SecureAge

SecureData

Application Whitelisting, Application Binding, 3Ps Data Encryption

What is APT?

Social Networks like Facebook, Twitter and LinkedIn are popular online hangouts for most people. But do you know that they can also be the most treacherous place? Have you ever accepted a LinkedIn invitation from someone whom you do not know at all? Are you aware that by opening an email attachment from an unknown sender may put you in a precarious situation? Have you ever wonder why standard applications that you always use are able to open other unassociated documents out of the blue? If you have ever encountered such unusual incidents, you may have potentially been attacked by APT (Advanced Persistent Threat) attackers! APT attacks have proliferated tremendously over the recent years. They are extremely deadly in their relentless efforts to steal company's confidential information undetected.

What is APT?

APT is a sophisticated network attack masqueraded by a team of organized cyber criminals. Their key intent is to steal sensitive data from their targeted organizations in specific sectors like the government, finance and manufacturing. They use their deep resources and advanced penetration skills to establish the back door that enable them to gain entry into the company network unnoticed.

This team of organized attackers are remarkably persistent in their efforts to circumvent most defences and stealthy tactics in order to maintain an ongoing and undetected corporate network access. They demonstrate good situational awareness by evaluating defenders' responses, relentlessly rewriting the code and then escalating their attack techniques accordingly.

How does APT strike?

Spear fishing is a social engineering ploy that frequently uses by APT attackers to inject malicious codes into their innocent victim's computer. These victims, very often, are lured by the hackers to click on the bogus social network link, like Facebook, Twitter and LinkedIN, which actually ended up with the installation of a malware application into their computer. The hackers, via the malware application, are able to wantonly access the victims' desktops, networks and even assume their credentials to steal sensitive data. Such victims, most of the time, are completely oblivious to the attack.

The social engineering ploy helps APT attackers to gain legitimate access and establish a back door. They will then try to gather valid administrator credentials that enable them to move across the network and install more back doors. Through these backdoors, they will install and distribute malware that went unnoticed for a long period of time.

One of the worst APT attacks is when the injected malicious malware disabled common safeguards like anti-virus and Intrusion Detection Systems (IDS). The intruders will even escalate their tools and techniques as a victimized firm's ability to counteract improves.

Therefore, APT attacks have become the most formidable challenges to address as compared to common computer security breaches.

Anti-APT Solutions

Is Application Whitelisting the right solution?

Many IT security products have emerged recently that claim to solve the APT problem, mostly by using the application whitelisting (some call it application control) technology. Such technology creates a complete list of trusted applications in the user computer system and allows only trusted applications to run. All unknown software, including malware, will be blocked from executing in the system. This does effectively block executable malware from running in the user machine and even prevent the existing malware from infecting the machine with more malwares.

However, application whitelisting does not prevent zero day attacks that inject malware code directly into trusted application during run-time and causing harm to the user machine. It also does not prevent malicious code injection into system drivers, like the network driver. Consequently, attackers can further inject rootkits into the user machine which can be executed without the application whitelisting or other anti-malware systems blocking them. This is because rookit are usually loaded before the anti-malware systems and stay at very low level in the operating system stack to effectively evade detection and removal.

Another danger is attacker disabling anti-malware engines in the user system or renders such protection ineffective. In this case, any malware can then proceed to execute further malicious code wantonly.

With so many sophisticated APT attacks that can easily evade application whitelisting and other anti-malware systems, how can we stop them?

SecureAge SecureData

1) Integrated Defense

SecureAge SecureData is designed to combat APT, especially the most sophisticated type of APT attacks. SecureData is bundled with a complete application whitelisting component that can prevent unauthorised malware from damaging the user system.

In addition, the application whitelisting is tightly coupled with a Proactive, Pervasive, and Persistent (3P) data encryption engine. The 3Ps encryption technology comprises of the following components:

Proactive – Smart and automatic encryption of all user data files without user's involvement.

Pervasive – All user data files are encrypted in all storage devices.

Persistent – All user data files are encrypted at rest and on the move.

Essentially, the 3P data encryption ensure that all user data are automatically encrypted everywhere without the user having to make any conscious decision. It ensures that plain data are not exposed in certain storage system or when they are on the move that can be exploited by malware. With 3P encryption tightly bundled with application whitelisting, we can prevent two types of sophisticated malware mentioned above:

i) Rootkit: very low level rootkit can avoid detection by application whitelisting because it can access user data without having the data passing through the whitelisting engine. With 3P encryption engine coupled with the application whitelisting, the data will also be bypassing the encryption engine. But the difference is the rootkit can only receive encrypted data. Hence, the sensitive user data are protected from the rootkit.

ii) Anti–malware Disabler: malware that disabled the application whitelisting will also disable the 3P encryption engine because they are tightly coupled. So once the application whitelisting is disabled, all

user data will appear as encrypted to any application or malware that access them. Again, the sensitive user data are protected from the malware in this case.

2) Application Binding

The encryption engine also supports an additional feature called Application Binding which allows specific applications to be bound with specific type of data or specific data path. For instance, we could bind *.doc & *.docx file with the Microsoft Word application so that only Microsoft Word can read and write *.doc & *.docx files. In this case, no other application can access such files. Hence, if another application, say Adobe Reader, is compromised by a zero-day malware, it will not be able to access any Microsoft Word documents.

The Application Binding also supports user prompting option when data file is accessed. We could use this option for high risk application like web browser so that whenever a file is attached to the browser, the user will be prompted to confirm the action. Hence, if the browser is attacked by malware, it cannot automatically access the user data file without the user consent. In fact, such high risk application can be further restricted to read and write files from only a specific user directory. This creates a "sandbox" for the application so that it can only read and write data to a specific directory and cannot harm the underlying user system in general.

We cannot entirely remove the risk of zero-day Attacks. But with Application Binding, the risk of zero-day attacks can be greatly mitigated and the damage can be reduced to the minimum in the worst case.

3) Application and Data Access Logs

A detailed log of application execution and data access activities is also a feature of SecureData. Entries pertaining to blocked application execution or abnormal user data access activities can help the system administrator to quickly identify potential threats that are happening in the enterprise systems. This will help to further mitigate the risk from malware and APT by enabling the easy identification of attacks that are in progress.

By uniquely combining Application Whitelisting, Application Binding and 3Ps Data Protection, SecureData provides a highly secure environment to protect sensitive user data from general malware and APT attacks. It is an easy-to-use solution without needing the users to be well trained in order to enjoy the full protection. Organizations using SecureAge SecureData solutions will be able to reduce risk, increase operational efficiencies, and achieve comprehensive security protection – even in the face of sophisticated APTs.

Need More Information?

General Enquiry: contactus@secureage.com
Public Relations / Marketing: pr@secureage.com
Technical Support: support@secureage.com

www.secureage.com
www.lockcube.com

Asia Pacific
SecureAge Technology Pte Ltd
3, Fusionopolis Way
#05-21, Symbiosis
Singapore 138633

Japan
SecureAge K.K.
Barbizon 18, 7F
5-18-18 Shirokanedai
Minato-ku, Tokyo 108-0071
Japan

North America
SecureAge Technology Inc
3 Twin Dolphin Drive Suite 150
Redwood City CA 94065
U.S.A.