TA505, Hive0065, Spandex Tempest, CHIMBORAZO, Group G0092

Archived: 2026-04-05 18:08:24 UTC

Enterprise T1087 .003 Account Discovery: Email Account

TA505 has used the tool EmailStealer to steal and send lists of e-mail addresses to a remote server.[8]

Enterprise T1583 .001 Acquire Infrastructure: Domains

TA505 has registered domains to impersonate services such as Dropbox to distribute malware.[5]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

TA505 has used HTTP to communicate with C2 nodes.[6]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

TA505 has used PowerShell to download and execute malware and reconnaissance scripts.[1][9][10][11]

.003 Command and Scripting Interpreter: Windows Command Shell

TA505 has executed commands using `cmd.exe`.[8]

.005 Command and Scripting Interpreter: Visual Basic

TA505 has used VBS for code execution.[1][2][8][6]

.007 Command and Scripting Interpreter: JavaScript

TA505 has used JavaScript for code execution.[1][2]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

TA505 has used malware to gather credentials from Internet Explorer.[1]

Enterprise T1486 Data Encrypted for Impact

TA505 has used a wide variety of ransomware, such as Clop, Locky, Jaff, Bart, Philadelphia, and GlobeImposter, to encrypt victim files and demand a ransom payment.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

TA505 has decrypted packed DLLs with an XOR key.[4]

Enterprise T1568 .001 Dynamic Resolution: Fast Flux DNS

TA505 has used fast flux to mask botnets by distributing payloads across multiple IPs.[8]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

TA505 has used malware to disable Windows Defender.[5]

Enterprise T1105 Ingress Tool Transfer

TA505 has downloaded additional malware to execute on victim systems.[10][11][9]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

TA505 has leveraged malicious Word documents that abused DDE.[2]

Enterprise T1112 Modify Registry

TA505 has used malware to disable Windows Defender through modification of the Registry.[5]

Enterprise T1106 Native API

TA505 has deployed payloads that use Windows API calls on a compromised host.[5]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

TA505 has used UPX to obscure malicious code.[6]

.010 Obfuscated Files or Information: Command Obfuscation

TA505 has used base64 encoded PowerShell commands.[10][11]

.013 Obfuscated Files or Information: Encrypted/Encoded File

TA505 has password-protected malicious Word documents.[1]

Enterprise T1588 .001 Obtain Capabilities: Malware

TA505 has used malware such as Azorult and Cobalt Strike in their operations.[4]

.002 Obtain Capabilities: Tool

TA505 has used a variety of tools in their operations, including AdFind, BloodHound, Mimikatz, and PowerSploit.[4]

Enterprise T1069 Permission Groups Discovery

TA505 has used TinyMet to enumerate members of privileged groups.[6] TA505 has also run `net group /domain`.[8]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

TA505 has used spearphishing emails with malicious attachments to initially compromise victims.[1][2][3][10][9][12][8][13][6]

.002 Phishing: Spearphishing Link

TA505 has sent spearphishing emails containing malicious links.[1][3][8][13]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

TA505 has been seen injecting a DLL into winword.exe.[6]

Enterprise T1608 .001 Stage Capabilities: Upload Malware

TA505 has staged malware on actor-controlled domains.[5]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

TA505 has signed payloads with code signing certificates from Thawte and Sectigo.[10][11][8]

.005 Subvert Trust Controls: Mark-of-the-Web Bypass

TA505 has used .iso files to deploy malicious .lnk files.[14]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

TA505 has used `msiexec` to download and execute malicious Windows Installer files.[10][11][8]

.011 System Binary Proxy Execution: Rundll32

TA505 has leveraged `rundll32.exe` to execute malicious DLLs.[10][11]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

TA505 has used malware to gather credentials from FTP clients and Outlook.[1]

Enterprise T1204 .001 User Execution: Malicious Link

TA505 has used lures to get users to click links in emails and attachments. For example, TA505 makes their malware look like legitimate Microsoft Word documents, .pdf and/or .lnk files. [1][2][3][10][9][12][8][13]

.002 User Execution: Malicious File

TA505 has used lures to get users to enable content in malicious attachments and execute malicious files contained in archives. For example, TA505 makes their malware look like legitimate Microsoft Word documents, .pdf and/or .lnk files. [1][2][3][10][9][12][8][13][6]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

TA505 has used stolen domain admin accounts to compromise additional hosts.[6]

Source: https://attack.mitre.org/groups/G0092/