Detection Enhancement ATIs – Information for Customers

Author: Rico Valdez

Software Version: Bit9 Detection Enhancement 1.3
Document Version: 1.1
Revised: 6/6/2016 10:29:00 AM by Sarah Miller
Classification: Confidential and Proprietary Information of Bit9, Inc.

Table of Contents

1 Introduction

1.1 Overview

The purpose of this document is to communicate details about the Advanced Threat Indicators (ATIs) that are delivered in the Bit9 Detection Enhancement. This document will outline the ATI events that are generated in the Bit9 console, and describe the threat the ATI is designed to detect, as well as other details around the ATI that may prove helpful in filtering, prioritization and analysis of these events.

ATI events are not always indicative of malicious activity; they are indications of highly suspicious activity that is typically worth investigating. These indicators look at the real time behavior of files and processes on the endpoints, not at specific hashes or known bad files.

1.1.1 Updaters Vs Indicators

Before version 7.2, ATIs were delivered via the updater mechanism. With versions 7.2 and above, ATIs are now delivered via the indicator set mechanism. For indicators that appear in both pre 7.2 versions and up, we include both the (historical) updater and the (current) indicator set. For indicators that appear only in versions later than 7.2, we include only the current indicator set.

1.2 False Positives

For our purposes, false-positives are defined as ATI events that have fired on legitimate behavior that is not associated with a threat. This can occur when software or users perform actions that match some of the behaviors an ATI is designed to look for. While we continuously work to minimize or mitigate these situations, it is impossible to predict the behaviors of the users or the various software packages deployed in customer environments. As such, false positives will inevitably occur in environments with the Detection Enhancement deployed.

The confidence associated with each ATI is based on our experience in both test and real world environments, but since every environment is different, it is important to observe the ATI events specific to each deployment to best determine the degree to which they are actionable. For example, when Adobe Reader is observed to create an executable file, that is a strong indication of a malformed document exploiting a vulnerability to drop a malicious payload. However, this same observable behavior may occur when installing a new printer driver from within Adobe Reader, and if that is a common activity in an environment, the false positive rate for this indicator may be high. In this case, for example, those non-malicious behaviors may be skipped by filtering out any "Possible exploit of document handling" ATI events where the target filename contains the Windows System path, or where the file is digitally signed, or where the file has a low file prevalence in the organization – thereby increasing the value of the remaining similar events. The actual filter and its effectiveness in reducing false positives depends on each environment.

As a general guideline, assuming most systems in a deployment are not infected with malware, if Bit9 is generating a comparatively high number of ATI events across a proportionately high number of distinct systems, it is more likely to be a false positive versus an ATI event that occurs either at low volume or across a small number of systems.

1.2.1 General Mitigation Strategies

Starting with the 7.2 release of the Bit9 platform, the console provides the ability to create exceptions for conditions under which a given ATI will not fire, using exception criteria such as process, user, and filename. Until then, it is possible that events might be generated that are not useful or interesting, and instead introduce noise making it difficult to identify higher-priority events. Consider the following techniques for filtering the noise:

- Additional filters within the Bit9 console can be added (and saved) to the views displaying ATI events. This can be used to exclude events based on any of the fields present, including filename, description, source (computer), user, process, file prevalence and rule name. If consuming these events from an external system like a SIEM, the same filters can often be created using the interface of the third-party software.
- Note that some attributes useful in the filtering process, such as Threat and Trust levels and File Prevalence, may not be present in the events exported to a SIEM. That is because this information is not event driven and changes based on the overall database state (e.g. file prevalence continually changes). The live information is available via the public API to the

Bit9 database if you are able to develop a custom extension to your SIEM that issues on-demand queries, or via direct access to the Bit9 console using a properly formed URL.

- When reviewing at ATI events, the 'Group by' feature can be used to group events by rule name, giving the end-user the ability to collapse the events that fire excessively and focus on the ones more relevant to their environment. As noted above, in many cases, prioritizing low prevalence ATI events and events which impact low numbers of systems over high prevalence or broad impacting events is a good first pass way to de-prioritize potential false positives.

Some ATIs rely on conditions that may be mitigated or suppressed with Bit9 policy changes. For example, if an ATI relies on the fact that a file or process is unapproved, then approving the file in question (using any of the available approval methods) will prevent that particular instance of the ATI from firing. The details in the next section cover any specific conditions such as file approval state.

2 Advanced Threat Indicators (ATIs)

This section lists each of the ATIs, details on what causes the rules to fire, the threats they are designed to identify, and information on false positives specific to each particular ATI.

