MAR-10330097-1.v1: DearCry Ransomware | CISA

Published: 2021-04-12 · Archived: 2026-04-05 13:03:40 UTC

body#cma-body { font-family: Franklin Gothic Medium, Franklin Gothic, ITC Franklin Gothic, Arial, sans-serif; font-size: 15px; } table#cma-table { width: 900px; margin: 2px; table-layout: fixed; border-collapse: collapse; } div#cma-exercise { width: 900px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; } div.cma-header { text-align: center; margin-bottom: 40px; } div.cma-footer { text-align: center; margin-top: 20px; } h2.cma-tlp { background-color: #000; color: #ffffff; width: 180px; height: 30px; text-align: center; line-height: 30px; font-weight: bold; font-size: 18px; float: right; } span.cma-fouo { line-height: 30px; font-weight: bold; font-size: 16px; } h3.cma-section-title { font-size: 18px; font-weight: bold; padding: 0 10px; margin-top: 10px; } h4.cma-object-title { font-size: 16px; font-weight: bold; margin-left: 20px; } h5.cma-data-title { padding: 3px 0 3px 10px; margin: 10px 0 0 20px; background-color: #e7eef4; font-size: 15px; } p.cma-text { margin: 5px 0 0 25px !important; word-wrap: break-word !important; } div.cma-section { border-bottom: 5px solid #aaa; margin: 5px 0; padding-bottom: 10px; } div.cma-avoid-page-break { page-break-inside: avoid; } div#cma-summary { page-break-after: always; } div#cma-faq { page-break-after: always; } table.cma-content { border-collapse: collapse; margin-left: 20px; } table.cma-hashes { table-layout: fixed; width: 880px; } table.cma-hashes td{ width: 780px; word-wrap: break-word; } .cma-left th { text-align: right; vertical-align: top; padding: 3px 8px 3px 20px; background-color: #f0f0f0; border-right: 1px solid #aaa; } .cma-left td { padding-left: 8px; } .cma-color-title th, .cma-color-list th, .cma-color-title-only th { text-align: left; padding: 3px 0 3px 20px; background-color: #f0f0f0; } .cma-color-title td, .cma-color-list td, .cma-color-title-only td { padding: 3px 20px; } .cma-color-title tr:nth-child(odd) { background-color: #f0f0f0; } .cma-color-list tr:nth-child(even) { background-color: #f0f0f0; } td.cma-relationship { max-width: 310px; word-wrap: break-word; } ul.cma-ul { margin: 5px 0 10px 0; } ul.cma-ul li { line-height: 20px; margin-bottom: 5px; word-wrap: break-word; } #cma-survey { font-weight: bold; font-style: italic; } div.cma-banner-container { position: relative; text-align: center; color: white; } img.cma-banner { max-width: 900px; height: auto; } img.cma-nccic-logo { max-height: 60px; width: auto; float: left; margin-top: -15px; } div.cma-report-name { position: absolute; bottom: 32px; left: 12px; font-size: 20px; } div.cma-report-number { position: absolute; bottom: 70px; right: 100px; font-size: 18px; } div.cma-report-date { position: absolute; bottom: 32px; right: 100px; font-size: 18px; } img.cma-thumbnail { max-height: 100px; width: auto; vertical-align: top; } img.cma-screenshot { margin: 10px 0 0 25px; max-width: 800px; height: auto; vertical-align: top; border: 1px solid #000; } div.cma-screenshot-text { margin: 10px 0 0 25px; } .cma-break-word { word-wrap: break-word; } .cma-tag { border-radius: 5px; padding: 1px 10px; margin-right: 10px; } .cma-tag-info { background: #f0f0f0; } .cma-tag-warning { background: #ffdead; }

Notification

Summary

Description

Six files were submitted for analysis. The files were identified as DearCry ransomware. The malware encrypts files on a device and demands ransom in exchange for decryption.

For a downloadable copy of IOCs, see: MAR-10330097-1.v1.stix.

Emails (2)

konedieyp[@]airmail.cc

uenwonken[@]memail.com

Submitted Files (6)

027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27 (027119161d11ba87acc908a1d284b9...)

10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da (10bce0ff6597f347c3cca8363b7c81...)

2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff (2b9838da7edb0decd32b086e47a31e...)

e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6 (e044d9f2d0f1260c3f4a543a1e67f3...)

fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65 (fdec933ca1dd1387d970eeea32ce5d...)

feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede (feb3e6d30ba573ba23f3bd1291ca17...)

Findings

2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff

Tags

downloaderloaderransomwaretrojan

Details

Name	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
Size	1322496 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	0e55ead3b8fd305d9a54f78c7b56741a
SHA1	f7b084e581a8dcea450c2652f8058d93797413c3
SHA256	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
SHA512	5c3d58d1001dce6f2d23f33861e9c7fef766b7fe0a86972e9f1eeb70bfad970b02561da6b6d193cf24bc3c1aaf2a42a950fa6e5dff36386653b8aa
ssdeep	24576:LU5NX2yJOiUXmEICxu2WAP0NIzkQM+KpPRQ9StIUDpl1fpxkHVZgMCS+:L7XP7P9o5QzUtl1fpxkHVZgMC3
Entropy	6.994611

Antivirus

Ahnlab	Ransomware/Win.DoejoCrypt
Antiy	Trojan[Ransom]/Win32.DearCry
Avira	TR/FileCoder.HW
BitDefender	Trojan.GenericKD.36477740
ClamAV	Win.Ransomware.Dearcry-9840778-0
Comodo	Malware
Cyren	W32/Trojan.FOGJ-5046
ESET	a variant of Win32/Filecoder.DearCry.A trojan
Emsisoft	Trojan.GenericKD.36477740 (B)
Ikarus	Trojan-Ransom.FileCrypter
K7	Trojan (005790de1)
Lavasoft	Trojan.GenericKD.36477740
McAfee	Ransom-DearCry!0E55EAD3B8FD
Microsoft Security Essentials	Ransom:Win32/DoejoCrypt.A
NANOAV	Trojan.Win32.Encoder.ipilfs
NetGate	Trojan.Win32.Malware
Quick Heal	Ransom.DearCry.S19261705
Sophos	Troj/Ransom-GFE
Symantec	Downloader
TACHYON	Ransom/W32.DearCry.1322496
TrendMicro	Ransom.56DC2A23

TrendMicro House Call	Ransom.56DC2A23
Vir.IT eXplorer	Ransom.Win32.DearCry.CUQ
VirusBlokAda	TrojanRansom.Encoder
Zillya!	Trojan.Encoder.Win32.2195

