Command and Scripting Interpreter: Visual Basic, Sub-technique T1059.005 - Enterprise

Archived: 2026-04-05 18:25:07 UTC

C0028 2015 Ukraine Electric Power Attack

During the 2015 Ukraine Electric Power Attack, Sandworm Team installed a VBA script called `vba_macro.exe`. This macro dropped `FONTCACHE.DAT`, the primary BlackEnergy implant; `rundll32.exe`, for executing the malware; `NTUSER.log`, an empty file; and desktop.ini, the default file used to determine folder displays on Windows machines. [7]

C0025 2016 Ukraine Electric Power Attack

During the 2016 Ukraine Electric Power Attack, Sandworm Team created VBScripts to run on an SSH server.[8]

G0099 APT-C-36

APT-C-36 has embedded a VBScript within a malicious Word document which is executed upon the document opening.[9]

G0050 APT32

APT32 has used macros, COM scriptlets, and VBS scripts.[10][11]

G0064 APT33

APT33 has used VBScript to initiate the delivery of payloads.[12]

G0067 APT37

APT37 executes shellcode and a VBA script to decode Base64 strings.[13]

G0082 APT38

APT38 has used VBScript to execute commands and other operational tasks.[14][15]

G0087 APT39

APT39 has utilized malicious VBS scripts in malware.[16]

G1044 APT42

APT42 has used a VBScript to query anti-virus products.[17]

S0373 Astaroth

Astaroth has used malicious VBS e-mail attachments for execution.[18]

S0414 BabyShark

BabyShark can execute additional VisualBasic content.[19]

S0475 BackConfig

BackConfig has used VBS to install its downloader component and malicious documents with VBA macro code.[20]

S0234 Bandook

Bandook has used malicious VBA code against the target system.[21]

S0268 Bisonal

Bisonal's dropper creates VBS scripts on the victim’s machine.[22][23]

G0060 BRONZE BUTLER

BRONZE BUTLER has used VBS and VBE scripts for execution.[24][25]

S1039 Bumblebee

Bumblebee can create a Visual Basic script to enable persistence.[26][27]

C0011 C0011

For C0011, Transparent Tribe used malicious VBA macros within a lure document as part of the Crimson malware installation process onto a compromised host.[28]

C0015 C0015

During C0015, the threat actors used a malicious HTA file that contained a mix of HTML and JavaScript/VBScript code.[29]

S0631 Chaes

Chaes has used VBscript to execute malicious code.[30]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP has executed a script named cln.vbs on compromised hosts.[31]

G0080 Cobalt Group

Cobalt Group has sent Word OLE compound documents with malicious obfuscated VBA macros that will run upon user execution.[32][33][34][35][36][37]

S0154 Cobalt Strike

Cobalt Strike can use VBA to perform execution.[38][39][40]

S0244 Comnie

Comnie executes VBS scripts.[41]

G0142 Confucius

Confucius has used VBScript to execute malicious code.[42]

G1052 Contagious Interview

Contagious Interview has utilized Visual Basic scripts in the execution of their downloader malware targeting Windows devices including as script called update.vbs.[43]

S1014 DanBot

DanBot can use a VBA macro embedded in an Excel file to drop the payload.[44]

S1111 DarkGate

DarkGate initial infection mechanisms include masquerading as pirated media that launches malicious VBScript on the victim.[45]

S0695 Donut

Donut can generate shellcode outputs that execute via VBScript.[46]

G1006 Earth Lusca

Earth Lusca used VBA scripts.[47]

S0367 Emotet

Emotet has sent Microsoft Word documents with embedded macros that will invoke scripts to download additional payloads. [48][49][50][51][52]

S0343 Exaramel for Windows

Exaramel for Windows has a command to execute VBS scripts on the victim’s machine.[53]

S0679 Ferocious

Ferocious has the ability to use Visual Basic scripts for execution.[54]

G1016 FIN13

FIN13 has used VBS scripts for code execution on comrpomised machines.[55]

G0085 FIN4

FIN4 has used VBA macros to display a dialog box and collect victim credentials.[56][57]

G0046 FIN7

FIN7 used VBS scripts to help perform tasks on the victim's machine.[58][59][60]

S0696 Flagpro

Flagpro can execute malicious VBA macros embedded in .xlsm files.[61]

C0001 Frankenstein

During Frankenstein, the threat actors used Word documents that prompted the victim to enable macros and run a Visual Basic script.[62]

C0007 FunnyDream

During FunnyDream, the threat actors used a Visual Basic script to run remote commands.[63]

G0047 Gamaredon Group

Gamaredon Group has embedded malicious macros in document templates, which executed VBScript. Gamaredon Group has also delivered Microsoft Outlook VBA projects with embedded macros.[64][65][66][67][68][69] Additionally, Gamaredon Group has executed VBScript files using wscript.exe.[70]

