APTualizator: The targeted malware patching Windows

An analysis performed by the CSIRT-SCC together with the Innovation and Labs team of ElevenPaths.

Telefónica CYBER SECURITY UNIT

elevenpaths.com

A report issued by the team of researchers from the CSIRT-SCC, in collaboration with ElevenPaths.

By the end of June 2019, we assisted to an incident were a high number of computers had started to reboot abnormally. In parallel, Kaspersky detected a file called *swaqp.exe*, which apparently was not available on any antivirus aggregator or public platform at that time. We tried to determine if such file may have caused those reboots and if we were actually facing a malware threat.

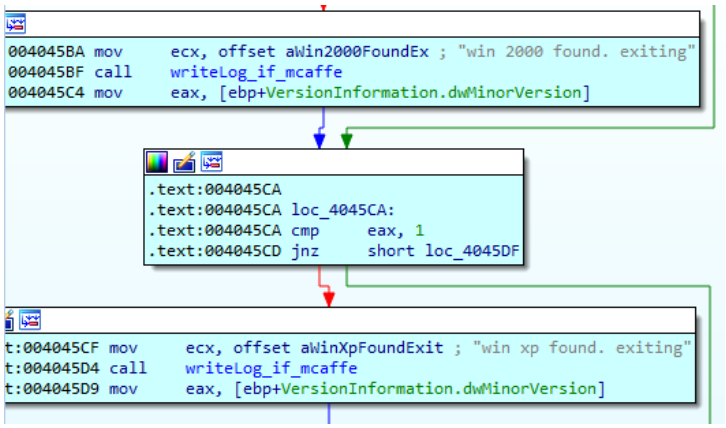
It caught our attention that in a first quick analysis we noticed that the sample downloaded the KB3033929 legitimate security update for Windows, although from an unofficial server. In other words: it installed the legitimate file (signed by Microsoft) from an unofficial server. It is not a typical malware behavior for two reasons:

- Malware creators usually develop their artifacts by minimizing additional dependencies (libraries) that might not be included in potential victims' computers.
- Malware is rarely interested in updating computers, still less in attempting to update them with any patch. It is not the usual behavior in the context of a potential malware sample.

Following this, we began to investigate.

1. Windows update KB3033929

The code of *swaqp.exe* checks if the system has an earlier version of Windows 7 on the desktop and Windows Server 2008 R1 on server version. In such a case, code execution process will terminate. The mentioned security patch is only available for these versions, so it makes clear its goal with that action.



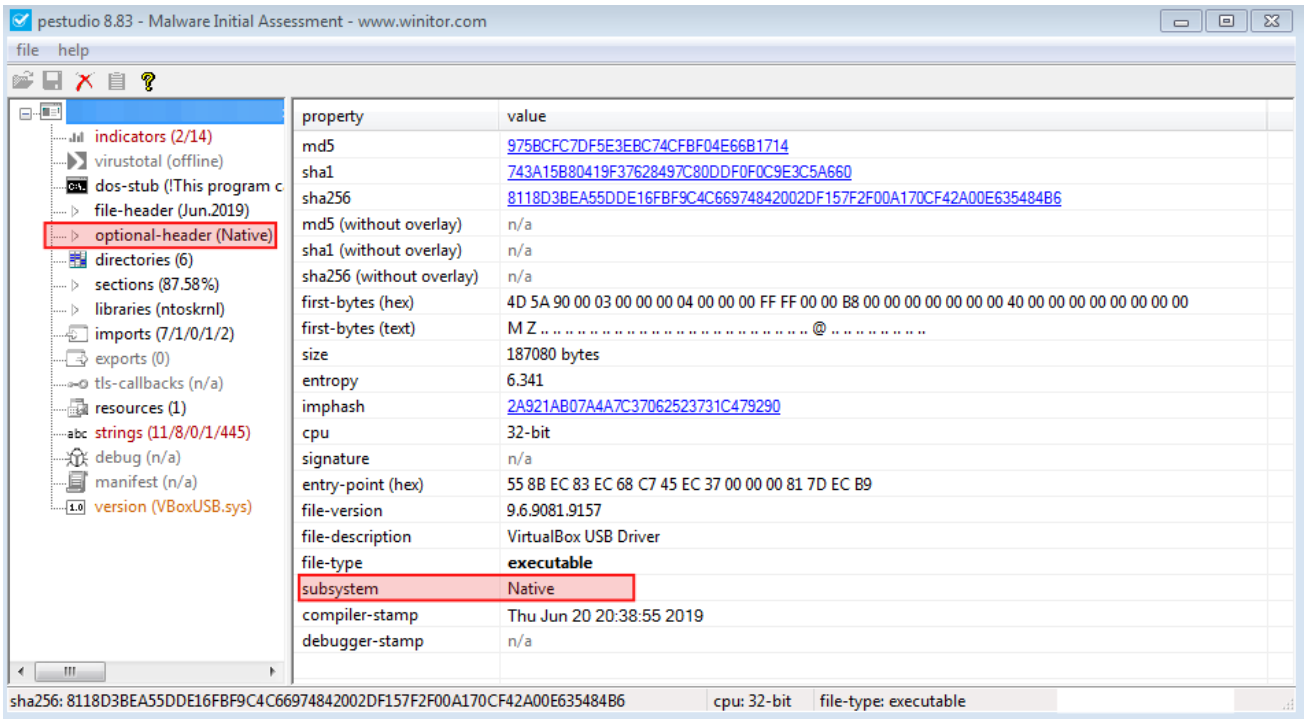
2. Downloading a rootkit

As the binary progress in its execution, we discover that it triggers a log where the actions carried out are described. This *log.txt* (which may be found in the same folder as the executable and is very likely to have been forgotten by the attacker in the final sample) is completed with personal debugging messages that would have helped the malware creator to follow its execution over the development phase, or that would have been used to detect execution flaws on the target computer. In the following image you can see an example of the log messages that we found:

6D	61	69	6E	20	69	73	20	4E	55	4C	4C	00	00	57	4F	52	4B
47	52	4F	55	50	00	00	00	50	72	6F	64	75	63	74	4E	61	6D
65	00	53	4F	46	54	57	41	52	45	5C	4D	69	63	72	6F	73	6F
66	74	5C	57	69	6E	64	6F	77	73	20	4E	54	5C	43	75	72	72
65	6E	74	56	65	72	73	69	6F	6E	00	00	00	00	63	70	75	00
30	00	00	00	6C	64	72	00	72	65	73	70	6F	6E	63	65	20	6E
6F	74	20	4E	55	4C	4C	00	00	00	72	65	73	70	6F	6E	63	65
20	4E	55	4C	4C	00	00	00	63	32	20	64	72	20	72	65	73	70
6F	6E	63	65	20	6F	6B	00	00	00	4D	5A	00	00	63	32	20	64
72	20	4D	5A	20	6F	6B	00	63	32	20	64	72	20	6E	6F	74	20
4D	5A	00	00	00	00	64	6F	77	6E	6C	6F	61	64	69	6E	67	20
62	6F	74	2E	2E	2E	00	00	00	00	00	00	41	42	43	44	45	46

m	a	i	n		i	s		N	U	L	L			W	O	R	K
G	R	O	U	P				P	r	o	d	u	c	t	N	a	m
e		S	O	F	T	W	A	R	E	\	M	i	c	r	o	s	o
f	t	\	W	i	n	d	o	w	s		N	T	\	C	u	r	r
e	n	t	V	e	r	s	i	o	n					c	p	u	
0				l	d	r		r	e	s	p	o	n	c	e		n
o	t		N	U	L	L				r	e	s	p	o	n	c	e
	N	U	L	L				c	2		d	r		r	e	s	p
o	n	c	e		o	k				M	Z			c	2		d
r		M	Z		o	k		c	2		d	r		n	o	t	
M	Z							d	o	w	n	l	o	a	d	i	n	g	
b	o	t	.	.	.									A	B	C	D	E	F

On the log messages, the words "rootkit" and "driver" can be seen. Indeed, when the KB is downloaded, more connections against the attacker's IP continue to be established. Once one of the objects received is decrypted, we find an executable. The field 'subsystem' presents the value 'Native'. This suggests that it is a driver from the system executed at the kernel level, which in turn would indicate that this file is in charge of hiding the infection on the system.



For the executable downloaded from the C&C to run at the kernel level, it will be installed as a driver of the operating system. As we know, on Windows this involves that the binary must be signed by one of the Certification Authorities allowed on the operating system to be executed as a Kernel, thereby offering certain guarantees to the critical software triggered on the system. Driver signature and authorization system on Windows is very demanding in recent times.

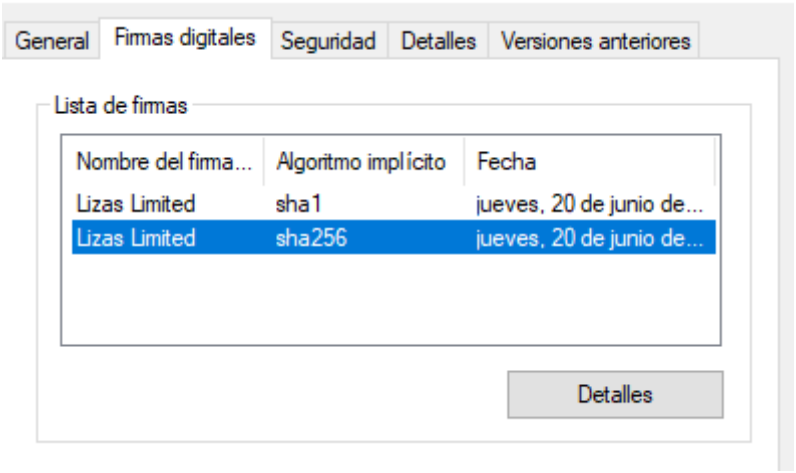
3. Why would it update?

So far, we have a malware that performs legitimately an update on the system and downloads what seems to be a driver (that must be signed to be installed). Why would the attacker update the operating system of a victim? To answer this question, we need to understand the changes included in this patch and how it is related to the rootkit installation.

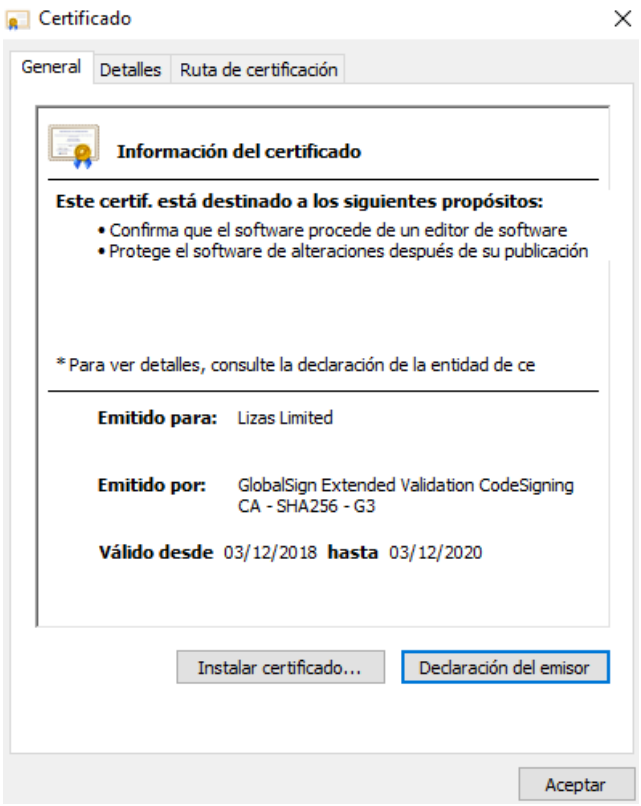
If we go over the details of the certificate used to sign this executable, we can see that SHA256 as a hash algorithm is used. Here is where we start to infer the malware behavior. KB3033929 is a Microsoft update issued in 2015, which is in turn an update of a patch released by the end of 2014. Windows 8 versions or later support signature verification with SHA256, but Windows 7 or Windows 2008 R2 do not. Microsoft had to issue this patch to continue supporting these versions (Windows 7 and 2008 R2), while the earlier ones (Vista, 2003, XP...) remain unable to verify those signatures created with hashes SHA256, and the later ones have natively this feature.

