Pro-Kremlin Hacktivist Groups Seeking Impact By Courting Notoriety

flashpoint.io/blog/pro-kremlin-hacktivist-groups/

October 26, 2022

Russia's February invasion of Ukraine has led to the emergence of a wide range of pro-Kremlin hacktivist groups. The loudest and most active of these groups has been "Killnet," a former DDoS-as-a-service group, which has conducted mostly distributed denial of service attacks against Ukrainian and Western targets.

While some groups (including one called "XakNet") have consistently denied that they are working together with the Russian government, even in the face of evidence, other cyber threat groups have been openly seeking opportunities for cooperation. A group called "RahDIt," for instance, claimed to have shared data on alleged "Ukrainian agents" with Russian security services. At the very least, we can confidently say that the groups are enthusiastically supporting the Russian government's objectives in Ukraine, and they seem to be receiving support from government-linked actors in return.

https://www.youtube.com/watch?v=FMFUi091JeY
September interview with hacktivist group Killnet.

These newfound relationships go beyond helping Russia with their own propaganda operations, also alluding to behind-the-scenes coordination between the government and these hacktivist groups that may aid their own recruitment for followers and members. It is

critical that organizations understand both sides of this alliance in order to ensure they are getting the most out of their intelligence to properly protect their assets and personnel.

The hacktivist family tree

Most other hacktivist groups are associated with Killnet to varying degrees, although some have distinct identities, such as the "XakNet" group, a group of self-confessed "patriotic hackers" active since the 2008 Russia-Georgia war, who were linked to Russia's military intelligence by Mandiant, or "RahDIt," a hack-and-leak group whose main project is a website sharing personal information on alleged Ukrainian agents and enemies of Russia.

Recommended Reading: An Exclusive Interview with XakNet by Cyber Shafarat

Instead of choosing and working on their victims strategically, as would often happen with disruptive cyber attacks, these groups have in common the tendency to instead pay close attention to the news cycle and focus on less sophisticated attacks or data leaks. In the approximately eight months since the outbreak of the Russia-Ukraine war there have been several prominent examples of this.

Killnet targeted the Eurovision Song Contest in Italy in May when it became clear that Ukraine was a clear favorite to win the contest. Several groups took part in an attack against Lithuanian networks at the time when the Baltic country was accused of "blockading" the Russian exclave of Kaliningrad in June. RaHDIt released information allegedly stolen from the Ukrainian military, to support Russian claims that Russia's military setback in Ukraine was partly due to a more active US involvement in the war. Killnet gave credence to claims made by pro-Kremlin commentators and Russia's Security Council, that the Security Service of Ukraine is aiding drug trade inside Russia.

Softball Interviews

The role of these groups seems to be partly to help a "shock and awe" form of information warfare, suggesting to Western audiences that their home networks are vulnerable and will be attacked if their countries continue supporting Ukraine. However, the hacktivist groups also play an important role in Russia's domestic propaganda, as evidenced by the frequent appearances of some of them in Kremlin-connected media.

Killnet and its founder, the threat actor using the alias "Killmilk", have been interviewed by the state-controlled RT media outlet three times since March. Killmilk also gave an interview to the Kremlin-friendly "Lenta" and "Gazeta" news sites in April and August respectively and the minor "Dontimes" portal in September. In the interviews, Killnet representatives talk about the group's origins, goals and recent attacks, and are in general portrayed as patriotic activists.

RaHDIt, similarly, gave several interviews to Russian media outlets. Like Killnet, the group was interviewed by Dontimes – in August – and has also become somewhat of a regular interlocutor of the state-owned RIA news agency, which quoted the group at least five times in June and July alone. Similarly to Killnet's appearances, RaHDIt's claims were handled uncritically in these reports, allowing the collective to appear as righteous cyber warriors. In one of the RIA interviews, RaHDit even offered advice on cyber hygiene, explaining that household appliances can be used to spy on people.

XakNet has been less forthcoming in mainstream media. However, the group has been interviewed by electronic platforms such as "Russian OSINT", which focuses on Russian-speaking cyber underground, and "Cyber Shafarat", another blog focused on illicit communities, where they mostly talked about their origins and recent attacks.

More PR Than APT

Apart from the propaganda value, these appearances can also hint at a closer alignment with state structures, due to the tight control, by the government, of some of the media outlets that published these interviews, which carry a significant PR-value for the groups (and thus opportunities to recruit followers and members).

Apart from pro-Kremlin media, the activity of hacktivist groups was also repeatedly extolled in chat channels linked to the Wagner Group, a private military company operating in Ukraine. RaHDIt, for instance, was praised by mercenaries claiming that their list of alleged Ukrainian agents helped them to do "filtration" work in the territory controlled by Russia in Ukraine.

Pro-Kremlin hacktivist groups have so far been louder than they have been disruptive. Nonetheless, their value is partly in shaping the conversation, domestically and internationally. They have been vessels of pro-Kremlin propaganda, relying on their own tens of thousands of followers on social media, as much as they have been helping to influence the conversation domestically by talking about cunning attacks on targets in a hostile West, or by "exposing" material that underpins the Kremlin's domestic talking points. They have also helped in the "branding" of the war for domestic audiences, by creating symbols and memes that have been shared by Russian internet users.

Proactively address risk with Flashpoint

Any organization's security capabilities are only as good as its threat intelligence. Flashpoint's suite of tools offer you a comprehensive overview of your threat landscape and the ability to proactively address risks and protect your critical data assets. To unlock the power of great threat intelligence, get started with a free trial.