The following information is provided for each ATI that might generate an event in the console:

- Rule Name – This is the name of the rule as shown in the event data.
- Updater – ATIs are currently integrated into the product using updaters. When the Detection Enhancement add-on is installed, updaters containing the ATIs are installed into the system. The updaters can be easily enabled or disabled in the console. If an updater is disabled, all ATIs contained within that updater will be disabled.
- Description – This is a short description of the ATI.
- Confidence – ATI Confidence values give an indication of the quality of the ATI in terms of identifying malicious behavior. In this document, ATIs are tagged with three possible confidence levels:
    - High: ATIs that tend to have very few, if any, false positives when observed in both test and real world environments. Any high confidence ATI should be assumed to be actionable or worth investigating.
    - Medium: ATIs that, given basic exceptions or filters specific to each environment, have a low false positive rate. In general, these ATIs have been observed to have high correlation to malicious activity but in real world environments, some legitimate applications have been observed that also trigger these events. It is recommended that medium confidence ATIs be investigated and legitimate instances be understood so they can be appropriately filtered. With proper filtering, medium confidence ATIs should be assumed to be actionable.
    - Low: ATIs that are often associated with legitimate behavior (false positives). Depending on the environment and frequency of low confidence ATIs, with proper filtering, they can identify malicious activity that might otherwise be missed.
- Threat – This gives a short description of the threat the ATI is designed to detect.
- Known Issues/False Positives – Discussion of information relating to known cases of false positives for the ATI and any other notable issues.

2.1.1 Possible exploit of document handling application

Name	Description
Rule Name	Possible exploit of document handling application
Updater	Windows Application Behavior
Indicator Set	Windows Application Behavior
Description	This ATI looks for files with executable content created by document handling applications, such as Microsoft Word, Microsoft Excel, and Adobe Acrobat Reader.
Confidence	Low
Threat	This rule detects malformed documents that leverage vulnerabilities in common desktop applications to create persistent executable content on a system. These documents are most often delivered via spear-phishing emails and are used to establish foothold when the user opens the document in an application like Adobe Reader or Microsoft Word.
Known Issues/ False Positives	It is possible for applications like Adobe Reader to install legitimate executable files, such as when adding a new plug-in, installing a new printer driver, or activating a new Microsoft Office component within any Office application. Additional file attributes available within the Bit9 Events page may be used to separate legitimate from unexpected cases, such as: • File Prevalence: A file with low prevalence (e.g. 1 or 2) indicates the file is not common in the environment and therefore less likely to be a well-known Office component or printer driver • File Publisher: Many printer drivers are digitally signed and will therefore have a Publisher • File Trust: Well-known components will have a positive (greater than 0) trust value from the Bit9 Software Reputation Service • File Path: While each document handling application is different, the location where printer drivers, add-ins and components are installed might be easily identifiable, and therefore filtered out, from the path (e.g. Windows System folder, Program Files, …) • File State: If your organization has Bit9 policies in place to automatically approve legitimate content like application components and drivers (necessary if you are using Bit9 in High Enforcement), then suspicious content should stand out with a file state of Unapproved. In some applications, users can create their own legitimate executable content. For example, in Microsoft Excel, users can create self-extracting archive files (.exe files). Such action would trigger a false positive of this ATI.

2.1.2 Possible name resolution tampering

Name	Description
Rule Name	Possible name resolution tampering
Updater	Windows System Configuration
Indicator Set	Windows System Configuration
Description	Flag when an unexpected process modifies the “hosts” file on a system
Confidence	Low
Threat	Modifying the “system32\drivers\etc\hosts” file is a way for an attacker to redirect traffic intended for a specific domain to someplace else. For example, you can use this file to cause the traffic intended for “www.yahoo.com” to be directed to a malicious website.
Known Issues/ False Positives	This could generate false positives if the user uses a command line text editor to change the file. In addition, some VPN clients modify the hosts file when VPN sessions are established and terminated. By observing the process names within the events generated by this ATI, you may be able to create an acceptable exception list that can be used to filter out legitimate or expected cases.