YARA Rules

- rule CISA_10330097_01 : trojan downloader ransomware DEARCRY
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10330097"
      Date = "2021-03-31"
      Last_Modified = "20210331_1630"
      Actor = "n/a"
      Category = "Trojan Downloader Ransomware"
      Family = "DEARCRY"
      Description = "Detects DearCry Ransomware"
      MD5_1 = "0e55ead3b8fd305d9a54f78c7b56741a"
      SHA256_1 = "2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff"
      MD5_2 = "cdda3913408c4c46a6c575421485fa5b"
      SHA256_2 = "e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6"
      MD5_3 = "c6eeb14485d93f4e30fb79f3a57518fc"
      SHA256_3 = "feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede"
    strings:
      $s0 = { 8B 85 04 EA FF FF 50 8B 8D 08 EA FF FF 51 8B 55 14 52 8B 45 10 50 8D 8D 68 F0 FF FF 51 8B 95 00 EA FF FF 52 }
      $s1 = { 43 72 79 70 74 6F 50 72 6F 2D 58 63 68 42 }
      $s2 = "-----BEGIN RSA PUBLIC KEY-----"
      $s3 = ".CRYPT"
    condition:
      all of them
  }

ssdeep Matches

99	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede

PE Metadata

Compile Date	2021-03-09 03:08:39-05:00
Import Hash	f8b8e20e844ccd50a8eb73c2fca3626d

PE Sections

MD5	Name	Raw Size	Entropy
4289116f218aa083456871506085e1be	header	1024	2.596118
46c15879afc7b600a23284d8e72f87aa	.text	976896	7.069452
d0093b4c33543ebd59b2c22c7e71670f	.rdata	265728	6.128934
40f8722b3a267afab34d8909cf5da682	.data	25600	4.794047
a0bf446401bdd255b7f7cb0215177d73	.rsrc	512	5.108717
bcd8233433c686e481a6c5a4f1f263ac	.reloc	51712	5.474063

Packers/Compilers/Cryptors

Relationships

2b9838da7e...	Related_To	konedieyp[@]airmail.cc
2b9838da7e...	Related_To	uenwonken[@]memail.com

Description

This file is a 32-bit Windows executable application. This file has been identified as a variant of the DearCry Ransomware. The ransomware attempts to encrypt specific files, identified by file extension, on the target system utilizing the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) encryption algorithms. The ransomware contains the following hard coded public RSA key, which is utilized to encrypt the target system's user files.

--Begin RSA public key--
MIIBCAKCAQEAyLBClz9hsFGRf9fk3z0zmY2rz2J1qqGfV48DSjPV4lcwnhCi4/5+C6UsAhkdI4/5HwbfZBAiMySXNB3DxVB2hOrjDjIeVAkFjQgZ19
--End RSA public key--

During runtime, the ransomware loads the hard-coded RSA public key. It then attempts to identify all drives that are connected to the attached system, from Drive A: to Drive Z:. For each drive identified, the ransomware will enumerate it and encrypt files with the following file extensions:

--Begin targeted file extensions--
.TIF .TIFF .PDF .XLS .XLSX .XLTM .PS .PPS .PPT .PPTX .DOC .DOCX .LOG .MSG .RTF .TEX .TXT .CAD .WPS .EML .INI .CSS .HTM .HTML .XHTML .JS .JSP .PHP .KEYCHAIN .PEM .SQL .APK .APP .BAT .CGI .ASPX .CER .CFM .C .CPP .GO .CONFIG .PL .PY .DWG .XML .JPG .BMP .PNG .EXE .DLL .CAD .AVI .H.CSV .DAT .ISO .PST .PGD .7Z .RAR .ZIP .ZIPX .TAR .PDB .BIN .DB .MDB .MDF .BAK .LOG .EDB .STM .DBF .ORA .GPG .EDB .MFS
--End targeted file extensions--

It will then write the ransom note "readme.txt" to every folder it enumerates on the connected drive.

--Begin ransom note--
Your file has been encrypted!
If you want to decrypt, please contact us.
konedieyp[@]airmail.cc or uenwonken[@]memail.com
And please send me the following hash!
638428e5021d4ae247b21acf9c0bf6f6
--End ransom note--

Next, the ransomware will attempt to encrypt files on the target system that have the file extensions listed above. After encrypting the target system's user files the ransomware will drop the ransom note "readme.txt" within folders with encrypted files on the target system.

The ransomware will then delete the original copy of the files and then replace them with encrypted copies of themselves with the file extension changed to .CRYPT. Before actually deleting the original target file, the malware will overwrite it with the repeating value 0x41 in order to make recovery of the file using computer forensics software impossible.

Before encrypting the target system's user files the malware will encrypt information about the files, including the file's full path and the AES key used to encrypt it, which will also be used to decrypt it. This data will be encrypted using the hard coded Public RSA key mentioned above, and added to the top of the encrypted file. Note: The ransomware will generate a new AES key for every file.

During execution, the ransomware runs a service named “msupdate." After the encryption process and installing the ransom note, the “msupdate" service is removed, which could indicate that the ransomware was executed under the Windows "msupdate" service.

Illustrated below are strings of interest extracted from this binary. These strings indicate the encryption process of the target system's user files is implemented utilizing the OPENSSL library:

--Begin strings of interest--
crypto\evp\e_aes.c
crypto\bio\bio_lib.c
crypto\rsa\rsa_lib.c
crypto\evp\evp_enc.c
assertion failed: bl <= (int)sizeof(ctx->buf)
assertion failed: b <= sizeof ctx->buf
assertion failed: b <= sizeof ctx->final
assertion failed: EVP_CIPHER_CTX_iv_length(ctx) <= (int)sizeof(ctx->iv)
assertion failed: ctx->cipher->block_size == 1 || ctx->cipher->block_size == 8 || ctx->cipher->block_size == 16
%lu:%s:%s:%d:%s
secure memory buffer

memory buffer
crypto\bio\bss_mem.c
CERTIFICATE REQUEST
NEW CERTIFICATE REQUEST
PKCS7
CERTIFICATE
RSA PUBLIC KEY
DH PARAMETERS
X9.42 DH PARAMETERS
crypto\rsa\rsa_crpt.c
crypto\evp\evp_lib.c
assertion failed: l <= sizeof(c->iv)
assertion failed: j <= sizeof(c->iv)
init fail
called a function that was disabled at compile-time
internal error
passed a null parameter
called a function you should not call
malloc failure
fatal
missing asn1 eos
nested asn1 error
ECDSA lib
ENGINE lib
X509V3 lib
PKCS7 lib
BIO lib
EC lib
ASN1 lib
X509 lib
DSA lib
PEM lib
OBJ lib
BUF lib
EVP lib
DH lib
RSA lib
BN lib
system lib
gethostbyname
getsockname
getsockopt
setsockopt
getnameinfo
getaddrinfo
fread
opendir
WSAstartup
accept
listen
bind
ioctlsocket
socket
getservbyname
connect
fopen
KDF routines
ASYNC routines
CT routines
HMAC routines
CMS routines
FIPS routines
OCSP routines
engine routines

