



SoftSphere
Technologies

WINDOWS 8 SMARTSCREEN APPLICATION CONTROL

What More Could You Ask For?

Randy Abrams – NSS Labs

Ilya Rabinovich – SoftSphere Technologies



WE MAKE SECURITY A SCIENCE

Show and Tell

- Tell First, Show Later
- The History of SmartScreen App Rep
- What App Rep Does and Does Not Do
- Showtime!!! (Technologies that Plug the Holes)
- It's a Wrap



Name That Virus

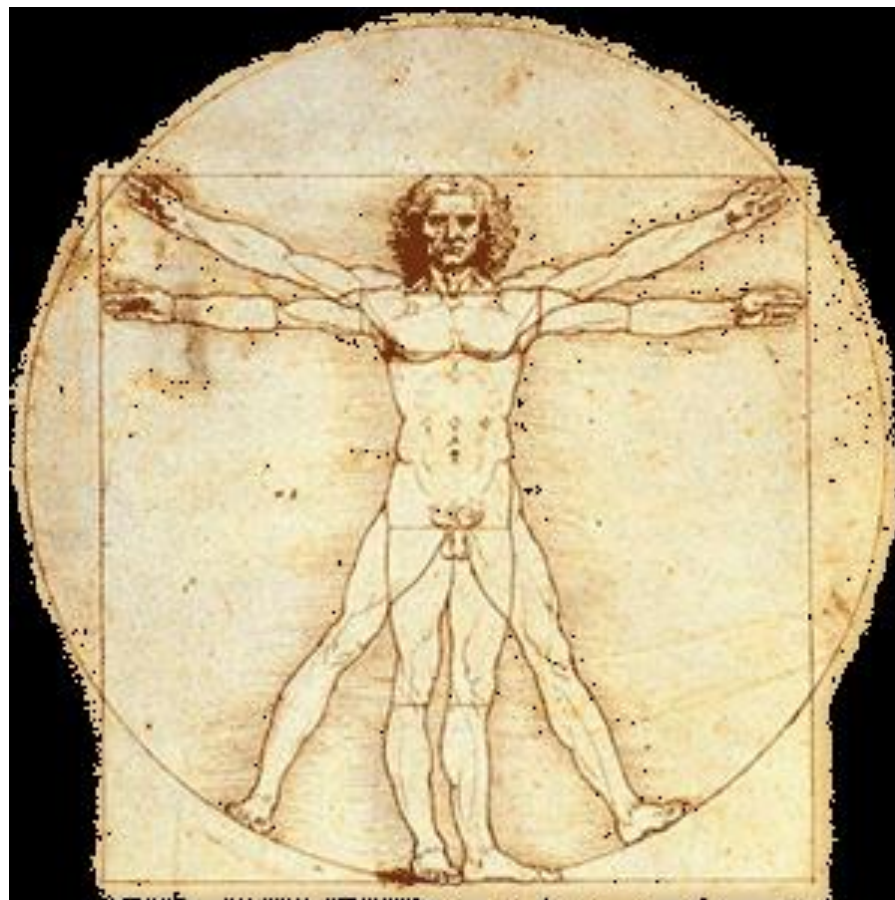
- W97M/Concept



Medieval App Rep



Renaissance App Rep



SmartScreen Evolution

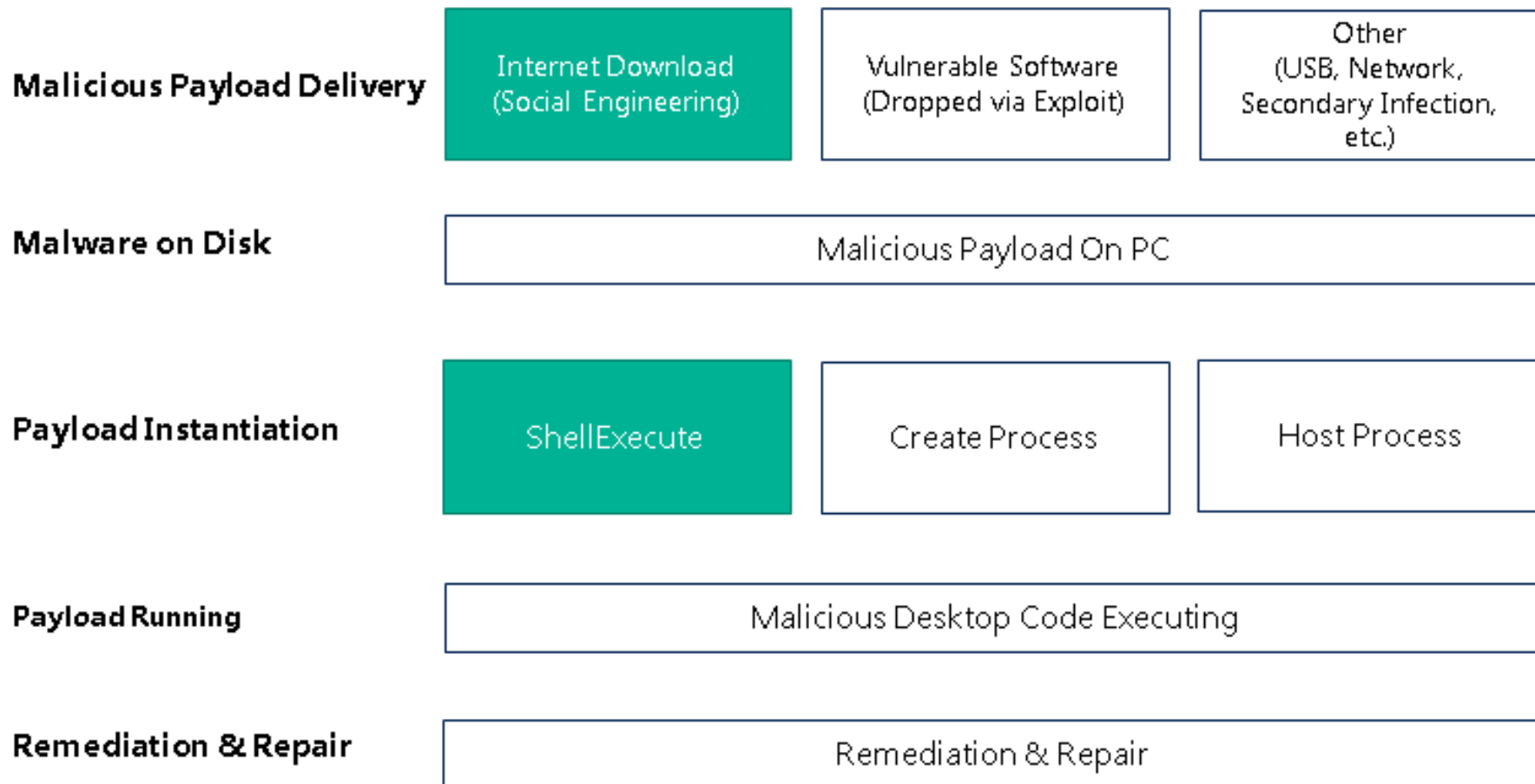


8 Years of Investment:

- Grown from 1 service to 3 (Phish, Malware, Apprep)
- Moved from (the browser on PC) to (the browser on all MSFT platforms and direct OS and in-app integration)
- Grown from 1 Client to eight
- Protecting approximately half a billion users

