Dark Tequila Añejo

By GReAT

Published: 2018-08-21 · Archived: 2026-04-05 21:15:24 UTC

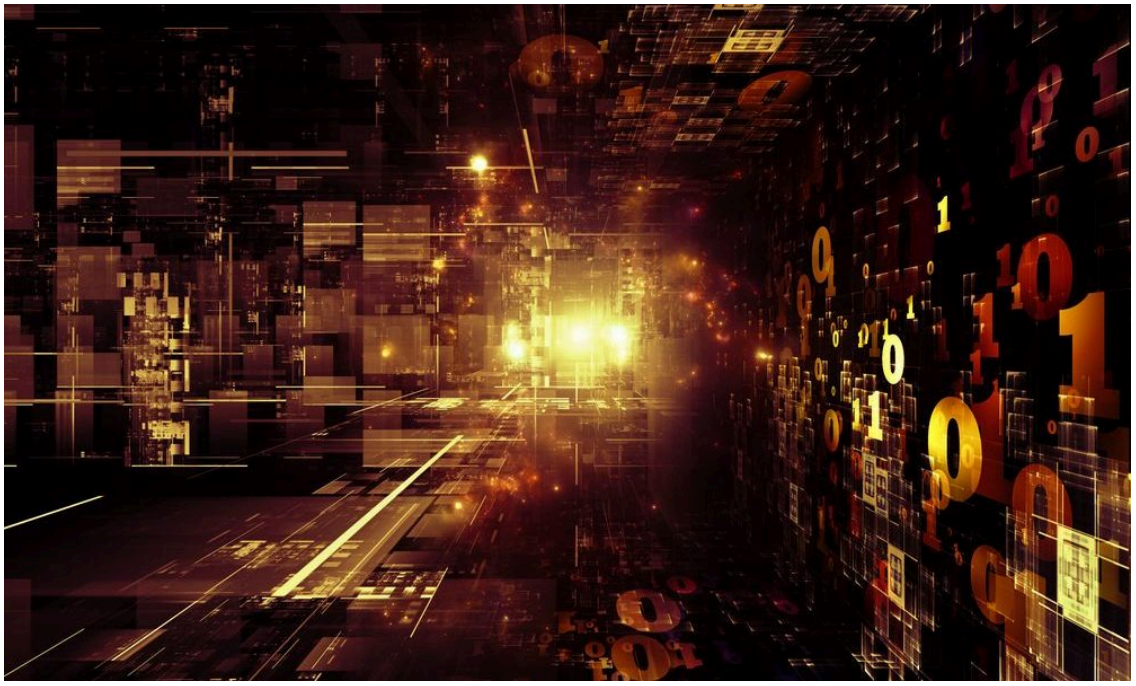
APT reports

APT reports

21 Aug 2018

2 minute read

- Expert GReAT



Dark Tequila is a complex malicious campaign targeting Mexican users, with the primary purpose of stealing financial information, as well as login credentials to popular websites that range from code versioning repositories to public file storage accounts and domain registrars.

A multi-stage payload is delivered to the victim only when certain conditions are met; avoiding infection when security suites are installed or the sample is being run in an analysis environment. From the target list retrieved from the final payload, this particular campaign targets customers of several Mexican banking institutions and contains some comments embedded in the code written in the Spanish language, using words only spoken in Latin America.

Most of the victims are located in Mexico. The campaign has been active since at least 2013, so it is a very ‘añejo’ (mature) product. There are two known infection vectors: spear-phishing and infection by USB device.

The threat actor behind it strictly monitors and controls all operations. If there is a casual infection, which is not in Mexico or is not of interest, the malware is uninstalled remotely from the victim’s machine.

```
CloseHandle = (void (__stdcall *)(HANDLE))::CloseHandle;
hObject_1 = (void *)beginthreadex(0, 0, monitor_usb_devices, 0, 0, 0);
::CloseHandle(hObject_1);
if ( hObject_1 )
{
  LOBYTE(disk_name) = 'A';
  for ( i = GetLogicalDrives(); i; i >>= 1 )
  {
    if ( i & 1 )
    {
      *(_DWORD *)RootPathName = 0;
      v49 = 0;
      v6 = decrypt_str_8(4);
      snprintf(RootPathName, 8, v6, (char)disk_name);
      if ( GetDriveTypeA(RootPathName) == DRIVE_REMOVABLE )
        append_item(1);
    }
    LOBYTE(disk_name) = (_BYTE)disk_name + 1;
  }
```

```
[autorun]
shell\open\command=autorun.exe
shell\open\default=1
shell\explore\command=autorun.exe
shell\explore\default=1
action=Abrir la carpeta para ver los archivos
shellexecute=autorun.exe
UseAutoPlay=1
icon=%systemroot%\system32\shell32.dll,7
```

(Translation for "Abrir la carpeta para ver los archivos" – "Open folder to see files". The word "Archivos" is used by Spanish speakers from Latin America only)

The Dark Tequila malware and its supporting infrastructure are unusually sophisticated for a financial fraud operation. The malicious implant contains all the modules required for the operation and, when instructed to do so by net command server, different modules decrypt and activate. All stolen data is uploaded to the server in encrypted form.

