Can we trust a trustee? An in-depth look into the digitally signed malware industry

Adrian Popescu Gheorghe Jescu

Bitdefender

September 25, 2014

Agenda

1. Introduction
2. Possible vulnerabilities
3. But why would anyone use this?
4. The economy
5. What can we do?

Introduction

- In 1988 the standard X.509 was initially issued. In 1989 IBM Lotus had code signing available.

X.509 is an ITU-T standard for a public key infrastructure, it assumes a strict hierarchical system of certificate authorities.
Code signing is the process of digitally signing executables and scripts.

Introduction

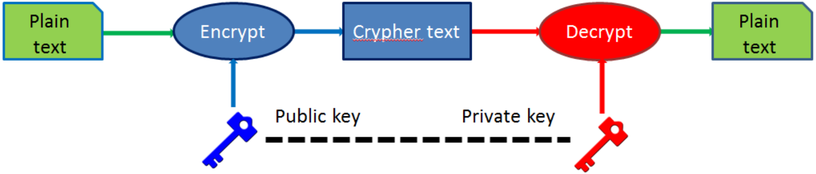
- In 1988 the standard X.509 was initially issued. In 1989 IBM Lotus had code signing available.

X.509 is an ITU-T standard for a public key infrastructure, it assumes a strict hierarchical system of certificate authorities.
Code signing is the process of digitally signing executables and scripts.

- The purpose is to confirm the software author and guarantee that the code has not been altered by a 3rd party channel.
- A digitally signed executable generates less warnings when executed.
- Nowadays some Windows versions enforce the signing of drivers in order to register them.

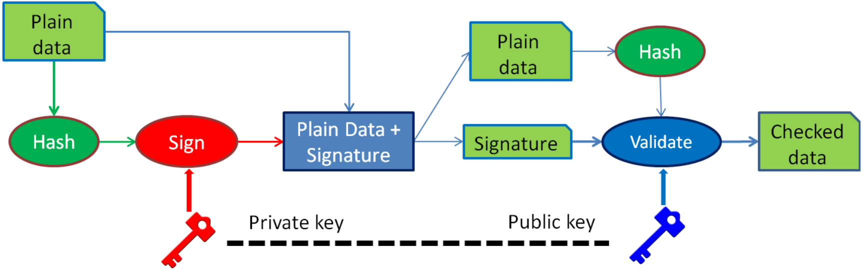
Cryptograhy behind digital certificates

Asymmetric cryptography, is a class of cryptographic algorithms which requires two separate keys.
One of which is private and one of which is public.
Two parts of the key pair are mathematically linked.



Cryptograhy behind digital certificates

Asymmetric cryptography, is a class of cryptographic algorithms which requires two separate keys.
One of which is private and one of which is public.
Two parts of the key pair are mathematically linked.



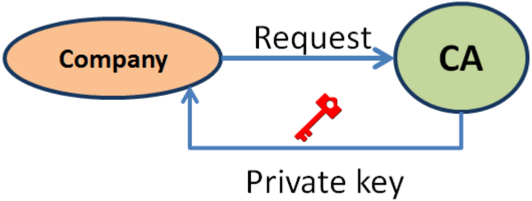
Steps into digitally signing a file

- Choosing a Certificate Authority that is trusted by Windows.

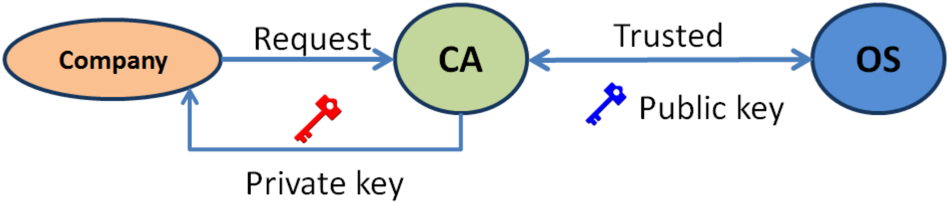
Certificate Authority (CA) is an entity that issues digital certificates.

