Botnet

PureCrypter is busy pumping out various malicious malware families

wanghao
Aug 29, 2022 • 12 min read

In our daily botnet analysis work, it is common to encounter various loaders.Compared to other types of malware, loaders are unique in that they are mainly used to "promote", i.e., download and run other malware on the infected machine. According to our observations, most loaders are proprietary and have a binding relationship with the family they are promoting. A few loader families make themselves into promotion platforms that can spread any other malware family, achieving the so-called malware-as-a-service (MaaS). Compared with proprietary loaders, MaaS types are obviously more dangerous and should be our primary target of concern.

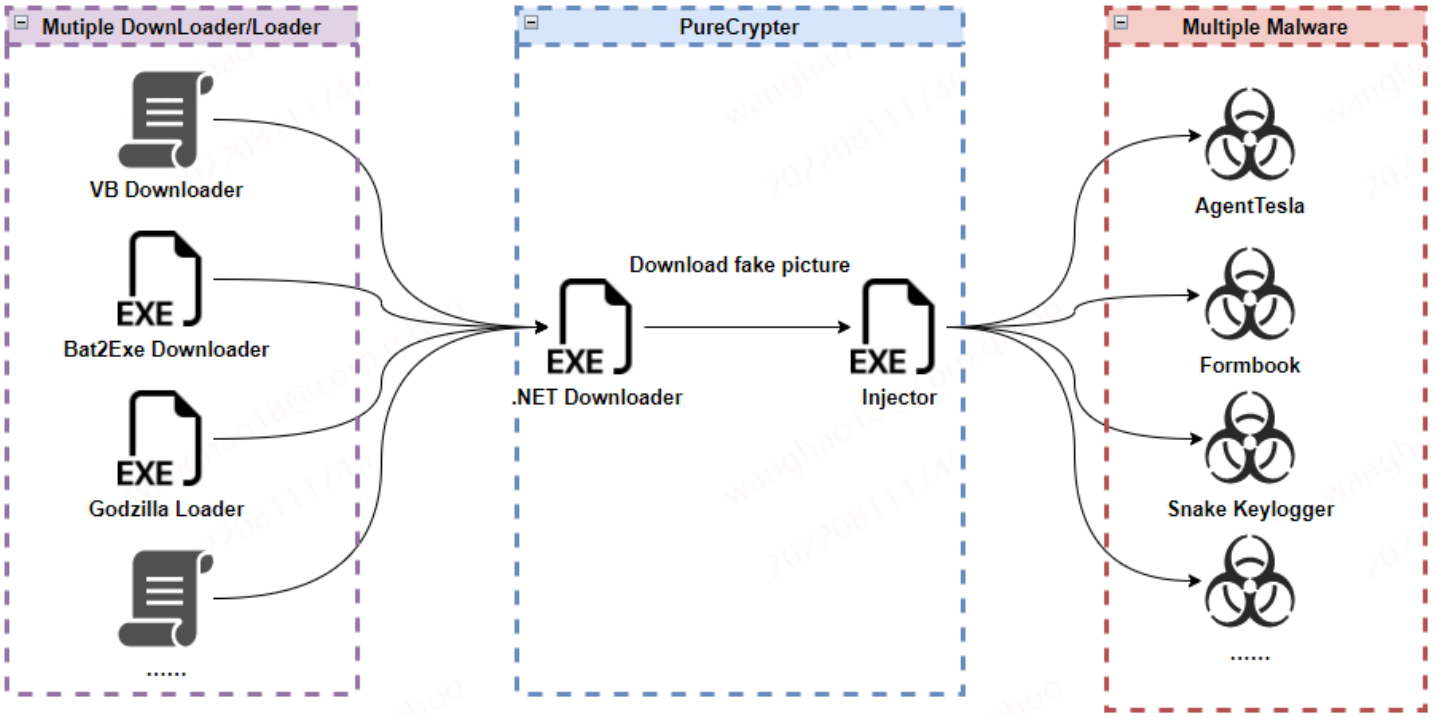
This article introduces a MaaS type loader we saw a while ago, named PureCrypter, which is very active this year, promoting more than 10 other families and using hundreds of C2s. Zscaler has done a detailed sample analysis, this blog mainly introduces the PureCrypter propagation activity we saw from the perspective of C2s and propagation chains to explore the operation of the MaaS type botnet.

