

ESET RESEARCH, UKRAINE CRISIS – DIGITAL SECURITY RESOURCE CENTER

IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine

ESET researchers uncover a new wiper that attacks Ukrainian organizations and a worm component that spreads HermeticWiper in local networks



ESET Research

01 Mar 2022 • 13 min. read

Share Article











 Digital Security
Progress. Protected.

APT Activity Report

IRAN-ALIGNED CYBERATTACKS:
RISE IN DISRUPTIVE OPERATIONS

(eset):research

[READ NOW](#)



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Accept all and close

[Manage cookies](#)

Update (March 4th, 2022): We fixed an error in the analysis of IsaacWiper. It uses the Mersenne Twister PRNG and not the ISAAC PRNG as initially written.

As the recent hostilities started between Russia and Ukraine, ESET researchers discovered several malware families targeting Ukrainian organizations.

- On February 23rd, 2022, a destructive campaign using HermeticWiper targeted multiple Ukrainian organizations.
- This cyberattack preceded, by a few hours, the start of the invasion of Ukraine by Russian Federation forces
- Initial access vectors varied from one organization to another. We confirmed one case of the wiper being dropped by GPO, and uncovered a worm used to spread the wiper in another compromised network.
- Malware artifacts suggest that the attacks had been planned for several months.
- On February 24th, 2022, a second destructive attack against a Ukrainian governmental network started, using a wiper we have named IsaacWiper.
- ESET Research has not yet been able to attribute these attacks to a known threat actor.

Destructive attacks in Ukraine

As stated in this ESETResearch [tweet](#) and [WLS blogpost](#), we uncovered a destructive attack against computers in Ukraine that started around 14:52 on February 23rd, 2022 UTC. This followed distributed denial-of-service (DDoS) [attacks against major Ukrainian websites](#) and preceded the Russian military invasion by a few hours.

These destructive attacks leveraged at least three components:

- HermeticWiper**: makes a system inoperable by corrupting its data
- HermeticWizard**: spreads HermeticWiper across a local network via WMI and SMB



