Obfuscated Files or Information: Software Packing, Sub-technique T1027.002 - Enterprise

Archived: 2026-04-05 12:55:37 UTC

C0025 2016 Ukraine Electric Power Attack

During the 2016 Ukraine Electric Power Attack, Sandworm Team used UPX to pack a copy of Mimikatz.[3]

S0504 Anchor

Anchor has come with a packed payload.[4]

G1007 Aoqin Dragon

Aoqin Dragon has used the Themida packer to obfuscate malicious payloads.[5]

S0622 AppleSeed

AppleSeed has used UPX packers for its payload DLL.[6]

G0016 APT29

APT29 used UPX to pack files.[7]

G0022 APT3

APT3 has been known to pack their tools.[8][9]

G0082 APT38

APT38 has used several code packing methods such as Themida, Enigma, VMProtect, and Obsidium, to pack their implants.[10]

G0087 APT39

APT39 has packed tools with UPX, and has repacked a modified version of Mimikatz to thwart anti-virus detection.[11][12]

G0096 APT41

APT41 uses packers such as Themida to obfuscate malicious files.[13]

S0373 Astaroth

Astaroth uses a software packer called Pe123\RPolyCryptor.[14]

S0638 Babuk

Versions of Babuk have been packed.[15][16][17]

S0534 Bazar

Bazar has a variant with a packed payload.[18][19]

S0268 Bisonal

Bisonal has used the MPRESS packer and similar tools for obfuscation.[20]

S0520 BLINDINGCAN

BLINDINGCAN has been packed with the UPX packer.[21]

C0017 C0017

During C0017, APT41 used VMProtect to slow the reverse engineering of malicious binaries.[22]

S0020 China Chopper

China Chopper's client component is packed with UPX.[23]

S0611 Clop

Clop has been packed to help avoid detection.[24][25]

S1105 COATHANGER

The first stage of COATHANGER is delivered as a packed file.[26]

S0614 CostaBricks

CostaBricks can implement a custom-built virtual machine mechanism to obfuscate its code.[27]

S0527 CSPY Downloader

CSPY Downloader has been packed with UPX.[28]

S0625 Cuba

Cuba has a packed payload when delivered.[29]

G0070 Dark Caracal

Dark Caracal has used UPX to pack Bandook.[30]

S0334 DarkComet

DarkComet has the option to compress its payload using UPX or MPRESS.[31]

S0187 Daserf

A version of Daserf uses the MPRESS packer.[32]

S0281 Dok

Dok is packed with an UPX executable packer.[33]

S0695 Donut

Donut can generate packed code modules.[34]

S0694 DRATzarus

DRATzarus's dropper can be packed with UPX.[35]

S0024 Dyre

Dyre has been delivered with encrypted resources and must be unpacked for execution.[36]

S0554 Egregor

Egregor's payloads are custom-packed, archived and encrypted to prevent analysis.[37][38]

G0066 Elderwood

Elderwood has packed malware payloads before delivery to victims.[39]

S0367 Emotet

Emotet has used custom packers to protect its payloads.[40]

S0512 FatDuke

FatDuke has been regularly repacked by its operators to create large binaries and evade detection.[41]

S0182 FinFisher

A FinFisher variant uses a custom packer.[42][43]

S0628 FYAnti

FYAnti has used ConfuserEx to pack its .NET module.[44]

G0093 GALLIUM

GALLIUM packed some payloads using different types of packers, both known and custom.[45]

S0588 GoldMax

GoldMax has been packed for obfuscation.[46]

S0342 GreyEnergy

GreyEnergy is packed for obfuscation.[47]

S0132 H1N1

H1N1 uses a custom packing algorithm.[48]

S0601 Hildegard

Hildegard has packed ELF files into other binaries.[49]

S0431 HotCroissant

HotCroissant has used the open source UPX executable packer.[50]

S0398 HyperBro

HyperBro has the ability to pack its payload.[51]

S0483 IcedID

IcedID has packed and encrypted its loader module.[52]

S0283 jRAT

jRAT payloads have been packed.[53]

G0094 Kimsuky

Kimsuky has packed malware with UPX.[6]

S0356 KONNI

KONNI has been packed for obfuscation.[54]

S1160 Latrodectus

The Latrodectus payload has been packed for obfuscation.[55]

S0513 LiteDuke

LiteDuke has been packed with multiple layers of encryption.[41]

S1202 LockBit 3.0

LockBit 3.0 can use code packing to hinder analysis.[56][57]

S0447 Lokibot

Lokibot has used several packing methods for obfuscation.[58]

S0532 Lucifer

Lucifer has used UPX packed binaries.[59]

S0409 Machete

Machete has been packed with NSIS.[60]

G1051 Medusa Group

Medusa Group has packed the code of dropped kernel drivers using the packer ASM Guard.[61]

S0530 Melcoz

Melcoz has been packed with VMProtect and Themida.[62]

