
infosecurity
EUROPE
Security Workshops

Advanced Malware, Tools and Tactics used in APTs and Targeted Attacks

Dana Tamir, David Lawton

29/04/14

infosecurity EUROPE

What we will be discussing today:

- What Makes APTs and Targeted Attacks Successful?
- Tools and Tactics
- Lessons learned
- Q&A

Attackers optimize and refine target selection

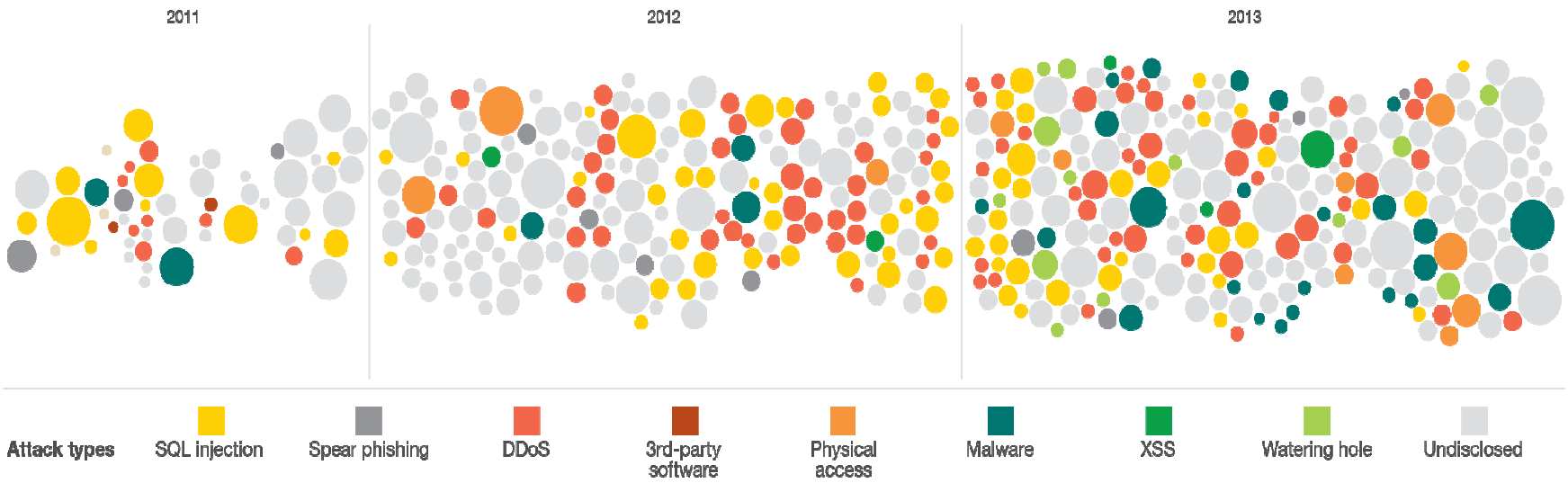


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

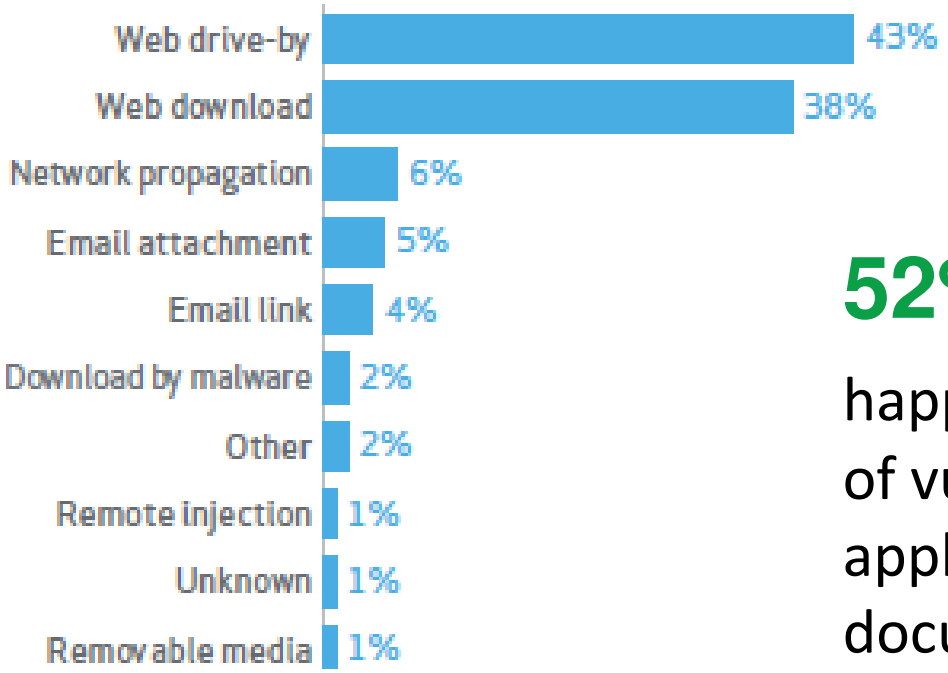
Source: IBM X-Force® Research and Development

