Investigating 3CX Desktop Application Attacks: What You Need to Know

By Threat Analysis Unit

Published: 2023-03-31 · Archived: 2026-04-05 17:55:15 UTC

This is a developing situation and this blog post will be updated as needed.

Reports of malicious code associated with the 3CX desktop application – part of the 3CX VoIP (Voice over Internet Protocol) platform – began on March 22, 2023. On March 30, 2023, 3CX confirmed the compromise, noting the affected 3CX desktop app versions were 18.12.407 and 18.12.416 for Windows and 18. 11.1213, 18.12.402, 18.12.407 and 18.12.416 versions for Mac. NIST National Vulnerability Database has assigned CVE-2023-29059 to track this issue.

Reports indicate that one of the bundled libraries included with the 3CX Windows and Mac desktop clients had been altered to contact command and control infrastructure, including a GitHub repository, to deliver second-stage malware. According to 3CX, the malicious domains and the GitHub repository have since been taken down.

What is the potential impact?

Software supply chain attacks, as seen with the SolarWinds attack in December 2020, can lead to security teams discovering that their environment has been breached months prior in what is disguised as a standard software update. This highlights the challenges associated with software validation as part of supply chains. The impact of such an attack can be devastating, causing long-term damage to the business, its reputation, and its customers

In the case of this 3CXDesktopApp attack, there is not yet enough information on how the compromised code ended up being included with 3CX digitally signed installers. 3CX has hired Mandiant to assist with forensic activities.

Observations by VMware Threat Analysis Unit

Note: This is a developing situation and threat analysis will be updated as needed.

VMware Contexa detected the first connections to the C2 domains included in the ICO files as early as 2023-03-06 (akamaitechcloudservices[.]com) and 2023-03-07 (pbxphonenetwork[.]com, sbmsa[.]wiki, azureonlinestorage[.]com, officeaddons[.]com, pbxsources[.]com, officestoragebox[.]com). See Figure 1 for the whole timeline.

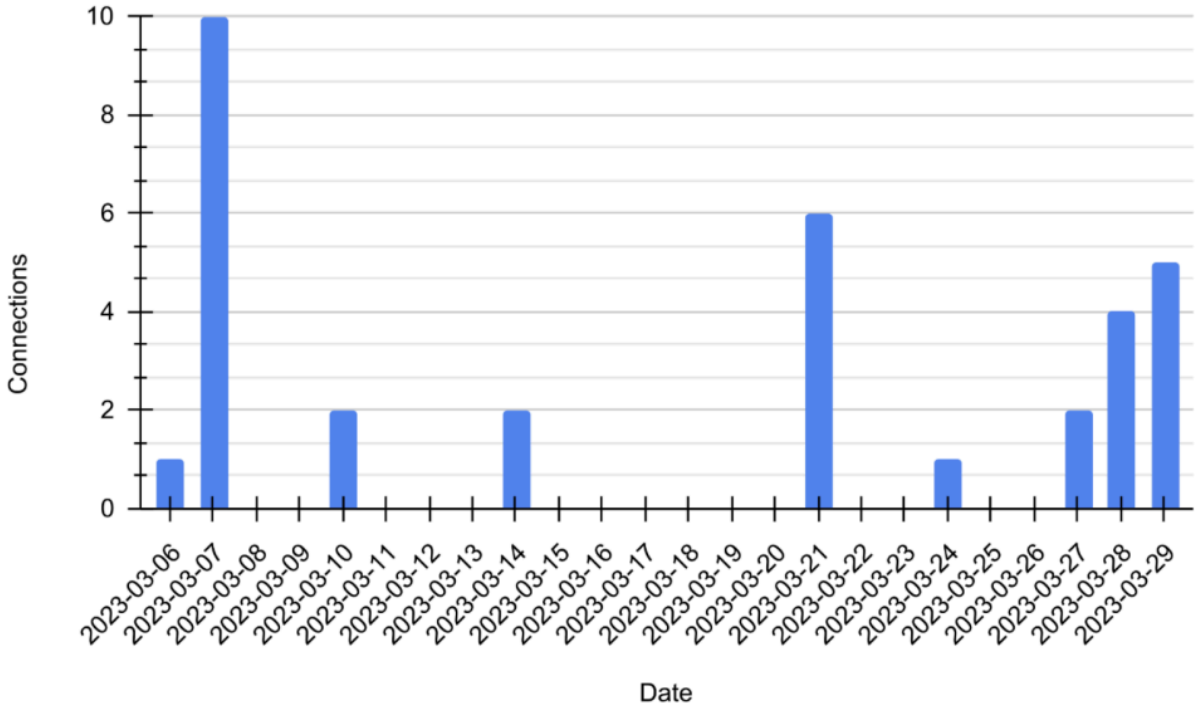

Figure 1: Connections to C2 domains as detected by VMware Contexa.

