

Latest Threats and Trends

Brad Antoniewicz

Who am I?

Hi, I'm @brad_anton

ARRESTED DURING HAIRCUT



**DAVID
DAVIS**

In the news

David Davis was in the middle of a haircut when he got into a scuffle and was then arrested. [Read More](#)

April 5, 2013

san francisco

my vouchers

log in

sign up

livingsocial

deals

escapes

fun & events

shop

takeout & delivery

important notice for customers

if you haven't already updated your LivingSocial password, please update it now

[create new password](#)

top san francisco deals

all deals

activities

families

food and drink

health and beauty

at home

online deals

★ featured deal

🔥 popular

🔥 popular

↗ most shared



50 Million customers



Compliance Assistance

Regulatory Library

About OWCP

OWCP Programs

- DFEC
- DEEOIC
- DLHWC
- DCMWC

Contact OWCP

OWCP Customer Assistance

EEOICP Site Exposure Matrices Website -- Home Page DOE FACILITIES AND RECA SITES DATA

UPDATED AS OF JANUARY 11, 2013

The Department of Labor (DOL) Site Exposure Matrices (SEM) Website is a repository of information gathered from a variety of sources regarding toxic substances present at Department of Energy (DOE) and Radiation Exposure Compensation Act (RECA) facilities covered under Part E of the Energy Employees Occupational Illness Compensation Program Act (EEOICPA). In putting together SEM, DOL held round table meetings with workers from DOE facilities all over the country and gathered their input on the hazards at these sites. DOL also obtained copies of thousands of documents from DOE regarding toxic substances at those facilities.

In addition to toxic substance information, the SEM Website also contains information regarding scientifically established links between toxic substances and illnesses. Displayed links for diagnosed illnesses show how these correlate to toxic substance exposures. The relationship between toxic substances and diagnosed illnesses shown in SEM is derived from the Haz-Map database published by the National Library of Medicine

(<http://hazmap.nlm.nih.gov/index.html>). DOL continually updates these relationships to reflect new disease associations published in Haz-Map. The causal links shown in SEM do not represent an exclusive list of the pathways necessary for an affirmative Part E causation determination. Every disease entered into the SEM database is a disease for which there is evidence that SEM does not address the relationship between radiation and cancer. For purposes of EEOICPA, the relationship between radiation and cancer is evaluated by the National Institute for Occupational Safety and Health (NIOSH).

Highlights

DOL WANTS YOUR INPUT!

The Department of Labor welcomes your input to the Site Exposure Matrices. If you have unclassified information that you would like to have considered for use in the Matrices, please submit it using this button:

[Submit Site-Related Information](#)

[Submit Disease-Related Information](#)

Review updates and status of the public input regarding site- and disease-related information on the SEM Website:

[Status of site-related input](#)

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

Подую сорцы карберп., Пост в лучших традициях вики ликс.

Подписка на тему | Соо

madeinrm

Вчера, 20:26

Ньюббн

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

Репутация: нет
(0%)

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 сопровождаться подтверждением личности на ряде не безизвестных площадок.

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 карберп включая комментарии к нему.
- инъекты.
- все модули продукта.
- исходный код RDPxTerm.
- исходный код RDPxTerm (популярный аналог).
- административную панель карберп (без ион куба).
- отлаженные билдеры всех версий.

- CVE-2012-1864

- CVE-2012-1864

- Биткит.

и многое другое.

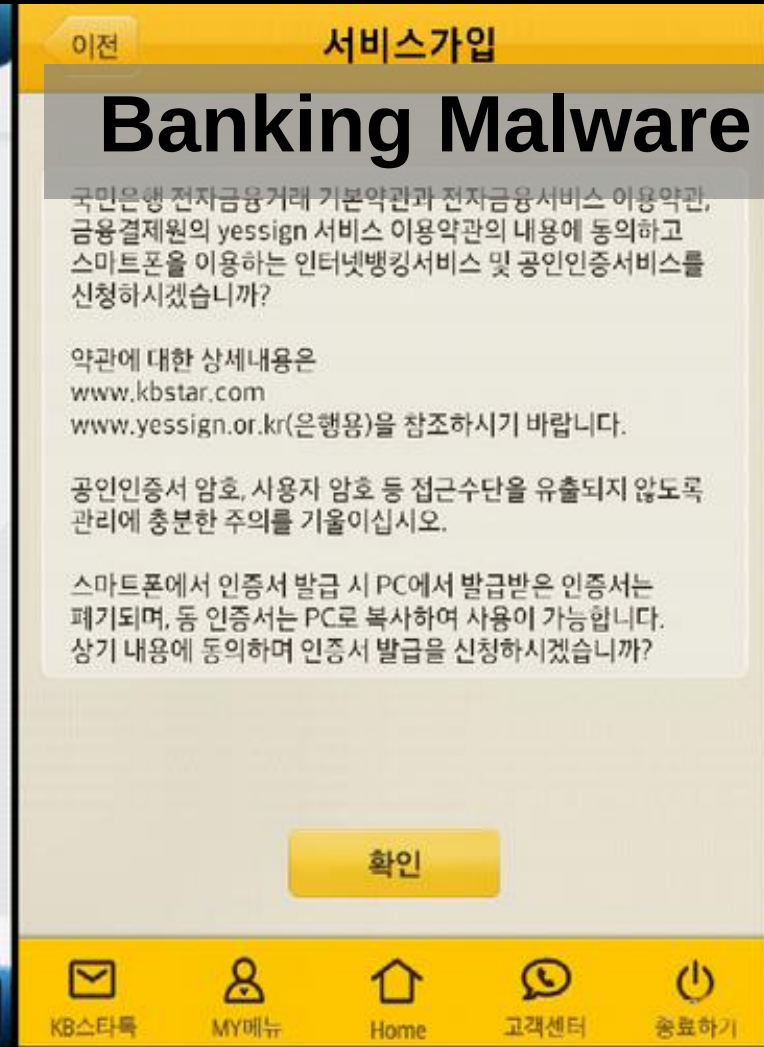
Весь архив доступен только для тех кто купил

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



Android/FakeBankDropper.A

- SMS Phish via FSC
- Replaces official App

- Collects phone logs
- Requests private info



ATTENTION !

IP: [REDACTED]
 Location: [REDACTED]
 IPS: [REDACTED]

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 1, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article 1, 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.