Question:
What is the most common cause for malware infections?

A.Web Drive-By Downloads
B.User downloads from the web
C.Network propagation
D. e-mail attachments

According to the 2014 Verizon Data Breach Report:

Figure 48.
Top 10 vectors for malware actions within Crimeware (n=337)



52% of malware infections happen via **exploitation** of vulnerabilities in user applications like browsers and document readers.

Exploiting Vulnerable Applications

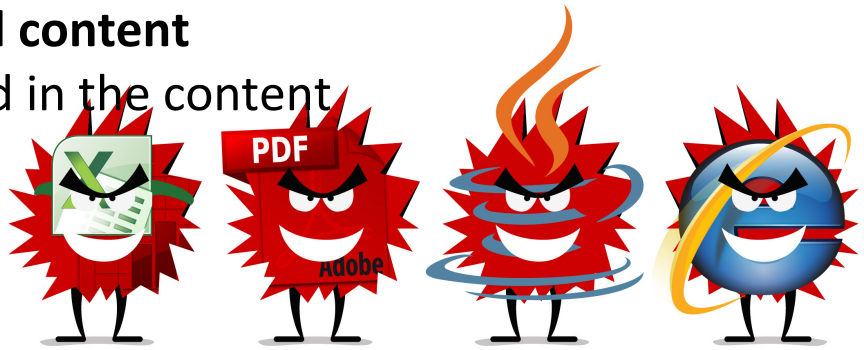
Based on reconnaissance, the attacker selects a target platform to attack: Adobe, Java, MS Office formats…

1.Create the exploit

- Zero-day vulnerability
- Using existing exploit kits to target a wide range of vulnerabilities

2.Create the weaponized content

- Exploit embedded in the content



You don’t need to be an expert...
The Russian underground offers exploits for $$$:

insomnius 23.03.2014, 13:29

Продам исходники CVE-2014-0497. Срабатывание ~95% на ие, фф.
Информация про все текущии экспы в первом посте.

Любопытный

Группа:
Сообщений:
Регистрация:
Пользователь №:
Деятельность:

infosecurity EUROPE

Manipulating Targets and Delivering the Payload

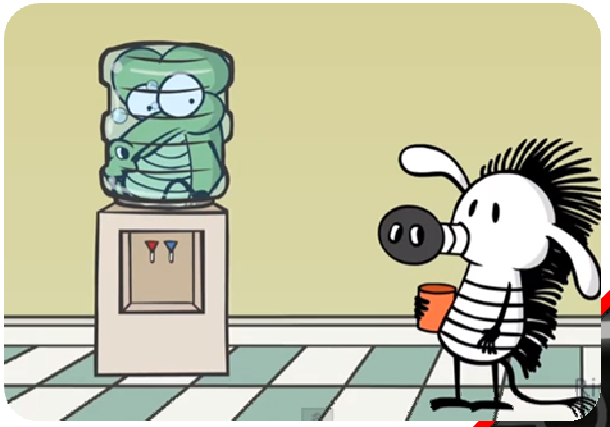
1. Create a phishing/spear-phishing email campaign
   - Attach the Weaponized content
   - Include a link to an Exploit Website (Drive-by Download)

