Enhanced Attack Report

Smooth Operator

Generated on 2025-03-26

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:

- The software development process for the targeted application is accessible.
- Tools for integrating malicious libraries into the build process.
- The target application relies on legitimate dependencies.
- Knowledge of the software's build process and dependencies.
- Connectivity to download and install necessary tools.

Post-Conditions:

- Compromised 3CX software installations
- Presence of malicious dylib file (libffmpeg.dylib)
- Network connections to the exfiltration URL (https:// sbmsa[.]wiki/blog/_insert)
- .main_storage file required for second-stage execution
- Configuration files written by Smooth Operator in the legitimate 3CX installation directory
- Potential for further malware execution and lateral movement
- Logs indicating execution of Smooth Operator components
- Modified 3CX software installation packages
- Beaconing activity from infected systems
- Data exfiltration from infected systems
- Victim ID included in malware beacons and exfiltration data

Attack Step 1.1

==
Name: Supply Chain Compromise: Compromise Software Dependencies and Development Tools as used by the malware
Description: The "Smooth Operator" malware compromises the software supply chain through a multi-stage process: Malicious libraries are injected into the legitimate 3CX software development process during the build stage of the 3CXDesktopApp application. Legitimate 3CX software components are subsequently trojanized, incorporating the Smooth Operator malware without user awareness. To enhance deception, the infected software is signed by 3CX and notarized by Apple, fostering a perception of security and legitimacy. Distribution occurs through established channels, including official downloads and software repositories, resulting in unwitting download and installation of compromised software by users.

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:

- A system running the 3CX software.
- The 3CX software package is installed on the victim's system.
- The malicious dylib file (libffmpeg.dylib) is present within the 3CX software package.

Post-Conditions:

- Modified libffmpeg.dylib file
- Configuration files written to the 3CX installation directory
- Files containing exfiltrated data
- Network connections to the C2 server
- Persistent malware execution on victim's system
- Compromised 3CX software installation
- Data exfiltration to a Command and Control (C2) server
- Logs of malware communication with C2 server
- "UpdateAgent" binary files
- Potential for further malicious activity

Attack Step 2.1

==

Name: Compromise Client Software Binary as used by the malware
Description: The Smooth Operator malware establishes persistence on victim systems by compromising legitimate 3CX client software binaries. This is achieved through the Trojanized distribution of tampered 3CX software packages, resulting in unwitting installation of the malware alongside intended software. Malicious code, including the "Smooth Operator" payload, is injected into the 3CX software binary, enabling execution as part of the legitimate application. Upon execution of the compromised 3CX software by victims, the embedded malicious code persists, ensuring Smooth Operator's presence on the system even after system restarts or logouts.

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:

- Access to files containing obfuscated data.
- A system infected with Smooth Operator malware.
- The malware has been executed.
- Data needs to be deobfuscated.
- Smooth Operator's custom data encoding algorithm is available.
- The malware's binary is present on disk.
- The malware's second stage has been executed.
- Operating System with file system access capabilities.
- The malware is executed.
- The .main_storage file exists.
- The ability to access and modify files on disk (e.g., write to the .main_storage file).
- A system running an operating system compatible with the malware's execution.
- Network connectivity to reach the internet for communication with C2 servers.

Post-Conditions:

- Modified 3CX installation directory
- Obfuscated data files
- Data exfiltration to C2 server
- Network traffic to C2 server (HTTPS)
- Compromised 3CX software functionality
- "UpdateAgent" file containing malicious code
- Logs indicating suspicious activity
- Altered system configurations
- Potential disruption of communication systems
- Increased risk of further attacks
- Deletion of UpdateAgent binary from disk
- Modified system registry settings
- Data exfiltration to https://sbmsa[.]wiki/blog/_insert
- Potential data theft and system compromise
- System event logs recording process creation and termination
- Log entries indicating execution of UpdateAgent
- Network traffic logs showing HTTPS GET requests to https://sbmsa[.]wiki/blog/_insert
- Compromised 3CX installation directory
- Persistence on the system
- Deleted files (Smooth Operator)
- Data exfiltration
- Registry entries for persistence
- Modified files (UpdateAgent, .main_storage)
- System logs indicating process execution and file modifications
- Compromised system
- Network traffic to C2 servers over HTTPS

Attack Step 3.1

==
Name: Deobfuscate/Decode Files or Information as used by the malware
Description: Smooth Operator's multi-layered approach to data obfuscation and handling is characterized by: 1. C2 Communication Obfuscation: Data transmitted over the Command and Control (C2) channel undergoes scrambling via a custom algorithm, rendering analysis of communication traffic challenging for security tools. Furthermore, specific symbols are replaced with their HTML encoded counterparts within the obfuscated strings, aiming to camouflage malicious data as legitimate web code. 2. On-Disk Data Handling: Upon disk write operations, Smooth Operator applies the reverse of its C2 communication obfuscation algorithm, effectively decoding the information for local storage. Similarly, responses received from the command and control server are decoded prior to processing. 3. Data Flow: Data collection encompasses sensitive information extracted from the 3CX system, potentially including user credentials, communication logs, and other valuable data. The collected data is then encrypted using its custom algorithm and HTML encoded before transmission to the C2 server. Upon receipt of obfuscated data, the C2 server decodes it and may transmit instructions back to Smooth Operator. Smooth Operator decodes any responses from the C2 server and executes them on the victim's system, potentially involving further data exfiltration, lateral movement within the network, or other malicious activities. Potential Impact: Data theft, encompassing user credentials, financial data, and confidential business documents, is a potential consequence. Smooth Operator may also gain control of the victim's network, facilitating further attacks and data breaches. Business disruption, resulting from communication system outages and critical service interruptions, can lead to significant downtime and financial losses. Mitigation: Organizations are advised to: - Update 3CX Software promptly with patches and updates released by 3CX to address known vulnerabilities exploited by Smooth Operator. - Implement Multi-Factor Authentication (MFA) for all user accounts, particularly those with administrative privileges, to enhance security against credential theft. - Harden network security through the implementation of robust firewalls, intrusion detection and prevention systems (IDPS), and network segmentation to limit malware lateral movement and impact. - Conduct security awareness training to educate users about phishing attacks and social engineering tactics employed by attackers to deliver malware such as Smooth Operator.

