Industroyer2 in Perspective

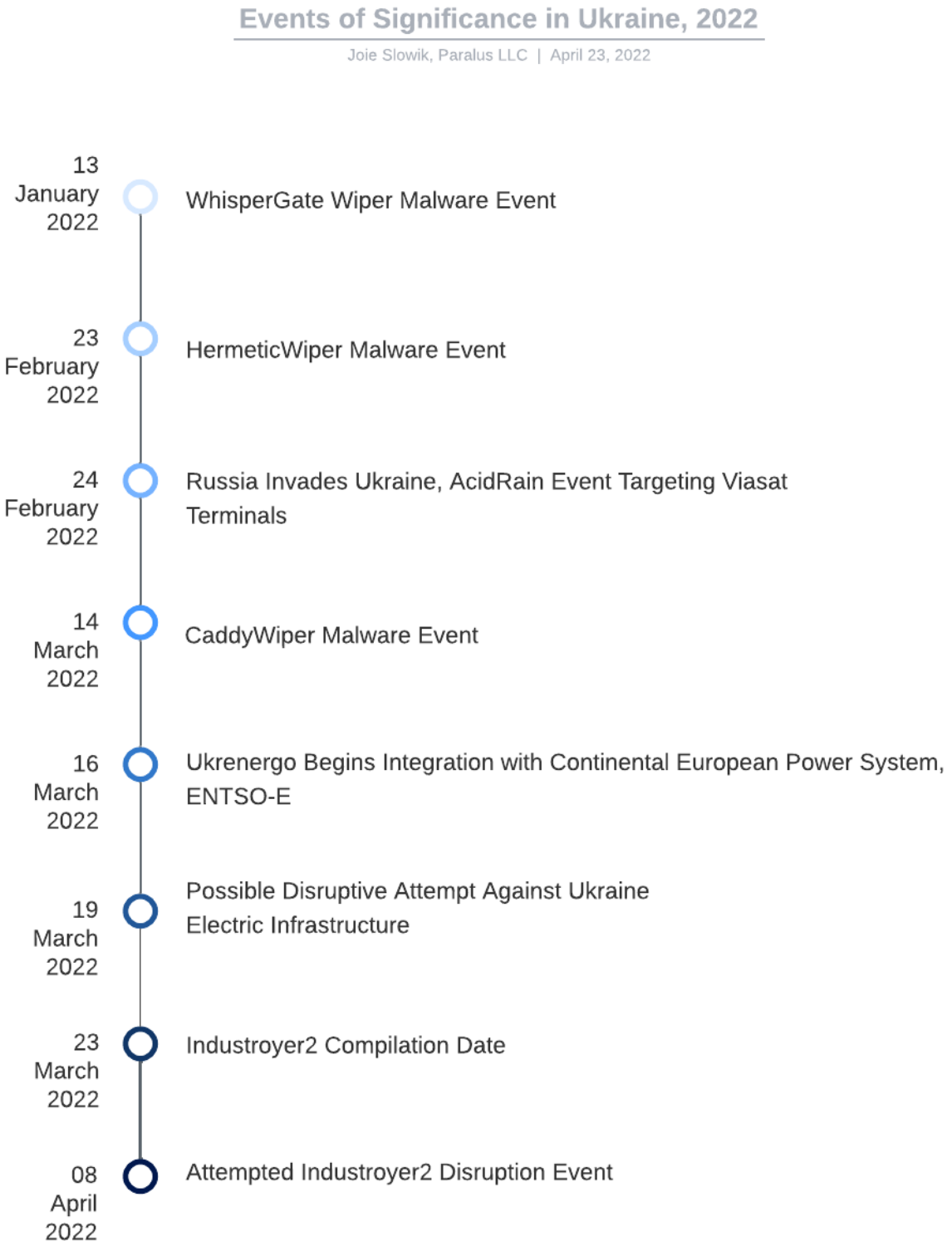
pylos.co/2022/04/23/industroyer2-in-perspective

Joe 04/23/2022

Background

On 12 April 2022, the Ukrainian CERT and ESET disclosed the existence of Industroyer2, a successor to the malware targeting Ukrainian electric distribution and transmission operations in 2016. Industroyer2 arrived after multiple disruptive cyber incidents of varying degrees of success surrounding Russia's brutal invasion of Ukraine, as presented in the following timeline:

Overall, cyber operations targeting Ukraine have ranged from the "merely annoying" (DDoS) to "quite concerning" (Industroyer2). Fully contextualizing events will take time and the release of additional information, evidence, and technical background, although some preliminary observations are possible. In the case of Industroyer, we have several mysteries to contend with:



- Leaked reporting indicating potentially successful disruptive events in mid-March, prior to the known Industroyer2 compilation date, across multiple substations.
- The overall timing of Industroyer2 events, well after the start of hostilities (and as Russian performance continued to deteriorate across its invasion).

- Reporting from Ukrainian authorities indicating attempted disruptive operations are quite widespread and may even be ongoing after the Industroyer2 disclosure.

There are many threads to pull to evaluate the Industroyer2 incident, given limited reporting but also the existence of samples in commercial malware repositories. While much remains to be uncovered with events, sufficient information is available at this time to draw some preliminary conclusions and set events in context with the current situation in Ukraine, as well as previous operations.

Industroyer2 and Past Events

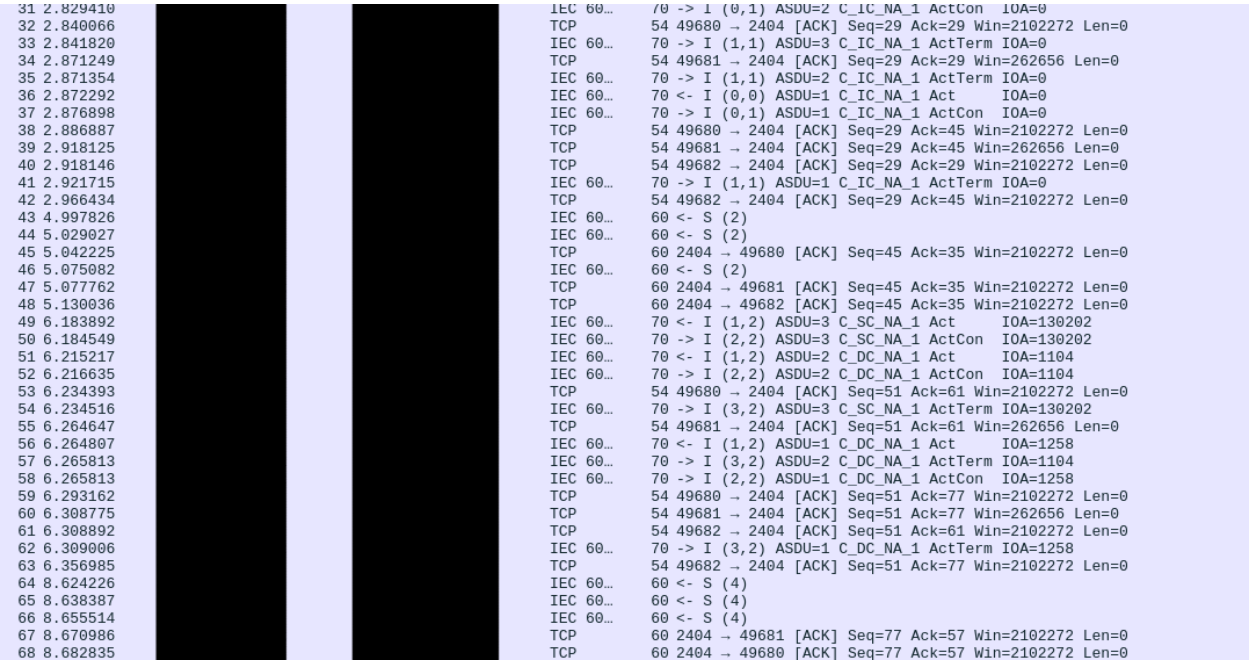
Industroyer2 represents the third (but presumably unsuccessful) electric power event targeting Ukrainian civilian infrastructure. The first such event took place in 2015, when three distribution substations were targeted through a combination of direct interaction with operator control systems and a "SCADA hijack" scenario to open breakers to disrupt the flow of electricity. The disruption was quickly followed by a wiper deployed to operator workstations, as well as disruption to control center Uninterrupted Power Supply (UPS) systems and deploying a malicious firmware update to serial-to-ethernet devices to effectively "brick" the systems. This also coincided with a DoS to utility telephone lines inhibiting the ability of customers to report outages to operators.