time stamp routines
DSO support routines
random number generator
PKCS12 routines
X509 V3 routines
PKCS7 routines
BIO routines
SSL routines
ECDH routines
ECDSA routines
elliptic curve routines
common libcrypto routines
configuration file routines
asn1 encoding routines
x509 certificate routines
dsa routines
PEM routines
object identifier routines
memory buffer routines
digital envelope routines
Diffie-Hellman routines
rsa routines
bignum routines
system library
unknown library
unknown
crypto\err\err.c
error:%08lX:%s:%s:%s
reason(%lu)
func(%lu)
lib(%lu)
crypto\modes\ocb128.c
crypto\threads_win.c
crypto\ex_data.c
OpenSSL PKCS#1 RSA (from Eric Young)
crypto\rsa\rsa_ossl.c
crypto\engine\eng_init.c
crypto\bn\bn_blind.c
crypto\bn\bn_lib.c
%I64i
OPENSSL_ia32cap
Service-0x
_OPENSSL_isservice
OpenSSL: FATAL
OpenSSL
no stack?
%s:%d: OpenSSL internal error: %s
crypto\engine\tb_cipher.c
?assertion failed: *sbuffer != NULL
assertion failed: *currlen <= *maxlen
assertion failed: *sbuffer != NULL || buffer != NULL
crypto\bio\b_print.c
<NULL>
0123456789abcdef
0123456789ABCDEF
0123456789
A-C
?FILE pointer
crypto\bio\bss_file.c
fopen('
','
crypto\buffer\buffer.c
@@You need to read the OpenSSL FAQ, https://www.openssl.org/docs/faq.html
.....

crypto\rand\md_rand.c
crypto\pem\pem_oth.c
X509_REQ
signature
sig_alg
req_info
X509_REQ_INFO
attributes
pubkey
subject
version
0123456789ABCDEF
Proc-Type:
ENCRYPTED
DEK-Info:
crypto\pem\pem_lib.c
phrase is too short, needs to be at least %d chars
Enter PEM pass phrase:
Proc-Type: 4,
BAD-TYPE
MIC-ONLY
MIC-CLEAR
ENCRYPTED
DEK-Info:
-----END

-----BEGIN
CMS
PKCS #7 SIGNED DATA
TRUSTED CERTIFICATE
X509 CERTIFICATE
PARAMETERS
PRIVATE KEY
ENCRYPTED PRIVATE KEY
ANY PRIVATE KEY
assertion failed: strlen(objstr) + 23 + 2 * EVP_CIPHER_iv_length(enc) + 13 <= sizeof buf
assertion failed: EVP_CIPHER_iv_length(enc) <= (int)sizeof(iv)
Expecting:
X509_CRL
crl
X509_CRL_INFO
revoked
nextUpdate
lastUpdate
issuer
X509_REVOKED
extensions
revocationDate
serialNumber
PKCS7_ATTR_VERIFY
PKCS7_ATTR_SIGN
PKCS7_ATTRIBUTES
PKCS7_DIGEST
digest
PKCS7_ENCRYPT
PKCS7_SIGN_ENVELOPE
PKCS7_ENC_CONTENT
algorithm
content_type
PKCS7_RECIP_INFO
enc_key
key_enc_algor
PKCS7_ENVELOPE
enc_data

recipientinfo
PKCS7_ISSUER_AND_SERIAL
serial
PKCS7_SIGNER_INFO
unauth_attr
enc_digest
digest_enc_alg
auth_attr
digest_alg
issuer_and_serial
PKCS7_SIGNED
signer_info
cert
contents
md_algs
type
d.encrypted
d.digest
d.signed_and_enveloped
d.enveloped
d.sign
d.data
d.other
NETSCAPE_CERT_SEQUENCE
certs
crypto\evp\p_lib.c
%s algorithm "%s" unsupported
Public Key
crypto\pem\pem_pkey.c
RSA_OAEP_PARAMS
pSourceFunc
maskGenFunc
hashFunc
RSA_PSS_PARAMS
trailerField
saltLength
maskGenAlgorithm
hashAlgorithm
RSA
X509_PUBKEY
public_key
algor
H/O
</O
h/O
P/O
0/O
crypto\x509\x_pubkey.c
crypto\dsa\dsa_lib.c
DSA
priv_key
pub_key
DSA_SIG
crypto\dsa\dsa_asn1.c
crypto\ec\ec_key.c
assertion failed: eckey->group->meth->keygen != NULL
ECDSA_SIG
EC_PRIVATEKEY
publicKey
parameters
privateKey
ECPKPARAMETERS
value.implicitlyCA
value.parameters

value.named_curve
ECPARAMETERS
cofactor
order
base
curve
fieldID
X9_62_CURVE
seed
X9_62_FIELDID
fieldType
p.char_two
p.prime
X9_62_CHARACTERISTIC_TWO
p.ppBasis
p.tpBasis
p.onBasis
p.other
X9_62_PENTANOMIAL
certificate extensions
set-certExt
set-policy
set-attr
message extensions
set-msgExt
content types
set-ctype
Secure Electronic Transactions
id-set
pseudonym
generationQualifier
id-hex-multipart-message
id-hex-partial-message
mime-mhs-bodies
mime-mhs-headings
MIME MHS
mime-mhs
x500UniqueIdentifier
documentPublisher
audio
dITRedirect
personalSignature
subtreeMaximumQuality
subtreeMinimumQuality
singleLevelQuality
dSAQuality
buildingName
mailPreferenceOption
janetMailbox
organizationalStatus
friendlyCountryName
pagerTelephoneNumber
mobileTelephoneNumber
personalTitle
homePostalAddress
associatedName
associatedDomain
cNAMERecord
sOARecord
nSRecord
mXRecord
pilotAttributeType27
aRecord
lastModifiedBy

lastModifiedTime
otherMailbox
secretary
homeTelephoneNumber
documentLocation
documentAuthor
documentVersion
documentTitle
documentIdentifier
manager
host
userClass
photo
roomNumber
favouriteDrink
info
rfc822Mailbox
mail
textEncodedORAddress
userId
UID
qualityLabelledData
pilotDSA
pilotOrganization
simpleSecurityObject
friendlyCountry
domainRelatedObject
dNSDomain
rFC822localPart
documentSeries
room
document
account
pilotPerson
pilotObject
caseIgnoreIA5StringSyntax
iA5StringSyntax
pilotGroups
pilotObjectClass
pilotAttributeSyntax
pilotAttributeType
pilot
ucl
pss
data
Hold Instruction Reject
holdInstructionReject
Hold Instruction Call Issuer
holdInstructionCallIssuer
Hold Instruction None
holdInstructionNone
Hold Instruction Code
holdInstructionCode
aes-256-cfb
AES-256-CFB
aes-256-ofb
AES-256-OFB
aes-256-cbc
AES-256-CBC
aes-256-ecb
AES-256-ECB
aes-192-cfb
AES-192-CFB
aes-192-ofb

