SoftSphere Technologies

WINDOWS 8 SMARTSCREEN APPLICATION CONTROL

What More Could You Ask For?

Randy Abrams – NSS Labs
Ilya Rabinovich – SoftSphere Technologies

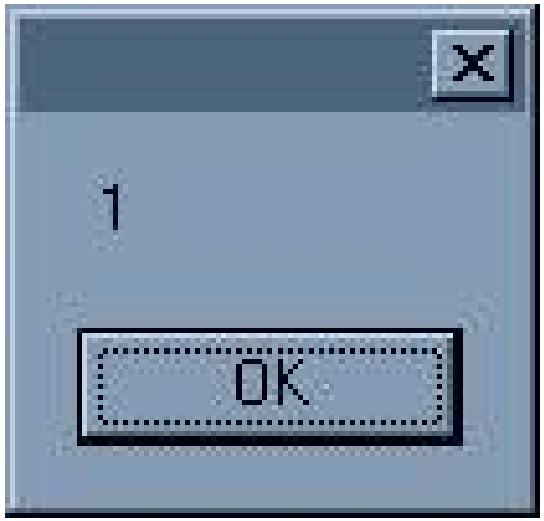
NSS LABS
WE MAKE SECURITY A SCIENCE

Show and Tell

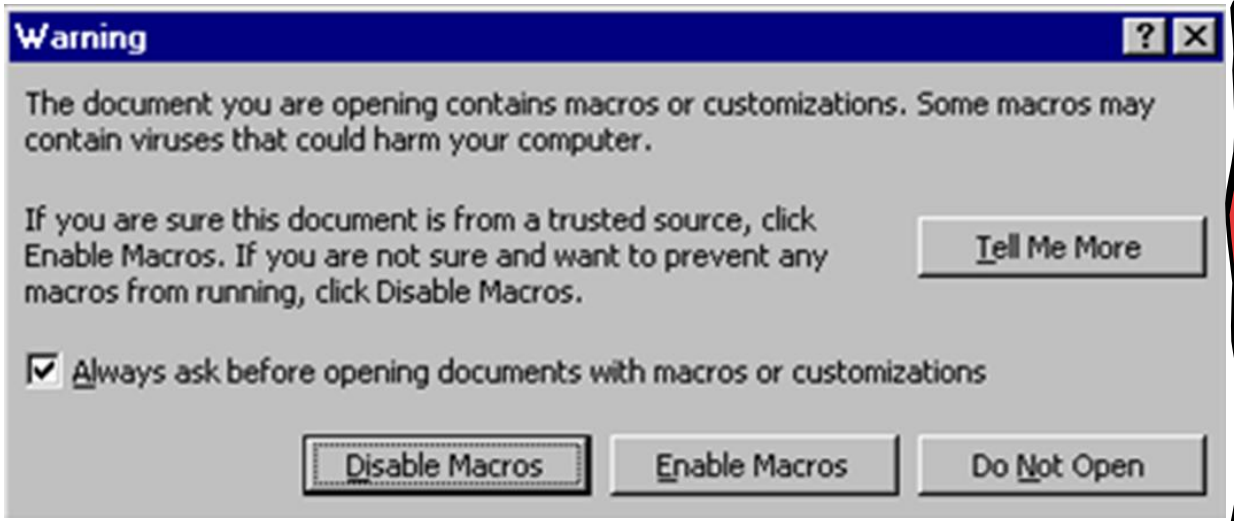
- Tell First, Show Later
- The History of SmartScreen App Rep
- What App Rep Does and Does Not Do
- Showtime!!! (Technologies that Plug the Holes)
- It’s a Wrap

