SECURITY SUMMIT

AIP Associazione Informatici Professionisti — ITCS Italian Computer Society

<< back | track

<<Back|track Italia

Milano, 16 Marzo 2010

Introduzione al tema delle minacce di **Phishing 3.0** attraverso tecniche di **Cross Application Scripting**

Relatori: Emanuele Gentili
Alessandro Scoscia
Emanuele Acri

PHISHING: l' eterna lotta tra
Sviluppatori Software
e
Natura Umana

Tipologie di attacco Phishing

✓ PHISHING 1.0

A. E-MAIL
B. XSS on site
C. Website Clone

✓ PHISHING 2.0

DNS CACHE POISONING

➡ PHISHING 3.0

Da XSS a CAS

Il **Cross-site scripting (XSS)** è una vulnerabilità che affligge siti web dinamici che impiegano un insufficiente controllo dell'input.
Un XSS permette ad un attaccante di inserire codice al fine di modificare il contenuto della pagina web visitata. In questo modo si potranno sottrarre dati sensibili presenti nel browser degli utenti che visiteranno successivamente quella pagina.
Gli attacchi alle vulnerabilità XSS hanno effetti dirompenti per i siti con un elevato numero di utenti, dato che è sufficiente una sola compromissione per colpire chiunque visiti la stessa pagina.

Il **Cross-Application scripting (CAS)** è una vulnerabilità che affligge applicazioni desktop che impiegano un insufficiente controllo dell'input. Un CAS permette ad un attaccante di inserire codice al fine di modificare il contenuto di una applicazione desktop utilizzata.
In questo modo si potranno sottrarre dati sensibili presenti nel sistema degli utenti.
Gli attacchi alle vulnerabilità CAS hanno effetti dirompenti perche' possono implicare la completa compromissione dei target indipendentemente da sistemi operativi e piattaforme.

Differenze sostanziali

	XSS	CAS
attacco ad applicazioni web	si	no
attacco a applicazioni	no	si
Sistemi Operativi	no	si
Remote Command Execution	no	si

