XLoader Botnet: Find Me If You Can

research.checkpoint.com/2022/xloader-botnet-find-me-if-you-can/

May 31, 2022

May 31, 2022
Research by: Alexey Bukhteyev & Raman Ladutska

Introduction

In July 2021, CPR released a series of three publications covering different aspects of how the **Formbook** and **XLoader** malware families function. We described how XLoader emerged in the Darknet community to fill the empty niche after Formbook sales were abruptly stopped by its author. We did a deep technical analysis followed by a description of XLoader for macOS along with common points and differences in how both malware families conceal the heart of the whole operation, the Command-and-Control (C&C) infrastructure. However, the world does not stand still, and this applies to the malware cyber-world as well.

A couple of months after our publications were released, we spotted a new XLoader version in-the-wild which was an upgrade of all the ones we described previously. The enhanced version features significant modifications in key parts of the malware logic to truly deserve the differentiation if compared with XLoader's previous implementation.

In this article, we describe the changes malware authors applied to XLoader to obscure the C&C infrastructure – more than anything we saw before. Now it is significantly harder to separate the wheat from the chaff and discover the real C&C servers among thousands of legitimate domains used by Xloader as a smokescreen. We explain how we got to the essence and identified the real C&C nodes in the evolving botnet.

Deep technical dive

The Formbook malware has not been updated for quite a long time. The latest version of this stealer is 4.1, and we already observed samples of this version in far 2020. This gives us reason to believe that Formbook has been discontinued.

At the same time, XLoader, Formbook's successor which we described last year, has already received 2 updates since our publication. In this article, we describe the most important changes that we found in XLoader version 2.5.

Camouflaging real C&C servers – methods used in 2021

All XLoader samples have 64 domains and one URI in their configurations. The XLoader configuration has the same structure as the Formbook configuration. In earlier versions Formbook used the URI stored separately in the configuration to access its C&C server. The 64 domains from the malware configuration are actually decoys, intended to distract the researchers' attention.

In Formbook version 4.1, the malware developers added another level of stealth which also migrated to early versions of XLoader (up to 2.5). A domain name for the real C&C server was hidden among the 64 decoys, while the URI that was always thought to be an address of the C&C server became another decoy and could point to a legitimate website. The malware of versions mentioned above randomly choose 16 decoy domains, two of which are replaced with the fake C&C server address and a real C&C server address. The real C&C server is accessed after a long delay.

