NERSOU

NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT

Protecting communities from organised crime

Detective Sergeant Martin Wilson
Cyber Protect Co-ordinator

Regional Intelligence Unit (RIU)

Regional Fraud Team (RFT)

Regional Crime Investigation Team

NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT
Protecting communities from organised crime

Regional Asset Recovery Team (RART)

Regional Prison Intelligence Unit

Regional Covert Specialist Units

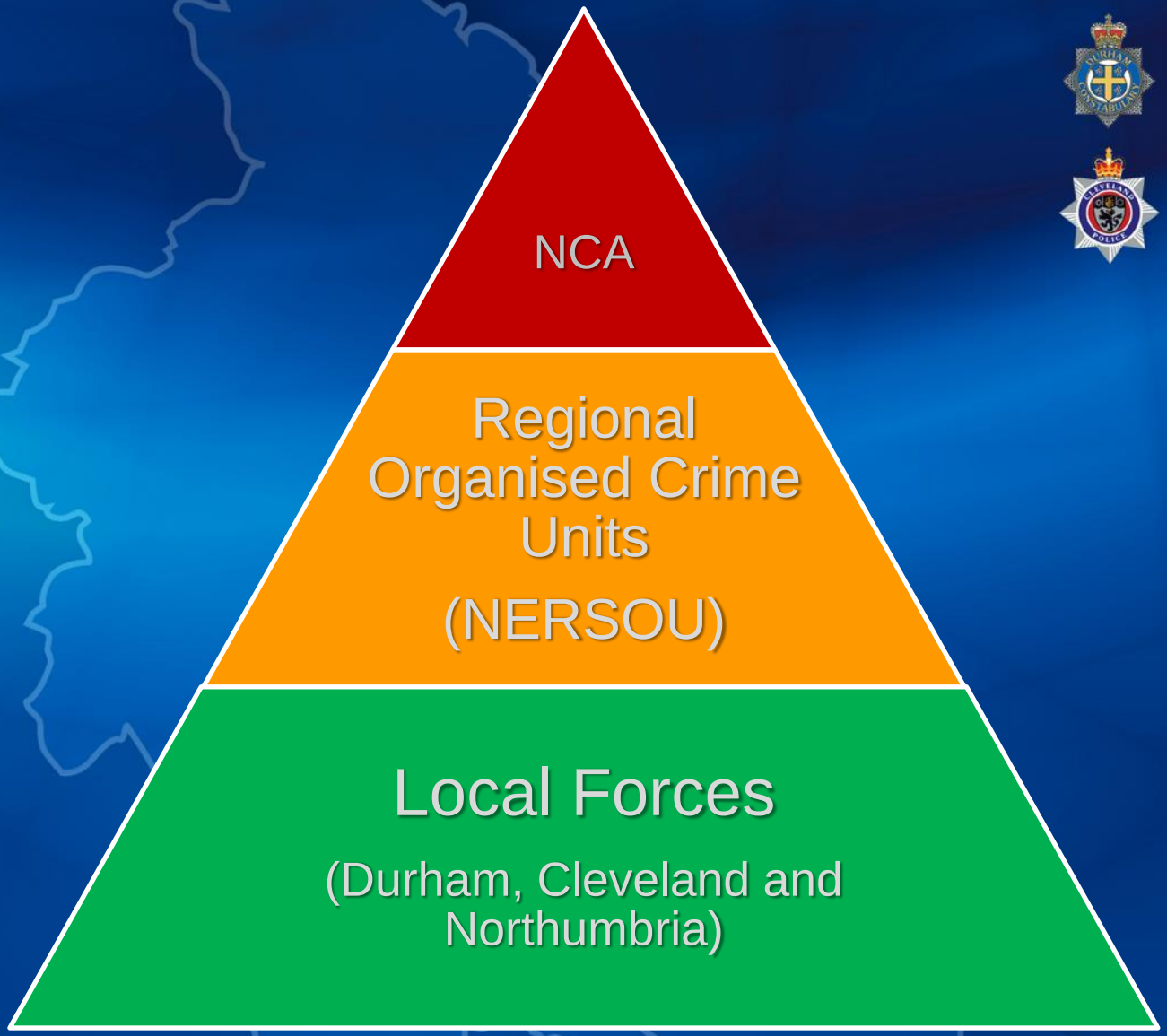
North East Regional Cyber Crime Unit (NERCCU)


