0111010
0101110
1110101
1010
0010

ROSCO

Repository Of Signed Code*

Levente Buttyán
Laboratory of Cryptography and System Security (CrySyS Lab)
Budapest University of Technology and Economics
www.crysys.hu

this is joint work with **D. Papp**, **B. Kócsó**, **T. Holczer**, and **B. Bencsáth**

* work funded by the Office of Naval Research Global (ONRG)

Motivation

- modern operating systems require digital signature on system software before it is installed
  - drivers, OS updates, ...

- advanced attackers (APTs) started to use malware signed with compromised keys or fake certificates
  - kernel drivers used by Stuxnet and Duqu were signed with **compromised keys** of otherwise legitimate hardware manufacturers
  - Flame appeared to be a signed Windows update; certificate chain contained a **fake certificate** that looked like a valid Microsoft certificate

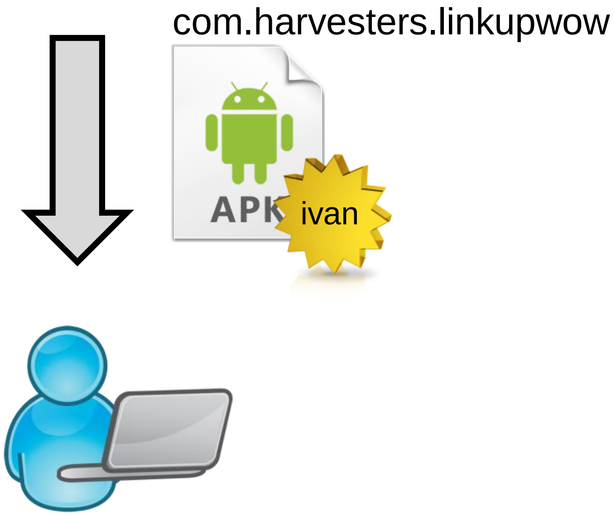
Motivation

- more recent examples
  - Winnti (2011, 2013)
    - in 2011, the group infected players of a popular online game via a malicious game update signed with the possibly compromised code signing key of a South-Korean game vendor
    - attacks against South Korean social networks Cyworld and Nate in 2011 used a Trojan that was digitally signed using a certificate stolen from a Japanese gaming company
    - a digital certificate of the same company was used in 2013 in Trojans deployed against Tibetan and Uyghur activists
  - return of Wild Neutron (2015)
    - successful cyber espionage attacks on companies such as Apple, Facebook, Twitter and Microsoft in 2013
    - attackers returned in 2015 and used a dropper that was signed with a stolen and still valid code signing certificate belonging to Taiwanese electronics maker Acer
- problem: standard signature verification procedure does not allow for detecting key compromise and fake certificates

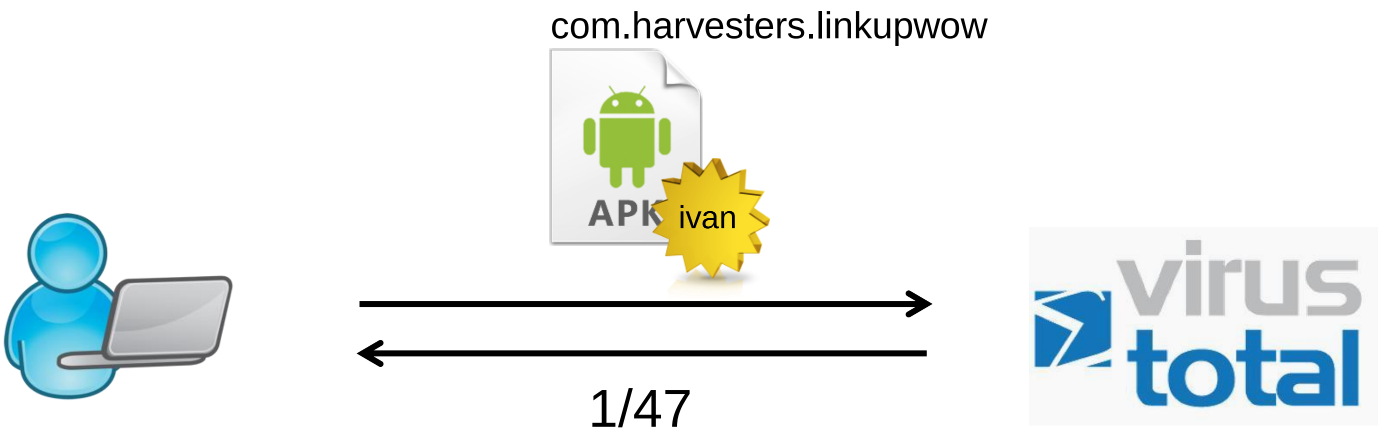
Objectives

- augment the standard signature verification workflow with additional services that help to detect malicious software
  - provide reputation information on signers and signed code
    - Is this a known signed software?
    - What do we know about it? (e.g., Virus Total score)
    - How many other users have requested information about this software?
    - Is this software has a known signer?
    - What do we know about pieces of software it signed before?
  - notify key owner when a new object signed with a specific key is seen
    - this makes it possible to detect key compromise and fake certificates relatively quickly
- build a system that provides the necessary infrastructure and mechanisms for these additional services

Use case: Checking signer reputation



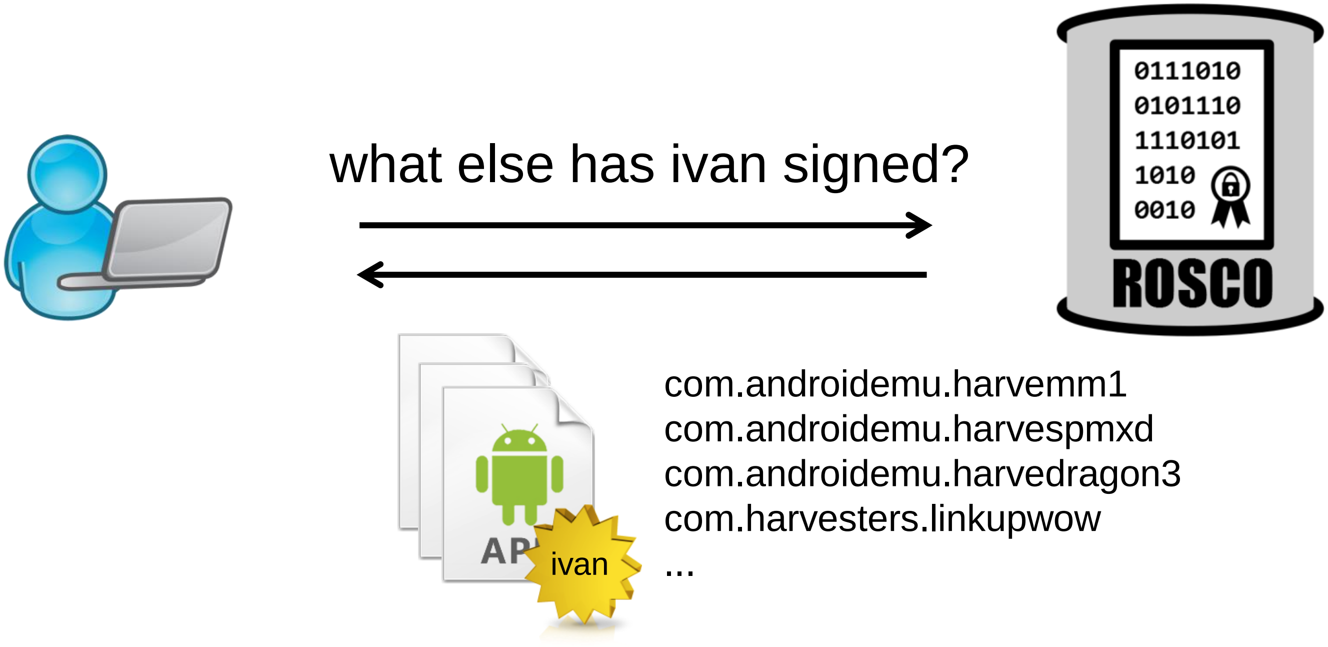
Use case: Checking signer reputation



com.harvesters.linkupwow

1/47

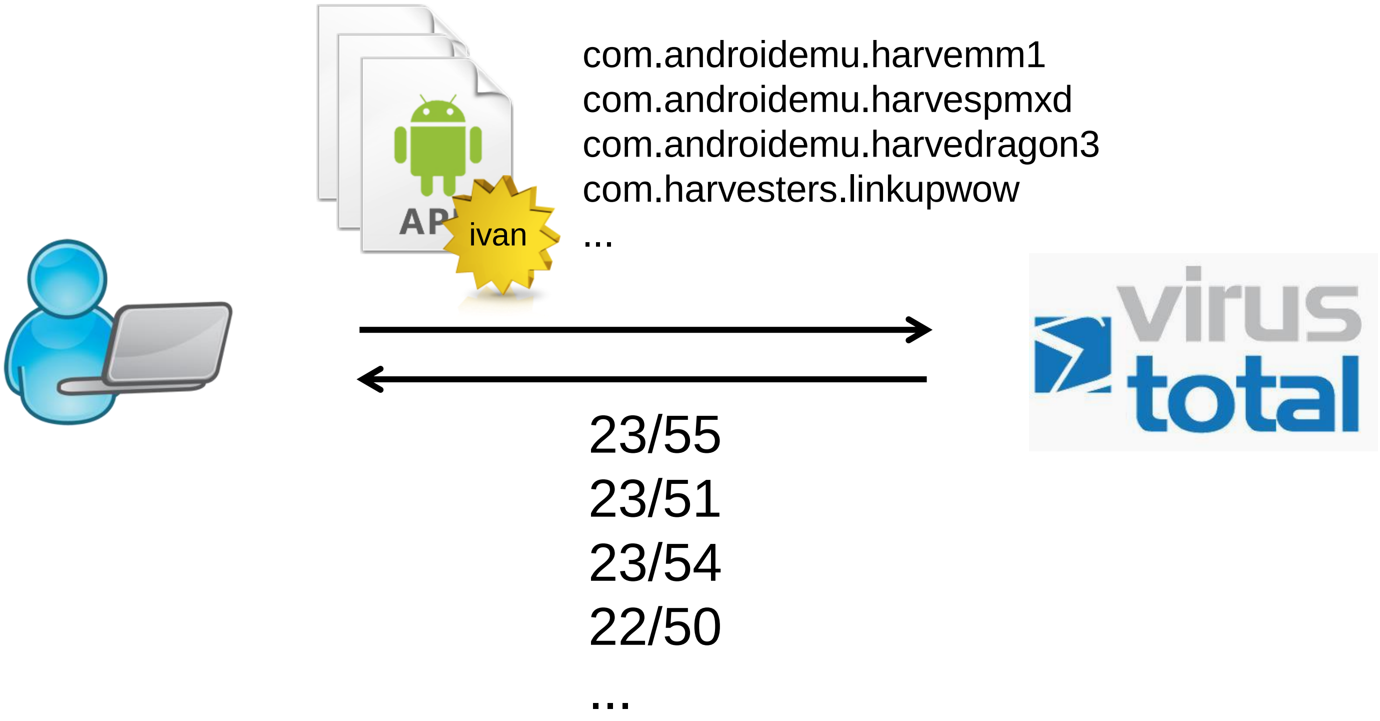
Use case: Checking signer reputation



what else has ivan signed?

com.androidemu.harvemm1
com.androidemu.harvespmxd
com.androidemu.harvedragon3
com.harvesters.linkupwow
...

Use case: Checking signer reputation



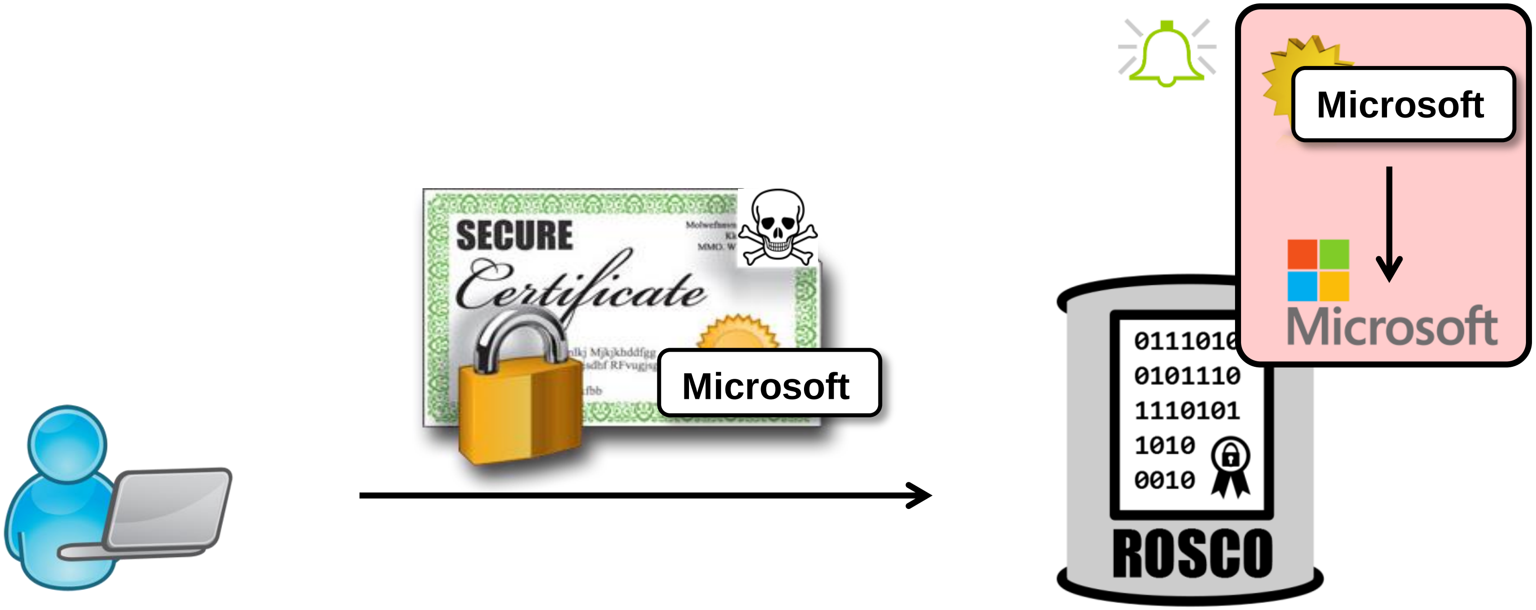
com.androidemu.harvemm1
com.androidemu.harvespmxd
com.androidemu.harvedragon3
com.harvesters.linkupwow
...

