blackpoint

THREAT PROFILE:

Cuba Ransomware

Table of Contents

Executive Summary

First Identified:
2019

Operation style:
Ransomware-as-a-Service (RaaS)

Extortion method:
Double extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

Most frequently targeted industry:
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- Tropical Scorpius
- Industrial Spy Ransomware
- UNC2595
- V for Vendetta

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, exploit external remote services, vulnerability exploitation, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1566)

Valid accounts, creating new accounts, account manipulation, create/modify system process, event triggered execution, boot or logon autostart execution (MITRE ATT&CK: T1078, T1098, T1136, T1543, T1546, T1547)

Exploitation of remote services, RDP, Lateral Tool Transfer (MITRE ATT&CK: T1021, T1563, T1570)

Description

Cuba ransomware was first discovered in 2019, making it one of the longest running ransomware-as-a-service (RaaS) operations. Cuba operators use the double extortion method, where victims' data is stolen and leaked via a data leak site or sold if the ransom demand is not paid.

Cuba ransomware is widely believed to be operated by a threat group, Tropical Scorpius, and has used aliases including COLDDRAW and Fidel. Despite the Cuba references, both on the data leak site and naming conventions, it is assessed that Cuba operators are likely based in Russia due to linguistic translations within the malware. However, as the group operates a RaaS, affiliates are likely located worldwide.

Cuba affiliates have been observed gaining initial access via social engineering attacks, exploit kits, valid accounts with weak or purchased credentials, and IABs. Due to the use of affiliates, there is likely a wide array of methods used to gain initial access to victims.

The group has made use of both publicly available and custom malware variants, including RomCom and Qakbot. Cuba has consistently updated their malware and tooling, which has likely aided in the group remaining active for more than four years. While they change tooling and adopt different publicly available tooling, their core TTPs appear to remain relatively consistent over the previous four years, including the use of LOLBins, exploits, and frequently observed use of Cobalt Strike and Metasploit.

Despite the Cuba references it is assessed that Cuba operators are likely based in Russia.

