Defensive Computing

Information Security for Individuals

Adam Reiser
July 21, 2014

Why should I care about computer security?

- Fraud/identity theft
- Behavioral tracking
- Exposure of third party data
- Discriminatory pricing
- Mass surveillance on an unprecedented scale
- Unknown future use of personal data

Necessary, but insufficient

- “I use an anti-virus program”
- “I keep my system updated”

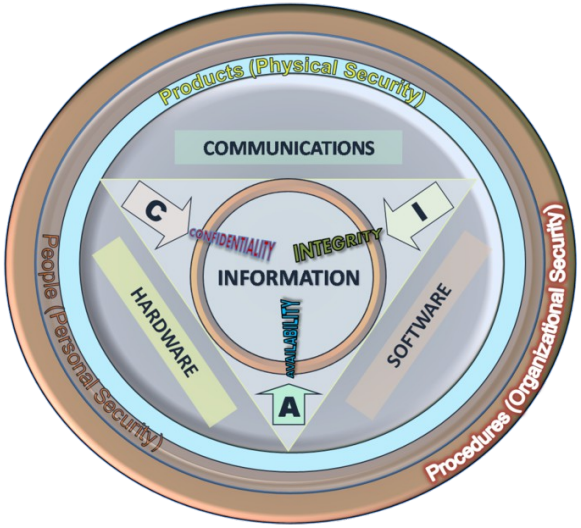
YOU CAN’T BUY SECURITY IN A BOX!

What do I need to know about security?

- Principles of information security
- Threat analysis
- Countermeasures to protect myself

Information Security:
Three Pillars

CONFIDENTIALITY



INTEGRITY

AVAILABILITY

Information Security: Integrity

- "Information" can refer to a text document, an email, a file, an image, a video, a website, a database…almost anything you can view on a computer.

- The integrity of the information is confirmed if a trusted authority vouches that the information you obtained (your copy) is <u>identical</u> to the original information.

- A lack of information integrity may result from carelessness on the supply side or it may mean that the information was deliberately altered for malicious purposes.

Information Security: Confidentiality

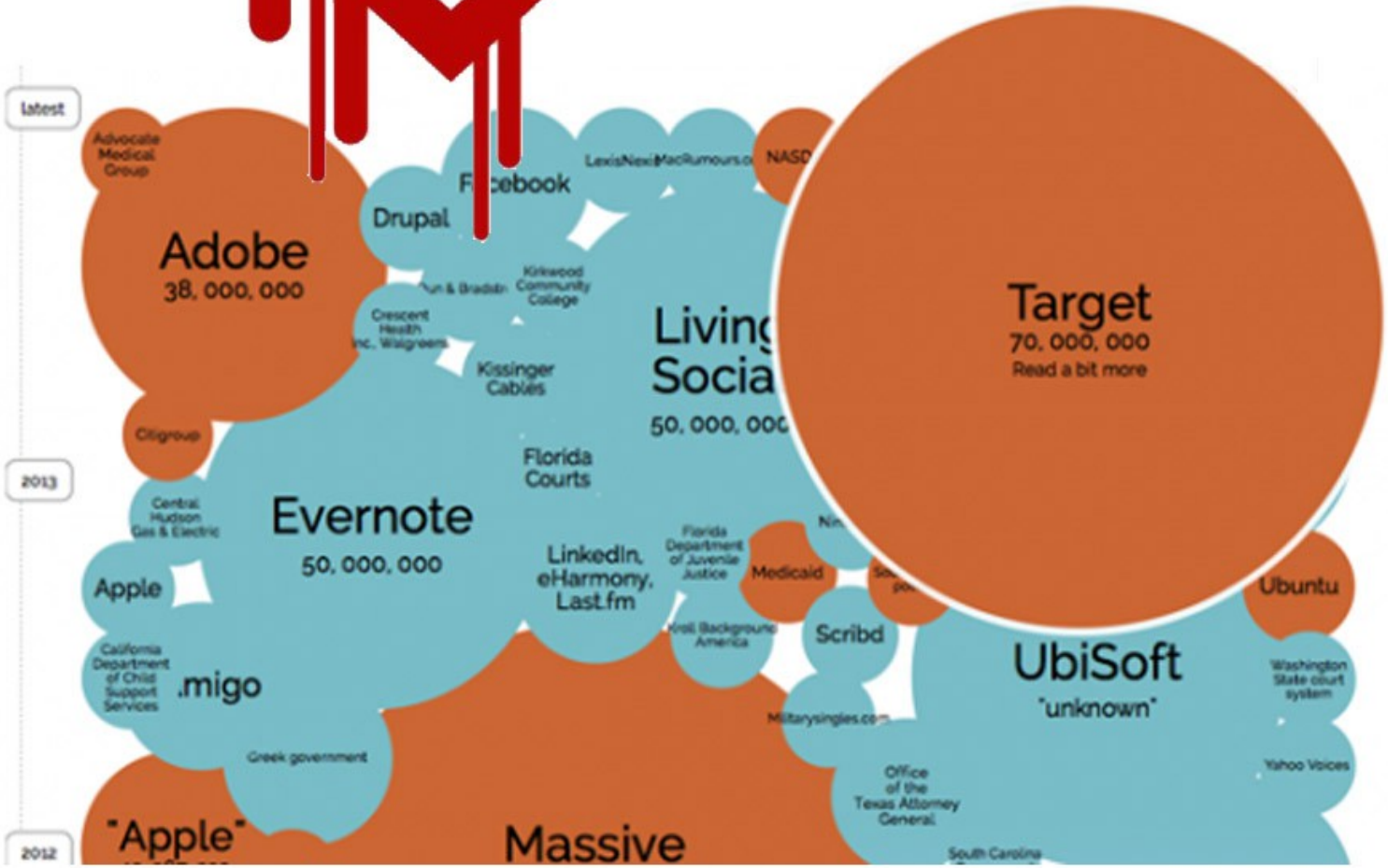
- Confidentiality means “secrets stay secret!”
- “Secrets” generally refer to any information that could affect your life or property if they were obtained by unauthorized individuals:
  - SSN
  - Bank account information
  - Medical history
- Your password is not a secret: it is a *security control* designed to protect your secrets.
- Definition of “secret” is ultimately up to you.

