NCA

National Crime Agency

Botnet Takedowns - Our GameOver Zeus Experience

Benedict Addis, ICANN SSAC, ShadowServer

Stewart Garrick, Senior Investigating Officer, National Cyber Crime Unit, NCA

Contents

What the average LE officer knows of botnets

Cryptolocker

Gameover ZeuS

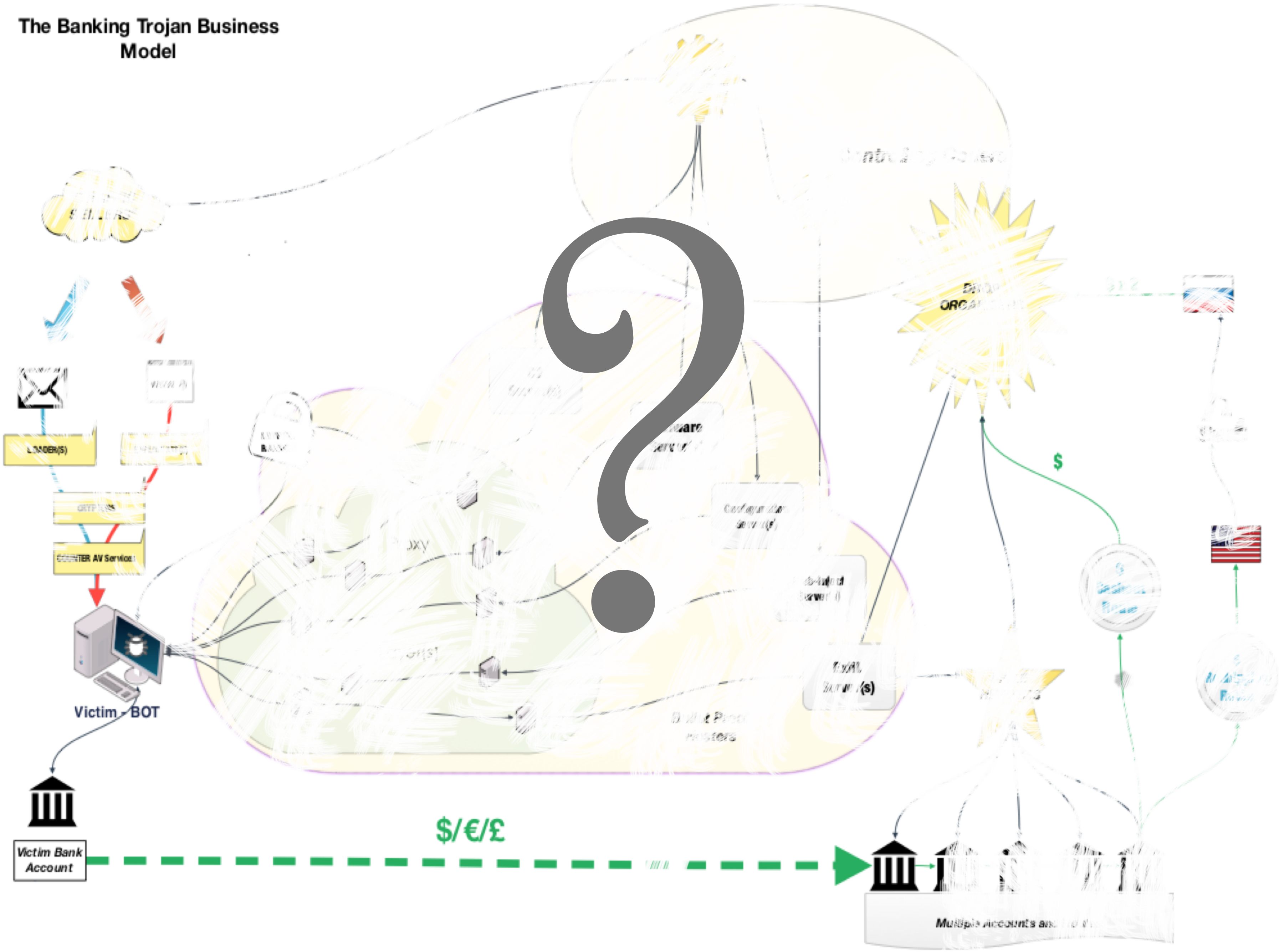
How both were broken

Learning the lessons of cooperation

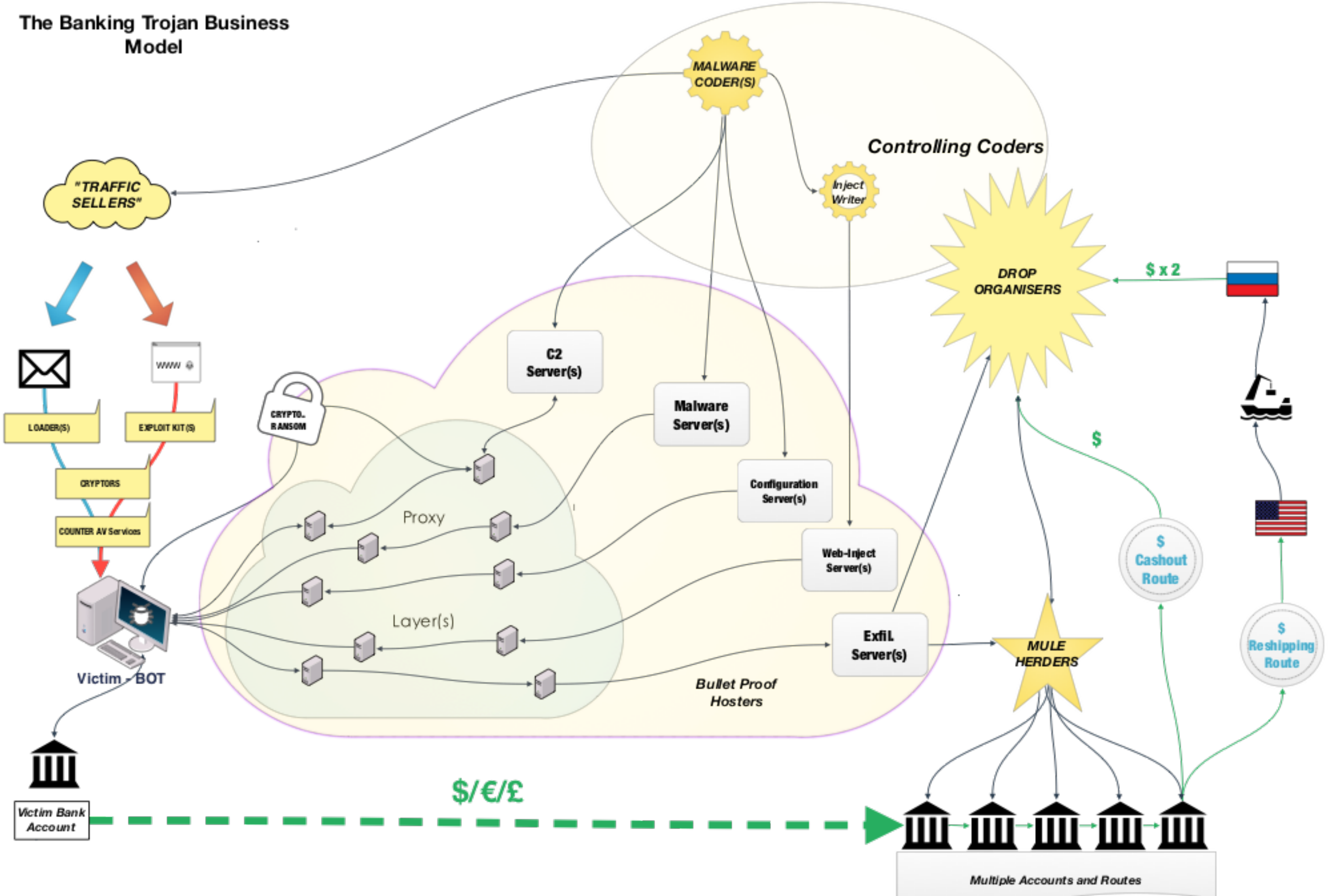
Looking to the future

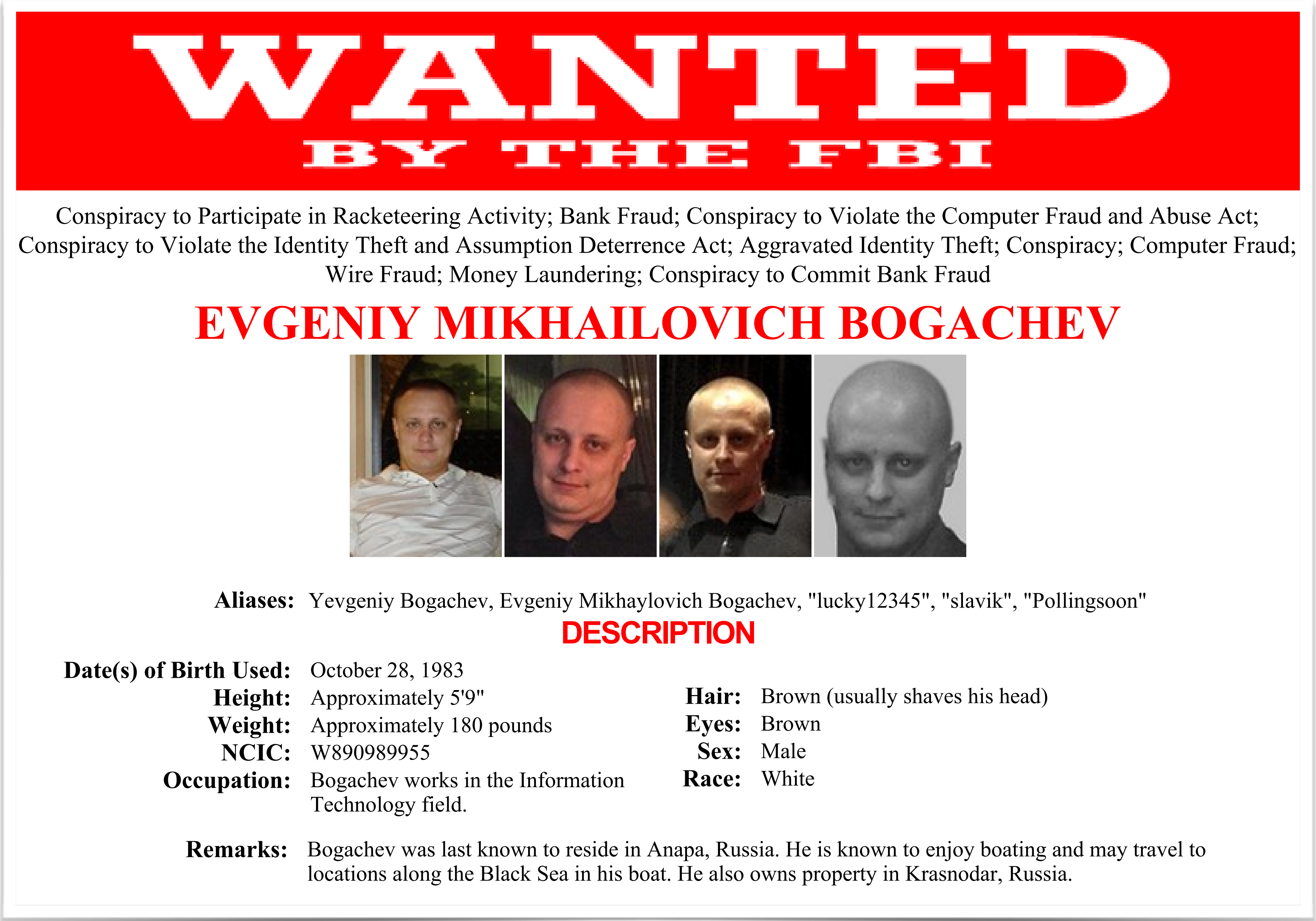
NCA
National Crime Agency

The Banking Trojan Business Model



The Banking Trojan Business Model