S0477 Goopy

Goopy has the ability to use a Microsoft Outlook backdoor macro to communicate with its C2.[11]

G0078 Gorgon Group

Gorgon Group has used macros in Spearphishing Attachments as well as executed VBScripts on victim machines.[71]

S0531 Grandoreiro

Grandoreiro can use VBScript to execute malicious code.[18][72]

S0170 Helminth

One version of Helminth consists of VBScript scripts.[73]

G1001 HEXANE

HEXANE has used a VisualBasic script named `MicrosoftUpdator.vbs` for execution of a PowerShell keylogger.[74]

G0126 Higaisa

Higaisa has used VBScript code on the victim's machine.[75]

S0483 IcedID

IcedID has used obfuscated VBA string expressions.[76]

G0100 Inception

Inception has used VBScript to execute malicious commands and payloads.[77][78]

S1132 IPsec Helper

IPsec Helper can run arbitrary Visual Basic scripts and commands passed to it.[79]

S0528 Javali

Javali has used embedded VBScript to download malicious payloads from C2.[18]

S0389 JCry

JCry has used VBS scripts. [80]

S0283 jRAT

jRAT has been distributed as HTA files with VBScript.[81]

S0648 JSS Loader

JSS Loader can download and execute VBScript files.[60]

C0044 Juicy Mix

During Juicy Mix, OilRig used VBS droppers to deliver and establish persistence for the Mango backdoor.[82]

S0585 Kerrdown

Kerrdown can use a VBS base64 decoder function published by Motobit.[83]

S0387 KeyBoy

KeyBoy uses VBS scripts for installing files and performing execution.[84]

G0094 Kimsuky

Kimsuky has used Visual Basic to download malicious payloads.[85][86][87][88] Kimsuky has also used malicious VBA macros within maldocs disguised as forms that trigger when a victim types any content into the lure.[88]

S0250 Koadic

Koadic performs most of its operations using Windows Script Host (VBScript) and runs arbitrary shellcode .[89]

S0669 KOCTOPUS

KOCTOPUS has used VBScript to call wscript to execute a PowerShell command.[90]

G0032 Lazarus Group

Lazarus Group has used VBA and embedded macros in Word documents to execute malicious code.[91][92]

G0140 LazyScripter

LazyScripter has used VBScript to execute malicious code.[90]

G0065 Leviathan

Leviathan has used VBScript.[93]

S0447 Lokibot

Lokibot has used VBS scripts and XLS macros for execution.[94]

S0582 LookBack

LookBack has used VBA macros in Microsoft Word attachments to drop additional files to the host.[95]

S1142 LunarMail

LunarMail has been installed using a VBA macro.[96]

G0095 Machete

Machete has embedded malicious macros within spearphishing attachments to download additional files.[97]

G0059 Magic Hound

Magic Hound malware has used VBS scripts for execution.[98]

G1026 Malteiro

Malteiro has utilized a dropper containing malicious VBS scripts.[99]

S0530 Melcoz

Melcoz can use VBS scripts to execute malicious DLLs.[18]

S0455 Metamorfo

Metamorfo has used VBS code on victims' systems.[100]

S1122 Mispadu

Mispadu's dropper uses VBS files to install payloads and perform execution.[99][101]

G0021 Molerats

Molerats used various implants, including those built with VBScript, on target machines.[102][103]

G0069 MuddyWater

MuddyWater has used VBScript files to execute its POWERSTATS payload, as well as macros.[104][105][106][107][108][109][110][111][112]

G0129 Mustang Panda

Mustang Panda has embedded VBScript components in LNK files to download additional files and automate collection.[113][114][115] Mustang Panda has also used VBA macros in maldocs to execute malicious DLLs.[116] Mustang Panda also utilized a VBS Script "autorun.vbs" that created persistence through saving the VBS Script in the startup directory which would cause it to run each time the machine was turned on.[117]

S0228 NanHaiShu

NanHaiShu executes additional VBScript code on the victim's machine.[118]

S0336 NanoCore

NanoCore uses VBS files.[119]

S0198 NETWIRE

NETWIRE has been executed through use of VBScripts.[120][121]

G0049 OilRig

OilRig has used VBScript macros for execution on compromised hosts.[122]

S0264 OopsIE

OopsIE creates and uses a VBScript as part of its persistent execution.[123][124]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors executed an encoded VBScript file using `wscript` and wrote the decoded output to a text file.[125]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group executed a VBA written malicious macro after victims download malicious DOTM files; Lazarus Group also used Visual Basic macro code to extract a double Base64 encoded DLL implant.[126][127]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors used Visual Basic scripts.[128]