Information Security: Availability

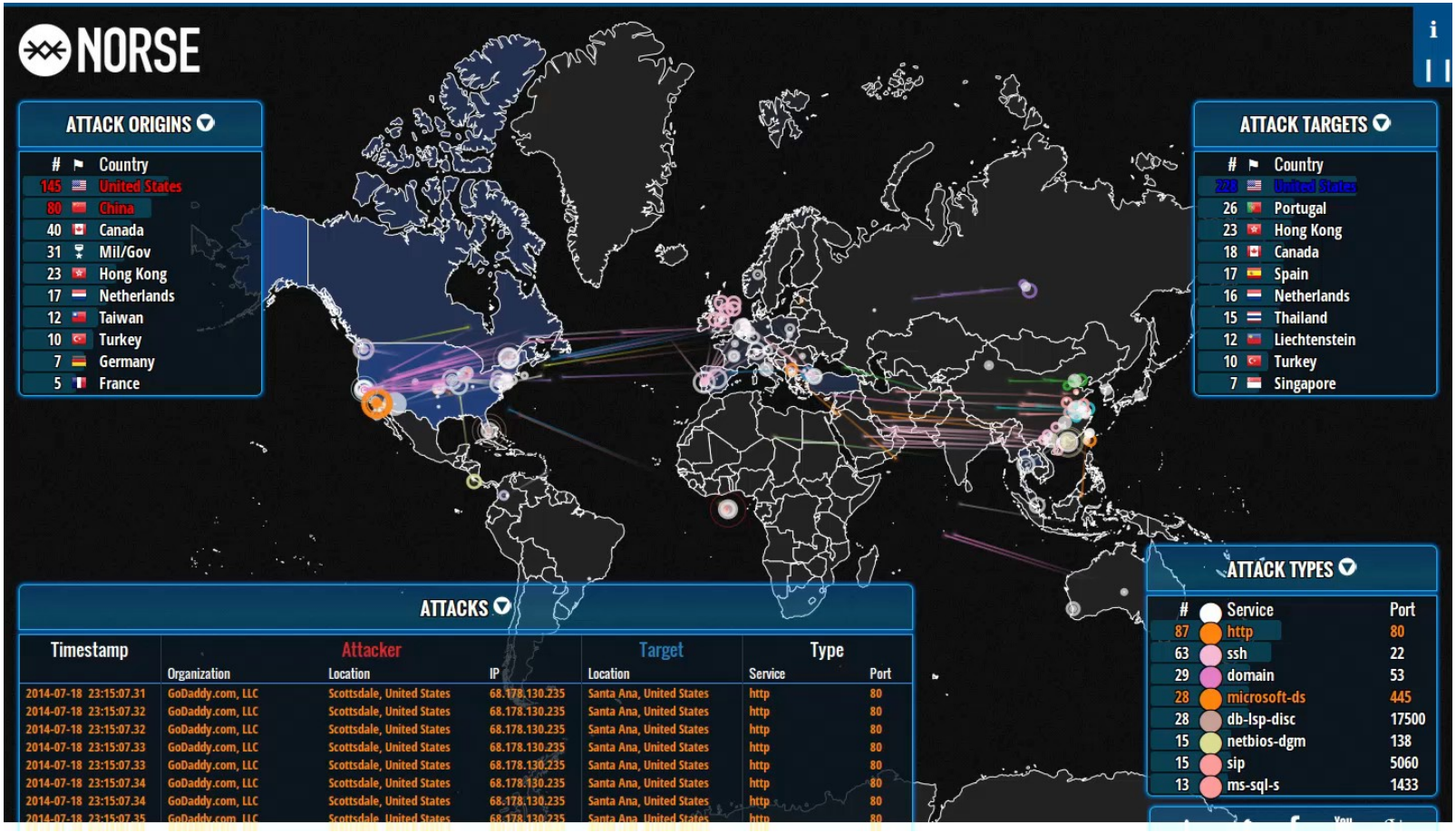
Security measures are only effective if they are used! If they interfere with working effectively, users may bypass them, especially when under time constraints.

A good password defeated by a mousepad

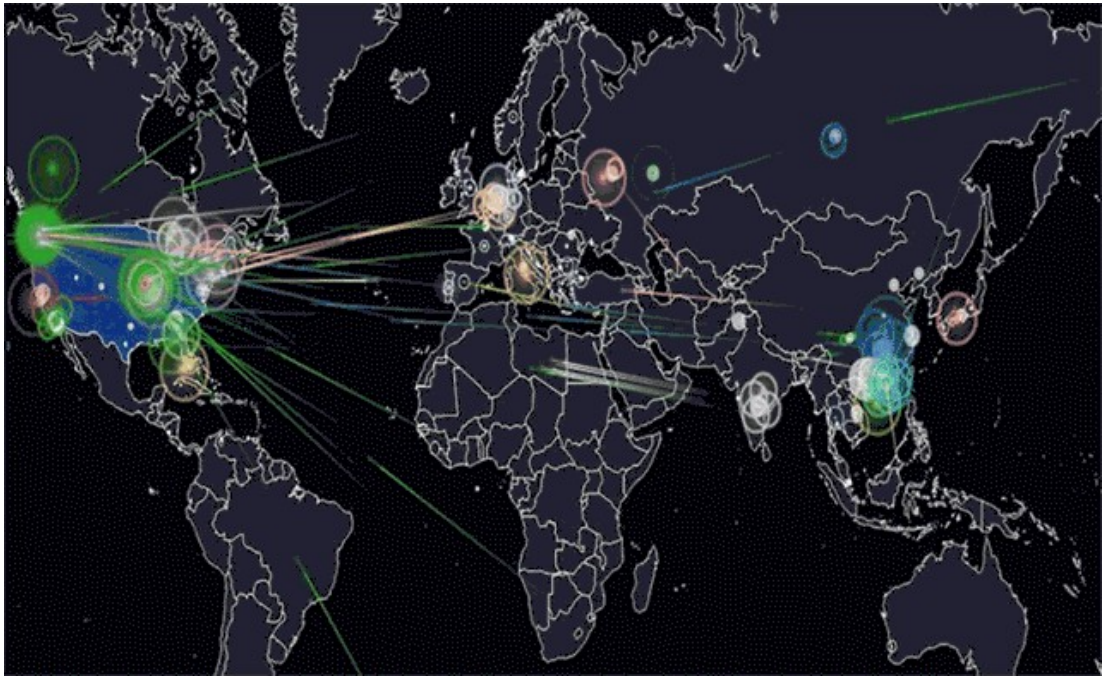
Threat Analysis



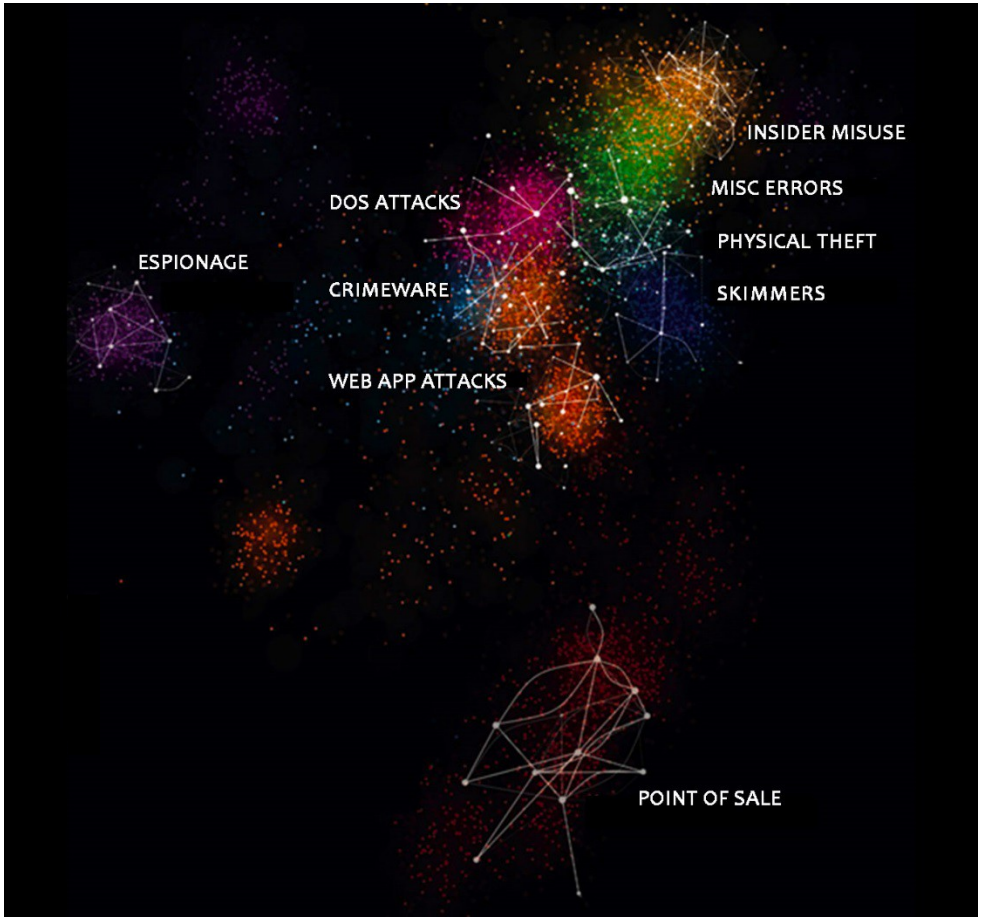
Threat Analysis: Real-time "Cyber-attack" Data from Norse



