

Cinnamon Tempest, DEV-0401, Emperor Dragonfly, BRONZE STARLIGHT, Group G1021

 attack.mitre.org/groups/G1021/

Cinnamon Tempest

[Cinnamon Tempest](#) is a China-based threat group that has been active since at least 2021 deploying multiple strains of ransomware based on the leaked [Babuk](#) source code. [Cinnamon Tempest](#) does not operate their ransomware on an affiliate model or purchase access but appears to act independently in all stages of the attack lifecycle. Based on victimology, the short lifespan of each ransomware variant, and use of malware attributed to government-sponsored threat groups, [Cinnamon Tempest](#) may be motivated by intellectual property theft or cyberespionage rather than financial gain. ^{[1][2][3][4]}

ID: G1021



Associated Groups: DEV-0401, Emperor Dragonfly, BRONZE STARLIGHT

Version: 1.0

Created: 06 December 2023

Last Modified: 04 April 2024

[Version Permalink](#)
[Live Version](#)

Associated Group Descriptions

Name	Description
------	-------------

Name	Description
DEV-0401	[2]
Emperor Dragonfly	[5]
BRONZE STARLIGHT	[6]

Techniques Used

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Cinnamon Tempest has used PowerShell to communicate with C2, download files, and execute reconnaissance commands. [5]
		.003	Command and Scripting Interpreter: Windows Command Shell	Cinnamon Tempest has executed ransomware using batch scripts deployed via GPO. [1]
		.006	Command and Scripting Interpreter: Python	Cinnamon Tempest has used a customized version of the Impacket wmiexec.py module to create renamed output files. [1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Cinnamon Tempest has created system services to establish persistence for deployed tooling. [5]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Cinnamon Tempest has used weaponized DLLs to load and decrypt payloads. [5]
Enterprise	T1484	.001	Domain or Tenant Policy Modification: Group Policy Modification	Cinnamon Tempest has used Group Policy to deploy batch scripts for ransomware deployment. [1]

Domain	ID		Name	Use
Enterprise	T1567	.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Cinnamon Tempest has uploaded captured keystroke logs to the Alibaba Cloud Object Storage Service, Aliyun OSS. ^[5]
Enterprise	T1190		Exploit Public-Facing Application	Cinnamon Tempest has exploited multiple unpatched vulnerabilities for initial access including vulnerabilities in Microsoft Exchange, Manage Engine AdSelfService Plus, Confluence, and Log4j. ^{[1][7][5][4]}
Enterprise	T1657		Financial Theft	Cinnamon Tempest has maintained leak sites for exfiltrated data in attempt to extort victims into paying a ransom. ^[1]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Cinnamon Tempest has used search order hijacking to launch Cobalt Strike Beacons. ^{[1][4]} Cinnamon Tempest has also abused legitimate executables to side-load weaponized DLLs. ^[5]
Enterprise	T1105		Ingress Tool Transfer	Cinnamon Tempest has downloaded files, including Cobalt Strike , to compromised hosts. ^[5]
Enterprise	T1588	.002	Obtain Capabilities: Tool	Cinnamon Tempest has used open-source tools including customized versions of the lox proxy tool, NPS tunneling tool, Meterpreter, and a keylogger that uploads data to Alibaba cloud storage. ^{[5][4]}
Enterprise	T1572		Protocol Tunneling	Cinnamon Tempest has used the lox and NPS proxy and tunneling tools in combination create multiple connections through a single tunnel. ^[5]
Enterprise	T1090		Proxy	Cinnamon Tempest has used a customized version of the lox port-forwarding and proxy tool. ^[5]

