Ember Bear, UNC2589, Bleeding Bear, DEV-0586, Cadet Blizzard, Frozenvista, UAC-0056, Group G1003

Archived: 2026-04-05 17:00:37 UTC

Enterprise T1583 Acquire Infrastructure

Ember Bear uses services such as IVPN, SurfShark, and Tor to add anonymization to operations.[2]

.003 Virtual Private Server

Ember Bear has used virtual private servers (VPSs) to host tools, perform reconnaissance, exploit victim infrastructure, and as a destination for data exfiltration.[1]

Enterprise T1595 .001 Active Scanning: Scanning IP Blocks

Ember Bear has targeted IP ranges for vulnerability scanning related to government and critical infrastructure organizations.[1]

.002 Active Scanning: Vulnerability Scanning

Ember Bear has used publicly available tools such as MASSCAN and Acunetix for vulnerability scanning of public-facing infrastructure.[1]

Enterprise T1071 .004 Application Layer Protocol: DNS

Ember Bear has used DNS tunnelling tools, such as dnscat/2 and Iodine, for C2 purposes.[1]

Enterprise T1560 Archive Collected Data

Ember Bear has compressed collected data prior to exfiltration.[1]

Enterprise T1119 Automated Collection

Ember Bear engages in mass collection from compromised systems during intrusions.[2]

Enterprise T1110 Brute Force

Ember Bear used the `su-bruteforce` tool to brute force specific users using the `su` command.[1]

.003 Password Spraying

Ember Bear has conducted password spraying against Outlook Web Access (OWA) infrastructure to identify valid user names and passwords.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Ember Bear has used PowerShell commands to gather information from compromised systems, such as email servers.[1]

Enterprise T1005 Data from Local System

Ember Bear gathers victim system information such as enumerating the volume of a given device or extracting system and security event logs for analysis.[2][1]

Enterprise T1491 .002 Defacement: External Defacement

Ember Bear is linked to the defacement of several Ukrainian organization websites.[2]

Enterprise T1561 .002 Disk Wipe: Disk Structure Wipe

Ember Bear conducted destructive operations against victims, including disk structure wiping, via the WhisperGate malware in Ukraine.[2]

Enterprise T1114 Email Collection

Ember Bear attempts to collect mail from accessed systems and servers.[2][1]

Enterprise T1585 Establish Accounts

Ember Bear has created accounts on dark web forums to obtain various tools and malware.[1]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

Ember Bear has used tools such as Rclone to exfiltrate information from victim environments to cloud storage such as `mega.nz`.[1]

Enterprise T1190 Exploit Public-Facing Application

Ember Bear gains initial access to victim environments by exploiting external-facing services. Examples include exploitation of CVE-2021-26084 in Confluence servers; CVE-2022-41040, ProxyShell, and other vulnerabilities in Microsoft Exchange; and multiple vulnerabilities in open-source platforms such as content management systems.[2][1]

Enterprise T1203 Exploitation for Client Execution

Ember Bear has used exploits to enable follow-on execution of frameworks such as Meterpreter.[1]

Enterprise T1210 Exploitation of Remote Services

Ember Bear has used exploits for vulnerabilities such as MS17-010, also known as `Eternal Blue`, during operations.[1]

Enterprise T1133 External Remote Services

Ember Bear have used VPNs both for initial access to victim environments and for persistence within them following compromise.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Ember Bear uses the NirSoft AdvancedRun utility to disable Microsoft Defender Antivirus through stopping the WinDefend service on victim machines. Ember Bear disables Windows Defender via registry key changes.[2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Ember Bear deletes files related to lateral movement to avoid detection.[2]

Enterprise T1570 Lateral Tool Transfer

Ember Bear retrieves follow-on payloads direct from adversary-owned infrastructure for deployment on compromised hosts.[2]

Enterprise T1654 Log Enumeration

Ember Bear has enumerated SECURITY and SYSTEM log files during intrusions.[1]

Enterprise T1036 Masquerading

Ember Bear has renamed the legitimate Sysinternals tool procdump to alternative names such as `dump64.exe` to evade detection.[2]

.005 Match Legitimate Resource Name or Location

Ember Bear has renamed tools to match legitimate utilities, such as renaming GOST tunneling instances to `java` in victim environments.[1]

Enterprise T1112 Modify Registry

Ember Bear modifies registry values for anti-forensics and defense evasion purposes.[2]

Enterprise T1046 Network Service Discovery

Ember Bear has used tools such as NMAP for remote system discovery and enumeration in victim environments.[1]

Enterprise T1095 Non-Application Layer Protocol

Ember Bear uses socket-based tunneling utilities for command and control purposes such as NetCat and Go Simple Tunnel (GOST). These tunnels are used to push interactive command prompts over the created sockets.[2] Ember Bear has also used reverse TCP connections from Meterpreter installations to communicate back with C2 infrastructure.[1]

Enterprise T1571 Non-Standard Port

Ember Bear has used various non-standard ports for C2 communication.[1]

Enterprise T1588 .001 Obtain Capabilities: Malware

Ember Bear has acquired malware and related tools from dark web forums.[1]

.005 Obtain Capabilities: Exploits

Ember Bear has obtained exploitation scripts against publicly-disclosed vulnerabilities from public repositories.[1]

Enterprise T1003 OS Credential Dumping

Ember Bear gathers credential material from target systems, such as SSH keys, to facilitate access to victim environments.[2]

.001 LSASS Memory

Ember Bear uses legitimate Sysinternals tools such as procdump to dump LSASS memory.[2][1]

.002 Security Account Manager

Ember Bear acquires victim credentials by extracting registry hives such as the Security Account Manager through commands such as `reg save`.[2][1]

.004 LSA Secrets

Ember Bear has used frameworks such as Impacket to dump LSA secrets for credential capture.[1]

Enterprise T1572 Protocol Tunneling

Ember Bear has used ProxyChains to tunnel protocols to internal networks.[1]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

Ember Bear has configured multi-hop proxies via ProxyChains within victim environments.[1]

Enterprise T1021 Remote Services

Ember Bear uses valid network credentials gathered through credential harvesting to move laterally within victim networks, often employing the Impacket framework to do so.[2]

Enterprise T1018 Remote System Discovery

Ember Bear has used tools such as Nmap and MASSCAN for remote service discovery.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Ember Bear uses remotely scheduled tasks to facilitate remote command execution on victim machines.[2]

Enterprise T1505 .003 Server Software Component: Web Shell

Ember Bear deploys web shells following initial access for either follow-on command execution or protocol tunneling. Example web shells used by Ember Bear include P0wnyshell, reGeorg, P.A.S. Webshell, and custom variants of publicly-available web shell examples.[2][1]

Enterprise T1195 Supply Chain Compromise

Ember Bear has compromised information technology providers and software developers providing services to targets of interest, building initial access to ultimate victims at least in part through compromise of service providers that work with the victim organizations.[2]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Ember Bear has dumped configuration settings in accessed IP cameras including plaintext credentials.[1]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

Ember Bear has used pass-the-hash techniques for lateral movement in victim environments.[1]

Enterprise T1078 .001 Valid Accounts: Default Accounts

Ember Bear has abused default user names and passwords in externally-accessible IP cameras for initial access.[1]

Enterprise T1125 Video Capture

Ember Bear has exfiltrated images from compromised IP cameras.[1]

Enterprise T1047 Windows Management Instrumentation

Ember Bear has used WMI execution with password hashes for command execution and lateral movement.[1]
