National Cyber Security Centre

a part of GCHQ

For sale : One snake. Good oil producer. No longer required.

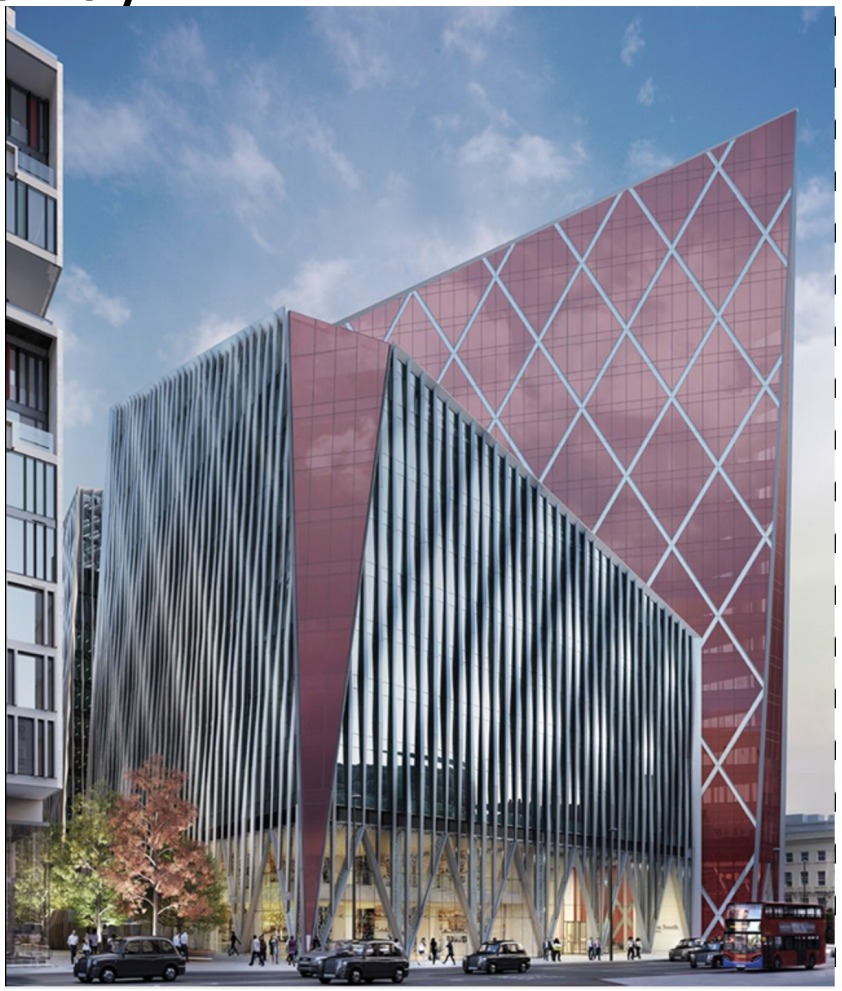
Dr Ian Levy

Technical Director

National Cyber Security Centre

National Cyber Security Centre
a part of GCHQ

A Different Sort of Agency



National Cyber Security Centre
a part of GCHQ

Early wins…

Why Nova Victoria won the 2017 Carbuncle Cup

By Thomas Lane | 6 September 2017

3 Comments

There were plenty of strong contenders on the shortlist but Nova's crass design secured it this year's wooden spoon

Nova Victoria from Victoria St

It is unfortunate although not entirely surprising that a London building has won the Carbuncle Cup for the sixth year running. The capital is in the middle of a massive construction boom so there is a

National Cyber Security Centre
a part of GCHQ

Know your competition…

National Cyber Security Centre
a part of GCHQ

Evidence driven policy

National Cyber Security Centre
a part of GCHQ

Simplify cybersecurity* to democratise it.

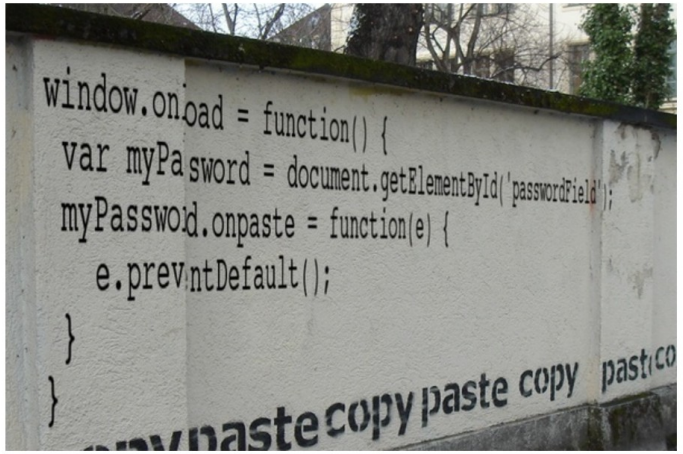
* Yes, I hate the C-word as well, but it’s what we’re stuck with.