Name That Virus

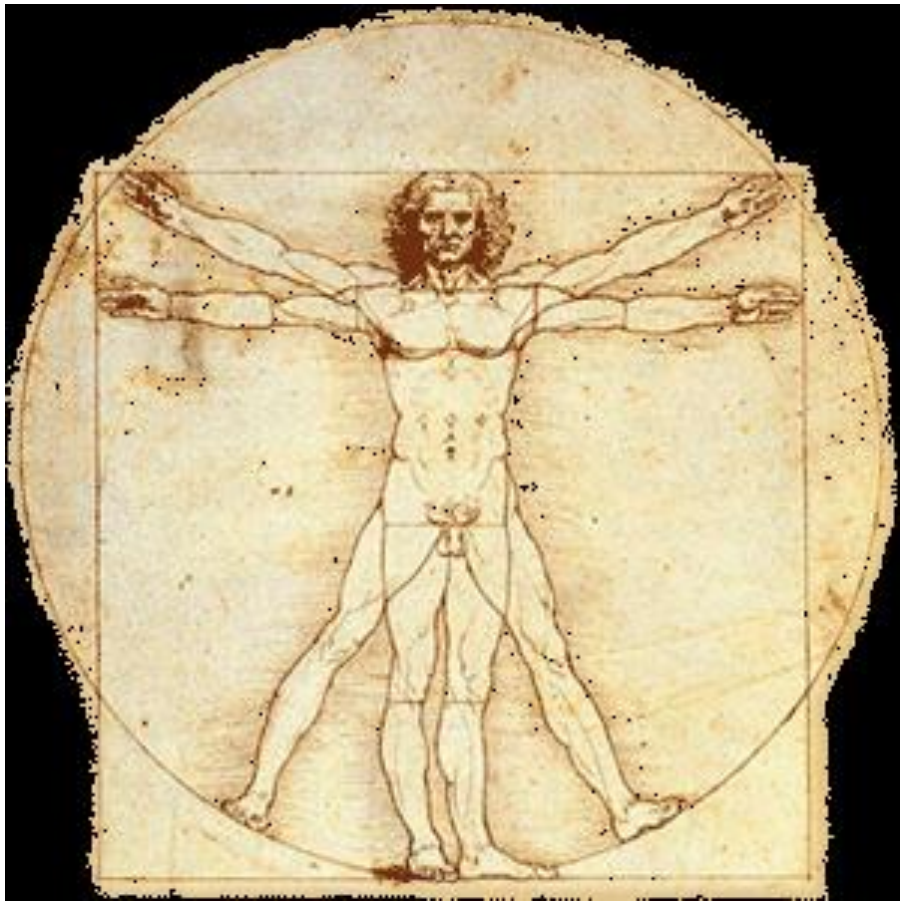
- W97M/Concept



Medieval App Rep



Renaissance App Rep



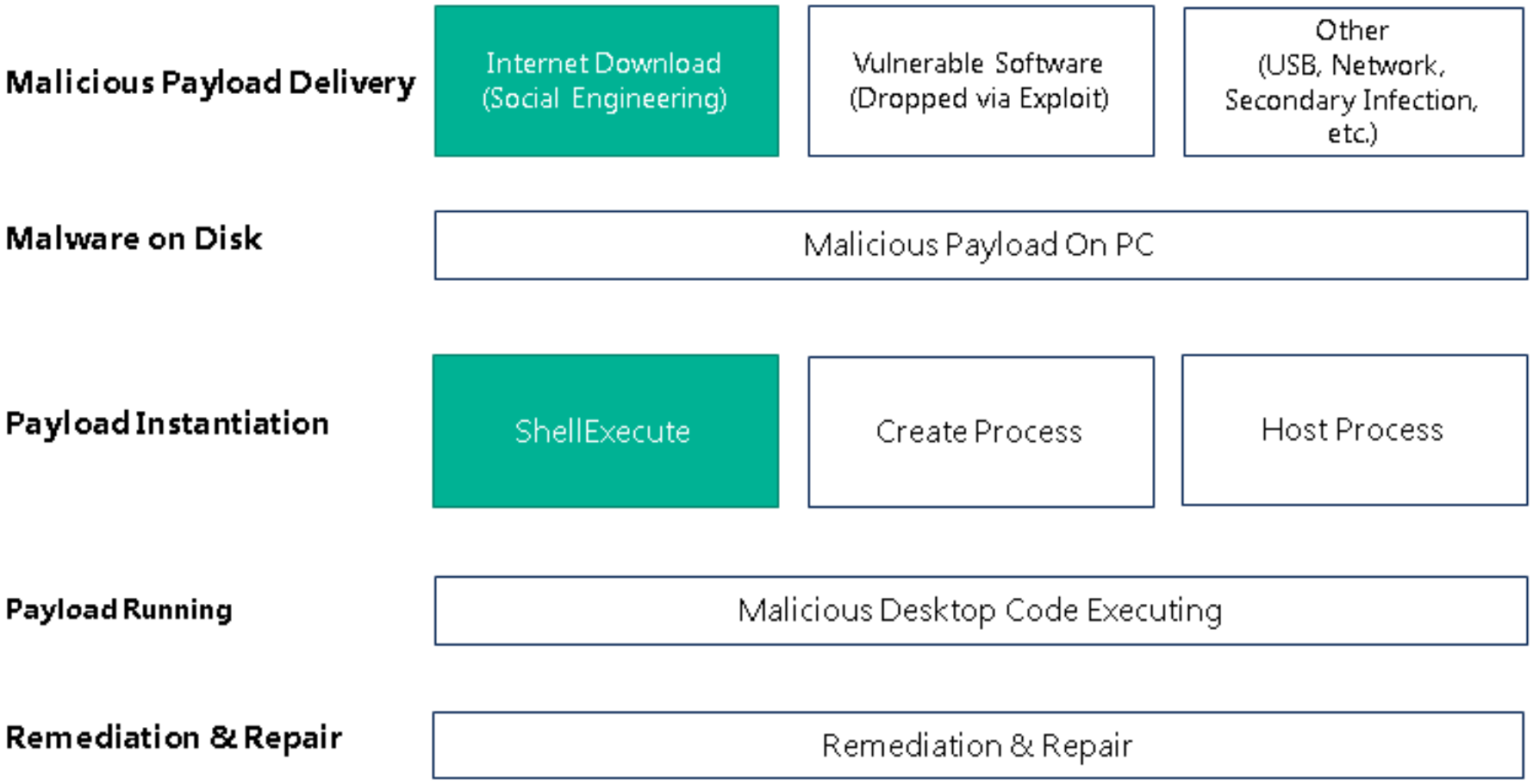
SmartScreen Evolution

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

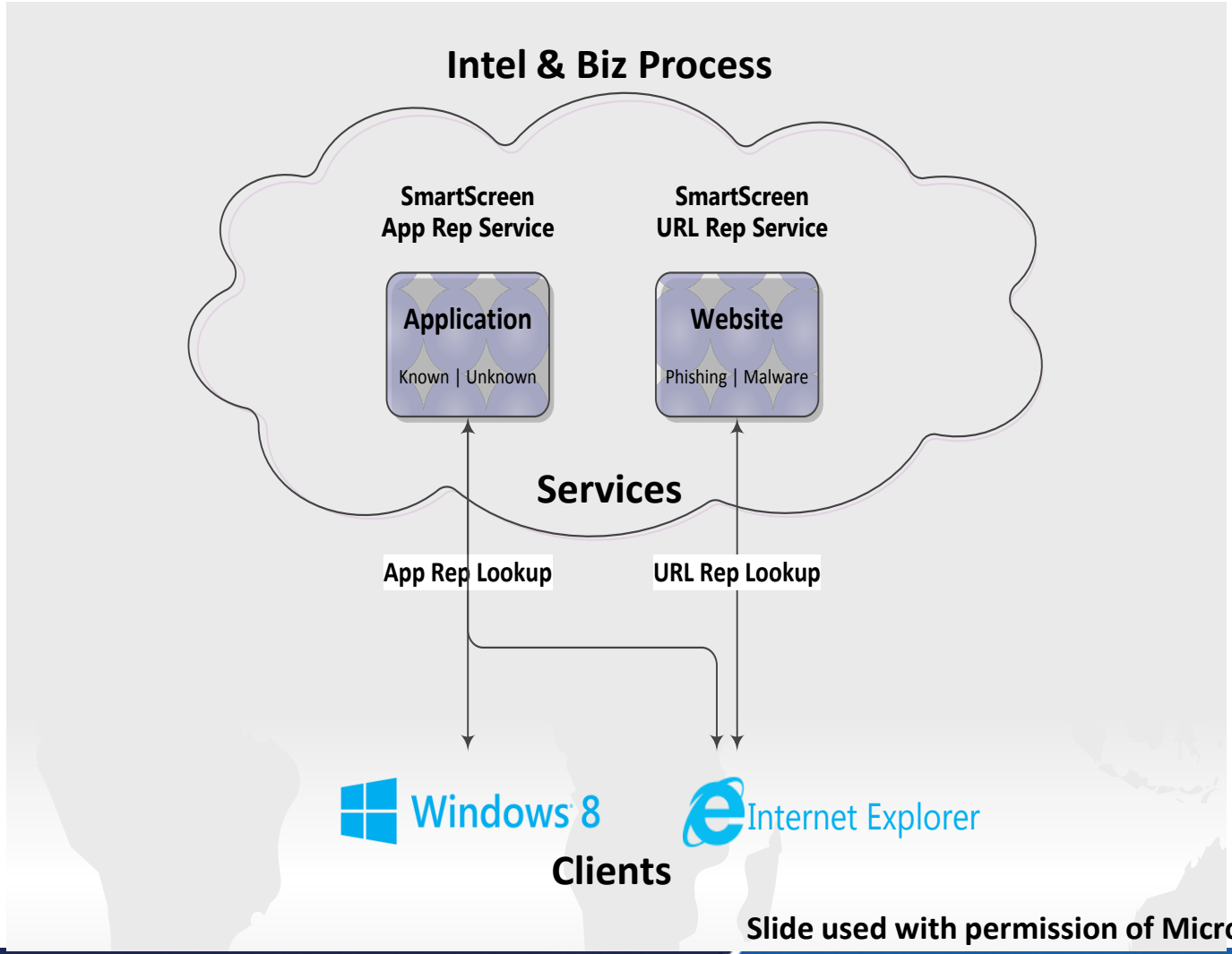
Slide used with permission of Microsoft Corporation