Threat Analysis: Real-time Visualization by Norse of June 20, 2014 “Cyberattack”

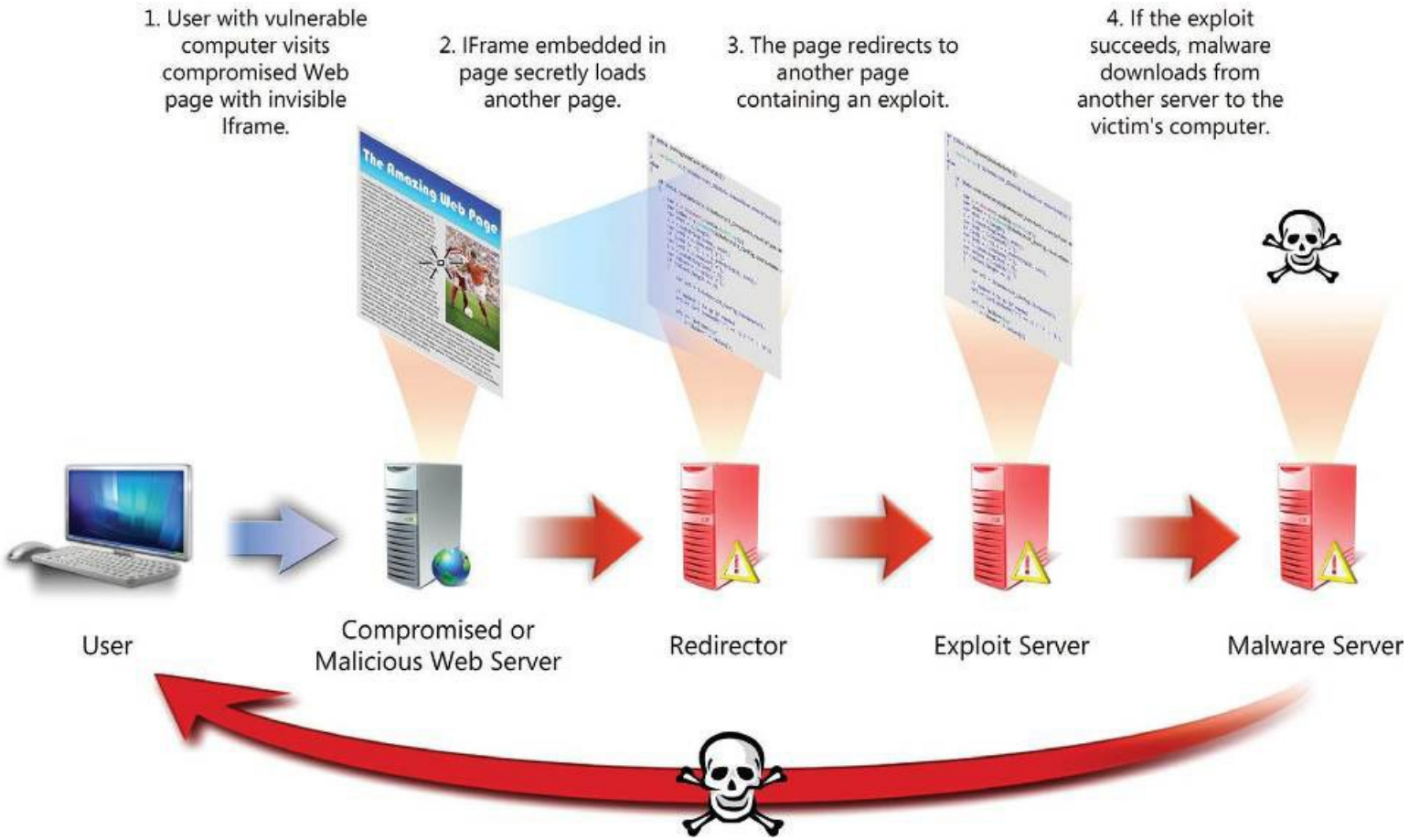


Threat Analysis: Pattern Identification



Analysis of 100,000 data breaches over 10 years: 95% of all incidents can be classified as one of 9 patterns ("2014 Data Breach Incident Report", Verizon)

Threat Vector: Web Drive-by



Threat Vector: Watering Hole

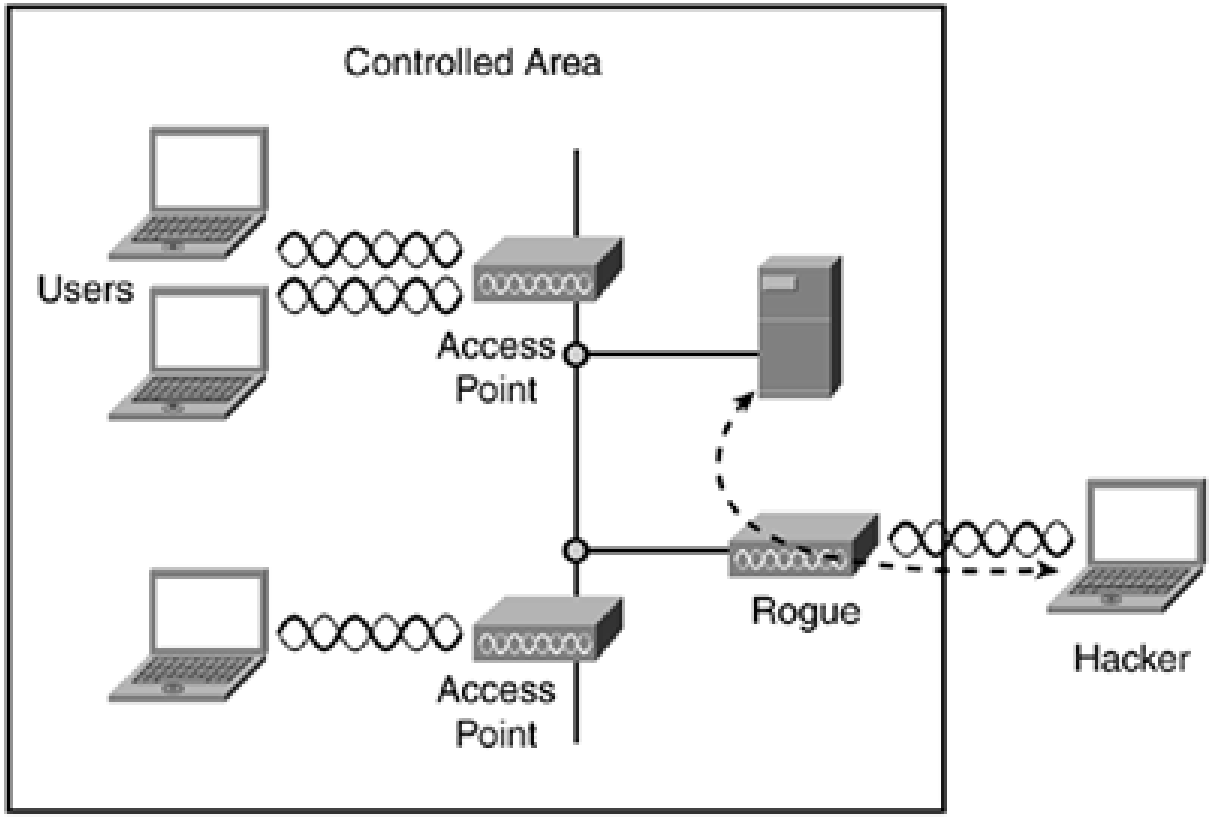
Threat Vector: Downloads

Injected ad for a fraudulent antivirus product falsely claiming to be recommended by Google. In reality, this is an ad for trafficconverter.biz, whose “affiliates” are paid on commission for installations.

