Reddit - Dive into anything

reddit.com/r/crowdstrike/comments/125r3uu/20230329_situational_awareness_crowdstrike/

Go to crowdstrike
r/crowdstrike
r/crowdstrike
Welcome to the CrowdStrike subreddit. CrowdStrike Falcon offers cloud-delivered solutions across endpoints, cloud workloads, identity and data; providing responders remote visibility across the enterprise and enabling instant access to the "who, what, when, where, and how" of a cyber attack.

Members Online

by Andrew-CS

•

// 2023-03-29 // SITUATIONAL AWARENESS // CrowdStrike Tracking Active Intrusion Campaign Targeting 3CX Customers //

What Happened

On March 29, 2023, Falcon OverWatch observed unexpected malicious activity emanating from a legitimate, signed binary, 3CXDesktopApp — a softphone application from 3CX. The malicious activity includes beaconing to actor-controlled infrastructure, deployment of second-stage payloads, and, in a small number of cases, hands-on-keyboard activity.

Falcon Prevent and Insight have behavioral preventions and atomic detections targeting the abuse of 3CXDesktopApp. OverWatch has notified customers where hands-on-keyboard activity has been observed and Falcon Complete is in contact with customers under their management where 3CXDesktopApp is present.

The 3CXDesktopApp is available for Windows, macOS, Linux, and mobile. At time of writing, activity has been observed on both Windows and macOS.

This is a dynamic situation and updates will be provided here as they become available. CrowdStrike's Intelligence Team is in contact with 3CX. There is suspected nation-state involvement by the threat actor LABYRINTH CHOLLIMA.

Detection and Prevention

Falcon has coverage utilizing behavior-based indicators of attack (IOAs) targeting malicious behaviors associated with 3CX on both MacOS and Windows. Please ensure that your prevention policies are properly configured with "Suspicious Processes" enabled.

Hunting

Falcon Discover

Falcon Discover customers can use the following link: US-1 | US-2 | EU | Gov to look for the presence of 3CXDesktopApp in their environment.

Falcon Spotlight

Falcon Spotlight customers can search for `CVE-2023-3CX` to identify vulnerable versions of 3CX software. Spotlight will automatically highlight this vulnerability in your vulnerability feed.

Falcon Insight - Application Search

Falcon Insight customers can assess if the 3CXDesktopApp is running in their environment with the following query:

Falcon LTR - Application Search

```
#event_simpleName=/^(PeVersionInfo|ProcessRollup2)$/ AND (event_platform=Win
ImageFileName=/\\3CXDesktopApp\.exe$/i) OR (event_platform=Mac
ImageFileName=/\/3CX\sDesktop\sApp/i)
| ImageFileName = /.+(\\|\/)(?<FileName>.+)$/i
| groupBy([event_platform, FileName, SHA256HashData], function=count(aid,
distinct=true, as=endpointCount))
```

Event Search - Application Search

```
event_simpleName IN (PeVersionInfo, ProcessRollup2) FileName IN ("3CXDesktopApp.exe",
"3CX Desktop App")
| stats dc(aid) as endpointCount by event_platform, FileName, SHA256HashData
```

Atomic Indicators

The following domains have been observed beaconing which should be considered an indication of malicious intent.

```
akamaicontainer[.]com
akamaitechcloudservices[.]com
azuredeploystore[.]com
azureonlinecloud[.]com
azureonlinestorage[.]com
dunamistrd[.]com
glcloudservice[.]com
journalide[.]org
msedgepackageinfo[.]com
msstorageazure[.]com
msstorageboxes[.]com
officeaddons[.]com
officestoragebox[.]com
pbxcloudeservices[.]com
pbxphonenetwork[.]com
pbxsources[.]com
qwepoi123098[.]com
sbmsa[.]wiki
sourceslabs[.]com
visualstudiofactory[.]com
zacharryblogs[.]com
```

Indicator Graph

Falcon Insight customers, regardless of retention period, can search for the presence of these domains in their environment spanning back one year using Indicator Graph: US-1 | US-2 | EU | Gov.

Falcon Insight - Domain Search

Falcon Insight customers can search for presence of these domains using the following queries.

