De cyber aanval op Oekraïene

## Inleiding

Doel van dit verslag is inzage te geven in de informatieverzameling en begrip van een complex scada systeem. De lezer krijgt inzage in de achtergrond achter cyberaanval, de gebruikte technieken en een opsomming van oplossingen en methoden voor beveiligingsvraagstukken.

## Algemeen

18 maart 2016 werd er een onderzoek gepublicerd van de E-ISAC. Een rapport met veel aanbevelingen waar ik in dit verslag alleen de aanbevelingen overneem voor een mitigatiestrategie.

<https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf>

analyse en mitigatiestrategie

<https://na.eventscloud.com/file_uploads/aed4bc20e84d2839b83c18bcba7e2876_Owens1.pdf>

In dit artikel wordt beweerd dat medewerkers op afstand konden inloggen op het SCADA netwerk en medewerkers op de netwerken voor Supervisory Control and Data Acquisitie hadden geen dubble- authorisatie nodig om in te loggen in het systeem.

<https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

<http://web.mit.edu/smadnick/www/wp/2016-22.pdf>

<https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack>

<https://www.wired.com/story/russian-hackers-attack-ukraine/>

<https://www.linkedin.com/notifications/>

<https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf>

<https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm-idUSKBN0UM00N20160108>

<https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>

<https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html>

Een overheidsinstantie van de Verenigde Staten biedt op haar website tekst en uitleg over een malware analyse van BlackEnergy malware.

<https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01>

Doel

Motivatie

## Opvallendheden

Na een analyse van bronnen die openbaar zijn gemaakt door instanties na onderzoek naar de stroomuitval bij energiebedrijven door media en onderzoekers is het duidelijk dat cyberaanvallen de oorzaak waren voor de stroomuitval in Oekraien. Het SANS ICS team heeft discussies gevolgd die gevoerd zijn door verschillende partijenen en organisaties in de internationale gemeenschap. Met enige zekerheid kan worden vastgesteld dat op basis van bedrijfsverklaringen, media rapportages, en eerstehand analyses he incident is veroorzaakt door een internationaal gecoordineerde aanval.

De aavallers tonen hierbij aan door planning, coordinatie, in combinatie met het gebruik van malware en de directe toegang op afstand de systeemcoordinators kunnen omzeilen. En erin slaagden de distributie van het elektriciteitsnetwerk te manipuleren en de resteloperaties voor de SCADA servers te vertragen nadat de schade op trad. De aanval bestond uit drie componenten: de malware, een Dos-aanval en een nog onbekend sluitend bewijststuk waarmee de impact werd geinitieerd. Huidige bewijsvoering suggerreert dat het missende component een directe interactie was van de aanvaller en niet het werk van malware.

De aanval werd bewerkstelligd door verschillende elementen waaronder de beperkingen voor ysteemcoordinators en het asluiten van telefoonlijnen om de ommunicatie naar buiten te saboteren. Met hoge zekerheid kan worden gesteld dat een coordinatie was waarbij meerdeere reginale energiecentra weden aangevallen.

Bij het uitvoeren van herstlwerkzaamheden werd er rekening gehouden met SCADA systemen die steeds geinfecteerd waren met malware. Medewerkers ter plaatse konden meedelen dat de substattions die werden aangevallen allemaal handmatig in plaats van automatisch werden herstart. De herstelwerkzaamheden duurden tussen de 3 en 6 werkuren.

Waarom is het aannemelijk dat malware wel is geactiveerd maar uiteindelijk niet de oorzaak was?

Er zijn twee theorien waarvan deeerste theorie beweert dat de KillDisk component aanwezig was in het netwerk maar niet de oorzaak was van de stroomuitval. De tweede theorie beweert dat de ‘KillDisk’ de directe oorzaak was voor het stroomuitval. Onderzoekers van SANS ICT beweren dat geen van beide theorien kloppen. Zij komen tot de conclusie dat malware de aanval mogelijk heeft gemaakt, de intentionele aanval, maar dat de KillDisk niet de oorzaak is geweest. De media gaat uit van BlackEnergy malware en het Sandworm team dat achter de aanval zou zitten. Maar het kan niet met zekerheid vastgesteld worden dat de excel bestanden die zijn aangetroffen bij de aanval samen met andere malware betrokken waren bij dit incident. Onderzoekers van SANS gaan er vanuit dat de malware bedoelt was om informatie uit bestanden te verzamelen di het mogelijk maken om de SCADA systemen niet te egbruiken of het gebruik daarvan te vertragen. Argument dat hiervoor is opgevoerd is dat de impact die is geconstateerd niet relateerd aan de schade van eerdere aanvallen waar dergelijke malware werdt gebruikt. Er wordt namelijk gesteld dat het draaien van een systeem zonder de voordelen die SCADA nou eenmaal biedt de risico’s op distributieniveau verhoogt maar zonder een status-wijziging kan er nog steeds stroom geleverd worden.

<https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/>

<https://www.reuters.com/article/us-ukraine-cybersecurity-sandworm/u-s-firm-blames-russian-sandworm-hackers-for-ukraine-outage-idUSKBN0UM00N20160108>

<https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN>

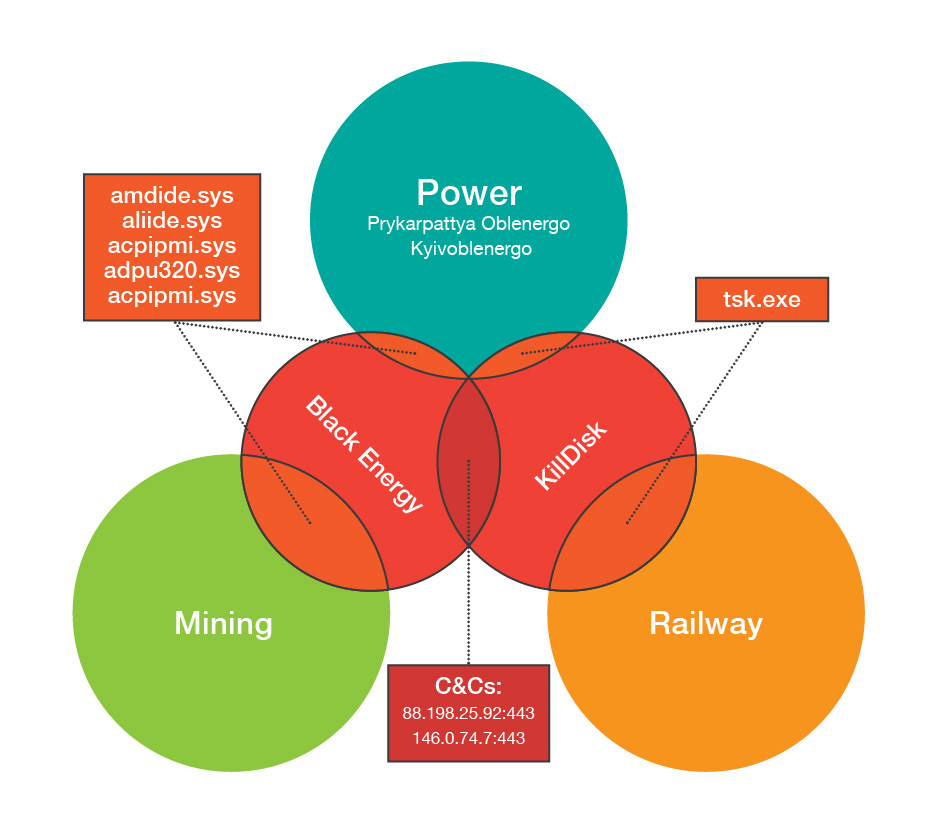
<https://www.wired.com/2014/10/russian-sandworm-hack-isight/>

<https://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/>

Dit artikel schets een situatie waarin er een overlap is van 5 samples van malware tussen de verschillende malware van het typpe BlackEnergy die is gebruikt bij de aanval op de krachtcentra en de mining-industrie in Oekraine.

In mindere mate is er een spilover van het gebruik van KillDisk bij de aanval op de mijn-sector en de aanval op de krachtcentralen.

Overal genomen is er een overlap bij het gebruik van malware als er gekeken wordt naar de naming-conventies, type malware, infrastructure en het tijdsslot waarin de malware werd gebruikt. Maar er wordt geen hard bewijsgeleverd wat de actieve rol was van de malware in de diverse fasen van de aanval.



<https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/>

<https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf>

<https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/>

<https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802>

<https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf>

<https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf>

Speculaties

Vermoedelijk cybercriminelen en staatsactoren

## BlackEnergy

Is een destructieve malware vermoedelijk ontwikkeld in Rusland en wijdverspreid in industriele systeemtechnologie. (ukraine-power-grid-attack-russia-us, 2016)

In December 2014, DHS concerned that a BlackEnergy 3 malware variant was present in a Ukraine energy system that was attacked, causing a power outage. In December 2014 was de United States Department of Homeland Security op de hoogte gesteld van een variant van BlackEnergy 3 die werd gevonden in een Oekraiense energy ststeem, met als gevolg een stroomuitval.