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

at least five Ukrainian

r in a Ukrainian
e currently assessing
that it was seen in an

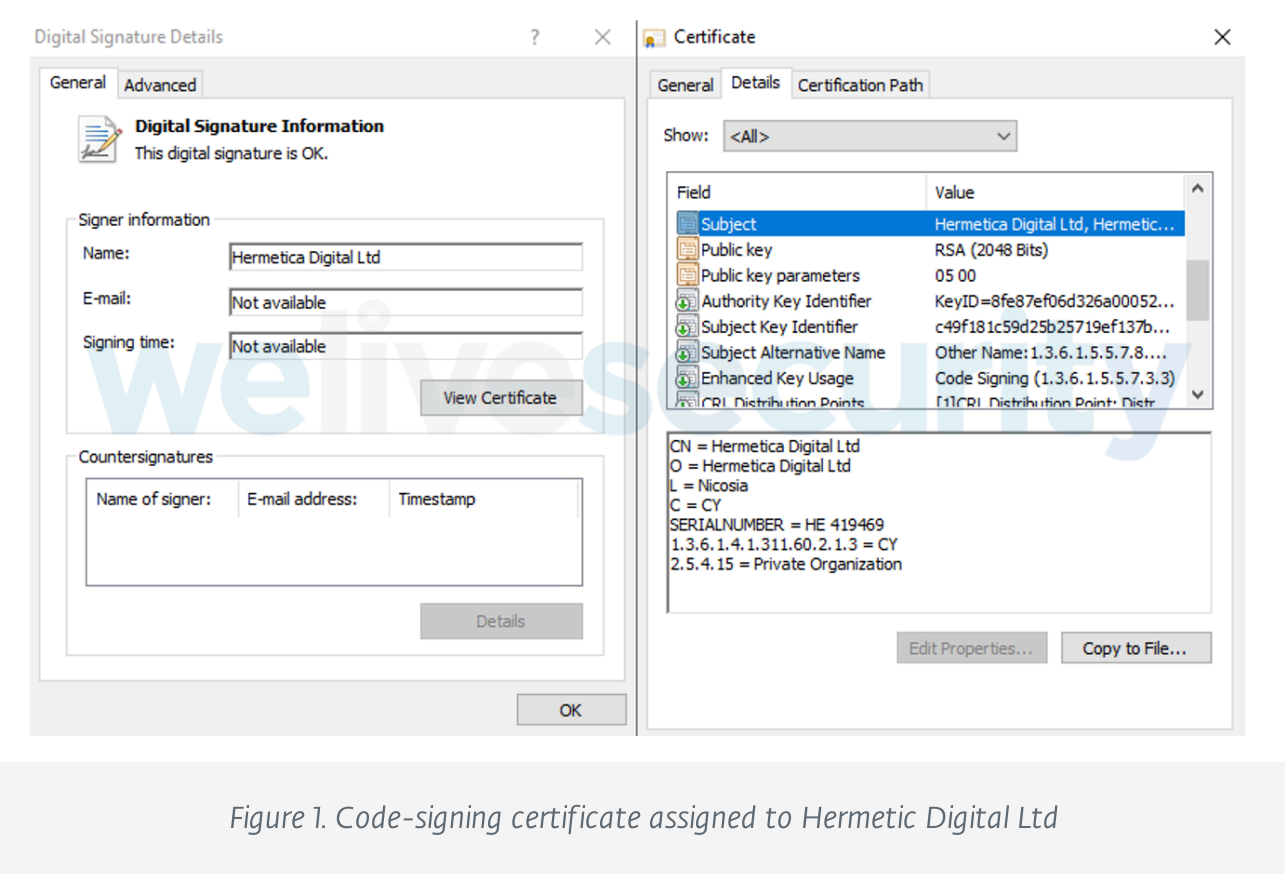
th a known threat
om do not share any

significant code similarity with other samples in the ESET malware collection

significant code similarity with other samples in the ESET malware collection. IsaacWiper is still unattributed as well.

Timeline

HermeticWiper and HermeticWizard are signed by a code-signing certificate (shown in Figure 1) assigned to Hermetica Digital Ltd issued on April 13th, 2021. We requested the issuing CA (DigiCert) to revoke the certificate, which it did on February 24th, 2022.



According to a [report by Reuters](#), it seems that this certificate was not stolen from Hermetica Digital. It is likely that instead the attackers impersonated the Cypriot company in order to get this certificate from DigiCert.

ESET researchers assess with high confidence that the affected organizations were compromised well in advance of the wiper’s deployment. This is based on several facts:

- HermeticWiper PE compilation timestamps, the oldest being December 28th, 2021
- The code-signing certificate issue date of April 13th, 2021



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

... suggests the
... servers

IsaacWiper deployed
in Ukraine
:
Code-signing
certificate revoked



Initial access

HermeticWiper

The initial access vector is currently unknown but we have observed artifacts of lateral movement inside the targeted organizations. In one entity, the wiper was deployed through the default domain policy (GPO), as shown by its path on the system:

```
C:\Windows\system32\GroupPolicy\DataStore\0\sysvol\
<redacted>\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\Machine\cc.exe
```

This indicates that attackers likely took control of the Active Directory server.

In other instances, it is possible that [Impacket](#) was used to deploy HermeticWiper. A Symantec [blogpost](#) states that the wiper was deployed using the following command line:

```
cmd.exe /Q /c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1
CSIDL_WINDOWS\policydefinitions\postgresql.exe 1>
\\127.0.0.1\ADMIN$\__1636727589.6007507 2>&1
```

The last part is the same as the default behavior in Impacket's `wmiexec.py`, found on [GitHub](#).

Finally, a custom worm that we have named HermeticWizard was used to spread HermeticWiper across the compromised networks via SMB and WMI.

IsaacWiper

... that attackers used ...s, we have also ...the same time as

... embedded in its ...ition Master software ...they implement low-

level disk operations. The following files were observed:

level disk operations. The following files were observed.

- 0E84AFF18D42FC691CB1104018F44403C325AD21: x64 driver
- 379FF9236F0F72963920232F4A0782911A6BD7F7: x86 driver
- 87BD9404A68035F8D70804A5159A37D1EB0A3568: x64 XP driver
- B33DD3EE12F9E6C150C964EA21147BF6B7F7AFA9: x86 XP driver

Depending on the operating system version, one of those four drivers is chosen and dropped in C:\Windows\System32\drivers\<4 random letters>.sys. It is then loaded by creating a service.

HermeticWiper then proceeds by disabling the Volume Shadow Copy Service (VSS) and wipes itself from disk by overwriting its own file with random bytes. This anti-forensic measure is likely intended to prevent the analysis of the wiper in a post-incident analysis.

It is interesting to note that most of the file operations are performed at a low level using DeviceIoControl calls.