National Cyber Security Centre
a part of GCHQ

Blog post

Let them paste passwords

Created: 12 Jan 2017
Updated: 12 Jan 2017
Author: Sacha B
Part of: Identity and passwords



One of the things people often tweet to us @ncsc are examples of websites which prevent you pasting in a password. Why do websites do this? The debate has raged - with most commentators raging how annoying it is.

So why do organisations do this? Often no reason is given, but when one is, that reason is 'security'. The NCSC don't think the reasons add up. We think that stopping password pasting (or SPP) is a bad thing that *reduces* security. We think customers should be allowed to paste their passwords into forms, and that it *improves* security.

No one knows where it came from

It is a mystery where SPP came from. No one has pointed to a paper, a rule, an RFC (a technical standards document to plan how the Internet should work) or anything else that started it off. If you know of one, let us know using the comments form below. We believe it's one of those 'best practice' ideas that has a common sense instant appeal that may have made sense once. Considering the bigger picture today, it really doesn't make sense.

Blogs by Topic

Identity and passwords (7)
The NCSC (5)
New talent (2)
Government strategy (2)
Research (2)
End user device (2)
Cyber strategy (2)
Cyber attacks (1)
Assurance (1)
End user technology (1)
Cyber threats (1)
Vulnerabilities (1)
All (27)

Blogs by Author

Emma W (4)
Jon L (2)
Andrew M (2)
Richard C (1)
Ciaran Martin (1)
Helen L (1)
Anne W (1)

National Cyber S

a pa

Andy Gambles @andygambles · Jul 10

So @BcardBusiness I was unable to use the password "uNq3>964;i6atMbwvkv@CH}Z(" generated by my password manager because you restrict passwords to 16 characters and disable the ability to paste. However "Password1234" was perfectly acceptable. #infosecurity

3 15 33

Karl Austin @KarlAustin · Jul 10

Banks are the absolute pits when it comes to good passwords. Hey @BcardBusiness check out what @NCSC has to say about passwords: ncsc.gov.uk/guidance/passw... then do something about it :)

Password Guidance: Simplifying Your Approach

Advice for system owners responsible for determining password policy, advocating a dramatic simplification of the current approach at a system ...

ncsc.gov.uk

1 2 13

Andy Gambles @andygambles · Jul 10

I tried manually typing in the random password twice until I realised they didn't permit special characters in the password!

2 1 11

Barclaycard Business @BcardBusiness · Jul 10

I'm sorry that you have had problems creating your password. If you would like to discuss this further please DM me with your company name, full company address and a contact telephone number ^RG

Send a private message

2 1

Andy Gambles @andygambles · Jul 10

I don't want to discuss it privately. I would like you to explain why my password can not be pasted?

1 18

Barclaycard Business @BcardBusiness · Jul 12

We're sorry for the slow response. We have been looking into this and a fix has been put in place so that passwords can be copied and pasted when logging in. We value your feedback and understand your frustration. ^RG

Troy Hunt @troyhunt

Following

How do you "not recognise password managers" @AskNationwide?! Maybe take some advice from your own @NCSC on this one: ncsc.gov.uk/blog-post/let- ...

Nationwide UK @AskNationwide

Replying to @tomharristech

Hi Tom, sorry we wouldn't be able to advise on this, as Nationwide do not recognise password managers as we have our own internet banking security in place. We are sorry we are unable to help you with this. Anna

12:19 am - 24 Sep 2018 From Gold Coast, Queensland

10 Retweets **70** Likes

7 10 70

National Cyber Security Centre

Blog post

The serious side of pranking

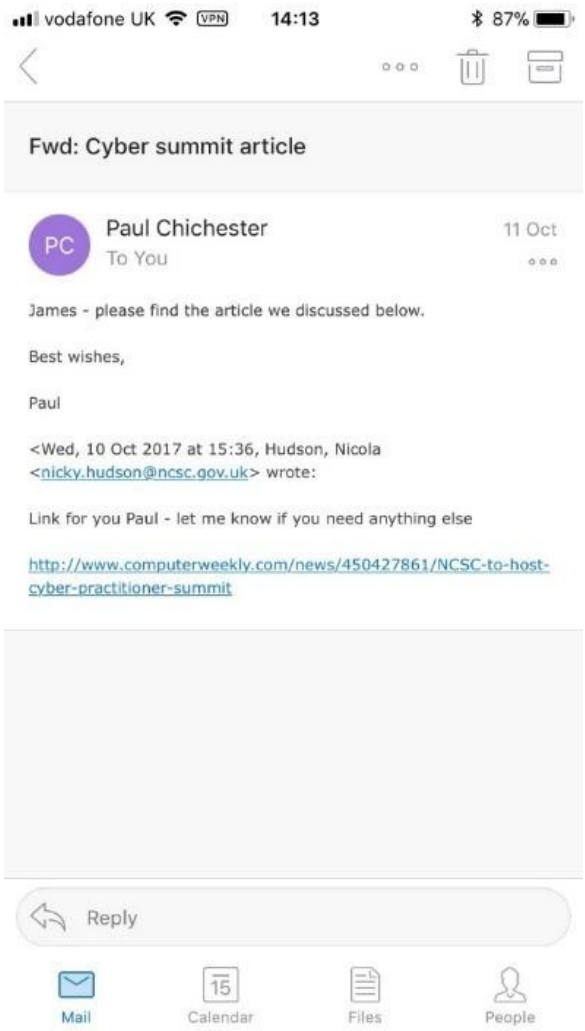
Created: 30 Oct 2017
Updated: 30 Oct 2017
Author: Ian Levy
Part of: Cyber threats, Vulnerabilities

