Securing Endpoint Devices using Next-Gen AV Solutions

Palo Alto Networks Traps and Cylance Protect

Technical Security Solution Brief

As malware continues to evolve, the endpoint solutions must evolve as well.

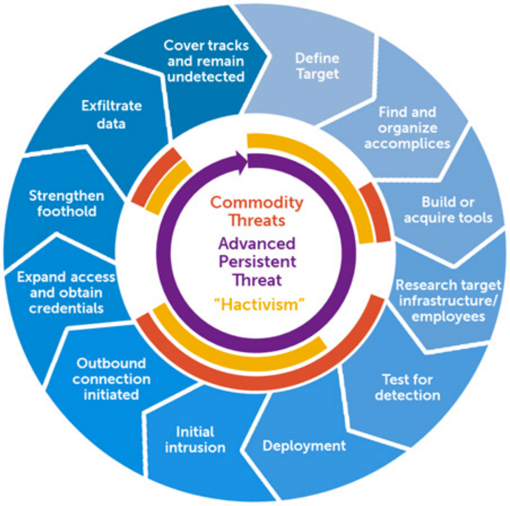
by Alex Jones
Sun Management, Inc.
22 May 2017

Overview

Traditional antivirus and antimalware software cannot keep up with the ever-changing environment that is today's threat landscape. Malware authors have found ways to completely bypass the traditional scan and repair tools and software by writing files that can manipulate their code to change their own signatures on the fly. Because of this, the need for new tools has become abundantly clear with the rise of outbreaks such as CryptoLocker, ZeuS, and wannacry / wannacryptor.

To understand how to prevent attacks, understanding how the attacks are performed is necessary. Typical attacks begin with an attacker performing reconnaissance on their target, determining end goals for their attack, and finally, determining the best method of attack to achieve their defined goals. At this point, the attacker will devise an attack strategy to deliver their payload via some form of manipulation of their victims. This strategy could be via social engineering, phishing, brute force, etc. to gain access to a computer, network, or user credentials. Once the attacker has been successful, they will begin by exploiting the system in some way to deliver their malicious payload to set up persistence in the environment so control can be maintained. If an attacker has gotten this far they then will begin to execute command and control traffic (C2) to achieve the goals that they set within the beginning of their attack lifecycle.

Security professionals only need to stop an attack at one point within the attack life cycle. If a defense in depth strategy is used in defense, we have many opportunities to stop and attack before it's successful preventing damage to the endpoint and network.


Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
"Hactivism"

- Figure 1 - APT Lifecycle

The Antivirus / Exploit Problem

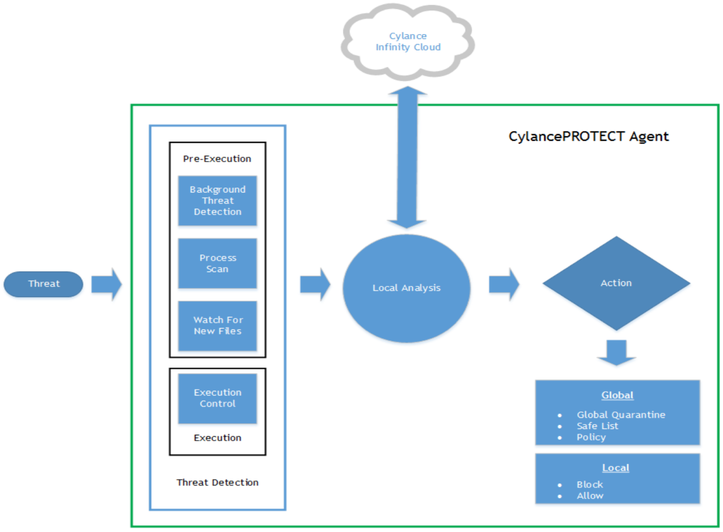
Today's methods for examining malware that would be used for persistence by attackers are archaic in design, because many use a scanning method that can only detect and protect when a threat is known. Files that are found to be bad get signatures written with a uniquely identifiable string allocated as a match criteria for a given file. An antivirus system will scan all files on disk within an environment and check each file against a long list of signatures looking for a match. With 1 million[1]+ new threats being released daily due to self-mutating (hash altering files that change themselves) and sheer number of malicious actors, the ideology of trying to keep up with the demand for signatures is an impossible battle.

Malware authors have also use exploit techniques to take advantage of logic flaws within legitimate applications to gain loop holes in a computer system bypassing most antivirus entirely. From this entry point an attacker can load shell script into memory and execute code while never leaving a file on disk, or they can use it as a platform to set up persistence to keep control over a machine. These exploits can be launched by methods such as: opening a document downloaded from a website, opening an email containing a .docx file with macros enabled, or simply running an exploitable piece / version of software.

Sun Management carries two different products that address these issues while avoiding the pit falls of traditional protection products.

Cylance Protect

Cylance Protect addresses the needs for antivirus signatures by using a math model created by artificial intelligence to determine good files from bad files. The math model in use looks at uniquely identifiable features within executable files to determine file verdict (clean, grayware, or malware.) This model was developed by analyzing millions of known good and known bad files to teach the AI machine learning engine responsible for the products math model the difference between a known good and known bad file so that it is able to determine an overall verdict within milliseconds. The Cylance Protect product works in a pre-execution state, examining files before they are executed or loaded to RAM, allowing Protect to take action on a file before it can cause any issues. Files on disk can be set to a one-time scan, a scheduled scan (every 9 days), or no scan at all based on preference.



