Persistence

Persistence Mechanisms as Indicators of Compromise

An automated technology for identifying cyber attacks designed to survive – indefinitely – the reboot process on PCs

White Paper

Date: April 2016

Contact: marcom (at) sampansecurity.com

http://www.sampansecurity.com

SAMPAN security inc

Executive Summary

MS Windows PC-based endpoints are vulnerable to zero-day attacks designed to bypass installed security. However Authentication Management of Persistence Mechanisms (AMPM), a technology that grew out of a combination of U.S. Department of Defense and commercial research (and that works alongside existing security solutions), detects and mitigates such cyberattacks. Based on reported incident responses, most cyberattacks include a *persistence mechanism*[5], wherein the attack code sets itself up to survive the reboot process. This new technology can automatically detect embedded code that would otherwise launch hidden malware.

Driving this point, consider the attacks that have occurred in recent years and note that all would likely have been detected with this solution. Also note that those attacks succeeded in spite of traditional security products in place on those systems.

Adding AMPM features to work alongside today's cybersecurity software would cover a gap that otherwise exists for all PCs. The remainder of this paper describes both the problem and the solution.

Zero-Day Attacks

Endpoint systems are far easier to breach than well-defended servers and can be used as a launching pad for targeted attacks.

Targeted attacks, and attacks of the Advanced Persistent Threat sponsored by nation-states, occur over multiple stages. Perpetrators of the targeted attacks employ different malware to accomplish different objectives of each stage of the attack: initial compromise, establishing a foothold, escalating privileges, moving laterally, and data theft.

Traditional AV solutions detect malware execution at the “perimeter” based on a signature that was created when the malware was first discovered and researched. Since there is no signature available to detect Zero-day attacks, Zero-day malware can pass through the endpoint perimeter and execute payloads with multiple malicious actors inside the endpoint. Any incident reported or detected during a Zero-day attack will most likely be partial and incomplete, but could serve as a trigger for the next phase of cyber incident response: containment and remediation.

Why Persistence Mechanisms

The rationale behind the use of persistence mechanisms (Microsoft Windows persistence mechanisms include Autorun settings) as Indicators of Compromise (IOCs) and to trigger an incident alert in real-time or in postmortem investigation is based on the two following points:

1. **Most Cyberattacks Include Persistence**
   Postmortem analysis indicated that the majority of recent zero-day cyber security attacks made use of injected or altered persistence mechanisms.

2. **Key to Forensic Investigation**
   Standard industry practice for incident response and forensic investigation focuses on persistence to find the compromise[1,2,3,4,5]

A single Microsoft Windows PC contains hundreds of Autorun settings which makes identifying and verifying their validity a time-consuming process. In a corporate, intelligence, or military environment with hundreds or thousands of PCs, this process becomes impractical to accomplish through manual software tools. Automated tools are critical for enabling support professionals and digital forensics investigators to perform their jobs more effectively and efficiently.

Automating Discovery with AMPM

Authentication Management of Persistence Mechanisms (AMPM) automates the detection of persistence-based attacks which in turn enables the automation of mitigation.

1. **Persistence Mechanism Discovery**
   A persistence mechanism (or Autorun setting in the Windows operating system context) is a program that is automatically started by Windows when the operating system starts, a user logs in, or an application starts. The Discovery task logs all existing “persistence mechanisms” including associated metadata and hash values of target binary files. For a real-time protection scenario, it will continue to monitor the persistence mechanisms and trigger automatic authentication on the changes.

2. **Persistence Mechanism Authentication**
   An internally developed, cloud-based Autorun Setting Repository (ASR) is used for persistence mechanism authentication. ASR provides detection scheme with ratings for Autorun entries and identifies them as known good, known bad, or unknown (possibly zero-day):

Green:	Autorun whitelist database kept at ASR
Red:	Autorun blacklist from cloud-based 60+ Anti-virus engines
Yellow:	Zero-day Entries, could be good or bad

   ASR allows support professionals and digital forensics investigators to quickly disregard the majority of good Autorun entries and focus on a smaller list of questionable or possibly malicious entries.