The following locations are overwritten with random bytes generated by the Windows API function CryptGenRandom:

- The master boot record (MBR)
- The master file table (MFT)
- \$Bitmap and \$LogFile on all drives
- The files containing the registry keys (NTUSER*)
- C:\Windows\System32\winevt\Logs

In addition, it also recursively wipes folders and files in Windows, Program Files, Program Files (x86), PerfLogs, Boot, System Volume Information, and AppData folders, using a FSCTL_MOVE_FILE operation. This technique appears to be quite unusual and very similar to what is implemented in the [Windows Wipe project on GitHub](#) (see the wipe_extent_by_defrag function). It also wipes symbolic links and big files in My Documents and Desktop folders by overwriting



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

t, because the MBR, the
e to recover the

certificate
ily that we named

:52:49 on February
s the functions

DllInstall, DllRegisterServer, and DllUnregisterServer. Its export Dll

`DIRNSCALL`, `DIRREGISERVER`, and `DIRREGISERVER`. Its export DLL name is `Wizard.dll`. It contains three resources, which are encrypted PE files:

- A sample of HermeticWiper (912342F1C840A42F6B74132F8A7C4FFE7D40FB77)
- `exec_32.dll`, responsible for spreading to other local computers via WMI (6B5958BFABFE7C731193ADB96880B225C8505B73)
- `romance.dll`, responsible for spreading to other local computers via SMB (AC5B6F16FC5115F0E2327A589246BA00B41439C2)

The resources are encrypted with a reverse XOR loop. Each block of four bytes is XORed with the previous block. Finally, the first block is XORed with a hardcoded value, `0x4A29B1A3`.

HermeticWizard is started using the command line `regsvr32.exe /s /i <path>`.

First, HermeticWizard tries to find other machines on the local network. It gathers known local IP addresses using the following Windows functions:

- `DNSGetCacheDataTable`
- `GetIpNetTable`
- `WNetOpenEnumW(RESOURCE_GLOBALNET, RESOURCETYPE_ANY)`
- `NetServerEnum`
- `GetTcpTable`
- `GetAdaptersAddresses`

It then tries to connect to those IP addresses (and only if they are local IP addresses) to see if they are still reachable. In case the `-s` argument was provided when HermeticWizard was started (`regsvr32.exe /s /i:-s <path>`), it also scans the full /24 range. So, if `192.168.1.5` was found in, for example, the DNS cache, it incrementally scans from `192.168.1.1` to `192.168.1.254`. For each IP address, it tries to open a TCP connection on the following ports:



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

445: smb

The ports are scanned in a random order so it's not possible to fingerprint HermeticWizard traffic that way.

When it has found a reachable machine, it drops the WMI spreader (detailed below) on disk and creates a new process with the command line `rundll32 <current folder>\<6 random letters>.ocx #1 -s <path to HermeticWizard> - i <target IP>`.

It does the same with the SMB spreader (detailed below) that is also dropped in `<current folder>\<6 random letters>.ocx`, but with different random letters.

Finally, it drops HermeticWiper in `<current folder>\<6 random letters>.ocx` and executes it.

WMI spreader

The WMI spreader, named by its developers `exec_32.dll`, takes two arguments:

- i: The target IP address
- s: The file to copy and execute on the target machine

First, it creates a connection to the remote `ADMIN$` share of the target using `WNetAddConnection2W`. The file provided in the `-s` argument is then copied using `CopyFileW`. The remote file has a random name generated with `CoCreateGUID` (e.g., `cB9F06408D8D2.dll`) and the string format `c%02X%02X%02X%02X%02X`.

Second, it tries to execute the copied file, HermeticWizard, on the remote machine using DCOM. It calls `CoCreateInstance` with `CLSID_WbemLocator` as argument. It then uses WMI `Win32_Process` to create a new process on the remote machine, with the command line `C:\windows\system32\cmd.exe /c start C:\windows\system32\regsvr32.exe /s /i C:\windows\<filename>.dll`.

Note that the `-s` argument is not passed to HermeticWizard, meaning that it

is executed on the compromised machine.


The SMB spreader works in a similar way to the WMI spreader described above.

It repeatedly attempts to connect to the target IP address until it can delete

The SMB spreader takes the same two arguments as the WMI spreader: a reference to the

target IP address and the path to the remote SMB share (on

port 445).