2.1.3 Unusual change to startup configuration

Name	Description
Rule Name	Unusual change to startup configuration
Updater	Windows System Configuration
Indicator Set	Windows Startup Configuration
Description	Flag when an unexpected process modifies registry settings that are used to control the Windows explorer (or shell) interface or other rarely used startup configuration settings
Confidence	High
Threat	Certain registry settings like Winlogon\Shell can be used to alter what loads during the Windows logon process, and these settings are rarely altered by legitimate applications. Malware like “Trojan:Win32/Ransom.FS” are known to use such settings to persist themselves after a system restart.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.4 Possible password hash tool execution

Name	Description
Rule Name	Possible password hash tool execution
Updater	Windows Process Injection
Indicator Set	Windows Process Injection
Description	Flag when an unapproved process requests read or write access to system processes known to handle credentials in memory (such as on lsass.exe)
Confidence	Medium
Threat	It is very common for a malicious attack to attempt to gather credentials after compromising a system. This is typically done by tools such as “pwdump” by injecting into, or directed attempting to read from, system processes that store or process credential information in memory.
Known Issues/ False Positives	Because there are many legitimate system and utility programs that routinely inject themselves into other processes, this particular ATI will only fire when the source process is Unapproved. Therefore, the mitigation of false positives is to simply approve (globally or locally or through any of the approval mechanisms available to Bit9) the legitimate files/processes that are observed to trigger this ATI. Note: Because Unapproved files will simply not load in High Enforcement environments, it is unlikely that this ATI will fire in those cases.

2.1.5 Possible file hiding

Name	Description
Rule Name	Possible file hiding
Updater	Windows System Configuration
Indicator Set	Windows System Configuration
Description	Flag when an unexpected process modifies the Explorer configuration setting that controls whether or not files marked as hidden will be displayed.
Confidence	Medium
Threat	A simple technique used by some malware for hiding it to simply mark their files with a “hidden” attribute and configure Windows Explorer to not display hidden files. It is otherwise rare for a legitimate application to programmatically alter this setting.
Known Issues/ False Positives	This ATI automatically excludes the case where a user manually adjusts the “show hidden” setting within Explorer. However, this setting is modified the first time a user logs into a system and that will trigger this ATI to fire. If the corresponding registry setting is modified via a GPO, it could also cause this event to fire.

2.1.6 File execution from Recycle Bin

Name	Description
Rule Name	File execution from Recycle Bin
Updater	Windows File Properties
Indicator	Windows Suspicious Based on Path
Description	Report execution of a file from the Recycle Bin
Confidence	High
Threat	Attackers, particularly APT, often hide their malware in unexpected locations such as the Recycle Bin. Legitimate software should never run from this location.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.7 Suspicious executable based on extension

Name	Description
Rule Name	Suspicious executable based on extension
Updater	Windows File Properties
Indicator	Windows Suspicious Based on File Name
Description	Report when files are created that are intentionally named to obfuscate their true purpose or mask the fact that they are executable.
Confidence	High
Threat	A common malware technique is to embed a fake/benign looking extension into their filename, so if file extensions are not displayed in Explorer (which is the default behavior), the file will appear to be non-executable. For example, a file called “foo.gif.exe” might just show as “foo.gif” and be thought to be an image. A user might double click on such a file to view the image, when in fact it will launch the malicious program.
Known Issues/ False Positives	A user could legitimately name a file in this manner, but it would be highly unlikely. Anything flagged by this ATI warrants further investigation.

2.1.8 Suspicious executable based on name

Name	Description
Rule Name	Suspicious executable based on name
Updater	Windows File Properties
Indicator	Windows Suspicious Based on File Name
Description	Report when files with names designed to hide in plain sight are executed or written
Confidence	High
Threat	A common technique for hiding malicious processes in plain sight is to use names that look like legitimate Windows system file names. For example, using a “0” (zero) instead of an uppercase “o”, or using a lowercase “L” instead of an uppercase “i". This rule looks for filenames using these techniques that have been associated with malware.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.9 Suspicious executable based on location

Name	Description
Rule Name	Suspicious executable based on location
Updater	Windows File Properties
Indicator	Windows Suspicious Based on Path
Description	Flag when a process creates an executable in the Java application data directory (<AppData>\Sun\Java*.exe) or (<AppData>\Oracle*.exe)
Confidence	Medium
Threat	Java related malware may use a vulnerability or simply malicious code to drop additional payloads. These are commonly created in the Java application data folder.
Known Issues/ False Positives	Some legitimate Java tools and uninstallers have been observed to create executable files in Application Data directory, although it is relatively rare. Such conditions can cause false positives. We are continuing to review this ATI for improvements.

