OceanLotus hackers turn to web archive files to deploy backdoors

bleepingcomputer.com/news/security/oceanlotus-hackers-turn-to-web-archive-files-to-deploy-backdoors

The OceanLotus group of state-sponsored hackers are now using the web archive file format (.MHT and .MHTML) to deploy backdoors to compromised systems.

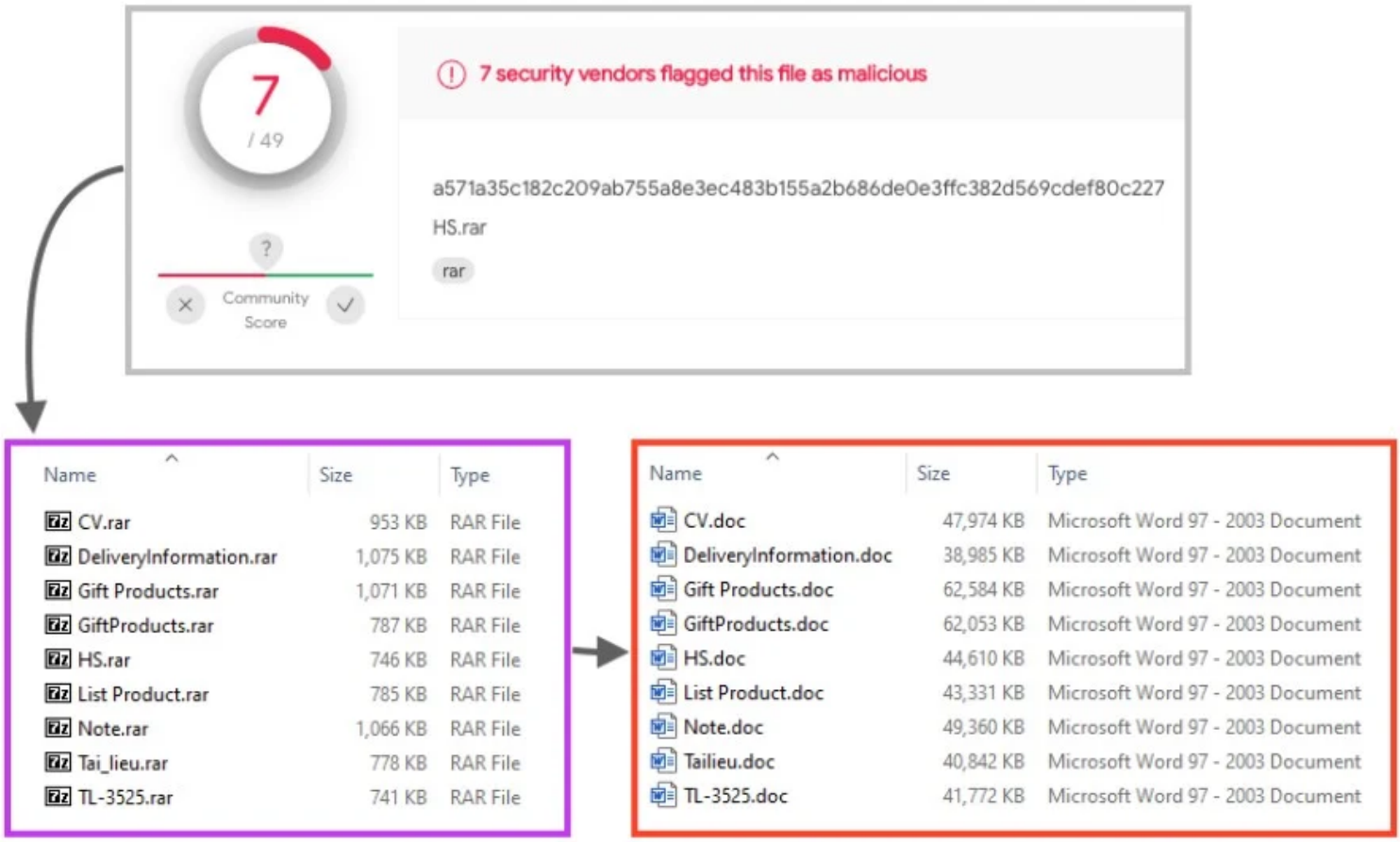
The goal is to evade detection by antivirus solutions tools which are more likely to catch commonly abused document formats and stop the victim from opening them on Microsoft Office.