AES-192-OFB
aes-192-cbc
AES-192-CBC
aes-192-ecb
AES-192-ECB
aes-128-cfb
AES-128-CFB
aes-128-ofb
AES-128-OFB
aes-128-cbc
AES-128-CBC
aes-128-ecb
AES-128-ECB
Microsoft CSP Name
CSPName
ecdsa-with-SHA1
prime256v1
prime239v3
prime239v2
prime239v1
prime192v3
prime192v2
prime192v1
id-ecPublicKey
characteristic-two-field
prime-field
ANSI X9.62
ansi-X9-62
X509v3 No Revocation Available
noRevAvail
X509v3 AC Targeting
targetInformation
X509v3 Policy Constraints
policyConstraints
role
id-aca-encAttrs
Subject Information Access
subjectInfoAccess
ac-proxying
md4WithRSAEncryption
RSA-MD4
clearance
Selected Attribute Types
selected-attribute-types
Domain
domain
domainComponent
dcObject
dcobject
Enterprises
enterprises
Mail
SNMPv2
snmpv2
Security
security
Private
private
Experimental
experimental
Management
mgmt
Directory
directory

iana
IANA
dod
DOD
org
ORG
directory services - algorithms
X500algorithms
rsaSignature
Trust Root
trustRoot
path
valid
Extended OCSP Status
extendedStatus
OCSP Service Locator
serviceLocator
OCSP Archive Cutoff
archiveCutoff
OCSP No Check
noCheck
Acceptable OCSP Responses
acceptableResponses
OCSP CRL ID
CrlID
OCSP Nonce
Nonce
Basic OCSP Response
basicOCSPResponse
ad dvcs
AD_DVCS
AD Time Stamping
ad_timestamping
id-cct-PKIResponse
id-cct-PKIData
id-cct-crs
id-qcs-pkixQCSyntax-v1
id-aca-role
id-aca-group
id-aca-chargingIdentity
id-aca-accessIdentity
id-aca-authenticationInfo
id-pda-countryOfResidence
id-pda-countryOfCitizenship
id-pda-gender
id-pda-placeOfBirth
id-pda-dateOfBirth
id-on-personalData
id-cmc-confirmCertAcceptance
id-cmc-popLinkWitness
id-cmc-popLinkRandom
id-cmc-queryPending
id-cmc-responseInfo
id-cmc-regInfo
id-cmc-revokeRequest
crypto\asn1\tasn_enc.c
crypto\asn1\tasn_new.c
crypto\asn1\tasn_fre.c
crypto\asn1\a_dup.c
assertion failed: niv <= EVP_MAX_IV_LENGTH
assertion failed: nkey <= EVP_MAX_KEY_LENGTH
crypto\evp\evp_key.c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
?456789:;<=

!"#$%&'()*+,-./0123
crypto\evp\encode.c
assertion failed: ctx->length <= (int)sizeof(ctx->enc_data)
assertion failed: n < (int)sizeof(ctx->enc_data)
crypto\asn1\ameth_lib.c
X509_EXTENSIONS
Extension
X509_EXTENSION
critical
--End strings of interest--

Screenshots

Figure 1 - Screenshot of the data that will be prepended to an encrypted file. This data will contain an AES key that can be used to decrypt the file, as well as the full path of the file. This block will be encrypted via the hard-coded RSA key before it is prepended to the newly encrypted files. The ransomware will generate a new AES key for each file it encrypts.

Figure 2 - Screenshot of data after it is encrypted using the malware's hard-coded RSA key.

Figure 3 - Screenshot of the header of an encrypted file after the encrypted AES key and the full path of the file data is appended.

Figure 4 - The ransomware enumerating all drives attached to the target system.

Figure 5 - The ransomware writing the ransom note "readme.txt" to a directory after it encrypts contents of a directory.

Figure 6 - The ransomware deleting the "msupdate" service after encryption of the target system's files complete.

konedieyp[@]airmail.cc

Tags

ransomware

Details

Address	konedieyp[@]airmail.cc

Relationships

konedieyp[@]airmail.cc	Related_To	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
konedieyp[@]airmail.cc	Related_To	fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65
konedieyp[@]airmail.cc	Related_To	027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27
konedieyp[@]airmail.cc	Related_To	e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
konedieyp[@]airmail.cc	Related_To	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
konedieyp[@]airmail.cc	Related_To	10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da

Description

The DearCry ransomware samples contain this email address in the ransom note as a contact for decrypting files.

uenwonken[@]memail.com

Tags

ransomware

Details

Address	uenwonken[@]memail.com

Relationships

uenwonken[@]memail.com	Related_To	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff

uenwonken[@]memail.com	Related_To	fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65
uenwonken[@]memail.com	Related_To	027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27
uenwonken[@]memail.com	Related_To	e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
uenwonken[@]memail.com	Related_To	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
uenwonken[@]memail.com	Related_To	10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da

Description

The DearCry ransomware samples contain this email address in the ransom note as a contact for decrypting files.

fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65

Tags

ransomwaretrojan

Details

Name	fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65
Size	1322521 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	6be28a4523984698e7154671f73361bf
SHA1	b974375ef0f6dcb6ce30558df2ed8570bf1ad642
SHA256	fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65
SHA512	c3a44431e8cbb76d75ea2a1caca6fe77dfbd2a9565da918620433d415d396c08394ecb1c6454fc69661d61683711e53b60a69435e25518a04e8
ssdeep	24576:C5Nv2SkWFP/529IC8u2bAs0NIzkQS+KpPbEasBY2iKDl1fpxkLVZgMCST:oB70s9yjE62iIl1fpxkLVZgMCA
Entropy	6.994288

Antivirus

Ahnlab	Ransomware/Win.DoejoCrypt
Antiy	Trojan[Ransom]/Win32.Encoder
Avira	TR/AD.DearcryRansom.dneew
BitDefender	Gen:Heur.Mint.Zard.46
ClamAV	Win.Ransomware.Dearcry-9840778-0
Comodo	Malware
Cyren	W32/Ransom.TNVJ-5084
ESET	a variant of Win32/Filecoder.DearCry.A trojan
Emsisoft	Gen:Heur.Mint.Zard.46 (B)
Ikarus	Trojan-Ransom.FileCrypter
K7	Trojan (005790ee1)
Lavasoft	Gen:Heur.Mint.Zard.46
McAfee	Ransom-DearCry!6BE28A452398
Microsoft Security Essentials	Ransom:Win32/DoejoCrypt.A
NANOAV	Trojan.Win32.Encoder.ioxcpd
Quick Heal	Ransom.DearCry.S19261705
Sophos	Troj/Ransom-GFE

