CrowdStrike Falcon Platform Detects and Prevents Active Intrusion Campaign Targeting 3CXDesktopApp Customers

CrowdStrike ⋮ 3/29/2023

Note: Content from this post first appeared in r/CrowdStrike

3/31 UPDATE

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.

All Falcon customers can view our actor profile on LABYRINTH CHOLLIMA (US-1 | US-2 | EU-1 | US-GOV-1)

CrowdStrike Intelligence Premium subscribers 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-1 | US-GOV-1)
- CSA-230489: LABYRINTH CHOLLIMA Suspected of Conducting Supply Chain Attack with 3CX Application (US-1 | US-2 | U-1 | US-GOV-1)
- CSA-230494: ArcfeedLoader Malware Used in Supply Chain Attack Leveraging Trojanized 3CX Installers Confirms Attribution to LABYRINTH CHOLLIMA (US-1 | US-2 | U-1 | US-GOV-1)

CrowdStrike recommends removing the 3CX software from endpoints until advised by the vendor that future installers and builds are safe.

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.

Original Post

On March 29, 2023, CrowdStrike 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.

The CrowdStrike Falcon® platform has behavioral preventions and atomic indicator detections targeting the abuse of 3CXDesktopApp. In addition, CrowdStrike® Falcon OverWatch™ helps customers stay vigilant against hands-on-

keyboard activity.

CrowdStrike customers can log into the customer support portal and follow the latest updates in Trending Threats & Vulnerabilities: Intrusion Campaign Targeting 3CX Customers

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

CrowdStrike Intelligence has assessed there is suspected nation-state involvement by the threat actor LABYRINTH CHOLLIMA. CrowdStrike Intelligence customers received an alert this morning on this active intrusion.

Get fast and easy protection with built-in threat intelligence — request a free trial of CrowdStrike Falcon® Pro today.

CrowdStrike Falcon Detection and Protection

Watch how the CrowdStrike Falcon platform detects and prevents an active intrusion campaign targeting 3CXDesktopApp users.

The CrowdStrike Falcon platform protects customers from this attack and has coverage utilizing behavior-based indicators of attack (IOAs) and indicators of compromise (IOCs) based detections targeting malicious behaviors associated with 3CX on both macOS and Windows.