Tecnologie analizzate

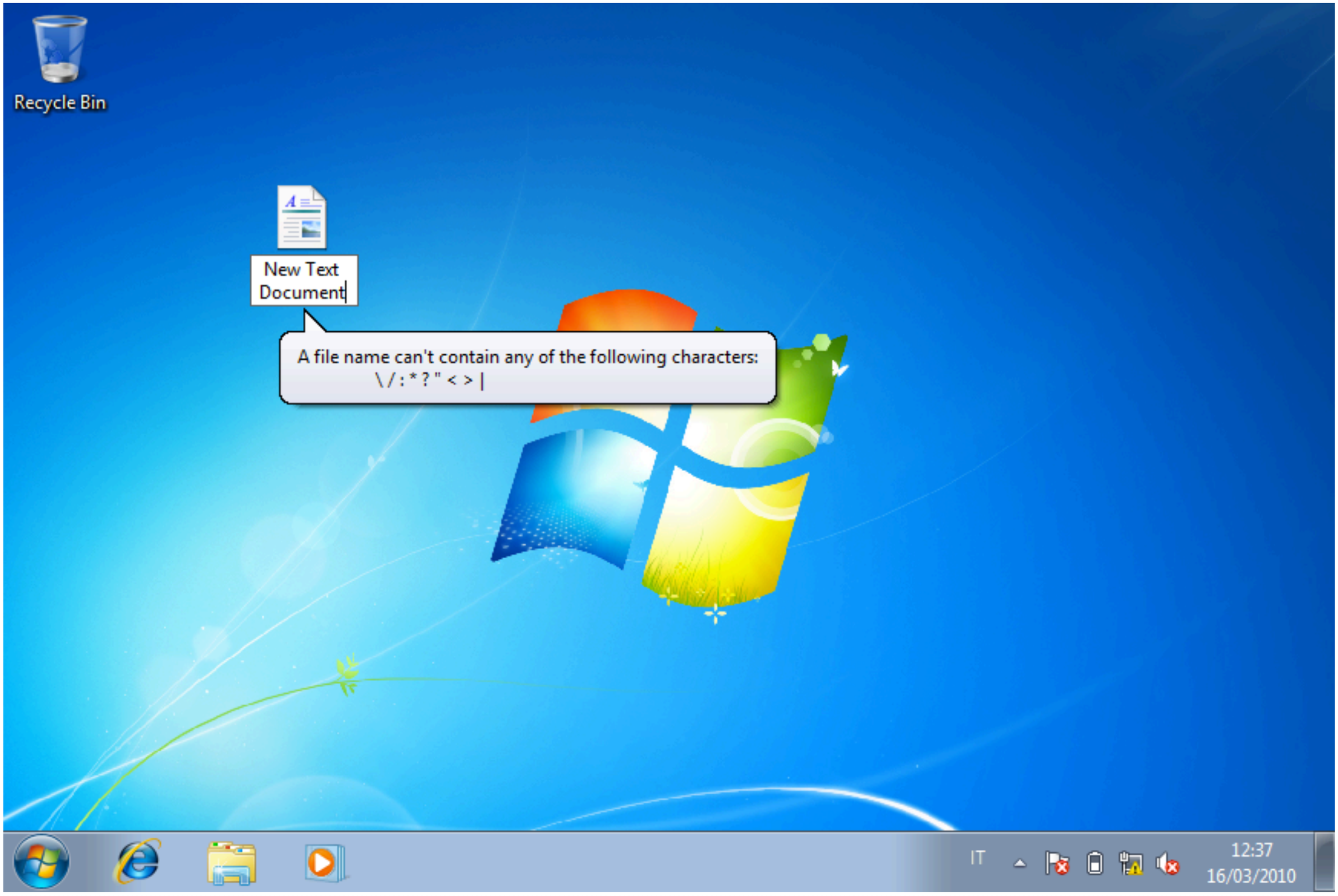
Frameworks grafici

- GTK
- QT

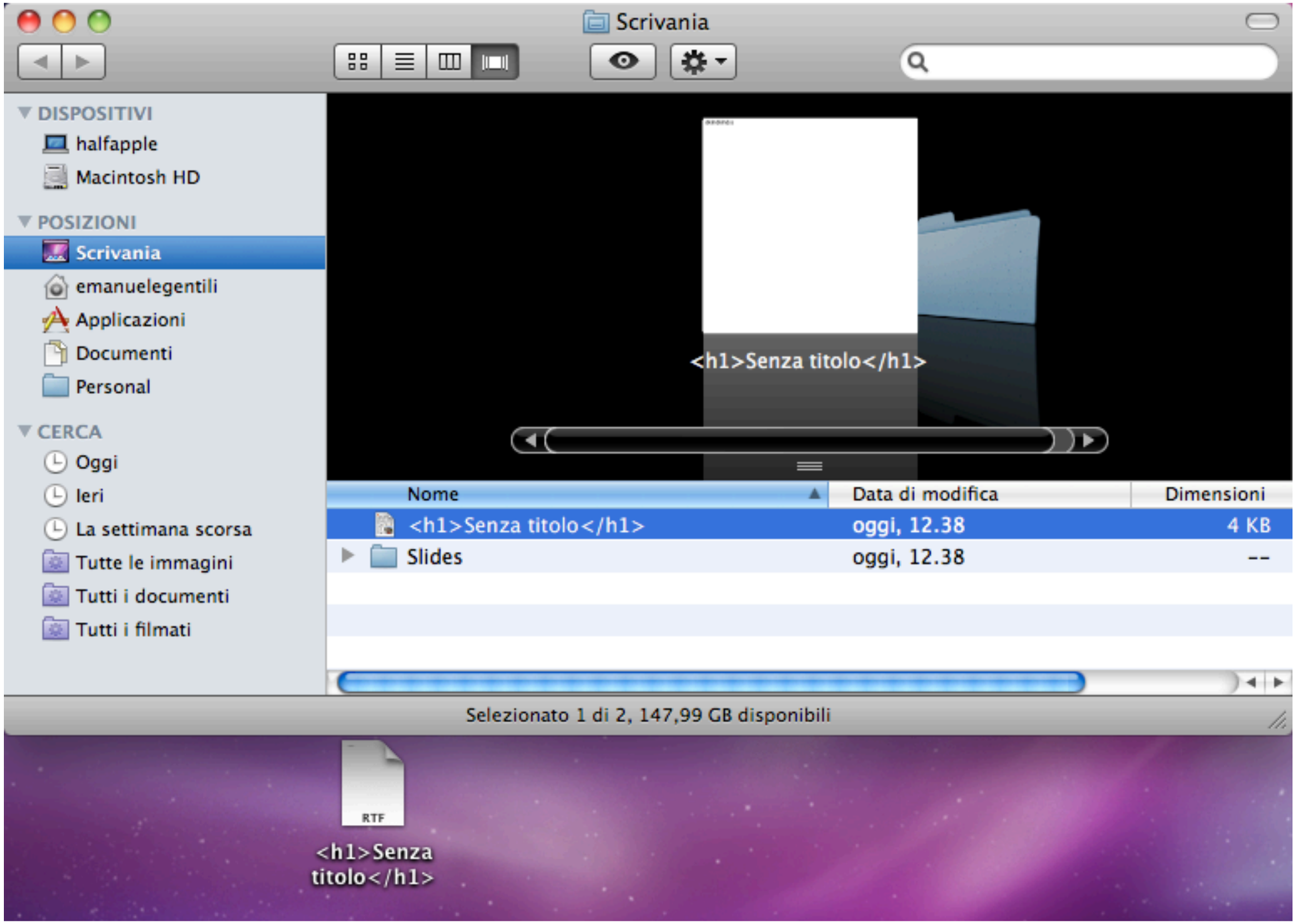
Desktop Environment

