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,

Featured
Recent
Video
Category
Start Free Trial

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 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

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

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

Featured
Recent
Video
Category
Start Free Trial

based detections targeting malicious behaviors associated with 3CX on both macOS and Windows.

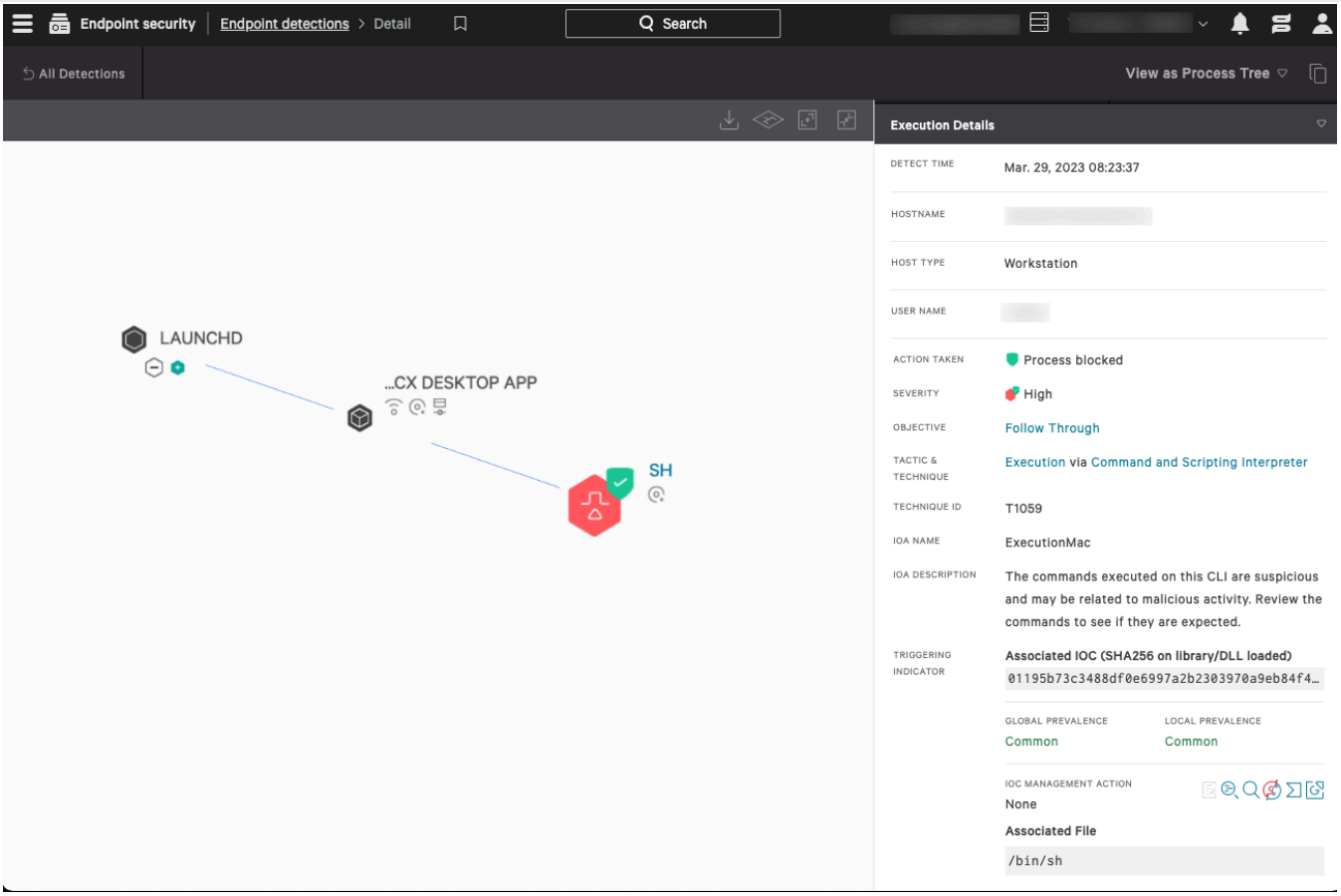


Figure 1. CrowdStrike's indicator of attack (IOA) identifies and blocks the malicious behavior in macOS (click to enlarge)

