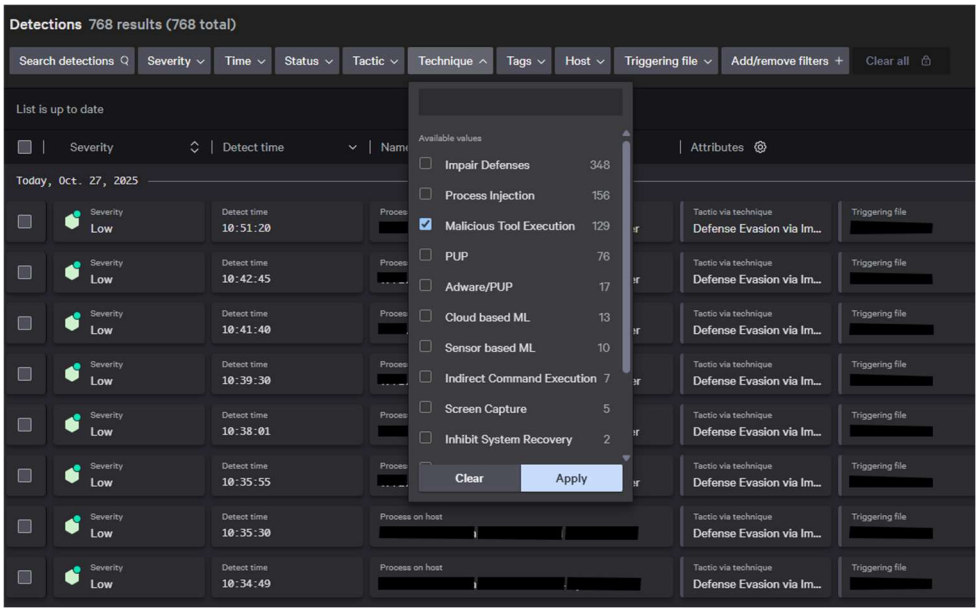
Hunting and Remediating Persistent Adware

MCNC Security Operations continues to monitor all client Crowdstrike environments for new detections and will reach out when there is an issue that requires your action to remediate. As a result of this monitoring we have broad awareness of current trends in malware and other threats. Recently we have noted a spike in detections for adware related to Node.js installations, which is a common cross-platform JavaScript runtime environment and also a popular attack vector.

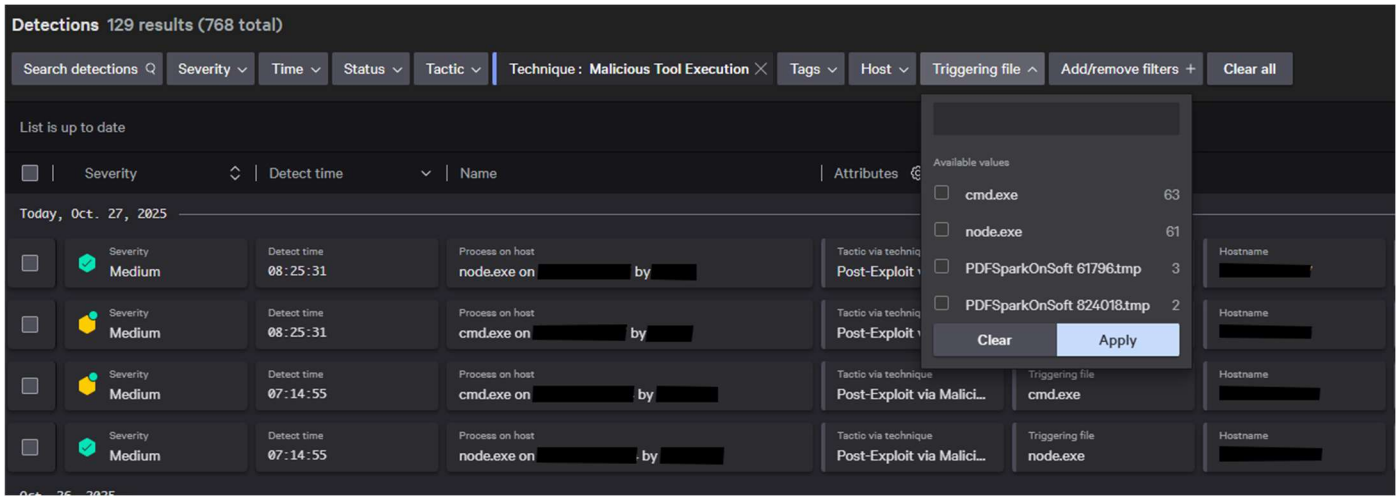
These detections generally do not rise to the level of Ops engagement, as the Crowdstrike sensor effectively blocks these executables from running; however, the files are common and persistent enough to generate large amounts of detections in many client environments. Removing this noise can help both you and SecOps focus on legitimate threats, so this document will discuss how to find this type of malware in your environment as well as potential avenues for remediation.

