OilRig, COBALT GYPSY, IRN2, APT34, Helix Kitten, Evasive Serpens, Hazel Sandstorm, EUROPIUM, ITG13, Earth Simnavaz, Crambus, TA452, Group G0049

Archived: 2026-04-05 14:01:53 UTC

Enterprise T1087 .001 Account Discovery: Local Account

OilRig has run `net user` , `net user /domain` , `net group "domain admins" /domain` , and `net group "Exchange Trusted Subsystem" /domain` to get account listings on a victim.[4]

.002 Account Discovery: Domain Account

OilRig has run `net user` , `net user /domain` , `net group "domain admins" /domain` , and `net group "Exchange Trusted Subsystem" /domain` to get account listings on a victim.[4]

Enterprise T1583 .001 Acquire Infrastructure: Domains

OilRig has set up fake VPN portals, conference sign ups, and job application websites to target victims.[3]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

OilRig has used HTTP for C2.[6][17][18]

During Outer Space, OilRig used HTTP to communicate between installed backdoors and compromised servers including via the Microsoft Exchange Web Services API.[16]

During Juicy Mix, OilRig used a VBS script to send POST requests to register installed malware with C2.[16]

.004 Application Layer Protocol: DNS

OilRig has used DNS for C2 including the publicly available `requestbin.net` tunneling service.[6][17][18][10]

Enterprise T1119 Automated Collection

OilRig has used automated collection.[6]

Enterprise T1217 Browser Information Discovery

During Outer Space, OilRig used a Chrome data dumper named MKG.[16]

During Juicy Mix, OilRig used the CDumper (Chrome browser) and EDumper (Edge browser) data stealers to collect cookies, browsing history, and credentials.[16]

Enterprise T1110 Brute Force

OilRig has used brute force techniques to obtain credentials.[17][12]

Enterprise T1115 Clipboard Data

OilRig has used infostealer tools to copy clipboard data.[14]

Enterprise T1059 Command and Scripting Interpreter

OilRig has used various types of scripting for execution.[1][19][20][7][21]

.001 PowerShell

OilRig has used PowerShell scripts for execution, including use of a macro to run a PowerShell command to decode file contents.[1][22][9][13]

During Juicy Mix, OilRig used a PowerShell script to steal credentials.[16]

.003 Windows Command Shell

OilRig has used macros to deliver malware such as QUADAGENT and OopsIE.[1][19][20][7][21] OilRig has used batch scripts.[1][19][20][7][21]

.005 Visual Basic

OilRig has used VBScript macros for execution on compromised hosts.[10]

During Outer Space, OilRig used VBS droppers to deploy malware.[16]

During Juicy Mix, OilRig used VBS droppers to deliver and establish persistence for the Mango backdoor.[16]

Enterprise T1586 .002 Compromise Accounts: Email Accounts

OilRig has compromised email accounts to send phishing emails.[3]

Enterprise T1584 .004 Compromise Infrastructure: Server

During Outer Space, OilRig compromised an Israeli human resources site to use as a C2 server.[16]

During Juicy Mix, OilRig compromised an Israeli job portal to use for a C2 server.[16]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

OilRig has used a compromised Domain Controller to create a service on a remote host.[14]

Enterprise T1555 Credentials from Password Stores

OilRig has used credential dumping tools such as LaZagne to steal credentials to accounts logged into the compromised system and to Outlook Web Access.[6][17][23][18]

.003 Credentials from Web Browsers

OilRig has used credential dumping tools such as LaZagne to steal credentials to accounts logged into the compromised system and to Outlook Web Access.[6][17][23][18] OilRig has also used tool named PICKPOCKET to dump passwords from web browsers.[18]

During Juicy Mix, OilRig used the CDumper (Chrome browser) and EDumper (Edge browser) to collect credentials.[16]

.004 Windows Credential Manager

OilRig has used credential dumping tool named VALUEVAULT to steal credentials from the Windows Credential Manager.[18]

During Juicy Mix, OilRig used a Windows Credential Manager stealer for credential access.[16]

Enterprise T1132 .001 Data Encoding: Standard Encoding

During Juicy Mix, OilRig used a VBS script to send the Base64-encoded name of the compromised computer to C2.[16]

Enterprise T1005 Data from Local System

OilRig has used PowerShell to upload files from compromised systems.[13]

Enterprise T1025 Data from Removable Media

OilRig has used Wireshark's usbcapcmd utility to capture USB traffic.[14]

Enterprise T1074 .001 Data Staged: Local Data Staging

During Juicy Mix, OilRig used browser data and credential stealer tools to stage stolen files named Cupdate, Eupdate, and IUpdate in the %TEMP% directory.[16]