Also tracked as APT32 and SeaLotus, the hackers have shown a tendency in the past to try out less common methods for deploying malware.

A report from Netskope Threat Labs shared with Bleeping Computer in advance notes that OceanLotus' campaign using web archive files is still active, although the targeting scope is narrow and despite the command and control (C2) server being disrupted.

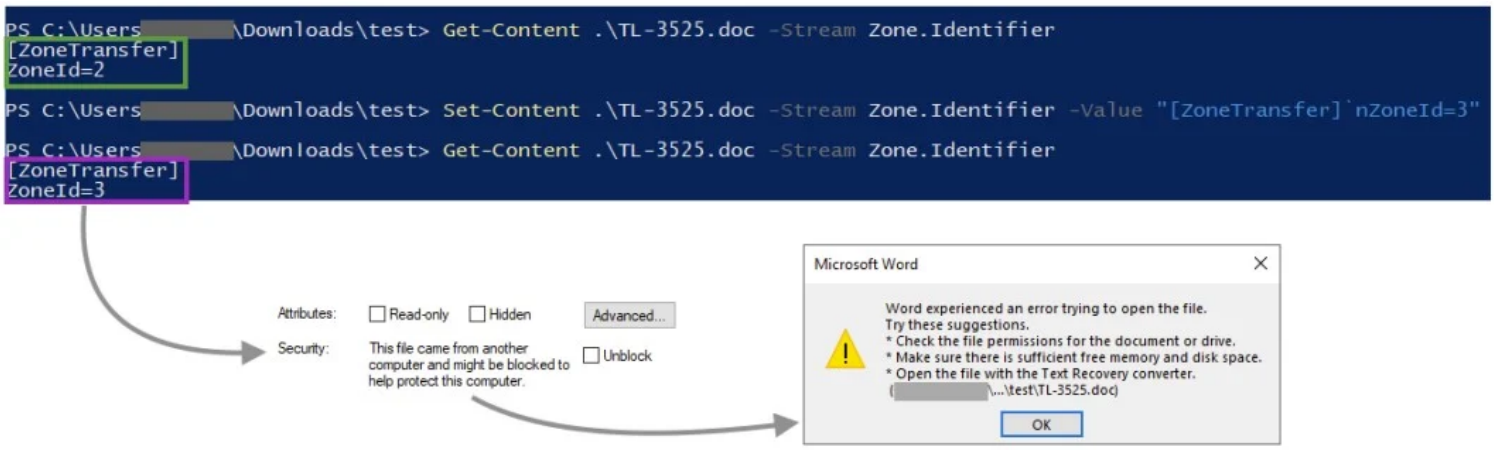
From trusty RARs to Word macros

The attack chain starts with a RAR compression of a 35-65MB large web archive file containing a malicious Word document.