- MICROSOFT WINDOWS
- Apple OS X
- KDE (KIO)
- GNOME

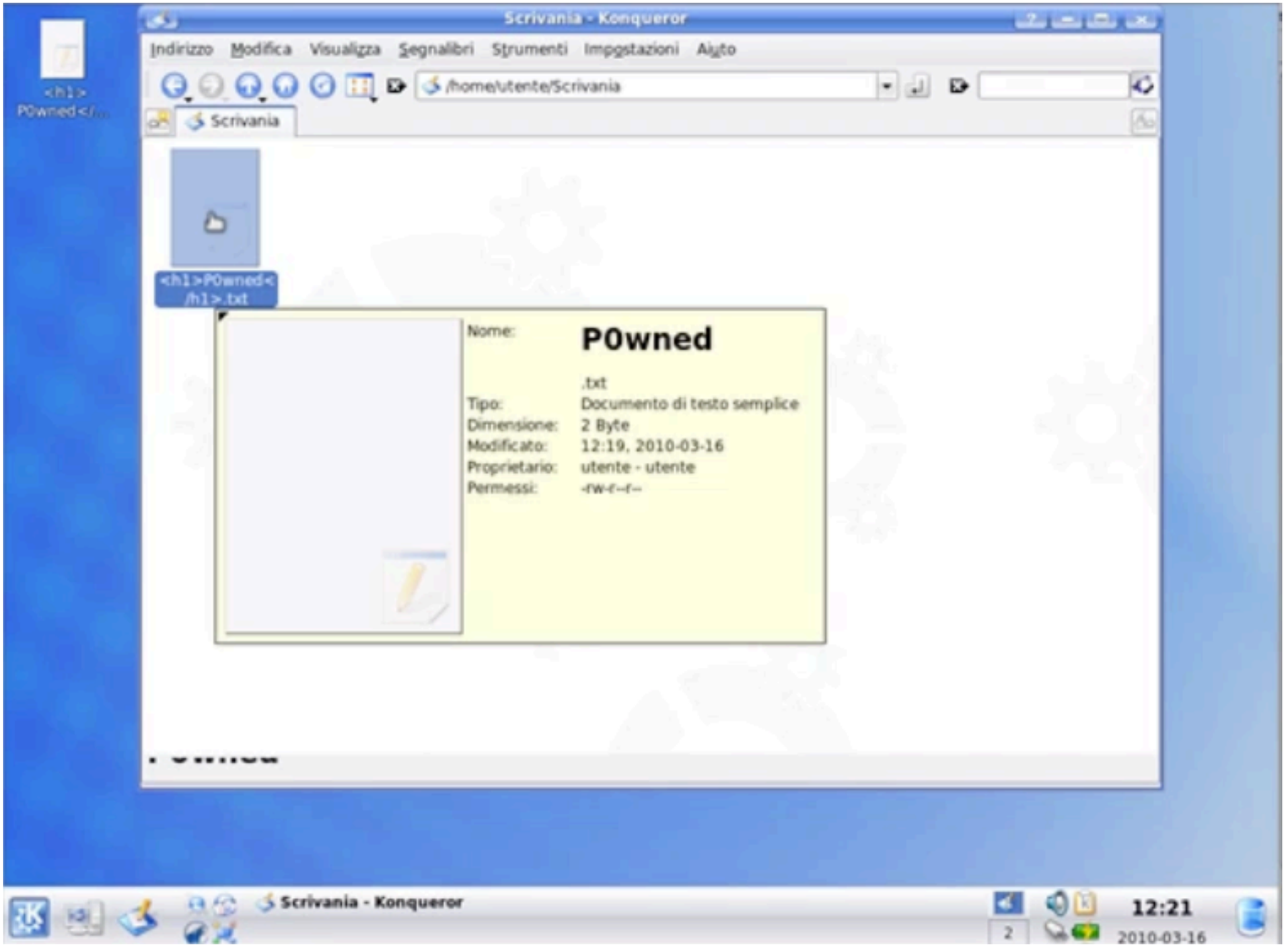
Architetture e Sistemi analizzati - Microsoft Windows