2. Watering Hole attacks and Malvertising
   - Compromise a legitimate website

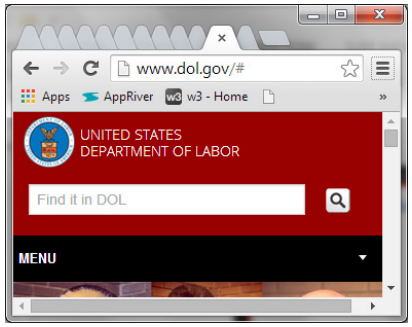
   Examples:

   iPhone SDK, Yahoo Ads…

When the user opens the weaponized content the exploit chain starts to deliver the payload



Anatomy of Watering Hole Attacks: DOL Case Study



1. DoL website compromised

3. Redirected to exploit site

DOL's "Site Exposure Matrices" website

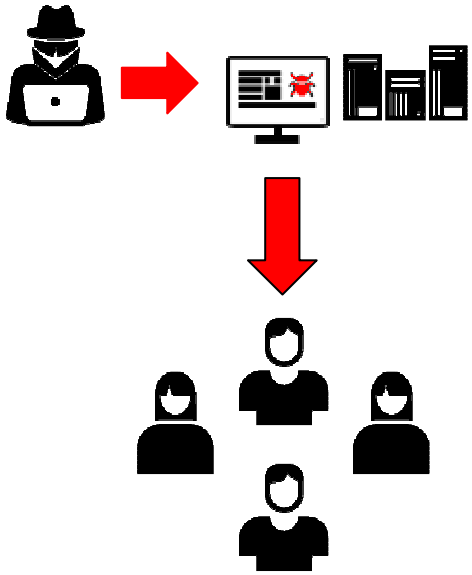
2. Website Visitors

4. Exploiting an IE zero-day remote code execution vulnerability

Visitors include aerospace, defense and security agencies

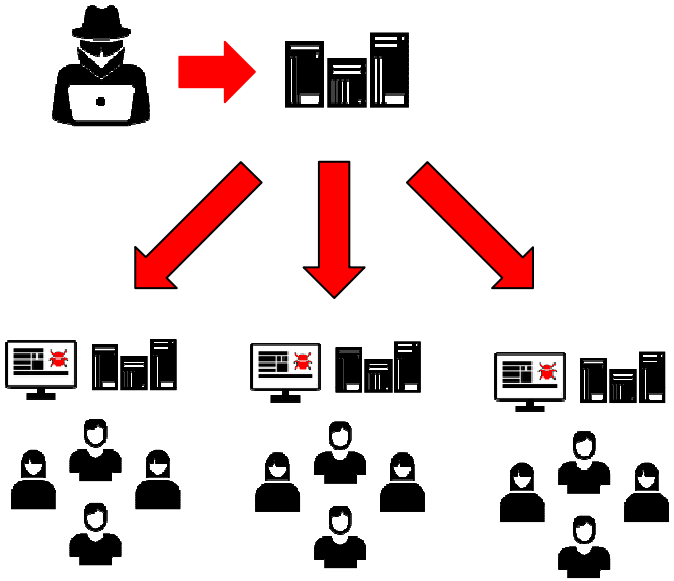
infosecurity EUROPE

Effectively targeting end users



Watering Hole

- Attacker injects malware on special interest website
- Vulnerable niche users exploited



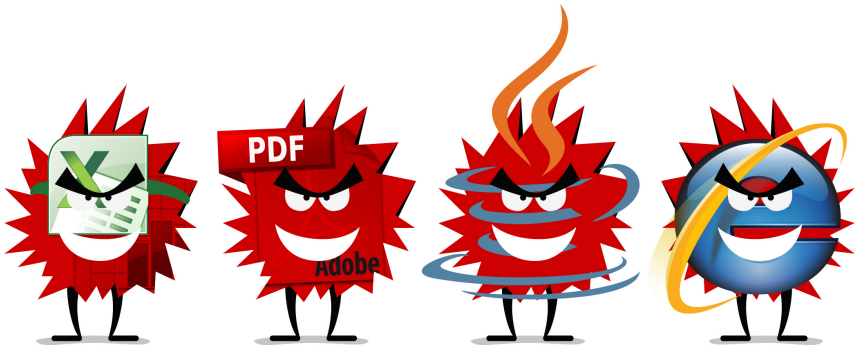
Malvertising

- Attacker exploits ad networks
- Malicious ad embedded on legitimate websites

Question:
In the RSA breach in 2011, how did the attackers infiltrate the network?