Enterprise T1140 Deobfuscate/Decode Files or Information

A OilRig macro has run a PowerShell command to decode file contents. OilRig has also used certutil to decode base64-encoded files on victims.[1][22][20][24]

During Juicy Mix, OilRig used a script to concatenate and deobfuscate encoded strings in Mango.[16]

Enterprise T1587 .001 Develop Capabilities: Malware

OilRig actively developed and used a series of downloaders during 2022.[25]

For Outer Space, OilRig created new implants including the Solar backdoor.[16]

For Juicy Mix, OilRig improved on Solar by developing the Mango backdoor.[16]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

OilRig used the PowerExchange utility and other tools to create tunnels to C2 servers.[17]

Enterprise T1585 .003 Establish Accounts: Cloud Accounts

During Outer Space, OilRig created M365 email accounts to be used as part of C2.[16]

Enterprise T1048 .003 Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol

OilRig has exfiltrated data via Microsoft Exchange and over FTP separately from its primary C2 channel over DNS.[5][13]

Enterprise T1203 Exploitation for Client Execution

OilRig has exploited CVE-2024-30088 to run arbitrary code in the context of `SYSTEM`.[13]

Enterprise T1068 Exploitation for Privilege Escalation

OilRig has exploited the Windows Kernel Elevation of Privilege vulnerability, CVE-2024-30088.[13]

Enterprise T1133 External Remote Services

OilRig uses remote services such as VPN, Citrix, or OWA to persist in an environment.[17]

Enterprise T1008 Fallback Channels

OilRig malware ISMAgent falls back to its DNS tunneling mechanism if it is unable to reach the C2 server over HTTP.[19]

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

OilRig has modified Windows firewall rules to enable remote access.[14]

Enterprise T1070 .004 Indicator Removal: File Deletion

OilRig has deleted files associated with their payload after execution.[1][20]

Enterprise T1105 Ingress Tool Transfer

OilRig had downloaded remote files onto victim infrastructure.[1][13]

During Outer Space, OilRig downloaded additional tools to comrpomised infrastructure.[16]

Enterprise T1056 .001 Input Capture: Keylogging

OilRig has employed keyloggers including KEYPUNCH and LONGWATCH.[17][18][14]

Enterprise T1036 Masquerading

OilRig has used .doc file extensions to mask malicious executables.[10]

.005 Match Legitimate Resource Name or Location

OilRig has named a downloaded copy of the Plink tunneling utility as \ProgramData\Adobe.exe.[14]

Enterprise T1556 .002 Modify Authentication Process: Password Filter DLL

OilRig has registered a password filter DLL in order to drop malware.[13]

Enterprise T1112 Modify Registry

OilRig has used reg.exe to modify system configuration.[14][13]

Enterprise T1046 Network Service Discovery

OilRig has used the publicly available tool SoftPerfect Network Scanner as well as a custom tool called GOLDIRONY to conduct network scanning.[17]

Enterprise T1027 .005 Obfuscated Files or Information: Indicator Removal from Tools

OilRig has tested malware samples to determine AV detection and subsequently modified the samples to ensure AV evasion.[2][21]

.013 Obfuscated Files or Information: Encrypted/Encoded File

OilRig has encrypted and encoded data in its malware, including by using base64.[1][7][6][9][21]

During Outer Space, OilRig deployed VBS droppers with obfuscated strings.[16]

Enterprise T1588 .002 Obtain Capabilities: Tool

OilRig has made use of the publicly available tools including Plink and Mimikatz.[14][13]

.003 Obtain Capabilities: Code Signing Certificates

OilRig has obtained stolen code signing certificates to digitally sign malware.[3]

Enterprise T1137 .004 Office Application Startup: Outlook Home Page

OilRig has abused the Outlook Home Page feature for persistence. OilRig has also used CVE-2017-11774 to roll back the initial patch designed to protect against Home Page abuse.[26]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

OilRig has used credential dumping tools such as Mimikatz to steal credentials to accounts logged into the compromised system and to Outlook Web Access.[6][17][23][18]

.004 OS Credential Dumping: LSA Secrets

OilRig has used credential dumping tools such as LaZagne to steal credentials to accounts logged into the compromised system and to Outlook Web Access.[6][17][23][18]

.005 OS Credential Dumping: Cached Domain Credentials

OilRig has used credential dumping tools such as LaZagne to steal credentials to accounts logged into the compromised system and to Outlook Web Access.[6][17][23][18]

Enterprise T1201 Password Policy Discovery

OilRig has used net.exe in a script with `net accounts /domain` to find the password policy of a domain.[27]

Enterprise T1120 Peripheral Device Discovery

OilRig has used tools to identify if a mouse is connected to a targeted system.[10]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