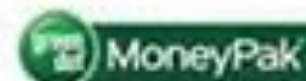
You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

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

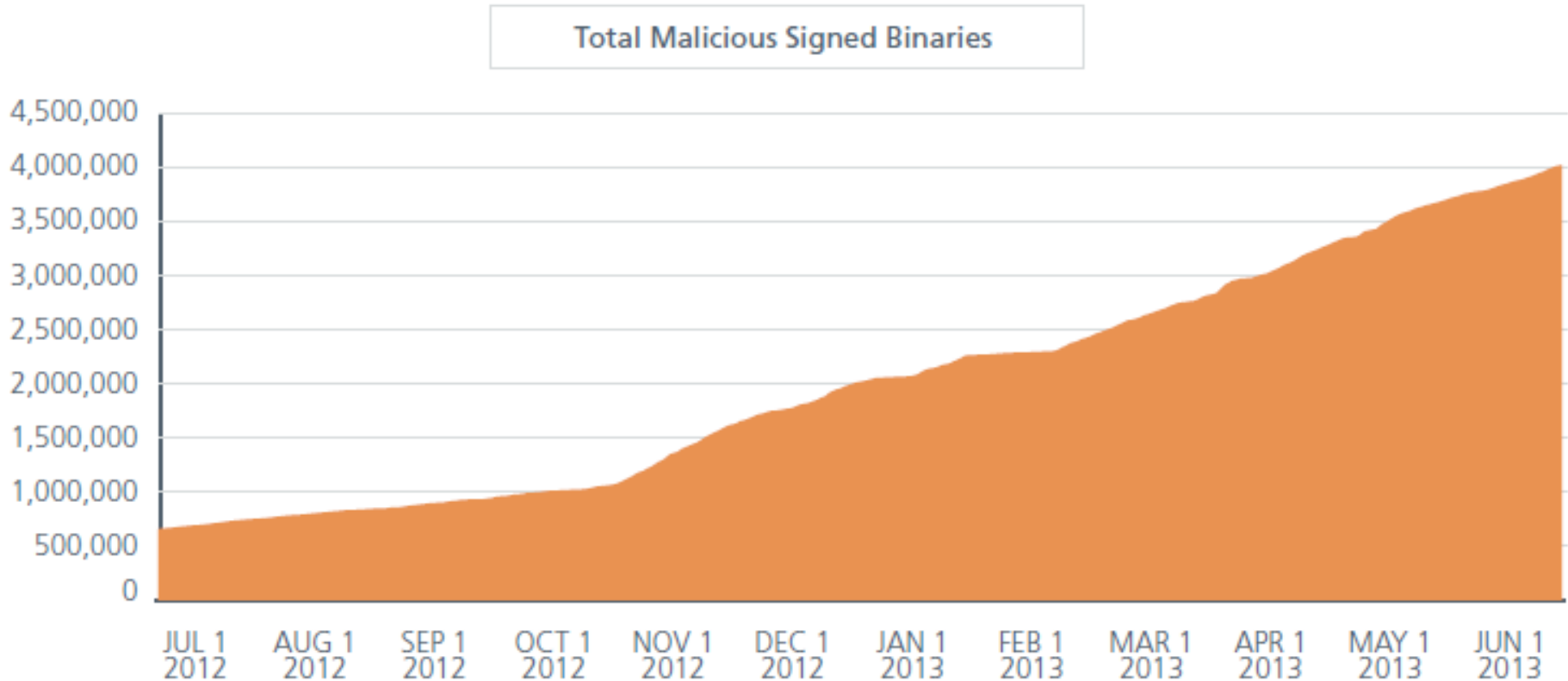


Code:

Sum:

Pay MoneyPak

Signed Malware

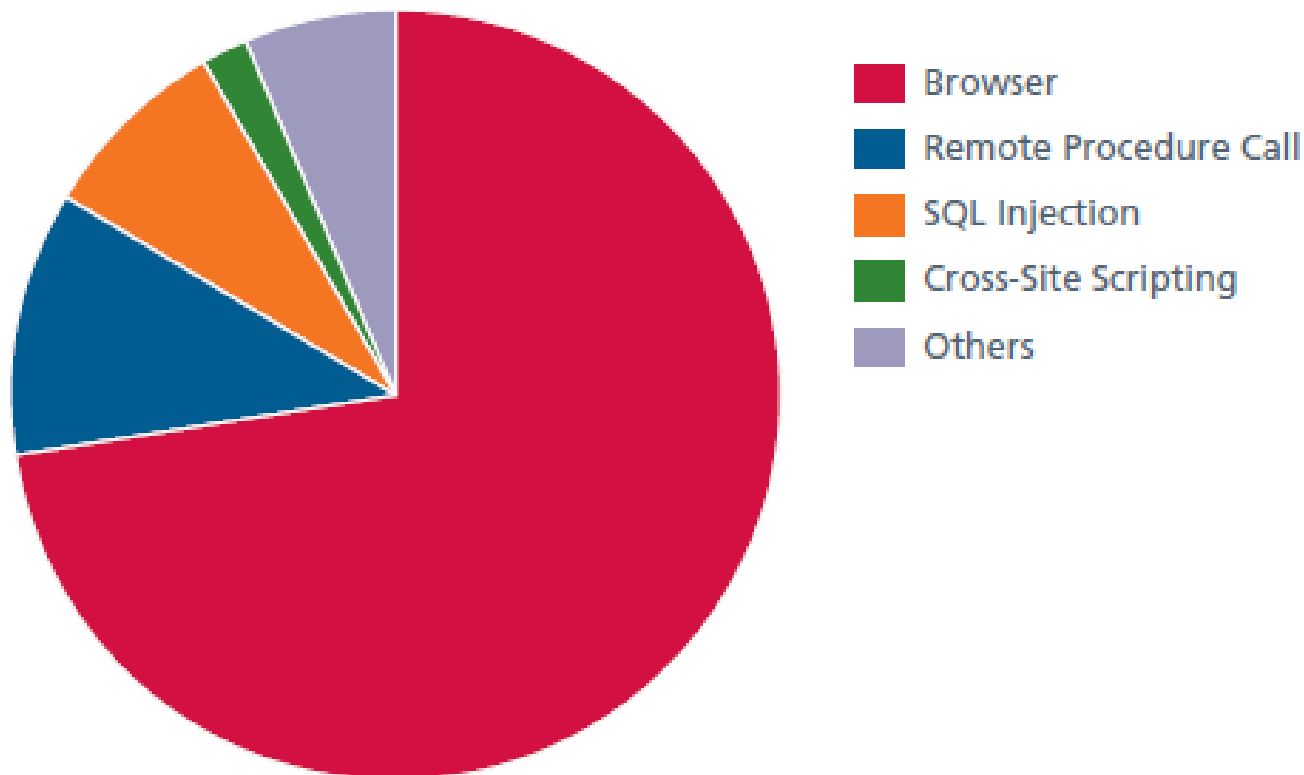


Stolen Certificates

Test-signed Malware

Top Network Attacks

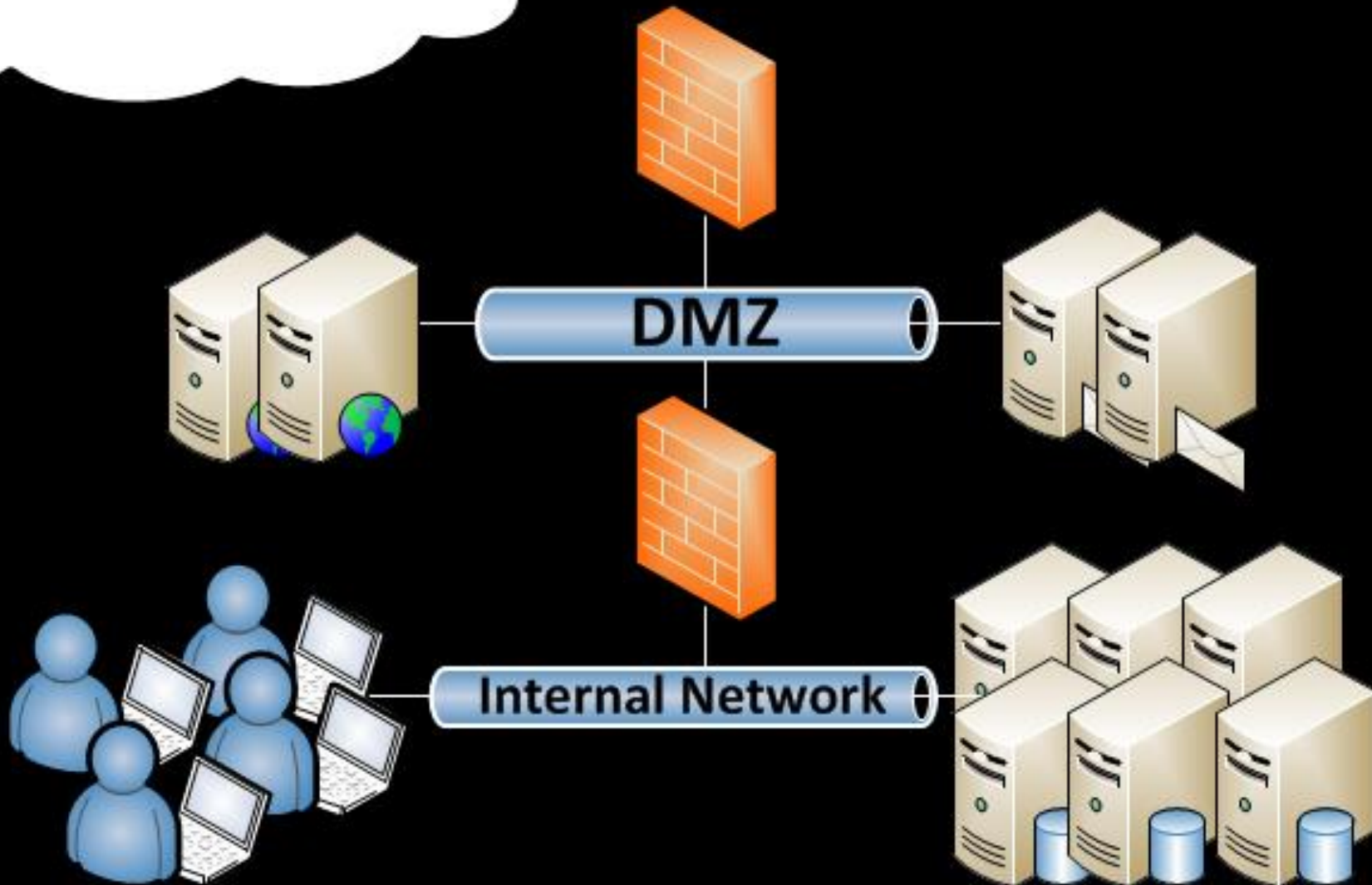
Top Network Attacks



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

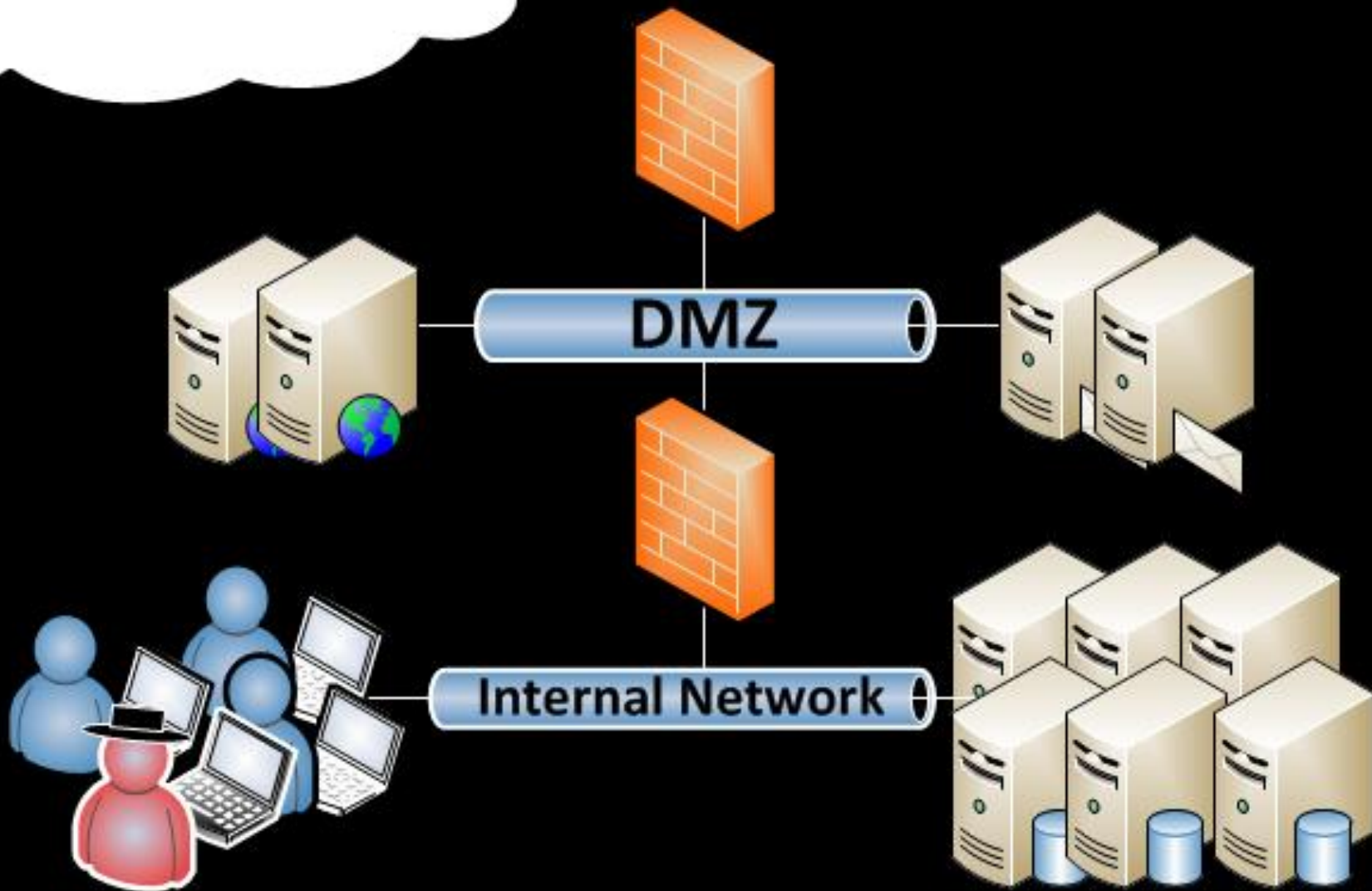
Traditional Network

Internet



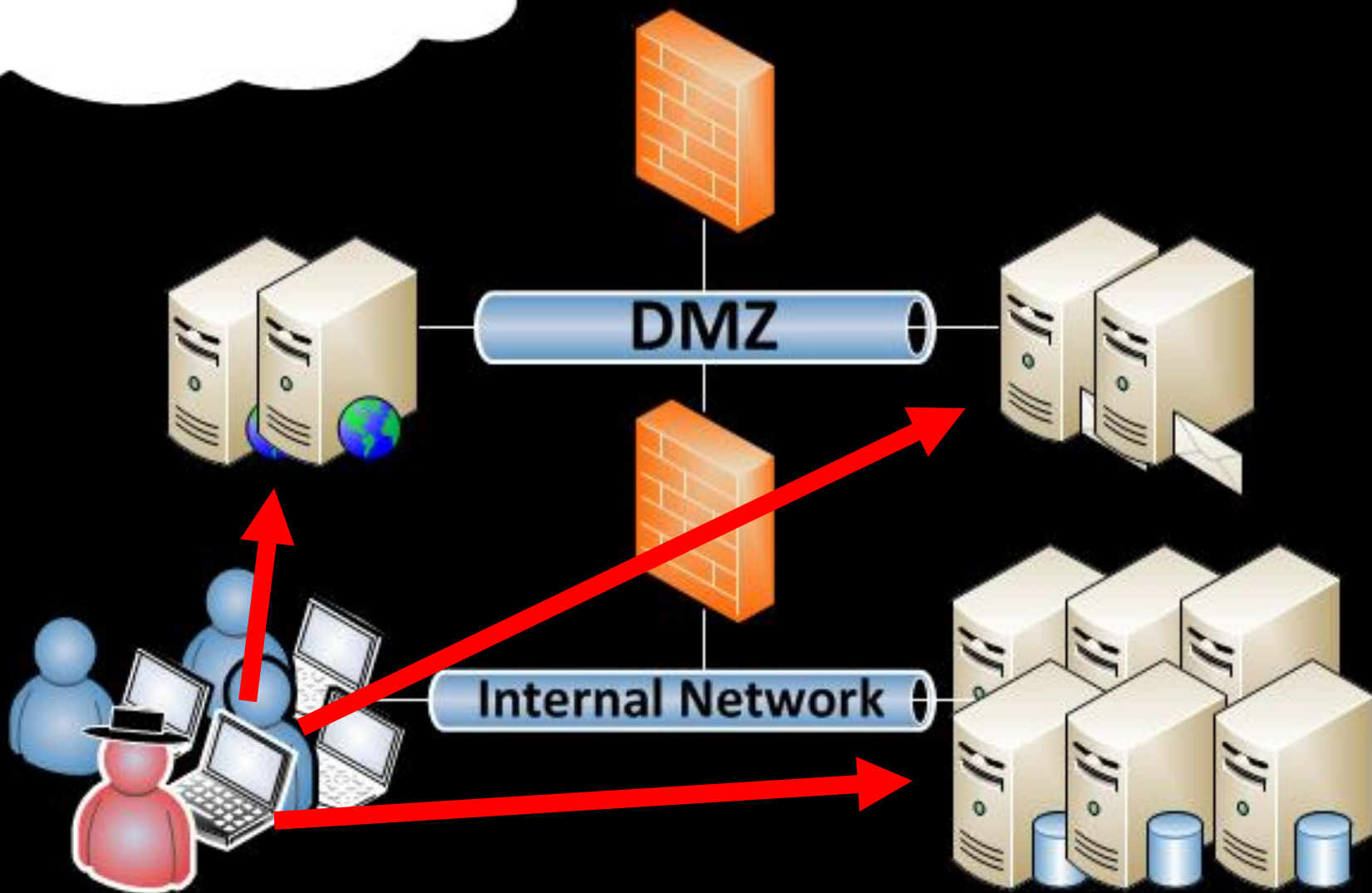
Internet

Target Users as Entry



Internet

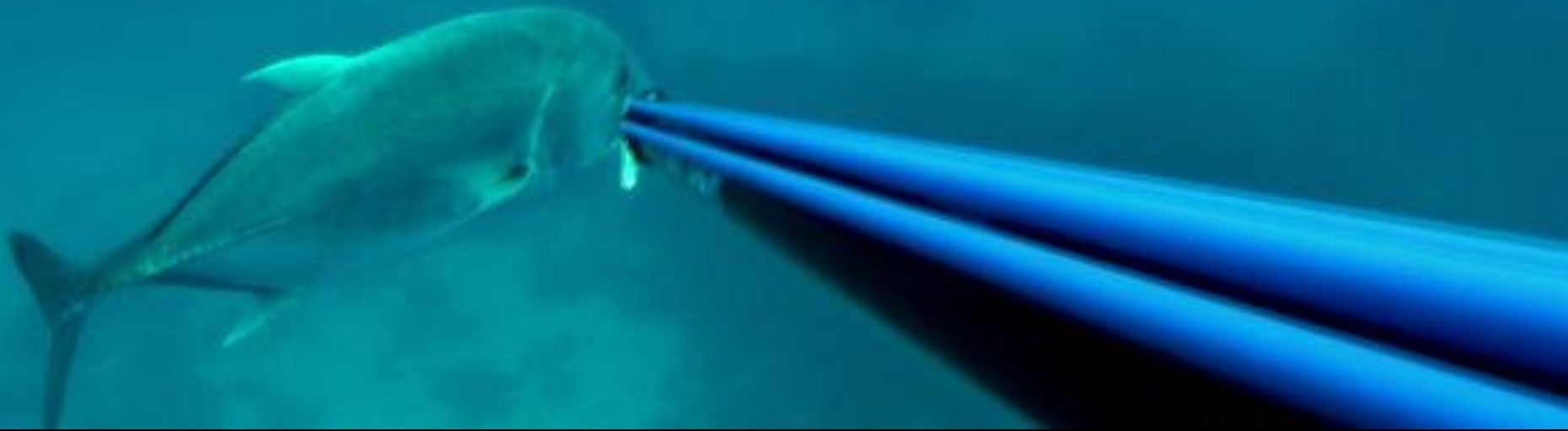
Attack



