Contagious Interview, DeceptiveDevelopment, Gwisin Gang, Tenacious Pungsan, DEV#POPPER, PurpleBravo, TAG-121, Group G1052

Archived: 2026-04-05 14:00:59 UTC

Enterprise T1583 Acquire Infrastructure

Contagious Interview has used services such as Astrill VPN.[9][4]

.001 Domains

Contagious Interview has registered domains to leverage in their social engineering campaigns.[4][5][8] Contagious Interview has also registered domains to utilize for C2.[9][12][1][13][14][15]

.003 Virtual Private Server

Contagious Interview has acquired virtual private servers from services such as Stark Industries Solutions and RouterHosting.[2][7] Contagious Interview has also utilized hosting providers to include Tier[.]Net, Majestic Hosting, Leaseweb Singapore, and Kaopu Cloud.[4]

.006 Web Services

Contagious Interview has used web services such as Dropbox to receive stolen data and Google Drive, Firebase, GitHub, and Telegram to disseminate files.[12][4] Contagious Interview has also used a cloud platform such as Vercel for C2 operations leveraging malicious web applications and static pages.[13][14][15] Contagious Interview has also used Slack to coordinate their activities.[9]

Enterprise T1071 .003 Application Layer Protocol: Mail Protocols

Contagious Interview has utilized email notifications from malware distribution servers to track victim engagement.[9]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Contagious Interview has established persistence using InvisibleFerret malware to place a .bat file in the Startup Folder.[6]

.013 Boot or Logon Autostart Execution: XDG Autostart Entries

Contagious Interview has established persistence using InvisibleFerret malware to create a .desktop entry to run on startup on GNOME-based Linux devices.[6]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Contagious Interview has utilized VBS scripts to open cmd.exe and run commands to include the go_batch.bat batch file.[12]

.004 Command and Scripting Interpreter: Unix Shell

Contagious Interview has targeted macOS victim hosts using a bash downloader coremedia.sh and a bash script cloud.sh.[12]

.005 Command and Scripting Interpreter: Visual Basic

Contagious Interview has utilized Visual Basic scripts in the execution of their downloader malware targeting Windows devices including as script called update.vbs.[12]

.006 Command and Scripting Interpreter: Python

Contagious Interview has used the Python-based malware such as InvisibleFerret to install and execute Python Packages and Python modules.[2][5][7]

.007 Command and Scripting Interpreter: JavaScript

Contagious Interview has leveraged JavaScript in the execution of their downloader malware targeting Windows devices using a NodeJS script titled nvidia.js.[12]

Enterprise T1543 .001 Create or Modify System Process: Launch Agent

Contagious Interview has established persistence using InvisibleFerret malware to create file to run the script on Startup via LaunchAgents.[6] Contagious Interview has also utilized a plist file located in `/Library/LaunchAgents` to enable a malicious bash script the ability to persist.[12]

Enterprise T1555 .001 Credentials from Password Stores: Keychain

Contagious Interview has leveraged malware variants configured to dump credentials from the macOS keychain.[12][14][15]

Enterprise T1587 Develop Capabilities

Contagious Interview developed malicious NPM packages for delivery to or retrieval by victims.[9][1][2][13][14][15][7]

.001 Malware

Contagious Interview has developed malware that utilizes Qt cross-platform framework to include BeaverTail.[5][8]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Contagious Interview has encrypted C2 traffic using RC4.[12]

Enterprise T1585 Establish Accounts

Contagious Interview has created and maintained personas on code repositories to distribute malicious payloads.[9][1][13][14][15][5]

.001 Social Media Accounts

Contagious Interview has created fake social media accounts such as LinkedIn and Telegram accounts for their targeting efforts.[4][5][16][17][8][6]

.002 Email Accounts

Contagious Interview has created fake email accounts to correspond with social media accounts, fake LinkedIn personas, code repository accounts, and job announcements on development job board services.[9][4][15][5][6][8] Contagious Interview has also utilized fake email accounts with Threat Intelligence vendor services.[9]

Enterprise T1546 .004 Event Triggered Execution: Unix Shell Configuration Modification

Contagious Interview has targeted macOS victim hosts using a bash downloader `coremedia.sh` and a bash script `cloud.sh`.[12]

Enterprise T1480 Execution Guardrails

Contagious Interview has configured C2 endpoints to review IP geolocation, request headers, victim environment details and runtime conditions prior to delivering payloads.[15]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

Contagious Interview has exfiltrated victim information using FTP.[5][7][8]

Enterprise T1041 Exfiltration Over C2 Channel

Contagious Interview has exfiltrated data from a compromised host to actor-controlled C2 servers.[9][2][4][13][14][15][5][16][7][8]

Enterprise T1567 Exfiltration Over Web Service

Contagious Interview has leveraged Telegram API to exfiltrate stolen data.[5]

