How to Use Trend Micro Vision One™ to Search for Potential Threats Associated With 3CX Desktop App

By Cihan Ayana, *Incident Response Engineer, Americas IR Team*

There is an ongoing supply chain attack risk linked to the video conferencing software 3CX Desktop App.

Trend Micro customers can benefit from Vision One for finding the affected computers, understanding the attack vector and search for the threat using the Search Application, Workbench, and Observed Attack Techniques.

Threat Hunting via Search App

Using the "Search App" in Vision One, our customers can find the 3CX exploit detections and observe that the malicious files are blocked by Trend Micro agent Real-time Scan feature. In this specific attack, the malicious binaries are detected as "Trojan.Win64.DEEFFACE.A" and this detection name can be used as a keyword while performing threat hunting in the environment. And then, it can also be observed that the files are cleaned, quarantined, or deleted successfully based on the policy configurations.

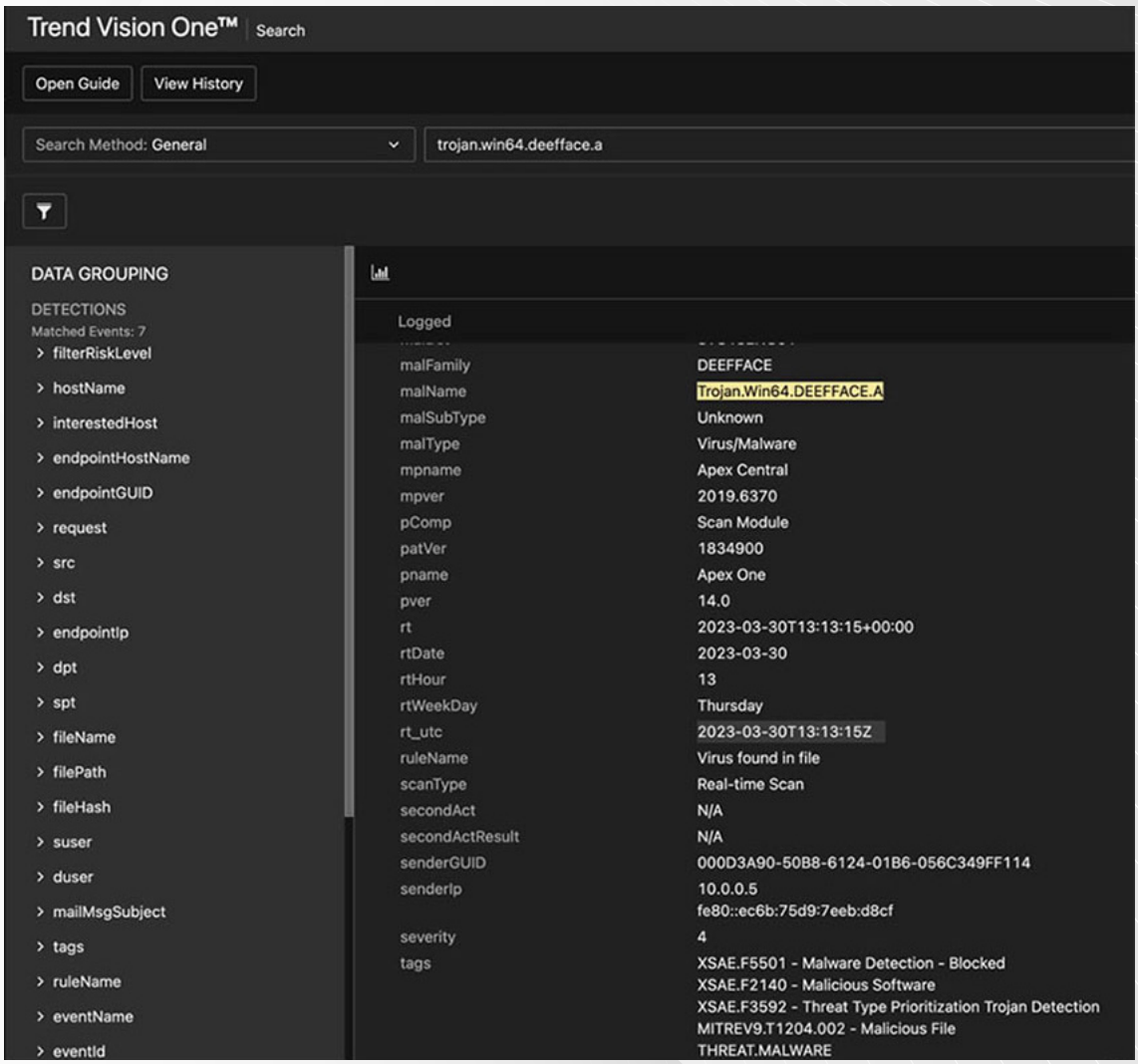

Figure 1. Screenshot displaying the malicious file on Vision One Search App.

Trend Micro customers can also utilize Vision One Search App for defining the scope of the affected machines. This can be achieved by adding the endpointHostName as a column in the “Trojan.Win64.DEEFFACE.A” search results and it will automatically list the affected machines.

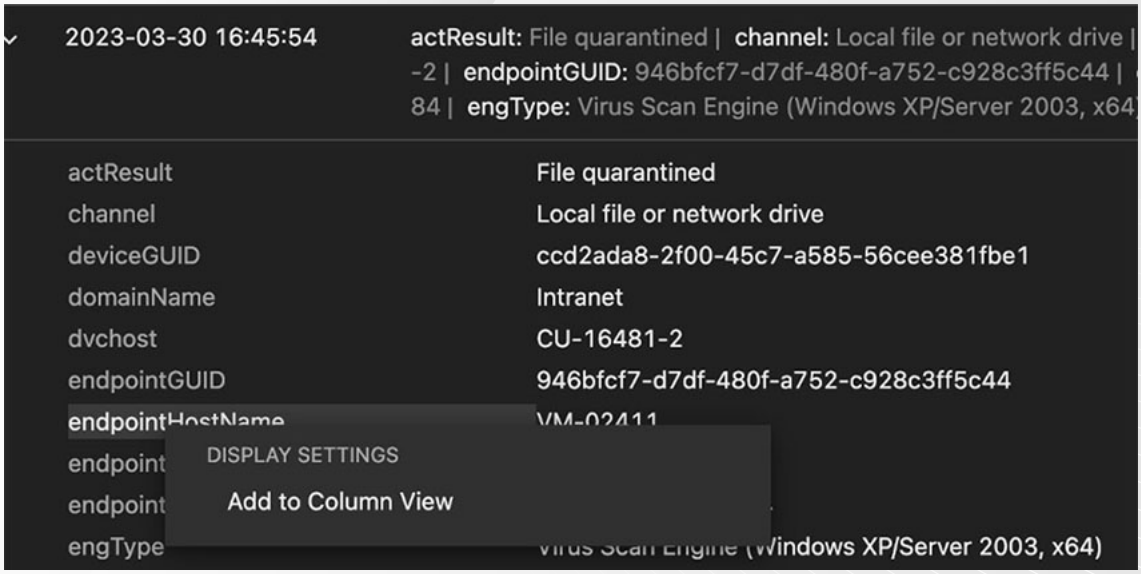

Figure 2. Screenshot displaying listing the affected machines by adding the host name as a column.

For more search keywords, see the “Search Keywords and Commands” section.

Vision One also creates execution profiles for these detections.