Endpoint Detections

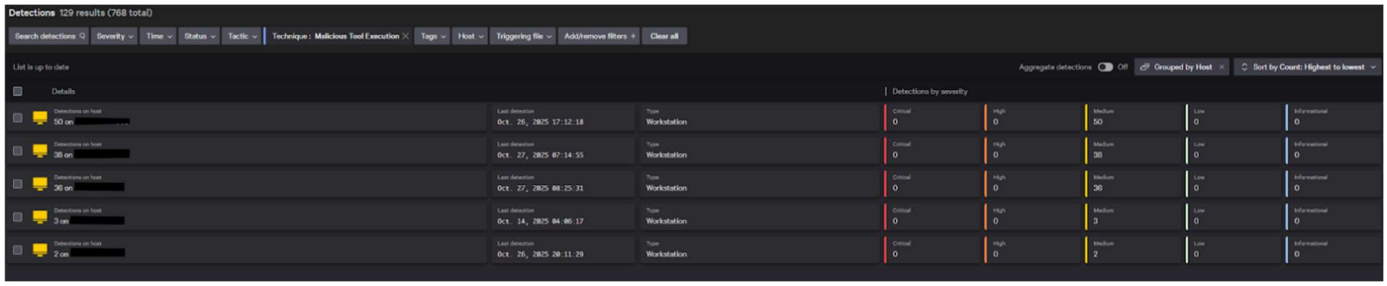
The Endpoint Detections tool (Menu>Endpoint Security>Monitor>Endpoint detections) lists all detections that have occurred in your environment over the past 90 days. As part of the managed service SecOps monitors these detections and will reach out when they see something that requires action on your part, but this data is available for your awareness as well. Data can be filtered to look for specific tactics & techniques, severity, hostnames, or any other parameter. Today we're interested in threats attempting to use legitimate tools maliciously, so we can filter on 'Technique: Malicious Tool Execution'.



We can filter further by the specific triggering file - most of what we see in this environment involves either node.exe or cmd.exe as the trigger. cmd.exe and node.exe are frequently paired because malicious instances of node.exe are commonly spawned via command prompt:



Grouping these results by Host allows you to quickly see which assets are generating these detections and may require remediation:



Advanced Event Search

Crowdstrike also provides access to event data in your environment, allowing more customizable queries, filtering, and presentation options. Advanced Event Search (Menu>Investigate>Search>Advanced Event Search) uses the Logscale platform which is similar to Splunk, and while Crowdstrike provides in-depth documentation, guidance on building queries is outside the scope of this document.

SecOps has developed the following query which can be used in your environment to track detections related to Node.js and call out the file paths of the malicious scripts as well as whether there's a scheduled task associated with the detection, which could indicate persistence:

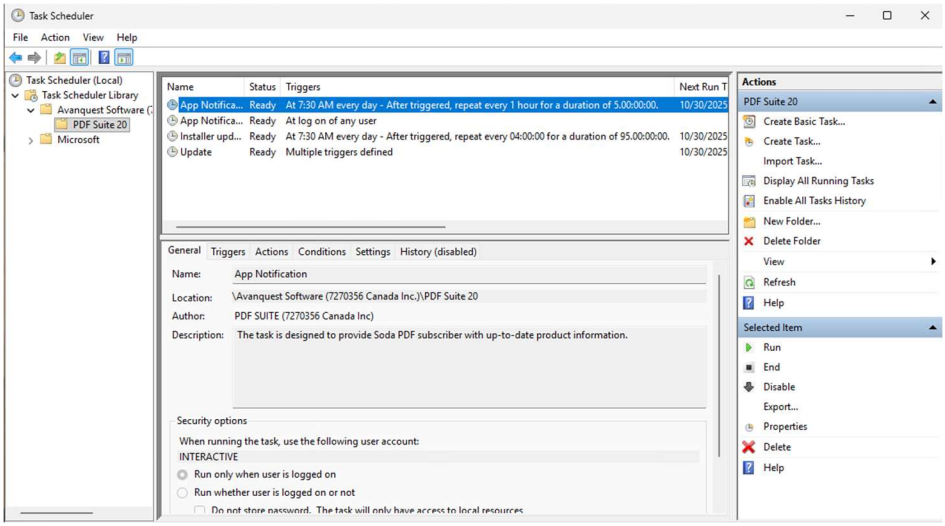
```
#event_simpleName = Event_EppDetectionSummaryEvent
| Technique = "Malicious Tool Execution"
| regex(field=FilePath, regex="(?<MalPath>\\\\Users\\\\.*?)\\w+\\.exe")
| regex(field=CommandLine,
regex="\\s{2}.*?(?<MalScripts>\\\\Users\\\\.*?\\w+\\\\.*)\"")
| case{
    GrandParentCommandLine = /svchost.exe -k netsvcs -p|svchost.exe -k netsvcs -p -s
Schedule/i | SchdTask := "There is an associated Scheduled Task running. Please
review the scheduled tasks on this host and remove any which references the
Malicious FilePath(s) or Malicious Script(s) loaded by Node.";
    * | SchdTask := "Cannot verify presence of scheduled task from process tree
command line"
}
| rename([[MalPath, "Malicious Path"], [MalScripts, "Malicious Script Loaded by
Node"], [SchdTask, "Scheduled Task"], [SHA256String, FileHash]])
| groupBy([Hostname, UserName], function=[count(as="Number of Detections"),
collect(["Malicious Path", "Malicious Script Loaded by Node", "Scheduled Task",
FileHash])])
```

