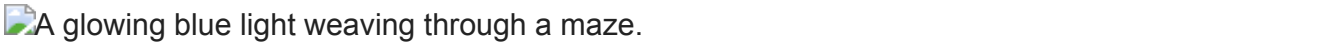
Technical Analysis

zscaler.com/blogs/security-research/technical-analysis-xloader-versions-6-and-7-part-2



This is Part 2 of our two-part technical analysis on Xloader versions 6 and 7. For details on how Xloader conceals its critical code and data, go to Part 1.

Introduction

In Part 2 of this blog series, we examine how Xloader obfuscates the command-and-control (C2) code and data to complicate analysis. We will also delve into the network communication protocol for the latest versions of Xloader with multi-layer encryption and fake servers to evade detection.

Key Takeways

- Xloader versions 6 and 7 use advanced obfuscation techniques to mask critical parts of code and data.
- The malware continues to utilize hardcoded decoy lists to blend real C2 network communications in with traffic to legitimate websites.
- The decoy lists and the real C2 server are encrypted using different keys and algorithms.
- Xloader versions 6 and 7 use the same network protocol and are protected by multiple layers of encryption.

C2 decryption

Decoy C2 servers

Xloader shares many characteristics as Formbook, its predecessor, including the use of a *decoy C2 list* and a *real C2 server*, which are encrypted differently and stored separately within the binary. The purpose of the decoys is to generate network traffic to legitimate domains to disguise real C2 traffic. This approach has been used by other malware families in the past such as Pushdo. Note that the so-called decoy list can also include actual C2 servers, but for simplicity, we'll continue to refer to these as the "decoy list" and "real" C2 server in this blog, since the former still primarily contains legitimate domains.

The figure below shows a high-level description of the process that Xloader uses to decrypt the decoy C2s.