Symantec	Ransom.Dearcry
Systweak	trojan-ransom.dearcry
TACHYON	Ransom/W32.DearCry.1322521
TrendMicro	Ransom.53933CA6
TrendMicro House Call	Ransom.53933CA6
Vir.IT eXplorer	Ransom.Win32.DearCry.CUQ
VirusBlokAda	TrojanRansom.Encoder
Zillya!	Trojan.Filecoder.Win32.18026

YARA Rules

- rule CISA_10330097_01 : trojan downloader ransomware DEARCRY
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10330097"
      Date = "2021-03-31"
      Last_Modified = "20210331_1630"
      Actor = "n/a"
      Category = "Trojan Downloader Ransomware"
      Family = "DEARCRY"
      Description = "Detects DearCry Ransomware"
      MD5_1 = "0e55ead3b8fd305d9a54f78c7b56741a"
      SHA256_1 = "2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff"
      MD5_2 = "cdda3913408c4c46a6c575421485fa5b"
      SHA256_2 = "e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6"
      MD5_3 = "c6eeb14485d93f4e30fb79f3a57518fc"
      SHA256_3 = "feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede"
    strings:
      $s0 = { 8B 85 04 EA FF FF 50 8B 8D 08 EA FF FF 51 8B 55 14 52 8B 45 10 50 8D 8D 68 F0 FF FF 51 8B 95 00 EA FF FF 52 }
      $s1 = { 43 72 79 70 74 6F 50 72 6F 2D 58 63 68 42 }
      $s2 = "-----BEGIN RSA PUBLIC KEY-----"
      $s3 = ".CRYPT"
    condition:
      all of them
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-03-08 01:29:05-05:00
Import Hash	f8b8e20e844ccd50a8eb73c2fca3626d

PE Sections

MD5	Name	Raw Size	Entropy
19c89970662b40d47561bb17377abe08	header	1024	2.591397
07abe3c7ee0a03e132be7d8e50cb59b3	.text	976896	7.069141
7133c887704081b6d3678f691a6754fe	.rdata	265728	6.128972
bef1589c6181fa392609e904f4410443	.data	26112	4.707707
a0bf446401bdd255b7f7cb0215177d73	.rsrc	512	5.108717

MD5	Name	Raw Size	Entropy
f3d5e7499f330d470ed5e0dd856b599c	.reloc	51712	5.474130

Packers/Compilers/Cryptors

Relationships

fdec933ca1...	Related_To	konedieyp[@]airmail.cc
fdec933ca1...	Related_To	uenwonken[@]memail.com

Description

This file is a malicious 32-bit Windows executable. It has been identified as a variant of the DearCry ransomware and is similar in design and functionality to the file 2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff. The hard-coded RSA key contained within this binary is illustrated below.

--Begin RSA public key--
MIIBCAKCAQEA5+mVBe75OvCzCW4oZHl7vqPwV2O4kgzgfp9odcL9LZc8Gy2+NJPDwrHbttKI3z4Yt3G04lX7bEp1RZjxUYfzX8qvaPC2EBduOjS
--End RSA public key--

This ransomware provides the following ransom note within directories of encrypted files on the target system and shared drives:

--Begin ransom note--
Your file has been encrypted!
If you want to decrypt, please contact us.
konedieyp[@]airmail.cc or uenwonken[@]memail.com
And please send me the following hash!
d37fc1eabc6783a418d23a8d2ba5db5a
--End ransom note--

027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27

Tags

ransomwaretrojan

Details

Name	027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27
Size	1322496 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	a7e571312e05d547936aab18f0b30fbf
SHA1	e0d643e759b2adf736b451aff9afa92811ab8a99
SHA256	027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27
SHA512	20e8af2770aa1be935f7d1b74d6db6f9aeb5aebab016ac6c2e58e60b1b5c9029726fda7b75ed003bf4a1a5a480024231c6a90f5a3d812bf2438dc
ssdeep	24576:C5Nv2SkWFP/529IC8u2bAs0NIzkQS+KpPbEasBY2iKDl1fpxkLVZgMCSZ:oB70s9yjE62iIl1fpxkLVZgMCk
Entropy	6.994270

Antivirus

Ahnlab	Ransomware/Win.DoejoCrypt
Avira	TR/AD.DearcryRansom.dneew
BitDefender	Gen:Heur.Mint.Zard.46
ClamAV	Win.Ransomware.Dearcry-9840778-0
Comodo	Malware

Cyren	W32/Trojan.UHTA-2594
ESET	a variant of Win32/Filecoder.DearCry.A trojan
Emsisoft	Gen:Heur.Mint.Zard.46 (B)
Ikarus	Trojan-Ransom.FileCrypter
K7	Trojan (005790ee1)
Lavasoft	Gen:Heur.Mint.Zard.46
McAfee	Ransom-DearCry!A7E571312E05
Microsoft Security Essentials	Ransom:Win32/DoejoCrypt.A
NANOAV	Trojan.Win32.Encoder.ioxcpd
Quick Heal	Ransom.DearCry.S19261705
Sophos	Troj/Ransom-GFE
Symantec	Unavailable (production)
Systweak	trojan-ransom.dearcry
TACHYON	Ransom/W32.DearCry.1322496
TrendMicro	Ransom.FC206072
TrendMicro House Call	Ransom.FC206072
Vir.IT eXplorer	Ransom.Win32.DearCry.CUQ
VirusBlokAda	TrojanRansom.Encoder
Zillya!	Trojan.Filecoder.Win32.18026

YARA Rules

- rule CISA_10330097_01 : trojan downloader ransomware DEARCRY
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10330097"
      Date = "2021-03-31"
      Last_Modified = "20210331_1630"
      Actor = "n/a"
      Category = "Trojan Downloader Ransomware"
      Family = "DEARCRY"
      Description = "Detects DearCry Ransomware"
      MD5_1 = "0e55ead3b8fd305d9a54f78c7b56741a"
      SHA256_1 = "2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff"
      MD5_2 = "cdda3913408c4c46a6c575421485fa5b"
      SHA256_2 = "e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6"
      MD5_3 = "c6eeb14485d93f4e30fb79f3a57518fc"
      SHA256_3 = "feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede"
    strings:
      $s0 = { 8B 85 04 EA FF FF 50 8B 8D 08 EA FF FF 51 8B 55 14 52 8B 45 10 50 8D 8D 68 F0 FF FF 51 8B 95 00 EA FF FF 52 }
      $s1 = { 43 72 79 70 74 6F 50 72 6F 2D 58 63 68 42 }
      $s2 = "-----BEGIN RSA PUBLIC KEY-----"
      $s3 = ".CRYPT"
    condition:
      all of them
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-03-08 01:29:05-05:00
Import Hash	f8b8e20e844ccd50a8eb73c2fca3626d