ICS-CERT published a special TLP Amber version of an alert containing additional information about the malware, plug-ins, and indicators to the DHS secure portal website. ICS-CERT publiceerde een special document met daarin een waarschiw en additionele informatie over het virus, de plug-ins, en verwijzingen naar de website van de veiligheidsdienst zelf.

ICS-CERT strongly encouraged asset owners and operators to use the indicators to look for

signs of compromise within their control system environments. ICS-CERT drong er sterk op aan dat eigenaren van dergelijke netwerken en installates en operators werkend aan die systemen signalen in hun eigen controlesystemen moeten controleren op indicaties.

## Ukraine Power Grid

Wat dit onderzoek niet bevat is een theorie over de betrokkenheid van een organisatie bij het uitvoeren van een dergelijke aanval zoals omschreven in het volgende artikel. Reden hervoor is dat de identificatie van een organisatie of rechtspersoon bedoeld is om een verantwoordelijke te beschuldigen voor een cyberaanval. Uit openbare bronnen die niet direct gelukt zijn aan bijvoorbeeld de amerikaanse autoriteiten blijkt dat de organisatie Sandworm voor de aanval verantwoordelijk wordt gehouden sinds haar activiteiten in oktober 2014.

(rand.org, sd)

De cuberaanval wordt op de voeten gevolgd door de amerikaanse inlichtingendiensten en de FBI omdat amerikaanse industriele complexen dezelfde kwetsbaarheden tonen als de systemen die actief gebruikt zijn in Oekraine. Het is daarmee ook de eerste cyberaanval met als gevolg de beinvloeding van de burgerbevolking en een aanslag op relevante kritische bedrijven en sectoren. De destructieve malware is volgende onderzoekers van Trend Micro ook gevonden bij mijnwinningsbedrijven en spoorwegbedrijven in de Oekraine.

(ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E, sd)

Example 1: Attack on the Ukraine distribution system operator in 2015 The electric power sector was forced to take a more aggressive approach to cybersecurity following the 2015 attack on the Ukrainian power grid, affecting 27 substations and approximately 225,000 end customers. Aanval o de oekraiense dissitributie operator in 2015. De elektrische energie-industrie werd gedwongen een regireuze aanpak op te zetten voor de de komende aanval in 2015 op het oekraiense electriciteitsnet, met invloed op 27 substations waar 225000 op waren aangesloten.

Target was the Ukrainian electricity distribution company Kyivoblenergo. Doel van de aanval was het oekraiense electriciteitsdistributiebedrijf Kyivoblonergo.

The attack can be classified as an advanced persistent threat (APT) and resulted in a disruption of service and blackout. De aanval kan worden gezien al seen geavanceerde aanhoudende dreiding and resulteerde in de verstoring van service en uiteindelijk een black-out.

The attackers used targeted emails carrying weaponised visual basic for application (VBA) Microsoft Word and Excel attachments. De aanvallers gebruikten emais met als bijlage een visual basic applicatie (macro) voor Microsoft Word en Excel bijlage.

Opening the files by employees installed a specific remote access tool (RAT) / malware, BlackEnergy3, on the workstations. Het openen van de bestanden door de medewerkers installeerde specifieke malafiede malware genaamd BlackEnergy3 op het bediedingspaneel.

From there the attackers got access privileges for at least 6 months until they fully deployed specially crafted malware to the SCADA and field system enabling them to affect multiple substations. Hierdoor kregen de aanvallers toegang voor ten inste 6 maanden tot priveleges tordat zij hun speciaal ontwikkelde malware installeerden op het SCADA systeem waarmee zij meerde substation konden besturen.

Finally, they were able to open a series of breakers of multiple substations, triggering the blackout. Seven 110 kV and twentythree 35 kV substations were disconnected. Uiteindelijk waren zij instaat enkele systeembrekers van meerdere substations te openen, waardoor er een blackout ontstond. Seven substations van 110kV an 23 van 35 kV warden Hiermee losgekoppeld

This incident received global attention and helped spread public awareness to the vulnerabilities of electric power systems. Dit incident wierp de aandacht op van media over de gehele wereld en stimuleerde het bewustzijn over de kwestsbaarheden van electrische energiesystemen.

A subsequent attack in December 2016 further exasperated industry concerns, with the country’s power grid quickly becoming a test bed of sorts for cyberattacks. Een volgende aanval in December 2016 maakt de industrie geirriteerd, met het gevaar van het nationale elextriciteitsnet in de nabije toekomst mogelijk als testomgeving viir een verscheidenheid aan soorten cyberaanvallen.

<https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf>

## Artikel: History of Industrial Control System Cyber Incidents door Kevin E. Hemsley, Dr. Ronald E. Fisher

In 2015, two days before Christmas, a cyber-attack cut electricity to nearly a quarter-million Ukrainians. In 2015, twee dagen voor kerstmis, was er een cyber-aanval waarmee de elektriciteit voor bijna eeen kwart miljoen oerkrainers wegviel.

This is the \_rst known successful cyber-attack on a power grid. Dit was de eerste bekende succesvolle cyberaanval op een electriciteitsnet.

Reuters reported that a power company located in the western portion

of the Ukraine suffered a power outage, which impacted a large area that

included the regional capital of Ivano-Frankivsk [55]. Reuters reporteerde da teen bedrijf in het westerse deel van Oekraine las had van een enorme uitval, met een impact op een groot deel dat viel in de regionale hoofdstad van Ivano\_Frankivsk.

Attackers shut off power at 30 substations and left 230,000 people without electricity for

up to six hours. Aanvallers zetten de stroom uit op 30 subcentrales en lieten 230000 mensen zonder elektriciteit voor meer dan 6 uur.

SCADA equipment was rendered inoperable, and power

restoration had to be completed manually|further delaying restoration

efforts [56]. SCADA materieel werd onklaar gemaakt, and stroomherstel moest handmatig worden bewerkstelligd, waardoor de herstart nog meer vertraging op liep.

Investigators discovered that attackers had facilitated the outage by

using the BlackEnergy malware to exploit the macros in Microsoft Excel

documents. Onderzoekers kwamer erachter dat de aanvallers een stroomuitval hadden bewerkstelligd door het gebruik van BlackEnergy3 malware te gebruiken als exploit in de macro’s van een Microsoft Excel document.

The malware was planted onto the company's network using

spear-phishing emails [57]. De malware werd ingebracht in het bedrijfsnetwerk door het versturen van spear-phising emails.

ICS-CERT and US-CERT worked with the Ukrainian CERT and international partners to analyze the malware and con\_rmed that a BlackEnergy 3 variant was present in the Ukrainian

power system [52].

ICS-CERT en US-CERT werkten samen met de oekraiense CERT en international partners om de malware te analyseren, en daaruit bleek date r een BlackEnergy 3 variant aanwezig was in het oekraiene energiesysteem.

The Ukrainian intelligence community blamed theattack on Russian attackers [58]. De oekraiense veligheidsdiensten hielden russische hackers verantwoordelijk voor de aanval.

BlackEnergy has been publically identified by DHS and the FBI to be part of the RIS GRIZZLEY STEPPE

[59] group. Door de Department of Homeland Security en de FBI is vastgesteld dat de BlakEnergy onderdeel is van de RIS GRIZZLEY STEPPE.

At the request of the Ukrainian government, a U.S. interagency team comprised of representatives from ICS-CERT and US-CERT, as well as DOE, the FBI, and the North American Electric Reliability Corporation, traveled to the Ukraine to gather information about the incident and identify potential mitigations [33]. Op verzoek van de oekraiense overheid, is een ameriaans agentschap naar oekraine gereisd om informatie te verzamelen over het incident en om doelen voor een mitigatiebeleid te formuleren.

This attack taught the world that it is indeed possible to damage the power grid through a cyber-attack, and was a wake-up call to ensure that the U.S. power grid is forti\_ed against such attacks. De aanval heft de diensten geleerd dat het mogelijk is schade aan een electriciteitsnet toe te brengen door middel van een cyber-aanval, en dat was een wake-up-callom er bivoorbeeld voor te zorgen dat de VS zijn eigen elexctriciteitsnet goed beveiligd.

In the case of the Ukraine, the attackers used technically unsophisticated techniques to achieve their goal. In het geval van Oekraiene, gebruikten de aanvaller niet zeer geavanceerde technieken om hun doel te bereiken.

The Ukraine power grid attack was a signi\_cantevent in cyber-history. De aanval op het oekraiense elektriciteitsnet bleek een mijlpaal in de cyber-geschiedenis.

Opportunities

Multiple opportunities existed for the adversary to execute its attack. Er waren vele mogelijkheden voor de aanvallers om een aanval uit te voeren.

