# Play, Group G1040 | MITRE ATT&CK®

Archived: 2026-04-05 14:08:34 UTC

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Play has used WinRAR to compress files prior to exfiltration.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Play has used Base64-encoded PowerShell scripts to disable Microsoft Defender.[2]

.003 Command and Scripting Interpreter: Windows Command Shell

Play has used a batch script to remove indicators of its presence on compromised hosts.[2]

Enterprise T1030 Data Transfer Size Limits

Play has split victims' files into chunks for exfiltration.[1][2]

Enterprise T1587 .001 Develop Capabilities: Malware

Play developed and employ Playcrypt ransomware.[2][1]

Enterprise T1048 Exfiltration Over Alternative Protocol

Play has used WinSCP to exfiltrate data to actor-controlled accounts.[1][2]

Enterprise T1190 Exploit Public-Facing Application

Play has exploited known vulnerabilities for initial access including CVE-2018-13379 and CVE-2020-12812 in FortiOS and CVE-2022-41082 and CVE-2022-41040 ("ProxyNotShell") in Microsoft Exchange.[1][2]

Enterprise T1133 External Remote Services

Play has used Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN) for initial access.[1][2]

Enterprise T1083 File and Directory Discovery

Play has used the Grixba information stealer to list security files and processes.[2]

Enterprise T1657 Financial Theft

Play demands ransom payments from victims to unencrypt filesystems and to not publish sensitive data exfiltrated from victim networks.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Play has used tools including GMER, IOBit, and PowerTool to disable antivirus software.[1][2]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

Play has used tools to remove log files on targeted systems.[1][2]

.004 Indicator Removal: File Deletion

Play has used tools including Wevtutil to remove malicious files from compromised hosts.[2]

Enterprise T1105 Ingress Tool Transfer

Play has used Cobalt Strike to download files to compromised machines.[2]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

Play has used Base64-encoded PowerShell scripts for post exploit activities on compromised hosts.[2]

Enterprise T1588 .002 Obtain Capabilities: Tool

Play has used multiple tools for discovery and defense evasion purposes on compromised hosts.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Play has used Mimikatz and the Windows Task Manager to dump LSASS process memory.[2]

Enterprise T1057 Process Discovery

Play has used the information stealer Grixba to check for a list of security processes.[2]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Play has used Cobalt Strike to move laterally via SMB.[2]

Enterprise T1018 Remote System Discovery

Play has used tools such as AdFind, Nltest, and BloodHound to enumerate shares and hostnames on compromised networks.[2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Play has used the information-stealing tool Grixba to scan for anti-virus software.[1]

Enterprise T1082 System Information Discovery

Play has leveraged tools to enumerate system information.[2]

Enterprise T1016 System Network Configuration Discovery

Play has used the information-stealing tool Grixba to enumerate network information.[1]

Enterprise T1078 Valid Accounts

Play has used valid VPN accounts to achieve initial access.[1]

.002 Domain Accounts

Play has used valid domain accounts for access.[2]

.003 Local Accounts

Play has used valid local accounts to gain initial access.[2]

---