Ke3chang, APT15, Mirage, Vixen Panda, GREF, Playful Dragon, RoyalAPT, NICKEL, Nylon Typhoon, Group G0004

Archived: 2026-04-05 17:35:43 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Ke3chang performs account discovery using commands such as `net localgroup administrators` and `net group "REDACTED" /domain` on specific permissions groups.[1]

.002 Account Discovery: Domain Account

Ke3chang performs account discovery using commands such as `net localgroup administrators` and `net group "REDACTED" /domain` on specific permissions groups.[1]

Enterprise T1583 .003 Acquire Infrastructure: Virtual Private Server

SPACEHOP Activity has used acquired Virtual Private Servers as control systems for devices within the ORB network.[6]

.005 Acquire Infrastructure: Botnet

Ke3chang has utilized an ORB (operational relay box) network for reconnaissance and vulnerability exploitation.[6]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Ke3chang malware including RoyalCli and BS2005 have communicated over HTTP with the C2 server through Internet Explorer (IE) by using the COM interface IWebBrowser2.[2][4]

.004 Application Layer Protocol: DNS

Ke3chang malware RoyalDNS has used DNS for C2.[2]

Enterprise T1560 Archive Collected Data

The Ke3chang group has been known to compress data before exfiltration.[1]

.001 Archive via Utility

Ke3chang is known to use 7Zip and RAR with passwords to encrypt data prior to exfiltration.[1][4]

Enterprise T1119 Automated Collection

Ke3chang has performed frequent and scheduled data collection from victim networks.[4]

Enterprise T1020 Automated Exfiltration

Ke3chang has performed frequent and scheduled data exfiltration from compromised networks.[4]

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

Several Ke3chang backdoors achieved persistence by adding a Run key.[2]

Enterprise T1059 Command and Scripting Interpreter

Malware used by Ke3chang can run commands on the command-line interface.[1][2]

.003 Windows Command Shell

Ke3chang has used batch scripts in its malware to install persistence mechanisms.[2]

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

Ke3chang backdoor RoyalDNS established persistence through adding a service called `Nwsapagent`.[2]

Enterprise T1213 .002 Data from Information Repositories: Sharepoint

Ke3chang used a SharePoint enumeration and data dumping tool known as spwebmember.[2]

Enterprise T1005 Data from Local System

Ke3chang gathered information and files from local directories for exfiltration.[1][4]

Enterprise T1140 Deobfuscate/Decode Files or Information

Ke3chang has deobfuscated Base64-encoded shellcode strings prior to loading them.[4]

Enterprise T1587 .001 Develop Capabilities: Malware

Ke3chang has developed custom malware that allowed them to maintain persistence on victim networks.[4]

Enterprise T1114 .002 Email Collection: Remote Email Collection

Ke3chang has used compromised credentials and a .NET tool to dump data from Microsoft Exchange mailboxes.[2][4]

Enterprise T1041 Exfiltration Over C2 Channel

Ke3chang transferred compressed and encrypted RAR files containing exfiltration through the established backdoor command and control channel during operations.[1]

Enterprise T1190 Exploit Public-Facing Application

Ke3chang has compromised networks by exploiting Internet-facing applications, including vulnerable Microsoft Exchange and SharePoint servers.[4]

SPACEHOP Activity has enabled the exploitation of CVE-2022-27518 and CVE-2022-27518 for illegitimate access.[7][6]

Enterprise T1133 External Remote Services

Ke3chang has gained access through VPNs including with compromised accounts and stolen VPN certificates.[2] [4]

Enterprise T1083 File and Directory Discovery

Ke3chang uses command-line interaction to search files and directories.[1][4]

Enterprise T1105 Ingress Tool Transfer

Ke3chang has used tools to download files to compromised machines.[4]

Enterprise T1056 .001 Input Capture: Keylogging

Ke3chang has used keyloggers.[2][4]

Enterprise T1036 .002 Masquerading: Right-to-Left Override

Ke3chang has used the right-to-left override character in spearphishing attachment names to trick targets into executing .scr and .exe files.[1]

.005 Masquerading: Match Legitimate Resource Name or Location

Ke3chang has dropped their malware into legitimate installed software paths including: `C:\ProgramFiles\Realtek\Audio\HDA\AERTSr.exe`, `C:\Program Files (x86)\Foxit Software\Foxit Reader\FoxitRdr64.exe`, `C:\Program Files (x86)\Adobe\Flash Player\AddIns\airappinstaller\airappinstall.exe`, and `C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd64.exe`.[4]

Enterprise T1027 Obfuscated Files or Information

Ke3chang has used Base64-encoded shellcode strings.[4]

Enterprise T1588 .002 Obtain Capabilities: Tool

Ke3chang has obtained and used tools such as Mimikatz.[2]

SPACEHOP Activity leverages a C2 framework sourced from a publicly-available Github repository for administration of relay nodes.[6]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Ke3chang has dumped credentials, including by using Mimikatz.[1][2][4]

.002 OS Credential Dumping: Security Account Manager

Ke3chang has dumped credentials, including by using gsecdump.[1][2]

.003 OS Credential Dumping: NTDS

Ke3chang has used NTDSDump and other password dumping tools to gather credentials.[4]

.004 OS Credential Dumping: LSA Secrets

Ke3chang has dumped credentials, including by using gsecdump.[1][2]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

Ke3chang performs discovery of permission groups `net group /domain` .[1]

Enterprise T1057 Process Discovery

Ke3chang performs process discovery using `tasklist` commands.[1][2]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

SPACEHOP Activity has routed traffic through chains of compromised network devices to proxy C2 communications.[6]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Ke3chang actors have been known to copy files to the network shares of other computers to move laterally.[1][2]

Enterprise T1018 Remote System Discovery

Ke3chang has used network scanning and enumeration tools, including Ping.[2]

Enterprise T1558 .001 Steal or Forge Kerberos Tickets: Golden Ticket

Ke3chang has used Mimikatz to generate Kerberos golden tickets.[2]

Enterprise T1082 System Information Discovery

Ke3chang performs operating system information discovery using `systeminfo` and has used implants to identify the system language and computer name.[1][2][4]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

Ke3chang has used implants to collect the system language ID of a compromised machine.[4]

Enterprise T1016 System Network Configuration Discovery

Ke3chang has performed local network configuration discovery using `ipconfig`.[1][2][4]

Enterprise T1049 System Network Connections Discovery

Ke3chang performs local network connection discovery using `netstat`.[1][2]

Enterprise T1033 System Owner/User Discovery

Ke3chang has used implants capable of collecting the signed-in username.[4]

Enterprise T1007 System Service Discovery

Ke3chang performs service discovery using `net start` commands.[1]

Enterprise T1569 .002 System Services: Service Execution

Ke3chang has used a tool known as RemoteExec (similar to PsExec) to remotely execute batch scripts and binaries.[2]

Enterprise T1078 Valid Accounts

Ke3chang has used credential dumpers or stealers to obtain legitimate credentials, which they used to gain access to victim accounts.[4]

.004 Cloud Accounts

Ke3chang has used compromised credentials to sign into victims' Microsoft 365 accounts.[4]
