loader

PureCrypter Loader持续活跃，已经传播了10多个其它家族

wanghao
Aug 29, 2022 • 14 min read

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-a-service（MaaS）。跟专有loader相比，MaaS类型显然更危险，更应该成为我们的首要关注目标。

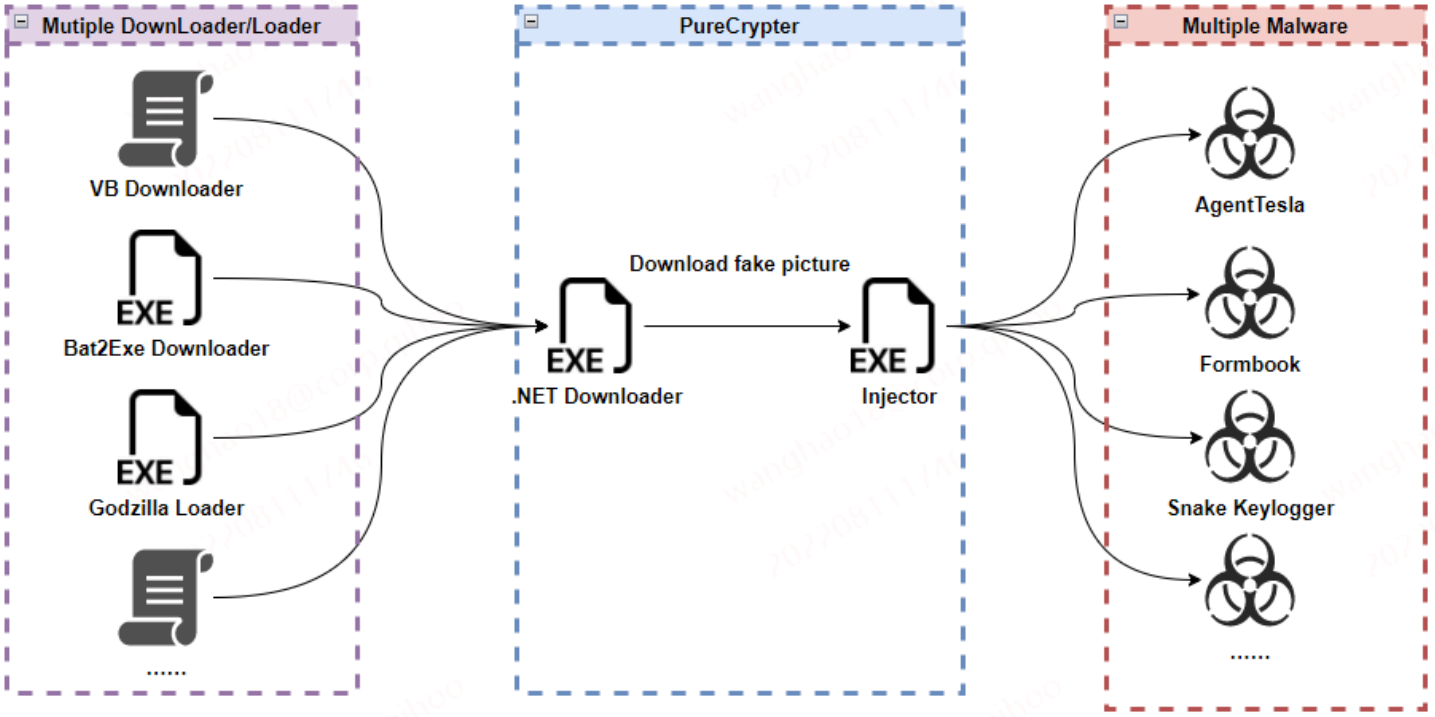
本文介绍我们前段时间看到的一个MaaS类型的loader，它名为PureCrypter，今年非常活跃，先后推广了10多个其它的家族，使用了上百个C2。因为zscaler已经做过详细的样本分析，本文主要从C2和传播链条角度介绍我们看到的PureCrypter传播活动，分析其运作过程。

本文要点如下：

- PureCrypter是一款使用C#编写的loader，至少2021年3月便已出现，能传播任意的其它家族。
- PureCrypter今年持续活跃，已经传播了包括Formbook、SnakeKeylogger、AgentTesla、Redline、AsyncRAT等在内的10多个恶意家族。
- PureCrypter作者拥有较多的推广资源，我们检测到的C2 域名和IP多达上百个。
- PureCrypter作者喜欢使用图片名后缀结合倒置、压缩和加密等方式躲避网络检测。