External to the oblenergos and prior to the attack, there was a variety of open‐source information available; including a detailed list of types of infrastructure such as Remote Terminal Unit (RTU) vendors and versions posted online by ICS vendors. Buiten de oblenergos en voordat de aanval plaatsvond, waren er verschillende open-source bronnen beschikbaar; waaronder een gedetailleerde lijst van typen infrastructuur zoals een Remote Terminal Unit(RTU) verkopers en versies online gezet door ICS verkopers.

19 The VPNs into the ICS from the business network appear to lack two‐factor authentication. De VPNs in de ICS van het business network bleken een gebrek een multi-factor authenticatie te hebbem.

Additionally, the firewall allowed the adversary to remote admin out of the environment by utilizing a remote access capability native to the systems. Daarnaast, is het opmerkelijk ten noemen dat de firewall toestind dat de aanvaller op afstand administratierechten had buiten de werkomgeving simpelweg via remote access capability op de systemen zelf.

In addition, based on media reporting, there did not appear to be any resident capability to continually monitor the ICS network and search for abnormalities and threats through active defense measures; like network security monitoring. Daarbovenop, blijkt uit media bronnen date er geen mogelihjkheid bleek om het ICS netwerk te monitoren en te zoeken naar afwijkingen and bedreidingen door actieve defensieve maatregelen.

These vulnerabilities would have provided the adversary the opportunity to persist within the environment for six months or more to conduct reconnaissance on the environment and subsequently execute the attack. Door deze kwestbaarheden is er een situatie ontstaan waarbij de aanvaller de mogelijk had om in de omgeving voor een periode van 6 maanden verkeningen te doen, informatie op te slaan en uiteindelijk een aanval uit te voeren.

20 Based on the details provided in the DHS report, the adversary used a consistent attack approach on all three impacted targets. Op basis van een gedetaileerd DHS rapport, heft de aanvaller een consistente aanpak voor alle drie specifieke doelen.

The adversary also used consistent tactics to impact field controllable elements and irreparably damage field devices. De aanvaller gebruikte een consistnete tactiek om coontrole-elementen de beinvloeden en uitwisbare schade toe te brengen aan onderdelen.

Why these oblenergos were targeted remains an open debate. Waarom precies deze oblenergos werden aangevallen is nog punt van discussie.

Based on the public reporting, it is unknown if the targets were selected based on common technologies in use, system architectures, reconnaissance operations, or service territories. Publieke media rapportreren dat het niet bekend is of de doelen zijn uitgekozen op basis van de gebruikte technologie, systeemarchitectuur,verkenningsoperaties, of dienstverledende fucntie aan het achterland.

Opportunity‐based considerations for selecting a specific target may focus on an attacker’s confidence and ability to cause an ICS effect. Opportunische argumenten voor het selecteredenvan een spcidifiek doel zou kunnen zijn dat de aanvallers genoeg vertrouwen en mogelijkheden hadden om een opmerkelijk effect te hebben op de werking van de ICS.

Voorbeelden van argumenten voor een keuzen kan zijn:

Some example decision factors could include:

• Targets with common systems and configurations

• Multiple systems with common centralized control points

• ICS impact duration estimates (e.g., long term orshort term)

• Existing capabilitiesrequired to achieve desired results

• Risk level of performing the operation and being discovered

• Achieved access and ability to move and act within the environment

bron: <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>

## Second Attack on the Ukraine Power Grid

Ook de tweede aanval op oekrainse kritische infrastructuur wordt toegerekend aan Sanndstorm. De KillDisk software die hier wordt gevonden wordt vergelijken met de software die gevonden werdt bij de hack op de Ukraiense verkiezingen in oktober 2015. (2016 ) KillDisk software verwijidert bestanden op de schijf, in dit geval van de systeemoperators. Maar dat niet alleen. KillDisk verwijdert ook de master boot record. Zodoende konden de computers crashen maar niet rebooten.

On December 17, 2016, almost one year after Ukraine suffered a major cyber-attack on its power grid, Kiev suddenly went dark again. Op 17 december 2016 bijna een jaar na de cyberaanval op het electriciteitsnet van oekraiene, was er weer een stroomuitval.

Cyber-attackers caused monitoring stations to suddenly go blind.

Break-ers tripped in 30 substations, turning o\_ electricity to approximately 225,000 customers. De breakers van 30 subbstations sloegen op hol, daardoor zaten ongeveer 225000 gebruikers zonder stroom.

To prolong the outage, attackers also launched a telephone denial-of-service attack (TDoS) against the utility's call center to prevent customers from reporting the outage, the same tactic that was used in 2015. Om de uitval te verlengen voerden de aanvallers eenn TDOS aanval uit., tegen het callcentrum van het hulpprogramma om te verkomen dat er telefonisch gerapporteerd kon worden over de schade.

The intruders also rendered devices, such as serial-to-Ethernet convertors, inoperable and unrecoverable on their way out to make it harder to restore electricity to customers [64]. De aanvallers zijn ook de serial-to-Ethernet schakelingen binnengedrongen en maakten deze onbruikbaar en niet-herstelbaar zodat het moeilijker werd om het stroom te herstellen.

Despite these setbacks in the original attack, power was restored in three hours in most

cases, but because the attackers had sabotaged management systems, workers had to travel to substations and manually close breakers the attackers had remotely opened [56], [57]. Ondanks al deze tegenslagen was de electriciteit binnen 3 uur hersteld in de meeste gevallen althans, maar omdat de aanvllers het management systeem hadden gesaboteerd moesten de operatos handmatig alle breakers sluiten.

However, the second attack was much more sophisticated than the first [64]. De tweede aanval was geraffineerder dan de eerste.

Where the first attack used remote control software to manually trip breakers, the second is believed to have used sophisticated malware that directly manipulated SCADA systems. Waar de eerste aanval gebruik maakte van remote control software om de breakers te dereguleren, is er bij de tweede aanval gebruik gemaakt van geavanceerde malware die direct de SCADA systemen manipuleerde.

Rob Lee with Dragos Security said, In my analysis, nothing about this attack looks like it's singular.

The way it's built and designed and run makes it look like it was meant to be used multiple times. And not just in Ukraine" [65].

The sophisticated malware used in that second attack would later be identi\_ed as

CRASHOVERRIDE." De malware die bij de tweede aanval werd gebruikt is later bekend geidentificeerd als CRASHENERGY.

Dragos Security, working in coordination with the Slovak anti-virus \_rm ESET, confirmed that the CRASHOVERRIDE (or \Industroyer") malware was indeed employed in the December 17, 2016, cyber-attack on a Kiev, Ukraine transmission substation, which resulted in the large power outage [65], [66]. Dragos Security in samenwerking met het slovaakse anti-virus bedrijf ESET, besestigde dat CRASHOVERRIDE malware werd gebruikt bij de aanval van 17 december 2016 op eenUkraiense transmissie substation in kiev, waarmee een stroomuitval werd verooraakt.

According to Dragos, CRASHOVERRIDE was the first ever malware framework specifically designed and deployed to attack electric grids. Volgens Dragos was CRASHOVERRIDE de este malware die specifiek ontwikkeld is vooreen aanval op een electrisch netwerk.

It is the fourth-ever piece of ICS-tailored malware used against specific targets, with Stuxnet, BlackEnergy-2, and Havex being the first three. Het is de vierde soort ICS malware gebruitk naa Stuxnet, BlackEnergy-2 en Havex.

It is the second malware ever designed and deployed for disrupting physical industrial processes, with Stuxnet being the first [65]. Het is de tweede malware ooit ontwikkeld en ingezet voor verstoring van industriele processen, waarbij Stuxnet de eerste was.

Dragos also stated that the functionality in the CRASHOVERRIDE framework serves no

espionage purpose, and the only real feature of the malware is for attacks leading to electric outages. Dragos beweerde dat de functionaliteit in het CRASHOVERRIDE raamwerk spionage doeleinden heeft, maar dat de enige feture van de malware is om stroomuitval te veroorzaken.

The CRASHOVERRIDE malware is a framework that has modules specific to ICS protocol stacks, including IEC 101, IEC 104, IEC 61850, and OPC. De CRASHOVERRIDE malare is een raamwerk dat bestaat uit modulen specifiek voor ICS protocollen waaronder IEC 101, IEC 104, IEC 61850 en OPC.

It is designed to allow the inclusion of additional payloads

like DNP3, but at the time, no such payloads had been confirmed. Het is ontworpen voor het gebrik en implementatie van payloads zoals DNP3.

The malware also contained additional non-ICS specific modules, such as a

wiper, to delete \_les and disable processes on the running system for a

destructive attack to operations [65]. De malware bevat ook non-ICS modules, zoals een wiper, voor de verwijdering van bestanden en het uitschakelen van processen op een draaiend system om zo operaties te verstoren.

The modules in CRASHOVERRIDE are leveraged to open circuit

breakers on remote terminal units (RTUs) and force them into an infinite

loop to keep the circuit breakers open, even if grid operators attempted

to close them, which resulted in the de-energization of substations forcing

grid operators to switch to manual operations in order to restart power

[65]. De modules in CRASHOVERRIDE zijn erop gebouwd om circuit breakers te openen aangesloten op remote terminal units, ook wel RTU’s genaamd, in deze om te zetten in een oneindige loop zodat de circuit breakers open blijven staan, ookal doen de operators een poging deze te sluiten, met als doel dat de operators de handeling handmatig moet uitvoeren om te herstarten.