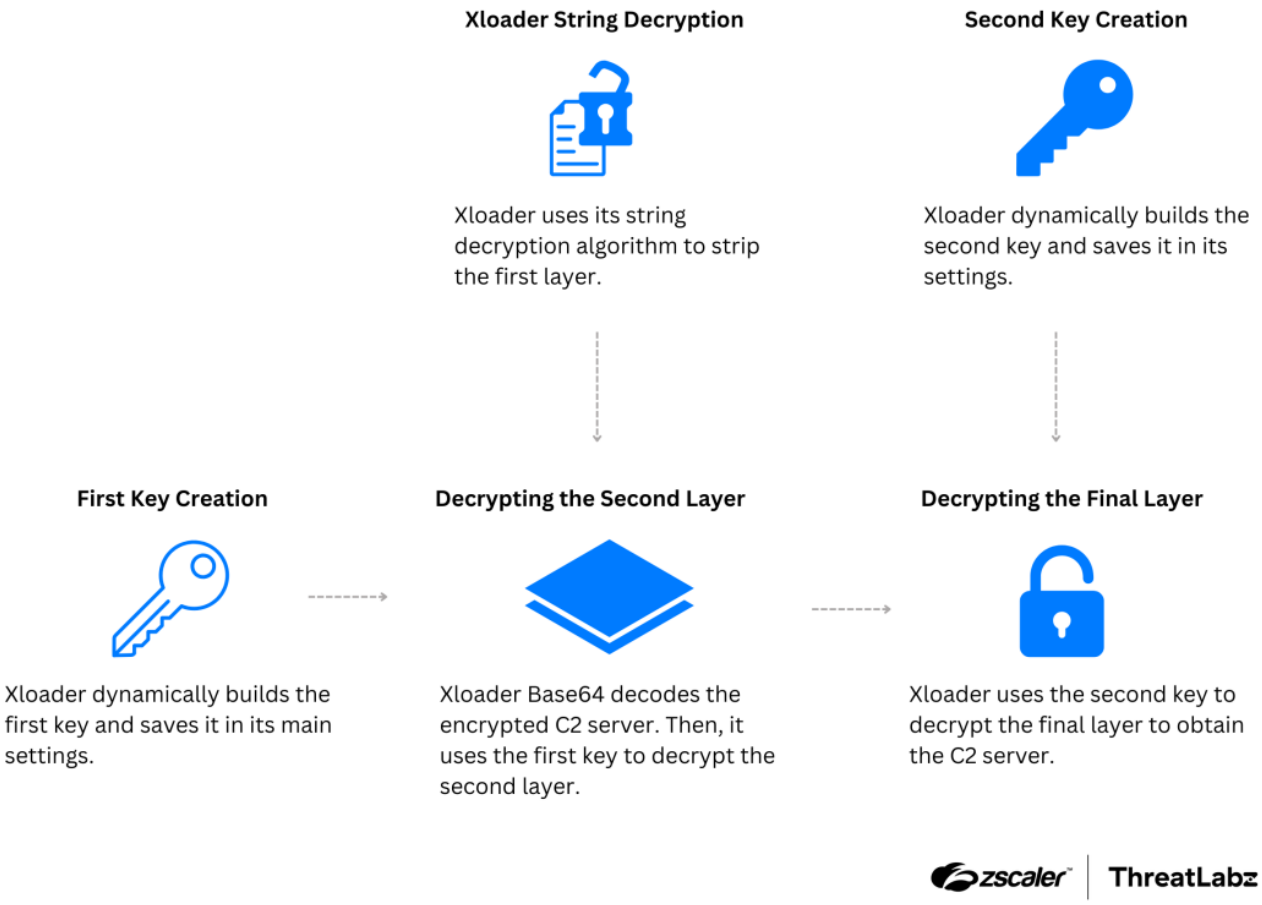


Figure 1: The functions that decrypt the decoy C2 servers in Xloader 6.2.

The Xloader decoy C2s are encrypted with three layers. The keys needed for decryption are generated by various functions within the malware code and are stored in global configuration structures as described below.

The first decryption key for the decoy C2 is constructed dynamically by one of the encrypted `NOPUSHEBP` functions. Five DWORDs are combined to construct an initial 20-byte seed. This seed is then XOR'ed with a hardcoded DWORD XOR key and an additional hardcoded 1-byte XOR key. The resulting 20-byte key is stored in the global configuration structure.

Similarly, the second key of the decoy C2 is generated by another encrypted `NOPUSHEBP` function. Once again, 5 DWORDs are initialized on the stack and XOR'ed with a DWORD XOR key retrieved from the global configuration structure. This DWORD XOR key was previously calculated and stored in the global configuration structure by another function.

The list of decoy C2s is stored among the encrypted strings with indexes that typically range from 1 to 63 (inclusive). Another function implements the process to retrieve and decrypt a specific decoy C2 server based on its index using Xloader's standard string encryption algorithm that we described in Part 1 of this blog series. The result of removing this first layer is the encrypted second layer, which is a Base64 encoded string.

The second layer is Base64 decoded and decrypted with Xloader's RC4 and subtraction algorithm using the first key XOR'ed with the index of the decoy C2. The third and final layer uses Xloader's RC4 and subtraction algorithm using the second key.

Below is a Python implementation of Xloader's decoy C2 decryption algorithm:

```
# Get the necessary seeds and xor keys from the binary
rc4_key_1_seed = get_rc4_key_1_seed()
rc4_key_1_xor = get_rc4_key_1_xor()
rc4_key_2_seed = get_rc4_key_2_seed()
rc4_key_2_xor = get_rc4_key_2_xor()

# Calculate final keys
decoy_C2s_key_1 = xor(rc4_key_1_seed, rc4_key_1_xor)
decoy_C2s_key_2 = xor(rc4_key_2_seed, rc4_key_2_xor)

# Decrypt the decoy C2
enc_C2 = decrypt_encrypted_string_by_index(target_C2_index)
b64dec = base64.b64decode(enc_C2)
key1 = xor(decoy_C2s_key_1, target_C2_index)
dec = rc4_sub(b64dec, key1)
decrypted_c2 = rc4_sub(dec, decoy_C2s_key_2)
```

Legitimate C2 servers

Following the C2 decoy list, is another encrypted string located at index `64`. This encrypted string contains the real Xloader C2, which is decrypted using a similar algorithm but with different keys. First, the encrypted string at index `64` is retrieved and decrypted. After decryption, the result is Base64 decoded, and a new key is dynamically built as follows:

1. A 20-byte seed is constructed.
2. This seed is XOR'ed with a hardcoded 1-byte XOR key.
3. The seed is then XOR'ed with a hardcoded DWORD XOR key.
4. Finally, the seed is XOR'ed with another hardcoded 1-byte XOR key.

The resulting 20-byte key is then used to decrypt the first encryption layer of the real C2 using RC4 and subtraction.

The next encryption layer of the real C2 is decrypted using another function:

1. A 20-byte seed is constructed.
2. This seed is then XOR'ed with a hardcoded 1-byte XOR key.
3. The resulting key is used to decrypt the final RC4 and subtraction layer of the real C2.

