Associated Group Descriptions

| **Name** | **Description** |
| --- | --- |
| APT15 | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Mirage | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Vixen Panda | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[3]](https://web.archive.org/web/20180615122133/https:/www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/) |
| GREF | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Playful Dragon | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[3]](https://web.archive.org/web/20180615122133/https:/www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/) |
| RoyalAPT | [[3]](https://web.archive.org/web/20180615122133/https:/www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/) |
| NICKEL | [[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |

**ATT&CK® Navigator Layers**

Techniques Used

| **Domain** | **ID** | | **Name** | **Use** |
| --- | --- | --- | --- | --- |
| Enterprise | [T1087](https://attack.mitre.org/techniques/T1087) | [.001](https://attack.mitre.org/techniques/T1087/001) | [Account Discovery](https://attack.mitre.org/techniques/T1087): [Local Account](https://attack.mitre.org/techniques/T1087/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) performs account discovery using commands such as net localgroup administrators and net group "REDACTED" /domain on specific permissions groups.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs) |
|  |  | [.002](https://attack.mitre.org/techniques/T1087/002) | [Account Discovery](https://attack.mitre.org/techniques/T1087): [Domain Account](https://attack.mitre.org/techniques/T1087/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) performs account discovery using commands such as net localgroup administrators and net group "REDACTED" /domain on specific permissions groups.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs) |
| Enterprise | [T1071](https://attack.mitre.org/techniques/T1071) | [.001](https://attack.mitre.org/techniques/T1071/001) | [Application Layer Protocol](https://attack.mitre.org/techniques/T1071): [Web Protocols](https://attack.mitre.org/techniques/T1071/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) malware including RoyalCli and BS2005 have communicated over HTTP with the C2 server through Internet Explorer (IE) by using the COM interface IWebBrowser2.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
|  |  | [.004](https://attack.mitre.org/techniques/T1071/004) | [Application Layer Protocol](https://attack.mitre.org/techniques/T1071): [DNS](https://attack.mitre.org/techniques/T1071/004) | [Ke3chang](https://attack.mitre.org/groups/G0004) malware RoyalDNS has used DNS for C2.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1560](https://attack.mitre.org/techniques/T1560) | | [Archive Collected Data](https://attack.mitre.org/techniques/T1560) | The [Ke3chang](https://attack.mitre.org/groups/G0004) group has been known to compress data before exfiltration.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs) |
|  |  | [.001](https://attack.mitre.org/techniques/T1560/001) | [Archive via Utility](https://attack.mitre.org/techniques/T1560/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) is known to use 7Zip and RAR with passwords to encrypt data prior to exfiltration.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1119](https://attack.mitre.org/techniques/T1119) | | [Automated Collection](https://attack.mitre.org/techniques/T1119) | [Ke3chang](https://attack.mitre.org/groups/G0004) has performed frequent and scheduled data collection from victim networks.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1020](https://attack.mitre.org/techniques/T1020) | | [Automated Exfiltration](https://attack.mitre.org/techniques/T1020) | [Ke3chang](https://attack.mitre.org/groups/G0004) has performed frequent and scheduled data exfiltration from compromised networks.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1547](https://attack.mitre.org/techniques/T1547) | [.001](https://attack.mitre.org/techniques/T1547/001) | [Boot or Logon Autostart Execution](https://attack.mitre.org/techniques/T1547): [Registry Run Keys / Startup Folder](https://attack.mitre.org/techniques/T1547/001) | Several [Ke3chang](https://attack.mitre.org/groups/G0004) backdoors achieved persistence by adding a Run key.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1059](https://attack.mitre.org/techniques/T1059) | | [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) | Malware used by [Ke3chang](https://attack.mitre.org/groups/G0004) can run commands on the command-line interface.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
