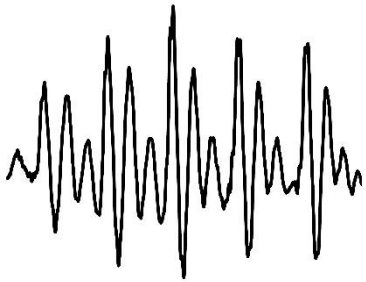
Targeted Cyber Attacks – Challenges and Some Solutions

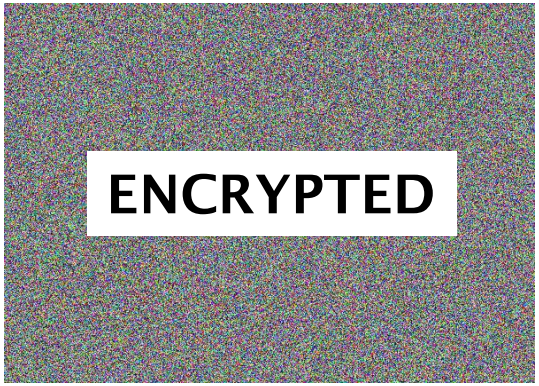
Levente Buttyán, PhD
Laboratory of Cryptography and System Security (CrySyS Lab)
Budapest University of Technology and Economics
www.crysys.hu

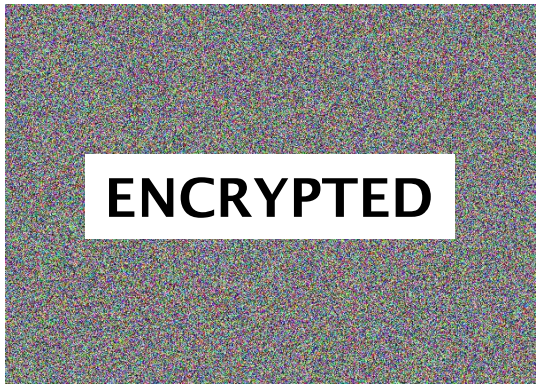
this is joint work with **all members of the lab**