Slide used with permission of Microsoft Corporation

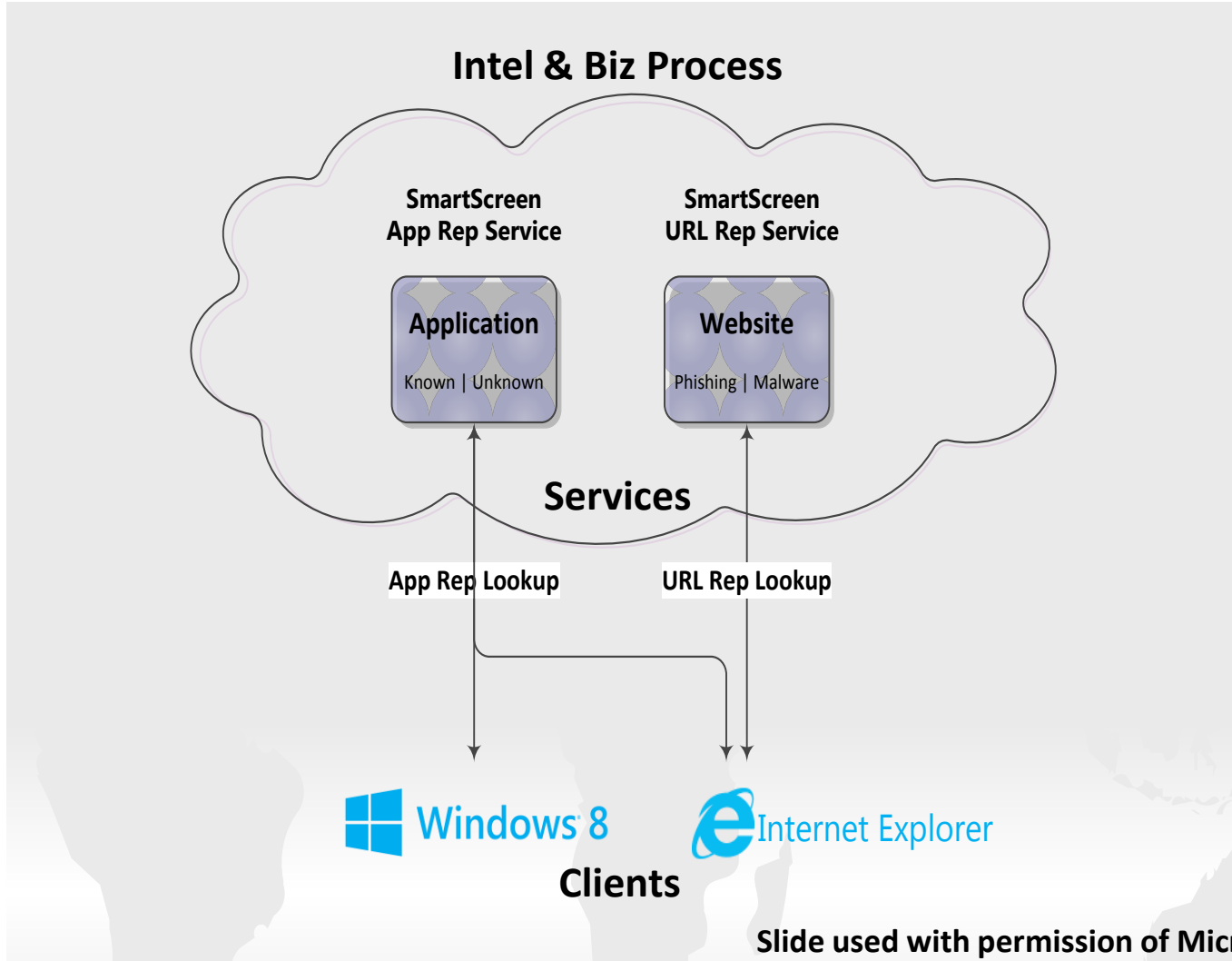
Scope of SmartScreen



Slide used with permission of Microsoft Corporation



High Level Architecture



Slide used with permission of Microsoft Corporation



The Mark Of The Web (MOTW)

What is the M

The MOTW is a comment that a browser user opens the webpage. When the browser references this comment, it runs the page. Here's

```
<!-- saved from url=(
```

To be valid, a MOTW comment must start with

```
<!-- saved from url=
```

The comment must end with

```
