

Kiev metro hit with a new variant of the infamous Diskcoder ransomware

By Editor

Archived: 2026-04-05 14:43:58 UTC

Critical Infrastructure

Ransomware

Ukraine Crisis – Digital Security Resource Center

Public sources have confirmed that computer systems in the Kiev Metro, Odessa naval port, Odessa airport, Ukrainian ministries of infrastructure and finance, and also a number of organizations in Russia are among the affected organizations.

24 Oct 2017 • , 1 min. read

Several transportation organizations in Ukraine and as well as some governmental organizations have suffered a cyberattack, resulting in some computers becoming encrypted, according to media reports.

Public sources have confirmed that computer systems in the Kiev Metro, Odessa airport and also a number of organizations in Russia are affected.

ESET discovered that in the case of the Kiev Metro, the malware used for the cyberattack was Diskcoder.D, — a new variant of ransomware known also as Petya. The previous variant of Diskcoder was used in a [damaging cyberattack](#) on a global scale in June, 2017.

```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforsstxqzf2nm.onion

Your personal installation key#1:

ZDRqoZdoI+vr6yMqMlccRe/TmI+r+JNFX60UpZd+RH267xJ2b/5/UU5bzvMQkRSX
FF3rcIQIKAD1HoaAcxC TupQyW9UyGnk1Fxp35vszHqArN7/MEWtXb8bb7BMSbJx8
6thxi0FSIRUPr+IZXm2tR938ohkDAhJMKroU+xBLBylqgScJGNIUXL44j7HcLJi
Ba3a/AC0Sgjb4tsGfXUTFft19Muik6UnLgoz4XAYwgWlyJLPD/69P7Jq80AUJyExN
EKheR2bz17LrpUcrg6DfnT4qE5J3I0PERfE/3fxLhc20293tcwhGrNinxsf4bL81
7M02LsCle0UNG/NgH1qK05SUpBAMiqY9Ug==

If you have already got the password, please enter it below.
Password#1: _
```

The Diskcoder.D ransom note

ESET's telemetry has detected hundreds of occurrences of Diskcoder.D. Most of the detections are in Russia and Ukraine, however, also there are reports of computers in Turkey, Bulgaria and other countries are affected.

ESET security researchers are working on a comprehensive analysis of the Diskcoder.D malware. According to their preliminary findings, Diskcoder.D uses the Mimikatz tool to extract credentials from the affected systems. Apart from this, it has also a hardcoded list of credentials.

For more information about this threat read our [detailed analysis](#).

ESET customers are protected against this threat.

IoCs

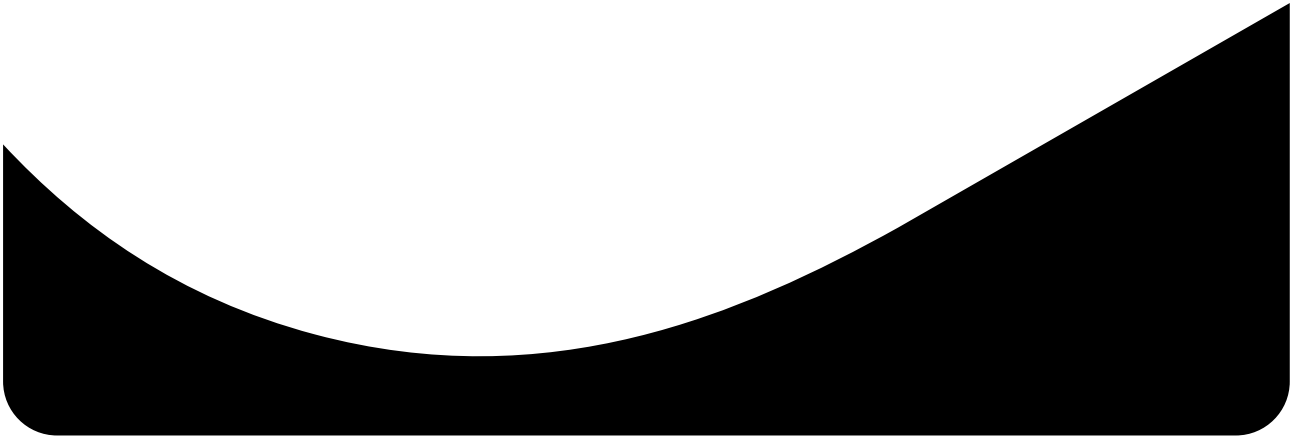
afeee8b4acff87bc469a6f0364a81ae5d60a2add

de5c8d858e6e41da715dca1c019df0bfb92d32c0 (install_flash_player.exe)

hxxp://1dnscontrol.com/flash_install.php

**Let us keep you
up to date**

Sign up for our newsletters



Source: https://www.welivesecurity.com/2017/10/24/kyiv-metro-hit-new-variant-infamous-diskcoder-ransomware/?utm_content=buffer8ffe4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer