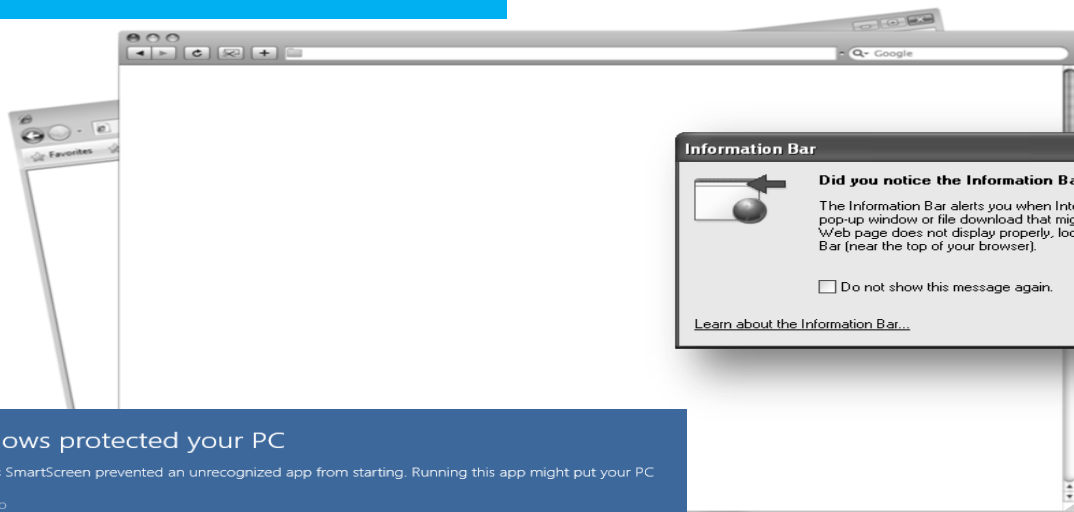


ABUSING BROWSER USER INTERFACES

FOR FUN & PROFIT



Windows protected your PC

Windows SmartScreen prevented an unrecognized app from starting. Running this app might put your PC at risk.
[More info](#)