The main points of this paper are as follows.

- PureCrypter is a loader written in C# that has been around since at least 2021 and can propagate any other family.
- PureCrypter continues to be active this year and has propagated more than 10 other malware families including Formbook, SnakeKeylogger, AgentTesla, Redline, AsyncRAT, and others.

- PureCrypter authors appears to be resourceful, as we have seen hundreds of C2 domains and IPs.
- PureCrypter use image name suffixes combined with inversion, compression and encryption to avoid detection.
- PureCrypter has a long propagation chain, and most of them use pre-protectors, some times mixed with other loaders, making detection more difficult.

In general, the spread of PureCrypter can be summarized in the following figure.



Now let's look at the samples and some typical propagation cases below.

Sample analysis

PureCrypter uses the package mechanism, which consists of two executables: downloader and injector, both written in C#, where downloader is responsible for propagating the injector, which releases and runs the final payload.

In practice, the attacker generates downloader and injector through builder, and then will try to propagate downloader, which will download and execute injector

on the target machine, and then injector will do the rest of the work. In terms of code logic, the downloader module is relatively simple, with a low level of binary obfuscation and no complex operations such as environment detection and persistence, while injector uses common tricks and techniques seen in popular loaders, such as binary obfuscation, runtime environment detection, starting puppet processes, etc. The following is a brief introduction to downloader and injector combined with actual examples.

downloader module

This module directly calls WebClient's DownloadData method for HTTP downloads, without setting any HTTP headers.

The following is an example of downloading a sample variant with inverted processing, from the parsing code you can see that the HTTP payload is inverted.

The inverted PE Header can be found at the end.

Finally, the recovered data (.DLL file) is loaded by Assembly.Load, and the entry method of plaintext encoding is called to proceed to the next stage.

PureCrypter is relatively simple to protect the injector download, so far, in addition to the above mentioned inverted (reverse) encoding, there are also gzip compression, symmetric encryption, etc. This encoding is fixed, that is, the builder has already determined the encoding method when generating the modules of downloader and injector.

The following is an example of using gzip compression and then transferring the injector, and the magic header of gzip can be found at the beginning: `1F 8B 08 00` .

We have also come across examples where AES encryption is used.

In addition to AES, PureCrypter also supports DES, RC4 and other encryption algorithms.

injector module

If you analyze the injector samples restored by downloader, you will find that the latter are heavily obfuscated. Here is an example of an injector obfuscated by SmartAssembly and partially encrypted with resources.

As shown in the figure above, first the relevant configuration information can be got from the combo of Reverse + GZip + Protubuf.Deserialize; then the runtime environment is checked to fight against sandboxing, with mutexes creation and persistence being done based on the configuration; and finally the payload is read from the resource section for loading. The sample does not enter any if statement, and soon reaches the last important function, which mainly implements the final payload injection. 4 injection methods are supported. While which one to use depends on the configuration, Process Hollowing is the most frequently used one.

The final payload is stored in the resource.

After reversing and gzip decompression, a puppet process is created to start the final payload.

The final payload promoted above is AgentTesla, whose configuration information is as follows.

```
host: raphaellasia.com
port:587
username: origin@raphaellasia.com
pwd: student@1980
to: origin2022@raphaellasia.com
```