Old days



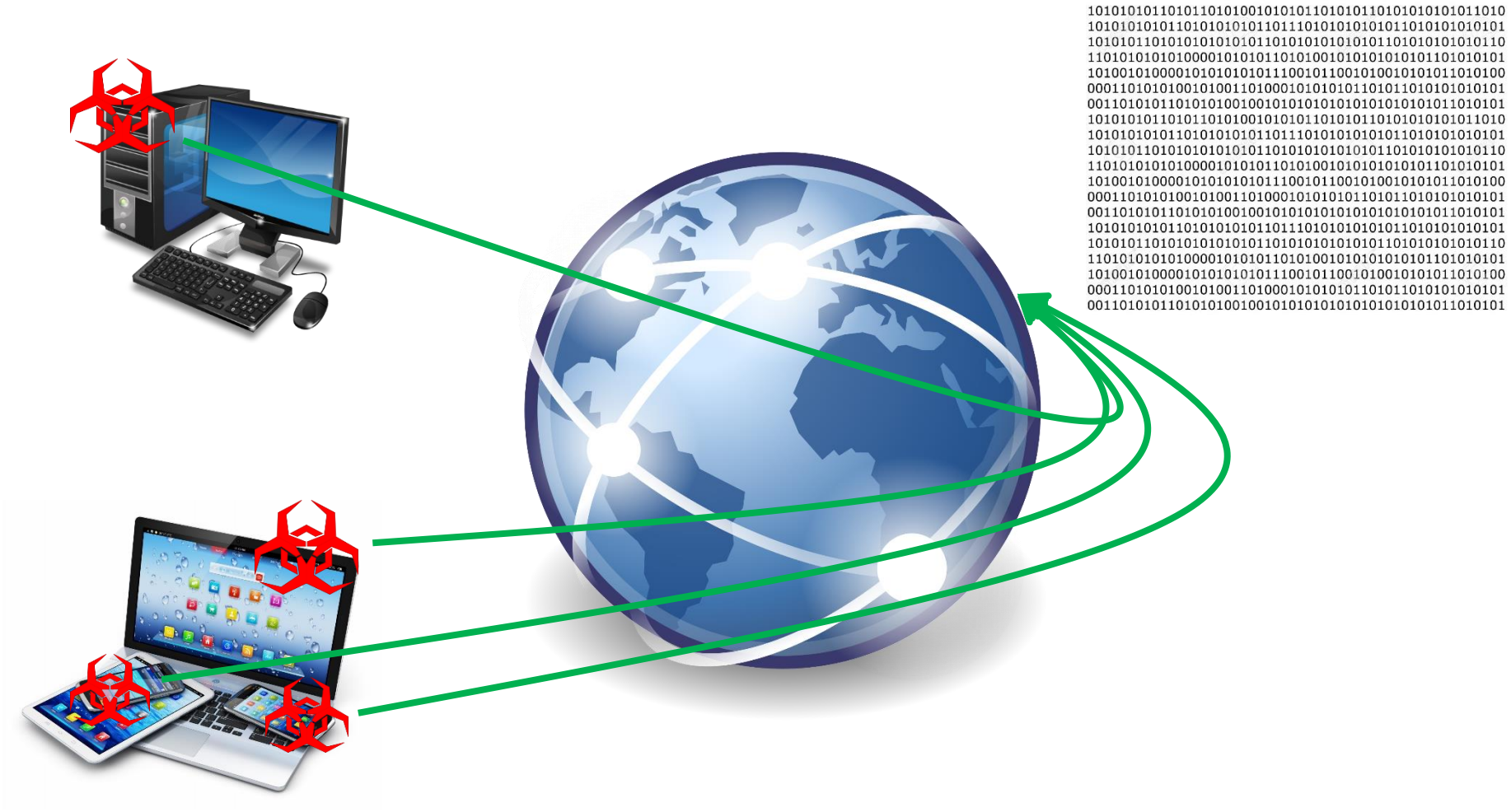
Today





Today

Today

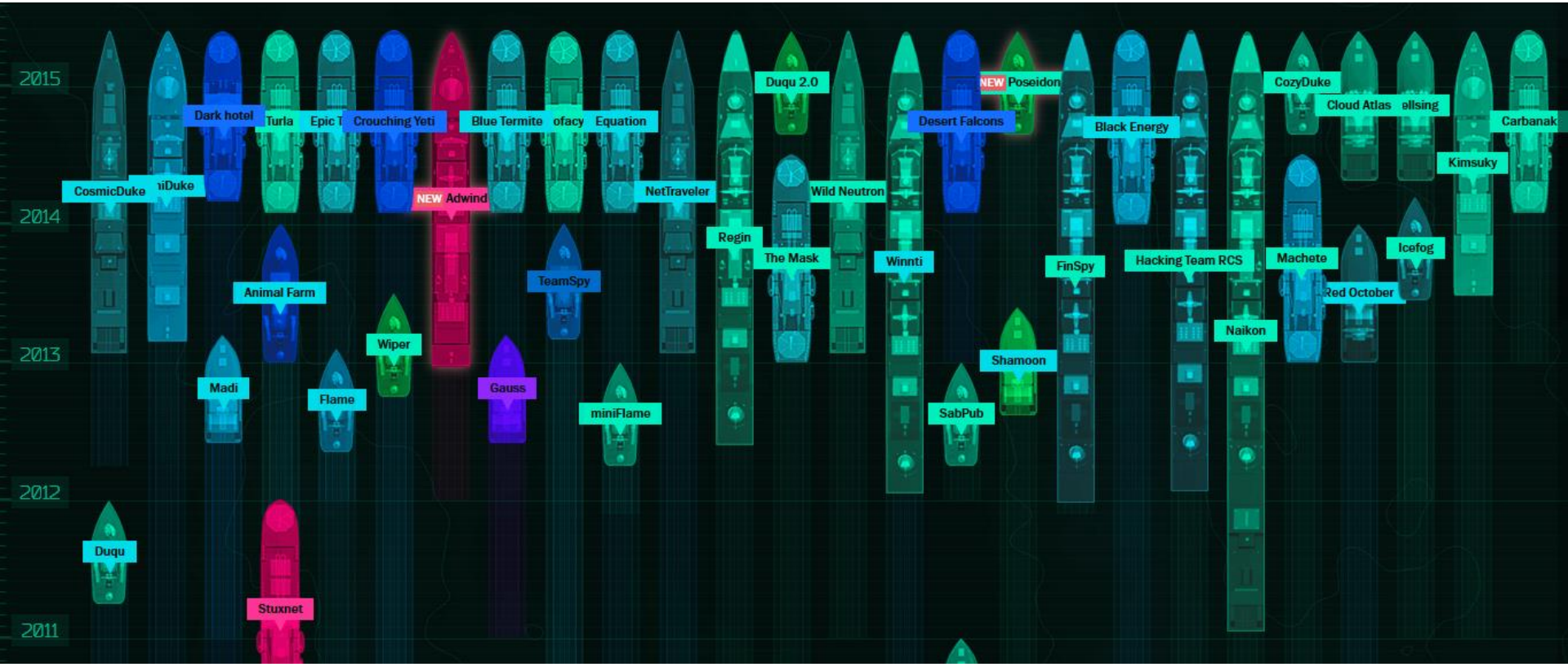


Malware

- **mal**icious soft**ware**
  - virus, worm, Trojan, ...