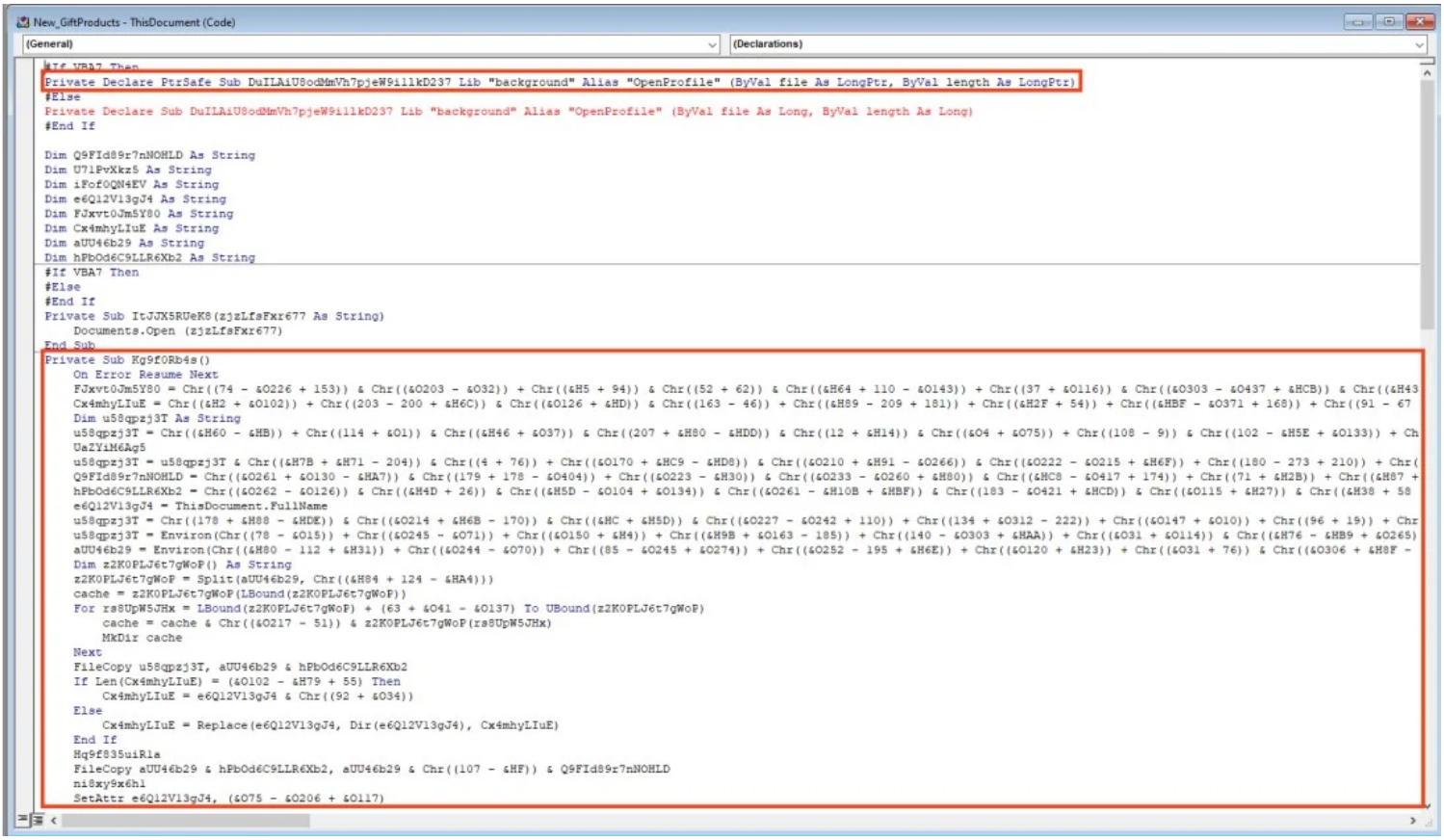
RAR file dropped as the first step of the attack
Source: Netskope

To bypass Microsoft Office protection, the actors have set the ZoneID property in the file's metadata to "2", making it appear as if it was downloaded from a trustworthy source.



Setting ZoneID value to bypass MS Office protection
Source: Netskope

When opening the web archive file with Microsoft Word, the infected document prompts the victim to "Enable Content", which opens the way to executing malicious VBA macro code.