TLS connections to visualstudiofactory[.]com taking place on 2023-03-24 and later were established to a server with a certificate with the following hash 'cda34a2b46a2269dc5934967175656a81bd3667a21855273dc2c777f8bd2d4c9', valid from 2022-11-17, expiring on 2023-11-17, and issued by "C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA". The recorded JA3S is 61be9ce3d068c08ff99a857f62352f9d, although note that it is only useful when looking for TLS connections established by the compromised 3CX desktop app.

A search on Censys can also reveal that the host had been online since 2022-11-19; our telemetry, however, does not show any activity related to this C2 domain prior to March 2023.

Current hashes identified to be banned are the following:

Compromised parents/Installers

- 59e1edf4d82fae4978e97512b0331b7eb21dd4b838b850ba46794d9c7a2c0983
- aa124a4b4df12b34e74ee7f6c683b2ebec4ce9a8edcf9be345823b4fdcf5d868
- 7c55c3dfa373b6b342390938029cb76ef31f609d9a07780772c6010a4297e321
- e32cc0103827e8eef5881bd6fcae30ccc6bf6d68e8378c007a8fac2d8edbc071
- B5e318240401010e4453e146e3e67464dd625cfef9cd51c5015d68550ee8cc09

Zip file

- 5c54932fdbb077d73c58ac41a1ad3f6ea5576b3e1f719c8b714b637c9ceb361b
- b57d7e6c47516aeb1fd8384a9bc002f8c637b7d42b8f008a0c9e872914344dad

ffmpeg.dll

- 7986bbaee8940da11ce089383521ab420c443ab7b15ed42aed91fd31ce833896
- c485674ee63ec8d4e8fde9800788175a8b02d3f9416d0e763360fff7f8eb4e02
- 253f3a53796f1b0fbe64f7b05ae1d66bc2b0773588d00c3d2bf08572a497fa59

d3dcompiler_47.dll

- 11be1803e2e307b647a8a7e02d128335c448ff741bf06bf52b332e0bbf423b03

Secondary stage Payloads

- 851c2c99ebafd4e5e9e140cfe3f2d03533846ca16f8151ae8ee0e83c692884b7
- 6a0f637546684c90809cf264c22a861c9a07b1ca3b2ef6a359a14d612e392c1a
- aa4e398b3bd8645016d8090ffc77d15f926a8e69258642191deb4e68688ff973
- F5fdefaa5321e2cea02ef8b479de8ec3c5505e956ea1484c84a7abb17231fe24
- 8ab3a5eaaf8c296080fadf56b265194681d7da5da7c02562953a4cb60e147423

MacOS Samples

- 5407cda7d3a75e7b1e030b1f33337a56f293578ffa8b3ae19c671051ed314290
- fee4f9dabc094df24d83ec1a8c4e4ff573e5d9973caa676f58086c99561382d7
- e6bbc33815b9f20b0cf832d7401dd893fbc467c800728b5891336706da0dbcec
- a64fa9f1c76457ecc58402142a8728ce34ccba378c17318b3340083eeb7acc67
- b86c695822013483fa4e2dfdf712c5ee777d7b99cbad8c2fa2274b133481eadb
- fd15a9619987925827ede24efa8990c3680c9c0b4a76eb1c43031de39c1b7ae1
- 9a47c9a3f7cf26ddc1fdb90dc48d30d69448e6d8ab64cc57dcb285c6b9d846c3
- 92005051ae314d61074ed94a52e76b1c3e21e7f0e8c1d1fdd497a006ce45fa61
- c649e7c1897bfd30aad85c6b6736fcb2d002a7eaf64186eea00c1a44d6220803
- fdad2f34e466782e4b272d3f8505c49c3bb6269c8d5fd8846f0cc399f9744cba
- 87c5d0c93b80acf61d24e7aaf0faae231ab507ca45483ad3d441b5d1acebc43c

How can you protect your organization?

3CX has provided mitigation guidance, which includes a recommendation to uninstall the 3CX desktop app. As of this writing, an updated desktop app was being prepared by 3CX.

One of the biggest challenges with supply chain attacks is that they are challenging to detect. Because the attack occurs through a third-party vendor, the business may not even be aware that an attack has taken place until it is too late. Organizations can minimize overall risk of a supply chain attack by following security best practices. These include:

- Developing a robust security strategy that encompasses the entire supply chain. This means conducting thorough security checks on all vendors, ensuring that they have appropriate security measures in place, and regularly monitoring their systems for any potential threats.

- Implementing endpoint and network security solutions that can detect and respond to threats in real-time, as well as advanced threat detection solutions that can identify potential anomalous threats as they occur.
- Ensuring a solid incident response plan is in place in case of a supply chain attack. This includes identifying the key stakeholders who need to be notified, as well as having a clear process in place for containing and mitigating the attack.