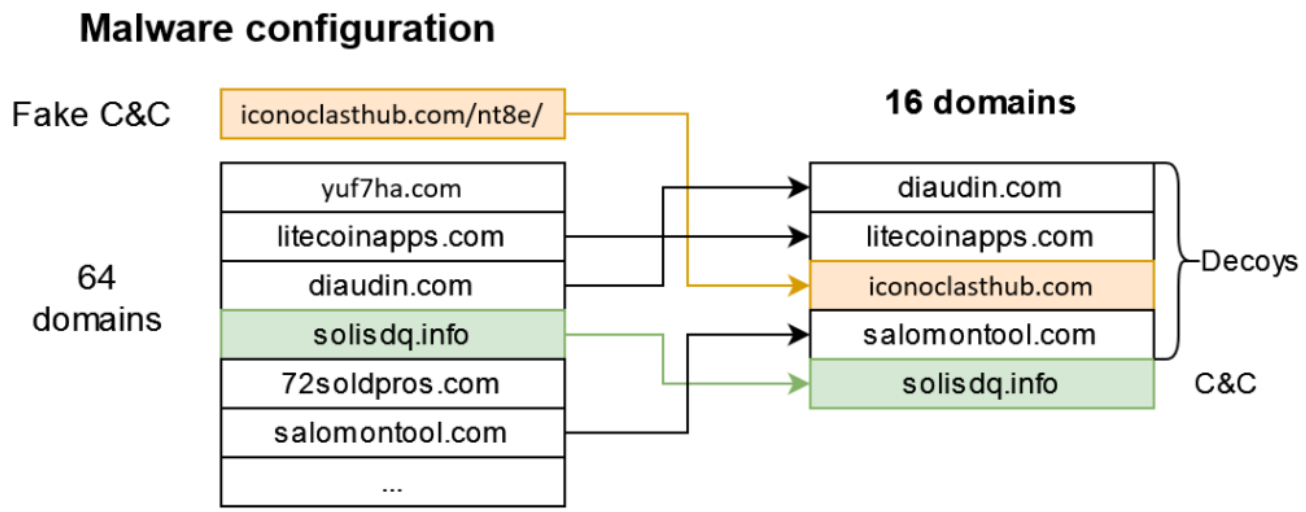

Figure 1 – Creating a list of domains for C&C communication in XLoader 2.3 and Formbook 4.1.

This already looks complicated. However, the newer version introduced an even more sophisticated algorithm.

New version – a new level of protection

The first samples of the new version of XLoader appeared in-the-wild a month after our publications in August 2021, Revealing the XLoader's C&C infrastructure. At first glance, we didn't see any difference because the configuration structure remained exactly the same.

However, when emulating samples in a sandbox, we noticed a change. With a long emulation time, the sample accessed more than 16 domains, unlike earlier versions. This behavior forced us to put aside automated analysis tools and arm ourselves with a disassembler. We soon discovered the part of the code responsible for the detected anomaly. As in the previous versions, XLoader first creates a list of 16 domains that are randomly selected from the 64 domains stored in the configuration. After each attempt to access the selected 16 domains, the following code is executed:

```
do
{
  rand_doman_index = ab_genrand_between(83, 146);// indexes of the 64 domains
                                                 // in the list of encrypted strings
  n = 0;
  while ( rand_doman_index != domain_idxs[n] )// check if the generated index is
  {                                           // not present in the list yet
    if ( ++n > k )
    {
      if ( rand_doman_index )
        domain_idxs[k++] = rand_doman_index;  // store the random domain index
      break;
    }
  }
}
while ( k < 8 );                              // choose 8 domains
```

Figure 2 – XLoader 2.5 overwrites the first 8 domains before each communication cycle.

The purpose of this piece of code is to partially overwrite the list of accessed domains with new random values. Therefore, if XLoader runs long enough, it will access new randomly selected domains. It's important to pay attention to the fact that only the first 8 values are overwritten, and the remaining 8 remain the same as those that were selected immediately after launch.

In addition, XLoader, as we thought, saves the index of its C&C server and does not allow it to be overwritten:

```
for ( i = 0; i < 7232; i += 904 )
{
  if ( xl->saved_c2_index != c )              // overwrite the domain in the list
  {                                           // only if its index is not equal to the
                                              // real_c2_idx
    rl_memset_wrap(&target_string, 46);
    str_buf = 0;
    ab_memset(v20, 0, 518);
    rl_memset_wrap(&xl->c2_structs->domain[i], 904);//
                                              // domain name decryption follows ...
```

Figure 3 – XLoader doesn't overwrite the C&C domain index.

However, while checking hosts that were supposed to be XLoader C&C servers, it turned out that many of them did not respond or else looked to be legitimate, such as this one:

Figure 4 – Fake C&C domain points to a likely legitimate site.

Also, most of them appear only once in various configurations, making them the underdogs in our preliminary bet for the real C&C candidates. From our previous research, we remembered that the number of real C&C servers was relatively small (we found less than 100 C&C servers among 90,000 domains used by the malware), and they were reused in many of the campaigns of different XLoader customers.

