CryptBot

research.openanalysis.net/cryptbot/botnet/yara/config/2023/03/16/cryptbot.html

OALABS Research

March 16, 2023

Overview

This is another C++ bot! According to Malpedia...

> A typical infostealer, capable of obtaining credentials for browsers, crypto currency wallets, browser cookies, credit cards, and creates screenshots of the infected system. All stolen data is bundled into a zip-file that is uploaded to the c2.

Samples

Samples available on UnpacMe- Packed
`7ccda59528c0151bc9f11b7f25f8291d99bcf541488c009ef14e2a104e6f0c5d`

Unpacked `cfbecf45c083efffff6d3000972a66cddb2f26d5c1845a697351b132e65049e0`

References

Analysis

This is a some in-memory string that was captured in a joe sandbox run

```
 Content-Length: Content-Type: multipart/form-data;boundary=httphttpstrue<>S-1-5-
18[<apis.google.com>]/[<443>][<www.google.com>][<"facebook">][<www.facebook.com>]
[<TEMP>][<APPDATA>][<LOCALAPPDATA>][<USERPROFILE>];[<ExternalDownload>][<Anti>]
[<true>][<UserAgent>][<UAC>]runas[<NTFS>][<Prefix>][<UID: >][<UserName: >]
[<ComputerName: >][<Info>][<OS: >][<DateTime: >][<UserAgent: >][<Keyboard Languages:
>][<Display Resolution: >][<CPU: >][<RAM: >][<GPU: >][<isGodMod: yes>][<isGodMod:
no>][<isAdmin: yes>][<isAdmin: no>][<Installed software:>][<Disk:>][<Process:>]
[<Screenshot>][<InfoFile>][<ScreenFile>][<PasswordFile>][<ChromeDBFolder>]
[<ChromeExt>][<WalletFolder>][<_Chrome_profile>][<EdgeDB>][<EdgeDBFolder>][<EdgeExt>]
[<_Edge_profile>][<Desktop>][<DesktopFolder>][<.txt>][<Wallet>]_test.err://[<80>]
[<OK>][< /c >][<cmd>][<open>][<MessageAfterEnd>][<System Error>][<The application was
unable to start correctly (0xc000007b). Click OK to close the application.>]
[<DeleteAfterEnd>][< /c timeout  -t  5  && del ">]
```

Yara Rule

Some of these strings exist in the binary unencrypted so we can use them for a yara rule

```
rule cryptbot {

    strings:
        $s1 = "UID:"
        $s2 = "UserName:"
        $s3 = "ComputerName:"
        $s4 = "DateTime:"
        $s5 = "UserAgent:"
        $s6 = "Keyboard Languages:"
        $s7 = "Display Resolution:"
        $s8 = "CPU:"
        $s9 = "RAM:"
        $s10 = "GPU:"
        $s11 = "isGodMod: yes"
        $s12 = "isGodMod: no"
        $s13 = "isAdmin: yes"
        $s14 = "isAdmin: no"
        $s15 = "Installed software:"
    condition:
        all of them
}
```

