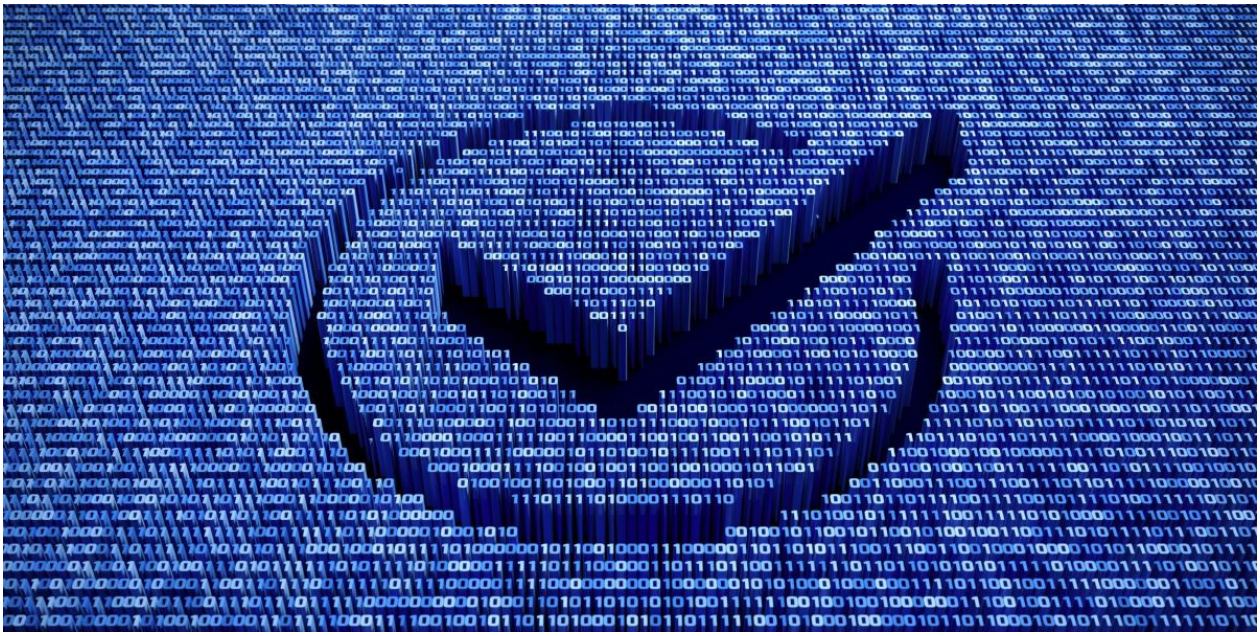
Ransomware and wiper signed with stolen certificates



Introduction

On July 17, 2022, Albanian news outlets reported a massive cyberattack that affected Albanian government e-services. A few weeks later, it was revealed that the cyberattacks were part of a coordinated effort likely intended to cripple the country's computer systems. On September 10, 2022, Albanian local news reported a second wave of cyberattacks targeting Albania's TIMS, ADAM and MEMEX systems – the latter two systems critical for law enforcement – reportedly using the same attack type and by the same actors.

Around the same time, we identified ransomware and wiper malware samples resembling those used in the first wave, though with a few interesting modifications that likely allowed evasion of security controls and better attack speeds. Chief among those changes are the embedding of a raw disk driver, providing direct hard disk access inside the malware itself, modified metadata, and the use of Nvidia's leaked code signing certificate to sign the malware.

So, what's new in this blogpost?

- We compare the first and second waves of ransomware and wiper malware used to target Albanian entities and detail connections with previously known ROADSWEEP ransomware and ZEROCLEARE variants.
- The threat actors used certificates from Nvidia and Kuwait Telecommunications Company to sign their malware; the former was already leaked, but we're not sure how they got their hands on the latter.
- We identified potential cooperation between different attack groups speaking different languages, and the possible use of AnyDesk as an initial entry point to start the ransomware/wiper infections.
- The changes implemented to automate and speed up wiping in the second wave of attacks are reminiscent of the notorious Shamoon wiper attacks in the Middle East.

Wiper and ransomware, comparing wave 1 and wave 2

Below, we compare and discuss the differences between the wave 1 and wave 2 ransomware and wiper malware.

