Bankshot, Software S0239 | MITRE ATT&CK®

Archived: 2026-04-05 15:12:42 UTC

Enterprise T1134 .002 Access Token Manipulation: Create Process with Token

Bankshot grabs a user token using WTSQueryUserToken and then creates a process by impersonating a logged-on user.[1]

Enterprise T1087 .001 Account Discovery: Local Account

Bankshot gathers domain and account names/information through process monitoring.[1]

.002 Account Discovery: Domain Account

Bankshot gathers domain and account names/information through process monitoring.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Bankshot uses HTTP for command and control communication.[1]

Enterprise T1119 Automated Collection

Bankshot recursively generates a list of files within a directory and sends them back to the control server.[1]

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

Bankshot uses the command-line interface to execute arbitrary commands.[1][2]

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

Bankshot can terminate a specific process by its process id.[1][2]

Enterprise T1132 .002 Data Encoding: Non-Standard Encoding

Bankshot encodes commands from the control server using a range of characters and gzip.[1]

Enterprise T1005 Data from Local System

Bankshot collects files from the local system.[1]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

Bankshot generates a false TLS handshake using a public certificate to disguise C2 network communications.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

Bankshot decodes embedded XOR strings.[2]

Enterprise T1041 Exfiltration Over C2 Channel

Bankshot exfiltrates data over its C2 channel.[1]

Enterprise T1203 Exploitation for Client Execution

Bankshot leverages a known zero-day vulnerability in Adobe Flash to execute the implant into the victims' machines.[1]

Enterprise T1083 File and Directory Discovery

Bankshot searches for files on the victim's machine.[2]

Enterprise T1070 Indicator Removal

Bankshot deletes all artifacts associated with the malware from the infected machine.[2]

.004 File Deletion

Bankshot marks files to be deleted upon the next system reboot and uninstalls and removes itself from the system.[1]

.006 Timestomp

Bankshot modifies the time of a file as specified by the control server.[1]

Enterprise T1105 Ingress Tool Transfer

Bankshot uploads files and secondary payloads to the victim's machine.[2]

Enterprise T1680 Local Storage Discovery

Bankshot gathers disk type and disk free space.[1][2]

Enterprise T1112 Modify Registry

Bankshot writes data into the Registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Pniumj`.[2]

Enterprise T1106 Native API

Bankshot creates processes using the Windows API calls: CreateProcessA() and CreateProcessAsUserA().[1]

Enterprise T1571 Non-Standard Port

Bankshot binds and listens on port 1058 for HTTP traffic while also utilizing a FakeTLS method.[2]

Enterprise T1057 Process Discovery

Bankshot identifies processes and collects the process ids.[1]

Enterprise T1012 Query Registry

Bankshot searches for certain Registry keys to be configured before executing the payload.[2]

Enterprise T1082 System Information Discovery

Bankshot gathers system information, network addresses, and the operation system version.[1][2]