- typical delivery methods
  - e-mail attachment
  - drive-by-download
  - watering hole
  - infected media (e.g., USB stick)
- infection by exploiting known or publicly unknown vulnerabilities
  - bugs in the OS and in popular applications (e.g., browser, pdf reader, office suite)
- complete control over compromised computers (including smart devices)

Campaigns discovered since 2010



source: https://apt.securelist.com/

Home / News & Blogs / Zero Day

Hungarian Lab found Duqu malware

By Ryan Naraine | October 21, 2011, 9:11am PDT

Summary: The Laboratory of Cryptography and System Se

ITcafé

Címlap | Archívum

Hírek » Biztonság rovat

Újabb állami kémprogramot elemzet CrySyS Lab

Írta: Dajkó Pál | 2013-02-27 16:33 | Forrás: IT café

A kutatók szerint egy hazai intézmény, szervezet is érintett, ide is eljuttatták a feltehetően állami célokat szolgáló malware-t.

A Kaspersky Labs és a velük szoros együttműködésben dolgozó, a BME-n tevékenykedő CrySyS Lab ma közölték legújabb kutatásuk eredményeit, melyek egy kifinomult, feltehetően állami célokat szolgáló (vagy bűnözők által állami intézmények ellen bevetett) malware leírását tartalmazzák, egy olyan kódét, mely Magyarországon is megfertőzte legalább egy – nem nevesített – szervezet rendszerét.

Mellékleteink: Unix / Linux | Gamekapocs Új felhasználó vagy? Regisztrálj itt | Bejelentkezés

hwsw

VÁLLALATI IT | DIGITÁLIS OTTHON | HIGH TECH

TESZTEK | ARCHÍVUM | HÍRLEVÉL | RSS APRÓHIRDETÉS | FÓRUM | BLOG | KARRIER

RENDSZERGAZDA vagy? Segítsd munkánkat, vegyél részt az ITPRO 201

IBM Storwize® V3700 4,2 TB adat-tárhellyel most

Több éve zajló támadást leplezett le a BME CrySyS

Bodnár Ádám, 2013. március 21. 10:24 Szólj hozzá!

Több éve zajló célzott informatikai támadást leplezett le a BME Adat- és Rendszerbiztonság Laboratórium (CrySyS). A publikált információk alapján magyar kormányzati szervek is érintettek.

A Nemzeti Biztonsági Felügyelet riasztása nyomán kezdett vizsgálódásba a BME CrySyS, a folyamat eredménye egy információgyűjtő kártevő leleplezése lett. A publikát adatok alapján a támadók feltehetően évek óta több hullámban hajtottak végre információgyűjtő tevékenységet, magyar kormányzati szervek mellett orosz iparvállalat, közel-keleti elektronikai cég, oroszországi követségek, illetve francia és belga kutatóintézetek is érintettek az incidensekben.

CHNOLOGY

Latin America | Mid-East | US & Canada | Business | Health

ne by the Laboratory of Cryptography and
ary's University of Technology and Economics
hidden because it was so different to the
that most security programmes were designed
to catch.

Common theme

- targeted → victims are not random, but chosen on purpose
  - a given organization or (set of) individual(s)
- highly customized tools and intrusion techniques
  - malware delivery by spear phishing and social engineering
  - using partners in the supply chain as stepping stones
  - multiple different exploits (often zero-day or very fresh)
- stealthy operation and persistence
  - bypassing mainstream AV and security products without detection
  - careful design and intensive testing to avoid causing anomalies
- well-funded and well-staffed organizations behind
  - military or state intelligence

Challenge #1: Sophisticated delivery methods

- spear phishing and social engineering
  - raising awareness by education may not be sufficient
  - when was the last time you opened an attachement or clicked on a link in an e-mail?
    - 5 minutes ago? 1 hour ago? 1 day ago?