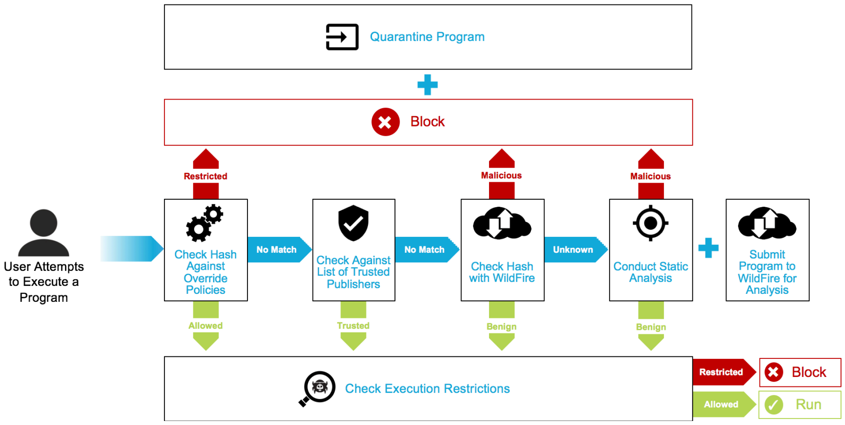
■ Figure 2 – Cylance execution logic flow

Protect additionally can watch for and stop exploits that would leverage alternate techniques that would not be caught. This feature is labeled as memory protection and covers exploits that would exploit vulnerable processes, inject additional processes below already running processes, or issue any form of privilege escalation to obtain admin or root access to a machine. Protect sits on top of the kernel of the endpoint monitoring active executable files that reside on disk or in memory to ensure that no malware is able to execute on the endpoint.

Cylance implements a cloud architecture design, having all endpoint connect up a cloud tenant for setting updates, math model updates (roughly every 6 to 8 months), and for general logging statistics. The cloud tenant runs in Amazon AWS requiring no onsite hardware, and no maintenance for the end user. A tenant instance is available for government agencies that require cloud applications to run in AWS GovCloud. Because of this there are no additional servers to scale up as an environment grows due to the nature of AWS's cloud service.

Palo Alto Traps

Palo Alto Networks (PAN) Traps addresses the malware issue in a different manner, utilizing a combination of static and dynamic analysis. Static analysis is the method of using a mathematic algorithm to determine a file as good or bad based on the attributes it shows in comparison to the files that were used in creation of the mathematical model. This model was created with both benign and malicious files and tuned based on behavior that was known about the files. Dynamic analysis is the terminology used to describe the use of the PAN WildFire cloud analysis engine for file verdicts. Traps will send any unknown file (based on hash value) to its manage platform called the Endpoint Security Manager (ESM). The ESM will report a verdict from local cache based if it has a verdict. If the ESM has no verdict from WildFire for a particular file it will be uploaded for evaluation into PANs WildFire environment for detonation. Wildfire then will detonate, watch, and evaluate exactly what a process does in an advanced sandbox environment to determine if a file is benign or malicious. This verdict is then returned to the ESM, and to the endpoint for policy based on verdict. PAN Traps will protect an endpoint pre-file-execution with Static Analysis, unless there is an immediate Dynamic Analysis verdict available as those will override the static analysis done locally on the endpoint.


Quarantine Program
Block
Restricted
Malicious
Malicious
User Attempts to Execute a Program
Check Hash Against Override Policies
No Match
Check Against List of Trusted Publishers
No Match
Check Hash with WildFire
Unknown
Conduct Static Analysis
Submit Program to WildFire for Analysis
Allowed
Trusted
Benign
Benign
Check Execution Restrictions
Restricted
Block
Allowed
Run

■ Figure 3 - Traps execution logic flow

Exploit prevention is handled by Traps via process injection, Exploit Prevention Modules (EPMs), and sanctified applications. Traps injects DLL processes into protected applications monitoring for the 23+ uniquely identifiable exploit techniques that Palo Alto Networks has identified to be the root algorithms used in all exploit based attacks. If an exploit is triggered within a protected process, Traps will halt all execution on the given process and force close the application, killing the attack lifecycle before the attack was successful.

Configuration of PAN Traps is a software deployment based on Microsoft Windows Server, Microsoft SQL Server, and IIS. The core components of the architecture are as follows: ESM Core (main server product, and backend connection for Traps Endpoint Connections) installation is installed on The Microsoft Windows Server, with a tie to the Microsoft SQL server. The Console (management software with web GUI) install is loaded onto a Microsoft Windows Server, pointing at the Microsoft SQL server installation as well, this will hook into the local IIS server on the Windows machine the Console is loaded to. All traps clients will point at the ESM core for their server location.

Summary

Previous methods of endpoint protection no longer are sufficient in the current threat landscape due to the ease of mutation and sheer number of new malware that is popping up every day. Sun Management's selected endpoint products are best of breed next-gen antivirus solutions that approach the problem in new ways eliminating the need for daily updating, continuous scanning, and high resource utilization.

Additional Resources

https://www.cylance.com/content/dam/cylance/pdfs/data_sheets/CylancePROTECT.pdf

https://www.cylance.com/content/dam/cylance/pdfs/data_sheets/CylancePROTECTplusMemoryProtection.pdf

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/endpoint-protection

https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/endpoint-protection

[1] http://blog.trendmicro.com/malware-1-million-new-threats-emerging-daily/