Initial Infection – traces of cooperation between different attack groups and use of AnyDesk utility

Although we weren't able to identify the initial entry point of the threat actor in the analyzed intrusion, a few days after the second wave wiping activities, we noticed underground chatter about someone having access to an AnyDesk account at another non-governmental but significant Albanian entity, and suggestions for Persian-speaking hackers to use it for deploying ransomware or wiper malware. This may increase the likelihood that the initial entry point for wave 2 is through legitimate remote access software such as AnyDesk, especially since we know that the wave 2 wiper modifications included automatic execution upon driver installation only – potential need for urgency due to the limited time/access window. The attackers and access provider seemed to belong to different attack groups and spoke different languages.

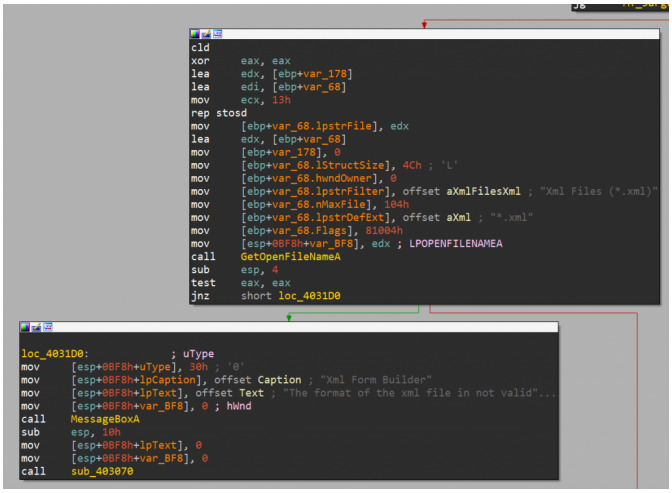
The ransomware – use of Kuwait Telecommunications Company signing certificate

MD5	96eabcc77a6734ea8587599685fbf1b4
SHA1	6a36962709abbfc1f88f87e7fe88a417302bfe43
SHA256	8ad01b028e6aa711d26879d346a7bef82516e372e0f14e8e69db6aef0f25d992
Imphash	653ee44c85bc91d12ec33dfed8056c27
Link time	Wed Jul 06 21:30:41 2016
File type	32-bit executable
Compiler	MinGW-w32 gcc
File size	45.48 KB
File name	PdftoDoc.exe

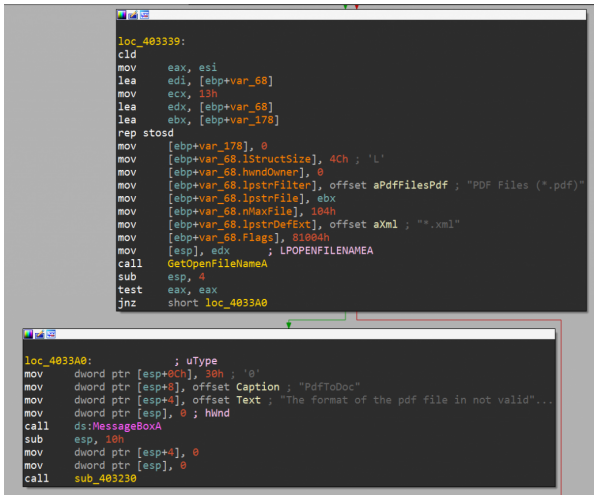
This second wave sample has the same signing certificate parameters as the first wave sample, which is related to Kuwait Telecommunications Company. It's unclear how the threat actor was able to sign its malware using Kuwait Telecommunications Company's certificate, but we suspect it was stolen. As of the date of this publication, the certificate is no longer valid and has been revoked.

Name	Kuwait Telecommunications Company KSC
Issuer	DigiCert SHA2 Assured ID Code Signing CA
Valid From	12:00 AM 08/11/2019
Valid To	12:00 PM 08/15/2022
Valid Usage	Code Signing
Algorithm	sha256RSA
Thumbprint	55D90EC44B97B64B6DD4E3AEE4D1585D6B14B26F
Serial Number	01 FD D0 93 F6 50 87 F4 E9 AE 11 ED 65 0D 83 E8

After the initial execution, the wave 2 ransomware checks for any six arguments (or more) supplied by the threat actor, as opposed to the wave 1 sample that checks for five arguments or more – a small modification that assists in defense evasion. Nevertheless, the intrusion analysis conducted on one of the affected machines indicates that in wave 2 the threat actor did not use a BAT file to invoke the ransomware while supplying seven digits similar to wave 1, but instead invoked the wave 2 ransomware immediately from the command line using six zeroes: "000000". If ransomware execution fails because the correct arguments are not supplied, the wave 2 sample displays a different message from that of wave 1; the wave 2 message resembles an error message displayed by a PDF to DOC converter.