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ports by:

- ☒ samr
- ☒ browser
- ☒ netlogon
- ☒ lsarpc
- ☒ ntsvcs
- ☒ svcctl

These are pipes known to be used in lateral movement. The spreader has a list of hardcoded credentials that are used in attempts to authenticate via NTLMSSP to the SMB shares:

```
-- usernames --
guest
test
admin
user
root
administrator
manager
operator

-- passwords --
123
Qaz123
Qwerty123
```

This list of credentials is surprisingly short and is unlikely to work in even the most poorly protected networks.

If the connection is successful, it attempts to drop, to the target ADMIN\$ share, the file referenced by the -s argument. As for the WMI spreader, the remote filename is generated by a call to CoCreateInstance.

It then executes, via SMB, the command line `cmd /c start regsvr32 /s /i`



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

software written in Go –
er campaign.
February 24th, 2022 UTC,
r deployment
ed at the same time as
ons. On one machine,

- ☒ 2022-02-23 17:49:55 UTC: HermeticWiper in C:\Windows\Temp\cc.exe deployed

- 2022-02-23 18:06:57 UTC: HermeticRansom in C:\Windows\Temp\cc2.exe deployed by the netsvcs service
- 2022-02-23 18:26:07 UTC: Second HermeticWiper in C:\Users\com.exe deployed

On one occasion, we observed HermeticRansom being deployed through GPO, just like HermeticWiper:

C:\WINDOWS\system32\GroupPolicy\DataStore\0\sysvol\
<redacted>\Policies\{31B2F340-016D-11D2-945F-
00C04FB984F9}\Machine\cpin.exe

A few strings were left in the binary by the attackers; they reference US President Biden and the White House:

- _/C_/projects/403forBiden/whiteHouseE.baggageGatherings
- _/C_/projects/403forBiden/whiteHouseE.lookUp
- _/C_/projects/403forBiden/whiteHouseE.primaryElectionProcess
- _/C_/projects/403forBiden/whiteHouseE.GoodOffice1

Once files are encrypted, the message in Figure 3 is displayed to the victim.

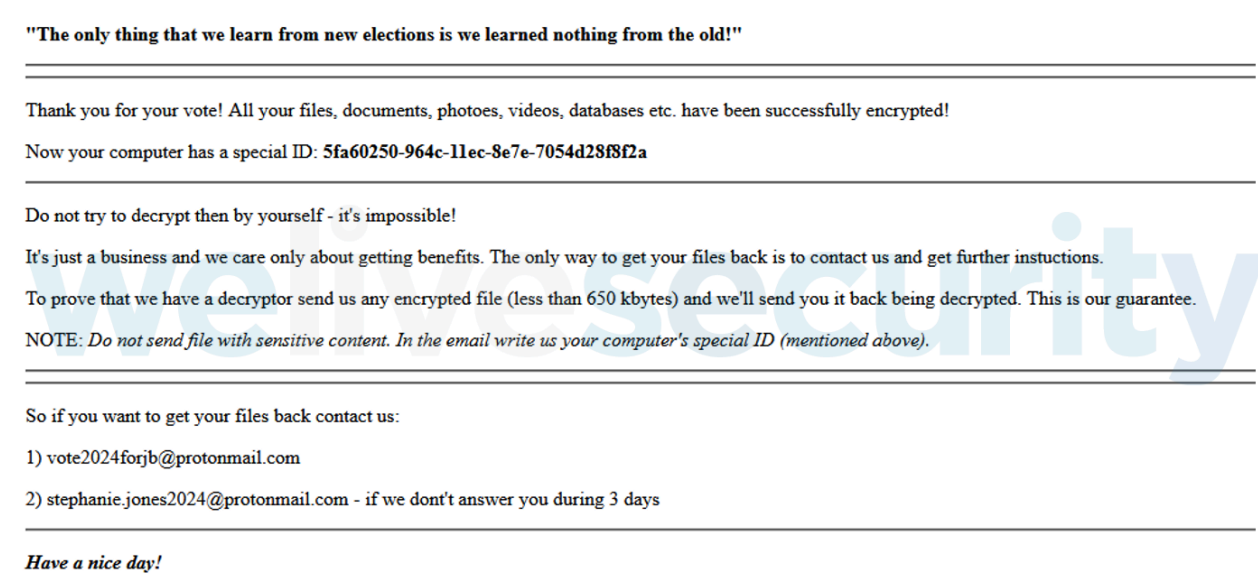


Figure 3. HermeticRansom's ransom note



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Authenticode

22. As mentioned in the previous section, the file is October 19th, 2021, and is signed with, IsaacWiper. The file is named cleaner.dll and it has a

C:\Windows\System32

under the following mechanics.

