Foundstone
A division of McAfee

Latest Threats and Trends

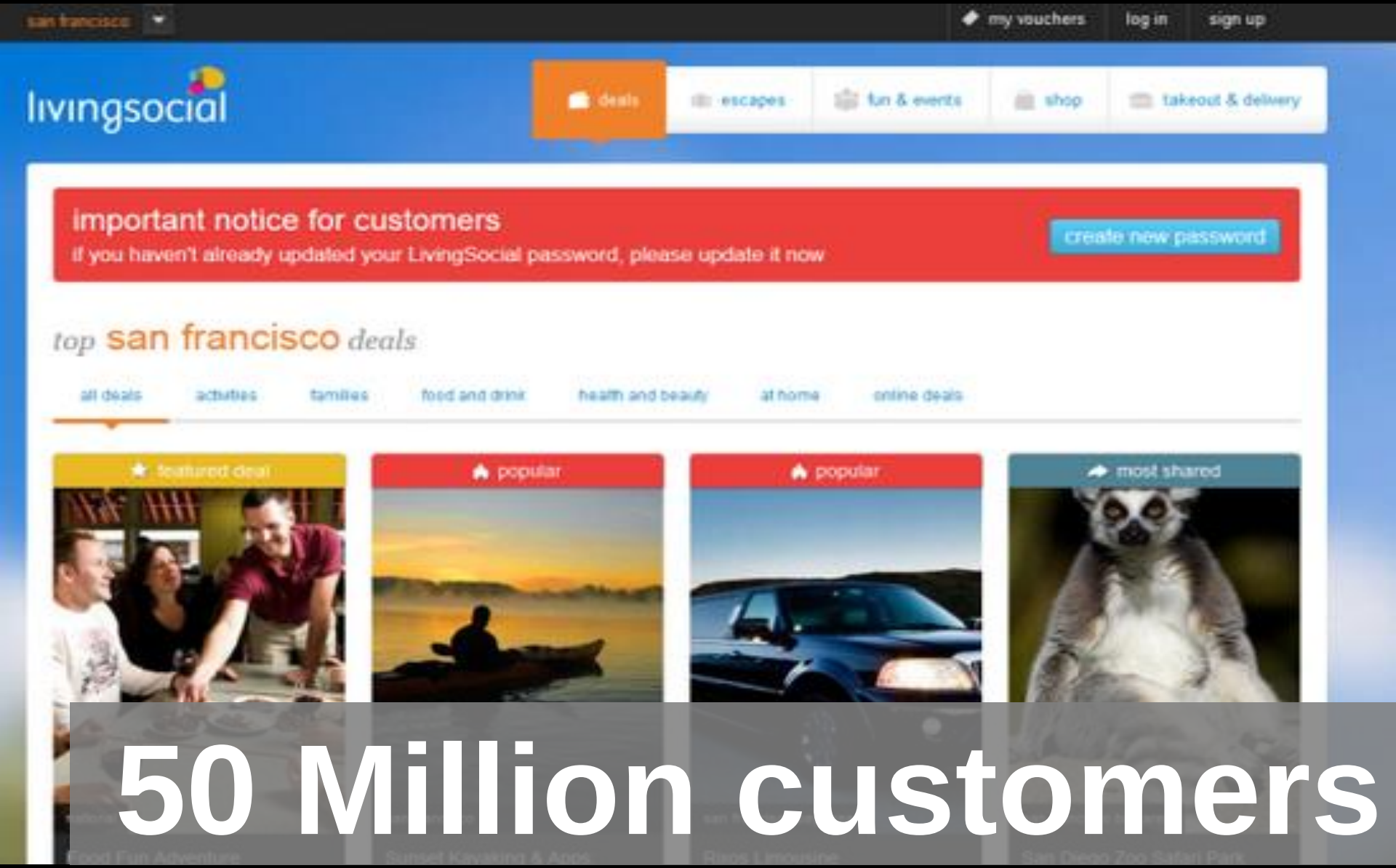
Brad Antoniewicz

McAfee
Proven Security™

Who am I?

Hi, I’m @brad_anton

April 5, 2013

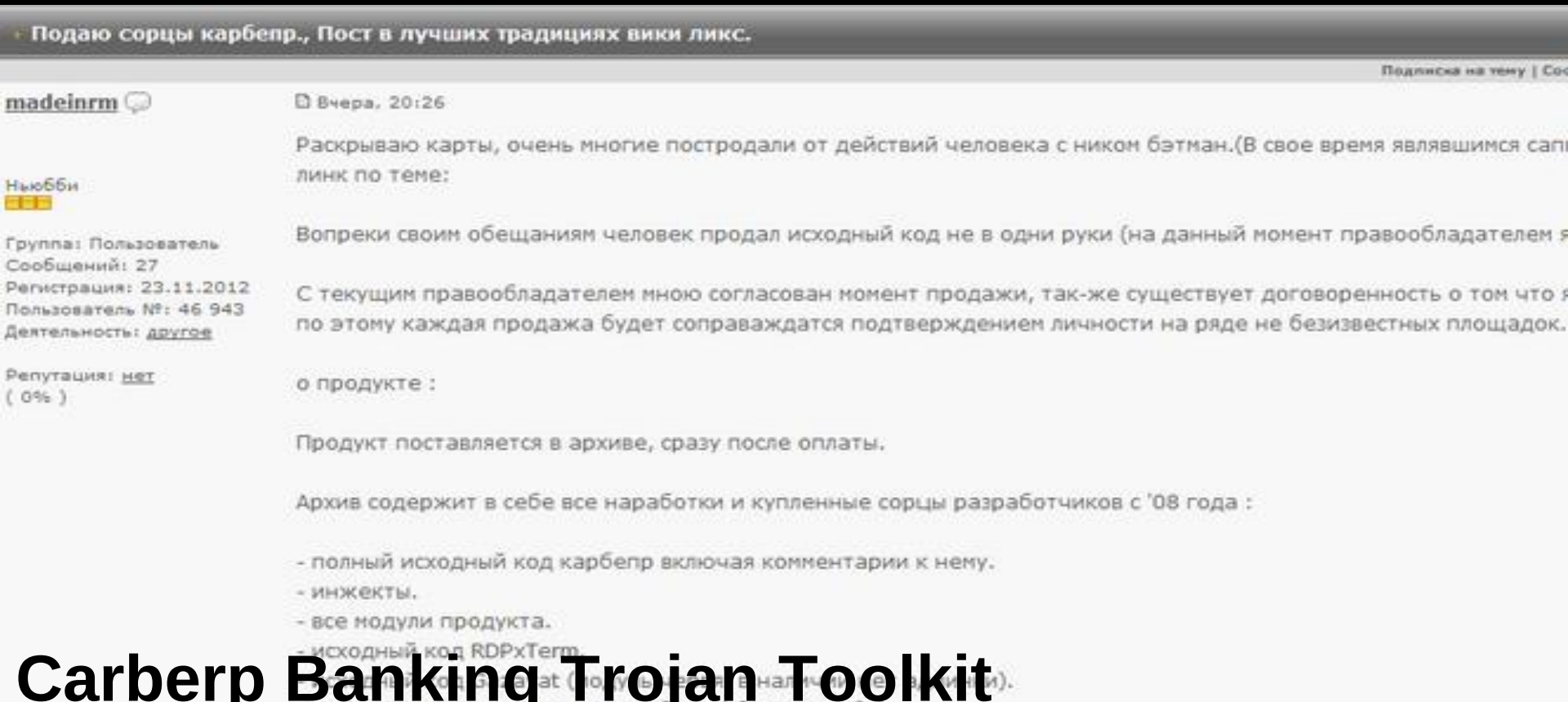


50 Million customers

May 1, 2013

- Exploits zero-day in IE8/WinXP
- Installs Poison Ivy Backdoor trojan
- Attributed to Chinese DeepPanda Group

June 15, 2013


Подаю сорцы карбепр., Пост в лучших традициях вики ликс.

Подписка на тему | Со

madeinrm

Вчера, 20:26

Раскрываю карты, очень многие пострадали от действий человека с ником бэтман.(В свое время являвшимся сап
линк по теме:

Вопреки своим обещаниям человек продал исходный код не в одни руки (на данный момент правообладателем я

С текущим правообладателем мною согласован момент продажи, так-же существует договоренность о том что я
по этому каждая продажа будет соправаждатся подтверждением личности на ряде не безизвестных площадок.

Ньюбби

Группа: Пользователь
Сообщений: 27
Регистрация: 23.11.2012
Пользователь №: 46 943
Деятельность: другое

Репутация: нет
(0%)

о продукте :

Продукт поставляется в архиве, сразу после оплаты.

Архив содержит в себе все наработки и купленные сорцы разработчиков с '08 года :

- полный исходный код карбепр включая комментарии к нему.
- инжекты.
- все модули продукта.
- исходный код RDPxTerm.
- административную панель карбепр (без ион куба).
- отвязанные билдеры всех версий.
- буткит.

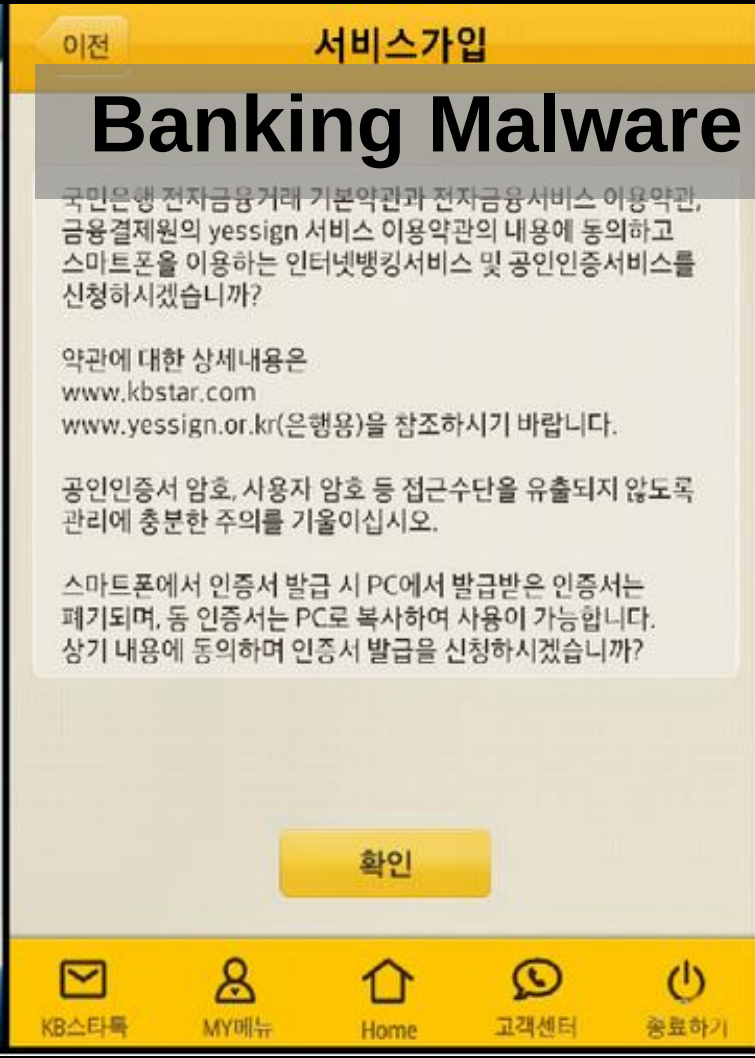
и многое другое.

Carberp Banking Trojan Toolkit

- June 5 – Developer “short on cash”, sells for $25k
- June 15th – User offers for $5,000.00
- June 18th – Download link spreads

TRENDS

Banking Malware



Android/FakeBankDropper.A

- SMS Phish via FSC
- Replaces official App
- Collects phone logs
- Requests private info

Ransomware

THE FBI FEDERAL BUREAU OF INVESTIGATION

ATTENTION !

