Sign in

ThreatHuntingProject / ThreatHunting

Public

Notifications Fork 373 Star 1.7k

Code Issues 3 Pull requests 4 Actions Projects Security Insights

ThreatHunting / hunts / suspicious_process_creation_via_windows_event_logs.md

68 lines (43 loc) · 2.61 KB

Preview Code Blame Raw

#Suspicious Process Creation via Windows Event Logs

Purpose

Find attacker tools in use

Data Required

Windows process creation logs (Event 4688 & 592) or equivalent (Carbon Black, Sysmon, etc)

Collection Considerations

Collect these from every host in the domain.

Analysis Techniques

stack counting

Description

Search all process creation log entries and look for:

- `svchost.exe` processes that are not children of `services.exe`

- Processes created by binaries in unsual locations, such as
  - `%windows%\fonts`
  - `%windows%\help`
  - `%windows%\wbem`
  - `%windows%\addins`
  - `%windows%\debut`
  - `%windows%\system32\tasks`
  - `*:\RECYCLER\`
  - `*:\SystemVolumeInformation\`
  - `%windir%\Tasks\`
  - `%systemroot%\debug\`
- Known attacker tool names, such as
  - `rar.exe`
  - `psexec.exe`
  - `whoami.exe`
- Processes that launched very few times during a 24 hour period

The following are based on a set of tweets by Jack Crook (@jackcr):

"Attackers need to execute tools. Look at Windows Event ID's 4688/592. Stack and look for outliers. Group by execution time and user."

"Finding webshells: Look at process creations (4688/592) that are spawned from users that own webserver processes."

"One of my favorites is that knowing when attackers bring tools in with them they will likely not execute them very often in a 24hr time period. Looking at precess creations with a hard limit of executing x number of times in a day and ordering by by file path. Can start to weed out, either manually or automated, those processes that have been validated as legit"

Other Notes

Event 4688 is even more valuable if logging policy is set to record the entire command line (some of these suggestions require that info). Review your domain audit policies and/or supplement with additional process logging as necessary. Sysmon is a very good free tool that can do nearly anything you'd need.

More Info

- Tweet by @jackcr #1
- Tweet by @jackcr #2
- Tweet by @jackcr #3
- Tweet by @jackcr #4
- Tweet by @jackcr #5
- Seek Evil, and Ye Shall Find: A Guide to Cyber Threat Hunting Operations, Tim Bandos, Digital Guardian
- CAR-2013-05-002: Suspicious Run Locations, MITRE Cyber Analytic Repository
-