Decoded VBA code used in APT32 docs
Source: Netskope

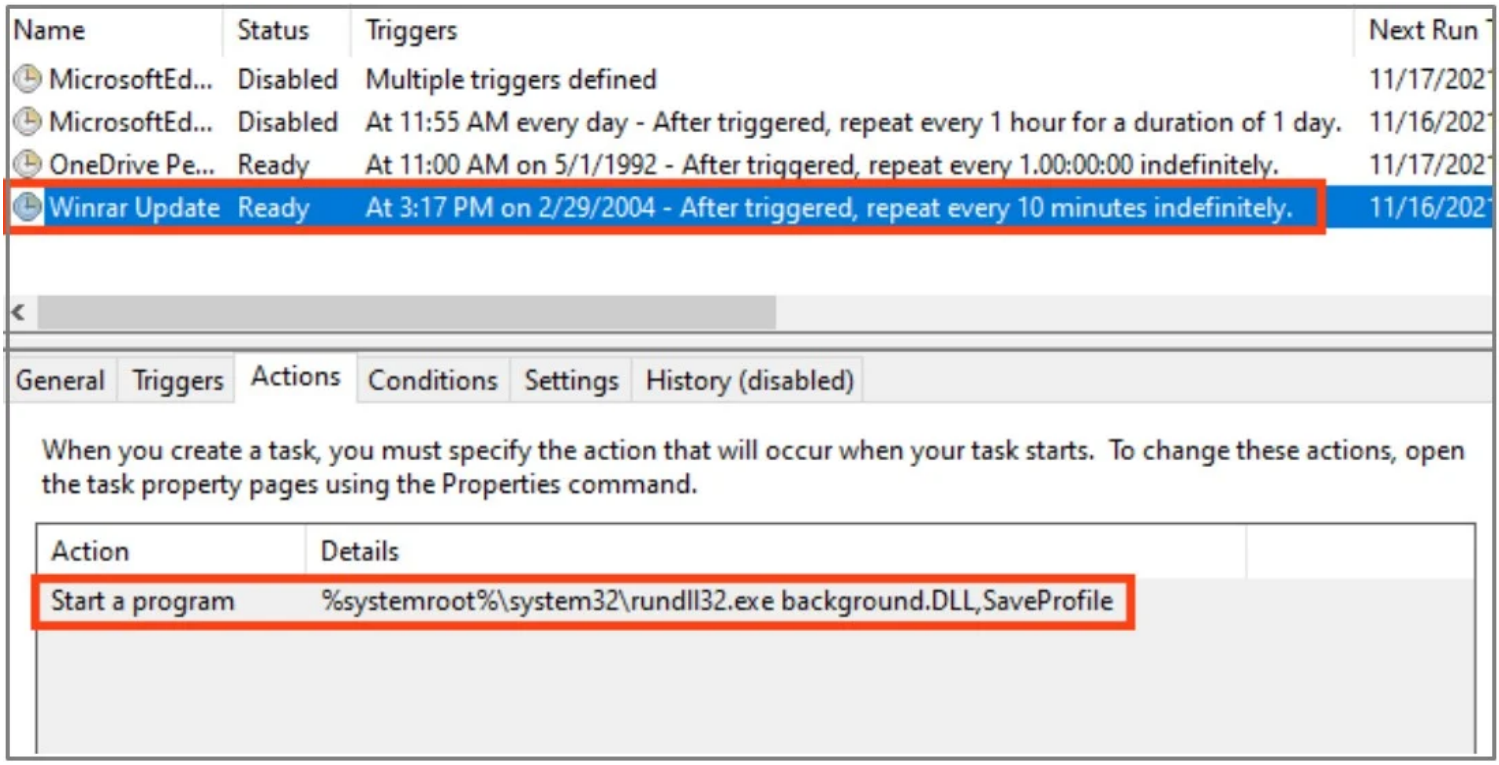
The script performs the following tasks on the infected machine:

1. Drops the payload to "C:\ProgramData\Microsoft\User Account Pictures\guest.bmp";
2. Copies the payload to "C:\ProgramData\Microsoft Outlook Sync\guest.bmp";
3. Creates and display a decoy document named "Document.doc";
4. Rename the payload from "guest.bmp" to "background.dll";
5. Executes the DLL by calling either "SaveProfile" or "OpenProfile" export functions

After the payload is executed, the VBA code deletes the original Word file and opens the decoy document which serves the victim a bogus error.