.002 Exfiltration to Cloud Storage

Contagious Interview has exfiltrated stolen passwords to Dropbox.[12]

Enterprise T1083 File and Directory Discovery

Contagious Interview has conducted key word searches within files and directories on a compromised hosts to identify files for exfiltration.[5][7]

Enterprise T1657 Financial Theft

Contagious Interview has stolen cryptocurrency wallet credentials and credit card information utilizing BeaverTail and InvisibleFerret malware.[2][14][15][5][6][7][8]

Enterprise T1589 Gather Victim Identity Information

Contagious Interview has researched specific professional groups such as software developers for targeting.[15][16][11][17][7][8] Contagious Interview has also researched individuals who work in roles related to cryptocurrency and blockchain technologies.[9][12]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Contagious Interview has convinced victims to disable Docker and other container environments and run code on their machine natively in attempts to bypass container isolation and ensure device infection.[15]

Enterprise T1656 Impersonation

Contagious Interview had impersonated HR hiring personnel through social media, job board notifications, and conducted interviews with victims in order to entice them to download malware disguised as legitimate applications or malicious scripts from code repositories.[9][1][15][16][11][17][7][8]

Enterprise T1070 .004 Indicator Removal: File Deletion

Contagious Interview has configured malware to remove archives used in collection activities following successful exfiltration.[14]

Enterprise T1036 Masquerading

Contagious Interview has delivered BeaverTail malware masquerading as legitimate software or applications.[2][5][6][7][8] Contagious Interview has also delivered malicious payloads masquerading as legitimate software drivers.[12]

Enterprise T1571 Non-Standard Port

Contagious Interview has used TCP port 1224 for C2.[13]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Contagious Interview has obfuscated JavaScript code using Base64 and variable substitutions.[5][16][11][6]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Contagious Interview has used hexadecimal string encoding to hide critical JavaScript module names, function names, and C2 URLs, which are decoded dynamically at runtime.[13]

Enterprise T1588 .002 Obtain Capabilities: Tool

Contagious Interview has used remote management and monitoring software such as "AnyDesk".[2][5][16][7][8]

.007 Obtain Capabilities: Artificial Intelligence

Contagious Interview has appeared to have used AI to generate images and content to facilitate their campaigns.[4]

Enterprise T1566 .003 Phishing: Spearphishing via Service

Contagious Interview has used fake job advertisements and messages sent via social media to spearphish targets.[12][1][4][5][16][17] Contagious Interview has also leveraged hiring websites to solicit victims.[4]

Enterprise T1090 Proxy

Contagious Interview has leveraged Astrill VPN for C2.[4]

Enterprise T1219 .002 Remote Access Tools: Remote Desktop Software

Contagious Interview has downloaded remote management and monitoring software such as "AnyDesk" for post compromise activities.[2][5][16][7][8]

Enterprise T1593 Search Open Websites/Domains

Contagious Interview has utilized open-source indicator of compromise repositories to determine their exposure to include VirusTotal, and MalTrail.[9]

.001 Social Media

Contagious Interview had identified and solicited victims through social media such as LinkedIn, X, and Telegram.[12][1][16][17][7][8]

.003 Code Repositories

Contagious Interview had identified and solicited victims through code repositories such as GitHub.[7]

Enterprise T1681 Search Threat Vendor Data

Contagious Interview has registered accounts with Threat Intelligence vendor services to check for reporting associated with their infrastructure and to evaluate new potential infrastructure.[9]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

Contagious Interview has hosted malicious payloads on code repositories used as lures for victims to download.[9][1][2][4][13][14][15][5][16][11][6][7]

Enterprise T1082 System Information Discovery

Contagious Interview has configured malicious webpages to identify the victim’s operating system by reviewing the details of the victims User-Agent of their browser.[12]

Enterprise T1204 .001 User Execution: Malicious Link

Contagious Interview has lured victims to click on a malicious link that led to download of a malicious payload.[4] Contagious Interview has also leveraged links to malicious payloads on social media and code repositories.[4]

.002 User Execution: Malicious File

Contagious Interview has distributed malicious files requiring direct victim interaction to execute through the guise of a code test.[16][17]

.004 User Execution: Malicious Copy and Paste

Contagious Interview has leveraged ClickFix type tactics enticing victims to copy and paste malicious code.[9][12][1]

.005 User Execution: Malicious Library

Contagious Interview has relied on users to install a malicious library from a code repository to infect the victim's device and has led to additional payload distribution and theft of sensitive data.[9][1][2][13][14][15][5][11][6][7]

Enterprise T1497 Virtualization/Sandbox Evasion

Contagious Interview has requested victims to disable Docker and other container environments in attempts to thwart container isolation and ensure device infection.[15]