IP:
Location:
ISP:

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011,

Video Recording
ON

MoneyPak

Code:

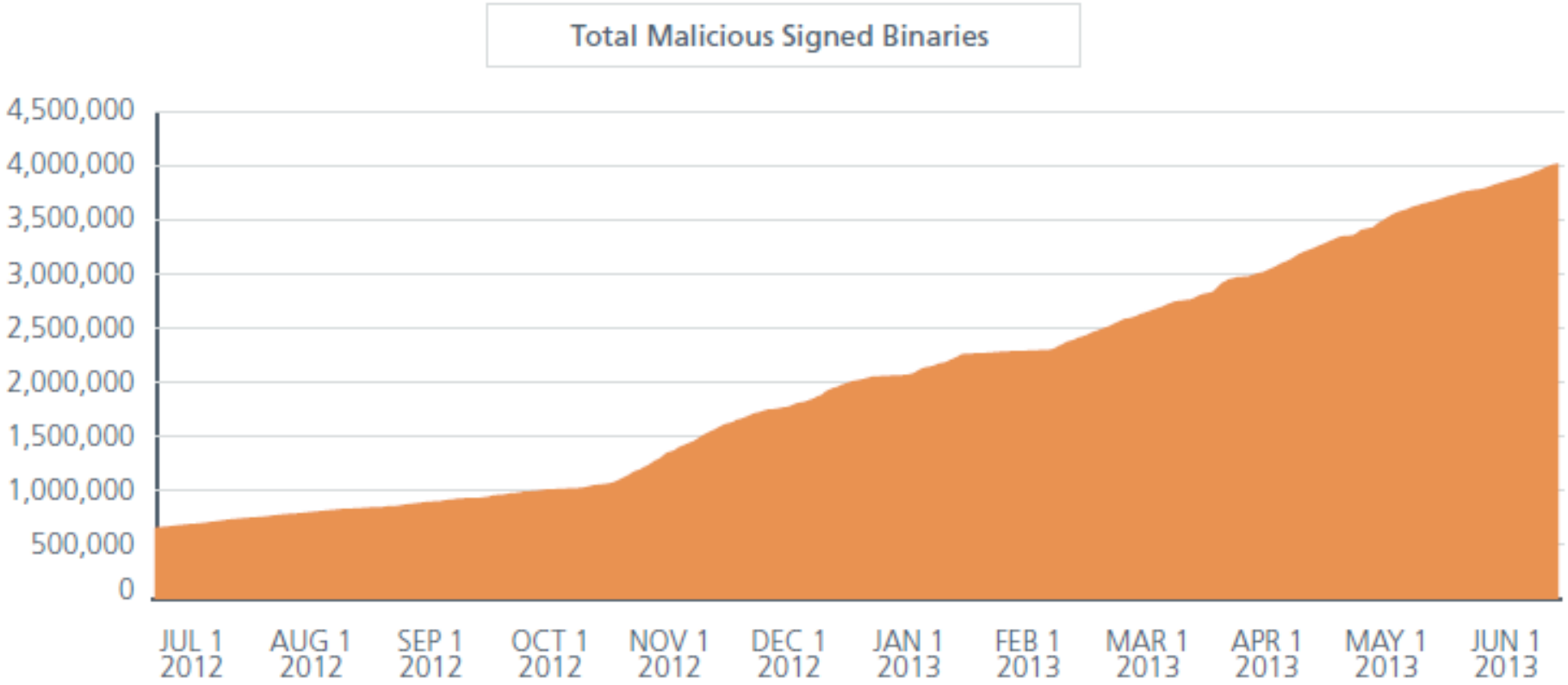
Sum:

100 $

1 2 3 4 5 6 7 8 9 0

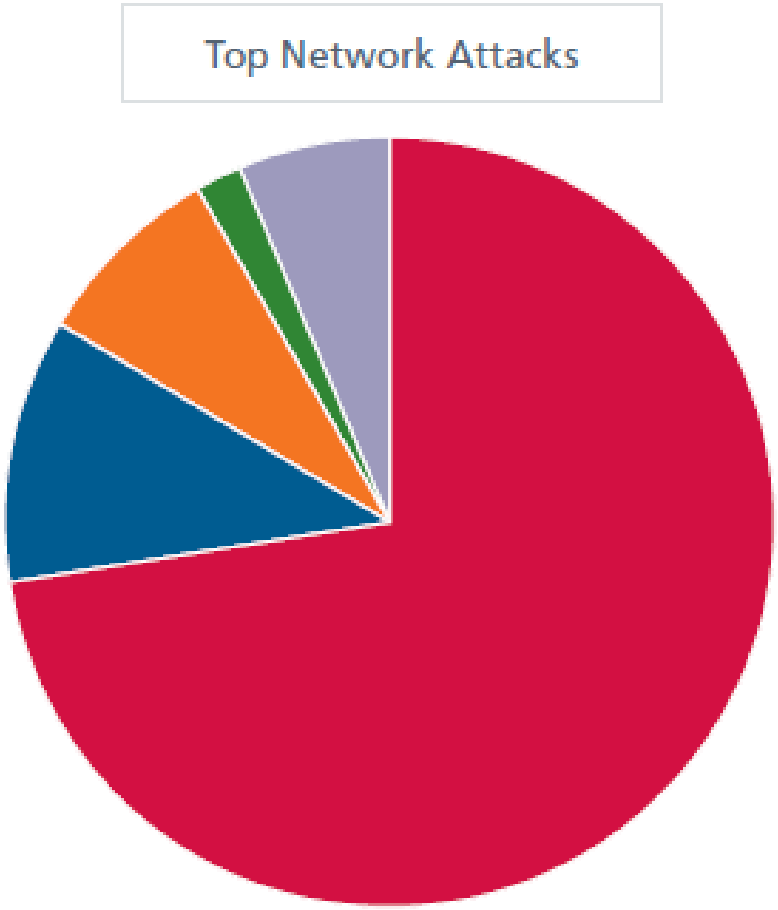
Pay MoneyPak

Signed Malware



Stolen Certificates

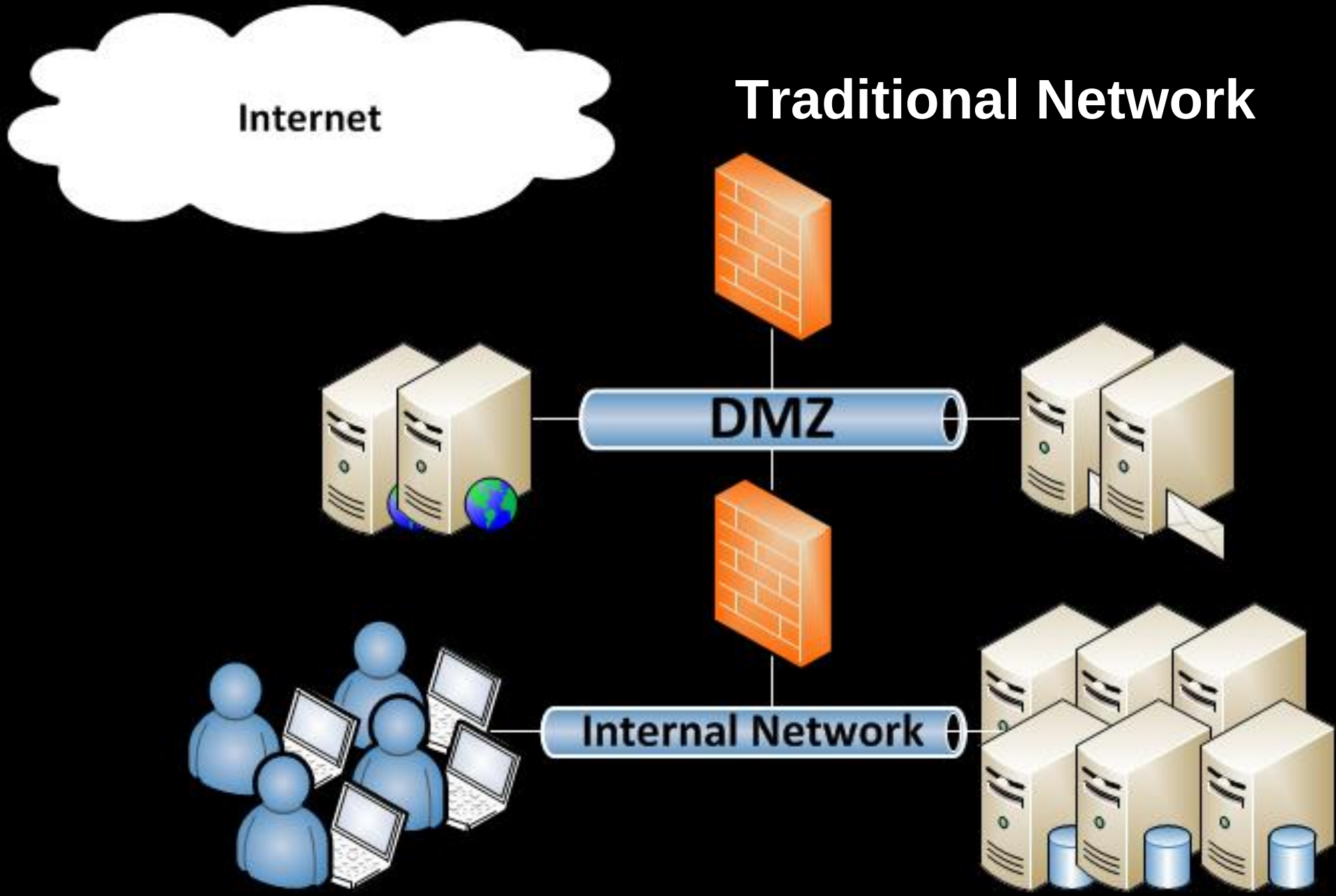
Test-signed Malware



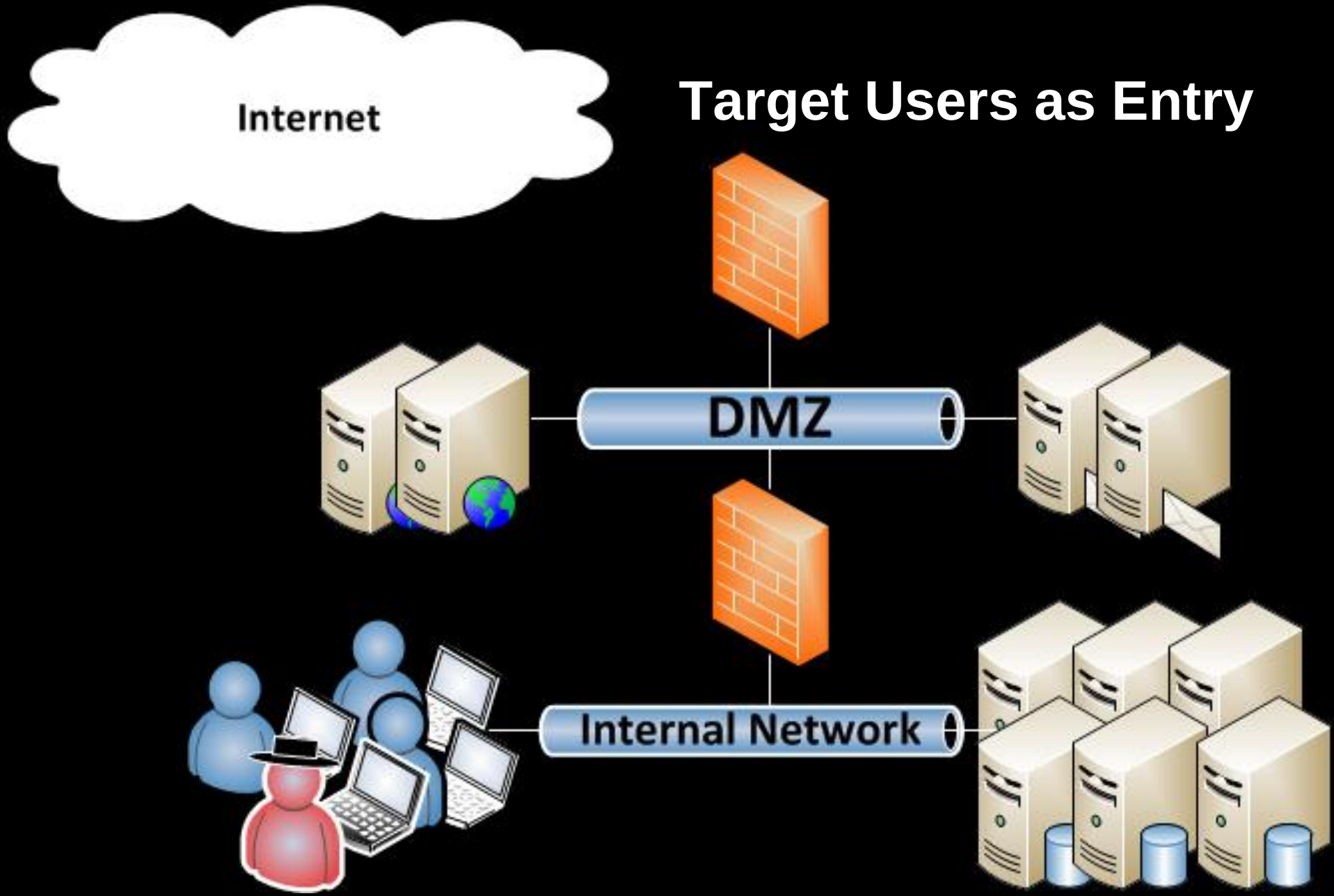
Top Network Attacks

73% of all attacks are browser-based, up from 44% last quarter

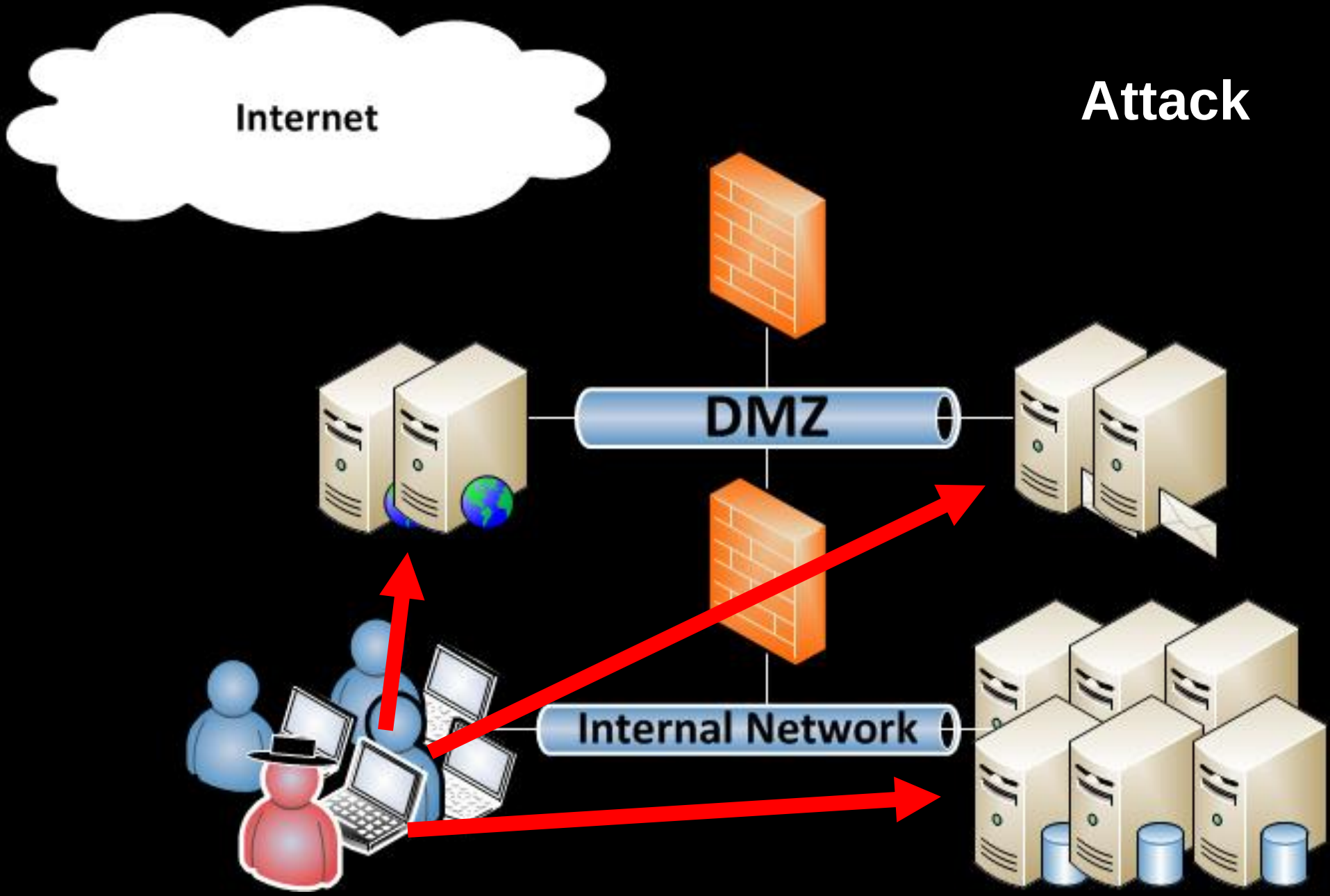
Traditional Network



Target Users as Entry

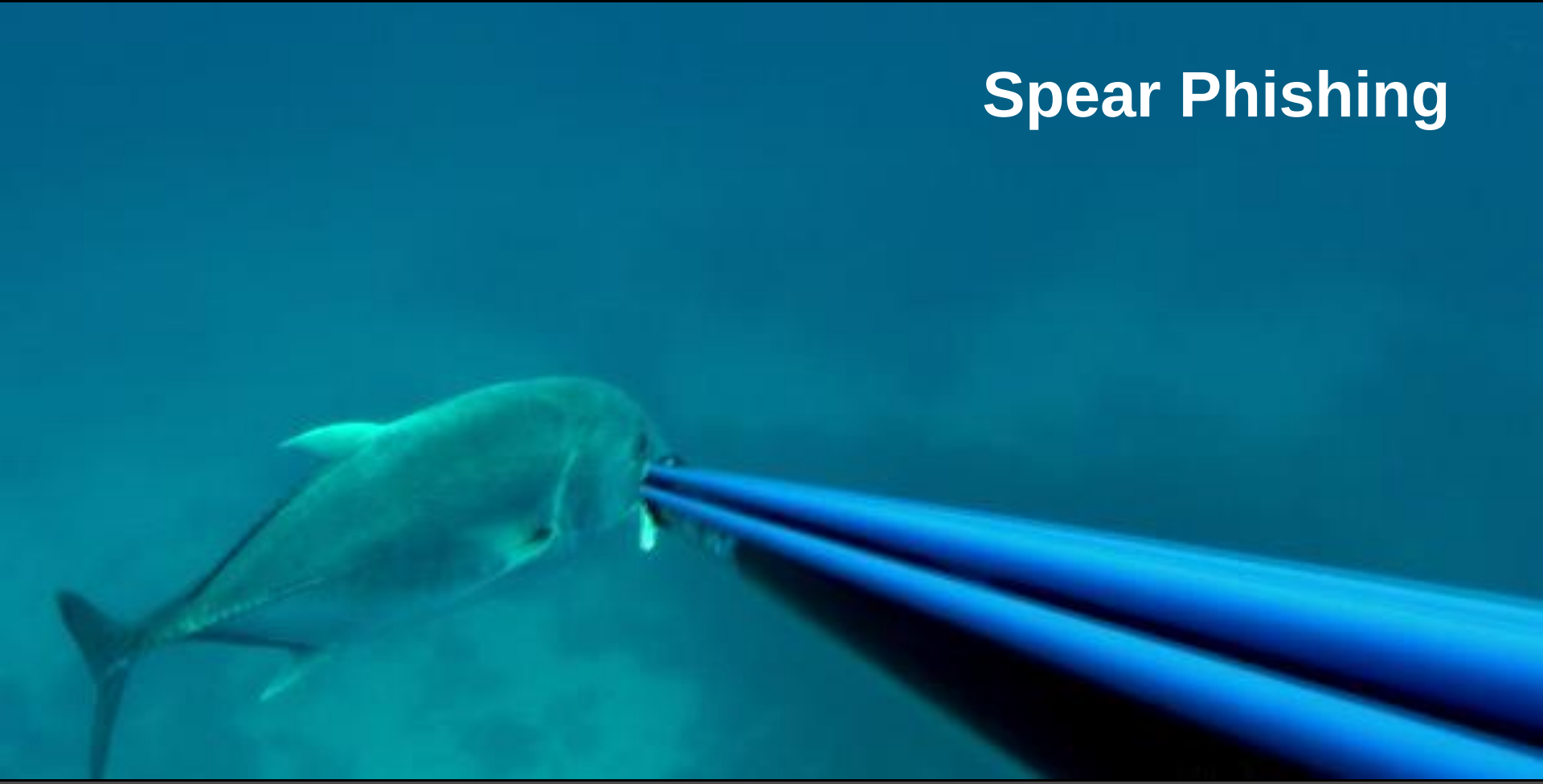


