ExtraHop Security Advisory: 67 Percent of Enterprise Environments Still Run Protocol Exploited by WannaCry and NotPetya

Four years after devastating ransomware attacks, SMBv1 and other vulnerable protocols still running in IT environments around the world

SYDNEY, May 14, 2021 – ExtraHop, the leader in cloud-native network detection and response, has released a security advisory about the prevalence of insecure protocols in enterprise IT environments. The report details the ongoing use of deprecated and insecure protocols, including Server Message Block version one (SMBv1), which was exploited by the WannaCry ransomware variant to encrypt nearly a quarter of a million machines world-wide four years ago today.

In early 2021, the ExtraHop threat research team conducted primary research examining the prevalence of insecure protocols in enterprise environments, specifically SMBv1, Link-Local Multicast Name Resolution (LLMNR), NT Lan Manager (NTLMv1), and Hypertext Transfer Protocol (HTTP). The research uncovered alarming usage of these protocols that expose organisations and their customers to considerable risk.

SMBv1: This protocol has been exploited for attacks like WannaCry and NotPetya and can quickly spread malware to other unpatched servers across a network. ExtraHop research shows that SMBv1 is still found in 67% of environments in 2021, more than four years after the EternalBlue and related vulnerabilities came to light.
LLMNR: LLMNR can be exploited to gain access to the user credential hashes. These credential hashes can be cracked to expose actual login information that gives malicious actors access to sensitive personal and business data. ExtraHop research found that 70% of environments are still running LLMNR.
NTLM: Despite the recommendation from Microsoft that organizations cease use of NTLM in favor of the much more secure Kerberos authentication protocol, NTLM is still quite common. Thirty-four percent of enterprise environments have at least 10 clients running NTLMv1.
HTTP: When plaintext credentials are transmitted over HTTP, those credentials are left exposed—the internet equivalent of shouting passwords across a crowded room. Despite the risks, data from ExtraHop shows that 81 percent of enterprise environments still use insecure HTTP plaintext credentials.
“It’s easy to say that organisations should get rid of these protocols in their environments, but often it’s not that simple. Migrating off SMBv1 and other deprecated protocols may not be an option for legacy systems, and even when it is an option, the migration can trigger disruptive outages. Many IT and security organisations will choose to try and contain the deprecated protocol instead of risking an outage,” said Ted Driggs, Head of Product, ExtraHop. “Organisations need an accurate and up-to-date inventory of their assets' behaviour to assess risk posture as it relates to insecure protocols. Only then can they decide how to remediate the issue or limit the reach of vulnerable systems on the network.”

Download the full report here: Security Advisory: Insecure Protocol Usage Exposes Organizations to Cybersecurity Risk.

You can learn more about protocols and threat activities associated with them by visiting the ExtraHop Network Protocol Library.

About ExtraHop
ExtraHop is on a mission to arm security teams to confront active threats and stop breaches. Our Reveal(x) 360 platform, powered by cloud-scale AI, covertly decrypts and analyses all cloud and network traffic in real time to eliminate blind spots and detect threats that other tools miss. Sophisticated machine learning models are applied to petabytes of telemetry collected continuously, helping ExtraHop customers to identify suspicious behaviour and secure over 15 million IT assets, 2 million POS systems, and 50 million patient records. ExtraHop is a market share leader in network detection and response with 30 recent industry awards including Forbes AI50, Cybercrime Ransomware 25, and SC Media Security Innovator.

Stop Breaches 84% Faster. Get Started at www.extrahop.com/demo

Contacts

David Bass
+61 2 9922 6820
mailto: david@basspr.com.au