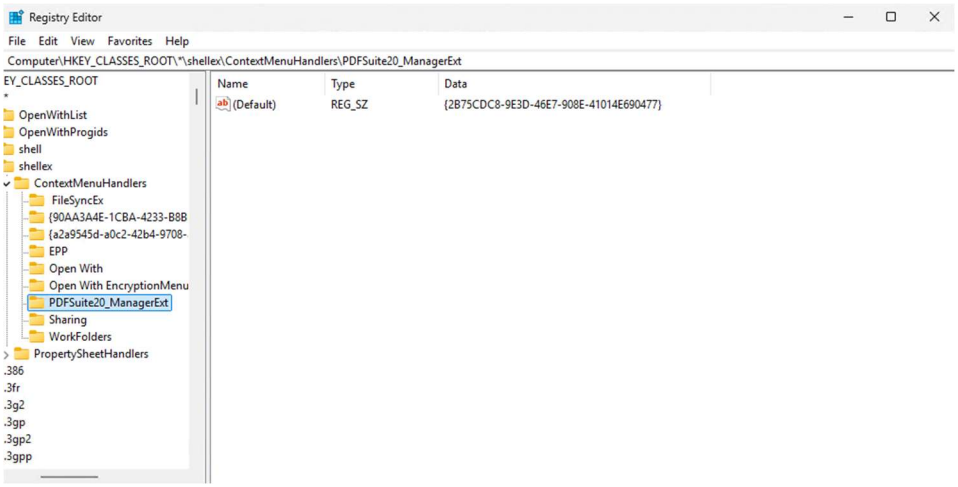
This search can also be executed automatically in your environment with the following link:

https://falcon.laggar.gcw.crowdstrike.com/investigate/search?end=&query=%23event_simpleName%20%3D%20Event_EppDetectionSummaryEvent%0A%7C%20Technique%20%3D%20%22Malicious%20Tool%20Execution%22%0A%7C%20regex%28field%3DFilePath%2C%20regex%3D%22%28%3F%3CMalPath%3E%5C%5C%5C%5CUsers%5C%5C%5C%5C.*%3F%29%5C%5Cw%2B%5C%5C.exe%22%29%0A%7C%20regex%28field%3DCommandLine%2C%20regex%3D%22%5C%5Cs%7B2%7D.*%3F%28%3F%3CMalScripts%3E%5C%5C%5C%5CUsers%5C%5C%5C%5C.*%3F%5C%5Cw%2B%5C%5C%5C%5C.*%29%5C%22%22%29%0A%7C%20case%7B%0A%20%20%20%20GrandParentCommandLine%20%3D%20%2Fsvchost.exe%20-k%20netsvcs%20-p%7Csvchost.exe%20-k%20netsvcs%20-p%20-s%20Schedule%2Fi%20%7C%20SchdTask%20%3A%3D%20%22There%20is%20an%20associated%20Scheduled%20Task%20running.%20Please%20review%20the%20scheduled%20tasks%20on%20this%20host%20and%20remove%20any%20which%20references%20the%20Malicious%20FilePath%28s%29%20or%20Malicious%20Script%28s%29%20loaded%20by%20Node.%22%3B%0A%20%20%20%20*%20%7C%20SchdTask%20%3A%3D%20%22Cannot%20verify%20presence%20of%20scheduled%20task%20from%20process%20tree%20command%20line%22%0A%7D%0A%7C%20rename%28%5B%5BMalPath%2C%20%22Malicious%20Path%22%5D%2C%20%5BMalScripts%2C%20%22Malicious%20Script%20Loaded%20by%20Node%22%5D%2C%20%5BSchdTask%2C%20%22Scheduled%20Task%22%5D%2C%20%5BSHA256String%2C%20FileHash%5D%5D%29%0A%7C%20groupBy%28%5BHostname%2C%20UserName%5D%2C%20function%3D%5Bcount%28as%3D%22Number%20of%20Detections%22%29%2C%20collect%28%5B%22Malicious%20Path%22%2C%20%22Malicious%20Script%20Loaded%20by%20Node%22%2C%20%22Scheduled%20Task%22%2C%20FileHash%5D%29%5D%29&repo=all&searchViewInteractions=NoXSA&start=1y&timezone=America%2FNew_York

Remediation

If you have identified a suspicious file path and/or scheduled task, the next step is remediation. Actions will depend on the specific asset type, threat, and persistence mechanisms but will typically involve removing registry keys and scheduled tasks associated with the malware. Here are some examples of tasks and keys added when installing PDF Suite, a known adware/PUP that generates frequent Crowdstrike detections for malicious tool execution:





This removal process could potentially be scripted in Powershell for scalability and ease of use. If you would like assistance identifying or removing these types of threats in your environment, please contact:

MCNC Security Operations

secops@mcnc.org

919-248-4141