Backdoor uses Glitch hosting service

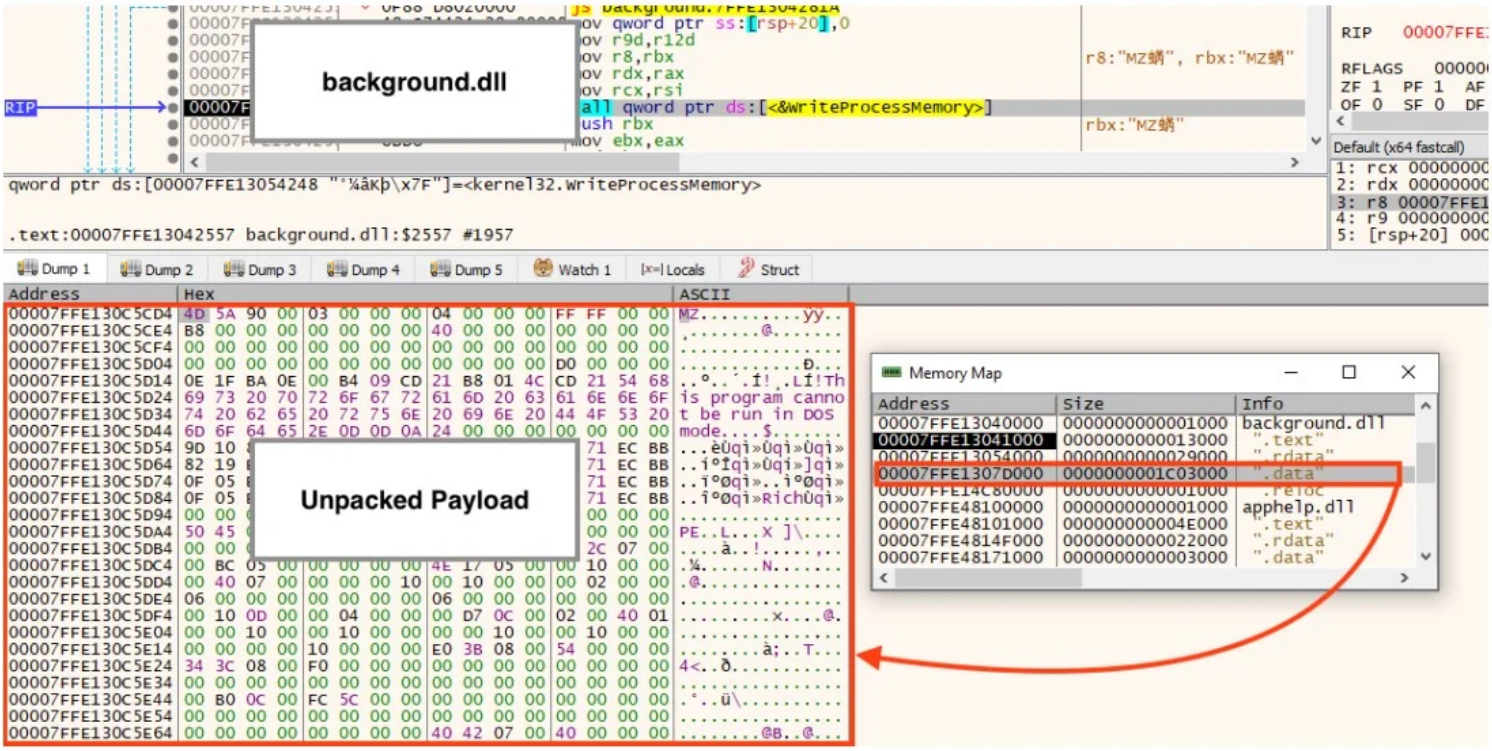
The payload dropped in the system is a 64-bit DLL that executes every 10 minutes thanks to a scheduled task impersonating a WinRAR update check.



Fake process carrying the payload injection

Source: Netskope

The backdoor is injected into the rundll32.exe process running indefinitely in the system memory to evade detection, Netskope notes in its technical report.



