NERSOU | Protecting communities from organised crime | NERCCU North East Regional Cyber Crime Unit

NORTH EAST REGIONAL SPECIAL OPERATIONS UNIT

Protecting **businesses** and **communities** in the North East from common cyber attacks

This report has been produced on **Monday 16 May 2022** and contains information for the last week.

The following information has been produced via an automated process and obtained from multiple sources which can be seen in each section; the relevance and accuracy of the data can not be verified.

If you have received this report in error; or can provide recommendations to any sources that should be added or removed please contact jonathan.green@nersou.police.uk

FIVE EYES - UK; US; Canada; Australia; New Zealand:

The Five Eyes (FVEY) is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.

1. https://www.ncsc.gov.uk/
2. https://www.cisa.gov/cybersecurity
3. https://cyber.gc.ca/en/
4. https://www.cyber.gov.au/
5. https://www.ncsc.govt.nz/

1. Relaunching the NCSC's Cloud security guidance collection

https://www.ncsc.gov.uk/blog-post/relaunching-the-ncscs-cloud-security-guidance-collection

Published: Wed, 11 May 2022 23:00:00 GMT
Source: https://www.ncsc.gov.uk/api/1/services/v1/all-rss-feed.xml

2. The Technology Assurance principles

https://www.ncsc.gov.uk/blog-post/the-technology-assurance-principles

Published: Tue, 10 May 2022 23:00:00 GMT
Source: https://www.ncsc.gov.uk/api/1/services/v1/all-rss-feed.xml

3. Laying the new foundations for enterprise device security

https://www.ncsc.gov.uk/blog-post/laying-foundations-enterprise-device-security

Published: Mon, 09 May 2022 23:00:00 GMT
Source: https://www.ncsc.gov.uk/api/1/services/v1/all-rss-feed.xml

4. Organisational use of Enterprise Connected Devices

https://www.ncsc.gov.uk/report/organisational-use-of-enterprise-connected-devices

Published: Mon, 09 May 2022 23:00:00 GMT
Source: https://www.ncsc.gov.uk/api/1/services/v1/all-rss-feed.xml

5. ACD - The Fifth Year: Summary of Key Findings

https://www.ncsc.gov.uk/report/acd-the-fifth-year

Published: Mon, 09 May 2022 23:00:00 GMT
Source: https://www.ncsc.gov.uk/api/1/services/v1/all-rss-feed.xml

6. Putting staff welfare at the heart of incident response

https://www.ncsc.gov.uk/guidance/putting-staff-welfare-at-the-heart-of-incident-response

Published: Mon, 09 May 2022 23:00:00 GMT
Source: https://www.ncsc.gov.uk/api/1/services/v1/all-rss-feed.xml

7. CISA Temporarily Removes CVE-2022-26925 from Known Exploited Vulnerability Catalog

https://us-cert.cisa.gov/ncas/current-activity/2022/05/13/cisa-temporarily-removes-cve-2022-26925-known-exploited

Published: Fri, 13 May 2022 20:20:30 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

8. Adobe Releases Security Updates for Multiple Products
https://us-cert.cisa.gov/ncas/current-activity/2022/05/12/adobe-releases-security-updates-multiple-products
Published: Thu, 12 May 2022 11:16:49 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

9. Google Releases Security Updates for Chrome
https://us-cert.cisa.gov/ncas/current-activity/2022/05/11/google-releases-security-updates-chrome
Published: Wed, 11 May 2022 12:00:00 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

10. Microsoft Releases May 2022 Security Updates
https://us-cert.cisa.gov/ncas/current-activity/2022/05/11/microsoft-releases-may-2022-security-updates
Published: Wed, 11 May 2022 11:00:00 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

11. CISA Adds One Known Exploited Vulnerability to Catalog
https://us-cert.cisa.gov/ncas/current-activity/2022/05/11/cisa-adds-one-known-exploited-vulnerability-catalog
Published: Wed, 11 May 2022 11:00:00 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

12. CISA Joins Partners to Release Advisory on Protecting MSPs and their Customers
https://us-cert.cisa.gov/ncas/current-activity/2022/05/11/cisa-joins-partners-release-advisory-protecting-msps-and-their
Published: Wed, 11 May 2022 07:00:00 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

13. Protecting Against Cyber Threats to Managed Service Providers and their Customers
https://us-cert.cisa.gov/ncas/alerts/aa22-131a
Published: Wed, 11 May 2022 07:00:00 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

