Persistence Mechanisms

The Missing Link for Zero-Day Attack Detection and Protection

A Persistence Mechanism Technology Primer

April 2016

Table of Contents

Persistence Mechanism Technology Primer

- This primer presents persistence mechanisms technology on endpoint computers
- For networked computers please refer to:
  - FireTower: A Networked Persistence Mechanism Technology Primer
- Persistence mechanism whitepaper:
  - Persistence Mechanisms as Indicators of Compromise

Cyber Security
Facts

- Zero-day attack incidents and major breaches are becoming increasingly pervasive as seen in news headlines
- Many of these affected businesses were equipped with top of the line enterprise network security appliances and elaborate security solutions on all endpoint computers, yet they failed to detect the Zero-day attacks that resulted in severe loss of data
- These deployed solutions are mostly based on a “perimeter” defense approach, using virus and malware signatures for detection and produce excellent results for detecting previously discovered malware

Cyber Security
Cyber Attack Characteristics

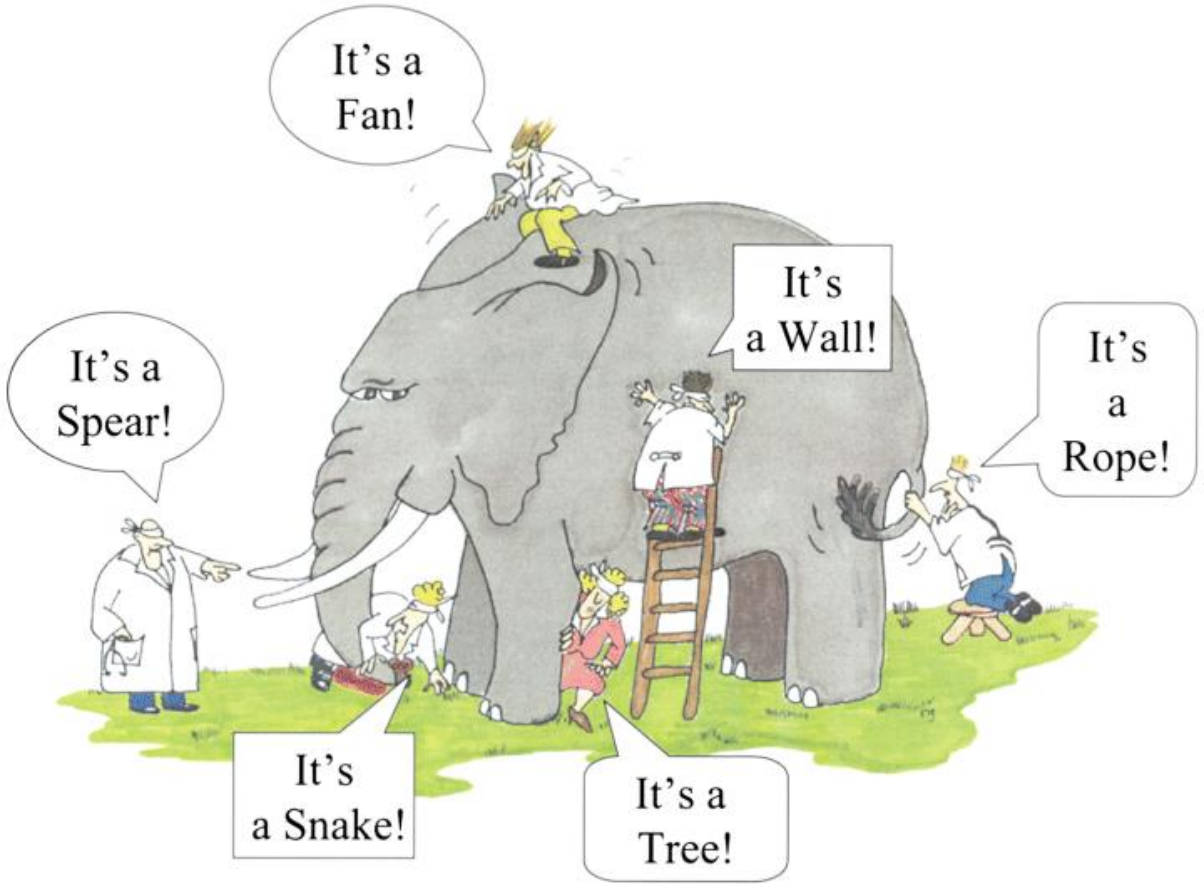
- Multi-Stage Attacks: Targeted attacks and Advanced Persistent Threat
  - Mostly traverse through enterprise network to reach valuable endpoint systems for critical data and for exfiltration.
- Multiple vectors/actors with different types of malicious actions for each attack incident at each attack stage