Dragos says there are concerns CRASHOVERRIDE could be lever-

aged to disrupt grid operations that would result in power outages lasting

hours. DRAGOS beweert date r zorgen zjin dat CRASHOVERRIDE niet alleen ervoor kan hebben gezorgd dat de grid operaties ontregeld werden waardoor de urenlange stroomstoring ontstond.

They assess that power outages could last up to a few days if an attack targeted multiple sites. Ze benadrukken dat de stroomuitvallen meerdere dagen konden duren als de aanval io meedere licaties werden uitgevoerd

However, Dragos also pointed out that there is no evidence that threat actors could use CRASHOVERRIDE to cause any power outages to last longer than that. Nochtans, DRAGOS steld ook dat er geen bewijs is dat de aanvallers CRASHOVERRIDE konden gebruiken om een stroomuitval te bwerkstelligen die langer duurt dan dat.

But to even get a few days of power outages would require the targeting of multiple sites

simultaneously, which is entirely possible, but not trivial [65]. Maar zelfs al ser een stroomuitval van enkele dagen zou zijn dan zoudeen meerde lccaties simultaan moeten zijn aangevallen

Using the National Cyber Awareness System (NCAS), DHS issued a

CRASHOVERRIDE malware Technical Analysis alert on June 12, 2017, notifying U.S. critical infrastructure of the serious threat the malware poses [67].

The significant takeaway from the discovery of CRASHOVER-

RIDE is that nation state threat actors have created an advanced reusable

malware framework specifically designed to cause power outages.

This same threat actor has demonstrated on multiple occasions that it is willing and able to cause power outages through cyber-means.

bron:

<https://www.osti.gov/servlets/purl/1505628>

crashoverride ukraine

<https://www.cybersecurityintelligence.com/blog/attack-on-ukraines-power-grid-targeted-transmission-stations-4530.html>

<https://www.recordedfuture.com/crashoverride-malware-overview/>

<https://www.us-cert.gov/ncas/alerts/TA17-163A>

<https://www.darkreading.com/threat-intelligence/first-malware-designed-solely-for-electric-grids-caused-2016-ukraine-outage/d/d-id/1329114>

<https://arstechnica.com/information-technology/2017/06/crash-override-malware-may-sabotage-electric-grids-but-its-no-stuxnet/>

<https://www.accenture.com/_acnmedia/pdf-69/accenture-managing-malware-crash-override.pdf>

<https://www.nixu.com/fi/node/53>

<https://www.vice.com/en_us/article/zmeyg8/ukraine-power-grid-malware-crashoverride-industroyer>

Anatonomy of an attack

<https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf>

modular ICS Malware

<https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf>

win32/industroyer

<https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf>

<https://collaborate.mitre.org/attackics/index.php/Software/S0001>

<https://www.webopedia.com/TERM/C/crashoverride-industroyer-malware.html>

<https://rhebo.com/en/service/glossar/industroyer-25114/>

<https://www.fda.gov/media/123073/download>

<https://www.waterisac.org/portal/new-vulnerability-discovery-reportedly-abuses-same-protocol-used-industroyercrashoverride>

<https://www.eweek.com/security/industroyer-cyber-attack-revealed-as-cause-of-ukraine-power-outage>

has been described as a sophisticated modular malware that has several components: a backdoor, a launcher, a data wiper, various tools, and at least four payloads. These payloads are the most interesting component as they allow the malware’s operators to control electric circuit breakers.

In one theoretical attack scenario described by Dragos in its report, malicious actors use the malware to open closed breakers in an infinite loop, causing the substation to de-energize. By executing commands in an infinite loop, the attackers ensure that operators of the targeted facility cannot close the breakers from the HMI. This can require operators to interrupt communications with the substation and manually address the issue, which could result in an outage that lasts for a few hours.

In another scenario described by researchers, the attackers initiate an infinite loop where breakers continually open and close, which can trigger protections and cause the substation to go offline. Experts believe that launching such an attack in a coordinated fashion against multiple sites could result in outages that last for a few days.

Industroyer/CRASHOVERRIDE components

The malware’s main backdoor component allows attackers to execute various commands on the infected system. It communicates with its command and control (C&C) servers over the Tor network and it can be programmed to be active only at specified times, which are likely mechanisms for avoiding detection.

This component also deploys a secondary backdoor disguised as a trojanized version of the Windows Notepad application. The main backdoor is also responsible for installing the launcher component, which initiates the wiper and the payloads.

Learn More at SecurityWeek’s ICS Cyber Security Conference

The wiper is apparently designed for the final stages of the attack to help the attackers hide their tracks and make it more difficult to restore affected systems. This includes clearing registry keys, and overwriting ICS configuration and Windows files.

The payloads, which allow attackers to control circuit breakers, leverage industrial communication protocols. This suggests that at least some of the malware’s developers have a deep understanding of power grid operations and industrial network communications.

Other tools tied to the Industroyer malware include a custom-built port scanner and a denial-of-service (DoS) tool that exploits CVE-2015-5374 to cause Siemens SIPROTEC relays to become unresponsive.

<https://www.securityweek.com/industroyer-ics-malware-linked-ukraine-power-grid-attack>

threat profile

<https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/crashoverride/>

<https://www.cfr.org/cyber-operations/compromise-causes-power-outage-kiev-ukraine>

<https://blog.paloaltonetworks.com/2017/06/crashoverrideindustroyer-protections-palo-alto-networks-customers/>

Scalable and Modular Implementation of Scenario-based Cyber Attacks and Defense Methodologies on CPS Security SCADATestbed

<https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1126&context=creativecomponents>

<https://www.nti.org/analysis/atomic-pulse/crash-override-could-similar-cyber-weapon-be-used-against-nuclear-facility/>

overview of malware

<https://www.zdnet.com/pictures/the-worlds-most-famous-and-dangerous-apt-state-developed-malware/6/>

<https://money.cnn.com/2017/07/28/technology/future/crashoverride-black-hat-blackouts-energy-grid/index.html>

<https://www.cnet.com/news/lights-crash-power-grid-industroyer-malware-blackout-override/>

<https://www.vtechsolution.com/crash-override-the-blackout-causing-cyber-super-weapon/>

<https://www.esecurityplanet.com/threats/malware-behind-ukraine-blackout-analyzed.html>

<https://www.vtechsolution.com/crash-override-the-blackout-causing-cyber-super-weapon/>

Dragos says its extensible design means adding a DNP3 stack would allow it to be used in the US, as well as adapted for use in other industries – “but the adversaries have not demonstrated the knowledge of other physical industrial processes to be able to make that assessment anything other than a hypothetical at this point, and protocol changes alone would be insufficient.” There is apparently no mechanism for espionage, with Dragos saying that the main purpose of the malware is just for attacks.

So, what we have is a modular malware toolkit that could be adapted to include different protocols as part of its attack, should the attackers be familiar enough with the system architecture of a particular industry. In this instance, it was used to flip circuit breakers in transmission substations to cause blackouts, but it could feasibly be used to shut down factories or other utility systems.

CrashOverride used the same approach as Stuxnet to understand the industrial processes at play, exploited the same OPC protocol as Havex, and the same library and configuration file attack vector used in BlackEnergy 2 – which targeted the HMI machines that were connected to the internet. Topping things off, CrashOverride displayed the same knowledge of the grid operations as the December 2015 attacks in Ukraine.

“It did all of these things with added sophistication in each category, giving the adversaries a platform to conduct attacks against grid operations in various environments and not confined to specific vendor platforms. It marks an advancement in capability by adversaries who intend to disrupt operations – they are growing in their ability to learn industrial processes and codify and scale that knowledge, and defenders must also adapt.”