14. CISA Adds One Known Exploited Vulnerability to Catalog
https://us-cert.cisa.gov/ncas/current-activity/2022/05/10/cisa-adds-one-known-exploited-vulnerability-catalog
Published: Tue, 10 May 2022 13:50:28 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

15. U.S. Government Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors
https://us-cert.cisa.gov/ncas/current-activity/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian
Published: Tue, 10 May 2022 09:27:23 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

16. Microsoft Releases Security Advisory for Azure Data Factory and Azure Synapse Pipelines
https://us-cert.cisa.gov/ncas/current-activity/2022/05/10/microsoft-releases-security-advisory-azure-data-factory-and-azure
Published: Tue, 10 May 2022 07:00:00 EDT
Source: https://us-cert.cisa.gov/ncas/all.xml

17. Delta Electronics CNCSoft
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-01
Published: Thu, 12 May 2022 10:52:10 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

18. Mitsubishi Electric MELSOFT iQ AppPortal
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-02
Published: Thu, 12 May 2022 10:50:22 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

19. Inkscape in Industrial Products
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-03

Published: Thu, 12 May 2022 10:48:49 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

20. Cambium Networks cnMaestro
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-04
Published: Thu, 12 May 2022 10:46:21 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

21. Siemens Industrial PCs and CNC devices
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-05
Published: Thu, 12 May 2022 10:44:29 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

22. Siemens SIMATIC WinCC
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-06
Published: Thu, 12 May 2022 10:42:23 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

23. Siemens SICAM P850 and SICAM P855
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-07
Published: Thu, 12 May 2022 10:40:12 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

24. Siemens Industrial Products with OPC UA
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-08
Published: Thu, 12 May 2022 10:38:16 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

25. Siemens JT2GO and Teamcenter Visualization
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-09
Published: Thu, 12 May 2022 10:36:59 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

26. Siemens Desigo PXC and DXR Devices
https://us-cert.cisa.gov/ics/advisories/icsa-22-132-10
Published: Thu, 12 May 2022 10:34:00 EDT
Source: https://us-cert.cisa.gov/ics/advisories/advisories.xml

27. End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003)
https://cyber.gc.ca/en/guidance/end-user-device-security-bring-your-own-device-byod-deployment-models-itsm70003
Published: Mon, 09 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/guidance

28. [Control Systems] Delta Electronics security advisory (AV22-271)
https://cyber.gc.ca/en/alerts/control-systems-delta-electronics-security-advisory-av22-271
Published: Fri, 13 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

29. [Control Systems] Mitsubishi Electric security advisory (AV22-272)
https://cyber.gc.ca/en/alerts/control-systems-mitsubishi-electric-security-advisory-av22-272
Published: Fri, 13 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

30. [Control Systems] Cambium Networks security advisory (AV22-273)
https://cyber.gc.ca/en/alerts/control-systems-cambium-networks-security-advisory-av22-273
Published: Fri, 13 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

31. [Control Systems] Inkscape security advisory (AV22-274)
https://cyber.gc.ca/en/alerts/control-systems-inkscape-security-advisory-av22-274
Published: Fri, 13 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

32. Dell security advisory (AV22-275)
https://cyber.gc.ca/en/alerts/dell-security-advisory-av22-275

Published: Fri, 13 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

33. Ubuntu security advisory (AV22-270)
https://cyber.gc.ca/en/alerts/ubuntu-security-advisory-av22-270
Published: Thu, 12 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

34. Dell security advisory (AV22-265)
https://cyber.gc.ca/en/alerts/dell-security-advisory-av22-265
Published: Wed, 11 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

35. Adobe security advisory (AV22-264)
https://cyber.gc.ca/en/alerts/adobe-security-advisory-av22-264
Published: Wed, 11 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

36. SAP security advisory – May 2022 monthly rollup (AV22-267)
https://cyber.gc.ca/en/alerts/sap-security-advisory-may-2022-monthly-rollup-av22-267
Published: Wed, 11 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

37. HPE security advisory (AV22-266)
https://cyber.gc.ca/en/alerts/hpe-security-advisory-av22-266
Published: Wed, 11 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

38. Red Hat security advisory (AV22-268)
https://cyber.gc.ca/en/alerts/red-hat-security-advisory-av22-268
Published: Wed, 11 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