2.1.10 Possible application hijacking

Name	Description
Rule Name	Possible application hijacking
Updater	Windows System Configuration
Indicator	Windows System Configuration
Description	Report when changes are made to configuration options that trigger the execution of an alternate application when a legitimate application is launched. Specifically, there is an “Image File Execution Options” registry key within Windows that allows users to set a Debug option to override the default behavior when an application is executed.
Confidence	Medium
Threat	The “Image File Execution Options” section of the registry allows you to configure a debugger to run with *any* application. While this is intended to be a useful ability, it is a common stealth way for malware to persist. For example, with a single setting, you can configure Windows to run “yourapp.exe” whenever someone runs Notepad – even if they directly double click on the correct icon or any other valid launch mechanism.
Known Issues/ False Positives	Development tools will often modify this registry key to facilitate code debugging. Outside of development tools, changing this configuration is very rare.

2.1.11 Windows firewall tampering

Name	Description
Rule Name	Windows firewall tampering
Updater	Windows System Configuration
Indicator	Windows System Configuration
Description	Flag when the firewall is disabled
Confidence	Medium
Threat	A common technique for malware is to disable any firewalls that might interfere with command-and-control communication used by malware. This indicators checks for unexpected changes to the firewall settings in the Windows registry.
Known Issues/ False Positives	Some custom applications or user scripts could cause this to false fire, though it is uncommon. Filtering on the process name can be done to exclude most observed legitimate cases.

2.1.12 Unusual change to startup configuration

Name	Description
Rule Name	Unusual change to startup configuration
Updater	Linux System Configuration
Indicator Set	Linux Startup Configuration
Description	Flag when an unexpected process modifies /bin/login
Confidence	Low
Threat	This looks for malware that attempts to persist by embedding itself in the login application of a Linux installation.
Known Issues/ False Positives	Some large companies have login scripts that could trigger this ATI event. Another possible false positive could be first time logins to an account when legitimate login files are first created.

2.1.13 Known malware file name

Name	Description
Rule Name	Known malware file name
Updater	Windows File Properties
Indicator Set	Windows Suspicious Based on File Name
Description	Report when files with uncommon names known to be associated with malware are written or executed
Confidence	High
Threat	Similar to the "*Suspicious executable based on name* "ATI, this indicator looks for filenames are that unique enough based on global observation to be interesting/rare and generally associated with known malware campaigns.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.14 Installation of language pack

Name	Description
Rule Name	Installation of language pack
Updater	Windows System Configuration
Indicator Set	Windows System Configuration
Description	Report when a new language pack is installed
Confidence	Low
Threat	Language packs are sometimes installed by foreign attackers to facilitate their interaction with a compromised system. Legitimate installations are typically done on initial system deployment, which should reduce false positives.
Known Issues/ False Positives	This ATI will alert on legitimate as well as illegitimate installations of a system language pack on Windows. This should be a low frequency event in most deployments, but may be more common in global deployments or environments where multiple languages are used by employees. Alerts should be validated to ensure that the installation of the language pack is authorized. The details of the ATI event data may provide clues as to the language installed.

2.1.15 Execution from System Volume Information path

Name	Description
Rule Name	File execution from System Volume Information
Updater	Windows File Properties
Indicator Set	Windows Suspicious Based on Path
Description	Report when files are executed from the "System Volume Information" folder
Confidence	High
Threat	Similar to the "*File execution from Recycle Bin*" ATI, this is another location where attackers are known to hide malware.
Known Issues/ False Positives	We have observed some false positives with paths that include GUIDs enclosed in braces {}. We are currently investigating these and will refine the rule as more is learned.

2.1.16 Execution of system file name outside of system folder

Name	Description
Rule Name	Execution of system file name outside of system folder
Updater	Windows File Properties
Indicator Set	Windows Suspicious Based on Path and File Name
Description	Report when files named the same as critical Windows system files are executed outside of their installed location
Confidence	High
Threat	Attackers will often use known system file names for malicious code, placing those files in alternate locations. This is done to hide in plain sight, as the names shown in a listing of active processes will not stand out as suspicious.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation. Note: Older versions of this ATI (prior to 1.2) generated many false positives for "wmiprvse." That issue has since been addressed.

2.1.17 Execution of obscure system utility

Name	Description
Rule Name	Execution of obscure system utility
Updater	Windows Application Behavior
Indicator Set	Windows Suspicious Based on Path and File Name
Description	Report when obscure (rarely used) system utilities useful in attacks are executed
Confidence	Low
Threat	One of the first things an attacker will do after gaining a foothold is determine what other users may be currently logged in. Quser.exe is an obscure system utility that provides this information and is routinely used by attackers, but less commonly used for legitimate purposes.
Known Issues/ False Positives	While rare, quser is a legitimate utility . If this event occurs at high volume, it may indicate that this utility is used for valid purposes in the environment, and this ATI may not be actionable. If this event rarely fires, then it is more likely to be indicative of an ongoing interactive attack.