Below is a Python implementation for decrypting Xloader's real C2:

```
# Get the necessary seeds and xor keys from the binary
rc4_key_1_seed = get_rc4_key_1_seed()
rc4_key_1_xor1byte = get_rc4_key_1_xor1byte()
rc4_key_1_xor4bytes = get_rc4_key_1_xor4bytes()
rc4_key_2_seed = get_rc4_key_2_seed()
rc4_key_2_xor = get_rc4_key_2_xor()

# Calculate the final keys
real_C2_key = xor(rc4_key_1_seed, rc4_key_1_xor1byte)
real_C2_key = xor(real_C2_key, rc4_key_1_xor4bytes)
real_C2_key_2 = xor(rc4_key_2_seed, rc4_key_2_xor)

# Decrypt the real C2
string_64 = decrypt_encrypted_string_by_index(64)
b64dec = base64.b64decode(string_64)
dec = rc4_sub(b64dec, real_C2_key)
dec = rc4_sub(dec, real_C2_key_2)
if dec.startswith(b'www'):
   return dec.decode()
```

Note that all of the real C2 servers observed by ThreatLabz (after decryption) start with a *www* subdomain. In contrast, the decoy C2 servers embedded in the malware do not start with a *www* subdomain, but that prefix is added by Xloader prior to establishing network communications.

C2 URL path

In Xloader versions 6 and earlier, the real C2 string included a domain and a path. However, each decoy C2 string only consisted of a domain. Therefore, Xloader appended the real C2's path to each decoy domain prior to generating network traffic.

In Xloader version 7.5, each decoy C2 and real C2 has its own URL path, and the decryption function now includes an additional argument to return either the domain or the path of the decrypted C2 server. This process uses a 20-byte key combined with the C2's index to decrypt each 4 character C2 path via Xloader's RC4 and subtraction algorithm.

Network protocol

We previously described Xloader's network protocol and a new encryption layer that was added to the malware's registration packet. In Xloader 4.3, we discovered that there was a bug that caused the registration packet to be truncated because of the improper placement of a NULL character. However, this issue has since been resolved in version 6, with the packet now formatted correctly.

Conclusion

Xloader continues to pose a significant threat to organizations with its powerful information stealing and second-stage downloader capabilities, combined with numerous techniques to evade host and network-based detection. The malware author continuously updates and refines the code to complicate automated and manual analysis. Versions 6 and 7 of Xloader add new multi-layer encryption algorithms and dynamic key generation to hinder static signatures and make reverse engineering efforts more tedious.

Zscaler Coverage

Zscaler's multilayered cloud security platform detects Xloader and Formbook, as well as various other types of cyberthreats, at multiple levels, as shown below:

- Win32.PWS.Xloader
- Win32.PWS.Formbook

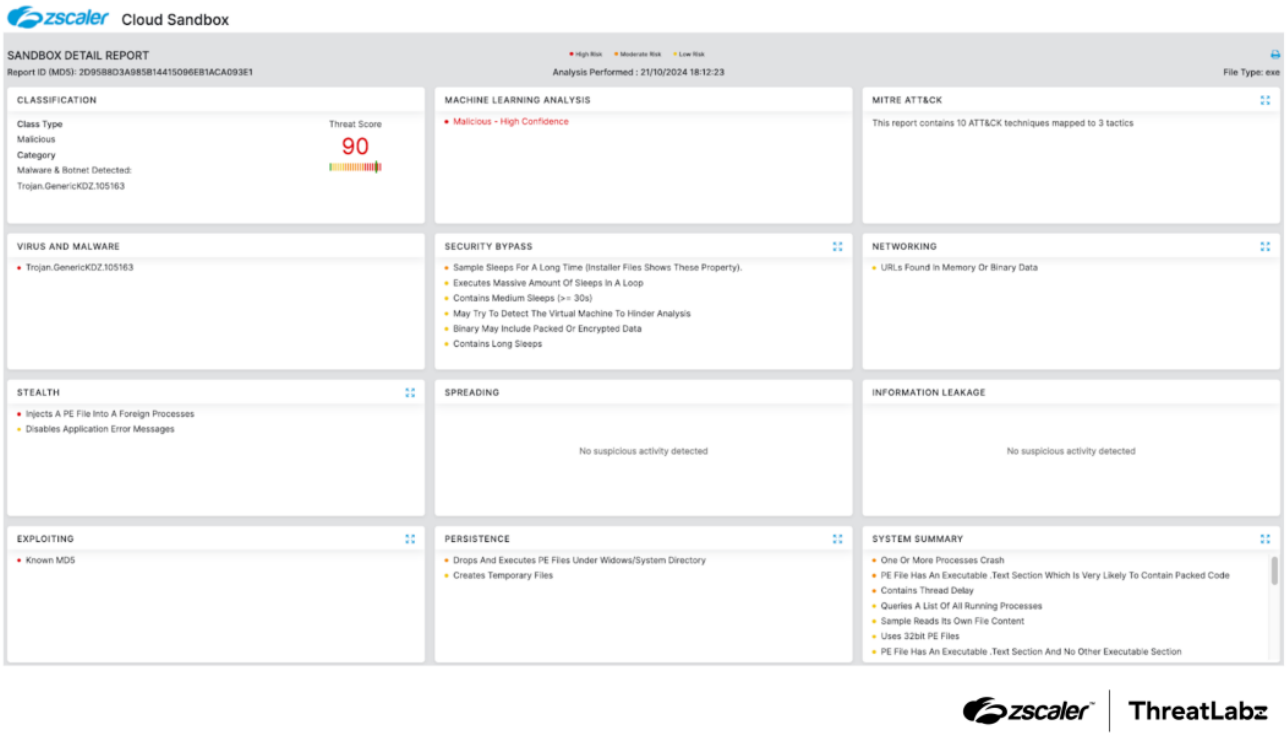


Figure 2: Zscaler Cloud Sandbox report for Xloader.

Indicators Of Compromise (IOCs)

Sample	Variant	Version
66ebf028ab0f226b6e4c6b17cec00102b1255a4e59b6ae7b32b062a903135cc9	Xloader	6.2

Sample	Variant	Version
88909cd27a422da91a651e87f493d16beff1f0e03adcc035f2835a2a25e871e7	Xloader	6.2
4ad101eef336dc2467ffaf584b272aa82f26711bfba4e2e29e8ad7c6d62bc6ae	Xloader	7.5
362207c53645346df6f36cf3f7792e5fc4655895b35a6e3477e218e0e0007be9	Xloader	7.5
b1fb20d5857d1ca65dbacd6cb100dc2d7da8eb7ce54d4faeebafb2bbb212beca	Xloader	7.5

Network indicators

C2	C2 Type
www.iwin[.]exposed/ir6g/	Real C2
www.everycreation[.]shop/nsev/	Real C2
• www.ok2yu[.]us/ir6g/ • www.zwetststuren[.]cfd/ir6g/ • www.fraternize[.]org/ir6g/ • www.mc9uh8d70[.]site/ir6g/ • www.scwspark[.]com/ir6g/ • www.royalkredit[.]online/ir6g/ • www.bkexclusivecars[.]net/ir6g/ • www.moncoop[.]coop/ir6g/ • www.tehranrizcomputer[.]com/ir6g/ • www.sazekents[.]cfd/ir6g/ • www.xediedie[.]icu/ir6g/ • www.eeja[.]uk/ir6g/ • www.mscfoundation[.]info/ir6g/ • www.brighterhomesdecor[.]com/ir6g/ • www.efidence[.]com/ir6g/ • www.tk254kr6rwr7mjtru[.]com/ir6g/ • www.haycoches[.]com/ir6g/ • www.electra-airways[.]info/ir6g/ • www.happiluv[.]com/ir6g/ • www.goog1evip15[.]com/ir6g/ • www.womenscalshion[.]com/ir6g/ • www.lenaguillemette[.]com/ir6g/ • www.jamesgadzikmd[.]com/ir6g/ • www.kavanzi[.]com/ir6g/ • www.tupinkeept[.]cfd/ir6g/ • www.portfutures[.]asia/ir6g/	Decoy C2