WANTED BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

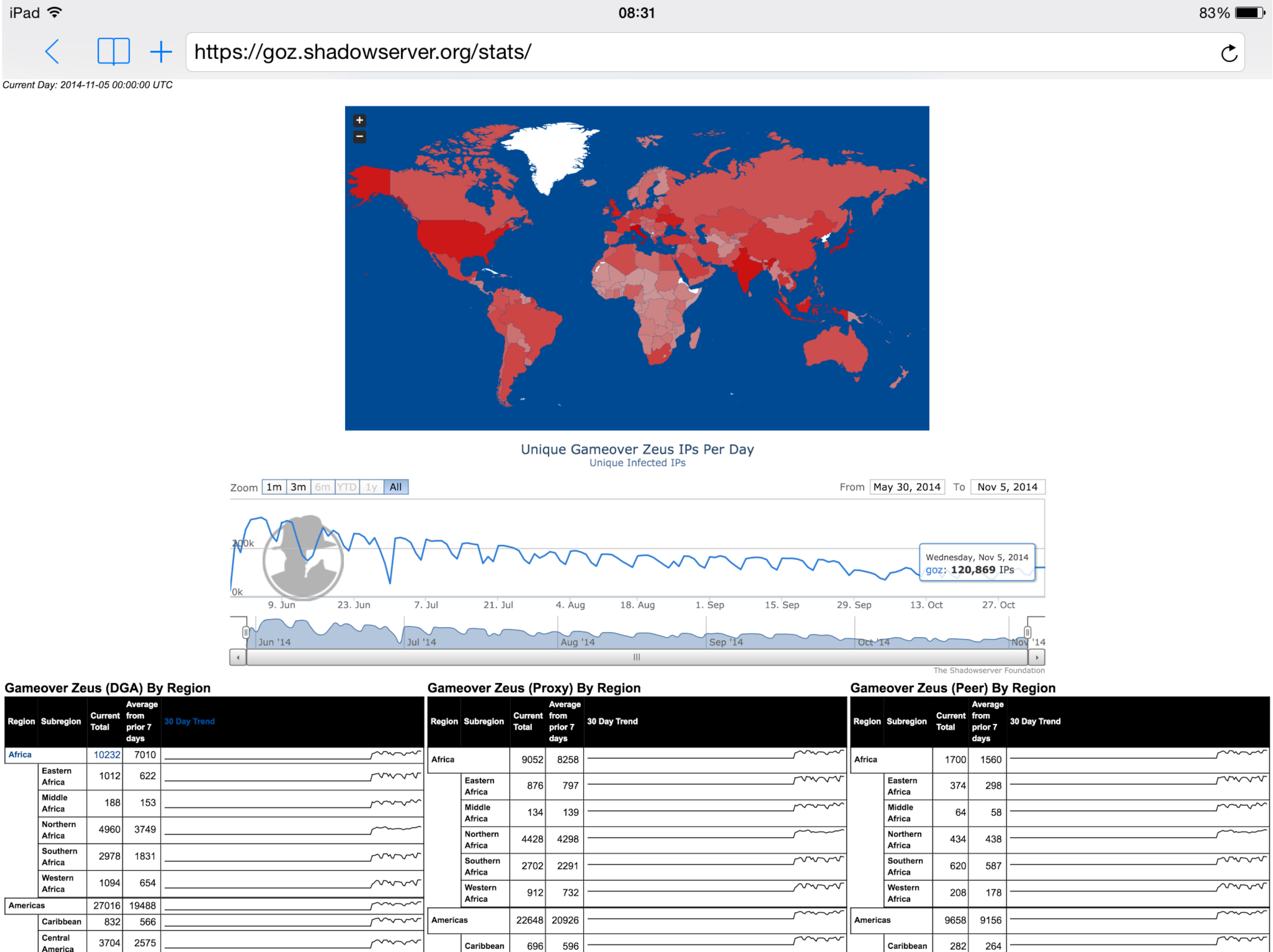
EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used:	October 28, 1983		
Height:	Approximately 5'9"	**Hair:**	Brown (usually shaves his head)
Weight:	Approximately 180 pounds	**Eyes:**	Brown
NCIC:	W890989955	**Sex:**	Male
Occupation:	Bogachev works in the Information Technology field.	**Race:**	White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.



Current Day: 2014-11-05 00:00:00 UTC

Unique Gameover Zeus IPs Per Day

Unique Infected IPs

Wednesday, Nov 5, 2014
goz: **120,869** IPs

Gameover Zeus (DGA) By Region