- PureCrypter的推广行为传播链条普遍较长，多数会使用前置protector，甚至搭配其它loader，检测难度较大。

总的来说，PureCrypter的传播情况可以用下图总结：



下面从样本分析和典型传播案例角度做一介绍。

样本分析

PureCrypter使用了package机制，由两个可执行文件组成：downloader和injector，它们都使用C#编写，其中downloader负责传播injector，后者释放并运行最终的目标家族二进制文件。实际操作时，攻击者通过builder生成downloader和injector，然后先设法传播downloader，后者会在目标机器上下载并执行injector，再由injector完成其余工作。从代码逻辑上看，downloader模块相对简单，样本混淆程度较低，没有复杂的环境检测和持久化等操作，而injector则使用了loader里常见的奇技淫巧，比如2进制混淆、运行环境检测、启动傀儡进程等，下面是结合实际的例子简单介绍下downloader和injector。

downloader模块

该模块直接调用WebClient的DownLoadData方法进行HTTP下载，没有设置单独的HTTP header。

injector的uri通常也是明文保存，下面是一个下载经过倒置处理的样本的变种的例子，从解析代码能看出来HTTP payload做了倒置处理。

在末尾可发现明显的被倒置的PE Header。

最后通过Assembly.Load加载恢复好的injector（.DLL文件），调用明文编码的入口方法，进入下一阶段。

PureCrypter对injector下载保护这块相对简单，目前看除了上面提到的倒置（reverse）编码外，还有 gzip压缩、对称加密等方式，这种编码是固定的，即builder在生成downloader和injector时就已经确定好编码方式，不存在运行动态改变的情况。

下面是使用使用gzip压缩后传输injector的例子，在流量开头可以发现GZip的magic header：`1F 8B 08 00`。

我们还碰到过使用AES加密的例子。

除了AES，PureCrypter还支持使用DES、RC4等加密算法。

injector模块

如果分析还原好的injector，会发现普遍做了混淆处理，差别只是混淆程度的大小。下面是一例SmartAssembly混淆并且资源部分被加密的injector：

如上图所示，首先通过Reverse + GZip + Protubuf.Deserialize组合拳，获取相关配置信息，之后是根据配置检查运行环境、对抗沙箱、创建互斥体、持久化等，最后

从资源中获取payload加载运行。该样本没有进入任何一个if语句，很快到了最后一个重要函数，该函数主要实现最终payload的注入。根据配置的不同存在4种注入方式，傀儡进程（Process Hollowing）是被最多使用的方式。

最终payload存储在资源中，解密后的资源如下图：

经过Reverse + GZip解压缩后创建傀儡进程启动最终的payload。

上面最终推广的payload为AgentTesla，其配置信息如下：

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

意外发现

PureCrypter喜欢将injector伪装成图片供downloader下载，图片名比较随机，具有明显机器生成的特点。下面是实际检测到的一些图片名。

```
# 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
```

在对多个样本进行分析后，我们发现请求的图片名与downloader的AssmblyName存在对应关系。

图片名	ASSMBLYNAME
Belcuesth_Ipdtbadv.png	Belcuesth
Kzzlcne_Prgftuxn.png	Kzzlcne
newminer2_Jrltkmeh.jpg	newminer2
Belcuesth_Ipdtbadv.png	Belcuesth
Nykymad_Bnhmcpqo.bmp	Nykymad
my_ori_Ywenb_Yzueqpjp.bmp	my ori Ywenb

下划线后面的内容总是符合正则表达式

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

基于这个发现可以结合样本和网络请求两个维度的数据确认PureCrypter的下载行为。

C2和传播分析

PureCrypter今年一直在活跃，我们先后检测到的C2 域名和IP有200多个，传播的家族数10多种。在我们看到的案例中，传播链条普遍比较长，PureCrypter的downloader模块经常跟各种其它类型的前置downloader配合使用。因为C2太多，这里主要以 `185.215.113.89` 为例从规模和传播手法方面做一个介绍。

C2分析

这个C2在我们检测到的C2中活跃度比较高，其活跃时间为今年4月中旬到6月初，如下图所示。

其活跃程度可以用我们的图系统直观反映出来。

能看到它关联到了比较多的域名和IP，下面是该IP在这段时间的部分域名解析情况。

```
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.
2022-04-23 16:23:41     2022-06-07 18:30:51     5       asdsadasrdc.ug  A       185.
2022-05-02 22:35:40     2022-06-07 04:34:12     17      leatherlites.ug A       185.
2022-05-29 17:46:00     2022-06-07 03:50:36     3       underdohg.ac.ug A       185.
2022-04-15 22:34:53     2022-06-07 03:33:10     18      rockphil.ac.ug  A       185.
2022-04-15 03:09:13     2022-06-07 03:19:50     14      pdshcjvnv.ug    A       185.
2022-04-15 03:04:12     2022-06-07 03:12:04     16      mistitis.ug     A       185.
2022-04-16 03:08:46     2022-06-07 03:08:48     18      nicoslag.ru     A       185.
2022-04-19 02:33:31     2022-06-07 02:37:08     16      danwisha.ac.ug  A       185.
2022-05-28 23:56:02     2022-06-05 05:14:50     7       underdohg.ug    A       185.
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.
2022-04-24 03:05:38     2022-06-01 16:54:59     2191    qwertasd.ru     A       185.
2022-04-17 09:34:27     2022-06-01 01:42:07     2       partaususd.ru   A       185.
2022-04-25 00:08:53     2022-05-31 07:17:00     5       timecheck.ug    A       185.
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.
2022-04-25 03:01:15     2022-05-30 03:04:29     10      mofdold.ug      A       185.
2022-04-15 02:36:21     2022-05-30 02:32:53     17      check-time.ru   A       185.
2022-04-18 02:21:26     2022-05-30 02:22:30     17      agenttt.ac.ug   A       185.
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.
2022-04-16 02:27:44     2022-05-29 02:22:47     16      asdasgs.ug      A       185.
```