<https://rethinkresearch.biz/articles/industroyer-crashoverride-malware-behind-ukraine-utility-attack/>

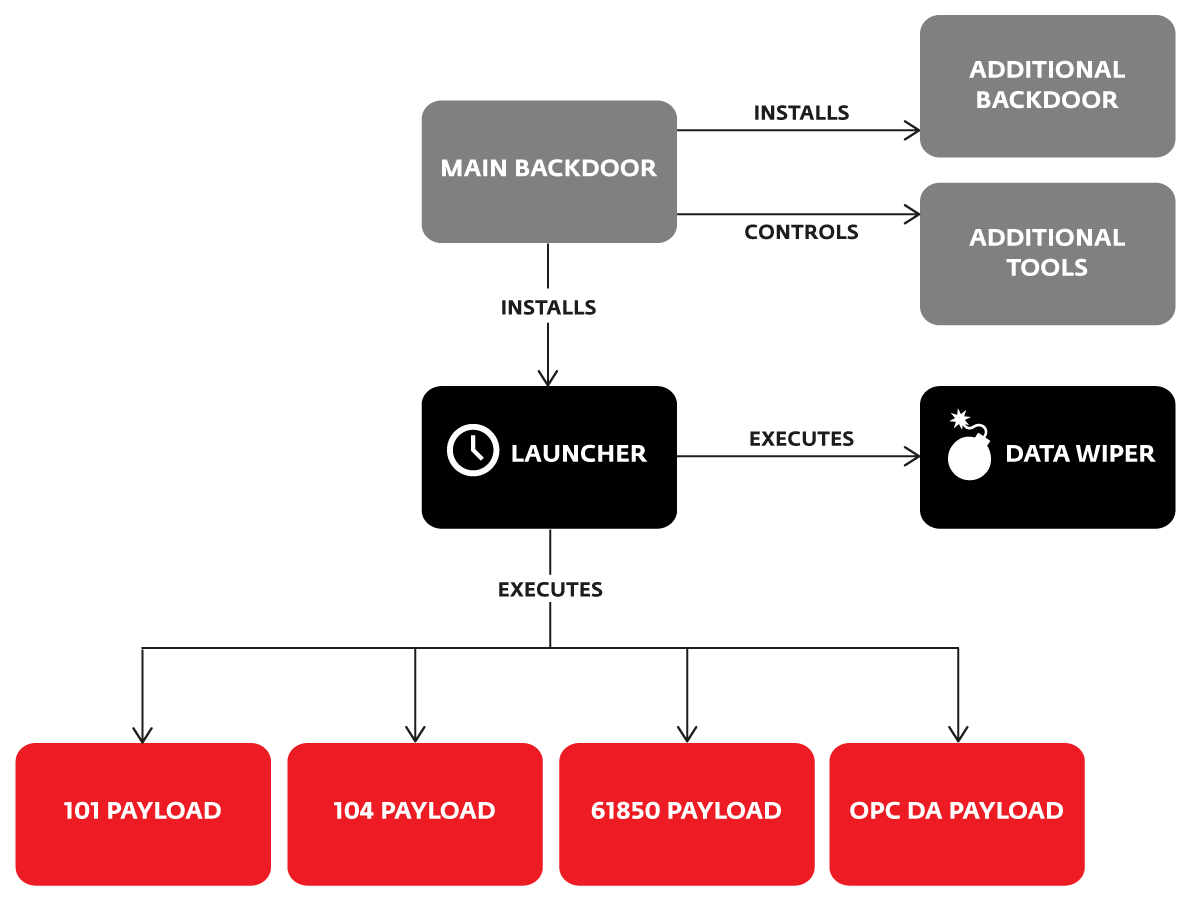
<https://www.vanimpe.eu/2017/06/16/mindmap-for-crashoverride/>

<https://www.forbes.com/sites/kalevleetaru/2017/06/24/crash-override-and-how-cyberwarfare-is-bringing-conflict-to-the-homefront/>

<https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/>

<https://www.computable.nl/artikel/opinie/security/6043507/1509029/malware-crash-override-maakt-dreiging-reeel.html>

<https://www.eenews.net/stories/1060437361> <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf>



The malware contains a few more features that are designed to enable it to remain under the radar, to ensure the malware’s persistence, and to wipe all traces of itself after it has done its job.

For example, the communication with the C&C servers hidden in Tor can be limited to non-working hours. Also, it employs an additional backdoor – masquerading as the Notepad application – designed to regain access to the targeted network in case the main backdoor is detected and/or disabled.

And its wiper module is designed to erase system-crucial Registry keys and overwrite files to make the system unbootable and the recovery harder. Of interest is the port scanner that maps the network, trying to find relevant computers: the attackers made their own custom tool instead of using existing software. Finally, yet another module is a Denial-of-Service tool that exploits the CVE-2015-5374 vulnerability in Siemens SIPROTEC devices and can render targeted devices unresponsive.

<https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/>

cyber and information warfare in the Ukranian conflict

* Armageddon
* BlackEnergy
* technological effects
* crashoverride
* fight spear fishing

<https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf>

Unlike Stuxnet, CrashOverRide is a software vulnerability aimed at "Zero-day attackIt does not use the characteristic point. It is a feature of CrashOverRide that exploits four industrial communication protocols that are used globally in important infrastructure systems such as power infrastructure and power transmission control system, rather than exploiting software vulnerabilities. Malware first installs the four payload components to control the power switch and circuit breaker, and then becomes itself a backdoor to secure the communication circuit with the remote server and can receive instructions from the attacker I was to wait.

The control system of switches and circuit breakers used by electric utilities at substations was designed several decades ago, sneaking into this system, disconnecting power supply arbitrarily and concealing the occurrence of failures, CrashOverRide is designed to cause failure of power transmission system. In addition, CrashOverRide seems to have multiple functions that hide all traces and hide in the system so that they can stay long in the system and cause a failure, hiding all the traces after the attack. Security researchers at ESET point out that "Developers of CrashOverRide have considerable knowledge and a deep understanding of industrial control systems."

Security researchers at ESET and Dragos analyzed CrashOverRide and found that it was refined so that it could be attacked in a wider range rather than just for Ukrainian power outage. Since CrashOverRide includes interchangeable plug-in components, it is also possible to change the target power company or attack multiple electric power companies at the same time. Security researchers at ESET and Dragos said that "CrashOverRide is not dependent on a specific company or specific system, but considering the design of the transmission grid and network communication, and in some countries in Europe, the Middle East and Asia CrashOverRide is extensible and incorporates the DNP 3 (Distributed Network Protocol 3) protocol stack, so attacking the North American power grid with minor modifications It is also possible. "

<https://gigazine.net/gsc_news/en/20170613-crashoverride>

<http://www.derechos.org/nizkor/espana/doc/industroyer1.html>

The malware, called “CrashOverride” or “Win32/Industroyer,” appears to pose the most significant cyber-based threat to a physical industrial process since the Stuxnet malware was reportedly used in 2009 to physically damage Iranian uranium enrichment centrifuges. A report issued by a cybersecurity firm analyzed the malware and found that it is very likely the same type of malware that shut down portions of the Ukraine electric grid in December 2016. The purpose of the malware seems to be limited to causing power outages. Notably, the malware is also reportedly capable of delaying restoration actions, including by erasing ICS network software, and deleting traces of the malware after the attack, preventing effective forensics.

It would be prudent for counsel advising affected industries to confirm that appropriate steps are being taken to exercise vigilance in light of this new information, for example by appropriate personnel taking steps now to review and mitigate system vulnerabilities; monitor for indicators of an attack; and prepare for and respond to this type of an attack.

<https://www.windpowerengineering.com/malware-capable-shutting-electric-grids-confirmed/>

According to Dragos, an industrial cybersecurity startup in Fulton, Md., the CrashOverride malware is "a modular framework consisting of an initial backdoor, a loader module, and several supporting and payload modules." In a practical ICS attack, the malicious actor would first need to establish an internal proxy in order to install the backdoor. At this point, CrashOverride would download a data-wiper module, which "clears registry keys, erase[s] files and kill processes running on the system.

"The functionality in the CrashOverride framework serves no espionage purpose and the only real feature of the malware is for attacks which would lead to electric outages," Dragos wrote in its report. "There are concerning scenarios in how this malware can be leveraged to disrupt grid operations that would result in hours of outages at targeted locations leading into a few days if done at multiple sites. However, it is important to know this is not a catastrophic scenario; there is no evidence the Electrum actors could use CrashOverride to do more than a few days of outages, and even to get a few days, [it] would require the targeting of multiple sites simultaneously, which is entirely possible, but not trivial. CrashOverride is an extremely concerning capability, but should not be taken with any doom and gloom type scenarios."

Robert Lee, founder and CEO of Dragos, said ESET had already planned to go public with the CrashOverride information on June 12, so Dragos had to move quickly on its analysis.

Another option for an ICS attack using CrashOverride would be to use an IEC 104 module "to serve in a 'master' role."

"This raw functionality creates a Swiss army knife for substation automation manipulation, yet also provides tailored functionality," Dragos wrote. "The functions exposed to the malware operator are confined by the options of the configuration file."

"The threat actor merely used legitimate commands to send incorrect directions to the substation control units," Carcano told SearchSecurity. "Once CrashOverride was able to penetrate the plant network, the communications it sent on the network were all using industrial protocols as they are intended to be used."

"It is a canonical example of multiparty vulnerability coordination, where the [vulnerabilities] are in a protocol implemented by many who must all fix [it]," Moussouris told SearchSecurity. "There's nothing typical about the timeline, but it can take years, especially if a protocol revision requires new hardware design. Mitigation is case-specific, from disabling functionality that uses the protocol -- usually not an option -- to segmentation to other filtering."

Richard Henderson, global security strategist at Absolute Software, an endpoint security company based in Vancouver, B.C., said an ICS attack using the IEC 104 module would be "pretty scary stuff if it was used to mess with remote terminal units [RTUs]."