Scope of SmartScreen

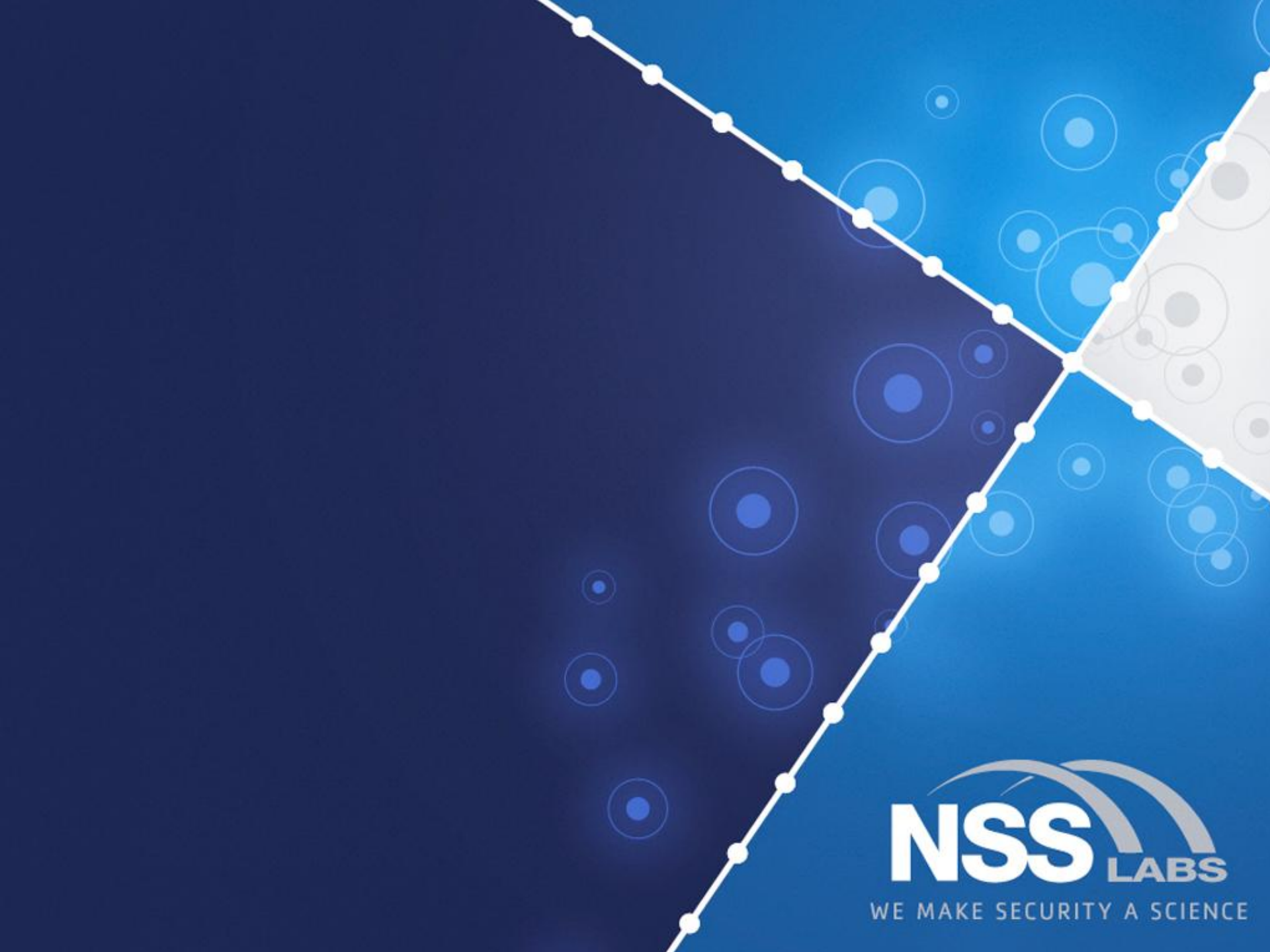


Slide used with permission of Microsoft Corporation

High Level Architecture



Slide used with permission of Microsoft Corporation


NSS LABS
WE MAKE SECURITY A SCIENCE

The Mark Of The Web (MOTW)

What is the M

The MOTW is a comm ‹up for a webpage. When a user opens the webp Internet Explorer references this comm y zone in which it should run the page. Here's