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 "UpdateAgent" binary, which constitutes the malware's second-stage payload. Upon execution, the "UpdateAgent" binary is immediately deleted from the storage medium. This action is intended to impede threat detection and analysis by eliminating any evidence of its presence on the compromised system.

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: A time-based evasion technique is employed by Smooth Operator to evade detection within virtualized or sandboxed environments. Following execution, the malware enters a dormant state characterized by a minimum sleep duration of seven days (604,800 seconds) prior to attempting communication with its command and control (C2) server. This extended latency period facilitates evasion by security tools that primarily monitor for immediate suspicious activity within a short timeframe. The limited lifespans often inherent in virtualization/sandbox environments further diminish the likelihood of these environments persisting sufficiently long enough for Smooth Operator to reactivate and initiate communication.

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:

- The malware is running on a victim machine.
- The ability to process and format collected data.
- The ability to read data from the SystemVersion.plist file.
- A functioning internet connection.
- The SystemVersion.plist file exists in /System/Library/CoreServices/.

Post-Conditions:

- HTTP GET requests to exfiltration URL
- Beacon communication logs
- New files created (e.g., UpdateAgent)
- System instability
- Cookie header modifications with victim data
- Altered registry settings
- Logs containing suspicious activity
- Network traffic to C2 servers over HTTPS
- Modified system files
- Data theft
- Compromised system
- Potential for further malware infections

Attack Step 4.1

==
Name: Automated Collection as used by the malware
Description: Data is collected from infected victim machines through automated processes implemented by Smooth Operator malware. System details, including operating system and hardware specifications, are extracted alongside information pertaining to running processes and network connections. User credentials and sensitive files are also targeted for acquisition. Specific data related to 3CX systems, such as call logs and configurations, may be gathered. The collected data is subsequently organized and prepared for transmission to the attacker's command and control (C2) server. This staged data may be embedded within beacon messages transmitted periodically to the C2 or transferred through dedicated exfiltration channels. Transmission of the gathered data to the C2 server is facilitated by HTTPS communication, thereby obscuring detection by conventional security measures.

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 is running.
- A system capable of executing the malware code exists.
- A network connection is available.
- HTTPS protocol support is present.
- The malware has a list of C2 servers.
- The malware is running.
- A list of C2 servers is available to the malware.
- The malware has the capability to communicate over a network.
- A C2 server is unreachable.

Post-Conditions:

- Obfuscated data remnants
- Registry entries
- Downloaded files (e.g., icon files)
- Data exfiltration
- Modified cookies
- Exfiltration logs
- .main_storage file with beaconing information
- C2 server logs
- System compromise
- Malware persistence
- Modified system files
- Potential data loss
- Network traffic analysis (HTTPS requests)
- Data exfiltration
- Exfiltrated data files
- Obfuscated C2 communication logs
- Unusual process activity logs
- Malware persistence
- Modified system files
- Compromised systems
- Network traffic to C2 servers and exfiltration URLs

Attack Step 5.1

==
Name: Application Layer Protocol: Web Protocols as used by the malware
Description: C2 communication for the malware is established via the HTTPS protocol. Encrypted connections are utilized for all interactions between the infected machine and the C2 server. This encryption complicates monitoring and interception efforts by security analysts, thereby enhancing the stealthiness of the malware's operations.

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 domain "glcloudservice.com" is accessed.

Attack Step 5.2

==
Name: Fallback Channels as used by the malware
Description: Command and Control (C2) server communication is facilitated by a fallback mechanism employing a predetermined list of servers. During each beacon transmission attempt, a C2 server is randomly selected from this list. A connection attempt is subsequently initiated with the chosen server. Upon successful establishment of the connection, standard communication protocols are executed. In the event of a connection failure, the malware proceeds to the subsequent C2 server on the list and reiterates the selection and connection processes. This iterative procedure persists until a successful connection is realized. This strategy ensures uninterrupted communication with the command center by leveraging alternative servers in the event of unavailability of primary servers.

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:

- The .main_storage file is present.
- A network connection is available.
- The malware has collected victim specific data.
- The malware has access to the internet.
- The malware has successfully infected a target system.

Post-Conditions:

- Network traffic to obfuscated C2 servers.
- Presence of malicious code in memory.
- Registry modifications related to malware execution.
- System instability or performance degradation.
- Increased risk of further attacks.
- Potential compromise of sensitive information.
- Modified system files.
- New log entries indicating suspicious activity.
- Data exfiltration from infected systems.
- Exfiltrated data files on remote servers.

Attack Step 6.1

==

Name: Automated Exfiltration as used by the malware
Description: Automated exfiltration of victim data collected by Smooth Operator is conducted through a separate channel distinct from its primary Command and Control (C2) infrastructure. The specific methodology employed by this distinct channel remains undisclosed. It is evident, however, that the exfiltration process operates independently of the C2 communication channels utilized for other malicious activities.

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.