Obfuscated Files or Information: Encrypted/Encoded File, Sub-technique T1027.013 - Enterprise

Archived: 2026-04-05 15:05:52 UTC

C0057 3CX Supply Chain Attack

During the 3CX Supply Chain Attack, AppleJeus encrypts its dynamic library files (.dll) using RC4, and when loaded only decrypts specific portions of the file using the key `3jB(2bsG#@c7`.[3]

G0026 APT18

APT18 obfuscates strings in the payload.[4]

G0073 APT19

APT19 used Base64 to obfuscate payloads.[5]

G0007 APT28

APT28 encrypted a .dll payload using RTL and a custom encryption algorithm. APT28 has also obfuscated payloads with base64, XOR, and RC4.[6][7][8][9][10]

G0050 APT32

APT32 has performed code obfuscation, including encoding payloads using Base64 and using a framework called "Dont-Kill-My-Cat (DKMC). APT32 also encrypts the library used for network exfiltration with AES-256 in CBC mode in their macOS backdoor.[11][12][13][14][15][16][17]

G0064 APT33

APT33 has used base64 to encode payloads.[18]

G0087 APT39

APT39 has used malware to drop encrypted CAB files.[19]

C0040 APT41 DUST

APT41 DUST used encrypted payloads decrypted and executed in memory.[20]

S0456 Aria-body

Aria-body has used an encrypted configuration file for its loader.[21]

S0373 Astaroth

Astaroth has used an XOR-based algorithm to encrypt payloads twice with different keys.[22]

S0438 Attor

Strings in Attor's components are encrypted with a XOR cipher, using a hardcoded key and the configuration data, log files and plugins are encrypted using a hybrid encryption scheme of Blowfish-OFB combined with RSA.[23]

S0347 AuditCred

AuditCred encrypts the configuration.[24]

S0473 Avenger

Avenger has the ability to XOR encrypt files to be sent to C2.[25]

S0534 Bazar

Bazar has used XOR, RSA2, and RC4 encrypted files.[26][27][28]

S1246 BeaverTail

BeaverTail has obfuscated strings of code with Base64 encoding within the JavaScript version of the malware.[29][30][31] BeaverTail has also utilized the open-source tool JavaScript-Obfuscator to obfuscate strings and functions.[32][33]

S0574 BendyBear

BendyBear has encrypted payloads using RC4 and XOR.[34]

S0268 Bisonal

Bisonal's DLL file and non-malicious decoy file are encrypted with RC4 and some function name strings are obfuscated.[35][36]

S0570 BitPaymer

BitPaymer has used RC4-encrypted strings and string hashes to avoid identifiable strings within the binary.[37]

G1002 BITTER

BITTER has used a RAR SFX dropper to deliver malware.[38]

S1180 BlackByte Ransomware

BlackByte Ransomware is distributed as an encrypted payload.[39]

S0520 BLINDINGCAN

BLINDINGCAN has obfuscated code using Base64 encoding.[40]

G0108 Blue Mockingbird

Blue Mockingbird has obfuscated the wallet address in the payload binary.[41]

S0657 BLUELIGHT

BLUELIGHT has a XOR-encoded payload.[42]

S1226 BOOKWORM

BOOKWORM has utilized Base64 encoding to obfuscate its payload.[43]

S0415 BOOSTWRITE

BOOSTWRITE has encoded its payloads using a ChaCha stream cipher with a 256-bit key and 64-bit Initialization vector (IV) to evade detection.[44]

S0484 Carberp

Carberp has used XOR-based encryption to mask C2 server locations within the trojan.[45]

S0348 Cardinal RAT

Cardinal RAT encodes many of its artifacts and is encrypted (AES-128) when downloaded.[46]

S0462 CARROTBAT

CARROTBAT has the ability to download a base64 encoded payload.[47]

S1041 Chinoxy

Chinoxy has encrypted its configuration file.[48]

S0667 Chrommme

Chrommme can encrypt sections of its code to evade detection.[49]

G1052 Contagious Interview

Contagious Interview has used hexadecimal string encoding to hide critical JavaScript module names, function names, and C2 URLs, which are decoded dynamically at runtime.[50]

S1235 CorKLOG

CorKLOG has encrypted collected contents using RC4.[51] CorKLOG has also utilized XOR encrypted strings.[51]

