Leviathan, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope, Gingham Typhoon, Group G0065

Archived: 2026-04-05 13:12:29 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

Leviathan has established domains that impersonate legitimate entities to use for targeting efforts. [1][5]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

Leviathan has conducted reconnaissance against target networks of interest looking for vulnerable, end-of-life, or no longer maintainted devices against which to rapidly deploy exploits.[4]

Enterprise T1560 Archive Collected Data

Leviathan has archived victim's data prior to exfiltration.[1]

Enterprise T1197 BITS Jobs

Leviathan has used BITSAdmin to download additional tools.[3]

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

Leviathan has used JavaScript to create a shortcut file in the Startup folder that points to its main backdoor.[2][3]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Leviathan has used JavaScript to create a shortcut file in the Startup folder that points to its main backdoor.[2][3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Leviathan has used PowerShell for execution.[2][3][1][5]

.005 Command and Scripting Interpreter: Visual Basic

Leviathan has used VBScript.[2]

Enterprise T1586 .001 Compromise Accounts: Social Media Accounts

Leviathan has compromised social media accounts to conduct social engineering attacks.[1]

.002 Compromise Accounts: Email Accounts

Leviathan has compromised email accounts to conduct social engineering attacks.[1]

Enterprise T1584 .004 Compromise Infrastructure: Server

Leviathan has used compromised legitimate websites as command and control nodes for operations.[4]

.008 Compromise Infrastructure: Network Devices

Leviathan has used compromised networking devices, such as small office/home office (SOHO) devices, as operational command and control infrastructure.[4]

Enterprise T1213 .006 Data from Information Repositories: Databases

Leviathan gathered information from SQL servers and Building Management System (BMS) servers during Leviathan Australian Intrusions.[4]

Enterprise T1074 .001 Data Staged: Local Data Staging

Leviathan has used C:\Windows\Debug and C:\Perflogs as staging directories.[3][1]

Leviathan stored captured credential material on local log files on victim systems during Leviathan Australian Intrusions.[4]

.002 Data Staged: Remote Data Staging

Leviathan has staged data remotely prior to exfiltration.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Leviathan has used a DLL known as SeDll to decrypt and execute other JavaScript backdoors.[2]

Enterprise T1587 .004 Develop Capabilities: Exploits

Leviathan has rapidly transformed and adapted public exploit proof-of-concept code for new vulnerabilities and utilized them against target networks.[4]

Enterprise T1482 Domain Trust Discovery

Leviathan performed Active Directory enumeration of victim environments during Leviathan Australian Intrusions.[4]

Enterprise T1189 Drive-by Compromise

Leviathan has infected victims using watering holes.[1]

Enterprise T1585 .001 Establish Accounts: Social Media Accounts

Leviathan has created new social media accounts for targeting efforts.[1]

.002 Establish Accounts: Email Accounts

Leviathan has created new email accounts for targeting efforts.[1]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

Leviathan has used WMI for persistence.[3]

Enterprise T1041 Exfiltration Over C2 Channel

Leviathan has exfiltrated data over its C2 channel.[1]

Leviathan exfiltrated collected data over existing command and control channels during Leviathan Australian Intrusions.[4]

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

Leviathan has used an uploader known as LUNCHMONEY that can exfiltrate files to Dropbox.[2][3]

Enterprise T1190 Exploit Public-Facing Application

Leviathan has used exploits against publicly-disclosed vulnerabilities for initial access into victim networks.[4]

Leviathan exploited public-facing web applications and appliances for initial access during Leviathan Australian Intrusions.[4]

Enterprise T1203 Exploitation for Client Execution

Leviathan has exploited multiple Microsoft Office and .NET vulnerabilities for execution, including CVE-2017-0199, CVE-2017-8759, and CVE-2017-11882.[2][3][1][5]

Enterprise T1212 Exploitation for Credential Access

Leviathan exploited vulnerable network appliances during Leviathan Australian Intrusions, leading to the collection and exfiltration of valid credentials.[4]

Enterprise T1068 Exploitation for Privilege Escalation

Leviathan exploited software vulnerabilities in victim environments to escalate privileges during Leviathan Australian Intrusions.[4]

Enterprise T1133 External Remote Services

Leviathan has used external remote services such as virtual private networks (VPN) to gain initial access.[1]

Enterprise T1589 .001 Gather Victim Identity Information: Credentials

Leviathan has collected compromised credentials to use for targeting efforts.[1]

Enterprise T1615 Group Policy Discovery

Leviathan performed extensive Active Directory enumeration of victim environments during Leviathan Australian Intrusions.[4]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

Leviathan modified system firewalls to add two open listening ports on 9998 and 9999 during Leviathan Australian Intrusions.[4]

Enterprise T1105 Ingress Tool Transfer

Leviathan has downloaded additional scripts and files from adversary-controlled servers.[2][3]

Enterprise T1056 Input Capture

Leviathan captured submitted multfactor authentication codes and other technical artifacts related to remote access sessions during Leviathan Australian Intrusions.[4]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

Leviathan has utilized OLE as a method to insert malicious content inside various phishing documents. [5]

Enterprise T1534 Internal Spearphishing

Leviathan has conducted internal spearphishing within the victim's environment for lateral movement.[1]

Enterprise T1111 Multi-Factor Authentication Interception

Leviathan abused compromised appliance access to collect multifactor authentication token values during Leviathan Australian Intrusions.[4]

Enterprise T1135 Network Share Discovery

Leviathan scanned and enumerated remote network shares in victim environments during Leviathan Australian Intrusions.[4]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Leviathan has inserted garbage characters into code, presumably to avoid anti-virus detection.[2]

.003 Obfuscated Files or Information: Steganography

Leviathan has used steganography to hide stolen data inside other files stored on Github.[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Leviathan has obfuscated code using base64.[2]

.015 Obfuscated Files or Information: Compression

Leviathan has obfuscated code using gzip compression.[2]

Enterprise T1588 .006 Obtain Capabilities: Vulnerabilities

Leviathan weaponized publicly-known vulnerabilities for initial access and other purposes during Leviathan Australian Intrusions.[4]

Enterprise T1003 OS Credential Dumping

Leviathan has used publicly available tools to dump password hashes, including HOMEFRY.[9]

.001 LSASS Memory

Leviathan has used publicly available tools to dump password hashes, including ProcDump and WCE.[9]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Leviathan has sent spearphishing emails with malicious attachments, including .rtf, .doc, and .xls files.[2][1]

.002 Phishing: Spearphishing Link

Leviathan has sent spearphishing emails with links, often using a fraudulent lookalike domain and stolen branding.[2][1]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Leviathan has utilized techniques like reflective DLL loading to write a DLL into memory and load a shell that provides backdoor access to the victim.[5]

Enterprise T1572 Protocol Tunneling

Leviathan has used protocol tunneling to further conceal C2 communications and infrastructure.[1]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

Leviathan has used multi-hop proxies to disguise the source of their malicious traffic.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Leviathan has targeted RDP credentials and used it to move through the victim environment.[9]

.002 Remote Services: SMB/Windows Admin Shares

Leviathan used remote shares to move laterally through victim networks during Leviathan Australian Intrusions.[4]

.004 Remote Services: SSH

Leviathan used ssh for internal reconnaissance.[9]

Leviathan used SSH brute force techniques to move laterally within victim environments during Leviathan Australian Intrusions.[4]

Enterprise T1018 Remote System Discovery

Leviathan performed extensive remote host enumeration to build their own map of victim networks during Leviathan Australian Intrusions.[4]

Enterprise T1594 Search Victim-Owned Websites

Leviathan enumerated compromised web application resources to identify additional endpoints and resources linkd to the website for follow-on access during Leviathan Australian Intrusions.[4]

Enterprise T1505 .003 Server Software Component: Web Shell

Leviathan relies on web shells for an initial foothold as well as persistence into the victim's systems.[9][1][4]

Leviathan relied extensively on web shell use following initial access for persistence and command execution purposes in victim environments during Leviathan Australian Intrusions.[4]

Enterprise T1528 Steal Application Access Token

Leviathan abused access to compromised appliances to collect JSON Web Tokens (JWTs), used for creating virtual desktop sessions, during Leviathan Australian Intrusions.[4]

Enterprise T1558 .003 Steal or Forge Kerberos Tickets: Kerberoasting

Leviathan used Kerberoasting techniques during Leviathan Australian Intrusions.[4]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Leviathan has used stolen code signing certificates to sign malware.[3][9]

Enterprise T1218 .010 System Binary Proxy Execution: Regsvr32

Leviathan has used regsvr32 for execution.[2]

Enterprise T1082 System Information Discovery

Leviathan performed host enumeration and data gathering operations on victim machines during Leviathan Australian Intrusions.[4]

Enterprise T1552 Unsecured Credentials

Leviathan gathered credentials hardcoded in binaries located on victim devices during Leviathan Australian Intrusions.[4]

.001 Credentials In Files

Leviathan gathered credentials stored in files related to Building Management System (BMS) operations during Leviathan Australian Intrusions.[4]

Enterprise T1204 .001 User Execution: Malicious Link

Leviathan has sent spearphishing email links attempting to get a user to click.[2][1]

.002 User Execution: Malicious File

Leviathan has sent spearphishing attachments attempting to get a user to click.[2][1]

Enterprise T1078 Valid Accounts

Leviathan has obtained valid accounts to gain initial access.[1][5][4]

Leviathan used captured, valid account information to log into victim web applications and appliances during Leviathan Australian Intrusions.[4]

.002 Domain Accounts

Leviathan compromised domain credentials during Leviathan Australian Intrusions.[4]

.003 Local Accounts

Leviathan used captured local account information, such as service accounts, for actions during Leviathan Australian Intrusions.[4]

Enterprise T1102 .003 Web Service: One-Way Communication

Leviathan has received C2 instructions from user profiles created on legitimate websites such as Github and TechNet.[3]

Enterprise T1047 Windows Management Instrumentation

Leviathan has used WMI for execution.[2]