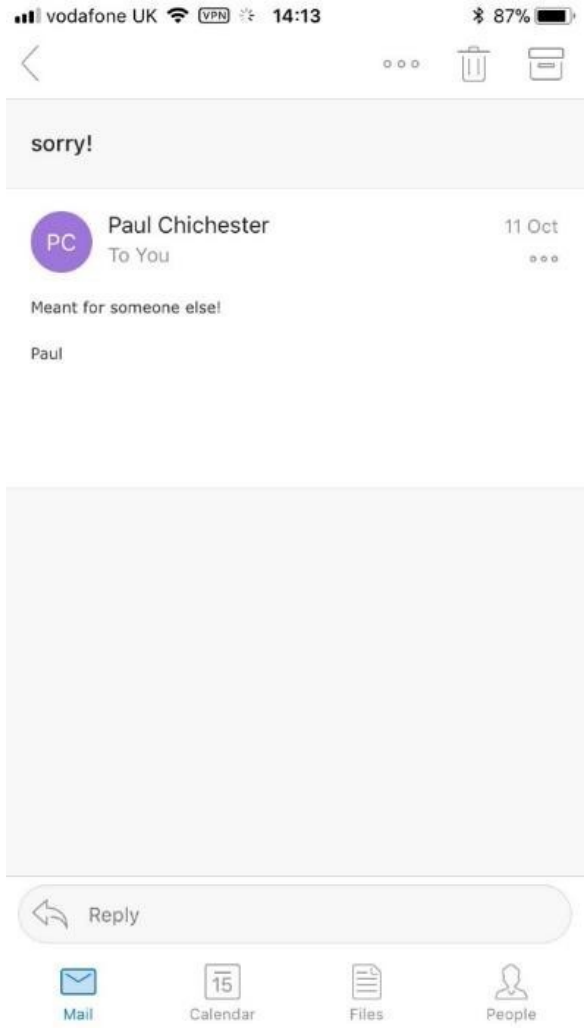
I was recently targeted for a prank and have taken the unorthodox step of asking James Linton, the very person who was trying to prank me, to help write this blog.

Our joint aim is to lay bare the realities of email security and, given that a cyber attack looks exactly like a prank, use this unique opportunity to show an attack from both sides.

The National Cyber Security Centre is doing as much as possible to make real people's lives easier and safer on the internet. Initiatives such as the Active Cyber Defence programme are blocking, disrupting and neutralising malicious cyber activity before it reaches users.

The blog concludes with some hard questions for the tech and security industry about the future of email security.





National Cyber Security Centre

a part of GCHQ

Department for Digital, Culture Media & Sport

Secure by Design: Improving the cyber security of consumer Internet of Things Report

4.5. As part of this work, the Government will consider how the uptake and impact of the Code of Practice can be measured once a final version has been published. The UK Government will also explore whether retailers can play a greater role in helping to reduce the burden on consumers. Additionally, in 2018 the Government will conduct work to map the finalised Code of Practice against the main standards on IoT security to help contextualise the Code for companies.

Proposed Code of Practice for Security in Consumer IoT Products and Associated Services

This Code of Practice is designed to improve the security of consumer IoT products and associated services. Many severe cyber security issues stem from poor security design and bad practice in products sold to consumers.

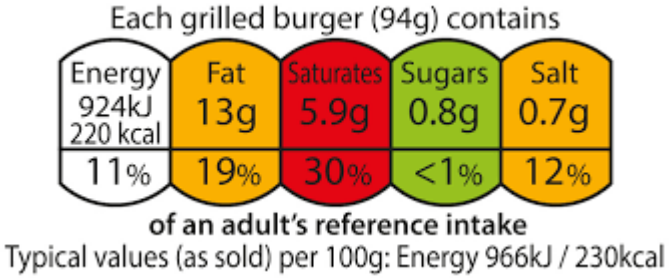
The guidance is listed in order of importance and the top three should be addressed as a matter of priority. An indication is given as to which stakeholder the responsibility primarily rests upon. These stakeholders are defined as:

Device Manufacturer: The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.
IoT Service Providers: Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.
Mobile Application Developers: Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.
Retailers: The sellers of internet-connected products and associated services to consumers.