- clean.exe
- cl.exe
- cl64.dll
- clbcatq.dll
- clbcatq.dll

It has no code similarity with HermeticWiper and is way less sophisticated. Given the timeline, it is possible that both are related but we haven't found any strong connection yet.

IsaacWiper starts by enumerating the physical drives and calls `DeviceIoControl` with the IOCTL `IOCTL_STORAGE_GET_DEVICE_NUMBER` to get their device numbers. It then wipes the first 0x10000 bytes of each disk using the Mersenne Twister pseudorandom generator. The generator is seeded using the `GetTickCount` value.

It then enumerates the logical drives and recursively wipes every file of each disk with random bytes also generated by the Mersenne Twister PRNG. It is interesting to note that it recursively wipes the files in a single thread, meaning that it would take a long time to wipe a large disk.

On February 25th, 2022, attackers dropped a new version of IsaacWiper with debug logs. This may indicate that the attackers were unable to wipe some of the targeted machines and added log messages to understand what was happening. The logs are stored in `C:\ProgramData\log.txt` and some of the log messages are:

- getting drives...
- start erasing physical drives...
- -- start erasing logical drive
- start erasing system physical drive...



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Ukrainian that affected a different 22. At this point, we

risk that the same es that back the

A list of IoCs can also be found in [our GitHub repository](#).

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.

ESET Research now also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the [ESET Threat Intelligence](#) page.

IoCs

SHA-1	Filename	ESET detection
912342F1C840A42F6B74132F8A7C4FFE7D40FB77	com.exe	Win32/KillDisk.N
61B25D11392172E587D8DA3045812A66C3385451	conhosts.exe	Win32/KillDisk.N
3C54C9A49A8DDCA02189FE15FEA52FE24F41A86F	c9EEAF78C9A12.dat	Win32/GenCBL.B
F32D791EC9E6385A91B45942C230F52AFF1626DF	cc2.exe	WinGo/Filecoder
AD602039C6F0237D4A997D5640E92CE5E2B3BBA3	c164.dll	Win32/KillMBR.N
736A4CFAD1ED83A6A0B75B0474D5E01A3A36F950	c1d.dll	Win32/KillMBR.N
E9B96E9B86FAD28D950CA428879168E0894D854F	clean.exe	Win32/KillMBR.N
23873BF2670CF64C2440058130548D4E4DA412DD	XqoYM1BX.exe	Win32/RiskWare



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

framework.

Description

Attackers used RemCom and potentially Impacket as part of their campaign.

Attackers acquired a code-signing certificate

13000000

Signing Certificates

			for their campaigns.
Initial Access	T1078.002	Valid Accounts: Domain Accounts	Attackers were able to deploy wiper malware through GPO.
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Attackers used the command line during their attack (e.g., possible Impacket usage).
	T1106	Native API	Attackers used native APIs in their malware.
	T1569.002	System Services: Service Execution	HermeticWiper uses a driver, loaded as a service, to corrupt data.
	T1047	Windows Management Instrumentation	HermeticWizard attempts to spread to local computers using WMI.
Discovery	T1018	Remote System Discovery	HermeticWizard scans local IP ranges to find local machines.
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	HermeticWizard attempts to spread to local computers using SMB.
	T1021.003	Remote Services: Distributed Component Object Model	HermeticWizard attempts to spread to local computers using WbemLocator to remotely start a new process via WMI.
			HermeticWiper corrupts data in the system's MBR and MFT.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

TI485	Data Destruction	HermeticWiper corrupts user data found on the system.
TI499.002	Endpoint Denial of Service: Service Exhaustion Flood	By using DDoS attacks, the attackers made a number of government websites unavailable.



Let us keep you up to date

Sign up for our newsletters

Your Email Address

- ☐ Ukraine Crisis newsletter
- ☐ Regular weekly newsletter

Subscribe



Your account, your cookies choice







We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ESET RESEARCH
Embargo
ransomware:
Rock’n’Rust

Discussion

What do you think?


0 Responses

- 
Upvote
- 
Funny
- 
Love
- 
Surprised
- 
Angry
- 
Sad

0 Comments

1

 Login ▼



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

- 
- 
- 
- 
- 
- 

Name

 • Share

Best Newest Oldest



Award-winning news, views, and insight from the ESET security community

- About us
- Contact us
- Legal Information
- RSS Feed

- ESET
- Privacy Policy
- Manage Cookies

- 
- 
- 
- 
- 

Copyright © ESET, All Rights Reserved



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).