Config

Finding a ref to the config in the code.

```
80 3D ?? ?? ?? ?? 09                    cmp     byte ptr ptr_config, 9 ; "PSJigdSdi8"
B9 00 01 00 00                          mov     ecx, 100h

B9 00 01 00 00                          mov     ecx, 100h
80 3D ?? ?? ?? ?? 09                    cmp     byte ptr a7m1fqxrljy, 9 ;
"7m1fqXrLJy"
```

```
import re
import pefile
import struct

file_data = open('/tmp/cryptbot.bin', 'rb').read()
pe = pefile.PE(data = file_data)
image_base = pe.OPTIONAL_HEADER.ImageBase

text_data = None

for s in pe.sections:
    if b'.text' == s.Name[:5]:
        text_data = s.get_data()
        break

assert text_data is not None


eggs = [
        rb'\x80\x3D(....)\x09\xB9\x00\x01\x00\x00',
        rb'\xB9\x00\x01\x00\x00\x80\x3D(....)\x09'
       ]

candidate_offsets = []

for egg in eggs:
    for m in re.finditer(egg, text_data, re.DOTALL):
        try:
            candidate_va = struct.unpack('<I', m.group(1))[0]
            candidate_offset = pe.get_offset_from_rva(candidate_va - image_base)
            candidate_offsets.append(candidate_offset)
        except:
            print(f"failed for group {m.group(1)}")
            pass
```

```
def xor_decrypt(data, key):
    out = []
    for i in range(len(data)):
        out.append(data[i] ^ key[i % len(key)])
    return bytes(out)


def get_config(data, offset):
    key = data[offset:].split(b'\x00')[0]
    assert 5  < len(key) < 20
    config_data_enc = data[offset + len(key) + 1:]
    return xor_decrypt(config_data_enc, key)


config_data = None

for candidate_offset in candidate_offsets:
    try:
        tmp_config = get_config(file_data, candidate_offset)
        if tmp_config[:4] == b'http':
            config_data = tmp_config
            break
    except:
        pass

assert config_data is not None


# config parse
config_array = []
for a in config_data.split(b'\x00'):
    if not a.isascii():
        break
    config_array.append(a)

c2 = config_array[0].decode('utf-8')
settings = []

for config_entries in config_array[1:]:
    for entry in config_entries.split(b'<>\r\n'):
        if len(entry) == 0:
            continue
        settings.append({'key':entry.split(b'<>_<>')[0].decode('utf-8'),
'value':entry.split(b'<>_<>')[1].decode('utf-8')})

print(c2)
print(settings)
```

```
http://erniku42.top/gate.php;
[{'key': 'CookiesEdge', 'value': 'false'}, {'key': 'HistoryEdge', 'value': 'false'},
{'key': 'HistoryFirefox', 'value': 'false'}, {'key': 'EdgeDB', 'value': 'true'},
{'key': 'Edge', 'value': 'false'}, {'key': 'Files', 'value': 'false'}, {'key':
'Opera', 'value': 'false'}, {'key': 'CookiesOpera', 'value': 'false'}, {'key':
'HistoryOpera', 'value': 'false'}, {'key': 'Screenshot', 'value': 'true'}, {'key':
'Chrome', 'value': 'false'}, {'key': 'Info', 'value': 'true'}, {'key':
'HistoryChrome', 'value': 'false'}, {'key': 'ChromeDB', 'value': 'true'}, {'key':
'Wallet', 'value': 'true'}, {'key': 'ChromeExt', 'value': 'true'}, {'key': 'Firefox',