-->
```

WWW

Hebrew Equivalent

vav vav vav

Hebrew Numeric Value

6 6 6

Coincidence ???

code for a webpage. When a browser user opens the webpage, the browser references this comment and runs the page. Here's

```
<!-- saved from url=(
```

To be valid, a MOTW comment must start with

```
<!-- saved from url=
```

The comment must end with

```
-->
```

Art by markbeast666.blogspot.com

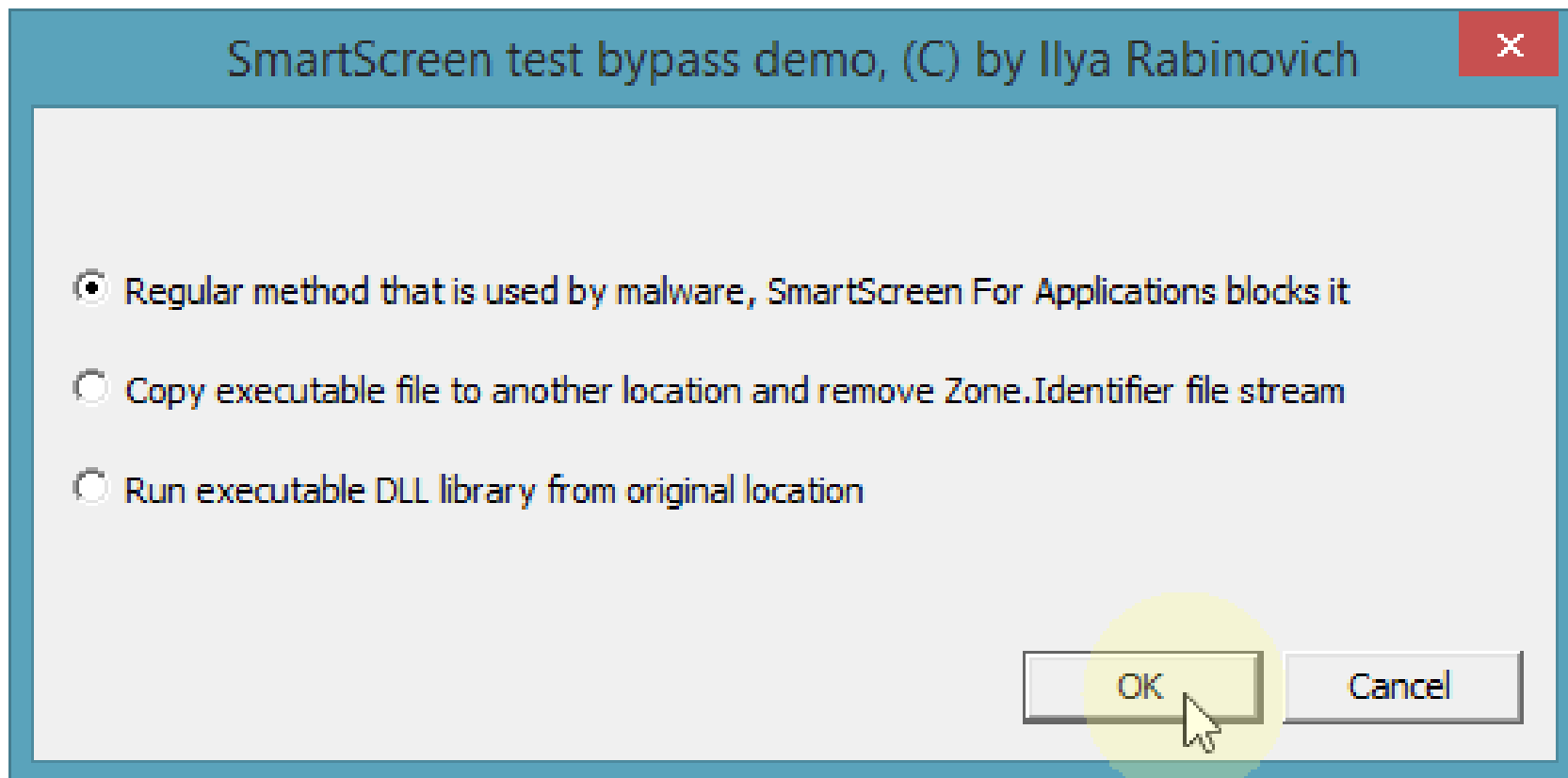
[http://msdn.microsoft.com/en-us/library/ms537628\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms537628(v=VS.85).aspx)