OK

HELLO

MY NAME IS

Rosario



sites.google.com/site/tentacoloviola/

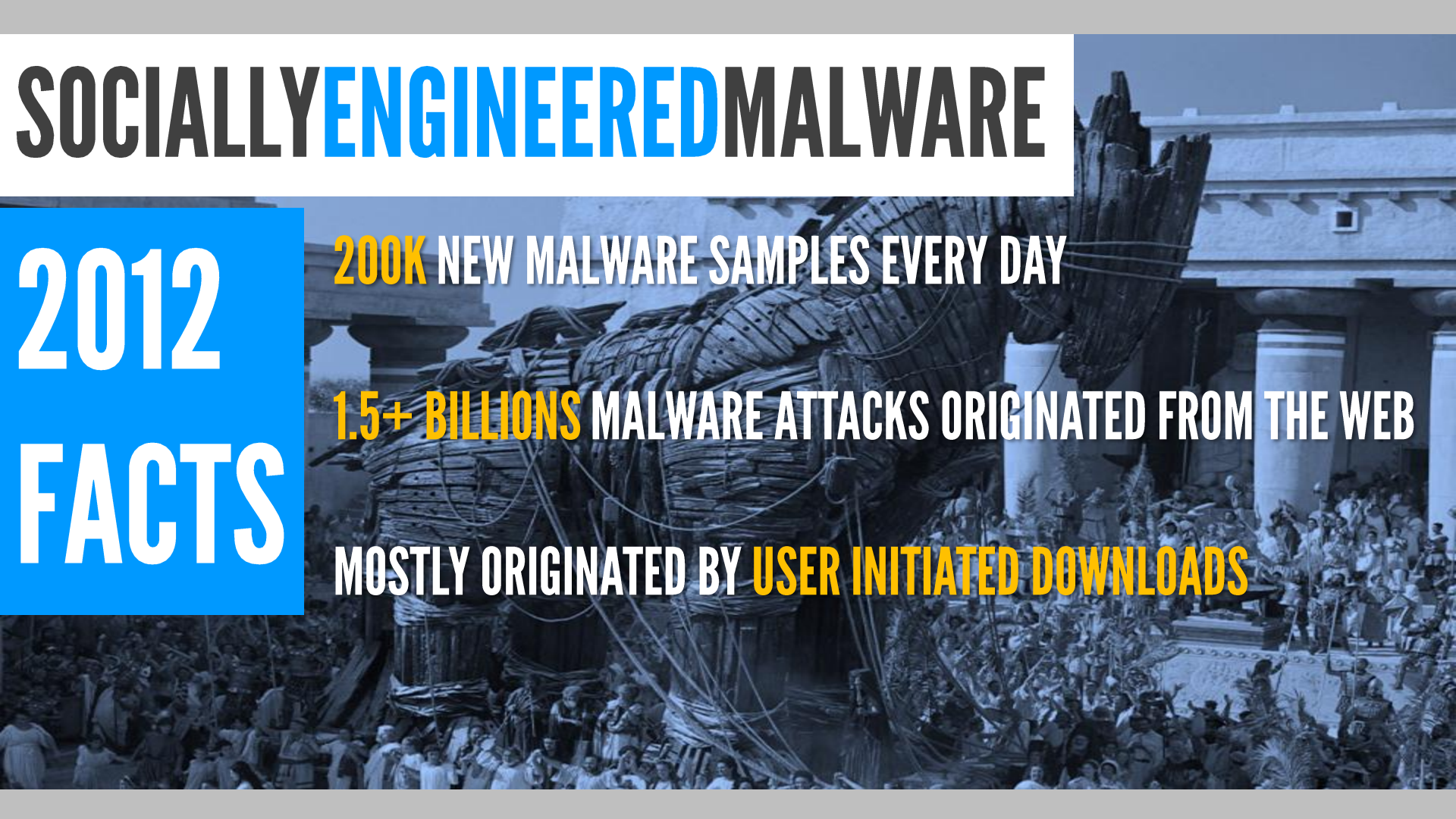
SOCIALLYENGINEEREDMALWARE

2012
FACTS

200K NEW MALWARE SAMPLES EVERY DAY

1.5+ BILLIONS MALWARE ATTACKS ORIGINATED FROM THE WEB

MOSTLY ORIGINATED BY USER INITIATED DOWNLOADS



USERS**ASK**FOR

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



VENDORSREPLIES

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

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

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

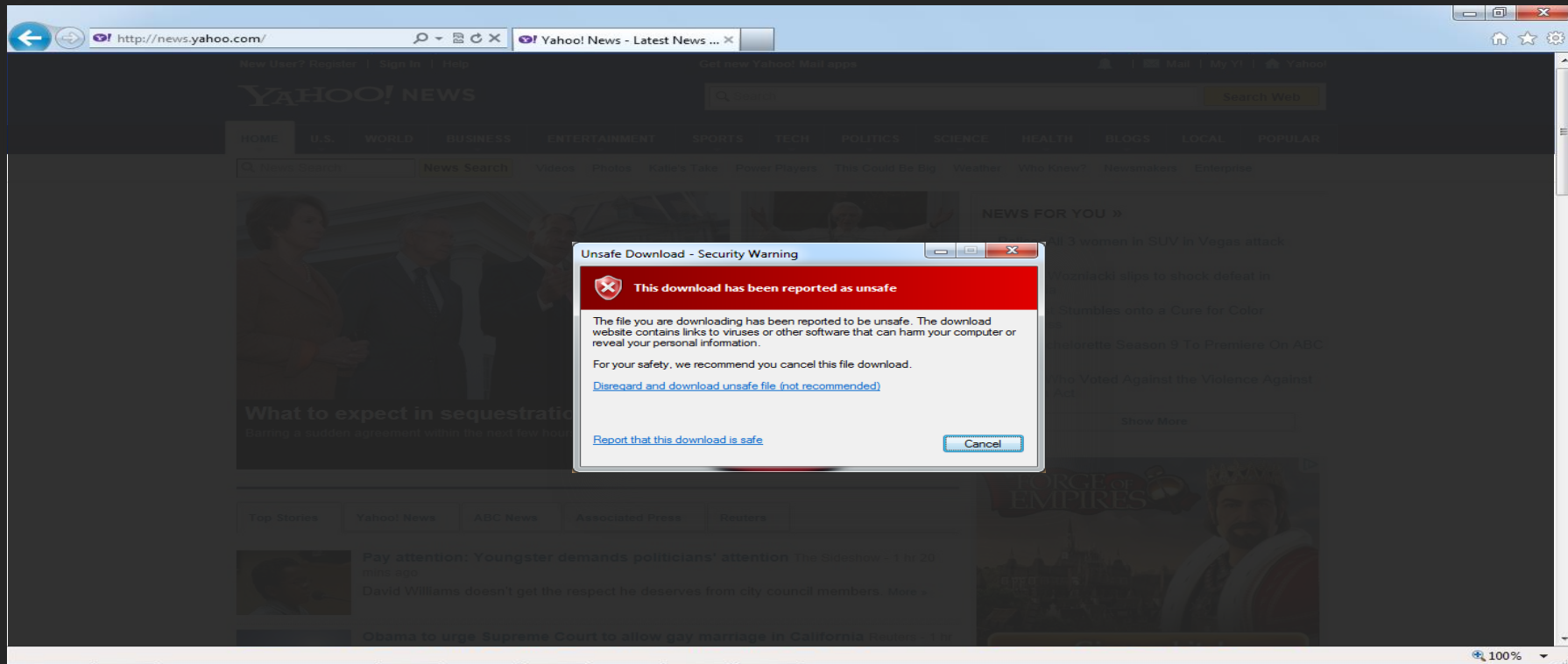
**TRUSTED AND RECOGNIZABLE USER INTERFACES TO
HELP USERS IN MAKING AWARE CHOICES WHILE
SURFING THE WEB**