|  |  | [.003](https://attack.mitre.org/techniques/T1059/003) | [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used batch scripts in its malware to install persistence mechanisms.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1543](https://attack.mitre.org/techniques/T1543) | [.003](https://attack.mitre.org/techniques/T1543/003) | [Create or Modify System Process](https://attack.mitre.org/techniques/T1543): [Windows Service](https://attack.mitre.org/techniques/T1543/003) | [Ke3chang](https://attack.mitre.org/groups/G0004) backdoor RoyalDNS established persistence through adding a service called Nwsapagent.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1213](https://attack.mitre.org/techniques/T1213) | [.002](https://attack.mitre.org/techniques/T1213/002) | [Data from Information Repositories](https://attack.mitre.org/techniques/T1213): [Sharepoint](https://attack.mitre.org/techniques/T1213/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) used a SharePoint enumeration and data dumping tool known as spwebmember.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1005](https://attack.mitre.org/techniques/T1005) | | [Data from Local System](https://attack.mitre.org/techniques/T1005) | [Ke3chang](https://attack.mitre.org/groups/G0004) gathered information and files from local directories for exfiltration.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1140](https://attack.mitre.org/techniques/T1140) | | [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) | [Ke3chang](https://attack.mitre.org/groups/G0004) has deobfuscated Base64-encoded shellcode strings prior to loading them.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1587](https://attack.mitre.org/techniques/T1587) | [.001](https://attack.mitre.org/techniques/T1587/001) | [Develop Capabilities](https://attack.mitre.org/techniques/T1587): [Malware](https://attack.mitre.org/techniques/T1587/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) has developed custom malware that allowed them to maintain persistence on victim networks.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1114](https://attack.mitre.org/techniques/T1114) | [.002](https://attack.mitre.org/techniques/T1114/002) | [Email Collection](https://attack.mitre.org/techniques/T1114): [Remote Email Collection](https://attack.mitre.org/techniques/T1114/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used compromised credentials and a .NET tool to dump data from Microsoft Exchange mailboxes.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1041](https://attack.mitre.org/techniques/T1041) | | [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041) | [Ke3chang](https://attack.mitre.org/groups/G0004) transferred compressed and encrypted RAR files containing exfiltration through the established backdoor command and control channel during operations.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs) |
| Enterprise | [T1190](https://attack.mitre.org/techniques/T1190) | | [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190) | [Ke3chang](https://attack.mitre.org/groups/G0004) has compromised networks by exploiting Internet-facing applications, including vulnerable Microsoft Exchange and SharePoint servers.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1133](https://attack.mitre.org/techniques/T1133) | | [External Remote Services](https://attack.mitre.org/techniques/T1133) | [Ke3chang](https://attack.mitre.org/groups/G0004) has gained access through VPNs including with compromised accounts and stolen VPN certificates.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1083](https://attack.mitre.org/techniques/T1083) | | [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) | [Ke3chang](https://attack.mitre.org/groups/G0004) uses command-line interaction to search files and directories.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1105](https://attack.mitre.org/techniques/T1105) | | [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used tools to download files to compromised machines.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1056](https://attack.mitre.org/techniques/T1056) | [.001](https://attack.mitre.org/techniques/T1056/001) | [Input Capture](https://attack.mitre.org/techniques/T1056): [Keylogging](https://attack.mitre.org/techniques/T1056/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used keyloggers.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1036](https://attack.mitre.org/techniques/T1036) | [.002](https://attack.mitre.org/techniques/T1036/002) | [Masquerading](https://attack.mitre.org/techniques/T1036): [Right-to-Left Override](https://attack.mitre.org/techniques/T1036/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used the right-to-left override character in spearphishing attachment names to trick targets into executing .scr and .exe files.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs) |
