Enhanced Attack Report

Smooth Operator

Generated on 2025-03-12

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 3CX software is installed on a victim's system.
- Distribution channels used by 3CX to deliver software updates.
- The ability to sign and notarize software packages.
- A malicious version of libffmpeg.dylib exists.

Post-Conditions:

- New files with malicious code
- Data exfiltration
- DNS queries to malicious domains
- Compromised systems
- Potential for further malware deployment
- Encrypted communication logs
- Altered registry entries
- System instability
- Shadow copies of infected files
- Modified system files
- Network traffic to C2 servers
- File access logs indicating suspicious file operations
- Unusual process activity logs
- Reputational damage

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 3CX software development processes. Malicious libraries, disguised as legitimate components, were introduced into the build phase, effectively "trojanizing" the software. Subsequently, the compromised 3CX software, incorporating the Smooth Operator payload, underwent signing by 3CX and notarization by Apple. This process conferred an appearance of authenticity upon the infected software, potentially misleading users into accepting its installation and execution as safe. Distribution of the compromised 3CX software occurred through established channels, indistinguishable from regular updates or installations. Consequently, unsuspecting users downloading and installing the infected software became victims of the attack.

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.
- Smooth Operator malware has been successfully deployed as part of the 3CX software.
- The ability to execute code within the context of the 3CX software process.

Post-Conditions:

- ".main_storage" file containing victim ID and other sensitive information.
- Data exfiltration from infected systems.
- Logs indicating suspicious activity and process executions.
- Files created or modified by the malware.
- Compromised 3CX software installations.
- Modified 3CX software binaries.
- Network traffic to C2 servers, potentially obfuscated.
- Evidence of data transfer to external locations.
- Potential for further malware deployment and lateral movement within the network.
- Loss of system integrity and confidentiality.
- Altered system registry entries.

Attack Step 2.1

===

Name: Compromise Client Software Binary as used by the malware
Description: Smooth Operator malware is analyzed to elucidate its tactics and techniques for system infiltration. Initial access is achieved through a supply chain compromise, wherein compromised 3CX software packages are distributed. This technique leverages trust in established software vendors to facilitate entry into systems. Persistence is maintained by compromising the client software binary. Once installed, Smooth Operator integrates itself into the running 3CX software, enabling persistence across system restarts and potential evasion of security measures. String obfuscation techniques employed by Smooth Operator include character encoding utilizing HTML style encoding to mask potentially suspicious characters within strings. Additionally, array offsets are utilized for string replacement, suggesting a complex mechanism for dynamically constructing and concealing malicious code. Understanding these tactics is crucial for developing effective defenses, contributing to threat intelligence, and guiding malware response efforts.

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 possesses the custom encoding algorithm used to obfuscate the data.
- The malware has successfully infected a target system.
- Exfiltrated data is available to the malware.
- The malware has successfully executed.
- The malware's second stage is active.
- A virtualized or sandboxed environment exists.
- The malware is running in a virtualized or sandboxed environment.
- The malware has access to a timer or clock functionality.

Post-Conditions:

- Data exfiltration
- System compromise
- Modified 3CX Desktop App executable
- Obfuscated data files on affected systems
- Indicators of compromise (IOCs) matching known malware signatures
- Files downloaded from malicious sources
- Backdoors or hidden processes running in memory
- Network connections to malicious C2 servers
- Disruption of communication systems
- Reputational damage
- Unusual system logs and event entries
- Altered registry settings
- Remote access granted to attackers
- Potential financial loss
- Data exfiltration
- System compromise
- Communication disruption
- Deleted log files
- Financial loss
- Modified system files
- New user accounts
- Exfiltrated data files
- C2 server communication logs
- Backdoor executables
- Unusual network traffic
- Reputational damage
- Log entries indicating suspicious activity
- Presence of backdoor executables or scripts
- New registry entries
- Data breaches and exfiltration
- Unusual network traffic to C2 servers
- Evidence of data transfer to external locations
- System instability and performance degradation
- Modified system files (e.g., 3CXDesktopApp.exe, ffmpeg.dll)
- Altered timestamps on critical files

- Disruption of communication channels
- Loss of sensitive information
- Remote code execution vulnerabilities
- Increased risk of further attacks
- Deleted or modified log files

Attack Step 3.1

==
Name: Deobfuscate/Decode Files or Information as used by the malware
Description: Smooth Operator malware is characterized by its sophisticated design and targeting of 3CX communications software. Infection is facilitated through compromised versions of the 3CXDesktopApp, exploiting identified vulnerabilities within trusted software applications. Upon successful intrusion, Smooth Operator establishes persistent connections with a designated Command and Control (C2) server, enabling sustained attacker control even after the initial infection vector is neutralized. Data exfiltration constitutes a primary objective, encompassing sensitive information such as internal communications, user credentials, financial data, and proprietary assets. Custom algorithms are employed to obfuscate both outgoing data transmitted to the C2 server and incoming commands received, thereby complicating analysis and detection by security tools. The ramifications of a successful Smooth Operator attack can be substantial for affected organizations. Data breaches resulting from stolen sensitive information may lead to financial losses, reputational damage, and legal consequences. Compromised systems can serve as launchpads for further attacks targeting other network segments. Threat actors may also exploit compromised systems for espionage purposes, seeking access to intellectual property or confidential information. Mitigation strategies are recommended to minimize the risk of Smooth Operator infection and its associated impacts. These include: regular patching of 3CXDesktopApp and other software to address known vulnerabilities; implementation of robust security monitoring tools to detect anomalous network activity or file modifications; network segmentation to isolate critical systems from less sensitive networks; utilization of Multi-Factor Authentication (MFA) to enhance user account protection; and comprehensive security awareness training for employees to mitigate the risk of phishing attacks and other common security threats.