39. Intel security advisory (AV22-269)
https://cyber.gc.ca/en/alerts/intel-security-advisory-av22-269
Published: Wed, 11 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

40. [Control Systems] Eaton security advisory (AV22-257)
https://cyber.gc.ca/en/alerts/control-systems-eaton-security-advisory-av22-257
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

41. Microsoft security advisory – May 2022 Monthly Rollup (AV22-258)
https://cyber.gc.ca/en/alerts/microsoft-security-advisory-may-2022-monthly-rollup-av22-258
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

42. [Control Systems] Siemens security advisory (AV22-260)
https://cyber.gc.ca/en/alerts/control-systems-siemens-security-advisory-av22-260
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

43. [Control Systems] Mitsubishi Electric security advisory (AV22-262)
https://cyber.gc.ca/en/alerts/control-systems-mitsubishi-electric-security-advisory-av22-262
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

44. [Control Systems] Schneider Electric security advisory (AV22-259)
https://cyber.gc.ca/en/alerts/control-systems-schneider-electric-security-advisory-av22-259
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

45. [Control Systems] AVEVA security advisory (AV22-261)
https://cyber.gc.ca/en/alerts/control-systems-aveva-security-advisory-av22-261
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

46. [Control Systems] Adminer security advisory (AV22-256)
https://cyber.gc.ca/en/alerts/control-systems-adminer-security-advisory-av22-256
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

47. Google Chrome security advisory (AV22-263)
https://cyber.gc.ca/en/alerts/google-chrome-security-advisory-av22-263
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

48. IBM security advisory (AV22-255)
https://cyber.gc.ca/en/alerts/ibm-security-advisory-av22-255
Published: Mon, 09 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

49. F5 security advisory (AV22-254)
https://cyber.gc.ca/en/alerts/f5-security-advisory-av22-254
Published: Mon, 09 May 2022 00:00:00 +0000
Source: https://cyber.gc.ca/webservice/en/rss/alerts

50. Joint cyber security advisory on protecting against cyber threats to managed service providers and their customers
https://cyber.gc.ca/en/news/joint-cyber-security-advisory-protecting-against-cyber-threats-managed-service-providers
Published: Mon, 09 May 2022 11:42:24 +0000
Source: https://cyber.gc.ca/webservice/en/rss/news

51. Protecting Against Cyber Threats to Managed Service Providers and their Customers
https://www.cyber.gov.au/acsc/view-all-content/advisories/protecting-against-cyber-threats-managed-service-providers-and-their-customers
Published: Thu, 12 May 2022 22:00:00 +1000
Source: https://www.cyber.gov.au/acsc/view-all-content/advisories/rss

52. Multiple vulnerabilities present in F5 products
https://www.cyber.gov.au/acsc/view-all-content/alerts/multiple-vulnerabilities-present-f5-products
Published: Mon, 09 May 2022 22:00:00 +1000
Source: https://www.cyber.gov.au/acsc/view-all-content/alerts/rss

53. Joint advisory released for Managed Service Providers and Customers to mitigate cybersecurity risks
https://www.cyber.gov.au/acsc/view-all-content/news/joint-advisory-released-managed-service-providers-and-customers-mitigate-cybersecurity-risks
Published: Thu, 12 May 2022 22:00:00 +1000
Source: https://www.cyber.gov.au/acsc/view-all-content/news/rss

54. Joint statement - attribution to Russia for malicious cyber activity against European networks
https://www.cyber.gov.au/acsc/view-all-content/news/joint-statement-attribution-russia-malicious-cyber-activity-against-european-networks
Published: Wed, 11 May 2022 22:00:00 +1000
Source: https://www.cyber.gov.au/acsc/view-all-content/news/rss

Trusted Sources and Referenced Material:

1. https://www.actionfraud.police.uk/
2. https://takefive-stopfraud.org.uk/
3. https://iasme.co.uk/
4. https://haveibeenpwned.com/
5. https://www.getsafeonline.org/
6. https://www.globalcyberalliance.org/

7. https://www.trendmicro.com/

1. Cyber Essentials Myth Busting
https://iasme.co.uk/cyber-blog/cyber-essentials-myth-busting/\n
Published: Thu, 12 May 2022 15:27:49 +0000
Source: https://iasme.co.uk/feed