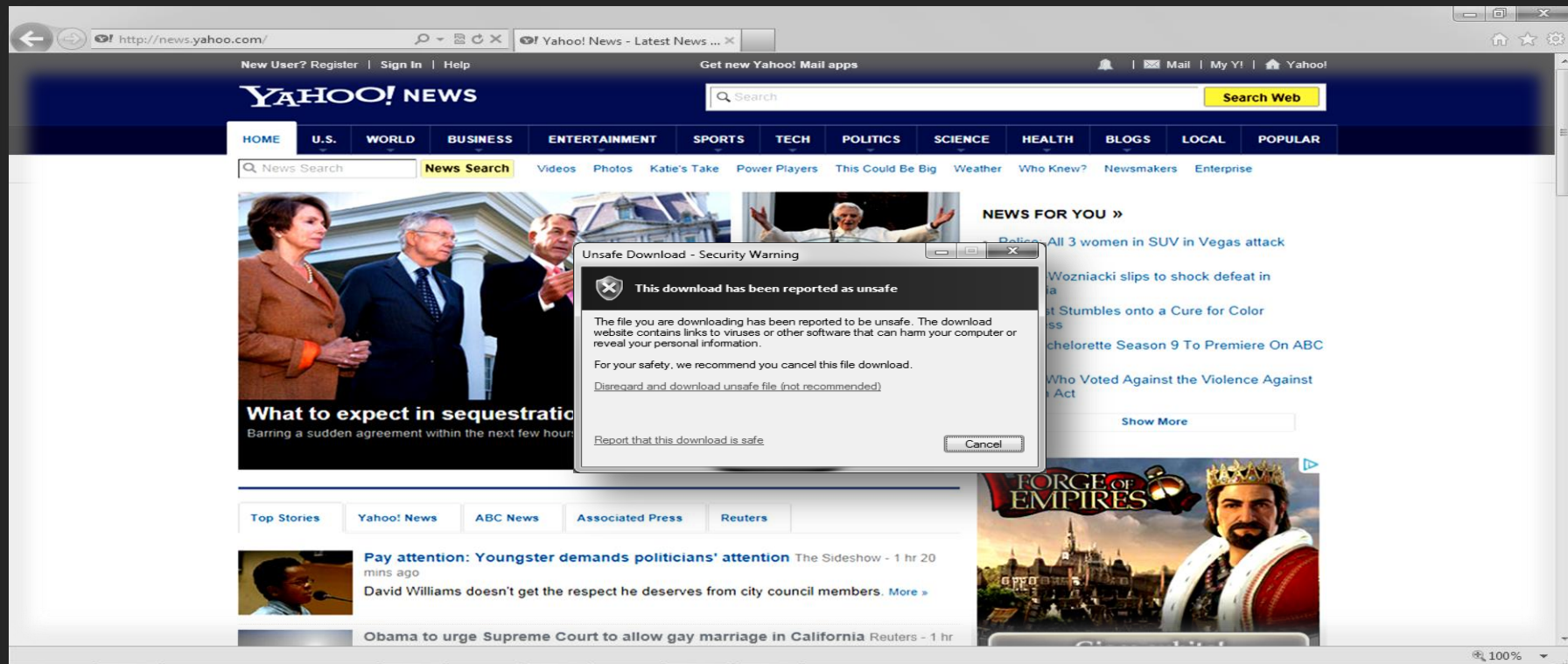
CHROME

IN TRUST WE

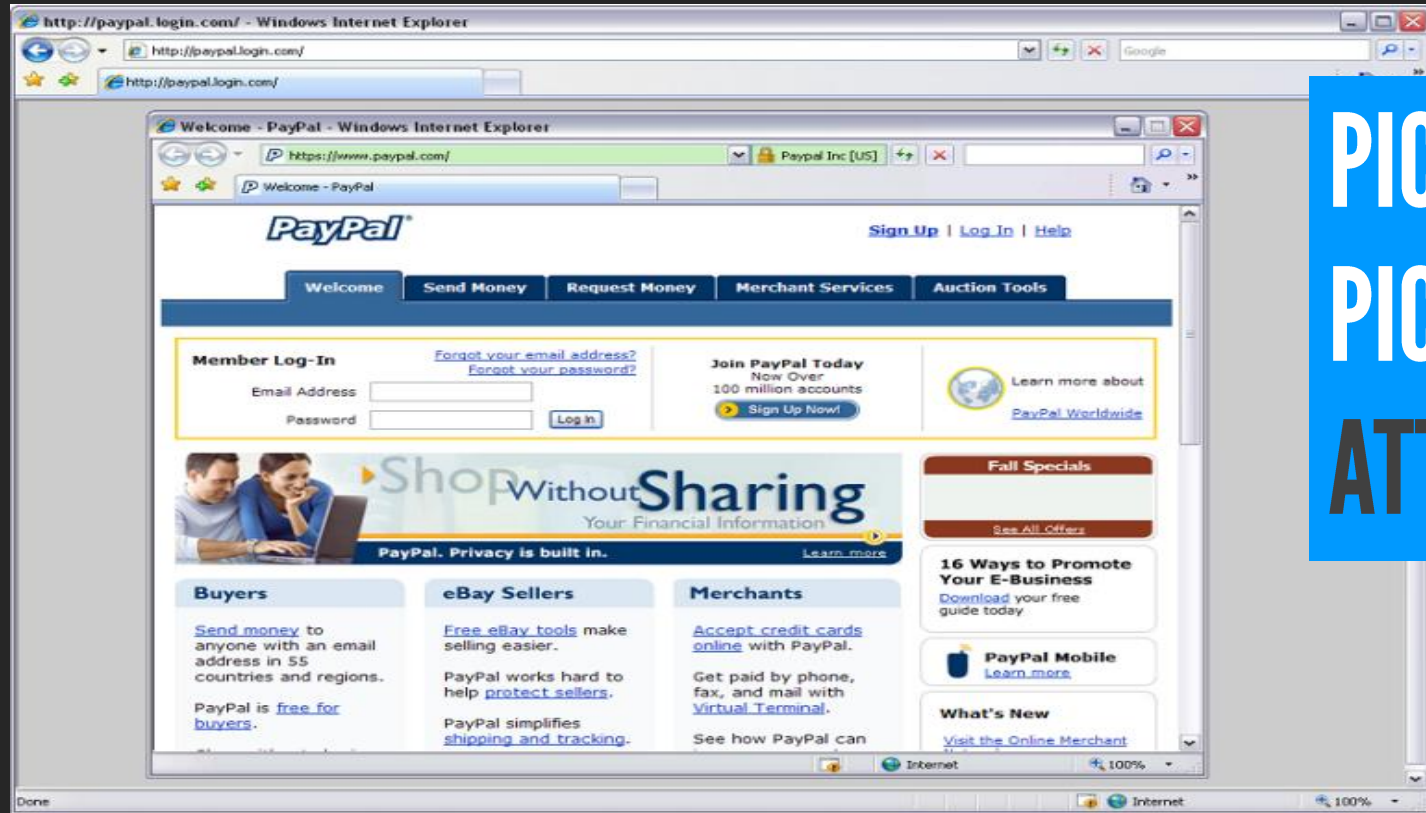
THIS IS CHROME



THIS IS CONTENT



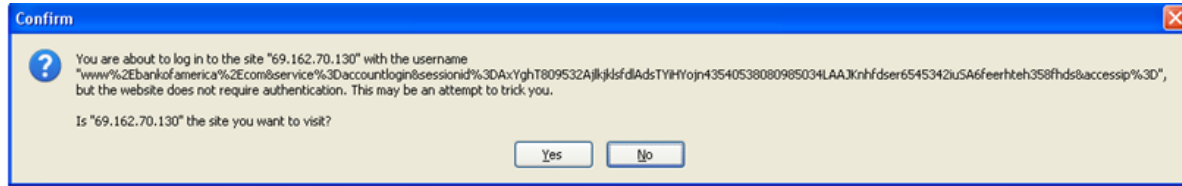
WHICH IS CHROME?



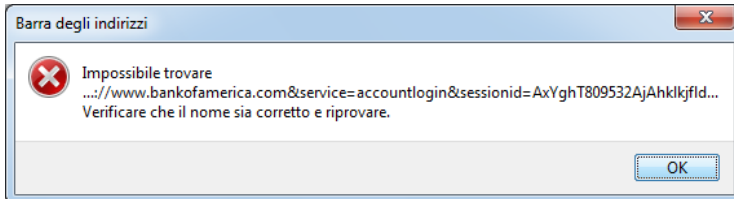
PICTURE IN
PICTURE
ATTACK

URL OBFUSCATION FLAWS

- **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
- `http://www.bankofamerica.com&service=...@174.120.41.176/~inferno/exploits/obfusurl/index.htm`