Region	Subregion	Current Total	Average from prior 7 days	30 Day Trend
Africa		10232	7010	
	Eastern Africa	1012	622	
	Middle Africa	188	153	
	Northern Africa	4960	3749	
	Southern Africa	2978	1831	
	Western Africa	1094	654	
Americas		27016	19488	
	Caribbean	832	566	
	Central America	3704	2575	

Gameover Zeus (Proxy) By Region

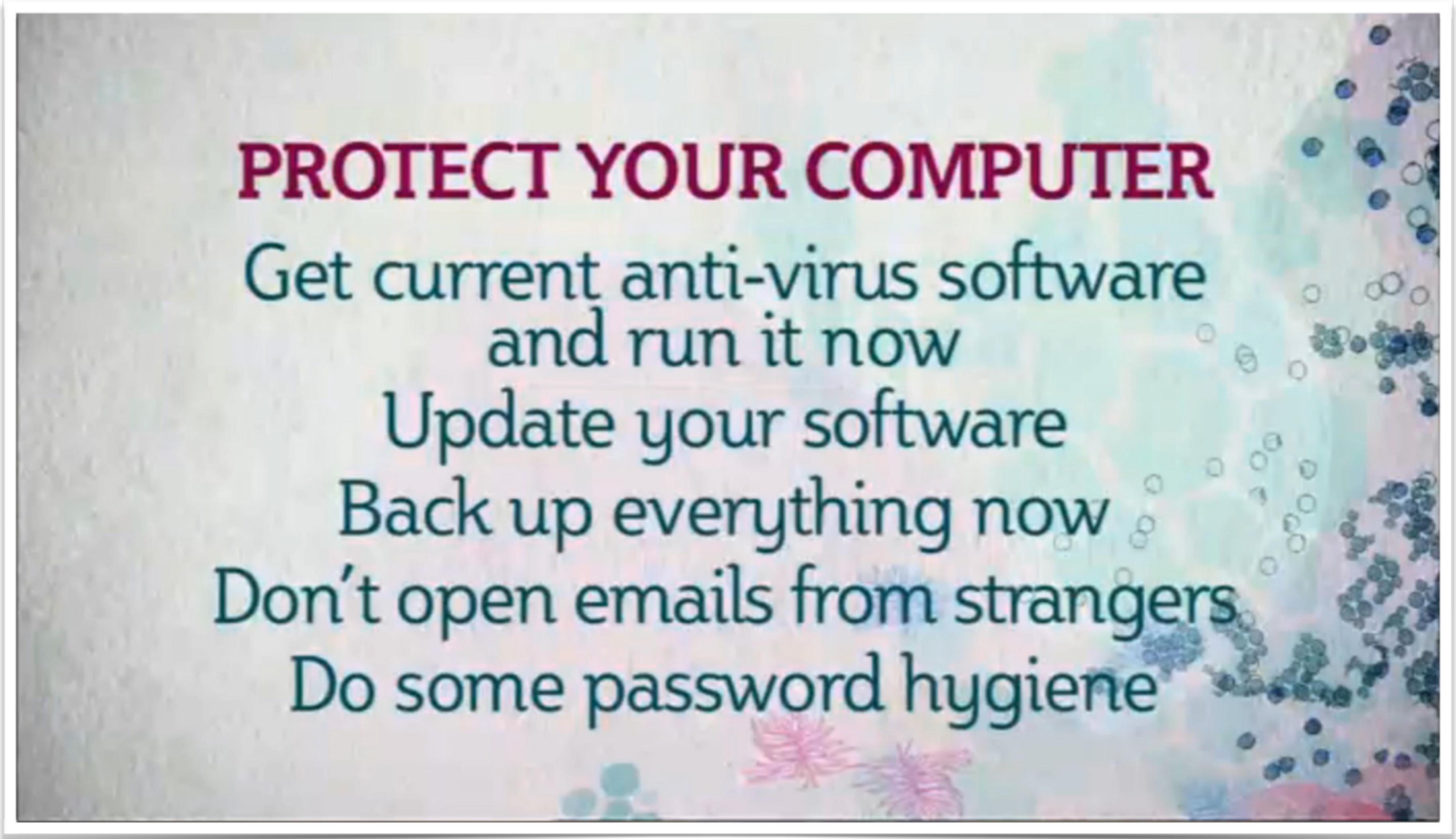
Region	Subregion	Current Total	Average from prior 7 days	30 Day Trend
Africa		9052	8258	
	Eastern Africa	876	797	
	Middle Africa	134	139	
	Northern Africa	4428	4298	
	Southern Africa	2702	2291	
	Western Africa	912	732	
Americas		22648	20926	
	Caribbean	696	596	

