For immediate release

CSIS Threat Matrix Report highlights challenges and shifts in the cyber threat landscape

A new report from CSIS Security Group reveals a significant rise in nation-state attacks, hacktivism and advanced cyber attacks, and offers actionable insights to help organisations strengthen their defences

CSIS reports over one billion compromised credentials circulating on the dark web every month

Copenhagen and London,13 December 2024: CSIS Security Group ("CSIS") has released its latest Threat Matrix Report – Autumn 2024, which provides in-depth research and analysis of the current cyber threat landscape. The report exposes the growing frequency and complexity of cyberattacks in the first half of 2024, including nation-state attacks, hacktivism, infostealer malware, ransomware and sophisticated phishing campaigns.

The report also highlights a rise in incident response cases where initial access was gained through stolen credentials leaked on the dark web, along with the importance of knowing your supply chain to mitigate both malicious and non-malicious incidents. CSIS's research and analysis also shows that hacktivist groups are continuing to organise and form alliances, with the aim of launching DDoS attacks and disrupting critical infrastructure.

"Incidents such as the compromise of Microsoft by Midnight Blizzard, who are linked to Russia's SVR, and North Korean threat actors adopting zero-day exploits, demonstrate the increasing sophistication and boldness of nation-state actors," explains CSIS CEO, Daniel Shepherd. "With these cybercriminals successfully adopting advanced technologies to exploit weakness in systems, the need for more robust intelligence-driven defences and international cooperation has never been greater.

"Our latest Threat Matrix report is both a warning and a guide for organisations to urgently build greater resilience against these evolving threats."

The report includes a host of facts and figures based on CSIS research. For example, there are now over 1 billion compromised credentials circulating on the dark web each month. It also reveals the most prolific ransomware operators in the first half of 2024, broken down by month. Despite some disruptions to its operations, lockbit3 topped the list overall in terms of numbers of attack. However, RansomHub, which was first identified in February 2024, grew fast to become became the top ransomware operator for June 2024.

USA tops the list of countries targeted by ransomware, with 47% of all attacks. The UK comes in second with 7%, followed by Canada at 6%. In terms of industries targeted, manufacturing experienced 22% of ransomware attacks in the first half of 2024, followed by healthcare with 10%, technology at 9% and education at 7%.

The report also shows the top ten brands targeted by phishing. Apple is in the number one spot at 25%, followed by the Royal Mail at 12%. Also included on the list are Ebay, HMRC, Microsoft, Amazon and Booking.com. The top 10 phishing hosts in the first half of 2024 are also revealed, with SonderCloud, Cloudflare and Tencent leading the list.

The CSIS Threat Matrix Report provides detailed Real-World Scenarios, including a RansomHub ransomware attack, and a corporate breach on a public facing VPN. These scenarios include information on reported incidents, the resulting investigation and the solutions implemented. They also provide lessons learned and recommendations to help organisations to become more resilient and improve defences against evolving cyber threats.

The rise of infostealers was notable in the first half of 2024, with recent Lumma Stealer upgrades contributing significantly to the growth. There is a direct link between infostealers, compromised credentials, and the risk of network compromise and ransomware attacks. CSIS identifies three of the most effective distribution methods for Lumma Stealer - fake cracked software delivered via piracy sites; FakeBat Loader-as-a-Service, which creates fake landing pages prompting users to update Chrome; and fake CAPTCHA pages, which is the newest distribution method.

CSIS's report underscores the critical need for threat intelligence, timely patch management, and enhanced network monitoring, as well as the need for robust incident response. Organisations are urged to use this report as a strategic resource to bolster their cybersecurity postures. With its detailed case studies and expert recommendations, the Threat Matrix Report provides actionable insights for decision-makers in both the public and private sectors.

The Threat Matrix Report is available for download at https://www.csis.com/the-hub/#ThreatMatrixReport

[ends]

About CSIS Security Group A/S

Founded in 2003, CSIS is a leading provider of advanced cybersecurity capabilities, focused on actionable and intelligence-driven detection and response services.

We are the preferred cybersecurity partner to notable organisations across various sectors, including Banking & Financial Services, Energy & Utilities, Manufacturing, Transportation & Logistics, as well as Government & Public Sector. We are a trusted adviser to law enforcement agencies (including the FBI, NCA, Europol) and are also sought-after speakers for public and closed-community conferences around the world.

Additionally, our depth of expertise and distinguished reputation ensure that we are regularly called upon as expert commentators on cyber topics for the media

For media enquiries:

Sarah Ward, PRPR, sarahw@prpr.co.uk , +44 1 442 245030