Therefore, the attackers apply the patch KB3033929 so that the verification of the signed driver may be valid. We infer that the attackers only had that signature possibility, so they had to adapt the victim to the malware (by updating the capacities of the operating system) and not the other way around.

For this purpose, we check the driver signature:



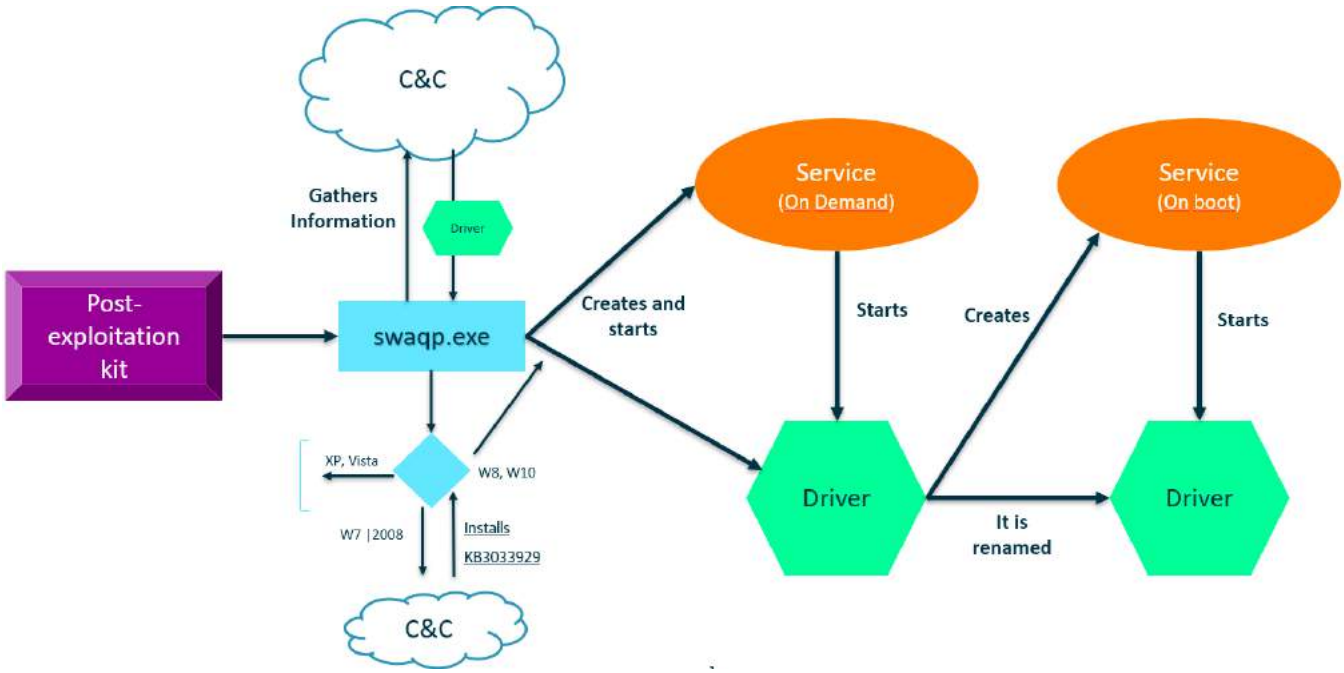
Surprisingly, it is signed with SHA256, but with SHA1 as well. This is a usual practice of Windows updates, for instance, for some time now, for the updates to work on Windows 7, 2008 R2 and the remaining systems. But in the case of updates, SHA1 hashes are signed by certificates different to SHA256 hashes in the same sample. In the case of this malware, both hashes SHA1 and SHA256 are signed by a SHA256 certificate.



This is a little strange action performed by the attacker. We infer that it only had a single certificate SHA256, so needing to update the system for the target Windows to verify the validity. The fact that it was signed by SHA1 may constitute a simple previous test performed by the attacker.

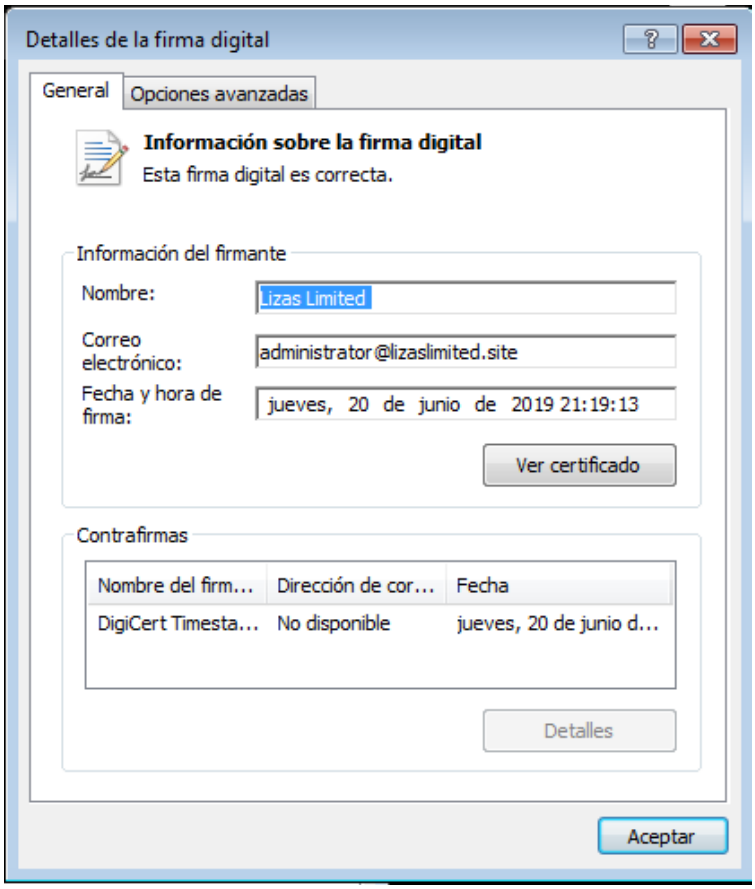
The rootkit is downloaded into the folder C:\WINDOWS\SYSTEM32\Drivers and a service at the kernel level referring to the file .sys -which is named as the service- is created. The name given to this rootkit is made up from parts of names given to other drivers located in the same folder, so detecting the file at first sight might not be trivial.