In this case, we also found many domains that appear multiple times in samples that belong to different campaigns. However, these domains belong to the list of decoys and do not stand out at first glance. Let's look at the websites pointed to by some of these domains. The root page looks like a parked domain page of famous domain registrars and hosting service providers (usually Hostinger and Namecheap):

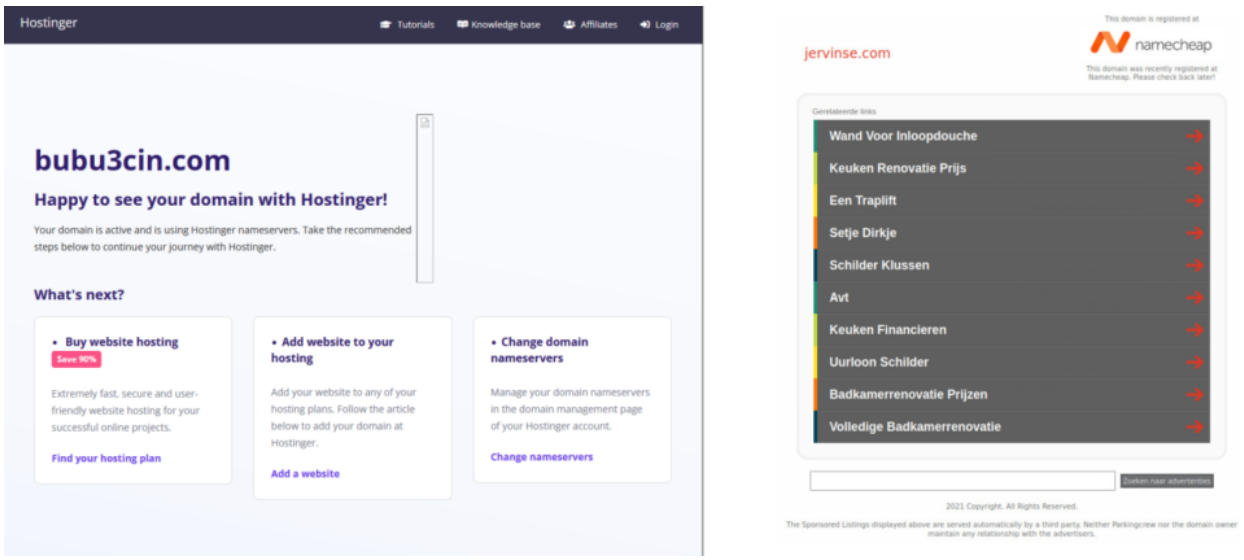

Figure 5 – Real C&C servers disguised as Hostinger and Namecheap parked domain pages.

However, if we check the source code of the page and compare it with the original page generated by the service provider, we see many differences:

Figure 6 – Differences in the fake (on the left side) and the real (on the right side) Namecheap parked domain page.

In the fake Hostinger page, we also see some visual differences:

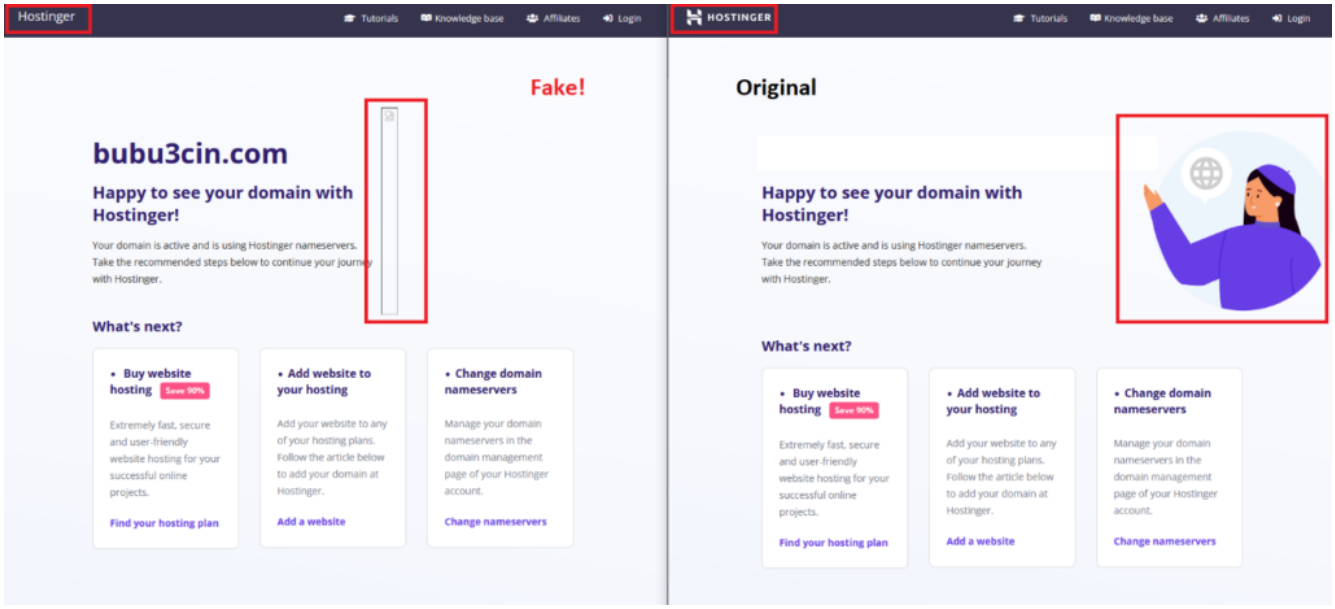

Figure 7 – Visual differences in the fake (on the left side) and the real (on the right side) Hostinger parked domain page.

We then collected IP addresses of all presumably malicious hosts and root pages from the corresponding websites. It appeared that all the domains point to a few IP address ranges, all of which belong to Namecheap. Some domains point to the same IP addresses.

Domain	IP	Root Page MD5 hash	Description
bubu3cin.com	162.0.214.189	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
highpacts.com	162.0.216.5	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
hype-clicks.com	162.0.223.146	f891f22cd94c80844fcfe6fddb4b7912	Fake Namecheap
moukse.com	162.0.223.146	f891f22cd94c80844fcfe6fddb4b7912	Fake Namecheap

besasin09.com	162.0.223.94	8d85df16ced80502c796649e4c806d31	Future home of…
brasbux.com	162.0.223.94	8d85df16ced80502c796649e4c806d31	Future home of…
finsits.com	162.0.225.82	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
arabatas.com	162.0.225.82	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
ocvcoins.com	162.0.238.238	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
gingure.com	162.0.238.238	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
coalmanses.com	162.213.253.206	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
fendoremi.com	162.213.253.206	ce866938b246a89fd98fc6a6f666d21c	Fake Hostinger
noun-bug.com	199.188.206.146	f891f22cd94c80844fcfe6fddb4b7912	Fake Namecheap
cobere9.com	199.188.206.146	f891f22cd94c80844fcfe6fddb4b7912	Fake Namecheap

…

Table 1 – XLoader domains and IP addresses to which they point.

All the websites display pages that appear to be “under construction”, primarily the fake Namecheap or Hostinger parked domain page, even though all the IP addresses belong to Namecheap.

It looks like we found the C&C servers, but is it possible to distinguish them in the list of 64 decoy domains in the malware configuration?

Let’s now look at the function that fills the initial list of 16 domains in XLoader 2.5 and compare it with the function from XLoader 2.3:

XLoader 2.3

```
xl->real_c2_idx = ab_getrandom_between(0, 15);
//…
for ( real_c2_idx = ab_getrandom_between(0, 15);
      real_c2_idx == _xl->real_c2_idx;
      real_c2_idx = ab_getrandom_between(0, 15) )
{
  ;
}
LABEL_24:
domain_idx_list[real_c2_idx] = 121;
counter = 0;
for ( i = 0; ; counter = i )
{
    //…
    index = domain_idx_list[counter];
    offset = ab_strlen(decrypted_domain);
    ab_get_enc_string(_xl, &decrypted_domain[offset], index);
    is_fake_c2_idx = counter == _xl->real_c2_idx;
    c2_domain = _xl->main_uri;                  // replace domain name with
                                                // the fake c2
    if ( !is_fake_c2_idx )
      c2_domain = decrypted_domain;             // store original domain
    //…
}
_xl->real_c2_idx = real_c2_idx;
```