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 (T1070.004) is a tactic employed by Smooth Operator. The malware's second stage, following initial infection, actively deletes itself from the victim system upon execution. This action hinders detection and investigation efforts by obfuscating evidence that could implicate the malware or its operators.

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 is employed by the "Smooth Operator" malware to circumvent detection within virtualization/sandbox environments. This technique involves a deliberate delay of at least one week prior to establishing communication with the command-and-control (C2) server. This extended latency period potentially enables the malware to evade detection mechanisms inherent in virtualized or sandboxed environments characterized by limited lifespans or automated monitoring protocols. The rationale behind this evasion tactic is to exploit the assumption that malicious software exhibits rapid and aggressive behavior. By delaying its activity, "Smooth Operator" presents a less conspicuous profile, potentially inducing a false sense of security within monitoring systems. Consequently, this evasion technique facilitates the undetected operation of "Smooth Operator" within virtualized or sandboxed environments, thereby impeding analysis and containment efforts.

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:

- A connection to the internet is established.
- Smooth Operator has access to data on the victim machine.
- The malware's custom encoding algorithm is functional.
- HTTPS protocol is available for communication.
- The second-stage payload of Smooth Operator is active.
- A malicious .dmg file containing the Smooth Operator malware has been opened and executed by the user.
- The victim machine is running a 64-bit Intel-based macOS system.

Post-Conditions:

- Data exfiltration
- Command-and-control server connections
- Compromised system functionality
- Increased security risks
- Hidden files and folders
- Altered firewall rules
- Remote access by attackers
- System instability
- Modified system files
- New user accounts
- Data transfer logs
- Unusual network traffic logs
- Backdoor executables
- Registry key modifications

Attack Step 4.1

==
Name: Automated Collection as used by the malware
Description: Automated Collection within the Smooth Operator malware framework involves a multi-stage process. Valuable data is identified on the victim's system through analysis encompassing system specifications, network configurations, and user activity patterns. This collected data is subsequently packaged and transmitted to an attacker-controlled command-and-control (C&C;) server via HTTPS beacons, disguised as legitimate web traffic. Upon receipt, the C&C; server processes the transmitted data for purposes such as intelligence gathering, lateral movement within compromised networks, and potential data theft. Organizations can mitigate the impact of Smooth Operator through a comprehensive security posture. This includes the implementation of regular software patching procedures, multi-factor authentication for critical accounts, robust network security monitoring systems, and advanced endpoint protection solutions with real-time threat detection capabilities. Furthermore, security awareness training programs are essential to educate employees regarding phishing attacks, social engineering tactics, and best practices for password management and multi-factor authentication. Data Loss Prevention (DLP) solutions can be deployed to monitor and control the movement of sensitive data within and outside organizational networks.

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:

- A victim machine infected with the Smooth Operator malware.
- A functioning web browser or related software on the victim machine capable of establishing HTTPS connections.
- The malware is present on a victim machine.
- The victim machine's web browser or related software is configured to allow communication with the C2 server.
- The victim machine has an active internet connection.
- A C2 server is unreachable.
- The malware is running.
- A list of C2 servers is embedded within the malware.
- The beacon error count exceeds a threshold.
- The malware can establish HTTPS connections.

Post-Conditions:

- Data exfiltration
- Network communication with malicious servers
- Unusual process activity in system logs
- Compromised system
- Malware persistence
- New files created by malware
- Modified system files
- Network traffic logs showing communication with C2 servers
- Registry entries added by malware
- Exfiltrated data on remote servers

Attack Step 5.1

==
Name: Application Layer Protocol: Web Protocols as used by the malware
Description: The malware's command and control (C2) communication is conducted via HTTPS, an Application Layer Protocol. Communication with the C2 server is established utilizing standard web protocols, such as HTTP, with encryption implemented to enhance security and obfuscate malicious activity.

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 are employed by Smooth Operator through the utilization of a plurality of Command & Control (C2) servers. During communication establishment, a random selection of a server from this enumerated list is performed for each beacon transmission. This methodology contributes to persistence by mitigating the impact of potential unavailability of one or more C2 servers resulting from takedowns or network disruptions.

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 malware has successfully infected a target machine.
- The malware has access to the collected data.
- Data has been collected from the victim machine.
- A network connection is available to the C2 server.

Post-Conditions:

- Data theft from compromised systems.
- Exfiltrated data files containing sensitive information.
- Unusual process creation and execution patterns in system logs.
- Altered registry settings reflecting malware presence.
- Presence of obfuscated or encoded strings within compromised files.
- Increased security vulnerabilities in the targeted environment.
- New log entries indicating suspicious activity.
- Potential financial losses due to data breaches.
- Disruption of communication and business operations.
- Network traffic to command-and-control servers.
- Reputational damage for affected organizations.
- Modified system files with malicious code.

Attack Step 6.1

==
Name: Automated Exfiltration as used by the malware
Description: Automated exfiltration is characterized by the clandestine transfer of sensitive data from compromised systems to remote servers, orchestrated without direct human intervention. Malware employed in this process is designed to autonomously: - Identify valuable data assets, encompassing financial records, personal information, intellectual property, and other sensitive files targeted by the attacker. - Extract the identified data utilizing various techniques for copying and packaging. - Select an exfiltration method, commonly including direct upload to attacker-controlled servers, embedding within seemingly innocuous email attachments, or leveraging encrypted communication channels to obfuscate data transfer. Persistence mechanisms, such as scheduled tasks or system service hijacking, may be implemented by the malware to ensure continuous data exfiltration even after initial detection attempts.

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.