In order to make sure that a full update of the DLL is performed, and the patch is applied, the attackers forced the computer to restart following the patch installation.



4. Certificate and digital signature

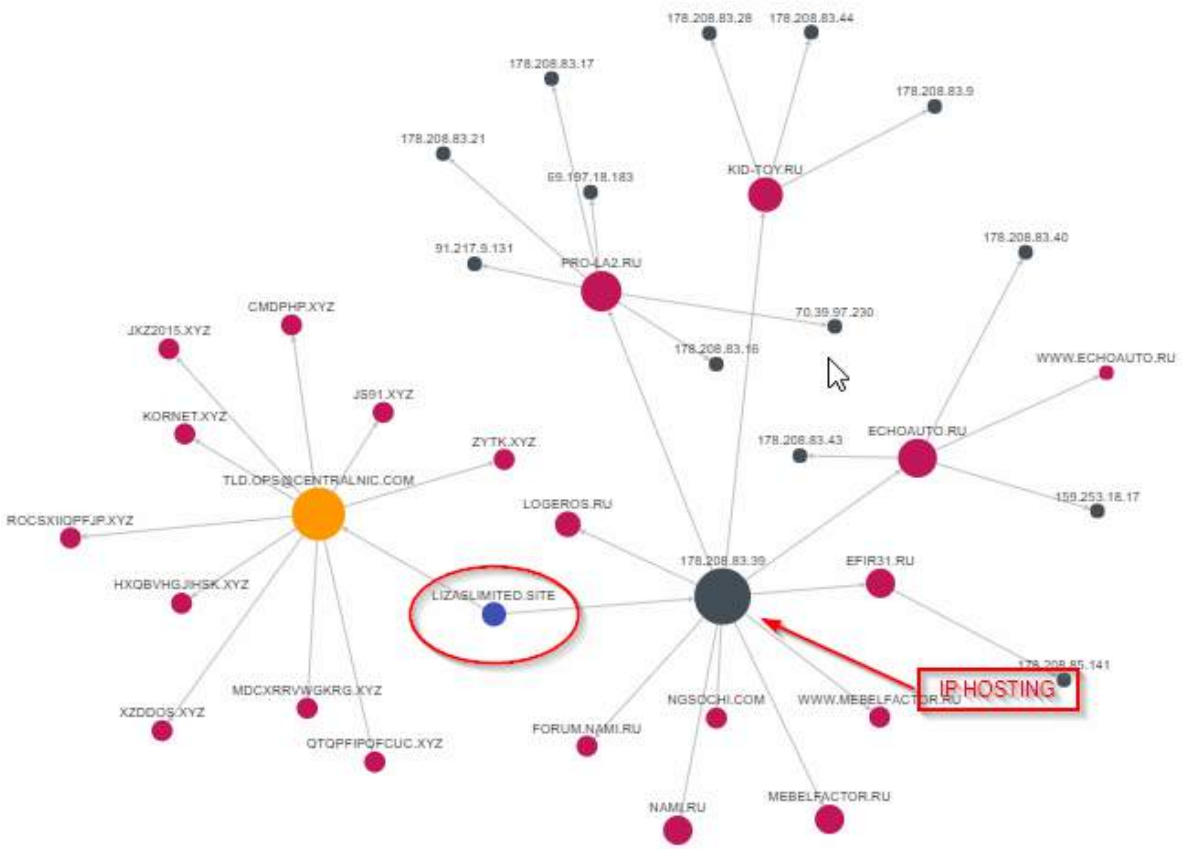
The sample was signed on 20 June 2019 with a certificate Lizas Limited issued by GlobalSign.



According to the information provided by the digital signature, we can see that **Lizas Limited** is a company located in Manchester (United Kingdom).

EMAILADDRESS=administrator@lizaslimited.site, CN=Lizas Limited, O=Lizas Limited, STREET=4 Herevale Grange, L=Worsley, ST=Greater Manchester, C=GB, OID.1.3.6.1.4.1.311.60.2.1.3=GB, SERIALNUMBER=06794337, OID.2.5.4.15=Private Organization	CN=GlobalSign Extended Validation CodeSigning CA - SHA256 - G3, O=GlobalSign nv-sa, C=BE Serial: 4d1473a40ace93522a2abf3b	12/03/2018 15:18:28 12/03/2020 15:18:28	1D:9A:5A:EC:BB:BC:59:23:52:AB:C2:EE:B0:97:09:24 11:14:E9:7C:21:0A:8A:EC:35:7C:F6:43:D7:FE:F5:CC:1A:1F:84:DA

However, there is no public information indicating that this company has to do with the domain *lizaslimited.site*, which is registered and hosted in Russia. Currently, the website *lizaslimited.site* do not provide relevant information.