XLoader 2.5

```
xl->saved_c2_index = ab_genrand_between(0, 15);
//…
for ( saved_c2_index = ab_genrandom_between(0, 15);
      saved_c2_index == _xl->saved_c2_index;
      saved_c2_index = ab_genrandom_between(0, 15) )
{
  ;
}
LABEL_24:
domain_idx_list[saved_c2_index] = 108;        // epplus.xyz
counter = 0;
domain_idx_list[ab_genrandom_between(0, 15)] = 127;// cures8t.com
for ( i = 0; ; counter = i )
{
    //…
    index = domain_idx_list[counter];
    offset = ab_strlen(decrypted_domain);
    ab_get_enc_string(_xl, &decrypted_domain[offset], index);
    is_fake_c2_idx = cnt == _xl->saved_c2_index;
    c2_domain = _xl->main_uri;                  // replace domain name with
                                                // the fake c2 from the main URI
    if ( !is_fake_c2_idx )                      //     www.gunhanforklift.com/p9iu/
      c2_domain = decrypted_domain;             // store original domain
    //…
}
_xl->saved_c2_index = saved_c2_index;         // overwrite c2 index
```

Figure 8 – XLoader 2.5 replaces three domains in the created list with 2 decoys and the real C&C server domain.

As we can see, XLoader 2.5 introduced an additional code that replaces one more domain in the list with a fixed value. Interestingly, this value doesn’t appear anywhere else in the code and is not saved; its position in the list of 16 domains is chosen randomly.

As the first 8 domains are overwritten with new values after the first hit, there is a 50% chance that this domain will be overwritten. However, we think that this is the domain which points to the real C&C server.

The domain selection scheme is as follows:

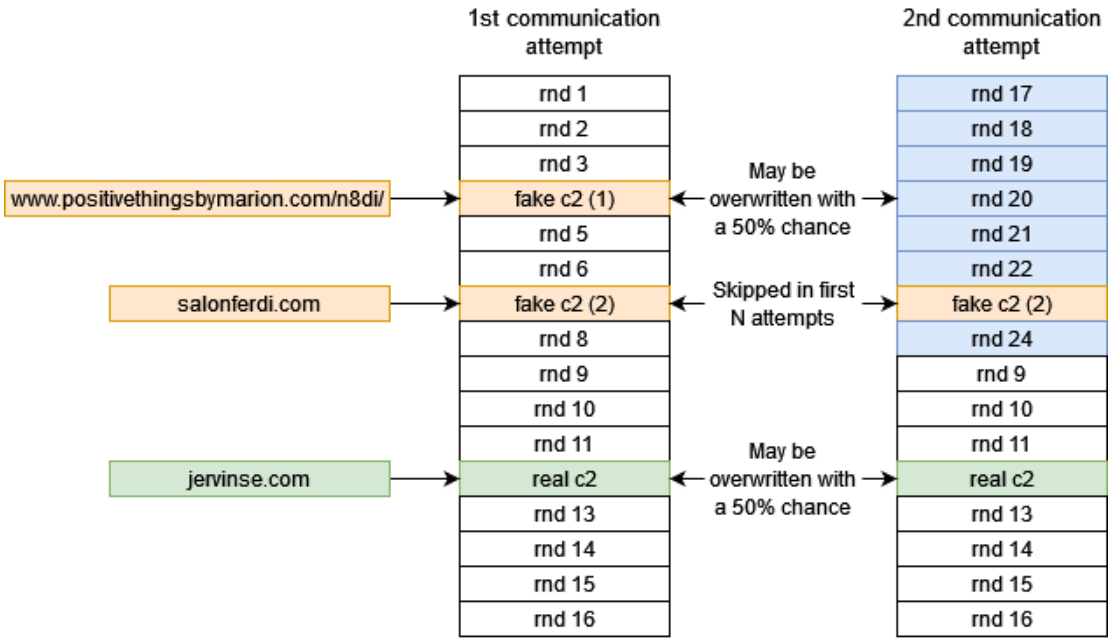

Figure 9 – Creating a list of domains for C&C communication in XLoader 2.5.

If the real C&C domain appears in the second part of the list, it is accessed in every cycle once in approximately 80-90 seconds. If it appears in the first part of the list, it will be overwritten by another random domain name.

