KOCTOPUS, Software S0669 | MITRE ATT&CK®

Archived: 2026-04-05 17:12:27 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

KOCTOPUS will perform UAC bypass either through fodhelper.exe or eventvwr.exe.[1]

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

KOCTOPUS can set the AutoRun Registry key with a PowerShell command.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

KOCTOPUS has used PowerShell commands to download additional files.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

KOCTOPUS has used `cmd.exe` and batch files for execution.[1]

.005 Command and Scripting Interpreter: Visual Basic

KOCTOPUS has used VBScript to call wscript to execute a PowerShell command.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

KOCTOPUS has deobfuscated itself before executing its commands.[1]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

KOCTOPUS has used `-WindowsStyle Hidden` to hide the command window.[1]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

KOCTOPUS will attempt to delete or disable all Registry keys and scheduled tasks related to Microsoft Security Defender and Security Essentials.[1]

Enterprise T1070 .009 Indicator Removal: Clear Persistence

KOCTOPUS can delete created registry keys used for persistence as part of its cleanup procedure.[1]

Enterprise T1105 Ingress Tool Transfer

KOCTOPUS has executed a PowerShell command to download a file to the system.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

KOCTOPUS has been disguised as legitimate software programs associated with the travel and airline industries.[2]

Enterprise T1112 Modify Registry

KOCTOPUS has added and deleted keys from the Registry.[1]

Enterprise T1106 Native API

KOCTOPUS can use the `LoadResource` and `CreateProcessW` APIs for execution.[1]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

KOCTOPUS has obfuscated scripts with the BatchEncryption tool.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

KOCTOPUS has been distributed via spearphishing emails with malicious attachments.[1]

.002 Phishing: Spearphishing Link

KOCTOPUS has been distributed as a malicious link within an email.[1]

Enterprise T1090 Proxy

KOCTOPUS has deployed a modified version of Invoke-Ngrok to expose open local ports to the Internet.[1]

Enterprise T1082 System Information Discovery

KOCTOPUS has checked the OS version using `wmic.exe` and the `find` command.[1]

Enterprise T1204 .001 User Execution: Malicious Link

KOCTOPUS has relied on victims clicking on a malicious link delivered via email.[1]

.002 User Execution: Malicious File

KOCTOPUS has relied on victims clicking a malicious document for execution.[1]