23/55
23/51
23/54
22/50
...

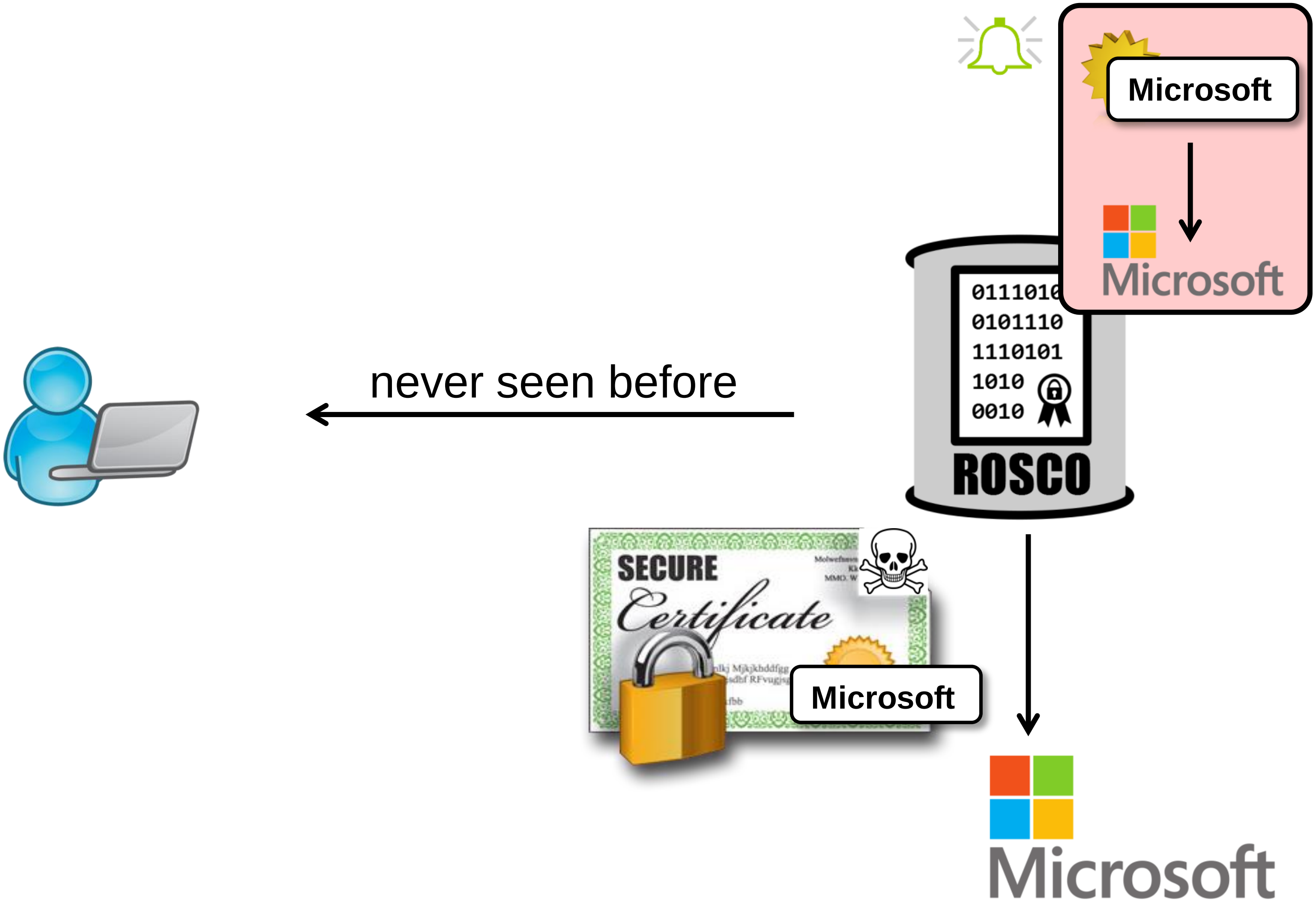
Use case: Alerting key owners

SECURE
Certificate
Microsoft

Use case: Alerting key owners



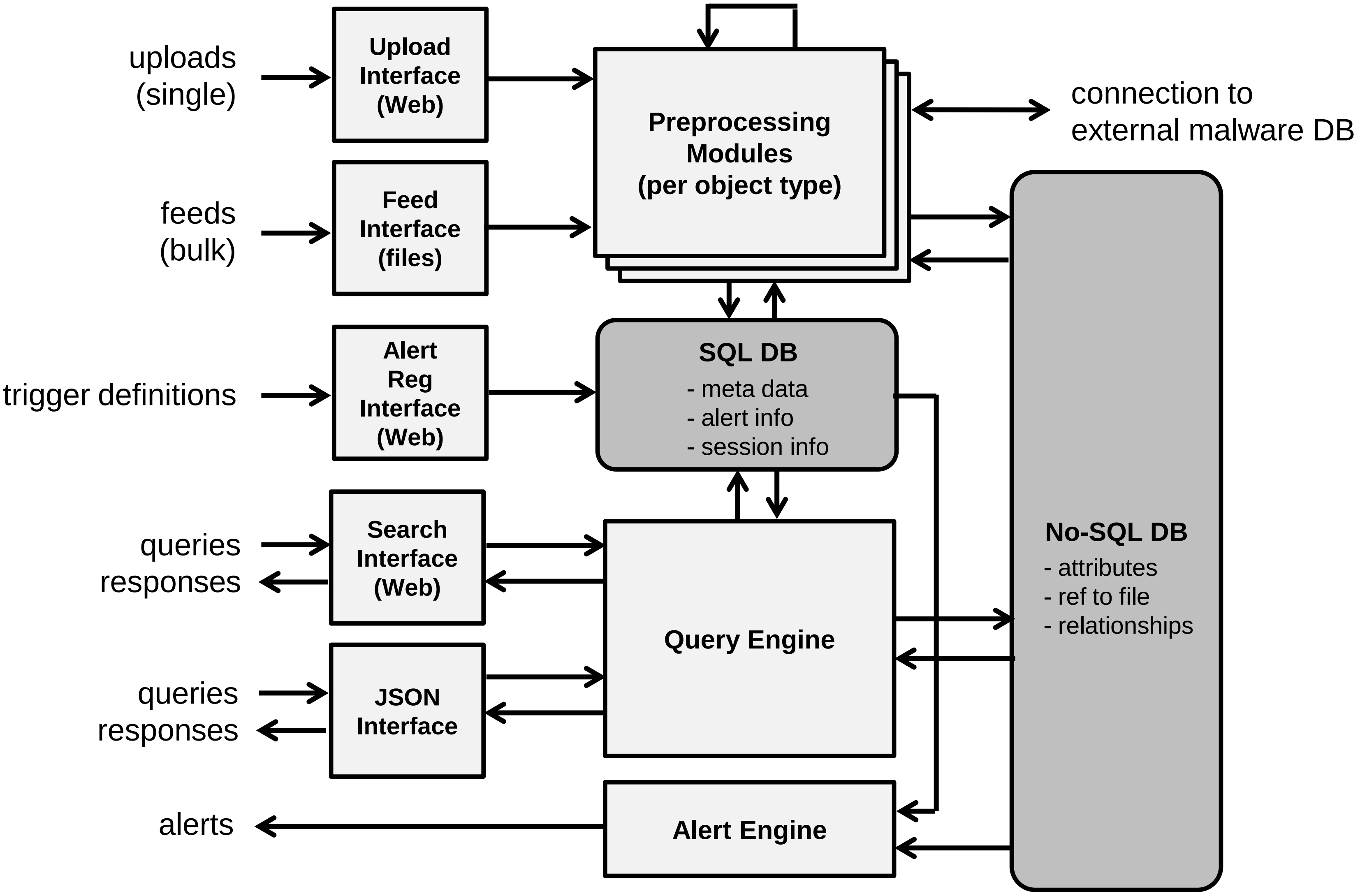
Use case: Alerting key owners



Approach

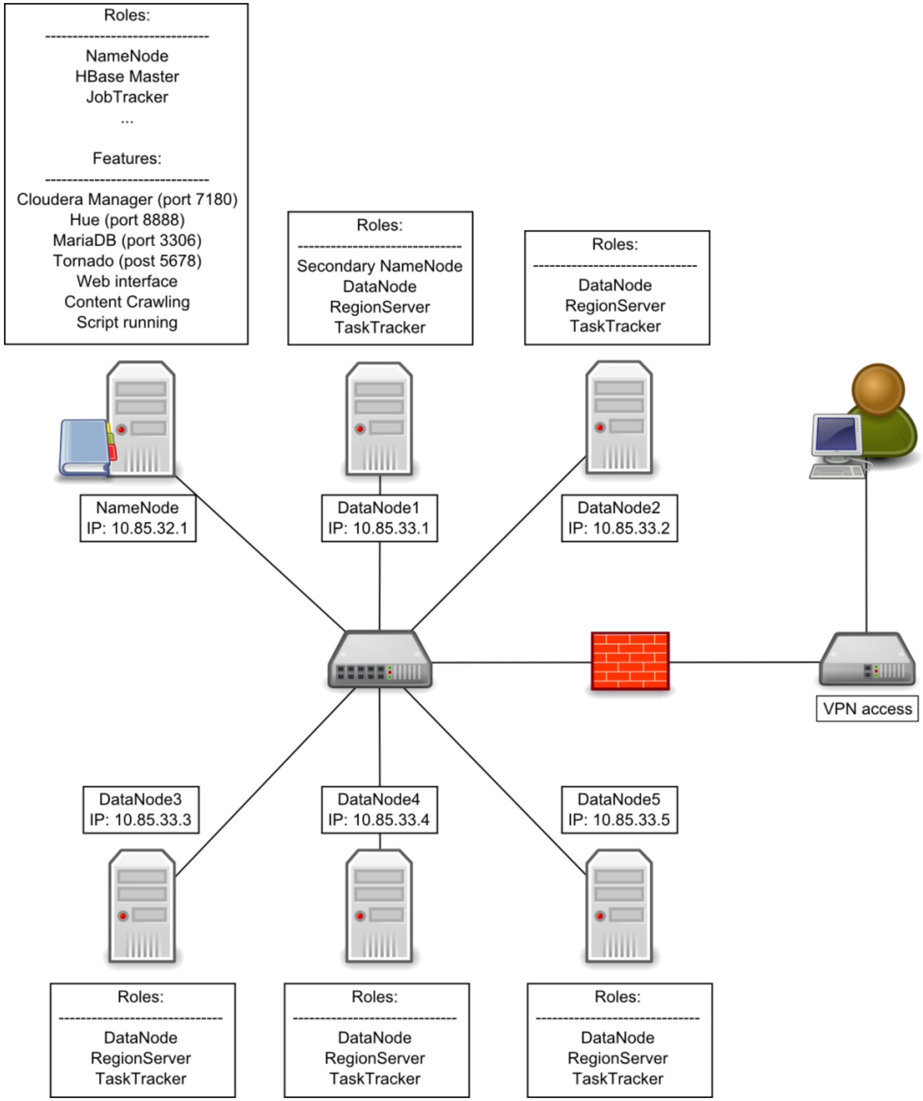
- develop a large database that can store millions of signed objects
  - Portable Executable (PE) files
  - Java Archives and Android Packages (JAR/APK)
  - public key certificates
- provide services built on top of the database
  - simple queries for file hashes
  - complex queries based on object attributes
  - visualization of relationships between signed software and certificates
  - alerting users when the system encounters an object matching some pre-registered criteria
- provide a web based and a programmatic (JSON) interface to the services
- collect signed software and certificates massively
  - proactive crawling of public sites and repositories
  - allow for uploading objects by users

System architecture



ROSCO DBs

- Hadoop cluster of 6 nodes
  - 1 name node, 5 data nodes
  - 100TB total disk space
  - ~33TB effective capacity
- HBase database
  - open source, no-SQL, distributed DB
  - tables for object attributes and relationships between objects
- regular SQL database
  - meta-data of objects
  - alert filters
  - user and session data



Roles:

NameNode
HBase Master
JobTracker
...