PE Sections

MD5	Name	Raw Size	Entropy
19c89970662b40d47561bb17377abe08	header	1024	2.591397
07abe3c7ee0a03e132be7d8e50cb59b3	.text	976896	7.069141
7133c887704081b6d3678f691a6754fe	.rdata	265728	6.128972
bef1589c6181fa392609e904f4410443	.data	26112	4.707707
a0bf446401bdd255b7f7cb0215177d73	.rsrc	512	5.108717
f3d5e7499f330d470ed5e0dd856b599c	.reloc	51712	5.474130

Packers/Compilers/Cryptors

Relationships

027119161d...	Related_To	konedieyp[@]airmail.cc
027119161d...	Related_To	uenwonken[@]memail.com

Description

This file is a malicious 32-bit Windows executable. It has been identified as a variant of the DearCry ransomware and is similar in design and functionality to the file 2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff. The hard-coded RSA key contained within this binary is illustrated below.

--Begin RSA public key--
MIIBCAKCAQEA5+mVBe75OvCzCW4oZHl7vqPwV2O4kgzgfp9odcL9LZc8Gy2+NJPDwrHbttKI3z4Yt3G04lX7bEp1RZjxUYfzX8qvaPC2EBduOjS
--End RSA public key--

This ransomware provides the following ransom note within directories of encrypted files on the target system and shared drives:

--Begin ransom note--
Your file has been encrypted!
If you want to decrypt, please contact us.
konedieyp[@]airmail.cc or uenwonken[@]memail.com
And please send me the following hash!
d37fc1eabc6783a418d23a8d2ba5db5a
--End ransom note--

e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6

Tags

downloaderloaderransomwaretrojan

Details

Name	e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
Size	1322496 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	cdda3913408c4c46a6c575421485fa5b
SHA1	56eec7392297e7301159094d7e461a696fe5b90f
SHA256	e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
SHA512	666b7419adaa2fba34e53416fc29cac92bbbe36d9fae57bae00001d644f35484df9b1e44a516866b000b8ab04cd2241414fe0692e1a5b6f36d54(

ssdeep	24576:C5Nv2SkWFP/529IC8u2bAs0NIzkQS+KpPbEasBY2iKDl1fpxkLVZgMCS+:oB70s9yjE62iIl1fpxkLVZgMC3
Entropy	6.994272

Antivirus

Ahnlab	Ransomware/Win.DoejoCrypt
Antiy	Trojan[Ransom]/Win32.Encoder
Avira	TR/AD.DearcryRansom.dneew
BitDefender	Gen:Heur.Mint.Zard.46
ClamAV	Win.Ransomware.Dearcry-9840778-0
Comodo	Malware
Cyren	W32/Trojan.UHSB-2594
ESET	a variant of Win32/Filecoder.DearCry.A trojan
Emsisoft	Gen:Heur.Mint.SP.Ransom.Dearcry.1 (B)
Ikarus	Trojan-Ransom.FileCrypter
K7	Trojan (005790ee1)
Lavasoft	Gen:Heur.Mint.SP.Ransom.Dearcry.1
McAfee	Ransom-DearCry!CDDA3913408C
Microsoft Security Essentials	Ransom:Win32/DoejoCrypt.A
NANOAV	Trojan.Win32.Encoder.ioxcpd
Quick Heal	Ransom.DearCry.S19261705
Sophos	Troj/Ransom-GFE
Symantec	Downloader
TACHYON	Ransom/W32.DearCry.1322496
TrendMicro	Ransom.56DC2A23
TrendMicro House Call	Ransom.56DC2A23
Vir.IT eXplorer	Ransom.Win32.DearCry.CUQ
VirusBlokAda	TrojanRansom.Encoder
Zillya!	Trojan.Filecoder.Win32.18026

YARA Rules

- rule CISA_10330097_01 : trojan downloader ransomware DEARCRY
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10330097"
      Date = "2021-03-31"
      Last_Modified = "20210331_1630"
      Actor = "n/a"
      Category = "Trojan Downloader Ransomware"
      Family = "DEARCRY"
      Description = "Detects DearCry Ransomware"
      MD5_1 = "0e55ead3b8fd305d9a54f78c7b56741a"
      SHA256_1 = "2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff"
      MD5_2 = "cdda3913408c4c46a6c575421485fa5b"
      SHA256_2 = "e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6"
      MD5_3 = "c6eeb14485d93f4e30fb79f3a57518fc"
      SHA256_3 = "feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede"

```
    strings:
        $s0 = { 8B 85 04 EA FF FF 50 8B 8D 08 EA FF FF 51 8B 55 14 52 8B 45 10 50 8D 8D 68 F0 FF FF 51 8B 95
00 EA FF FF 52 }
        $s1 = { 43 72 79 70 74 6F 50 72 6F 2D 58 63 68 42 }
        $s2 = "-----BEGIN RSA PUBLIC KEY-----"
        $s3 = ".CRYPT"
    condition:
        all of them
}
```

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-03-08 01:29:05-05:00
Import Hash	f8b8e20e844ccd50a8eb73c2fca3626d

PE Sections

MD5	Name	Raw Size	Entropy
19c89970662b40d47561bb17377abe08	header	1024	2.591397
07abe3c7ee0a03e132be7d8e50cb59b3	.text	976896	7.069141
7133c887704081b6d3678f691a6754fe	.rdata	265728	6.128972
bef1589c6181fa392609e904f4410443	.data	26112	4.707707
a0bf446401bdd255b7f7cb0215177d73	.rsrc	512	5.108717
f3d5e7499f330d470ed5e0dd856b599c	.reloc	51712	5.474130

Packers/Compilers/Cryptors

Relationships

e044d9f2d0...	Related_To	konedieyp[@]airmail.cc
e044d9f2d0...	Related_To	uenwonken[@]memail.com

Description

This file is a malicious 32-bit Windows executable. It has been identified as a variant of the DearCry ransomware and is similar in design and functionality to the file 2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff. The hard-coded RSA key contained within this binary is illustrated below.