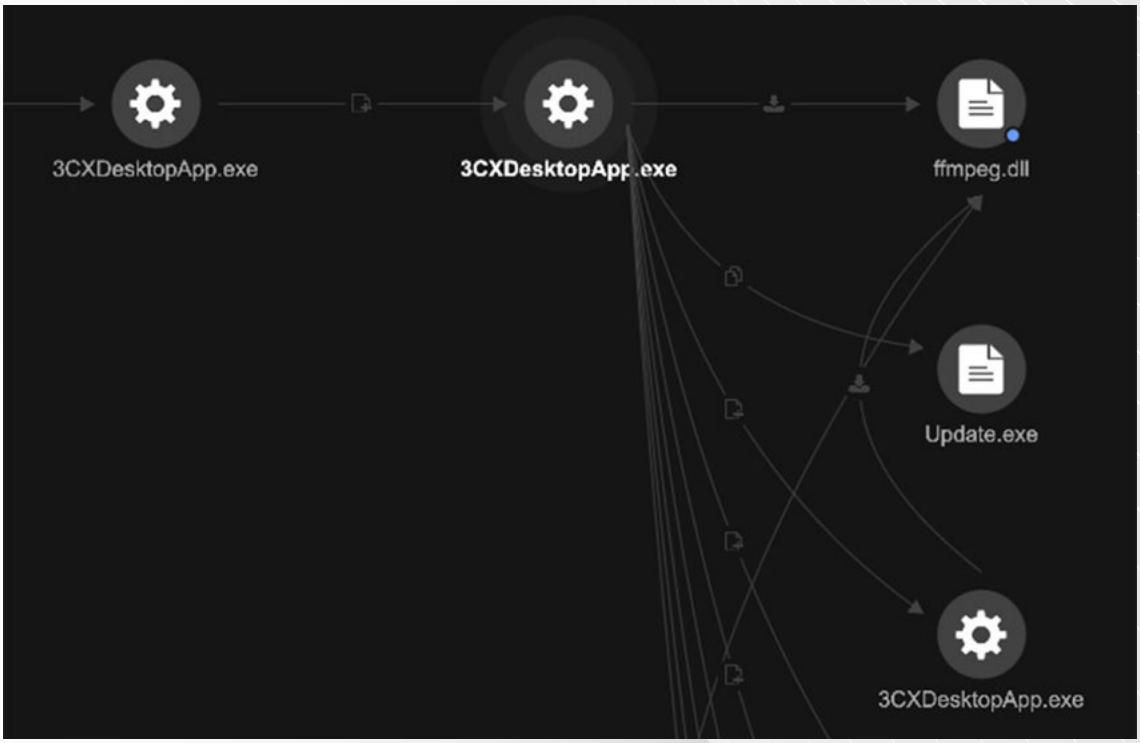

Figure 3. Screenshot displaying the execution profile for the 3CXDesktopApp.exe.

Search Keywords and Commands

- In the search bar, our customers can use either the keywords shared below or use threat hunting commands.

Keywords

- Trojan.Win64.DEEFFACE.A
- *malware.950fa7b1*
- *raw.githubusercontent.com/IconStorages*
- All Indicators of Compromise (IoC) published on Preventing and Detecting Attacks Involving 3CX Desktop App

