Evaluation of cyber activities and the threat landscape in Ukraine

PUBLICATIONS

17 MAY 2022

Introduction

When the war in Ukraine broke out, many analysts were surprised to discover that what was simultaneously happening in the cyber domain did not match their predictions[1]. Since the beginning of the fighting, new cyberattacks taking place in Ukraine have been identified every week, which lead to a variety of interpretations – and indeed a global feeling of confusion. In this report, we aim to provide a strategic technical assessment of our understanding of current events.

Much of the debate around the situation concerns the question of whether or not a cyberwar is taking place. However, we find this question to be entirely irrelevant. While there is no question that a high number of cyberattacks have taken place and are still taking place in the country, we recognize that the overwhelming majority of cyber events thus far have been overshadowed by the kinetic aspects of the conflict. We nevertheless do still see value in attempting to interpret the data at hand, in alignment with Kaspersky's constant commitment to understand more about threat actors and how they are organized. Therefore, with this article, our core aim is to share a threat landscape overview, which Kaspersky cybersecurity researchers in its Global Research and Analysis Team (GReAT) are observing in relation to the conflict, with the wider international community and thus to contribute to broader ongoing cyber-stability discussions of threat-related insights.

Overview of cyber activities

Since the beginning of the war, the international community has observed a very high number of attacks of various kinds and degrees of sophistication. These attacks include:

- Destructive attacks such as:
  - Ransomware (IsaacRansom);
  - Fake ransomware (WhisperGate);
  - Wipers (HermeticWiper, CaddyWiper, DoubleZero, IsaacWiper); and
  - ICS/OT wipers (AcidRain, Industroyer2).
- Advanced persistent threats (APTs) and campaigns focused on intelligence gathering, such as:
  - Gamaredon;
  - Hades (Sandworm);
  - PandoraBlade; and
  - UNC1151.

Focusing on the destructive attacks, we cannot help but notice that many of the malicious programs discovered showcase vastly disparate degrees of sophistication. At one end of the spectrum, HermeticWiper is an extremely well-designed piece of software, which must have required weeks of development (at least) before it was released. At the other end,

programs such as IsaacWiper appear to be the product of rushed development – as if their operators had been tasked with destroying data at the eleventh hour.
Contrary to some declarations, we have not noticed any particular coordination efforts, neither between separate instances of these attacks, nor with military operations occurring at the same time (with the notable exception of AcidRain). We have also been unable to identify any particular trends in the targeting involved. Our best guess is that separate groups decided to take advantage and wreak havoc immediately after the conflict erupted.
The overall limited operational impact of such attacks could certainly be viewed as surprising when we consider that some threat actors active in the region have demonstrated highly-disruptive capabilities in the past (e.g., BlackEnergy). We can only speculate as to why such capabilities were not used since late February, but our best guess is that the attacks were not coordinated, and each such attack with a more disruptive impact typically requires more effort for careful planning and execution from the threat actors. This supposition may be given more weight by ESET's discovery of Industroyer2 in a Ukrainian energy company: the research reports that destructive actions were planned for April 8, but that "the attack had been planned for at least two weeks". It is safe to assume that such an attack requires careful planning and that preparations for it only started after it became clear that the war would last longer than widely expected.
In this regard, summing up the above-mentioned discussions, these are our three key takeaways:
1.Attacks observed against infrastructure in Ukraine so far appear to be uncoordinated and conducted by groups of varying technical levels;
2.While these cyber activities hint at a role cyberspace could take during a military conflict, what we have seen so far can hardly be regarded as the full extent of threat actors' capabilities; and
3.It is likely that as a clearer perception of the scale and duration of the war emerges, the various groups will find ways of coordinating better – possibly leading to highly disruptive impacts as outlined above.