2.1.18 File associated with SSH backdoor

Name	Description
Rule Name	File associated with SSH backdoor
Updater	Linux File Properties
Indicator Set	Linux Possible Backdoor
Description	Report on creation or execution of known SSH backdoor files and behavior
Confidence	High
Threat	Files flagged here are associated with known Linux SSH backdoors. In some cases, the files may appear to be legitimate libraries, but are associated with versions that do not legitimately exist.
Known Issues/ False Positives	Poorly maintained updates to Libkeyutils could trigger a false positive under extremely limited conditions.

2.1.19 Possible exploit of document handling application

Name	Description
Rule Name	Possible exploit of document handling application
Updater	Mac Application Behavior
Indicator Set	Mac Application Behavior
Description	Similar to the Windows version of this same rule, this ATI looks for files with executable content created by document handling applications, such as Microsoft Office.
Confidence	Low
Threat	This rule detects malformed documents that leverage vulnerabilities in common desktop applications to create persistent executable content on a system. These documents are most often delivered via spear-phishing emails and are used to establish foothold when the user opens the document in an application like Adobe Reader or Microsoft Word.
Known Issues/ False Positives	Possible false positive conditions include those identified in the Windows version of this ATI – namely, self-extracting archives created from the application, updates, and possible plugin additions.

2.1.20 File execution from Trash

Name	Description
Rule Name	File execution from Trash
Indicator Set	Mac Suspicious Based on Path
Updater	Mac File Properties
Description	Report execution of a file from the trash
Confidence	High
Threat	This addresses a common malware tactic of hiding a file in the trash, similar to using the Recycle Bin on Windows.
Known Issues/ False Positives	While it is possible to manually execute a file placed in the trash, it is highly unlikely. Anything flagged by this ATI warrants further investigation.

2.1.21 Suspicious shell use

Name	Description
Rule Name	Suspicious shell use
Updater	Mac Application Behavior
Indicator Set	Mac Shell Activity
Description	Report when a command shell is executed by a browser process
Confidence	Low
Threat	A web browser launching a command shell is a common technique used in drive-by infections.
Known Issues/ False Positives	If an environment uses an internal help desk web site to launch configuration or other scripts, such as mounting a network drive, that could trigger this ATI.

2.1.22 Browser dropping Trojan behavior

Name	Description
Rule Name	Browser dropping Trojan behavior
Updater	Windows Application Behavior
Indicator Set	Windows Application Behavior
Description	Report when a browser process writes files consistent with known malware
Confidence	Low
Threat	This looks for typical behavior observed when a browser is exploited and malicious files are dropped on the system. These techniques are common with attacks such as Zeus and SpyEye.
Known Issues/ False Positives	We have observed some environments generating a high number of false positives for this ATI. We are currently reviewing for improvements. Typically, files triggering this ATI existing directly under %appdata% and those under %appdata%\<6 random characters>\ should be the focus of any investigation.

2.1.23 Modification of the root finder plist

Name	Description
Rule Name	Modification of the root finder plist
Updater	Mac System Configuration
Indicator Set	Mac System Configuration
Description	Report when an attempt is made to modify the Finder properties list (plist) from the command line
Confidence	Medium
Threat	Malware may modify the plist in an attempt to persist or hide itself. This is uncommon under legitimate circumstances.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.24 Possible file hiding

Name	Description
Rule Name	Possible file hiding
Updater	Mac System Configuration
Indicator Set	Mac System Configuration
Description	Report when an attempt is made to modify the hidden attributes of a file from the command line
Confidence	Medium
Threat	Malware may use the chflags utility to hide files. This activity is atypical and usually indicative of a script trying to hide something from Finder.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.25 Modification of boot plist

Name	Description
Rule Name	Modification of boot plist
Updater	Mac System Configuration
Indicator Set	Mac System Configuration
Description	Report unexpected changes to the boot properties list
Confidence	Medium
Threat	This boot properties list (plist) file is used during startup to configure boot operations. Malware may modify this file in an attempt to run commands as the root user early in the boot sequence.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.26 Modification of boot time kernel extensions

Name	Description
Rule Name	Modification of boot time kernel extensions
Updater	Mac System Configuration
Indicator Set	Mac System Configuration
Description	Report unexpected modifications to the configuration of startup kernel extensions
Confidence	Medium
Threat	Malware may modify this configuration file in an attempt to persist on restart
Known Issues/ False Positives	Some application installs and legitimate system updates may modify this same file and trigger this ATI to fire.

