Bitdefender®

The Ransomware Threat and a State of High Anxiety

Recent WannaCry and Golen Eye/Petya Attacks A Painful Reminder

News of these two massively destructive attacks rattled the business and tech worlds, reminding us of the real and present danger of ransomware. Both attacks used components to spread globally in hours, affecting hundreds of companies and bringing down critical infrastructures. Perhaps the most chilling aspect of both the WannaCry and GoldenEye/Petya attacks is their ability to spread automatically to Windows-based systems, with no user interaction. The cyberattack has inflicted fresh pain globally, and on a huge number of users. It has also renewed fears of the destructive power of ransomware when combined with publicly available cyberespionage tools and vulnerabilities. Beyond that, the attack once again spotlights the importance of delpoying the right kind of multi-layered defensive framework to protect crucial data and the IT infrastructure.

Heightened Anxiety

Ransomware and other continuously evolving and morphing threats have created a high level of anxiety among business executives. Ransomware concerns have escalated among the vast majority of those executives, placing it alongside phishing and other attacks, according to published research.

Ransomware's defining characteristic is its attempt to deny users access to their data, typically by encrypting specific file types or the entire drive. To make sure that users pay a ransom, hackers try to inflict maximum damage by encrypting the data on a server, disrupting backups, or by modifying the Master Boot Record, which renders systems unbootable. As shown in recent attacks, adversaries may also deploy ransomware that destroys data or loads additional malware to sabotage their victims.

Clearly, this threat has caused many sleepless nights for those in charge at businesses and organizations. The reasons for their concern are clear. A partial accounting of the damage from an attack include: reduced productivity and efficiency; increased system downtime; loss of proprietary data; loss of personal identifiable information; lost time restoring data after a breach or infection; damage to a company's reputation (which can result in lost opportunity costs); and compliance fines.

These worries are compelling the healthcare industry to respond to the growing Ransomware concerns. A recent update of the Health Insurance Portability and Accountability Act (HIPAA) shows that the healthcare sector has come to see ransomware as a significant threat. Specifically, HIPAA rules now state that the presence of ransomware in an organization oblibes the organization to initiate its security incident, response and reporting procedures. In other words, HIPAA now sees a ransomware attack as a data breach.

The damage is substantial. But what leads to this havoc? Let's look at some examples.

Attack Vectors

The attack vector used by cybercriminals to infect businesses with ransomware is similar to other types of malware infections. Top infection channels include email and web. Spam or phishing email messages are designed to bait users into opening attached documents and enabling Macros or run scripts. Other messages contain links that lead to exploit-hosting sites, serving vulnerabilities for outdated browser versions or commonly installed plugins, such as Java, Adobe Flash, and Adobe Reader.

For example, once the user enables a macro in the attached Word document, the macro, which is essentially a visualBasic Script, sends commands to download and run a malicious payload, in this case ransomware.

Once the payload is dropped, the ransomware can use encryption to deny users access to crucial data, often to extort payment from the victims. However, it might also exfiltrate or simply distort data or even modify the Master Boot Record (MBR), preventing PCs from booting the operating system.

The Defensive Landscape

Ever-developing exploit tactics and malware obfustication techniques are over-stressing traditional defensive measures.

While standard approaches to security have had some success in the past, they are now outmaneuvered by evolving threats. Traditional signature-based AV struggle to keep up. Some user sites run additional AV tools on top of existing endpoint defenses to augment prevention, but they have to manage multiple agents and use different consoles. The value of these solutions is further diminished by the high number of false positives they deliver.

Tthe shortcomings of traditional defensive tools make it clear that something else is needed; something that combines a multi-layered approach with strong prevention as a key consideration.

The Bitdefender Approach

This is where Bitdefender's core technologies come into play. Key elements of Bitdefender's Layered Next Generation endpoint security have been carefully crafted to evade, prevent and detect the early stages of ransomware attacks.

Evasion: the anti-ransomware Vaccine evades ransomware by taking advantage of a design feature in some ransomware families meant to prevent re-infection of machines.

Prevention: Bitdefender advanced machine learning leverages unpacking capability to perform dynamic file analysis at pre-execution stage and can detect unknown and obfuscated malware/ransomware or ransomware. Bitdefender, using a machine learning model, is one of the few security vendors that blocked WannaCry at zero-hour without any updates.

Bitdefender also uses machine learning to dynamically identify exploit-hosting websites or compromised websites that unknowingly host exploit kits or serve malware.

Memory Protection – focuses on attack techniques designed to exploit software vulnerabilities such as Adobe Reader, Word, Flash Player and browsers, then stops malicious code from landing and running on the system. This is especially effective against exploit kits.

Behavior Anomaly Detection with P**rocess Inspector** – Operating on a zero-trust assumption, Bitdefender continuously monitors all active processes, looking for suspicious signs or abnormal behavior. It can then take immediate actions to contain a threat, including process termination, and undoes any changes the process makes. It is highly effective in detecting unknown ransomware, advanced malware and fileless attacks.

In Summary

We've seen that hackers are engaged in a constant game of invention and re-invention. Defensive measures must be just as nimble. The stakes are high: tremendous damage can be done to an organization. We also know that strengthened security is the result a wide array of factors, including: policies and procedures; heightened security awareness among an organization's staff; and controls that restrict access to sensitive information. These are just a few elements, but it's clear that strong information security won't come from a magic pill. An ongoing treatment program is needed. However, the treatment can be incredibly effective with technologies such as Real-Time Process Monitoring, Machine-learning anti-Malware, Advanced Anit-exploit, and Anti-Ransomware Vaccine. Good cyber-security health and prevention are just what the doctor ordered.

BD-NGZ-Oct.20.2017-TH#
Bitdefender-NGZ-Ransomware-SolutionBrief-cres2085-A4-EN