C0006 Operation Honeybee

For Operation Honeybee, the threat actors used a Visual Basic script embedded within a Word document to download an implant.[129]

C0013 Operation Sharpshooter

During Operation Sharpshooter, the threat actors used a VBA macro to execute a simple downloader that installed Rising Sun.[130]

C0014 Operation Wocao

During Operation Wocao, threat actors used VBScript to conduct reconnaissance on targeted systems.[131]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D uses Word macros for execution.[132]

C0042 Outer Space

During Outer Space, OilRig used VBS droppers to deploy malware.[82]

G0040 Patchwork

Patchwork used Visual Basic Scripts (VBS) on victim machines.[133][134]

S0428 PoetRAT

PoetRAT has used Word documents with VBScripts to execute malicious activities.[135][136]

S0441 PowerShower

PowerShower has the ability to save and execute VBScript.[77]

S0223 POWERSTATS

POWERSTATS can use VBScript (VBE) code for execution.[108][137]

S0147 Pteranodon

Pteranodon can use a malicious VBS file for execution.[138]

S0650 QakBot

QakBot can use VBS to download and execute malicious files.[139]
[140][141][142][143][144][145]

S0269 QUADAGENT

QUADAGENT uses VBScripts.[146]

S0458 Ramsay

Ramsay has included embedded Visual Basic scripts in malicious documents.[147][148]

G0075 Rancor

Rancor has used VBS scripts as well as embedded macros for execution.[149]

G1039 RedCurl

RedCurl has used VBScript to run malicious files.[150][151]

S0375 Remexi

Remexi uses AutoIt and VBS scripts throughout its execution process.[152]

S0496 REvil

REvil has used obfuscated VBA macros for execution.[153][154]

S0240 ROKRAT

ROKRAT has used Visual Basic for execution.[155]

S1018 Saint Bot

Saint Bot has used `.vbs` scripts for execution.[156]

G0034 Sandworm Team

Sandworm Team has created VBScripts to run an SSH server.[157][158][159][8]

S1178 ShrinkLocker

ShrinkLocker is a VisualBasic script (VBS) object that calls multiple other operating system functions during execution.[160][161]

S0589 Sibot

Sibot executes commands using VBScript.[162]

G1008 SideCopy

SideCopy has sent Microsoft Office Publisher documents to victims that have embedded malicious macros that execute an hta file via calling `mshta.exe`.[163]

G0121 Sidewinder

Sidewinder has used VBScript to drop and execute malware loaders.[164]

G0091 Silence

Silence has used VBS scripts.[165]

S0226 Smoke Loader

Smoke Loader adds a Visual Basic script in the Startup folder to deploy the payload.[166]

S1086 Snip3

Snip3 can use visual basic scripts for first-stage execution.[167][168]

C0024 SolarWinds Compromise

For the SolarWinds Compromise, APT29 wrote malware such as Sibot in Visual Basic.[169]

S1030 Squirrelwaffle

Squirrelwaffle has used malicious VBA macros in Microsoft Word documents and Excel spreadsheets that execute an `AutoOpen` subroutine.[170][171]

S1037 STARWHALE

STARWHALE can use the VBScript function `GetRef` as part of its persistence mechanism.[172]

S0380 StoneDrill

StoneDrill has several VBS scripts used throughout the malware's lifecycle.[173]

S0559 SUNBURST

SUNBURST used VBScripts to initiate the execution of payloads.[174]

S1064 SVCReady

SVCReady has used VBA macros to execute shellcode.[175]

G1018 TA2541

TA2541 has used VBS files to execute or establish persistence for additional payloads, often using file names consistent with email themes or mimicking system functionality.[176][177]

G0062 TA459

TA459 has a VBScript for execution.[178]

G0092 TA505

TA505 has used VBS for code execution.[179][180][181][182]

S1193 TAMECAT

TAMECAT has used VBScript to query anti-virus products.[17]

G0134 Transparent Tribe

Transparent Tribe has crafted VBS-based malicious documents.[183][184]

G0010 Turla

Turla has used VBS scripts throughout its operations.[185]

S0263 TYPEFRAME

TYPEFRAME has used a malicious Word document for delivery with VBA macros for execution.[186]

S0386 Ursnif

Ursnif droppers have used VBA macros to download and execute the malware's full executable payload.[187]

S0442 VBShower

VBShower has the ability to execute VBScript files.[188]

S0689 WhisperGate

WhisperGate can use a Visual Basic script to exclude the `C:\` drive from Windows Defender.[189][190]

G0112 Windshift

Windshift has used Visual Basic 6 (VB6) payloads.[191]

G0090 WIRTE

WIRTE has used VBScript in its operations.[192]

S0341 Xbash

Xbash can execute malicious VBScript payloads on the victim’s machine.[193]

Source: https://attack.mitre.org/techniques/T1059/005