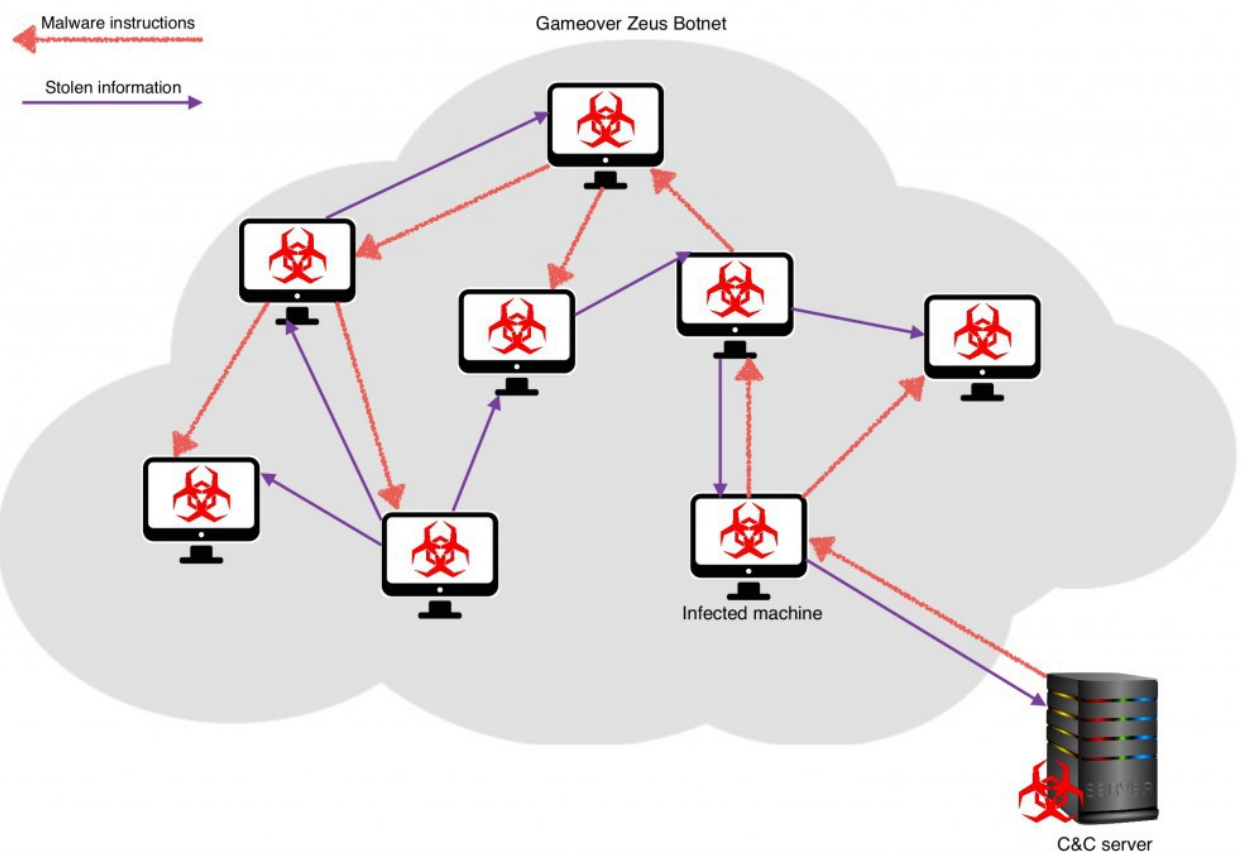
Threat Vector: Email

Email (phishing, attachments) is still one of the top ten malware vectors.

Threat Vector: Rogue Hotspots

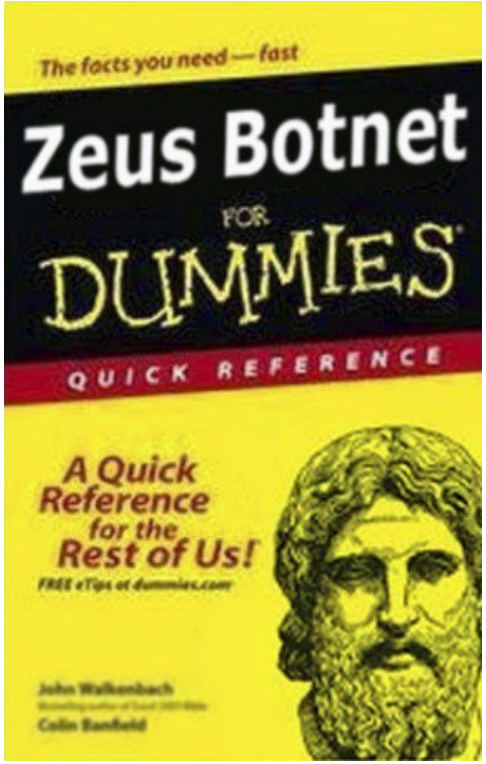


Threat Activity: Botnets



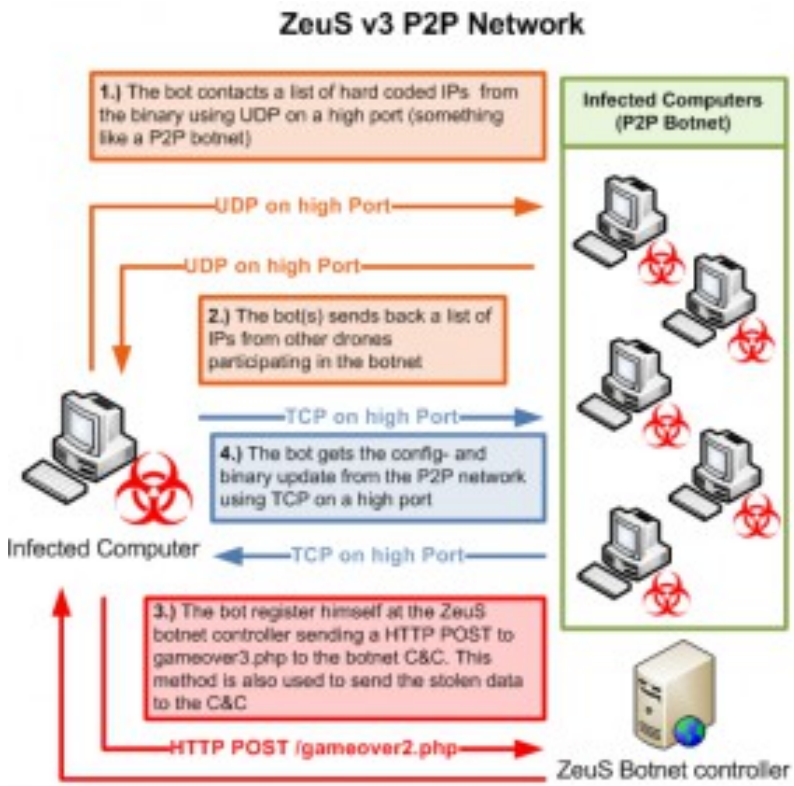
Users may be unaware their computer has joined the ranks of the zombies.