Accidental discovery

PureCrypter likes to disguise the injector as an image for downloading, the image name is relatively random and has obvious machine generated features. Here are some of the actual detected image names.

```
# pattern 1
/dl/0414/net_Gzhsuovx.bmp
/dl/0528/mars2_Hvvpvuns.bmp
/dl/0528/az_Tsrqixjf.bmp

# pattern 2
/040722/azne_Bvaquebo.bmp
/04122022/net_Ygikzmai.bmp
/04122022/azne_Jzoappuq.bmp
/04122022/pm_Dxjlqugu.bmp
/03252022/azne_Rmpsyfmd.bmp

# pattern 3
/Rrgbu_Xruauocq.png
/Gepstl_Mouktkmu.bmp
/Zhyor_Uavuxobp.png
/Xgjbdziy_Kglkvdfb.png
/Ankwgqtwf_Bdevsqnz.bmp
/Osgyjgne_Ymgrebdt.png
/Rrgbu_Xruauocq.png
/Gepstl_Mouktkmu.bmp
/Osgyjgne_Ymgrebdt.png
/Osgyjgne_Ymgrebdt.png
/Zhyor_Uavuxobp.png
```

After analyzing several samples, we found that there is a correspondence between the requested image name and the downloader's AssmblyName.

PICTURENAME	ASSMBLYNAME
Belcuesth_lpdtbadv.png	Belcuesth
Kzzlcne_Prgftuxn.png	Kzzlcne
newminer2_Jrltkmeh.jpg	newminer2
Belcuesth_lpdtbadv.png	Belcuesth

PICTURENAME	ASSMBLYNAME
Nykymad_Bnhmcpqo.bmp	Nykymad
my_ori_Ywenb_Yzueqpjp.bmp	my ori Ywenb

and the content after the underscore always matches the regular expression

> *[A-Z][a-zA-Z]{7}*

C2 and propagation analysis

PureCrypter has been active this year, and we have detected more than 200 C2 domains and IPs, and more than 10 propagated families. In the cases we have seen, the propagation chain is generally long, and the downloader module of PureCrypter is often used in conjunction with various other types of predecessor downloaders. Because there are too many C2s, here is an introduction to `185.215.113.89` as an example in terms of scale and propagation methods.

C2 analysis

This C2 is more active than others among the C2s we detected, and its active time is from mid-April to early June this year, as shown in the figure below.

Its activity level can be reflected visually by our graph system.

It can be seen that it is associated with more domains and IPs, and the following is part of the IP's domain name resolution during this period.

```
2022-04-14 22:47:34     2022-07-05 00:42:16     22      rockrock.ug     A       185.
2022-04-21 08:22:03     2022-06-13 09:17:50     15      marnersstyler.ug        A
2022-04-17 03:17:41     2022-06-10 04:31:27     2538    qwertzx.ru      A       185.
2022-04-24 02:16:46     2022-06-09 00:11:24     3       hubvera.ac.ug   A       185.
2022-04-15 23:47:43     2022-06-08 19:24:59     43      timekeeper.ug   A       185.
2022-04-15 11:34:35     2022-06-08 19:24:59     35      boundertime.ru  A       185.
2022-04-14 23:01:50     2022-06-08 15:33:25     24      timebound.ug    A       185.
2022-04-15 21:58:54     2022-06-08 05:43:21     7       www.rockrock.ug A       185.
```

```
2022-04-16 20:50:41     2022-06-08 01:44:01     54      beachwood.ug    A       185.2
2022-04-23 16:23:41     2022-06-07 18:30:51     5       asdsadasrdc.ug  A       185.2
2022-05-02 22:35:40     2022-06-07 04:34:12     17      leatherlites.ug A       185.2
2022-05-29 17:46:00     2022-06-07 03:50:36     3       underdohg.ac.ug A       185.2
2022-04-15 22:34:53     2022-06-07 03:33:10     18      rockphil.ac.ug  A       185.2
2022-04-15 03:09:13     2022-06-07 03:19:50     14      pdshcjvnv.ug    A       185.2
2022-04-15 03:04:12     2022-06-07 03:12:04     16      mistitis.ug     A       185.2
2022-04-16 03:08:46     2022-06-07 03:08:48     18      nicoslag.ru     A       185.2
2022-04-19 02:33:31     2022-06-07 02:37:08     16      danwisha.ac.ug  A       185.2
2022-05-28 23:56:02     2022-06-05 05:14:50     7       underdohg.ug    A       185.2
2022-05-10 14:44:28     2022-06-02 17:40:12     24      jonescourtney.ac.ug     A
2022-06-02 07:44:25     2022-06-02 07:44:25     1       triathlethe.ug  A       185.2
2022-04-24 03:05:38     2022-06-01 16:54:59     2191    qwertasd.ru     A       185.2
2022-04-17 09:34:27     2022-06-01 01:42:07     2       partaususd.ru   A       185.2
2022-04-25 00:08:53     2022-05-31 07:17:00     5       timecheck.ug    A       185.2
2022-04-21 02:36:41     2022-05-31 01:20:37     21      courtneyjones.ac.ug     A
2022-04-16 19:09:02     2022-05-31 01:02:02     14      marksidfgs.ug   A       185.2
2022-04-25 03:01:15     2022-05-30 03:04:29     10      mofdold.ug      A       185.2
2022-04-15 02:36:21     2022-05-30 02:32:53     17      check-time.ru   A       185.2
2022-04-18 02:21:26     2022-05-30 02:22:30     17      agenttt.ac.ug   A       185.2
2022-04-17 03:17:46     2022-05-29 03:17:26     15      qd34g34ewdfsf23.ru      A
2022-04-19 02:25:06     2022-05-29 02:22:57     14      andres.ug       A       185.2
2022-04-16 02:27:44     2022-05-29 02:22:47     16      asdasgs.ug      A       185.2
```