Cyber Security
Malware Root Cause at Endpoint Computers

Cyber attack steps at an endpoint computer

[Malware Root Cause Analysis by Corey Harrell]

Cyber Security
Attack Vectors and Infection Techniques



Cyber attack vectors at an endpoint computer

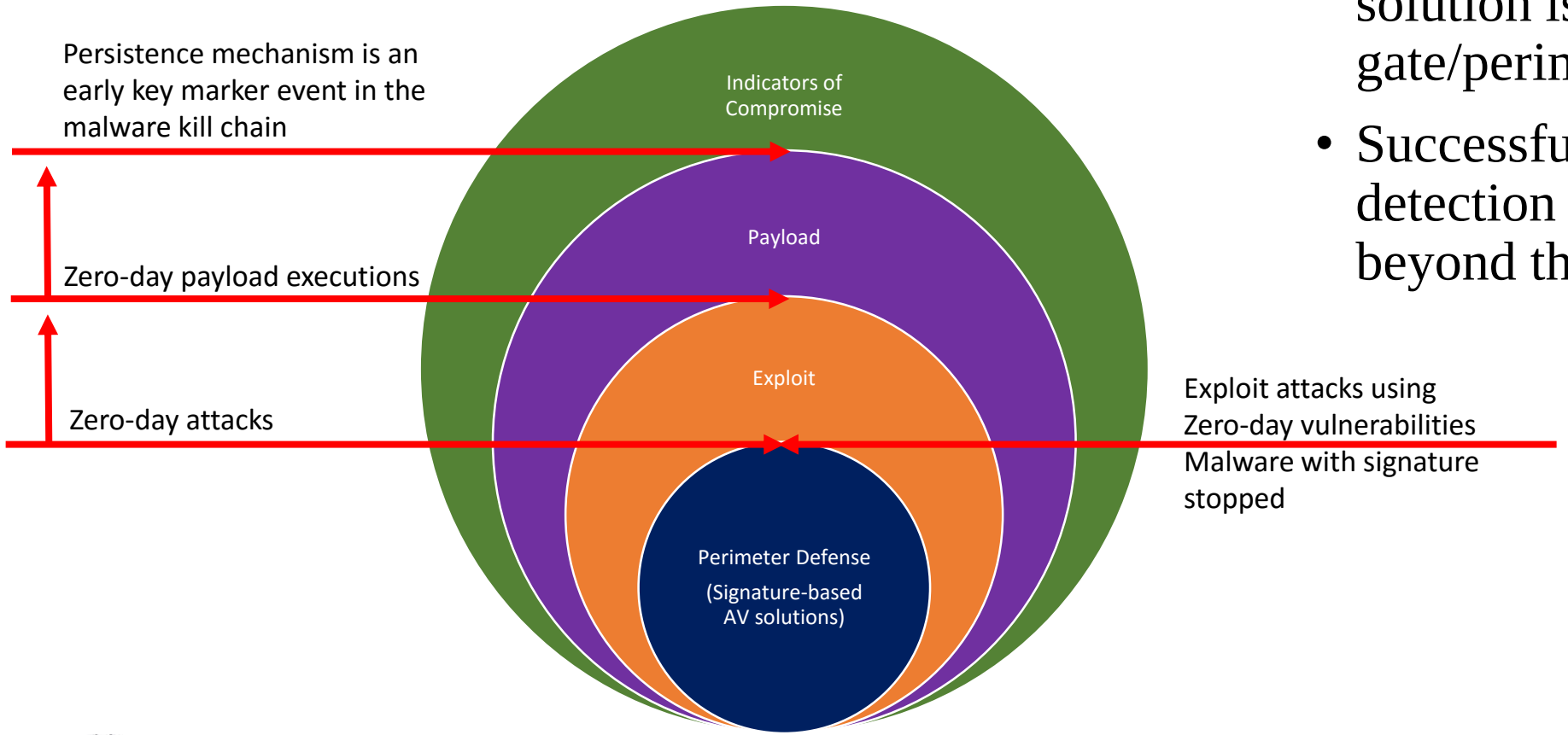
Cyber Infection techniques at an endpoint computer