This campaign modules are as follows:

- Module 1, which is responsible for communication with the command and control server. It verifies if a man-in-the-middle network check is being performed, by validating the certificates with a few very popular websites.
- Module 2 – CleanUp. If the service detects any kind of 'suspicious' activity in the environment, such as the fact that it is running on a virtual machine, or that debugging tools are running in the background, it will execute this module to perform a full cleanup of the system, removing the persistence service as well as any files created previously on the system.
- Module 3 – Keylogger and Windows Monitor. This is designed to steal credentials from a long list of online banking sites, as well as generic Cpanels, Plesk, online flight reservation systems, Microsoft

Office365, IBM lotus notes clients, Zimbra email, Bitbucket, Amazon, GoDaddy, Register, Namecheap, Dropbox, Softlayer, Rackspace, and other services.

- Module 4 – Information stealer, which is designed to steal saved passwords in email and FTP clients, as well as from browsers.
- Module 5 – The USB infector. This copies an executable file to a removable drive to run automatically. This enables the malware to move offline through the victim's network, even when only one machine was initially compromised via spear-phishing. When another USB is connected to the infected computer, it automatically becomes infected, and ready to spread the malware to another target.
- Module 6 – The service watchdog. This service is responsible for making sure that the malware is running properly.

All the described modules are embedded inside the main sample and could be extracted during the analysis process.

The campaign remains active. It is designed to be deployed in any part of the world, and attack any targets according to the interests of the threat actor behind it. Kaspersky Lab detects the campaign as Trojan.Win32.DarkTequila and Trojan.Win64.DarkTequila.

Reference hashes:

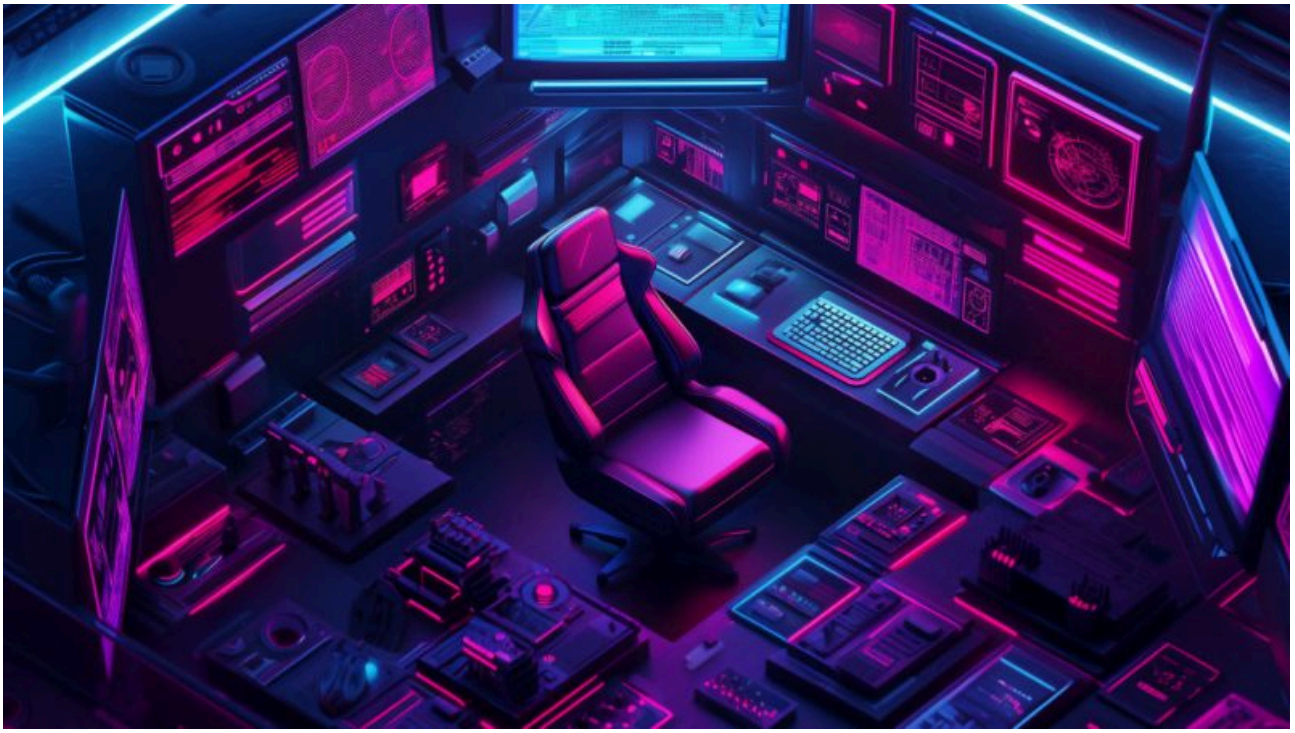
4f49a01e02e8c47d84480f6fb92700aa091133c894821fff83c7502c7af136d9
dce2d575bef073079c658edfa872a15546b422ad2b74267d33b386dc7cc85b47