Architetture e Sistemi analizzati - Apple OS X



Architetture e Sistemi analizzati - KDE



Responsible Disclosure

NOKIA
Connecting People

symbian

Adobe™

skype™

Google™

CANONICAL

K Desktop Environment

ubuntu

GNOME™

SECURITY SUMMIT

AIP Associazione Informatici Professionisti

ITCS Italian Computer Society

<<Back|track

Introduzione al tema delle minacce di phishing 3.0 attraverso tecniche di Cross Application Scripting

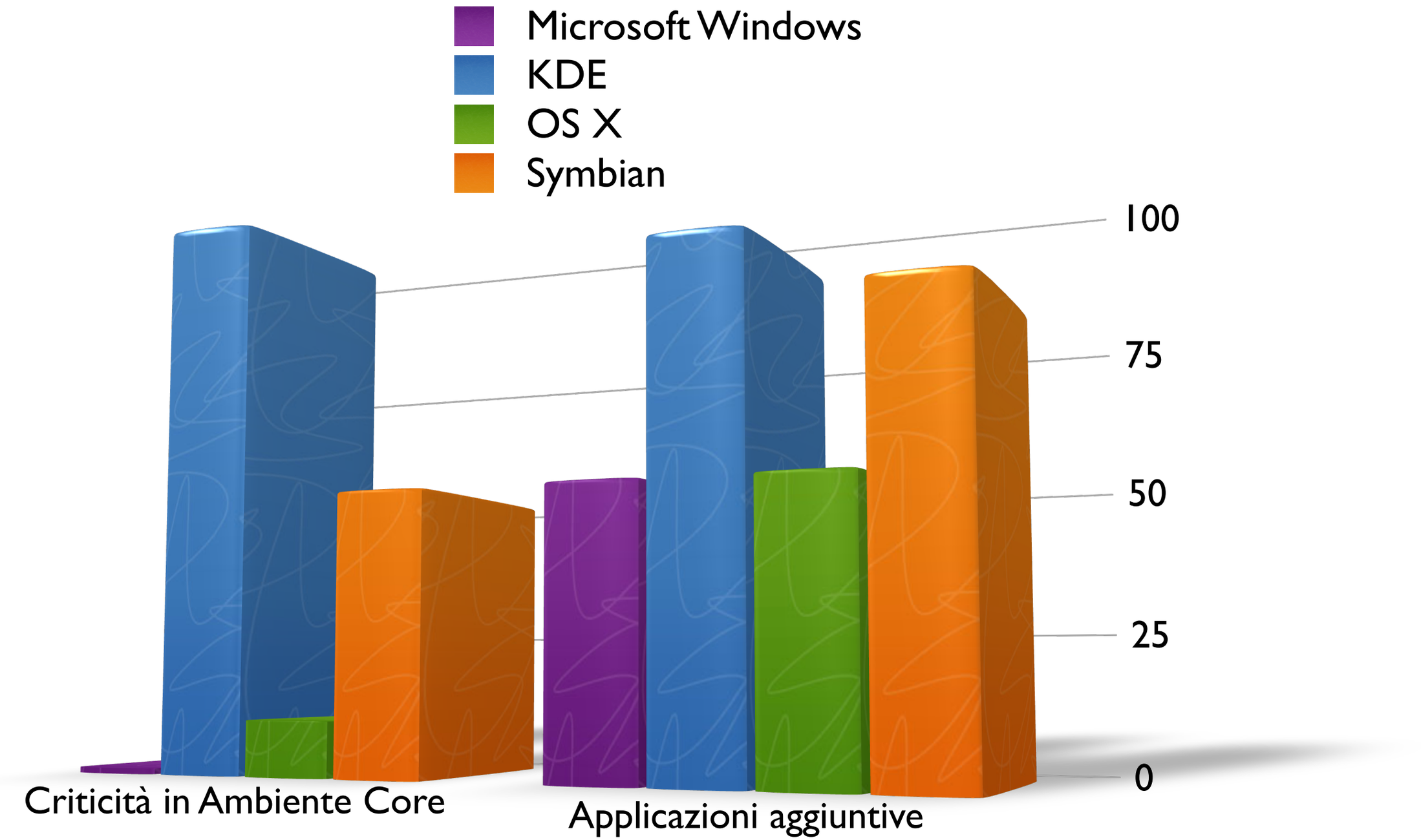
Emanuele Gentili, Alessandro Scoscia, Emanuele Acri

Milano, 16 Marzo 2010

Vettori potenziali di attacco

Metodi Anti Phishing per attacchi CAS

Previsione di impatto in prima indagine



Pericolosità in attacchi COMBO

Cross Application Scripting

Modifica interfaccia applicativa

Redirezione utenti a sito web malevolo
da applicazione con alterazione GUI.