Gameover Zeus (Peer) By Region

Region	Subregion	Current Total	Average from prior 7 days	30 Day Trend
Africa		1700	1560	
	Eastern Africa	374	298	
	Middle Africa	64	58	
	Northern Africa	434	438	
	Southern Africa	620	587	
	Western Africa	208	178	
Americas		9658	9156	
	Caribbean	282	264	

How To Explain This?

this morning



PROTECT YOUR COMPUTER

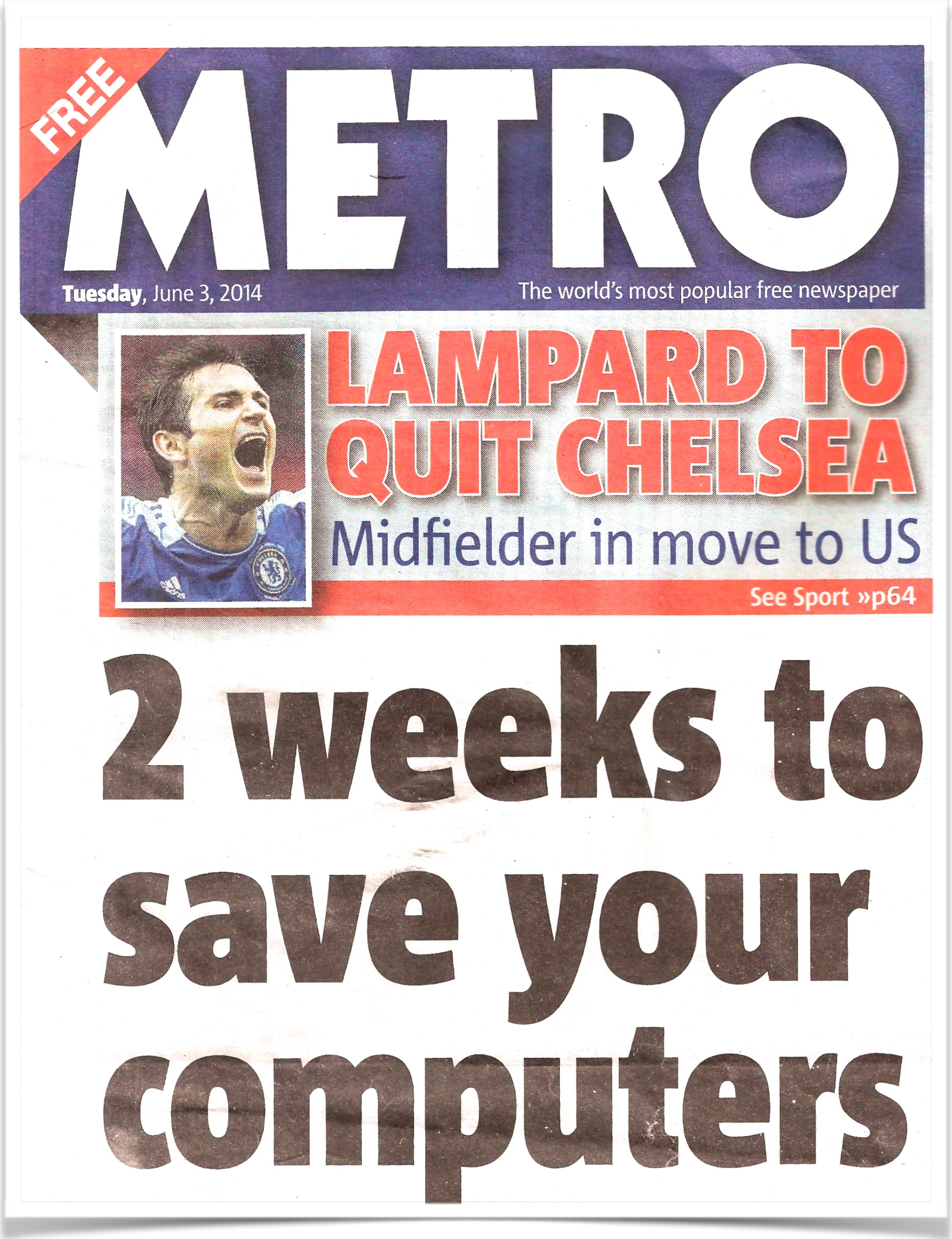
Get current anti-virus software
and run it now

