

## PikaBot Is Back With a Vengeance - Part 2

Published: 2023-11-19 · Archived: 2026-04-06 00:57:37 UTC

```
Key string: b'l9SpFBoXEyglbY0ginoTUBd=pP=y6rVcQG8tP/zV4iqr06yZKEb+VCg1yQJ5jUNE'  
Key: 6c39537046426f584579676c62593067696e6f545542643d70503d7936725663  
IV string: b'FdbAwsDj0FJcgkLPb1J/mqGU7T6e98p9CMnoB'  
IV: 466462417773446a30464a63676b4c50  
Decrypted: b'{"mdPNC6f8": "%s", "NUn3h77h": "%s", "W381C": "Win %d.%d %d", "SJ3sWSeKQ": %s, "YlSwktC  
Decrypted: b'CreateMutexW'  
Decrypted: b'GetLastError'  
Decrypted: b'%s'  
Decrypted: b'wsprintfA'  
Decrypted: b'&  
Decrypted: b'&tfDgx='  
Decrypted: b'whoami.exe /all'  
Decrypted: b'&M1LWU='  
Decrypted: b'ipconfig.exe /all'  
Decrypted: b'&VC76f='  
Decrypted: b'netstat.exe -aon'  
Decrypted: b'&SBS10='  
Decrypted: b'{"mdPNC6f8": "%s"}'  
Decrypted: b'wsprintfA'  
Decrypted: b'{"mdPNC6f8": "%s"}'  
Decrypted: b'wsprintfA'  
Decrypted: b'HydrohemothoraxCoenaesthesia/2bQbdHQI1z9PoD?SnarlishAllobars=59eYpYysBS&UndoubtableEthn  
Decrypted: b'&  
Decrypted: b'BaylZ'  
Decrypted: b'AV89JS'  
Decrypted: b'IsWow64Process'  
Decrypted: b'GetProductInfo'  
Decrypted: b'%d'  
Decrypted: b'wsprintfW'  
Decrypted: b'unknown'  
Decrypted: b'GetComputerNameW'  
Decrypted: b'unknown'  
Decrypted: b'GetComputerNameExW'  
Decrypted: b'unknown'  
Decrypted: b'DsGetDcNameW'  
Decrypted: b'unknown'  
Decrypted: b'EnumDisplayDevicesW'  
Decrypted: b'GlobalMemoryStatusEx'  
Decrypted: b'GetDesktopWindow'  
Decrypted: b'GetWindowRect'
```

Decrypted: b'%dx%d'  
Decrypted: b'wsprintfW'  
Decrypted: b'unknown'  
Decrypted: b'GetTickCount'  
Decrypted: b'OpenProcessToken'  
Decrypted: b'GetCurrentProcess'  
Decrypted: b'GetTokenInformation'  
Decrypted: b'Kernel32.dll'  
Decrypted: b'User32.dll'  
Decrypted: b'Wininet.dll'  
Decrypted: b'Advapi32.dll'  
Decrypted: b'NetApi32.dll'  
Decrypted: b'MultiByteToWideChar'  
Decrypted: b'WaitForSingleObjectEx'  
Decrypted: b'GetTickCount'  
Decrypted: b'%s&%s'  
Decrypted: b'UndoubtableEthnologically=antitwilightFluidextract&birefractingUndeaitfulness=huehuetl  
Decrypted: b'UdvGU='  
Decrypted: b'wsprintfA'  
Decrypted: b'POST'  
Decrypted: b'%s&%s'  
Decrypted: b'UndoubtableEthnologically=antitwilightFluidextract&birefractingUndeaitfulness=huehuetl  
Decrypted: b'UdvGU='  
Decrypted: b'wsprintfA'  
Decrypted: b'POST'  
Decrypted: b'{"mdPNC6f8": "%s", "MsDkQb2T": %s, "jVeNAqf": %d, "5ScPjT": "'  
Decrypted: b'"}'  
Decrypted: b'wsprintfA'  
Decrypted: b'fabledOverstridence/h31BYUqJ28W62tz?nonresister=jYnT8Hj13x&Sixtine=TXEWWGZ&DogvaneHered  
Decrypted: b'InternetOpenW'  
Decrypted: b'&  
Decrypted: b'HttpOpenRequestW'  
Decrypted: b'InternetQueryOptionW'  
Decrypted: b'Content-Type: application/x-www-form-urlencoded\r\nAccept: \*/\*\r\nAccept-Language: en-U  
Decrypted: b'lstrlenW'  
Decrypted: b'lstrlenA'  
Decrypted: b'HttpSendRequestW'  
Decrypted: b'InternetReadFile'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetSetOptionW'  
Decrypted: b'InternetOpenW'  
Decrypted: b'&  
Decrypted: b'InternetConnectW'