By taking these steps, businesses can reduce the risk of a supply chain attack and ensure the safety and security of their operations and customers.

How can VMware security products help?

- The hashes listed in this blog post have a known malware reputation and should be blocked automatically by **Carbon Black Cloud**.
- **Carbon Black EDR** customers can search for netconn traffic to the domains listed in this blog post.
- **Carbon Black App Control** customers can ban the hashes listed in this blog post.
- Carbon Black customers can also find additional product related details and instructions by logging on to the user community and accessing this link: HERE
- For **NSX Advanced Threat Prevention** (ATP), all published indicators are currently detected as malicious. Where guest virtual machines are protected by the Distributed Malware Prevention Service leveraging Guest Introspection, all malicious DLL files associated with this threat can be mitigated with a 'detect and prevent' malware prevention profile (Figure 2 shows how **NSX ATP** detect the malicious DLLs through Guest Introspection). **NSX ATP** has also anomaly-based detectors specifically tailored to identify anomalous beaconing; the malicious domains associated with 3CXDesktopApp are now part of the network reputation feed provided by **NSX ATP**.

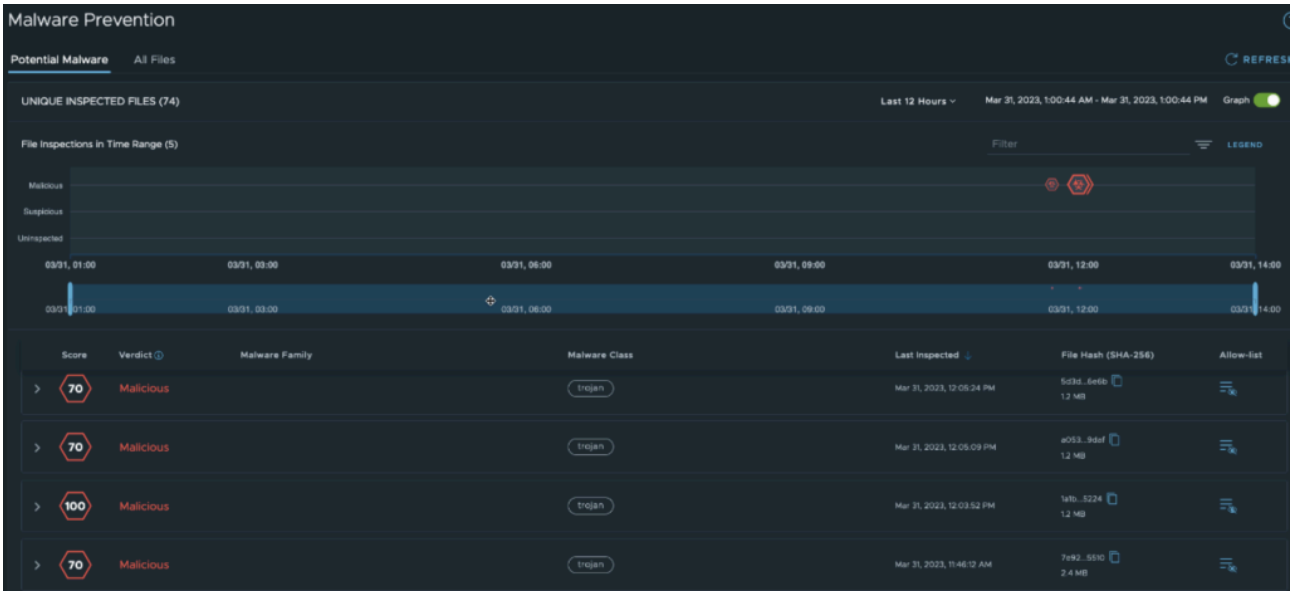

Figure 2: User interface of NSX Guest Introspection Malware Prevention Service.

- **NSX ATP Standalone** customers can also increase upload limits to support analyzing large files (up to 100MB on on-premise, see the following article for instructions on how to change this: INSTRUCTIONS), and threat hunt for the associated malicious network activity via the Network Explore console using the

following search query: *“akamaicontainer.com OR akamaitechcloudservices.com OR azuredeploystore.com OR azureonlinecloud.com OR azureonlinestorage.com OR dunamistrd.com OR glcloudservice.com OR journalide.org OR msedgepackageinfo.com OR msstorageazure.com OR msstorageboxes.com OR officeaddons.com OR officestoragebox.com OR pbxcloudeservices.com OR pbxphonenetwork.com OR pbxsources.com OR sbmsa.wiki OR sourceslabs.com OR visualstudiofactory.com OR zacharryblogs.com OR* qwepoi123098.com*”*.