1) No default passwords
All IoT device passwords must be unique and not resettable to any universal factory default value.

Many IoT devices are being sold with universal default usernames and passwords (such as "admin, admin") which are expected to be changed by the consumer. This has been the source of many security issues in IoT and the practice needs to be eliminated. Best practice on passwords and other authentication methods should be followed. Further details are available on the NCSC website.[25]

[25] National Cyber Security Centre, guidance, 2017, accessed at: https://www.ncsc.gov.uk/guidance



National Cyber Security Centre
a part of GCHQ

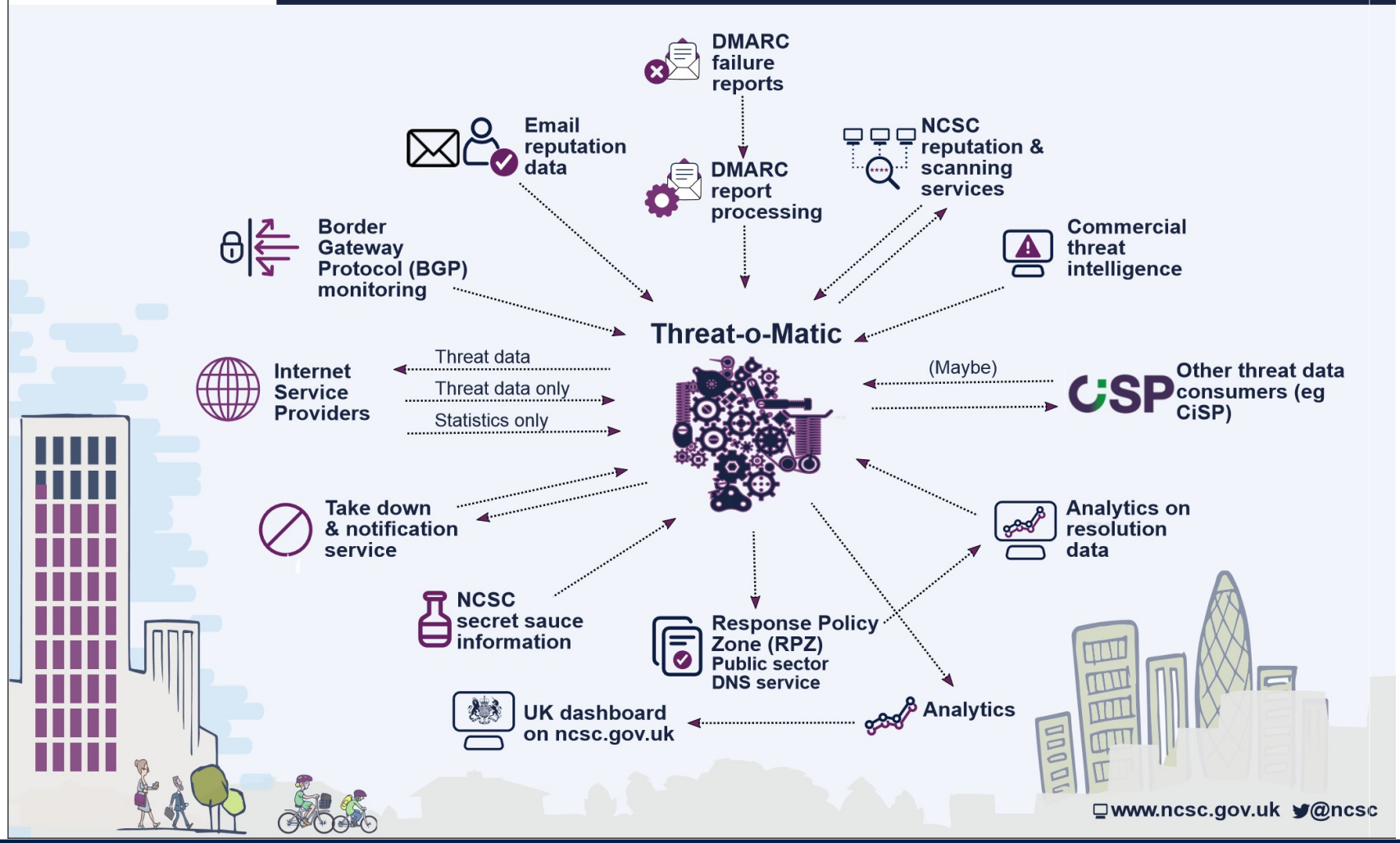
Protect the majority of the people from the majority of the harm caused by the majority of the attacks, the majority of the time.

