Enhanced Attack Report

Smooth Operator

Generated on 2025-03-11

Disclaimer

This report has been generated automatically and should be used for informational purposes only. To generate this report, Large Language Models (LLMs) were used to analyze the provided data. This technology is not perfect and may generate incorrect or misleading results. The results should be reviewed by a human expert before taking any action based on the information provided.

Definitions

Pre-Conditions: Conditions that must be true to execute the attack steps in the milestone.

Post-Conditions: Traces that an attacker leaves behind after executing the attack steps in the milestone.

Attack Steps: Steps that an attacker would take to achieve the goal of the milestone.

MITRE Technique: Techniques from the MITRE ATT&CK; framework that are relevant to the milestone.

STIX

Malware Name: Smooth Operator
Malware Description: â€¢ Smooth Operator malware targets the macOS operating system. â€¢ Smooth Operator was distributed to victims as part of the 3CX supply chain attack. â€¢ The infected software package was signed by 3CX and notarized by Apple. â€¢ HTTPS is used as a C2 channel, with an additional custom encoding algorithm used to obfuscate exfiltrated data. â€¢ Smooth Operator randomises the C2 server it communicates with. The 3CX website is included in the list of C2 Servers it can beacon to. â€¢ Malicious code inserted into a dynamic library (dylib) packaged with the 3CX software, downloads and runs a second stage payload.

Quick Overview

Milestone 1
1. Supply Chain Compromise: Compromise Software Dependencies and Development Tools as used by the malware (T1195.001)

Milestone 2
1. Compromise Client Software Binary as used by the malware (T1554)

Milestone 3
1. Deobfuscate/Decode Files or Information as used by the malware (T1140)
2. Indicator Removal: File Deletion as used by the malware (T1070.004)
3. Virtualization/Sandbox Evasion: Time Based Evasion as used by the malware (T1497.003)

Milestone 4
1. Automated Collection as used by the malware (T1119)

Milestone 5
1. Application Layer Protocol: Web Protocols as used by the malware (T1071.001)
2. Fallback Channels as used by the malware (T1008)

Milestone 6
1. Automated Exfiltration as used by the malware (T1020)

Milestone 1

Pre-Conditions:

- Knowledge of software development practices and tools.
- Malicious libraries exist.
- The ability to modify the software dependencies and development tools used in the 3CX Desktop App's build process.

Post-Conditions:

- Potential for further malware deployment and lateral movement within compromised networks.
- Modified 3CXDesktopApp installation files with embedded malicious code.
- Data exfiltration from infected systems to C2 servers.
- Obfuscated logs containing communication with C2 servers.
- Reputational damage to 3CX and affected users.
- Compromised 3CX Desktop App installations on user devices.
- New files created by the malware on infected systems.
- Unusual process activity and memory usage patterns.
- Altered system configurations related to network settings or security features.
- Network connections to malicious domains and IP addresses.
- Registry entries made by the malware for persistence.

Attack Step 1.1

==========
Name: Supply Chain Compromise: Compromise Software Dependencies and Development Tools as used by the malware
Description: The "Smooth Operator" malware is disseminated through a supply chain compromise involving the infiltration of legitimate software development processes. Malicious libraries were surreptitiously introduced into the build process of the 3CXDesktopApp software during compilation. Subsequently, the compromised installation packages were authenticated and notarized by 3CX, thereby conferring an appearance of legitimacy and circumventing Apple's security protocols. Distribution occurred through established channels, inducing users to install the malware under the presumption of its authenticity. Upon installation, the malicious libraries embedded within the 3CXDesktopApp package facilitate the download and execution of a secondary payload. The nature of this secondary payload remains indeterminate due to implemented security measures that preclude comprehensive analysis.

MITRE Technique

ID: T1195.001
Name: Supply chain compromise: compromise software dependencies and development tools
Description: Adversaries may manipulate software dependencies and development tools prior to receipt by a final consumer for the purpose of data or system compromise. Applications often depend on external software to function properly. Popular open source projects that are used as dependencies in many applications may be targeted as a means to add malicious code to users of the dependency.
More info: https://attack.mitre.org/techniques/T1195/001

Indicators

- Domain names may be registered for malicious purposes.
- Files with unusual or generic names may be created.

