BitPaymer, Software S0570 | MITRE ATT&CK®

Archived: 2026-04-02 12:05:23 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

BitPaymer can suppress UAC prompts by setting the `HKCU\Software\Classes\ms-settings\shell\open\command` registry key on Windows 10 or `HKCU\Software\Classes\mscfile\shell\open\command` on Windows 7 and launching the `eventvwr.msc` process, which launches BitPaymer with elevated privileges.[1]

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

BitPaymer can use the tokens of users to create processes on infected systems.[1]

Enterprise T1087 .001 Account Discovery: Local Account

BitPaymer can enumerate the sessions for each user logged onto the infected host.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

BitPaymer has set the run key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` for persistence.[1]

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

BitPaymer has attempted to install itself as a service to maintain persistence.[1]

Enterprise T1486 Data Encrypted for Impact

BitPaymer can import a hard-coded RSA 1024-bit public key, generate a 128-bit RC4 key for each file, and encrypt the file in place, appending `.locked` to the filename.[1]

Enterprise T1480 Execution Guardrails

BitPaymer compares file names and paths to a list of excluded names and directory names during encryption.[1]

Enterprise T1222 .001 File and Directory Permissions Modification: Windows File and Directory Permissions Modification

BitPaymer can use `icacls /reset` and `takeown /F` to reset a targeted executable's permissions and then take ownership.[1]

Enterprise T1564 .004 Hide Artifacts: NTFS File Attributes

BitPaymer has copied itself to the `:bin` alternate data stream of a newly created file.[1]

Enterprise T1070 .006 Indicator Removal: Timestomp

BitPaymer can modify the timestamp of an executable so that it can be identified and restored by the decryption tool.[1]

Enterprise T1490 Inhibit System Recovery

BitPaymer attempts to remove the backup shadow files from the host using `vssadmin.exe Delete Shadows /All /Quiet`.[1]

Enterprise T1112 Modify Registry

BitPaymer can set values in the Registry to help in execution.[1]

Enterprise T1106 Native API

BitPaymer has used dynamic API resolution to avoid identifiable strings within the binary, including `RegEnumKeyW`.[1]

Enterprise T1135 Network Share Discovery

BitPaymer can search for network shares on the domain or workgroup using `net view`.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

BitPaymer has used RC4-encrypted strings and string hashes to avoid identifiable strings within the binary.[1]

Enterprise T1012 Query Registry

BitPaymer can use the RegEnumKeyW to iterate through Registry keys.[1]

Enterprise T1018 Remote System Discovery

BitPaymer can use `net view` to discover remote systems.[1]

Enterprise T1007 System Service Discovery

BitPaymer can enumerate existing Windows services on the host that are configured to run as LocalSystem.[1]