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre

Active Cyber Defence

The Active Cyber Defence (ACD) Programme outlines how the NCSC intends to tackle - in a relatively automated way - many of the cyber attacks that hit the UK. The diagram below is **not** an architecture, so not all these initiatives will be in place at day one.



National Cyber Security Centre

a part of GCHQ

Active Cyber Defence -

.gov.uk/blog-post/active-cyber-defence-one-year

Blog post

Active Cyber Defence - one year on

Created: 05 Feb 2018
Updated: 05 Feb 2018
Author: Ian Levy
Part of: Cyber strategy, The NCSC

In November 2016, just after the NCSC formally came into existence, and as the National Cyber Security Strategy was launched, I blogged about our ideas for our Active Cyber Defence programme. I described it as an automated set of interventions intended to tackle a range of commodity attacks.

Some people said it sounded great. Some people said I was talking rubbish (many were not quite so polite!).

Well, we said from the start that the NCSC was going to be transparent and open, and we intend to keep that promise. So today, we're publishing a paper that describes the first year of the ACD programme - both the successes and the things that aren't exactly as we'd want. It's a big paper and there's a lot in it. We've tried to draw out the high-level benefits in the Executive Summary, but the rest of it is worth a read if you've got a technical or scientific bent (or have trouble sleeping).

This is only a start and there's lots more to do. But the paper demonstrates that we've already achieved some cool stuff. I think we can summarise by saying that people in the UK are objectively safer in cyberspace because of the ACD programme.

We've got some great plans for the next year, but in the meantime if you want to find out how much malware was sent in the name of government, how many vulnerabilities we found in

Blogs by Topic

- Sociotechnical security (29)
- Identity and passwords (18)
- The NCSC (18)
- Cyber strategy (16)
- End user technology (15)
- End user device (14)
- New talent (14)
- Cyber attacks (10)
- Skills and training (10)
- Vulnerabilities (10)
- Partnerships (9)
- Sectoral engagement (9)
- Cyber threats (7)
- IT infrastructure (7)
- Research (5)
- Digital services (5)
- Cloud security (5)
- Assurance (5)
- Government strategy (4)
- Secure by default (4)
- Operational security (4)
- Design and configuration (4)
- Secure communications (3)
- Technology at OFFICIAL (3)
- Risk management (3)
- Network security (2)

