Encrypted Channel: Asymmetric Cryptography, Sub-technique T1573.002 - Enterprise

Archived: 2026-04-05 16:22:26 UTC

S0202 adbupd

adbupd contains a copy of the OpenSSL library to encrypt C2 traffic.[1]

S0045 ADVSTORESHELL

A variant of ADVSTORESHELL encrypts some C2 with RSA.[2]

C0040 APT41 DUST

APT41 DUST used HTTPS for command and control.[3]

G1044 APT42

APT42 has used tools such as NICECURL with command and control communication taking place over HTTPS.[4]

S0438 Attor

Attor's Blowfish key is encrypted with a public RSA key.[5]

S1081 BADHATCH

BADHATCH can beacon to a hardcoded C2 IP address using TLS encryption every 5 minutes.[6]

S0534 Bazar

Bazar can use TLS in C2 communications.[7]

S0017 BISCUIT

BISCUIT uses SSL for encrypting C2 communications.[8]

S1184 BOLDMOVE

BOLDMOVE uses the WolfSSL library to implement SSL encryption for command and control communication.[9]

C0021 C0021

During C0021, the threat actors used SSL via TCP port 443 for C2 communications.[10]

S0335 Carbon

Carbon has used RSA encryption for C2 communications.[11]

S1224 CASTLETAP

CASTLETAP can initiate a C2 connection over an SSL socket.[12]

S0023 CHOPSTICK

CHOPSTICK encrypts C2 communications with TLS.[13]

S1105 COATHANGER

COATHANGER connects to command and control infrastructure using SSL.[14]

G0080 Cobalt Group

Cobalt Group has used the Plink utility to create SSH tunnels.[15]

S0154 Cobalt Strike

Cobalt Strike can use RSA asymmetric encryption with PKCS1 padding to encrypt data sent to the C2 server.[16]

S0126 ComRAT

ComRAT can use SSL/TLS encryption for its HTTP-based C2 channel. ComRAT has used public key cryptography with RSA and AES encrypted email attachments for its Gmail C2 channel.[17][18]

S1155 Covenant

Covenant can utilize SSL to encrypt command and control traffic.[19]

S0687 Cyclops Blink

Cyclops Blink can encrypt C2 messages with AES-256-CBC sent underneath TLS. OpenSSL library functions are also used to encrypt each message using a randomly generated key and IV, which are then encrypted using a hard-coded RSA public key.[20]

S0673 DarkWatchman

DarkWatchman can use TLS to encrypt its C2 channel.[21]

S0600 Doki

Doki has used the embedTLS library for network communications.[22]

S0384 Dridex

Dridex has encrypted traffic with RSA.[23]

S0363 Empire

Empire can use TLS to encrypt its C2 channel.[24]

G0037 FIN6

FIN6 used the Plink command-line utility to create SSH tunnels to C2 servers.[25]

G0061 FIN8

FIN8 has used the Plink utility to tunnel RDP back to C2 infrastructure.[26]

S1144 FRP

FRP can be configured to only accept TLS connections.[27]

S0168 Gazer

Gazer uses custom encryption for C2 that uses RSA.[28][29]

S0588 GoldMax

GoldMax has RSA-encrypted its communication with the C2 server.[30]

S1198 Gomir

Gomir uses reverse proxy functionality that employs SSL to encrypt communications.[31]

S0531 Grandoreiro

Grandoreiro can use SSL in C2 communication.[32]

S0342 GreyEnergy

GreyEnergy encrypts communications using RSA-2048.[33]

S0632 GrimAgent

GrimAgent can use a hardcoded server public RSA key to encrypt the first request to C2.[34]

S0087 Hi-Zor

Hi-Zor encrypts C2 traffic with TLS.[35]

S0483 IcedID

IcedID has used SSL and TLS in communications with C2.[36][37]

C0043 Indian Critical Infrastructure Intrusions

During Indian Critical Infrastructure Intrusions, RedEcho used SSL for network communication.[38]

S1203 J-magic

J-magic can communicate back to send a challenge to C2 infrastructure over SSL.[39]

S1051 KEYPLUG

KEYPLUG can use TLS-encrypted WebSocket Protocol (WSS) for C2.[40]

S0250 Koadic

Koadic can use SSL and TLS for communications.[41]

S0641 Kobalos

Kobalos's authentication and key exchange is performed using RSA-512.[42][43]

S1121 LITTLELAMB.WOOLTEA

LITTLELAMB.WOOLTEA can communicate over SSL using the private key from the Ivanti Connect Secure web server.[44]

S1213 Lumma Stealer

Lumma Stealer has used HTTPS for command and control purposes.[45]

S1141 LunarWeb

LunarWeb can send short C2 commands, up to 512 bytes, encrypted with RSA-4096.[46]

S0409 Machete

Machete has used TLS-encrypted FTP to exfiltrate data.[47]

S1169 Mango

Mango can use TLS to encrypt C2 communications.[48]