C2	C2 Type

- www.cgm-logistics[.]org/ir6g/
- www.dutch-wildlife[.]shop/ir6g/
- www.dsisarl[.]com/ir6g/
- www.haftplicht[.]com/ir6g/
- www.roundhaygardenscene[.]com/ir6g/
- www.alace5[.]com/ir6g/
- www.sathyfe[.]com/ir6g/
- www.electronicraw[.]com/ir6g/
- www.earn50k[.]com/ir6g/
- www.arasymimbi[.]com/ir6g/
- www.lriz[.]site/ir6g/
- www.pinnaclebyte[.]info/ir6g/
- www.avolci[.]com/ir6g/
- www.am8pw[.]us/ir6g/
- www.projectimprov[.]com/ir6g/
- www.energeticfranchise[.]top/ir6g/
- www.devocionmusic[.]com/ir6g/
- www.markthing[.]site/ir6g/
- www.myhosting[.]co[.]in/ir6g/
- www.solar-windturbine[.]life/ir6g/
- www.flusznwrldwide[.]com/ir6g/
- www.lifedrawingbristol[.]co[.]uk/ir6g/
- www.weberze[.]com/ir6g/
- www.getmylinks[.]cc/ir6g/
- www.aspasskeoffice[.]homes/ir6g/
- www.uxzl[.]site/ir6g/
- www.carpmaxxbait[.]online/ir6g/
- www.dumpstedoctorca[.]com/ir6g/
- www.revelationfithub[.]com/ir6g/
- www.cuffbow[.]com/ir6g/
- www.hk9[.]xyz/ir6g/
- www.lollybowly[.]com/ir6g/
- www.aarunifoodcrafters[.]com/ir6g/
- www.jarvisandbrown[.]com/ir6g/
- www.gattosat[.]icu/ir6g/
- www.xfgqbh[.]site/ir6g/
- www.mag-flex[.]com/ir6g/
- www.trisixnine[.]net/0057/
- www.softillery[.]info/cyhg/
- www.easestore[.]shop/qflp/
- www.yu35n[.]top/kejj/
- www.yourhomecopilot[.]online/gctn/
- www.fastr[.]live/gsjn/
- www.dto20[.]shop/efvy/
- www.aromavida[.]net/4rlw/
- www.crochetpets[.]online/vand/
- www.queima[.]shop/mdoj/
- www.nojamaica[.]net/g7eq/
- www.komart[.]shop/b2t1/
- www.livemarkat[.]live/8h0p/
- www.d27dm[.]top/ptbb/
- www.rtpgaruda888resmi[.]xyz/u8o7/

C2	C2 Type
www.chalet-tofane[.]net/3bhs/	
www.platinumkitchens[.]info/dquo/	
www.eslameldaramlly[.]site/nlx0/	
www.theproselytizer[.]net/od1n/	
www.amitayush[.]digital/93j5/	
www.030002304[.]xyz/d7z8/	
www.aaavvejibej[.]bond/lh0g/	
www.useanecdotenow[.]tech/vera/	
www.bayarcepat19[.]click/q1x3/	
www.bluegirls[.]blog/g1ze/	
www.wdeb18[.]top/kv48/	
www.weatherbook[.]live/tfj4/	
www.pachuco[.]supply/7gdu/	
www.childlesscatlady[.]today/2kmz/	
www.kabaribukota[.]press/nr90/	
www.federall[.]store/afqz/	
www.inf30027group23[.]xyz/xzfm/	
www.allthingsjasmin[.]com/pbmf/	
www.ntn[.]solar/fcmy/	
www.torex33[.]online/pvct/	
www.resumeyourway[.]info/vn92/	
www.kx507981[.]shop/q3r9/	
www.ohio-adr[.]net/j0y4/	
www.serverplay[.]live/6b8s/	
www.meg21c[.]top/3jg0/	
www.rockbull[.]pro/0tt2/	
www.trapkitten[.]website/y6hh/	
www.44ddw[.]top/3e3b/	
www.ngmr[.]xyz/4muf/	
www.sansensors[.]info/ip84/	
www.allsolar[.]xyz/cph9/	
www.bismarckrecovery[.]com/kp5k/	
www.vegastinyhomes[.]net/f2tm/	
www.airbatchnow[.]online/ekgk/	
www.huemanstudio[.]today/0ob6/	
www.rtpngk[.]xyz/yd3l/	
www.mechecker[.]life/b6h1/	
www.lojashelp[.]video/ao78/	
www.tracy[.]club/rwcg/	
www.limitlesssky[.]org/50p5/	
www.luismoreno[.]monster/06xo/	
www.dhkatp[.]vip/4qrw/	
www.hentaistgma[.]net/j6o1/	
www.promasterev[.]shop/zjp0/	
www.pethut[.]shop/wrhe/	
www.polarmuseum[.]info/m8hf/	
www.greekhause[.]org/tn42/	
www.wdcb30[.]top/s7v2/	

Thank you for reading

Was this post useful?

Yes, very!Not really

Disclaimer: This blog post has been created by Zscaler for informational purposes only and is provided "as is" without any guarantees of accuracy, completeness or reliability. Zscaler assumes no responsibility for any errors or omissions or for any actions taken based on the information provided. Any third-party websites or resources linked in this blog post are provided for convenience only, and Zscaler is not responsible for their content or practices. All content is subject to change without notice. By accessing this blog, you agree to these terms and acknowledge your sole responsibility to verify and use the information as appropriate for your needs.

Explore more Zscaler blogs

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our privacy policy.