Features:

Cloudera Manager (port 7180)
Hue (port 8888)
MariaDB (port 3306)
Tornado (post 5678)
Web interface
Content Crawling
Script running

Roles:

Secondary NameNode
DataNode
RegionServer
TaskTracker

Roles:

DataNode
RegionServer
TaskTracker

NameNode
IP: 10.85.32.1

DataNode1
IP: 10.85.33.1

DataNode2
IP: 10.85.33.2

VPN access

DataNode3
IP: 10.85.33.3

DataNode4
IP: 10.85.33.4

DataNode5
IP: 10.85.33.5

Roles:

DataNode
RegionServer
TaskTracker

Roles:

DataNode
RegionServer
TaskTracker

Roles:

DataNode
RegionServer
TaskTracker

Object types collected

- X.509 public key certificates
  - millions of certificates collected (~60 million) by
    - acquiring available collections (e.g., SSL Observatory) and using ZMap
    - extracting certificates from signed software
- signed Portable Executables (exe, dll)
  - thousands of files collected by
    - crawling public software repos (e.g., SourceForge)
    - browsing OS distributions
    - filtering malware feeds
- signed Java Archives (jar) and Android Packages (apk)
  - thousands of files collected by crawling third party app stores

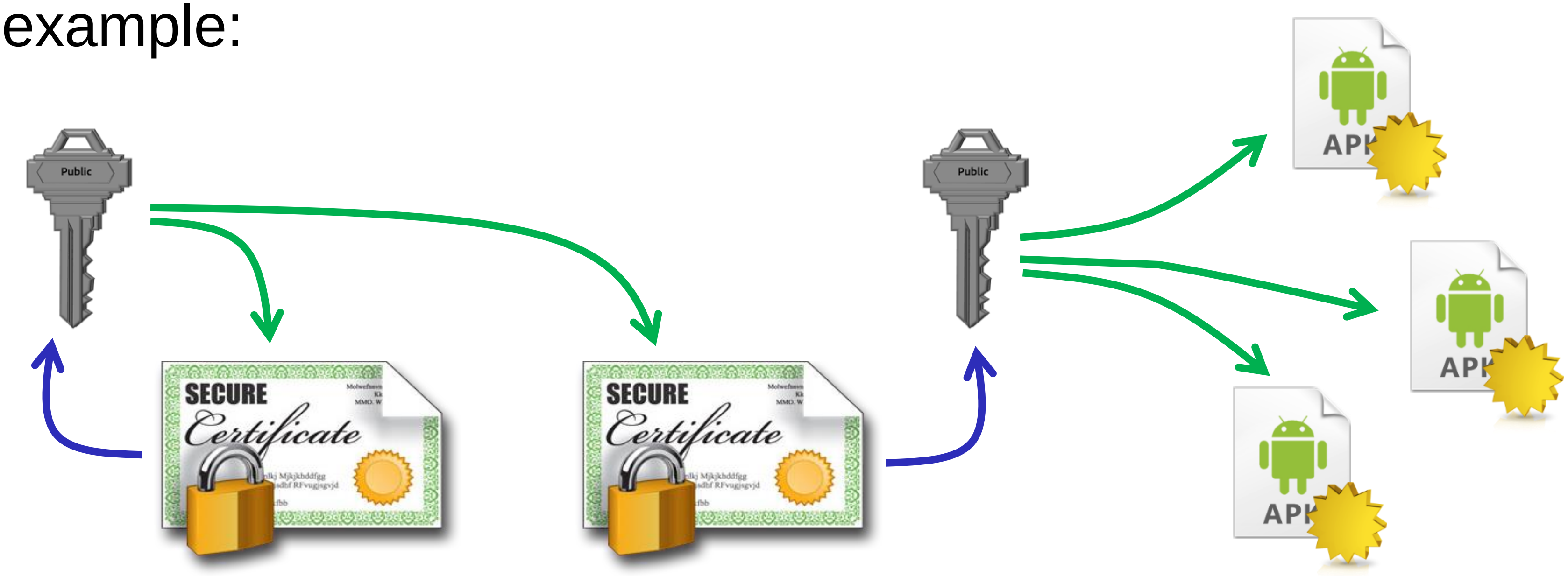
Pre-processing modules

- each object type has its own pre-processing module that parses the object and inserts appropriate data in the DBs
- parsing process may invoke other pre-processing modules
  - e.g., PE file may have certificates embedded, which are passed to the pre-processing module responsible for certificates
- duplicates are checked before inserting data into the DB
  - crawlers may return objects that have already been stored
  - in case of duplicates, only meta-data is updated
- relationships to already stored objects are identified when inserting a new object
  - is the new object signed with a known public key?
  - if the new object is a certificate, does it contain a known public key?

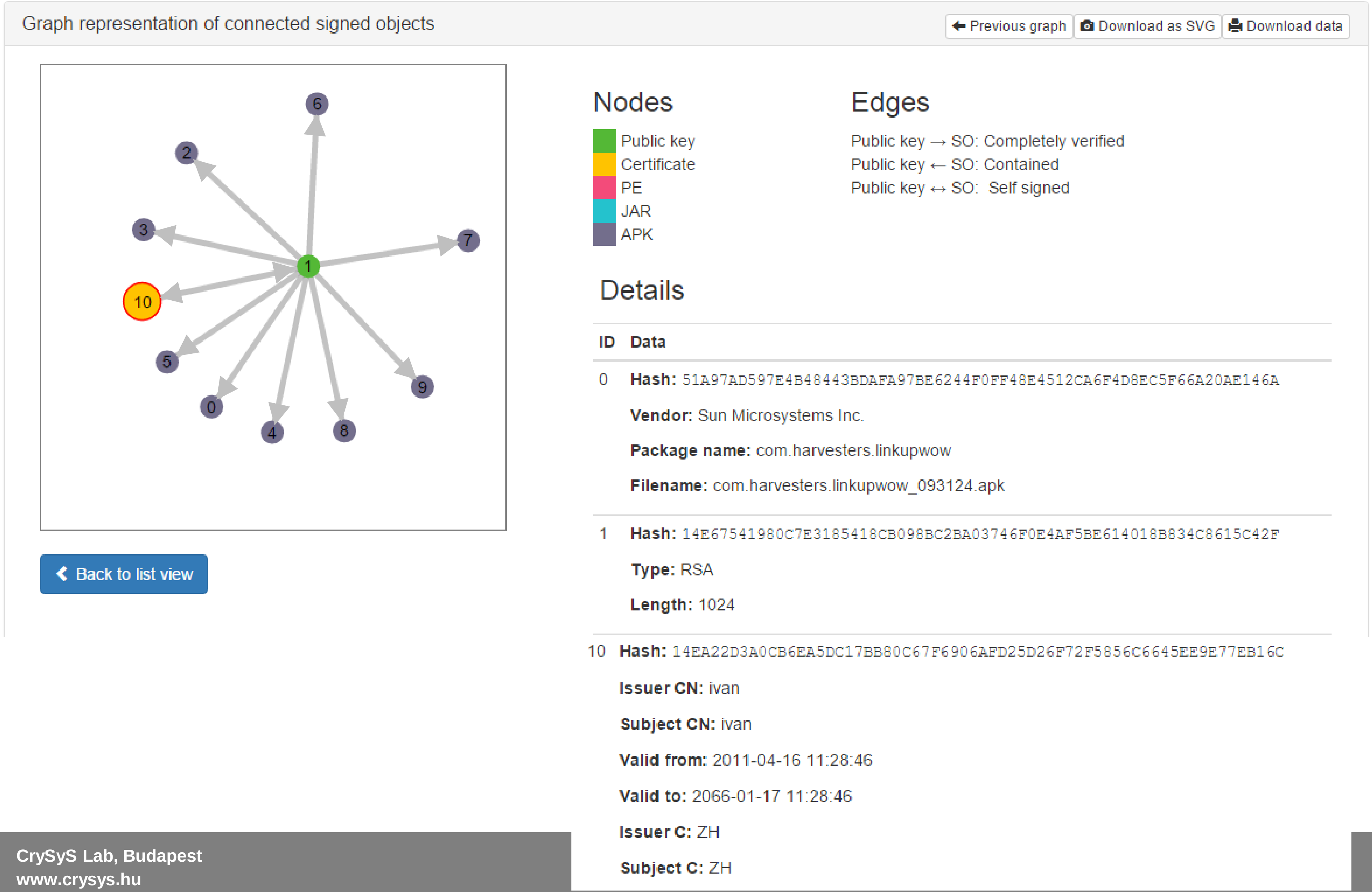
Relationships between objects

- can be represented by a directed graph
  - three types of nodes: certificate, public key, signed software
  - two types of edges:
    - certificate → public key: certificate contains the public key
    - public key → signed object : public key verifies signature

- example:



Relationships between objects



Graph representation of connected signed objects

Nodes

🟩	Public key
🟨	Certificate
🟥	PE
🟦	JAR
🟪	APK

Edges

Public key → SO: Completely verified

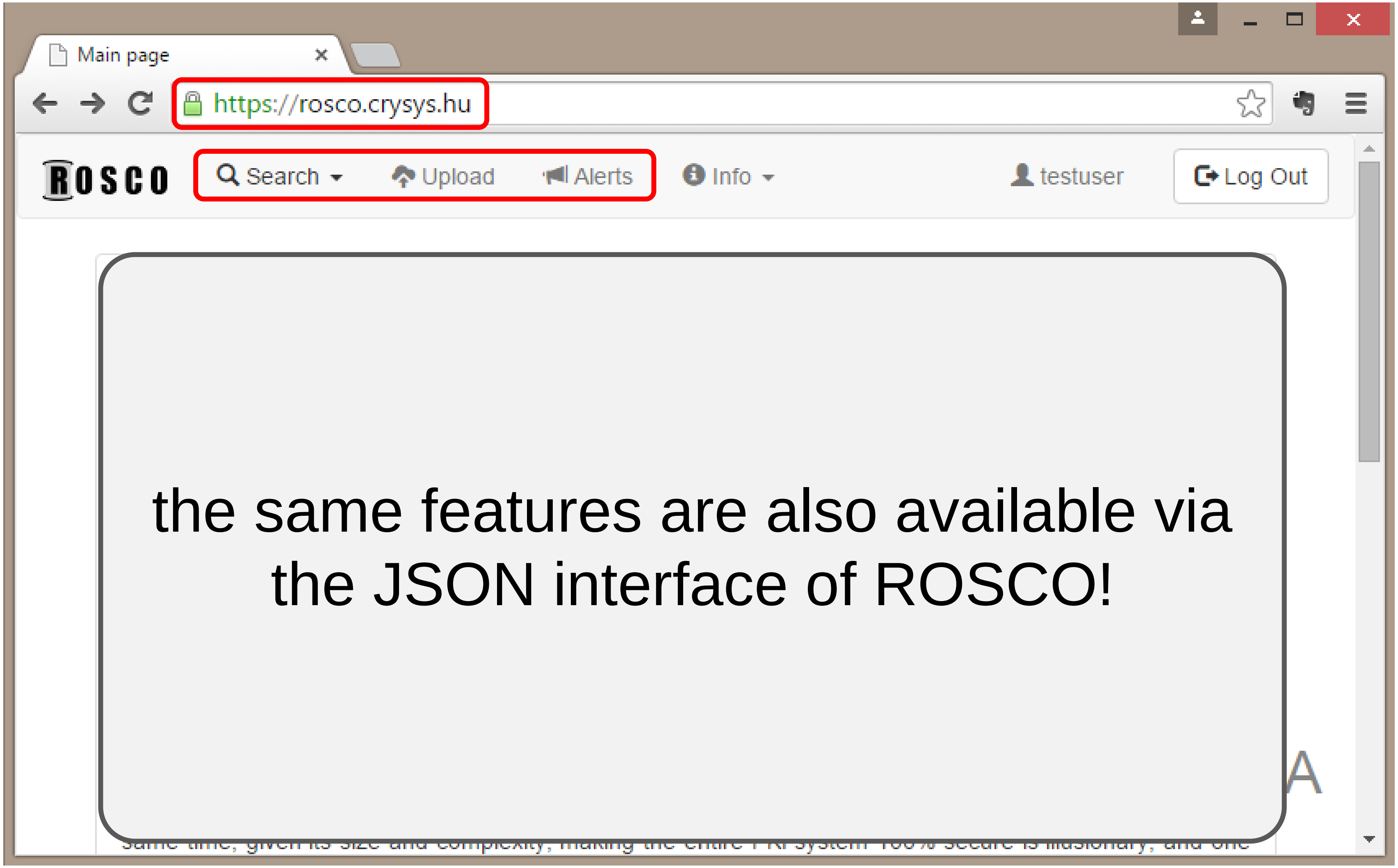
Public key ← SO: Contained

Public key ↔ SO: Self signed

Details

ID	Data
0	**Hash:** 51A97AD597E4B48443BDAFA97BE6244F0FF48E4512CA6F4D8EC5F66A20AE146A **Vendor:** Sun Microsystems Inc. **Package name:** com.harvesters.linkupwow **Filename:** com.harvesters.linkupwow_093124.apk
1	**Hash:** 14E67541980C7E3185418CB098BC2BA03746F0E4AF5BE614018B834C8615C42F **Type:** RSA **Length:** 1024
10	**Hash:** 14EA22D3A0CB6EA5DC17BB80C67F6906AFD25D26F72F5856C6645EE9E77EB16C **Issuer CN:** ivan **Subject CN:** ivan **Valid from:** 2011-04-16 11:28:46 **Valid to:** 2066-01-17 11:28:46 **Issuer C:** ZH **Subject C:** ZH