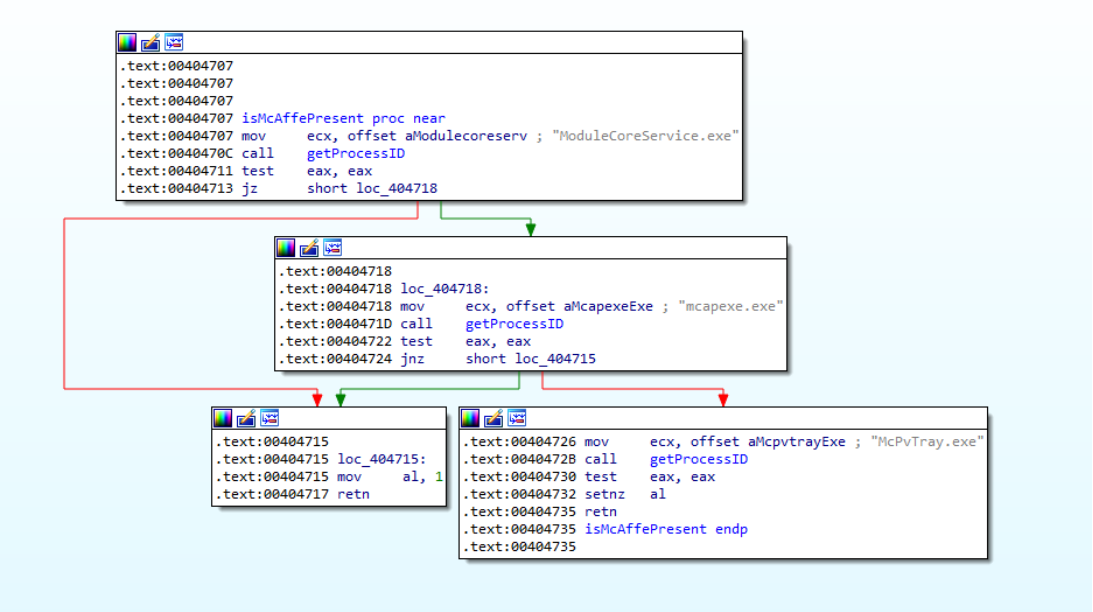
We may be facing a case of impersonation, where the identity of a legitimate company has been stolen before **GlobalSign**. There are evidences that this behavior is not new, since more old samples of malicious malware signed by **Lizas Limited**, with code signing certificates and issued by **Sectigo**, were detected.

5. References to McAfee

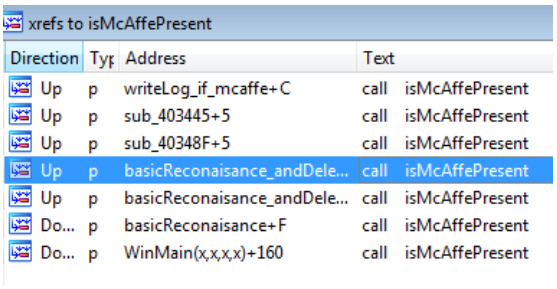
Over the sample execution there are constant references to McAfee that make it change the malware behavior depending on whether antivirus processes are running or not. This is the main antivirus engine installed in the affected

computers. A significant part of the malware behavior is contingent upon the existence of this antivirus on the computer. This might suggest a targeted attack.

One of the behaviors that are contingent upon the existence of McAfee is the creation of the log file previously mentioned. This log file is only written if the victim has not such antivirus already installed on the computer.



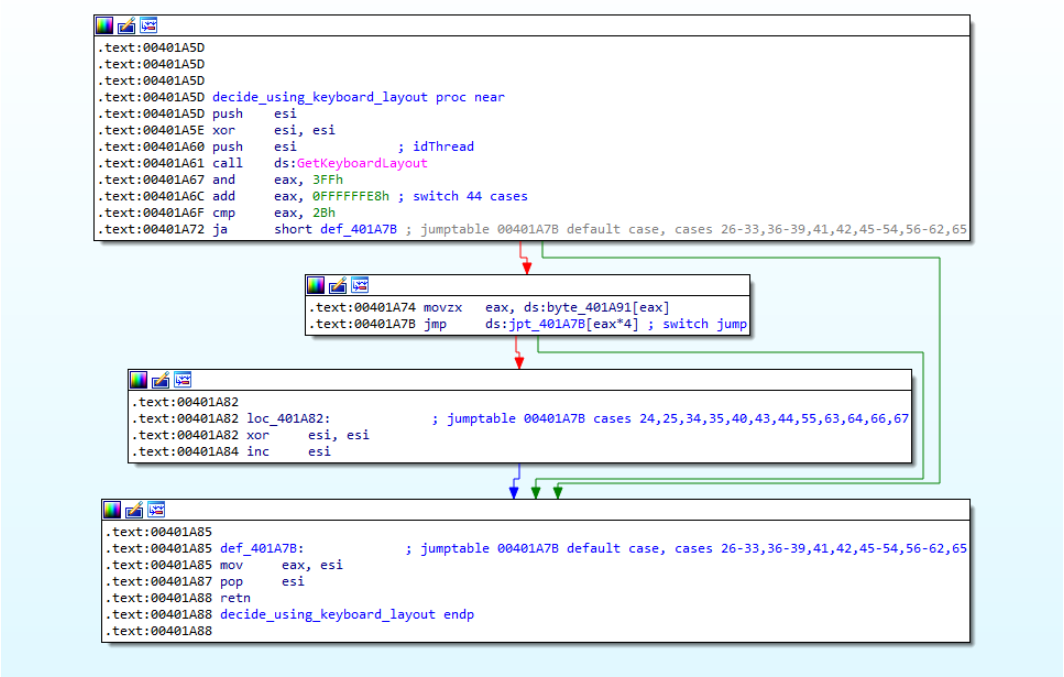
As an example, in the first line of the following image we can see a reference to a function that we have renamed as *writeLog if mcafee*. We found at least seven more references or internal verifications related to the existence of McAfee.



6. Potential attribution by country

Moreover, we found a code snippet where the sample checked the language of the victim's keyboard, according to which they would go ahead with the infection or not. This is quite usual, malware creators usually do so; since in case of execution on their own computer by mistake, they will not be infected by the malware. Other cases may be very targeted at some countries where it will only be executed for a specific region.

Nevertheless, the case found here is a little bit different. Instead, we found a range of up to 43 languages that, through consecutive language identifiers, would be freed from the infection.



Those countries that would not be affected -and among which the presumably threat source is located- are the ranges between 0x18 and 0x43. Russia is precisely within the list of these 43 countries, the country that we linked to the signature **Lizas Limited**.