第3列为访问量，不同域名访问量有差别，整体评估应该在千级，而这只是我们看到的众多C2中的一个。

通过关联分析，我们发现 `185.215.113.89` 经常跟 `62.204.41.69` (3月)和 `45.143.201.4` （6月）这两个C2配合使用，它们关系可以用下图关联。

传播分析

PureCrypter采用了downloader+injector的双模块机制，前者被传播后再传播后者，相当于在传播链条上增加了一环，加上作者惯用图片名后缀、编码传输等手段隐藏injector，这些本身就已足够复杂。而作者在downloader传播这块也下了不少功夫，我们看到的有通过bat2exe捆绑破解软件的方式、使用VBS和powershell脚本loader的方式、结合Godzilla前置loader等多种方式，这些操作叠加起来的结果就是PureCrypter的传播链条普遍较深较复杂。在5月份我们甚至发现通过PureCrypter传播Raccoon，后者进一步传播Azorult、Remcos、PureMiner、PureClipper的案例。

下面介绍几个典型传播手法。

1，“Bat2Exe+Powershell+VBS+Meteorite+PureCrypter”传播Mars Stealer

这个主要在一些破解软件上有见到，downloader模块通过Bat2Exe捆绑到前者进行传播。实际运行时保存在资源中的恶意文件被释放到tmp目录下，通过start.bat来触发运行。释放在tmp目录下的文件形如下图：

start.bat命令形如：

在我们分析的案例中，.lnk文件被用来启动powershell执行恶意命令。

Powershell解码出一个base64编码的VBS loader：

VBS loader进一步释放一个downloader，并通过shellcode运行后者。该downloader的敏感信息都保存在资源中，包括进程名和download url，如下图所示。

根据运行后的进程名将该downloader命名为`Meteorite`，上图中的url就对应PureCrypter的downloader模块，完整的通信过程如下图：

最终payload为Mars Stealer，c2: `rockrock.ug/gggate.php`，配置信息如下：

2，“VBS/Powershell + PureCrypter” 传播PureMiner

涉及的C2为`89.34.27.167`，入口为一个VBS脚本或者Powershell脚本，下面是VBS脚本的例子。

网络通信流量如下：

Powershell脚本如下：

Powershell脚本下载并运行PureCrypter的downloader模块，后者继续下载injector，这里比较特殊的是使用Discord来分发injector:

最终的payload为PureMiner，C2如下：

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

port: 8080, 8444
```

3，利用未知.NET downloader传播 AgentTesla、RedLine

该downloader家族未知，其运行时同样分为多个阶段，其中stage0模块负责加载资源中的stage1恶意模块：

stage1模块运行后会继续加载下一阶段模块stage2：

stage2模块也是一个Crypter(暂未命名)，与PureCrypter不同，他还提供了下载功能，用来下载恶意PureCrypter的downloader模块，即图中的`puty.exe`。

从资源中异或解密恶意软件，key为`bnvFGkCKlnhQ`，相关算法如下：

因此实际传播了两个家族：

stage2的payload为AgentTesla，c2为`https[:]//api.telegram.org/bot5421147975:AAGrsGnLOHZfFv7yHuj3hZdQSOVmPodIAVI/sendDocument`

PureCrypter的payload为RedLine，c2为

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

总结

PureCrypter是一个仍在活跃的MaaS类型的botnet，已经传播了10多种影响比较大的其它恶意家族。PureCrypter的传播手法普遍比较复杂，其背后应该存在至少一个比较专业的黑产组织，他们拥有较多的技术、域名和IP资源，预计今后会继续传播其它的恶意家族。我们对PureCrypter的传播活动一直有较好的检测，会第一时间将C2等威胁信息添加到我们的威胁情报库中。后续我们会继续保持关注，及时更新最新的威胁信息。

联系我们

感兴趣的读者，可以在 twitter 或者通过邮件**netlab[at]360.cn**联系我们。

IOC

MD5

FAMILY NAME	MD5
Bat2Exe Downloader	424ed5bcaae063a7724c49cdd93138f5
VBS downloader	3f20e08daaf34b563227c797b4574743
Powershell downloader	c4c5167dec23b6dd2d565cd091a279e4
未知.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_
```

loader

PureCrypter is busy pumping out various malicious malware families

1 post →

PureCrypter is busy pumping out various malicious malware families

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

Aug 29, 2022 · 12 min read

A new botnet Orchard Generates DGA Domains with Bitcoin Transaction Information

DGA is one of the classic techniques for botnets to hide their C2s, attacker only needs to selectively register a very small number of C2 domains, while for the defenders, it is difficult to determine in advance which domain names will be generated and registered. 360 netlab has long focused

Aug 5, 2022 · 13 min read