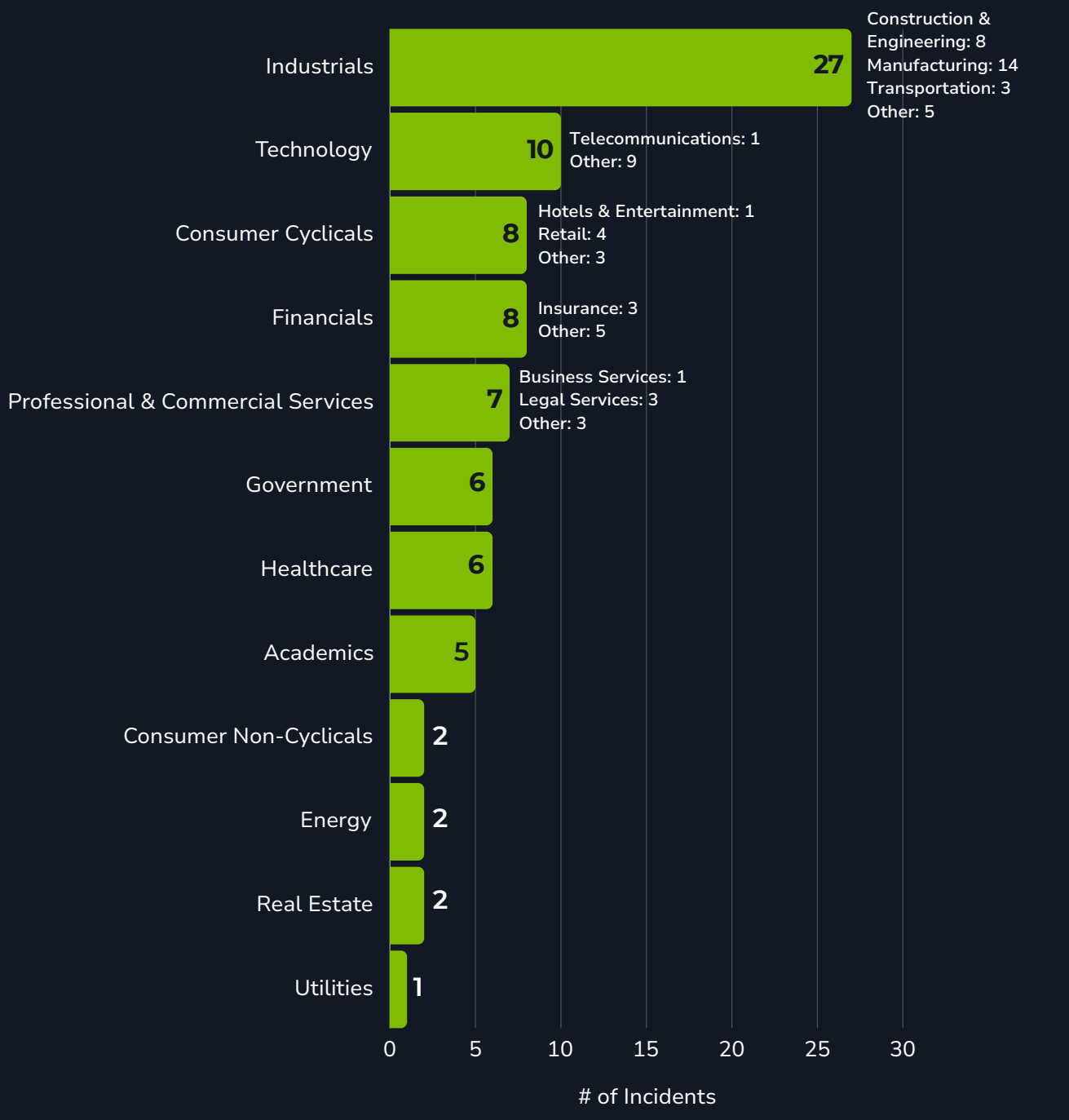
In 2022, the Cuba operators appeared to partner with the operators of Industrial Spy ransomware. Victims that were encrypted with the Cuba ransomware were observed listed for sale on the Industrial Spy ransomware marketplace side. Additionally, another site "V for Vendetta" emerged that was hosted on the Cuba domain, indicating that the groups were related or that Cuba was attempting to rebrand.

Cuba ransomware encrypted data using the Xsalsa20 symmetric algorithm, and the encryption key with the RSA-2048 symmetric algorithm. Other versions of the malware encrypted data using the symmetric encryption algorithm ChaCha20 and the asymmetric encryption algorithm RSA to protect the ChaCha20 Key and Initialization Vector (IV). The ransomware searches for and encrypts Microsoft Office documents, images, archives, and others in the %AppData%\Microsoft\Windows\Recent\ directory rather than all files on the devices. Additionally, the malware terminates all SQL services to encrypt any available databases.

Analysis of Bitcoin wallets attributed to the Cuba operators identified more than 3,600 BTC (approximately 103,000,000 at the time of identification). The group reportedly consistently transfer funds between multiple wallets, utilizes bitcoin mixers, and conducts anonymous transactions in an attempt to make the funds harder to track.