RAISE A WARNING



DISABLES RESOLUTION FOR URLS WITH EMBEDDED CREDENTIALS

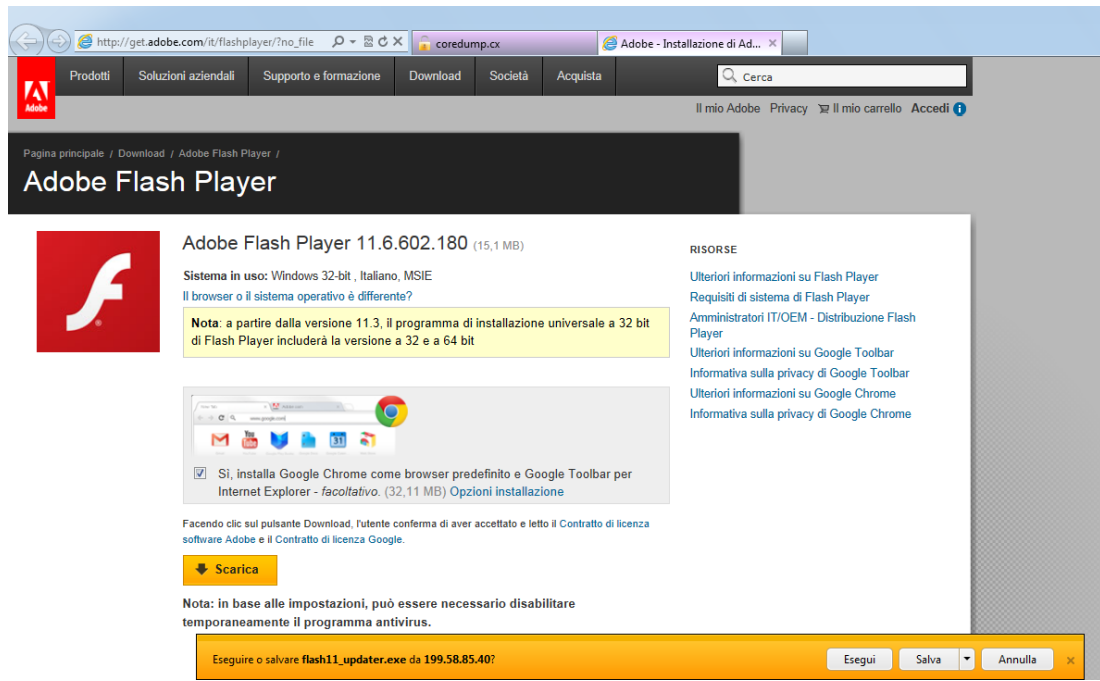


RENDERS PAGE AND STRIPS CREDENTIALS FROM THE URL AND REVEALING TRUE NATURE OF THE DOMAIN

DOWNLOAD DIALOG SPOOFING

STILL WORKS ON IE9, CHROME 25 AND
FIREFOX 19!

- 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 BAR/DIALOG APPEARS IN THE CONTEXT OF THE NEW NAVIGATION WINDOW
- VICTIM IS TRICKED TO BELIEVE DOWNLOAD HAS BEEN ORIGINATED FROM THE BENIGN WEBSITE



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

BROWSER SECURITY NOTIFICATIONS

- CRUCIAL PART OF THE BROWSER TRUST MODEL
- NOTIFY USERS BEFORE MAKING IMPORTANT CHOICES
- COMMUNICATION MEDIUM BETWEEN USERS AND BROWSERS
- NEED TO BE RECOGNIZABLE AND TRUSTED

MODAL NOTIFICATIONS

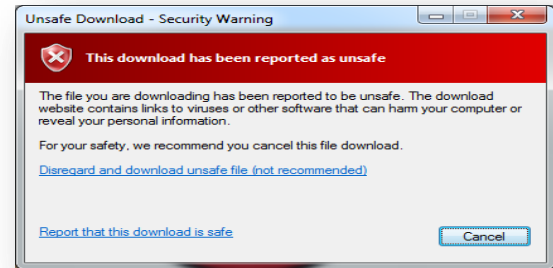
STRONG VISUAL CONTRAST • GRAB USER ATTENTION • BLOCK WORKFLOW

OS GENERATED



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

BROWSER GENERATED



- TRIGGERED IN SEVERAL SCENARIOS
- SOMETIMES CAN BE VERY ANNOYING
- DEFAULT ANSWER PROBLEM

MODELESSNOTIFICATIONS

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



FILE**DOWNLOADING**



HTML5APIS



PLUGINSACTIVATION

Do you want to open or save **a-sample_mp3.mp3** (10.0 MB) from **susanm10?**

Open

Save



Cancel



The publisher of **dumptrash.exe** couldn't be verified.

[Learn more](#)

Run

View downloads



MODAL TO MODELESS SHIFT



MODELESS

MODELESS

MODELESS

MIXED

MODAL



MODELESS

MODELESS

MODELESS

MODAL

MODAL



MODAL

MODAL

MODAL

MODAL

MODAL



MODELESS

MODELESS

MODELESS

MODELESS

MODAL



4PROBLEMSABOUTMODELESSNOTIFICATIONS

A movie poster for X-Men: The Movie, featuring four characters in a blue-tinted, high-contrast style. From left to right: Cyclops, the Beast, Jean Grey, and Wolverine. The background shows a cityscape with a bridge. The text is overlaid in large, white, bold, sans-serif font.