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

Please provide a direction



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

Typical Program



Anatomy of an Exploit



Anatomy of an Exploit

0x4ff01298



0x0234abf1

Payload

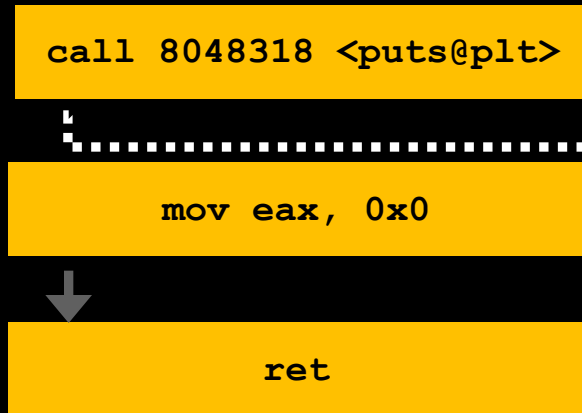


Exploit Mitigations

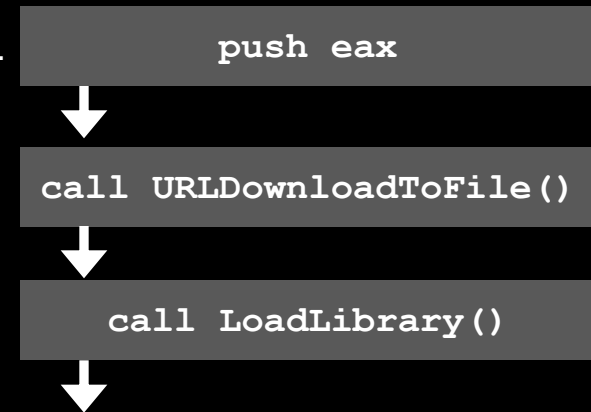


Data Execution Prevention (DEP)

0x4ff01298



~~0x024abf1~~
[read/write]



Data Execution Prevention (DEP)