Attacks Against App Rep

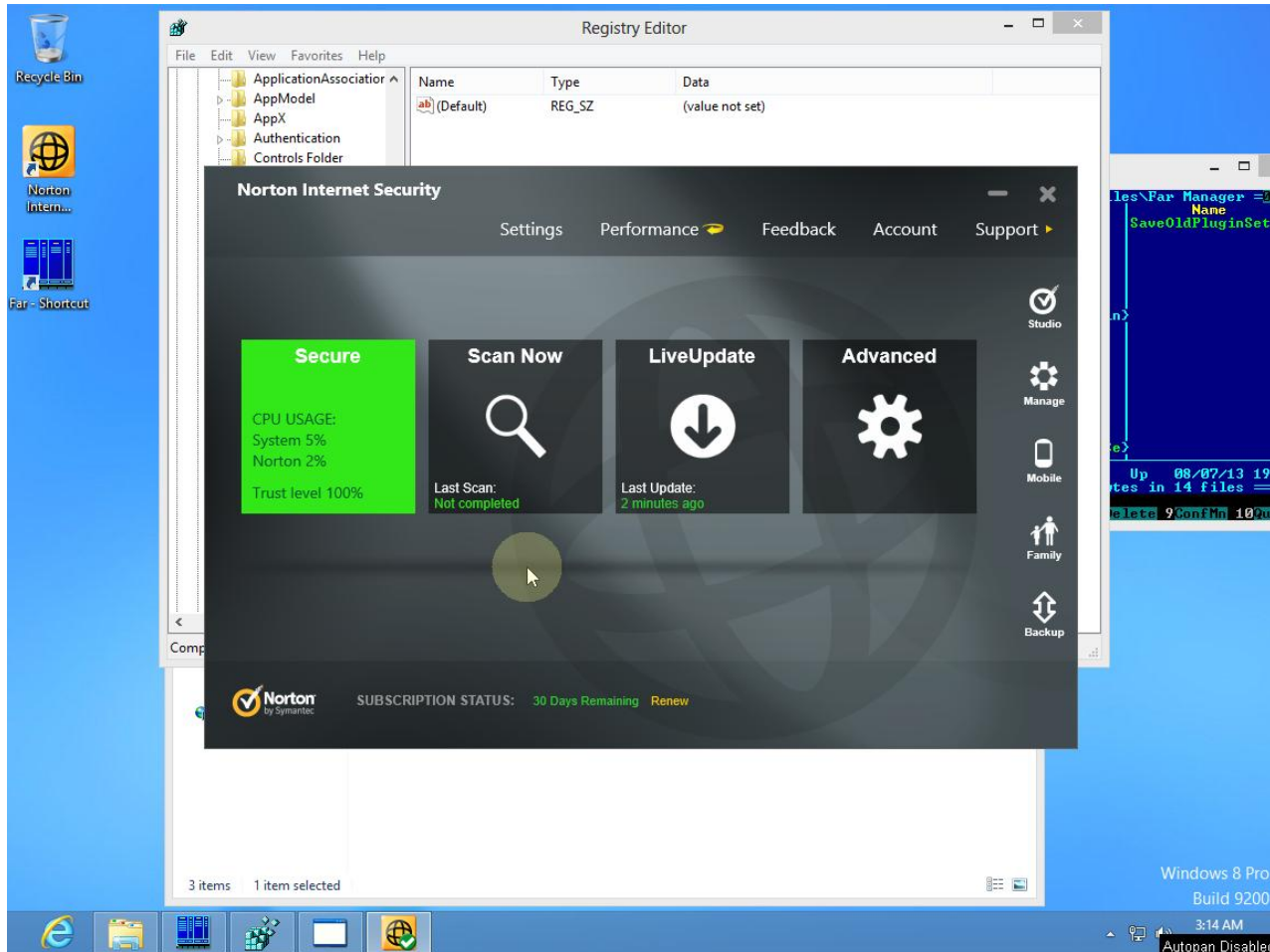
- Remove MOTW
- Run From DLL
- COM Elevation bypassing UAC whitelists



