ZIRCONIUM, APT31, Violet Typhoon, Group G0128

Archived: 2026-04-05 13:23:39 UTC

Enterprise T1583 .001 Acquire Infrastructure: Domains

ZIRCONIUM has purchased domains for use in targeted campaigns.[1]

.006 Acquire Infrastructure: Web Services

ZIRCONIUM has used GitHub to host malware linked in spearphishing e-mails.[4][5]

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

ZIRCONIUM has created a Registry Run key named `Dropbox Update Setup` to establish persistence for a malicious Python binary.[5]

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

ZIRCONIUM has used a tool to open a Windows Command Shell on a remote host.[5]

.006 Command and Scripting Interpreter: Python

ZIRCONIUM has used Python-based implants to interact with compromised hosts.[4][5]

Enterprise T1584 .008 Compromise Infrastructure: Network Devices

ZIRCONIUM has compromised network devices such as small office and home office (SOHO) routers and IoT devices for ORB (operational relay box) Proxy networks.[6][7]

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

ZIRCONIUM has used a tool to steal credentials from installed web browsers including Microsoft Internet Explorer and Google Chrome.[5]

Enterprise T1140 Deobfuscate/Decode Files or Information

ZIRCONIUM has used the AES256 algorithm with a SHA1 derived key to decrypt exploit code.[2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

ZIRCONIUM has used AES encrypted communications in C2.[5]

Enterprise T1041 Exfiltration Over C2 Channel

ZIRCONIUM has exfiltrated files via the Dropbox API C2.[5]

Enterprise T1567 .002 Exfiltration Over Web Service: Exfiltration to Cloud Storage

ZIRCONIUM has exfiltrated stolen data to Dropbox.[5]

Enterprise T1068 Exploitation for Privilege Escalation

ZIRCONIUM has exploited CVE-2017-0005 for local privilege escalation.[2]

Enterprise T1665 Hide Infrastructure

ZIRCONIUM has utilized an ORB (operational relay box) network – consisting compromised devices such as small office and home office (SOHO) routers, IoT devices, and leased virtual private servers (VPS) – to obfuscate the origin of C2 traffic.[7]

Enterprise T1105 Ingress Tool Transfer

ZIRCONIUM has used tools to download malicious files to compromised hosts.[5]

Enterprise T1036 Masquerading

ZIRCONIUM has spoofed legitimate applications in phishing lures and changed file extensions to conceal installation of malware.[4][5]

.004 Masquerade Task or Service

ZIRCONIUM has created a run key named `Dropbox Update Setup` to mask a persistence mechanism for a malicious binary.[5]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

ZIRCONIUM has used multi-stage packers for exploit code.[2]

Enterprise T1566 .002 Phishing: Spearphishing Link

ZIRCONIUM has used malicious links in e-mails to deliver malware.[1][4][5]

Enterprise T1598 Phishing for Information

ZIRCONIUM targeted presidential campaign staffers with credential phishing e-mails.[4]

.003 Spearphishing Link

ZIRCONIUM has used web beacons in e-mails to track hits to attacker-controlled URL's.[1]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

ZIRCONIUM has utilized an ORB (operational relay box) network – consisting compromised devices such as small office and home office (SOHO) routers, IoT devices, and leased virtual private servers (VPS) – to proxy traffic.[7]

Enterprise T1012 Query Registry

ZIRCONIUM has used a tool to query the Registry for proxy settings.[5]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

ZIRCONIUM has used the msiexec.exe command-line utility to download and execute malicious MSI files.[5]

Enterprise T1082 System Information Discovery

ZIRCONIUM has used a tool to capture the processor architecture of a compromised host in order to register it with C2.[5]

Enterprise T1016 System Network Configuration Discovery

ZIRCONIUM has used a tool to enumerate proxy settings in the target environment.[5]

Enterprise T1033 System Owner/User Discovery

ZIRCONIUM has used a tool to capture the username on a compromised host in order to register it with C2.[5]

Enterprise T1124 System Time Discovery

ZIRCONIUM has used a tool to capture the time on a compromised host in order to register it with C2.[5]

Enterprise T1204 .001 User Execution: Malicious Link

ZIRCONIUM has used malicious links in e-mails to lure victims into downloading malware.[4][5]

Enterprise T1102 .002 Web Service: Bidirectional Communication

ZIRCONIUM has used Dropbox for C2 allowing upload and download of files as well as execution of arbitrary commands.[4][5]

Source: https://attack.mitre.org/groups/G0128