Threat Report 24th March 2023

The NCSC's threat report is drawn from recent open source reporting.

Mandiant report that UNC3886 actor is targeting firewalls, IOT devices and VPNs

The cyber security company Mandiant has published a blog detailing ongoing campaigns by a Chinese espionage threat actor it calls UNC3886. The actor takes advantage of technologies that don't support endpoint detection response, such as firewalls, IoT devices, hypervisors and VPN technologies.

The actor has exploited zero-day vulnerabilities and then deployed custom malware as an attack vector before traversing the target environment and gaining persistence.

The report that concludes that communication and collaboration across organisations is essential for both vendors and investigators to help mitigate the activity.

CISA establishes Ransomware Vulnerability Warning Pilot programme

The Cybersecurity and Infrastructure Security Agency (CISA) has launched the Ransomware Vulnerability Warning Pilot (RVWP), which will alert critical infrastructure providers in the US of potential internet-accessible vulnerabilities linked to known threat actors and ransomware attacks.

CISA has reported they initiated the RVWP by alerting 93 organisations to the 'ProxyNotShell' vulnerability in certain instances of organisations using Microsoft Exchange.

The NCSC provides a range of advice, guidance and content aimed specifically at those with an interest in UK Critical National Infrastructure as part of the CNI Hub.

DNS data shows one in ten organisations have malware traffic on their networks

An investigation by Akamai has shown that between 10% and 16% of organisations had Domain Name System (DNS) traffic originating on their network towards command-and-control (C2) servers associated with known botnets and various other malware threats.

The report also showed that over 9% of devices that generated C2 traffic, did so to domain names associated with known ransomware threats. Of these, REvil and LockBit were the most common ones.

The NCSC has produced guidance on the selection and deployment of protective DNS and there is also the Protective DNS for public sector organisations.

TrendMicro on the return of Emotet

A report by TrendMicro shows that Emotet activity resumed in March, using a botnet to deliver malicious documents via Zip file attachments to emails.

The documents use social engineering tactics to encourage the user to enable macros as Microsoft disabled macros by default in 2022. The botnet also uses binary padding to artificially inflate the file size in order to avoid triggering some security solutions.

The NCSC has guidance on implementing email security solutions and how to mitigate against malware attacks.

PUBLISHED

24 March 2023