--Begin RSA public key--
MIIBCAKCAQEA5+mVBe75OvCzCW4oZHl7vqPwV2O4kgzgfp9odcL9LZc8Gy2+NJPDwrHbttKI3z4Yt3G04lX7bEp1RZjxUYfzX8qvaPC2EBduOjS
--End RSA public key--

This ransomware provides the following ransom note within directories of encrypted files on the target system and shared drives:

--Begin ransom note--
Your file has been encrypted!
    If you want to decrypt, please contact us.
    konedieyp[@]airmail.cc or uenwonken[@]memail.com
    And please send me the following hash!
    d37fc1eabc6783a418d23a8d2ba5db5a
--End ransom note--

feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede

Tags

downloaderloaderransomwaretrojan

Details

Name	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
Size	1322496 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	c6eeb14485d93f4e30fb79f3a57518fc
SHA1	b7d99521348d319f57d2b2ba7045295fc99cf6a7
SHA256	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
SHA512	1cf95db6bb1b4b047ae91711c5f14c618c19ddee2465df44905e082a59c53d3aeee0e69e9aaf562ba117015e2e84ccfaed6b94d863dc6c153ba4a
ssdeep	24576:LU5NX2yJOiUXmEICxu2WAP0NIzkQM+KpPRQ9StIUDpl1fpxkzVZgMCS+:L7XP7P9o5QzUtl1fpxkzVZgMC3
Entropy	6.994636

Antivirus

Ahnlab	Ransomware/Win.DoejoCrypt
Antiy	Trojan[Ransom]/Win32.DearCry
Avira	TR/AD.DearcryRansom.prkjk
BitDefender	Trojan.GenericKD.36489973
ClamAV	Win.Ransomware.Dearcry-9840778-0
Comodo	Malware
Cyren	W32/Trojan.BMMM-2027
ESET	a variant of Win32/Filecoder.DearCry.A trojan
Emsisoft	Trojan.GenericKD.36489973 (B)
Ikarus	Trojan-Ransom.FileCrypter
K7	Trojan (005790de1)
Lavasoft	Trojan.GenericKD.36489973
McAfee	Ransom-DearCry!C6EEB14485D9
Microsoft Security Essentials	Ransom:Win32/DoejoCrypt.A
NANOAV	Trojan.Win32.Encoder.ipilfs
Quick Heal	Ransom.DearCry.S19261705
Sophos	Troj/Ransom-GFE
Symantec	Downloader
TACHYON	Ransom/W32.DearCry.1322496
TrendMicro	Ransom.56DC2A23
TrendMicro House Call	Ransom.56DC2A23
Vir.IT eXplorer	Ransom.Win32.DearCry.CUQ
VirusBlokAda	TrojanRansom.Encoder
Zillya!	Trojan.Encoder.Win32.2195

YARA Rules

- rule CISA_10330097_01 : trojan downloader ransomware DEARCRY
  {
    meta:

```
        Author = "CISA Code & Media Analysis"
        Incident = "10330097"
        Date = "2021-03-31"
        Last_Modified = "20210331_1630"
        Actor = "n/a"
        Category = "Trojan Downloader Ransomware"
        Family = "DEARCRY"
        Description = "Detects DearCry Ransomware"
        MD5_1 = "0e55ead3b8fd305d9a54f78c7b56741a"
        SHA256_1 = "2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff"
        MD5_2 = "cdda3913408c4c46a6c575421485fa5b"
        SHA256_2 = "e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6"
        MD5_3 = "c6eeb14485d93f4e30fb79f3a57518fc"
        SHA256_3 = "feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede"
    strings:
        $s0 = { 8B 85 04 EA FF FF 50 8B 8D 08 EA FF FF 51 8B 55 14 52 8B 45 10 50 8D 8D 68 F0 FF FF 51 8B 95
00 EA FF FF 52 }
        $s1 = { 43 72 79 70 74 6F 50 72 6F 2D 58 63 68 42 }
        $s2 = "-----BEGIN RSA PUBLIC KEY-----"
        $s3 = ".CRYPT"
    condition:
        all of them
}
```

ssdeep Matches

99	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff

PE Metadata

Compile Date	2021-03-09 03:08:39-05:00
Import Hash	f8b8e20e844ccd50a8eb73c2fca3626d

PE Sections

MD5	Name	Raw Size	Entropy
4289116f218aa083456871506085e1be	header	1024	2.596118
46c15879afc7b600a23284d8e72f87aa	.text	976896	7.069452
d0093b4c33543ebd59b2c22c7e71670f	.rdata	265728	6.128934
8883af046ae6ebae63ae3882d79bfc4e	.data	25600	4.793715
a0bf446401bdd255b7f7cb0215177d73	.rsrc	512	5.108717
bcd8233433c686e481a6c5a4f1f263ac	.reloc	51712	5.474063

Packers/Compilers/Cryptors

Relationships

feb3e6d30b...	Related_To	konedieyp[@]airmail.cc
feb3e6d30b...	Related_To	uenwonken[@]memail.com

Description

This file is a malicious 32 bit Windows executable. It has been identified as a variant of the DearCry ransomware and is similar in design and functionality to the file 2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff. The hard-coded RSA key contained within this binary is illustrated below.

--Begin RSA public key--
MIIBCAKCAQEA1Qdzdr0sRv1i+hUXF6rzsLYjQ3NRuJO16S4MpmG54q5mX0TxEEh1FmkQwULatEQkDSBC1Qbi6ZNAYhvYGj4K2G2dfIexSXfaz
--End RSA public key--

This ransomware provides the following ransom note within directories of encrypted files on the target system and shared drives:

--Begin ransom note--
Your file has been encrypted!
If you want to decrypt, please contact us.
konedieyp[@]airmail.cc or uenwonken[@]memail.com
And please send me the following hash!
2133c369fb115ea61eebd7b62768decf
--End ransom note--

10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da

Tags

ransomwaretrojan

Details

Name	10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da
Size	1322521 bytes
Type	PE32 executable (console) Intel 80386, for MS Windows
MD5	9f05994819a3d8c1a3769352c7c39d1d
SHA1	eb2457196e04dfdd54f70bd32ed02ae854d45bc0
SHA256	10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da
SHA512	32cac848f47a0096773435c6365fcbd6bdb02115aae2677aec5a86031b6def938033210fdcf0e12f735aa5ceb8cd4be5f7edb5cdc437bbca61f0d7
ssdeep	24576:LU5NX2yJOiUXmEICxu2WAP0NIzkQM+KpPRQ9StIUDpl1fpxkzVZgMCST:L7XP7P9o5QzUtl1fpxkzVZgMCA
Entropy	6.994652