Decrypted: b'HttpOpenRequestW'  
Decrypted: b'InternetQueryOptionW'  
Decrypted: b'Content-Type: application/x-www-form-urlencoded\r\nAccept: \*/\*\r\nAccept-Language: en-U'  
Decrypted: b'lstrlenA'  
Decrypted: b'HttpSendRequestW'  
Decrypted: b'InternetReadFile'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetSetOptionW'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetCloseHandle'  
Decrypted: b'InternetReadFile'  
Decrypted: b'RegCreateKeyExW'  
Decrypted: b'RegSetValueExW'  
Decrypted: b'RegCloseKey'  
Decrypted: b'RegOpenKeyExW'  
Decrypted: b'RegQueryValueExW'  
Decrypted: b'RegCloseKey'  
Decrypted: b'RegCloseKey'  
Decrypted: b'C:\\'  
Decrypted: b'GetVolumeInformationW'  
Decrypted: b'%s\\%s|%s'  
Decrypted: b'wsprintfW'  
Decrypted: b'%07lX%09lX%lu'  
Decrypted: b'wsprintfW'  
Decrypted: b'GetUserDefaultLangID'  
Decrypted: b'%appdata%\Microsoft\\'  
Decrypted: b'lotterSig'  
Decrypted: b'\\'  
Decrypted: b'ExpandEnvironmentStringsW'  
Decrypted: b'GetFileAttributesW'  
Decrypted: b'Synanthic'  
Decrypted: b'.dll'  
Decrypted: b'.exe'  
Decrypted: b'CreateFileW'  
Decrypted: b'WriteFile'  
Decrypted: b'CloseHandle'  
Decrypted: b'CreateDirectoryW'  
Decrypted: b'&'  
Decrypted: b'SOFTWARE\\Microsoft\\%s'  
Decrypted: b'lotterSig'  
Decrypted: b'Subadmini'  
Decrypted: b'wsprintfW'

Decrypted: b'{"mdPNC6f8": "%s", "NUn3h77h": "%s", "W381C": "Win %d.%d %d", "SJ3sWSeKQ": %s, "YlSwktC  
Decrypted: b'GG9TU@T@f0adda360d2b4ccda11468e026526576'  
Decrypted: b'wsprintfW'  
Decrypted: b'AV89JS'  
Decrypted: b'TrichinopolyUncontriving/uiDV6mKfgGakdg?unshelledSplitnut=vEzLHkL'  
Decrypted: b'&  
Decrypted: b'SOFTWARE\\Microsoft\\%s'  
Decrypted: b'lotterSig'  
Decrypted: b'Subadmini'  
Decrypted: b'wsprintfW'  
Decrypted: b'CreateToolhelp32Snapshot'  
Decrypted: b'Process32FirstW'  
Decrypted: b'CloseHandle'  
Decrypted: b'Process32NextW'  
Decrypted: b'explorer.exe'  
Decrypted: b'OpenProcess'  
Decrypted: b'CloseHandle'  
Decrypted: b'InitializeProcThreadAttributeList'  
Decrypted: b'InitializeProcThreadAttributeList'  
Decrypted: b'UpdateProcThreadAttribute'  
Decrypted: b>DeleteProcThreadAttributeList'  
Decrypted: b'NvtocV4e'  
Decrypted: b'UpdateProcThreadAttribute'  
Decrypted: b'InitializeProcThreadAttributeList'  
Decrypted: b'InitializeProcThreadAttributeList'  
Decrypted: b'UpdateProcThreadAttribute'  
Decrypted: b'CreateProcessW'  
Decrypted: b>DeleteProcThreadAttributeList'  
Decrypted: b'UpdateProcThreadAttribute'  
Decrypted: b'IsWow64Process'  
Decrypted: b'CreateToolhelp32Snapshot'  
Decrypted: b'Process32FirstW'  
Decrypted: b '['  
Decrypted: b'"%s:%d:%d:%d:%d:%d:%d"  
Decrypted: b', "%s:%d:%d:%d:%d:%d:%d"  
Decrypted: b']'  
Decrypted: b'wsprintfW'  
Decrypted: b'Process32NextW'  
Decrypted: b'wsprintfW'  
Decrypted: b'CloseHandle'  
Decrypted: b'CloseHandle'  
Decrypted: b'wsprintfW'  
Decrypted: b'wsprintfW'  
Decrypted: b'CreatePipe'  
Decrypted: b'CreateProcessW'  
Decrypted: b'CloseHandle'  
Decrypted: b'CloseHandle'

