ingin sign program harus memiliki sepasang kunci, private-public key. Private key digunakan untuk melakukan sign, dan kunci ini harus dijaga hanya dia yang tau. Sementara public key, dilepas ke publik dan biasanya tertanam di sertifikat sehingga dapat digunakan untuk memverifikasi bahwa program ini benar. 4:37:24 PM

mirip kalo konek ke web HTTPS (yang pake SSL), kita akan meminta (dan dikasih) sertifikat yang menandakan identitas si server, beserta kunci publiknya. Bedanya di sini kita hanya menggunakan sertifikat itu untuk memverifikasi identitas program apakah benar dibikin oleh developer 4:39:22 PM

Satria Ady Pradana

darimana sertifikat bisa didapat? 4:41:00 PM
ada 2, bisa self-signed, bisa minta pihak lain untuk membuatkannya.
1. self sign berarti kita bikin sendiri sertifikatnya, kita tanda tangani sendiri
2. kalo minta pihak lain, berarti kita ngasih kan public key kita beserta beberapa informasi ke sebuah entitas bernama CA (Certificate Authority) untuk dibuatkan sertifikat.

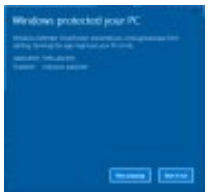
hello_app.exe 17 KB 4:42:34 PM
Download ()

hello_app_signexe 24 KB 4:42:51 PM
Download ()

di atas adalah 2 aplikasi yang melakukan hal yang sama yaitu menampilkan teks melalui messagebox. Bedanya satu aplikasi nggak ditandatangani, satunya ditandatangani 4:43:38 PM

ini kita batasi pake windows ya, dalam kasus ini aku pake windows 10. 4:44:30 PM

ketika aku jalankan, karena aplikasi ini masih belum dikenal (unknown publisher) maka dia akan menampilkan pesan peringatan seperti ini 4:45:48 PM



tmp_run.png 14 KB 4:45:55 PM
Download () Open ()

kalo kita klik kanan dan klik properties pada masing-masing program, kita akan liat ada perbedaan. 4:47:28 PM
aplikasi yang punya digital signature akan memiliki tab tambahan seperti ini

tmp_properties.png 8 KB 4:47:36 PM
Download () Open ()

kebetulan itu aku ambil dari internet, jadi sertifikatnya ya sertifikat orang :v 4:48:10 PM

kalo kita klik details maka akan tampil detail pemilik sertifikat itu dan siapa yang menjaminnya 4:48:48 PM

Satria Ady Pradana

karena tadi dijelaskan salah satu alternatif pembuatan sertifikat adalah memanfaatkan jasa pihak ketiga (CA), makan kita akan lihat bahwa sertifikat itu nanti berbentuk hirarki. 4:51:13 PM

sertifikat A diterbitkan oleh B
B juga punya sertifikat, diterbitkan oleh C
dsb

sampe ke suatu entitas yang disebut root CA, paling dipercaya untuk menerbitkan sertifikat.

konsepnya sama kayak ijazah sekolah kita. 4:53:56 PM

aku lulus SMA, bagaimana membuktikannya? dari ijazah (sertifikat) yang dikeluarkan oleh sekolahku.
bagaimana mempercayai kalo sekolahnya bener / gak abal-abal (terutama yang swasta)? bisa dilihat dari sertifikat yang dikeluarkan oleh pemerintah melalui badan terkait (telah terakreditasi)
dengna begitu orang bisa memverifikasi kalo aku bener udah lulus.

maka kalo dilihat di details, bagian certification path, kita akan melihat daftar beberapa sertifikat yang membentuk hirarki 4:55:28 PM

tmp_detail_cert.png 8 KB 4:56:22 PM
Download () Open ()

nah windows menyimpan secara default menyimpan beberapa sertifikat root yang otomatis tepercaya. 4:57:03 PM

biasanya kalo ada perubahan, windows akan melakukan update dari server windows untuk download daftar sertifikat baru. 4:58:22 PM
kita juga bisa daftarkan sertifikat sendiri yang dipercaya. Tapi itu bahasan lain.

jadi itu tadi soal definisi code signing. dan efeknya. 4:59:23 PM
selanjutnya akan dilanjutkan oleh om @rhmtnf untuk demo ngelabui Anti Virus dengan code signing

RN

Rahmat Nurfauzi 5:01:36 PM

oke, selanjutnya saya akan mendemo kan bagaimana beberapa AvP (Antivirus Product) bisa melewati deteksi dengan cara ini, tetapi tidak semua antivirus product.

