Overview
"Freedom is Free. If You Have Paid, It Is a Ransom."

The Council of the European Union (EU) fired its second shot against cyber attackers threatening the EU or its member states when on October 22, 2020, it sanctioned two individuals working for the Russian 85th Main Centre for Special Services (GTsSS) who took part in the cyber-attacks against the German Federal Parliament in April and May 2015. The GTsSS is also included on the list of sanctioned legal persons, entities and bodies. The cyber-attacks were reported to be conducted against the parliament information systems and to disrupt the parliament’s operations for several days. A significant amount of data was stolen during the cyber-attacks and emails account of several members of parliament, as well as Chancellor Angela Merkel’s were affected. Targeted measures against those attackers include assets freeze and travel bans, two usual suspects in the EU sanction’s toolbox.

This is the second wave of sanctions following the ones issued on July 30, 2020, against six individuals and three entities for numerous cyber-attacks known as ‘WannaCry,’ ‘NotPetya’ and ‘Operation Cloud Hopper’ in 2017, as well as an attempted cyber-attack on the Organization for the Prohibition of Chemical Weapons in 2018.

To date, the EU is listing eight individuals and four entities on the cyber-attacks sanctions lists. This update covers the background for those measures and why are they relevant to a wider audience, outside of the sanctioned individuals or entities themselves.

The EU Sanctions Regime
The restrictive measures are imposed under a relatively new sanctions regime on persons involved in cyber-attacks (or attempted cyber-attacks) targeting the EU, a member state, a third country or an international organization (the EU Sanctions Regime), first adopted back in May 2019. The sanctions can be imposed upon the occurrence of significant cyber-attacks (or attempted attacks) that pose an external threat to the EU and its member states. “Significance” is determined by a range of factors, such as the scope, scale, impact or severity of disruption caused and the amount of data loss or economic loss. “External” means the attack is carried out, or supported, from outside the EU.

Sanctions can be imposed on individuals or entities who: (i) are responsible for cyber-attacks or attempted cyber-attacks, (ii) provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging these attacks or facilitating them whether by action or omission; or (iii) are associated with the entities or individuals covered under (i) and (ii).

Why One (and Who) Should Look To The Lists …
Ransom payments following cyber-attacks are subject to increased scrutiny and challenges; similar to kidnapping, no one wants to publicly disclose that ransom payment was made, even if such payment might be necessary to retrieve your data. This is relevant not only for victims but to a wider ecosystem; "facilitating" payments may expose parties to civil and criminal liability for "making funds available" to sanctioned individuals.

... as Well as To US "Similar" Regimes?

Similar to the US, making funds or economic resources available directly or indirectly to sanctioned individuals or companies or for their benefit is indeed prohibited under the EU Sanctions Regime. Both the EU and the US regimes confront victims of ransomware or anyone facilitating payments' requests (from crypto intermediary to cyber insurance carriers) to a similar dilemma between paying versus potential violating of sanction regimes. As it is the case for many other extortions, attribution proves to be challenging, especially within the limited timeframe hackers will give victims to pay the ransom, increasing the uncertainty (and hence the risks).

The complexity of these scenarios has been recognized by the US Department of the Treasury’s Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) who, on October 1, 2020, published advisories on the sanctions and anti-money laundering risks of facilitating ransomware payments.[1] One of the ways the US is dealing with the issue includes the possibility to apply for a license authorizing the payment, an avenue not contemplated (yet) under the EU regimes.

More Attacks, More Sanctions, More Challenges?

With cyber-attacks growing in numbers and ransomware being more accessible, recourse to insurance coverage of ransom payment would provide some relief to contain financial exposures. This has been a driver for the increased reliance on cyber insurance products. Prospects of a potential breach of sanctions or other regulatory rules and increased scrutiny might require insurers to hold back or introduce new coverage exclusions, as it could increase pressures on forensic experts or intermediaries (crypto-assets providers, financial institutions, etc.) part of the ecosystem and on actual victims.

As the list of sanctioned individuals and entities is expected to grow in the future, stakeholders should carefully consider how they will avoid traps, wherever they are in the cyber-attack response chain. A sound check should be done when onboarding new business partners, when conducting due diligence and/or when monitoring existing relationships, and where requested to pay or facilitate the payment of a ransom. This would require investing in cyber threat intelligence and building up risk-based compliance programs. If payments are made without any safeguards in place, companies will risk violating the European or US sanction regimes.

"It takes 20 years to build a reputation and few minutes to cyber-attack to ruin it."

[1] For a comment on those guidelines, please see previous Steptoe coverage here.