G1051 Medusa Group

Medusa Group has used HTTPS for command and control.[49]

S0455 Metamorfo

Metamorfo's C2 communication has been encrypted using OpenSSL.[50]

S1122 Mispadu

Mispadu contains a copy of the OpenSSL library to encrypt C2 traffic.[51]

S0699 Mythic

Mythic supports SSL encrypted C2.[52]

S1192 NICECURL

NICECURL has used HTTPS for C2 communications.[4]

S1172 OilBooster

OilBooster can use the OpenSSL library to encrypt C2 communications.[53]

G0049 OilRig

OilRig used the PowerExchange utility and other tools to create tunnels to C2 servers.[54]

C0014 Operation Wocao

During Operation Wocao, threat actors' proxy implementation "Agent" upgraded the socket in use to a TLS socket.[55]

S0556 Pay2Key

Pay2Key has used RSA encrypted communications with C2.[56]

S0587 Penquin

Penquin can encrypt communications using the BlowFish algorithm and a symmetric key exchanged with Diffie Hellman.[57]

S1123 PITSTOP

PITSTOP has the ability to communicate over TLS.[44]

S0428 PoetRAT

PoetRAT used TLS to encrypt command and control (C2) communications.[58]

S0150 POSHSPY

POSHSPY encrypts C2 traffic with AES and RSA.[59]

S0223 POWERSTATS

POWERSTATS has encrypted C2 traffic with RSA.[60]

S0192 Pupy

Pupy's default encryption for its C2 communication channel is SSL, but it also has transport options for RSA and AES.[61]

G1039 RedCurl

RedCurl has used HTTPS for C2 communication.[62][63]

G1042 RedEcho

RedEcho uses SSL for network communication.[38]

S1219 REPTILE

REPTILE can use TLS over raw TCP for secure C2.[64][12]

S0496 REvil

REvil has encrypted C2 communications with the ECIES algorithm.[65]

S0448 Rising Sun

Rising Sun variants can use SSL for encrypting C2 communications.[66]

S1210 Sagerunex

Sagerunex uses HTTPS for command and control communication.[67]

S1085 Sardonic

Sardonic has the ability to send a random 64-byte RC4 key to communicate with actor-controlled C2 servers by using an RSA public key.[68]

S0382 ServHelper

ServHelper may set up a reverse SSH tunnel to give the attacker access to services running on the victim, such as RDP.[69]

S0633 Sliver

Sliver can use mutual TLS and RSA cryptography to exchange a session key.[70][71][72][73][74]

S1035 Small Sieve

Small Sieve can use SSL/TLS for its HTTPS Telegram Bot API-based C2 channel.[75]

S1163 SnappyTCP

SnappyTCP can use OpenSSL and TLS certificates to encrypt traffic.[76]

S0627 SodaMaster

SodaMaster can use a hardcoded RSA key to encrypt some of its C2 traffic.[77]

S0615 SombRAT

SombRAT can SSL encrypt C2 traffic.[78][79][80]

S0491 StrongPity

StrongPity has encrypted C2 traffic using SSL/TLS.[81]

S0018 Sykipot

Sykipot uses SSL for encrypting C2 communications.[82]

G1018 TA2541

TA2541 has used TLS encrypted C2 communications including for campaigns using AsyncRAT.[83]

S0668 TinyTurla

TinyTurla has the ability to encrypt C2 traffic with SSL/TLS.[84]

S0183 Tor

Tor encapsulates traffic in multiple layers of encryption, using TLS by default.[85]

S0094 Trojan.Karagany

Trojan.Karagany can secure C2 communications with SSL and TLS.[86]

G0081 Tropic Trooper

Tropic Trooper has used SSL to connect to C2 servers.[87][88]

S0022 Uroburos

Uroburos has used a combination of a Diffie-Hellman key exchange mixed with a pre-shared key (PSK) to encrypt its top layer of C2 communications.[89]

G1047 Velvet Ant

Velvet Ant has used a reverse SSH shell to securely communicate with victim devices.[90]

C0039 Versa Director Zero Day Exploitation

Versa Director Zero Day Exploitation used HTTPS for command and control of compromised Versa Director servers.[91]

S0180 Volgmer

Some Volgmer variants use SSL to encrypt C2 communications.[92]

S0366 WannaCry

WannaCry uses Tor for command and control traffic and routes a custom cryptographic protocol over the Tor circuit.[93]

S0515 WellMail

WellMail can use hard coded client and certificate authority certificates to communicate with C2 over mutual TLS.[94][95]

S0514 WellMess

WellMess can communicate to C2 with mutual TLS where client and server mutually check certificates.[96][97][98][95]

S1065 Woody RAT

Woody RAT can use RSA-4096 to encrypt data sent to its C2 server.[99]

S0117 XTunnel

XTunnel uses SSL/TLS and RC4 to encrypt traffic.[100][13]

S0251 Zebrocy

Zebrocy uses SSL and AES ECB for encrypting C2 communications.[101][102][103]
