# Dragonfly, TEMP.Isotope, DYMALLOY, Berserk Bear, TG-4192, Crouching Yeti, IRON LIBERTY, Energetic Bear, Ghost Blizzard, BROMINE, Group G0035

Archived: 2026-04-05 18:32:39 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

Dragonfly has used batch scripts to enumerate users on a victim domain controller.[15]

Enterprise T1098 .007 Account Manipulation: Additional Local or Domain Groups

Dragonfly has added newly created accounts to the administrators group to maintain elevated access.[15]

Enterprise T1583 .001 Acquire Infrastructure: Domains

Dragonfly has registered domains for targeting intended victims.[8]

.003 Acquire Infrastructure: Virtual Private Server

Dragonfly has acquired VPS infrastructure for use in malicious campaigns.[7]

Enterprise T1595 .002 Active Scanning: Vulnerability Scanning

Dragonfly has scanned targeted systems for vulnerable Citrix and Microsoft Exchange services.[8]

Enterprise T1071 .002 Application Layer Protocol: File Transfer Protocols

Dragonfly has used SMB for C2.[15]

Enterprise T1560 Archive Collected Data

Dragonfly has compressed data into .zip files prior to exfiltration.[15]

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

Dragonfly has added the registry value ntdll to the Registry Run key to establish persistence.[15]

Enterprise T1110 Brute Force

Dragonfly has attempted to brute force credentials to gain access.[8]

.002 Password Cracking

Dragonfly has dropped and executed tools used for password cracking, including Hydra and CrackMapExec.[15][16]

Enterprise T1059 Command and Scripting Interpreter

Dragonfly has used the command line for execution.[15]

.001 PowerShell

Dragonfly has used PowerShell scripts for execution.[15][5]

.003 Windows Command Shell

Dragonfly has used various types of scripting to perform operations, including batch scripts.[15]

.006 Python

Dragonfly has used various types of scripting to perform operations, including Python scripts. The group was observed installing Python 2.7 on a victim.[15]

Enterprise T1584 .004 Compromise Infrastructure: Server

Dragonfly has compromised legitimate websites to host C2 and malware modules.[7]

Enterprise T1136 .001 Create Account: Local Account

Dragonfly has created accounts on victims, including administrator accounts, some of which appeared to be tailored to each individual staging target.[15]

Enterprise T1005 Data from Local System

Dragonfly has collected data from local victim systems.[15]

Enterprise T1074 .001 Data Staged: Local Data Staging

Dragonfly has created a directory named "out" in the user's %AppData% folder and copied files to it.[15]

Enterprise T1189 Drive-by Compromise

Dragonfly has compromised targets via strategic web compromise (SWC) utilizing a custom exploit kit.[4][15][7]

Enterprise T1114 .002 Email Collection: Remote Email Collection

Dragonfly has accessed email accounts using Outlook Web Access.[15]

Enterprise T1190 Exploit Public-Facing Application

Dragonfly has conducted SQL injection attacks, exploited vulnerabilities CVE-2019-19781 and CVE-2020-0688 for Citrix and MS Exchange, and CVE-2018-13379 for Fortinet VPNs.[8]

Enterprise T1203 Exploitation for Client Execution

Dragonfly has exploited CVE-2011-0611 in Adobe Flash Player to gain execution on a targeted system.[7]

Enterprise T1210 Exploitation of Remote Services

Dragonfly has exploited a Windows Netlogon vulnerability (CVE-2020-1472) to obtain access to Windows Active Directory servers.[8]

Enterprise T1133 External Remote Services

Dragonfly has used VPNs and Outlook Web Access (OWA) to maintain access to victim networks.[15][8]

Enterprise T1083 File and Directory Discovery

Dragonfly has used a batch script to gather folder and file names from victim hosts.[15][7][8]

Enterprise T1187 Forced Authentication

Dragonfly has gathered hashed user credentials over SMB using spearphishing attachments with external resource links and by modifying .LNK file icon resources to collect credentials from virtualized systems.[15][7]

Enterprise T1591 .002 Gather Victim Org Information: Business Relationships

Dragonfly has collected open source information to identify relationships between organizations for targeting purposes.[7]

Enterprise T1564 .002 Hide Artifacts: Hidden Users

Dragonfly has modified the Registry to hide created user accounts.[15]