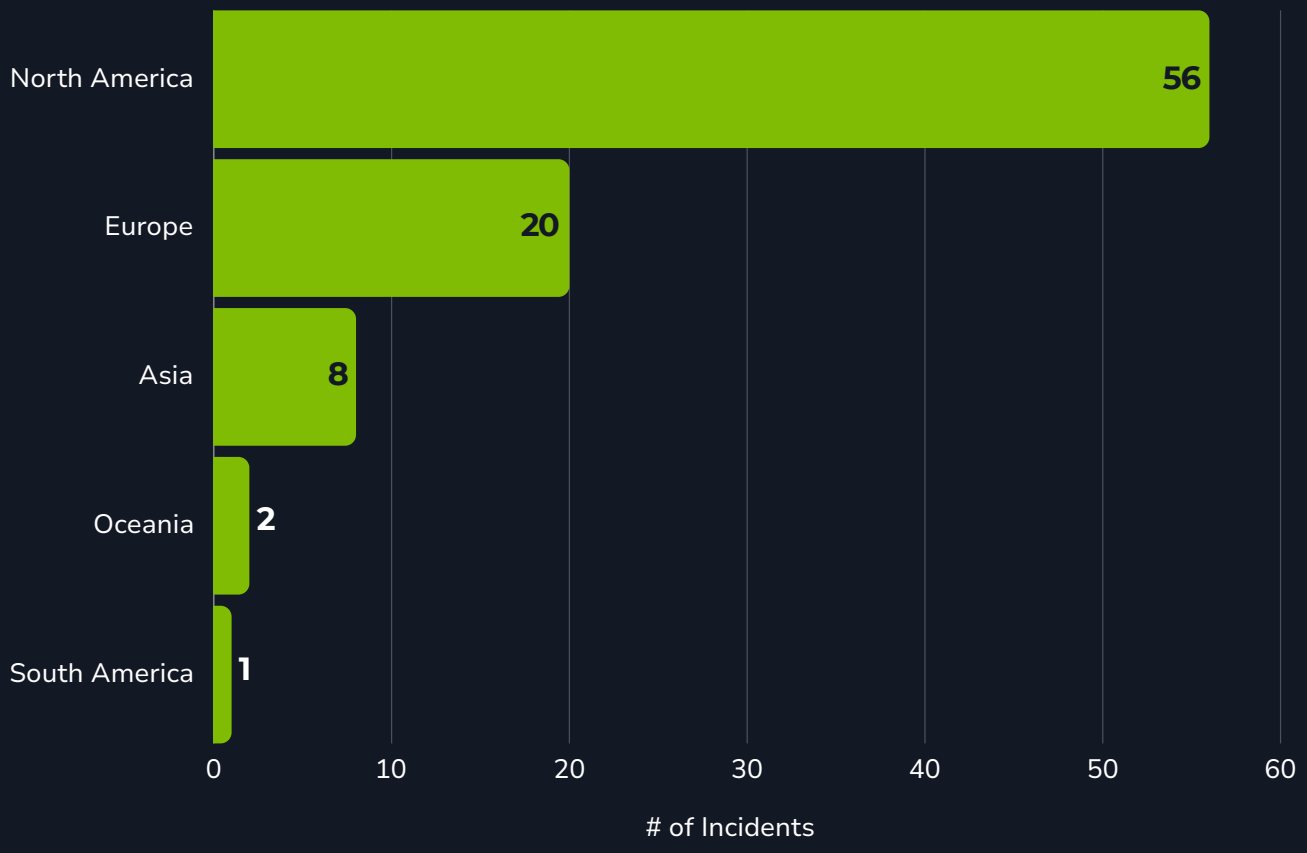
Previous Targets: Cuba

Previous Industry Targets

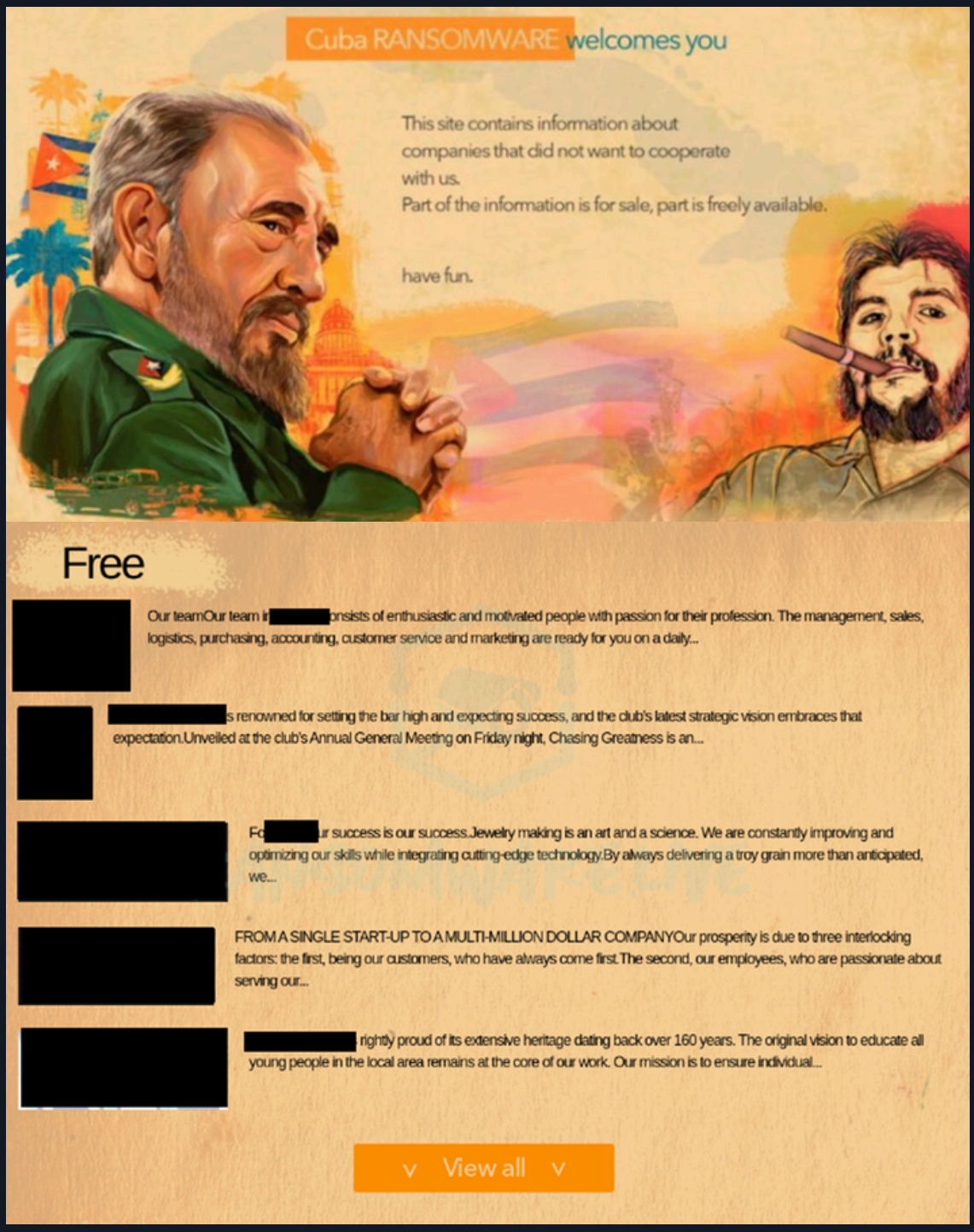


Previous Targets: Cuba

Previous Victim HQ Regions



Data Leak Site: Cuba



hxxp://cuba4ikm4jakjgmkezytyawtdgr2xymvy6nvzgw5cglswg3si76icnqd[.]onion/
hxxp://cuba4mp6ximo2zlo[.]onion/

Known Exploited Vulnerabilities

CVE-2022-24521 (CVSS: 7.8)

Privilege Escalation Vulnerability
Product Affected: Windows Common Log File System Driver

CVE-2022-26500 (CVSS: 8.8)

RCE Vulnerability
Product Affected: Veeam Backup & Replication

CVE-2022-26501 (CVSS: 9.8)

RCE Vulnerability
Product Affected: Veeam Backup & Replication

CVE-2022-26504 (CVSS: 8.8)

RCE Vulnerability
Product Affected: Veeam Backup & Replication

CVE-2022-26522 (CVSS: N/A)

Privilege Escalation Vulnerability
Product Affected: Avast Anti Rootkit Driver

CVE-2022-26523 (CVSS: N/A)

Privilege Escalation Vulnerability
Product Affected: Avast Anti Rootkit Driver

CVE-2023-27532 (CVSS: 7.5)

Missing Authentication for Critical Function Vulnerability
Product Affected: Veeam Backup & Replication Cloud Connect