- Provide the company information (commercial registration number, current address, service bills, contact details).
- Wait until the information is checked by the CA and the confirmation is received.
- Install all the necessary softwares and implement the methodology of good practice.
- Sign files just before deployment and distribute them.

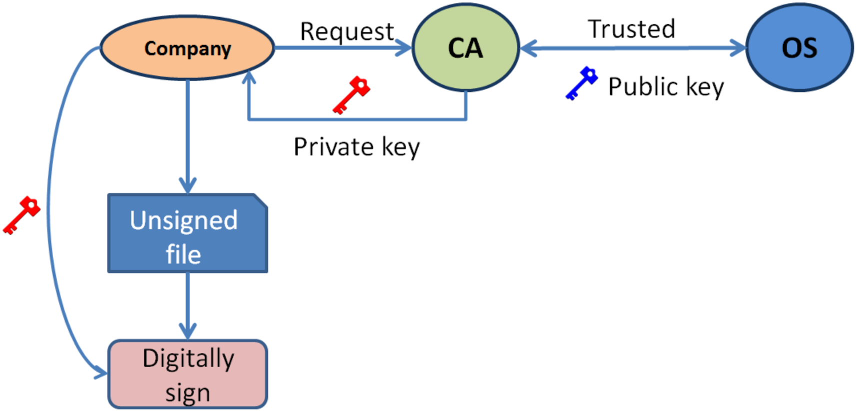
Overview of the process



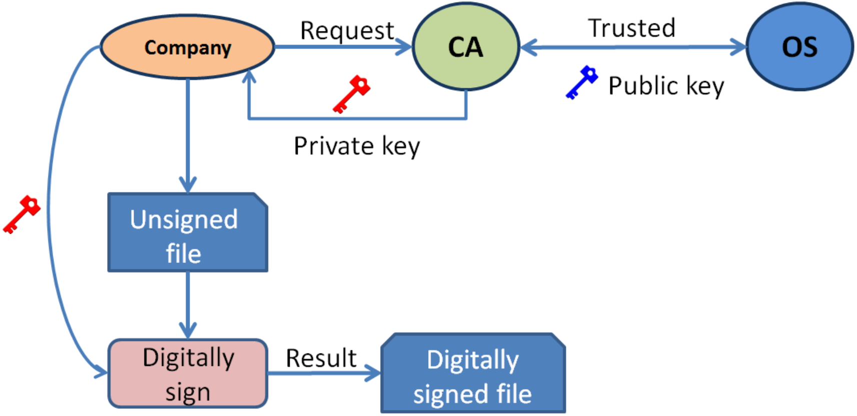
Overview of the process



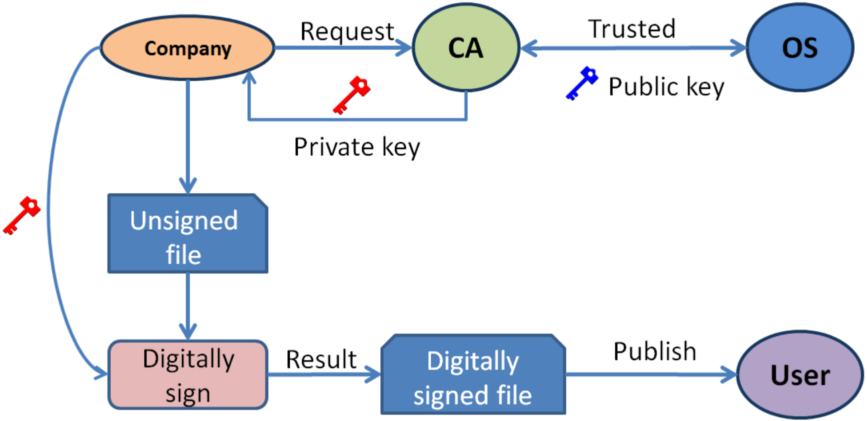
Overview of the process



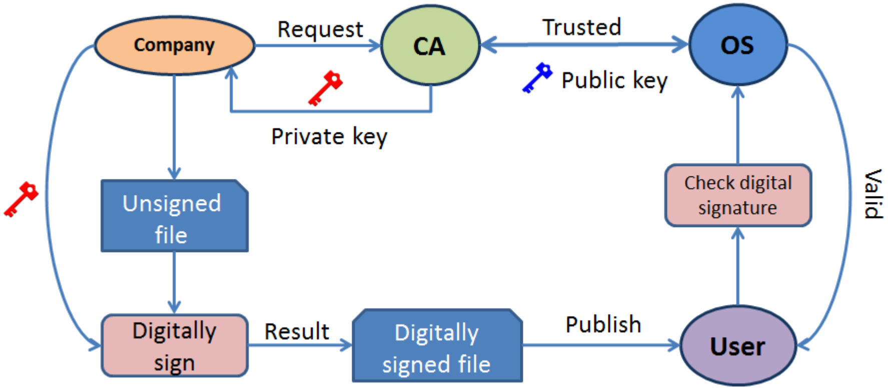
Overview of the process



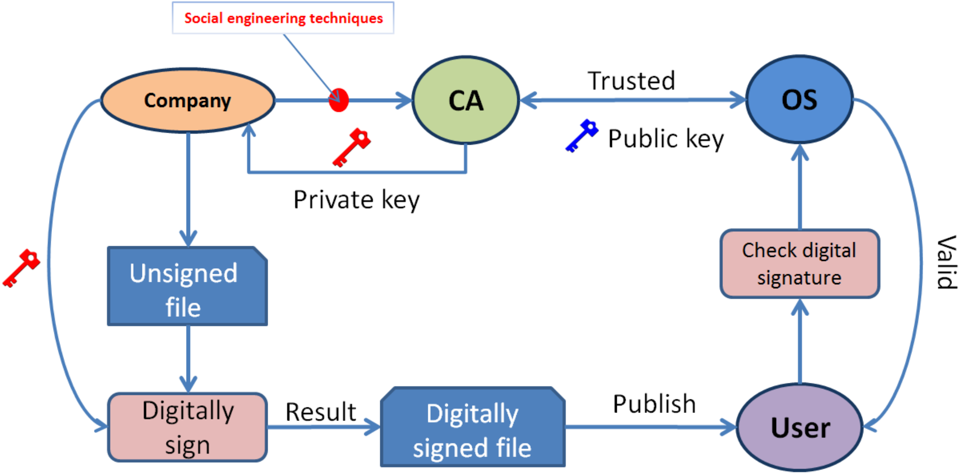
Overview of the process