A. Using a spear-phishing email with a weaponized attachment
B. Using malvertising
C. Using drive-by downloads
D. Using credentials stolen from a 3rd party

Demo



Top Targets

Question:
Which end user application is most targeted by exploits that attempt to infect the user machine with malware?

A.Adobe Acrobat
B.The Calculator
C.Browsers
D.Java

explosive growth of **Java vulnerabilities...**

Exploitation of application vulnerabilities

from survey of 1 million Trusteer customers, December 2013

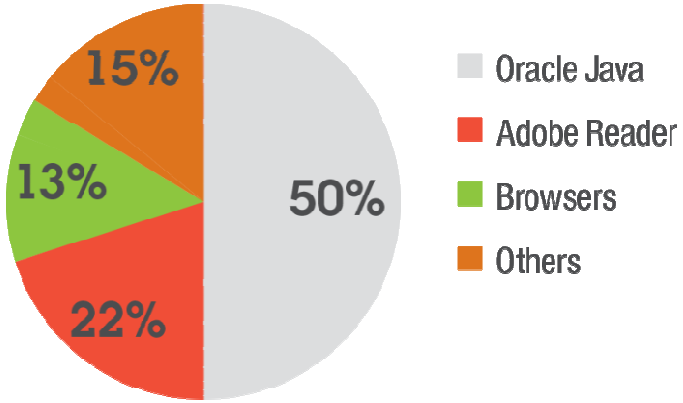


Figure 4. Exploitation of application vulnerabilities

Source: IBM X-Force® Research and Development

Java vulnerability disclosures growth by year, 2010 to 2013

originating in either the core Oracle Java or in IBM Java SDKs

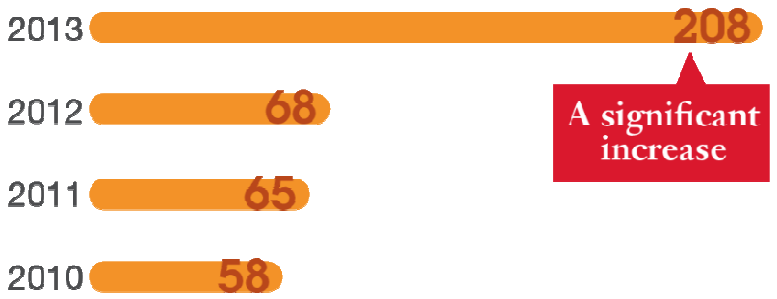


Figure 5. Java vulnerability disclosures growth by year, 2010 to 2013

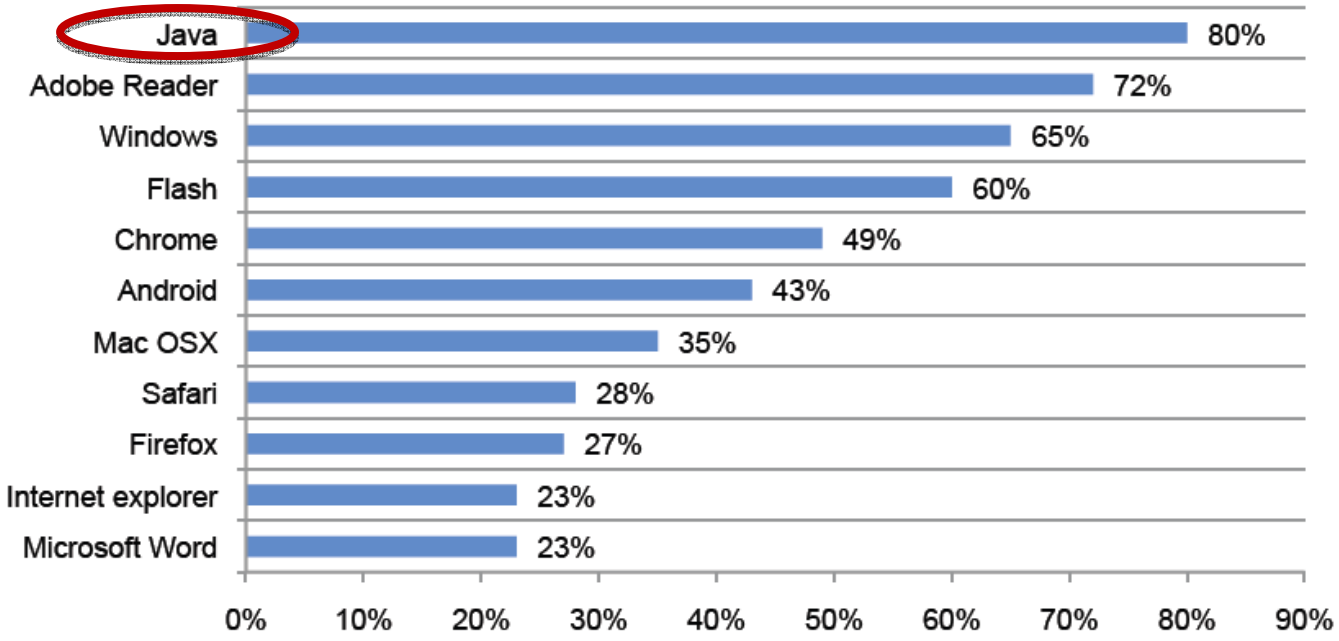
Source: IBM X-Force® Research and Development

… combined with a presence in every enterprise makes Java the **top target** for exploits.

infosecurity EUROPE

Do you patch applications?

Figure 4. Which applications make it difficult to ensure all security patches have been fully implemented in a timely manner
Very difficult and difficult response combined



Source: Ponemon

Most successful Java exploits are **applicative**, exploiting vulnerabilities related to the **Java security manager** and bypassing native OS-level protections.

Native exploits

- Buffer Overflow
- Illegal memory use
- Use-after-free

Applicative exploits

- Difficult to defend
- Gain unrestricted privileges
- Bypass native OS-level protections