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

Dragonfly has disabled host-based firewalls. The group has also globally opened port 3389.[15]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

Dragonfly has cleared Windows event logs and other logs produced by tools they used, including system, security, terminal services, remote services, and audit logs. The actors also deleted specific Registry keys.[15]

.004 Indicator Removal: File Deletion

Dragonfly has deleted many of its files used during operations as part of cleanup, including removing applications and deleting screenshots.[15]

Enterprise T1105 Ingress Tool Transfer

Dragonfly has copied and installed tools for operations once in the victim environment.[15]

Enterprise T1036 .010 Masquerading: Masquerade Account Name

Dragonfly has created accounts disguised as legitimate backup and service accounts as well as an email administration account.[15]

Enterprise T1112 Modify Registry

Dragonfly has modified the Registry to perform multiple techniques through the use of Reg.[15]

Enterprise T1135 Network Share Discovery

Dragonfly has identified and browsed file servers in the victim network, sometimes , viewing files pertaining to ICS or Supervisory Control and Data Acquisition (SCADA) systems.[15]

Enterprise T1588 .002 Obtain Capabilities: Tool

Dragonfly has obtained and used tools such as Mimikatz, CrackMapExec, and PsExec.[4]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

Dragonfly has dropped and executed SecretsDump to dump password hashes.[15]

.003 OS Credential Dumping: NTDS

Dragonfly has dropped and executed SecretsDump to dump password hashes. They also obtained ntds.dit from domain controllers.[15][17]

.004 OS Credential Dumping: LSA Secrets

Dragonfly has dropped and executed SecretsDump to dump password hashes.[15][17]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

Dragonfly has used batch scripts to enumerate administrators and users in the domain.[15]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Dragonfly has sent emails with malicious attachments to gain initial access.[7]

Enterprise T1598 .002 Phishing for Information: Spearphishing Attachment

Dragonfly has used spearphishing with Microsoft Office attachments to enable harvesting of user credentials.[15]

.003 Phishing for Information: Spearphishing Link

Dragonfly has used spearphishing with PDF attachments containing malicious links that redirected to credential harvesting websites.[15]

Enterprise T1012 Query Registry

Dragonfly has queried the Registry to identify victim information.[15]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Dragonfly has moved laterally via RDP.[15]

Enterprise T1018 Remote System Discovery

Dragonfly has likely obtained a list of hosts in the victim environment.[15]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Dragonfly has used scheduled tasks to automatically log out of created accounts every 8 hours as well as to execute malicious files.[15]

Enterprise T1113 Screen Capture

Dragonfly has performed screen captures of victims, including by using a tool, scr.exe (which matched the hash of ScreenUtil).[15][5][7]

Enterprise T1505 .003 Server Software Component: Web Shell

Dragonfly has commonly created Web shells on victims' publicly accessible email and web servers, which they used to maintain access to a victim network and download additional malicious files.[15]

Enterprise T1608 .004 Stage Capabilities: Drive-by Target

Dragonfly has compromised websites to redirect traffic and to host exploit kits.[7]

Enterprise T1195 .002 Supply Chain Compromise: Compromise Software Supply Chain

Dragonfly has placed trojanized installers for control system software on legitimate vendor app stores.[4][7]

Enterprise T1016 System Network Configuration Discovery

Dragonfly has used batch scripts to enumerate network information, including information about trusts, zones, and the domain.[15]

Enterprise T1033 System Owner/User Discovery

Dragonfly used the command `query user` on victim hosts.[15]

Enterprise T1221 Template Injection

Dragonfly has injected SMB URLs into malicious Word spearphishing attachments to initiate Forced Authentication.[15]

Enterprise T1204 .002 User Execution: Malicious File

Dragonfly has used various forms of spearphishing in attempts to get users to open malicious attachments.[7]

Enterprise T1078 Valid Accounts

Dragonfly has compromised user credentials and used valid accounts for operations.[15][7][8]

ICS T0817 Drive-by Compromise

Dragonfly utilized watering hole attacks on energy sector websites by injecting a redirect iframe to deliver Backdoor.Oldrea or Trojan.Karagany. [18]

ICS T0862 Supply Chain Compromise

Dragonfly trojanized legitimate ICS equipment providers software packages available for download on their websites.[18]

---