Digital Security
Progress. Protected.

RANSOMWARE: PART 5

Ransomware:
A game of cat and mouse

In previous blogs we focused on how cybercriminals utilize vulnerabilities in Remote Desktop Protocol (RDP), email and supply chains to drop ransomware onto an organization's systems. Although these are popular methods, they are by no means the only techniques used by those with malicious intent.

Zero-day vulnerability

While cybercriminals can benefit from exploiting both known and unknown vulnerabilities, laying hands on a zero-day vulnerability is seen as the mother lode for bad guys. This is because a **zero-day vulnerability is one that is either unknown to the vendor in question, or one that is known but does not yet have a patch to correct for it**.

Zero-day vulnerabilities are generally the preserve of advanced persistent threat (APT) groups or state-sponsored actors because of the sheer time and resources required. A zero-day vulnerability is serious business and something that businesses large and small need to be wary of. It is a constant game of cat and mouse between cybercriminals finding vulnerabilities and vendors racing to plug the gaps. Barely a week goes by without a new zero-day vulnerability being discovered and dominating the news worldwide.

Long shelf-life vulnerabilities

It is not just zero-day vulnerabilities that organizations need to be cautious about. It's almost five years later and the WannaCryptor (also known as WannaCry) ransomware is still a global threat to be reckoned with. The infamous trojan that compromises machines vulnerable to the **EternalBlue exploit** topped ESET's ransomware detections charts last year, **accounting for over one in five (21.3%) of all detections in T2 2021**.

The long shelf life of vulnerabilities like **WannaCryptor** unfortunately points toward poor update and patch management strategies in organizations. The importance of patch management mustn't be underestimated. Patching systems closes off potential avenues of attack and can prevent ransomware from getting into your organization. Or if it does get in, patching will reduce the damage.

Virtual private network (VPN)

The third vulnerability security admins and business owners need to treat seriously is the incorrect use of a virtual private network. With workers forced to work from home during the pandemic, global use of VPNs exploded. VPN providers had to flex major muscle to handle the increase in overall internet traffic seen, not just from remote workers, but from those furloughed and on an entertainment streaming frenzy. According to independent research, **demand for VPNs increased by 44% at the start of the pandemic** and remains 22% higher than pre-pandemic levels.

However, the use of VPN by workers adds an additional responsibility when it comes to updating the product as required. Not only should there be a focus on timely updates; organizations should also insist upon workers using multifactor authentication when signing into the VPN. Should suspicions of credential abuse arise, organizations should not take any chances and should pursue comprehensive account resets.

Ransomware is everywhere

Unfortunately, ransomware is everywhere. For further details on all the techniques employed by cybercriminals to try to infiltrate your systems and data, please read other parts in our ransomware series. However difficult the situation may seem, know that providers are working tirelessly at fixing bugs and ensuring your security. Having a reliable digital security provider is key to minimizing risks. Ensure you don't cut corners: Be sure to implement a comprehensive award-winning security solution.