Featured
Recent
Video
Category
Start Free Trial

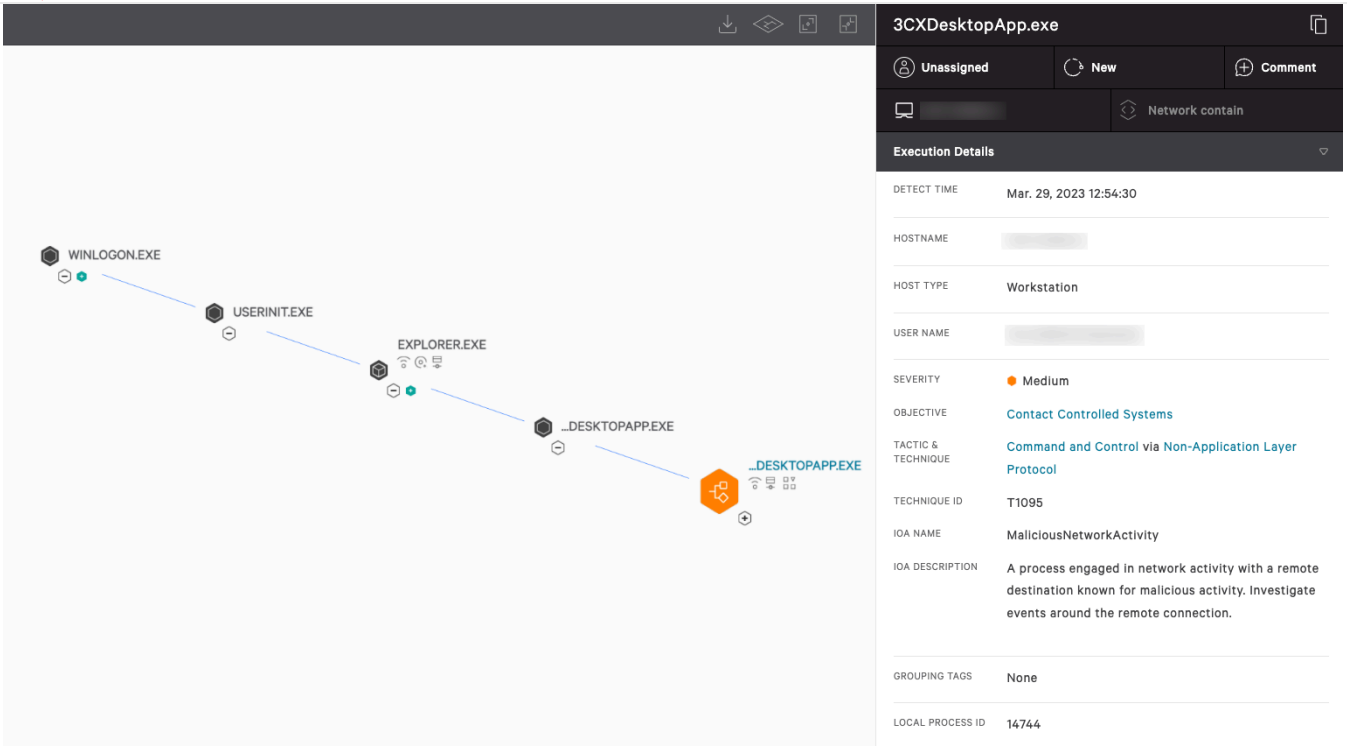


Figure 2. CrowdStrike's indicator of attack (IOA) identifies and blocks the malicious behavior in Windows (click to enlarge)

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

Atomic Indicators

The following domains have been observed beaconing, which should be considere

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

Featured
Recent
Video
Category
Start Free Trial

Graph: US-1 | US-2 | EU-1 | US-GOV-1. **Event Search — Domain Search**

```
event_simpleName=DnsRequest DomainName IN (akamaicontainer.com, akama
| stats dc(aid) as endpointCount, earliest(ContextTimeStamp_decimal)
```

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

File Details

SHA256	Oper
dde033480755127962413 89dfea5560c20a3d2a2eac95c894e7bbed5e85a0acc	Winc
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405	Winc
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61	macO
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb	macO

Recommendations

Featured
Recent
Video
Category
Start Free Trial

CrowdStrike Intelligence Confidence Assessment

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.*

Featured
Recent
Video
Category
Start Free Trial

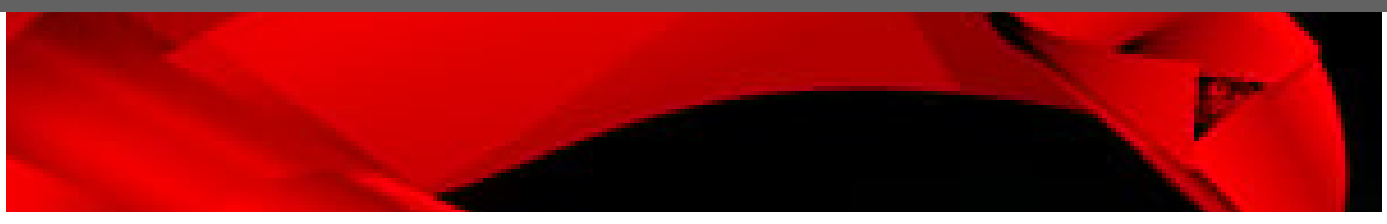
U.S. Department of Justice Indicts Hacktivist Group Anonymous Sudan for Prominent DDoS Attacks in 2023 and 2024