Antivirus

Ahnlab	Ransomware/Win.DoejoCrypt
Antiy	Trojan[Ransom]/Win32.DearCry
Avira	TR/AD.DearcryRansom.prkjk
BitDefender	Trojan.GenericKD.36489973
ClamAV	Win.Ransomware.Dearcry-9840778-0
Comodo	Malware
Cyren	W32/Trojan.NIBO-1126
ESET	a variant of Win32/Filecoder.DearCry.A trojan
Emsisoft	Trojan.GenericKD.36489973 (B)
Ikarus	Trojan-Ransom.FileCrypter
K7	Trojan (005790de1)
Lavasoft	Trojan.GenericKD.36489973
McAfee	Ransom-DearCry!9F05994819A3
Microsoft Security Essentials	Ransom:Win32/DoejoCrypt.A
NANOAV	Trojan.Win32.Encoder.ipilfs
NetGate	Trojan.Win32.Malware
Quick Heal	Ransom.DearCry.S19261705
Sophos	Troj/Ransom-GFE

Symantec	Ransom.Dearcry
Systweak	trojan-ransom.dearcry
TACHYON	Ransom/W32.DearCry.1322521
TrendMicro	Ransom.53933CA6
TrendMicro House Call	Ransom.53933CA6
Vir.IT eXplorer	Ransom.Win32.DearCry.CUQ
VirusBlokAda	TrojanRansom.Encoder
Zillya!	Trojan.Encoder.Win32.2195

YARA Rules

- rule CISA_10330097_01 : trojan downloader ransomware DEARCRY
  {
    meta:
      Author = "CISA Code & Media Analysis"
      Incident = "10330097"
      Date = "2021-03-31"
      Last_Modified = "20210331_1630"
      Actor = "n/a"
      Category = "Trojan Downloader Ransomware"
      Family = "DEARCRY"
      Description = "Detects DearCry Ransomware"
      MD5_1 = "0e55ead3b8fd305d9a54f78c7b56741a"
      SHA256_1 = "2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff"
      MD5_2 = "cdda3913408c4c46a6c575421485fa5b"
      SHA256_2 = "e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6"
      MD5_3 = "c6eeb14485d93f4e30fb79f3a57518fc"
      SHA256_3 = "feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede"
    strings:
      $s0 = { 8B 85 04 EA FF FF 50 8B 8D 08 EA FF FF 51 8B 55 14 52 8B 45 10 50 8D 8D 68 F0 FF FF 51 8B 95 00 EA FF FF 52 }
      $s1 = { 43 72 79 70 74 6F 50 72 6F 2D 58 63 68 42 }
      $s2 = "-----BEGIN RSA PUBLIC KEY-----"
      $s3 = ".CRYPT"
    condition:
      all of them
  }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-03-09 03:08:39-05:00
Import Hash	f8b8e20e844ccd50a8eb73c2fca3626d

PE Sections

MD5	Name	Raw Size	Entropy
4289116f218aa083456871506085e1be	header	1024	2.596118
46c15879afc7b600a23284d8e72f87aa	.text	976896	7.069452
d0093b4c33543ebd59b2c22c7e71670f	.rdata	265728	6.128934
8883af046ae6ebae63ae3882d79bfc4e	.data	25600	4.793715
a0bf446401bdd255b7f7cb0215177d73	.rsrc	512	5.108717

MD5	Name	Raw Size	Entropy
bcd8233433c686e481a6c5a4f1f263ac	.reloc	51712	5.474063

Packers/Compilers/Cryptors

Relationships

10bce0ff65...	Related_To	konedieyp[@]airmail.cc
10bce0ff65...	Related_To	uenwonken[@]memail.com

Description

This file is a malicious 32-bit Windows executable. It has been identified as a variant of the DearCry ransomware and is similar in design and functionality to the file 2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff. The hard-coded RSA key contained within this binary is illustrated below.

--Begin RSA public key--
MIIBCAKCAQEA1Qdzdr0sRv1i+hUXF6rzsLYjQ3NRuJO16S4MpmG54q5mX0TxEEh1FmkQwULatEQkDSBC1Qbi6ZNAYhvYGj4K2G2dfIexSXfaz
--End RSA public key--

This ransomware provides the following ransom note within directories of encrypted files on the target system and shared drives:

--Begin ransom note--
Your file has been encrypted!
If you want to decrypt, please contact us.
konedieyp[@]airmail.cc or uenwonken[@]memail.com
And please send me the following hash!
2133c369fb115ea61eebd7b62768decf
--End ransom note--

Relationship Summary

2b9838da7e...	Related_To	konedieyp[@]airmail.cc
2b9838da7e...	Related_To	uenwonken[@]memail.com
konedieyp[@]airmail.cc	Related_To	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
konedieyp[@]airmail.cc	Related_To	fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65
konedieyp[@]airmail.cc	Related_To	027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27
konedieyp[@]airmail.cc	Related_To	e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
konedieyp[@]airmail.cc	Related_To	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
konedieyp[@]airmail.cc	Related_To	10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da
uenwonken[@]memail.com	Related_To	2b9838da7edb0decd32b086e47a31e8f5733b5981ad8247a2f9508e232589bff
uenwonken[@]memail.com	Related_To	fdec933ca1dd1387d970eeea32ce5d1f87940dfb6a403ab5fc149813726cbd65
uenwonken[@]memail.com	Related_To	027119161d11ba87acc908a1d284b93a6bcafccc012e52ce390ecb9cd745bf27
uenwonken[@]memail.com	Related_To	e044d9f2d0f1260c3f4a543a1e67f33fcac265be114a1b135fd575b860d2b8c6
uenwonken[@]memail.com	Related_To	feb3e6d30ba573ba23f3bd1291ca173b7879706d1fe039c34d53a4fdcdf33ede
uenwonken[@]memail.com	Related_To	10bce0ff6597f347c3cca8363b7c81a8bff52d2ff81245cd1e66a6e11aeb25da
fdec933ca1...	Related_To	konedieyp[@]airmail.cc
fdec933ca1...	Related_To	uenwonken[@]memail.com
027119161d...	Related_To	konedieyp[@]airmail.cc
027119161d...	Related_To	uenwonken[@]memail.com
e044d9f2d0...	Related_To	konedieyp[@]airmail.cc

e044d9f2d0...	Related_To	uenwonken[@]memail.com
feb3e6d30b...	Related_To	konedieyp[@]airmail.cc
feb3e6d30b...	Related_To	uenwonken[@]memail.com
10bce0ff65...	Related_To	konedieyp[@]airmail.cc
10bce0ff65...	Related_To	uenwonken[@]memail.com

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, **"Guide to Malware Incident Prevention & Handling for Desktops and Laptops".**

Contact Information

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances this report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the CISA at 1-844-Say-CISA or SayCISA@cisa.dhs.gov✉.

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov✉
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.