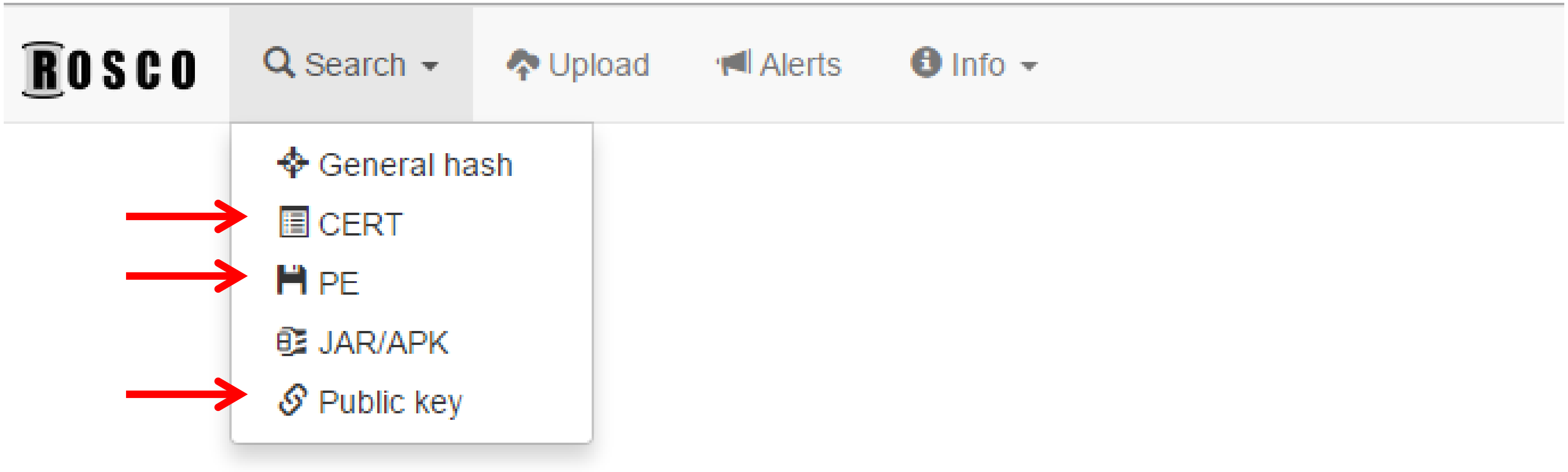
ROSCO web-based interface



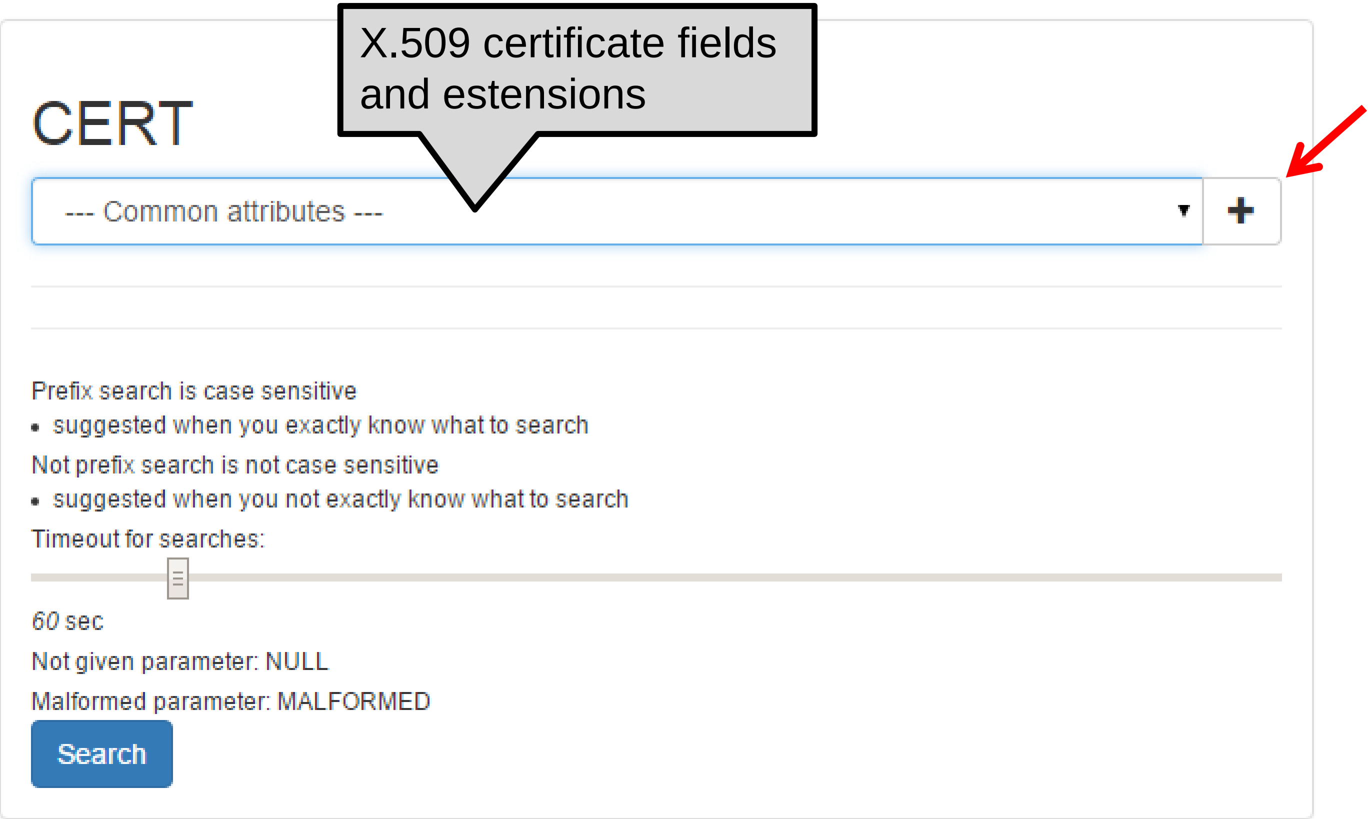
same time, given its size and complexity, making the entire PKI system 100% secure is illusionary, and one

the same features are also available via the JSON interface of ROSCO!

Search options



Certificate search



X.509 certificate fields and estensions

CERT

Prefix search is case sensitive

- suggested when you exactly know what to search

Not prefix search is not case sensitive

- suggested when you not exactly know what to search

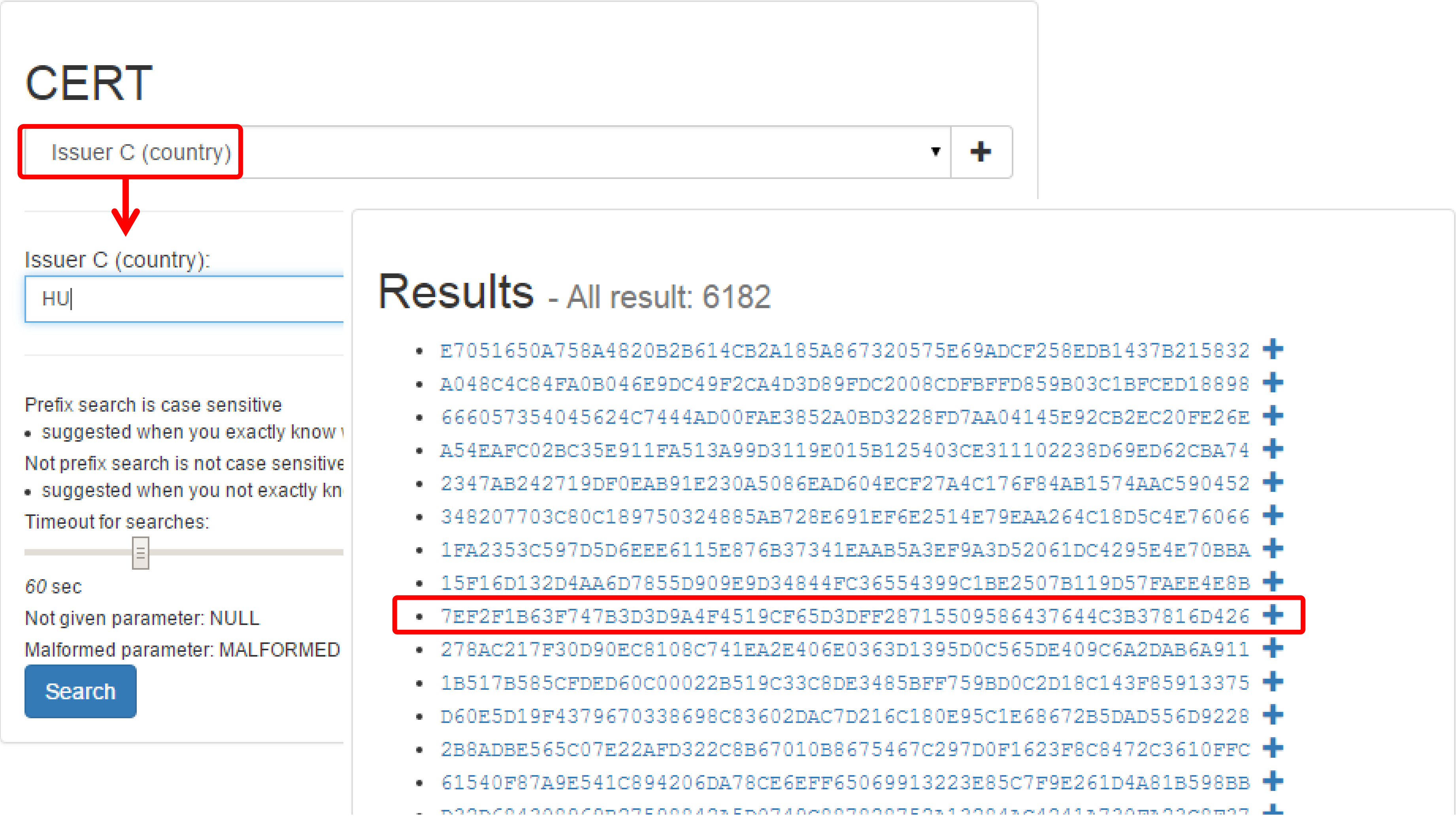
Timeout for searches:

60 sec

Not given parameter: NULL

Malformed parameter: MALFORMED

Certificate search



CERT

Issuer C (country) ▾

Issuer C (country):

HU

Prefix search is case sensitive

- suggested when you exactly know

Not prefix search is not case sensitive

- suggested when you not exactly kn

Timeout for searches:

60 sec

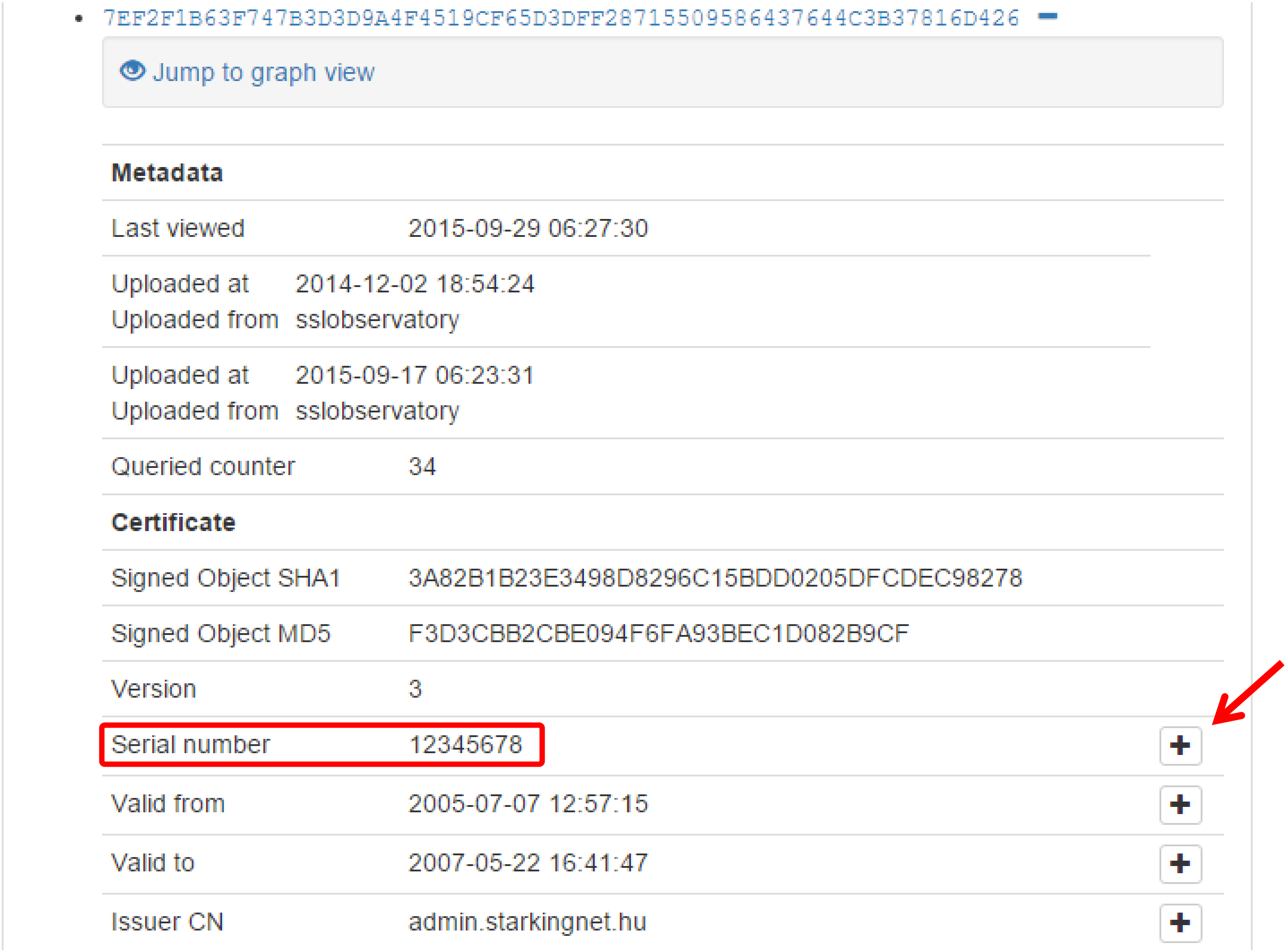
Not given parameter: NULL

Malformed parameter: MALFORMED

Results - All result: 6182

- E7051650A758A4820B2B614CB2A185A867320575E69ADCF258EDB1437B215832
- A048C4C84FA0B046E9DC49F2CA4D3D89FDC2008CDFBFFD859B03C1BFCED18898
- 66605735404562 4C7444AD00FAE3852A0BD3228FD7AA04145E92CB2EC20FE26E
- A54EAFC02BC35E911FA513A99D3119E015B125403CE311102238D69ED62CBA74
- 2347AB242719DF0EAB91E230A5086EAD604ECF27A4C176F84AB1574AAC590452
- 348207703C80C189750324885AB728E691EF6E2514E79EAA264C18D5C4E76066
- 1FA2353C597D5D6EEE6115E876B37341EAAB5A3EF9A3D52061DC4295E4E70BBA
- 15F16D132D4AA6D7855D909E9D34844FC36554399C1BE2507B119D57FAEE4E8B
- 7EF2F1B63F747B3D3D9A4F4519CF65D3DFF2871550958643764 4C3B37816D426
- 278AC217F30D90EC8108C741EA2E406E0363D1395D0C565DE409C6A2DAB6A911
- 1B517B585CFDED60C00022B519C33C8DE3485BFF759BD0C2D18C143F85913375
- D60E5D19F4379670338698C83602DAC7D216C180E95C1E68672B5DAD556D9228
- 2B8ADBE565C07E22AFD322C8B67010B8675467C297D0F1623F8C8472C3610FFC
- 61540F87A9E541C894206DA78CE6EFF65069913223E85C7F9E261D4A81B598BB

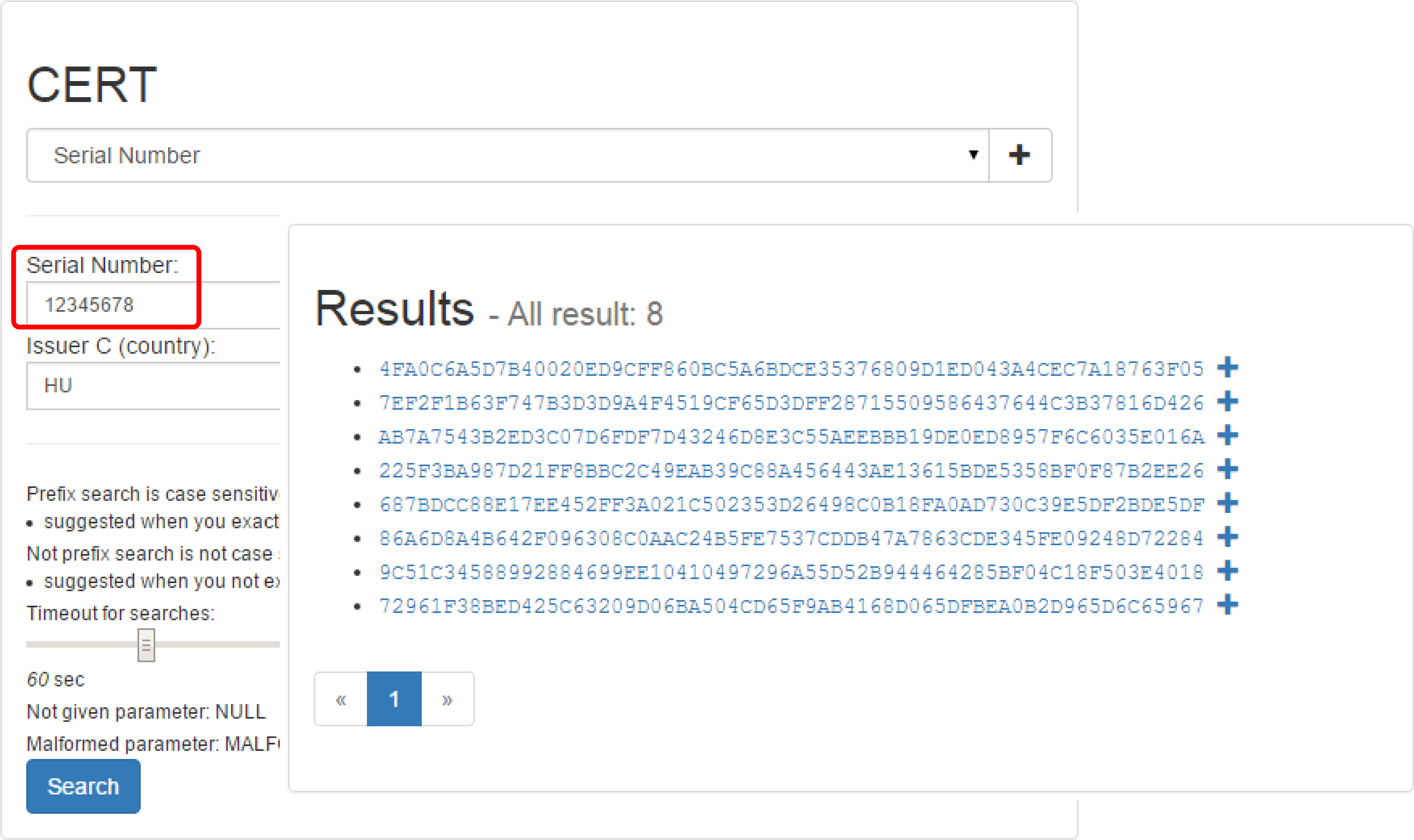
Certificate search



- 7EF2F1B63F747B3D3D9A4F4519CF65D3DFF28715509586437644C3B37816D426 −

Metadata		
Last viewed	2015-09-29 06:27:30	
Uploaded at Uploaded from	2014-12-02 18:54:24 sslobservatory	
Uploaded at Uploaded from	2015-09-17 06:23:31 sslobservatory	
Queried counter	34	
Certificate		
Signed Object SHA1	3A82B1B23E3498D8296C15BDD0205DFCDEC98278	
Signed Object MD5	F3D3CBB2CBE094F6FA93BEC1D082B9CF	
Version	3	
Serial number	12345678	+
Valid from	2005-07-07 12:57:15	+
Valid to	2007-05-22 16:41:47	+
Issuer CN	admin.starkingnet.hu	+

Certificate search



CERT

Serial Number: 12345678

Issuer C (country): HU

Prefix search is case sensitiv

- suggested when you exact

Not prefix search is not case

- suggested when you not ex

Timeout for searches:

60 sec

Not given parameter: NULL

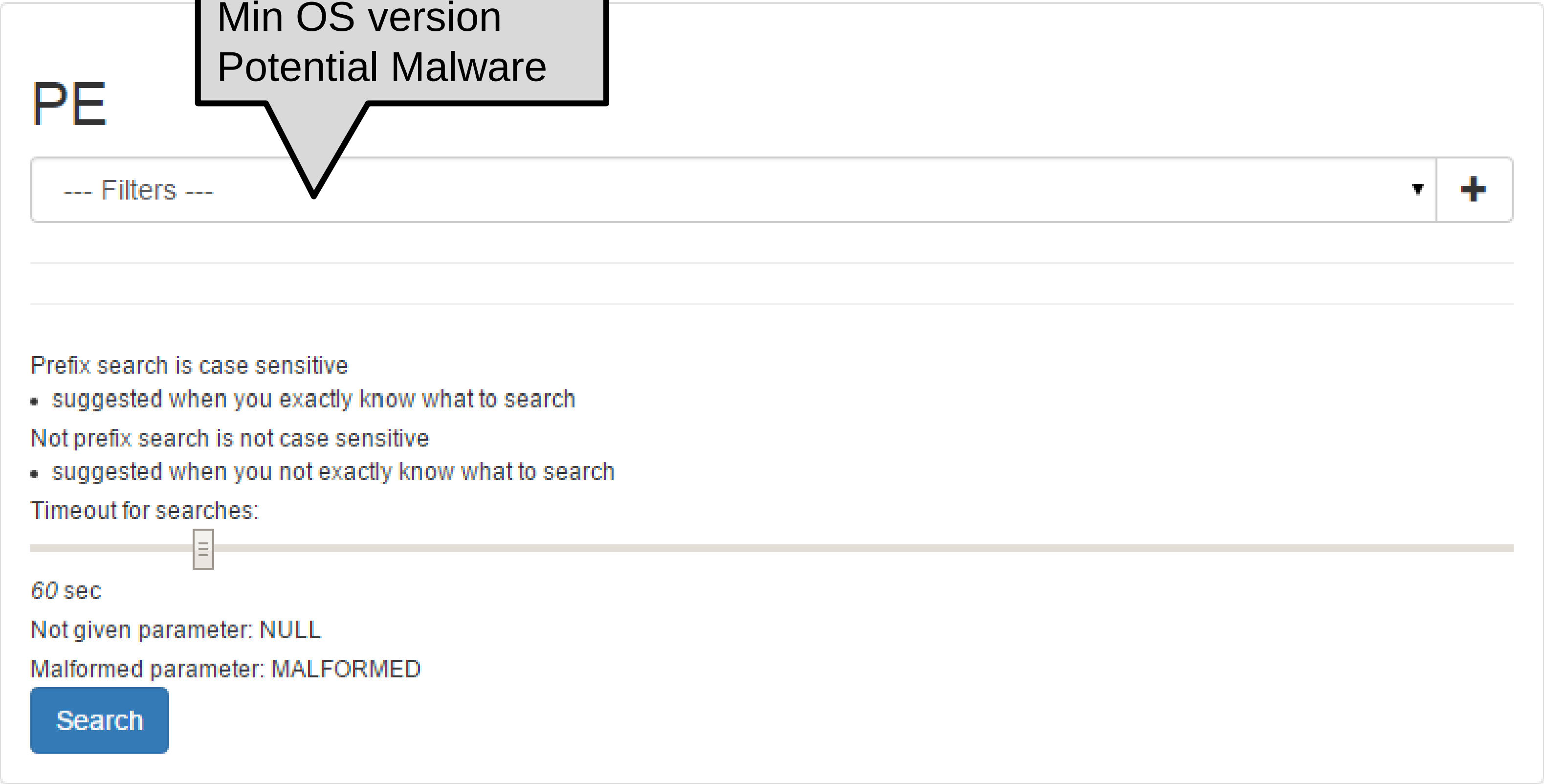
Malformed parameter: MALF

Results - All result: 8

- 4FA0C6A5D7B40020ED9CFF860BC5A6BDCE35376809D1ED043A4CEC7A18763F05 +
- 7EF2F1B63F747B3D3D9A4F4519CF65D3DFF2871550958643764 4C3B37816D426 +
- AB7A7543B2ED3C07D6FDF7D43246D8E3C55AEEBBB19DE0ED8957F6C6035E016A +
- 225F3BA987D21FF8BBC2C49EAB39C88A456443AE13615BDE5358BF0F87B2EE26 +
- 687BDCC88E17EE452FF3A021C502353D26498C0B18FA0AD730C39E5DF2BDE5DF +
- 86A6D8A4B642F096308C0AAC24B5FE7537CDDB47A7863CDE345FE09248D72284 +
- 9C51C3458899288469 9EE10410497296A55D52B944464285BF04C18F503E4018 +
- 72961F38BED425C63209D06BA504CD65F9AB4168D065DFBEA0B2D965D6C65967 +

PE search

Type
Filename
Timestamp
Min OS version
Potential Malware



PE

Prefix search is case sensitive

- suggested when you exactly know what to search

Not prefix search is not case sensitive

- suggested when you not exactly know what to search

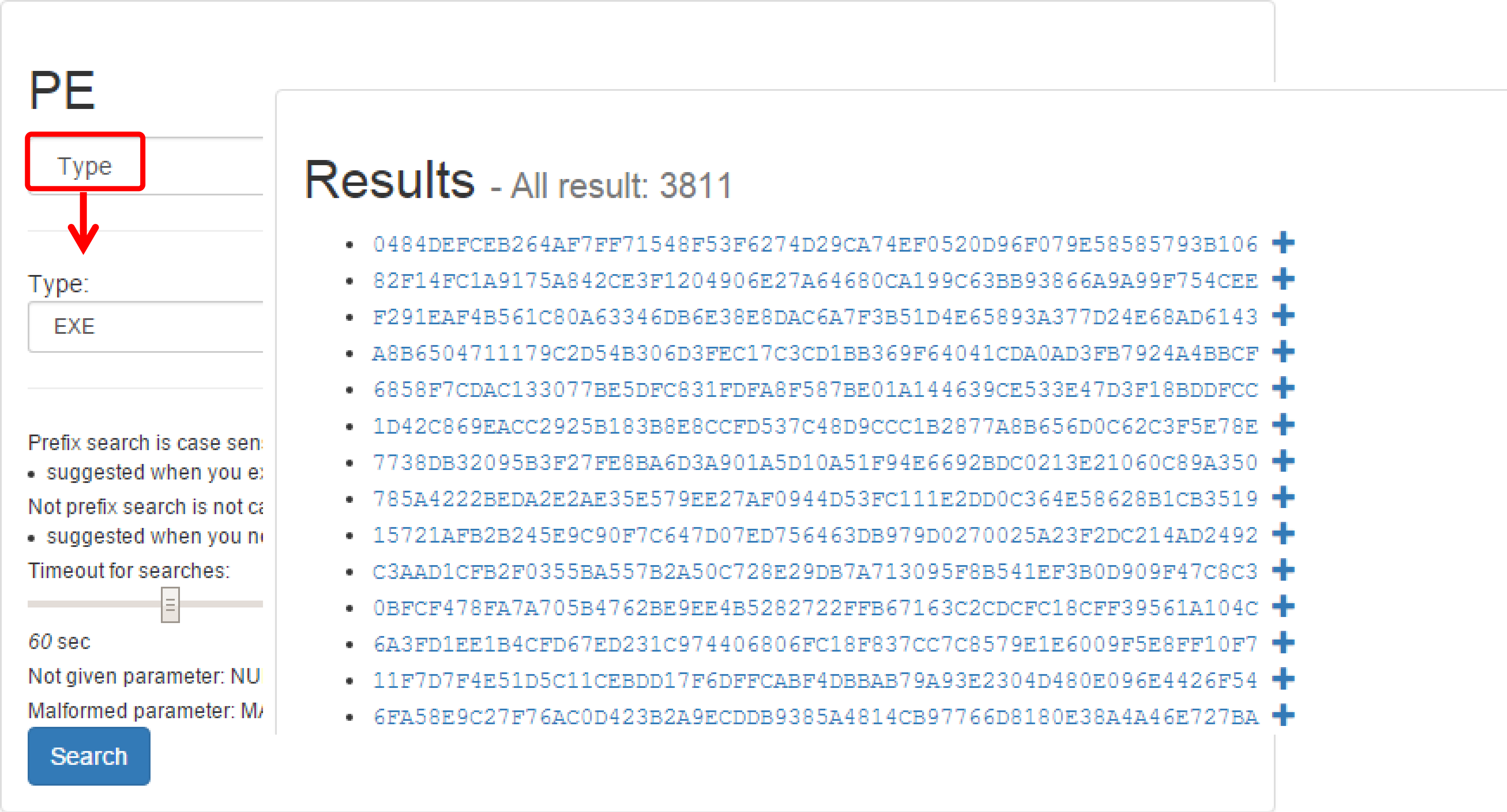
Timeout for searches:

60 sec

Not given parameter: NULL

Malformed parameter: MALFORMED

PE search



PE

Type: EXE

Prefix search is case sen

- suggested when you e

Not prefix search is not ca

- suggested when you n

Timeout for searches:

60 sec

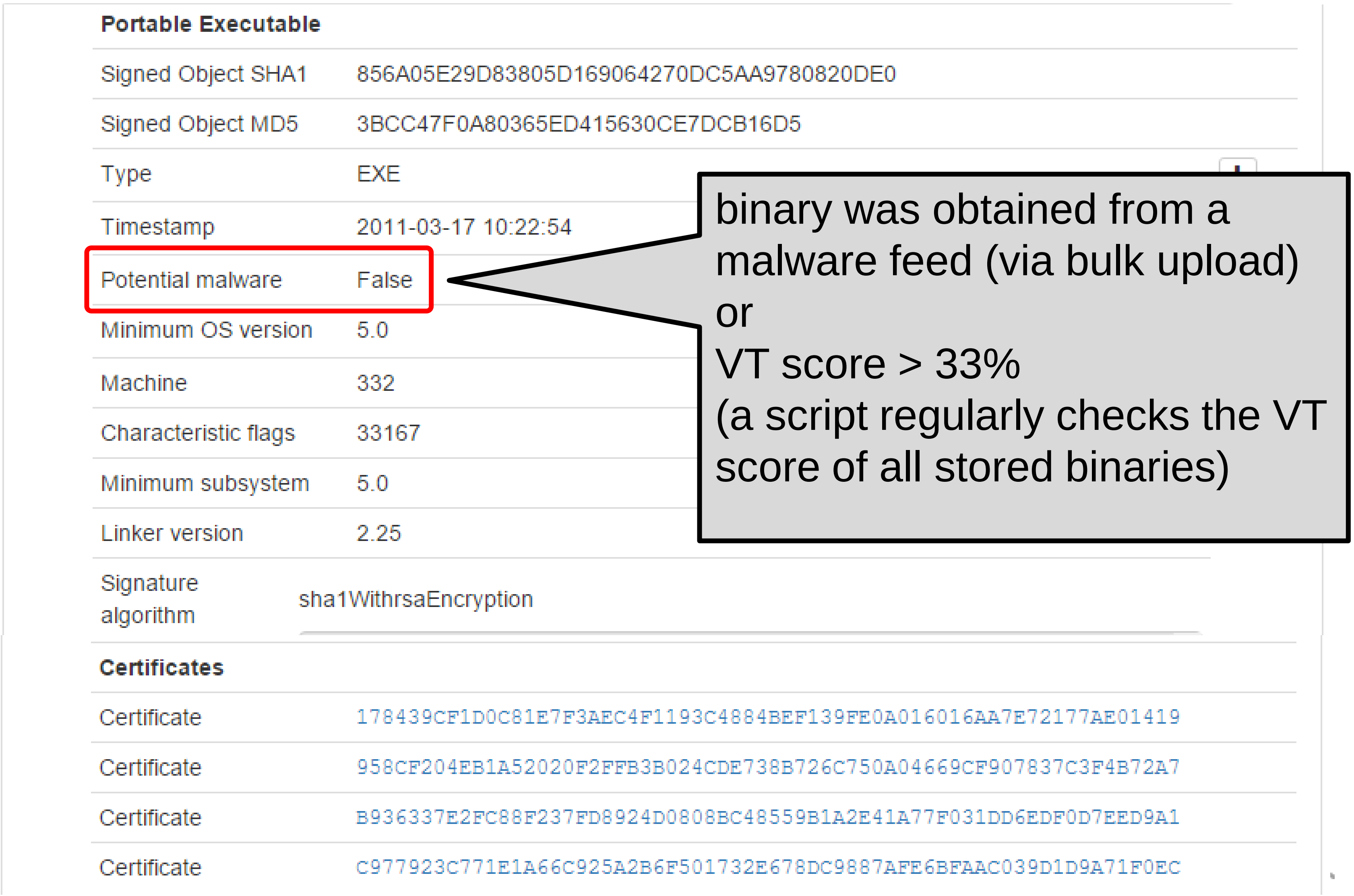
Not given parameter: NU

Malformed parameter: M/

Results - All result: 3811

- 0484DEFCEB264AF7FF71548F53F6274D29CA74EF0520D96F079E58585793B106 ✚
- 82F14FC1A9175A842CE3F1204906E27A64680CA199C63BB93866A9A99F754CEE ✚
- F291EAF4B561C80A63346DB6E38E8DAC6A7F3B51D4E65893A377D24E68AD6143 ✚
- A8B6504711179C2D54B306D3FEC17C3CD1BB369F64041CDA0AD3FB7924A4BBCF ✚
- 6858F7CDAC133077BE5DFC831FDFA8F587BE01A144639CE533E47D3F18BDDFCC ✚
- 1D42C869EACC2925B183B8E8CCFD537C48D9CCC1B2877A8B656D0C62C3F5E78E ✚
- 7738DB32095B3F27FE8BA6D3A901A5D10A51F94E6692BDC0213E21060C89A350 ✚
- 785A4222BEDA2E2AE35E579EE27AF0944D53FC111E2DD0C364E58628B1CB3519 ✚
- 15721AFB2B245E9C90F7C647D07ED756463DB979D0270025A23F2DC214AD2492 ✚
- C3AAD1CFB2F0355BA557B2A50C728E29DB7A713095F8B541EF3B0D909F47C8C3 ✚
- 0BFCF478FA7A705B4762BE9EE4B5282722FFB67163C2CDCFC18CFF39561A104C ✚
- 6A3FD1EE1B4CFD67ED231C974406806FC18F837CC7C8579E1E6009F5E8FF10F7 ✚
- 11F7D7F4E51D5C11CEBDD17F6DFFCABF4DBBAB79A93E2304D480E096E4426F54 ✚
- 6FA58E9C27F76AC0D423B2A9ECDDB9385A4814CB97766D8180E38A4A46E727BA ✚

PE search

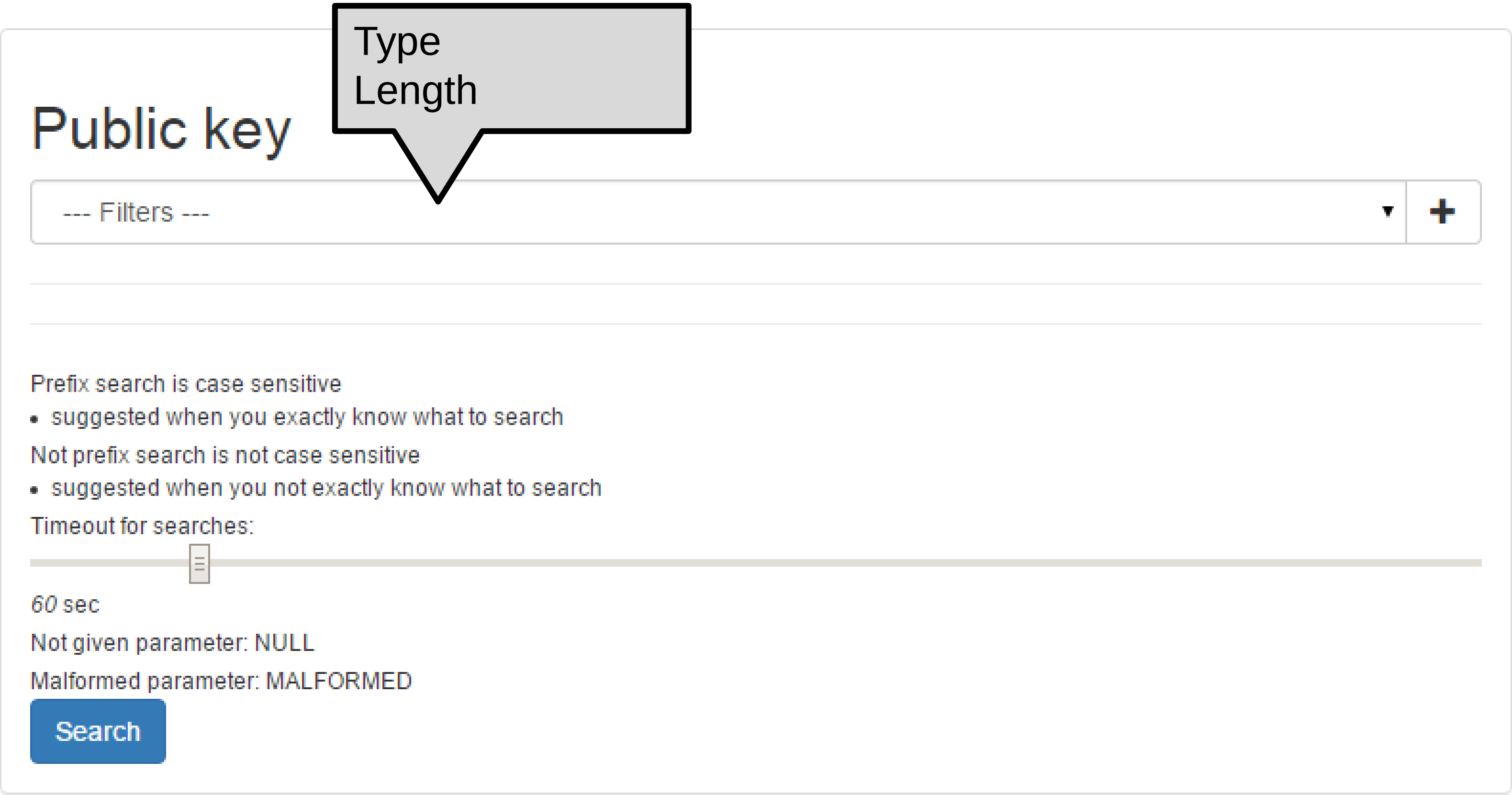


Portable Executable	
Signed Object SHA1	856A05E29D83805D169064270DC5AA9780820DE0
Signed Object MD5	3BCC47F0A80365ED415630CE7DCB16D5
Type	EXE
Timestamp	2011-03-17 10:22:54
Potential malware	False
Minimum OS version	5.0
Machine	332
Characteristic flags	33167
Minimum subsystem	5.0
Linker version	2.25
Signature algorithm	sha1WithrsaEncryption

Certificates	
Certificate	178439CF1D0C81E7F3AEC4F1193C4884BEF139FE0A016016AA7E72177AE01419
Certificate	958CF204EB1A52020F2FFB3B024CDE738B726C750A04669CF907837C3F4B72A7
Certificate	B936337E2FC88F237FD8924D0808BC48559B1A2E41A77F031DD6EDF0D7EED9A1
Certificate	C977923C771E1A66C925A2B6F501732E678DC9887AFE6BFAAC039D1D9A71F0EC

binary was obtained from a malware feed (via bulk upload)
or
VT score > 33%
(a script regularly checks the VT score of all stored binaries)

Public key search



Type
Length

Public key

Prefix search is case sensitive

- suggested when you exactly know what to search

Not prefix search is not case sensitive

- suggested when you not exactly know what to search

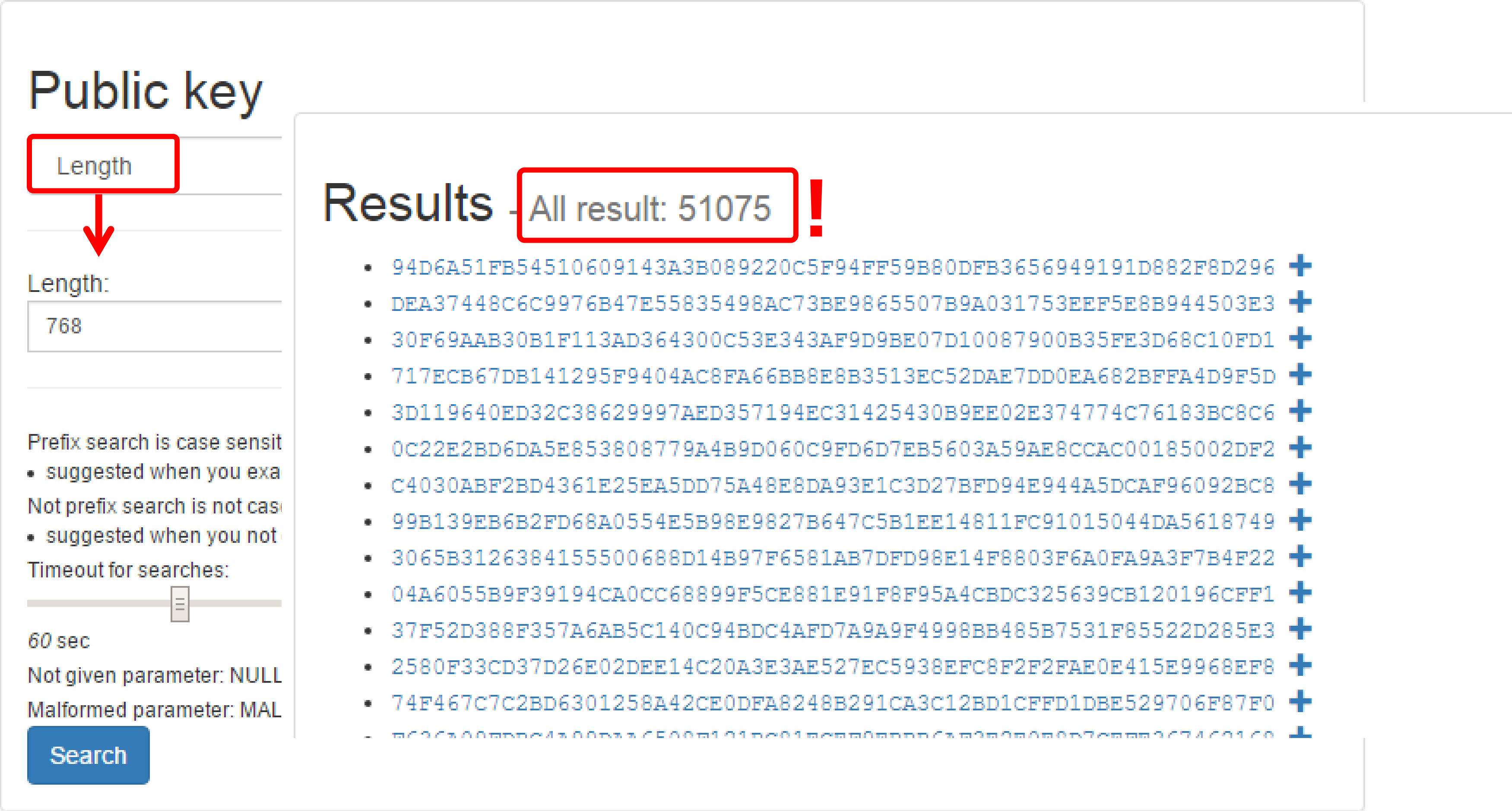
Timeout for searches:

60 sec

Not given parameter: NULL

Malformed parameter: MALFORMED

Public key search



Public key

Length:

768

Prefix search is case sensit

- suggested when you exa

Not prefix search is not cas

- suggested when you not

Timeout for searches:

60 sec

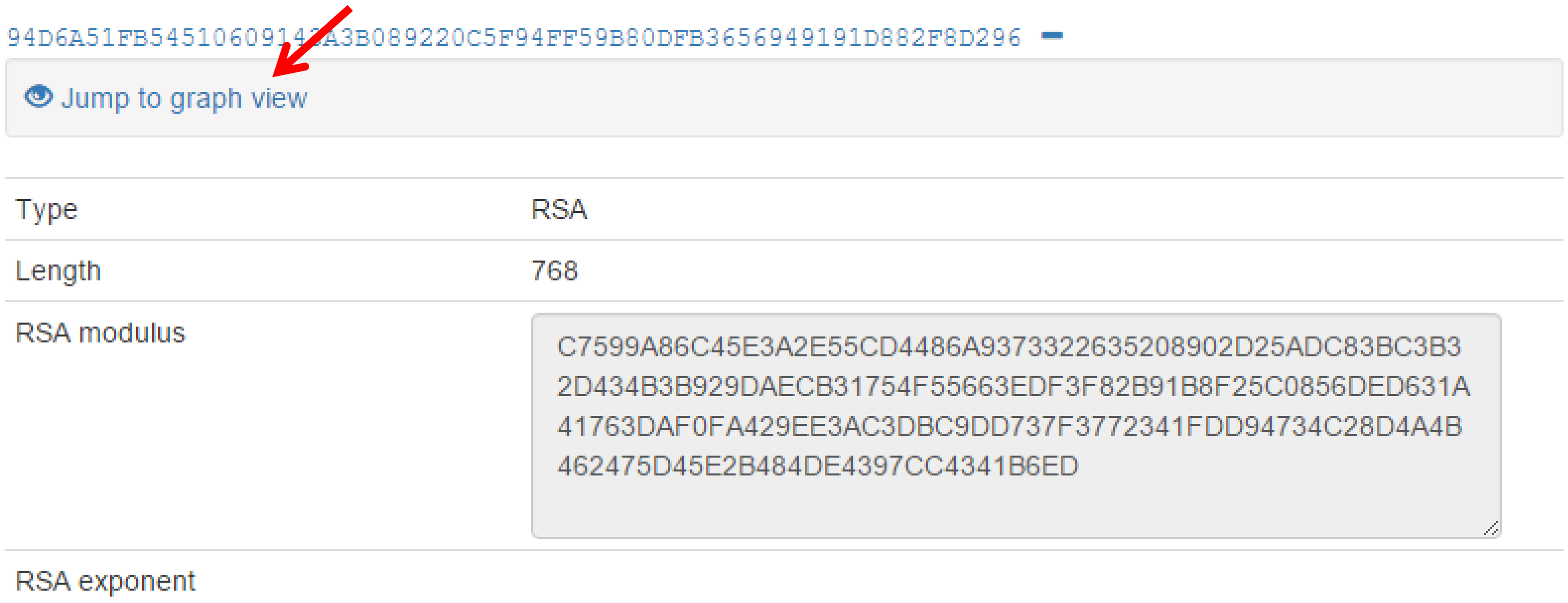
Not given parameter: NULL

Malformed parameter: MAL

Results - All result: 51075 !

- 94D6A51FB5451060914 3A3B089220C5F94FF59B80DFB3656949191D882F8D296 +
- DEA37448C6C9976B47E55835498AC73BE9865507B9A031753EEF5E8B944503E3 +
- 30F69AAB30B1F113AD364300C53E343AF9D9BE07D10087900B35FE3D68C10FD1 +
- 717ECB67DB141295F9404AC8FA66BB8E8B3513EC52DAE7DD0EA682BFFA4D9F5D +
- 3D119640ED32C38629997AED357194EC31425430B9EE02E374774C76183BC8C6 +
- 0C22E2BD6DA5E853808779A4B9D060C9FD6D7EB5603A59AE8CCAC00185002DF2 +
- C4030ABF2BD4361E25EA5DD75A48E8DA93E1C3D27BFD94E944A5DCAF96092BC8 +
- 99B139EB6B2FD68A0554E5B98E9827B647C5B1EE14811FC91015044DA5618749 +
- 3065B31263841555006 88D14B97F6581AB7DFD98E14F8803F6A0FA9A3F7B4F22 +
- 04A6055B9F39194CA0CC68899F5CE881E91F8F95A4CBDC325639CB120196CFF1 +
- 37F52D388F357A6AB5C140C94BDC4AFD7A9A9F4998BB485B7531F85522D285E3 +
- 2580F33CD37D26E02DEE14C20A3E3AE527EC5938EFC8F2F2FAE0E415E9968EF8 +
- 74F467C7C2BD6301258A42CE0DFA8248B291CA3C12BD1CFFD1DBE529706F87F0 +

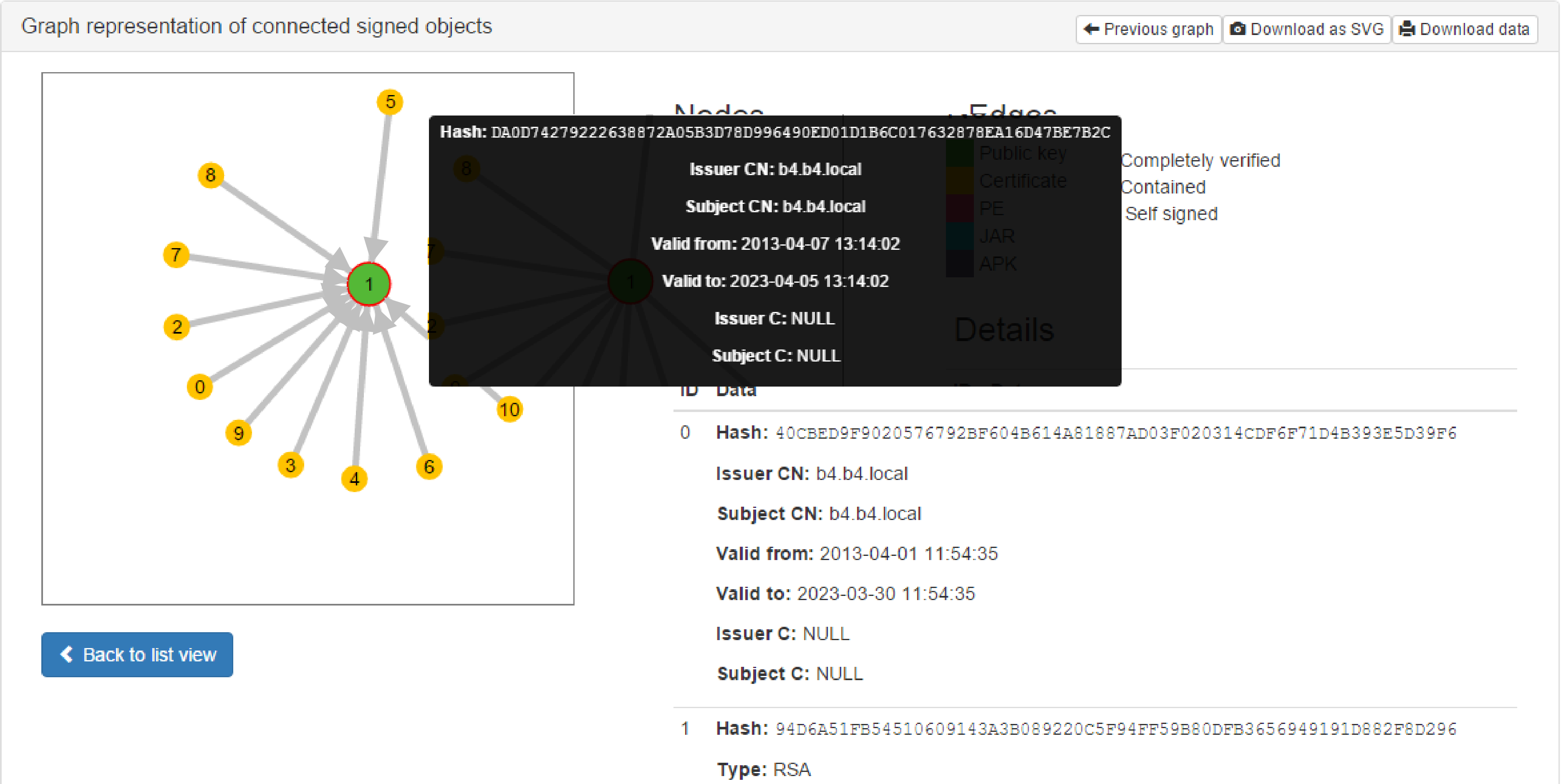
Public key search



94D6A51FB54510609142A3B089220C5F94FF59B80DFB3656949191D882F8D296 −

Type	RSA
Length	768
RSA modulus	C7599A86C45E3A2E55CD4486A9373322635208902D25ADC83BC3B3 2D434B3B929DAECB31754F55663EDF3F82B91B8F25C0856DED631A 41763DAF0FA429EE3AC3DBC9DD737F3772341FDD94734C28D4A4B 462475D45E2B484DE4397CC4341B6ED
RSA exponent	

Public key search – graph view



Graph representation of connected signed objects

Hash: DA0D74279222638872A05B3D78D996490ED01D1B6C017632878EA16D47BE7B2C

Issuer CN: b4.b4.local

Subject CN: b4.b4.local

Valid from: 2013-04-07 13:14:02

Valid to: 2023-04-05 13:14:02

Issuer C: NULL

Subject C: NULL

Nodes

- Public key
- Certificate
- PE
- JAR
- APK

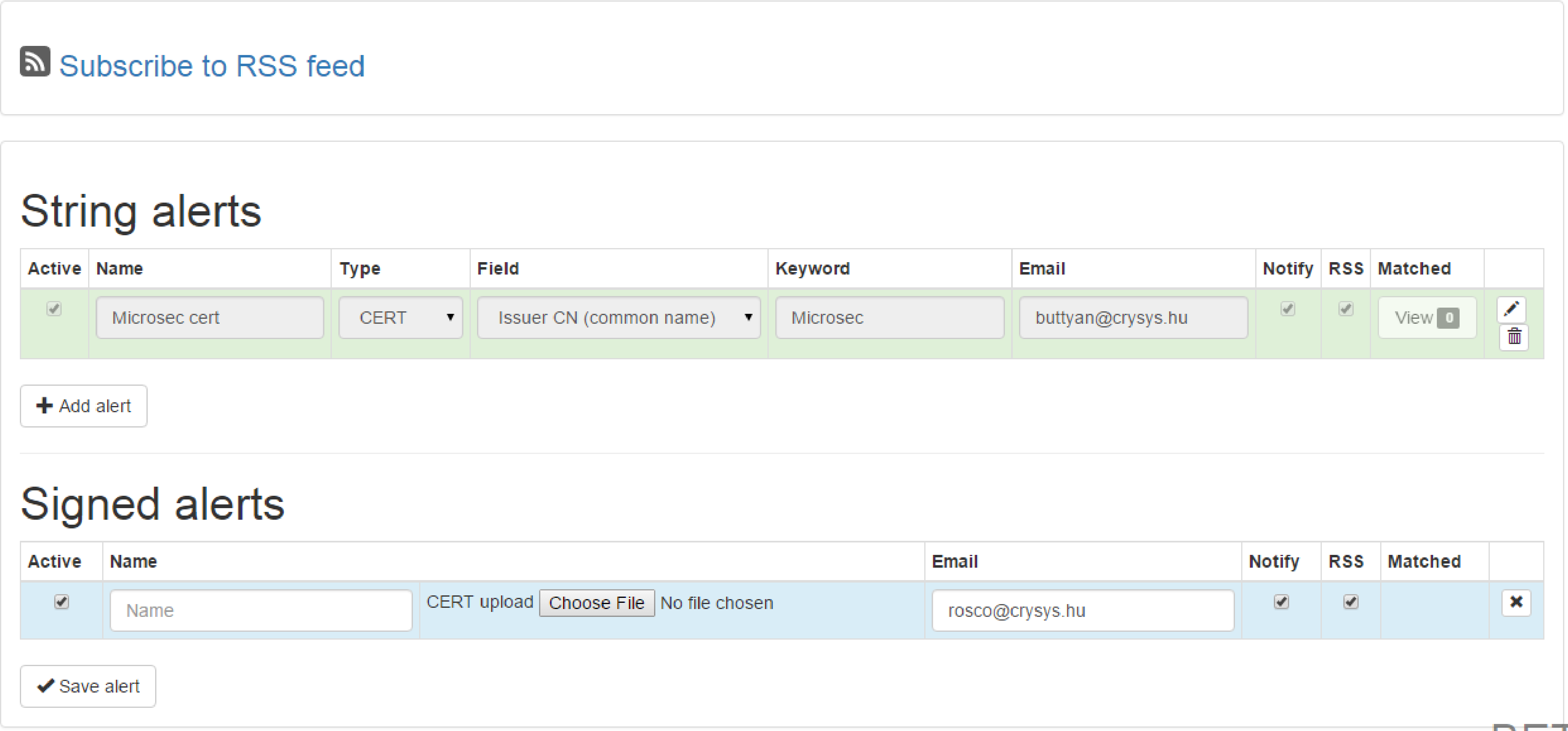
Edges

- Completely verified
- Contained
- Self signed

Details

ID	Data
0	**Hash:** 40CBED9F9020576792BF604B614A81887AD03F020314CDF6F71D4B393E5D39F6 **Issuer CN:** b4.b4.local **Subject CN:** b4.b4.local **Valid from:** 2013-04-01 11:54:35 **Valid to:** 2023-03-30 11:54:35 **Issuer C:** NULL **Subject C:** NULL
1	**Hash:** 94D6A51FB54510609143A3B089220C5F94FF59B80DFB3656949191D882F8D296 **Type:** RSA

Alerts



Subscribe to RSS feed

String alerts

Active	Name	Type	Field	Keyword	Email	Notify	RSS	Matched	
☑	Microsec cert	CERT ▾	Issuer CN (common name) ▾	Microsec	buttyan@crysys.hu	☑	☑	View 0	✎ 🗑

+ Add alert

Signed alerts

Active	Name		Email	Notify	RSS	Matched	
☑	Name	CERT upload Choose File No file chosen	rosco@crysys.hu	☑	☑		✖

✔ Save alert

Why should anyone use ROSCO?