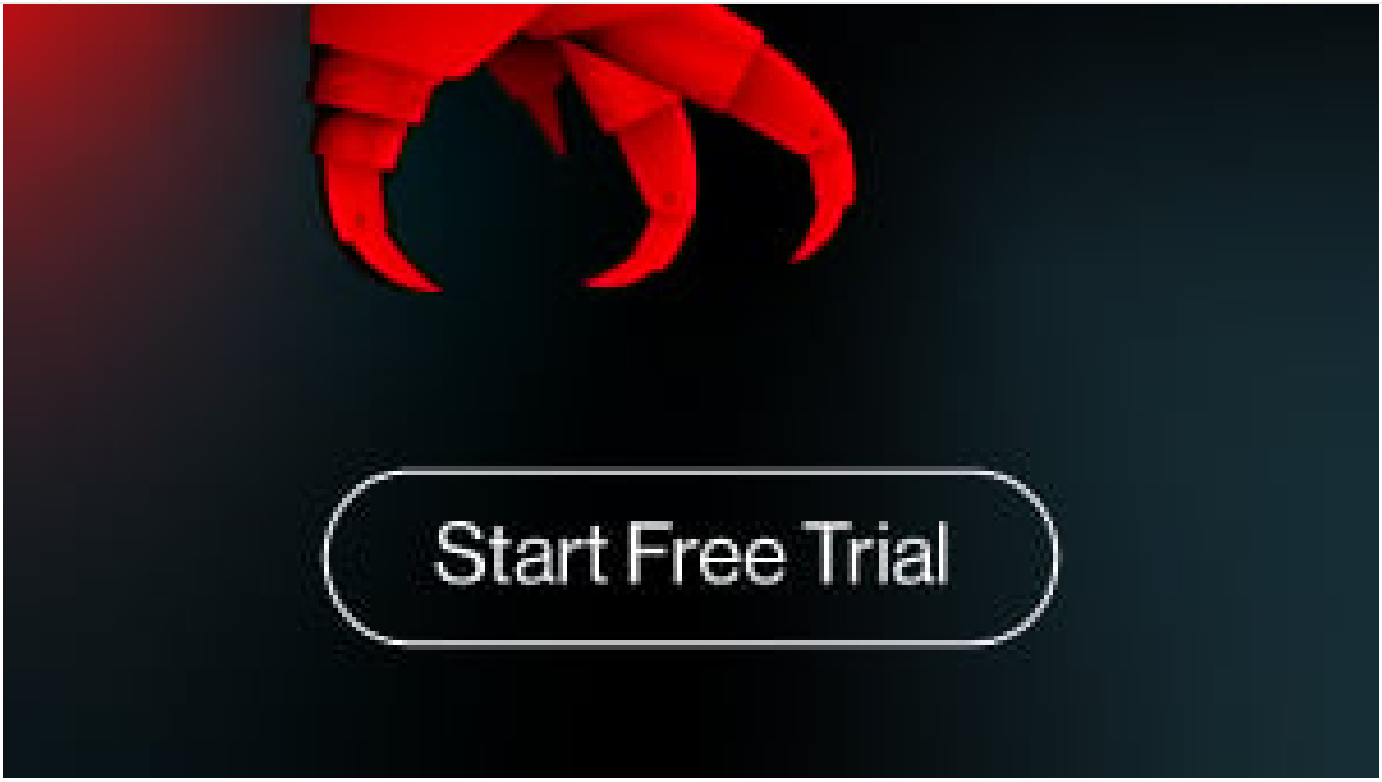
International Authorities Indict, Sanction Additional INDRIK SPIDER Members and Detail Ties to BITWISE SPIDER and Russian State Activity

How CrowdStrike Hunts, Identifies and Defeats Cloud-Focused Threats

CATEGORIES

Featured
Recent
Video
Category
Start Free Trial





Featured
Recent
Video
Category
Start Free Trial

September 25, 2024

Recognizing the Resilience of the CrowdStrike Community

SIEM and Identity Protection

September 18, 2024