Untuk melakukan code signing disini saya akan mengunakan tools seperti openssl dan signcode. untuk tool openssl digunakan untuk membuat certificate self-signed sedangkan tool signcode digunakan untuk melakukan sign ke PE executable. 5:01:50 PM

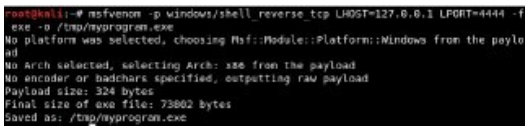
RN

Rahmat Nurfauzi 5:02:04 PM

Jadi sebelumnya kita harus meninstall kedua tools tersebut terlebih dahulu:

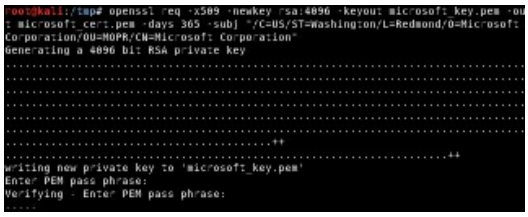
```
# apt-get install -y mono-devel openssl
```

Contoh untuk program disini agar lebih cepat, saya membuat sebuah malicious program dengan menggunakan tool `msfvenom` yang sudah tersedia di OS Kali Linux. 5:03:26 PM



5:03:51 PM

Hal pertama yang harus kita lakukan adalah membuat RSA key dengan panjang 4096 bit untuk root CA nya dengan expire 365 hari dengan tool `openssl` : 5:04:42 PM



5:05:36 PM

disini kita sedang membuat certificate self-signed 5:05:50 PM

untuk command yg diatas : 5:06:17 PM

```
openssl req -x509 -newkey rsa:4096 -keyout
microsoft_key.pem -out microsoft_cert.pem -days 365 -
subj "/C=US/ST=Washington/L=Redmond/O=Microsoft
Corporation/OU=MOPR/CN=Microsoft Corporation"
```

lalu masukan pass phrase, disini saya menggunakan pass phrase yg sama untuk setiap pass pharse `H@LXSDE$@$!` 5:07:27 PM

Kedua mengubah private key dari microsoft_key.pem ke format .pvk dengan perintah dibawah ini: 5:07:51 PM

```
openssl rsa -in microsoft_key.pem -outform PVK -pvk-
strong -out authenticode.pvk
```

image.png 8 KB 5:08:09 PM
Download () Open ()

File .pvk yang berisi informasi private key. 5:08:29 PM
File .spc (software publisher certificate) yang berisi informasi public key.

RN **Rahmat Nurfauzi** 5:08:29 PM

informasi lebih lanjut mengenai software publisher certificate bisa lihat disini http://www.softwarepublishercertificate.com/ (http://www.softwarepublishercertificate.com/)

> Softwarepublishercertificate
> **Software Publishers Certificates Explained - Certificate Authority Price List (http://www.softwarepublishercertificate.com/)**
> Code signing explained, including advice, links to industry resources, and a price list of certificate authorities.

Ketiga mengubahnya ke .spc file 5:09:46 PM

```
openssl crl2pkcs7 -nocrl -certfile microsoft_cert.pem
-outform DER -out authenticode.spc
```

RN **Rahmat Nurfauzi** 5:10:23 PM

image.png 7 KB
Download () Open ()

Rahmat Nurfauzi 5:11:40 PM

Kedua mengubah private key dari microsoft_key.pem ke form…

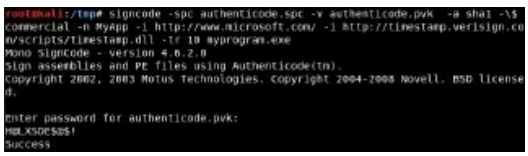
di step ini akan diminta memasukan pass pharse lagi saya menggunakan pass phrase sebelumnya yg awal

Dalam kasus ini sepasang file (.pvk dan.spc) harus dikonversi ke file .pfx untuk menambahkan informasi di sertifikat. 5:12:14 PM

Yang terakhir melakukan code signing ke PE executable yang telah dibuat tadi, myprogram.exe adalah programnya: 5:12:35 PM

```
signcode -spc authenticode.spc -v authenticode.pvk  -
a sha1 -\$ commercial -n MyApp -i
http://www.microsoft.com/ -i
http://timestamp.verisign.com/scripts/timestamp.dll -
tr 10 myprogram.exe
```

5:13:10 PM



5:13:21 PM

lalu diminta untuk memasukan key dari authenticode.pvk yang telah dimasukan sebelumnya. Disini kita berhasil melakukan code signing, selanjutnya kita akan analisa melalui virustotal berapa banyak yang berhasil terlewati dari program sesudah dilakukan code signing dan sebelum dilakukan code signing. 5:15:50 PM