Milestone 2

Pre-Conditions:

- The 3CX software is installed on the victim's system.
- The malicious version of the 3CX software contains the Smooth Operator malware.
- A network connection to facilitate communication with the command and control (C2) server.

Post-Conditions:

- Modified libffmpeg.dylib file in the 3CX software installation directory.
- Data exfiltration from infected systems.
- .main_storage file containing victim ID and other sensitive information.
- Potential for further malware stages to be deployed.
- Altered system registry entries related to the compromised software.
- Traces of obfuscated OS version, hostname, and C2 information in 3cx_auth_token_content field.
- Increased risk of future attacks targeting the compromised system.
- Modified application logs with suspicious activity.
- Compromised 3CX software on victim machines.
- Malware beacon communication logs on infected systems.
- Network connections to Command and Control (C2) servers.

Attack Step 2.1

==========

Name: Compromise Client Software Binary as used by the malware
Description: The Compromise Client Software Binary (T1554) technique is employed by Smooth Operator to establish persistence within victim systems. Trojanized 3CX software, containing a compromised libffmpeg.dylib component, is disseminated through seemingly credible channels. This malware is presented as legitimate and updated software for the 3CX communication platform. Upon installation and execution by the user, Smooth Operator leverages its integration within the 3CX application to achieve persistence. The second stage of the malware exhibits an adhoc signature, lacking a certificate from a trusted authority and consequently failing to provide a verifiable chain of trust. Additionally, this stage is not notarized by Apple, further diminishing its legitimacy. The trojanised libffmpeg.dylib is designed as a universal binary, facilitating execution on both Intel-based and ARM-based macOS systems. This tactic exploits the trust associated with legitimate software such as 3CX, enabling Smooth Operator to operate under the guise of a harmless program and gain persistent access to the victim's system.

MITRE Technique

ID: T1554
Name: Compromise host software binary
Description: Adversaries may modify host software binaries to establish persistent access to systems. Software binaries/executables provide a wide range of system commands or services, programs, and libraries. Common software binaries are SSH clients, FTP clients, email clients, web browsers, and many other user or server applications.
More info: https://attack.mitre.org/techniques/T1554/

Indicators

- Filename: UpdateAgent
- Filename: .main_storage

Milestone 3

Pre-Conditions:

- The malware has been executed.
- Exfiltrated data exists in an obfuscated format.
- Data needs to be deobfuscated and decoded.
- A custom data encoding algorithm is available within the malware.
- Smooth Operator malware is present.
- The malware's second stage is active.
- The malware has successfully executed.
- The file to be deleted is accessible by the UpdateAgent binary.
- The UpdateAgent binary exists.
- Smooth Operator is running.
- A system with a functioning clock and timekeeping mechanism.
- The malware has executed its first stage.
- An internet connection to potentially verify the current date and time.

Post-Conditions:

- Modifying system settings: Which settings? How?
- Executing code: What kind of code? Where is it stored?
- Connecting to networks: Which networks? For what purpose?
- Downloading files: From where? What type of files?
- Exfiltrated data logs on C2 servers
- Potential for further malware installation and execution
- Deleted files related to Smooth Operator second-stage payload
- Increased risk of system compromise and data loss
- Unusual activity logs in Windows event viewer
- New files created in legitimate 3CX installation directory
- Presence of custom encoding algorithm artifacts in exfiltrated data
- Data exfiltration from infected systems
- Modified 3CX desktop app files
- Altered timestamps in system and application logs
- Compromised 3CX desktop application functionality
- Network connections to C2 servers using HTTPS
- Modified system registry entries
- Deleted malicious second-stage payload files
- Obfuscated data in network traffic logs
- Unusual file access patterns in event logs
- Modified 3CX Desktop App installation package
- Compromised 3CX Desktop App functionality
- System instability and performance degradation
- Potential for further malware infections
- Data exfiltration from infected systems
- Increased risk of future attacks
- Modified DLL files with altered signature blobs
- C2 server communication logs
- Loss of sensitive information
- Modified system registry entries

- Network connections to suspicious domains

Attack Step 3.1

==========
Name: Deobfuscate/Decode Files or Information as used by the malware
Description: Data intended for transmission to the Command and Control (C2) server by Smooth Operator is subject to obfuscation via a custom algorithm. Upon writing data to files on the infected system, the malware applies this algorithm, rendering the information unreadable in its original form. Conversely, incoming responses from the C2 server are initially obfuscated. The malware subsequently utilizes the same custom algorithm to deobfuscate these messages, facilitating comprehension.