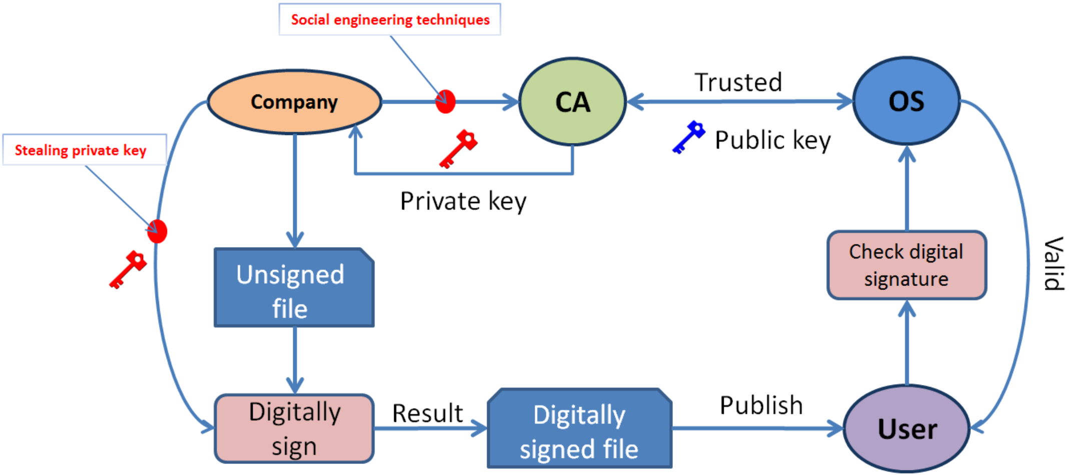
Overview of the process



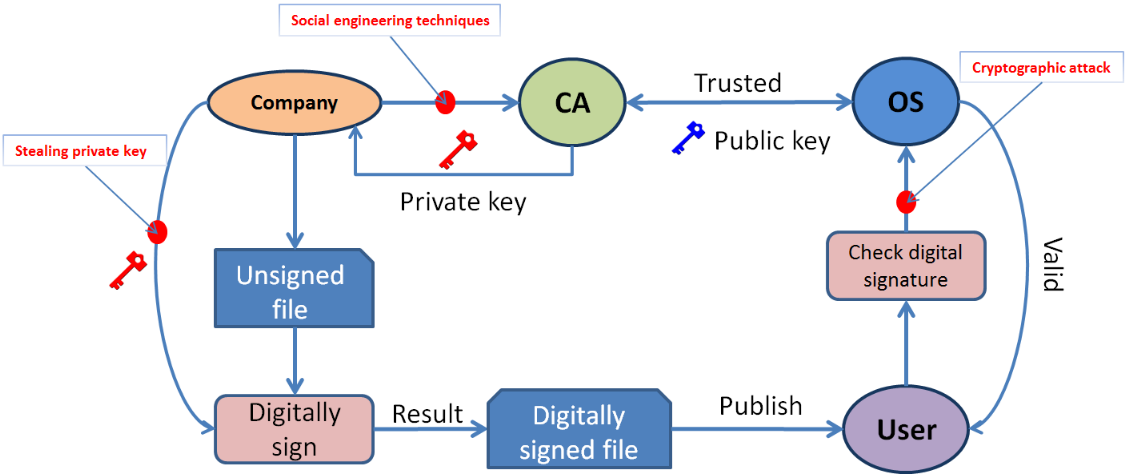
Possible attacks



Possible attacks



Possible attacks



Social engineering techniques

Social engineering, in this context, refers to psychological manipulation of people or companies into divulging confidential information or performing actions.

Usage of fake identities to trick the CA into issuing a certificate.

Usage of fake identities to trick the CA into issuing a certificate.

Impersonate a large company employee and trick the CA to issue a certificate.

Example

Issued to: Microsoft Corporation
Issued by: VeriSign Commercial Software Publishers CA
Valid from 1/29/2001 to 1/30/2002
Serial number is 1B 51 90 F7 37 24 39 9C 92 54 CD 42 46 37 99 6A

Usage of stolen identities to trick the CA into issuing a certificate

Usage of stolen identities to trick the CA into issuing a certificate

Usage of appropriate Internet searches to find information about employees with managerial positions.

Example

Issued to: Hemant Mehta
Issued by: SafeScrypt sub-CA for RCAI Class 3 2012
Valid from 06/19/2013 to 06/19/2015
Valid in June 2014

Usage of information that can be difficult to validate

Usage of information that can be difficult to validate

The same name, or variation of it, used to issue multiple certificates from different CAs.