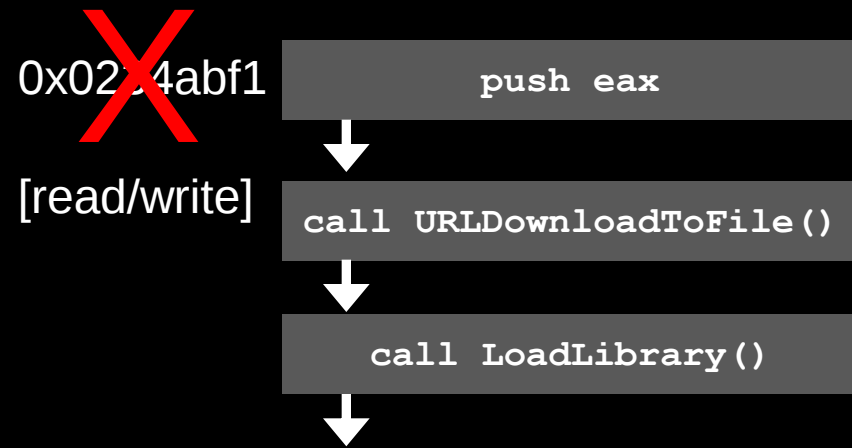
0x4ff01298



0x7ff0a920



0x52a9291a



Address Space Layout Randomization (ASLR)

0x4ff01298

```
call 8048318 <puts@plt>
```

```
mov eax, 0x0
```

```
ret
```

0x7ff0a920

```
call URLDownloadToFile()
```

0x52a9291a

```
call LoadLibrary()
```

Address Space Layout Randomization (ASLR)

0x4ff01298 0x3a280bcd

call 8048318 <puts@plt>

mov eax, 0x0

ret

0x7ff0a920

????

0x52a9291a

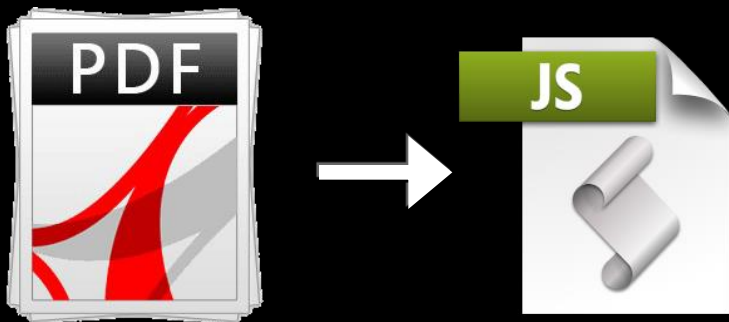
????