1. DISPLAYED EVEN IF THE WINDOW IS IN BACKGROUND

2. KEYBOARD SHORTCUTS ENABLED FOR NOTIFICATION BARS

3. NOTIFICATION BARS CAN BE NAVIGATED USING TAB KEY

4. NOTIFICATION BARS ARE BOUND TO THE NAVIGATION WINDOW

PREPARE FOR THE FUTURE
JULY 8, 2005

NOTIFICATIONS IN BACKGROUND WINDOWS

SCENARIO:

1. USER BROWSES ON ATTACKER WEBSITE
2. WEB PAGE SPAWNS A POPUP WINDOW
3. POPUP IS OPENED ON THE BACKGROUND (POPUNDER)
4. ON WINDOWS 7/8 THE POPUNDER IS MERELY UNNOTICED



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

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 ENABLES POPUNDERS IN CROSS BROWSER ENVIRONMENTS.

KEYBOARD SHORTCUTS

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

Do you want to run or save **thebat_home_4-2-42.msi** (6.87 MB) from **fs13.filehippo.com**?

Run

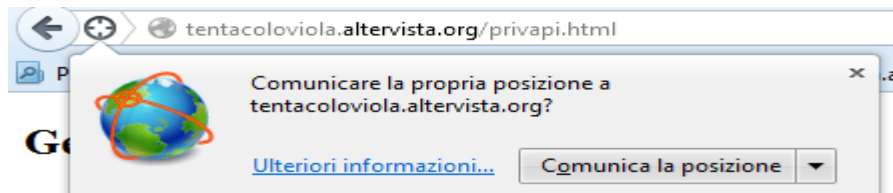
Save

Cancel

×

ALT + R • ALT + S • ALT + O

- IE & FF ALLOW THIS FOR HTML5 API NOTIFICATIONS



ALT + O

ALT + A • ALT + O

tentacoloviola.altervista.org wants to track your physical location.

Allow once

Options for this site

×

- NAVIGATION WINDOW NEEDS TO BE **FOCUSED** FOR USING SHORTCUTS

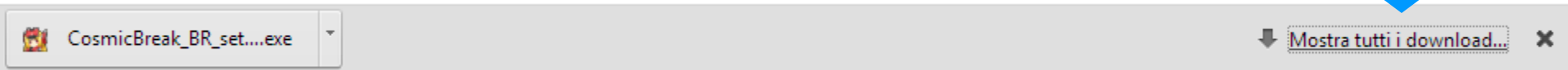
USING TAB IN NOTIFICATION BARS

SOME BROWSERS ALLOW USING TAB KEY TO NAVIGATE ON NOTIFICATION BARS

- IE ALLOWS THIS FOR FILE DOWNLOAD NOTIFICATION



- CHROME SKIPS THE FILE OPENING BUTTON

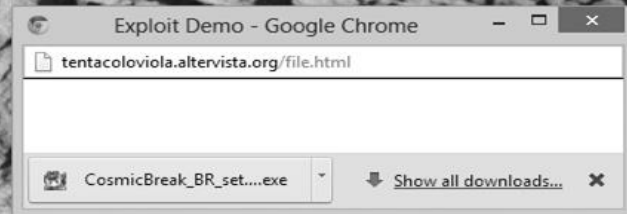


NOTIFICATION BAR IS PART OF CHROME: NO NAVIGATION USING DOM EVENTS IS ALLOWED

BOUND TO NAVIGATION WINDOW

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 TOGETHER WITH THE NAVIGATION WINDOW
- ALSO BOUND TO ORIGINATING DOMAIN



Windows 8 Pro
Build 9200

22:51
03/03/2013

ATTACKSCENARIO#1



Windows 8



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!
8. EVERY KEYBOARD INPUT WILL BE DIRECTED TO THE POPUNDER...
9. USER ENTERS "TAB" + "R" or "SPACE" or "ENTER"
10. CODE EXECUTION WITHOUT ANY NOTIFICATION OR USER CONFIRMATION