Update your software

Back up everything now

Don’t open emails from strangers

Do some password hygiene



FREE

METRO

Tuesday, June 3, 2014

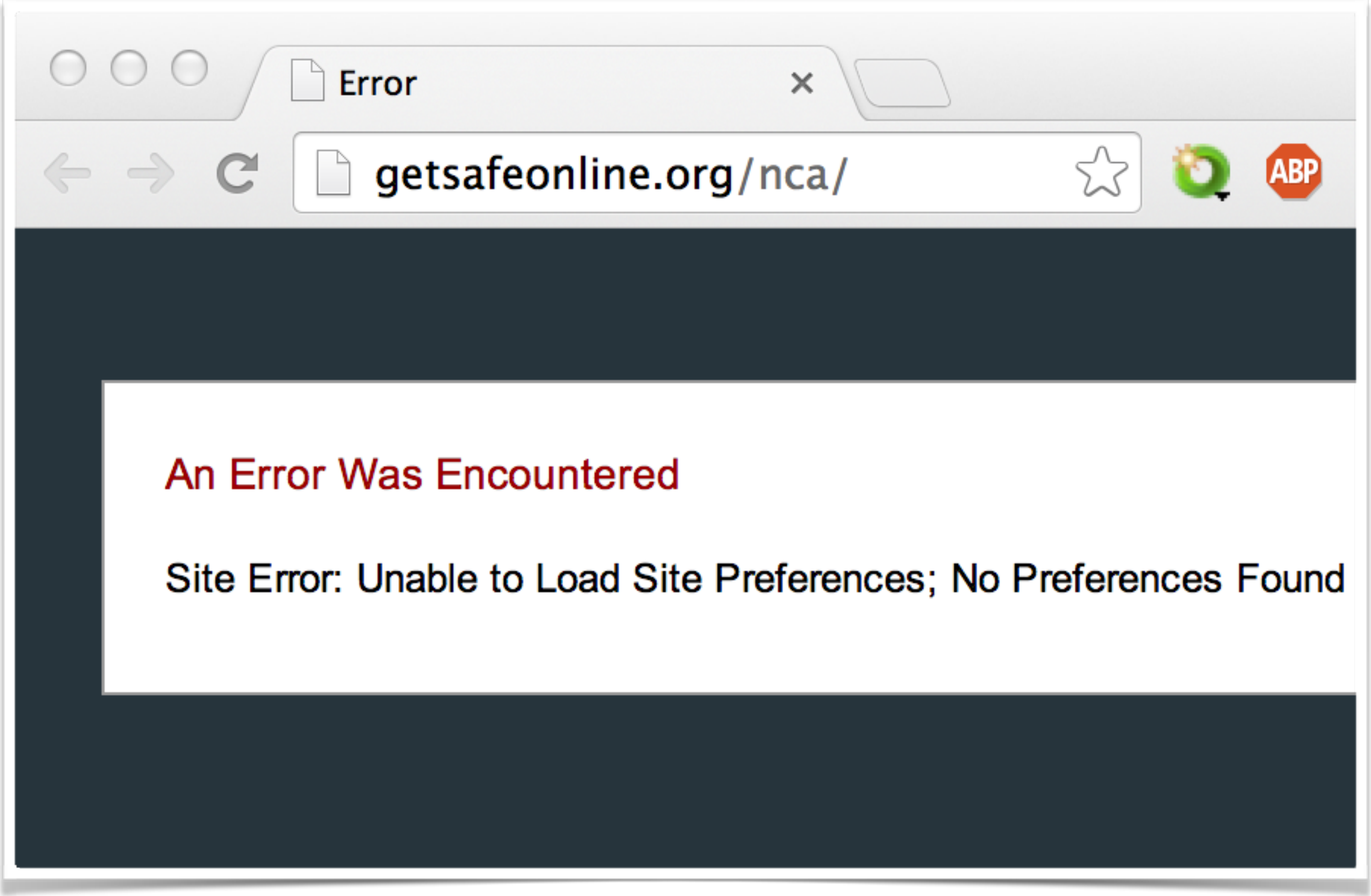
The world's most popular free newspaper

LAMPARD TO QUIT CHELSEA

Midfielder in move to US

See Sport »p64

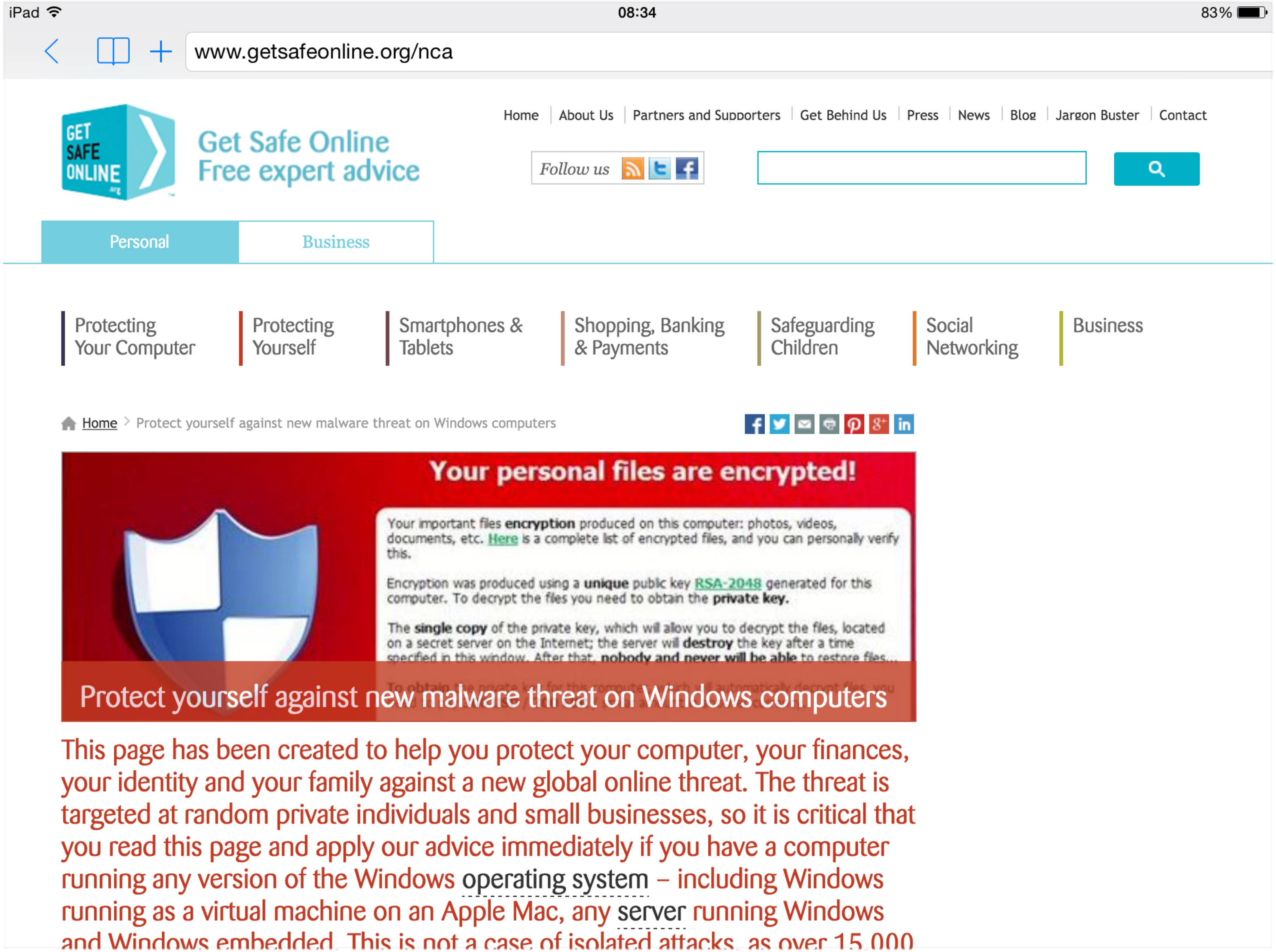
2 weeks to save your computers



An Error Was Encountered

Site Error: Unable to Load Site Preferences; No Preferences Found

NCA
National Crime Agency



iPad 08:34 83%

www.getsafeonline.org/nca

Home | About Us | Partners and Supporters | Get Behind Us | Press | News | Blog | Jargon Buster | Contact

GET SAFE ONLINE

Get Safe Online
Free expert advice

Follow us

Personal | Business

Protecting Your Computer | Protecting Yourself | Smartphones & Tablets | Shopping, Banking & Payments | Safeguarding Children | Social Networking | Business