'value': 'false'}, {'key': 'CookiesChrome', 'value': 'false'}, {'key': 'FirefoxDB',
'value': 'true'}, {'key': 'CookiesFirefox', 'value': 'false'}, {'key': 'Desktop',
'value': 'true'}, {'key': 'EdgeExt', 'value': 'true'}, {'key': 'CookiesFile',
'value': '_AllCookies.txt'}, {'key': 'HistoryFile', 'value': '_AllHistory.txt'},
{'key': 'NTFS', 'value': 'true'}, {'key': 'Key', 'value': 'NkB7vazOVtAR2LZ'}, {'key':
'DesktopFolder', 'value': '_Desktop'}, {'key': 'UAC', 'value': 'false'}, {'key':
'ScreenFile', 'value': '$CREEN.PNG'}, {'key': 'DeleteAfterEnd', 'value': 'true'},
{'key': 'MessageAfterEnd', 'value': 'false'}, {'key': 'FirefoxDBFolder', 'value':
'_Firefox'}, {'key': 'Anti', 'value': 'false'}, {'key': 'EdgeDBFolder', 'value':
'_Edge'}, {'key': 'UserAgent', 'value': ''}, {'key': 'Prefix', 'value': 'mrd-'},
{'key': 'WalletFolder', 'value': '_Wallet'}, {'key': 'PasswordFile', 'value':
'_AllPasswords.txt'}, {'key': 'ChromeDBFolder', 'value': '_Chrome'}, {'key':
'ExternalDownload', 'value': 'http://ovapfa05.top/unfele.dat'}, {'key':
'FilesFolder', 'value': '_Files'}, {'key': 'InfoFile', 'value': '_Information.txt'}]
```

```
def get_config_from_file(file_path):
    file_data = open(file_path, 'rb').read()
    pe = pefile.PE(data = file_data)
    image_base = pe.OPTIONAL_HEADER.ImageBase

    text_data = None

    for s in pe.sections:
        if b'.text' == s.Name[:5]:
            text_data = s.get_data()
            break

    assert text_data is not None


    eggs = [
            rb'\x80\x3D(....)\x09\xB9\x00\x01\x00\x00',
            rb'\xB9\x00\x01\x00\x00\x80\x3D(....)\x09'
           ]

    candidate_offsets = []

    for egg in eggs:
        for m in re.finditer(egg, text_data, re.DOTALL):
            try:
                candidate_va = struct.unpack('<I', m.group(1))[0]
                candidate_offset = pe.get_offset_from_rva(candidate_va - image_base)
                candidate_offsets.append(candidate_offset)
            except:
                print(f"failed for group {m.group(1)}")
                pass

    assert len(candidate_offsets) != 0

    config_data = None

    for candidate_offset in candidate_offsets:
        try:
            tmp_config = get_config(file_data, candidate_offset)
            if tmp_config[:4] == b'http':
                config_data = tmp_config
                break
        except:
            pass

    assert config_data is not None


    # config parse
    config_array = []
    for a in config_data.split(b'\x00'):
        if not a.isascii():
            break
        config_array.append(a)

    c2 = config_array[0].decode('utf-8')
    settings = []

    for config_entries in config_array[1:]:
        for entry in config_entries.split(b'<>\r\n'):
            if len(entry) == 0:
                continue
            settings.append({'key':entry.split(b'<>_<>')[0].decode('utf-8'),
'value':entry.split(b'<>_<>')[1].decode('utf-8')})