Domain	ID		Name	Use
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	Cinnamon Tempest has used SMBexec for lateral movement. ^[5]
Enterprise	T1080		Taint Shared Content	Cinnamon Tempest has deployed ransomware from a batch file in a network share. ^[1]
Enterprise	T1078		Valid Accounts	Cinnamon Tempest has used compromised user accounts to deploy payloads and create system services. ^[5]
		.002	Domain Accounts	Cinnamon Tempest has obtained highly privileged credentials such as domain administrator in order to deploy malware. ^[1]
Enterprise	T1047		Windows Management Instrumentation	Cinnamon Tempest has used Impacket for lateral movement via WMI. ^{[1][5]}

Software

ID	Name	References	Techniques
S1096	Cheerscrypt	^{[5][3]}	Command and Scripting Interpreter: Hypervisor CLI , Data Encrypted for Impact , File and Directory Discovery , Service Stop , Virtual Machine Discovery
S0154	Cobalt Strike	^{[1][6]}	Abuse Elevation Control Mechanism: Sudo and Sudo Caching , Abuse Elevation Control Mechanism: Bypass User Account Control , Access Token Manipulation: Parent PID Spoofing , Access Token Manipulation: Token Impersonation/Theft , Access Token Manipulation: Make and Impersonate Token , Account Discovery: Domain Account , Application Layer Protocol: DNS , Application Layer Protocol: Web Protocols , Application Layer Protocol: File Transfer Protocols , BITS Jobs , Browser Session Hijacking , Command and Scripting Interpreter: JavaScript , Command and Scripting Interpreter: Visual Basic , Command and Scripting Interpreter: PowerShell , Command and Scripting Interpreter: Python , Command and

ID	Name	References	Techniques
			Scripting Interpreter: Windows Command Shell , Create or Modify System Process: Windows Service , Data Encoding: Standard Encoding , Data from Local System , Data Obfuscation: Protocol or Service Impersonation , Data Transfer Size Limits , Deobfuscate/Decode Files or Information , Encrypted Channel: Asymmetric Cryptography , Encrypted Channel: Symmetric Cryptography , Exploitation for Client Execution , Exploitation for Privilege Escalation , File and Directory Discovery , Hide Artifacts: Process Argument Spoofing , Impair Defenses: Disable or Modify Tools , Indicator Removal: Timestamp , Ingress Tool Transfer , Input Capture: Keylogging , Modify Registry , Native API , Network Service Discovery , Network Share Discovery , Non-Application Layer Protocol , Obfuscated Files or Information: Indicator Removal from Tools , Obfuscated Files or Information , Office Application Startup: Office Template Macros , OS Credential Dumping: LSASS Memory , OS Credential Dumping: Security Account Manager , Permission Groups Discovery: Domain Groups , Permission Groups Discovery: Local Groups , Process Discovery , Process Injection: Dynamic-link Library Injection , Process Injection: Process Hollowing , Process Injection , Protocol Tunneling , Proxy: Domain Fronting , Proxy: Internal Proxy , Query Registry , Reflective Code Loading , Remote Services: Remote Desktop Protocol , Remote Services: SSH , Remote Services: Windows Remote Management , Remote Services: SMB/Windows Admin Shares , Remote Services: Distributed Component Object Model , Remote System Discovery , Scheduled Transfer , Screen Capture , Software Discovery , Subvert Trust Controls: Code Signing , System Binary Proxy Execution: Rundll32 , System Network Configuration Discovery , System Network Connections Discovery , System Service Discovery , System Services: Service Execution , Use Alternate Authentication Material: Pass the Hash , Valid Accounts: Domain Accounts , Valid Accounts: Local Accounts , Windows Management Instrumentation
S1097	HUI Loader	[4][6]	Deobfuscate/Decode Files or Information , Hijack Execution Flow: DLL , Impair Defenses: Indicator Blocking

