Integrity Monitoring Detailed Change Report

Time Filter:	August 5, 2021 12:00 AM - August 6, 2021 12:00 AM	**Generated By:**	MasterAdmin
Computer Filter:	All Computers	**Generated On:**	August 6, 2021 8:30 AM
Tag Filter:	All		

172.19.0.32

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.19.0.33

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.19.0.34

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.19.0.35

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.19.0.36

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.19.0.37

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.19.0.38

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.19.0.39

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

172.20.0.10

Number of Changes:	50
Number of Objects Created:	0
Number of Objects Updated:	50
Number of Objects Deleted:	0
Number of Objects Renamed:	0

Number of Changes to Objects of Each Type

File	4
Service	46

Integrity Events

Time:	August 5, 2021 12:18:18 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 12:44:21 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 12:58:33 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 1:32:57 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 2:10:49 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 2:37:11 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 2:47:33 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\.net framework\.net framework ngen v4.0.30319 64
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 02:57:54" to "August 5, 2021 02:47:33" After the change the File had the following attributes: Created: August 22, 2013 20:41:27 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 02:47:33 Owner: NT AUTHORITY\SYSTEM Permissions: D:ARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FR;;;AU)(A;;0x1200a9;;;LS)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;SY) SHA-1: 5DC95C7FF58CAEBDEB93B0565F45D1CDC14904E6 Size: 3710

Time:	August 5, 2021 2:47:35 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\.net framework\.net framework ngen v4.0.30319
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 02:57:56" to "August 5, 2021 02:47:35" After the change the File had the following attributes: Created: August 22, 2013 20:41:11 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 02:47:35 Owner: NT AUTHORITY\SYSTEM Permissions: D:ARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FR;;;AU)(A;;0x1200a9;;;LS)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;SY) SHA-1: BB35B0877283D6D9335E1F9D8698992910899BCD Size: 3704

Time:	August 5, 2021 3:12:33 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 3:40:07 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 4:00:03 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 4:50:18 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 5:28:03 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 5:55:30 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 5:56:47 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 6:05:57 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\customer experience improvement program\server\serverceipassistant
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 05:59:12" to "August 5, 2021 06:05:57" SHA-1 changed from "B16D5AEC3E0E7785A3280AD9E48A9F5C384C18F3" to "65FC92CE15EA6559D0D0114B2BC7E77FB4230DFA" After the change the File had the following attributes: Created: August 22, 2013 20:41:08 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 06:05:57 Owner: NT AUTHORITY\SYSTEM Permissions: D:ARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;SY) SHA-1: 65FC92CE15EA6559D0D0114B2BC7E77FB4230DFA Size: 4344

Time:	August 5, 2021 6:32:42 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 7:11:43 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 7:38:43 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 8:14:37 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 8:42:36 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 9:21:04 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 9:48:19 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 10:30:49 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 10:58:21 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 10:58:19" to "August 5, 2021 10:58:21" SHA-1 changed from "D33CDE62AFEFB2AE9634110ADF32FDC56BA6CF72" to "3AA812773DDA9D07A3CB7235A3A929B2E2013536" After the change the File had the following attributes: Created: August 22, 2013 20:40:20 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 10:58:21 Owner: NT AUTHORITY\SYSTEM Permissions: D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-80-123231216-2592883651-3715271367-3753151631-4175906628)(A;;FR;;;S-1-5-87-2912274048-3994893941-1669128114-1310430903-1263774323)(A;;FR;;;NS) SHA-1: 3AA812773DDA9D07A3CB7235A3A929B2E2013536 Size: 4680

Time:	August 5, 2021 11:26:42 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 11:35:01 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 12:01:06 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 12:44:42 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 1:11:20 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 1:45:53 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 2:12:33 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 2:56:56 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 3:24:40 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 3:58:00 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 4:26:59 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 5:00:22 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 5:27:14 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 6:05:08 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 6:32:34 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 7:15:34 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 7:42:35 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 8:18:22 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 8:46:01 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 9:02:41 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 9:37:59 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 10:11:24 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 10:37:59 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 11:00:26 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 11:47:56 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