2.1.27 Possible backdoor installation

Name	Description
Rule Name	Possible backdoor installation
Updater	Mac File Properties
Indicator Set	Mac Suspicious Based on Path and File Name
Description	This rule looks for the creation of Known Malicious Plist or Component
Confidence	High
Threat	This is a known artifact of multiple Tibet.c variants.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.28 Possible POS malware registry entry

Name	Description
Rule Name	Possible POS malware registry entry
Updater	Windows System Configuration
Indicator Set	Windows POS Indicators
Description	This rule is designed to report on registry modifications indicative of POS malware
Confidence	Medium
Threat	This rule looks for known POS malware artifacts. These artifacts were found in malware analysis of samples from some of the biggest POS breaches in 2014
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.29 Possible APT backdoor installation

Name	Description
Rule Name	Possible APT backdoor installation
Updater	Windows System Configuration
Indicator Set	Windows POS Indicators
Description	This ATI looks for indications of sethc.exe or utilmon.exe being replaced. This activity can effectively create a backdoor to the system.
Confidence	High
Threat	One tactic observed to be associated with APT activity is the creation of a 'backdoor' by replacing one of these files with cmd.exe. This will allow the attacker unauthenticated access to cmd.exe with SYSTEM privileges. If this ATI fires, these files should be checked to ensure they are the right files, and have not been replaced with cmd.exe or any other binary.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything flagged by this ATI warrants further investigation.

2.1.30 Suspicious modification to windows service

Name	Description
Rule Name	Suspicious modification to windows service
Updater	Windows System Configuration
Indicator Set	Windows System Configuration
Description	This looks for modifications to the services keys in the windows registry performed by reg.exe
Confidence	Medium
Threat	Attackers often use the windows services architecture to gain persistence and have their code execute early on in the boot process. They often accomplish this by modifying the registry using the reg.exe command. Legitimately installed services will normally update the registry via windows API calls and not via reg.exe.
Known Issues/ False Positives	Potential for FPs due to sloppy installers, but this activity is typically only seen during attacks

2.1.31 Possible ransomware file artifact

Name	Description
Rule Name	Possible ransomware file artifact
Updater	Windows File Properties
Indicator Set	Windows Ransomware Indicators
Description	This rule looks for some generic behaviors of ransomware
Confidence	Medium
Threat	Threats covered by this ATI include some variants of Reveton and similar ransomeware.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.32 Possible ransomware registry entry

Name	Description
Rule Name	Possible ransomware registry entry
Updater	Windows System Configuration
Indicator Set	Windows Ransomware Indicators
Description	Report on registry activity consistent with reveton and CryptoLocker v1.0 and v2.0 infections.
Confidence	High
Threat	Ransomware infections such as reveton and cryptolocker
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.33 Possible POS malware file artifact

Name	Description
Rule Name	Possible POS malware file artifact
Updater	Windows File Properties
Indicator Set	Windows POS Indicators
Description	This rule looks for the known artifacts of various POS malware.
Confidence	Medium
Threat	POS-targeted malware designed to facilitate the theft of credit card data.
Known Issues/ False Positives	Some legitimate printer applications create system logs in the temp directory. This is not common but could be a source of false positives.

2.1.34 Suspicious file activity in known APT staging area

Name	Description
Rule Name	Suspicious file activity in known APT staging area
Updater	Windows File Properties
Indicator Set	Windows Suspicious Based on Path and File Name
Description	Report on specific file types being written to locations that would be highly unusual and indicative of an APT activity.
Confidence	Medium
Threat	Locations monitored by this ATI have been observed to be used by APT actors to drop executables and run them. Because of the relative obscurity of these directories under Windows, they may not seem unusual at first glance. We are unaware of any legitimate reasons for an executable to exist or run from these locations.
Known Issues/ False Positives	We are currently unaware of any false positive conditions.

2.1.35 Possible credential theft or misuse

Name	Description
Rule Name	Possible credential theft or misuse
Updater	Windows File Properties
Indicator Set	Windows Suspicious Based on Path and File Name
Description	This looks for indications of the execution of wce.exe
Confidence	High
Threat	Wce.exe (windows credential editor), is a tool that allows for the harvesting of credentials on a system and performs pass-the-hash and pass-the-ticket attacks. This tool is often used during attacks to escalate privileges and move through the target environment.
Known Issues/ False Positives	We are currently unaware of any false positive conditions.