Case Study: CVE-2013-0640



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

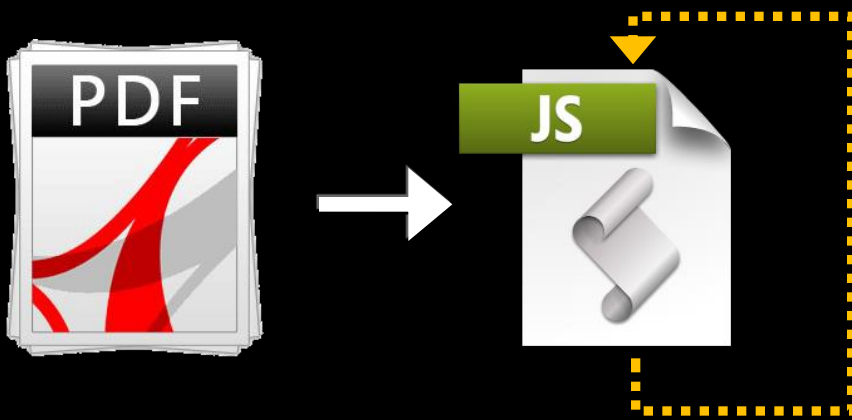






Triggers
Address Leak

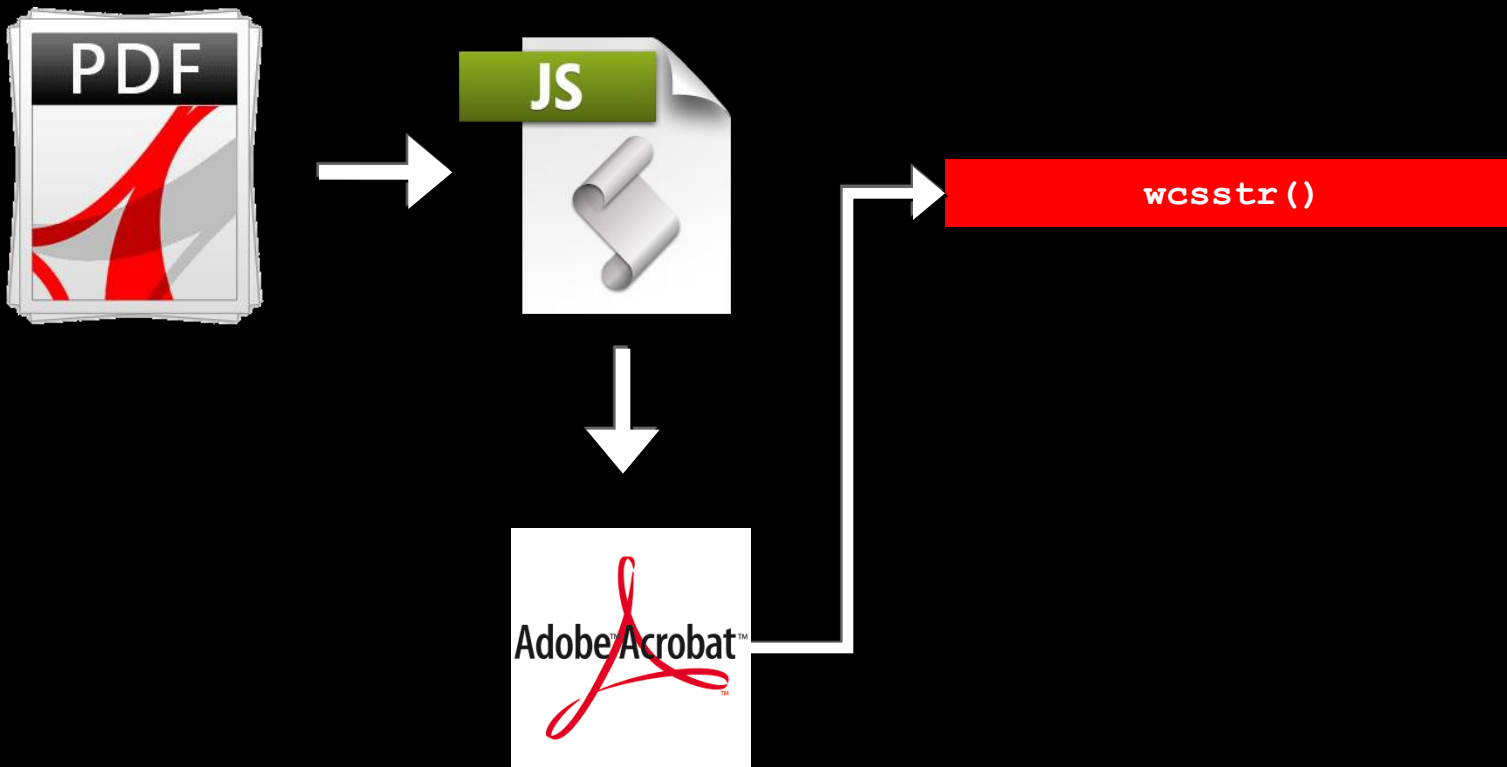


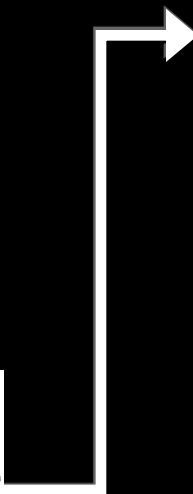




Triggers
Code execution

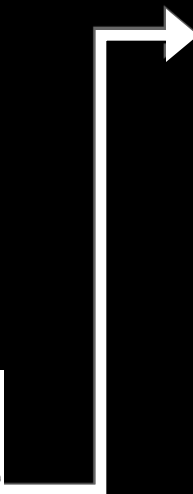






`wcsstr()`

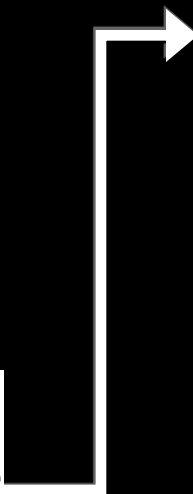
`CryptStringToBinary()`



`wcsstr()`

`CryptStringToBinary()`

`RtlDecompressBuffer()`