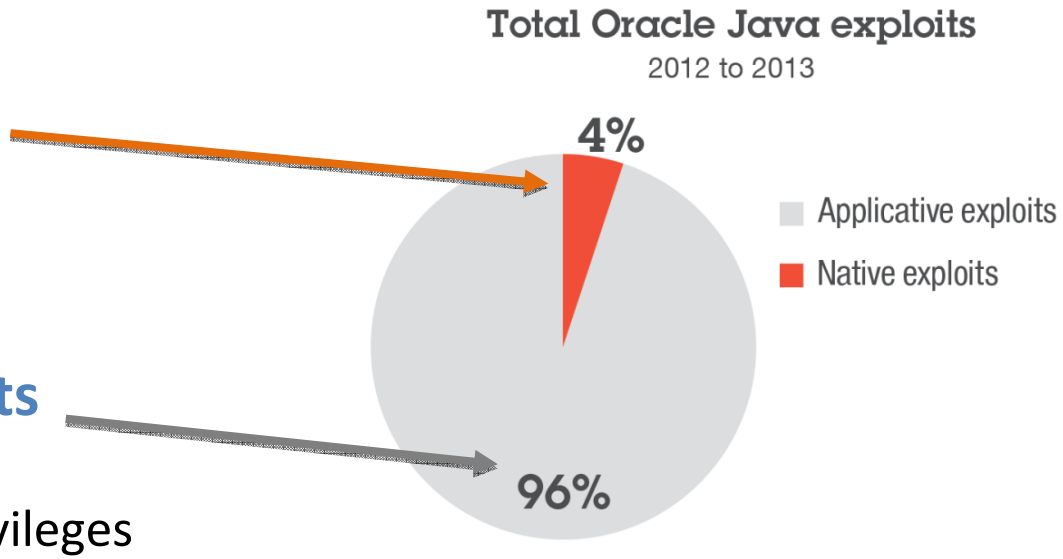


Figure 6. Total Oracle Java expoits, 2012 to 2013

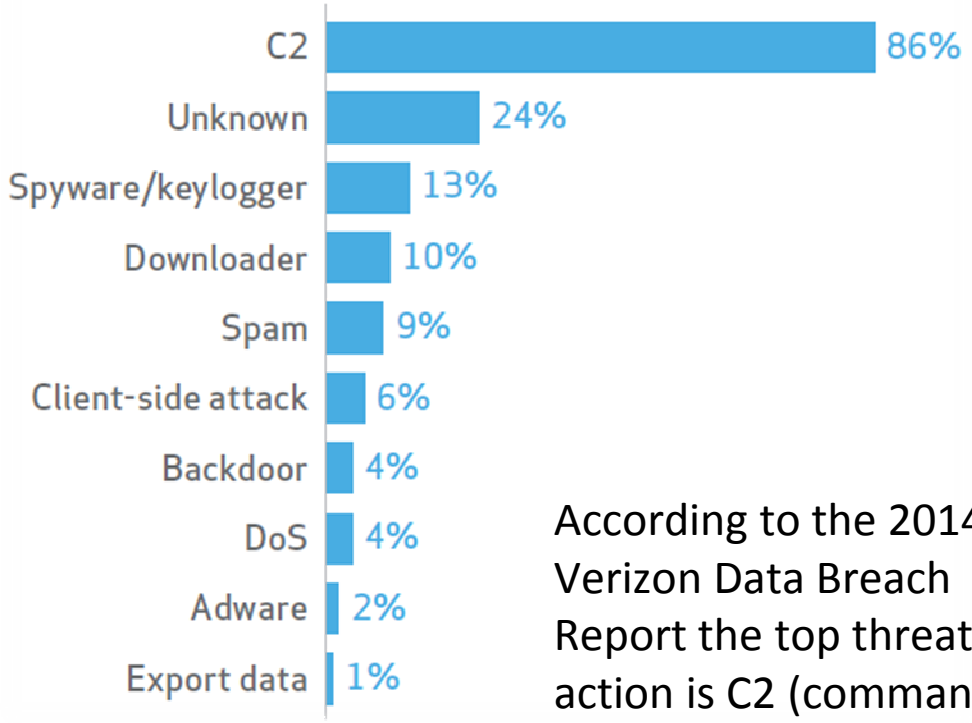
Source: IBM X-Force® Research and Development

Question:
What is the top threat action taking place after a malware download?

A.Spamming
B.Exporting data
C.Establishing communication channels
D.Logging user keystrokes and capturing screen images