|  |  | [.005](https://attack.mitre.org/techniques/T1036/005) | [Masquerading](https://attack.mitre.org/techniques/T1036): [Match Legitimate Name or Location](https://attack.mitre.org/techniques/T1036/005) | [Ke3chang](https://attack.mitre.org/groups/G0004) 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]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1027](https://attack.mitre.org/techniques/T1027) | | [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used Base64-encoded shellcode strings.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1588](https://attack.mitre.org/techniques/T1588) | [.002](https://attack.mitre.org/techniques/T1588/002) | [Obtain Capabilities](https://attack.mitre.org/techniques/T1588): [Tool](https://attack.mitre.org/techniques/T1588/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) has obtained and used tools such as [Mimikatz](https://attack.mitre.org/software/S0002).[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1003](https://attack.mitre.org/techniques/T1003) | [.001](https://attack.mitre.org/techniques/T1003/001) | [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [LSASS Memory](https://attack.mitre.org/techniques/T1003/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) has dumped credentials, including by using [Mimikatz](https://attack.mitre.org/software/S0002).[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
|  |  | [.002](https://attack.mitre.org/techniques/T1003/002) | [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [Security Account Manager](https://attack.mitre.org/techniques/T1003/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) has dumped credentials, including by using gsecdump.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
|  |  | [.003](https://attack.mitre.org/techniques/T1003/003) | [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [NTDS](https://attack.mitre.org/techniques/T1003/003) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used NTDSDump and other password dumping tools to gather credentials.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
|  |  | [.004](https://attack.mitre.org/techniques/T1003/004) | [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [LSA Secrets](https://attack.mitre.org/techniques/T1003/004) | [Ke3chang](https://attack.mitre.org/groups/G0004) has dumped credentials, including by using gsecdump.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1069](https://attack.mitre.org/techniques/T1069) | [.002](https://attack.mitre.org/techniques/T1069/002) | [Permission Groups Discovery](https://attack.mitre.org/techniques/T1069): [Domain Groups](https://attack.mitre.org/techniques/T1069/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) performs discovery of permission groups net group /domain.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs) |
| Enterprise | [T1057](https://attack.mitre.org/techniques/T1057) | | [Process Discovery](https://attack.mitre.org/techniques/T1057) | [Ke3chang](https://attack.mitre.org/groups/G0004) performs process discovery using tasklist commands.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1021](https://attack.mitre.org/techniques/T1021) | [.002](https://attack.mitre.org/techniques/T1021/002) | [Remote Services](https://attack.mitre.org/techniques/T1021): [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) actors have been known to copy files to the network shares of other computers to move laterally.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1018](https://attack.mitre.org/techniques/T1018) | | [Remote System Discovery](https://attack.mitre.org/techniques/T1018) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used network scanning and enumeration tools, including [Ping](https://attack.mitre.org/software/S0097).[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1558](https://attack.mitre.org/techniques/T1558) | [.001](https://attack.mitre.org/techniques/T1558/001) | [Steal or Forge Kerberos Tickets](https://attack.mitre.org/techniques/T1558): [Golden Ticket](https://attack.mitre.org/techniques/T1558/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used [Mimikatz](https://attack.mitre.org/software/S0002) to generate Kerberos golden tickets.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1082](https://attack.mitre.org/techniques/T1082) | | [System Information Discovery](https://attack.mitre.org/techniques/T1082) | [Ke3chang](https://attack.mitre.org/groups/G0004) performs operating system information discovery using systeminfo and has used implants to identify the system language and computer name.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1614](https://attack.mitre.org/techniques/T1614) | [.001](https://attack.mitre.org/techniques/T1614/001) | [System Location Discovery](https://attack.mitre.org/techniques/T1614): [System Language Discovery](https://attack.mitre.org/techniques/T1614/001) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used implants to collect the system language ID of a compromised machine.