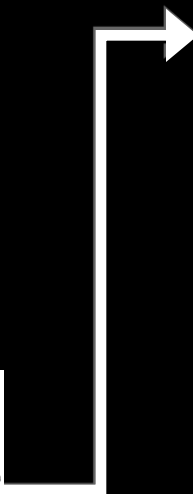


`wcsstr()`

`CryptStringToBinary()`

`RtlDecompressBuffer()`

`fwrite()`



`wcsstr()`

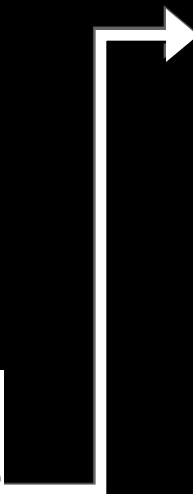
`CryptStringToBinary()`

`RtlDecompressBuffer()`

`fwrite()`



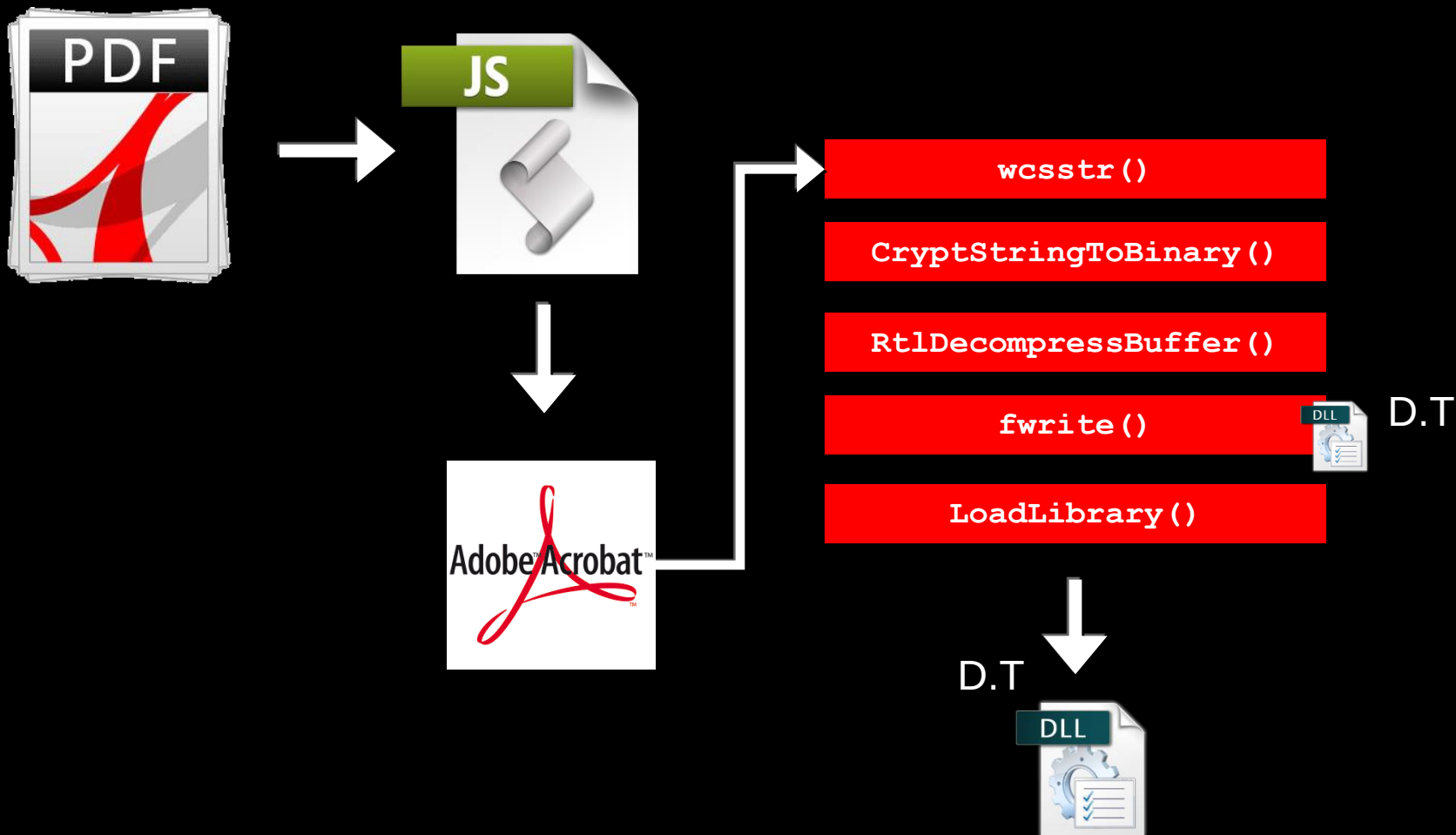
D.T

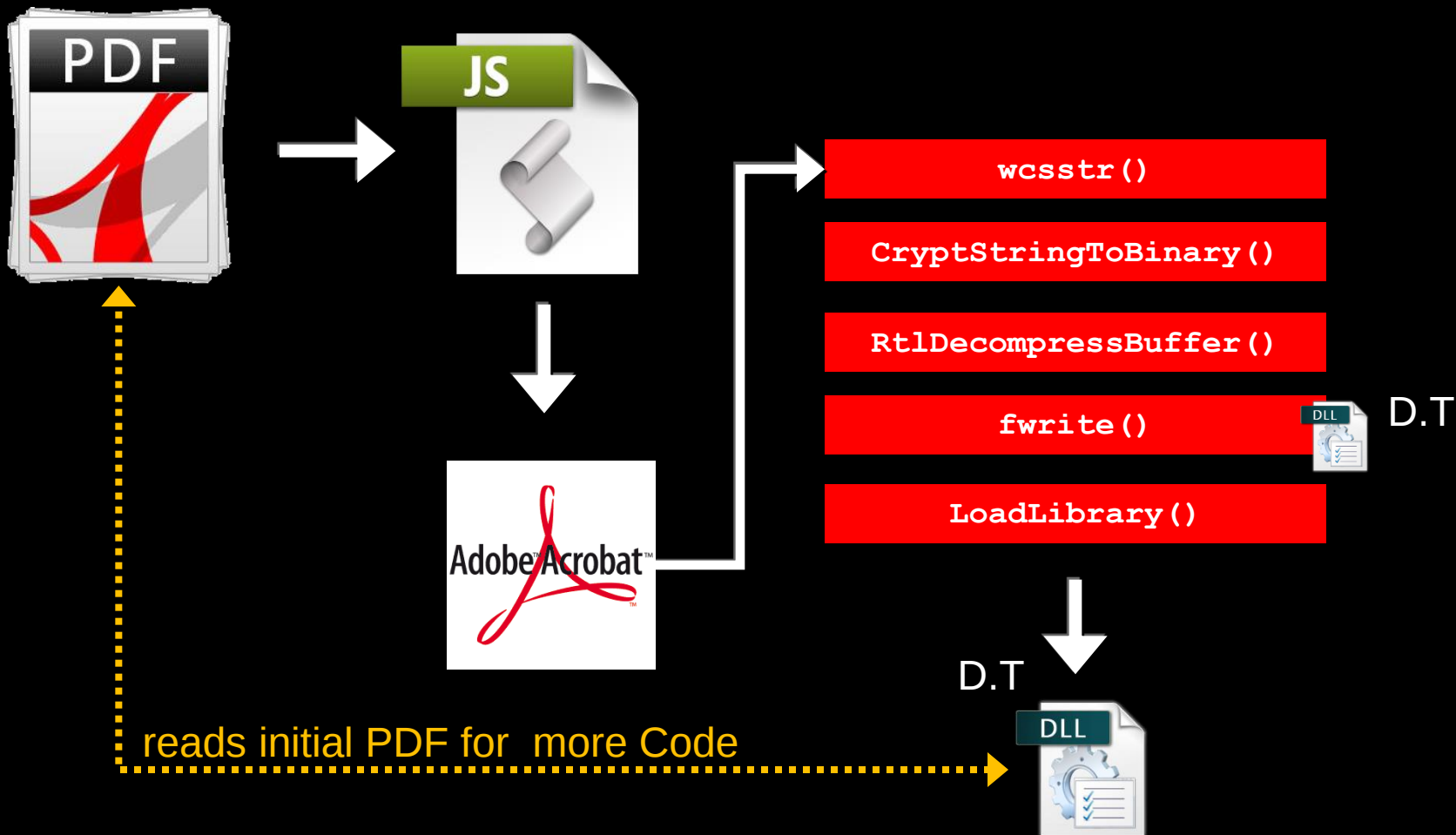


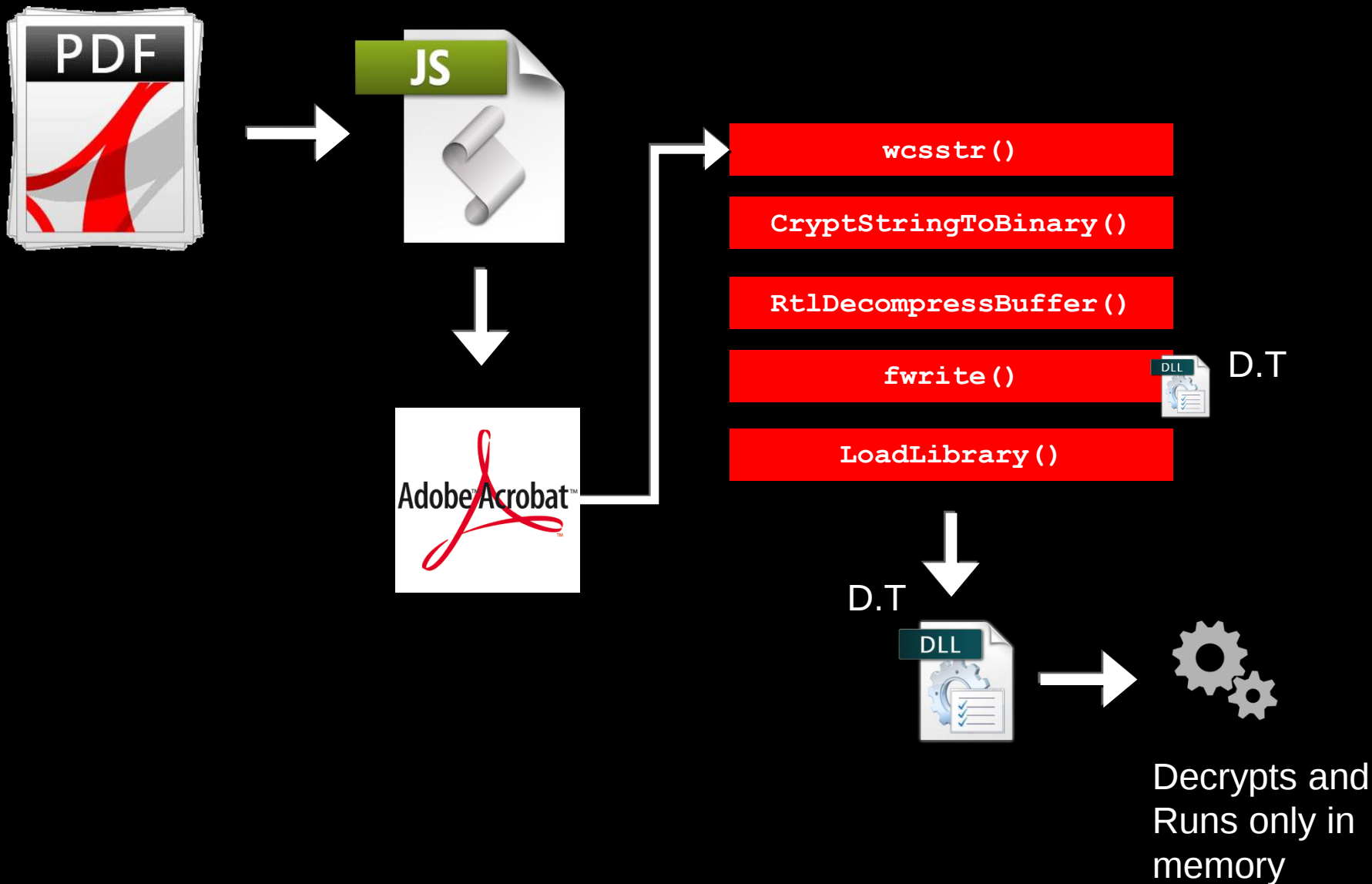
- `wcsstr()`
- `CryptStringToBinary()`
- `RtlDecompressBuffer()`
- `fwrite()`
- `LoadLibrary()`

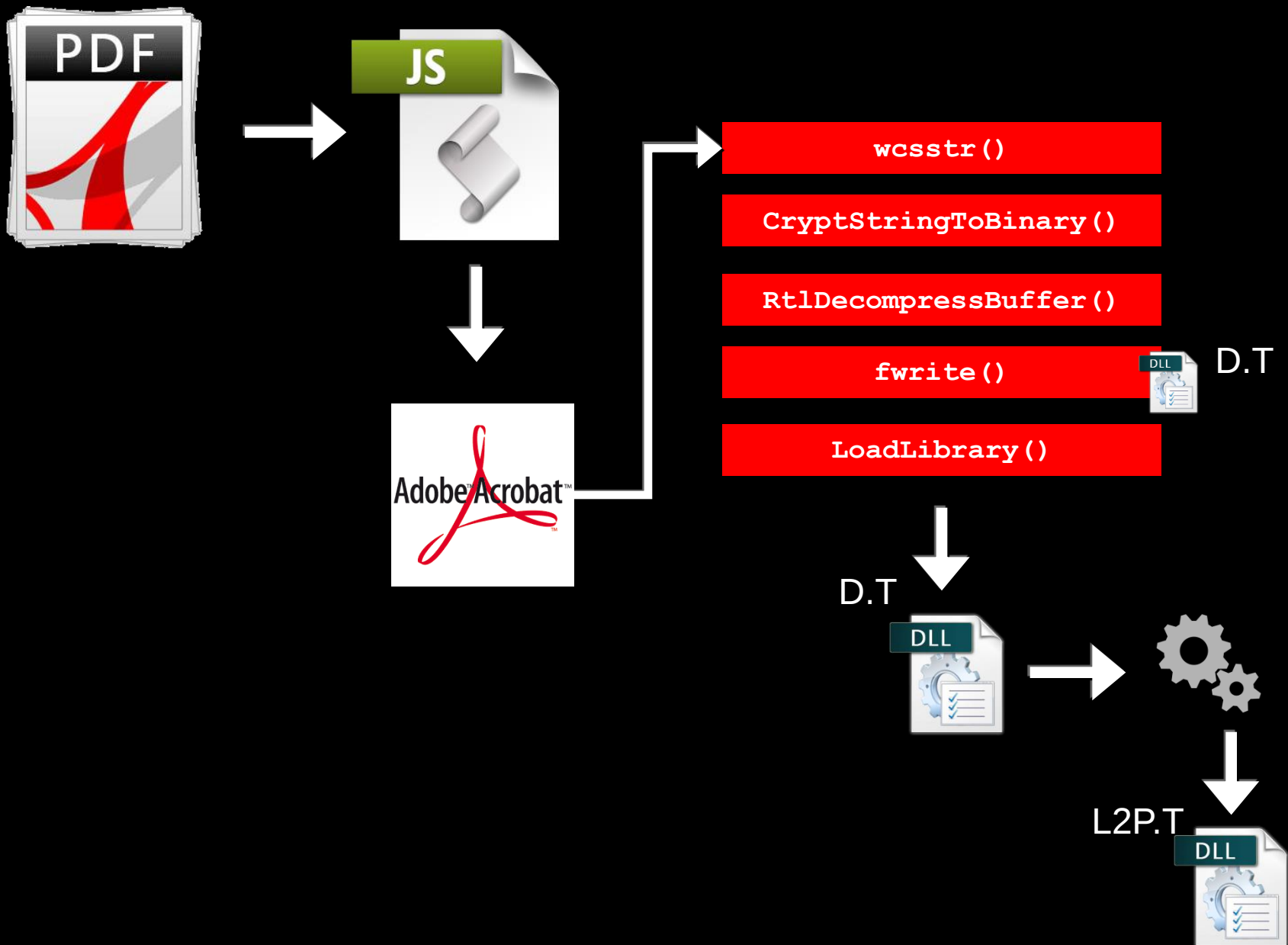


D.T









A close-up photograph of a baby with light brown hair and blue eyes, looking directly at the camera with a grumpy or determined expression. The baby is holding a clump of sand in their right fist. They are wearing a green long-sleeved shirt with a white chest panel. The background is a blurred beach scene with sand and waves.

Owned



@brad_anton

Brad.Antoniewicz@foundstone.com

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