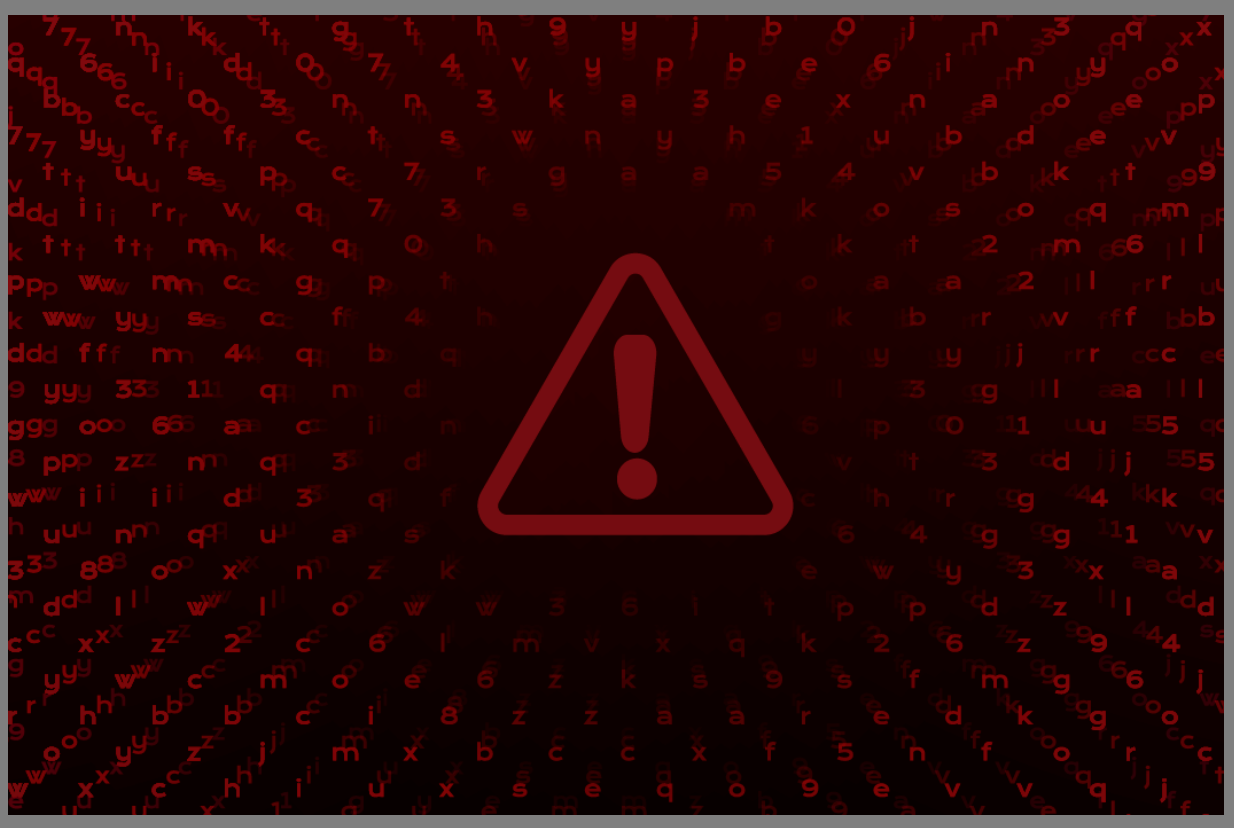
CrowdStrike Falcon Platform Detects and Prevents Active Intrusion Campaign Targeting 3CXDesktopApp Customers

March 29, 2023 | CrowdStrike | Counter Adversary Operations



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

CATEGORIES

Cloud & Application Security 104
Counter Adversary Operations 184
Endpoint Security & XDR 307
Engineering & Tech 78
Executive Viewpoint 162
Exposure Management 84
From The Front Lines 190
Identity Protection 37
Next-Gen SIEM & Log Management 91
Public Sector 37
Small Business 8

CONNECT WITH US

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

September 25, 2024

Recognizing the Resilience of the CrowdStrike Community

September 25, 2024

CrowdStrike Drives Cybersecurity Forward with New Innovations Spanning AI, Cloud, Next-Gen SIEM and Identity Protection