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1016](https://attack.mitre.org/techniques/T1016) | | [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) | [Ke3chang](https://attack.mitre.org/groups/G0004) has performed local network configuration discovery using ipconfig.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1049](https://attack.mitre.org/techniques/T1049) | | [System Network Connections Discovery](https://attack.mitre.org/techniques/T1049) | [Ke3chang](https://attack.mitre.org/groups/G0004) performs local network connection discovery using netstat.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1033](https://attack.mitre.org/techniques/T1033) | | [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used implants capable of collecting the signed-in username.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
| Enterprise | [T1007](https://attack.mitre.org/techniques/T1007) | | [System Service Discovery](https://attack.mitre.org/techniques/T1007) | [Ke3chang](https://attack.mitre.org/groups/G0004) performs service discovery using net start commands.[[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs) |
| Enterprise | [T1569](https://attack.mitre.org/techniques/T1569) | [.002](https://attack.mitre.org/techniques/T1569/002) | [System Services](https://attack.mitre.org/techniques/T1569): [Service Execution](https://attack.mitre.org/techniques/T1569/002) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used a tool known as RemoteExec (similar to [PsExec](https://attack.mitre.org/software/S0029)) to remotely execute batch scripts and binaries.[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) |
| Enterprise | [T1078](https://attack.mitre.org/techniques/T1078) | | [Valid Accounts](https://attack.mitre.org/techniques/T1078) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used credential dumpers or stealers to obtain legitimate credentials, which they used to gain access to victim accounts.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |
|  |  | [.004](https://attack.mitre.org/techniques/T1078/004) | [Cloud Accounts](https://attack.mitre.org/techniques/T1078/004) | [Ke3chang](https://attack.mitre.org/groups/G0004) has used compromised credentials to sign into victims’ Microsoft 365 accounts.[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) |

Software

| **ID** | **Name** | **References** | **Techniques** |
| --- | --- | --- | --- |
| [S0100](https://attack.mitre.org/software/S0100) | [ipconfig](https://attack.mitre.org/software/S0100) | [[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) | [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016) |
| [S0002](https://attack.mitre.org/software/S0002) | [Mimikatz](https://attack.mitre.org/software/S0002) | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/)[[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) | [Access Token Manipulation](https://attack.mitre.org/techniques/T1134): [SID-History Injection](https://attack.mitre.org/techniques/T1134/005), [Account Manipulation](https://attack.mitre.org/techniques/T1098), [Boot or Logon Autostart Execution](https://attack.mitre.org/techniques/T1547): [Security Support Provider](https://attack.mitre.org/techniques/T1547/005), [Credentials from Password Stores](https://attack.mitre.org/techniques/T1555), [Credentials from Password Stores](https://attack.mitre.org/techniques/T1555): [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004), [Credentials from Password Stores](https://attack.mitre.org/techniques/T1555): [Credentials from Web Browsers](https://attack.mitre.org/techniques/T1555/003), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [Security Account Manager](https://attack.mitre.org/techniques/T1003/002), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [LSASS Memory](https://attack.mitre.org/techniques/T1003/001), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [LSA Secrets](https://attack.mitre.org/techniques/T1003/004), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [DCSync](https://attack.mitre.org/techniques/T1003/006), [Rogue Domain Controller](https://attack.mitre.org/techniques/T1207), [Steal or Forge Authentication Certificates](https://attack.mitre.org/techniques/T1649), [Steal or Forge Kerberos Tickets](https://attack.mitre.org/techniques/T1558): [Silver Ticket](https://attack.mitre.org/techniques/T1558/002), [Steal or Forge Kerberos Tickets](https://attack.mitre.org/techniques/T1558): [Golden Ticket](https://attack.mitre.org/techniques/T1558/001), [Unsecured Credentials](https://attack.mitre.org/techniques/T1552): [Private Keys](https://attack.mitre.org/techniques/T1552/004), [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550): [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003), [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550): [Pass the Hash](https://attack.mitre.org/techniques/T1550/002) |