ATTACKSCENARIO#1 - BONUS



- 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

LIMITATIONS FOR ATTACK #1

1. SMARTSCREEN FILTER
2. USER ACCESS CONTROL

**RESTRICTED AREA
UNAUTHORIZED ACCESS
PROHIBITED**

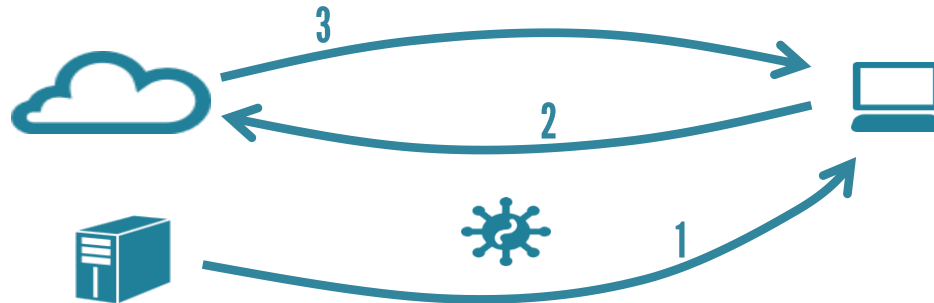
MALICIOUS DOWNLOAD PROTECTIONS

BLOCKING ACCESS TO MALICIOUS URL&FILES BEFORE LOADING THE CONTENT

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

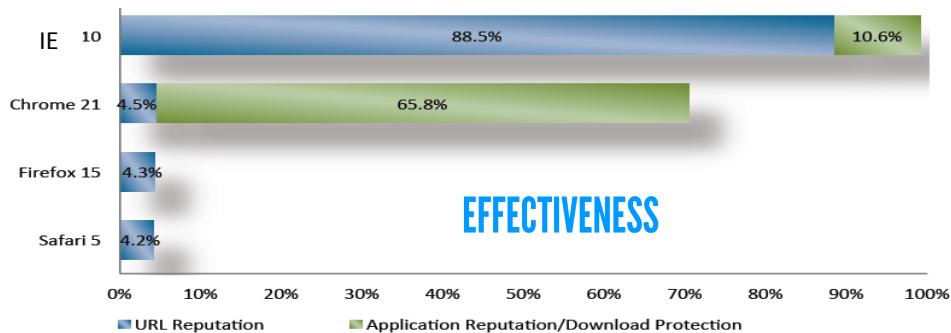


IMPLEMENTATIONS

SAFEBROWSING



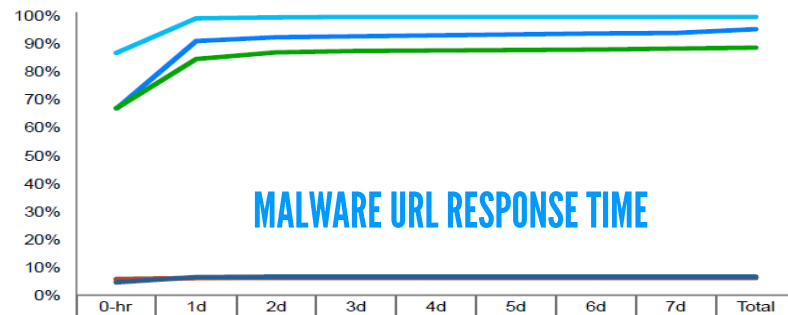
- BASED ON GOOGLE SAFEBROWSING API V.2
- SUPPORTS URL REPUTATION
- APPLICATION REPUTATION (CHROME ONLY)



SMARTSCREENFILTER



- INTRODUCED IN IE8
- SUPPORTS APP REPUTATION SINCE IE9
- SYSTEM WIDE EXTENSION IN WINDOWS 8



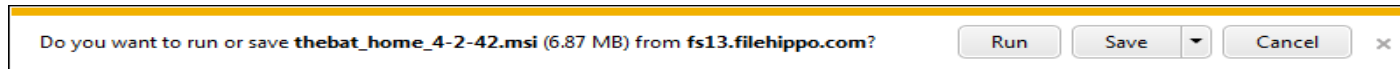
CHARTS FROM NSS LABS REPORT 2012

SMARTSCREENFILTER

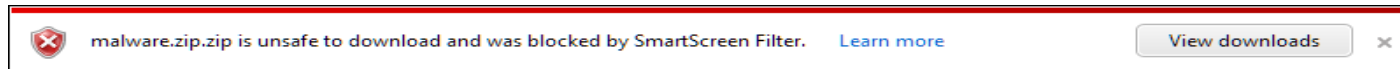
INPUT: IP • URL • FILE HASH (SHA256) • FILENAME (BASE64) →
• SIGNING CERTIFICATE (if available)

```
<App>
  <FName>U2FtZUdhbWUuZXh1</FName>
  <FHash>d3ff5939726c9f8fa6e514fb65eb470
    a1f9ec7a65b2706732a03749226c25
    20</FHash>
  <Sig>0</Sig>
  <Sz>45056</Sz>
  <M>1</M>
  <SR>100</SR>
</App>
```

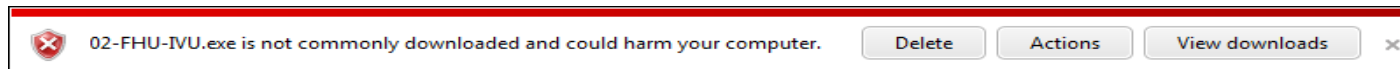
OUTPUT:



← SUCCEEDED



← BLACKLISTED



← REPUTATION FAILURE

BAR COLOR CHANGES ACCORDING TO THE **SIGNING CERTIFICATE** + CHECK RESULT

(NOTSO)SMARTSCREENFILTER

REPUTATION CHECK IS NOT 100% RELIABLE
MORE THAN 20% SAMPLES ON

<http://minotauranalysis.com/exetweet/default.aspx> WILL
PASS THROUGH

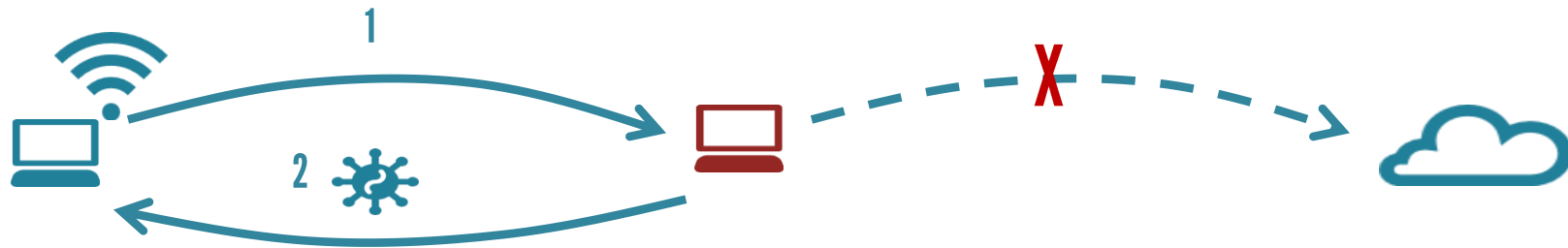
RESPONSE TIME FOR CATCHING NEW EXECUTABLE
SAMPLES ALLOWS FOR EASY BYPASS IN THE FIRST
PUBLISHING DAYS

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

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


ATTACK SCENARIO #1 ON STEROIDS

MITM SCENARIO



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

4. TRICK VICTIM TO TYPE "R" / "Enter" / "Space" ONCE AGAIN...
5. **ARBITRARY CODE EXECUTION!**

 The publisher of dumptrash.exe couldn't be verified.

[Learn more](#)

Run

View downloads

×

USERACCESSCONTROL



ONLY TRIGGERED WHEN ADMINISTRATIVE PRIVILEGES ARE REQUIRED

YOU CANNOT BYPASS THAT. FULL STOP.

DO YOU REALLY NEED THAT FOR CAUSING SERIOUS TROUBLES? ASK ZEUS / CARBERP...

LIMITATIONS FOR ATTACK #1 REVISITED

1. SMARTSCREEN FILTER

2. USER ACCESS CONTROL ← *Not a problem*

**RESTRICTED AREA
UNAUTHORIZED ACCESS
PROHIBITED**

ATTACKSCENARIO#2

TIMING/POSITIONATTACK



Windows 8

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, WINDOW IS CLOSED
9. IF TIMING IS APPROPRIATE THERE ARE GOOD CHANCES OF VICTIM CLICKING ON THE UNDERLYING POPUNDER

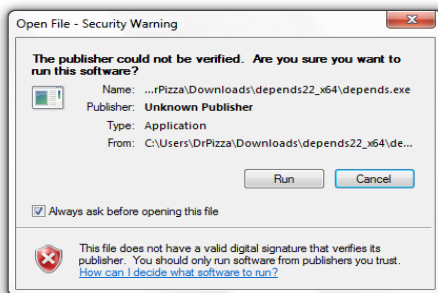
ATTACKSCENARIO#2RELOADED



- 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**
8. **AS SOON AS THE MOUSE IS HOVERING ON THE BUTTON, WINDOW IS CLOSED**
9. **IF TIMING IS APPROPRIATE THERE GOOD CHANCES THE VICTIM CLICKS ON THE UNDERLYING POPUNDER**

ATTACKSCENARIO#2.c

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 ENGINEERED
3. SOME SENSITIVE NOTIFICATIONS (E.G. FILE DOWNLOADING) SHOULD BE EVER KEPT IN A STATIC FRAME OF THE CHROME, NOT BOUND TO NAVIGATION WINDOW
4. BROWSER INITIATED SWITCHES BETWEEN WINDOWS OF DIFFERENT DOMAINS SHOULD BE COMBINED WITH A GRAPHICAL EFFECT (e.g. fading, etc) IN ORDER TO GIVE USERS ADEQUATE REACTION TIME

CONCLUSIONS

1. THE BROWSERS SHIFT FROM MODAL TO MODELESS NOTIFICATIONS IS STILL NOT MATURE
2. IMPLEMENTATIONS ARE NOT SECURE ENOUGH TO PROTECT USERS SAFETY: AT LEAST TWO TECHNIQUES ALLOW FOR STEALTH REMOTE CODE EXECUTION
3. WHY TRING TO BUILD COMPLEX AND UNRELIABLE EXPLOITS IF GETTING CODE EXECUTION IS SIMPLE LIKE PRESSING ONE KEY? 😊

THANK YOU

valotta.rosario@gmail.com

[@tentacolo_Viola](#)

sites.google.com/site/tentacoloviola/