The event resulted in an outage lasting several hours impacting over 200,000 customers. Overall, the 2015 event appears to be a "success," in terms of the capabilities deployed resulting in an impact scenario commensurate with tools used. While Ukrainian operators were able to restore operations relatively quickly by manually reclosing breakers, anecdotal evidence indicates the system wiping and effective destruction of serial-to-ethernet converters produced damage taking years to effectively correct.

The 2015 event was followed roughly a year later by another incident, this time using power system-specific malware referred to as Industroyer or CRASHOVERRIDE. In 2016, a transmission substation was targeted, providing for a potentially larger impact scenario than the 2015 event. However, as detailed in analysis in 2019, the first Industroyer event appears to have been very ambitious as an integrity- and protection-targeting industrial incident, but also a failure due to various mistakes in designing and deploying tools for the (attempted) disruption. Thus the 2016 event resulted in relatively less-significant impact than 2015, largely due to errors on the part of the attackers.

Industroyer2 appears to have learned some lessons from the 2016 incident. As detailed in public presentations, the IEC-104 manipulation module for the original Industroyer failed due to programmatic errors and ignoring proper state change requirements for proper protocol communication. Shown in the following packet capture, Industroyer2 appears to properly implement the IEC-104 protocol in following appropriate state transitions. While

findings are preliminary and complete assessment would require testing on equipment similar to what was targeted in victim environments, preliminary analysis would indicate the attackers paid attention to past failures and implemented corrections in their code.



However, other aspects of Industroyer2 are significantly different than past incidents. While several wipers are associated with Industroyer2's deployment, preliminary analysis from ESET and CERT-UA assesses this was likely for destroying intrusion artifacts and evidence, with limited targeting of non-Windows systems that has not yet been thoroughly evaluated in terms of impact and likely adversary intent. Lacking from this event are the sort of physically destructive applications, such as the serial-to-ethernet converter targeting or the attempted removal of line protection in 2016.

Given currently-available evidence, it would appear that the 2022 attempt, although potentially of much wider scope (up to two million potentially impacted customers, based on Ukrainian assessment), was also potentially less destructive than prior activity. Precisely why this is the case is unknown. Some possibilities include:

1. Desire on the part of Russian decision-makers to enable relatively quick restoration of the impacted sites as part of an invasion plan.
2. Inability to develop a suitable physical destruction capability for the targeted substations in time for deployment because of a "rushed" decision-making process.
3. Failure to deploy a destructive capability because the attack was interrupted by Ukrainian defenders before an impact could occur.

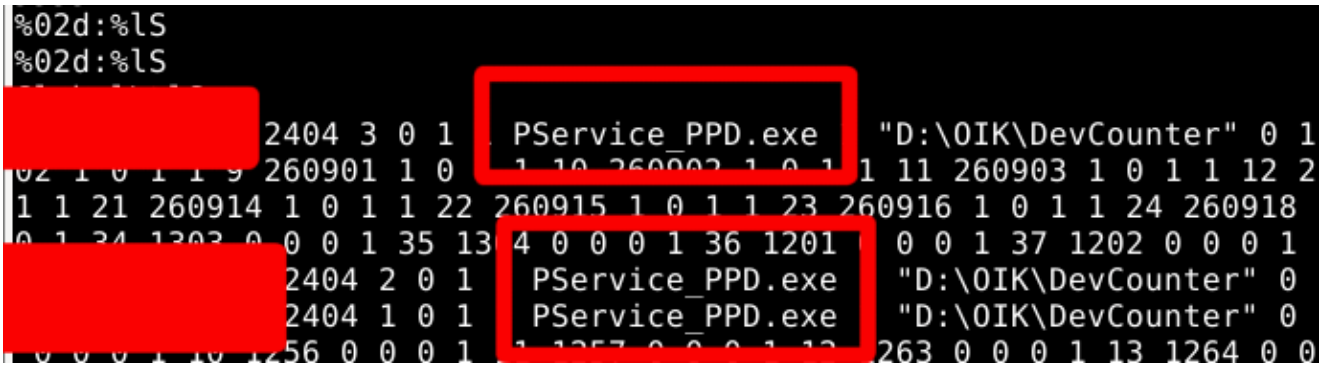
Each of these possibilities require more evidence to evaluate, although the first might be possible to examine if the targeted sites were disclosed. For example, if the sites were tightly correlated with Russian invasion lines of (attempted) advance, having a way to restore

electricity service but disrupting it during operations might make sense. The other two possibilities will require information not likely to be available for some time in order to properly assess.

