KnowBe4 Issues 2018 Threat Impact and Endpoint Protection Report

Submitted by: Origin Comms Ltd
Wednesday, 28 February 2018

Midmarket and Enterprise Organisations Are the Hardest Hit with Ransomware and External Malware

KnowBe4 (https://www.knowbe4.com), the world's largest provider of security awareness training and simulated phishing, today released its "2018 Threat Impact and Endpoint Protection Report." In 2017, ransomware was a multi-billion dollar business with the number of new ransomware variants continuing to grow quarter-over-quarter. Despite the many security offerings available, organisations continue to fall victim to attacks with an average of 13% of organisations surveyed experiencing a ransomware attack and 25% of organisations experiencing an external malware attack. Knowing these factors, KnowBe4 sought to understand the overall impact ransomware has on an organisation.

Regardless of size or industry, every organisation has the potential to become a victim of ransomware. The widespread, opportunistic nature of many attacks, mixed with an improvement in phishing-based social engineering, has led cybercriminal organisations to take the "shotgun" approach, targeting every business for whatever ransom can be paid.

KnowBe4 surveyed more than 500 organisations around the globe to determine the impact a ransomware attack has on an organisation, including who is at risk, what is being held for ransom, what does it take to remediate and how does it impact the overall organisation. Specific findings included:

Ransomware Attacks
- Organisation Size & Industry: Midmarket organisations (1,000-5,000 employees) were hit the hardest with ransomware in 2017, with 29% indicating they experienced a ransomware attack. Organisations in manufacturing, technology and consumer-focused industries experienced the most ransomware attacks.

- Productivity Impact: On average, 16 workstations, 5 servers and 22 users within an organisation were affected in a given attack with an average downtime of 14 hours. The organisations with the most downtime hours were mid-market and enterprise (5000+ employees) organisations.

- Data Impact: The more critical the data is to an organisation, the higher likelihood of the ransom being paid. Ninety-seven percent of organisations stated that encryption impacted common Office-type files which included critical, sensitive and proprietary data. However, it is important to note that organisations are realizing the value in maintaining backup copies of their data, with 61% recovering server data from backups and 35% recovering workstation data from backups.

- Cost Impact: While most organisations do not pay the ransom, the ransoms ranged from $500 to $1 Million (USD). Most bitcoin-related ransoms were 1-3 bitcoins, ranging from $600 to $11,000.

External Malware Attacks

- Organisation Size & Industry: On average, 24% of all organisations experienced an external attack in the last 12 months, with consumer-focused businesses, non-profits, technology and professional services being hit the hardest. Of those hit in 2017, 28% were hit in 2016.

- Productivity Impact: The number of systems impacted during an external attack was far more than a single endpoint; the average malware-based external attack impacted 5 workstations and one server.

- Data Impact: Organisations with documented breaches varied in the number of records breached. The average number of records breached was slightly higher than 15,000. The organisations with the highest number of record breaches, which went up to 100K, were mid-market and enterprise organisations.

Prevention
- Implementation of Security Software: 89% implementation, up from last year's total of 76%.
- Break Room-Style Training: 36% implementation, up from last year's total of 28%.
- Monthly Training Videos and Emails: 52% implementation, up from last year's total of 26%.
- Regular Phishing Tests: 57% implementation, up from last year's total of 36%.
- Security Assessment Training & Testing: 54% implementation, up from last year's total of 34%.

"While ransomware attacks are becoming more and more sophisticated, they are preventable. As the report shows, endpoint protection solutions help protect against a material percentage of malware, but don't actually put a stop to the threat," said Stu Sjouwerman, CEO of KnowBe4. "It's only by adding continual testing and training of employees that organisations create their strongest security posture and see a material decrease in both ransomware and external malware attacks. This shows a well-implemented security awareness training program makes an organisation much less susceptible to an attack. As these threats continue to grow, it's imperative that organisations mobilise their last line of defence - their employees - to help protect against this threat."

The full report and KnowBe4's recommendations on how to improve the overall security stance can be viewed here (https://www.knowbe4.com/typ-2018-endpoint-protection-report).

About KnowBe4

KnowBe4, the provider of the world's most popular integrated new-school security awareness training and simulated phishing platform, is used by more than 15,000 organisations worldwide. Founded by data and IT security expert Stu Sjouwerman, KnowBe4 helps organisations address the human element of security by raising awareness of ransomware, CEO fraud and other social engineering tactics through a new-school approach to security awareness training. Kevin Mitnick, internationally recognized computer security expert and KnowBe4's Chief Hacking Officer, helped design KnowBe4's training based on his well-documented social engineering tactics. Thousands of organisations trust KnowBe4 to mobilize their end-users as the last line of corporate IT defence.

Number 231 on the 2017 Inc. 500 list, #50 on 2016 Deloitte's Technology Fast 500 and #6 in Cybersecurity Ventures Cybersecurity 500. KnowBe4 is headquartered in Tampa Bay, Florida with European offices in England and The Netherlands. For more information, visit www.knowbe4.com and follow Stu on Twitter at @StuAllard

-ends-

Media Contact:
Louise Burke
Origin Communications
Tel: +44 (0) 7917 176095
louise@origincomms.com