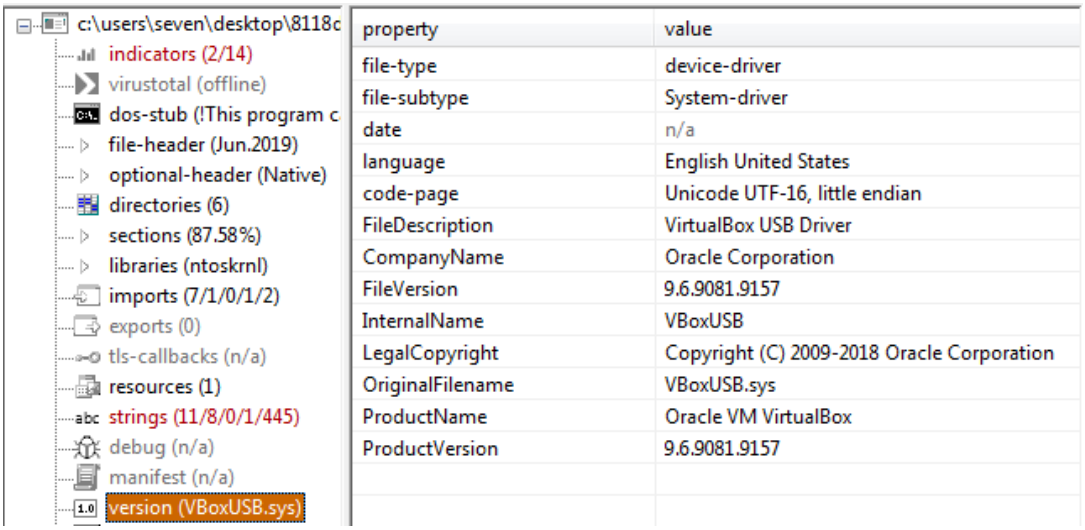
The list of language identifiers is available on https://docs.microsoft.com/en-us/windows/desktop/intl/language-identifier-constants-and-strings.

This may suggest that:

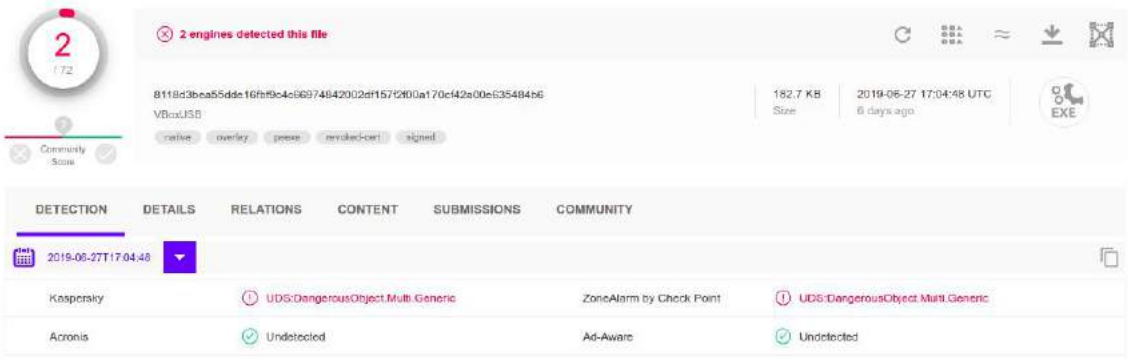
- The authors are within the range, and the remaining ones were included to make unclear the authorship of the attack.
- The attack was **targeted**, since if it had been an undefined-victim attack, it would make no sense to have excluded so many potential infections (up to 43 different language identifiers would be excluded from the attack). It is important to point out that the only relationship between these identifiers is that they are consecutive. In other words: they do not constitute a close group neither geographically nor politically.

7. The driver

In the description of the file .sys it may be seen how the attackers have used misinformation on Oracle with the aim of going unnoticed:



This driver was uploaded to VirusTotal on 27 June 2019 with a very low ratio of static detection by two engines. Soon after, more engines joined the detection.

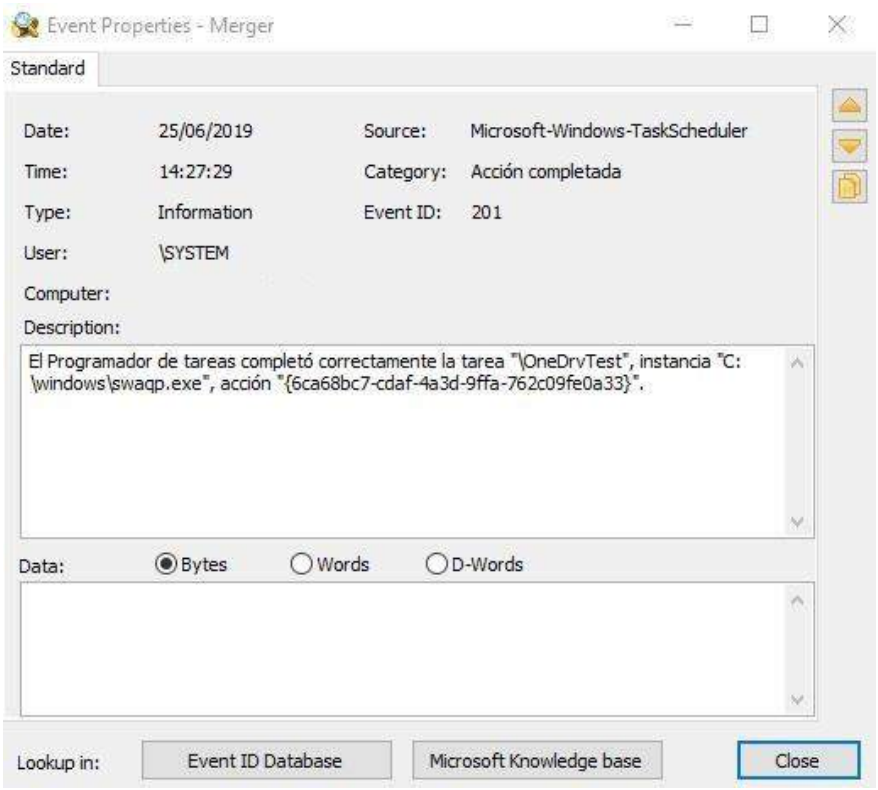


However, as we have mentioned before, while searching for files with the signature **Lizas Limited** on their certificate, we found files uploaded since April 2019. In particular, we found a file named *rootkit.sys* that was detected by most of the engines on 18 May. It would have been more useful to take preventive measures against the signature **Lizas Limited** rather than detect files by other features.