5:16:30 PM

diatas adalah program yang sebelum dilakukan code signing, terlihat bahwa terdeteksi 50 / 63 5:17:23 PM

5:17:54 PM

diatas adalah program yang sudah dilakukan code signing, terlihat bahwa terdeteksi 35 / 63 yang artinya kita berhasil melewati 15 Antivirus product yang dilakukan dengan cara code signing. 5:19:07 PM

Program setelah dilakukan code signing myprogram.exe : https://www.virustotal.com/en/file/5017c397af608cdc53bdeee0ae5d4186372f48577ada29df5b842d55f0204170/analysis/1499592176/ (https://www.virustotal.com/en/file/5017c397af608cdc53bdeee0ae5d4186372f48577ada29df5b842d55f0204170/analysis/1499592176/) 5:24:09 PM

Program yang belum dilakukan code signing myprogram.exe.bak: https://www.virustotal.com/en/file/0f6e78c825b134c8ca3c5494db65651fa1e7e5a80256299042cdbe6632fd234f/analysis/1499592319/ (https://www.virustotal.com/en/file/0f6e78c825b134c8ca3c5494db65651fa1e7e5a80256299042cdbe6632fd234f/analysis/1499592319/)

> Virustotal
> **Antivirus scan for 5017c397af608cdc53bdeee0ae5d4186372f48577ada29df5b842d55f0204... (https://www.virustotal.com/en/file/5017c397af608cdc53bdeee0ae5d4186372f48577ada29df5b842d55f0204170/analysis/1499592176/)**
> VirusTotal's antivirus scan report for the file with MD5 a44b6af829d507a86a61ed970128f487 at 2017-07-09 09:22:56 UTC.
> 35 out of 63 antivirus de...

Cara diatas adalah bisa menjadi alternatif untuk menghindari dari deteksi antivirus, beberapa malware seperti Petya menggunakan teknik ini 5:27:04 PM

http://securitywatch.pcmag.com/security-software/283583-malware-digitally-signed-with-fake-certificate (http://securitywatch.pcmag.com/security-software/283583-malware-digitally-signed-with-fake-certificate) https://www.symantec.com/connect/blogs/malware-using-fake-certificate-evade-detection (https://www.symantec.com/connect/blogs/malware-using-fake-certificate-evade-detection) 5:27:40 PM

> PCMAG
> **Malware Digitally Signed With Fake Certificate (http://securitywatch.pcmag.com/security-software/283583-malware-digitally-signed-with-fake-certificate)**

> Otherwise unremarkable Trojan attempts to fool users by claiming it was digitally signed by antivirus company Avira.

mungkin itu dari saya 5:28:05 PM

Satria Ady Pradana 5:29:18 PM

file yang udah sign bisa dikirim ke sini gak?

dword 5:29:41 PM

Ok, terimakasih om @xathrya dan om @rhmtnf sudah mengisi materi hari ini, sesi tanya jawab sudah kita buka. jadi Silahkan kalo ada yang mau ditanyakan, bisa langsung bertanya

RN **Rahmat Nurfauzi** 5:29:46 PM

ok

myprogram.exe 75 KB 5:30:37 PM
Download ()

myprogram.exe.bak 72 KB 5:30:38 PM
Download ()

Aditya Irwansyah 5:30:57 PM

saya mau tanya ini sama seperti bypass UAC ?

Satria Ady Pradana 5:32:18 PM

bisa

AA **Arief A.** 5:34:41 PM

Dari mana asal muasal file cert milik microsoft ini?

Satria Ady Pradana 5:35:45 PM

hmm...

kurang tau kalo itu 5:35:58 PM

AA **Arief A.** 5:36:01 PM

Hasil leak NSA krmn kah?

Satria Ady Pradana 5:36:06 PM

oh...

di sini kita gak nyolong ato dapatkan cert milik si microsoft, tapi kita bikin cert sendiri dengan data mirip seperti data yang diberikan microsoft, tapi kita tanda tangani sendiri 5:36:45 PM

RN **Rahmat Nurfauzi** 5:36:56 PM

> **Arief A.**
> Dari mana asal muasal file cert milik microsoft ini?

ini self-signed jadi buat sendiri dengan perintah `openssl req -x509 -newkey rsa:4096 -keyout microsoft_key.pem -out microsoft_cert.pem -days 365 -subj "/C=US/ST=Washington/L=Redmond/O=Microsoft`

`Corporation/OU=MOPR/CN=Microsoft Corporation"` yang sudah dijelaskan diawal

Satria Ady Pradana 5:37:55 PM

kalo tanya jawab udah selesai, nanti aku tambahin sedikit ya ;)

R.3volv3.R 5:38:02 PM

itu kan cuma nama filenya aja waktu buat dgn openssl ..