Attack



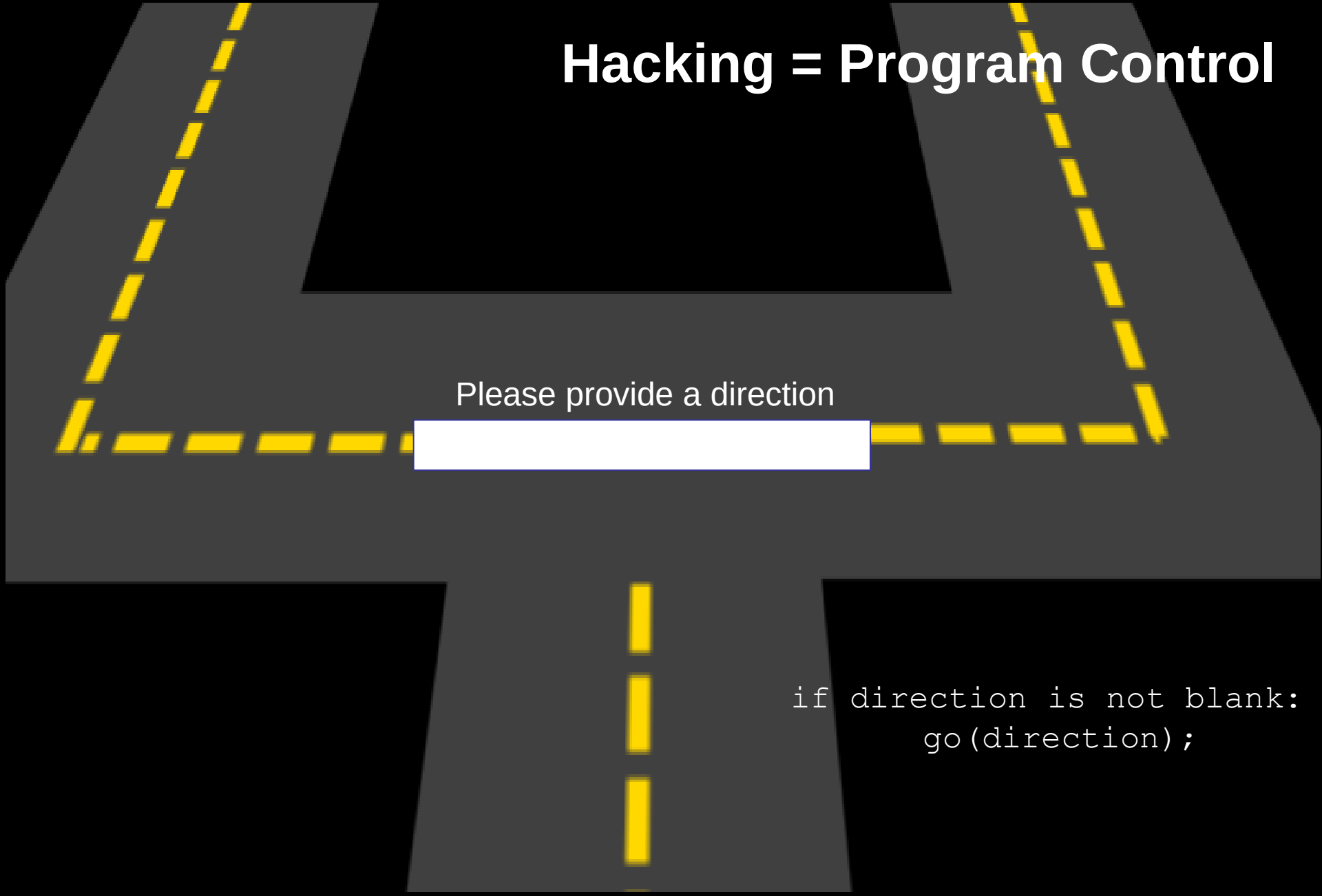
Sophisticated Attacks

Spear Phishing



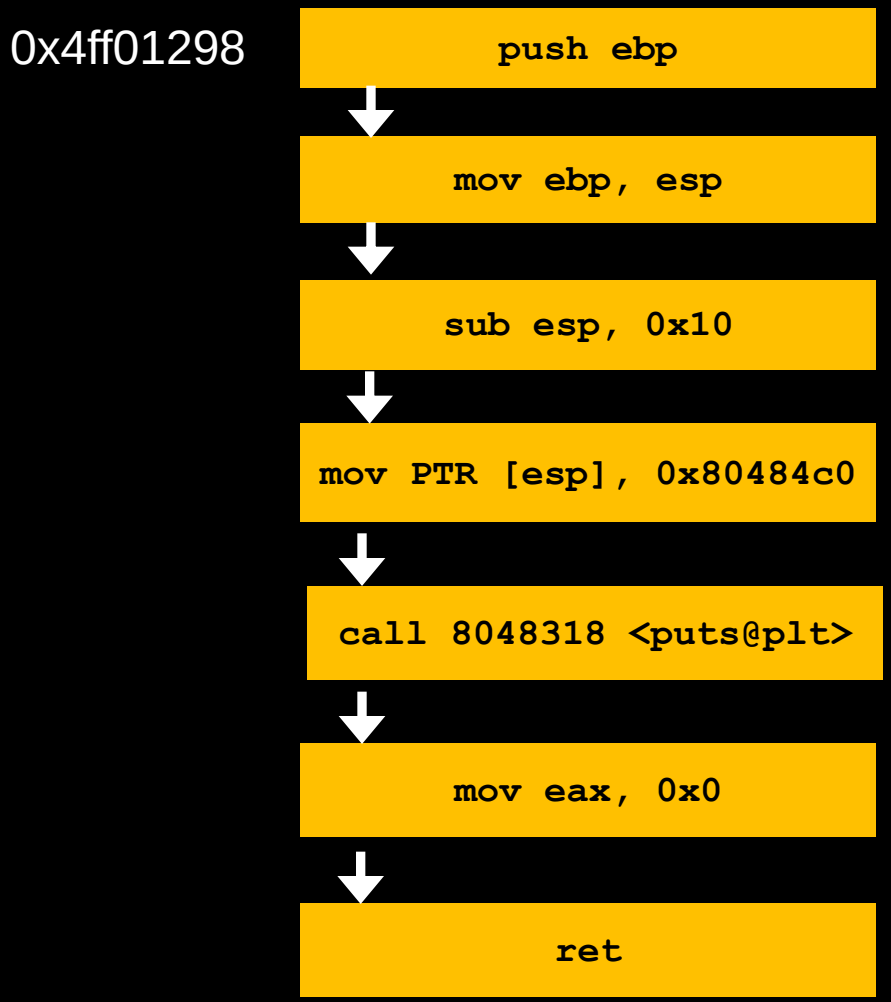
- Carefully crafted email targeting a specific user
- Contains malicious attachment or download link
- (also see watering hole, drive by download, etc..)

Hacking = Program Control

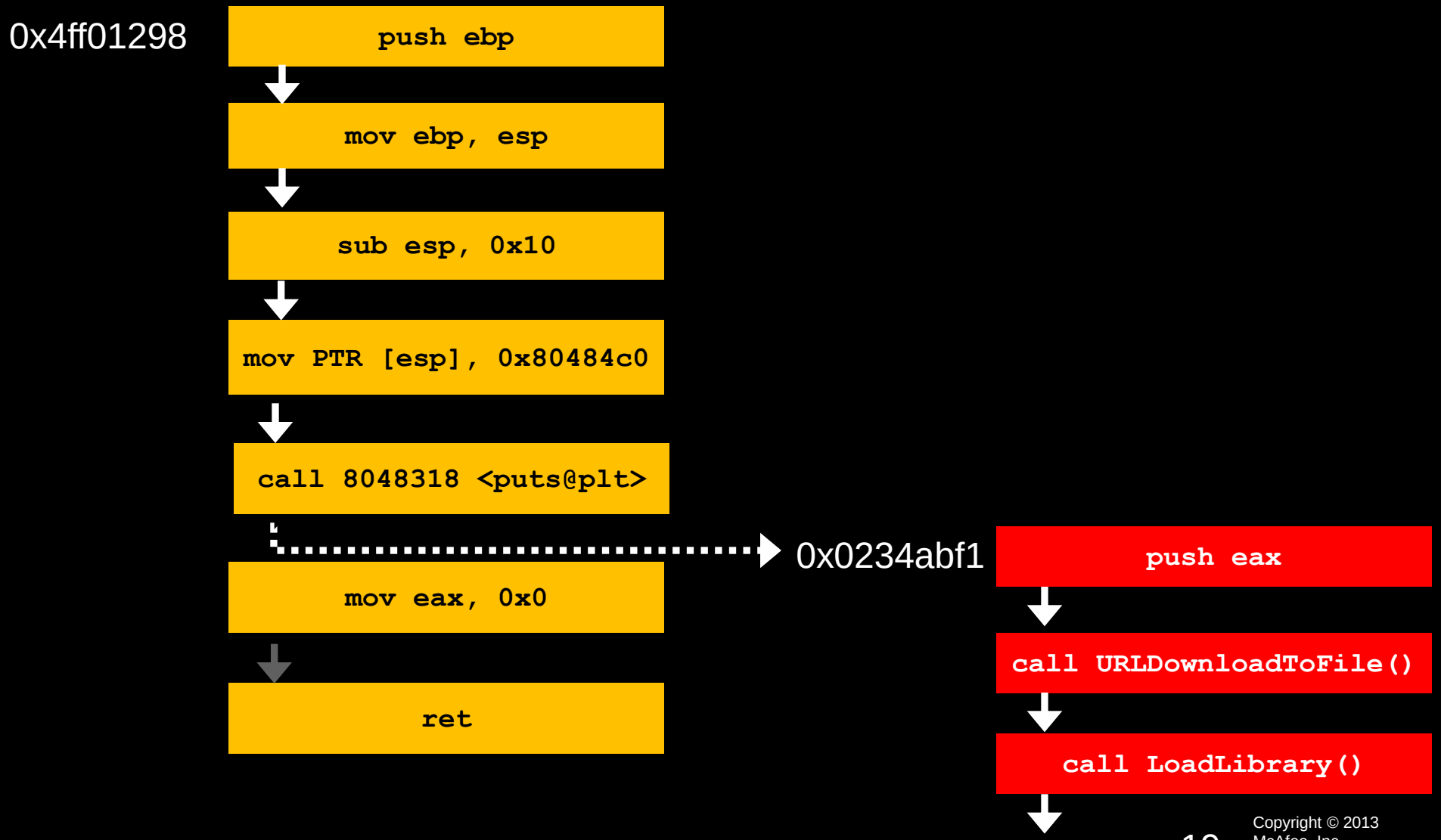



```
if direction is not blank:
    go(direction);
```