172.20.0.20

Number of Changes:	58
Number of Objects Created:	3
Number of Objects Updated:	55
Number of Objects Deleted:	0
Number of Objects Renamed:	0

Number of Changes to Objects of Each Type

File	47
Service	8
User	3

Integrity Events

Time:	August 5, 2021 4:36:50 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 4:37:34 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\.net framework\.net framework ngen v4.0.30319 64
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 04:50:25" to "August 5, 2021 04:37:34" After the change the File had the following attributes: Created: August 22, 2013 20:41:27 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 04:37:34 Owner: NT AUTHORITY\SYSTEM Permissions: D:ARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FR;;;AU)(A;;0x1200a9;;;LS)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;SY) SHA-1: 5DC95C7FF58CAEBDEB93B0565F45D1CDC14904E6 Size: 3710

Time:	August 5, 2021 4:37:35 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\.net framework\.net framework ngen v4.0.30319
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 04:50:26" to "August 5, 2021 04:37:35" After the change the File had the following attributes: Created: August 22, 2013 20:41:11 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 04:37:35 Owner: NT AUTHORITY\SYSTEM Permissions: D:ARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FR;;;AU)(A;;0x1200a9;;;LS)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;SY) SHA-1: BB35B0877283D6D9335E1F9D8698992910899BCD Size: 3704

Time:	August 5, 2021 4:42:34 AM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 8:26:13 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\customer experience improvement program\server\serverceipassistant
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 08:18:43" to "August 5, 2021 08:26:13" SHA-1 changed from "F78914EE7062A830AFEEC9E3E9E18F0F6E26B9FA" to "5EEB4B3C5A43790EEC47DD248F73E3B19C063DA2" After the change the File had the following attributes: Created: August 22, 2013 20:41:08 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 08:26:13 Owner: NT AUTHORITY\SYSTEM Permissions: D:ARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;SY) SHA-1: 5EEB4B3C5A43790EEC47DD248F73E3B19C063DA2 Size: 4344

Time:	August 5, 2021 9:22:34 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask
Details:	When scanned the following changes were detected: Last Modified changed from "August 4, 2021 16:09:31" to "August 5, 2021 09:22:34" SHA-1 changed from "441F63A829E546DE801B025A034805134DBBB732" to "D06FF34B142BBC81BC4CD22BDC9B6477C86004DB" After the change the File had the following attributes: Created: August 22, 2013 20:40:20 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 09:22:34 Owner: NT AUTHORITY\SYSTEM Permissions: D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-80-123231216-2592883651-3715271367-3753151631-4175906628)(A;;FR;;;S-1-5-87-2912274048-3994893941-1669128114-1310430903-1263774323)(A;;FR;;;NS) SHA-1: D06FF34B142BBC81BC4CD22BDC9B6477C86004DB Size: 4680

Time:	August 5, 2021 9:26:59 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\optimize start menu cache files-s-1-5-21-1266428993-2899273040-1413466038-1175
Details:	When scanned the following changes were detected: Last Modified changed from "July 16, 2021 16:00:04" to "August 5, 2021 09:26:59" SHA-1 changed from "D71422692D6C3FD018BC5C3E36BDF37DE2E6A176" to "DB32D07DC2A79965857F5CACFDCF3D9B4966FE04" Size changed from "3600" to "3598" After the change the File had the following attributes: Created: November 22, 2019 18:15:07 Flags: 0 Group: ISMAILINDUSTRIE\Domain Users Last Modified: August 5, 2021 09:26:59 Owner: mhanif@ismailindustries.com Permissions: D:PARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FA;;;S-1-5-21-1266428993-2899273040-1413466038-1175)(A;;FR;;;S-1-5-21-1266428993-2899273040-1413466038-1175) SHA-1: DB32D07DC2A79965857F5CACFDCF3D9B4966FE04 Size: 3598

Time:	August 5, 2021 9:29:29 AM
Reason:	1008720 - Users and Groups - Create and Delete Activity (ATT&CK T1136)
Severity:	Medium
Change:	Created
Type:	User
Key:	anaeem
Details:	No description is available.

Time:	August 5, 2021 9:34:37 AM
Reason:	1008720 - Users and Groups - Create and Delete Activity (ATT&CK T1136)
Severity:	Medium
Change:	Created
Type:	User
Key:	ebintory
Details:	No description is available.