Threat Activity: DIY Botnets



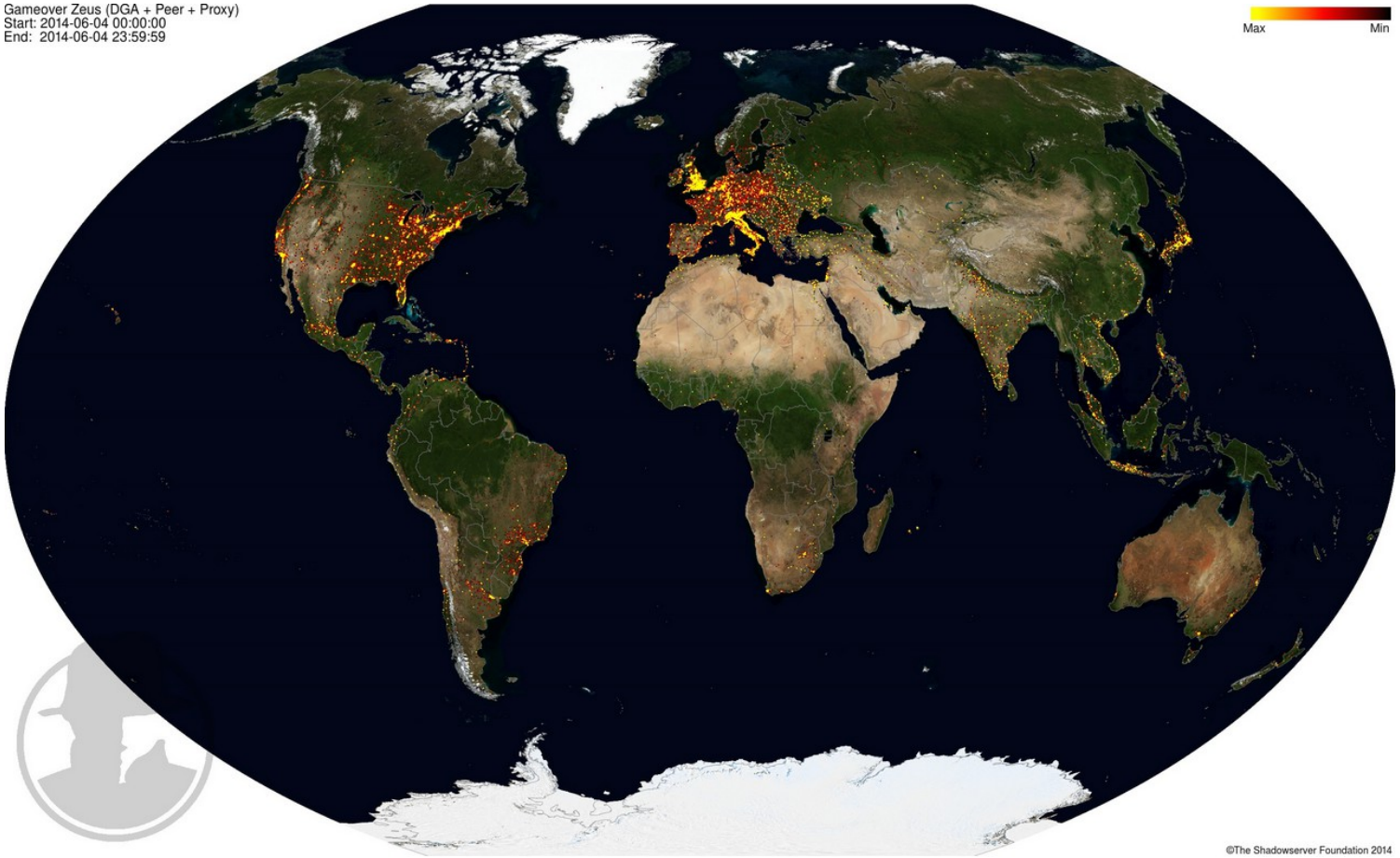
The Zeus trojan was widely available as a botnet creation kit.

Threat Activity: Gameover ZeuS



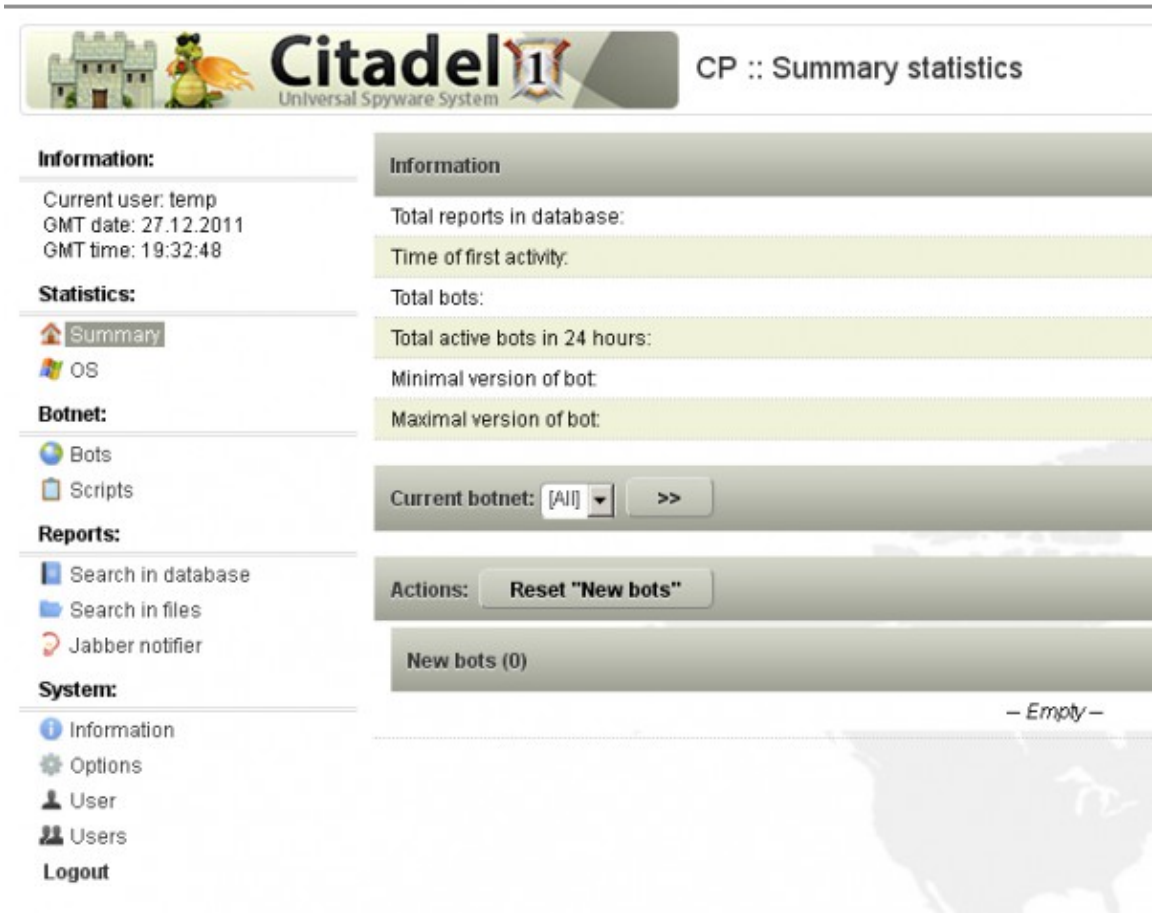
GameOver ZeuS was extremely difficult to eradicate due to advanced P2P propagation mechanisms.