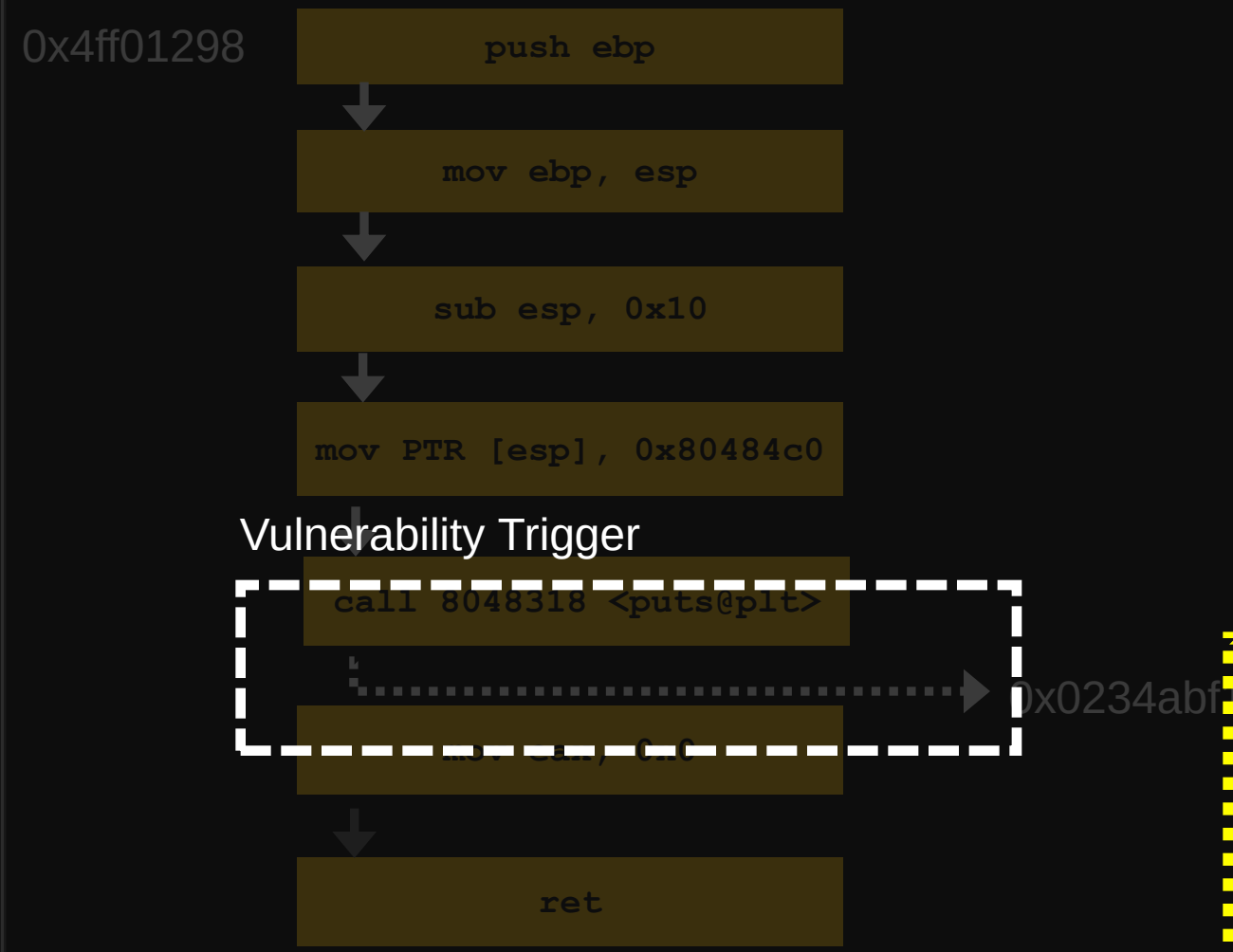
Typical Program



Anatomy of an Exploit

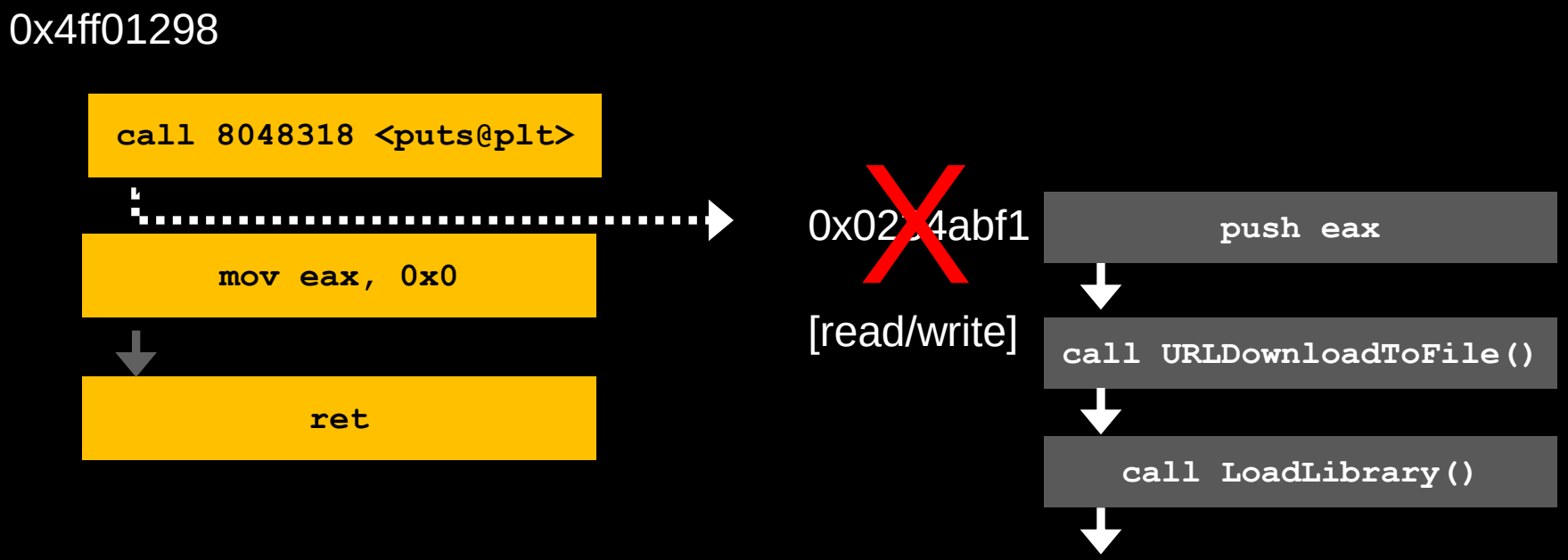


Anatomy of an Exploit

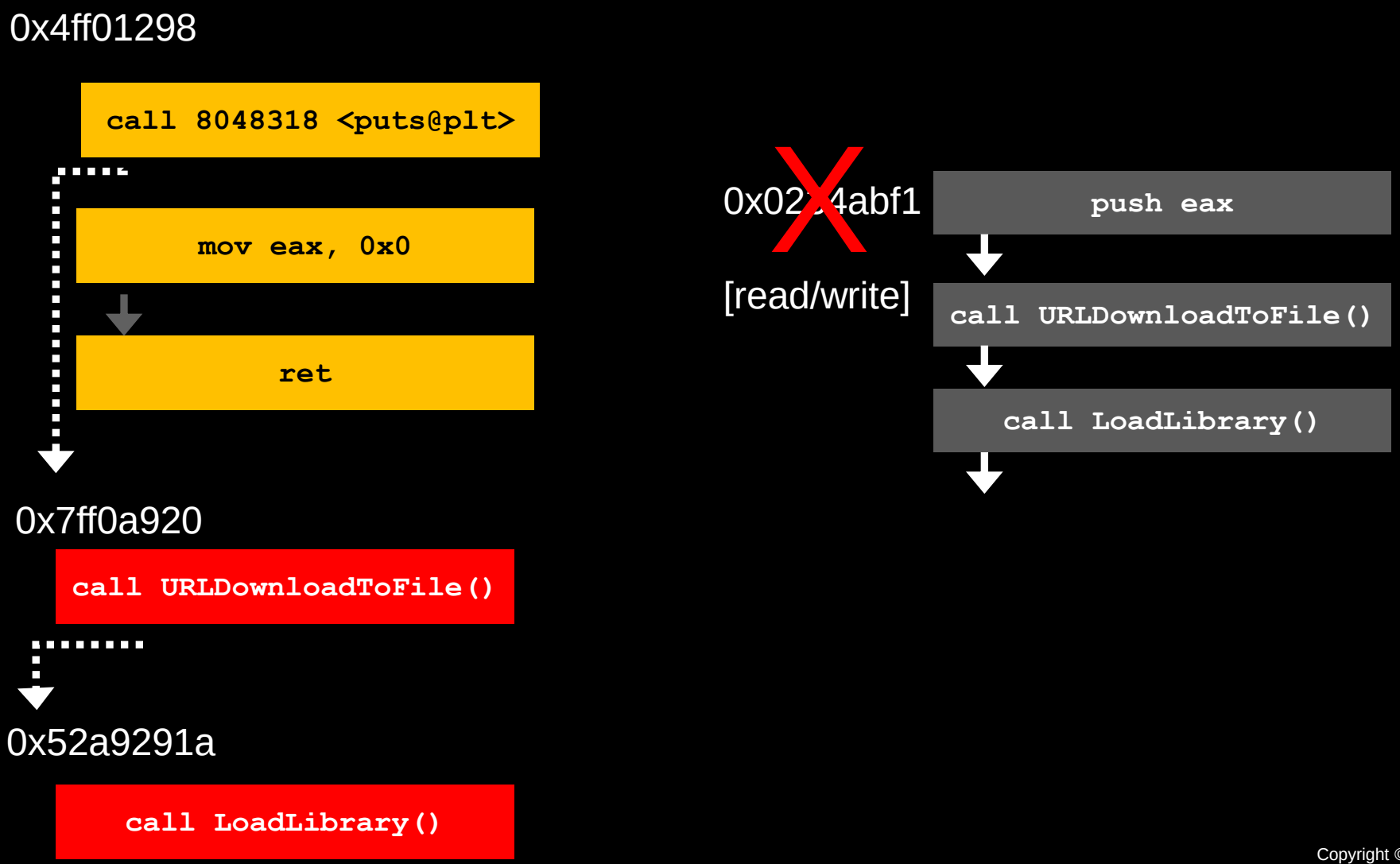


Exploit Mitigations

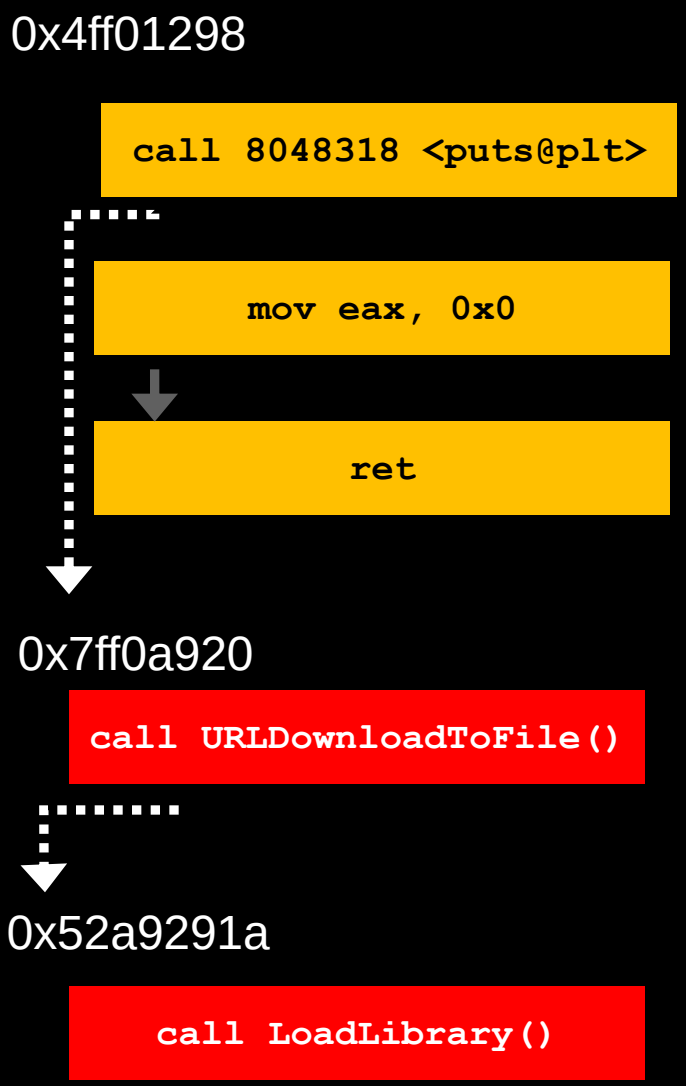
Data Execution Prevention (DEP)



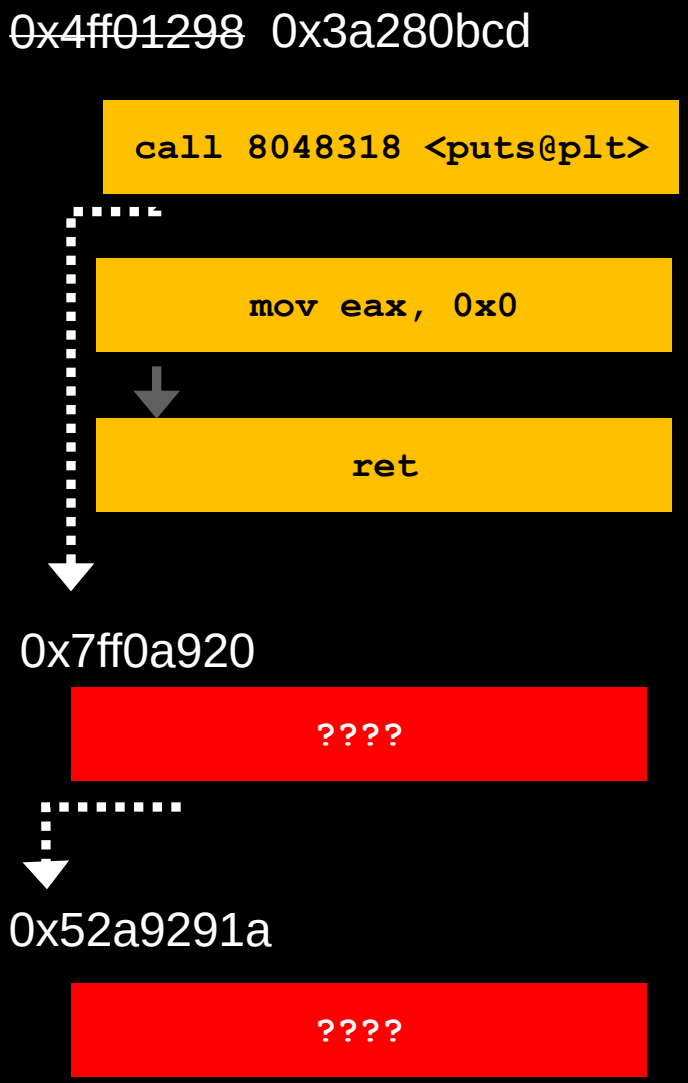
Data Execution Prevention (DEP)



Address Space Layout Randomization (ASLR)

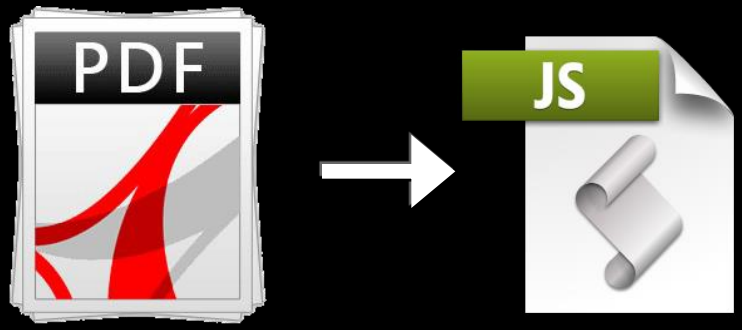


Address Space Layout Randomization (ASLR)