Time:	August 5, 2021 9:51:34 AM
Reason:	1008720 - Users and Groups - Create and Delete Activity (ATT&CK T1136)
Severity:	Medium
Change:	Created
Type:	User
Key:	ahsheraz
Details:	No description is available.

Time:	August 5, 2021 10:01:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "July 25, 2021 19:19:24" to "August 5, 2021 10:01:20" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:01:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 10:01:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "July 25, 2021 19:19:24" to "August 5, 2021 10:01:20" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:01:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA)

Size: 4992

Time:	August 5, 2021 10:01:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "July 25, 2021 19:19:24" to "August 5, 2021 10:01:20" SHA-1 changed from "CAE846C9C0D3BAFD5141CA58FAB0A4F6A382F805" to "B916F9356EB53BFF17C1934BE05E917C7DAE30C9" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:01:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 10:01:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "July 25, 2021 19:19:25" to "August 5, 2021 10:01:20" SHA-1 changed from "C3956A7B45ADEF8128A08B042559BAB4A6BED4F9" to "5C692D08906EDCB66A03F74184DF4241BB5B0745" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:01:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 10:15:01 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:01:20" to "August 5, 2021 10:15:01" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:15:01 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 10:15:01 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:01:20" to "August 5, 2021 10:15:01" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:15:01 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 10:15:01 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:01:20" to "August 5, 2021 10:15:01" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:15:01 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 10:15:01 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:01:20" to "August 5, 2021 10:15:01" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:15:01 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 10:25:04 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:15:01" to "August 5, 2021 10:25:04" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:25:04 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 10:25:04 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:15:01" to "August 5, 2021 10:25:04" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:25:04 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 10:25:04 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:15:01" to "August 5, 2021 10:25:04" After the change the File had the following attributes: SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902 Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:25:04 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA)

Time:	August 5, 2021 10:25:04 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:15:01" to "August 5, 2021 10:25:04" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:25:04 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 10:35:08 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:25:04" to "August 5, 2021 10:35:08" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:35:08 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 10:35:08 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:25:04" to "August 5, 2021 10:35:08" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:35:08 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 10:35:08 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:25:04" to "August 5, 2021 10:35:08" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:35:08 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 10:35:08 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:25:04" to "August 5, 2021 10:35:08" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:35:08 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 10:45:11 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:35:08" to "August 5, 2021 10:45:11" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:45:11 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 10:45:11 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:35:08" to "August 5, 2021 10:45:11" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:45:11 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 10:45:11 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:35:08" to "August 5, 2021 10:45:11" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:45:11 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 10:45:11 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:35:08" to "August 5, 2021 10:45:11" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 10:45:11 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 11:00:13 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:45:11" to "August 5, 2021 11:00:13" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:00:13 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 11:00:13 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:45:11" to "August 5, 2021 11:00:13" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:00:13 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 11:00:13 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:45:11" to "August 5, 2021 11:00:13" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:00:13 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 11:00:13 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 10:45:11" to "August 5, 2021 11:00:13" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:00:13 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 11:10:17 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:00:13" to "August 5, 2021 11:10:17" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:10:17 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 11:10:17 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:00:13" to "August 5, 2021 11:10:17" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:10:17 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 11:10:17 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:00:13" to "August 5, 2021 11:10:17" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:10:17 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 11:10:17 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:00:13" to "August 5, 2021 11:10:17" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:10:17 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 11:20:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:10:17" to "August 5, 2021 11:20:20" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:20:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 11:20:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:10:17" to "August 5, 2021 11:20:20" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:20:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 11:20:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:10:17" to "August 5, 2021 11:20:20" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:20:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 11:20:20 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:10:17" to "August 5, 2021 11:20:20" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:20:20 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 11:35:23 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\auscheduledinstall
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:20:20" to "August 5, 2021 11:35:23" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:35:23 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 8886DF71ECB07321E77E8FB8BA82CCD9C97D9EC6 Size: 3392