- ✓ Memory infection
- ✓ Command and Control
- ✓ Key loggers
- ✓ Backdoors and Trojans
- ✓ Privilege Escalation
- ✓ DLL Injections
- ✓ Rootkits
- ✓ Dictionary attacks
- ✓ BHO
- ✓ SQL Injections
- ✓ Server only infection
- ✓ …….

Cyber Attacks
Malware at Endpoint Computers

Each stage of a cyber attack could have multiple actors with different types of malicious actions

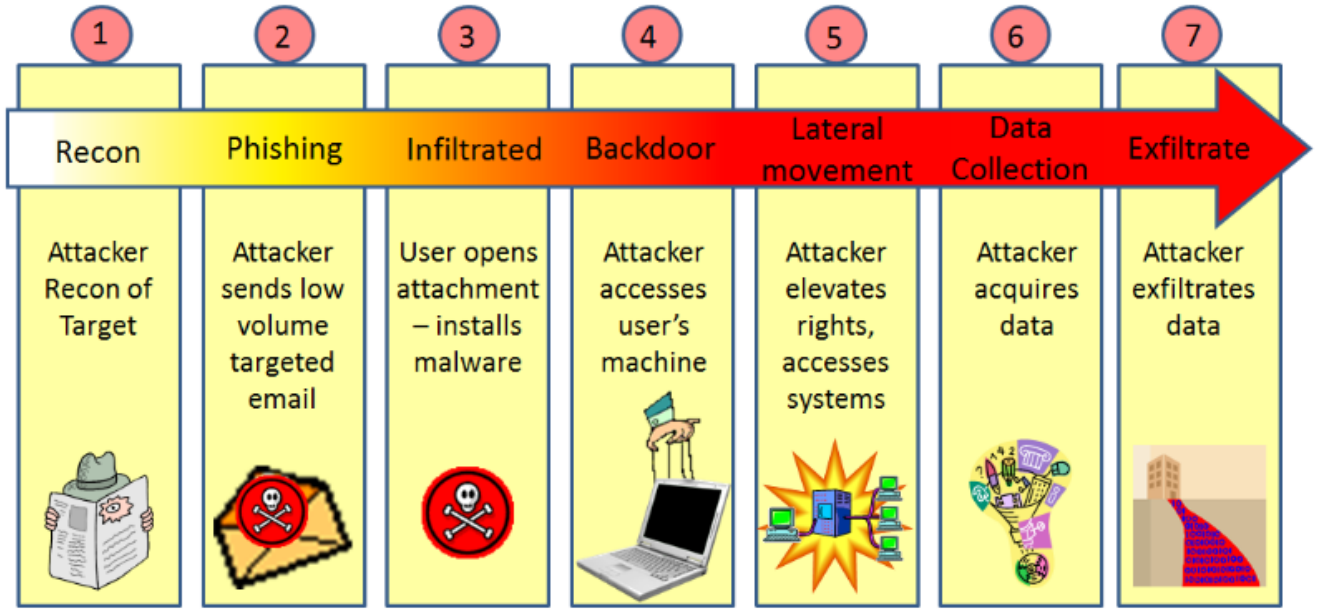
Cyber Security
Zero-day vs. Known Malware Attacks



- Signature-based security solution is very successful at gate/perimeter
- Successful Zero-day attack detection usually occurs beyond the perimeter

Cyber Security
Multi-stages of An Attack Lifecycle

- Initial compromise (1,2,3)
- Establish foothold (3)
- Escalate privileges (3,4)
- Internal reconnaissance (4,5)
- Move laterally (5)
- Maintain presence (6)
- Complete mission (7)