National Cyber Security Centre
a part of GCHQ

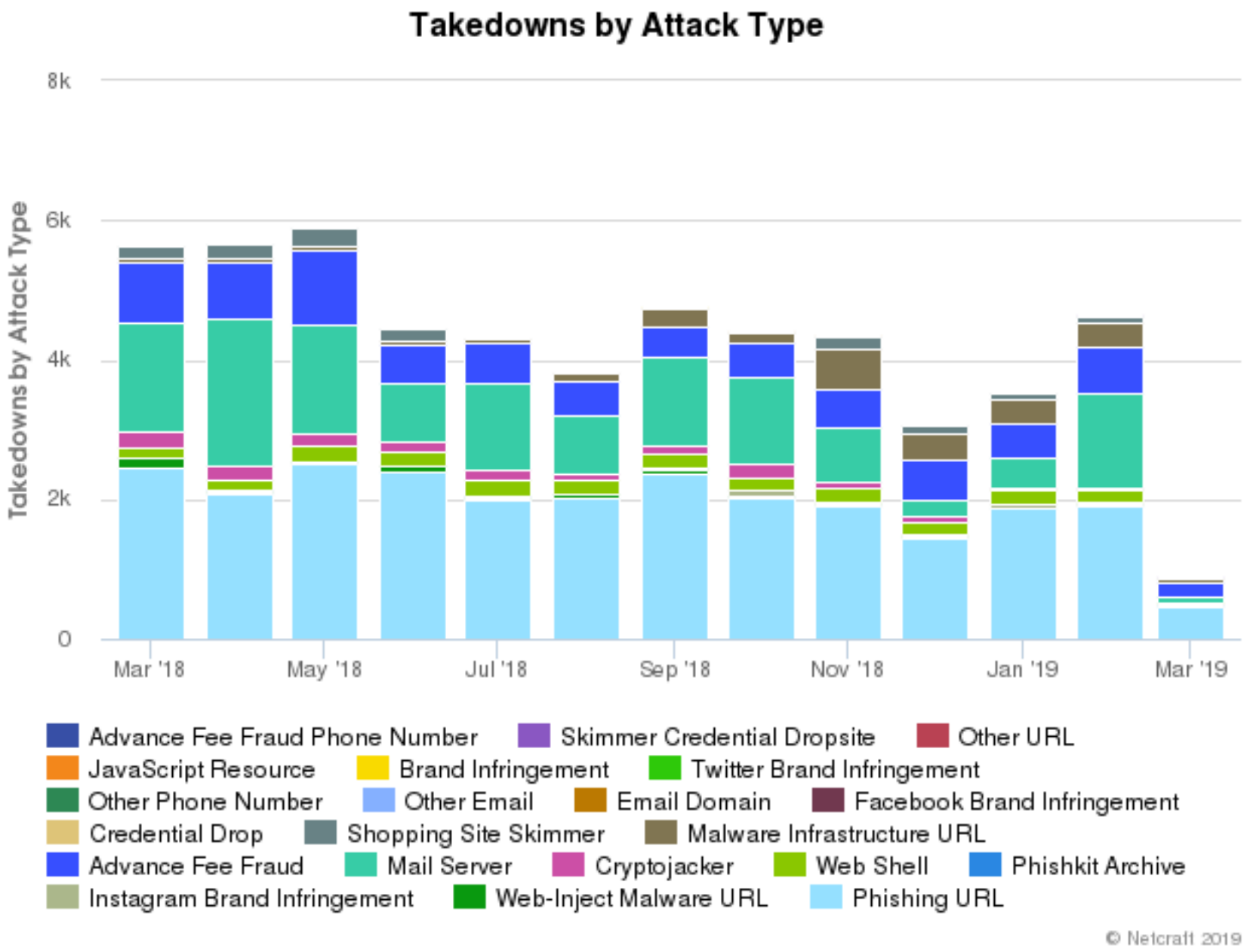
ACD by the numbers

DMARC: 572/1369/6974

Synthetic DMARC : 430k Aug-Nov 2018

HMRC: 16th to 146th

National Cyber Security
a part of GCHQ



National Cyber Security Centre

From: Netcraft Takedown Service <takedown-response+2653399@netcraft.com>
To: webmaster@[redacted].uk
Subject: Issue 2653399: malware attack at https://www[redacted]uk/checkout/cart/
Attachments: report.txt (https://takedown.netcraft.com/view_attachment.php?hash=31d73585906c5e869d2d00222e269ba8)

Dear Sir or Madam,

We have identified a site on your network that has been compromised with malicious javascript which steals credit card details from the site's checkout page:

https://www[redacted]uk/checkout/cart/ [217.174.249.143]

Even if the site does not directly process payment details, the presence of this malicious JavaScript indicates that it has been compromised by a criminal.

You may not have been aware of this attack, however, you are still responsible for removing it.

Would it be possible to have the malware removed as soon as possible?

For more information please see https://incident.netcraft.com/w/e60432ee063d/

Regards,

Netcraft

Phone: +44(0)1225 447500
Fax: +44(0)1225 448600

National Cyber Security Centre

	Date Found	Site	IP	CC	ReverseDNS	ForwardDNS	NetblockOwner	Review Category
+	2017-09-20	income-tax-gov-uk.cf	104.18.52.168	US		cloudflare.com	Cloudflare, Inc.	Suspicious
+	2017-09-13	authorizesecured-hmrc.co.uk				demys.com		Suspicious
+	2017-09-13	government-gateway-servic…	51.15.170.129	FR	te-dns.net	verisign-grs.com	Dedicated Servers and cloud assignment, abuse reports : http:	Suspicious
+	2017-09-11	tax-refunds-hmrc.co.uk	89.36.217.207	DE		tax-refunds-hmrc.co.uk	Cloud Services DC05	Suspicious
+	2017-09-07	hmrc-login.co.uk	198.57.151.195	US	unifiedlayer.com	gator3106.hostgator.com	Unified Layer	Suspicious
+	2017-09-07	loucollgov.uk	94.126.40.154	UK	ai270.net	lcn.com	QUANTUM WEB HOSTING	Suspicious
+	2017-09-06	hmrc-taxrefund.org.uk	134.213.221.69	UK	rackspace.com	demys.com	Cloud Servers UK IP Space	Suspicious

National Cyber Security Centre
a part of GCHQ

ACD by the numbers

25th M arch

~1 47

National Cyber Security Centre
a part of GCHQ

ACD by the numbers

In 2018, Public Sector Protective DNS:

- Protecting about 1.4 million public sector employees
- Blocked 57.4 million queries out of 68.7 billion for 118,527 unique blocks
- Blocked 28 million queries related to 15 DGAs, including Conficker, Ramnit, Suppobox, Tiny Banker, Matsnu, Bedep, Fobber
- Blocked 13,800 queries for specific botnet C2, including Betabot, Graybird, Katrina, Lokibot, StealRat, Godzilla
- Blocked 796,000 queries related to exploit kits, including Magnitude, RIG, Sweet Orange, Neutrino
- 450,000 WannaCry related queries from 15 different departments
- Around 20 APT-related things per week