September 18, 2024

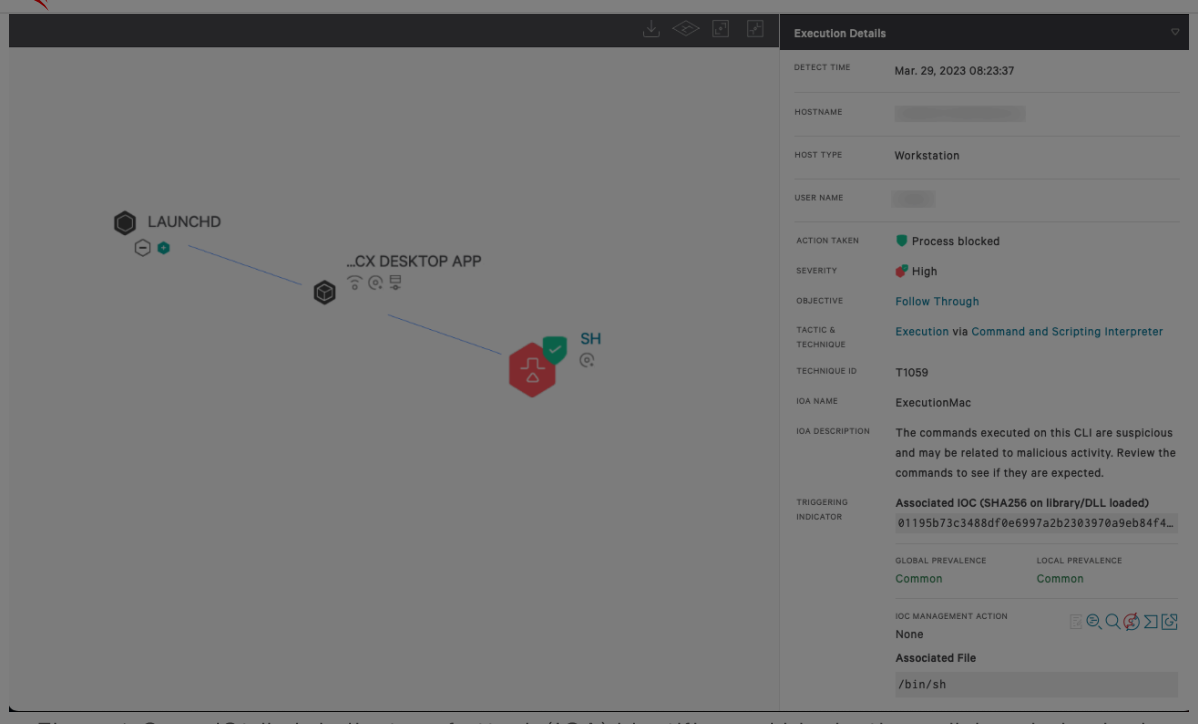


Figure 1. CrowdStrike's indicator of attack (IOA) identifies and blocks the malicious behavior in macOS (click to enlarge)

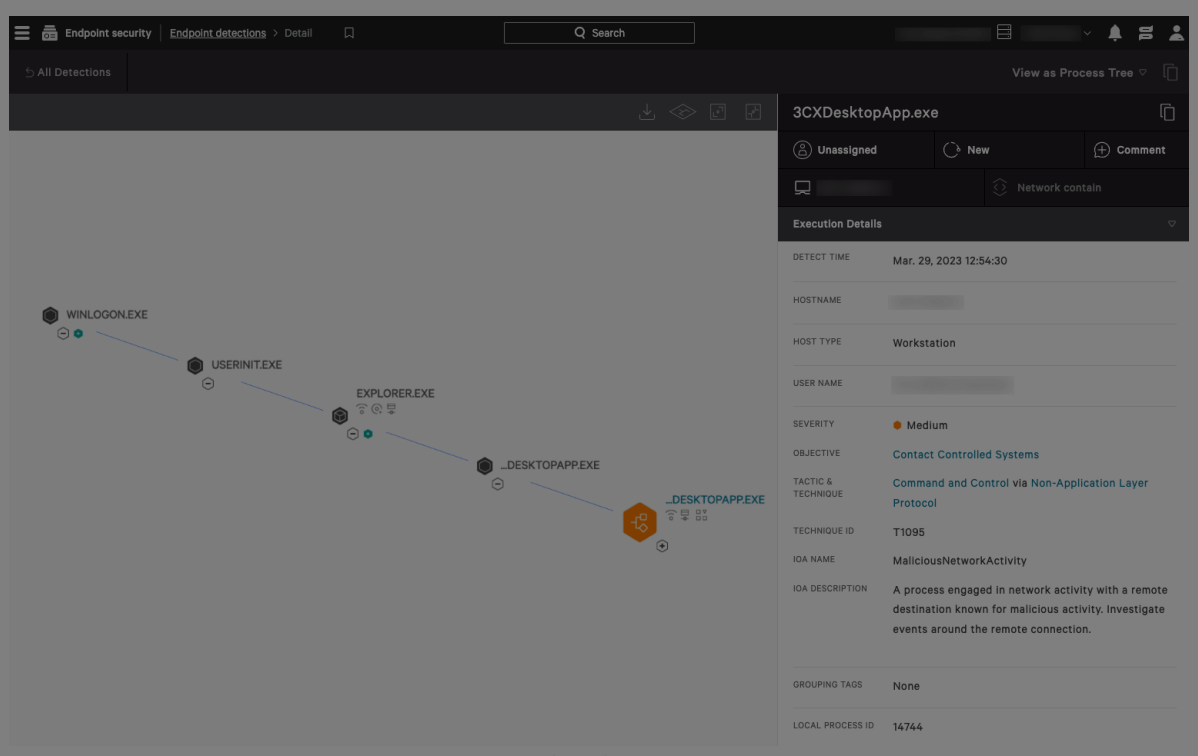


Figure 2. CrowdStrike's indicator of attack (IOA) identifies and blocks the malicious behavior in Windows (click to enlarge)

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
| stats dc(aid) as endpointCount by event_platform, FileName,
```

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

```
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.co
| stats dc(aid) as endpointCount, earliest(ContextTimeStamp_d
| convert ctime(firstSeen) ctime(lastSeen)
```

Falcon LTR — Domain Search

```
#event_simpleName=DnsRequest
| in(DomainName, values=)
| groupBy(, function=())
| firstSeen := firstSeen * 1000 | formatTime(format="%F %T.%L
| lastSeen := lastSeen * 1000 | formatTime(format="%F %T.%L",
| sort(endpointCount, order=desc)
```

File Details

SHA256
dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a367040
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb

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.*

DDoS Attacks in 2023 and 2024

Detail Ties to BITWISE SPIDER and Russian State Activity

« QakBot eCrime Campaign Leverages Microsoft OneNote Attachments

Hypervisor Jackpotting, Part 3: Lack of Antivirus Support Opens the Door to Adversary Attacks »