Commands

Windows

- 3CXDesktopApp.msi - Trojan.Win64.DEEFFACE.A
  - FileSHA1:(bea77d1e59cf18dce22ad9a2fad52948fd7a9efa OR bfecb8ce89a312d2ef4af-c64a63847ae11c6f69e)
- 3CXDesktopApp.exe - Trojan.Win64.DEEFFACE.A
  - FileSHA1:(8433a94aedb6380ac8d4610af643fb0e5220c5cb OR 6285ffb5f98d35cd98e78d-48b63a05af6e4e4dea)
- ffmpeg.dll - Trojan.Win64.DEEFFACE.A
  - FileSHA1:(188754814b37927badc988b45b7c7f7d6b4c8dd3 OR bf939c9c261d27ee7bb92325c-c588624fca75429 OR ff3dd457c0d00d00d396fdf6ebe7c254fed2a91e)
- d3dcompiler_47.dll - Trojan.Win64.DEEFFACE.A
  - FileSHA1:(20d554a80d759c50d6537dd7097fed84dd258b3e)
- ico files - Trojan.Win32.DEEFFACE.ICO
  - FileSHA1:(“9c943baad621654cc0a0495262b6175276a0a9fb” OR “96910a3dbc194a7b-f9a452afe8a35eceb904b6e4” OR “0d890267ec8d6d2aaf43eaca727c1fbba6ac-d16e” OR “0d890267ec8d6d2aaf43eaca727c1fbba6acd16e” OR “b1dee3ebcffad01a51f-f31ff495fef1d40fdfaa0” OR “64ab912d0af35c01355430d85dd4181f25e88838” OR “8377fb-40c76aa3ba3efae3d284fa51aa7748e010” OR “11ae67704ea0b930b2cc966e6d07f8b-898f1a7d2” OR “ffccc3a29d1582989430e9b6c6d2bff1e3a3bb14” OR “89827af650640c-7042077be64dc643230d1f7482” OR “b5de30a83084d6f27d902b96dd12e15c77d-1f90b” OR “3992dbe9e0b23e0d4ca487faffeb004bcfe9ecc8” OR “caa77bcd0a1a6629ba1f3ce8d-1fc5451d83d0352” OR “57a9f3d5d1592a0769886493f566930d8f32a0fc” OR “f533bea1c0558f-73f6a3930343c16945fb75b20f” OR “31d775ab577f3cc88991d90e9ae58501dbe1f0da”)
- S0 stealer
  - FileSHA1:(“cad1120d91b812acafef7175f949dd1b09c6c21a”)
- Stealer - TrojanSpy.Win64.ICONICSTEALER.THCCABC
  - FileSHA1:(“3b3e778b647371262120a523eb873c20bb82beaf”)

Mac

- Mac Installer - Trojan.MacOS.FAKE3L3CTRON.A
  - FileSHA1:(19f4036f5cd91c5fc411afc4359e32f90caddaac)
- libffmpeg.dylib - Trojan.MacOS.FAKE3L3CTRON.A / Trojan.MacOS.SAMSCISSORS.0NA103CV23
  - FileSHA1:(769383fc65d1386dd141c960c9970114547da0c2 OR b2a89eebb5be-61939f5458a024c929b169b4dc85)
- child macho file of libffmpeg.dylib Trojan.MacOS.FAKE3L3CTRON.A / Trojan.MacOS.SAMSCIS-SORS.0NA103CV23
  - FileSHA1:(354251ca9476549c391fbd5b87e81a21a95949f4 OR 5b0582632975d230c8f73c768b9ef-39669fefa60)

Network

- Connections to GitHub from the Compromised Executable
  - CLICommand:(3cxDesktopApp.exe) AND ("*raw.githubusercontent.com//IconStorages*")
- Connections to Malicious Domains from the Compromised Executable
  - CLICommand:(3cxDesktopApp.exe) AND ("akamaicontainer.com" OR "akamaitechcloudser-vices.com" OR "azuredeploystore.com" OR "azureonlinecloud.com" OR "azureonlinestorage.com" OR "dunamistrd.com" OR "glcloudservice.com" OR "journalide.org" OR "msedgepackage-info.com" OR "msstorageazure.com" OR "msstorageboxes.com" OR "officeaddons.com" OR "of-ficestoragebox.com" OR "pbxcloudeservices.com" OR "pbxphonenetwork.com" OR "pbxsources.com" OR "qwepoi123098.com" OR "sbmsa.wiki" OR "sourceslabs.com" OR "visualstudiofactory.com" OR "zacharryblogs.com")
- Outbound Connections to Malicious Domains (Select Endpoint Activity Data in the Search Method)
  - eventSubId:(203 OR 204 OR 301 OR 602 OR 603) AND ("akamaicontainer.com" OR "akamait-echcloudservices.com" OR "azuredeploystore.com" OR "azureonlinecloud.com" OR "azureon-linestorage.com" OR "dunamistrd.com" OR "glcloudservice.com" OR "journalide.org" OR "msedge-packageinfo.com" OR "msstorageazure.com" OR "msstorageboxes.com" OR "officeaddons.com" OR "officestoragebox.com" OR "pbxcloudeservices.com" OR "pbxphonenetwork.com" OR "pbxsources.com" OR "qwepoi123098.com" OR "sbmsa.wiki" OR "sourceslabs.com" OR "visualstudiofactory.com" OR "zacharryblogs.com")
- Connections to Malicious IPs (Select Endpoint Activity Data in the Search Method)
  - eventSubId:(203 OR 204 OR 301 OR 602 OR 603) AND ("198.54.114.192" OR "198.54.125.101" OR "185.38.151.11" OR "91.235.116.231" OR "199.188.206.6" OR "198.54.116.74" OR "89.45.67.160" OR "91.235.116.231" OR "198.54.115.118" OR "162.213.255.24" OR "45.141.152.19" OR "185.244.151.84" OR "199.33.112.228" OR "199.33.112.228" OR "198.54.115.59" OR "162.213.255.22" OR "162.213.255.23" OR "104.194.215.229" OR "162.213.255.24" OR "172.93.201.88" OR "198.54.115.169" OR "162.0.229.159")