Decrypted: b'CloseHandle'  
Decrypted: b'CloseHandle'  
Decrypted: b'CloseHandle'  
Decrypted: b'CloseHandle'  
Decrypted: b'WaitForSingleObject'  
Decrypted: b'PeekNamedPipe'  
Decrypted: b'ReadFile'  
Decrypted: b'CloseHandle'  
Decrypted: b'CloseHandle'  
Decrypted: b'CloseHandle'  
Decrypted: b'&'  
Decrypted: b'NvtocV4e'  
Decrypted: b'{"mdPNC6f8": "%s", "isjuuMr": "%s", "MsDkQb2T": %s}'  
Decrypted: b'wsprintfA'  
Decrypted: b'nanoinstructionFrisesororum/XjqtQzQyyeNZVoIQ?unapplicability=i73MV07GwaCH13Q'  
Decrypted: b'BayLZ'  
Decrypted: b'ExpandEnvironmentStringsW'  
Decrypted: b'&'  
Decrypted: b'{"mdPNC6f8": "%s", "isjuuMr": "%s", "MsDkQb2T": %s}'  
Decrypted: b'wsprintfA'  
Decrypted: b'nanoinstructionFrisesororum/XjqtQzQyyeNZVoIQ?unapplicability=i73MV07GwaCH13Q'  
Decrypted: b'BayLZ'  
Decrypted: b'ExpandEnvironmentStringsW'  
Decrypted: b'{"mdPNC6f8": "%s", "isjuuMr": "%s", "MsDkQb2T": %s}'  
Decrypted: b'wsprintfA'  
Decrypted: b'nanoinstructionFrisesororum/XjqtQzQyyeNZVoIQ?unapplicability=i73MV07GwaCH13Q'  
Decrypted: b'&'  
Decrypted: b'qqmyS'  
Decrypted: b'tK5nVvwh'  
Decrypted: b'mGTYP'  
Decrypted: b'2bjHya'  
Decrypted: b'whoami.exe /all'  
Decrypted: b'ipconfig.exe /all'  
Decrypted: b'netstat.exe -aon'  
Decrypted: b'&'  
Decrypted: b'dLmghDRe'  
Decrypted: b'ExitProcess'  
Decrypted: b'&'  
Decrypted: b'&'  
Decrypted: b'bustlingly/e9vLiMRRWKSd?DeediestBromes=awIAh8S&bonaght=5vh1psTtP2mk9&stiltyKetoHexose=j  
Decrypted: b'Software\\Microsoft\\Windows\\CurrentVersion\\Run'  
Decrypted: b'Synanthic'  
Decrypted: b'rundll32'  
Decrypted: b'.dll'  
Decrypted: b'wsprintfW'  
Decrypted: b'.exe'  
Decrypted: b'wsprintfW'

```
Decrypted: b'&'
Decrypted: b'HxTPXf'
Decrypted: b'yAJsnWxR'
Decrypted: b'4qRRAR0'
Decrypted: b'NvtocV4e'
Decrypted: b'qo9g3J'
Decrypted: b'GhPTR'
Decrypted: b'dLmghDRe'
Decrypted: b'9PpreQMX'
Decrypted: b'pKW7fqi2'
Rejected:
b'{F542086F-F5EF-48C4-8B12-49ED805B0205}'
b'0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz/='+
b'l9SpFB0XEyglbY0ginoTUBd=pP=y6rVcQG8tP/zV4iqr06yZKEb+VCg1yQJ5jUNE'
b'FdbAwsDj0FJcgkLPb1J/mqGU7T6e98p9CMnoB'
b'\x19<jcy]X\r]'
b'1.1.15-ghost'
b'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
b'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
b'%s "%s%s%s", %s'
b'LJK\x03\x190'
{'strings': [{'offset': 5621, 'value': 'CreateMutexW'}, {'offset': 6224, 'value': 'GetLastError'}, {
```

---

Source: <https://research.openanalysis.net/pikabot/debugging/string%20decryption/emulation/memulator/2023/11/19/new-pikabot-strings.html>