Advanced Persistent Threats, SP Guard APT/Spearphishing Defense from Iconix.com

Cyber Security
Malware Categories

Malware categories for cyber attacks

- Known malware with signature
  - Malware signatures: > 500 millions total with > 12 millions per month for the last two months AV-Test.org (2016)
  - Malware signatures are created when a malware is first discovered and researched
- Unknown malware without signature: Zero-day exploits and payloads
  - > 390K new malware registered everyday by AV-Test.org (2016)
  - Zero-day malware has no signature because it was never discovered and identified and has no information detailing whether it is legitimate, suspicious, or malicious

Cyber Security
Available Solutions

Security solutions for cyber attacks

- Known malware with signature
  - Security solutions are mostly based on a “perimeter” defense approach, using virus and malware signatures for detection and produce excellent results for detecting previously discovered malware
- Unknown malware without signature
  - Contrary to claims made by most security solution vendors that their security solutions are capable of detecting Zero-day attacks, Zero-day attacks continue as evident by recently reported incidents

Cyber Security
Zero-day Attack Detection

- Cyber Attack Characteristics
  - Multi-Stage Attacks
  - Multiple vectors/actors with different types of malicious actions (malware) for each attack incident at each attack stage
- Zero-day Attack Detection Criteria
  - No security solutions can detect all Zero-day attack payloads because there is no signature existed, hence Zero-day attacks
  - Only need to detect one attack stage of any cyber attack
  - Only need to detect one actor/vector of each attack incident per attack stage
  - Zero-day attack detection triggers the incident response to enter containment and remediation phases to remove the cyber attack payload and footprints
- Persistence mechanism is an early key marker event in the malware kill chain

Persistence Mechanisms
The WHAT

- A persistence mechanism is a program that is automatically started when the operating system starts, a user logs in, or an application starts

Persistence Mechanisms
The WHAT

In Windows PC environments, persistence mechanisms consist of:

- Autorun settings
- Tripwires
  - e.g. DLL Search Order Hijacking, Malicious executables with same file names as system files, Windows host file changes
- Security settings
  - e.g. default program setting changes, image path in Alternate Data Streams, Autorun.inf at root folder, etc.

Persistence Mechanisms
The WHAT

Autorun Settings: Main persistence mechanisms in Windows

- Run, RunOnce Keys
- Winlogon
- Explorer
- Internet Explorer and BHO
- Providers and Monitors
- Services
- Drivers
- Startup Files
- Scheduler
- Scripts including WMI, PowerShell, PowerShell Profile, HTML, INI,

Persistence Mechanisms
The WHAT

- A typical business could have hundreds to thousands of endpoint computers
- Each Windows PC may have 300 to 500+ persistence mechanisms (Windows XP/Vista/7/8/10 and Windows Server 2003/2008/2012)
- Each persistence mechanism has to be discovered, analyzed, authenticated, and stacked across the enterprise network

Persistence Mechanisms
The WHY

Application of persistence mechanism technology to cyber security solutions:

- For incident response and forensic investigation
  - Standard industry practice for forensic analysis focuses on persistence to find the compromise during incident response and forensic investigation
  - Most forensic investigations begin the incident response process by looking at Autoruns as they are an effective way to discover most malware and are extremely fast to triage
- For endpoint protection of Zero-day attack detection and containment
  - Persistence mechanism is included in all recently reported attacks and breaches
  - Malware is virtually always persistent
  - A reliable way to detect and contain Zero-day Attacks and alert the attacks in progress

Persistence Mechanisms: The WHY

Incident Response and forensic investigation

- Persistence mechanism is an early key marker event in the malware kill chain
- Incident response investigation cannot be started without all the persistence mechanisms at the endpoint computers discovered, authenticated, and stacked across the enterprise network
- Threat intelligence of persistence mechanisms is manageable and maintainable (65K+ persistence mechanisms vs. millions of malware or billions of whitelist such as reputation database and software registry)

Persistence Mechanisms: The WHY

Incident Response and forensic investigation

References:

- Triaging Malware Incidents by Corey Harrell, Journey Into Incident Response, 2013
- Finding Evil: Automating Autoruns Analysis by Dave Hull, Trustedsignal Blog, 2012
- Stick Around, Persistence Mechanisms in Recent APT Compromises, Mandiant, 2011 DOD Cyber Crime Conference