MOTW Removal & Execution From DLL



Protection Techniques – App Rep

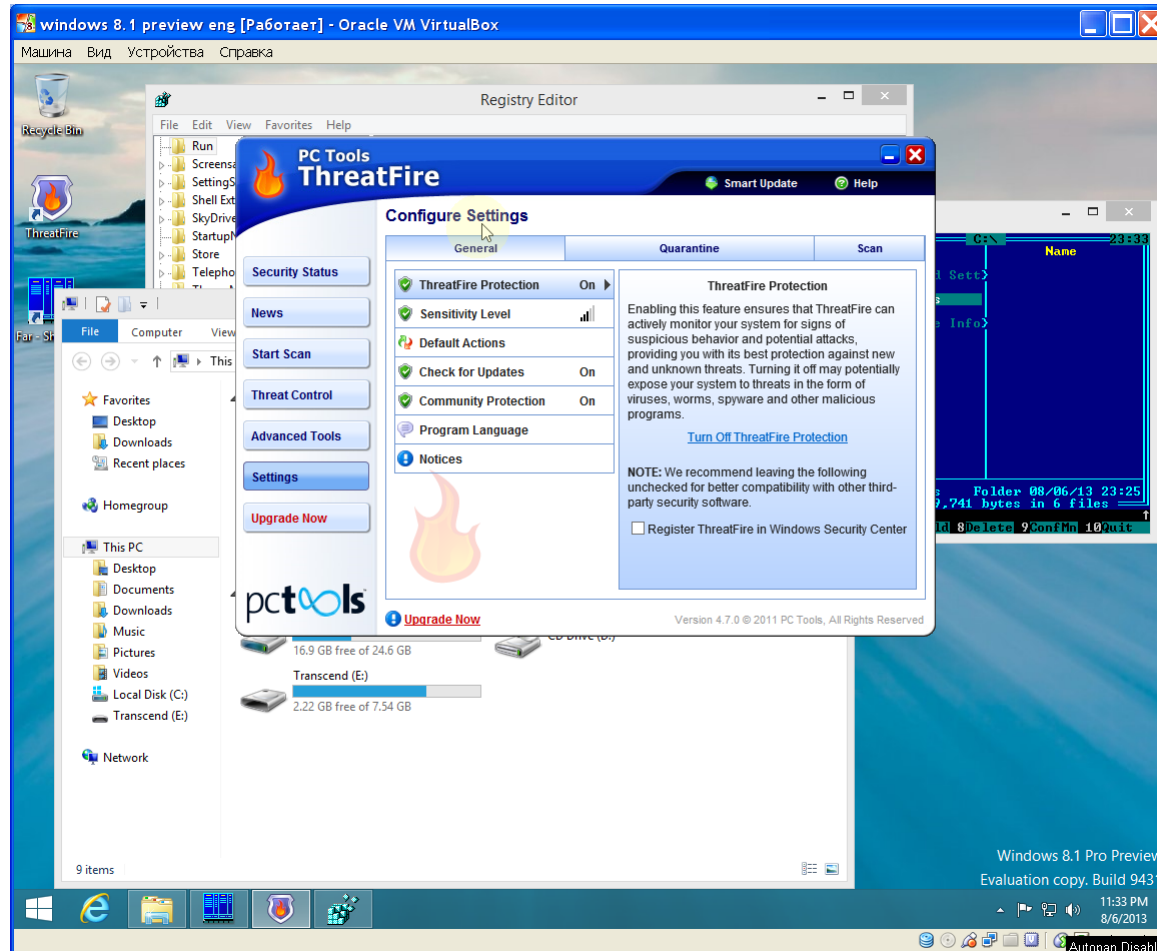


Protection Techniques – App Rep

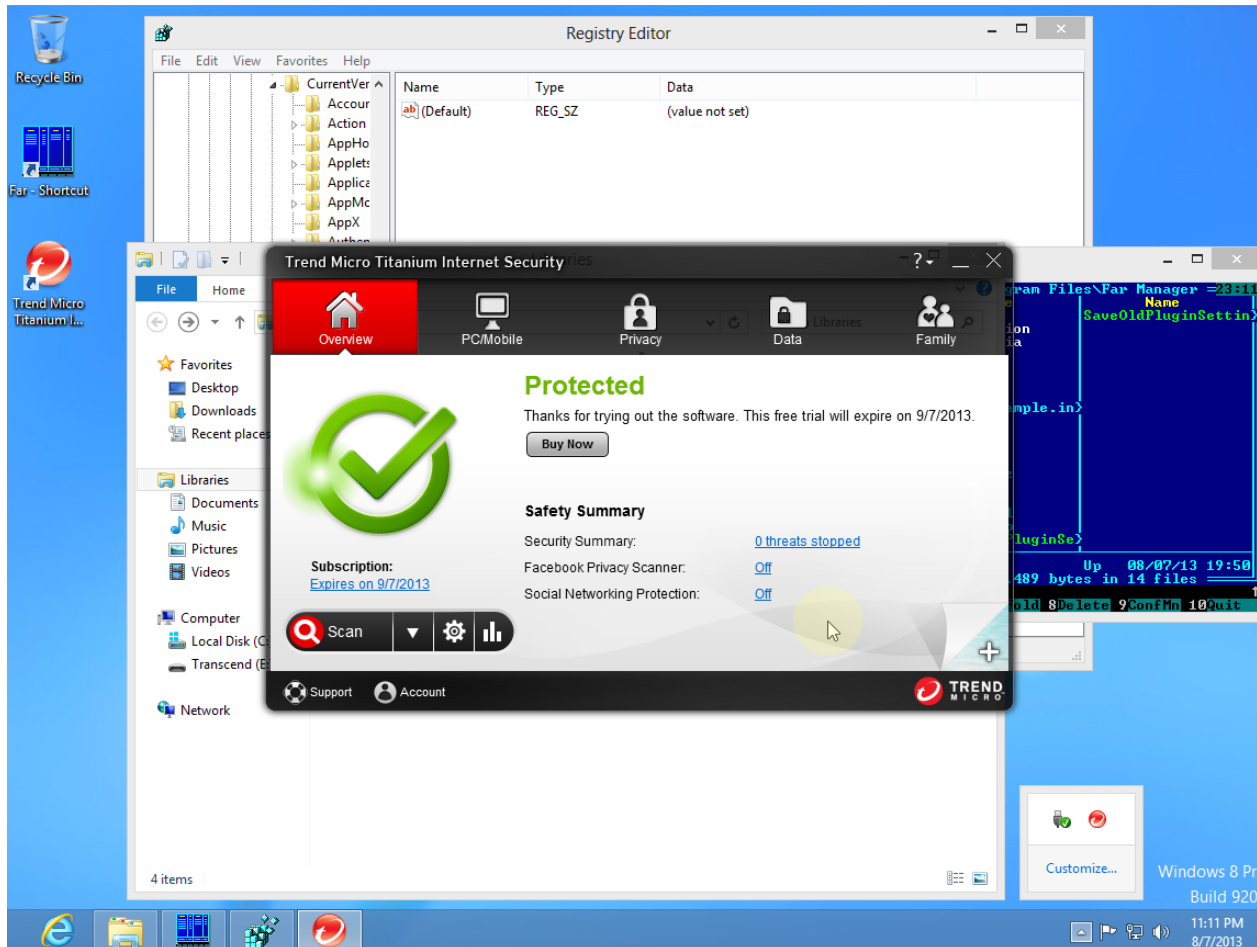
The screenshot displays a Windows 8 Pro desktop environment. In the foreground, the Avast! Internet Security application is open, showing the 'Virus protection' dashboard. The dashboard includes a 'SUMMARY' section with 'Current Status' and 'Statistics', and a 'Cloud Intelligence' section with 'REPUTATION SERVICES' (Enabled) and 'STREAMING UPDATES' (Enabled). A 'Connection established' message