S0046 CozyCar

The payload of CozyCar is encrypted with simple XOR with a rotating key. The CozyCar configuration file has been encrypted with RC4 keys.[52]

S1153 Cuckoo Stealer

Cuckoo Stealer strings are XOR-encrypted.[53][54]

C0029 Cutting Edge

During Cutting Edge, threat actors used a Base64-encoded Python script to write a patched version of the Ivanti Connect Secure `dsls` binary.[55]

S0497 Dacls

Dacls can encrypt its configuration file with AES CBC.[56]

S1014 DanBot

DanBot can Base64 encode its payload.[57]

G0070 Dark Caracal

Dark Caracal has obfuscated strings in Bandook by base64 encoding, and then encrypting them.[58]

S1111 DarkGate

DarkGate drops an encrypted PE file, pe.bin, and decrypts it during installation.[59] DarkGate also uses custom base64 encoding schemas in later variations to obfuscate payloads.[60]

G0012 Darkhotel

Darkhotel has obfuscated code using RC4, XOR, and RSA.[61][62]

S1033 DCSrv

DCSrv's configuration is encrypted.[63]

S1052 DEADEYE

DEADEYE has encrypted its payload.[64]

S1134 DEADWOOD

DEADWOOD contains an embedded, AES-encrypted resource named `METADATA` that contains configuration information for follow-on execution.[65]

S0213 DOGCALL

DOGCALL is encrypted using single-byte XOR.[66]

S0695 Donut

Donut can generate encrypted, compressed/encoded, or otherwise obfuscated code modules.[67]

S1158 DUSTPAN

DUSTPAN decrypts an embedded payload.[20][68]

S1159 DUSTTRAP

DUSTTRAP begins with an initial launcher that decrypts an AES-128-CFB encrypted file on disk and executes it in memory.[20]

G0066 Elderwood

Elderwood has encrypted documents and malicious executables.[69]

S0081 Elise

Elise encrypts several of its files, including configuration files.[70]

S1247 Embargo

Embargo has encrypted both MDeployer and MS4 Killer payloads with RC4.[71]

S0082 Emissary

Variants of Emissary encrypt payloads using various XOR ciphers, as well as a custom algorithm that uses the "srand" and "rand" functions.[72][73]

S0367 Emotet

Emotet uses obfuscated URLs to download a ZIP file.[74]

S0634 EnvyScout

EnvyScout can Base64 encode payloads.[75]

S0401 Exaramel for Linux

Exaramel for Linux uses RC4 for encrypting the configuration.[76][77]

S0267 FELIXROOT

FELIXROOT encrypts strings in the backdoor using a custom XOR algorithm.[78][79]

S0618 FIVEHANDS

The FIVEHANDS payload is encrypted with AES-128.[80][81][82]

S0383 FlawedGrace

FlawedGrace encrypts its C2 configuration files with AES in CBC mode.[83]

S0661 FoggyWeb

FoggyWeb has been XOR-encoded.[84]

G0117 Fox Kitten

Fox Kitten has base64 encoded payloads to avoid detection.[85]

S1044 FunnyDream

FunnyDream can Base64 encode its C2 address stored in a template binary with the `xyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvw_-` or `xyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvw_=` character sets.[48]

S0410 Fysbis

Fysbis has been encrypted using XOR and RC4.[86]

S0168 Gazer

Gazer logs its actions into files that are encrypted with 3DES. It also uses RSA to encrypt resources.[87]

S0493 GoldenSpy

GoldenSpy's uninstaller has base64-encoded its variables. [88]

S0588 GoldMax

GoldMax has written AES-encrypted and Base64-encoded configuration files to disk.[89][90]

S0531 Grandoreiro

The Grandoreiro payload has been delivered encrypted with a custom XOR-based algorithm and also as a base64-encoded ZIP file.[22][91][91]

S0237 GravityRAT

GravityRAT supports file encryption (AES with the key "lolomycin2017").[92]

S0342 GreyEnergy

GreyEnergy encrypts its configuration files with AES-256 and also encrypts its strings.[79]

G0043 Group5

Group5 disguised its malicious binaries with several layers of obfuscation, including encrypting the files.[93]

S0391 HAWKBALL

HAWKBALL has encrypted the payload with an XOR-based algorithm.[94]

S0170 Helminth

The Helminth config file is encrypted with RC4.[95]

S0698 HermeticWizard

HermeticWizard has the ability to encrypt PE files with a reverse XOR loop.[96]

