Windshift, Bahamut, Group G0112 | MITRE ATT&CK®

Archived: 2026-04-02 12:32:39 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Windshift has used tools that communicate with C2 over HTTP.[4]

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

Windshift has created LNK files in the Startup folder to establish persistence.[4]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

Windshift has used Visual Basic 6 (VB6) payloads.[4]

Enterprise T1189 Drive-by Compromise

Windshift has used compromised websites to register custom URL schemes on a remote system.[2]

Enterprise T1105 Ingress Tool Transfer

Windshift has used tools to deploy additional payloads to compromised hosts.[4]

Enterprise T1036 Masquerading

Windshift has used icons mimicking MS Office files to mask malicious executables.[2] Windshift has also attempted to hide executables by changing the file extension to ".scr" to mimic Windows screensavers.[4]

.001 Invalid Code Signature

Windshift has used revoked certificates to sign malware.[2][1]

Enterprise T1027 Obfuscated Files or Information

Windshift has used string encoding with floating point calculations.[4]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Windshift has sent spearphishing emails with attachment to harvest credentials and deliver malware.[1]

.002 Phishing: Spearphishing Link

Windshift has sent spearphishing emails with links to harvest credentials and deliver malware.[1]

.003 Phishing: Spearphishing via Service

Windshift has used fake personas on social media to engage and target victims.[1]

Enterprise T1057 Process Discovery

Windshift has used malware to enumerate active processes.[4]

Enterprise T1518 Software Discovery

Windshift has used malware to identify installed software.[4]

.001 Security Software Discovery

Windshift has used malware to identify installed AV and commonly used forensic and malware analysis tools.[4]

Enterprise T1082 System Information Discovery

Windshift has used malware to identify the computer name of a compromised host.[4]

Enterprise T1033 System Owner/User Discovery

Windshift has used malware to identify the username on a compromised host.[4]

Enterprise T1204 .001 User Execution: Malicious Link

Windshift has used links embedded in e-mails to lure victims into executing malicious code.[1]

.002 User Execution: Malicious File

Windshift has used e-mail attachments to lure victims into executing malicious code.[1]

Enterprise T1047 Windows Management Instrumentation

Windshift has used WMI to collect information about target machines.[4]

Mobile T1429 Audio Capture

Windshift has included phone call and audio recording capabilities in the malicious apps deployed as part of Operation BULL and Operation ROCK.[4]

Mobile T1533 Data from Local System

Windshift has exfiltrated local account data and calendar information as part of Operation ROCK.[4]

Mobile T1407 Download New Code at Runtime

Windshift has included malware functionality capable of downloading new DEX files at runtime during Operation BULL.[4]

Mobile T1521 .001 Encrypted Channel: Symmetric Cryptography

Windshift has encrypted C2 communications using AES in CBC mode during Operation BULL and Operation ROCK.[4]

Mobile T1627 .001 Execution Guardrails: Geofencing

Windshift has region-locked their malicious applications during their Operation BULL campaign.[4]

Mobile T1420 File and Directory Discovery

Windshift has included file enumeration in the malicious apps deployed as part of Operation BULL and Operation ROCK.[4]

Mobile T1628 .003 Hide Artifacts: Conceal Multimedia Files

Windshift has hidden multimedia files from the user.[5]

Mobile T1417 .001 Input Capture: Keylogging

Windshift has included keylogging capabilities as part of Operation ROCK.[4]

Mobile T1430 Location Tracking

Windshift has included location tracking capabilities in the malicious apps deployed as part of Operation BULL and Operation ROCK.[4]

Mobile T1406 Obfuscated Files or Information

Windshift has encrypted application strings using AES in ECB mode and Blowfish, and stored strings encoded in hex during Operation BULL. Further, in Operation BULL, encryption keys were stored within the application's launcher icon file.[4]

Mobile T1636 .003 Protected User Data: Contact List

Windshift has included contact list exfiltration in the malicious apps deployed as part of Operation BULL.[4]

.004 Protected User Data: SMS Messages

Windshift has included SMS message exfiltration in the malicious apps deployed as part of Operation BULL and Operation ROCK.[4]

Mobile T1632 .001 Subvert Trust Controls: Code Signing Policy Modification

Windshift has installed malicious MDM profiles on iOS devices as part of Operation ROCK.[4]

Mobile T1426 System Information Discovery

Windshift has included system information enumeration in the malicious apps deployed as part of Operation BULL and Operation ROCK.[4]

Mobile T1512 Video Capture

Windshift has included video recording in the malicious apps deployed as part of Operation BULL.[4]

Mobile T1633 .001 Virtualization/Sandbox Evasion: System Checks

Windshift has deployed anti-analysis capabilities during their Operation BULL campaign.[4]
