BlueHat 2023: Hunting Qakbot with Daniel Taylor & Ben Magee

Published: 2023-03-02 · Archived: 2026-04-05 16:55:13 UTC

When it comes to attack surfaces, there are few quite as large as that of NHS England’s Microsoft Defender for Endpoint estate. With close to 1.7 million endpoints enrolled in a tenant, spanning thousands of separate organizations across the healthcare service, it presents a uniquely challenging environment to protect – one where cyber incidents can have very real, human consequences. How then do we go about defending an IT estate as large and complex as this one? It's a challenge that couldn’t be better illustrated than with the perpetual battle against Qakbot. With delivery mechanisms and TTPs that shift week to week, a repertoire ranging from access-for-sale to the deployment of ransomware and no scruples about targeting healthcare organizations from its operators, Qakbot truly is a formidable adversary. In this talk, Dan Taylor and Ben Magee from NHS England walk through: • A brief overview of the NHS and the role NHS Digital CSOC plays in its defense • The scale of the challenges facing security teams tasked with securing the NHS against the likes of Qakbot, and why common malware poses such an acute threat • The critical role threat hunting (and intelligence) plays in that defense, with technical breakdowns of Qakbot TTPs, the methods we use to stay ahead of them, and the key advantages afforded by Microsoft Defender for Endpoint • Examples of the mistakes, successes, close calls, and critical lessons learned in the interminable battle against Qakbot and its contemporaries About Ben Magee: Ben is a senior threat hunter within the NHS England Cyber Security Operations Centre (CSOC), currently standing in as the CSOC Threat Hunting Lead. Ben and the TH team conduct hunting activities at scale on one of the largest estates in the world in order to stay ahead of a whole host of threats and protect the NHS. Since graduating in 2017 with a First Class degree in Computer Forensics & Security, Ben has worked in both the private and public sectors as a protective monitoring analyst and security engineer respectively. About Dan Taylor: Dan Taylor leads the threat intelligence and threat modelling functions in NHS England’s centralized Cyber Security Operations Centre (CSOC), providing critical security services to health and social care organizations across the country. With a background in security operations and incident response, Dan first joined the NHS to help build a dedicated protective monitoring capability for NHS England’s Covid 19 response efforts before joining the CSOC to help defend the health service at large. Dan focuses on keeping the broader healthcare estate informed of the ever-changing threat landscape with a focus on the tangible ways threat intelligence can help protect healthcare organizations on the ground.