S1249 HexEval Loader

HexEval Loader has encoded module names and C2 URLs as hexadecimal strings in attempts to evade analysis.[50][97]

S1027 Heyoka Backdoor

Heyoka Backdoor can encrypt its payload.[98]

S0087 Hi-Zor

Hi-Zor uses various XOR techniques to obfuscate its components.[99]

S0394 HiddenWasp

HiddenWasp encrypts its configuration and payload.[100]

G0126 Higaisa

Higaisa used Base64 encoded compressed payloads.[101][102]

S0601 Hildegard

Hildegard has encrypted an ELF file.[103]

S0232 HOMEFRY

Some strings in HOMEFRY are obfuscated with XOR x56.[104]

S0431 HotCroissant

HotCroissant has encrypted strings with single-byte XOR and base64 encoded RC4.[105]

S0398 HyperBro

HyperBro can be delivered encrypted to a compromised host.[106]

S0483 IcedID

IcedID has utilzed encrypted binaries and base64 encoded strings.[107]

G0100 Inception

Inception has encrypted malware payloads dropped on victim machines with AES and RC4 encryption.[108]

S1245 InvisibleFerret

InvisibleFerret has utilized the XOR and Base64 encoding for each of its modules.[29] InvisibleFerret has also obfuscated files with a combination of zlib, Base64 and reverse string order.[32] InvisibleFerret has also utilized the XOR and Base64 encoding some of its Python scripts.[30]

S1132 IPsec Helper

IPsec Helper contains an embedded XML configuration file with an encrypted list of command and control servers. These are written to an external configuration file during execution.[65]

S0581 IronNetInjector

IronNetInjector can obfuscate variable names, encrypt strings, as well as base64 encode and Rijndael encrypt payloads.[109]

S0044 JHUHUGIT

Many strings in JHUHUGIT are obfuscated with a XOR algorithm.[110][111][9]

S1190 Kapeka

Kapeka utilizes AES-256 (CBC mode), XOR, and RSA-2048 encryption schemas for various configuration and other objects.[112]

S0585 Kerrdown

Kerrdown can encrypt, encode, and compress multiple layers of shellcode.[113]

S0487 Kessel

Kessel's configuration is hardcoded and RC4 encrypted within the binary.[114]

S1020 Kevin

Kevin has Base64-encoded its configuration file.[115]

S0387 KeyBoy

In one version of KeyBoy, string obfuscation routines were used to hide many of the critical values referenced in the malware.[116]

S1051 KEYPLUG

KEYPLUG can use a hardcoded one-byte XOR encoded configuration file.[64]

S0526 KGH_SPY

KGH_SPY has used encrypted strings in its installer.[117]

S0356 KONNI

KONNI is heavily obfuscated and includes encrypted configuration files.[118]

S0236 Kwampirs

Kwampirs downloads additional files that are base64-encoded and encrypted with another cipher.[119]

S1160 Latrodectus

Latrodectus has used a pseudo random number generator (PRNG) algorithm and a rolling XOR key to obfuscate strings.[120][121][122]

G0032 Lazarus Group

Lazarus Group has used multiple types of encryption and encoding for their payloads, including AES, Caracachs, RC4, XOR, Base64, and other tricks such as creating aliases in code for Native API function names.[123][124][125][126][56][127][128]

G0065 Leviathan

Leviathan has obfuscated code using base64.[129]

S0395 LightNeuron

LightNeuron encrypts its configuration files with AES-256.[130]

S1185 LightSpy

LightSpy encrypts the C2 configuration file using AES with a static key, while the module `.dylib` files use a rolling one-byte encoding for obfuscation.[131]

S1202 LockBit 3.0

The LockBit 3.0 payload includes an encrypted main component.[132][133]

S0451 LoudMiner

LoudMiner has encrypted DMG files.[134]

S1213 Lumma Stealer

Lumma Stealer has used AES-encrypted payloads contained within PowerShell scripts.[135]

S1142 LunarMail

LunarMail has used RC4 and AES to encrypt strings and its exfiltration configuration respectively.[136]

S1141 LunarWeb

The LunarWeb install files have been encrypted with AES-256.[136]

S1060 Mafalda

Mafalda has been obfuscated and contains encrypted functions.[137]

G0059 Magic Hound

Magic Hound malware has used base64-encoded files and has also encrypted embedded strings with AES.[138][139]