National Cyber Security Centre
a part of GCHQ

ACD by the numbers

Other crap in the name of government we've cleaned up globally this year:

- 14,071 phishing URLs
- 44,608 Mail servers sending malicious attachments
- 4,107 Mail servers sending Advance Fee Fraud campaigns (419 scams)
- 1,984 Mail servers sending Phishing links
- 546 Malware distribution URLs
- 234 Malware Command & Control Centres
- 175 Malware Infrastructure URLs
- 75 Malicious Web Shells
- Millions of spoofed emails

National Cyber Security Centre
a part of GCHQ

ACD by the numbers

27 hours to 1 hour

138,587

National Cyber Security Centre
a part of GCHQ

ACD by the numbers

5.3% (6/16) to 2.1% (12/18)

National Cyber Security Centre
a part of GCHQ

ACD by the numbers

Other crap we've cleaned up in UK delegated IP space :

- 1,581 Non-consensual *Monero* Miners
- 2,311 Malicious Web Shells
- 2,156 Web-Inject URLs
- 2,333 Credit Card Skimmers attached to website shopping carts (3 months)

National Cyber Security Centre
a part of GCHQ

Scaling : ISPs

BT : 6 million residential customers.

135 million malware C2 blocks/month

National Cyber Security Centre
a part of GCHQ

>1500

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
a part of GCHQ

Search

Guidance | Threats | Incident Management | Marketplace | Education & Research | Insight | Press & Media | Topics

The National Cyber Security Centre

Helping to make the UK the safest place to live and do business online. Read more about the NCSC.

National Cyber Security Centre
a part of GCHQ

Russian cyber attacks

Foreign Secretary's statement on Russia's campaign of cyber attacks and the NCSC's identification of the actors as Russia's military intelligence service, the GRU.

NCSC's technical advisory: Indicators of Compromise for Malware used by APT28.

National Cyber Security Centre
a part of GCHQ

Alerts and Advisories

Advisory: Russian state-sponsored cyber actors targeting network infrastructure devices

Created: 16 Apr 2018
Updated: 16 Apr 2018

This advisory provides information on the worldwide cyber exploitation of network infrastructure devices (e.g. routers, switches, firewalls, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors.

Report Download

Introduction

This joint Technical Alert (TA) or advisory is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC). It provides information on the worldwide cyber exploitation of network infrastructure devices (e.g. routers, switches, firewalls, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors.

Download the advisory here or, alternatively, use the download tab at the top of this page.

National Cyber Security Centre
a part of GCHQ

Search

Guidance | Threats | Incident Management | Marketplace | Education & Research | Ins

Home

UK Internet Edge Router Devices: Advisory

Created: 11 Aug 2017
Updated: 11 Aug 2017

You should read this advice if you are an internet service provider, or an enterprise that manages your own customer edge (CE) devices.

Summary

- This advice builds on existing technical guidance on the NCSC website.
- The NCSC is aware of a number of router compromises in telecommunications companies and Internet Service Providers, where a hostile actor has extracted configuration files from internet facing network devices. The configuration files can contain administrative credentials which may then be used to compromise all traffic passing through the router, and allow the actor to target other devices on the network. They have also gained interactive engineer access to some routers.
- In some cases where routers have been successfully compromised, the NCSC is aware that the hostile actor has created Generic Routing Encapsulation (GRE) tunnels to extract traffic traversing the router. They do this by using an Access Control List which they control on the compromised router, and exfiltrate the traffic they are interested in to infrastructure which they control, which is often outside the victim's country. In these cases where the NCSC is aware, we have already contacted the impacted organisations.
- The incident is still under investigation, and the NCSC is working with ISPs to make affected entities aware, and support remediation.
- This advisory note details mitigation strategies to secure networks against these

National Cyber Security Centre
a part of GCHQ

Search

Guidance | Threats | Incident Management | Marketplace | Education & Research | Insig

Published guidance | Infographics | NCSC glossary

Home > Guidance > Published guidance

Guidance

Internet edge device security

Created: 12 May 2017
Updated: 12 May 2017

What to do if you suspect your internet edge router has been compromised

Introduction

An *internet edge router* is the device which provides your network with its 'window on the world'. An adversary who has control over this equipment is in a particularly privileged position to affect the security of your network. Certain attacks that are very difficult over the internet become extremely easy when launched from equipment on your network edge.

Though organisations of almost any size may have internet facing routers, this guidance is aimed specifically at larger, enterprise-level installations.

Your ISP might manage these devices or you may handle things in-house. Either way, if you suspect an internet edge router has been compromised, you must act immediately. Ensure that your traffic does not go through the compromised device either by reconfiguring your own systems or contacting your ISP to have them re-route your traffic away from that router. In extremis, disabling the router in-situ may be preferable.