"Cascade failures are a very real risk in our modern, connected power system -- we only need to go back to the Northeast blackout of 2003 to see how quickly an issue can spread and cause massive outages. In some cases, it took days before power was restored," Henderson told SearchSecurity. "A targeted attack on RTUs, which can physically toggle station [and] substation breakers on or off, could place other sections of the grid under massive stress ... it wouldn't be too much of a stretch to imagine some of those other systems on the grid falling over. This is one of the biggest threats facing ICS and SCADA today: There is a very real-world threat when we marry cyber to the kinetic."

The larger question would be whether utilities are ready to handle a persistent malware threat, which may require them to run their system with far more manual intercession than utilities today are used to doing. One thing that made some of the original attacks on the Ukrainian power grid have such minimal real impact is that they had only recently moved to digital systems, so there were knowledgeable operators ready and able to run in manual mode to keep the power on. In many other areas of the world, including the United States, we are capable of the same manual operation, but it may take more resources than we have on hand at any given point if the outage is significant.

"There seems an undercurrent of surprise or reactionary concern when we hear details on how bad actors are advancing sophisticated means to attack critical infrastructure," Zahn told SearchSecurity. "In power, we are in denial that a similar attack could happen in the U.S. We also get mired in misconceptions that we are well-prepared because of regulation, or squirrels -- yes, squirrels -- are more likely to bring down power than a hacker. The problem is that nation states have a plan; squirrels do not."

<https://searchsecurity.techtarget.com/news/450420683/CrashOverride-ICS-attack-targets-vulnerable-electrical-grid>

<https://www.sueddeutsche.de/digital/cyber-angriff-auf-die-ukraine-it-forscher-cyberwaffe-russischer-hacker-schaltete-stromnetz-von-kiew-aus-1.3543072>

Crash Override works by hijacking a power plant's computers in order to create a software loop that forces its circuit breakers to stay open, thereby taking the plant offline, according to the Dragos report. The only way to stop it is for a repair crew to manually assume control of the breakers to close them. Crash Override's methods could likely work for any power station with computer-controlled breakers, and could even be expanded to affect other industrial plants.

<https://www.entrepreneur.com/article/295755>

<https://www.icsvillage.com/talks/crashoverride-re-assessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack>

<https://www.tripwire.com/state-of-security/latest-security-news/petya-ransomware-outbreak-hits-ukraine-russia-and-europe/>

Technical AnalysisCrashOverride malware represents a scalable, capable platform. The modules and capabilities publically reported appear to focus on organizations using ICS protocols IEC101, IEC104, and IEC61850, which are more commonly used outside the United States in electric power control systems. The platform fundamentally abuses the functionality of a targeted ICS system’s legitimate control system to achieve its intended effect. While the known capabilities do not appear to be U.S.-focused, it is important to recognize that the general TTPs used in CrashOverride could be leveraged with modified technical implementations to affect U.S.-based critical infrastructure. With further modification, CrashOverride or similar malware could have implications beyond electric power so all critical infrastructure organizations should be evaluating their systems to susceptibilities in the TTPs outlined. The malware has several reported capabilities:Issues valid commands directly to remote terminal units (RTUs) over ICS protocols. As reported by Dragos, one such command sequence toggles circuit breakers in a rapid open-close-open-close pattern. This could create conditions where individual utilities may island from infected parties, potentially resulting in a degradation of grid reliability.Denies service to local serial COM ports on windows devices, therefore preventing legitimate communications with field equipment over serial from the affected device.Scans and maps ICS environment using a variety of protocols, including Open Platform Communications (OPC). This significantly improves the payload’s probability of success.Could exploit Siemens relay denial-of-service (DoS) vulnerability, leading to a shutdown of the relay. In this instance, the relay would need to be manually reset to restore functionality.Includes a wiper module in the platform that renders windows systems inert, requiring a rebuild or backup restoration.DetectionAs CrashOverride is a second stage malware capability and has the ability to operate independent of initial C2, traditional methods of detection may not be sufficient to detect infections prior to the malware executing. As a result, organizations are encouraged to implement behavioral analysis techniques to attempt to identify precursor activity to CrashOverride. As additional information becomes available on stage one infection vectors and TTPs, this alert will be updated.NCCIC is providing a compilation of IOCs (see links above) from a variety of sources to aid in the detection of this malware. The sources provided do not constitute an exhaustive list and the U.S. Government does not endorse or support any particular product or vendor’s information referenced in this report. However, NCCIC has included this data to ensure wide distribution of the most comprehensive information available and will provide updates as warranted.Signaturesimport “pe”import “hash”rule dragos\_crashoverride\_exporting\_dlls{meta:description = “CRASHOVERRIDE v1 Suspicious Export”author = “Dragos Inc”condition:pe.exports(“Crash”) & pe.characteristics}rule dragos\_crashoverride\_suspcious{meta:description = “CRASHOVERRIDE v1 Wiper”author = “Dragos Inc”strings:$s0 = “SYS\_BASCON.COM” fullword nocase wide$s1 = “.pcmp” fullword nocase wide$s2 = “.pcmi” fullword nocase wide$s3 = “.pcmt” fullword nocase wide$s4 = “.cin” fullword nocase widecondition:pe.exports(“Crash”) and any of ($s\*)}rule dragos\_crashoverride\_name\_search {meta:description = “CRASHOVERRIDE v1 Suspicious Strings and Export”author = “Dragos Inc”strings:$s0 = “101.dll” fullword nocase wide$s1 = “Crash101.dll” fullword nocase wide$s2 = “104.dll” fullword nocase wide$s3 = “Crash104.dll” fullword nocase wide$s4 = “61850.dll” fullword nocase wide$s5 = “Crash61850.dll” fullword nocase wide$s6 = “OPCClientDemo.dll” fullword nocase wide$s7 = “OPC” fullword nocase wide$s8 = “CrashOPCClientDemo.dll” fullword nocase wide$s9 = “D2MultiCommService.exe” fullword nocase wide$s10 = “CrashD2MultiCommService.exe” fullword nocase wide$s11 = “61850.exe” fullword nocase wide$s12 = “OPC.exe” fullword nocase wide$s13 = “haslo.exe” fullword nocase wide$s14 = “haslo.dat” fullword nocase widecondition:any of ($s\*) and pe.exports(“Crash”)}rule dragos\_crashoverride\_hashes {meta:description = “CRASHOVERRIDE Malware Hashes”author = “Dragos Inc”condition:filesize < 1MB andhash.sha1(0, filesize) == “f6c21f8189ced6ae150f9ef2e82a3a57843b587d” orhash.sha1(0, filesize) == “cccce62996d578b984984426a024d9b250237533” orhash.sha1(0, filesize) == “8e39eca1e48240c01ee570631ae8f0c9a9637187” orhash.sha1(0, filesize) == “2cb8230281b86fa944d3043ae906016c8b5984d9” orhash.sha1(0, filesize) == “79ca89711cdaedb16b0ccccfdcfbd6aa7e57120a” orhash.sha1(0, filesize) == “94488f214b165512d2fc0438a581f5c9e3bd4d4c” orhash.sha1(0, filesize) == “5a5fafbc3fec8d36fd57b075ebf34119ba3bff04” orhash.sha1(0, filesize) == “b92149f046f00bb69de329b8457d32c24726ee00” orhash.sha1(0, filesize) == “b335163e6eb854df5e08e85026b2c3518891eda8”}rule dragos\_crashoverride\_moduleStrings {meta:description = “IEC-104 Interaction Module Program Strings”author = “Dragos Inc”strings:$s1 = “IEC-104 client: ip=%s; port=%s; ASDU=%u” nocase wide ascii$s2 = “ MSTR ->> SLV” nocase wide ascii$s3 = “ MSTR

<https://humanit.asia/ta17-163a/>

De malware bevat softwarecode die volledig automatisch acties onderneemt om elektrische substations uit te schakelen. Om te beginnen brengt de software in kaart waar kritische onderdelen zich bevinden en hoe ze werken in de praktijk. Volgens die methode kan de malware bepaalde schakelaars herkennen en open zetten, zodat de stroomvoorziening wegvalt. Tegelijk wordt de software voor die schakelaars gewist, zodat een operator die niet meer van afstand kan sluiten. Die moet dus fysiek naar de installatie komen, wat extra tijd kost.

Industroyer/Crash Override heeft vier modules aan boord om aanvallen uit te voeren. Elke module communiceert via een ander protocol met de apparaten in het stroomnet. Afhankelijk van welke protocollen in een bepaald land worden gebruikt, zet de malware een betreffende module in. Dit wijst er ook op dat de malware speciaal is geschreven om in verschillende landen te worden ingezet. De stroomuitval in de Oekraïne was waarschijnlijk maar een test, en de beheerders van stroomnetten in andere landen doen er goed aan om hun beveiliging te checken.