Known Exploited Vulnerabilities

OWASSRF (CVE-2022-41080) (CVSS: 9.8)

SSRF Vulnerability
Product Affected: Microsoft Exchange

ProxyLogon (CVE-2021-26855) (CVSS: 9.8)

RCE Vulnerability
Product Affected: Microsoft Exchange

ProxyShell (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) (CVSS: 9.8, 9.8, 7.2)

Pre-Auth Path Confusion, Privilege Escalation, Post-Auth RCE Vulnerabilities
Product Affected: Microsoft Exchange

ZeroLogon (CVE-2020-1472) (CVSS: 10)

Privilege Escalation Vulnerability
Product Affected: Netlogon

Associations: Cuba

COLDDRAW

The name of Cuba ransomware's encryptor malware and an alias for the Cuba operation.

Fidel

An alias used by the Cuba ransomware operation.

Tropical Scorpius

Tropical Scorpius is believed to be the operators behind the Cuba ransomware operation.

Industrial Spy Ransomware

Industrial Spy has been tied to the Cuba ransomware operation and Tropical Scorpius based on the similarities in their ransom notes, which included identical contact information. Additionally, victims with encrypted files containing the ".cuba" extension were observed being posted for sale on the Industrial Spy ransomware marketplace.

UNC2595

A purported affiliate of the Cuba ransomware operation.

V for Vendetta

V for Vendetta's data leak was hosted on the Cuba ransomware domain, indicating that the groups were likely connected. There is an even chance that Cuba was testing or attempting to rebrand.

Known Tools: Cuba

AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Bughatch	A downloader that executes arbitrary code on the compromised system downloaded from a C2 server. The malware has been loaded in-memory by a dropper written in PowerShell or loaded by a PowerShell script from a remote URL.
Burnt Cigar	A utility observed in November 2021 that terminates processes associated with endpoint security software to allow ransomware and other tools to execute without detection.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
ColdDraw	The name given to the Cuba ransomware encryptor. When executed it terminates services associated with common server applications an encrypts files on the local filesystem and attached network drives.
Ficker Stealer	An information stealing malware that can collect sensitive information including login credentials, payment card information, cryptocurrency wallets, and browser information.
GoToAssist	A cloud-based remote support platform designed and targeted at IT support teams and customer support organizations.
Hancitor	AKA Chanitor, Tordal. A downloader that is capable of establishing persistence, execute commands, delete files, and download additional payloads to compromised devices.
Impacket	An open-source collection of modules written in Python for programmatically constructing and manipulating network protocols.
IOBit Unlocker	A tool to unlock files/folders used by another program or user.

Known Tools: Cuba

KerberCache	A tool used to extract cached Kerberos tickets from a host's Local Security Authority Server Service (LSASS) memory.
LongFall	AKA CryptOne. A packer that is composed of multiple stages of execution and attempts to evade detection by subverting static analysis, reducing the entropy of the data, and confusing disassembly algorithms.
LSASS	A Windows process that takes care of security policy for the OS.
Meterpreter	Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
NetScan	A utility that scans within a subnet or IP range to check for devices.
NetSupport RAT	A Windows-centric cross-platform remote control software, allowing remote screen control and systems management from a Windows or Windows Mobile device of Windows, Mac, Linux, Solaris and Mobile devices.
Ping	A tool used to test whether a particular host is reachable across an IP network.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PsExec	A utility tool that allows users to control a computer from a remote location.
Qakbot	A malware that steals sensitive information that has been used to deploy additional malware payloads, including ransomware.

Known Tools: Cuba

RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
RomCom	A backdoor malware that has been used by multiple threat groups, both APT and cybercriminal, to establish remote access to victim environments and deploy additional malware payloads.
SystemBC	AKA Coroxy. A malware written in C that turns infected computers into SOCKS5 proxies.
Termite	A password protected memory-only dropper that contains an encrypted shellcode payload.
Veeamp	A custom Veeam password dumper written in Microsoft .NET - used to collect Veeam credentials.
Wedgecut	A reconnaissance tool that takes an argument containing a list of hosts or IP addresses and checks whether they are online using ICMP packets.
Wicker	A credential stealing malware that can be used to collect credentials from a compromise machine allowing the threat actor to move laterally and elevate privileges. The malware has been used by multiple threat groups and has historically been available for purchase on cybercriminal forums.
ZenPak	A trojan malware that bears similarities to the Bazar malware family. The malware has been used to deploy additional tools.