Wave 1 sample – messaging after failed execution



Wave 2 sample – different messaging after failed execution

The wave 2 ransomware sample continues execution and checks for the mutex *Screenlimitsdevices#77!;*, a value that differs from the wave 1 sample's mutex: *abcdefghijklmnoklmnopqrstuvwxyz01234567890abcdefghijklmnopqrstuvwxyz01234567890*

Although we call this malware ransomware based on its behavior, the encrypted files are, in fact, unrecoverable. When comparing wave 2 ransomware samples to wave 1, we notice that both have the same , and both use CreateFile and WriteFile APIs to overwrite files. During the process of execution, wave 2 ransomware attempts to decrypt and execute embedded scripts, malware settings or API function names. The encryption algorithm used is RC4 in both wave 1 and wave 2. However, the RC4 key for decryption in wave 2 has been changed in another attempt to evade detection.

- Wave 1 RC4 key: *8C E4 B1 6B 22 B5 88 94 AA 86 C4 21 E8 75 9D F3*
- Wave 2 RC4 key: *F0 B4 ED D9 43 F5 C8 43 C9 D0 A2 4F 22 9B BC 3A*

It's worth noting that in both waves, the RC4 decryption method uses CryptoAPI (CryptDecrypt) instead of the usual substitution box method. The intrusion we analyzed in wave 2 indicates that the ransomware was probably deployed over the internal network, possibly from another compromised machine. This is reinforced by the fact that we didn't see anything else dropped or executed before the ransomware execution, and the ransomware executable name was randomly generated, potentially by the tool the threat actor used to deploy it over the network (e.g., *Mellona.exe*).

Despite all the changes made in the wave 2 ransomware, the ransom notes remained the same and included political messaging that reflects the geopolitical tensions between Albania and Iran.

Ransom note in both wave 1 and wave 2 ransomware

The wiper – use of Nvidia signing certificate

MD5	64cb923be15ae255b82e7ebcf24ccfc5
SHA1	e1b8b72fbd1e3b9bbf8bebd2e14a3f2e071c6048
SHA256	d8ec8ec8dfa582c44e81b8a7fcc44defc3d2fa658f75fa495124aedc3b0db367
Imphash	81CA8B811412284938148FC4F2A76C09
Link time	0x6319C758 (Thu Sep 08 03:43:36 2022)
File type	PE 64-bit
Compiler	Microsoft Visual C/C++
File size	174.00 KB
File name	DiskSnapshot.exe
Driver PDB path	c:\projects\rawdisk\bin\wnet\fre\amd64\rawdsk3.pdb
Driver key	B4B615C28CCD059CF8ED1ABF1C71FE03C0354522990AF63ADF3C911E2287A4B906D47D

Similar to the wave 2 ransomware sample, the threat actor made several modifications to the wave 2 wiper malware, probably to evade detection. The three main changes are:

- Modified malware signing
- Embedding of EldoS RawDisk driver inside the wiper malware
- Automatic wiping after driver installation command

Historically, in ZEROCLEARE and DUSTMAN incidents from 2019, the wiper malware and raw disk drivers were not signed and therefore could not directly access the raw disk for speedy data wiping. So, the wipers had to use a third-party loader such as TDL – a signed loader for unsigned drivers – to install the unsigned raw disk driver that allows the wiper malware to directly access the raw disk for wiping data using DeviceControl API methods. However, in the first attack wave targeting Albania, the threat actor signed the wave 1 wiper using the Kuwait Telecommunications Company certificate, thus removing the need for a third-party loader. The speed and automation improvements remind us of previous Shamoon operations in the Middle East.

Since the wave 1 wipers were exposed in July 2022, and likely to avoid static detections, the threat actor used Nvidia's leaked signing certificate to sign the wave 2 wiper in September 2022, again eliminating the need for a third-party loader for the raw disk driver.