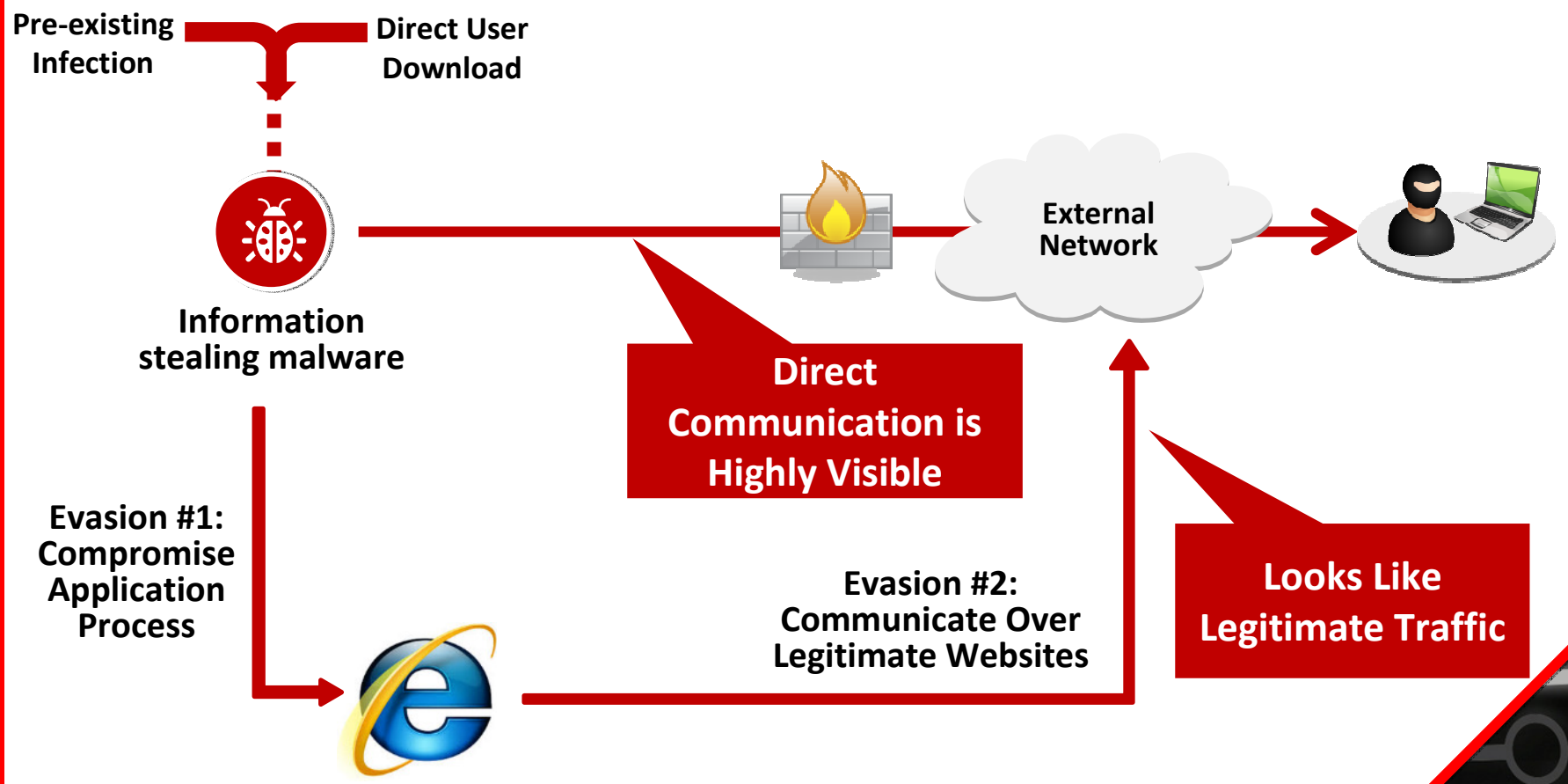
In order to enable **control** over a compromised device and **exfiltrate data**, malware must establish communication channels.

Figure 47.