Observed Cuba Behaviors: Windows

Execution	cmd.exe /c cmd.exe /c copy Rundll32.exe c:\windows\temp\komar.dll,ClearMyTracksByProcess 11985756
Persistence	sc create ApcHelper binPath= %SYSTEMROOT%\system\ApcHelper.sys type=kernel OpenService ChangeServiceConfig
Privilege Escalation	Invoke-WebRequest SeDebugPrivilege AdjustTokenPrivileges
Defense Evasion	cmd.exe /c del NetShareEnum QueryServiceStatusEx
Credential Access	GetKeyState VkKeyScan
Discovery	GetIpNetTable GetKeyboardLayoutList PsLookupThreadByThreadId

MITRE ATT&CK® Mappings: Cuba

Reconnaissance	
T1589: Gather Victim Identity Information	.001: Credentials
T1595: Active Scanning	.002: Vulnerability Scanning
Resource Development	
T1583: Acquire Infrastructure	.003: Virtual Private Server
T1584: Compromise Infrastructure	.001: Domains
T1587: Develop Capabilities	.003: Digital Certificates
T1588: Obtain Capabilities	.003: Code Signing Certificates
T1608: Stage Capabilities	.001: Upload Malware .002: Upload Tool .003: Install Digital Certificate .005: Link Target
Initial Access	
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link

MITRE ATT&CK® Mappings: Cuba

Execution	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Shell Command
T1078: Valid Accounts	
T1106: Native API	
T1129: Shared Modules	
T1204: User Execution	.002: Malicious File
T1569: System Services	.002: Service Execution
Persistence	
T1078: Valid Accounts	.002: Domain Accounts .003: Local Accounts
T1098: Account Manipulation	
T1136: Create Account	.001: Local Account
T1543: Create or Modify System Process	.003: Windows Service
T1546: Event Triggered Execution	.013: PowerShell Profile
T1547: Boot or Logon Autostart Execution	

MITRE ATT&CK® Mappings: Cuba

Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1134: Access Token Manipulation	
Defense Evasion	
T1014: Rootkit	
T1027: Obfuscated Files or Information	.002: Software Packing
T1036: Masquerading	.005: Match Legitimate Name or Location
T1055: Process Injection	.003: Threat Execution Hijacking .012: Process Hollowing
T1070: Indicator Removal	.004: File Deletion
T1112: Modify Registry	
T1134: Access Token Manipulation	.001: Token Impersonation/Theft
T1140: Deobfuscate/Decode Files or Information	
T1211: Exploitation for Defense Evasion	
T1218: System Binary Proxy Execution	.011: Rundll32
T1480: Execution Guardrails	
T1497: Virtualization/Sandbox Evasion	.001: System Checks
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control

MITRE ATT&CK® Mappings: Cuba

Defense Evasion	
T1553: Subvert Trust Controls	.002: Code Signing
T1562: Impair Defenses	.001: Disable or Modify Tools .002: Disable Windows Event Logging
T1564: Hide Artifacts	.002: Hidden Users .003: Hidden Window
T1574: Hijack Execution Flow	.011: Services Registry Permissions Weakness
T1620: Reflective Code Loading	
Credential Access	
T1003: OS Credential Access	.001: LSASS Memory
T1056: Input Capture	.001: Keylogging
T1110: Brute Force	.001: Password Guessing
T1212: Exploitation for Credential Access	
T1555: Credentials from Password Stores	.003: Credentials from Web Browsers
T1558: Steal or Forge Kerberos Tickets	.003: Kerberoasting
Discovery	
T1007: System Service Discovery	
T1010: Application Window Discovery	
T1012: Query Discovery	