Monitoring

In addition to the threat hunting efforts, Trend Micro customers can use both the Workbench and Observed Attack Techniques (OAT) for monitoring their environments.

Workbench

Vision One automatically creates workbenches for the malicious 3CX application activities. As an example, a workbench was created with the name “Cybercrime Malware Mitigation” for the Trojan Win64.DEEFFACE.A binary detection. To find more relevant results in a quicker manner, Trend Micro customers can choose the “Cybercrime Malware Mitigation” rule to filter the workbenches.

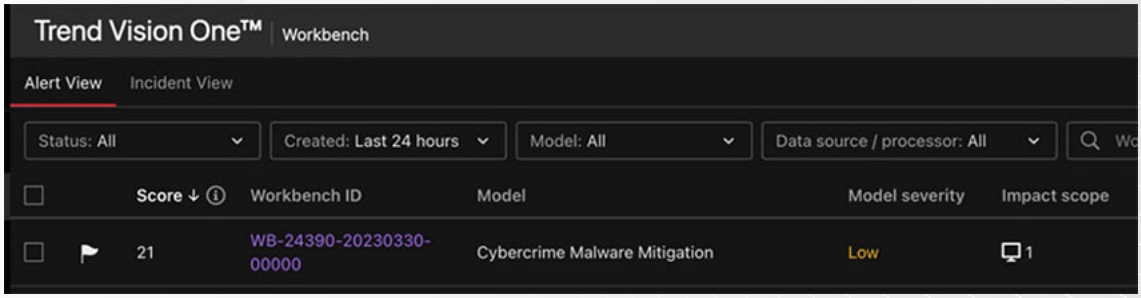

Figure 4. Workbench “Cybercrime Malware Mitigation” created for the Trojan Win64.DEEFFACE.A.

The workbench elaborates the threat information with a relational graph and includes details regarding the file name, scan type, event date and time, and the risk score.