3. **Persistence Mechanism Stacking**
   For the enterprise continuous monitoring and real-time forensics, the detection task also delivers and stacks all persistence mechanisms from the networked endpoints with an Inter-Host Intrusion Protection Service, IHIPS (network server is required to host the database).

   The IHIPS enables a situational awareness management to:
   a. Analyze malware kill chains and multi-stage attack artifacts
   b. Alert persistence mechanism exception relative to a group template

c. Identify possible malware distribution (yellow and red) and at-risk endpoints

Zero-day Attack Containment:

Each endpoint system is associated with an endpoint protection profile for containing possible zero-day software. For example, a lockdown mode specification in the endpoint protection profile will allow only Windows system software signed with a Microsoft digital certificate to change.

The containment task, which includes monitoring the dynamic attribute of malware payload artifacts, will adjust the authentication result presented from ASR with endpoint local behavioral intelligence. Once the containment task has been triggered, it will:

A. Kill the parent task that dropped the payload (malicious actor)
B. Quarantine and break the persistence mechanism
C. Monitor the temporal properties of the quarantined persistence mechanism. If the same persistence mechanism is re-inserted then the containment task will initiate a cleanup and reboot to remove other associated malware actors performing reinsertion.

Scope of Persistence Mechanism Detection:

Among persistence mechanisms, there are macro-persistence and micro-persistence (discussed in this excerpt). Macro-persistence, which is not covered here, includes persistence mechanisms from an endpoint PC or mobile device (tablets or smartphones), but the execution is targeted at another endpoint system.

In Windows PC environments, persistence mechanisms extend beyond the traditional Autorun settings and include tripwires (e.g. DLL Search Order Hijacking, default program setting changes, image path in Alternate Data Streams) and security settings (e.g. Killing active AV software) which will be contained automatically once detected by AMPM.

There are some challenges to the hit rate of using persistence mechanisms to detect Zero-day attacks, such as: memory only scrapping malware, registry only persistence mechanisms, DLL injection, etc. However, the persistence mechanism based detection scheme only needs to detect one malicious actor deploying persistence mechanisms among all the actors of a security incident. The detection scheme will also work for just one actor's deployment of persistence mechanisms at any stage of a multi-stage targeted attack scenario.

As for rootkits, there are additional persistence mechanism tools developed for postmortem investigation and for real-time continuous monitoring by comparing live persistence mechanisms vs. on-disk Autorun analysis using native mode access (no Windows API). For real-time protection, Rootkits require persistence mechanisms as well, and the real-time detection component will capture the persistence mechanism deployed before the rootkits have a chance to hide them.

Summary

All of the recent zero-day attacks or breaches would have been detected and contained if AMPM was deployed based on the technical details of the security responses published by various vendors and research institutes regarding the persistence deployed. This technology, AMPM, is available now for incorporation into U.S. defense as well as commercial solutions.

[1] Triaging Malware Incidents, by Corey Harrell, 24 September 2013, Journey Into Incident Response: http://journeyintoir.blogspot.com/2013/09/triaging-malware-incidents.html

[2] Finding Evil: Automating Autoruns Analysis, by Dave Hull, 4 February 2012, TrustedSignal: http://trustedsignal.blogspot.com/2012/02/finding-evil-automating-autoruns.html

[3] Stick Around: Persistence Mechanisms in Recent APT Compromises, a presentation by Ryan Kazanciyan and Christopher Glyer of Mandiant at the 2011 DoD Cyber Crime Conference in Atlanta GA: https://www.mandiant.com/general/search-results/0eb044c34418a70c5b6c350356fa758c/

[4] Definitive Guide to Advanced Threat Protection, by Steve Piper, CISSP, Compliments of FireEye: http://www.cyber-edge.com/wp-content/uploads/2015/03/Definitive-Guide-to-ATP.pdf

[5] A Persistence Mechanism Technology Primer, 2016, PersistenceMechanisms.com: http://persistencemechanism.com/downloads/PM_Primer_2016.pdf