| [S0280](https://attack.mitre.org/software/S0280) | [MirageFox](https://attack.mitre.org/software/S0280) | [[3]](https://web.archive.org/web/20180615122133/https:/www.intezer.com/miragefox-apt15-resurfaces-with-new-tools-based-on-old-ones/) | [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059): [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003), [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140), [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574): [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), [System Information Discovery](https://attack.mitre.org/techniques/T1082), [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) |
| [S0691](https://attack.mitre.org/software/S0691) | [Neoichor](https://attack.mitre.org/software/S0691) | [[4]](https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe) | [Application Layer Protocol](https://attack.mitre.org/techniques/T1071): [Web Protocols](https://attack.mitre.org/techniques/T1071/001), [Data from Local System](https://attack.mitre.org/techniques/T1005), [Indicator Removal](https://attack.mitre.org/techniques/T1070), [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105), [Inter-Process Communication](https://attack.mitre.org/techniques/T1559): [Component Object Model](https://attack.mitre.org/techniques/T1559/001), [Modify Registry](https://attack.mitre.org/techniques/T1112), [System Information Discovery](https://attack.mitre.org/techniques/T1082), [System Location Discovery](https://attack.mitre.org/techniques/T1614): [System Language Discovery](https://attack.mitre.org/techniques/T1614/001), [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016), [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016): [Internet Connection Discovery](https://attack.mitre.org/techniques/T1016/001), [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) |
| [S0039](https://attack.mitre.org/software/S0039) | [Net](https://attack.mitre.org/software/S0039) | [[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) | [Account Discovery](https://attack.mitre.org/techniques/T1087): [Local Account](https://attack.mitre.org/techniques/T1087/001), [Account Discovery](https://attack.mitre.org/techniques/T1087): [Domain Account](https://attack.mitre.org/techniques/T1087/002), [Create Account](https://attack.mitre.org/techniques/T1136): [Local Account](https://attack.mitre.org/techniques/T1136/001), [Create Account](https://attack.mitre.org/techniques/T1136): [Domain Account](https://attack.mitre.org/techniques/T1136/002), [Indicator Removal](https://attack.mitre.org/techniques/T1070): [Network Share Connection Removal](https://attack.mitre.org/techniques/T1070/005), [Network Share Discovery](https://attack.mitre.org/techniques/T1135), [Password Policy Discovery](https://attack.mitre.org/techniques/T1201), [Permission Groups Discovery](https://attack.mitre.org/techniques/T1069): [Local Groups](https://attack.mitre.org/techniques/T1069/001), [Permission Groups Discovery](https://attack.mitre.org/techniques/T1069): [Domain Groups](https://attack.mitre.org/techniques/T1069/002), [Remote Services](https://attack.mitre.org/techniques/T1021): [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002), [Remote System Discovery](https://attack.mitre.org/techniques/T1018), [System Network Connections Discovery](https://attack.mitre.org/techniques/T1049), [System Service Discovery](https://attack.mitre.org/techniques/T1007), [System Services](https://attack.mitre.org/techniques/T1569): [Service Execution](https://attack.mitre.org/techniques/T1569/002), [System Time Discovery](https://attack.mitre.org/techniques/T1124) |
| [S0104](https://attack.mitre.org/software/S0104) | [netstat](https://attack.mitre.org/software/S0104) | [[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) | [System Network Connections Discovery](https://attack.mitre.org/techniques/T1049) |