However, there is still a probability that this domain will appear in the list again. This is possible because the 8 domains that overwrite the first part of the list are chosen randomly, and the real C&C domain might be one of them. In this case, the probability that a real C&C server will be accessed in the next cycle is **7/64** or **1/8** depending on the position of the "**fake c2 (2)**" domain (see Figure 9 above).

The malware authors once again proved their high technical skills and out-of-the-box approach. By implementing the Law of Large Numbers in the malware, they achieved two goals: not only did they disguise the real C&C servers in common sandbox emulations (which are usually short), but also kept up the effectiveness of the malware.

In the table below we provide the probabilities of the real C&C server not being accessed again within a given time-frame. We take into consideration the lowest possible probability for the server to appear in any given cycle, which is **7/64**, as well as the longest possible pause between two cycles, which is **90 seconds**.

Time passed	Probability of the real C&C server being not accessed	Notes
9 minutes	50%	Like a coin toss
15 minutes	31%	Less than 1 in 3
18 minutes	25%	1 in 4
30 minutes	10%	1 in 10
1 hour	1%	1 in 100

2 hours	0.09%	Less than 1 in 10,000
2.5 hours	0.0009%	Less than 1 in 1,000,000

We see from the table that out of one million launches, only in one case the malware might not access the real C&C server in a period of 2.5 hours. In reality, the probability of such an event is even lower as a cycle time period can vary between 80 and 90 seconds, and the probability of the real C&C server to show up in a cycle may be higher and equal to 1/8.

Even 9 minutes are enough to fool the emulators and prevent the detection of the real C&C server, based on the delays between accesses to the domains. At the same time, the regular knockback period maintained by the malware with the help of probability theory allows it to keep victims as botnet parts without sacrificing the functionality.

XLoader 2.6

On May 5, 2022, we spotted a new version of XLoader malware in-the-wild. The main update in XLoader v2.6 concerns the network communication. The random index of the real C&C server is now saved in the malware state structure:

```
real_c2_index = (unsigned __int8)ab_genrand_between(0, 15i64);
xl_->saved_real_c2_index = (unsigned __int8)real_c2_index;
domain_idx_list[real_c2_index] = real_c2;
```

Figure 10 – XLoader 2.6 generates and stores the index of a real C&C server.

During each communication cycle, when the malware overwrites the first 8 entries in the list of accessed domains, it keeps the values for the real and the fake C&C domains:

```
do
{
  if ( xl->saved_fake_c2_index != c && xl->saved_real_c2_index != c )
  {                                         // overwrite the domain in the list
                                            // only if its index is not equeal to
                                            // the real_c2_idx or fake_c2_idx
    ab_memset(target_string, 46i64);
    ptr = 928i64 * c;                       //
                                            // domain name decryption follows...
```

Figure 11 – XLoader 2.6 doesn't overwrite the fake and the C&C domain indices.

Therefore, the real C&C server is now accessed in every communication cycle, or once in approximately 80-90 seconds.

However, this logic is activated only when the malware runs in an x64 system. When it runs in an x86 system, the variable **real_c2_index** stores the same value as is stored in the **fake_c2_index**. This results in the real C&C server being accessed with the same probability as any of the 63 decoys while running in x86 system. This looks like an evasion technique, as currently a lot of sandboxes still use x86 virtual machines.

Conclusion

To stay in business, malware actors have to stay in the forefront of progress and invent new tricks to prolong the lives of their creations as long as possible. In the case of XLoader malware, we see a vivid example of such a process.

In July 2021, we described the method of uncovering real C&C servers among the thousands of legitimate servers abused by XLoader v.2.3. The upgraded XLoader v.2.5 introduced significant changes in this algorithm using the power of the Law of Big Numbers from probability theory. These modifications achieve two goals at once: each node in the botnet maintains a steady knockback rate while fooling automated scripts and preventing the discovery of the real C&C servers. The latter indeed became more difficult, but not impossible.