In any case, Industroyer2 appears to represent both an advance from earlier operations, in that industrial communication seems to be properly implemented, and a step back in terms of hard-coded configurations (making each sample unique to its victim site) and lack of a post-disruption destructive element.

BlackEnergy3 Connections

One curious aspect of Industroyer2 concerns service names used during execution in deployment. In analysis of non-public samples published by ESET and analysis of different (but apparently functionally equivalent) samples in commercial malware repositories, the following set of strings are present for targeting purposes:



While seemingly innocuous, those with good memories (or a bit of search engine skill) can rapidly identify where this name – PService_PPD.exe – previously appeared: in past reporting on BlackEnergy3 use in connection with the 2015 Ukraine power event.

While BlackEnergy3 is not "industrial-specific" in the same sense as either Industroyer variant or other items such as Triton, it did serve a critical enabling function as part of the overall attack sequence leading up to power disruption. The name has no other significance or notable observations beyond this context.

Indicator	Type
hxxp://31.210.111.154/Microsoft/Update/KS081274.php	Malicious URL
hxxp://41.77.136.250/Microsoft/Update/KS081274.php	Malicious URL
hxxp://xxx.xxx.xxx.xxx /Microsoft/Update/KC074913.php	Malicious URL
hxxps://31.210.111.154/Microsoft/Update/KS081274.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /Microsoft/Update/KS1945777.php	Malicious URL
hxxps://146.0.74.7/l7vogLG/BVZ99/rt170v/solocVI/eegL7p.php	Malicious URL
hxxps://148.251.82.21/Microsoft/Update/KS4567890.php	Malicious URL
hxxps://188.40.8.72/l7vogLG/BVZ99/rt170v/solocVI/eegL7p.php	Malicious URL
hxxps://31.210.111.154/Microsoft/Update/KS081274.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /Microsoft/Update/KC074913.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /Microsoft/Update/KS1945777.php	Malicious URL
hxxps://xxx.xxx.xxx.xxx /fHKfvEhleQ/maincraft/derstatus.php	Malicious URL
DropBear.exe	Malware Variant Observed
Pnoto_e.exe	Malware Variant Observed
Pservice_PPD.exe	Malware Variant Observed
Starter.exe	Malware Variant Observed
tsk.exe (PC)	Malware Variant Observed

Both ESET and CERT-UA link Industroyer2 (as well as the original Industroyer and at least some of the wiper events in Ukraine in 2022) to the Sandworm actor, linked to GRU post 74455. Previous reporting and government disclosures also linked Sandworm to the 2015 power event, and the use of BlackEnergy3 malware. Re-use of a specific process name or string would therefore appear to be a very strange mistake in operational security – or it could represent some degree of "victim trolling" by threat actors.

The name itself has no significance or function beyond the BlackEnergy3-Industroyer2 connection. Why this appears is an open question, and likely one that will never be satisfactorily resolved. However, this instance may be an interesting cyber threat intelligence counter-example of where indicator-like alerting (e.g., on specific filenames or references to specific processes) may actually be a reasonable defensive measure for identifying certain adversaries.

Relationship to Wider Operations and Events

When Russia initiated its terrible invasion of Ukraine in late February 2022, commentators and analysis anticipated early operations to feature significant cyber components. While some effects certainly were observed and others discovered after collection of more evidence, many expected to observe critical infrastructure disruption along the lines of the 2015 and 2016 power events. That such an impact was *attempted* but only over a month into the conflict seems exceptionally strange, and defies expectations and assumptions around when to deploy such capabilities in conjunction with more traditional military operations.