| [S0439](https://attack.mitre.org/software/S0439) | [Okrum](https://attack.mitre.org/software/S0439) | [[5]](https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET_Okrum_and_Ketrican.pdf) | [Access Token Manipulation](https://attack.mitre.org/techniques/T1134): [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001), [Application Layer Protocol](https://attack.mitre.org/techniques/T1071): [Web Protocols](https://attack.mitre.org/techniques/T1071/001), [Archive Collected Data](https://attack.mitre.org/techniques/T1560): [Archive via Custom Method](https://attack.mitre.org/techniques/T1560/003), [Archive Collected Data](https://attack.mitre.org/techniques/T1560): [Archive via Utility](https://attack.mitre.org/techniques/T1560/001), [Boot or Logon Autostart Execution](https://attack.mitre.org/techniques/T1547): [Shortcut Modification](https://attack.mitre.org/techniques/T1547/009), [Boot or Logon Autostart Execution](https://attack.mitre.org/techniques/T1547): [Registry Run Keys / Startup Folder](https://attack.mitre.org/techniques/T1547/001), [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059): [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003), [Create or Modify System Process](https://attack.mitre.org/techniques/T1543): [Windows Service](https://attack.mitre.org/techniques/T1543/003), [Data Encoding](https://attack.mitre.org/techniques/T1132): [Standard Encoding](https://attack.mitre.org/techniques/T1132/001), [Data Obfuscation](https://attack.mitre.org/techniques/T1001): [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003), [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140), [Encrypted Channel](https://attack.mitre.org/techniques/T1573): [Symmetric Cryptography](https://attack.mitre.org/techniques/T1573/001), [Exfiltration Over C2 Channel](https://attack.mitre.org/techniques/T1041), [File and Directory Discovery](https://attack.mitre.org/techniques/T1083), [Hide Artifacts](https://attack.mitre.org/techniques/T1564): [Hidden Files and Directories](https://attack.mitre.org/techniques/T1564/001), [Indicator Removal](https://attack.mitre.org/techniques/T1070): [File Deletion](https://attack.mitre.org/techniques/T1070/004), [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105), [Input Capture](https://attack.mitre.org/techniques/T1056): [Keylogging](https://attack.mitre.org/techniques/T1056/001), [Masquerading](https://attack.mitre.org/techniques/T1036): [Masquerade Task or Service](https://attack.mitre.org/techniques/T1036/004), [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027): [Steganography](https://attack.mitre.org/techniques/T1027/003), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [Cached Domain Credentials](https://attack.mitre.org/techniques/T1003/005), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003): [LSASS Memory](https://attack.mitre.org/techniques/T1003/001), [Proxy](https://attack.mitre.org/techniques/T1090): [External Proxy](https://attack.mitre.org/techniques/T1090/002), [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053): [Scheduled Task](https://attack.mitre.org/techniques/T1053/005), [System Information Discovery](https://attack.mitre.org/techniques/T1082), [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1016), [System Network Connections Discovery](https://attack.mitre.org/techniques/T1049), [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033), [System Services](https://attack.mitre.org/techniques/T1569): [Service Execution](https://attack.mitre.org/techniques/T1569/002), [System Time Discovery](https://attack.mitre.org/techniques/T1124), [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497): [System Checks](https://attack.mitre.org/techniques/T1497/001), [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497): [User Activity Based Checks](https://attack.mitre.org/techniques/T1497/002), [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497): [Time Based Evasion](https://attack.mitre.org/techniques/T1497/003) |
| [S0097](https://attack.mitre.org/software/S0097) | [Ping](https://attack.mitre.org/software/S0097) | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) | [Remote System Discovery](https://attack.mitre.org/techniques/T1018) |
| [S0227](https://attack.mitre.org/software/S0227) | [spwebmember](https://attack.mitre.org/software/S0227) | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) | [Data from Information Repositories](https://attack.mitre.org/techniques/T1213): [Sharepoint](https://attack.mitre.org/techniques/T1213/002) |
| [S0096](https://attack.mitre.org/software/S0096) | [Systeminfo](https://attack.mitre.org/software/S0096) | [[1]](https://www.mandiant.com/resources/operation-ke3chang-targeted-attacks-against-ministries-of-foreign-affairs)[[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) | [System Information Discovery](https://attack.mitre.org/techniques/T1082) |
| [S0057](https://attack.mitre.org/software/S0057) | [Tasklist](https://attack.mitre.org/software/S0057) | [[2]](https://research.nccgroup.com/2018/03/10/apt15-is-alive-and-strong-an-analysis-of-royalcli-and-royaldns/) | [Process Discovery](https://attack.mitre.org/techniques/T1057), [Software Discovery](https://attack.mitre.org/techniques/T1518): [Security Software Discovery](https://attack.mitre.org/techniques/T1518/001), [System Service Discovery](https://attack.mitre.org/techniques/T1007) |