Issued to: JOHN WILLIAM RICHARD
Issued by: Thawte Code Signing CA - G2
Valid from 10/30/2013 to 10/31/2014

Issued to: John W. Richard
Issued by: COMODO Code Signing CA 2
Valid from 11/08/2013 to 11/09/2014

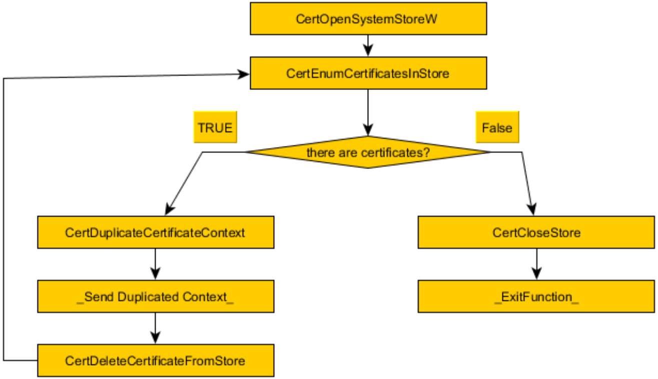
Issued to: William Richard John
Issued by: StartCom Class 2 Primiary Intermidiate Object CA
Valid from 12/11/2013 to 12/12/2015

Steal private keys - How to steal certificates?

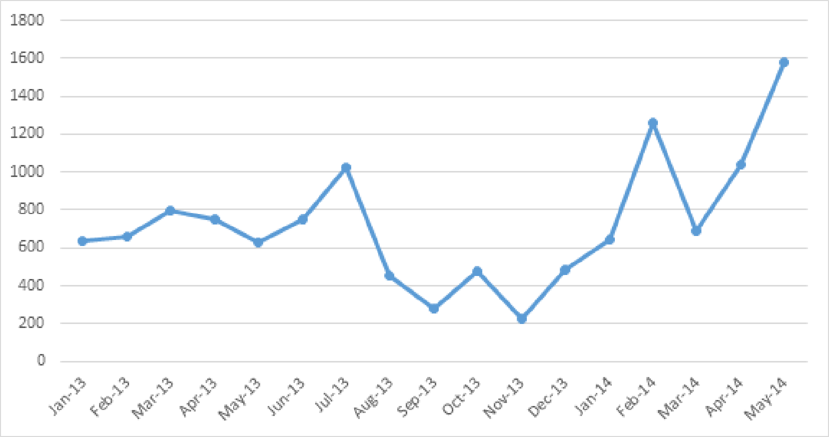
Distribute malware through spam or exploits in order to infect the computers that manage the digital signing process and then steal the certificates and eventually delete them.

Steal private keys - How to steal certificates?

Distribute malware through spam or exploits in order to infect the computers that manage the digital signing process and then steal the certificates and eventually delete them.


CertOpenSystemStoreW
CertEnumCertificatesInStore
TRUE
False
there are certificates?
CertDuplicateCertificateContext
Send Duplicated Context
CertDeleteCertificateFromStore
CertCloseStore
ExitFunction

Malware files with certificate-stealing capabilities



Similar malware files with certificate-stealing capabilities

Cryptographic attack and MD5 or SHA-1 forgery

- Has NOT been encountered on malware families yet
- It is possible to generate two files with different behavior with the same MD5 hash.
- A mathematical approach for creating SHA-1 collisions with a complexity of less than 2^{69} was demonstrated

Why would anyone use this?

Why are malware creators interested in this?

Detection experiment

Subjects

10 Well-known Anti-Virus products.

Detection experiment

Subjects

10 Well-known Anti-Virus products.

Camouflage

One **test certificate** installed on the system.