AA

Arief A. 5:38:09 PM

Siap

Megi Oliver 5:38:21 PM

Saya ingin bertanya : ketika program sebelum di signing dan ketika program sesudah signing langsung berubah ekstensinya, sebelum di signing, .exe.bak ketika di signing, .exe

Satria Ady Pradana 5:38:37 PM

bentar, @darkro5e , masih mau kutambahi setelah sesi tanya jawab

RN

Rahmat Nurfauzi 5:40:03 PM

> **Megi Oliver**
> Saya ingin bertanya : ketika program sebelum di signing dan …

ini berubah otomatis pakai tool `signcode`

seperti cara sign diatas 5:40:21 PM

Aditya Irwansyah 5:40:48 PM

btw bagaimana cara mengetahui klo signcode itu bukan dari penyedia aslinya apakah ada pola tertentu?

Megi Oliver 5:41:52 PM

Tapi apakah akan mempengaruhi struktur code program nya pak?

Satria Ady Pradana 5:42:22 PM

> **Megi Oliver**
> Tapi apakah akan mempengaruhi struktur code program nya …

nah, ini mau kubahas setelah sesi tanya jawab

Megi Oliver 5:43:18 PM

Okey mas

Satria Ady Pradana 5:45:24 PM

> **Aditya Irwansyah**
> btw bagaimana cara mengetahui klo signcode itu bukan dari …

nah, memang rada-rada tricky, harus punya sense. Kalo ngeliat programnya signed pake data perusahaan tertentu yang terkenal tapi self-signed, mesti diwaspadai.
tapi ya susah juga sih

oke kutambahkan dikit yak 5:46:06 PM
live reversing tadi :9

Satria Ady Pradana 5:46:40 PM

dari aplikasi yang diupload sama om rahmat, aku ambil malware yang signed.
kita pengen tau, sertifikat disimpannya dimana sih?

apakah mengubah struktur program? 5:46:51 PM

jawabnya, struktur program berubah tapi kode tetap. 5:47:48 PM
bagian mananya?
ada penambahan pada bagian DIRECTORY_ENTRY_SECURITY. Di sini entri sertifikat ditambahkan.

Aku memakai aplikasi PPEE untuk membedah struktur file PE (Portable Execution) alias format file executable di windows. Terlihat di sini screenshotnya 5:48:28 PM

tmp_PPEE.png 46 KB 5:48:55 PM
Download () Open ()

terlihat tipe sertifikatnya yaitu PKCS dan informasi-informasi yang ada di sertifikat ditampilkan di bawah seperti Issuer Name dan timestamp. 5:50:22 PM

tapi... liat bahwa validity-nya broken, alias nggak chaining ke mana-mana, alias dia self-sign jadi gak terlalu valid.

oke sekian tambahannya 5:50:28 PM

RN **Rahmat Nurfauzi** 5:52:27 PM

https://arstechnica.com/security/2016/03/to-bypass-code-signing-checks-malware-gang-steals-lots-of-certificates/ (https://arstechnica.com/security/2016/03/to-bypass-code-signing-checks-malware-gang-steals-lots-of-certificates/)

>  (https://arstechnica.com/security/2016/03/to-bypass-code-signing-checks-malware-gang-steals-lots-of-certificates/)
>
> Ars Technica
>
> **To bypass code-signing checks, malware gang steals lots of certificates (https://arstechnica.com/security/2016/03/to-bypass-code-signing-checks-malware-gang-steals-lots-of-certificates/)**
>
> Legitimate code-signing certificates provide secret cover for attack groups.

Aditya Irwansyah 5:53:14 PM

thanks for share

Willy Surya Hidayat 5:55:18 PM

> **Satria Ady Pradana**
> terlihat tipe sertifikatnya yaitu PKCS dan informasi-informasi y

Terima kasih mas Satria Ady tambahan nya sangat membantu sekali, jadi tahu klo sertifikat asli itu gimana tipe nya dan yg bukan jg seperti apa

Satria Ady Pradana 5:57:19 PM

balik lagi ke kepercayaan (trust)
kita harus liat itu hirarki sapa-sapa aja yang berperan dalam pembuatan sertifikat. Kalo diliat di bagian properties tadi (di explorer) kan ada certificate path. Sebaiknya pastikan kalo dia berasal dari CA yang tepercaya