S1182 MagicRAT

MagicRAT stores base64 encoded command and contorl URLs in a configuraiton file, with each URL prefixed with the value `LR02DPt22R`.[140]

G1026 Malteiro

Malteiro has used scripts encoded in Base64 certificates to distribute malware to victims.[141]

S1169 Mango

Mango contains a series of base64 encoded substrings.[142]

S1220 MEDUSA

MEDUSA can XOR encrypt configuration strings.[143]

S1244 Medusa Ransomware

Medusa Ransomware has utilized XOR encrypted strings.[144][145]

G0045 menuPass

menuPass has encoded strings in its malware with base64 as well as with a simple, single-byte XOR obfuscation using key 0x40.[146][147][148]

G1013 Metador

Metador has encrypted their payloads.[137]

S1059 metaMain

metaMain's module file has been encrypted via XOR.[149]

S0455 Metamorfo

Metamorfo has encrypted payloads and strings.[150][151]

S0339 Micropsia

Micropsia obfuscates the configuration with a custom Base64 and XOR.[152][153]

S1015 Milan

Milan can encode files containing information about the targeted system.[154][115]

S1122 Mispadu

Mispadu uses a custom algorithm to obfuscate its internal strings and uses hardcoded keys.[155]

Mispadu also uses encoded configuration files and has encoded payloads using Base64.[155][156][141]

G0103 Mofang

Mofang has encrypted payloads before they are downloaded to victims.[157]

G1036 Moonstone Sleet

Moonstone Sleet has used encrypted payloads within files for follow-on execution and defense evasion.[158]

S1221 MOPSLED

MOPSLED can encrypt configuration files with a custom ChaCha20 algorithm.[143]

S0284 More_eggs

More_eggs's payload has been encrypted with a key that has the hostname and processor family information appended to the end.[159]

G1009 Moses Staff

Moses Staff has used obfuscated web shells in their operations.[63]

S0256 Mosquito

Mosquito's installer is obfuscated with a custom crypter to obfuscate the installer.[160]

S0228 NanHaiShu

NanHaiShu encodes files in Base64.[161]

C0002 Night Dragon

During Night Dragon, threat actors used a DLL that included an XOR-encoded section.[162]

S1100 Ninja

The Ninja payload is XOR encrypted and compressed.[163] Ninja has also XORed its configuration data with a constant value of `0xAA`.[164][163]

S0385 njRAT

njRAT has included a base64 encoded executable.[165]

G0049 OilRig

OilRig has encrypted and encoded data in its malware, including by using base64.[166][167][168][169][170]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group encrypted malware such as DRATzarus with XOR and DLL files with base64.[171][172][173][174]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors encoded some payloads with a single-byte XOR, both skipping the key itself and zeroing in an attempt to avoid exposing the key; other payloads were Base64-encoded.[175]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors used Base64 to encode files with a custom key.[176]

C0005 Operation Spalax

For Operation Spalax, the threat actors used XOR-encrypted payloads.[177]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D encrypts its strings in RSA256 and encodes them in a custom base64 scheme and XOR.[178]

C0042 Outer Space

During Outer Space, OilRig deployed VBS droppers with obfuscated strings.[142]

S1233 PAKLOG

PAKLOG has utilized a simple encoding mechanism to encode characters in the buffer.[51]

S1050 PcShare

PcShare has been encrypted with XOR using different 32-long Base16 strings.[48]

S0587 Penquin

Penquin has encrypted strings in the binary for obfuscation.[179]

S0501 PipeMon

PipeMon modules are stored encrypted on disk.[180]

S0013 PlugX

PlugX has leveraged XOR encryption with the key of 123456789.[181]

S0113 Prikormka

Some resources in Prikormka are encrypted with a simple XOR operation or encoded with Base64.[182]

S0613 PS1

PS1 is distributed as a set of encrypted files and scripts.[183]

G0024 Putter Panda

Droppers used by Putter Panda use RC4 or a 16-byte XOR key consisting of the bytes 0xA0 – 0xAF to obfuscate payloads.[184]

S1032 PyDCrypt

PyDCrypt has been compiled and encrypted with PyInstaller, specifically using the --key flag during the build phase.[63]

S1242 Qilin

Qilin can employ several code obfuscation methods, including renaming functions, altering control flows, and encrypting strings.[185]