Customers should ensure that prevention policies are properly configured with Suspicious Processes enabled.
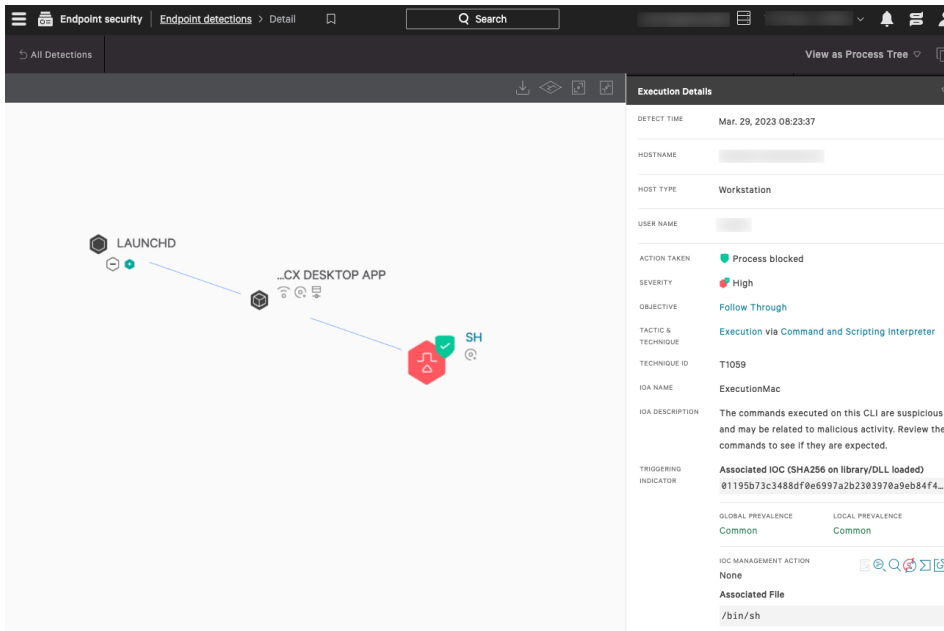
Figure 1. CrowdStrike's indicator of attack (IOA) identifies and blocks the malicious behavior in macOS (click to enlarge)
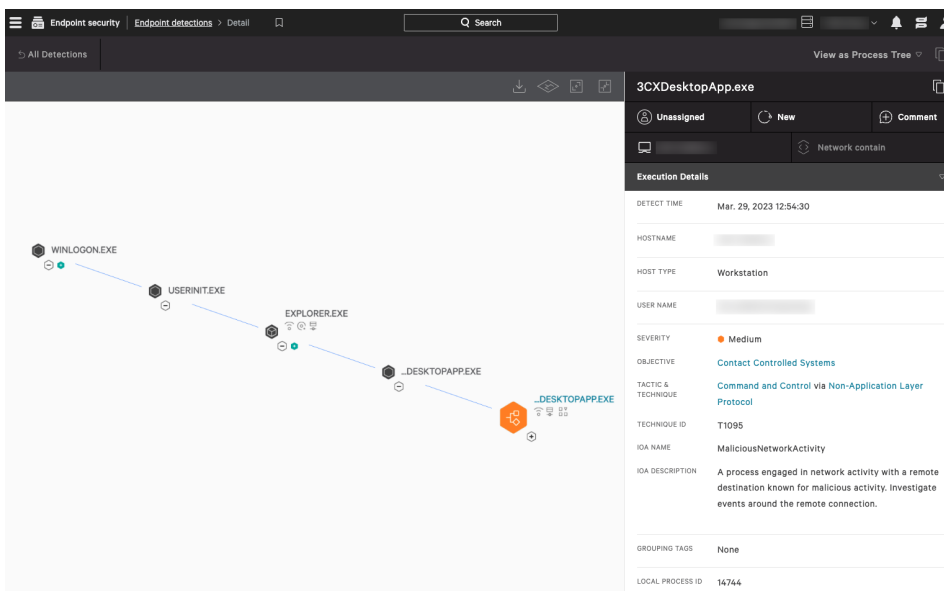

Figure 2. CrowdStrike's indicator of attack (IOA) identifies and blocks the malicious behavior in Windows (click to enlarge)

Hunting in the CrowdStrike Falcon Platform

Falcon Discover

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

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

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
```

Falcon Long Term Repository (LTR) powered by Falcon LogScale — Application Search

```
#event_simpleName=/^(PeVersionInfo|ProcessRollup2)$/ AND (event_platform=Win
ImageFileName=/\\3CXDesktopApp\.exe$/i) OR (event_platform=Mac
ImageFileName=/\/3CX\sDesktop\sApp/i)
| ImageFileName = /.+(\\|\/)(?.+)$/i
```

```
| groupBy([event_platform, FileName, SHA256HashData], function=count(aid,
distinct=true, as=endpointCount))
```

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
```

CrowdStrike 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-1 | US-GOV-1.

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)
```

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)
```

File Details

SHA256	Operating System	Installer SHA256
dde03348075512796241389dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc	Windows	aa124a4b4df12b34e74ee7f6c683b2ebe
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405	Windows	59e1edf4d82fae4978e97512b0331b7eb

92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61   macOS   5407cda7d3a75e7b1e030b1f33337a56f

b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb   macOS   e6bbc33815b9f20b0cf832d7401dd893ft

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).

CrowdStrike Intelligence Confidence Assessment

High Confidence: Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.

Moderate Confidence: Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.

Low Confidence: Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Additional Resources

- *Request a free CrowdStrike Intelligence threat briefing and learn how to stop adversaries targeting your organization.*
- *The industry-leading CrowdStrike Falcon platform sets the new standard in cybersecurity. Watch this demo to see the Falcon platform in action.*
- *Experience how the industry-leading CrowdStrike Falcon platform protects against modern threats. Start your 15-day free trial today.*
- *Find more information on this situation on our Trending Threats & Vulnerabilities: Intrusion Campaign Targeting 3CX Customers tracking page.*