Persistence Mechanisms: The WHY

Endpoint Protection for Zero-day attacks

- Detecting the payload execution during the malware installation phase provides an early window of opportunity to kill the entire malware chain
- Payload during execution is most visible without obfuscation and encryption when dropping a persistence mechanism
- While malware payloads may involve many actors, we only have to detect one actor setting up persistence mechanisms per incident or per stage in the attack lifecycle
- DLL Injection, Rootkit, memory malware, trojan, backdoor, keyloggers all need persistence mechanisms to launch at endpoint computers

Persistence Mechanisms
The HOW

- Recommended procedures from Finding Evil: Automating Autoruns Analysis by Dave Hull, Trustedsignal Blog, 2012:
  - Discovering Autorun entries using Microsoft Autoruns for Windows on all endpoint computers
  - Authenticating Autorun entries or identifying malicious executables (using scripts and checking against VirusTotal.com database)
  - Stacking across all endpoint systems in the network using scripts

Persistence Mechanisms
The HOW

- Persistence mechanism methodologies
  - Discovery all endpoint persistence mechanisms
  - Authenticate all discovered persistence mechanisms using their metadata
  - Stack all discovered and authenticated persistence mechanisms from all endpoint systems across the enterprise network for monitoring, malware triage, and forensic investigation

Persistence Mechanisms: The HOW

Discovery Task Requirements

- Being able to detect persistence mechanism change events in real-time can greatly enhance incident response and forensic investigation
- Persistence mechanisms have long been used by support professionals to diagnose and resolve crashes, instability, degraded performance, unwanted programs, and virus incidents in Windows and therefore some utilities perform a persistence mechanism discovery for generic support use;
  - case in point: this type of utility will list persistence mechanisms even with non-AutoStart setting which does not pose a threat in cyber security environment
- Discovery task should be integrated with authentication task in order to automate the whole process

Persistence Mechanisms: The HOW
Discovery Task

- Persistence mechanism discovery:
  - On-demand triggering
    - On-demand snapshot-based Autorun utilities
    - Additional steps needed to detect persistence mechanism change events by comparing two snapshots taken at different times
  - Real-Time triggering
    - Real-Time Autorun utility to detect live persistence mechanism change events

Persistence Mechanisms: The HOW
Discovery Task

- Available discovery utilities – on-demand triggering vs. real-time
  - On-demand snapshot-based Autorun utilities:
    - Autoruns from Microsoft Technet
    - HijackThis from SourceForge and Trend Micro, Inc.
    - AutorunCheck Snapshot Edition from imagine LAN, Inc.
  - Real-Time Autorun utility to detect persistence mechanism change events
    - FireTower Guard PC Edition from Sampan Security, Inc. *

* Note: FireTower Guard software is a combination of real-time persistence mechanism discovery and authentication software with an optional 30-day trial for Guard function which will automatically quarantine suspicious or malicious persistence mechanisms according to the profile settings. After 30-day trial FireTower will only perform persistence mechanism discovery and authentication without Guard function.

Persistence Mechanisms: The HOW
Authentication Task

Persistence mechanism authentication prospects:

- Known Good (Green) 
- Known Bad (Red) 
- Unknown and Zero-days (Yellow) (no digital certificate, no metadata, …) 
  - malicious
  - suspicious
  - benign

Persistence Mechanisms: The HOW

Authentication Task Requirements

- Real-time and automated authentication for the most up-to-date security information
- Using multiple threat intelligence sources to identify Zero-day persistence mechanisms and to avoid false positives and false negatives
- Cost and overhead consideration for authentication methodology and threat intelligence databases
- In a typical business environment, all installed software should be approved by IT prior to deployment; therefore all “unknown software” should be categorically blocked

Persistence Mechanisms: The HOW

Threat Intelligence Source Requirements

Threat Intelligence Source Requirements

- How many sources/databases
- How frequently is it updated
- How are the threats evaluated
- How is data formatted
- Can the threat data be correlated with other existing data