OilRig has used `net localgroup administrators` to find local administrators on compromised systems.[4][14]

.002 Permission Groups Discovery: Domain Groups

OilRig has used `net group /domain` , `net group "domain admins" /domain` , and `net group "Exchange Trusted Subsystem" /domain` to find domain group permission settings.[4]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

OilRig has sent spearphising emails with malicious attachments to potential victims using compromised and/or spoofed email accounts.[20][7][9][3]

.002 Phishing: Spearphishing Link

OilRig has sent spearphising emails with malicious links to potential victims.[20][3]

.003 Phishing: Spearphishing via Service

OilRig has used LinkedIn to send spearphishing links.[18]

Enterprise T1057 Process Discovery

OilRig has run `tasklist` on a victim's machine and used infostealers to capture processes.[4][14]

Enterprise T1572 Protocol Tunneling

OilRig has used the Plink utility and other tools to create tunnels to C2 servers.[6][17][18][14]

Enterprise T1012 Query Registry

OilRig has used `reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default"` on a victim to query the Registry.[4]

Enterprise T1219 Remote Access Tools

OilRig has incorporated remote monitoring and management (RMM) tools into their operations including ngrok.[13]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

OilRig has used Remote Desktop Protocol for lateral movement. The group has also used tunneling tools to tunnel RDP into the environment.[6][17][24][14][14]

.004 Remote Services: SSH

OilRig has used Putty to access compromised systems.[6]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

OilRig has created scheduled tasks that run a VBScript to execute a payload on victim machines.[20][7][18][10]

During Juicy Mix, OilRig used VBS droppers to schedule tasks for persistence.[16]

Enterprise T1113 Screen Capture

OilRig has a tool called CANDYKING to capture a screenshot of user's desktop.[17]

Enterprise T1505 .003 Server Software Component: Web Shell

OilRig has used web shells, often to maintain access to a victim network.[6][17][24][13]

Enterprise T1518 Software Discovery

During Juicy Mix, OilRig used browser data dumper tools to create a list of users with Google Chrome installed.[16]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

OilRig has hosted malware on fake websites designed to target specific audiences.[3]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

OilRig has signed its malware with stolen certificates.[3]

Enterprise T1195 Supply Chain Compromise

OilRig has leveraged compromised organizations to conduct supply chain attacks on government entities.[13]

Enterprise T1218 .001 System Binary Proxy Execution: Compiled HTML File

OilRig has used a CHM payload to load and execute another malicious file once delivered to a victim.[4]

Enterprise T1082 System Information Discovery

OilRig has run `hostname` and `systeminfo` on a victim.[4][5][18][10][14]

During Juicy Mix, OilRig used a script to send the name of the compromised host via HTTP `POST` to register it with C2.[16]

Enterprise T1016 System Network Configuration Discovery

OilRig has run `ipconfig /all` on a victim.[4][5]

Enterprise T1049 System Network Connections Discovery

OilRig has used `netstat -an` on a victim to get a listing of network connections.[4]

Enterprise T1033 System Owner/User Discovery

OilRig has run `whoami` on a victim.[4][5][10]

Enterprise T1007 System Service Discovery

OilRig has used `sc query` on a victim to gather information about services.[4]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

OilRig has used credential dumping tools such as LaZagne to steal credentials to accounts logged into the compromised system and to Outlook Web Access.[6][17][23][18]

Enterprise T1204 .001 User Execution: Malicious Link

OilRig has delivered malicious links to achieve execution on the target system.[20][7][9][3]

.002 User Execution: Malicious File

OilRig has delivered macro-enabled documents that required targets to click the "enable content" button to execute the payload on the system.[20][7][9][10][3]

Enterprise T1078 Valid Accounts

OilRig has used compromised credentials to access other systems on a victim network.[6][17][24][12]

.002 Domain Accounts

OilRig has used an exfiltration tool named STEALHOOK to retreive valid domain credentials.[13]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

OilRig has used macros to verify if a mouse is connected to a compromised machine.[10]

Enterprise T1047 Windows Management Instrumentation

OilRig has used WMI for execution.[17][14]

ICS T0817 Drive-by Compromise

OilRig has been seen utilizing watering hole attacks to collect credentials which could be used to gain access into ICS networks. [28]

ICS T0853 Scripting

OilRig has embedded a macro within spearphishing attachments that has been made up of both a VBScript and a PowerShell script.[29]

ICS T0865 Spearphishing Attachment

OilRig used spearphishing emails with malicious Microsoft Excel spreadsheet attachments. [29]

ICS T0869 Standard Application Layer Protocol

OilRig communicated with its command and control using HTTP requests. [29]

ICS T0859 Valid Accounts

OilRig utilized stolen credentials to gain access to victim machines.[30]