Top 10 threat action varieties within Crimeware (n=2,274)



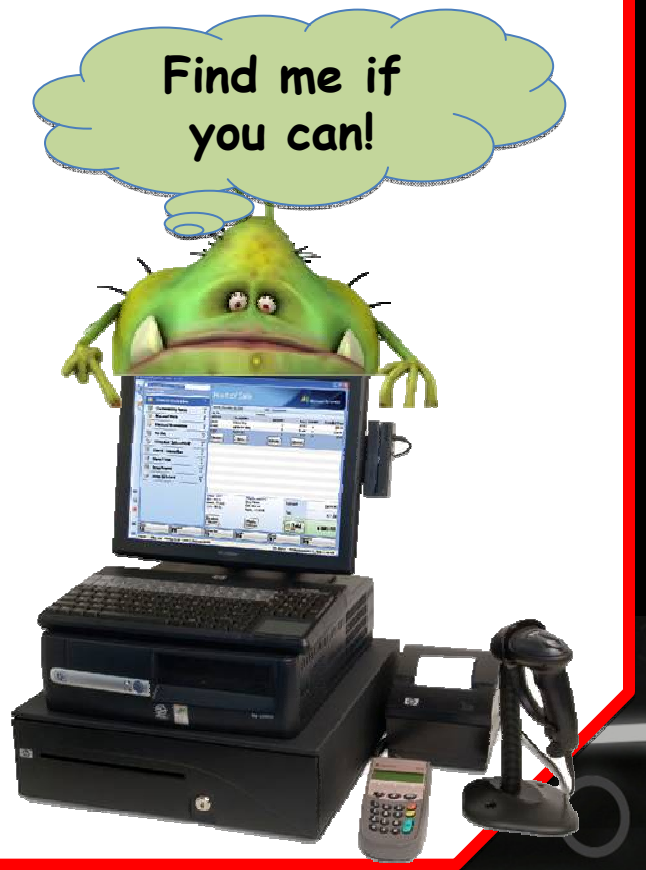
According to the 2014 Verizon Data Breach Report the top threat action is C2 (command and control).