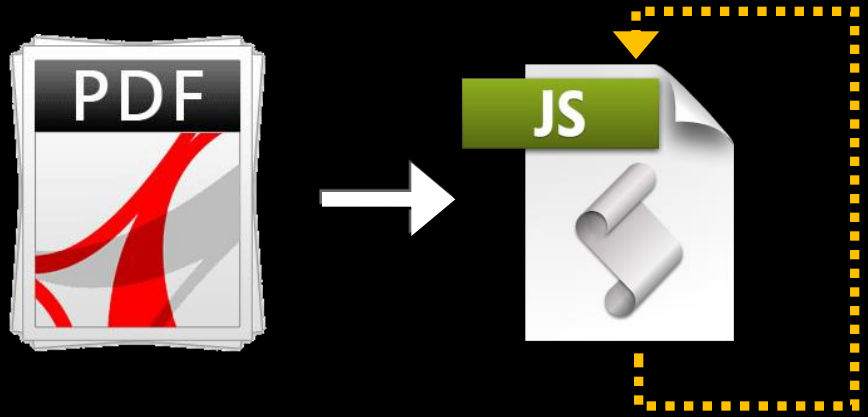


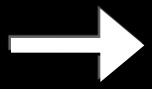
Case Study: CVE-2013-0640

- Code Execution Vulnerability
- Address Leak (to bypass ASLR)