<https://www.deingenieur.nl/artikel/gevaarlijke-malware-legt-stroomnet-plat>

Advanced Components

CrashOverride includes multiple components that allow hackers to quickly and easily modify the malware for a variety of ICSs. This means that rather than being designed to specifically target one electrical system in one location, it can be used to target multiple systems around the world. It does this by leveraging information about power grid operations and network communications in order to cause the biggest impact to each specific ICS. Some of the components that make the effects of this malware so devastating are the abilities to:

Manipulate Electric Power Control Systems Settings: CrashOverride scans for critical components that keep the power grid functioning. Once the malware has found them, it can manipulate settings and force certain functions even if an in-person operator tries to intervene.

Wipe System Software: The malware is able to infiltrate the computer systems that control the circuit breakers and erase the software that keeps these systems running. This forces ICSs into manual operations, which includes having to send operators out to each substation.

Schedule Time-Bomb Attacks: CrashOverride has the ability to schedule simultaneous attacks across multiple power grids all at once. Luckily, the US electric industry is trained to handle outages in multiple locations due to severe weather, but future variations of this kind of malware could make that more difficult.

Future malware varitions could result in doomsday-like ICS attacks.

According to industry experts, this type of malware would not have too much of an impact on current electric power grid operations. They predict that if a Russian hacking operation like this occurred, outages would last for a few hours and at most a few days. There is no need to fear for a doomsday type of attack – yet.

However, even brief electrical outages can be extremely disruptive and expensive. Mortality rates increase and consumer costs are estimated at between $2-$20 per kilowatt hour lost. Utilities can be heavily fined, lose financing for upcoming projects, or find future rate increases at risk.

The introduction of this type of malware outlines why it is so important for energy and other utility infrastructure companies to have advanced security measures in place. Although it is not completely clear how this malware is spread, it is important to remember that most cyberattacks involve the misappropriation of privileged credentials in some fashion. In fact, a whopping 80% of all IT breaches involved the misuse of privileged credentials according to the Privileged Identity Management Wave, Q3 report from Forrester.

Privileged Accounts and PAM

PAM gives ICS complete control over privileged accounts, which typically have advanced administrative capabilities that allow them to:

Change system configurations

Install software

Create and modify users

Access or modify data

Modify administrative privileges of all users

If credentials to these accounts get into the wrong hands or are misused by malicious insiders, there can be devastating consequences for ICSs. PAM helps ensure that your organization is protected from both internal and external threats, by controlling and documenting all actions taken within an organization.

PAM allows ICS to monitor, manage, and audit all privileged account activities.

The bottom line is that no one should be given direct privileged access to critical industrial systems or infrastructure. The responsible action is to route all access through PAM which allows access to be monitored, managed, and audited.

ICS Security with WALLIX

Utilities and energy companies have a tremendous responsibility to their stockholders, customers, and to public safety. This responsibility is matched by the challenge of high regulatory hurdles and aggressive attackers. In order to meet the challenges associated with ICS security, companies must invest in managing privileged accounts.

<http://blog.wallix.com/ics-security-russian-hacking>

<https://fortune.com/2017/06/12/malware-cybersecurity-ukraine/>

<https://www.expressnews.com/business/eagle-ford-energy/article/San-Antonio-s-CPS-Energy-guards-against-94-000-11300850.php>

<https://www.bgp4.com/2018/10/19/new-information-and-analysis-on-the-ukraine-2016-electric-grid-attack-detecting-and-defeating-crashoverride/>

<https://www.techrepublic.com/article/malware-that-took-down-ukraine-power-grid-could-be-used-in-us-report-says/>

<https://www.tpr.org/post/ukraine-paints-grim-portrait-cyber-attacks-come>

<https://www.techspot.com/news/69680-stuxnet-20-crash-override-malware-linked-kiev-power.html>

<http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/74/Research-Reports/Amir_SCADA.pdf>

<https://malware.news/t/found-crash-override-malware-that-triggered-ukrainian-power-outage/12720>

<https://www.livemint.com/Industry/9cKsivqTXa1C5joHeuaspN/Cyber-firms-warn-of-malware-that-could-cause-power-outages.html>

<https://www.smart-energy.com/regional-news/europe-uk/encs-crash-override-virus/>

<https://www.nozominetworks.com/blog/defending-against-industroyer-with-ics-anomaly-detection/>

<https://www.datto.com/blog/crash-override-malware-prompts-cybersecurity-alert>

<https://www.blackhat.com/us-17/briefings/schedule/#industroyercrashoverride-zero-things-cool-about-a-threat-group-targeting-the-power-grid-6159>

<https://medium.com/@verovaleros/can-a-piece-of-malware-take-down-a-power-grid-meet-crashoverride-c4e438282650>

<https://www.stripes.com/russia-has-developed-cyber-weapon-that-can-disrupt-power-grids-new-research-finds-1.473115>

<https://digitalsupport.ge.com/servlet/fileField?retURL=%2Fapex%2FKnowledgeDetail%3Fid%3DkA21A000000HShPSAW%26lang%3Den_US%26Type%3DArticle__kav&entityId=ka21A000000HccQQAS&field=File_1__Body__s>

## Artikel

Op 23 december, 2015, werden de bestuurscentra van drie Orkraiense electriciteitsdistributiecentra op afstand bestuurd. Door controle te nemen over SCADA systemen konden aanvallers stroomonderbrekers van 30 distributie onderstations openzetten in de hoofdstad Kiev en in het westen van Ivano-Frankovisk regio, waardoor meer dan 200,000 gebruikers zonder stroom zaten. Bijna een jaar later, op 17 December 2016 verloor een onderstation met een transmissie zijn stroom in noorden van Kiev.

Overheidsunctionarissen van de oekraiene en de verenigde staten hebben samen onderzoek gedaan naar de aanval. Uit een onderzoek is naar voren gekomen dat een deel van de aanval kan worden toegeschreven aan een trojan malware genaamd “BlackEnergy3”, waarmee niet onomstotelij is vastgesteld dat de hack is opgezet door het Sandworm Team. Een russiche organisatie die wellicht banden heeft met statelijke actoren. Onderzoekers gaan er ook van uit dat de tweede aanval op de electriciteitscentra in de oekraiene is uitgevoerd door het Sandworm Team. Onderzoekers van het private beveiligingsbedrijf Dragos, schrijven de aanval ook toe aan het Sandworm Team, waarbij gebruik werd gemaakt van een nieuw type malware genaamd Industroyer , ook wel CRASHOVERRIDE genoemd.

De eerste versie van de BlackEnergy malware werd voor het eerst gebruikt in 2007 bij enkele Ddos aanvallen; de tweede versie was erop gericht om mens-machine-interfaces voor industrielecontroleverwerking aan te vallen. BlackEnergy3 is meer modulair ontwikkeld in vergelijking met zijn voorlopers. De malware kwam binnen via spearfishing email. De malware maakt een backdoor zodat de aanvaller toegang heeft tot het systeem om zo wachtwoorden van de hoofdgebruikers te verzamelen voor meer invloed en toegang in het netwerk. BlackEnergy3 word ook gebruikt om KillDisk malware te implementeren; killdisk verwijdert bestanden en verwijdert ook de Master Boot Record zodat computers niet kunnen rebooten. Beiden malware zijn gevonden in netwerken van bedrijven die gebruik maken van industruele procestechnieken waaronder een Oekraiens mijnbouwbedrijf en een spoorwegexpointant in handen van de oekraiense staat.

Het Sandworm Team begon de hackcampagne in de periode van Mei 2014 met phishing emails en reconnaissance. Het ishier aannemelijk om te stellen dat BlackEnergy3 was geinstalleerd op bedrijfssystemen 6 maanden voordat de hackaanval plaatsvond op 23 december 2015. De emails met geinfecteerde bijlage, word of excel bestand, werden gestuurd naar de kantoren van de bedrijven. Bij het openen van de geinfeteerde mails werd er een macro ingeschakeld waardoor de aanvallers op afstand toegang konden krijgen tot het systeem. Na deze opening begonnen de aanvallers met het verzamelen van inloggegevens voor de VPN verbindingen die gebruikt worden door de netbeheerders zodat zij op afstand de controlecentra konden besturen. Door het gebruik van de VPN-verbinding konden zij de netwerken van de controlecentra verkennen alswel de aangesloten devices.

Naast het openen van de stroomonderbrekers bij de onderstations, heeft het team nog andere methoden gebruik om het verhelpen van de stroomuitval te vertragen. Zo werd er een TDos-aanval gelanceerd zodat het bedrijfspersoneel niet kon communiceren over de stroomuitval en de situatie niet goed ingeschat kon worden. Bij de controlecentra, werd er geknoeid met ondersteunend materiaal om het verhelpen van de storing te bemoeilijken.

Het Sandworm Team ontwikkelde voor de aanval op een transmissie onderstation op 17 december 2016. Industroyer is vergeleken met BlackEnergy3 specifiek ontwikkeld voor de manipulatie van industriele controlesystemen. Met ingebouwde kennis voor de communicatieprotocollen die gebruikt worden in een electriciteitsnet kan de Industroyer malware direct op afstand controle nemen van industrieel materiaal zonder afhankelijk te zijn van de software die gebruikt wordt door de netoperators. Het is in feite een ugrade van BlackEnergy 2 en 3.