Home > Protect yourself against new malware threat on Windows computers

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

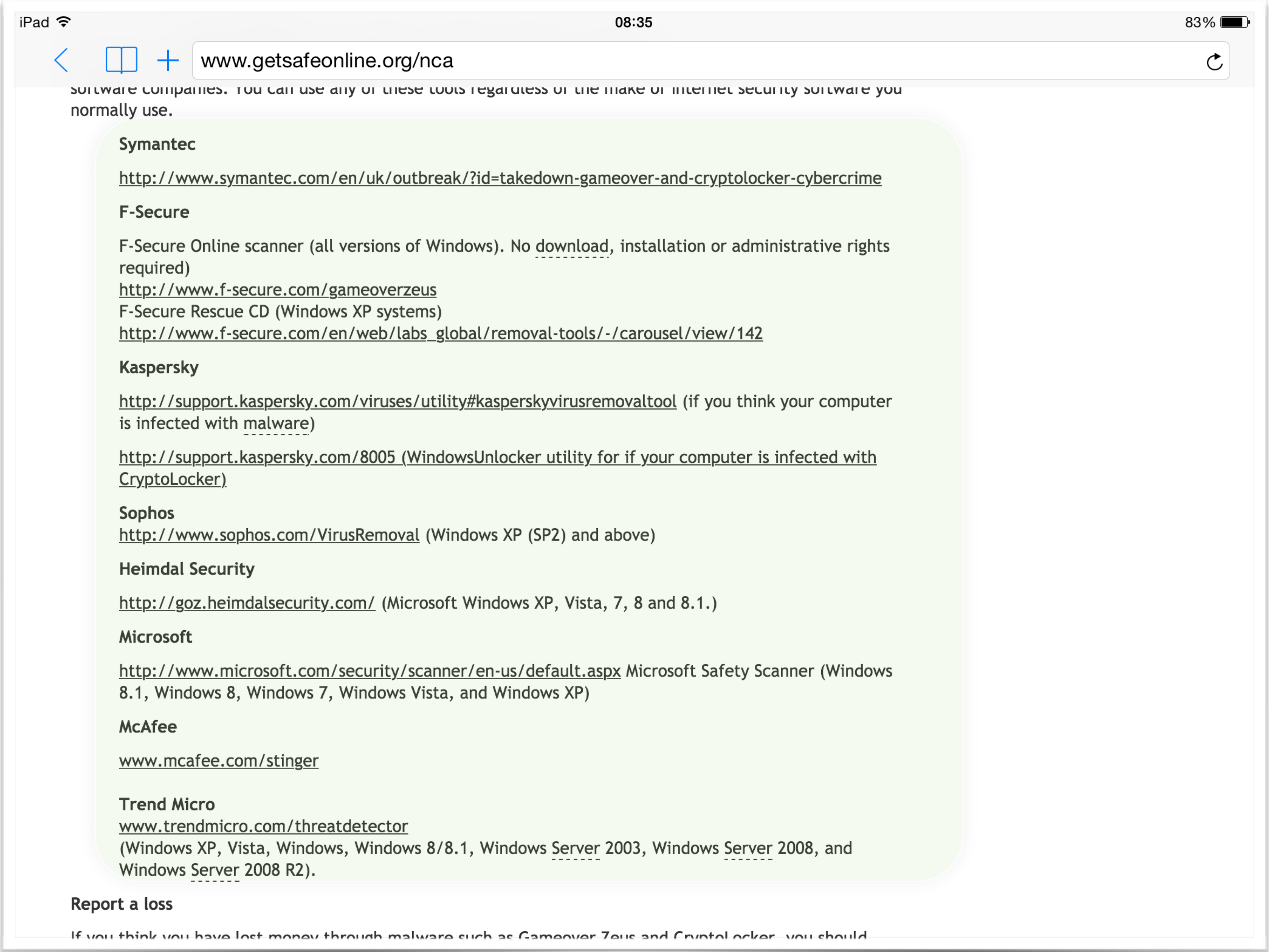
Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you

Protect yourself against new malware threat on Windows computers

This page has been created to help you protect your computer, your finances, your identity and your family against a new global online threat. The threat is targeted at random private individuals and small businesses, so it is critical that you read this page and apply our advice immediately if you have a computer running any version of the Windows operating system – including Windows running as a virtual machine on an Apple Mac, any server running Windows and Windows embedded. This is not a case of isolated attacks, as over 15,000



software companies. You can use any of these tools regardless of the make of internet security software you normally use.

Symantec

http://www.symantec.com/en/uk/outbreak/?id=takedown-gameover-and-cryptolocker-cybercrime

F-Secure

F-Secure Online scanner (all versions of Windows). No download, installation or administrative rights required)
http://www.f-secure.com/gameoverzeus
F-Secure Rescue CD (Windows XP systems)
http://www.f-secure.com/en/web/labs_global/removal-tools/-/carousel/view/142

Kaspersky

http://support.kaspersky.com/viruses/utility#kasperskyvirusremovaltool (if you think your computer is infected with malware)

http://support.kaspersky.com/8005 (WindowsUnlocker utility for if your computer is infected with CryptoLocker)

Sophos
http://www.sophos.com/VirusRemoval (Windows XP (SP2) and above)

Heimdal Security

http://goz.heimdalsecurity.com/ (Microsoft Windows XP, Vista, 7, 8 and 8.1.)

Microsoft

http://www.microsoft.com/security/scanner/en-us/default.aspx Microsoft Safety Scanner (Windows 8.1, Windows 8, Windows 7, Windows Vista, and Windows XP)

McAfee

www.mcafee.com/stinger

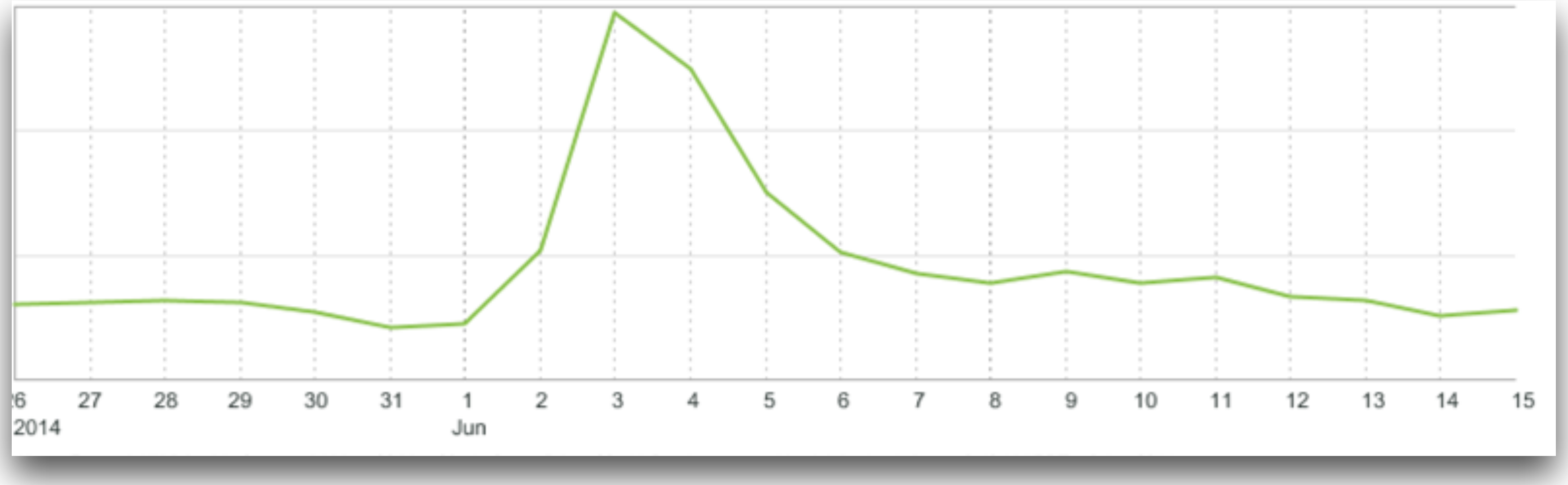
Trend Micro
www.trendmicro.com/threatdetector
(Windows XP, Vista, Windows, Windows 8/8.1, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2).