From the visits in column 3, differences in the number of visits to these domains can be found, with overall visits in the thousands, and this is only one of the many C2s we see.

Through correlation analysis, we found that `185.215.113.89` is often used in conjunction with two C2s, `62.204.41.69` (March) and `45.143.201.4` (June), and their relationship can be correlated using the chart below.

Propagation analysis

PureCrypter uses the dual module mechanism of downloader+injector, the former is disseminated and then the latter is disseminated, which is equivalent to adding a link to the dissemination chain, plus the author's usual means to hide the objector by means of fake image, encoding transmission, etc., which is complicated enough in itself.

The author also put a lot of effort in the downloader propagation piece, we see the way through the bat2exe bundled crack software, the use of VBS and powershell

script loader, combined with Godzilla front loader and many other ways, the result of these operations superimposed is the spread chain is generally deeper and more complex. In May we even found cases of spreading Raccoon through PureCrypter, which further spread Azorult, Remcos, PureMiner, and PureClipper.

Here are a few typical propagation techniques.

1, "Bat2Exe+Powershell+VBS+Meteorite+PureCrypter" spreading Mars Stealer

This is mainly seen in some cracking software, downloader module is bundled to the former for propagation with Bat2Exe. The actual payload files stored in the resource are released to the tmp directory and triggered by the start.bat. The files released in the tmp directory are shaped as follows.

The start.bat command takes the shape of：

In the case we analyzed, the .lnk file is used to start the powershell to execute the malicious command.

Powershell decodes a base64-encoded VBS loader.

The VBS loader further releases a downloader and runs the latter via shellcode. The key information of this downloader is stored in the resource, including the process name and download url, as shown in the image below.

The downloader is named Meteorite according to the process name after running, and the url in the above figure corresponds to the downloader module of PureCrypter, and the complete communication process is as follows.

The final payload is Mars Stealer, c2: `rockrock.ug/gggate.php`, with the following configuration information:

2, "VBS/Powershell + PureCrypter" propagating PureMiner

The C2 involved is `89.34.27.167`. The entry can be either a VBS script or a Powershell script, here is an example of VBS script.

The network communication traffic is as follows.

Powershell script is as follows.

The Powershell script downloads and runs the downloader module of PureCrypter, which proceeds to download the injector, here it is more specific to use Discord to distribute the injector:

The final payload is PureMiner and C2 is as follows:

```
185.157.160.214
pwn.oracleservice.top
pwn.letmaker.top

port: 8080, 8444
```

3, "unknown .NET downloader + PureCrypter" to spread AgentTesla, RedLine

The downloader family is unknown, and its runtime is also divided into multiple stages, where the stage0 module is responsible for loading the stage1 malicious module in the resource.