Name	NVIDIA Corporation
Issuer	VeriSign Class 3 Code Signing 2010 CA
Valid From	2015-07-28 00:00:00
Valid To	2018-07-26 23:59:59
Algorithm	sha1RSA
Thumbprint	30632EA310114105969D0BDA28FDCE267104754F
Serial Number	14 78 1B C8 62 E8 DC 50 3A 55 93 46 F5 DC C5 18

In wave 1, the wiper malware expected to find the raw disk driver in the execution directory or in the system directory. The driver wasn't dropped by the wiper, and the threat actor likely dropped it using other means. Conversely, in wave 2 the threat actor embedded the signed raw disk driver in the wiper executable, dropped it and then installed it. In addition, the driver being used by the threat actor in wave 2 seems to copy metadata and a few functions from Microsoft's diskdump.sys crash dump driver[1] (version 10.0.19041.1682) as another means to avoid detections. The wiping activity starts automatically after the driver installation command; as opposed to the wave 1 wiper, where installation is one step and wiping execution is a second step.

Finally, for the most part, wave 1 and wave 2 wipers remained the same, including the reliance on the same authentication key to access the raw disk driver, and the use of the same DeviceControl API methods, but with one exception, as shown below. It's worth noting that the method IOCTL_DISK_GET_LENGTH_INFO is exclusive to all Persian-speaking APT wipers.

- Wave 1 wiper DeviceControl API methods:
  - IOCTL_DISK_GET_DRIVE_GEOMETRY_EX
  - IOCTL_DISK_GET_DRIVE_GEOMETRY
  - IOCTL_DISK_GET_LENGTH_INFO
- Wave 2 wiper DeviceControl API methods:
  - IOCTL_VOLUME_GET_VOLUME_DISK_EXTENTS (new method in wave 2; used in multiple instances)
  - IOCTL_DISK_GET_DRIVE_GEOMETRY
  - IOCTL_DISK_GET_LENGTH_INFO

Based on our telemetry, we suspect the infections are associated with law enforcement institutions in Albania. This targeting is consistent with the previous wave of cyberattacks affecting the Albanian government during the

July 2022 wave of cyberattacks.

Conclusions

In this publication, we discussed the changes made to the second wave of ransomware and wiper samples that targeted Albanian institutions to evade detection and inflict maximum damage.

Aside from the changes made to evade detection in wave 2, we suspect that the threat actors needed an automated and speedy wiper execution. In wave 2, the raw disk driver was embedded inside the malware and the wiping routine started immediately after driver installation, as opposed to the wave 1 procedure. This is reminiscent of Shamoon operations in the Middle East.

Finally, for defenders we can highlight two important elements from the intrusion and malware analysis presented here:

- Monitor for remote software activities such as AnyDesk for unauthorized use
- Always hunt and monitor for expired and/or leaked signing certificates as they can be used by threat actors to load and execute malware

Threat detection

The detection logic has been improved in all our solutions to ensure that our customers remain protected. We continue to investigate this threat using our Threat Intelligence and we will add additional detection logic once they are available.

Our products protect against this threat and detect it with the following names:

- HEUR:Trojan-Ransom.Win32.Agent.gen
- Trojan-Ransom.Win32.Gen.aghh
- Trojan-Ransom.Win64.Agent.dpf
- Trojan.Win32.Agentb.kzkj

Indicators of compromise

File hashes (malicious documents, Trojans, emails, decoys)

Ransomware

96eabcc77a6734ea8587599685fbf1b4	PdftoDoc.exe (wave 2)
bbe983dba3bf319621b447618548b740	GoXml.exe (wave 1)

Wiper

64cb923be15ae255b82e7ebcf24ccfc5	DiskSnapshot.exe (wave 2)
7b71764236f244ae971742ee1bc6b098	cl.exe (wave 1)

Driver

C7BE7E90F63DADA6CD541FA84880874B	$windir\$system32\drivers\disksdump.sys (originally known as diskdump.sys)

Signing certificates serial numbers

14 78 1B C8 62 E8 DC 50 3A 55 93 46 F5 DC C5 18	Nvidia certificate
01 FD D0 93 F6 50 87 F4 E9 AE 11 ED 65 0D 83 E8	Kuwait Telecommunications company certificate

[1] Original, legitimate driver's MD5 is 015caeec9148194054b5b1de64762a43