Report a loss

If you think you have lost money through malware such as Gameover Zeus and CryptoLocker, you should

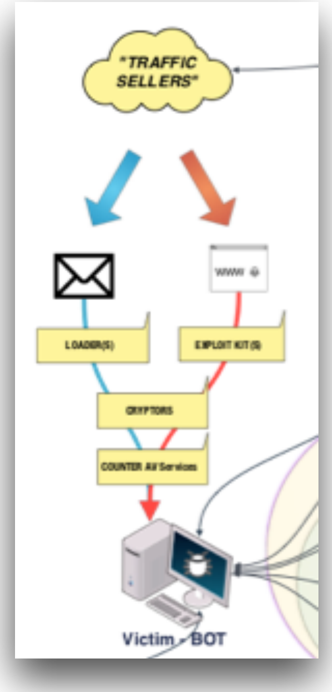
Public Response

- ⅔ reduction in UK IP addresses hitting sinkhole
- Massive uptake of AV tools



Sounds Simple…

Infection Basics



Cutwail botnet aka **Pushdo**

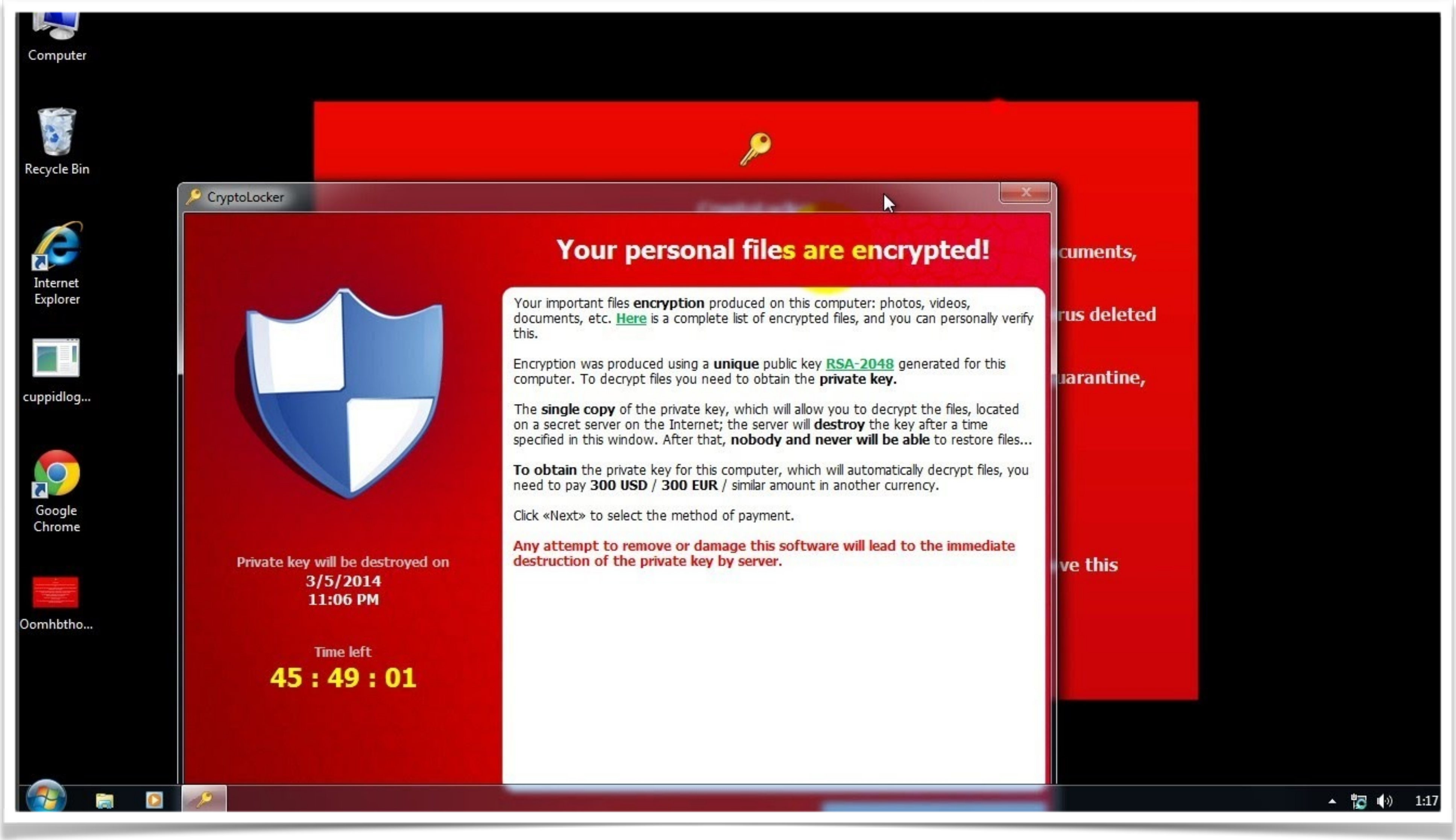
Spams **Upatre** downloader

Installs **Gameover ZeuS** malware

optionally loads **Cryptolocker** ransomware

NCA
National Crime Agency

Visible Threat: Cryptolocker



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

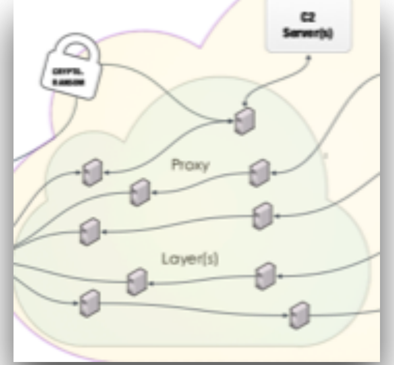
Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
3/5/2014
11:06 PM

Time left
45 : 49 : 01

Cryptolocker DGA



“Taus88” (as per Wikipedia)

- 1,000 *possible* domains generated **daily**
- Across seven TLD’s (.com, .net … .ru)
- Predictable!

