

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

Featured

Recent

Video

Category

Start Free Trial

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.

Endpoint security | Endpoint detections > Detail

All Detections

View as Process Tree

Execution Details

LAUNCHD

...CX DESKTOP APP

SH

DETECT TIME Mar. 29, 2023 08:23:37

HOSTNAME [REDACTED]

HOST TYPE Workstation

USER NAME [REDACTED]

ACTION TAKEN Process blocked

SEVERITY High

OBJECTIVE Follow Through

TACTIC & TECHNIQUE Execution via Command and Scripting Interpreter

TECHNIQUE ID T1059

IOA NAME ExecutionMac

IOA DESCRIPTION The commands executed on this CLI are suspicious and may be related to malicious activity. Review the commands to see if they are expected.

TRIGGERING INDICATOR Associated IOC (SHA256 on library/DLL loaded)
01195b73c3488df0e6997a2b2303970a9eb84f4...

GLOBAL PREVALENCE Common LOCAL PREVALENCE Common

IOC MANAGEMENT ACTION None

Associated File /bin/sh

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

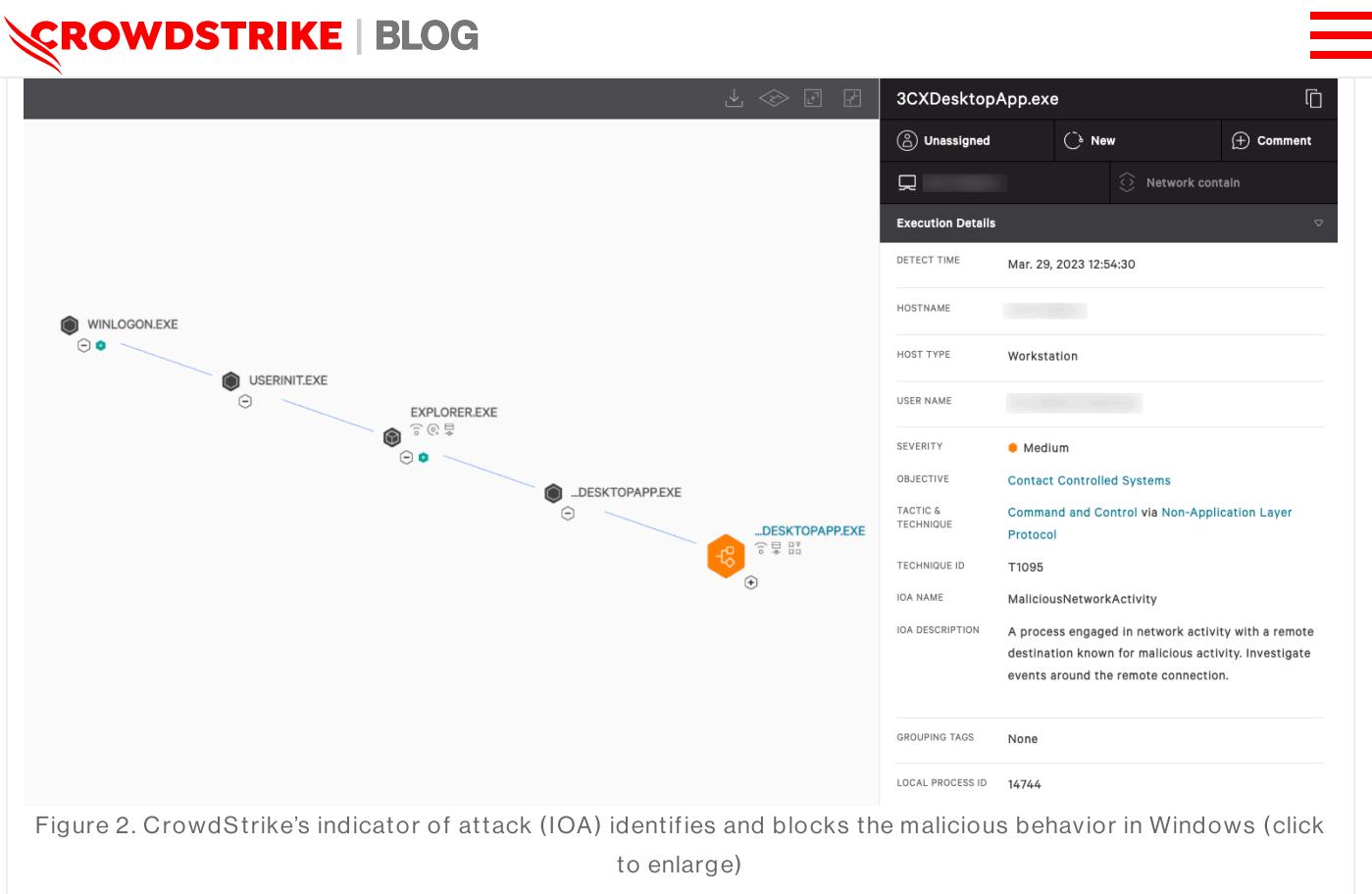
Featured

Recent

Video

Category

Start Free Trial



Hunting in the CrowdStrike Falcon Platform

Falcon Discover CrowdStrike Falcon® Discover customers can use the following link: [US-1](#)

Featured

Recent

Video

Category

[Start Free Trial](#)

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



Atomic Indicators

The following domains have been observed beaconing, which should be considered suspicious:

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
pbxphonetwork<.>.com
pbxsources<.>.com
swapi123008<.>.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, 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, pbxphonetwork.com, pbxsources.com, swapi123008.com)
```

| stats dc(aid) as endpointCount, earliest(ContextTimeStamp_decimal)



```
#eventSimpleName=DnsRequest
| in(DomainName, values=)
| groupBy(, function=())
| firstSeen := firstSeen * 1000 | formatTime(format="%F %T.%L", field=1)
| lastSeen := lastSeen * 1000 | formatTime(format="%F %T.%L", field=1)
| sort(endpointCount, order=desc)
```

File Details

SHA256	Open
dde03348075512796241389dfa5560c20a3d2a2eac95c894e7bbcd5e85a0acc	Wincom
fad482ded2e25ce9e1dd3d3ecc3227af714bdfbbde04347dbc1b21d6a3670405	Wincom
92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61	macos
b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb	macos

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



BREACHES STOP HERE

PROTECT AGAINST MALWARE, RANSOMWARE AND FILELESS ATTACKS

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

 Cloud & Application Security	104
 Counter Adversary Operations	184
 Endpoint Security & XDR	307

Featured

Recent

Video

Category

Start Free Trial

 Next-Gen SIEM & Log Management	91
 Public Sector	37



CONNECT WITH US



Featured

Recent

Video

Category

Start Free Trial



CROWDSTRIKE

Get started
with CrowdStrike
for free.

[Featured](#)

[Recent](#)

[Video](#)

[Category](#)

[Start Free Trial](#)



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



SUBSCRIBE

Sign up now to receive the latest notifications and updates from CrowdStrike.

Sign Up



See CrowdStrike Falcon® in Action

Detect, prevent, and respond to attacks— even malware-free intrusions—at any stage, with next-generation endpoint protection.

See Demo

Featured

Recent

Video

Category

Start Free Trial



Copyright © 2024 CrowdStrike | [Privacy](#) | [Request Info](#) | [Blog](#) | [Contact Us](#) | [1.888.512.8906](#) | [Accessibility](#)