IDG CONNECT

Malwarebytes

Ransomware piercing the anti-virus bubble

Better prevention is needed to protect organizations from the growing threat landscape

The WannaCry ransomware attack that had such a widespread and damaging effect on public and private sector organizations around the world highlights the challenge IT departments face in protecting themselves against new cyber threats, which are constantly evolving and expanding. Even organizations that weren't hit directly by the ransomware felt the effects of the attack as the business operations of their impacted suppliers, distributors, or other business-related partners were halted while they coordinated remediation efforts.

In the UK, 61 National Health Service (NHS) Trusts were infected by WannaCry, with medical staff left unable to access patient record systems and other critical data on a busy weekday morning. The incident led to numerous appointments and operations being cancelled or postponed, impacting patient care with potentially life or death consequences.

The attack also hit Spanish telecommunications provider Telefónica, automakers Nissan and Renault, German railway operator Deutsche Bahn, FedEx, and the Russian Interior Ministry. This incident was the largest scale ransomware infection in history. European law enforcement agency Europol estimated over 200,000 computers in 150 countries were affected.

Complacency creates opportunity for attack

The criminal hackers that unleashed WannaCry modified a tool developed by the US National Security Agency called EternalBlue to exploit a vulnerability in Microsoft operating systems. Shortly after being notified of the vulnerability, Microsoft issued security bulletin MS17-010 on March 14, 2017, but many organizations had still not installed the updates by the time WannaCry hit on Friday May 12th, nearly two months after the patches had been made available.

The issue of performing timely patch management highlights the similar challenge many IT professionals face in continually evaluating their existing security tools to ensure they are able to combat the latest threats

Malwarebytes

Endpoint security needs to work in the face of overburdened security operations

Security solutions that require constant attention, maintenance, and tuning to maintain effectiveness are difficult, if not impossible, for organizations to sustain. For example, legacy AV solutions that must always be connected to the internet to receive updates to ensure protection – or that require patches to immediately be installed or policies adjusted, fail to deliver protection that fits how today's overextended security operations function.

The scale of the cyber security management overhead is a common theme across different industries and geographies. The IDG Connect survey found that between 69 and 71 percent of US organizations spend over ten hours a week deploying security patches and upgrades, and also identifying networking, application and system vulnerabilities before they are exploited. Yet despite all the time and effort being spent on threat prevention, attacks are still getting through.

More ransomware attacks on the way

Ransomware is a growing menace, with tools easily leased as on-demand, cloud-hosted 'malware-as-a-service' kits, enabling attacks to be conducted by enthusiastic amateurs with very little technical skills. In its 2017 Data Breach Incident Report (DBIR), Verizon documents over 42,000 cyber security incidents and 1,900 data breaches experienced by 65 organizations in 84 countries, and calculates that ransomware incidents specifically surged 50 percent in 2016 compared to the previous year.

That growth in the volume and sophistication of ransomware attacks is widely expected to continue in 2017 and 2018. Malwarebytes predicts that while ransomware attacks today are launched indiscriminately against as many organizations as possible to maximize financial gains, that is likely to change. Attacks will become increasingly targeted and personalized as hackers identify vulnerable business and consumer users and find new avenues of extortion by not only encrypting files but threatening to expose personal data or individually sensitive information.

IDG CONNECT

Existing approaches need to critically analyze

With so many high profile incidents of ransomware and other data security breaches generating news headlines around the world (often to the detriment of the affected organization's reputation and revenue), it is no surprise that companies are starting to change their approach to securing their endpoints.

In a report "Market Insight: Security Market Transformation Disrupted by the Emergence of Smart, Pervasive and Efficient Security" published earlier this year, research company Gartner noted a shift in cyber security investment which sees organizations putting more money into new approaches to threat prevention, detection and response. CISOs are reevaluating where to invest their cybersecurity funds due to the pressing growth and success of effective ransomware and advanced fileless attacks. Legacy "all-in-one" endpoint protection platforms (EPP) that include nonmalware detection features, such as port control and data protection, are being deprioritized in favor of investments in threat detection layers that deliver cyber resiliency against unknown malware attacks. To get a sense of the investment shift, Gartner forecasts that global spending on information security will exceed $90bn in 2017, and reflect a balance between risk and resilience as companies seek to improve threat prevention and blocking as well as damage limitation.

The market for endpoint protection solutions is forecasted to grow from US$4.8bn to US$5.8bn between 2017 and 2020 (Radicati Group). IDC predicts that large organizations will invest heavily in upgrading existing endpoint protection solutions over the next couple of years, with spending on corporate endpoint security worth $4.2bn this year set to grow at a compound annual growth rate (CAGR) of 5.2%.

Research conducted by IDG Connect on behalf of Malwarebytes published earlier this year confirms that existing cyber security defenses fail frequently. The survey of 200 senior IT staff working for US organizations carried out by the company revealed that 64 percent had been impacted by a ransomware attack in 2016. The consistent, predictable failures by the traditional AV solutions have forced security practioners to re-evaluate their endpoint strategy. The increased expenditure is largely targeted towards new malware detection techniques to detect what their existing solutions are missing.

Best practices for endpoint security

In light of successful ransomware and multi-vector attacks, organizations should initiate some key planning to manage the risk associated with threats to the endpoint:

1. Investigate the types of threats facing your organization

Review the threat intelligence reports from your security operations center and categorize the endpiont remediations by the attack's tactics, techniques and procedures (TTPs). What attacks are getting through and why?

2. Prioritize endpoint protection featueres that align to those threats

If your data shapes a picture like most organizations, the majority of attacks are unknown malware. Many dynamic detection capabilities exist to secure the endpoint against these attacks. Nonsignature-based methods that apply techniques like behavioral analysis and anomaly detection are proactive in their prevention capabilities and provide higher threat coverage to protect against the majority of cyberattacks before they execute and cause damage.

3. Deprioritize the features that don't align with the malicious attacks you're seeing today

Based on the attacks on the endpoint, an organization's endpoint protection platform features should focus on protecting the enterprise from malicious adversaries. Therefore, reevaluate the need for your endpoint security to incorporate periphery market capabilities, such as disk encryption and USB device controls and mobile device management (MDM).

Conclusion

Every indication is that the scale and sophistication of ransomware attacks and other types of malware will increase as different groups – criminal hackers, amateur enthusiasts, and even state-sponsored attackers – find new ways of exploiting security vulnerabilities, extracting cash, and causing commercial disruption on a massive scale.

The large number of organizations impacted by WannaCry demonstrates the extent to which existing defenses often fail to protect data and systems from new strains of attack, and will continue to fall short unless IT departments can identify fresh approaches to cyber security that minimize their risk of being caught out.

In the face of overburdened security operations, organizations should assume that allocating more resource time to endpoint security management will not provide a short or longterm fix to the growing tide of complex, multi-vector attacks. Instead, organizations should reevaluate if their endpoint protection is providing the right security-focused capabilities and make the necessary shifts in investment for detection techniques that provide the highest efficacy for ransomware and unknown malware.