2.1.36 Possible privilege escalation attempt

Name	Description
Rule Name	Possible privilege escalation attempt
Updater	Mac System Configuration
Indicator Set	Mac System Configuration
Description	This rule looks for password reset conditions on OSX
Confidence	High
Threat	The modification or deletion of this file causes OSX to go into user setup mode upon reboot. The attacker can then create a local admin account on the host and have admin/root privileges.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.37 SQL services creating a binary

Name	Description
Rule Name	SQL services creating a binary
Updater	Windows Application Behavior
Indicator Set	Windows Application Behavior
Description	This looks for indications of an SQL server writing an executable file.
Confidence	Medium
Threat	Under normal circumstances, it would be very unusual for the SQL Server to create executables. However, if the SQL server service is compromised, arbitrary files can be written to the file system. This is particularly true with SQL Injection or other attacks targeting the back-end database that serves websites.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.38 Remote System Admin Tool Usage – Source

Name	Description
Rule Name	Remote System Admin Tool Usage - Source
Updater	Windows Admin Tool Tracking
Indicator Set	Windows Admin Tool Tracking
Description	Looks for the use of commonly abused administration tools
Confidence	Low
Threat	Attackers often use legitimate tools to fly under the radar and move laterally within an environment. As such, this ATI tracks this activity for psexec. This ATI will generate an event on the system where psexec is launched. This can help to determine where the attacker is operating from during an attack.
Known Issues/ False Positives	While we are not aware of any False Positives, psexec is used heavily in some environments and this tracking may not be desirable for all customers. As such, this ATI and the related one 'Remote System Admin Tool Usage – Target', are included in a separate indicator set that can easily be disabled.

2.1.39 Remote System Admin Tool Usage – Target

Name	Description
Rule Name	Remote System Admin Tool Usage – Target
Updater	Windows Admin Tool Tracking
Indicator Set	Windows Admin Tool Tracking
Description	Looks for commonly abused admin tools being leveraged against a target system
Confidence	Low
Threat	Attackers often use legitimate tools to fly under the radar and move laterally within an environment. As such, this ATI tracks this activity for psexec. This ATI will generate an event on the remote system psexec is accessing. This can help to determine the systems that an attacker has used psexec to run commands on.
Known Issues/ False Positives	While we are not aware of any False Positives, psexec is used heavily in some environments and this tracking may not be desirable for all customers. As such, this ATI and the related one 'Remote System Admin Tool Usage – Source', are included in a separate indicator set that can easily be disabled.

2.1.40 Suspicious svchost execution

Name	Description
Rule Name	Suspicious svchost execution
Updater	Windows Application Behavior
Indicator Set	Windows Suspicious Based on Parent
Description	Looks for svchost being launched by something outside the norm
Confidence	Medium
Threat	Malware will often times launch an instance of svchost as a container for their malicious process. Execution of svchost is fairly well-defined and under normal circumstances, should not be launched by anything other than a handful of processes. This ATI looks for svchost.exe being spawned in an unusual manner.
Known Issues/ False Positives	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.41 Suspicious process execution

Name	Description
Rule Name	Suspicious process execution
Updater	Windows Application Behavior
Indicator Set	Windows Suspicious Based on Parent
Description	Looks for processes launched by programs that shouldn't spawn processes
Confidence	Medium
Threat	To avoid detection, attackers will often inject code into other processes to carry out their malicious activities. Two popular targets of this activity are notepad.exe and calc.exe, as they are present on every windows system and generally benign. Any process spawned by these programs would be considered highly suspicious.
Testing	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.42 Possible Java Attack

Name	Description
Rule Name	Possible Java attack
Indicator Set	Windows Application Behavior
Description	This rule fires if Java writes an executable to the temp directory.
Confidence	High
Threat	Java is frequently used as an exploit vector by attackers, and should not be writing executables in unusual places.
Testing	We are currently unaware of any specific conditions that would generate false positives for this ATI. Anything found in this view would most likely warrant further investigation.

2.1.43 Possible WMI Persistence

Name	Description
Rule Name	Possible WMI persistence
Indicator Set	Windows Application Behavior
Description	This query looks for evidence of a persistence mechanism using WMI that appears when registering a WMI event filter that uses w32_localtime.
Confidence	Medium
Threat	Windows Management Instrumentation (WMI) can be leveraged to provide a persistence mechanism to attackers. One of the techniques often used is to have an event kick off at a specific time which typically requires win32_localtime.
Testing	A legitimate WMI filter may use w32_localtime as well.

2.1.44 Modification of the powershell execution policy

Name	Description
Rule Name	Modification of powershell execution policy
Indicator Set	Windows System Configuration
Description	This rule looks for changes to the registry key that set the powershell execution policy.
Confidence	Medium
Threat	Attackers may modify this registry key to change the powershell execution policy to facilitate their attack – for instance, allowing powershell to run unsigned scripts downloaded from the Internet.
Testing	While this key may be modified by system administrators, it should be a rare occurrence.