ID	Name	References	Techniques
S0357	Impacket	[1][5]	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay , Lateral Tool Transfer , Network Sniffing , OS Credential Dumping: NTDS , OS Credential Dumping: LSASS Memory , OS Credential Dumping: Security Account Manager , OS Credential Dumping: LSA Secrets , Steal or Forge Kerberos Tickets: Kerberoasting , Steal or Forge Kerberos Tickets: Ccache Files , System Services: Service Execution , Windows Management Instrumentation
S0664	Pandora	[1][4][5][6]	Application Layer Protocol: Web Protocols , Create or Modify System Process: Windows Service , Encrypted Channel: Symmetric Cryptography , Exploitation for Privilege Escalation , Hijack Execution Flow: DLL , Ingress Tool Transfer , Modify Registry , Obfuscated Files or Information: Compression , Process Discovery , Process Injection , Subvert Trust Controls: Code Signing Policy Modification , System Services: Service Execution , Traffic Signaling
S0013	PlugX	[6]	Application Layer Protocol: Web Protocols , Application Layer Protocol: DNS , Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder , Command and Scripting Interpreter: Windows Command Shell , Create or Modify System Process: Windows Service , Deobfuscate/Decode Files or Information , Encrypted Channel: Symmetric Cryptography , File and Directory Discovery , Hide Artifacts: Hidden Files and Directories , Hijack Execution Flow: DLL , Impair Defenses: Disable or Modify System Firewall , Ingress Tool Transfer , Input Capture: Keylogging , Masquerading: Masquerade Task or Service , Masquerading: Match Legitimate Resource Name or Location , Modify Registry , Native API , Network Share Discovery , Non-Application Layer Protocol , Non-Standard Port , Obfuscated Files or Information , Process Discovery , Query Registry , Screen Capture , System Network Connections Discovery , Trusted Developer Utilities Proxy Execution: MSBuild , Virtualization/Sandbox Evasion: System Checks , Web Service: Dead Drop Resolver

ID	Name	References	Techniques
S1040	Rclone	[5]	Archive Collected Data: Archive via Utility , Data Transfer Size Limits , Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol , Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol , Exfiltration Over Web Service: Exfiltration to Cloud Storage , File and Directory Discovery
S0633	Sliver	[1]	Abuse Elevation Control Mechanism: Bypass User Account Control , Access Token Manipulation , Application Layer Protocol: DNS , Application Layer Protocol: Web Protocols , Application Layer Protocol: Command and Scripting Interpreter: PowerShell , Data Encoding: Standard Encoding , Data Obfuscation: Steganography , Encrypted Channel: Asymmetric Cryptography , Encrypted Channel: Symmetric Cryptography , Exfiltration Over C2 Channel , File and Directory Discovery , Ingress Tool Transfer , Obfuscated Files or Information , Obfuscated Files or Information: Compile After Delivery , Obfuscated Files or Information: Encrypted/Encoded File , OS Credential Dumping: LSASS Memory , Process Injection , Proxy: Internal Proxy , Screen Capture , Steal or Forge Kerberos Tickets: Golden Ticket , System Network Configuration Discovery , System Network Connections Discovery

References

[Microsoft. \(2022, May 9\). Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself. Retrieved March 10, 2023.](#) [Microsoft . \(2023, July 12\). How Microsoft names threat actors. Retrieved November 17, 2023.](#) [Dela Cruz, A. et al. \(2022, May 25\). New Linux-Based Ransomware Cheerscrypt Targeting ESXi Devices Linked to Leaked Babuk Source Code. Retrieved December 19, 2023.](#) [Counter Threat Unit Research Team . \(2022, June 23\). BRONZE STARLIGHT RANSOMWARE OPERATIONS USE HUI LOADER. Retrieved December 7, 2023.](#) [Biderman, O. et al. \(2022, October 3\). REVEALING EMPEROR DRAGONFLY: NIGHT SKY AND CHEERSCRYPT - A SINGLE RANSOMWARE GROUP. Retrieved December 6, 2023.](#) [SecureWorks. \(n.d.\). BRONZE STARLIGHT. Retrieved December 6, 2023.](#) [Microsoft Threat Intelligence. \(2021, December 11\). Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability. Retrieved December 7, 2023.](#)