Threat Intelligence Scales

- Thousands of new vulnerabilities each year
- Millions of malware and variants are recorded with signatures
- Billions of whitelist applications have been registered
- There are fewer than 100K persistence mechanisms

Persistence Mechanisms: The HOW
Authentication Sources

- Not an exhaustive list
- Threat Intelligence Services: Free or Fee-based
  - Bit9 Software registry (Enterprise whitelist database)
  - VirusTotal.com (General malware database)
  - HerdProtect.com (General malware database)
  - BleepingComputer.com (Windows Autorun Setting)
  - Autorun Setting Repository (Windows Autorun Setting)

Persistence Mechanisms: The HOW
Authentication Sources

Some ideas on numbers

- Malware signature: > 500 millions total + 390K per day, AV-Test.org (2016)
- Startup list: 26,677, BleepingComputer.com (March 2016)
- Autorun Setting Repository, Sampan Security Inc. (~65,000) March 2016
- Bit9 Software Registry: 6 billion + 20 million per day
  (Application Whitelisting: Panacea or Propaganda, SANS Institute 2010)

Persistence Mechanisms: The HOW
Stacking Task

- Upload discovered and authenticated persistence mechanism events to enterprise threat database
- Present a situational awareness view of threat intelligence within the enterprise network by performing Inter-Host Intrusion Prevention data-mining

Persistence Mechanisms: The HOW
Stacking Task Requirements

- Real-time enterprise threat database from all endpoint persistence mechanism change events and other security information assembled from stacked local intelligences
- Flexible GUI to filter and focus on specific PC, workgroups, and specific persistence mechanism type and timeline for situational awareness and incident investigation
- Remote access for security monitoring operation
- Continuous monitoring for attack in progress alert, detection, and containment
- Further detail will be explored in FireTower Primer, a Networked Persistence Mechanism Technology primer

Persistence Mechanisms:
Integration and Automation

- All phases of persistence mechanism change event discovery, authentication, and stacking should be completely automated without human intervention
- The software should work for most modern desktop Windows operating systems such as Windows XP/Vista/7/8/10 and Windows Server 2003/2008/2012
- Performance implication at the endpoint computers and overall cost should be minimized
- Snapshot based tool should be enough for postmortem incident response and forensic investigation
- Real-time tool should be used to perform continuous monitoring and attack in progress detection

Persistence Mechanisms
Integration and Automation

On-demand/Snapshot integrated persistence mechanism tool:

- AutorunCheck Snapshot Edition Software (Free tool)
- AutorunCheck Snapshot Edition Factsheet

Real-Time integrated persistence mechanism tool:

- FireTower Guard Standalone Edition * (Free with 30-day trial for Guard function)
- FireTower Guard Standalone Edition Factsheet

* Note: FireTower Guard software is a combination of real-time persistence mechanism discovery and authentication software with an optional 30-day trial for Guard function which will automatically quarantine suspicious or malicious persistence mechanisms according to the profile settings. After 30-day trial FireTower will only perform persistence mechanism discovery and authentication without Guard function.

Persistence Mechanisms Technology Primer
Summary

- Major cyber breaches with Zero-day attacks continue to prosper and have been covered in news headlines extensively
- Standard industry practice for forensic analysis focuses on persistence to find the compromise during incident response and forensic investigation
- Malware is virtually always persistent
- Persistence mechanism change event is a reliable way to detect Zero-day Attacks and to alert cyber attack in progress
- An integrated and automated persistence mechanism software can contribute greatly to incident response and forensic investigation

Postmortem Forensic Tools
Resources

Cyber security forensic software for postmortem investigation

PC-based or USB-based Volume Shadow Copy Service aware forensic tools for Autorun setting or Windows configuration:

- AutorunCheck Software:
  - AutorunCheck Professional and Forensic Edition Product Page
  - AutorunCheck Professional and Forensic Edition Factsheet

- ConfigSafe Software
  - ConfigSafe Professional and Forensic Edition Product Page
  - ConfigSafe Professional and Forensic Edition Factsheet

Please contact imagine LAN, Inc. for additional information

Contact Us

For the Persistence Mechanism Technology Primer:

- Contact email: contact.us @ persistencemechanisms.com