    assert len(settings) != 0

    final_config = {'c2':c2, 'settings':settings}
    return final_config

get_config_from_file('/tmp/cryptbot.bin')
```

```
{'c2': 'http://erniku42.top/gate.php;',
 'settings': [{'key': 'CookiesEdge', 'value': 'false'},
  {'key': 'HistoryEdge', 'value': 'false'},
  {'key': 'HistoryFirefox', 'value': 'false'},
  {'key': 'EdgeDB', 'value': 'true'},
  {'key': 'Edge', 'value': 'false'},
  {'key': 'Files', 'value': 'false'},
  {'key': 'Opera', 'value': 'false'},
  {'key': 'CookiesOpera', 'value': 'false'},
  {'key': 'HistoryOpera', 'value': 'false'},
  {'key': 'Screenshot', 'value': 'true'},
  {'key': 'Chrome', 'value': 'false'},
  {'key': 'Info', 'value': 'true'},
  {'key': 'HistoryChrome', 'value': 'false'},
  {'key': 'ChromeDB', 'value': 'true'},
  {'key': 'Wallet', 'value': 'true'},
  {'key': 'ChromeExt', 'value': 'true'},
  {'key': 'Firefox', 'value': 'false'},
  {'key': 'CookiesChrome', 'value': 'false'},
  {'key': 'FirefoxDB', 'value': 'true'},
  {'key': 'CookiesFirefox', 'value': 'false'},
  {'key': 'Desktop', 'value': 'true'},
  {'key': 'EdgeExt', 'value': 'true'},
  {'key': 'CookiesFile', 'value': '_AllCookies.txt'},
  {'key': 'HistoryFile', 'value': '_AllHistory.txt'},
  {'key': 'NTFS', 'value': 'true'},
  {'key': 'Key', 'value': 'NkB7vazOVtAR2LZ'},
  {'key': 'DesktopFolder', 'value': '_Desktop'},
  {'key': 'UAC', 'value': 'false'},
  {'key': 'ScreenFile', 'value': '$CREEN.PNG'},
  {'key': 'DeleteAfterEnd', 'value': 'true'},
  {'key': 'MessageAfterEnd', 'value': 'false'},
  {'key': 'FirefoxDBFolder', 'value': '_Firefox'},
  {'key': 'Anti', 'value': 'false'},
  {'key': 'EdgeDBFolder', 'value': '_Edge'},
  {'key': 'UserAgent', 'value': ''},
  {'key': 'Prefix', 'value': 'mrd-'},
  {'key': 'WalletFolder', 'value': '_Wallet'},
  {'key': 'PasswordFile', 'value': '_AllPasswords.txt'},
  {'key': 'ChromeDBFolder', 'value': '_Chrome'},
  {'key': 'ExternalDownload', 'value': 'http://ovapfa05.top/unfele.dat'},
  {'key': 'FilesFolder', 'value': '_Files'},
  {'key': 'InfoFile', 'value': '_Information.txt'}]}
```

```
from pathlib import Path

for file in Path('/tmp/samples/').glob('*'):
    print(file)
    try:
        config = get_config_from_file(file)
        print(config.get('c2'), 'None')
    except Exception as e:
        print("ERROR")
        print(e)
```

```
/tmp/samples/909ce699e4a2680687b65ca3d4ff8cd24a410c05ceda581741e17aa429b12983
http://ernjxs12.top/gate.php; None
/tmp/samples/c20a40b230e26207a392fc196ecf818cd41c400aff19cd124bcb6a831ea5c1b9
ERROR

/tmp/samples/f8675c4a0fa94fb4d0bf070bc171ddfd732143bf1fba1847c537ef43ea00f6a6
http://ewzpak62.top/gate.php; None
/tmp/samples/de9216d23a71a911d38028743d3d7af93da2e29774601cd96a4bf8ead842058f
http://lahwsg62.top/gate.php; None
/tmp/samples/4aee291fc52bf99bf92331c7c6eeedc87d5c2e7a00291af522a6e2249794cf76
http://lahrom42.top/gate.php; None
/tmp/samples/bcbbba94fb3901541a97a0cf5c95209cf4520eb9d731691ce28e7995459b8eac