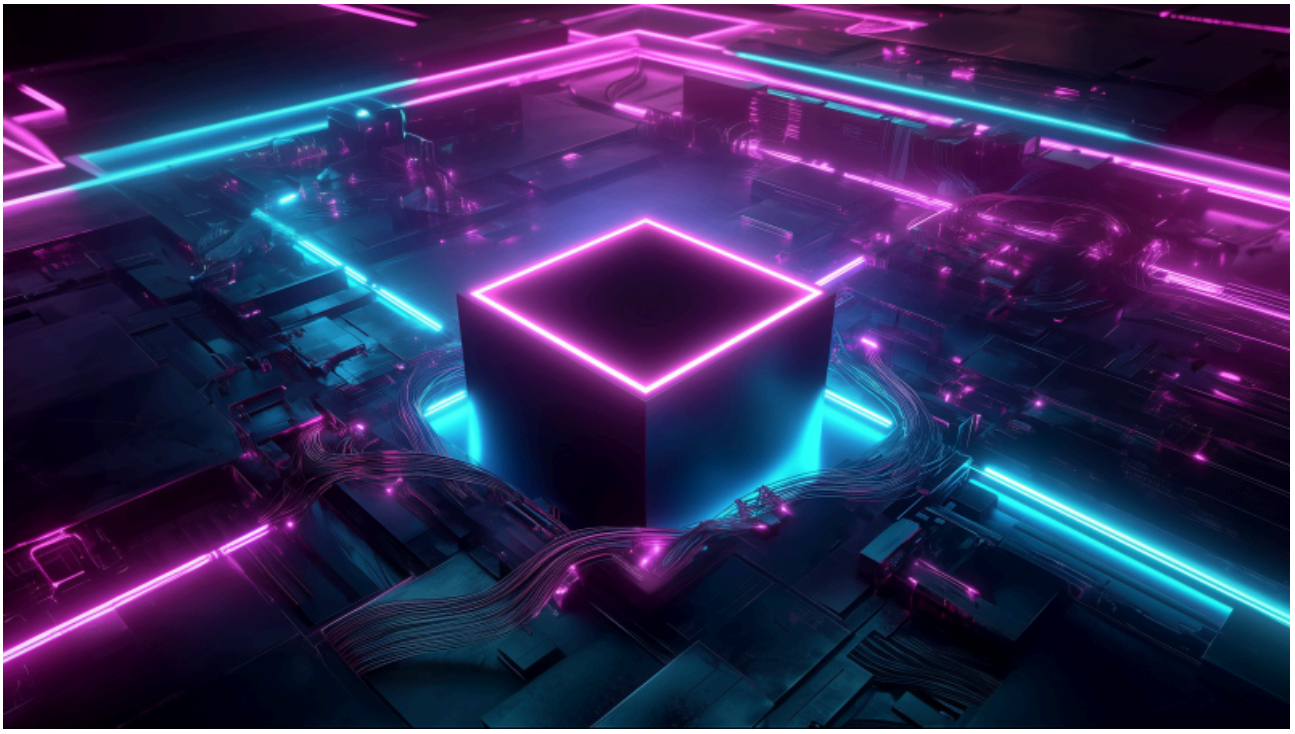
Reference C2s:

https://46[.]17[.]97[.]12/website/
https://174[.]37[.]6[.]34/98157cdfe45945293201e71acb2394d2
https://75[.]126[.]60[.]251/store/

For more information about this campaign, please contact us at financialintel@kaspersky.com

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