Time:	August 5, 2021 11:35:23 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\ausessionconnect
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:20:20" to "August 5, 2021 11:35:23" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:35:23 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 4A74ECE002DFD2B69C9ED183A7DCA19F06AF244F Size: 4992

Time:	August 5, 2021 11:35:23 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start with network
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:20:20" to "August 5, 2021 11:35:23" After the change the File had the following attributes: Created: September 15, 2017 17:02:00 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:35:23 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: B916F9356EB53BFF17C1934BE05E917C7DAE30C9 Size: 4902

Time:	August 5, 2021 11:35:23 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\windowsupdate\scheduled start
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:20:20" to "August 5, 2021 11:35:23" After the change the File had the following attributes: Created: August 22, 2013 20:40:14 Flags: 0 Group: S-1-5-21-1903268029-2347705814-775326603-513 Last Modified: August 5, 2021 11:35:23 Owner: BUILTIN\Administrators Permissions: D:ARAI(A;;FA;;;SY)(A;;0x1200a9;;;LS)(A;;FA;;;BA)(A;;FR;;;SY)(A;ID;0x1f019f;;;BA)(A;ID;0x1f019f;;;SY)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)(A;ID;FA;;;BA) SHA-1: 5C692D08906EDCB66A03F74184DF4241BB5B0745 Size: 4904

Time:	August 5, 2021 11:53:58 AM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 09:22:34" to "August 5, 2021 11:53:58" SHA-1 changed from "D06FF34B142BBC81BC4CD22BDC9B6477C86004DB" to "236B999CF29DA99217A9A3AC24B2AEF22064B5D5" After the change the File had the following attributes: Created: August 22, 2013 20:40:20 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 11:53:58 Owner: NT AUTHORITY\SYSTEM Permissions: D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-80-123231216-2592883651-3715271367-3753151631-4175906628)(A;;FR;;;S-1-5-87-2912274048-3994893941-1669128114-1310430903-1263774323)(A;;FR;;;NS) SHA-1: 236B999CF29DA99217A9A3AC24B2AEF22064B5D5 Size: 4680

Time:	August 5, 2021 12:14:04 PM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 11:53:58" to "August 5, 2021 12:14:04" SHA-1 changed from "236B999CF29DA99217A9A3AC24B2AEF22064B5D5" to "17659C308626FE62F47C86330D953CA7FB296918" After the change the File had the following attributes: Created: August 22, 2013 20:40:20 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 12:14:04 Owner: NT AUTHORITY\SYSTEM Permissions: D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-80-123231216-2592883651-3715271367-3753151631-4175906628)(A;;FR;;;S-1-5-87-2912274048-3994893941-1669128114-1310430903-1263774323)(A;;FR;;;NS) SHA-1: 17659C308626FE62F47C86330D953CA7FB296918 Size: 4680

Time:	August 5, 2021 2:03:43 PM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 12:14:04" to "August 5, 2021 14:03:43" SHA-1 changed from "17659C308626FE62F47C86330D953CA7FB296918" to "67F0F8DEF9F74849DB6678328B5B495AA0B54C83" After the change the File had the following attributes: Created: August 22, 2013 20:40:20 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 14:03:43 Owner: NT AUTHORITY\SYSTEM Permissions: D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-80-123231216-2592883651-3715271367-3753151631-4175906628)(A;;FR;;;S-1-5-87-2912274048-3994893941-1669128114-1310430903-1263774323)(A;;FR;;;NS) SHA-1: 67F0F8DEF9F74849DB6678328B5B495AA0B54C83 Size: 4680

Time:	August 5, 2021 2:07:21 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	RemoteRegistry
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k localService dependsOn: RPCSS firstFailure: 60000,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400 secondFailure: 60000,Restart startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 2:08:13 PM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\optimize start menu cache files-s-1-5-21-1266428993-2899273040-1413466038-1175
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 09:26:59" to "August 5, 2021 14:08:13" After the change the File had the following attributes: Created: November 22, 2019 18:15:07 Flags: 0 Group: ISMAILINDUSTRIE\Domain Users Last Modified: August 5, 2021 14:08:13 Owner: mhanif@ismailindustries.com Permissions: D:PARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FA;;;S-1-5-21-1266428993-2899273040-1413466038-1175)(A;;FR;;;S-1-5-21-1266428993-2899273040-1413466038-1175) SHA-1: DB32D07DC2A79965857F5CACFDCF3D9B4966FE04 Size: 3598

