Indrik Spider, Evil Corp, Manatee Tempest, DEV-0243, UNC2165, Group G0119

Archived: 2026-04-05 13:11:56 UTC

Enterprise T1583 Acquire Infrastructure

Indrik Spider has purchased access to victim VPNs to facilitate access to victim environments.[5]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Indrik Spider has used PowerShell Empire for execution of malware.[1][6]

.003 Command and Scripting Interpreter: Windows Command Shell

Indrik Spider has used batch scripts on victim's machines.[1][5]

.007 Command and Scripting Interpreter: JavaScript

Indrik Spider has used malicious JavaScript files for several components of their attack.[6]

Enterprise T1584 .004 Compromise Infrastructure: Server

Indrik Spider has served fake updates via legitimate websites that have been compromised.[1]

Enterprise T1136 Create Account

Indrik Spider used `wmic.exe` to add a new user to the system.[6]

.001 Local Account

Indrik Spider has created local system accounts and has added the accounts to privileged groups.[5]

Enterprise T1555 .005 Credentials from Password Stores: Password Managers

Indrik Spider has accessed and exported passwords from password managers.[5]

Enterprise T1486 Data Encrypted for Impact

Indrik Spider has encrypted domain-controlled systems using BitPaymer.[1] Additionally, Indrik Spider used PsExec to execute a ransomware script.[5]

Enterprise T1074 .001 Data Staged: Local Data Staging

Indrik Spider has stored collected data in a .tmp file.[6]

Enterprise T1587 .001 Develop Capabilities: Malware

Indrik Spider has developed malware for their operations, including ransomware such as BitPaymer and WastedLocker.[1]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

Indrik Spider has used Group Policy Objects to deploy batch scripts.[1][5]

Enterprise T1585 .002 Establish Accounts: Email Accounts

Indrik Spider has created email accounts to communicate with their ransomware victims, to include providing payment and decryption details.[1]

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

Indrik Spider has exfiltrated data using Rclone or MEGASync prior to deploying ransomware.[5]

Enterprise T1590 Gather Victim Network Information

Indrik Spider has downloaded tools, such as the Advanced Port Scanner utility and Lansweeper, to conduct internal reconnaissance of the victim network. Indrik Spider has also accessed the victim's VMware VCenter, which had information about host configuration, clusters, etc.[5]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Indrik Spider used PsExec to leverage Windows Defender to disable scanning of all downloaded files and to restrict real-time monitoring.[6] Indrik Spider has used `MpCmdRun` to revert the definitions in Microsoft Defender.[5] Additionally, Indrik Spider has used WMI to stop or uninstall and reset anti-virus products and other defensive services.[5]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

Indrik Spider has used Cobalt Strike to empty log files.[6] Additionally, Indrik Spider has cleared all event logs using `wevutil`.[5]

Enterprise T1105 Ingress Tool Transfer

Indrik Spider has downloaded additional scripts, malware, and tools onto a compromised host.[1][6][5]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Indrik Spider used fake updates for FlashPlayer plugin and Google Chrome as initial infection vectors.[1]

Enterprise T1112 Modify Registry

Indrik Spider has modified registry keys to prepare for ransomware execution and to disable common administrative utilities.[5]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Indrik Spider used Cobalt Strike to carry out credential dumping using ProcDump.[6]

Enterprise T1012 Query Registry

Indrik Spider has used a service account to extract copies of the `Security` Registry hive.[5]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Indrik Spider has used RDP for lateral movement.[5]

.004 Remote Services: SSH

Indrik Spider has used SSH for lateral movement.[5]

Enterprise T1018 Remote System Discovery

Indrik Spider has used PowerView to enumerate all Windows Server, Windows Server 2003, and Windows 7 instances in the Active Directory database.[6]

Enterprise T1489 Service Stop

Indrik Spider has used PsExec to stop services prior to the execution of ransomware.[6]

Enterprise T1558 .003 Steal or Forge Kerberos Tickets: Kerberoasting

Indrik Spider has conducted Kerberoasting attacks using a module from GitHub.[5]

Enterprise T1007 System Service Discovery

Indrik Spider has used the win32_service WMI class to retrieve a list of services from the system.[6]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Indrik Spider has searched files to obtain and exfiltrate credentials.[5]

Enterprise T1204 .002 User Execution: Malicious File

Indrik Spider has attempted to get users to click on a malicious zipped file.[6]

Enterprise T1078 Valid Accounts

Indrik Spider has used valid accounts for initial access and lateral movement.[5] Indrik Spider has also maintained access to the victim environment through the VPN infrastructure.[5]

.002 Domain Accounts

Indrik Spider has collected credentials from infected systems, including domain accounts.[1]

Enterprise T1047 Windows Management Instrumentation

Indrik Spider has used WMIC to execute commands on remote computers.[6]