Threat Activity: Gameover ZeuS



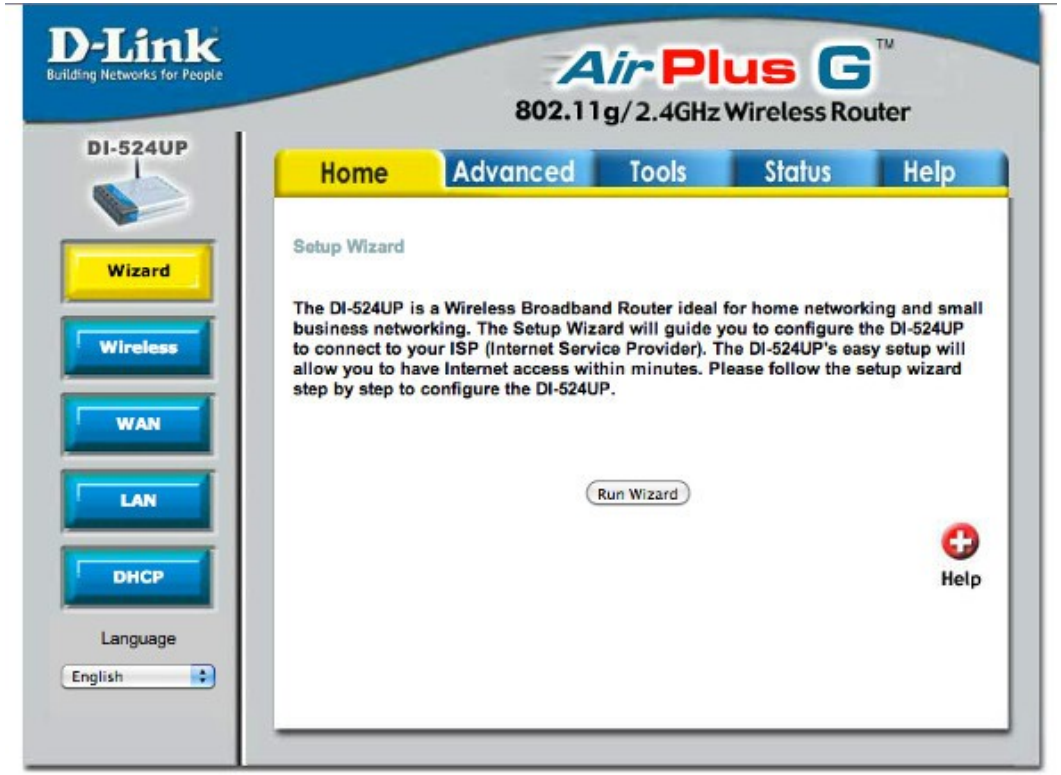
Global infection by Gameover ZeuS at time of takedown 6/4/2014

Threat Activity: Citadel Botnet



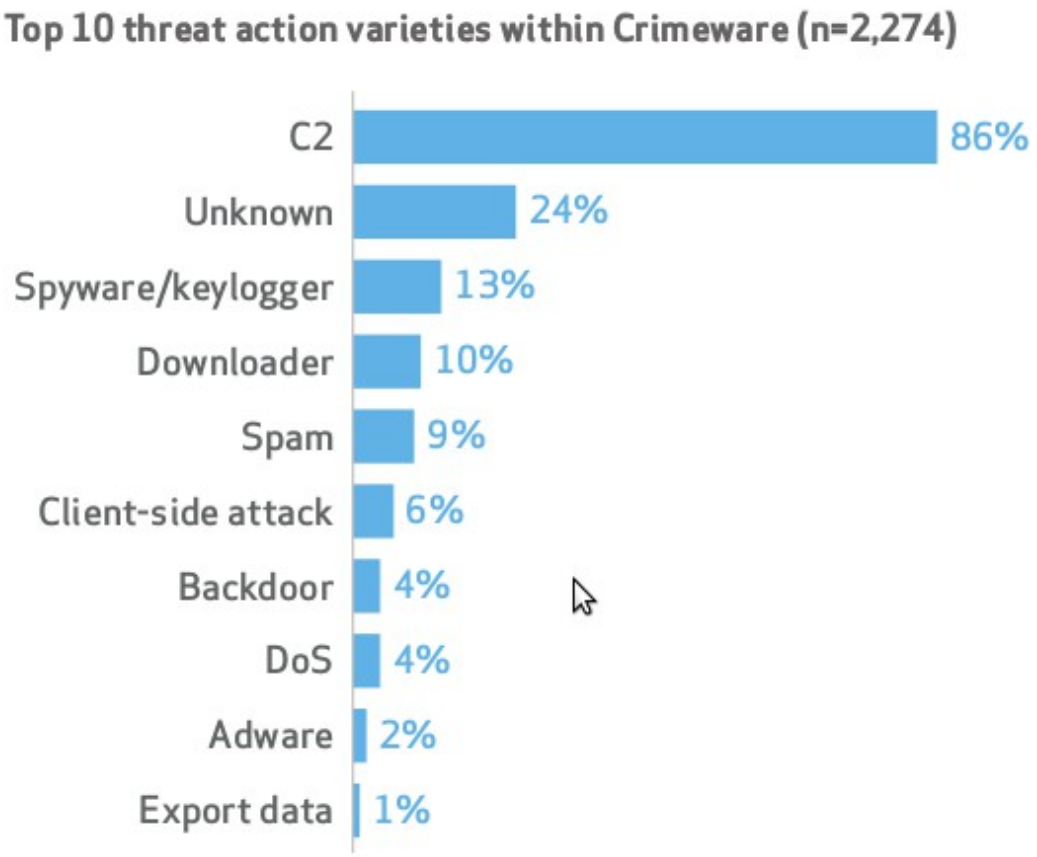
Citadel botnets, evolved from Zeus, set up a business model that included a trouble ticket system for consumers unhappy with product performance.

Threat Vector: Home Router Firmware



D-Link was the first router in which firmware was found to have a backdoor; subsequently many other routers were found to be vulnerable.

Threat Activities



Data from “2014 Data Breach Investigations Report”

Threat Activity: Ransomware

Noncriminal Threat Modeling

$$\text{threat} = \text{probability} \times \text{magnitude}$$

- For businesses, this definition is the basis for cost/benefit calculations to determine whether to implement a particular security control

- How do we apply this formulation to an individual?
  - You have to decide what you care about
  - Examples: browsing history, purchases, transactions
  - You have the RIGHT to decide to keep this information secret

Countermeasures

- Access control
  - Passwords / two-factor authentication
- Hardware
  - Firmware replacement
- Software
  - Software updates
  - Integrity verification
- Network activity
  - Click/cookie tracking
  - Firewalls
  - VPN

Countermeasures: Access Control

- Passwords
  - Strength
  - Management
- Two-factor authentication
- Hard drive encryption

Countermeasures: Hardware

Routers: Backdoors have been identified in router firmware from many manufacturers.