MITRE ATT&CK® Mappings: Cuba

Discovery	
T1016: System Network Configuration Discovery	.002: Internet Connection Discovery
T1018: Remote System Discovery	
T1033: System Owner/User Discovery	
T1049: System Network Connection Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	
T1124: System Time Discovery	
T1135: Network Share Discovery	
T1518: Software Discovery	
T1614: System Location Discovery	.001: System Language Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .004: SSH
T1563: Remote Service Session Hijacking	.002: RDP Hijacking
T1570: Lateral Tool Transfer	

MITRE ATT&CK® Mappings: Cuba

Collection	
T1056: Input Capture	.001: Keylogging
T1074: Data Staged	.002: Remote Data Signing
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols .004: DNS
T1090: Proxy	.003: Multi-hop Proxy
T1095: Non-Application Layer Protocol	
T1005: Data from Local System	
T1219: Remote Access Software	
T1572: Protocol Tunneling	
T1573: Encrypted Channel	.002: Asymmetric Cryptography
Exfiltration	
T1041: Exfiltration Over C2 Channel	
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1657: Financial Theft	

References

- Avertium (2023, May 31) “AN IN-DEPTH LOOK AT CUBA RANSOMWARE.” https://explore.avertium.com/resource/an-in-depth-look-at-cuba-ransomware
- Bitam, Salim (2023, February 13) Elastic: “CUBA Ransomware Malware Analysis.” https://www.elastic.co/security-labs/cuba-ransomware-malware-analysis
- CISA (2023, January 05) “#StopRansomware: Cuba Ransomware.” https://www.cisa.gov/newsevents/cybersecurity-advisories/aa22-335a
- ETDA (2024, January 17) “Tool: Cuba.” https://apt.etda.or.th/cgi-bin/listgroups.cgi?t=Cuba&n=1
- FBI (2021, December 02) “Indicators of Compromise Associated with Cuba Ransomware.” https://www.ic3.gov/Media/News/2021/211203-2.pdf
- Galiette, Anthony; Bunce, Daniel; Santos, Doel; Westfall, Shawn (2022, August 09) Palo Alto: “Novel News on Cuba Ransomware: Greetings From Tropical Scorpius.” https://unit42.paloaltonetworks.com/cubaransomware-tropical-scorpius/
- Kirichenko, Alexander; Ivanov, Gleb (2023, September 11) Securelist: “From Caribbean shores to your devices: analyzing Cuba ransomware.” https://securelist.com/cuba-ransomware/110533/
- McLellan, Tyler; Shilko, Joshua; Sadayappan, Shambavi (2022, February 23) Mandiant: “(Ex)Change of Pace: UNC2596 Observed Leveraging Vulnerabilities to Deploy Cuba Ransomware.” https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware
- MITRE (2021, October 12) “Cuba.” https://attack.mitre.org/software/S0625/
- Raj, Aravind (n.d.) Quick Heal: “The Cuba Ransomware.” https://www.quickheal.co.in/documents/technical-paper/cubaransomware.pdf
- SOCRadar (2022, March 03) “Dark Web Threat Profile: Cuba Ransomware Group.” https://socradar.io/dark-web-threat-profile-cuba-ransomware-group/
- Swagler, Chris (2023, October 30) Speartip: “Cuba Ransomware Group’s Latest Malware: A Stealthy Threat to Global Organizations.” https://www.speartip.com/cuba-ransomware-malware-a-threat-to-organizations/
- The BlackBerry Research & Intelligence Team (2023, August 17) “Cuba Ransomware Deploys New
- Tools: BlackBerry Discovers Targets Including Critical Infrastructure Sector in the U.S. and IT Integrator in Latin America.” https://blogs.blackberry.com/en/2023/08/cuba-ransomware-deploys-new-toolstargets-critical-infrastructure-sector-in-the-usa-and-it-integrator-in-latin-america
- Trend Micro Research (2022, December 07) “Ransomware Spotlight: Cuba.” https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-cuba

Adversary Pursuit Group

blackpoint