Time:	August 5, 2021 2:19:06 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	RemoteRegistry
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k localService dependsOn: RPCSS firstFailure: 60000,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400 secondFailure: 60000,Restart startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 3:17:50 PM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\microsoft\windows\softwareprotectionplatform\svcrestarttask
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 14:03:43" to "August 5, 2021 15:17:50" SHA-1 changed from "67F0F8DEF9F74849DB6678328B5B495AA0B54C83" to "455D481BC35359850BFE57BC5D185AAED34D85C9" After the change the File had the following attributes: Created: August 22, 2013 20:40:20 Flags: 0 Group: NT AUTHORITY\SYSTEM Last Modified: August 5, 2021 15:17:50 Owner: NT AUTHORITY\SYSTEM Permissions: D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FA;;;S-1-5-80-123231216-2592883651-3715271367-3753151631-4175906628)(A;;FR;;;S-1-5-87-2912274048-3994893941-1669128114-1310430903-1263774323)(A;;FR;;;NS) SHA-1: 455D481BC35359850BFE57BC5D185AAED34D85C9 Size: 4680

Time:	August 5, 2021 3:22:19 PM
Reason:	1006076 - Task Scheduler Entries Modified (ATT&CK T1168)
Severity:	Medium
Change:	Updated
Type:	File
Key:	c:\windows\system32\tasks\optimize start menu cache files-s-1-5-21-1266428993-2899273040-1413466038-1175
Details:	When scanned the following changes were detected: Last Modified changed from "August 5, 2021 14:08:13" to "August 5, 2021 15:22:19" After the change the File had the following attributes: Created: November 22, 2019 18:15:07 Flags: 0 Group: ISMAILINDUSTRIE\Domain Users Last Modified: August 5, 2021 15:22:19 Owner: mhanif@ismailindustries.com Permissions: D:PARAI(A;;FA;;;BA)(A;;FA;;;SY)(A;;FA;;;S-1-5-21-1266428993-2899273040-1413466038-1175)(A;;FR;;;S-1-5-21-1266428993-2899273040-1413466038-1175) SHA-1: DB32D07DC2A79965857F5CACFDCF3D9B4966FE04 Size: 3598

Time:	August 5, 2021 6:59:16 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	RemoteRegistry
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k localService dependsOn: RPCSS firstFailure: 60000,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400 secondFailure: 60000,Restart startType: manual state: running subsequentFailures: 0,None

Time:	August 5, 2021 7:10:47 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	RemoteRegistry
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k localService dependsOn: RPCSS firstFailure: 60000,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400 secondFailure: 60000,Restart startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 8:15:07 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "running" to "stopped" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: stopped subsequentFailures: 0,None

Time:	August 5, 2021 8:21:00 PM
Reason:	1002781 - Microsoft Windows - Attributes of a service modified (ATT&CK T1050, T1036, T1031)
Severity:	Medium
Change:	Updated
Type:	Service
Key:	WinHttpAutoProxySvc
Details:	When scanned the following changes were detected: state changed from "stopped" to "running" After the change the Service had the following attributes: binaryPathName: C:\Windows\system32\svchost.exe -k LocalService dependsOn: Dhcp firstFailure: 0,Restart Group: NT AUTHORITY\SYSTEM logOnAs: NT AUTHORITY\LocalService Owner: NT AUTHORITY\SYSTEM Permissions: D:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWRPLOCRRC;;;AU)(A;;CCLCSWRPLOCRRC;;;IU)(A;;CCLCSWRPLOCRRC;;;SU)(A;;LCRPLO;;;AC)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) resetFailCountAfter: 86400000 secondFailure: 0,None startType: manual state: running subsequentFailures: 0,None

172.20.0.30

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

192.168.10.220

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

192.168.80.2

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

192.168.90.10

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

192.168.90.11

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0

192.168.90.12

Number of Changes:	0
Number of Objects Created:	0
Number of Objects Updated:	0
Number of Objects Deleted:	0
Number of Objects Renamed:	0