- zero-day exploits
  - keeping OS and applications up-to-date do not really help
  - traditional security products do not really help
  - zero-day exploits do exist and will remain with us !
    - some companies build their business model on this

Challenge #2: Stealthiness and persistence

- careful design and intensive testing
  - avoid anomalies and detectable side effects
  - attackers buy mainstream security products and fine-tune their malware until it by-passes detection
  - when ”APT detection” products (e.g., Sourcefire, FireEye, ...) will become mainstream (or simply an obstacle to the attacker), then they will be acquired and tested too

New anti-APT tools are no silver bullets

- they claim to detect previously unseen, new malware
- how good they are?
- testing them needs previously unseen, new malware
- we developed 4 custom samples that resemble targeted malware
  - all test samples implemented RAT functionality
  - remote C&C communication via back-connect
  - 2 weeks of development without access to any anti-APT products
- then we tested 5 products (in 2014), and got this result:

Sample\Product	Product 1	Product 2	Product 3	Product 4	Product 5
Test sample 1	detected	detected	detected	detected	detected
Test sample 2	detected	detected	detected	detected	detected
Test sample 3	detected	bypassed	bypassed	detected	bypassed
Test 4 - BAB0	bypassed	bypassed	bypassed	bypassed	bypassed

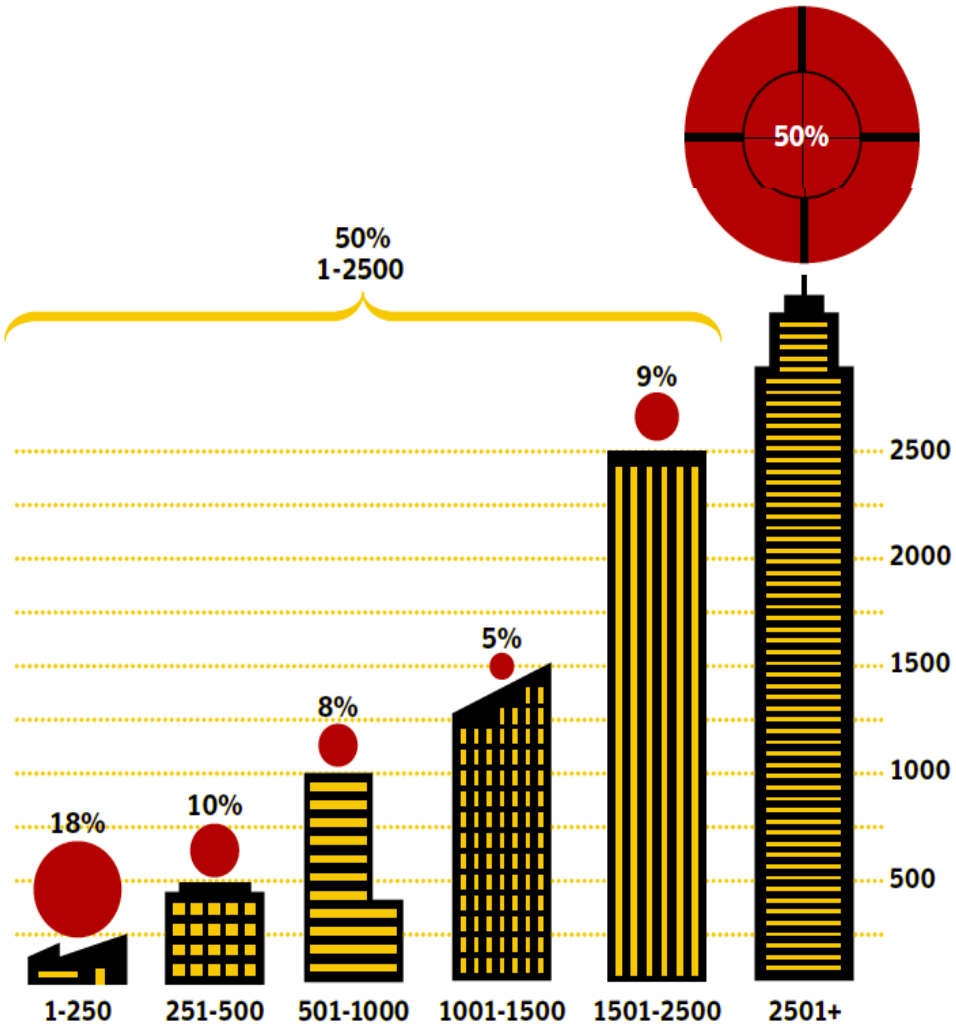
Challenge #3: Attackers are rich in resources

- we do not know how rich they are, but ...
  - a zero-day exploit costs ~250K USD on the black market
  - malware such as Stuxnet needs to be tested too
    - who has an uranium centrifuge at home?

- and they are certainly richer than many of their targets...

Size of victim organizations

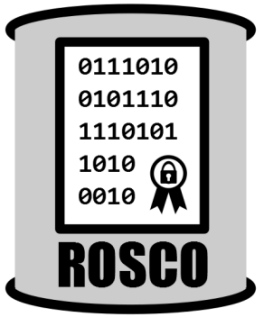
small organizations in the supply-chain of large ones are often used as stepping stones



So, we face attackers ...

- with large amount of resources (challenge #3)
- in possession of lethal weapons (challenge #1)
- having much much more knowledge about us, than we have about them (challenge #2)

Who said its a fair game, after all?



Repository Of Signed COde

in collaboration with IT-SEC Expert
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

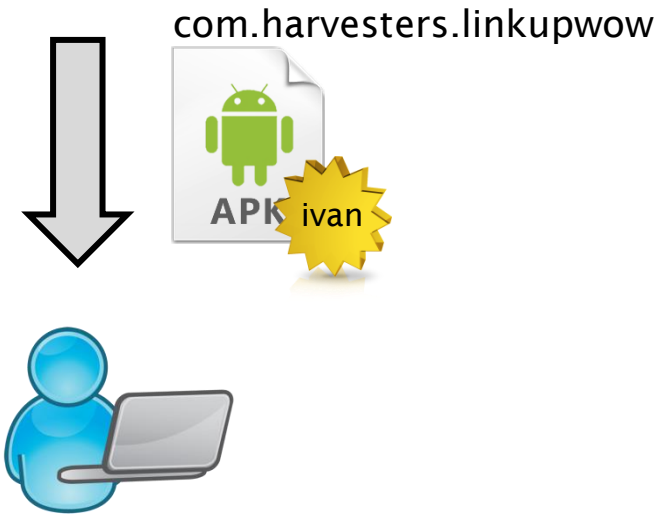
Motivation

- 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 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 Acer
- <u>problem:</u> standard signature verification procedure does not allow for detecting key compromise and fake certificates

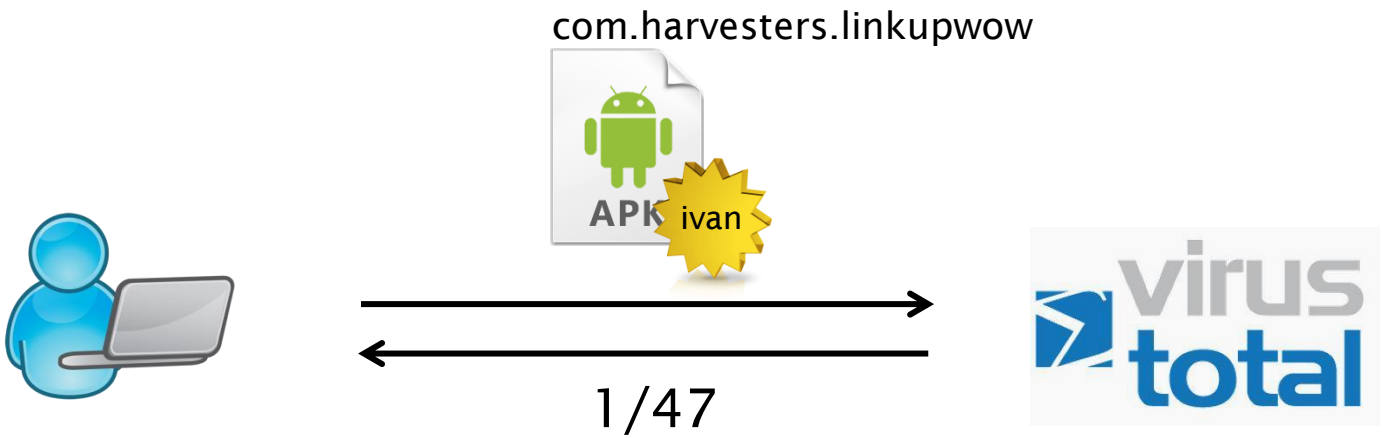
ROSCO

- we designed and implemented ROSCO, a Hadoop cluster for storing a massive amount of signed objects
- our crawlers collect signed objects from the Internet
  - certificates (~60 million)
  - exe and dll files (~500 000)
  - apk packages (~100 000)
- ROSCO can be used
  - to provide reputation information on signers and signed code
  - to notify key owner when a new object signed with his key is seen

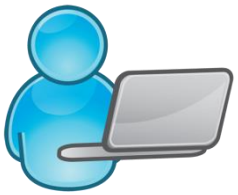
Use case: Checking signer reputation



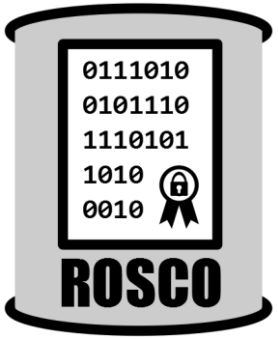
Use case: Checking signer reputation



Use case: Checking signer reputation

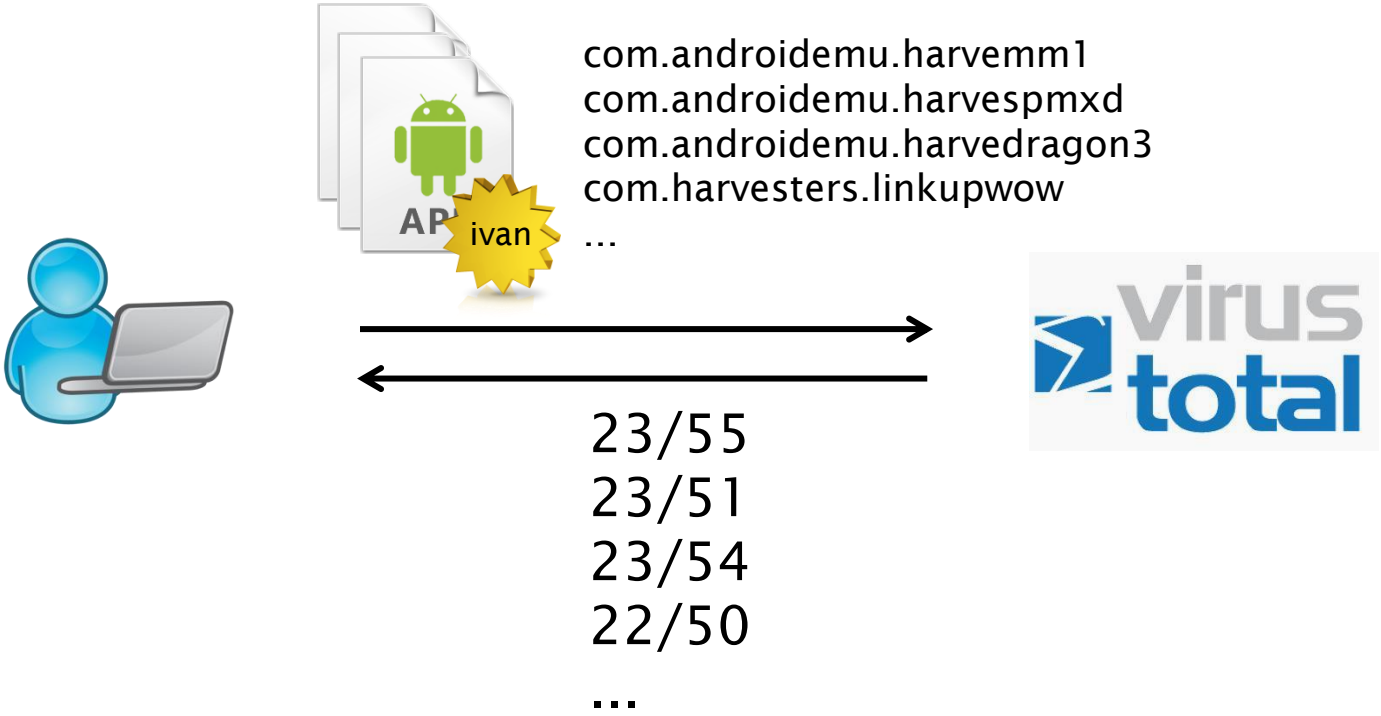


what else has ivan signed?



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

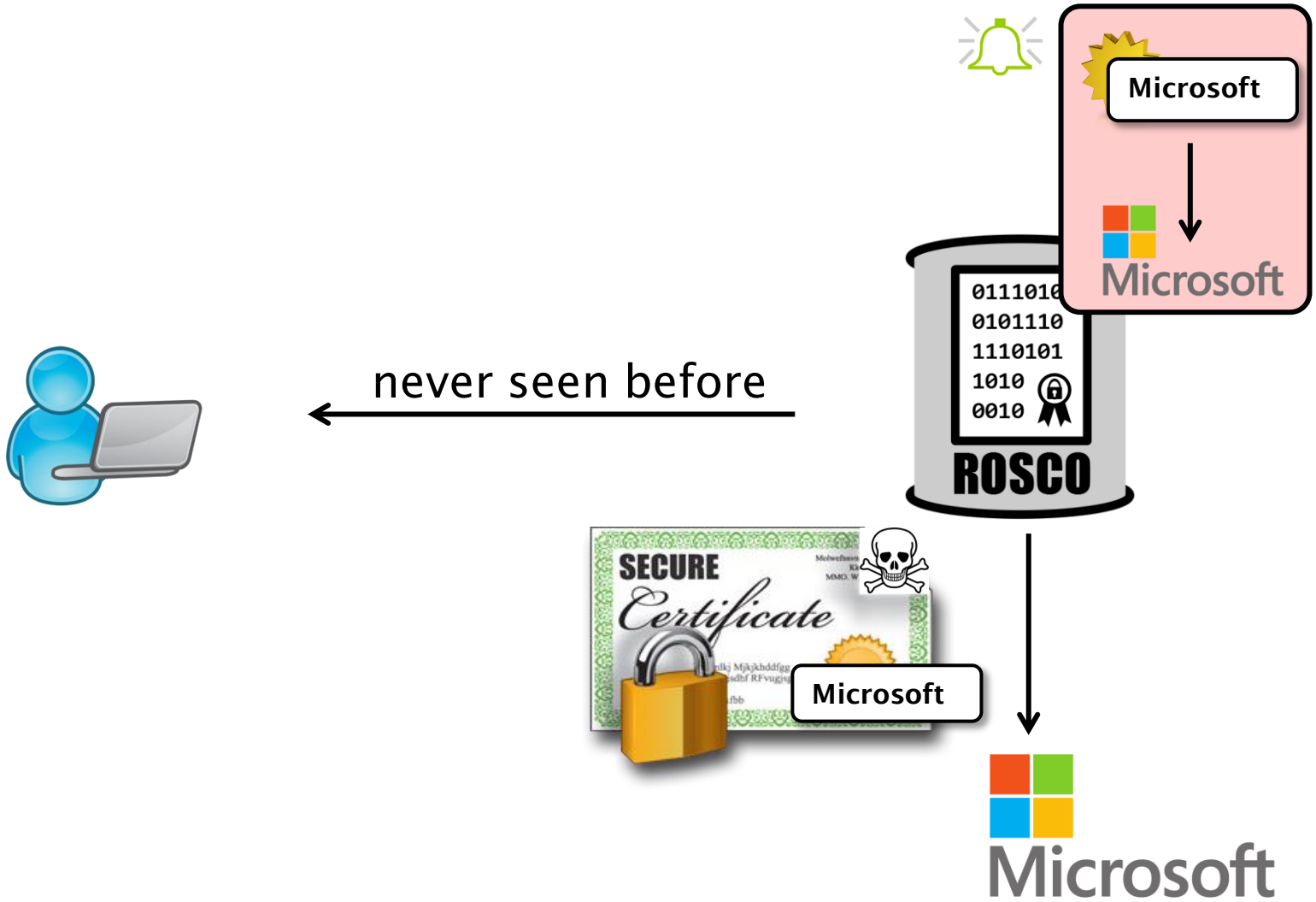
Use case: Checking signer reputation

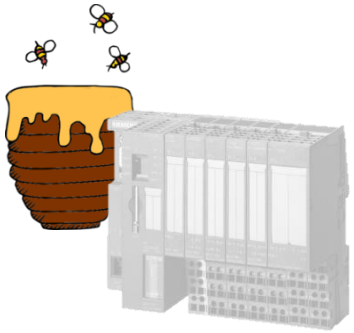


Use case: Alerting key owners

Use case: Alerting key owners

Use case: Alerting key owners



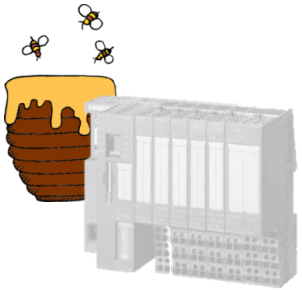


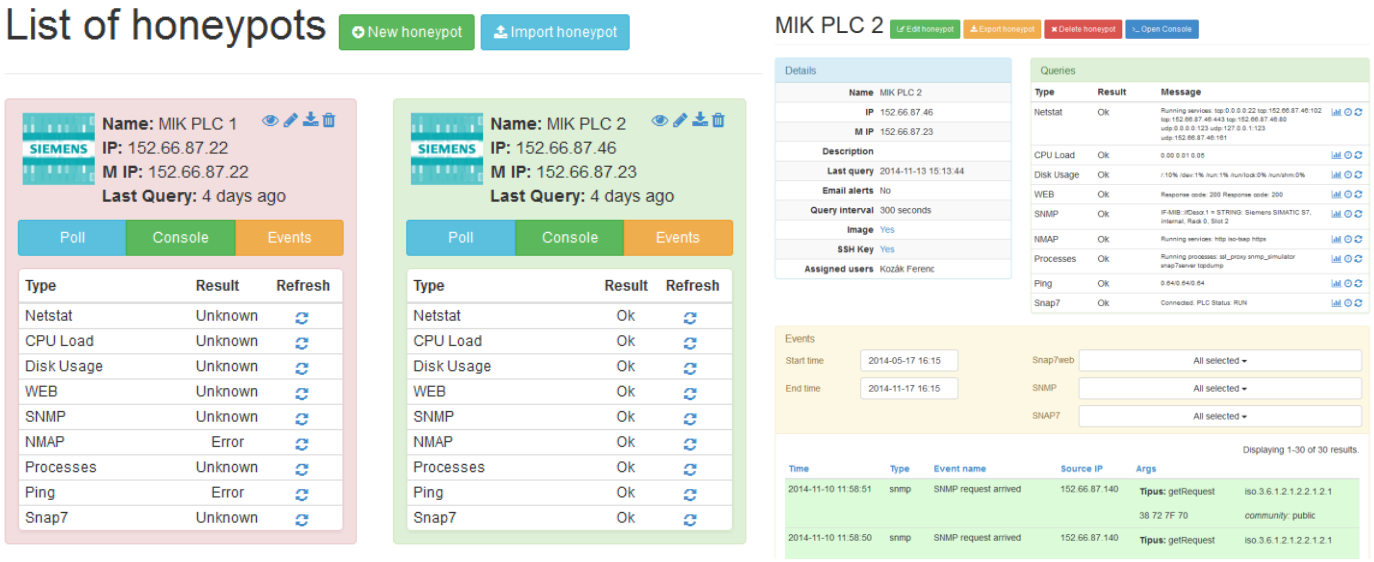
Design and Implementation of a PLC Honeypot

in collaboration with MIK and the AddICT lab of our department
work funded by EIT Digital in the Smart Energy Systems action line

PLC honeypot

- a decoy system that apears to be a real PLC
- allows for the observation of attacker steps
- our honeypot simulates a Siemens Simatic 300 PLC
- high interaction level (set values can be read back)
- special attention to make it indistinguishable from a real PLC
- web based honeypot management system





avatao™

avatao offers hands-on IT security exercises for people to sharpen their skills

the most recent spin-off from the CrySyS Lab

avatao – on-line IT security exercises

avatao | Dashboard | Discover | Paths | Search for... | Welcome Avatao admin

Challenge details

Mastering Computer Security

- Path description
- Challenge list
- Path statistics

Challenges

Memory corruption

- FlagSafe
- 2010_4344
- DawgLea
- TWC
- VM Migration
- Warmup
- PlanB
- LastResort

Secure Programming in C

- Secure BMP Compression Syndicate
- Oh My Secure Sums

Oh My Secure Sums

47 | 200 points

by Gabor Acs-Kurucz

Skill tags

Secure C Programm

Description

Your task is to secur
You don't need to im
automatically upon s

The function gets a z
INT_MAX (skip the c
sum those integers a
error occured, otherw
should be (kind-of) securely randomized.

Parameters

`const char *text`: This is the user input you need to process. This input can contain anything, but it is zero-terminated.