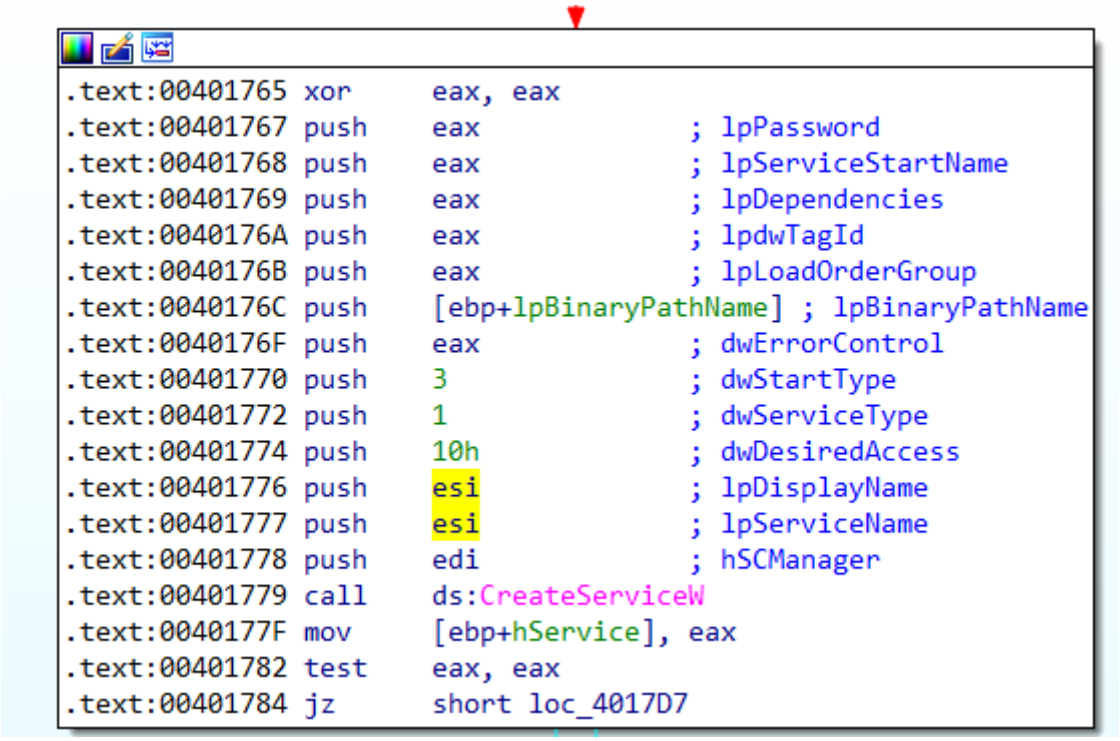
For our part, since we learnt about the existence and use of the signature, we requested its revocation. That way, this signature is no longer accepted. We can see more references to similar samples at least since 25 April. It also appeared on this Twitter thread, on 30 May: references and even images of the Control Panel from a quite similar sample.

8. Persistence

The sample swaqp.exe did not suggest any Indicator of Compromise related to the persistence on those machines that executed it. However, the forensic analysis performed over the infected computers showed that the attackers accessed remotely the computers and created tasks programmed to launch the sample:



Nevertheless, the reason for creating the programmed task is to be able to restart the malware in case the mentioned Windows updates had been successfully installed, so they were not persistence techniques as such. Consequently, and considering the attack formula and the artifacts used, we identified this executable as a dropper/installer as a non-persistent threat aimed to create a malicious service, and without persistence as such.



```
.text:00401765 xor     eax, eax
.text:00401767 push    eax             ; lpPassword
.text:00401768 push    eax             ; lpServiceStartName
.text:00401769 push    eax             ; lpDependencies
.text:0040176A push    eax             ; lpdwTagId
.text:0040176B push    eax             ; lpLoadOrderGroup
.text:0040176C push    [ebp+lpBinaryPathName] ; lpBinaryPathName
.text:0040176F push    eax             ; dwErrorControl
.text:00401770 push    3               ; dwStartType
.text:00401772 push    1               ; dwServiceType
.text:00401774 push    10h             ; dwDesiredAccess
.text:00401776 push    esi             ; lpDisplayName
.text:00401777 push    esi             ; lpServiceName
.text:00401778 push    edi             ; hSCManager
.text:00401779 call    ds:CreateServiceW
.text:0040177F mov     [ebp+hService], eax
.text:00401782 test    eax, eax
.text:00401784 jz      short loc_4017D7
```

Regarding driver persistence, as you can see on the image, the types of StartType and ServiceType suggest that it is manually started (SERVICE_DEMAND_START = 3) and that it is a kernel driver-related service (SERVICE_KERNEL_DRIVER = 1). Albeit later, the driver itself created a new copy of the driver with different name and homonymous service, starting along with the system. The first installed driver and service were deleted over this process. This way, the driver achieved persistence.

Therefore, the main goal of *swaqp.exe* is to install a set of tools on the infected computer, among which there is a rootkit signed with a certificate SHA256, so it forces the target operating system to reboot. In next reports we will discuss the remaining artifacts entered into the infected systems.