2.1.45 Shell Spawned from a browser

Name	Description
Rule Name	Shell Spawned from a browser
Indicator Set	Mac Application Behavior
Description	This rule looks for command shells spawned from web browsers.
Confidence	Medium
Threat	This may indicate an attacker has compromised a web browser and is using it as an initial foothold into a local host.
Testing	Some VOIP applications (GoToMeeting, WebEx) may spawn a shell when launched from a browser. In addition, browsers such as Chrome may spawn a shell as part of their update process.

2.1.46 Possible privilege escalation attempt

Name	Description
Rule Name	Possible privilege escalation attempt
Indicator Set	Mac System Configuration
Description	This rule looks for modifications of the AppleSetUpDone file.
Confidence	High
Threat	An attacker could modify this file in order to change passwords or add a new administrative account to a system.
Testing	After the computer is initially configured, it is very rare for this file to be modified.

2.1.47 Suspicious OSX persistence

Name	Description
Rule Name	Suspicious OSX Persistence
Indicator Set	Mac System Configuration
Description	This rule looks for activity related to launchd.conf, startupparameters.plist, or loginitems.plist
Confidence	Medium
Threat	An attacker may add entries to these files in order to maintain persistence on a system; similar to a Windows scheduled task.
Testing	These files may be modified as part of legitimate system activity.

2.1.48 Modification of rc.common

Name	Description
Rule Name	Modification of rc.common
Indicator Set	Mac System Configuration
Description	This rule identifies processes that modify /etc/rc.common.
Confidence	Medium
Threat	Attackers may modify this file in order to gain persistence for malicious code on a target system.
Testing	We are currently unaware of any specific conditions that would generate false positives for this query. Any hits would most likely warrant further investigation.

2.1.49 Modification to crontab

Name	Description
Rule Name	Modification to crontab
Indicator Set	Mac System Configuration
Description	This reports on changes to the system's crontab.
Confidence	Medium
Threat	An attacker may add entries to the crontab in order to maintain persistence (similar to a Windows scheduled task.)
Testing	Some normal system processes may modify the crontab.

2.1.50 Powershell or WinRM remoting activity

Name	Description
Rule Name	Powershell or WinRM remoting activity
Indicator Set	Windows Admin Tool Tracking
Description	This query identifies use of powershell remoting (WinRM).
Confidence	Medium
Threat	Attackers may use WinRM remoting to move laterally or perform remote code execution. Wsmprovhost.exe is the host process that is spawned when powershell is executed on a remote host. The powershell script is run within this context.
Testing	Administrators may legitimately use this functionality

2.1.51 Processes started by Powershell remoting (WinRM)

Name	Description
Rule Name	Process started via powershell remoting (WinRM).
Indicator Set	Windows Admin Tool Tracking
Description	This query looks for processes spawned remotely via powershell or WinRM
Confidence	Medium
Threat	When powershell remoting (WinRM) is used to run processes on remote systems, the processes are spawned by wsmprovhost.exe.
Testing	Administrators may legitimately use this functionality

2.1.52 Winrm Activity

Name	Description
Rule Name	WinRM command activity
Indicator Set	Windows Admin Tool Tracking
Description	This query identifies executions of WinRM.cmd or WinRM.vbs with the invoke parameter.
Confidence	Medium
Threat	Windows Remote Management (WinRM) is a protocol that allows for remotely administering systems. It can be leveraged by attackers for lateral movement or remote command execution.
Testing	The WinRM command may be legitimately used by administrators.

2.1.53 Shell spawned by office app

Name	Description
Rule Name	Shell spawned by office app
Indicator Set	Windows Suspicious Based on Parent
Description	This ATI flags instances of cmd or powershell run by Excel, Powerpoint or Word.
Confidence	High
Threat	This behavior may indicate an Office file attempting to run malicious code.
Testing	We are currently unaware of any specific conditions that would generate false positives for this query. Any hits would most likely warrant further investigation.

2.1.54 Possible regsvr32 misuse

Name	Description
Rule Name	Possible regsvr32 misuse
Indicator Set	Windows Application Behavior
Description	This query looks for dlls loaded by regsvr32 that may be used to execute remote commands.
Confidence	High
Threat	Attackers may use regsvr32 to run a script hosted on an external webserver; this is a technique to avoid application whitelisting.
Testing	No false positives observed so far