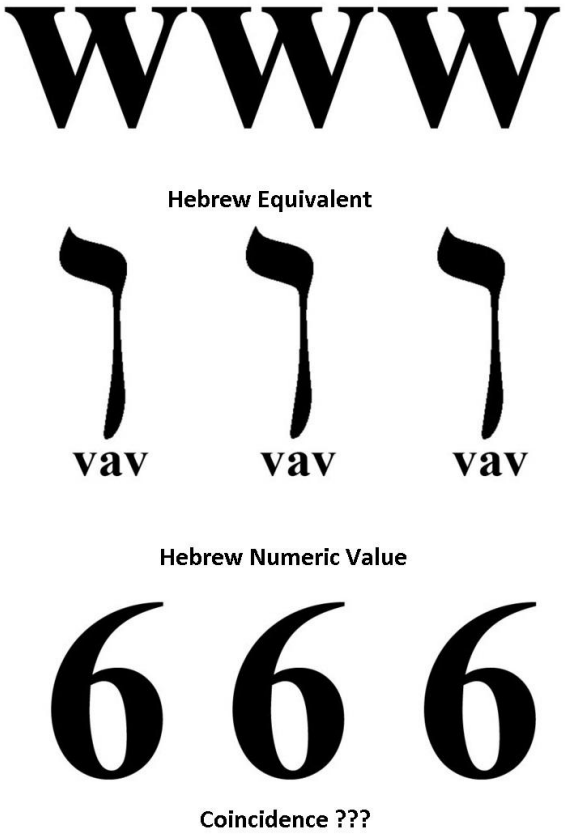
<!-- saved from url=(ɔm/ -->

To be valid, a MOTW simple rules. The comment must s

<!-- saved from url=

The comment must e

-->