S1148 Raccoon Stealer

Raccoon Stealer uses RC4 encryption for strings and command and control addresses to evade static detection.[186][187][188]

S0565 Raindrop

Raindrop encrypted its payload using a simple XOR algorithm with a single-byte key.[189][190]

S0629 RainyDay

RainyDay has downloaded as a XOR-encrypted payload.[191]

S1212 RansomHub

RansomHub has an encrypted configuration file.[192]

S1113 RAPIDPULSE

RAPIDPULSE has the ability to RC4 encrypt and base64 encode decrypted files on compromised servers prior to writing them to stdout.[193]

S0172 Reaver

Reaver encrypts some of its files with XOR.[194]

C0047 RedDelta Modified PlugX Infection Chain Operations

Mustang Panda stored installation payloads as encrypted files in hidden folders during RedDelta Modified PlugX Infection Chain Operations.[195]

S0153 RedLeaves

A RedLeaves configuration file is encrypted with a simple XOR key, 0x53.[196]

S1240 RedLine Stealer

RedLine Stealer has encrypted and encoded configuration data with Base64 and XOR functions.[197]

C0056 RedPenguin

During RedPenguin, UNC3886 generated Base64-encoded files in the FreeBSD shell environment of targeted Juniper devices.[198][199]

S0375 Remexi

Remexi obfuscates its configuration data with XOR.[200]

S0125 Remsec

Some data in Remsec is encrypted using RC5 in CBC mode, AES-CBC with a hardcoded key, RC4, or Salsa20. Some data is also base64-encoded.[201][202]

S0496 REvil

REvil has used encrypted strings and configuration files.[203][204][205][206][207][208][209]

S0433 Rifdoor

Rifdoor has encrypted strings with a single byte XOR algorithm.[105]

S0448 Rising Sun

Configuration data used by Rising Sun has been encrypted using an RC4 stream algorithm.[210]

S1150 ROADSWEEP

The ROADSWEEP binary contains RC4 encrypted embedded scripts.[211][212][213]

S1210 Sagerunex

Sagerunex can be passed a reference to an XOR-encrypted configuration file at runtime.[214]

G1031 Saint Bear

Saint Bear initial payloads included encoded follow-on payloads located in the resources file of the first-stage loader.[215]

S0074 Sakula

Sakula uses single-byte XOR obfuscation to obfuscate many of its files.[216]

S0370 SamSam

SamSam has been seen using AES or DES to encrypt payloads and payload components.[217][218]

S0345 Seasalt

Seasalt obfuscates configuration data.[219]

C0045 ShadowRay

During ShadowRay, threat actors used Base64-encrypted Python code to evade detection.[220]

S1019 Shark

Shark can use encrypted and encoded files for C2 configuration.[154][221]

G0121 Sidewinder

Sidewinder has used base64 encoding and ECDH-P256 encryption for payloads.[222][223][224]

S0468 Skidmap

Skidmap has encrypted it's main payload using 3DES.[225]

S0633 Sliver

Sliver can encrypt strings at compile time.[226][227]

S0226 Smoke Loader

Smoke Loader uses a simple one-byte XOR method to obfuscate values in the malware.[228][229]

S1124 SocGholish

SocGholish has single or double Base-64 encoded references to its second-stage server URLs.[230]

S0374 SpeakUp

SpeakUp encodes its second-stage payload with Base64. [231]

S1232 SplatDropper

SplatDropper has also utilized XOR encrypted payload.[51]

S1030 Squirrelwaffle

Squirrelwaffle has been obfuscated with a XOR-based algorithm.[232][233]

S1037 STARWHALE

STARWHALE has been obfuscated with hex-encoded strings.[234]

S1200 StealBit

StealBit stores obfuscated DLL file names in its executable.[235]

S0380 StoneDrill

StoneDrill has obfuscated its module with an alphabet-based table or XOR encryption.[236]

G1046 Storm-1811

Storm-1811 XOR encodes a Cobalt Strike installation payload in a DLL file that is decoded with a hardcoded key when called by a legitimate 7zip installation process.[237]

S1183 StrelaStealer

StrelaStealer uses XOR-encoded strings to obfuscate items.[238]

S0491 StrongPity

StrongPity has used encrypted strings in its dropper component.[239][240]

S0603 Stuxnet

Stuxnet uses encrypted configuration blocks and writes encrypted files to disk.[241]

S0578 SUPERNOVA

SUPERNOVA contained Base64-encoded strings.[242]