In this article we described all the steps you need to take, and all the details you need to pay attention to in order to identify the real C&C domain among the 65 encountered in every XLoader sample. We analyzed more than 100,000 domains to discover a tiny percentage of actual C&C servers in the multitude of abused domains – only 120 of the real servers, which is about 0.12% of the total number.

We continue to stay vigilant for any upcoming changes that might be implemented by future versions, not only in XLoader but in other malware families as well.

Check Point Protections

Check Point Provides Zero-Day Protection across Its Network, Cloud, Users and Access Security Solutions. Whether you're in the cloud, the data center, or both, Check Point's Network Security solutions simplify your security without impacting network performance, provide a unified approach for streamlined operations, and enable you to scale for continued business growth. Quantum provides the best zero-day protection while reducing security overhead.

SandBlast Network Protections:

```
Trojan.WIN32.Formbook.A
Trojan.WIN32.Formbook.B
Trojan.WIN32.Formbook.C
Trojan.WIN32.Formbook.D
Trojan.WIN32.Formbook.E
Trojan.WIN32.Formbook.F
Trojan.WIN32.Formbook.G
Trojan.WIN32.Formbook.H
Trojan.WIN32.Formbook.I
Trojan.WIN32.Formbook.J
Trojan.WIN32.Formbook.K
Trojan.WIN32.Formbook.L
Trojan.WIN32.Formbook.M
Trojan.WIN32.Formbook.N
Trojan.WIN32.Formbook.O
Trojan.WIN32.Formbook.P
Trojan.WIN32.Formbook.Q
Trojan.WIN32.Formbook.R
```

Threat Emulation protections:

```
Infostealer.Win32.Formbook.C
Infostealer.Win32.Formbook.D
Infostealer.Win32.Formbook.E
Infostealer.Win32.Formbook.gl.F
Infostealer.Win32.Formbook.TC
Formbook.TC
Infostealer.Win32.XLoader.TC
XLoader.TC
Trojan.Mac.XLoader.B
```

Appendix: Indicators of Compromise

XLoader samples

SHA256	Version	C&C domain
c3bf0677dfcb32b35defb6650e1f81ccfa2080e934af6ef926fd378091a25fdb	2.6	travelsagas.com
77ed8c0589576ecaf87167bc9e178b15da57f7b341ea2fda624ecc5874b1464b	2.6	click-tokens.com
041992cc47137cb45d4e93658be392bb82cdc7ec53f959c6af4761d41dfc9160	2.6	motarasag.com
e704bc09c7da872b5d430d641e9bd7c8c396cf79ea382870e138f88d166df4a8	2.6	tumpiums.com
a7023d5b16691b20334955294a80c10d435e24048f6416d1b3af3c58d0b48954	2.5	sasanos.com
862fba20ce7613356018ca44f665819522f862f040b34410a58892229aba6d9c	2.5	binbin-ads.com
d56e8522cf147e2b964a5a03e51a17d24d4cb3a4a20f36ef3fd3caeda0b105f3	2.5	range4tis.com
59048fa3b523121866f79a8a2f7a3c9c7cf609a98be5a1ec296030de2353d559	2.5	cablinqee.com

XLoader C&C servers

Domain	IP
besasin09.com	162.0.223.94
brasbux.com	162.0.223.94
munixc.info	162.0.223.94
ceser33.com	162.0.223.94
ducer.info	199.192.23.209
amenosu.com	199.192.23.209
sanfireman.info	199.192.23.209
trc-clicks.com	199.192.25.68
bantasis.com	199.192.25.68
brass-tip.info	199.192.25.68
neurosise.com	199.192.30.112
finsith.com	199.192.30.112
gate334.com	199.192.30.112
seo-clicks6.com	199.192.30.247
tangodo9.info	199.192.31.5