The stage1 module will continue to load the next stage module stage2 after running.

stage2 module is also a Crypter (not yet named), different from PureCrypter, he also provides a download function, used to download the malicious PureCrypter downloader module, that is, the figure of puty.exe.

The malware can be decrypted from the resource with the key `bnvFGkCKlnhQ` using the following algorithm.

Two families of binaries are spread. Stage2's payload is AgentTesla with C2: `https[:]//api.telegram.org/bot5421147975:AAGrsGnLOHZfFv7yHuj3hZdQSOVmPodIAVI/sendDocument`

PureCrypter's payload is RedLine with C2:

```
IP: workstation2022.ddns.net:62099
ID: cheat
```

Summary

PureCrypter is a MaaS type botnet that is still active and has spread more than 10 other families of payloads, with generally complex spreading practices. There might be a fairly big and resourceful team behind it, so it won't surprised us if they continuously add and spread other malicious families in the future. We will keep an eye on it and share more information when it is needed.

Contact us

Readers are always welcomed to reach us on twitter or email us to **netlab[at]360.cn**.

IoCs

MD5

FAMILY NAME	MD5
Bat2Exe Downloader	424ed5bcaae063a7724c49cdd93138f5
VBS downloader	3f20e08daaf34b563227c797b4574743
Powershell downloader	c4c5167dec23b6dd2d565cd091a279e4
Unknown .NET Downloader	9b70a337824bac612946da1432295e9c

C2 &URL

```
agenttt.ac.ug
andres.ug
asdasgs.ug
asdsadasrdc.ug
beachwood.ug
boundertime.ru
check-time.ru
courtneyjones.ac.ug
danwisha.ac.ug
hopeforhealth.com.ph
hubvera.ac.ug
jonescourtney.ac.ug
leatherlites.ug
marksidfgs.ug
marnersstyler.ug
mistitis.ug
mofdold.ug
momomolastik.ug
nicoslag.ru
partaususd.ru
pdshcjvnv.ug
```

```
qd34g34ewdfsf23.ru
qwertasd.ru
qwertzx.ru
raphaellasia.com
rockphil.ac.ug
rockrock.ug
timebound.ug
timebounder.ru
timecheck.ug
timekeeper.ug
triathlethe.ug
underdohg.ac.ug
underdohg.ug
www.rockrock.ug
212.192.246.195
37.0.11.164:8080
80.66.75.123
89.34.27.167
91.243.44.142
185.215.113.89
62.204.41.69
45.143.201.4
https://cdn.discordapp.com/attachments/994652587494232125/1004377750762704896/ps1-6_
```

— 360 Netlab Blog - Network Security Research Lab at 360 —

Botnet

僵尸网络911 S5的数字遗产

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

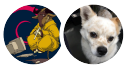
警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

See all 114 posts →

Botnet

卷土重来的DDoS狂魔：Fodcha僵尸网络再次露出獠牙

背景 2022年4月13日，360Netlab首次向社区披露了Fodcha僵尸网络，在我们的文章发表之后，Fodcha遭受到相关部门的打击，其作者迅速做出回应，在样本中留下Netlab pls leave me alone I surrender字样向我们投降。本以为Fodcha会就此淡出江湖，没想到这次投降只是一个不讲武德的假动作，Fodcha的作者在诈降之后并没有停下更新的脚...

Oct 27, 2022 · 23 min read

loader

PureCrypter Loader持续活跃，已经传播了10多个其它家族

在我们的日常botnet分析工作中，碰到各种loader是常事。跟其它种类的malware相比，loader的特殊之处在于它主要用来“推广”，即在被感染机器上下载并运行其它的恶意软件。根据我们的观察，大部分loader是专有的，它们和推广的家族之间存在绑定关系。而少数loader家族会将自己做成通用的推广平台，可以传播其它任意家族，实现所谓的malware-as-...

· Aug 29, 2022 · 14 min read