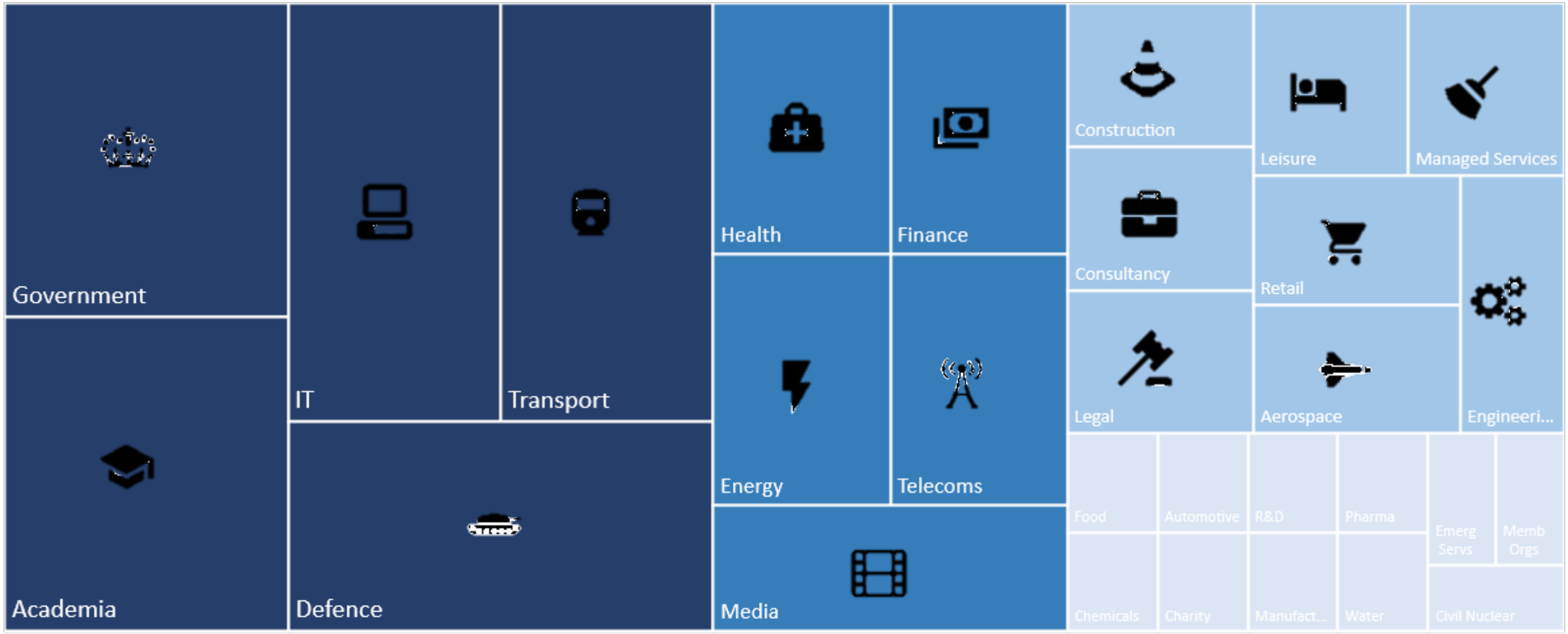
This document details how to determine whether your router is vulnerable, and the potential harm that could come from such a security breach.

How can I tell if my internet edge router is

National Cyber Security Centre

a part of GCHQ

Number of cyber security incidents by industry sector, June 2018 - February 2019



National Cyber Security Centre
a part of GCHQ

It’s not all 0-day wielding nation states

National Cyber Security Centre
a part of GCHQ

If your administrators browse the web or get email using their admin machine or account, you're too stupid to help.

National Cyber Security Centre
a part of GCHQ

What’s connected to your external IP ranges and who’s responsible for looking after it?

National Cyber Security Centre
a part of GCHQ

Creds matter.

National Cyber Security Centre
a part of GCHQ

Why SMART?

National Cyber Security Centre
a part of GCHQ

Security being baked in to protocols.

Designs need to be cognisant of *actual* attacks

National Cyber Security Centre
a part of GCHQ

People are increasingly part of protocols

National Cyber Security Centre
a part of GCHQ

Bad guys can use the shiny too

National Cyber Security Centre
a part of GCHQ

Adversaries are not passive

National Cyber Security Centre

a part of GCHQ

Security != encryption

National Cyber Security Centre
a part of GCHQ

Side-effects can scale badly from a defence point of view

National Cyber Security Centre
a part of GCHQ

Need to make sure that we don’t enable new attack modalities

Security != Privacy != Resilience

National Cyber Security Centre
a part of GCHQ

Questions?