Detection experiment

Subjects

10 Well-known Anti-Virus products.

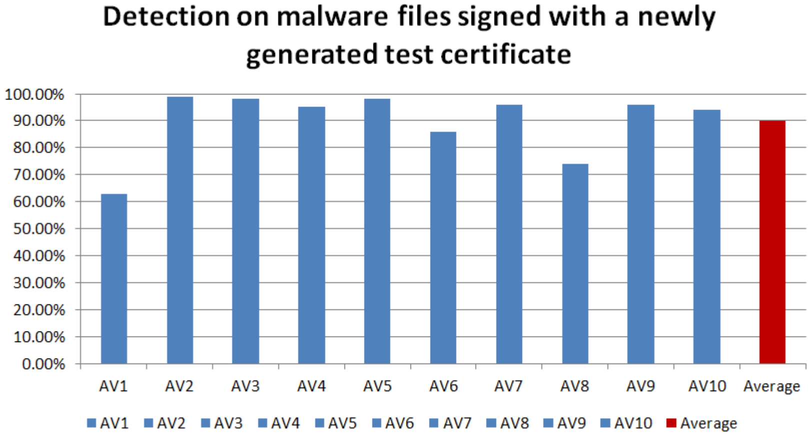
Camouflage

One **test certificate** installed on the system.

Virus

100 malware files from well-known malware families

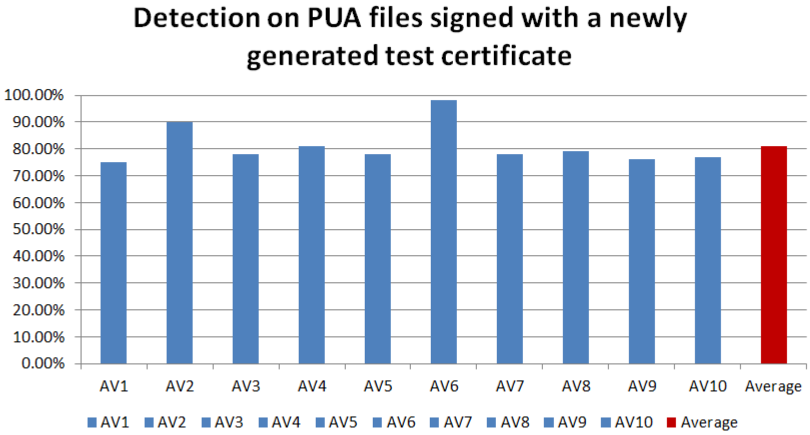
Detection experiment



The grey side of digital signatures

Not only creators of malware abuse of digitally signed files, but also creators of potentially unwanted applications (PUAs). Mostly due to the lack of clear rules of detection.

Detection experiment



Supply and demand

Advantages

- Lower detection rate.
- Only drivers with valid certificate can be loaded in new Windows version.
- Illusion of trustworthy environment.

Supply and demand

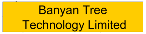
Advantages

- Lower detection rate.
- Only drivers with valid certificate can be loaded in new Windows version.
- Illusion of trustworthy environment.

Supply

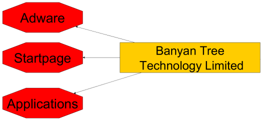
- Increasing number of malware with certificates-stealing capabilities results in plenty certificates to choose from.
- Vulnerable drivers with a valid digital signatures.

Is there a market?

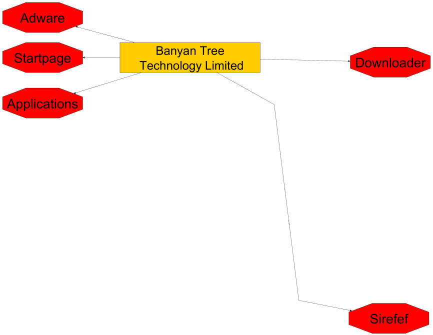


Banyan Tree
Technology Limited

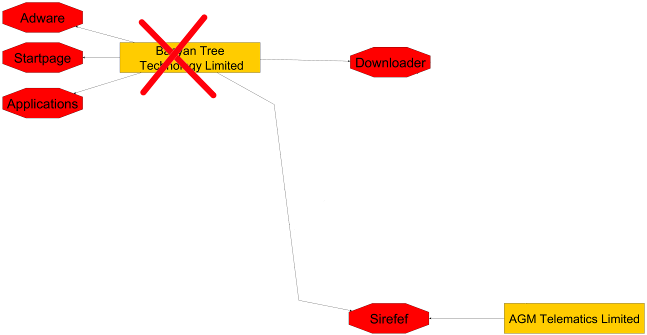
Is there a market?