<https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/>

## Invloed, impact en effect van het probleem

health or safety, national security, economic security, foreign relations, civil liberties,

## De fouten van de verschillende protollen die gebruikt werden bij de SCADA systemen.

IEC\_60870-5

<http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=0513EED48102FDAD1BD940260EF12B11?doi=10.1.1.548.7490&rep=rep1&type=pdf>

<https://scialert.net/fulltext/?doi=tasr.2014.396.405>

<https://www.researchgate.net/publication/333671061_Attacking_IEC-60870-5-104_SCADA_Systems>

<http://www.salvage-project.com/uploads/4/9/5/5/49558369/art3_-_salvage_2015_-_cyber_security_in_communication_of_scada_systems_using_iec_61850.pdf>

<https://eg.uc.pt/bitstream/10316/35720/1/Security%20Probes%20for%20Industrial%20Control%20Networks.pdf>

<https://owlcyberdefense.com/products/data-diode-products/software-modules/iec-104/>

<https://ris.utwente.nl/ws/files/6028066/3-s2_0-B9780128015957000227.pdf>

<https://waterfall-security.com/static/Waterfall-for-IEC-60870-5-104_FINAL.pdf>

<http://www.scada.sl/2013/11/last-week-four-guys-of-scada.html>

<https://repositorio-aberto.up.pt/bitstream/10216/119066/2/315683.pdf>

<https://www.diva-portal.org/smash/get/diva2:1046339/FULLTEXT01.pdf>

<https://www.semanticscholar.org/paper/Cybersecurity-analysis-of-a-SCADA-system-under-and-Rocha/dfa7c12551ebe7b24da8d806e87e946051a57cb9>

<https://control.com/forums/threads/comparison-between-iec60870-5-103-and-modbus-rtu.20317/>

<https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf>

<https://www.securonix.com/web/wp-content/uploads/2019/08/RSAC_2019_Scada_Attack_Detection_101.pdf>

<https://dreamlab.net/en/blog/post/fuzzing-ics-protocols/>

<https://library.e.abb.com/public/f74f9c8be95f4cd09b0b1fbbde699108/4CAE000416_RTU_Secure%20communications_web.pdf>

<https://www.slideshare.net/qqlan/scada-zn>

<https://virsec.com/virsec-hack-analysis-deep-dive-into-industroyer-aka-crash-override/>

<https://tutcris.tut.fi/portal/files/16294332/jafary_1534.pdf>

<http://www.connectivity4ir.co.uk/article/175490/IEC-62351--Secure-communication-in-the-energy-industry.aspx>

<https://www.win.tue.nl/~setalle/2017_fauri_encryption.pdf>

<https://assets.barracuda.com/assets/docs/dms/Barracuda_CloudGen_Firewall_SB_Security_for_ICS_and_OT.pdf>

<https://www.checkpoint.com/products/industrial-control-systems-appliances/>

<https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>

<https://dl.acm.org/doi/fullHtml/10.1145/3381038>

<https://arxiv.org/pdf/2001.02925.pdf>

### <http://blog.nettedautomation.com/2017/>

IEC 61850, hack

iec 104

opc

iec 101

## CRASHOVERRIDE

<https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf>

## Manier om de aanvaller te ondermijnen

1. Management
   1. Company security policies in place
   2. Security policies written and enforced through training
   3. Computer software and hardware asset list
   4. Data classified by usage and sensitivity
   5. Established chain of data ownership
2. Employees
   1. Training on phishing, handling suspicious emails, social engineering hackers
   2. Password training and enforcement
   3. Training on dealing with strangers in the workplace
   4. Training on carrying data on laptops and other devices and ensuring the security of this data
   5. All security awareness training passed and signed off ensuring that all employees not only understand the importance of security but are active guardians for security
   6. Ensure that Secure Bring Your Own Device (BYOD) plans are in place
3. Business practices
   1. Emergency and cybersecurity response plans
   2. Determine all possible sources of business disruption cybersecurity risk
   3. Plans in place to lessen business disruptions and security breaches
   4. Emergency disaster recovery plans in place
   5. Alternative locations for running business in case of emergencies or disruptions
   6. Redundancy and restoration paths for all critical business operations
   7. Have you tested your restoration and redundancy plans?
4. IT staff
   1. System hardening plans
   2. Automated system hardening on all operating systems on servers, routers, workstations, and gateways
   3. Software patch management automated
   4. Security mailing lists?
   5. Regular [security audits](https://reciprocitylabs.com/cloud-security-vs-traditional-security/) and penetration testing
   6. Anti-virus software installed on all devices with auto-updates
   7. Systematic review of log files and backup logs to make sure there are no errors
   8. Remote plans in place, as well as policies regarding remote access
5. Physical security
   1. Lock servers and network equipment
   2. Have a secure and remote backup solution
   3. Make sure keys for the network are in a secure location
   4. Keep computers visible
   5. Use locks on computer cases
   6. Perform regular inspections
   7. Prevent unauthorized users from entering the server room or even in the workstation areas
   8. Security camera monitoring system
   9. Keycard system required for secure areas
   10. Secure Data Policy in place and ensure users understand the policy through training
   11. Secure trash dumpsters and paper shredders to prevent dumpster diving
6. Secure data
   1. Encryption enabled wherever required
   2. Secure laptops, mobile devices, and storage devices
   3. Enable automatic wiping of lost or stolen devices
   4. Secure Sockets Layer (SSL) in place when using the Internet to ensure secure data transfers
   5. Secure email gateways ensuring data is emailed securely
7. Active monitoring and testing
   1. Regular monitoring of all aspects of security
   2. Regularly scheduled security testing
   3. External penetration testing to ensure your staff hasn’t missed something
   4. Scanning for data types to make sure they are secure and properly stored

<https://www.us-cert.gov/ics/Recommended-Practices>

## Bijlage A: Checklists

• Introduction to Network Security Audit Checklist:

• 2Record the audit details

• 3Make sure all procedures are well documented

• 4Review the procedure management system

• 5Assess training logs and processes

• 6Review security patches for software used on the network

• 7Check the penetration testing process and policy

• 8Test software which deals with sensitive information

• 9Look for holes in the firewall or intrusion prevention systems

• 10Make sure sensitive data is stored separately

• 11Encrypt company laptop hard disks

• 12Check wireless networks are secured

• 13Scan for unauthorized access points

• 14Review the process for monitoring event logs

• 15Compile your report

• 16Approval:

• 17Send your report to the relevant stakeholders

iso standaarden

<https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/04/201902-Handreiking-Information-Security-Management-System-ISMS-v2.0.pdf>

<https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/NL/Checklist_of_ISO_27001_Mandatory_Documentation_NL.pdf>

<https://info.advisera.com/hubfs/27001Academy/27001Academy_FreeDownloads/NL/Checklist_of_ISO_27001_Mandatory_Documentation_NL.pdf>

<https://www.iso.org/isoiec-27001-information-security.html>

<https://www.iso27001security.com/html/faq.html>

<https://www.iso27001security.com/ISO27k_FAQ.pdf>

<https://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.pdf>

<https://webstore.iec.ch/preview/info_isoiec27019%7Bed1.0%7Den.pdf>

[https://web.archive.org/web/20150924001524/http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002003738](https://web.archive.org/web/20150924001524/http:/www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002003738)

<https://webstore.iec.ch/publication/25948>

<https://webstore.iec.ch/publication/6912>

<https://webstore.iec.ch/publication/6911>

<https://www.ipcomm.de/protocol/IEC62351/en/sheet.html>

UK NCSC Guidelines

BDEW and Oesterreichs Energie

NERC CIP

<https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0>

<https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1>

<https://nvlpubs.nist.gov/nistpubs/ir/2010/NIST.IR.7628.pdf>

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

<https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf>

# Bibliografie

(n.d.). Retrieved from rand.org: https://www.rand.org/pubs/research\_reports/RR2081.html

(n.d.). Retrieved from dpstele.com: https://dpstele.com/blog%20major%20scada%20hacks

*/checklist/network-security-audit-checklist/#related-checklists*. (n.d.). Retrieved from process.st: https://www.process.st/checklist/network-security-audit-checklist/#related-checklists

(2016 ). Retrieved from https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html

*cybersecurity-audit-checklist*. (n.d.). Retrieved from reciprocitylabs.com: https://reciprocitylabs.com/cybersecurity-audit-checklist/

*ukraine-power-grid-attack-russia-us*. (2016, 2 11). Retrieved from edition.cnn.com: https://edition.cnn.com/2016/02/11/politics/ukraine-power-grid-attack-russia-us/index.html

*ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E*. (n.d.). Retrieved from reuters.com: https://www.reuters.com/article/us-ukraine-cybersecurity/ukraine-sees-russian-hand-in-cyber-attacks-on-power-grid-idUSKCN0VL18E