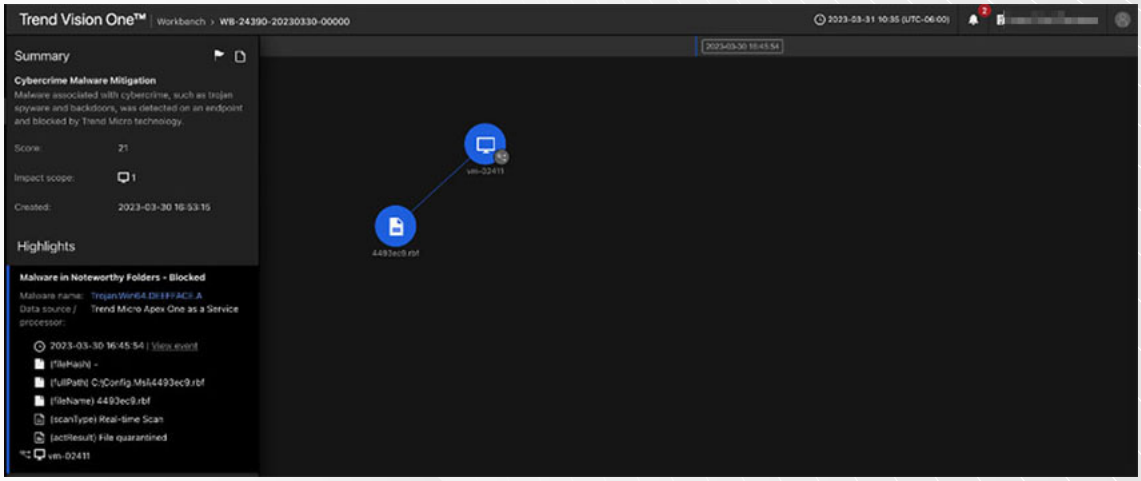

Figure 5. Workbench created for the Trojan Win64.DEEFFACE.A.

Observed Attack Techniques

Like the workbenches, the malicious activities can be observed in the “Observed Attack Techniques” created for this specific attack. As seen in this example, the malicious file was quarantined, and the attack was stopped immediately in real-time.

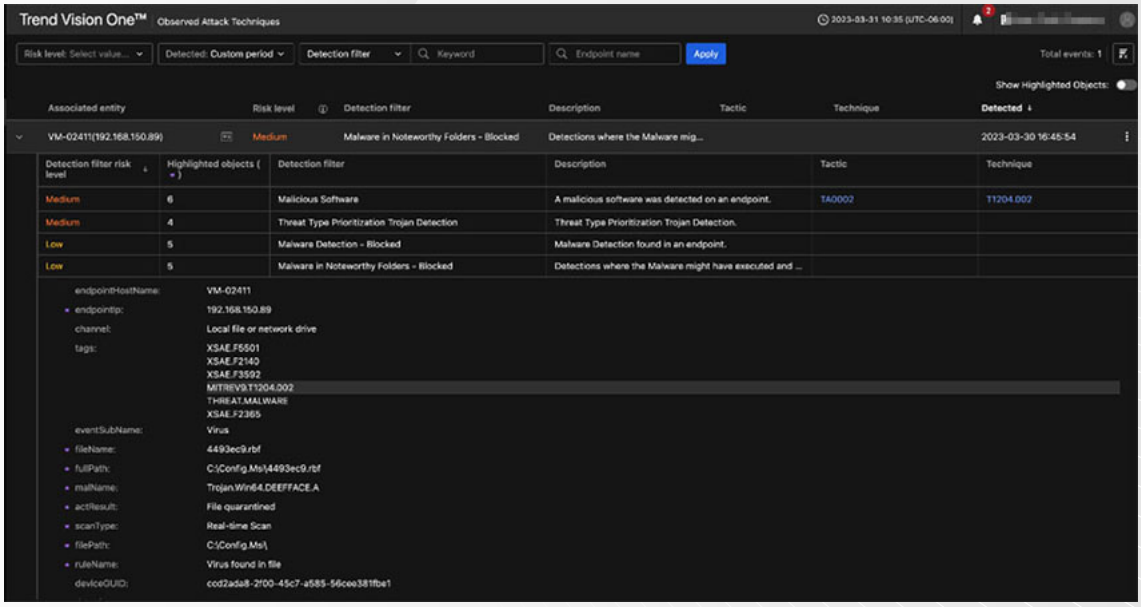

Figure 6. Observed Attack Techniques.

Trend Micro Vision One provides a high visibility in this attack. Using the above-mentioned threat hunting techniques, companies can perform further investigations, define the scope, and mitigate the risk for this supply chain attack campaign. Trend Micro will update the artifacts seen in this attack and it’s highly recommended for our customers to configure their product policies based on the Trend Micro Best Practice Policy documents. It’s also recommended monitoring and performing threat hunting in their networks using advanced Vision One capabilities.