9. IOCs

- 45.227.252.54
- 139.60.160.6
- 185.55.243.15
- 92.223.73.11
- **Mutex:** system32_host_service
- **Mutex:** system32_mutant_service
- ***Swapqp.exe:*** 6c865c6864c8d7/efe1002b/3fc1ddda1a4a35/d3023/c6bfcefb6305/e/45c41
- ***Driver:*** 8118d3bea5dde16fbf9c4c669/4842002df15/f2f00a1/0cf42a00e635484b6

Other hashes signed by the same certificate:

- c0cff/ff5663c/c9c6c69dc645b86222b/4ef2dc5d2b2633a6aa/9d4959d/d2b

- 8118d3bea55dde16fbf9c4c669/4842002df15/f2f00a1/0cf42a00e635484b6
- c554148084d05195a08bf00e3331beb85dc362/8/d88bdb/a8088f1336131d91
- b6f156e4a9bd40/0d0e502b94ec143e1e349cfff5b10/9/fae8e36bface8605f
- fb112fc/6835d02f0ec2f830b0cd1bb8/e1/e03cb3c/bff66e/cbf485b6af71f

-----BEGIN CERTIFICATE-----
MIIF1zCCBL+gAwIBAgIMTRRzpArOk1IqKr8/MA0GCSqGSIb3DQEBCwUAMG4xCzAJ
BgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iYWx1aWduIG52LXNhMUQwQgYDVQQDEztH
bG9iYWx1aWduIEV4dGVuZGVkIFZhbGlkYXRpb24gQ29kZVNpZ25pbmcgQ0EgLSBI
SEEyNTYgLSBHMzAeFw0xODEyMDMxNTE4MjhaFw0yMDEyMDMxNTE4MjhaMIH/MR0w
GwYDVQQPDBRQcml2YXRlIE9yZ2FuaXphdGlvbjERMA8GA1UEBRMIMDY3OTQzMzcx
EzARBgsrBgEEAYI3PAIBAxMCR0IxCzAJBgNVBAYTAkdCMRswGQYDVQQIExJHcmVh
dGVyIE1hbmNoZXN0ZXIxEDAOBgNVBAcTB1dvcnNsZXkxGjAYBgNVBAkTEQgSGVy
ZXZhbGLgR3JhbmdlMRYwFAYDVQQKEw1MaXphcyBMaW1pdGVkMRYwFAYDVQQDEw1M
aXphcyBMaW1pdGVkMS4wLAYJKoZIhvcNAQkBFh9hZG1pbmlzdHJhdG9yQGxpemFz
bGltaXRlZC5zaXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAl05B
EUfpErPpREHoq1M+//N638+NF6iZE/I/S+0FBNoX1p9OcMXD+ZIDfnWZSHPtP0wc
4UpsZGEEdboY5dEIFISCUj/KmoAJI/k3JHMc25eHIQIPU/jxbH8zlb5Ku/RuJVs2
Q0dkfiSG/emHres+dIKXjMjQixWZxOEtOdX2X/cM5ybUECi62LY1WuO6Kz2/nj/D
/9m9hC0YAdmBL4liaP8QB50tkm5gGH4I8rupwFrvwPou1Yq/66RQcqnRw+Y4WiQI
HEM9rw366lsPhMvUfIDkr03zgoL/+x0mieMq3SdF55Vakv1dIMP+Rkf0IBSuwSqL
jDFAntpnioXWiW/fGQIDAQABo4IB4TCCAd0wDgYDVR0PAQH/BAQDAgeAMIGgBggr
BgEFBQcBAQSBkzCBkDBOBggrBgEFBQcwAoZCaHR0cDovL3NlY3Vy5snbG9iYWxz
aWduLmNvbS9jYWNlcnQvZ3NleHRlbmRjb2Rlc2lnbnNoYTJnM29jc3AuY3J0MD4G
CCsGAQUFBzABhjJodHRwOi8vb2NzcDIuZ2xvYmFsc2lnbi5jb20vZ3NleHRlbmRj
b2Rlc2lnbnNoYTJnMzBVBgNVHSAETjBMMEEGCSsGAQQBoDIBAjA0MDIGCCsGAQUF
BwIBFiZodHRwczovL3d3dy5nbG9iYWxzaWduLmNvbS9yZXBvc2l0b3J5LzAHBgVn
gQwBAzAJBgNVHRMEAjAAMEUGA1UdHwQ+MDwwOqA4oDaG1Gh0dHA6Ly9jcmwuZ2xv
YmFsc2lnbi5jb20vZ3NleHRlbmRjb2Rlc2lnbnNoYTJnMy5jcmwwKgYDVR0RBCMw
IYEfYWRtaW5pc3RyYXRvckBsaXphc2xpbWl0ZWQuc2l0ZTAfBgNVHSUEGDAKBggr
BgEFBQcDAzAdBgNVHQ4EFgQUFeavK8qKjtluSAQeuEeIY9/HKKIwHwYDVR0jBBgw
FoAU3CxYLCpvNS2feZWoSF3EbI5v1/kwDQYJKoZIhvcNAQELBQADggEBAMY/uhfn
ssh6Nc/9c11lAp+QasEyN/juRv6GUWwfy8sXNAkDPGgR/aan8s+khjVpH2iapzut
XG0f9qtg9kGAfnSHwnEEA/Cv3Z5xmHXZppFOhsc1nd4pW3MNZchlCYqg3um09hdA
Cb3MtefroAvLACdJjFIR8CB8ugBPEgqQhudYd58/PSHcv1V/eA/QdCOPIL/WGvb6
sNFYuV1d0GGG5eeHVqbqeDtyArfoVjHbwQ3EDRIS3dB8dpw1u+EAtRO93b9f6mYh
Yo3dcFafk/vXONIWW2L2iZgd68rsoZup3cB8S61vFWCoJlwwSkXUo8cLz/2mz4WX
OoqoUS1In5KbP1I=
-----END CERTIFICATE-----

About ElevenPaths

At ElevenPaths, Telefónica Cyber Security Unit, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology.

We're always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

About CSIRT-SCC

The Computer Security Incident Response Team (CSIRT) SCC (Security Cyberoperations Center) is made up of a team of professionals specialized in the various disciplines related to incident response: management, forensic analyses and malware analyses.

Furthermore, the CSIRT-SCC is supported by the remaining security areas of the SOC (security device management, threat hunting...) and the latest technologies available, as well as by the whole team of ElevenPaths.