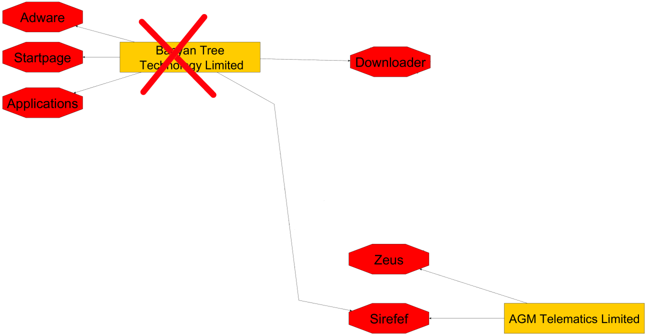
Is there a market?



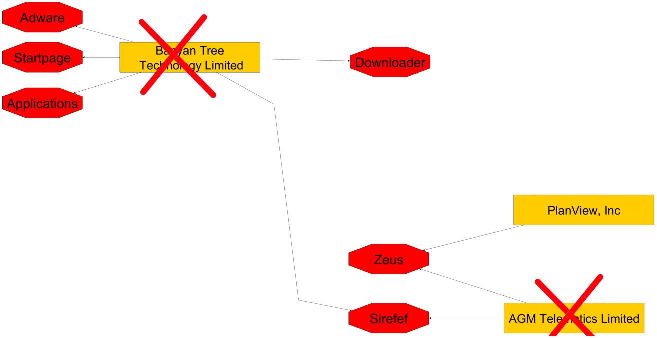
Is there a market?



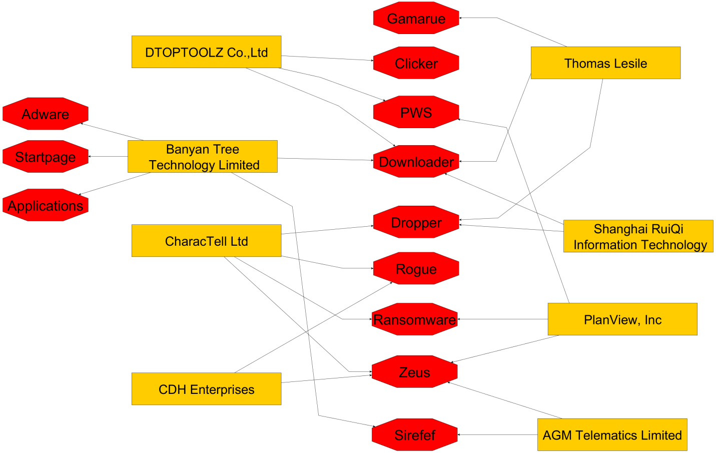
Is there a market?



Is there a market?



Is there a market?



What can we do?

What can we do?

What can we do?

Operating system

- Block execution of non-critical files signed with revoked certificate
- Alert the user if a file is already running and is signed with revoked certificate

What can we do?

Operating system

- Block execution of non-critical files signed with revoked certificate
- Alert the user if a file is already running and is signed with revoked certificate

Certificate Authorities

- Improve validation of applicants
- Improve revocation list in order to proper specify which certificate is used by malware

What can we do?

Operating system

- Block execution of non-critical files signed with revoked certificate
- Alert the user if a file is already running and is signed with revoked certificate

Certificate Authorities

- Improve validation of applicants
- Improve revocation list in order to proper specify which certificate is used by malware

Vendors

- Proper share of information
- Collaborate with CAs to revoke the known certificates that are known to be used with malicious intentions

What can we do?

Software developers

- Better security around the signing system
- Use test certificates until software deployment
- Revoke old unused certificates

What can we do?

Software developers

- Better security around the signing system
- Use test certificates until software deployment
- Revoke old unused certificates

Users

- Check the certificate information
- Be aware that this is widely used by malware creators

Q&A

Q&A