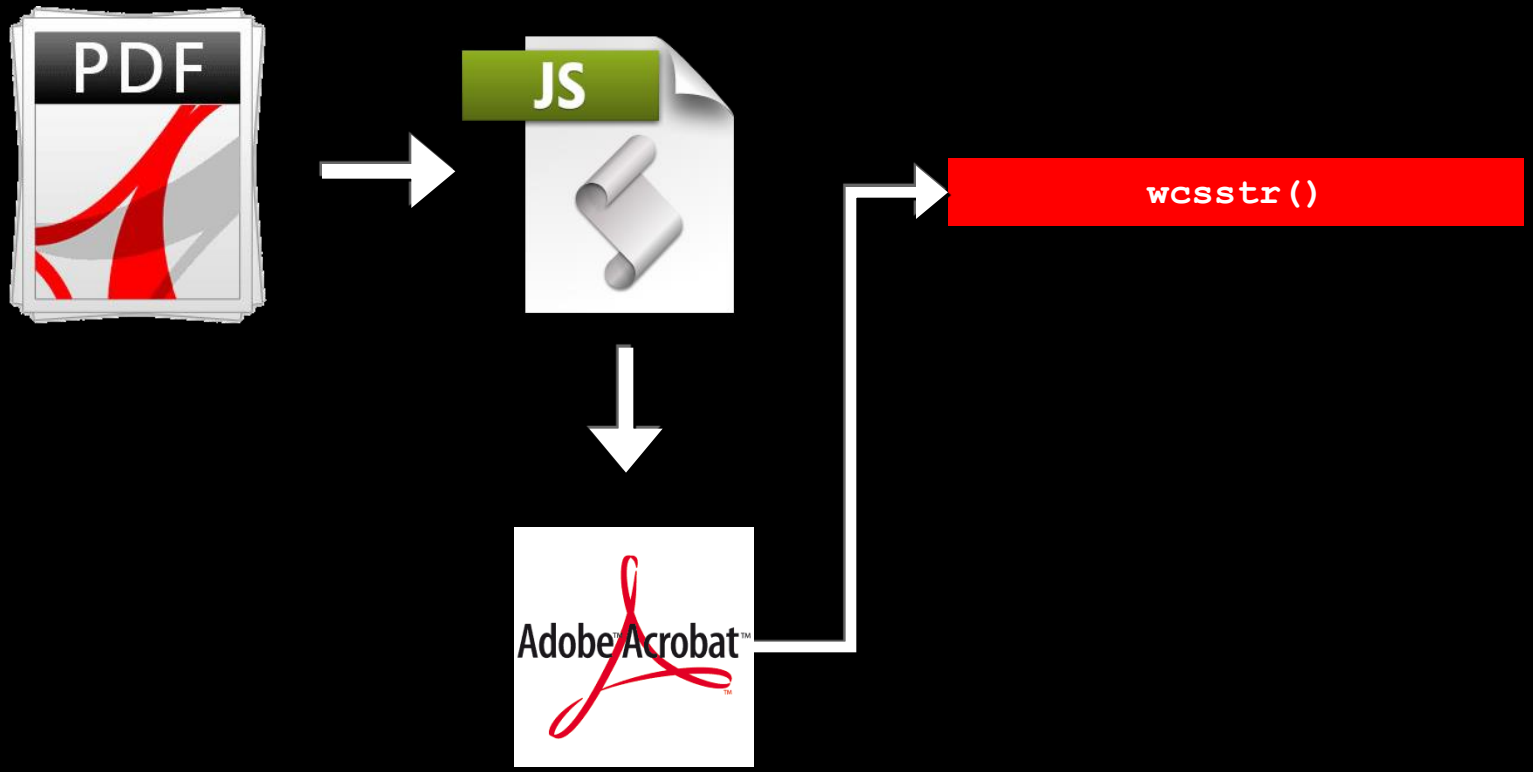


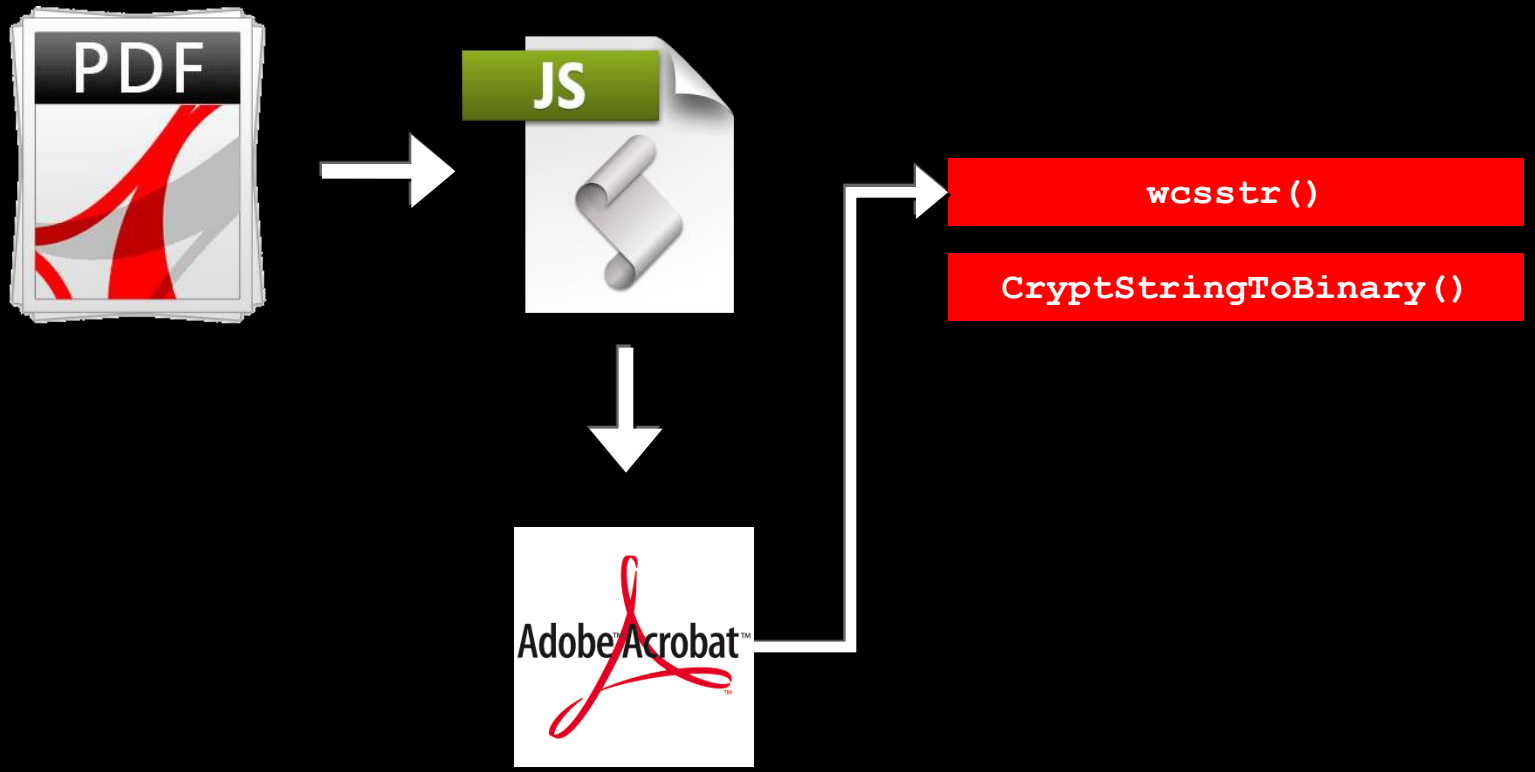
Triggers
Address Leak

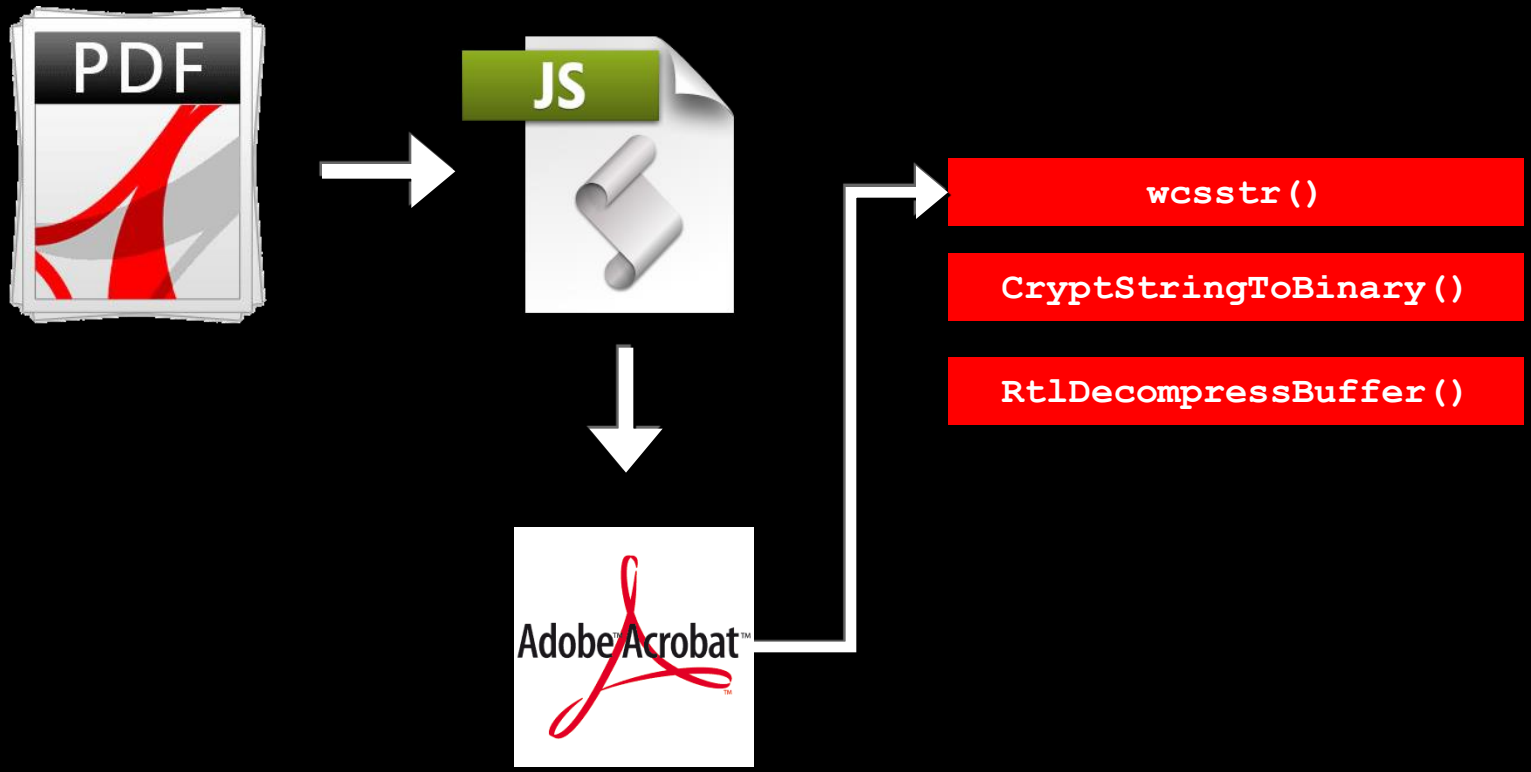


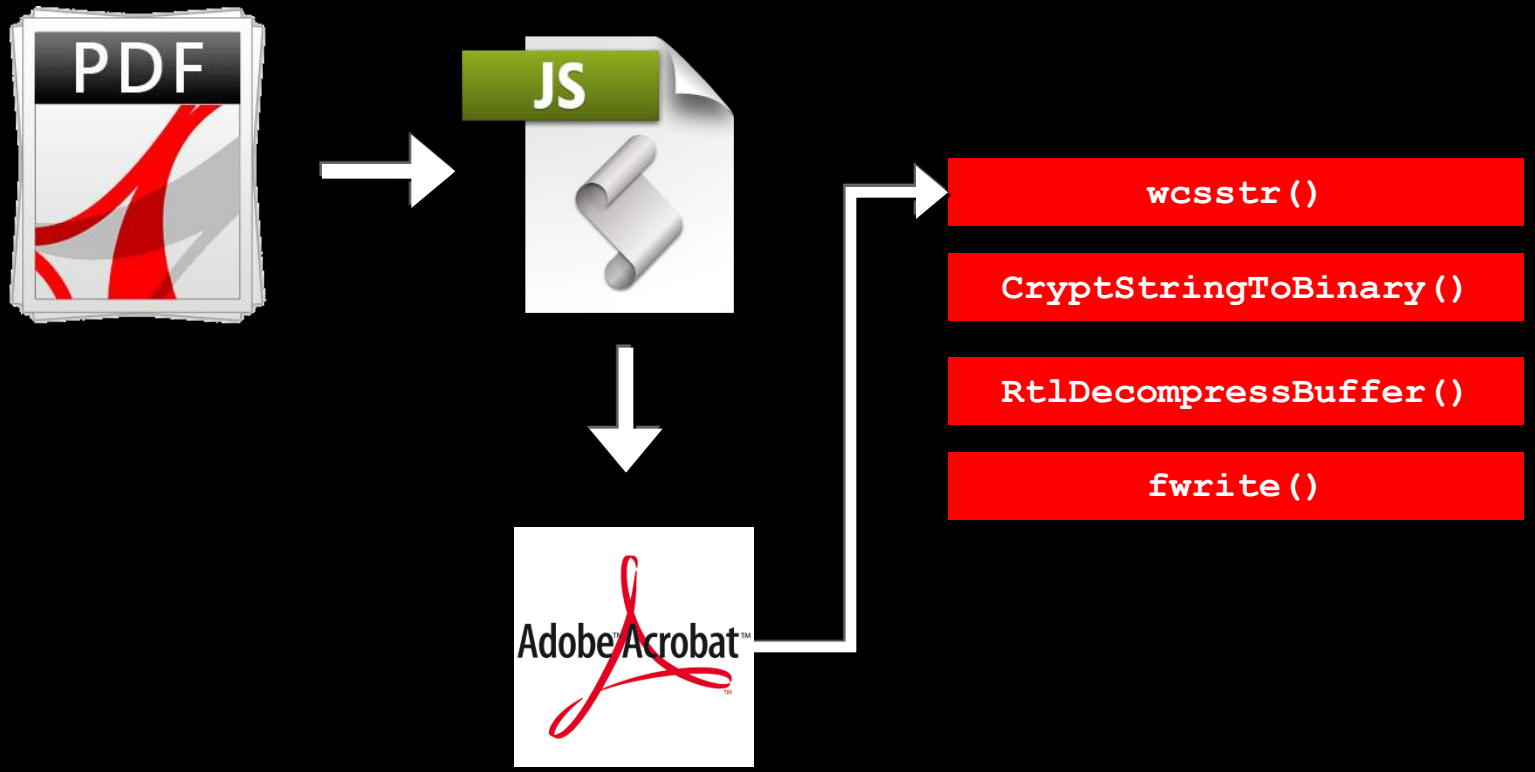


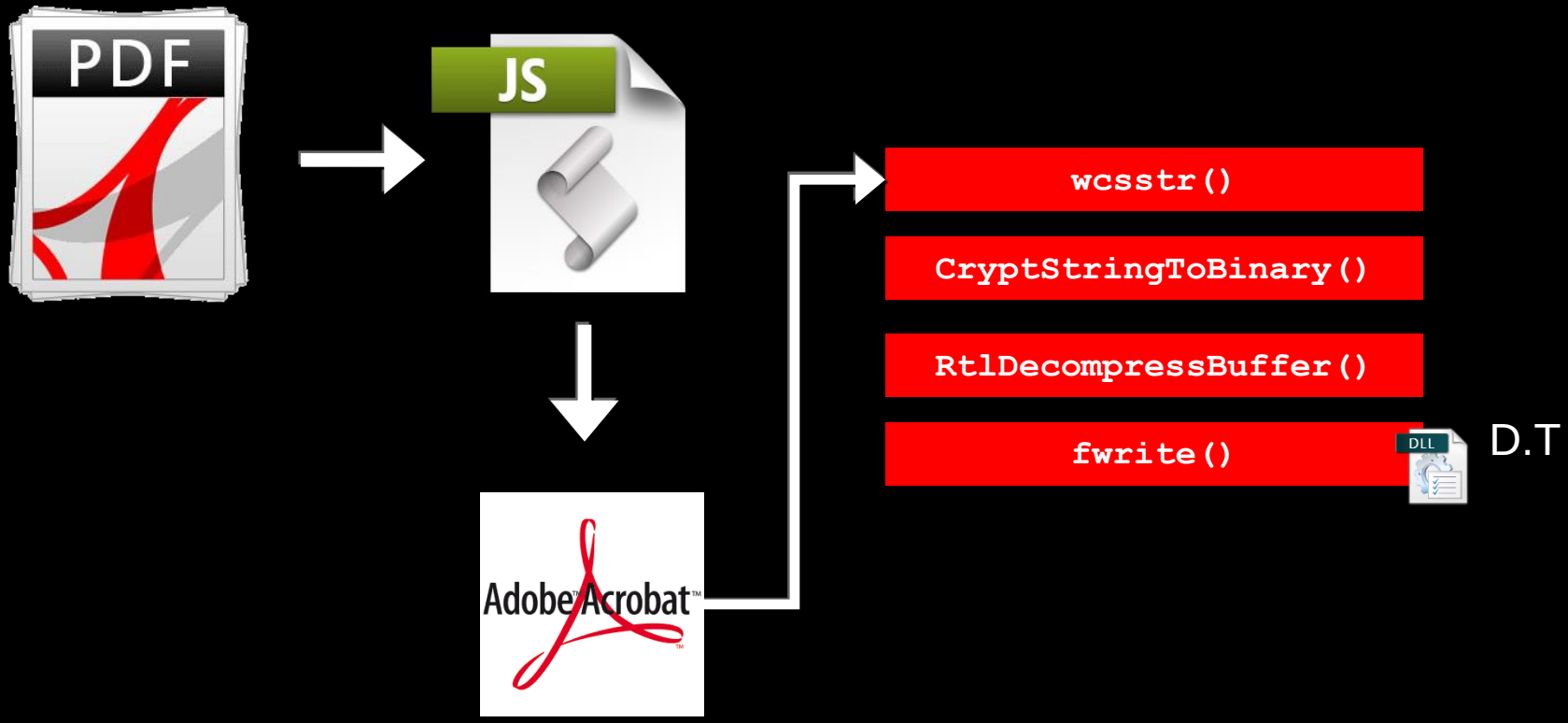
Triggers
Code execution

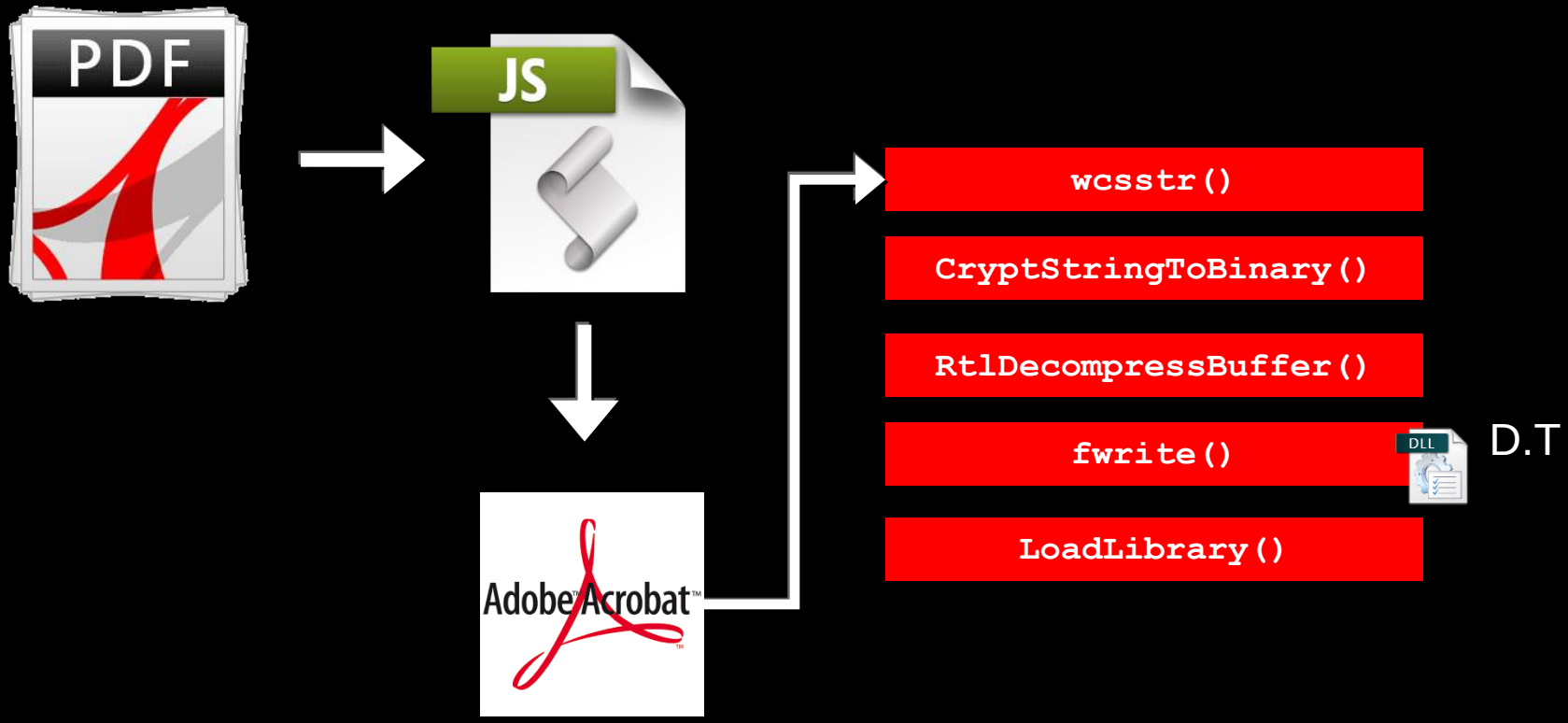


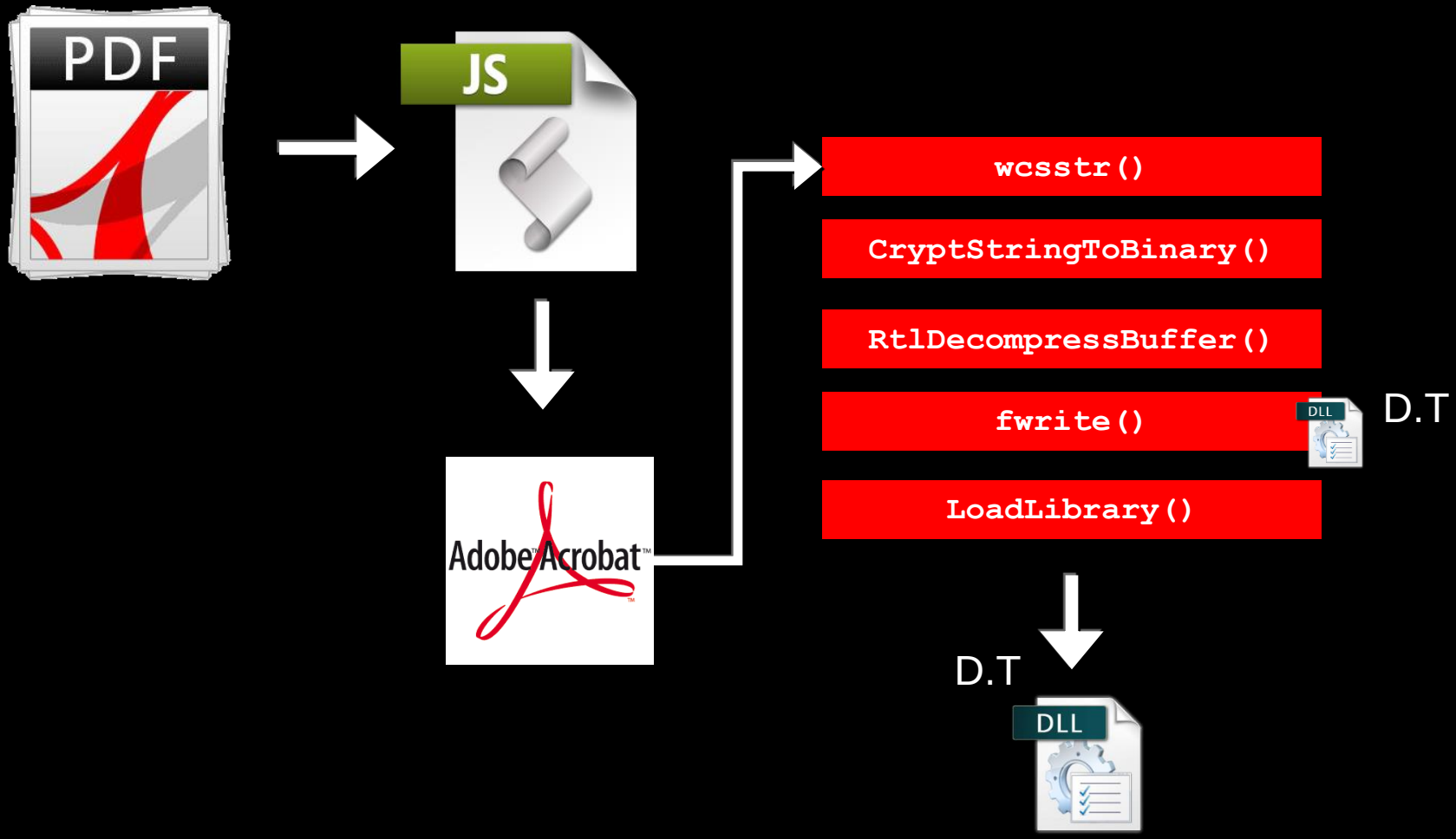


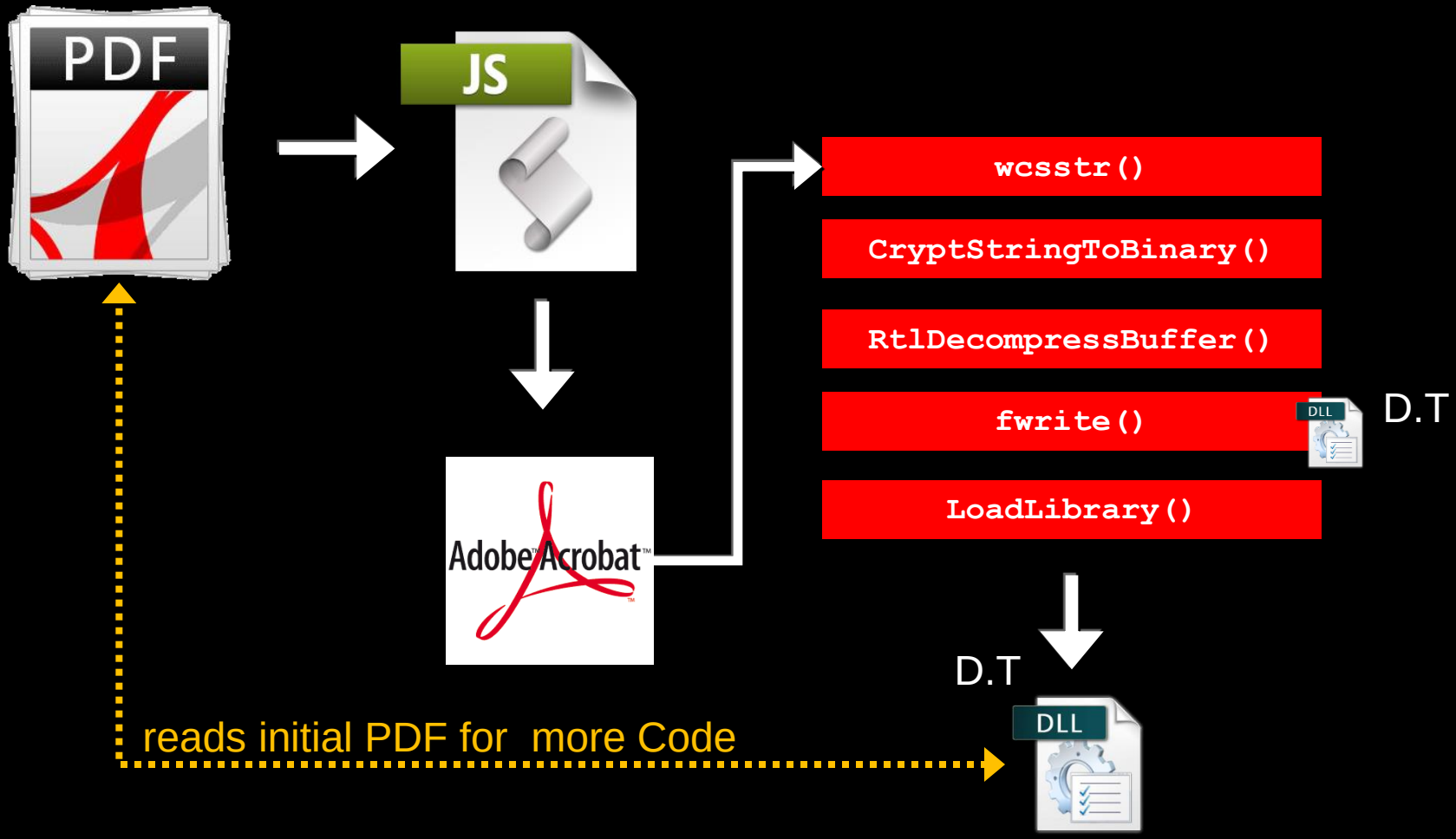












wcsstr()

CryptStringToBinary()

RtlDecompressBuffer()

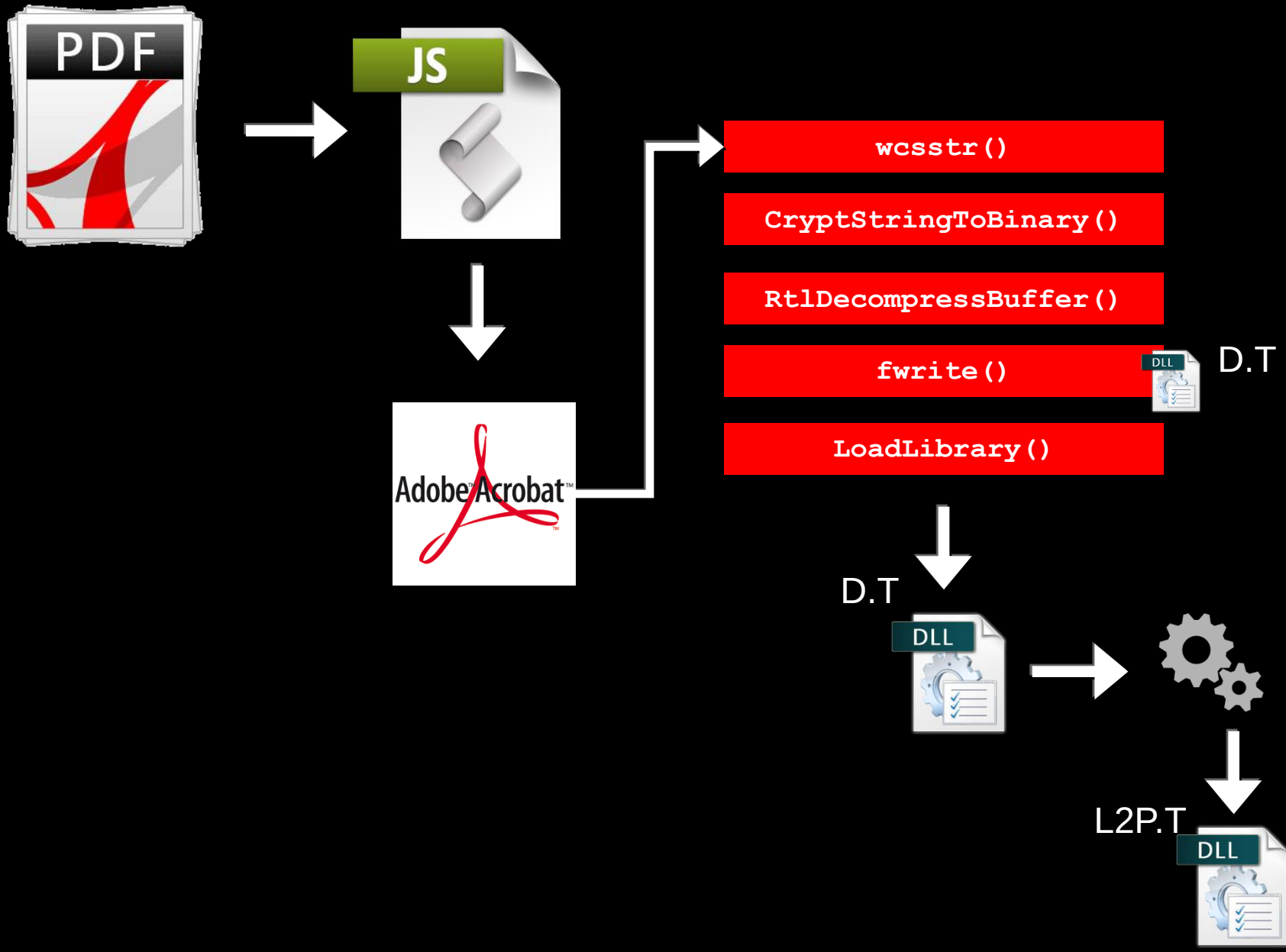
fwrite()

LoadLibrary()

D.T

D.T

Decrypts and Runs only in memory



?

@brad_anton

Brad.Antoniewicz@foundstone.com

*many of the pics in this presentation were found on the internet – credit goes to images.google.com