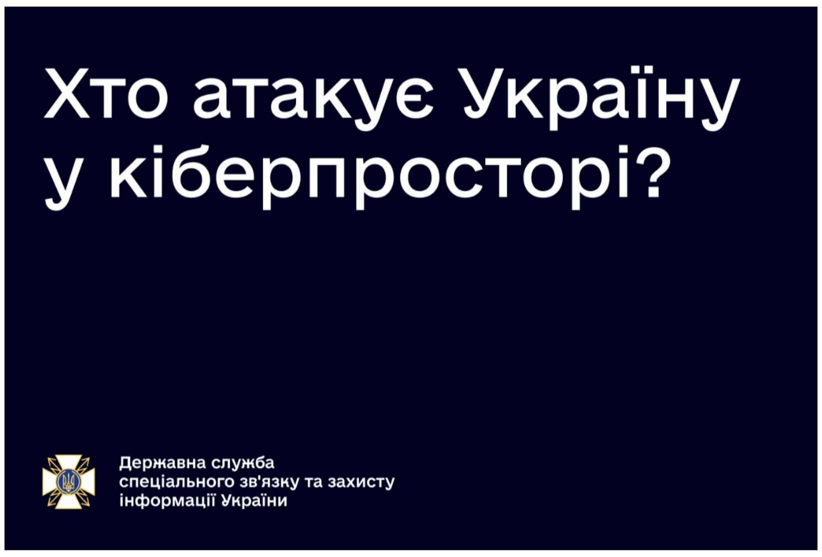
STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE



Who is behind the Cyberattacks on Ukraine's Critical Information Infrastructure: Statistics for March 15-22

03/25/2022 11:05 p.m

During March 15 - 22, the Ukrainian infrastructure underwent cyber attacks (according to the classification of the CERT-UA state response command):

- UAC-0056 (Pandora hVNC, RemoteUtilities, GrimPlant, GraphSteel)
- UAC-0051 aka unc1151 (Cobalt Strike Beacon, MicroBackdoor)
- UAC-0010 (GammaLoad, GammaDrop, HarvesterX)
- UAC-0082 (HermeticWiper, IsaacWiper, CaddyWiper)
- UAC-0088 (DoubleZero)
- UAC-0035 (LoadEdge)
- UAC-0041 (AgentTesla, XLoader)
- UAC-0020 aka Vermin (SPECTR)
- UAC-0028 aka APT28
- UAC-0026 (HeaderTip)
- UAC-0086 (QuasarRAT)
- UAC-0084 aka TA416 (PlugX)
- UAC-0064 (SunSeed)
- UAC-0033 aka XDSpy (JobDrop, StepDrum)

These include organizations that are affiliated with the government or the security services of the Russian Federation, the Republic of Belarus and the so-called security agencies of the so-called LNR.

"We can see that the same hackers who attack our information infrastructure also attack EU organizations that help our refugees. Thus, hackers are no longer limited to attacks on Ukraine but also attack the EU cyber space", - said SSSCIP Deputy Head Viktor Zhora during the briefing on March 23.

We would like to remind you that SSSCIP together with teams of the best Ukrainian security companies and the world's leading solution manufacturers have introduced a high-end cyber protection system for the state and business. Any company in Ukraine can contact CERT-UA and receive targeted assistance in protection against DDoS attacks, security monitoring, integration in a cloudy environment, development of modern protection systems against cyber threats to your workstations and servers, etc.