`unsigned *count`: Output parameter, the number of integers found, 0 if error occurs.

144.76.199.141:32851 | Search

File | Editor | View | Find

FOLDERS | untitled | app.c

app
.ignore
app.c

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <limits.h>


int *get_randomized(const char *text, unsigned *count, int *sum){
    *count = 0;
    *sum = 0;
    return NULL;
}
```

avatao – advantages

- convenient for students
  - **no need to install** anything, it just works
  - potential solutions can be submitted and there's **immediate response**
  - if something goes wrong, just **re-start any time** the exercise
  - many exercises have a **step-by-step solution guide**

- offers great opportunities for teachers
  - **no need for infrastructure** to set up and maintain
  - there are already **250+ exercises** (and growing)
  - it takes just a **few minutes to create a new path**
  - can be used for **homeworks, lab exercises, exams, CTFs, ...**
  - **free access** by contributing new content

Conclusions

- we face attackers
  - with lot of resources (~challenge #3)
  - in possession of advanced cyber weapons (~challenge #1)
  - having substantially more knowledge about us, than we have about them (~challenge #2)
- it seems that our traditional security tools (firewalls, IDS, AV products) are ineffective against such attackers
- we need to improve
  - preventive tools (although they will never be perfect!)
  - detection speed (1 year → 1 day)
  - information asymmetry between attackers and defenders
  - information sharing between victims and security companies
  - education and training of good security experts
- plenty of room for innovative research and better education

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