S0455 Metamorfo

Metamorfo has used VMProtect to pack and protect files.[63]

S0083 Misdat

Misdat was typically packed using UPX.[64]

S1026 Mongall

Mongall has been packed with Themida.[5]

G1019 MoustachedBouncer

MoustachedBouncer has used malware plugins packed with Themida.[65]

S0198 NETWIRE

NETWIRE has used .NET packer tools to evade detection.[66]

C0002 Night Dragon

During Night Dragon, threat actors used software packing in its tools.[67]

S0264 OopsIE

OopsIE uses the SmartAssembly obfuscator to pack an embedded .Net Framework assembly used for C2.[68]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group packed malicious .db files with Themida to evade detection.[35][69][70]

C0016 Operation Dust Storm

For Operation Dust Storm, the threat actors used UPX to pack some payloads.[64]

C0005 Operation Spalax

For Operation Spalax, the threat actors used a variety of packers, including CyaX, to obfuscate malicious executables.[71]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D has a variant that is packed with UPX.[72]

G0040 Patchwork

A Patchwork payload was packed with UPX.[73]

S0650 QakBot

QakBot can encrypt and pack malicious payloads.[74]

S0565 Raindrop

Raindrop used a custom packer for its Cobalt Strike payload, which was compressed using the LZMA algorithm.[75][76]

S1130 Raspberry Robin

Raspberry Robin contains multiple payloads that are packed for defense evasion purposes and unpacked on runtime.[77]

S1240 RedLine Stealer

RedLine Stealer has used obfuscation tools such as DNGuard and Boxed App to pack their code.[78]

G0106 Rocke

Rocke's miner has created UPX-packed files in the Windows Start Menu Folder.[79][80][81]

S0085 S-Type

Some S-Type samples have been packed with UPX.[64]

S1210 Sagerunex

Sagerunex has used VMProtect to pack and obscure itself.[82]

G1031 Saint Bear

Saint Bear clones .NET assemblies from other .NET binaries as well as cloning code signing certificates from other software to obfuscate the initial loader payload.[83]

S1018 Saint Bot

Saint Bot has been packed using a dark market crypter.[84]

S0461 SDBbot

SDBbot has used a packed installer file.[85]

S0053 SeaDuke

SeaDuke has been packed with the UPX packer.[86]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors UPX-packed malicous payloads including 4L4MD4R ransomware.[87]

S0444 ShimRat

ShimRat's loader has been packed with the compressed ShimRat core DLL and the legitimate DLL for it to hijack.[88]

S0543 Spark

Spark has been packed with Enigma Protector to obfuscate its contents.[89]

S1030 Squirrelwaffle

Squirrelwaffle has been packed with a custom packer to hide payloads.[90][91]

G1053 Storm-0501

Storm-0501 has used Themida to pack Cobalt Strike payloads.[92]

S1183 StrelaStealer

StrelaStealer variants have used packers to obfuscate payloads and make analysis more difficult.[93]

S0663 SysUpdate

SysUpdate has been packed with VMProtect.[51][94]

G1018 TA2541

TA2541 has used a .NET packer to obfuscate malicious files.[95]

G0092 TA505

TA505 has used UPX to obscure malicious code.[85]

G0139 TeamTNT

TeamTNT has used UPX and Ezuri packer to pack its binaries.[96]

G0089 The White Company

The White Company has obfuscated their payloads through packing.[97]

G0027 Threat Group-3390

Threat Group-3390 has packed malware and tools, including using VMProtect.[98][51]

S0671 Tomiris

Tomiris has been packed with UPX.[99]

S0678 Torisma

Torisma has been packed with Iz4 compression.[70]

S0266 TrickBot

TrickBot leverages a custom packer to obfuscate its functionality.[100]

S0094 Trojan.Karagany

Trojan.Karagany samples sometimes use common binary packers such as UPX and Aspack on top of a custom Delphi binary packer.[101][102]

S1196 Troll Stealer

Troll Stealer has been delivered as a VMProtect-packed binary.[103][104]

S0022 Uroburos

Uroburos uses a custom packer.[105][106]

S0476 Valak

Valak has used packed DLL payloads.[107]

S0257 VERMIN

VERMIN is initially packed.[108]

G1017 Volt Typhoon

Volt Typhoon has used the Ultimate Packer for Executables (UPX) to obfuscate the FRP client files BrightmetricAgent.exe and SMSvcService.ex) and the port scanning utility ScanLine.[109]

S1207 XLoader

XLoader uses various packers, including CyaX, to obfuscate malicious executables.[110]

S0248 yty

yty packs a plugin with UPX.[111]

S0251 Zebrocy

Zebrocy's Delphi variant was packed with UPX.[112][113]

S0230 ZeroT

Some ZeroT DLL files have been packed with UPX.[114]

G0128 ZIRCONIUM

ZIRCONIUM has used multi-stage packers for exploit code.[115]