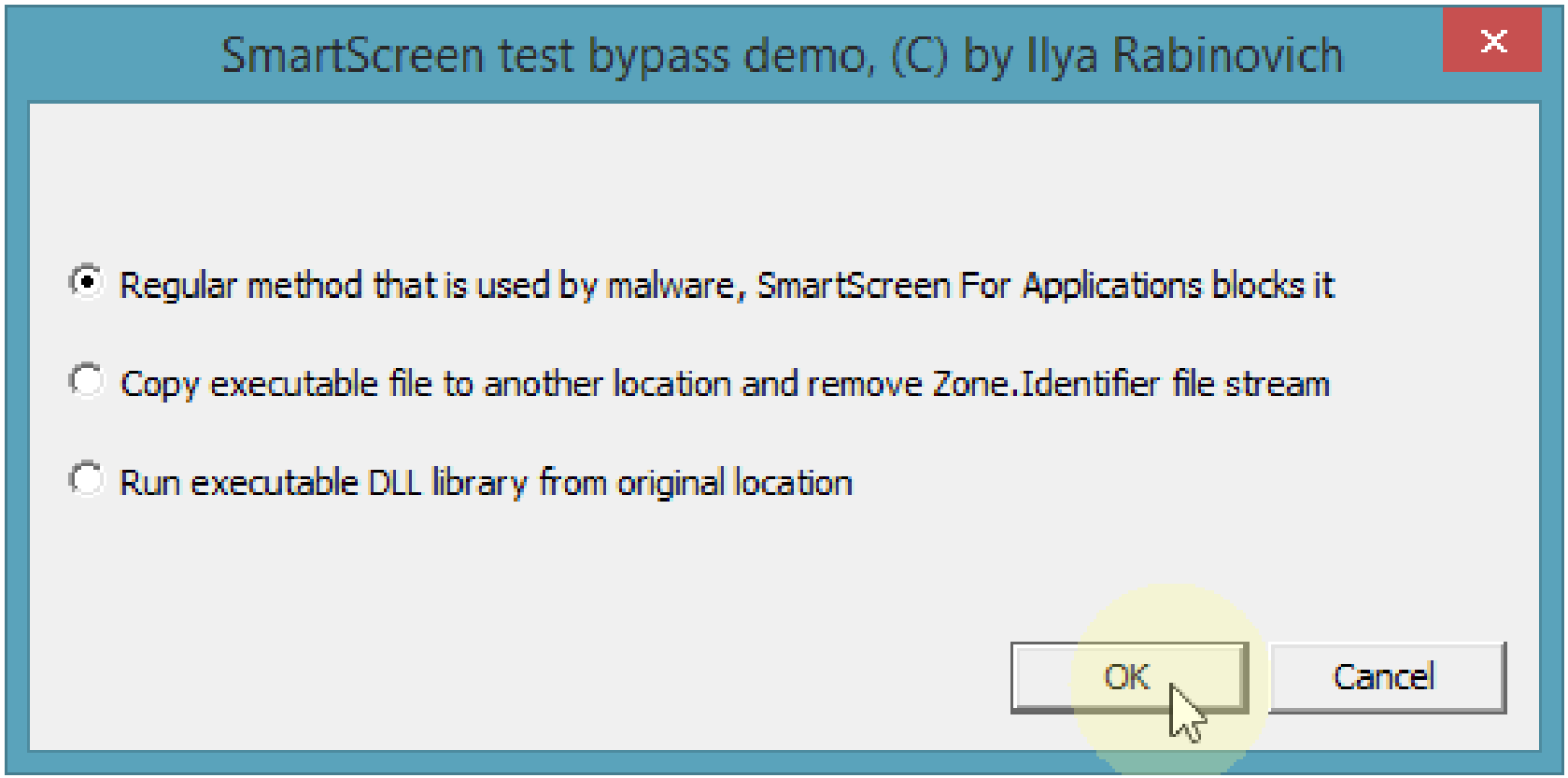


http://msdn.microsoft.com/en-us/library/ms537628(v=VS.85).aspx

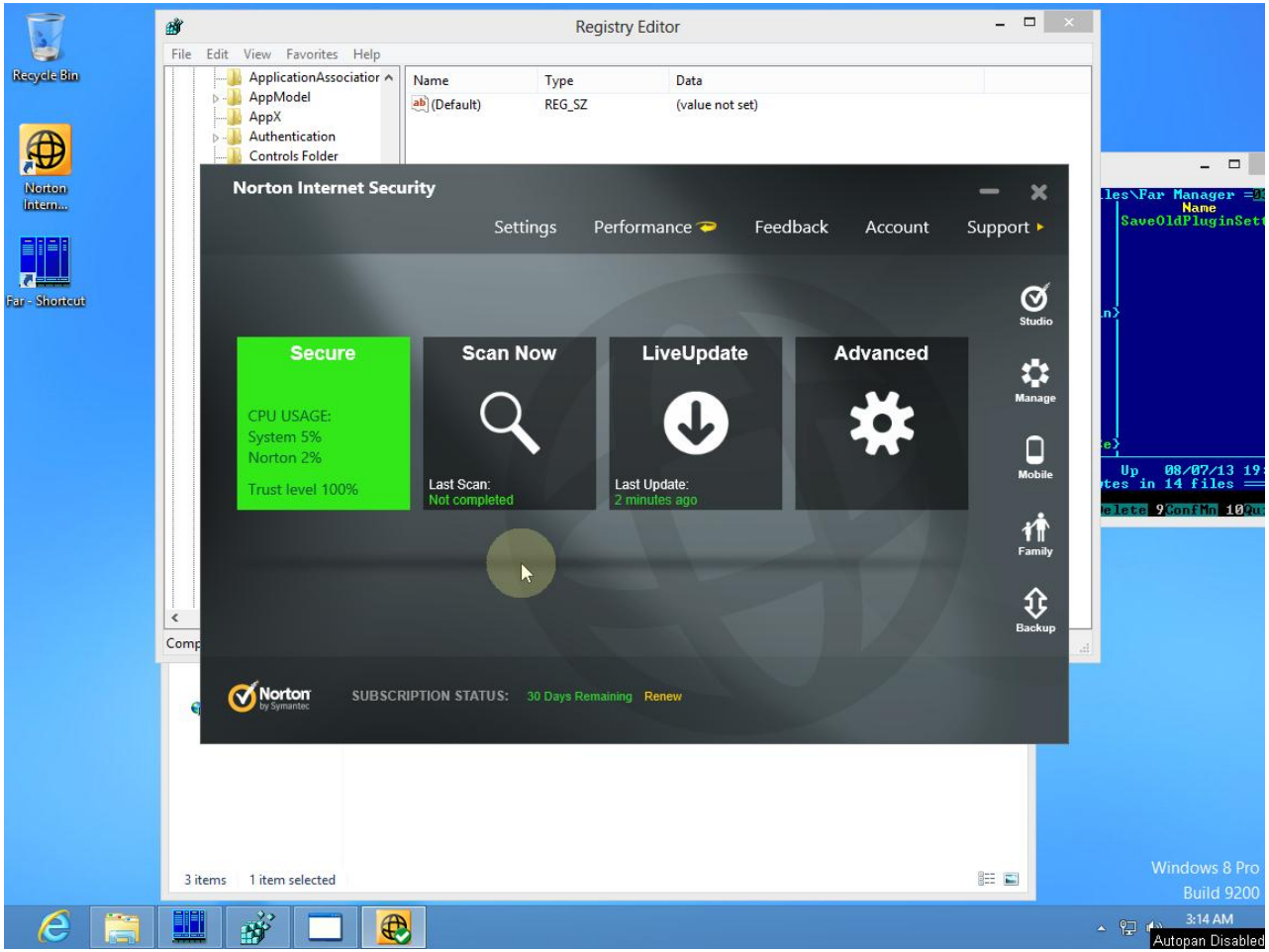
Attacks Against App Rep

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

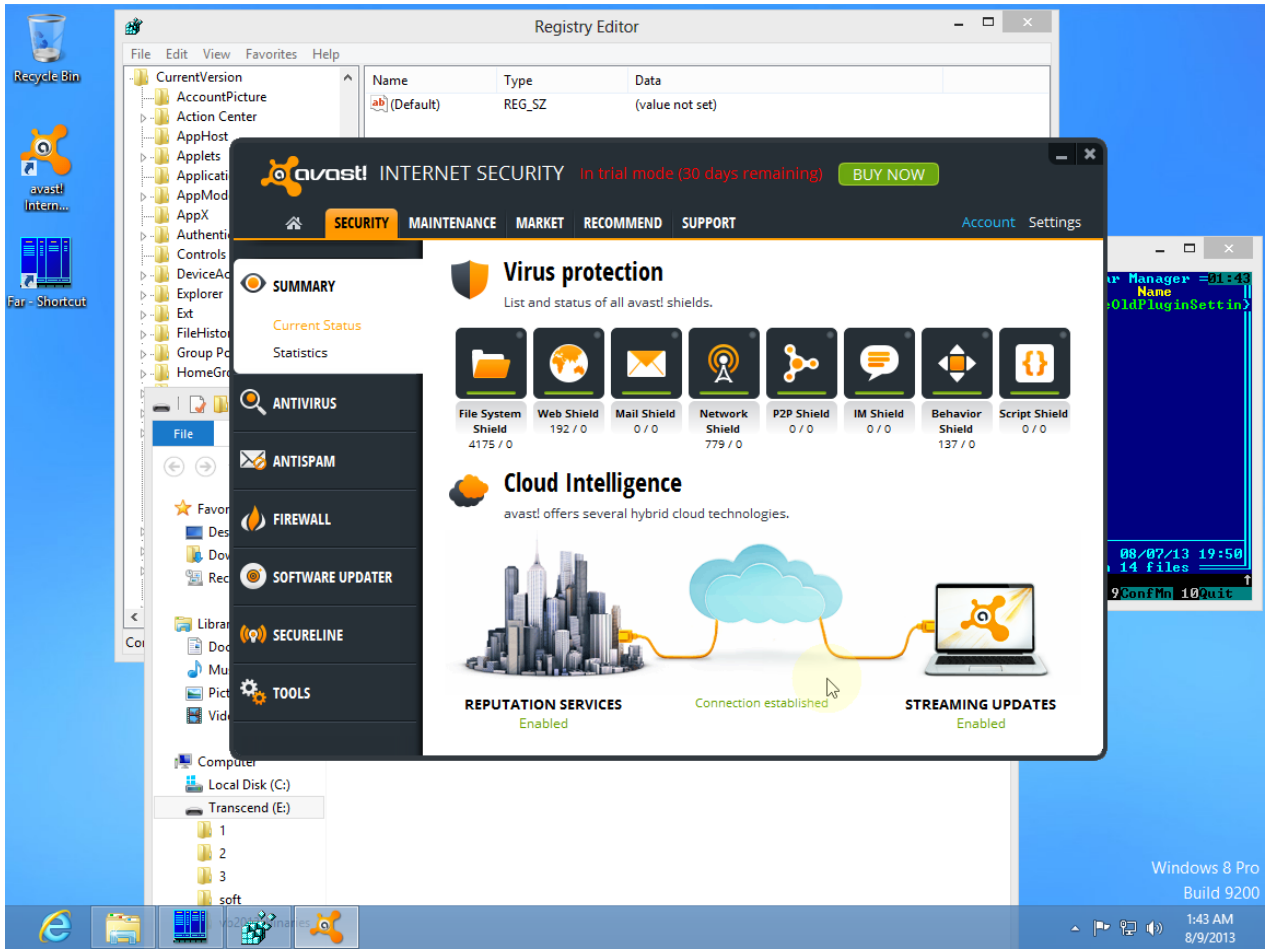
MOTW Removal & Execution From DLL



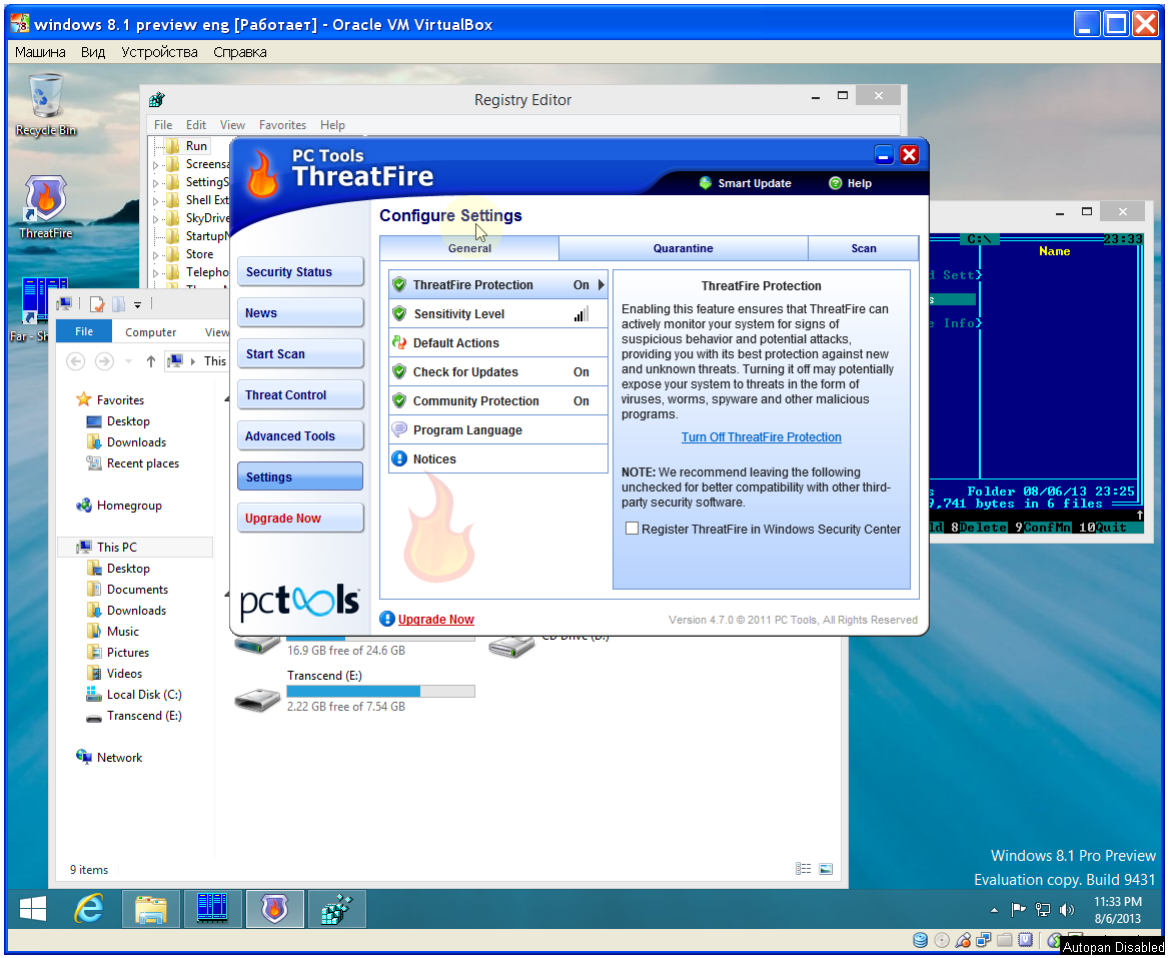
Protection Techniques – App Rep



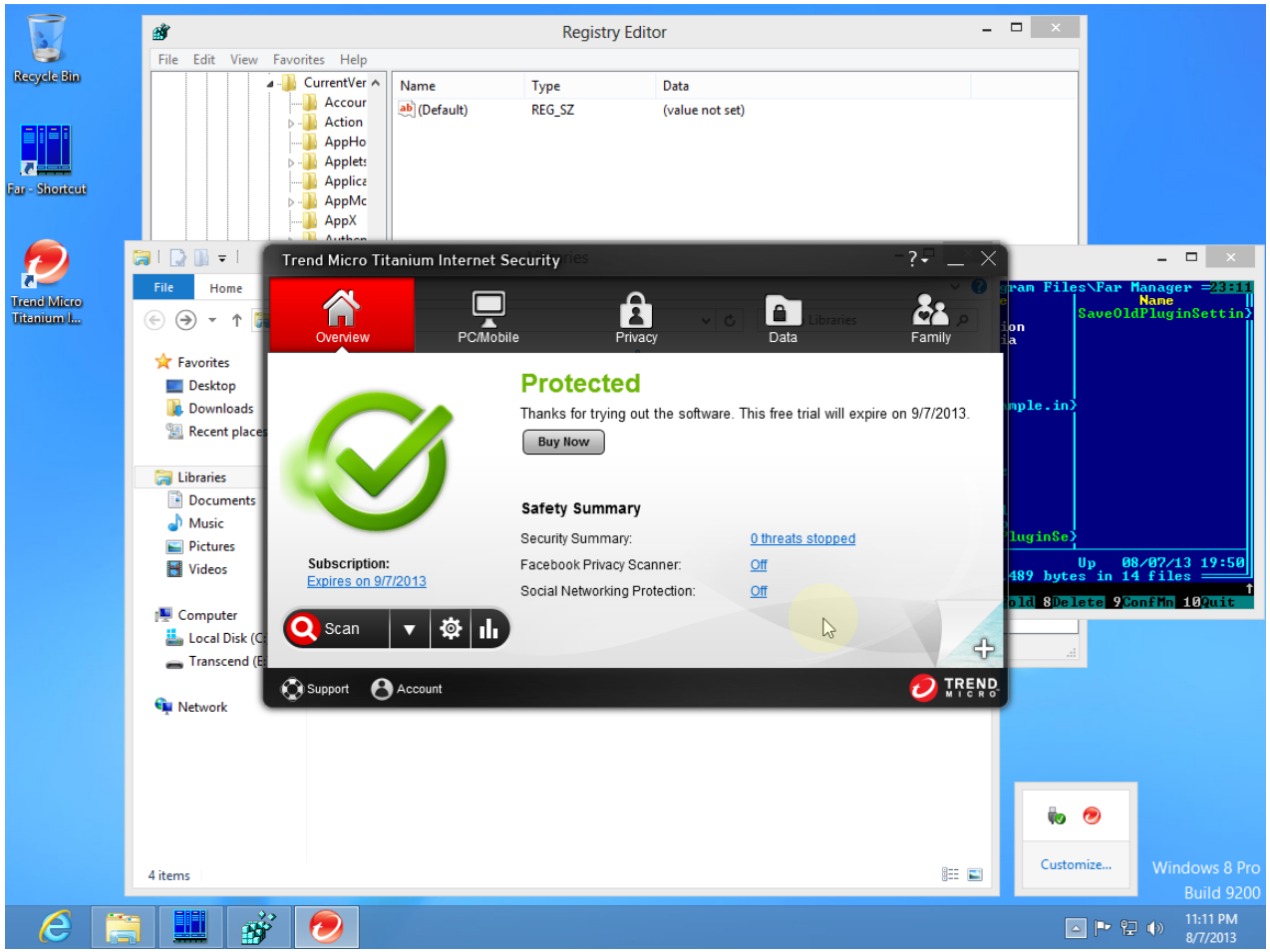
Protection Techniques – App Rep



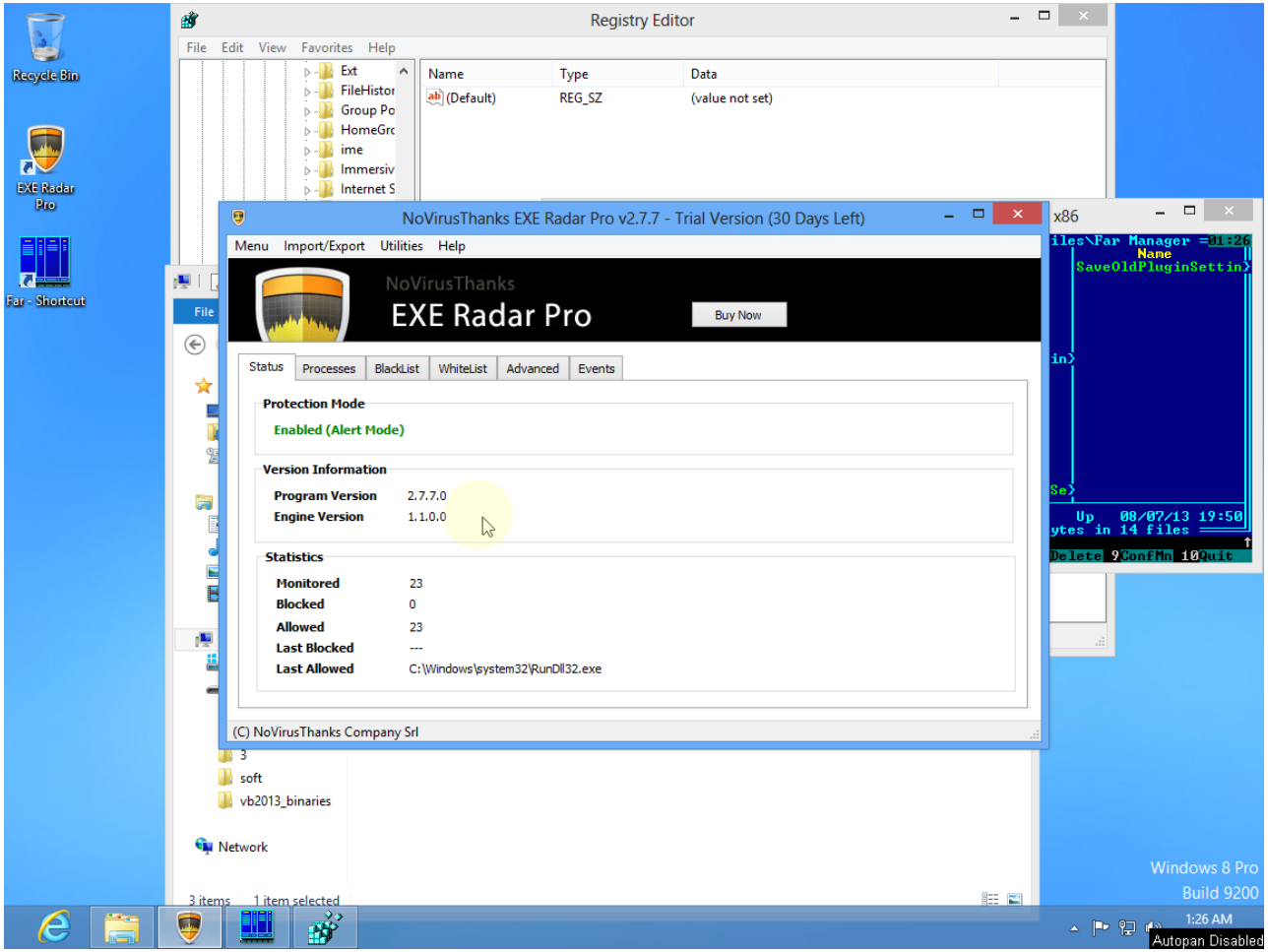
Protection Techniques – Behavior Blocking



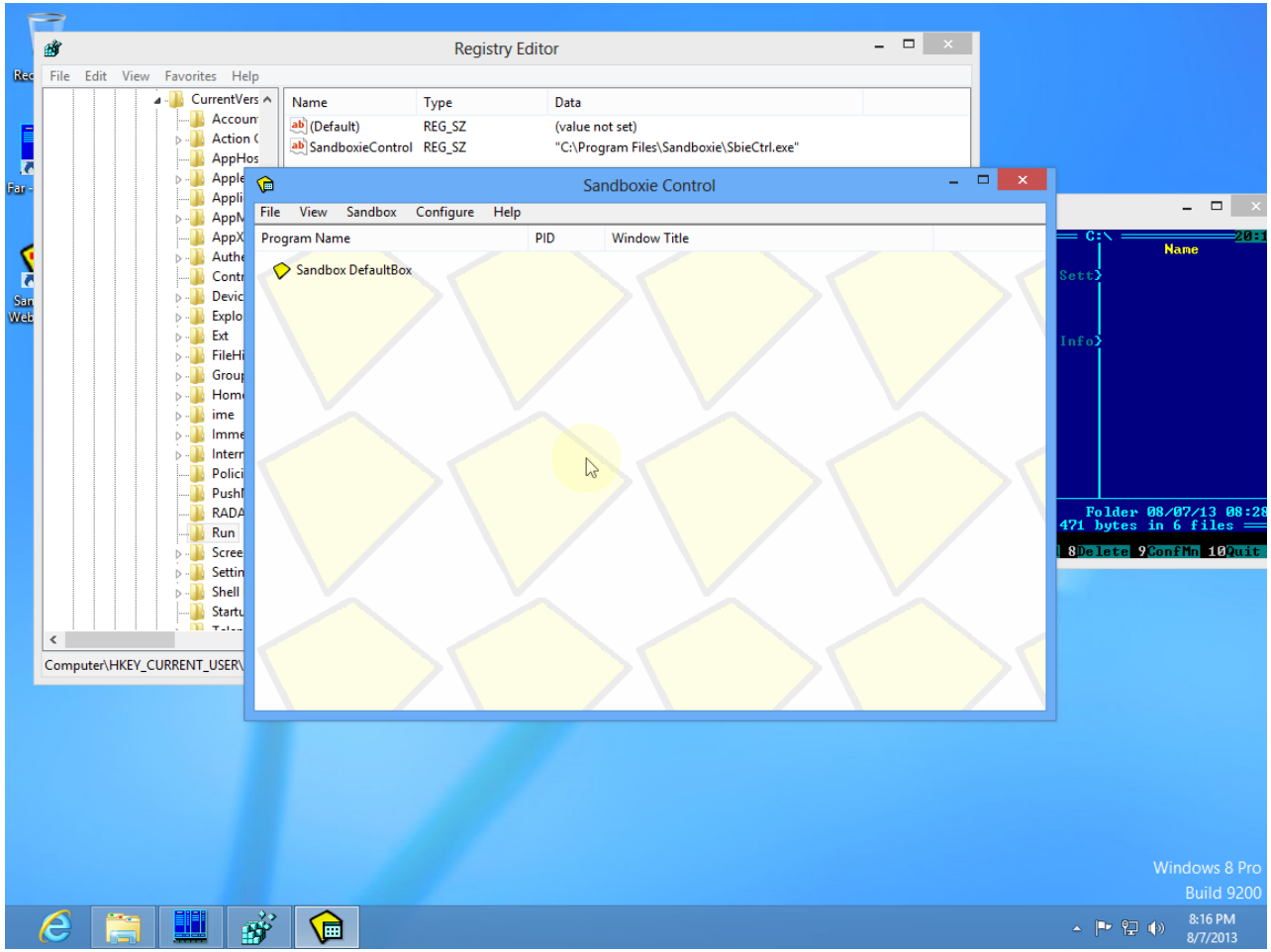
Protection Techniques – Behavior Blocking



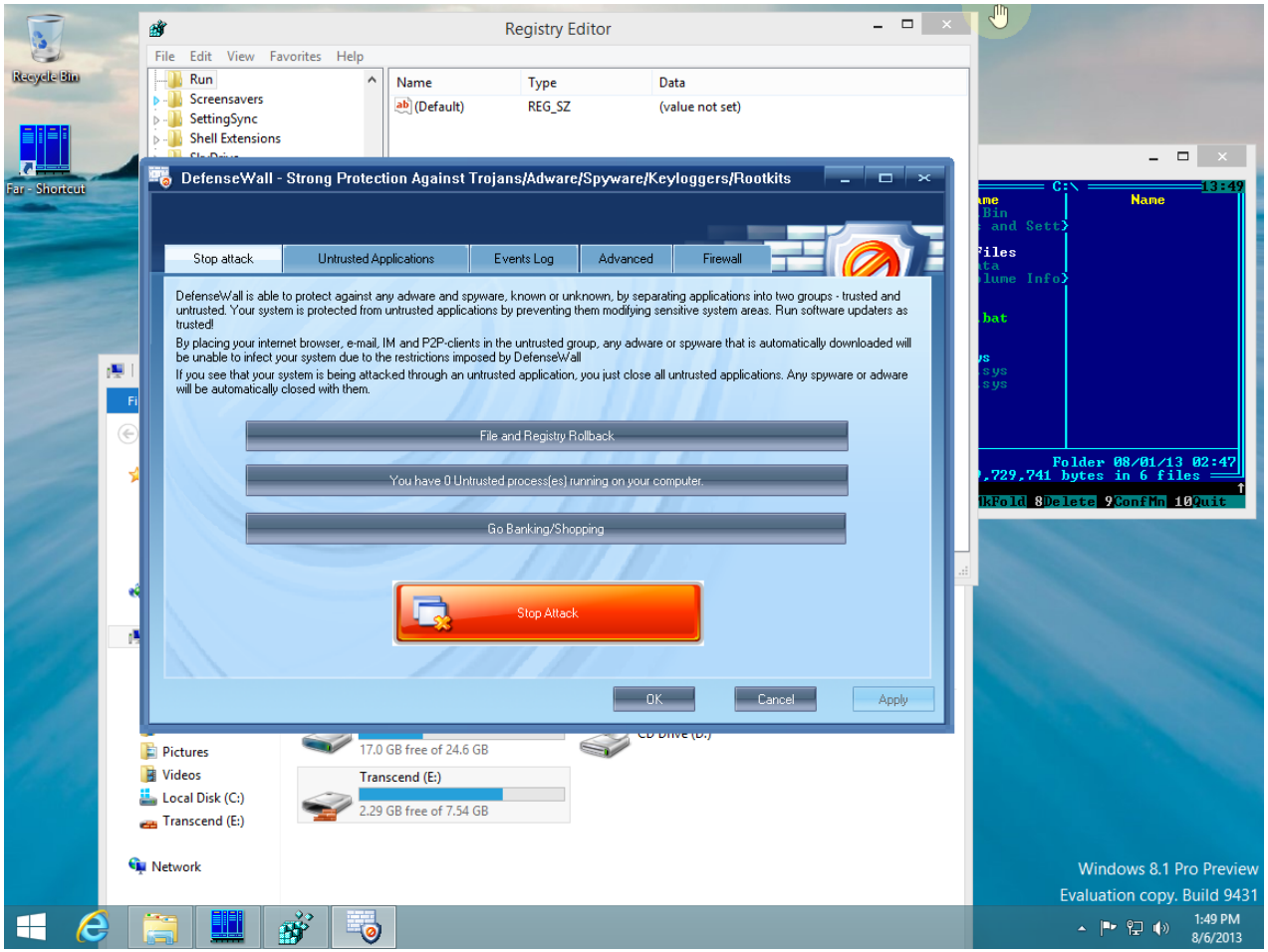
Protection Techniques – Whitelisting



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!!!

Randy Abrams – rabrams@nsslabs.com

Ilya Rabinovich – rabninovich@softsphere.com