Multiple Jurisdictions…

1st April 2014

…

avyrwkqfybrxsy**.com**

natuwpmsqjecsm**.net**

aksgduuoktdyac**.biz**

nonjdaqcccpdqk**.ru**

cfdkwfiapjrvsd**.org**

pjxnwkenhreasx**.co.uk**

cgwaulfcrjrovc**.info**

…

Multiple Jurisdictions…

1st April 2014

…

avyrwkqfybrxsy**.com**	= Verisign (USA)
natuwpmsqjecsm**.net**	= Verisign (USA)
aksgduuoktdyac**.biz**	= Neustar (USA)
nonjdaqcccpdqk**.ru**	= ccTLD.ru (Russia)
cfdkwfiapjrvsd**.org**	= Public Interest Registry (USA)
pjxnwkenhreasx**.co.uk**	= Nominet (UK)
cgwaulfcrjrovc**.info**	= Afilias (USA)

…

NCA
National Crime Agency

…Different Approaches

.com, **.net**, **.org**, **.biz** & **.info** - US Court orders to compel 4 Registries to sinkhole

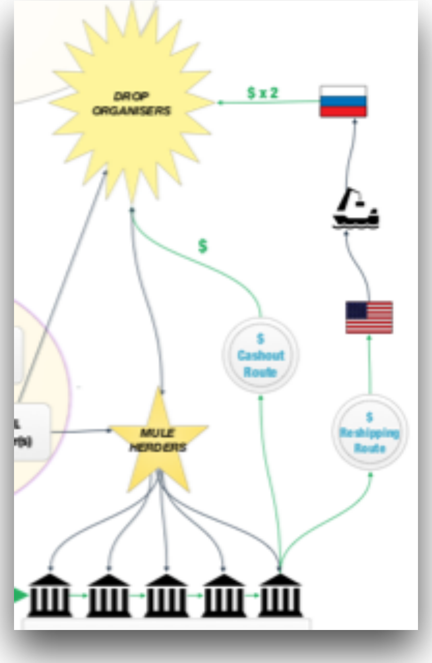
.co.uk - Nominet flagged for manual review

.ru - Registry blocked DGA registrations*

+ ‘Belt and Braces’ - court orders compelled 20 US ISPs to block DGA domains

++ Some 3rd party DNS providers took measures to block

Silent Threat: Gameover ZeuS



- Classic banking / credential-stealing trojan
- P2P communications hinder detection
- Access to live user sessions via webinjects
- Responsible for more than $100m losses
- “3D” money laundering

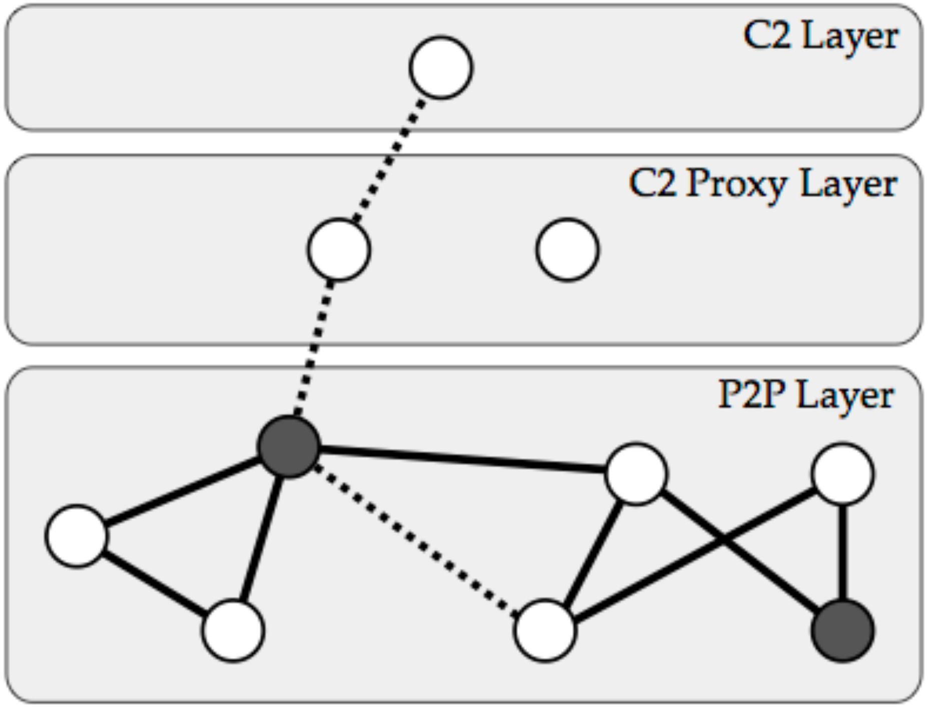
Gameover ZeuS DGA

- 1,000 *possible* domains generated **weekly**
- Across **six** TLD’s (.com, .net … .ru) - Dealt with as per Cryptolocker DGA

…
pkfhpbstogaschewbiusxoxlrk.net
dynjxvcvopzgyrhfmud.org
ppojgajhdeinqoocecyf.info
eqmzlrhekfxoqcjzdqdlmrorgymr.biz
tsbuciycqsvoxivuocmwhbcy.ru
rwclzjzjvcqxbiswnjsklrrg.com
…

NCA
National Crime Agency

Gameover ZeuS P2P



Highly Resilient Peer-to-Peer Botnets Are Here: An Analysis of Gameover Zeus

Dennis Andriesse[1], Christian Rossow[1], Brett Stone-Gross[2], Daniel Plohmann[3], and Herbert Bos[1]

[1]*VU University Amsterdam, The Netherlands, {d.a.andriesse,c.rossow,h.j.bos}@vu.nl*
[2]*Dell SecureWorks, bstonegross@secureworks.com*
[3]*Fraunhofer FKIE, Bonn, Germany, daniel.plohmann@fkie.fraunhofer.de*

Coordinated Effort

1. Industry-led replay attack on p2p mechanism
2. Court-ordered DGA *sinkholing* by Registries
3. Court-ordered DGA *blocking* at US ISP’s
4. LE seized servers in 11 countries
5. Supernodes removed from DHCP pool
6. NCA support in sinkholing last domains

Ops Rooms

EC3 - Europol early shift - NCFTA/FBI - late shift

Single operation - 11 nations intelligence sharing in real time

Industry experts present / on hand in Ops Room

- Shadowserver
- Dell Secureworks
- Crowdstrike
- Cisco

Learning

- Understanding the criminal business model
- Mapping infrastructure
- Intelligence shared whilst actionable in trustgroups
- Mistakes happened - reacted quickly & fairly
- Use of media attention to upskill users
- Use of CERTs & Industry to aid public remediation
- Focus on what we each do best then shared and coordinated!

Future

- What happens when court orders expire?
- Development of Registrar of Last-Resort?
- Increase in cooperation & trust between LE - EC3/J-CAT - Industry - Experts

Questions?

- baddis@shadowserver.org
- stewart.garrick@nca.x.gsi.gov.uk