The KA-SAT event and risks of spillover

On February 24, around 04:00 UTC – around the time of the start of the Russian invasion of Ukraine – several Viasat KA-SAT modems ceased functioning due to yet another wiper attack (AcidRain). This attack is officially reported to have affected Ukrainian military communications and is unlikely to be a coincidence considering the timing. No matter who orchestrated it, this is a rare example of a cyberattack providing operational support for a physical military operation, which in itself makes it significant in terms of understanding modern warfare. It is however unclear whether this provided any brief or lasting tactical value: as far as we are aware, other means of communication (e.g., 3G, 4G) remained available in the same timeframe.
This attack also disabled the remote control of wind turbines located in Germany, raising concerns about potential spillover of the conflict into other European countries. It is unclear why routers belonging to a German customer were affected: maybe the means of distribution used to spread the malware did not allow for granular targeting, or maybe the operators made a mistake. In any case, we have little reason to believe that there was any intent to provoke adverse effects outside Ukraine.
Whenever the spillover question comes up, it is usually associated with memories of the NotPetya incident (fake-ransomware distributed through a supply-chain attack in Ukraine in 2017). It is worth pointing out that NotPetya contained self-spreading code and its uncontrollable spread was powered by a very potent Windows exploit. No such thing has been observed in any of the malware families used in Ukraine recently. As such, we estimate the risk of witnessing another NotPetya-level event as very low.

One final point of interest is whether it is likely that similar events will take place during the remainder of the conflict. It is important to understand that ICS attacks are far from trivial to organize due to the complex nature of systems they affect and the fact that such machines are typically not connected to the internet. This means that an attacker would have to breach the victim's network first, figure out where the target appliances are located, and finally devise an attack scenario involving specific equipment it likely does not own a copy of to conduct experiments. In other words, highly-disruptive attacks require meticulous preparation that range in the order of weeks – if not months. In conclusion such attacks would only be achievable a long time from now – unless attackers already present in strategic networks chose not to leverage this access to date.

Summing up the above-mentioned discussion, our key takeaways are the following:

1.The Viasat attack is a very significant cyber event. It is hard to tell whether others will take place in the near future, but that probability increases significantly as time passes.
2.The recent Industroyer2 discovery indicates that there may be a desire among threat actors to conduct highly-disruptive attacks soon.
3.The threat campaigns observed so far have been very focused on Ukraine.
4.Any observed spillover to date should be interpreted as accidental, and the potential for uncontrolled malware spread has so far been non-existent.

Takeaways from Kaspersky for international discussions on stability in cyberspace

As we are still transitioning from one phase of the conflict to another, we expect that some of the observations outlined in this report will become less accurate. Though the various cyberattacks observed so far have been disorganized and uncoordinated, we consider that more structured activity may surface soon amid this constant background noise.

As the conflict drags on, we predict that more sophisticated threat actors will get involved and refocus their intelligence collection activities. For this reason, we advise companies all around the world to prepare for a resurgence of ransomware attacks.

Taking a broader perspective on the threat landscape these days in the light of ongoing inter-state negotiations at the UN, the international community more than ever needs to further advance the operationalization of the agreed non-binding cyber norms and confidence-building measures (CBMs), and extend them to relevant stakeholders. In particular, it is important to advance discussions on cross-border cooperation between the CERT/CSIRT community and relevant security experts to ensure that they can do their job – protecting victims of cyber incidents – despite any political or geopolitical context. And in this regard, one of the core aspects we at Kaspersky have continuously been advocating[2] for is developing effective interaction between national points of contacts (PoCs) as well as points of contacts from relevant stakeholders (such as the private sector, owners and manufacturers of ICTs, cybersecurity experts and others), which can be utilized during significant cyber events.

One of the open questions that remains for the international community is clarification on the protection of civilian infrastructure in cyberspace. In this regard, more information and transparency from states on how they interpret the application of international law and, particularly, international humanitarian law, is urgently needed to provide effective safeguards to civilian infrastructure in cyberspace. The ongoing efforts, such as those of the International Committee of the Red Cross (ICRC), to signal legal protection through digital emblems seems an important contribution in this regard.

Finally, the public core of the internet, whose security and availability is essentially vital for digitized societies and economies, needs to be discussed further and acknowledged by UN Member States and the larger international community. The current acute geopolitical

tensions pose a serious risk of further fragmenting the baseline fundamental internet infrastructure, which was initially created and designed in a multistakeholder, decentralized spirit. These factors have the potential to create greater insecurity affecting many users of ICTs, and therefore, more than ever require international dialogue among all states to preserve cyberspace.
We have also previously shared our views to the UN cyber-dialogue (i.e. UN Open-Ended Working group) which can be found at the official web-page of the UN OEWG.

[1] For instance, https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051 or https://www.csis.org/analysis/russias-possible-invasion-ukraine
[2] Eight practical suggestions to the UN OEWG from a cybersecurity research perspective, Kaspersky's submission in December 2021 https://documents.unoda.org/wp-content/uploads/2021/12/Kaspersky-submission-UN-OEWG_December-2021.pdf