- end-user
  - ROSCO helps identifying potentially malicious software before it is installed
- singing party (CA or software maker)
  - ROSCO helps detecting key compromise and fake certificates
- software platform operators (e.g., operating system providers and global software service providers)
  - they are also signing parties
  - providing data to ROSCO helps to maintain trust in their platform
- security companies
  - ROSCO can be an additional source of information
    - on end-user behavior (what applications they install?)
    - on attack campaigns and trends in signing malicious code
- regulators and authoritites
  - ROSCO can help them to derive statistics that can serve as an input when defining global defense strategies and coordination mechanisms

Potential limitations

- central database operated by a single entity
  - needs to be trusted (→ independent academic research lab)
  - single point of failure (→ only extends current PKI, not replaces it)
- database must be fed with new data all the time
  - new signed objects (code and certificates)
  - regular update of ”potential malware” flags
- users should learn about ROSCO and be motivated to use it
  - average user may not understand how ROSCO differs from Virus Total, Google’s Certificate Transparency, or Microsoft SmartScreen’s Filter
- signing parties should learn about ROSCO and be motivated to use it
  - usefulness of the alert service depends on the upload rate of new content and the overall coverage of ROSCO

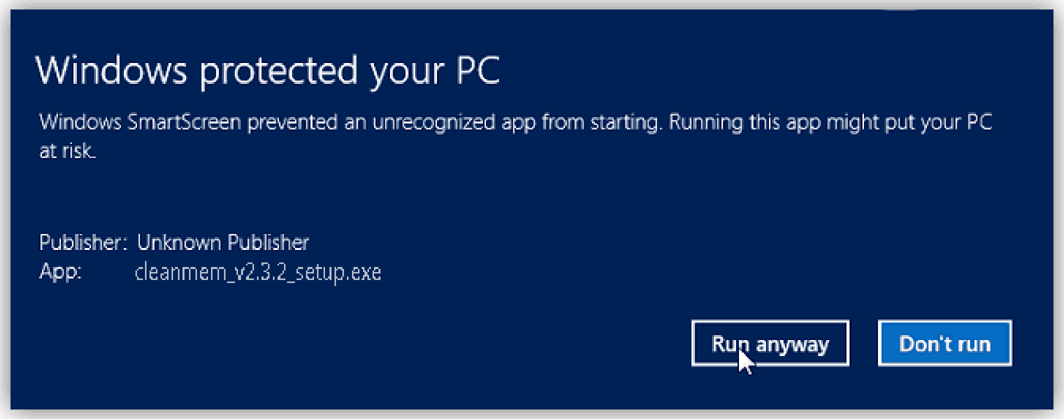
Related work

- Virus Total
  - also allows for identifying potentially malicious software
  - based on a completely different approach
    - scanning submitted file with AV products
  - does not detect new malware immediately
    - ROSCO can identify fresh malware based on signer information
  - however, unlike ROSCO, VT also works for unsigned software

→ ROSCO complements the services provided by Virus Total

Related work

- Windows SmartScreen
  - a feature that helps to detect phishing websites and protects the user from installing malware
    - checks the visited sites against a dynamic list of reported phishing sites
    - checks files downloaded from the web against a black list of reported malicious software and a white list of well-known applications
  - only works on Windows
  - details are not public
    - are digital signatures used to reduce false positives?
    - does it use any other reputation information?



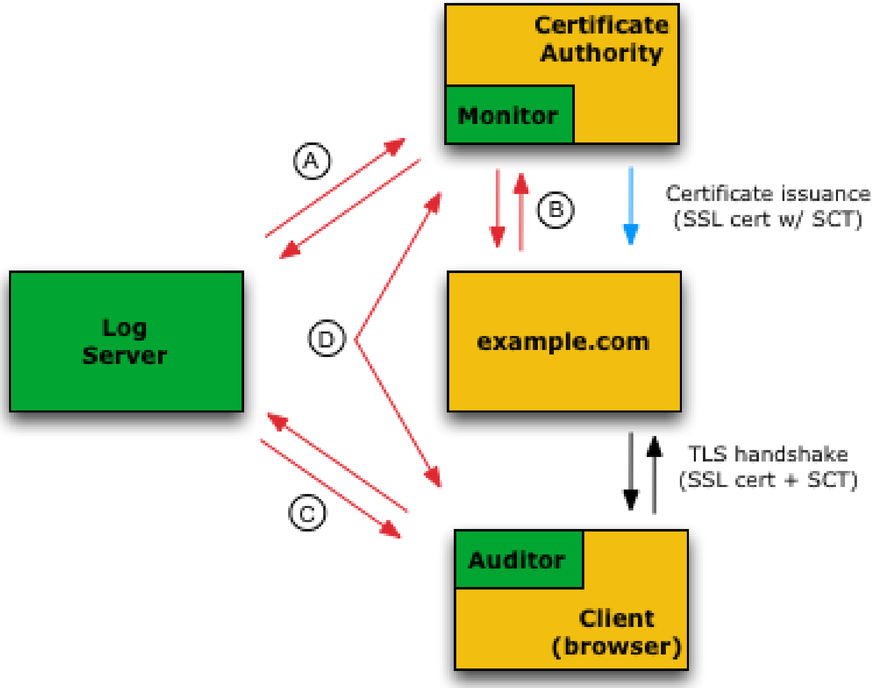
Windows protected your PC

Windows SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.

Publisher: Unknown Publisher
App: cleanmem_v2.3.2_setup.exe

Related work

- Google Certificate Transparency
  - makes it possible to detect certificates that have been mistakenly issued or maliciously acquired
  - based on three components
    - Certificate Logs
      - publicly auditable, append-only records of certificates
    - Monitors
      - periodically contact all of the log servers and watch for suspicious certificates
    - Auditors
      - verify that a particular certificate appears in a log
  - similar concept but focuses only on SSL/TLS certificates



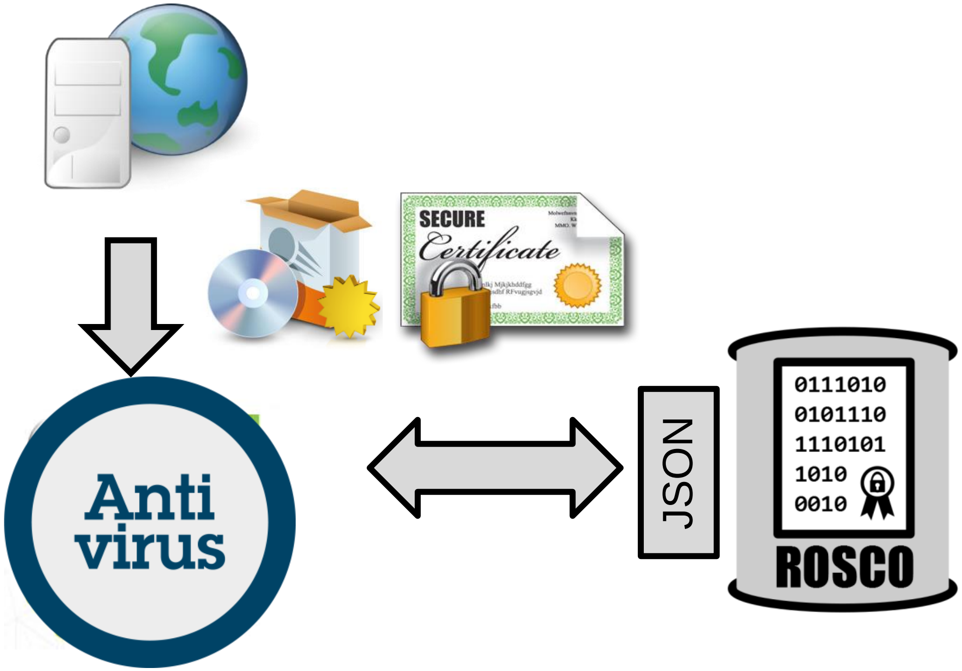
Ⓐ Monitors watch logs for suspicious certs and verify that all logged certs are visible.

Ⓑ Certificate owners query monitors to verify that nobody has logged illegitimate certs for their domain.

Ⓒ Auditors verify that logs are behaving properly; they can also verify that a particular cert has been logged.

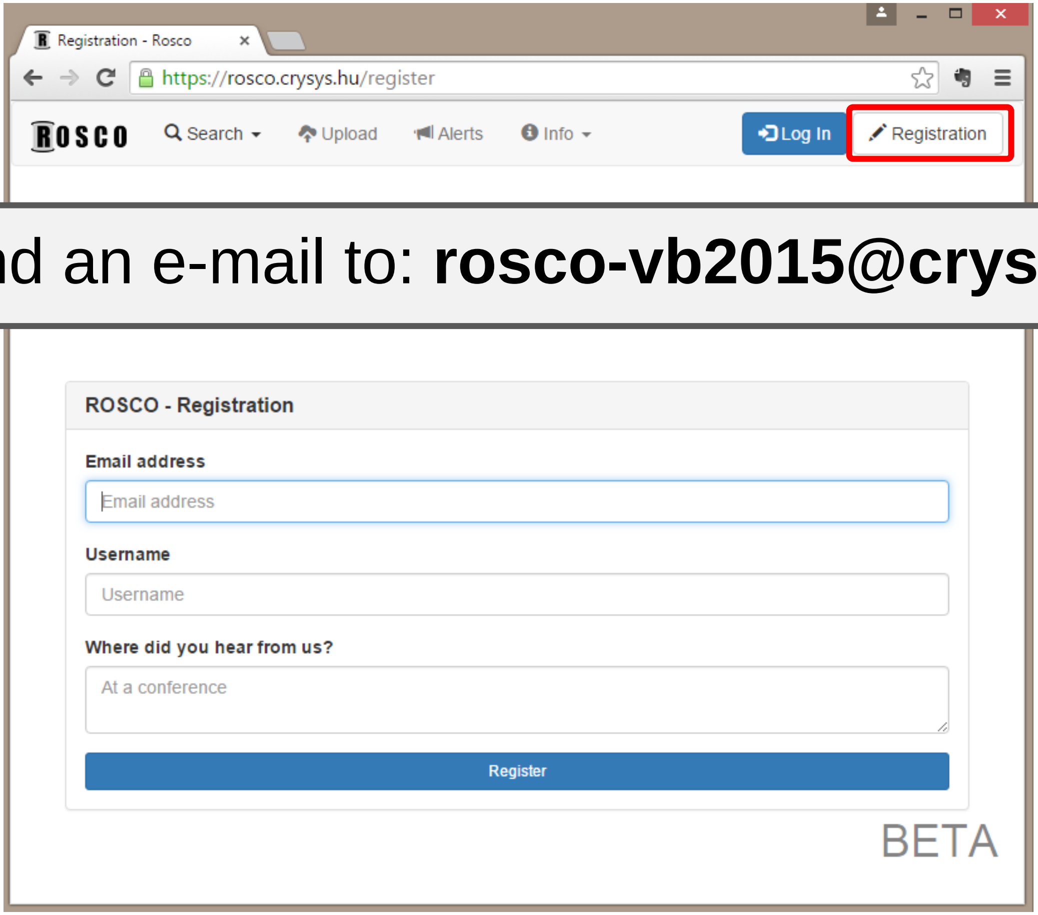
Ⓓ Monitors and auditors exchange information about logs to help detect forked or branched logs.

Future plans



- acquire more data
  - continue crawling
  - develop collector apps
    - browser plug-in
    - mobile app
  - collaboration
  - build and run a Monitor for Certificate Transparency
- search for interesting anomalies and statistics in the DB
- open ROSCO for public non-commercial use

Interested in trying out?



ROSCO - Registration

Email address

Email address

Username

Username

Where did you hear from us?

At a conference

Register

BETA

or send an e-mail to: **rosco-vb2015@crysys.hu**

please send feedback to: **rosco-feedback@crysys.hu**

Laboratory of Cryptography and System Security (CrySyS Lab)
Budapest University of Technology and Economics
www.crysys.hu

contact:
Levente Buttyán, PhD
Associate Professor, Head of the CrySyS Lab
buttyan@crysys.hu