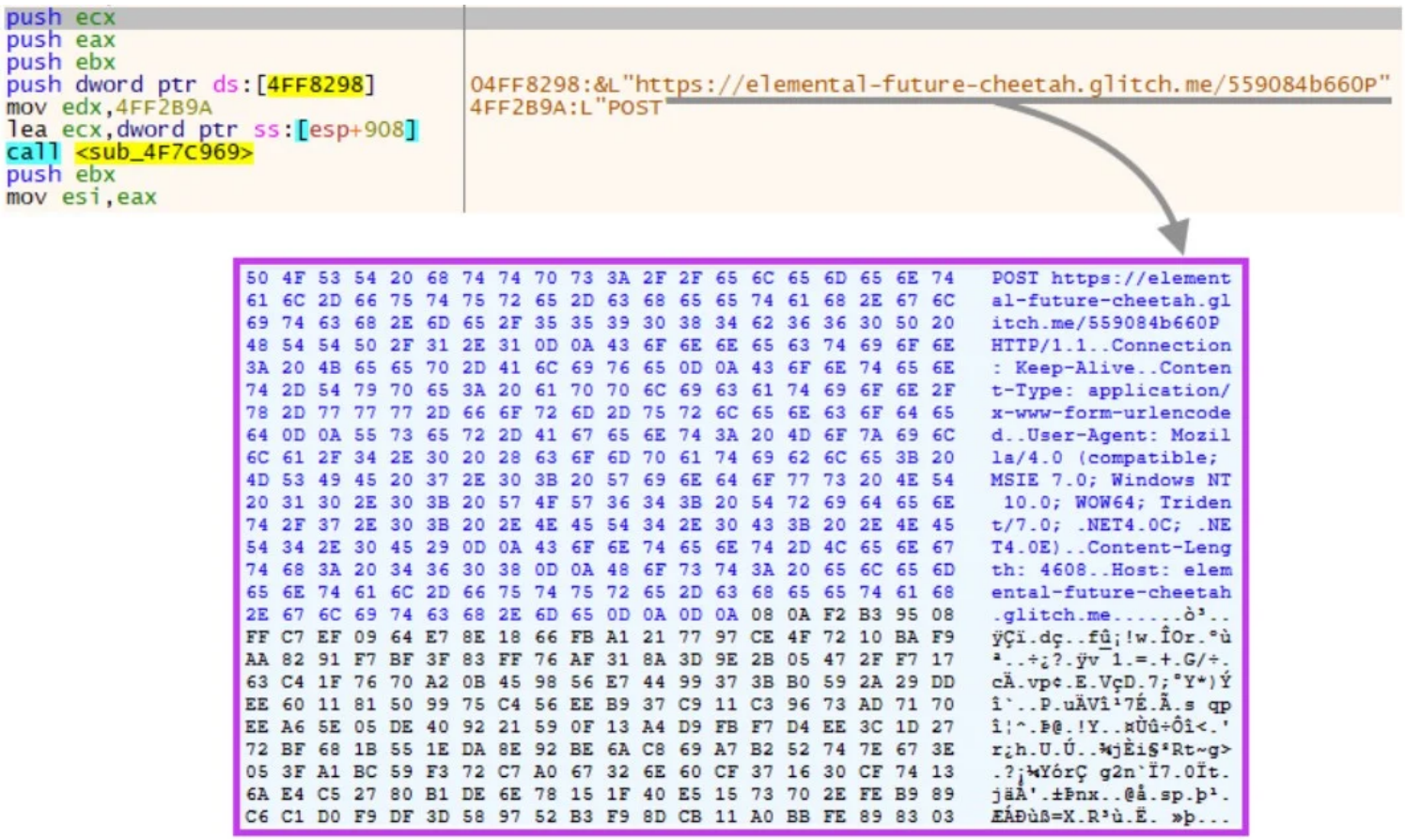
Payload injected and unpacked into memory

Source: Netskope

The malware collects network adapter information, computer name, username, enumerates system directories and files, checks the list of running processes.

Once that basic data is gathered, the backdoor compiles everything into a single packages and encrypts the content before it's sent to the C2 server.

This server is hosted on Glitch, a cloud hosting and web development collaboration service that is frequently abused for malicious purposes.



Backdoor communicating with a Glitch-hosted C2
Source: Netskope

By using a legitimate cloud hosting service for C2 communication, the actors further reduce the chances of being detected even when network traffic monitoring tools are deployed.

Although Glitch took down the C2 URLs identified and reported by Netskope researchers, it's unlikely that this will stop APT32 from creating new ones using different accounts.

For the complete list of the indicators of compromise from this campaign, you may check this GitHub repository.