is visible between the reputation services and streaming updates. The background shows the Registry Editor window with the 'CurrentVersion' key selected, and a taskbar with various icons including Recycle Bin, avast! Internet Security, and Far-Shortcut. The system tray shows the date and time as 1:43 AM on 8/9/2013.

Shield	Status
File System Shield	4175 / 0
Web Shield	192 / 0
Mail Shield	0 / 0
Network Shield	779 / 0
P2P Shield	0 / 0
IM Shield	0 / 0
Behavior Shield	137 / 0
Script Shield	0 / 0

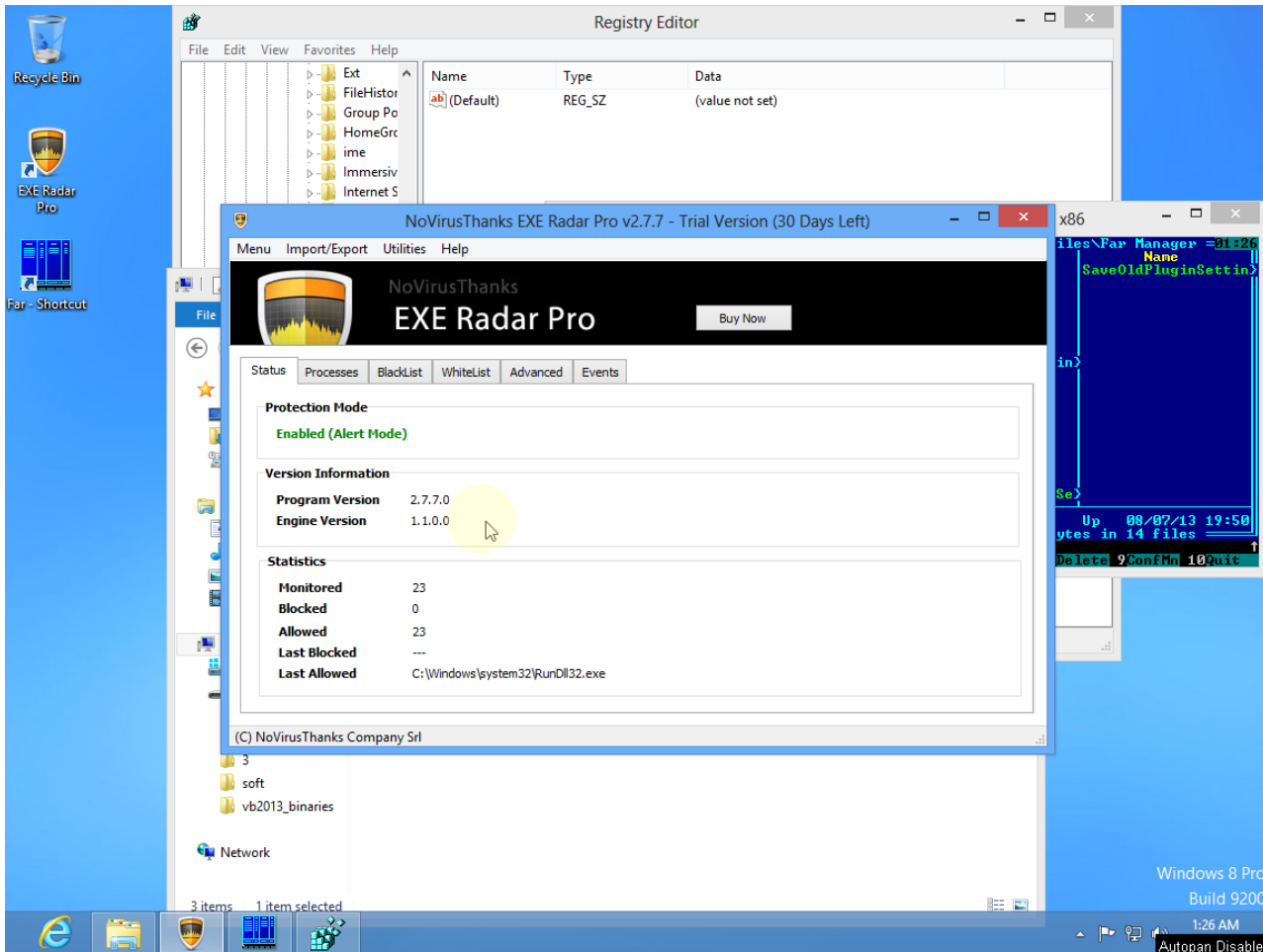
Protection Techniques – Behavior Blocking



