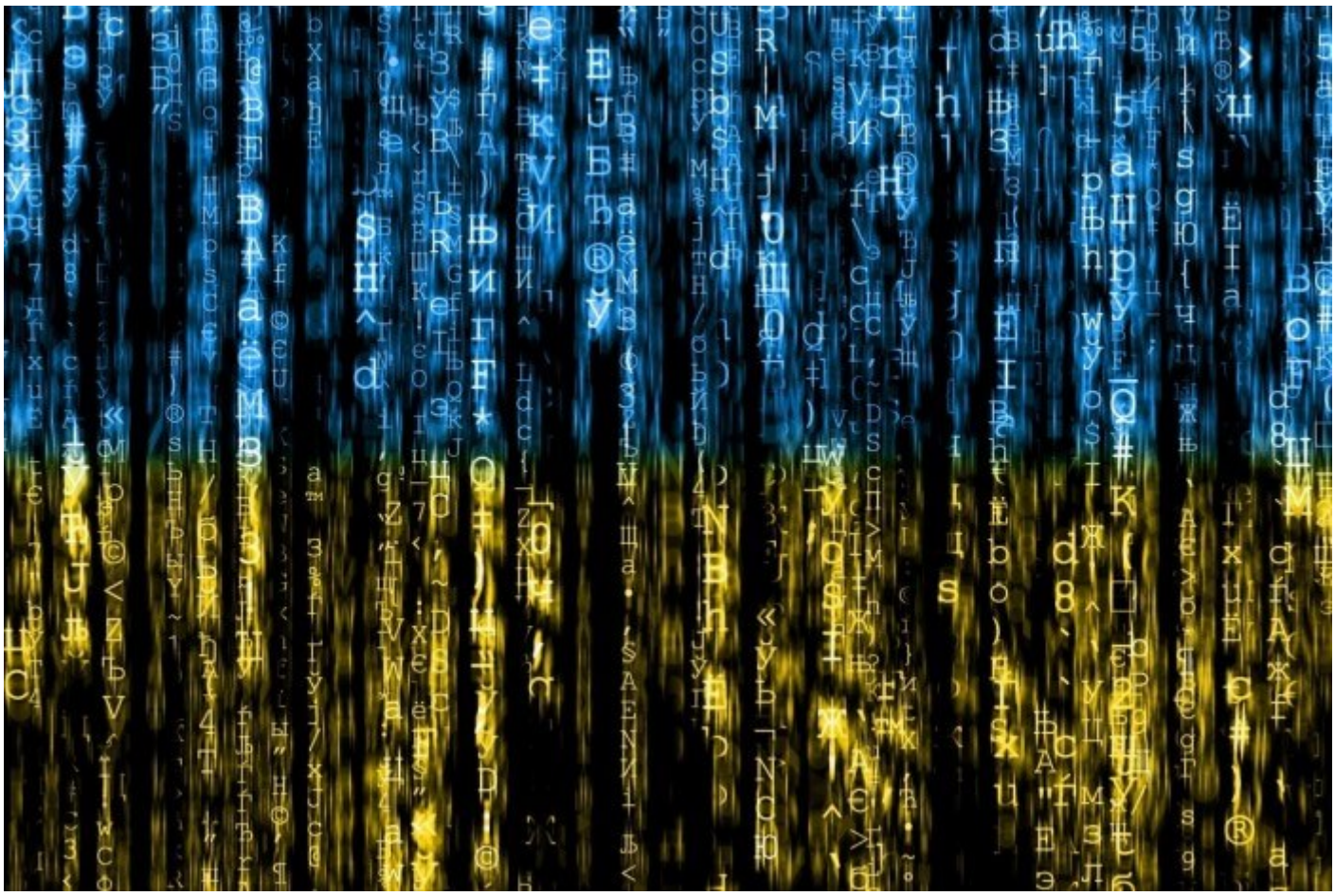
SwiftSlicer: New destructive wiper malware strikes Ukraine

⋮ 1/27/2023



27 Jan 2023 - 06:45PM

Sandworm continues to conduct attacks against carefully chosen targets in the war-torn country

ESET researchers have uncovered a new wiper attack in Ukraine that they attribute to the Sandworm APT group.

Dubbed SwiftSlicer, the destructive malware was spotted on the network of a targeted organization on January 25th. It was deployed through Group Policy, which suggests that the attackers had taken control of the victim's Active Directory environment.

Some of the wipers spotted by ESET in Ukraine early into Russia's invasion – HermeticWiper and CaddyWiper – were in some instances also planted in the same fashion. The latter was last spotted on the network of Ukraine's news agency Ukrinform just days ago.

> #BREAKING On January 25th #ESETResearch discovered a new cyberattack in 🇺🇦 Ukraine. Attackers deployed a new wiper we named #SwiftSlicer using Active Directory Group Policy.

> The #SwiftSlicer wiper is written in Go programing language. We attribute this attack to #Sandworm. 1/3 pic.twitter.com/pMij9lpU5J
>
> — ESET Research (@ESETresearch) January 27, 2023

SwiftSlicer is detected by ESET products as WinGo/KillFiles.C. The malware was written in Go, a highly versatile, cross-platform programming language.

When it comes to SwiftSlicer's method of destruction, ESET researchers had this to say: "Once executed it deletes shadow copies, recursively overwrites files located in %CSIDL_SYSTEM%\drivers, %CSIDL_SYSTEM_DRIVE%\Windows\NTDS and other non-system drives and then reboots computer. For overwriting it uses 4096 bytes length block filled with randomly generated byte".

Two months ago, ESET detected a wave of RansomBoggs ransomware attacks in the war-torn country that were also linked to Sandworm. The campaigns were just one of the latest additions to the long résumé of damaging attacks that the group has conducted against Ukraine over the past near-decade. Sandworm's track record also includes a string of attacks – BlackEnergy, GreyEnergy and the first iteration of Industroyer – that targeted energy providers. An Industroyer2 attack was thwarted with help from ESET researchers in April of last year.