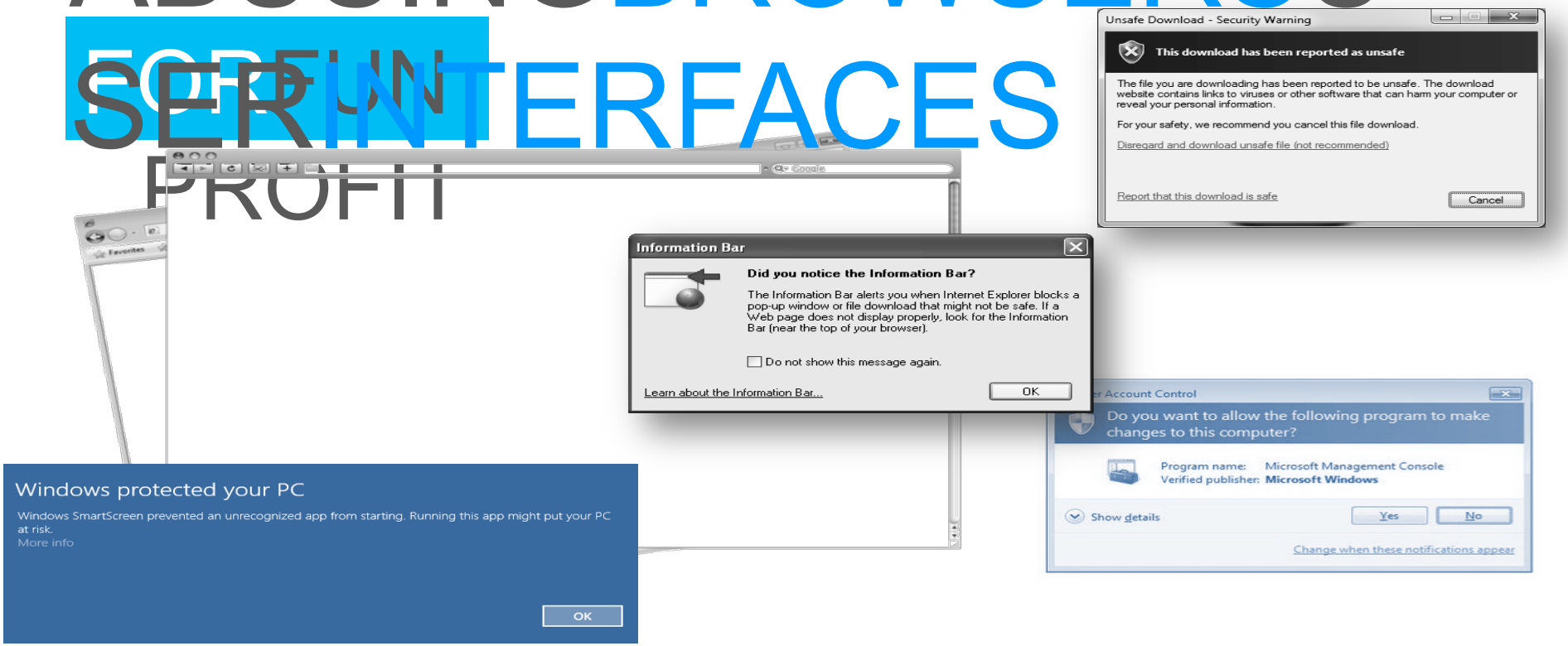
ABUSING BROWSERS UI FOR FUN AND PROFIT



HELLO

MY NAM Rosario

sites.google.com/site/tentacoloviola/

SOCIALLYENGINEERED

2012 FACTS

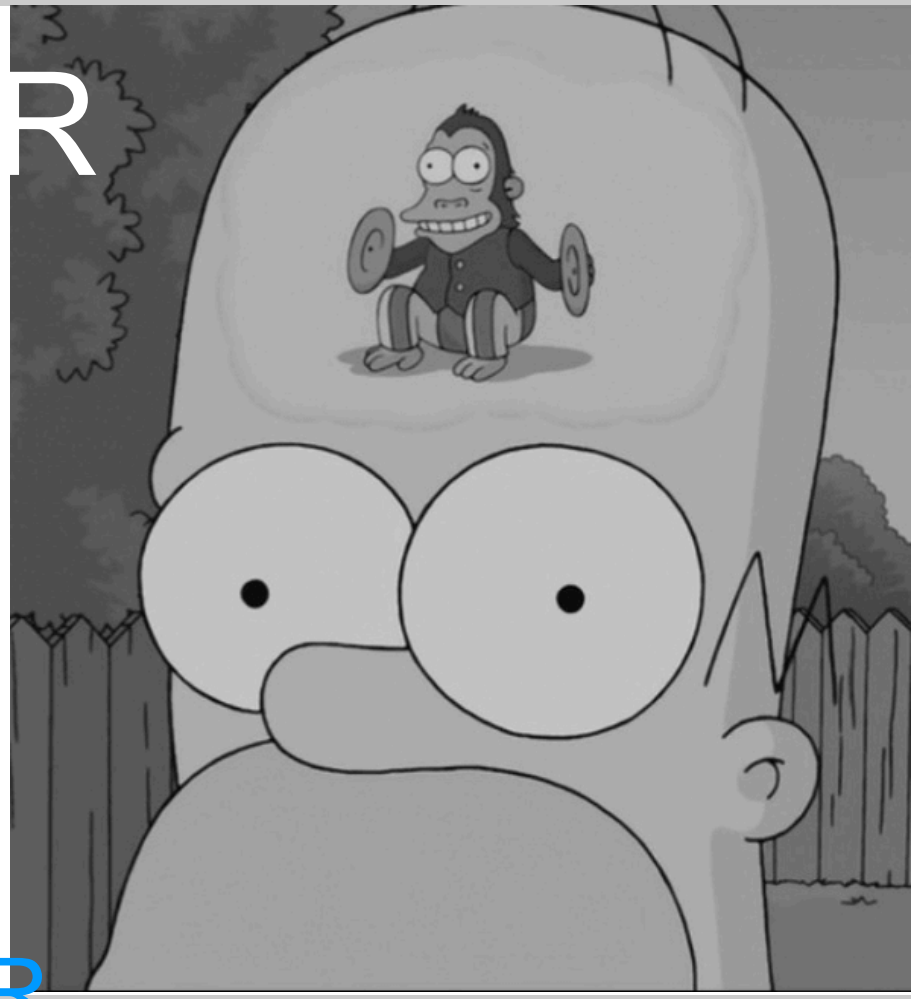
200K NEW MALWARE SAMPLES EVERY DAY

1.5+ BILLIONS MALWARE ATTACKS ORIGINATED FROM THE WEB

MOSTLY ORIGINATED BY USER INITIATED DOWNLOADS

USERSASKR

- GUIDANCE WHILE SURFING THE WEB
- PROTECTION FROM MALICIOUS SITES
- RELIABLE BROWSER



VENDORSREPLIES

ENHANCED MEMORY PROTECTION TECHNOLOGIES FOR PROTECTING AGAINST EXPLOITS AND DRIVEBY DOWNLOADS (ASLR, DEP, GS, ETC)

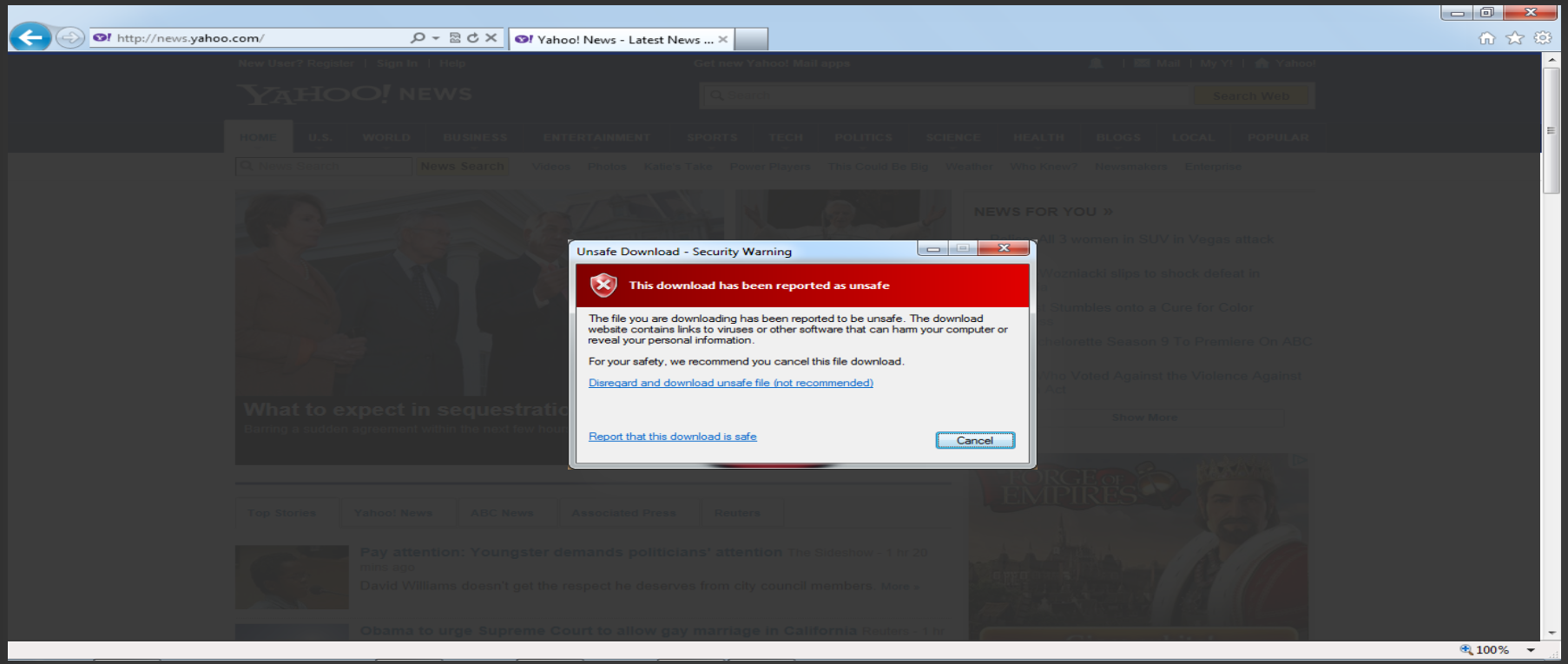
EMBEDDED SECURITY FITERS AGAINST WEB ATTACKS (XSS FILTER, ANTI FRAMING/ CLICKJACKING, ETC)

MALWARE/PHISHING RECOGNITION TECHNOLOGIES (SAFE BROWSING, SMARTSCREEN FILTER, ETC)

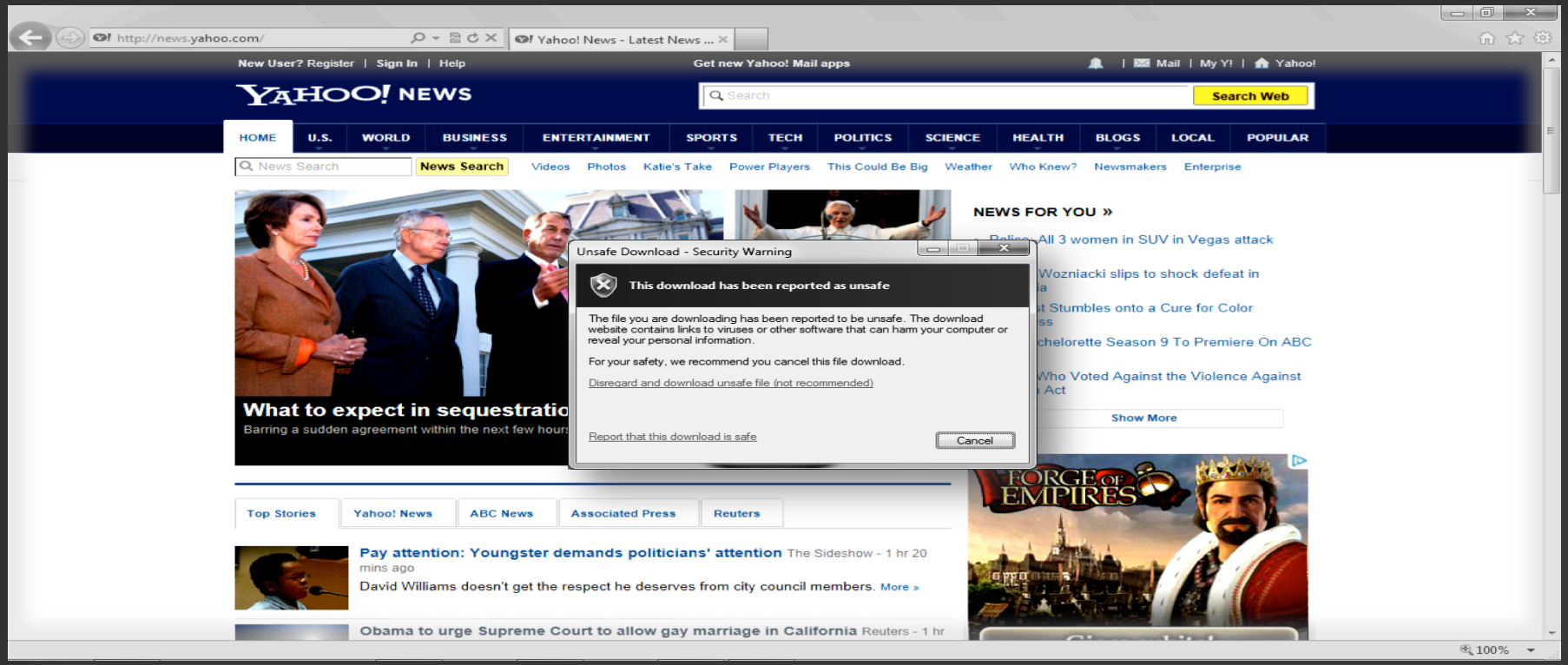
TRUSTED AND RECOGNIZABLE USER INTERFACES TO HELP USERS IN MAKING AWARE CHOICES WHILE SURFING THE WEB


CHROME
IN TRUST

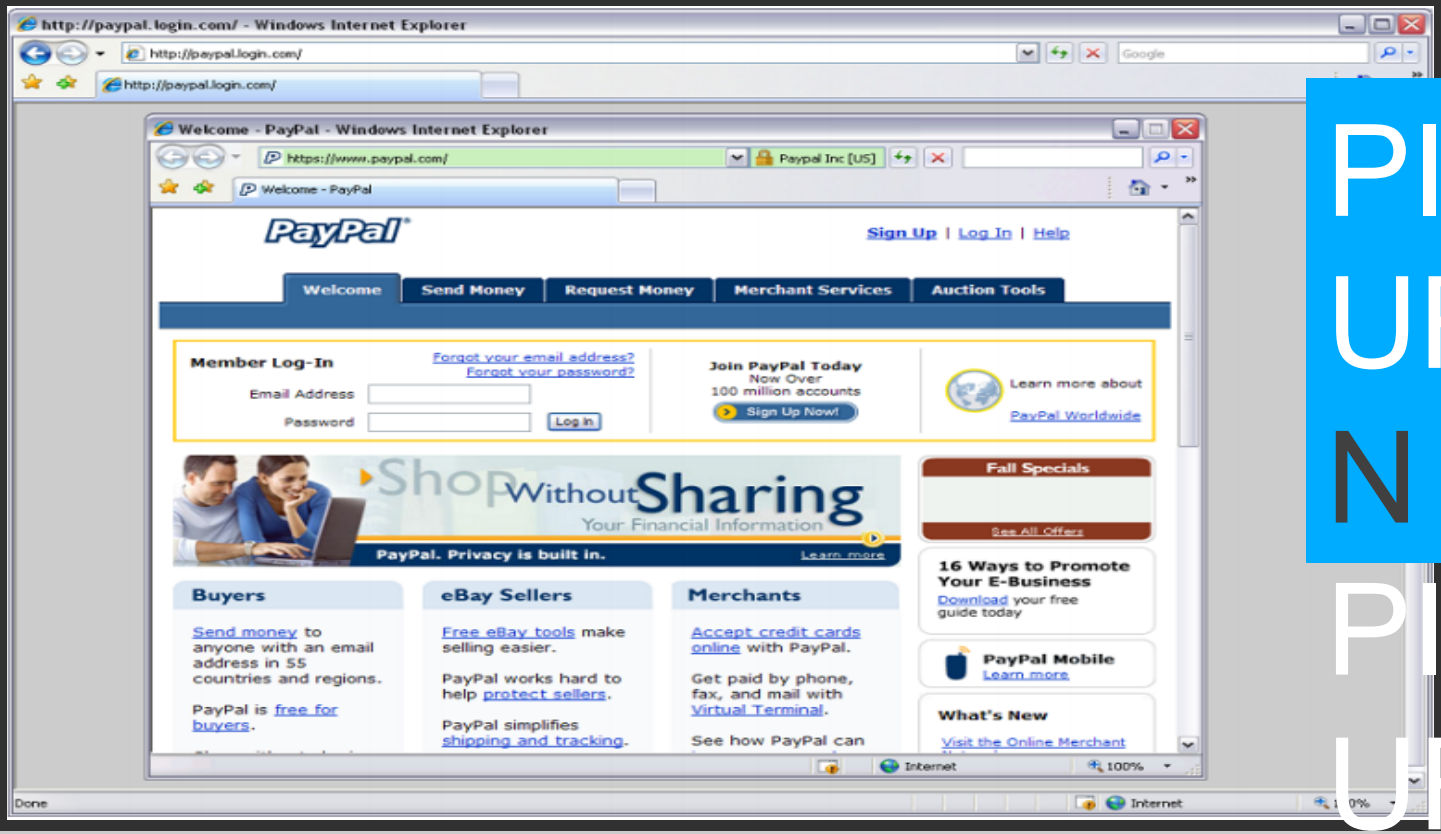
THIS IS CHROME



THIS IS CONTENT

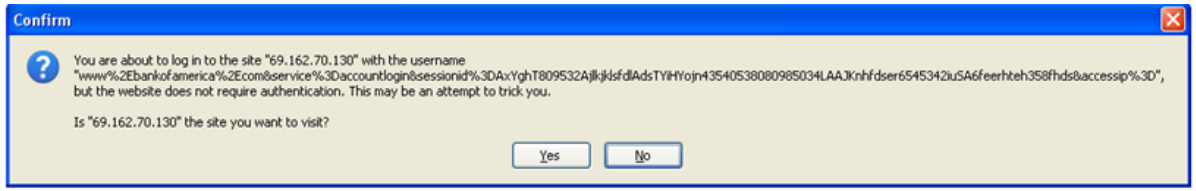


WHICHISCHROME?

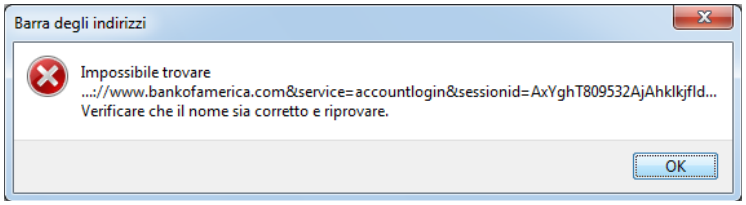


PICT
UREI
N
PICT
URE

URL OBFUSCATION FLAW

- EXPLOIT A DESIGN FLAW IN BROWSERS THAT ARE NOT ABLE TO RELIABLY RENDER THE URL REQUIRED BY THE USER
- URL FORMAT FOLLOWS THE GENERAL PATTERN http://username:password@mysite.com WITH OPTIONAL password FIELD
- 

RAISE A WARNING



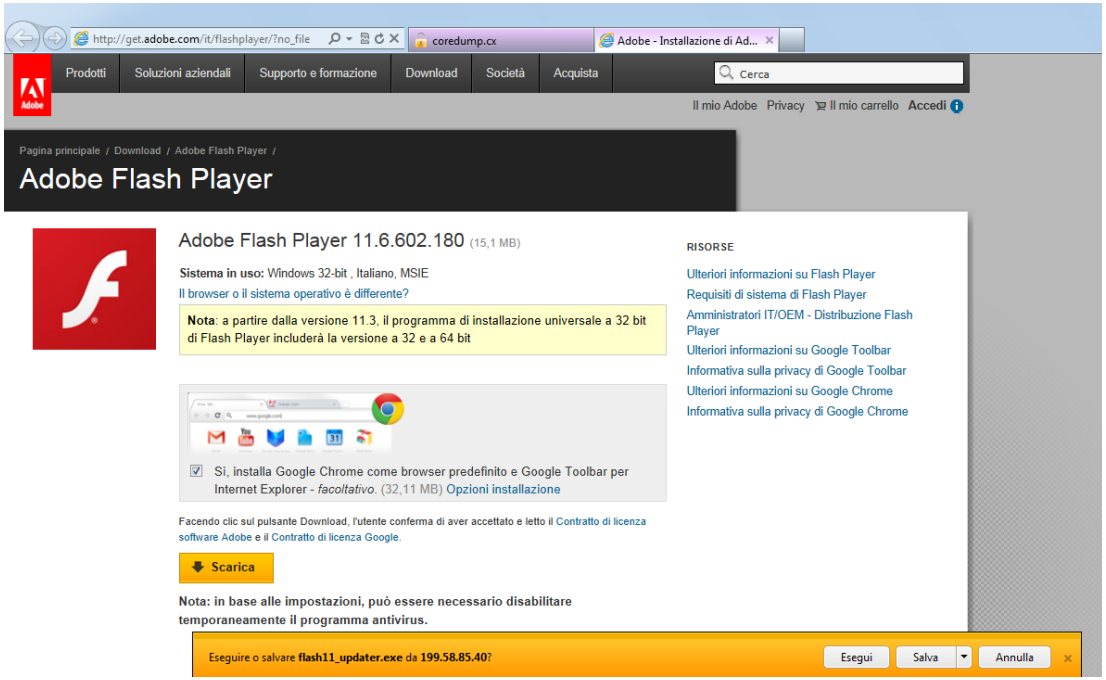
DISABLES RESOLUTION FOR URLS WITH EMBEDDED CREDENTIALS

RENDERS PAGE AND STRIPS CREDENTIALS FROM THE URL AND REVEALING TRUE NATURE OF THE DOMAIN

DOWNLOAD DIA

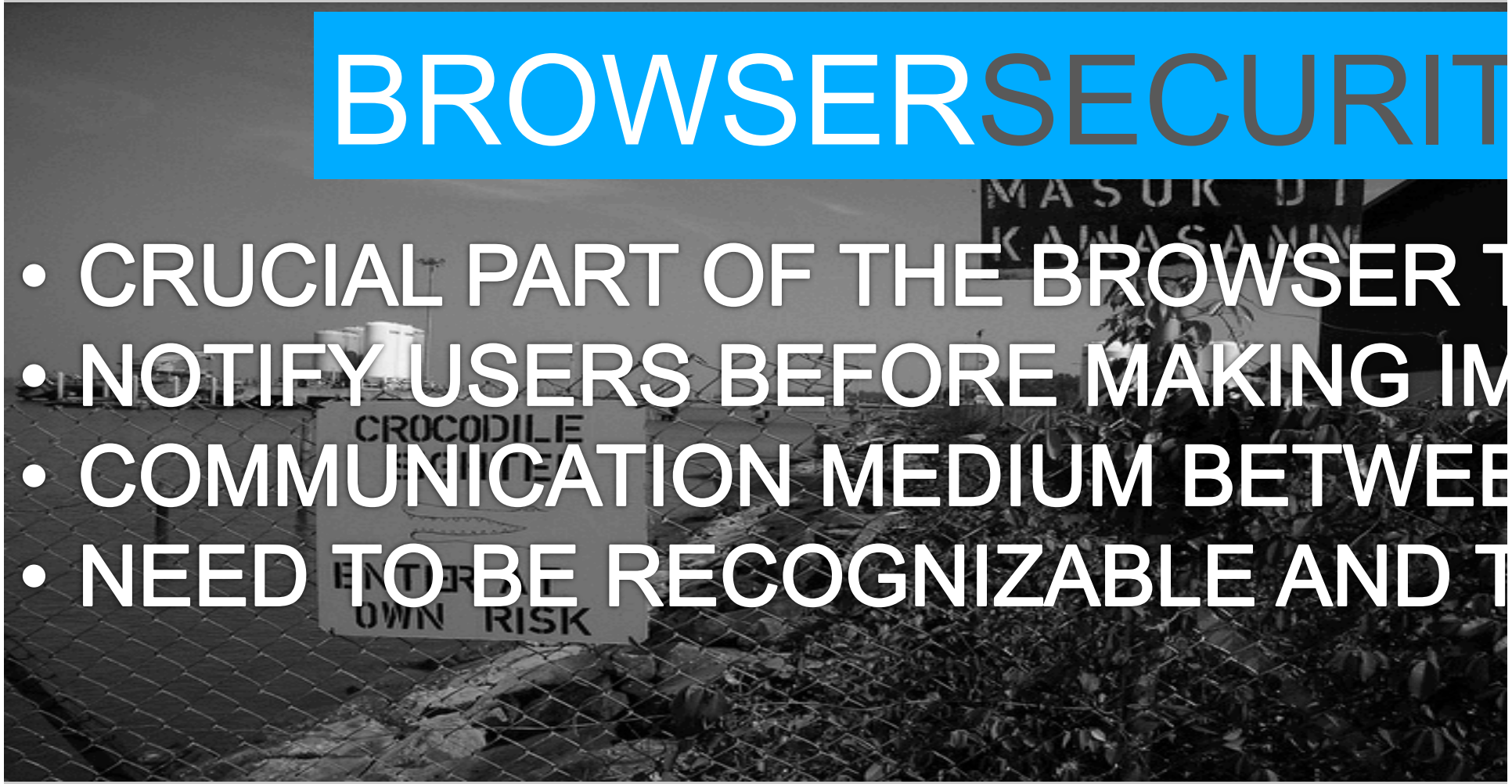
STILL WORKS ON IE9, CHROME 25 AND

- VICTIM VISITS ROGUE WEBSITE
- WEBSITE IMMEDIATELY SPAWNS A NEW NAVIGATION WINDOW LINKING TO A BENIGN WEBPAGE
- ROGUE WEBSITE SETS THE NEW NAVIGATION WINDOW URL TO A RESOURCE SERVED WITH Content-Disposition: attachment HEADER
- A DOWNLOAD NOTIFICATION



http://lcamtuf.coredump.cx/fldl/

BROWSERSECURIT



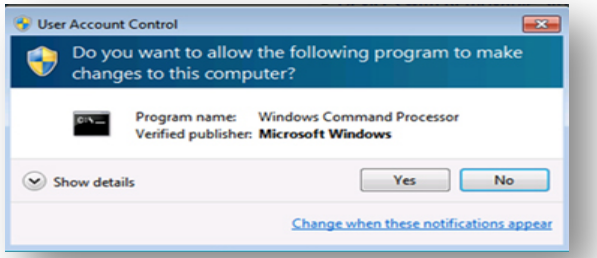
BROWSERSECURIT

- CRUCIAL PART OF THE BROWSER T
- NOTIFY USERS BEFORE MAKING IM
- COMMUNICATION MEDIUM BETWEE
- NEED TO BE RECOGNIZABLE AND T

MODALNOTI

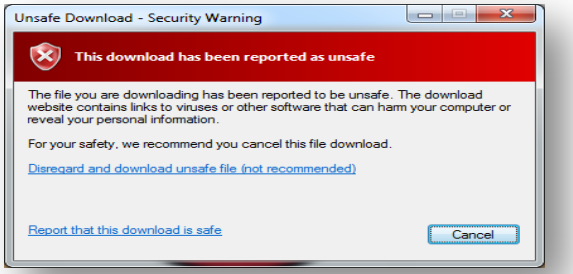
STRONG VISUAL CONTRAST • GRAB USER ATTENTION • BLOCK WORKFLOW

OS GENERATED



- IMPORTANT NOTIFICATIONS ONLY
- NOT STRICTLY PART OF CHROME
- DEFAULT ANSWER

BROWSER GENER



- TRIGGERED IN SEVERAL SCENARIOS
- SOMETIMES CAN BE VERY ANNOYING

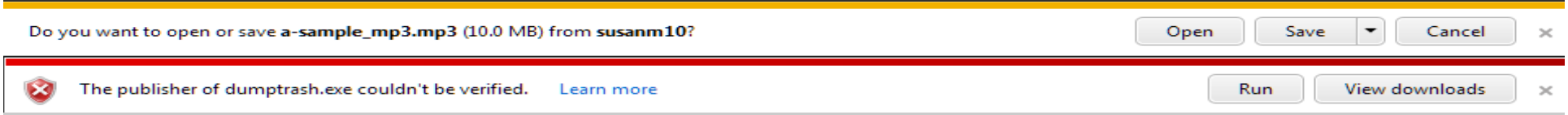
MODELESSNOTIFICATIONS

- DESIGNED TO INFORM USER WITHOUT INTERRUPT
- STAY IN CONTEXT OF THE NAVIGATION WINDOW
- CHROME NOT DOM

FILEDOWNLO

ADING PLUGINSACTI VATION

HTML5APIS



MODALTOMODELESS SHIFT





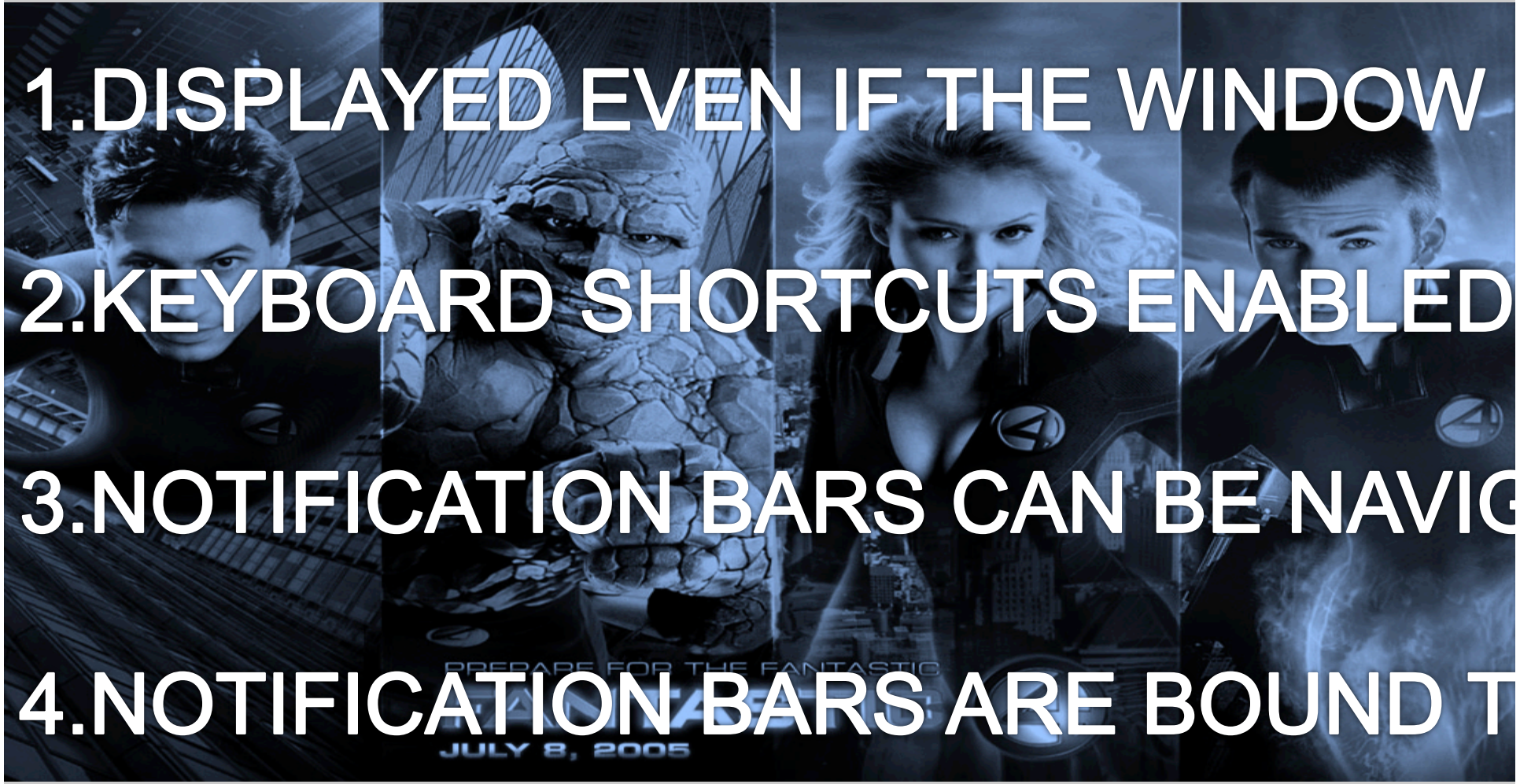
	MODELESS	MODELESS	MODELESS	MIXED	MODAL
	MODELESS	MODELESS	MODELESS	MODAL	MODAL
EXTENSIONS/ADDONS	MODAL	MODAL	MODAL	MODAL	MODAL
	MODELESS	MODELESS	MODELESS	MODELESS	MODAL

4PROBLEMSABOUTMOD

1.DISPLAYED EVEN IF THE WINDOW


1.DISPLAYED EVEN IF THE WINDOW
2.KEYBOARD SHORTCUTS ENABLED
PREPARE FOR THE FANTASTIC
FANTASTIC 4
JULY 8, 2005


1.DISPLAYED EVEN IF THE WINDOW
2.KEYBOARD SHORTCUTS ENABLED
3.NOTIFICATION BARS CAN BE NAVIG
PREPARE FOR THE FANTASTIC
FANTASTIC 4
JULY 8, 2005


1.DISPLAYED EVEN IF THE WINDOW
2.KEYBOARD SHORTCUTS ENABLED
3.NOTIFICATION BARS CAN BE NAVIG
4.NOTIFICATION BARS ARE BOUND T
PREPARE FOR THE FANTASTIC
JULY 8, 2005

NOTIFICATIONSINBACKG

SCENARIO:

1. USER BROWSES ON ATTACKER WE
2. WEB PAGE SPAWNS A POPUP WIND
3. POPUP IS OPENED ON THE BACK
4. ON WINDOWS 7/8 THE POPUNDER I ED

A LITTLE BIT OF JS MAGIC IS REQUIRED FOR THIS TO WORK IN EVERY BROWSER. blur() DOESN'T WORK PROPERLY ON SOME IMPLEMENTATIONS. JSPOPUNDER PROJECT

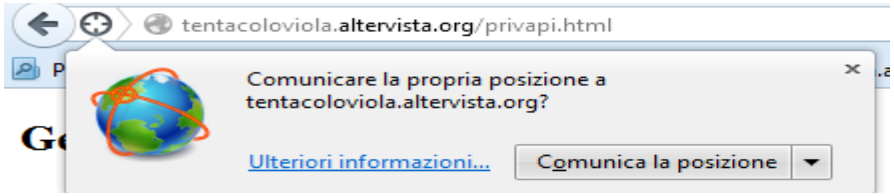
5. POPUNDER INITIATES A DOWNLOAD
6. MODELESS NOTIFICATION IS TRIGGERED (HIDDEN FROM
7. POPUNDER TAB DOESN'T BLINK TO GIVE EVIDENCE OF A

KEYBOARDSHORTCUTS

- ARE AVAILABLE FOR ACTIVATING ACTIONS ON NOTIFICATI
- IE ALLOWS THIS FOR FILE DOWNLOAD NOTIFICATIONS

ALT +R • ALT +S • ALT + O

- IE & FF ALLOW THIS FOR HTML5 API NOTIFICATIONS



ALT + O

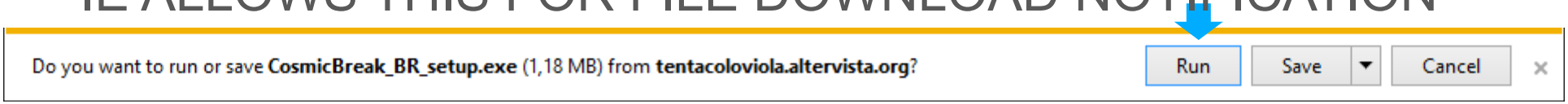
ALT +A • ALT + O

- NAVIGATION WINDOW NEEDS TO BE FOCUSED FOR USIN

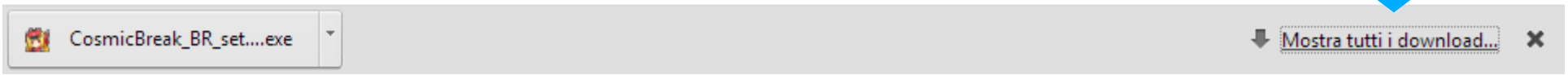
USINGTABINNOTIFICATIC

SOME BROWSERS ALLOW USING TAB KEY TO NAVIG

- IE ALLOWS THIS FOR FILE DOWNLOAD NOTIFICATION



- CHROME SKIPS THE FILE OPENING BUTTON

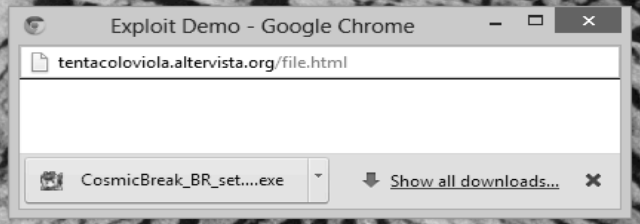


NOTIFICATION BAR IS PART OF CHROME: NO NAVIGATION US

BOUNDTONAVIGATIONW

AS THEY ARE BUILT IN CHROME, NOTIFICATION BARS CAN BE:

- MOVED AROUND THE SCREEN ALONG WITH THE NAVIGATION WINDOW
- RESIZED ALONG WITH THE NAVIGATION WINDOW
- CLOSED TOGHETER WITH THE NAVIGATION WINDOW
- ALSO BOUND TO ORIGINATING



ATTACKSCENA

Windows 7 Windows 8 9 -10

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW
3. ON WINDOWS 7/8 THE POPUNDER IS MERELY UNNOTICED
4. POPUNDER INITIATES A DOWNLOAD OF A .EXE FILE
5. MODELESS NOTIFICATION IS TRIGGERED (HIDDEN FROM USER VIEW)
6. POPUNDER TAB DOESN'T BLINK TO GIVE EVIDENCE OF A PENDING NOTIFICATION
7. AFTER NOTIFICATION IS READY, POPUNDER IS STILL IN BACKGROUND BUT HAS THE FOCUS!

ATTACKSCENARIO

- IN IE9 OPENING POPUNDER WINDOW USING:

```
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" />
```

WILL BRING THE FOCUS OF THE POPUNDER DIRECTLY ON THE NOTIFICATION BAR

- THIS MEANS YOU CAN TRIGGER CODE EXECUTION BY JUST TYPING A KEY:
  - R key (key changes according to OS language)
  - SPACE key
  - ENTER key

LIMITATIONSFORATTACK

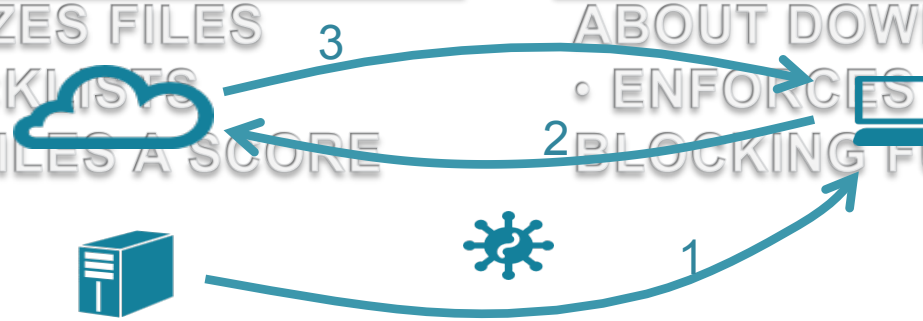
MALICIOUSDOWNLOADF

BLOCKING ACCESS TO MALICIOUS URLS&FILES BEF

FUNCTIONAL COMPONENTS:

- A CLOUD REPUTATION-BASED SYSTEM
- SCOURS THE WEB FOR MALWARE
- CATEGORIZES FILES USING BLACKLISTS
- ASSIGNS FILES A SCORE

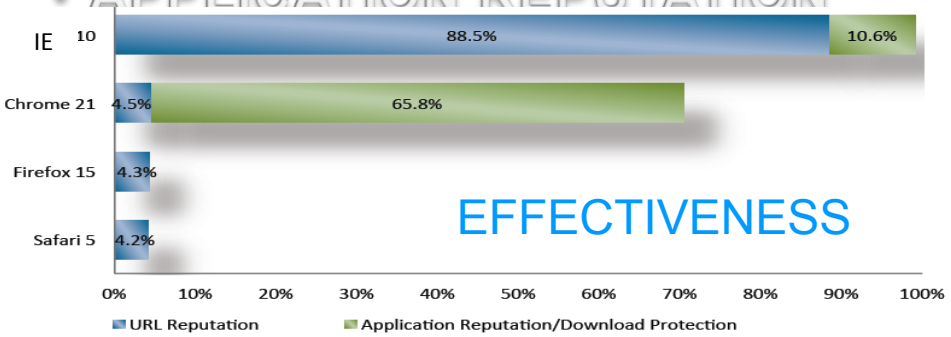
- A BROWSER AGENT
- REQUESTS INFORMATIONS FROM THE CLOUD
- PROVIDES FEEDBACKS ABOUT DOWNLOADED FILES
- ENFORCES WARNING/ BLOCKING FUNCTIONS



IMPLEMENTATIONS

SAFEBROWSING

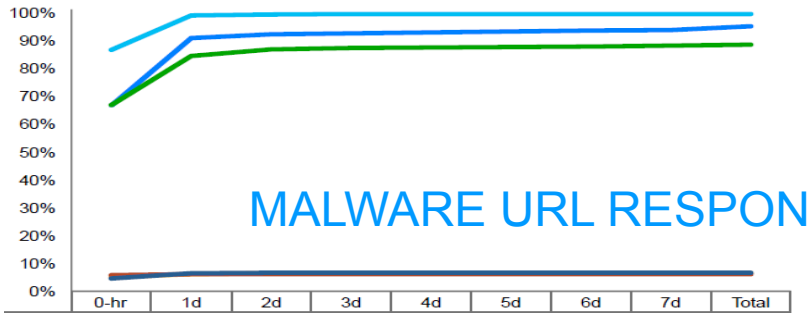
- BASED ON GOOGLE SAFEBROWSING API V.2
- SUPPORTS URL REPUTATION
- APPLICATION REPUTATION



EFFECTIVENESS

SMARTSCREENFILT

- INTRODUCED IN IE8
- SUPPORTS APP REPUTATION SINCE IE9
- SYSTEM WIDE EXTENSION



MALWARE URL RESPONSE T

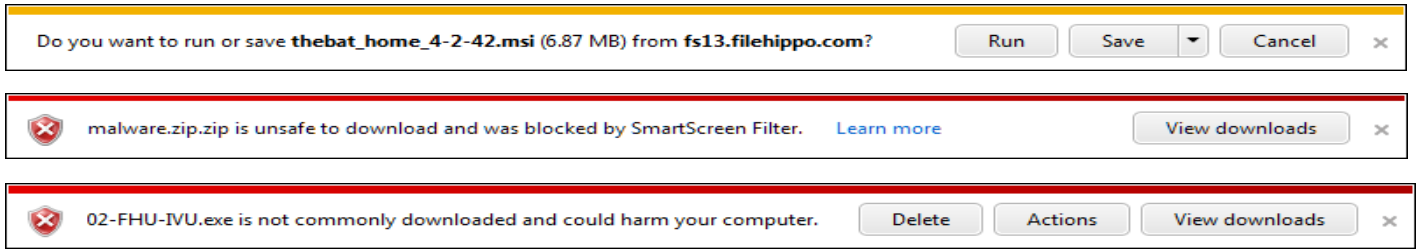
CHARTS FROM NSS LABS REPORT 2012

SMARTSCREENFILTER

INPUT: IP • URL • FILE HASH (SHA256)
FILENAME (BASE64)
• SIGNING CERTIFICATE (if available)

```
<App>
  <FName>U2FtZUdhbWUuZXhl</FName>
  <FHash>d3ff5939726c9f8fa6e514fb65eb470
         a1f9ec7a65b2706732a03749226c25
         20</FHash>
  <Sig>0</Sig>
  <Sz>45056</Sz>
  <M>1</M>
  <SR>100</SR>
</App>
```

OUTPUT:



← SUCCEDED
← BLACKLISTED
← REPUTATION FAILURE

BAR COLOR CHANGES ACCORDING TO THE SIGNING CERTIFICATE + CHECK RESULT

(NOTSO)SMARTSCREEN

REPUTATION CHECK IS NOT 100% RELIABLE
MORE THAN 20% SAMPLES ON http://minotauranalysis.com/exetweet/default.aspx WILL PASS THROUGH

BUY AN EV CERTIFICATE AND GAIN REPUTATION.

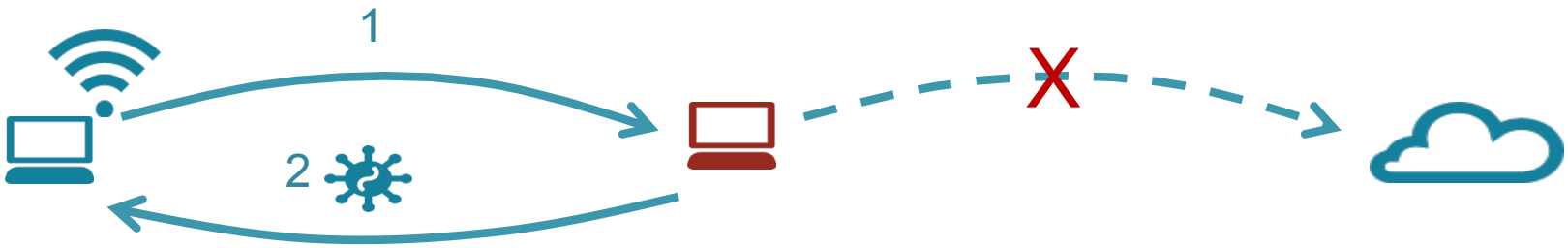
NEWLY PUBLISHED EXECUTABLES SIGNED WITH AN EV CERTIFICATE WILL IMMEDIATELY ESTABLISH A GOOD REPUTATION EVEN IF NO PRIOR REPUTATION EXISTS

RESPONSE TIME FOR CATCHING NEW EXECUTABLE SAMPLES ALLOWS FOR EASY BYPASS IN THE FIRST PUBLISHING DAYS

INTERNET CONNECTION NEEDED FOR PERFORMING THE CHECK (more on this later…)

ATTACKSCENARIO#1ONS

MITM SCENARIO



1. ATTACKER SETS UP A FREE ACCESS
2. BLOCKS COMMUNICATIONS TO SMA
3. RESULT IS:

4. TRICK VICTIM TO TYPE “R”/ ”Enter” /
5. ARBITRARY CODE EXECUTION!

USERACCESS 

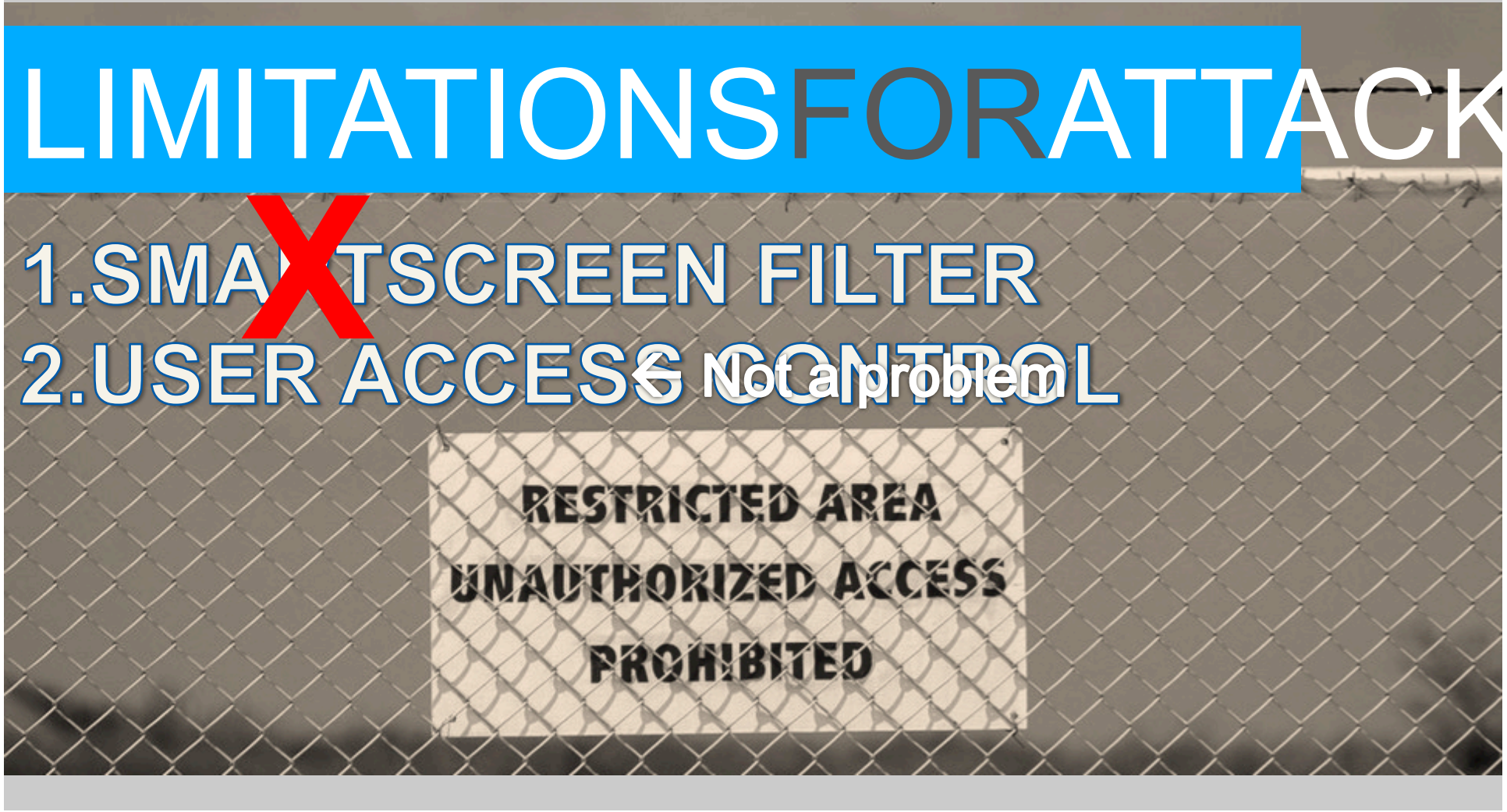
OL

ONLY TRIGGERED WHEN ADMINITRATIVE PRIVILEGE

YOU CANNOT BYPASS THAT. FULL STOP.

DO YOU REALLY NEED THAT FOR CAUSING SERIOU

LIMITATIONSFORATTACK



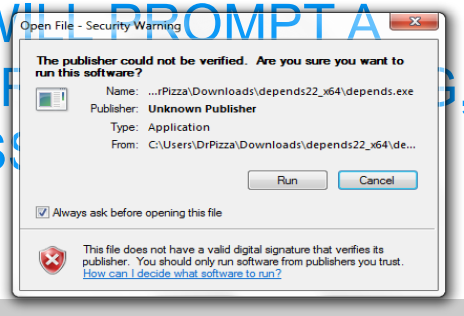
ATTACKSCENARIO#2 TIMING/POSITIONATTA

DYNAMIC WINDOW OVERLAY

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW AT SOME GIVEN COORDINATES
3. POPUNDER INITIATES A DOWNLOAD OF A .EXE FILE
4. MODELESS NOTIFICATION IS TRIGGERED (HIDDEN FROM USER VIEW)
5. POPUNDER TAB DOESN'T BLINK TO GIVE EVIDENCE OF A PENDING NOTIFICATION
6. ATTACKER TRICKS VICTIM TO CLICK ON A GIVEN LINK/ BUTTON
7. PAGE IS LISTENING ON MOUSE MOVES
8. AS SOON AS THE MOUSE IS HOVERING ON THE BUTTON

ATTACKSCENARIO#2.REL

- EVERY TIME A FILE IS DOWNLOADED FROM THE WEB THE OS ADDS A ZONE INFORMATION FILE TO THE DISK
- ZONE INFORMATION FILE IS WRITTEN IN AN ASD (alternate data stream)
- IT CONTAINS A REFERENCE TO THE SECURITY ZONE THE FILE WAS DOWNLOADED FROM (e.g. INTERNET)
- LAUNCHING AN UNKNOWN .EXE FILE DOWNLOADED FROM THE WEB WILL PROMPT A CONFIRMATION DIALOG, NOT BYPASSABLE



- A SMARTSCREEN CHECK IS PERFORMED (BUT YOU ALREADY KNOW HOW TO BYPASS IT)
- NO FURTHER DIALOGS ARE DISPLAYED
- CODE EXECUTION!

ATTACKSCENARIO#2.b

DYNAMIC WINDOW OVERLAY

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW AT SOME GIVEN COORDINATES
3. POPUNDER LOADS A WEBPAGE REQUIRING SOME PRIVILEGES (e.g. YOUR POSITION)
4. MODELESS NOTIFICATION IS SHOWN (HIDDEN FROM USER VIEW)
5. POPUNDER TAB DOESN'T BLINK TO GIVE EVIDENCE OF A PENDING NOTIFICATION
6. ATTACKER TRICKS VICTIM TO CLICK ON A GIVEN LINK/ BUTTON
7. PAGE IS LISTENING ON MOUSE MOVES

ATTACKSCENARIO#2.5

DYNAMIC WINDOW OVERLAY

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUNDER WINDOW AT SOME GIVEN COORDINATES
3. POPUNDER LOADS A WEBPAGE SERVED WITH X-FRAME-OPTIONS (e.g. TWITTER)
4. ATTACKER TRICKS VICTIM TO CLICK ON A GIVEN LINK/ BUTTON
5. PAGE IS LISTENING ON MOUSE MOVES
6. AS SOON AS THE MOUSE IS HOVERING ON THE BUTTON, WINDOW IS CLOSED
7. IF TIMING IS APPROPRIATE THERE GOOD CHANCES THE VICTIM CLICKS ON THE UNDERLYING POPUNDER

SOME PROPOSALS

1. NOTIFICATIONS ON BACKGROUND WINDOWS ARE USELESS (AT BEST). LET THE NOTIFICATION POPS-UP AFTER SOME SECONDS SINCE THE WINDOW HAS REGAINED FOCUS

2. DISABLE TAB KEY IN THE NOTIFICATION BAR, JUST USE THE MOUSE. IF YOU ARE CONCERNED ABOUT ACCESSIBILITY ENABLE COMPLEX KEYBOARD SHORTCUTS IN ORDER TO LIMIT THE CHANCE OF BEING SOCIAL ENGINEREED

3. SOME SENSITIVE NOTIFICATIONS (E.G. FILE DOWNLOADING) SHOULD BE EVER KEPT IN A STATIC FRAME OF THE CHROME, NOT BOUND TO NAVIGATION WINDOW

CONCLU

1. THE BROWSERS SHIFT FROM MODAL TO MODELESS NOTIFICATIONS IS STILL NOT MATURE

2. IMPLEMENTATIONS ARE NOT SECURE ENOUGH TO PROTECT USERS SAFETY: AL LEAST TWO TECHNIQUES ALLOW FOR STEALTH REMOTE CODE EXECUTION

valotta.rosario@gmail.com @tentacolo_Viola sites.google.com/site/tentacol