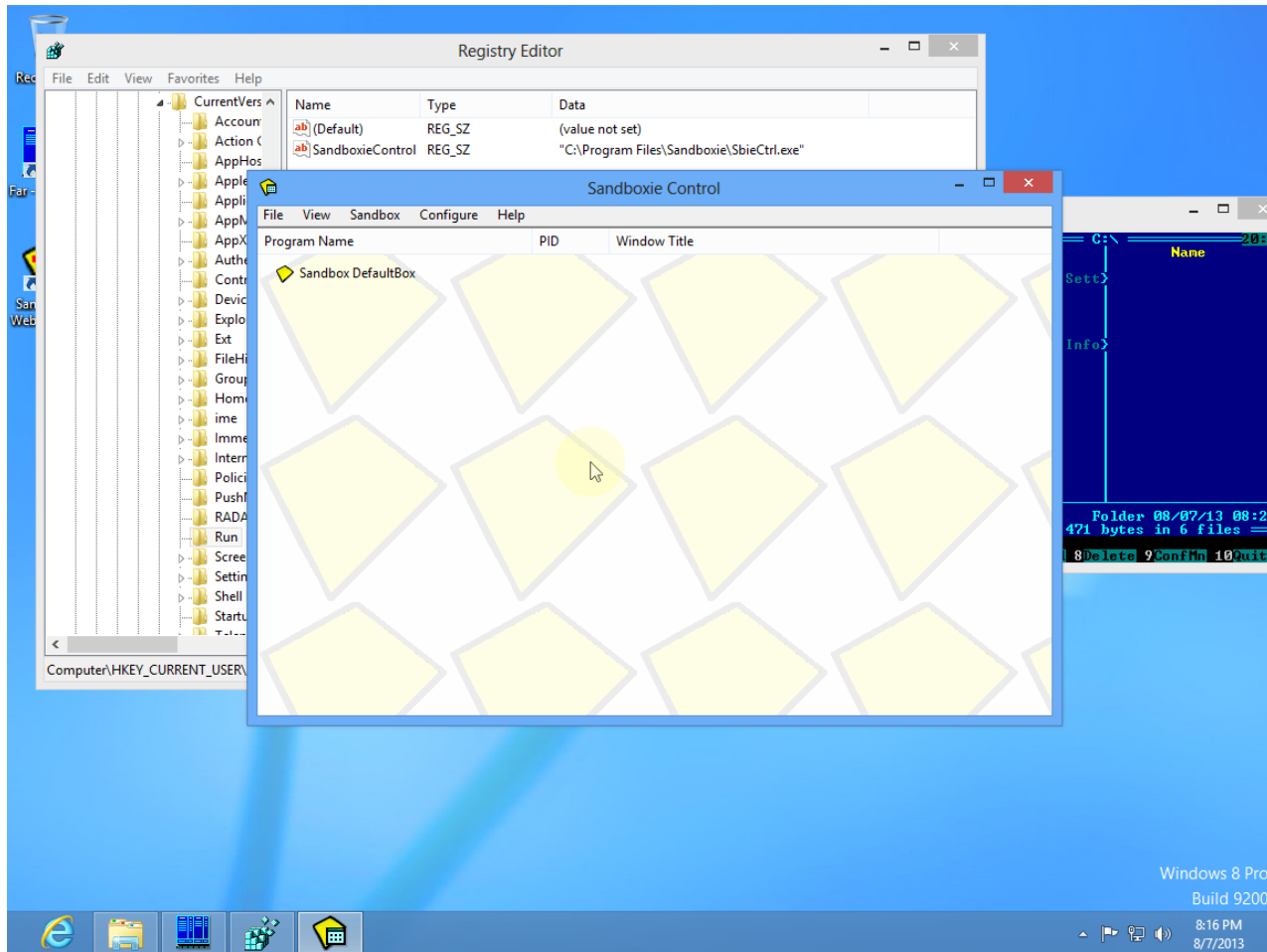
Protection Techniques – Behavior Blocking



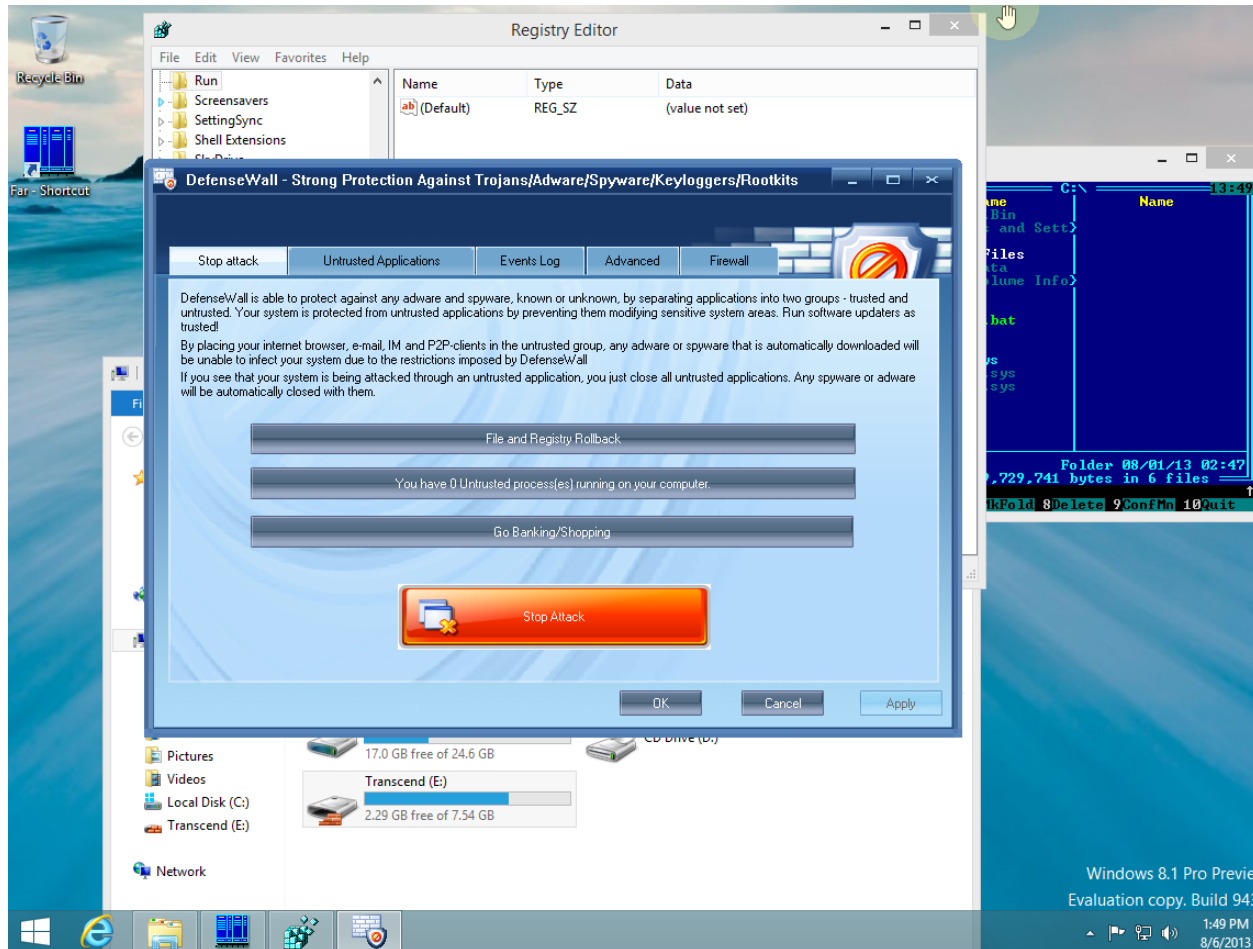
Protection Techniques – Whitelisting



Protection Techniques – Sandboxing



Protection Techniques – Sandboxing



Remember...

- SmartScreen App Rep adds meaningful protection, but...
- Some critical vectors are not covered by SmartScreen
- Additional security protections are required
- “If you see only one solution you probably don’t understand the problem” *Author unknown*



Thank You!!!

QUESTION

Randy Abrams – rabrams@nsslabs.com

Ilya Rabinovich – rabinovich@softsphere.com