S0663 SysUpdate

SysUpdate can encrypt and encode its configuration file.[243]

G1018 TA2541

TA2541 has used compressed and char-encoded scripts in operations.[244]

G0092 TA505

TA505 has password-protected malicious Word documents.[245]

S0011 Taidoor

Taidoor can use encrypted string blocks for obfuscation.[246]

G0139 TeamTNT

TeamTNT has encrypted its binaries via AES and encoded files using Base64.[247][248]

G0027 Threat Group-3390

A Threat Group-3390 tool can encrypt payloads using XOR. Threat Group-3390 malware is also obfuscated using Metasploit's shikata_ga_nai encoder.[249][250][251]

S0665 ThreatNeedle

ThreatNeedle has been compressed and obfuscated using RC4, AES, or XOR.[252]

S0131 TINYTYPHON

TINYTYPHON has used XOR with 0x90 to obfuscate its configuration file.[253]

S0678 Torisma

Torisma has been Base64 encoded and AES encrypted.[174]

G0134 Transparent Tribe

Transparent Tribe has dropped encoded executables on compromised hosts.[254]

S0266 TrickBot

TrickBot uses an AES CBC (256 bits) encryption algorithm for its loader and configuration files.[255]

G0081 Tropic Trooper

Tropic Trooper has encrypted configuration files.[256][257]

S0263 TYPEFRAME

APIs and strings in some TYPEFRAME variants are RC4 encrypted. Another variant is encoded with XOR.[258]

S1164 UPSTYLE

UPSTYLE stores primary content as base64-encoded objects.[259][260]

S0022 Uroburos

Uroburos can use AES and CAST-128 encryption to obfuscate resources.[261]

S0386 Ursnif

Ursnif has used an XOR-based algorithm to encrypt Tor clients dropped to disk.[262] Ursnif droppers have also been delivered as password-protected zip files that execute base64 encoded PowerShell commands.[263]

S0136 USBStealer

Most strings in USBStealer are encrypted using 3DES and XOR and reversed.[264]

S0257 VERMIN

VERMIN is obfuscated using the obfuscation tool called ConfuserEx.[265]

S1154 VersaMem

VersaMem encrypted captured credentials with AES then Base64 encoded them before writing to local storage.[266]

S0180 Volgmer

A Volgmer variant is encoded using a simple XOR cipher.[267]

S0612 WastedLocker

The WastedLocker payload includes encrypted strings stored within the .bss section of the binary file.[268]

S0579 Waterbear

Waterbear has used RC4 encrypted shellcode and encrypted functions.[269]

S0689 WhisperGate

WhisperGate can Base64 encode strings, store downloaded files in reverse byte order, and use the Eazfuscator tool to obfuscate its third stage.[270][271][272]

G0107 Whitefly

Whitefly has encrypted the payload used for C2.[273]

S0466 WindTail

WindTail can be delivered as a compressed, encrypted, and encoded payload.[274]

S0430 Winnti for Linux

Winnti for Linux can encode its configuration file with single-byte XOR encoding.[275]

S0141 Winnti for Windows

Winnti for Windows has the ability to encrypt and compress its payload.[276]

S1065 Woody RAT

Woody RAT has used Base64 encoded strings and scripts.[277]

S0658 XCSSET

Older XCSSET variants use `xxd` to encode modules. Later versions pass an `xxd` or `base64` encoded blob through multiple decoding stages to reconstruct the module name, AppleScript, or shell command. For example, the initial network request uses three layers of hex decoding before executing a curl command in a shell.[278]

S1207 XLoader

XLoader features encrypted functions using the RC4 algorithm and bytecode operations.[279][280]

S1248 XORIndex Loader

XORIndex Loader has encoded module names and C2 URLs as hexadecimal strings in attempts to evade analysis.[281]

S0388 YAHOYAH

YAHOYAH encrypts its configuration file using a simple algorithm.[282]

S0230 ZeroT

ZeroT has encrypted its payload with RC4.[283]

S0330 Zeus Panda

Zeus Panda encrypts strings with XOR. Zeus Panda also encrypts all configuration and settings in AES and RC4.[284][285]

S0672 Zox

Zox has been encoded with Base64.[286]

S1013 ZxxZ

ZxxZ has been encoded to avoid detection from static analysis tools.[287]

Source: https://attack.mitre.org/techniques/T1027/013