INC Ransom, GOLD IONIC, Group G1032

Archived: 2026-04-05 17:19:48 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

INC Ransom has scanned for domain admin accounts in compromised environments.[5]

Enterprise T1071 Application Layer Protocol

INC Ransom has used valid accounts over RDP to connect to targeted systems.[6]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

INC Ransom has used 7-Zip and WinRAR to archive collected data prior to exfiltration.[6][3][5][7]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

INC Ransom has used `cmd.exe` to launch malicious payloads.[6]

Enterprise T1486 Data Encrypted for Impact

INC Ransom has used INC Ransomware to encrypt victim's data.[4][6][1][3][2][5]

Enterprise T1074 Data Staged

INC Ransom has staged data on compromised hosts prior to exfiltration.[6][5]

Enterprise T1190 Exploit Public-Facing Application

INC Ransom has exploited known vulnerabilities including CVE-2023-3519 in Citrix NetScaler for initial access. [5][4]

Enterprise T1657 Financial Theft

INC Ransom has stolen and encrypted victim's data in order to extort payment for keeping it private or decrypting it.[2][1][3][5][4]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

INC Ransom can use SystemSettingsAdminFlows.exe, a native Windows utility, to disable Windows Defender.[7]

Enterprise T1070 .004 Indicator Removal: File Deletion

INC Ransom has uninstalled tools from compromised endpoints after use.[7]

Enterprise T1105 Ingress Tool Transfer

INC Ransom has downloaded tools to compromised servers including Advanced IP Scanner. [6][7]

Enterprise T1570 Lateral Tool Transfer

INC Ransom has used a rapid succession of copy commands to install a file encryption executable across multiple endpoints within compromised infrastructure.[6][3]

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

INC Ransom has named a PsExec executable winupd to mimic a legitimate Windows update file.[6][5]

Enterprise T1046 Network Service Discovery

INC Ransom has used NETSCAN.EXE for internal reconnaissance.[5][4]

Enterprise T1135 Network Share Discovery

INC Ransom has used Internet Explorer to view folders on other systems.[6]

Enterprise T1588 .002 Obtain Capabilities: Tool

INC Ransom has acquired and used several tools including MegaSync, AnyDesk, esentutl and PsExec.[2][6][5][7][4]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

INC Ransom has enumerated domain groups on targeted hosts.[6]

Enterprise T1566 Phishing

INC Ransom has used phishing to gain initial access.[5][4]

Enterprise T1219 Remote Access Tools

INC Ransom has used AnyDesk and PuTTY on compromised systems.[6][5][7][4]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

INC Ransom has used RDP to move laterally.[2][6][5][7]

Enterprise T1049 System Network Connections Discovery

INC Ransom has used RDP to test network connections.[5]

Enterprise T1569 .002 System Services: Service Execution

INC Ransom has run a file encryption executable via `Service Control Manager/7045;winupd,%SystemRoot%\winupd.exe,user mode service,demand start,LocalSystem`.[6]

Enterprise T1537 Transfer Data to Cloud Account

INC Ransom has used Megasync to exfiltrate data to the cloud.[3]

Enterprise T1078 Valid Accounts

INC Ransom has used compromised valid accounts for access to victim environments.[2][6][5][7]

Enterprise T1047 Windows Management Instrumentation

INC Ransom has used WMIC to deploy ransomware.[2][6][5]