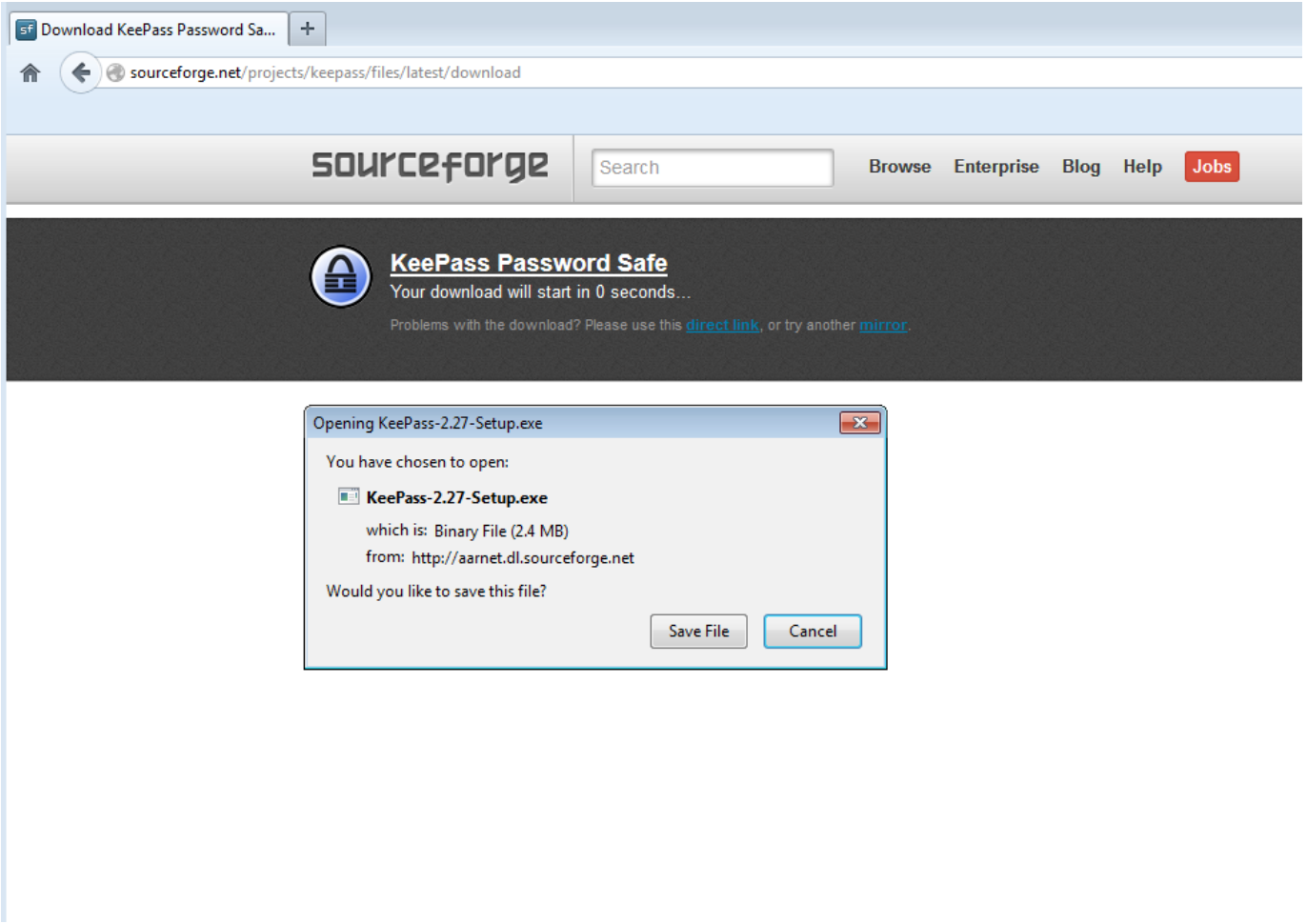
- Countermeasures: Wipe proprietary firmware; install open source firmware (e.g., *EasyTomato* for Asus RT-N16)

CPU: Intel chips (Sandy Bridge and newer) are equipped with built-in remote access via a second operating system that cannot be disabled. (It is promoted as useful for “remote evaluation”)

- No countermeasures are known; individual evaluation of risk/benefits of using this hardware is necessary.

Countermeasures: Integrity

You can safely download applications from third party sources by validating their *checksums*:



Countermeasures: Integrity

Identify the checksum for your download:

Hash Sums - KeePass

keepass.info/integrity.html

KeePass
Password Safe

Home
- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass
- Downloads
- Translations
- Plugins / Ext.

Information / WWW
- Help
- FAQ
- Security
- Awards
- Links
- Search

Support KeePass
- Donate

KeePass Distributions Hash Sums

KeePass can be downloaded from many mirror servers. If you want to check if the offered files are verified by the KeePass authors (i.e. official and original files), you can hash the downloaded file using the hash computation utility of your choice (you can try one of these utilities: Visual Hash Calculator, ReHash, MD5sums) and see if the hashes match.

Are you looking for hashsums of pre-1.0 versions (0.8 to 0.99c)? Have a look at the pre-1.0 hashsums page.

Hashes of all official downloadable files:

- KeePass 2.x Files
- KeePass 1.x Files
- OpenPGP Signatures

```
<KeePass-2.27.zip>
MD5          : 77887F44 33682DB3 4F246571 020DB9DC
SHA1         : 025CFAD1 D9D309F5 10008073 81CAA697 E9E03FE9
SHA256       : CA1DCD5B 120C31AB 433560C2 DD049ADD
               EE16D138 6AF2358A AA67E75E 34BD27E2
Size64       : 00000000 00237C09

<KeePass-2.27-Setup.exe>
MD5          : 80A2FA47 AB77546F 5E9C59A5 50746CC7
SHA1         : C70D3188 9FF98675 81EFDFE6 0864E7DE FB7BDE69
SHA256       : BBAD404A D80B04CF B618A3A9 03D5EB56
               82CF9DCD 749A4FFD E0A20D26 E657155E
Size64       : 00000000 0026FC2C

<KeePass-2.27.msi>
MD5          : C43DA220 CF973180 72AB5000 7E9AEE4A
SHA1         : 372BA249 7723B6EB 7D51DDA2 2F1A51F5 321EED0C
SHA256       : 2058B347 3060F503 9581D2A1 711FC93C
               C0EFC04F 5E4C6E39 BFA1CEF6 8FFCCE81
Size64       : 00000000 002AEA00

<KeePass-2.27-Source.zip>
MD5          : F34D38EB E6FA1661 E56BE5A0 D1C2FBFD
SHA1         : 309B6A65 41DB359E 70A22A08 2A4BC8AA 068FA084
SHA256       : F812A7BC 2921A491 D7DCF4A2 47373FA5
               3F32843B 1DF6A34E CE488A25 D599CA44
Size64       : 00000000 0035E1F6

-------------------------------------------------------------
```

Countermeasures: Integrity

Verify that the checksum of the downloaded file matches the published checksum:

Terminal

File Edit View Search Terminal Help

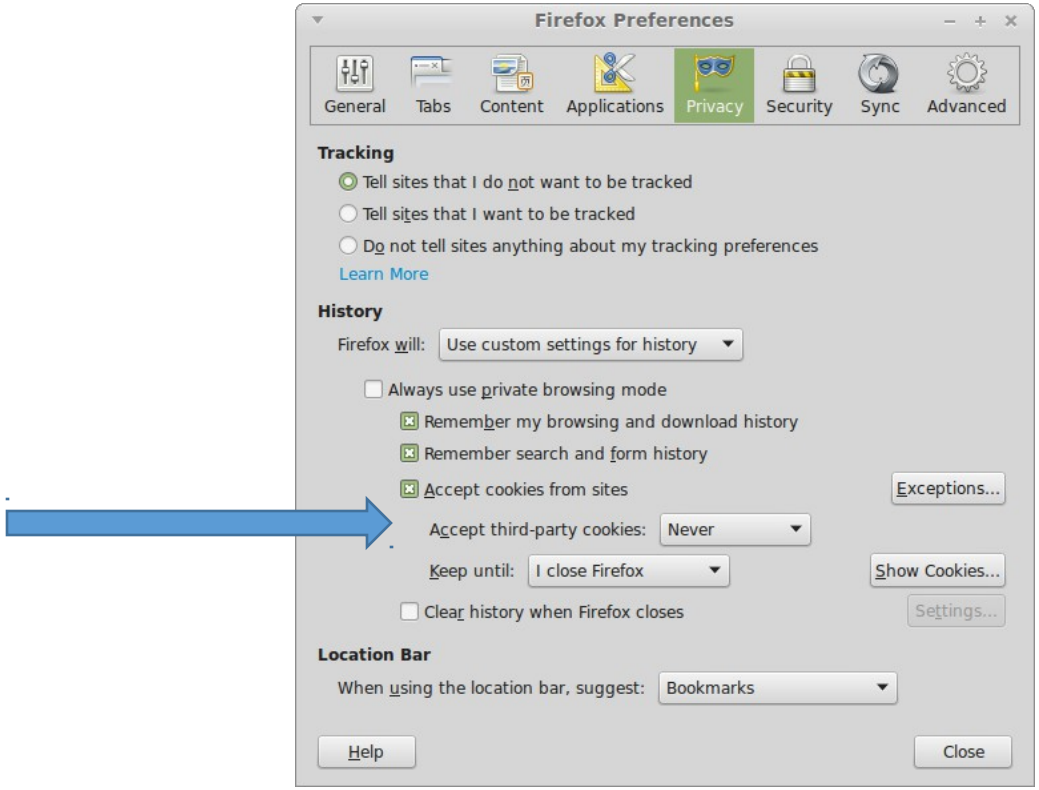
```
raven@angel ~/Downloads $ openssl dgst -sha256 KeePass-2.27-Setup.exe
SHA256(KeePass-2.27-Setup.exe)= bbad404ad80b04cfb618a3a903d5eb5682cf9dcd749a4ffde0a20d26e657155e
```

```
<KeePass-2.27-Setup.exe>
MD5          : 80A2FA47 AB77546F 5E9C59A5 50746CC7
SHA1         : C70D3188 9FF98675 81EFDFE6 0864E7DE FB7BDE69
SHA256       : BBAD404A D80B04CF B618A3A9 03D5EB56
               82CF9DCD 749A4FFD E0A20D26 E657155E
```

Countermeasures: Integrity Summary

- Download file
- Obtain published checksum
- Generate checksum of downloaded file
- *If they match*: file integrity is confirmed
- *If they don't match*: the file may be corrupt or malicious

Countermeasures:
Tracking Cookies



Firefox preferences +

add-on

Self-Destructing Cookies 0.4.4

By Ove

Countermeasures:
Click Tracking

- “Twitter uses the t.co domain as part of a service to protect users from harmful activity, to provide value for the developer ecosystem, and as a quality signal for surfacing relevant, interesting Tweets.” (https://t.co/)
- What they *don't* mention is that it allows Twitter to know what links you click on: even if *you* don’t know where they go!

http://t.co/eV0G7ADksz

http://bltch69.com/miley-cyrus-can-t-keep-her-top-on

Firefox add-on gives you the

direct URL:

Countermeasures:
Malicious/Compromised Webpages

FEATURED

NoScript Security Suite 2.6.8.33

by Giorgio Maone

The best security you can get in a web browser!
Allow active content to run only from sites you trust, and protect yourself against XSS and Clickjacking attacks.

Certificate Patrol 2.0.14

by Carlo v. Loesch, tg(x), 20after4

Your browser trusts many certification authorities and intermediate sub-authorities quietly, every time you enter an HTTPS web site. This add-on reveals when certificates are updated, so you can ensure it was a legitimate change.

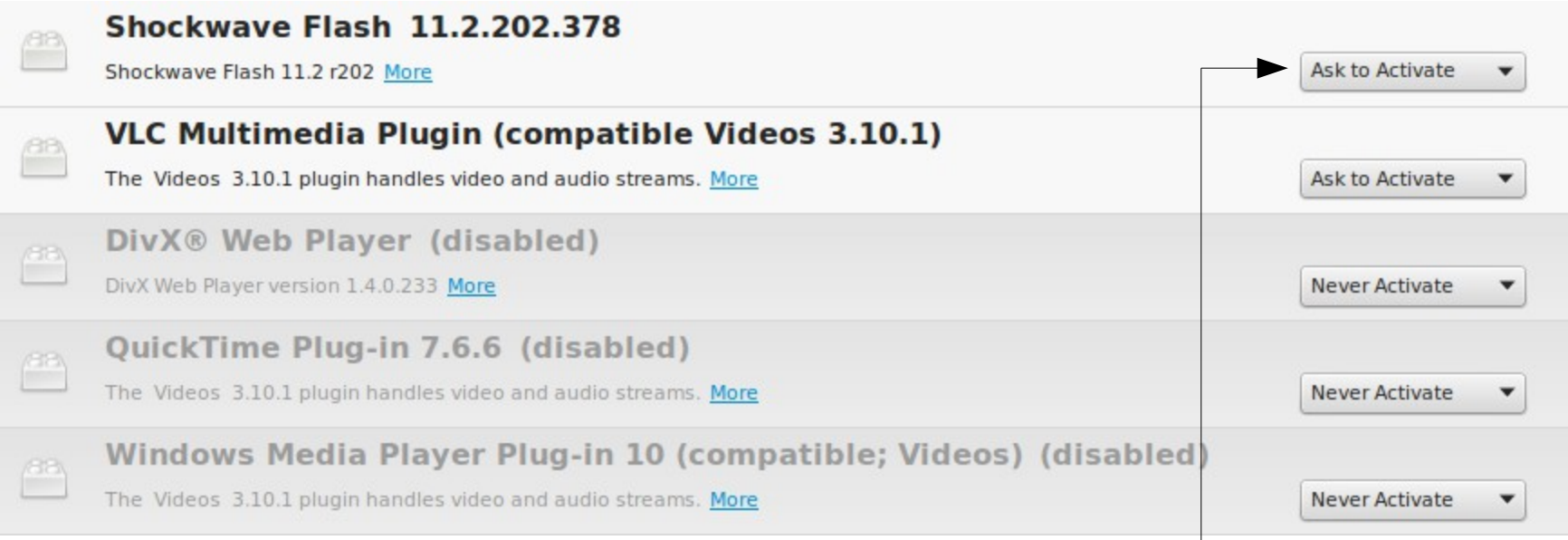
Pure URL 1.2.4 NO RESTART

by VEG

Removes garbage like "utm_source" from URLs

Mozilla Firefox and selected add-ons provide excellent protection from tracking and attacks.

Countermeasures:
Disable unnecessary Plugins



Disable Flash, or at least set "Ask to Activate".

Countermeasures: VPNs

VPN solves many different types of security problems (Firesheep, rogue hotspots, your ISP spying on you)