MITRE Technique

ID: T1140
Name: Deobfuscate/decode files or information
Description: Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.
More info: https://attack.mitre.org/techniques/T1140/

Indicators

- Filename: UpdateAgent
- Filename: .main_storage

Attack Step 3.2

==========
Name: Indicator Removal: File Deletion as used by the malware
Description: Indicator Removal: File Deletion is executed by the malware's second stage, involving the immediate deletion of the malware executable from the disk subsequent to its execution.

MITRE Technique

ID: T1070.004
Name: Indicator removal: file deletion
Description: Adversaries may delete files left behind by the actions of their intrusion activity. Malware, tools, or other non-native files dropped or created on a system by an adversary (ex: Ingress Tool Transfer) may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.
More info: https://attack.mitre.org/techniques/T1070/004

Indicators

- Filename: .main_storage

Attack Step 3.3

==========
Name: Virtualization/Sandbox Evasion: Time Based Evasion as used by the malware
Description: Time-Based Evasion techniques are employed by Smooth Operator to circumvent detection within virtualization or sandboxing environments. A delay mechanism is implemented, resulting in a minimum of one week of inactivity following execution. During this period, beaconing activity to Command and Control servers is suspended. This extended quiescence reduces the likelihood of triggering alerts from security tools that primarily monitor for immediate suspicious behavior within shorter timeframes. The deliberate "sleep" duration aims to facilitate integration with legitimate software and hinder detection as potentially malicious.

MITRE Technique

ID: T1497.003
Name: Virtualization/sandbox evasion: time based evasion
Description: Adversaries may employ various time-based methods to detect and avoid virtualization and analysis environments. This may include enumerating time-based properties, such as uptime or the system clock, as well as the use of timers or other triggers to avoid a virtual machine environment (VME) or sandbox, specifically those that are automated or only operate for a limited amount of time.
More info: https://attack.mitre.org/techniques/T1497/003

Indicators

- The filename ".main_storage" is observed.

Milestone 4

Pre-Conditions:

- Access to files and data within the 3CX installation.
- A 3CX installation is present on the victim machine.
- The Smooth Operator malware has successfully infected the victim machine.
- Internet connectivity to communicate with the command and control server.

Post-Conditions:

- Presence of malicious code in memory
- Data transfer logs
- Backdoor access points
- Reputational damage to affected organizations
- Modified system files
- Indicators of compromise (IOCs) in security logs
- Compromised user data exfiltration
- System instability and performance degradation
- Obfuscated communication artifacts
- Potential for further malware infections
- Unusual process activity logs
- Altered registry entries
- New or modified network connections

Attack Step 4.1

==========

Name: Automated Collection as used by the malware
Description: Data is actively collected from infected systems by "Smooth Operator" malware stages. This data encompasses system information such as operating system version, hostname, and hardware specifications. User-related data points, including login credentials, browsing history, and accessed files, are also gathered. Network information, comprising IP addresses, network configurations, and active connections, is collected. The acquired data undergoes processing and formatting into a structured format, likely optimized for transmission to the command-and-control (C&C;) server. Transmission methods may include encrypted channels and proxy servers to ensure secure data transfer. Data is either periodically transmitted as "beacon" signals to the C&C; server, indicating system status and activity, or entirely exfiltrated to the server for analysis. Upon reception at the C&C; server, the data is further processed for purposes such as intelligence gathering, vulnerability identification, and potential data theft.

MITRE Technique

ID: T1119
Name: Automated collection
Description: Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a Command and Scripting Interpreter to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals.

More info: https://attack.mitre.org/techniques/T1119/

Indicators

- A file named "UpdateAgent" is present.
- A file named ".main_storage" is present.

Milestone 5

Pre-Conditions:

- The malware has established a connection to the command and control server.
- A web browser or similar application capable of making HTTP requests is present.
- A network connection is available.
- The malware is active.
- HTTPS protocol support is enabled.
- An internet connection is available to the infected device.
- The 3CX website URL is included in the C2 server list.
- The malware is running on an infected device.
- A C2 server list is embedded within the malware.