Scotland
NERSOU
NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT
Protecting communities from organised crime
Cumbria
TITAN
North West Regional Organised Crime Unit
POLICING
YORKSHIRE & THE HUMBER
Joint thinking, joint working
ROCU
Regional Organised Crime Unit
WEST MIDLANDS POLICE
East Midlands Special Operations Unit
police
TARIAN
LROCU
METROPOLITAN POLICE
Working together for a safer London
BRITISH TRANSPORT POLICE
CITY OF LONDON POLICE
Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME
www.ersourocu.org.uk
Zephyr
Destroying Organised Crime
Dorset
south east
Regional Organised Crime Unit

National/ International

Cross Border

First Responders & Local Investigations




£
3
$
4
&
6
7
B
Y
M
F
G
H
J
N
E
R
C
C
U

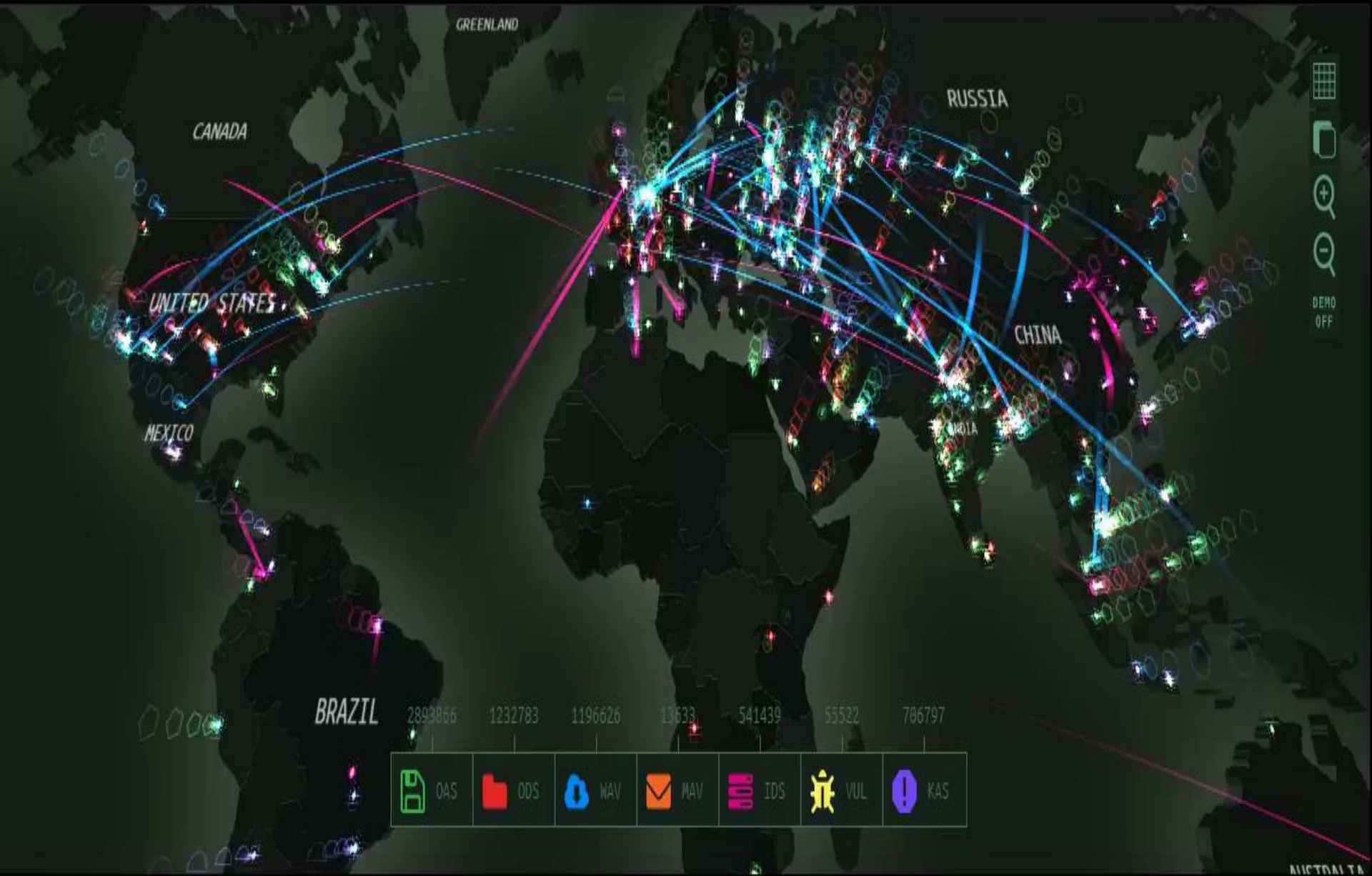
CYBERTHREAT REAL-TIME MAP

EN RU

AM I INFECTED?