Esecuzione Comandi

Possibilità di far eseguire alla vittima
comandi nel sistema utilizzato

Attacchi dipendenti ESCLUSIVAMENTE dalle applicazioni

Pillole Tecniche: SKYPE

```
# Title: Skype for Linux (<=2.1 Beta) multiple strange behavior
# Author: Emanuele Gentili (Emgent), Emanuele Acri (Crossbower)
# Contacts: emgent@backtrack.it, crossbower@backtrack.it
# Published: 2010-01-04
# Software Link: http://www.skype.com/intl/it/download/skype/linux/
# Version: <=2.1 Beta (the latest version)
# Tested on: Ubuntu 8.10, Debian 6.0 Testing
# Special greetz: Backtrack-Italy Community
```

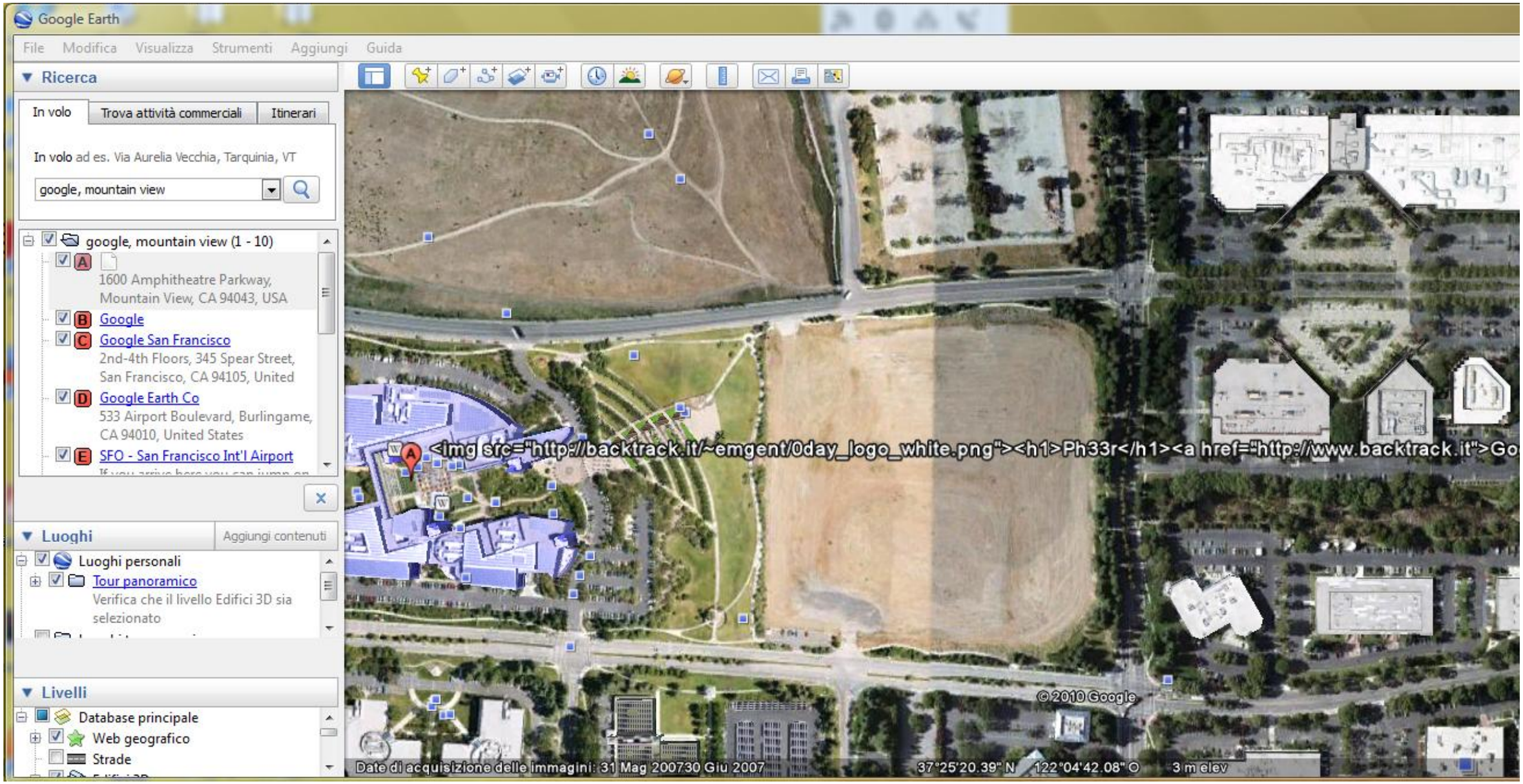
- Phishing proof of concept:

If you type this string in your profile (Homepage field), 'www.google.com' will be displayed, but the link points to -> http://backtrack.it:

```
backtrack.it">www.google.it<script>
```

http://www.exploit-db.com/exploits/10980

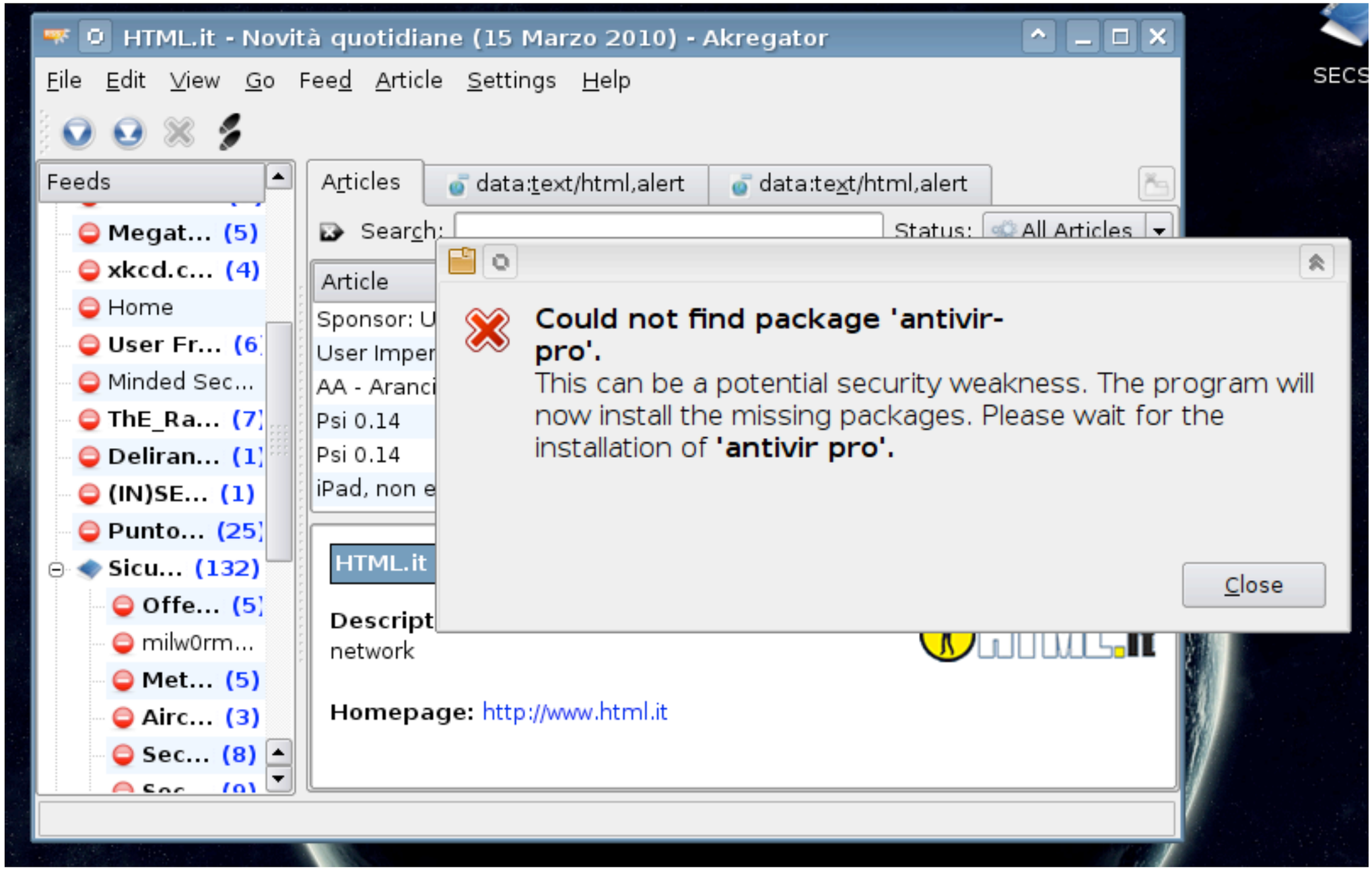
Pillole Tecniche: Google Earth (I)



Pillole Tecniche: Google Earth (II)

Pillole Tecniche: Akregator

```
apt:antivir-pro'. </b> <span /> ... <span /> <span /> <span /> <span /> <span /> <span />
<span /> <span /> This can be a potential security weakness. The program will now install
the missing packages. Please wait for the installation of <b>'antivir pro,netcat
```

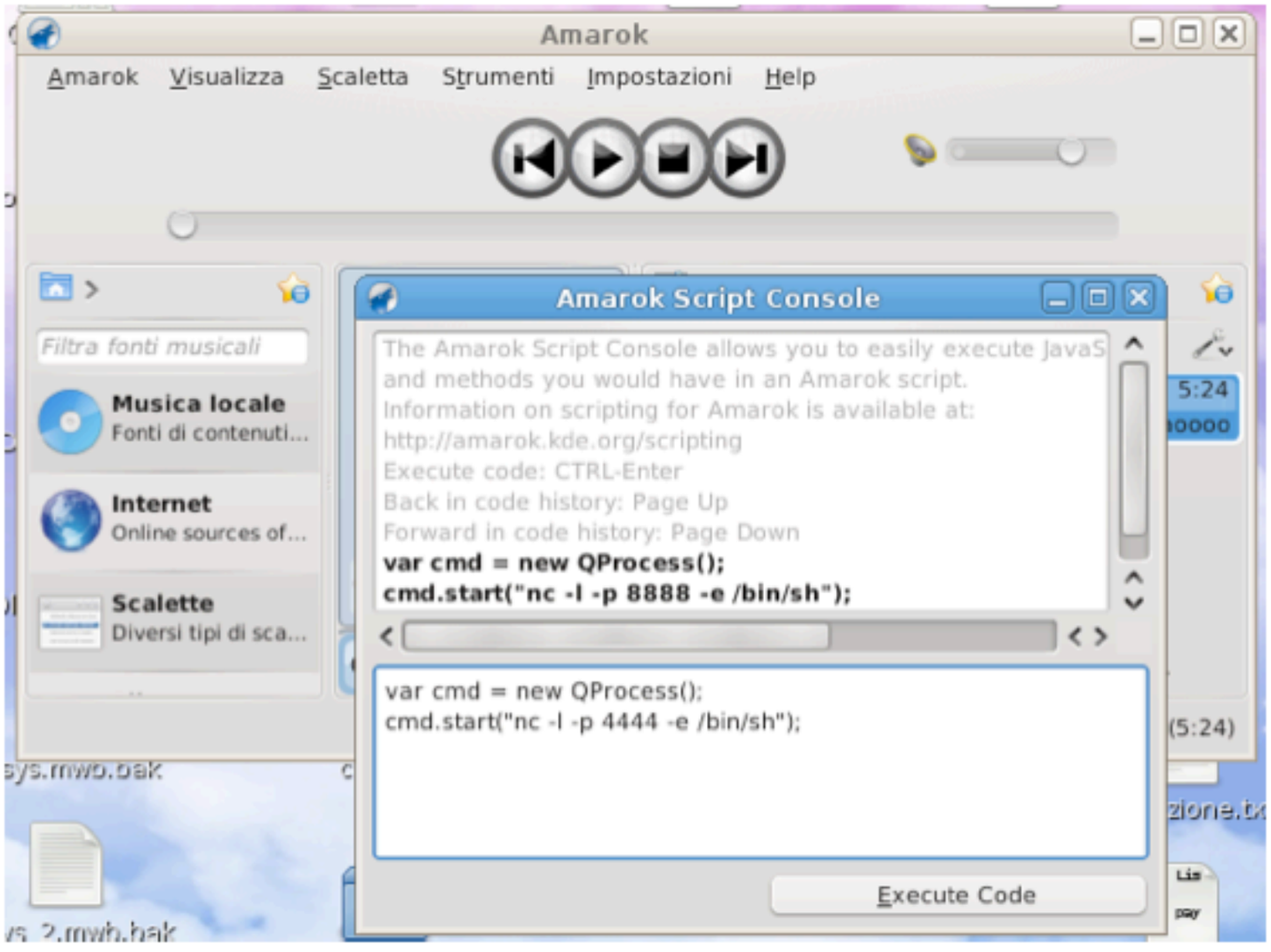


KDE OWNAGE VIA
CROSS APPLICATION SCRIPTING

http://www.backtrack.it/~emgent/videos/16032010_-_SecuritySummit_CAS_OWNING_KDE.mov

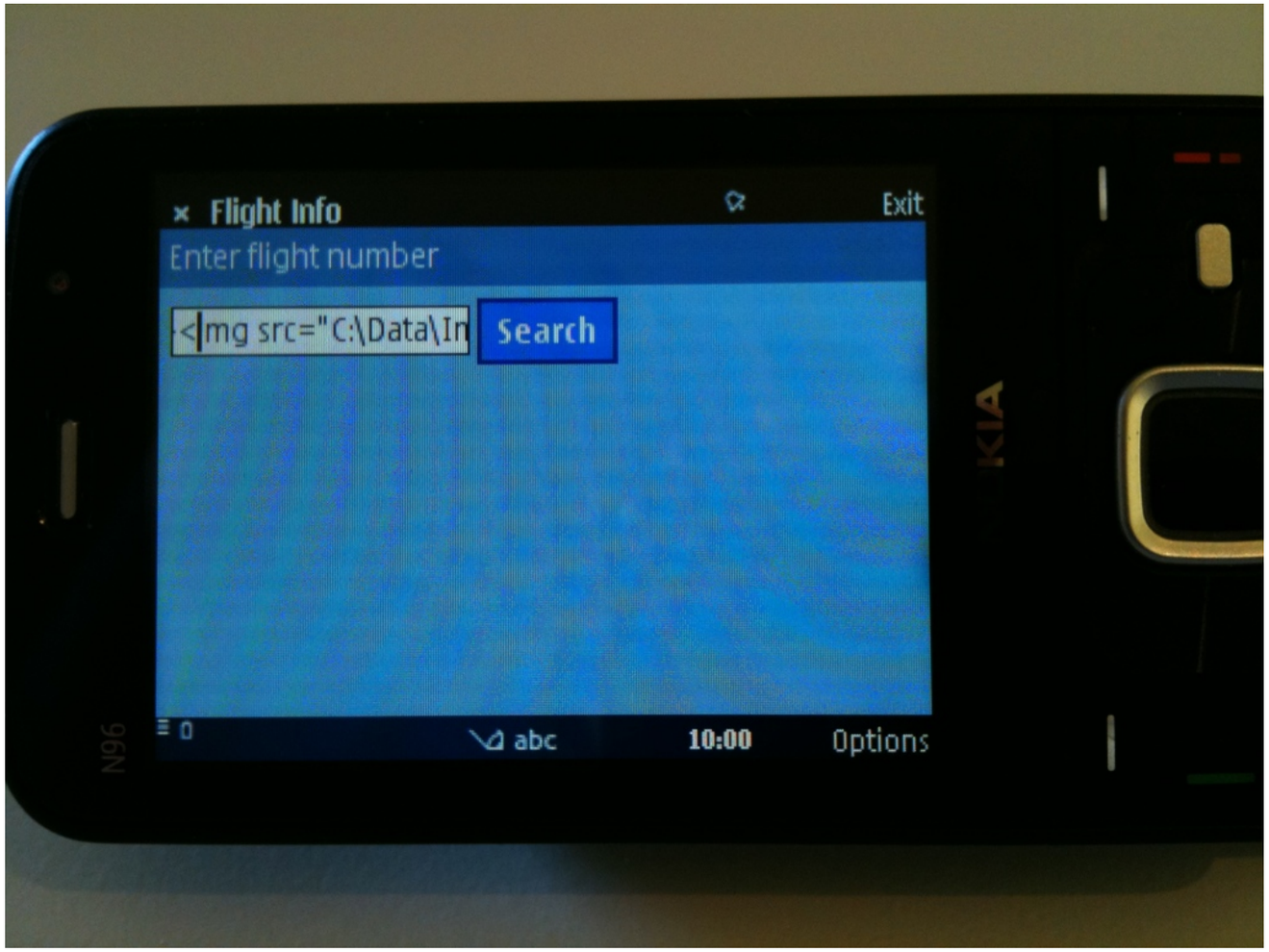
Nuove Frontiere (I)

QT Script Module



Nuove Frontiere (II)

Applicativi Mobile



Ringraziamenti

Marco Rondini
Simone Quatrini
Mauro Gasperini
Francesco Morucci

CLUSIT

Associazione Informatici Professionisti