This week's threat report, UK-based cybercriminals targeting healthcare, persistent supply chain attacks, and a critical Chrome vulnerability that's already being exploited. Let's get started.

UK Teenagers Arrested in Connection with Major International Healthcare Hacks

The UK’s National Crime Agency (NCA) arrested two teenagers, aged 18 and 19, for their alleged involvement in the “Scattered Spider” cybercrime group. This group is linked to major attacks on critical infrastructure, including Transport for London. One of the suspects is also charged in the US with attacks on American healthcare organisations, including SSM Health and Sutter Health, which were compromised through third-party software vendors. The group is known for using sophisticated social engineering techniques to gain access to networks before deploying ransomware.

This is a reminder that significant cyber threats can originate from within the UK. The targeting of healthcare, combined with the use of social engineering and attacks on the software supply chain, presents a direct risk to NHS trusts, private clinics, and health tech companies that rely on a complex network of software and services.

Recommendations:

- Conduct a thorough review of all third-party software vendors and their security postures.
- Enhance staff training on identifying and reporting sophisticated social engineering and phishing attempts.
- Ensure that all systems have multi-factor authentication (MFA) enabled to mitigate the impact of stolen credentials.

Major US Healthcare Data Breaches Highlight Third-Party Vendor Risks

In a single week, three separate data breaches at US healthcare providers, Goshen Medical Center, Retina Group of Florida, and Medical Associates of Brevard, exposed the personal and medical data of over 850,000 individuals.

A consistent pattern in these and other major healthcare breaches, including the incident at Change Healthcare, is the exploitation of vulnerabilities within third-party software suppliers. Attackers are increasingly targeting the healthcare supply chain to gain access to the sensitive data held by providers.

The UK’s digital health ecosystem, like the US is also heavily reliant on a wide range of software and service providers. These incidents demonstrate that even with robust internal security, a vulnerability in a single supplier can lead to a massive data breach. It is crucial for healthcare organisations to have a clear understanding of their supply chain and to hold their vendors to the highest security standards.

Recommendations:

- Implement a comprehensive third-party risk management programme.
- Include security clauses and the right to audit in all vendor contracts.
- Develop an incident response plan that specifically addresses supply chain breaches.

Google Chrome Zero-Day Vulnerability Under Active Exploitation

Google has released an emergency patch for a high-severity Chrome vulnerability (CVE-2025-10585) that is already being actively exploited. This is a type confusion flaw in Chrome's V8 JavaScript and WebAssembly engine, which can lead to system crashes, arbitrary code execution, and potentially full system compromise through malicious web pages.

Google's Threat Analysis Group discovered the flaw. Although specific details about the attackers haven't been disclosed, the group typically tracks nation-state actors and commercial spyware vendors.

Organisations rely heavily on web browsers to access electronic health records, patient management systems, and cloud-based healthcare applications. A compromised browser can serve as a gateway for attackers to access sensitive data and critical healthcare systems. Given that this vulnerability is already being exploited, immediate action is required.

Recommendations:

- Update Chrome immediately to version 140.0.7339.185/.186 (Windows/macOS) or 140.0.7339.185 (Linux).
- Force an immediate update by typing chrome://settings/help in the address bar and restarting the browser.
- Consider implementing browser security policies that automatically update browsers across your organisation.
- Review and restrict access to sensitive healthcare systems from potentially compromised browsers until patching is complete.

{% module_block module "widget_f6998f19-9555-4241-b9b4-512408e1378d" %}{% module_attribute "child_css" is_json="true" %}{% raw %}{}{% endraw %}{% end_module_attribute %}{% module_attribute "css" is_json="true" %}{% raw %}{}{% endraw %}{% end_module_attribute %}{% module_attribute "definition_id" is_json="true" %}{% raw %}null{% endraw %}{% end_module_attribute %}{% module_attribute "extra_classes" is_json="true" %}{% raw %}"widget-type-form"{% endraw %}{% end_module_attribute %}{% module_attribute "field_types" is_json="true" %}{% raw %}
{"follow_up_type_simple":"boolean","form_follow_ups_workflow_id":"workflow","notifications_override_email_addresses":"email","form":"form","follow_up_type_automation":"boolea
{% endraw %}{% end_module_attribute %}{% module_attribute "form" is_json="true" %}{% raw %}{"form_id":"7417466b-b98b-47b7-8b1e-a1c25a9431b1","form_type":"HUBSPOT","message":"Thanks for submitting the form.","redirect_id":null,"redirect_url":"http://www.google.com","response_type":"redirect"}{% endraw %}{% end_module_attribute %}{% module_attribute "label" is_json="true" %}{% raw %}null{% endraw %}{% end_module_attribute %}{% module_attribute "module_id" is_json="true" %}{% raw %}1155238{% endraw %}{% end_module_attribute %}{% module_attribute "path" is_json="true" %}{% raw %}"@hubspot/form"{% endraw %}{% end_module_attribute %}{% module_attribute "schema_version" is_json="true" %}{% raw %}2{% endraw %}{% end_module_attribute %}{% module_attribute "smart_objects" is_json="true" %}{% raw %}[]{% endraw %}{% end_module_attribute %}{% module_attribute "smart_type" is_json="true" %}{% raw %}"NOT_SMART"{% endraw %}{% end_module_attribute %}{% module_attribute "tag" is_json="true" %}{% raw %}"module"{% endraw %}{% end_module_attribute %}{% module_attribute "type" is_json="true" %}{% raw %}"module"{% endraw %}{% end_module_attribute %}{% module_attribute "wrap_field_tag" is_json="true" %}{% raw %}"div"{% endraw %}{% end_module_attribute %}{% end_module_block %}

{% module_block module "widget_4f28fca2-1a75-44a4-a343-6beef4f37ffe" %}{% module_attribute "child_css" is_json="true" %}{% raw %}null{% endraw %}{% end_module_attribute %}{% module_attribute "css" is_json="true" %}{% raw %}null{% endraw %}{% end_module_attribute %}{% module_attribute "label" is_json="true" %}{% raw %}null{% endraw %}{% end_module_attribute %}{% module_attribute "module_id" is_json="true" %}{% raw %}202392304878{% endraw %}{% end_module_attribute %}{% module_attribute "schema_version" is_json="true" %}{% raw %}2{% endraw %}{% end_module_attribute %}{% module_attribute "tag" is_json="true" %}{% raw %}"module"{% endraw %}{% end_module_attribute %}{% end_module_block %}