Falcon LTR - Domain Search

```
#event_simpleName=DnsRequest
| in(DomainName, values=[akamaicontainer.com, akamaitechcloudservices.com,
azuredeploystore.com, azureonlinecloud.com, azureonlinestorage.com, dunamistrd.com,
glcloudservice.com, journalide.org, msedgepackageinfo.com, msstorageazure.com,
msstorageboxes.com, officeaddons.com, officestoragebox.com, pbxcloudeservices.com,
pbxphonenetwork.com, pbxsources.com, qwepoi123098.com, sbmsa.wiki, sourceslabs.com,
visualstudiofactory.com, zacharryblogs.com])
| groupBy([DomainName], function=([count(aid, distinct=true, as=endpointCount),
min(ContextTimeStamp, as=firstSeen), max(ContextTimeStamp, as=lastSeen)]))
| firstSeen := firstSeen * 1000 | formatTime(format="%F %T.%L", field=firstSeen,
as="firstSeen")
| lastSeen := lastSeen * 1000 | formatTime(format="%F %T.%L", field=lastSeen,
as="lastSeen")
| sort(endpointCount, order=desc)
```

Event Search - Domain Search

```
event_simpleName=DnsRequest DomainName IN (akamaicontainer.com,
akamaitechcloudservices.com, azuredeploystore.com, azureonlinecloud.com,
azureonlinestorage.com, dunamistrd.com, glcloudservice.com, journalide.org,
msedgepackageinfo.com, msstorageazure.com, msstorageboxes.com, officeaddons.com,
officestoragebox.com, pbxcloudeservices.com, pbxphonenetwork.com, pbxsources.com,
qwepoi123098.com, sbmsa.wiki, sourceslabs.com, visualstudiofactory.com,
zacharryblogs.com)
| stats dc(aid) as endpointCount, earliest(ContextTimeStamp_decimal) as firstSeen,
latest(ContextTimeStamp_decimal) as lastSeen by DomainName
| convert ctime(firstSeen) ctime(lastSeen)
```

File Details

SHA256	Operating System
dde0334807551279624 1389dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc	Windows
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405	Windows
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61	macOS
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb	macOS

Recommendations

The current recommendation for all CrowdStrike customers is:

1. Locate the presence of 3CXDesktopApp software in your environment by using the queries outlined above.
2. Ensure Falcon is deployed to applicable systems.
3. Ensure “Suspicious Processes” is enabled in applicable Prevention Policies.
4. Hunt for historical presence of atomic indicators in third-party tooling (if available).

Helpful Links

- Find answers and contact Support with our Support Portal
- Specific Tech Alert
- CSA-230489 LABYRINTH CHOLLIMA Suspected of Conducting Supply Chain Attack with 3CX Application: (US-1 | US-2 | EU | GOV) [Intelligence subscription required]

- LABYRINTH CHOLLIMA battle card (US-1 | US-2 | EU | GOV)

Conclusion

Again, this situation is dynamic and we will continue to provide updates as they become available.

**** UPDATE 2023-03-29 20:35 ET ****

After review and reverse engineering by the CrowdStrike Intelligence Team, the signed MSI (`aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868`) is malicious. The MSI will drop three files, with the primary fulcrum being the compromised binary `ffmpeg.dll` (`7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896`). Once active, the HTTPS beacon structure and encryption key match those observed by CrowdStrike in a March 7, 2023 campaign attributed with high confidence to DPRK-nexus threat actor LABYRINTH CHOLLIMA. CrowdStrike Intelligence customers can view the following reports for full technical details:

- CSA-230387: LABYRINTH CHOLLIMA Uses TxRLoader and Vulnerable Drivers to Target Financial and Energy Sectors (US-1 | US-2 | EU | GOV)
- CSA-230489: LABYRINTH CHOLLIMA Suspected of Conducting Supply Chain Attack with 3CX Application (US-1 | US-2 | EU | GOV)
- CSA-230494: ArcfeedLoader Malware Used in Supply Chain Attack Leveraging Trojanized 3CX Installers Confirms Attribution to LABYRINTH CHOLLIMA (US-1 | US-2 | EU | GOV)

At this point, my recommendation would be to remove 3CX software from endpoints until advised by the vendor that future installers and builds are safe.

**** UPDATE 2023-03-30 08:45 ET ****

- For those looking for additional details on macOS, Patrick Wardle has a great thread on Twitter where he reverse engineers a 3CX binary (Twitter link). There is also an associated blog post.
- Side note: thanks to all those sharing and crowdsourcing details below. This post has gotten quite a bit of attention and there are quite a few *non-regulars* posting and lurking. It's nice to see everyone stepping up to help one another.