MAP STATISTICS DATA SOURCES BUZZ WIDGET

Share:



From: [redacted]@humbermerchants.co.uk
To:
Cc:
Subject: Industrial Invoices
Sent: Wed 10/22/2014 6:46 AM

Message | 15040BII3646501.doc (63 KB)

Attached are accounting documents from Humber Merchants

Humber Merchants Group

Head Office:
Parkinson Avenue
Scunthorpe
North Lincolnshire
DN15 7JX

Tel: [redacted]
Fax: [redacted]
Email: [redacted]

--
Automated mail message produced by DbMail.
Registered to Humber Merchants Limited , License MBS2008354.

Around 80% of cyber attacks could be prevented if businesses put simple security controls in place.

The Cyber Essentials scheme shows how to put these controls in place.

The Cyber Essentials Badge allows your company to advertise the fact that it adheres to a government endorsed standard.

There are **two** levels of badges that your organisation can apply for:

Cyber Essentials

Requires the organisation to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.

Cyber Essentials PLUS

Tests of the systems are carried out by an external certifying body, using a range of tools and techniques.


Warning From AntiSpy Pro
Malware Found
Your systems is infected!
File: swg.dll
Malware: Google Toolbar Notifier BHO
swg.dll - Google Toolbar Notifier, http://googlesystem.blogspot.com/2006/07/google-is-your-default-search.html
Remove
Remove dangerous unit
AntiSpy Pro
http://AntiSpy-Pro.com

Lets Secure Our Supply Chains

CiSP

A CATALYST FOR COLLABORATION

Cyber Security Information Sharing Partnership

simonw@southwestwater 26-Nov-2015 12:50 (in response to simonw@southwestwater)

Re: Phishing emails with Subject of "xxx Payment" or "xx Transaction"

SHA256 fd874df06b05a901d3f6c21d8edc8e4b3f3416a979b402b2dd40c6fb364ed5f3

Being identified by McAfee as of today as W97M/Dropper.ae

Actions ▾ Like (0) Reply

MartinH1@objective 26-Nov-2015 12:58 (in response to simonw@southwestwater)

Re: Phishing emails with Subject of "xxx Payment" or "xx Transaction"

Hmm variation of the Cryptolocker I bet - engage the macros and you'll be held to ransom when it encrypts the files it can see

Actions ▾ Like (0) Reply

ChrisW1@proofpoint.com 26-Nov-2015 14:15 (in response to MartinH1@objective)

Re: Phishing emails with Subject of "xxx Payment" or "xx Transaction"

No, actually it's Dridex banking trojan (botnet 302). I've posted IOCs and details at https://share.cisp.org.uk/docs/DOC-3012#comment-12415

Best Wishes,
Chris

Actions ▾ Like (0) Reply

The Dridex downloader, known as the W97M.downloader is not particularly sophisticated and is well known to security professionals and AV vendors. However, the obfuscation and encryption methods utilised and the speed at which the attack vectors change make it difficult for network defenders and security specialists to respond ever changing attacks.

One of the key aspects of Dridex is that it runs in memory, making traditional file-based anti-virus less effective. It is able to maintain persistence by writing itself to disk at shutdown, then writing itself into memory and deleting the disk file on start-up.

Defensive recommendations

- Organisations are advised that unless there is a specific business need, macros should be disabled throughout your networks.
- Use a host intrusion prevention system to stop programs from being executed in temporary folders.
- Maintaining a white list of trusted executables and blocking others adds a very effective layer of defence.
- Ensure archive files such as .cab files, are expanded and examined before being passed onto the endpoint.
- The best defence against the Dridex malware, or any other spam phishing campaign, is to ensure that all staff in an organisation, are educated on the dangers that email attachments or links can bring.

The criminals behind the Dridex campaign have shown that they have the ability to adapt and react quickly to new defences being employed by security professionals. In the case of malware such as Dridex, defensive methodologies should not be aimed at treating the symptoms but focused on the inherent operating system (OS) tools the malware uses. CERT- UK would encourage our members to use the defensive measures offered in this paper as a framework for preventing Dridex malware infecting your organisation.

CiSP Champion

SIGNACURE
RESILIENCE

Follow us on twitter for regularly updated tips and hints on cyber security

@nerccu

To find out how to join the CiSP contact, the North East CiSP Champion Dave Lloyd of Signacure Resilence at dave@signacure.co.uk

Or DS Wilson, the North East Cyber Protect Co-ordinator at martin.wilson@durham.pnn.police.uk