First, while we cannot say this with complete confidence, it does appear that initial Russian plans for invading Ukraine envisioned a relatively quick decapitation of national leadership and centers of gravity, centered around the sack of Kyiv. As part of this operation, one can assume that leaving critical infrastructure largely intact was probably an initial requirement to facilitate occupation and subsequent installation of a puppet regime. As Russia's incompetence and Ukraine's bravery stymied these plans, a noticeable shift to indiscriminate attacks on population centers and infrastructure was observed. That a latent capability such as power system-targeting malware would be unleashed after such initial aims failed may therefore make sense, along the lines of similar questionable Russian decisions such as using sophisticated anti-ship cruise missiles to target stationary targets on land.

Changing war aims aside, at the start of the conflict Ukraine's electric sector remained linked to Russian grid operations. Coinciding with the start of Russia's invasion, Ukrainian operators initiated an isolation test from Russian grid operations, and subsequently decided to not reconnect. While separating Ukraine from Russian grid operations, this also left Ukraine's grid isolated and thus more easily susceptible to disruption. Russian operations to capture electric infrastructure, such as events in Chernobyl and Zaporizhzhia, could thus give Russia ready control over Ukrainian electric operations, or at least significant influence over them.

This changed in mid-March, when Ukraine (and Moldova) successfully connected to the European electric grid under ENTSO-E. As stated previously, this timing is interesting as some suspected disruptive events appeared to take place immediately after this switchover. But with Ukraine now part of the wider European electric system, unilateral options for

Russia to control or manipulate Ukrainian electric operations were removed, or significantly reduced. Thus the timing of Industroyer2 after not just the start of the conflict, but also after integration with ENTSO-E, makes more sense in light of these changes.

Conclusions

Many details surrounding Industroyer2 and related (attempted) attacks on Ukrainian electric infrastructure are unavailable, but sufficient information has emerged to allow for the preliminary observations above. Overall, the evolution of operations in Russia's invasion of Ukraine show that many assumptions surrounding the use of cyber capabilities as part of a conventional conflict require revision – but at the same time, we should also note that cyber has been far from absent as part of hostilities. While paling in comparison to Russia's physical brutality, cyber operations appear to form a continuing area of interest and investment for Russia in attempting to achieve its goals in Ukraine.

With time and additional data, the items above can be revisited and improved. I would caution anyone reading this, or any other, analysis that in the case of both the 2015 and especially the 2016 power incidents in Ukraine, reasonably complete understanding of these events did not occur until years after the events in question. Especially given the difficulties of network defense, forensics, and electric system operations in the middle of an invasion, researchers would do well to be patient with matters such as this, and maintain a willingness to revise conclusions appropriately as more information emerges.

Overall, Industroyer2 represents an interesting and important development surrounding the broader violence Russia is inflicting upon Ukraine. Given that the malware did not result in a disruption of service, other asset owners and operators should take note that robust, alert operations are critical in maintaining sufficient defense and resilience in the face of critical infrastructure threats. We can learn much from Ukraine's efforts in this conflict, not the least of which being how to maintain fundamental civilian services even in the face of a brutal, all-out assault.

Technical Details

While CERT-UA and ESET published some indicators related to Industroyer2, some other samples appeared with equivalent functionality that were not previously identified in original reports. The following table provides a list of known Industroyer2 samples and potential variants.

File Name	SHA1	Note
108_100.exe	FD9C17C35A68FC505235E20C6E50C622AED8DEA0	Industroyer2 variant listed by ESET, CERT-UA.
40_115.exe	FDEB96BC3D4AB32EF826E7E53F4FE1C72E580379	Industroyer2 variant discovered on VirusTotal.
N/A	39B27DE81915B748EC56D1C5DF7E017B4A20323B	Possible researcher modification of available sample.
N/A	1574A402E5604F17BC0068F196D8BCDCB05286E7	Possible researcher modification of available sample.

Acknowledgments

Huge thanks to the teams at ESET and CERT-UA for disclosing information for defenders and enabling this analysis, as well as the team at MSTIC for their continued support of Ukrainian defenders. Special thanks to Dan Gunter and InsaneForensics for enabling protocol analysis of available Industroyer2 samples in a functioning lab environment.