nu865ci.com	199.192.31.5
rapibest.com	199.192.31.5
recbi56ni.com	199.192.31.5
heinousas.com	66.29.143.39
pordges.com	66.29.143.39
serenistin.com	66.29.143.39
aminsfy.com	66.29.155.250
dempius.com	66.29.155.250
buge-link.com	66.29.155.250
norllix.com	66.29.155.250
sacremots.com	66.29.155.250
beputis4.com	68.65.121.46
bubu3cin.com	162.0.214.189
highpacts.com	162.0.216.5
finsits.com	162.0.225.82
arabatas.com	162.0.225.82
cutos2.com	162.0.225.82
nropes.com	162.0.233.84
gogoma3.com	162.0.233.84
fraiuhs.com	162.0.233.84
busipe6.com	162.0.238.116
bupis44.info	162.0.238.116
gesips.com	162.0.238.116
ocvcoins.com	162.0.238.238
gingure.com	162.0.238.238
nifaji.com	162.0.238.238
coalmanses.com	162.213.253.206
fendoremi.com	162.213.253.206
cusio3c.com	162.213.253.206
nutri6si.com	162.213.253.206

breskizci.com	192.64.116.180
high-clicks.com	192.64.116.180
gunnipes.com	199.192.23.164
dugerits.com	199.192.23.164
keepitng.com	199.192.23.164
fellasies.com	199.192.28.149
butuns.com	199.192.28.149
bendisle.com	66.29.155.108
ci-ohio.com	66.29.155.108
minimi36.com	66.29.155.108
pedorc.com	68.65.121.125
cures8t.com	68.65.121.125
mecitiris.com	162.0.222.70
high-clicks2.com	162.0.224.219
nerosbin.info	162.0.231.105
b8ceex.com	162.0.231.105
dashmints.com	162.0.231.244
rap8b55d.com	198.54.112.103
rastipponmkh.com	199.192.17.24
blendeqes.com	199.192.17.24
private-clicks.com	199.192.26.170
abros88.com	199.192.30.127
bracunis.com	199.192.30.127
hugefries3.com	199.192.30.127
saint444.com	63.250.44.164
bra866.com	66.29.130.171
hype-clicks.com	162.0.223.146
moukse.com	162.0.223.146
ammarus.com	162.0.223.146
cablinqee.com	162.0.223.146

funtabse.com	162.0.223.146
gulebic.com	162.0.223.146
catdanos.com	199.188.206.146
noun-bug.com	199.188.206.146
cobere9.com	199.188.206.146
ranbix.com	199.188.206.146
tes5ci.com	199.188.206.146
blackbait6.com	199.188.206.146
mimihin.com	199.192.18.217
cesiesis.com	199.192.18.217
moreosin.com	199.192.18.217
side-clicks.com	199.192.29.43
davinci65.info	199.192.29.43
plick-click.com	199.192.29.43
redandseven.com	199.192.29.61
berdisen.com	199.192.29.61
arches2.com	199.192.29.61
price-hype.com	199.192.30.202
becbares.com	199.192.30.202
budistx.com	199.192.30.202
dain6544.com	199.192.30.202
erisibu85.com	199.192.30.202
piecebin.com	66.29.133.181
probinns.com	66.29.133.181
bumabagi.com	66.29.133.181
hughers3.com	66.29.133.181
n4sins.com	66.29.133.181
busy-clicks.com	66.29.140.185
minismi2.com	66.29.140.185
wecuxs.com	66.29.140.185

lopsrental.lease	66.29.140.185
alpeshpate.com	66.29.142.52
motometics.com	66.29.142.52
cinasing.com	66.29.142.52
gamusemenu.com	66.29.142.52
kraines3.com	66.29.142.52
ban-click.com	66.29.145.216
butsins.com	66.29.145.216
earches3.com	66.29.145.216
jervinse.com	66.29.154.112
gimbases.com	66.29.154.112
motarase.com	66.29.154.112
cusmose.com	66.29.154.157
becu84ts.com	66.29.154.157
buresdx.com	66.29.154.157
travelsagas.com	162.0.216.71
click-tokens.com	66.29.142.85
motarasag.com	162.0.233.154
tumpiums.com	66.29.155.51
sasanos.com	45.132.241.87
binbin-ads.com	31.220.18.33
range4tis.com	45.15.25.154