Establishing Communication Channels



Execution Analysis: Dexter Malware

1. After execution, malware starts IE (in suspend-state) with no GUI
2. IE writes a reg key so windows will not show warning messages when running this file type
3. IE writes a copy of the infection file and then deletes the original
4. IE writes another reg key for internal use
5. IE writes three runkeys which links to the new copy of the malware
6. IE posts encrypted data to its C&Cs



Demo

Stolen Credentials Provide the Keys to the Kingdom

Question:
How often are weak or stolen credentials used for penetrating organizations?

A.33% of attacks
B.55% of attacks
C.76% of attacks
D.94% of attacks

According to the 2013 Verizon Data Breach report 76% of breaches exploit weak or stolen credentials.

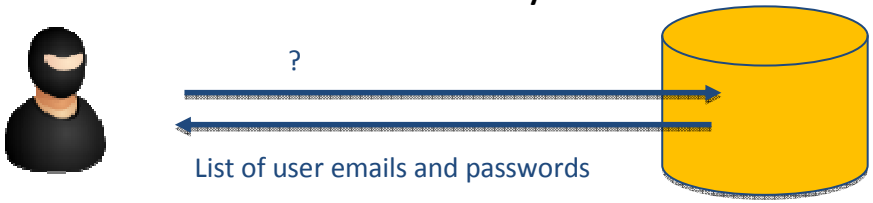
Credentials Phishing

- Advanced Malware can steal credentials but it's not the only way
- Phishing: Manipulate users to login to a phishing site
- Very common technique

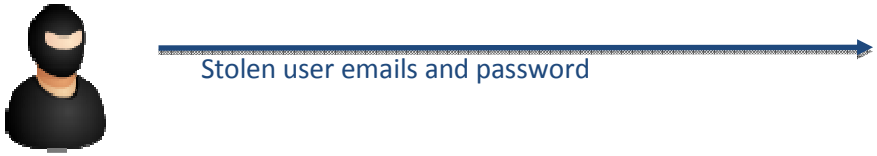
the ONION®
America's Finest News Source

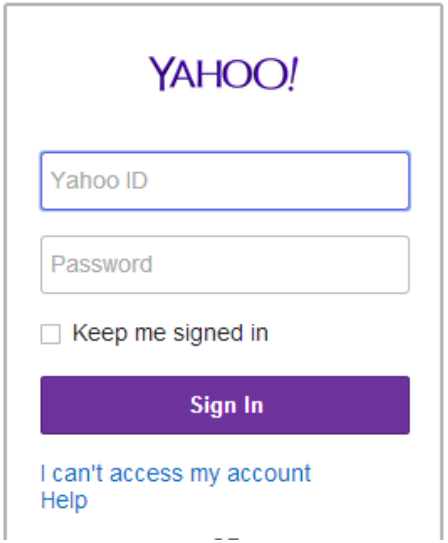
Third Party Breach – The Yahoo Example

Phase I: Hack into a 3rd Party database



Phase II: Used stolen credentials to log into Yahoo email accounts





Credentials Theft – What is the Risk?

- Access to Corporate Systems
- Access to Personal Systems:
  - Use personal information for reconnaissance
  - Use personal email account for sending phishing messages
  - Use personal email to reset credentials (forgot password…)

Tip: Prevent Password Reuse!

Targeted Attacks and APTs

What makes targeted attacks successful?

- Unique, tailored tools
  - Spear phishing specially designed for the target
  - Drive-by downloads, watering hole attacks
  - Zero-day attacks: 1st time used, never seen before
- Sophistication, ability to bypass traditional controls
  - Multiple techniques can be used
- Remain Stealthy
  - Provide the attacker more time to find resources and extract valuable data
- Gain access to data and resources
- Adversaries are getting better and better

Questions?

Visit us at stand J50 to learn about our solutions

Trusteer
an IBM Company

infosecurity
EUROPE