http://xjuxjt32.top/gate.php; None
/tmp/samples/c6338e4242cf07ce63beb69365c79b6101cbde5e6101a04d4398b2433ac20786
http://olsodv72.top/gate.php; None
/tmp/samples/004b0ef1531d232cd379ade9a64548618ea5652c9b3c6adf8fd9614a6b64d752
ERROR

/tmp/samples/addc404a3575d31882a52539d77c379c2efd6bd7d3c9adde1cf0480b128cd8ad
ERROR

/tmp/samples/c7348d5113889d4527e6f2deab6620ad36c6fa693aff1f604d12338f6fc57e54
http://ewzsvl72.top/gate.php; None
/tmp/samples/b35d7d4f1396708cb3ab73b44676a59b093e0992c3d41615bdc618239d356389
ERROR

/tmp/samples/50b3f06b47de1c90b02c2866286e980a2e69349388de986f2cba9c208419c1df
ERROR

/tmp/samples/4b62e5a44c931decf395e9d50f4c8a5493fc15c1192292b80ff46b959255c84a
http://xjuoso62.top/gate.php; None
/tmp/samples/a13f4d7f199437414060bb981904506d51d2b9498e9d30d74fc04a993088ebbf
ERROR

/tmp/samples/8ac5b6f4cfed8d1d089cf3c5a2fd634652cdf6193411cad2b25d65914f833066
ERROR

/tmp/samples/00f18e515f076e1b327e90ff4eebe344b1bb4e30ac362700004b5bbc681783f7
ERROR

/tmp/samples/371aa5cf136719c2056ea54cc0e748809e6db74a949f3d861e0d436942e6a6e2
ERROR

/tmp/samples/eeded5f5d006dacd9e2f33ba9fad47332c04b57f621c89731376f51127198345
http://trenio65.top/gate.php; None
/tmp/samples/b42db646291fffc82f030f7bab50c2ecb452a51682fa5c4227f39d4dbc9124e3
http://lahlra52.top/gate.php; None
/tmp/samples/c56043cbaedc47339c3d9e9b9fa96097665051ec4d9e9bfe1db461f52706b1bc
ERROR

/tmp/samples/74fa24b3334856b2828bcfd21d0529a00af8a42fa23447e1080f450852595efd
http://lahmkf22.top/gate.php; None
```

```
/tmp/samples/6cc65eb24b4ca1e5114b54ee233c2f0cbfb94027a15acda7afc6145568a48956
http://trenio65.top/gate.php; None
/tmp/samples/daa64610c5eaed232802858540f4084f70c45fed4ef6c389639f6890999216b7
http://ewzvpq52.top/gate.php; None
/tmp/samples/c515e59148e526a3eb95abf2b80b59ccad556b9a343e1ee377e962739c84d816
http://lahxam72.top/gate.php; None
/tmp/samples/cfc7e9c6a2f034d1c8526bbb8b080b7a60868f5fd1dc99bb50dab34f53a5617d
http://xjupom52.top/gate.php; None
/tmp/samples/d0870aca3b4a3bb20886f8187146badf97a6b58137aa4091d6a163870e9cb24b
http://ewzmix42.top/gate.php; None
/tmp/samples/bfb5bf361c6cf10444d15950a186ab3430369f3c5f5365610b6c1507dcb4d74e
ERROR

/tmp/samples/cff473cf9ddd2cc651e2058928c255cd8e23266ab517478aa20f2ca7d1566c3a
ERROR

/tmp/samples/38263337d1751f59525e383cc17f87d44abc32394e2c82dee460dc88d6a441d0
ERROR

/tmp/samples/66bc0cd0343be9eb0b30e068e906fc16d1e99cdf21a940950988d79bc0573aee
http://xjuupt72.top/gate.php; None
/tmp/samples/28e09347b5ccc3eaf3ce9670b7061210f7dd63e4627fad7a805878e774a48e78
ERROR
list index out of range
/tmp/samples/22075a63aef35075b6a7bf3eb1f3ba9ccccfec7fc90f7925c1f02f7747a938ce
http://yawvtr72.top/gate.php; None
/tmp/samples/a04e8c97dac994a7b5954362f0670cc647026b9ecb5f60f8d1b7c5984556e197
ERROR

/tmp/samples/cd0b222baefe6b0246907ff4c082f4653c93c3c0c220c8c78a5ba316d760be1e
http://ewzjvx32.top/gate.php; None
/tmp/samples/82c38736da805cc142e27926680d06d31ec733d2f3930b4fa0f857ac98774c10
ERROR

/tmp/samples/ce3f93e47845e2b665a5505c29de94f5f5029ff6b108bb8c09a1f138e1d6597e
ERROR

/tmp/samples/fefa4e0170a001f1875cc357c745c00cf1557f126abdb81fa739fc12d279ca7f
http://lahsfr12.top/gate.php; None
/tmp/samples/65c277ca5ba40e11db36dc51fdfd036ef9778c55edea6a8e98c9b6ba04a2b1b6
ERROR

/tmp/samples/277ef9b811aca7a6e7dd1574b68d280d576cab8770cfe1c495a051a9739e2358
ERROR

/tmp/samples/ace4d349300a37250a1d76a00a8b241d82a6c8cca5676011bb4bdbb295f5f9f3
ERROR

/tmp/samples/cdf256f6a714e539a54952df7524f277d079606bbfb6c108b34fc17d268c0b15
ERROR

/tmp/samples/828515a42c0e7db8faf64f062f83f753a6fccbb7052e0e3238ca5d5e928f7215
```

```
ERROR

/tmp/samples/39a9db0ecee2824dbb62ed1a06f675fd0fffe7cfb8074581d9c1ea1a3cf20cd7
http://ernlen22.top/gate.php; None
/tmp/samples/eb96e80c723c8b351930589c9413d265bf3416f75649676de6d94bc431f07693
ERROR

/tmp/samples/30fa111f7f2b020edbe5d1ee5a7e62494c4ac3161a99e6bbfb07f477f5acfa64
ERROR

/tmp/samples/1624b18bb44aa9f1f7d2e9aa48e74c693455fc1eccc1d0b1469f27d4d6c006bd
ERROR

/tmp/samples/d4cbaa220dd19b9e4f25f0415837d9547ac975e7526fa434eaa6e0db1a8a333e
http://quwtdc72.top/gate.php; None
/tmp/samples/e7639c2a22b8c467be67f5d847c1a18c77451e87b287ccf16acd19e3f18fec71
http://xjustw22.top/gate.php; None
/tmp/samples/71abbc801d92086b20929e988a66cd2fb78abf8bb73f670dd7973102f64bd991
ERROR

/tmp/samples/2311089547a7ffa27cd0c8129dba3e0eb2086feae4d8113da55d5bf3e34baf21
ERROR

/tmp/samples/775cfdbd07e34efd365efd84defdca572b6f611183003f4223ec67ece4fa9a16
ERROR

/tmp/samples/41bc80901eabb49a2e9b1d384d213ff7418a8c1efc2366af6a264eebcd7f423f
ERROR

/tmp/samples/e7a72071085ca3be73c47f5b7b582874ac09cf3a66216823440d98dba0a44221
ERROR
list index out of range
/tmp/samples/bc56fd3f2052ee668b0a850b33b2017de51a21b3d3c4ff0904a2da5caf1d400d
ERROR

/tmp/samples/0e99abfb5d04c8d2896a5c1b585a7ae728508a775adcea2a441d50406882b7ed
ERROR

/tmp/samples/00f9cbe4b91fe5d2ae34aa1b29d3baa5ddf9bb84fb28d65270665ca454b4fa2c
http://xjulqa12.top/gate.php; None
/tmp/samples/130aeda14ea655ef6186420c8655bd2f92a875d0ea3089a40f3bc550deef84b5
http://xjupom52.top/gate.php; None
/tmp/samples/9ccd1ac9a965d09a74e753c262e02fb3f413cd8f103e3aad0978634bb005e785
http://lahdlk32.top/gate.php; None
/tmp/samples/3ac544d58365a618c777ff55f57403fde19fc3ff13ba1859a4c410a657ac4164
ERROR

/tmp/samples/e501d6ff65fdadc0e05a842652290f4d66cd4e2791f047816e86a2c57262880e
ERROR

/tmp/samples/62e1d6730f4b657f592f88ff74d6b3656d7d3f05fb6c1f06a2061cf5c3080200
ERROR
```

```
/tmp/samples/2805c1a81174e671123118e1d204b41f09c182f14d7ad01c7283fb7addea9b91
http://ernblt32.top/gate.php; None
/tmp/samples/134ee19e860f2c229787a6e2b954c79bde7831e4865f27c00ca9c84fcb0e2c1f
http://trenio65.top/gate.php; None
/tmp/samples/7176c6e5e8bad8e91d2ce9fb694bb261daa371b39e2af274bb0e8d15f996043b
ERROR

/tmp/samples/ecaf51ccb3476a0077ba18eac41d9efc9939c00e10eebf6155ff8695594a7052
ERROR

/tmp/samples/66995600f5b4291a2bbab619926e7df878b7955b3b5f8c957701feee59855a60
ERROR
list index out of range
```