Bisonal, Software S0268 | MITRE ATT&CK®

Archived: 2026-04-05 18:38:09 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Bisonal has used HTTP for C2 communications.[1][3]

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

Bisonal has added itself to the Registry key `HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Run\` for persistence.[1][2]

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

Bisonal has launched cmd.exe and used the ShellExecuteW() API function to execute commands on the system.[1][3][2]

.005 Command and Scripting Interpreter: Visual Basic

Bisonal's dropper creates VBS scripts on the victim’s machine.[1][2]

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

Bisonal has been modified to be used as a Windows service.[2]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Bisonal has encoded binary data with Base64 and ASCII.[3][2]

Enterprise T1005 Data from Local System

Bisonal has collected information from a compromised host.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Bisonal has decoded strings in the malware using XOR and RC4.[1][2]

Enterprise T1568 Dynamic Resolution

Bisonal has used a dynamic DNS service for C2.[2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Bisonal variants reported on in 2014 and 2015 used a simple XOR cipher for C2. Some Bisonal samples encrypt C2 communications with RC4.[1][3][2]

Enterprise T1041 Exfiltration Over C2 Channel

Bisonal has added the exfiltrated data to the URL over the C2 channel.[2]

Enterprise T1083 File and Directory Discovery

Bisonal can retrieve a file listing from the system.[3][2]

Enterprise T1070 .004 Indicator Removal: File Deletion

Bisonal will delete its dropper and VBS scripts from the victim's machine.[1][3][2]

Enterprise T1105 Ingress Tool Transfer

Bisonal has the capability to download files to execute on the victim's machine.[1][3][2]

Enterprise T1036 Masquerading

Bisonal dropped a decoy payload with a .jpg extension that contained a malicious Visual Basic script.[2]

.005 Match Legitimate Resource Name or Location

Bisonal has renamed malicious code to `msacm32.dll` to hide within a legitimate library; earlier versions were disguised as `winhelp` .[2]

Enterprise T1112 Modify Registry

Bisonal has deleted Registry keys to clean up its prior activity.[2]

Enterprise T1106 Native API

Bisonal has used the Windows API to communicate with the Service Control Manager to execute a thread.[2]

Enterprise T1095 Non-Application Layer Protocol

Bisonal has used raw sockets for network communication.[2]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Bisonal has appended random binary data to the end of itself to generate a large binary.[2]

.002 Obfuscated Files or Information: Software Packing

Bisonal has used the MPRESS packer and similar tools for obfuscation.[2]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Bisonal's DLL file and non-malicious decoy file are encrypted with RC4 and some function name strings are obfuscated.[1][2]

Enterprise T1137 .006 Office Application Startup: Add-ins

Bisonal has been loaded through a `.wll` extension added to the `%APPDATA%\microsoft\word\startup\` repository.[2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Bisonal has been delivered as malicious email attachments.[2]

Enterprise T1057 Process Discovery

Bisonal can obtain a list of running processes on the victim's machine.[1][3][2]

Enterprise T1090 Proxy

Bisonal has supported use of a proxy server.[2]

Enterprise T1012 Query Registry

Bisonal has used the RegQueryValueExA function to retrieve proxy information in the Registry.[2]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Bisonal has used rundll32.exe to execute as part of the Registry Run key it adds: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"vert" = "rundll32.exe c:\windows\temp\pvcu.dll , Qszdez"` .[1]

Enterprise T1082 System Information Discovery

Bisonal has used commands and API calls to gather system information.[1][3][2]

Enterprise T1016 System Network Configuration Discovery

Bisonal can execute `ipconfig` on the victim's machine.[1][3][2]

Enterprise T1124 System Time Discovery

Bisonal can check the system time set on the infected host.[3]

Enterprise T1204 .002 User Execution: Malicious File

Bisonal has relied on users to execute malicious file attachments delivered via spearphishing emails.[2]

Enterprise T1497 Virtualization/Sandbox Evasion

Bisonal can check to determine if the compromised system is running on VMware.[2]

.003 Time Based Checks

Bisonal has checked if the malware is running in a virtual environment with the anti-debug function GetTickCount() to compare the timing.[3][2]