2. BlackBerry Fans - 174,168 breached accounts
https://haveibeenpwned.com/PwnedWebsites#BlackBerryFans\n
Published: Mon, 16 May 2022 02:15:13 Z
Source: https://feeds.feedburner.com/HavelBeenPwnedLatestBreaches

3. OGUsers (2021 breach) - 348,302 breached accounts
https://haveibeenpwned.com/PwnedWebsites#OGUsers2021\n
Published: Mon, 16 May 2022 00:40:46 Z
Source: https://feeds.feedburner.com/HavelBeenPwnedLatestBreaches

4. Paragon Cheats - 188,089 breached accounts
https://haveibeenpwned.com/PwnedWebsites#ParagonCheats\n
Published: Sat, 14 May 2022 02:26:40 Z
Source: https://feeds.feedburner.com/HavelBeenPwnedLatestBreaches

5. Routing Security Survey Report: Findings IV
https://www.globalcyberalliance.org/routing-security-survey-report-findings-iv/\n
Published: Thu, 12 May 2022 20:29:44 +0000
Source: https://www.globalcyberalliance.org/feed/

6. Threat Roundup for May 6 to May 13
http://blog.talosintelligence.com/2022/05/threat-roundup-0506-0513.html\n
Published: Fri, 13 May 2022 12:04:28 PDT
Source: https://blog.talosintelligence.com/feeds/posts/default

7. EMEAR Monthly Talos Update: Wiper malware
http://blog.talosintelligence.com/2022/05/emear-monthly-talos-update-wiper-malware.html\n
Published: Fri, 13 May 2022 05:00:00 PDT
Source: https://blog.talosintelligence.com/feeds/posts/default

8. Threat Source newsletter (May 12, 2022) — Mandatory MFA adoption is great, but is it too late?
http://blog.talosintelligence.com/2022/05/threat-source-newsletter-may-12-2022.html\n
Published: Thu, 12 May 2022 11:00:00 PDT
Source: https://blog.talosintelligence.com/feeds/posts/default

9. Vulnerability Spotlight: How an attacker could chain several vulnerabilities in an industrial wireless router to gain root access
http://blog.talosintelligence.com/2022/05/blog-post-.html\n
Published: Thu, 12 May 2022 05:00:00 PDT
Source: https://blog.talosintelligence.com/feeds/posts/default

10. Bitter APT adds Bangladesh to their targets
http://blog.talosintelligence.com/2022/05/bitter-apt-adds-bangladesh-to-their.html\n
Published: Wed, 11 May 2022 05:00:11 PDT
Source: https://blog.talosintelligence.com/feeds/posts/default

11. Sandstone CTO shares how to assess cyber risk in the cloud
https://www.trendmicro.com/en_us/ciso/22/e/cyber-risk-assessment-sandstone-cto.html\n
Published: Fri, 13 May 2022 00:00:00 +0000
Source: https://feeds.feedburner.com/TrendMicroSimplySecurity

12. S4x22: ICS Security Creates the Future
https://www.trendmicro.com/en_us/research/22/e/ics-security-event-s4-2022-review.html\n
Published: Thu, 12 May 2022 00:00:00 +0000
Source: https://feeds.feedburner.com/TrendMicroSimplySecurity

13. The Difference Between Virtual Machines and Containers
https://www.trendmicro.com/en_us/devops/22/e/the-difference-between-virtual-machines-and-containers.html\n

Published: Thu, 12 May 2022 00:00:00 +0000
Source: https://feeds.feedburner.com/TrendMicroSimplySecurity

14. Adding Guardrails To A Cloud Account After The Fact

https://www.trendmicro.com/en_us/devops/22/e/cloud-configuration-management-guardrails.html\n
Published: Wed, 11 May 2022 00:00:00 +0000
Source: https://feeds.feedburner.com/TrendMicroSimplySecurity

15. Security Above and Beyond CNAPPs

https://www.trendmicro.com/en_us/research/22/e/more-secure-than-cnapps.html\n
Published: Tue, 10 May 2022 00:00:00 +0000
Source: https://feeds.feedburner.com/TrendMicroSimplySecurity

16. Examining the Black Basta Ransomware's Infection Routine

https://www.trendmicro.com/en_us/research/22/e/examining-the-black-basta-ransomwares-infection-routine.html\n
Published: Mon, 09 May 2022 00:00:00 +0000
Source: https://feeds.feedburner.com/TrendMicroSimplySecurity