ExtraHop Report: Ransomware Continues to Hinder 85% of Organisations, but UK Leads the Way in Refusal to Pay Hackers

Submitted by: Positive Marketing
Tuesday, 1 March 2022

Newly released Cyber Confidence Survey reveals false sense of security felt by security and IT decision-makers despite prevalence of attacks

LONDON, UK – March 1, 2022 – ExtraHop, the leader in cloud-native network detection and response, today released findings from a new survey on ransomware that sheds light on the discrepancies between how IT decision-makers (ITDMs) globally see their current security practices, and the reality of the ransomware attack landscape. The ExtraHop Cyber Confidence Index 2022 report (https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/) shows that however capable IT organisations have been in managing the dramatic transformations of the past couple of years, confidence still tends to outstrip actual security posture.

The survey, conducted by Wakefield Research, found that 75% of UK ITDMs are very or extremely confident in their company's ability to prevent or mitigate cybersecurity threats. Despite this confidence, 58% admit that half (or more) of their cybersecurity incidents are the result of their own outdated IT security postures, including widespread use of insecure and deprecated protocols, as well as growing numbers of unmanaged devices. This inflated confidence is even more dangerous in light of the frequency of ransomware attacks — as 85% reported globally having suffered at least one ransomware attack, and 74% reported experiencing multiple incidents in the past five years.

Other key survey findings include:

- The cost of ransomware is high: 72% of global respondents admitted to paying a hacker's ransom on at least one occasion, whilst 42% of companies that suffered a ransomware attack said they paid the ransom most or all of the time. The UK was most resistant in this regard with 67% and 37%, whilst the US was the most likely to give in to ransomware demands with figures being 79% and 52%, respectively.

- Organisations are less than transparent: While almost two-thirds (63%) of UK respondents agreed it was good to disclose attacks, only 32% said they were fully open about attacks and willing to make information available for public knowledge when they actually took place.

- Damage to the business: Ransomware attacks affect the entire organisation with 40% of respondents reporting business downtime resulting from attacks on IT infrastructure, 43% reported business downtime resulting from attacks on OT infrastructure, such as medical devices, factory automation systems, and 40% reported end user downtime resulting from attacks targeting users.

- Everyone Is Looking For Better Insights, Data, and Cooperation: When asked to identify their top challenges, 44% cited a lack of investment, 40% cited a lack of cooperation between their network, security, and cloud operations teams, 33% cited the long time required to train new hires, and 29% cited inadequate or overlapping tooling. In addition, 24% in the UK say the biggest disruption to their incident response is having too much data to find real insights. Compared to European data, both the UK and US appear to be lagging behind in investment as 31% in France, and 36% in Germany, cite lack of

investment as a key challenge.

- WFH with Outdated Protocols: Despite the shift to working from home, 67% of respondents acknowledged transmitting sensitive data over unencrypted HTTP connections instead of more secure HTTPS connections. Another 71% of UK respondents are still running SMBv1, the protocol exploited in major attacks like WannaCry and NotPetya, leading to more than $1 billion in damages worldwide. This is higher than the global average of 68% and the highest percentage of use in Europe.

“This research highlights the discrepancies between the reality of today’s sophisticated attack landscape and the overconfidence that many business leaders have in their ability to manage an attack,” said Jeff Costlow, CISO at ExtraHop. “Defenders need tools that can track attacker activity across cloud, on-premises, and remote environments so they can identify and stop an attack before they can compromise the business.”

This study shows that, even as companies continue to innovate with cloud technologies and remote workforces, their IT infrastructures remain mired in the past, with obsolete protocols providing ongoing opportunities for attackers to infiltrate networks and unleash ransomware attacks. A lack of visibility and effective use of data has also contributed to organisations’ obstacles in identifying vulnerabilities and preventing ongoing ransomware attacks. To combat these challenges, organisations should look for ransomware mitigation tools that can capture network communications across all devices, and use technologies like behavioural analytics and artificial intelligence to detect behaviours that signal a ransomware attack in progress. By leveraging a Network Detection and Response platform like ExtraHop’s Reveal(x) 360 (https://www.extrahop.com/solutions/security/ransomware-prevention/), defenders can detect and stop the lateral movement and other post-compromise activity of ransomware attackers before they achieve real damage.

Additional Resources

ExtraHop Cyber Confidence Index 2022 full report (https://www.extrahop.com/resources/papers/cyber-confidence-index-2022/)

Find out more about how ExtraHop can help your business protect against ransomware (https://www.extrahop.com/solutions/security/ransomware-prevention/)

Ransomware Retrospective 2021: The Rise of the Advanced Extortionate Threat (https://www.extrahop.com/resources/learning/ransomware-retrospective/)

Methodology

The survey of 500 security and IT decision makers in the US, UK, France, and Germany was conducted by Wakefield Research and sponsored by ExtraHop. Survey participants came from a wide range of industries, including financial services, healthcare, manufacturing, and retail, and worked at companies of varying sizes, including companies with annual revenue exceeding $50 million. About half the participants were in

the US, with the rest hailing from the UK, France, and Germany.

About ExtraHop

Cyberattackers have the advantage. ExtraHop is on a mission to help you take it back with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defence platform, Reveal(x) 360, helps organisations detect and respond to advanced threats—before they compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioural analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, enterprises can detect malicious behaviour, hunt advanced threats, and forensically investigate any incident with confidence. ExtraHop has been recognized as a market leader in network detection and response by IDC, Gartner, Forbes, SC Media, and numerous others.

Learn more at www.extrahop.com.

# # #

PR Contact:
Ashley Stewart
ExtraHop
pr@extrahop.com

UK PR Contact:
Jake Galland
Positive
jgalland@positivemarketing.com