

Putin's cyberwarfare tactics

Amazon, Google and Microsoft operate huge cloud computing platforms used by governments and businesses. Together they offer a unique insight into cyberattacks being perpetrated against Ukraine



CAUGHT IN THE ACT



AMAZON AWS*

Seeing increase in malicious activity from known perpetrators, some specifically targeting charities, NGOs and other aid organisations, such as medical supplies, food and clothing relief. AWS assisting movement of data from Ukraine to cloud, to protect it from physical and virtual attack



MICROSOFT AZURE

Detected destructive cyberattacks against Ukraine's digital infrastructure several hours before invasion began. Witnessing attacks targeting more than 20 Ukrainian government, IT and financial sector organisations, as well as humanitarian aid, emergency response services, agriculture and energy

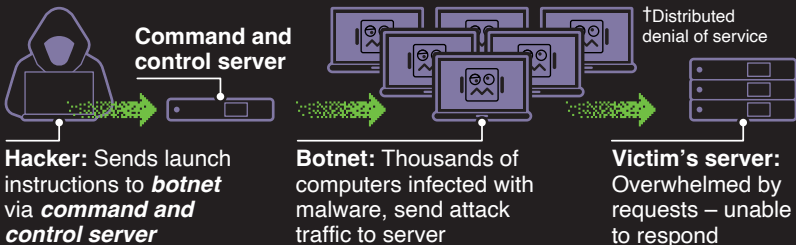


GOOGLE CLOUD

Observing activity from **FancyBear/APT28**, linked to Russia's **Main Intelligence Directorate** (*ukr.net email phishing campaigns*), and **Ghostwriter/UNC1151**, associated to **Belarus Ministry of Defence** (*phishing attacks against Ukrainian and Polish military personnel*)

Mustang Panda (Chinese hackers): Google finds them targeting Europe with malware hidden in emails purporting to contain information on Ukraine crisis

RUSSIA HITTING UKRAINE WITH NON-STOP DDoS[†] ATTACKS



Microsoft president **Brad Smith** believes some cyberattacks may be breaking **Geneva Convention** and constitute war crimes

*Amazon Web Services. Original picture: Russian Presidential Executive Office

Sources: VentureBeat, Microsoft, Harvard Business Review, F5