Open in app ↗

Sign up

Sign in

Medium

Search

Write

Code Signing Certificate Cloning Attacks and Defenses

Matt Graeber · Follow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

together and start focusing on outliers in the data set. You find the following outlier on

6 systems out of 40,000:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   SecurityAudit
     C:\Windows Defender\MpCmdRun.exe
     Microsoft Malware Protection Command Line Utility
     (Verified) Microsoft Corporation
     4.12.16299.15
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- Distraction-free reading. No ads.
- Organize your knowledge with lists and highlights.
- Tell your story. Find your audience.

Sign up for free

Membership

- Read member-only stories
- Support writers you read most
- Earn money for your writing
- Listen to audio narrations
- Read offline with the Medium app

Try for 5 $/month

does not exist.

5. You accept that it's an outlier but you are confident that MpCmdRun.exe isn't being abused in the wild and you subsequently filter future hits of this hash. After all, you have many more outliers to wade through.

Does this scenario sound familiar to anyone? Unfortunately, as much as I hate to say it, that Autoruns entry was positive evidence of compromise and you overlooked it and decided to overlook it in the future as well.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

3. You'll also want to export the cloned root certificate as you will need to trust this certificate on the victim system in order for any of your signed, malicious code to verify properly and blend in with many security tools.

The following video shows the manual process of exporting the certificate chain used to sign kernel32.dll:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

5. Root CA validation — Is the root certificate in the signer chain a trusted certificate?

Technically, our cloned certificate chain passes all of these checks so any tool that performs signature validation (sigcheck, autoruns, procexp, AV?, etc.) will likely be fooled.

You may have noticed in the video, upon installation of the root certificate in the “CurrentUser” certificate store, a dialog popped up asking if you trust the

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

Detecting Malicious Root CA Certificate Installation

Considering the root of this attack involves installation of a root CA certificate, this action will be the focus of building a detection. The installation of root CAs should be sufficiently uncommon such that a high-fidelity alert should be possible by monitoring the registry. Sysmon serves this purpose really well and what follows is an ideal config for catching root certificate installation:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

```
Image: C:\WINDOWS\system32\wbem\wmiprvse.exe
TargetObject:
HKLM\SOFTWARE\Microsoft\SystemCertificates\ROOT\Certificates\1F3D3
8F280635F275BE92B87CF83E40E40458400\Blob
Details: Binary Data
```

Using this rule set, you will likely get a lot of CreateKey event false positives. The high-fidelity events to pay attention to are SetValue events where the TargetObject property ends with “<THUMBPRINT_VALUE>\Blob” as this indicates the direct installation or modification of a root certificate binary blob. Unfortunately, as of this writing, Sysmon configurations don’t allow

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

```
Microsoft.PowerShell.Security\Certificate::LocalMachine\Root
PSChildName                 :
1F3D38F280635F275BE92B87CF83E40E40458400
PSDrive                     : Cert
PSProvider                  :
Microsoft.PowerShell.Security\Certificate
PSIsContainer               : False
EnhancedKeyUsageList        : {}
DnsNameList                 : {Microsoft Root Certificate Authority
2010}
SendAsTrustedIssuer         : False
EnrollmentPolicyEndPoint :
Microsoft.CertificateServices.Commands.EnrollmentEndPointProperty
EnrollmentServerEndPoint :
Microsoft.CertificateServices.Commands.EnrollmentEndPointProperty
PolicyId                    :
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

To any observer, this certificate definitely has the “look and feel” of a legitimate certificate but what is it exactly that makes a certificate “legitimate” or trusted? That process will be described in the last section of the post.

. . .

Preventing Malicious “CurrentUser” Root CA Certificate Installation

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

```
// The .Default physical store open's the CurrentUser
SystemRegistry "Root"
// store.
#define CERT_PROT_ROOT_DISABLE_CURRENT_USER_FLAG    0x1

// Set the following flag to inhibit the adding of roots from the
// CurrentUser SystemRegistry "Root" store to the protected root
list
// when the "Root" store is initially protected.
#define CERT_PROT_ROOT_INHIBIT_ADD_AT_INIT_FLAG     0x2
```

After setting this key, you will get an access denied error when attempting to install a root CA to the CurrentUser Root certificate store.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

for whatever reason there is a business justification for permitting any user to trust a root certificate, you accept that an attacker or rogue software can trust arbitrary root certificates as well. Windows administrators will always have the ability to push trusted root certificates via Group Policy. A recent case where software installed its own root certificate without alerting the user was a Savitech audio driver. In this case, you would have needed to be admin to trust this root certificate but arbitrary root certificates have no basis for the establishment of trust compared to the arduous steps required to get your root certificate trusted by Microsoft.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

```
User\Root:
  Microsoft Root Certificate Authority 2010
     Cert Status:    Valid
     Valid Usage:    All
     Cert Issuer:    Microsoft Root Certificate Authority 2010
     Serial Number:  52 76 17 36 EE A4 45 81 42 45 3E 2D 73 FA 89
B2
     Thumbprint:     1F3D38F280635F275BE92B87CF83E40E40458400
     Algorithm:      sha256RSA
     Valid from:     1:55 PM 12/1/2017
     Valid to:       9:06 PM 11/30/2042
```

So why should this entry not be trusted? What is Microsoft's basis for trust?

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

It is also possible to parse authroot.stl with certutil.exe:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month

```
Thumbprint : 3B1EFD3A66EA28B16697394703A72CA340A05BD5
Subject    : CN=Microsoft Root Certificate Authority 2010,
O=Microsoft Corporation, L=Redmond, S=Washington, C=US
```

So the way in which Microsoft-signed code should ideally be validated (versus simply pulling the publisher name and validating that it chains to a “trusted” root) is to perform the following:

1. Validate that the integrity of the binary has not been compromised.
2. Validate that each certificate in the chain is valid.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 $/month

Lastly, an astute reader will have noted that there may have been additional anomalies associated with the cloned certificate chain and signed code. I'll leave discussion of these anomalies for another blog post. See you in 2018!

Security Code Signing

-- 2

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Try for 5 $/month