Post-Conditions:

- Modified registry entries
- Evidence of data encryption/decryption activities
- Potential for further attacks
- Unusual file access patterns
- Logs of suspicious network activity (e.g., communication with C2 servers)
- Exfiltrated data stored on remote servers
- Increased security risks
- Data theft
- Modified DLL files with altered signature blobs
- Changes to firewall rules
- System instability
- New user accounts created without authorization
- Altered timestamps in system files
- Compromised system functionality
- Presence of malicious code within the 3CX Desktop App
- Compromised 3CX system
- New log entries indicating suspicious activity
- Unusual process creation and network connections logs
- Obfuscated data files containing stolen information
- System instability and performance degradation
- Potential for further malware infections
- Altered system settings favoring malware execution
- Modified 3CX application files
- Network traffic to malicious C2 servers
- Data exfiltration
- Registry modifications related to malware persistence

Attack Step 5.1

==========

Name: Application Layer Protocol: Web Protocols as used by the malware
Description: Communications between the malware and its Command and Control (C2) servers are encrypted via the Hypertext Transfer Protocol Secure (HTTPS). This encryption protocol renders the

malicious instructions exchanged between the malware and C2 servers difficult to intercept and decipher by analysts.

MITRE Technique

ID: T1071.001
Name: Application layer protocol: web protocols
Description: Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.
More info: https://attack.mitre.org/techniques/T1071/001

Indicators

- The domain "azureonlinestorage.com" is accessed.
- The domain "akamaitechcloudservices.com" is accessed.
- The domain "sourceslabs.com" is accessed.
- The domain "pbxcloudeservices.com" is accessed.
- The domain "pbxphonenetwork.com" is accessed.
- The domain "msstorageboxes.com" is accessed.
- The domain "officeaddons.com" is accessed.
- The domain "zacharryblogs.com" is accessed.
- The URL "https://azureonlinestorage.com/google/storage" is accessed.

Attack Step 5.2

==========
Name: Fallback Channels as used by the malware
Description: Fallback channels within Smooth Operator are implemented through the utilization of a plurality of command-and-control (C2) servers. For each beacon transmission, a novel C2 server is randomly selected from this enumerated list. This methodology enhances malware resilience against service disruptions; should a designated C2 server become inaccessible or compromised, alternative servers within the list can be employed for communication.

MITRE Technique

ID: T1008
Name: Fallback channels
Description: Adversaries may use fallback or alternate communication channels if the primary channel is compromised or inaccessible in order to maintain reliable command and control and to avoid data transfer thresholds.
More info: https://attack.mitre.org/techniques/T1008/

Indicators

- A domain name is used.
- A file named "UpdateAgent" is present.

Milestone 6

Pre-Conditions:

- HTTPS is available for communication.
- The victim ID is available.
- A connection to the internet is established.
- A compromised 3CX Desktop App installation is present.
- The .main_storage file is present.
- Smooth Operator's second stage is running.
- A custom encoding algorithm is implemented.

Post-Conditions:

- Altered registry entries related to 3CX software and malware execution
- Unusual file access patterns and modifications
- Increased risk of ransomware attacks and other malicious activities
- Presence of Smooth Operator malware binaries
- Compromised 3CX Desktop App functionality
- Potential for further malware deployment and lateral movement within networks
- Network connections to custom C2 servers
- Data exfiltration from infected systems
- Modified DLLs with altered signature blobs
- Exfiltrated data files
- Modified .main_storage file
- Suspicious activity in system event logs
- Obfuscated C2 communication logs

Attack Step 6.1

==========

Name: Automated Exfiltration as used by the malware
Description: Automated exfiltration by Smooth Operator is inferred to be executed through potential techniques based on common malware behavior patterns. Modified application channels may be utilized to discreetly transmit stolen data via existing communication pathways employed by legitimate applications, such as email or file transfer protocols. Alternatively, custom backdoors could be established for the direct transmission of exfiltrated data to Command and Control (C2) servers. The precise methods employed by Smooth Operator for automated exfiltration remain to be elucidated through comprehensive analysis of network traffic, system logs, and associated files. Indicators of Compromise (IOCs) are instrumental in identifying and mitigating Smooth Operator infections.

MITRE Technique

ID: T1020
Name: Automated exfiltration
Description: Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.
More info: https://attack.mitre.org/techniques/T1020/

Indicators

- A file named "UpdateAgent" is present.
- A file named ".main_storage" is present.