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 de eerste 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 gebruiken of het gebruik daarvan te vertragen. Argument dat hiervoor is opgevoerd is dat de impact die is geconstateerd niet gerelateerd aan de schade van eerdere aanvallen waar dergelijke malware werd 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>

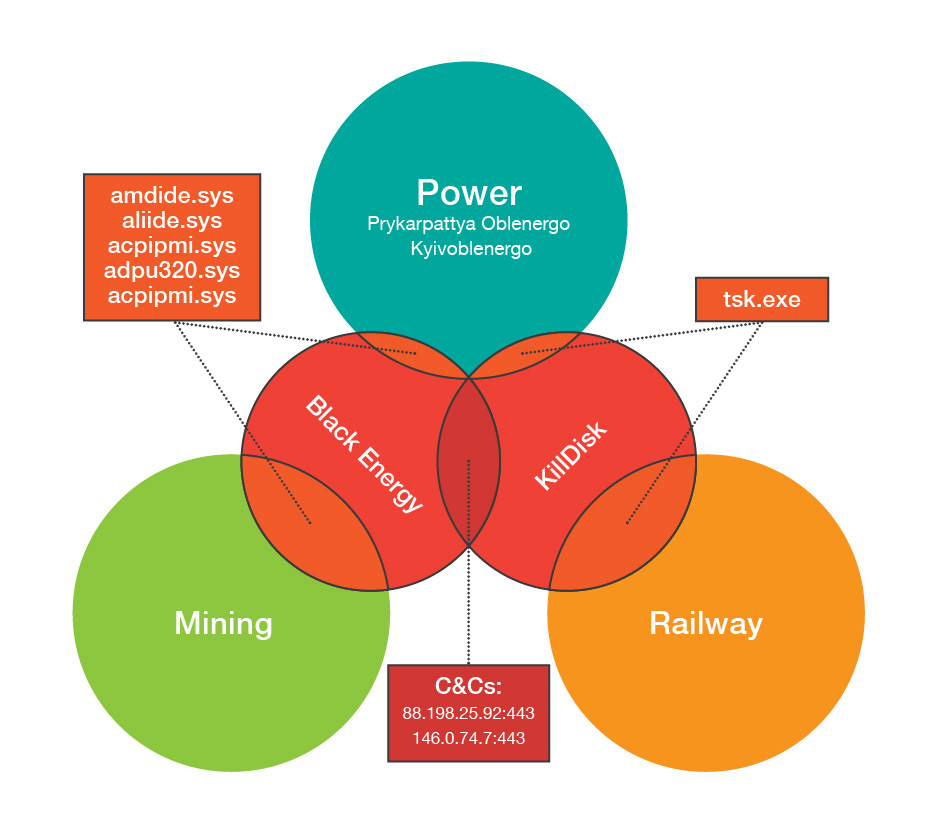
<https://www.wired.com/2014/10/russian-sandworm-hack-isight/>

<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>

## 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/>

## 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>

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

<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>

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

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

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

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

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

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

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

<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>

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

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

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

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

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

Een elekctriciteitsnet kan worden ingedeeld in 3 functies: het opwekken van elektriciteit bij een elektriciteitscentrale, het overdragen van de elektriciteitscentrale over een lange afstand op ee hoog voltage, en de overstap naar een lager voltage om via distributienetwerken de consumenten te bedienen. Bij het transport van de energie wordt gebruik gemaakt van een onderstations voor het omzetten van spanningsniveaus, functie als wisselstation en feeders en om fout bescherming tegen te gaan.

Elektriciteitscentrales gebruiken SCADA systemen als robuust systeem om de balans van energielering tussen grote regio’s in stand te houden. Eigenaren van distributie- en transmissiesystemen managen de cross-territoriale SCADA systemen 24/7 met ‘human operators’. De controlecentra waar de human operators dienst doen onderhouden te aanhoudende vraag naar elektriciteit van hun afnemers, reageren op fouten, en werken samen met andere organisaties in de industrie samen om de stroomvoorziening te onderhouden.

Dit is een simplistisch beeld dat uitgewerkt is in energiemarkten in Europa, Azie en Noord-Amerika. De protocollen die gebruikt worden zijn nagenoeg hetzelfde: controle van physieke apparatuur door middel van RTU’s, progrmmable logic controllers (PLC) en andere controle elementen als HMI’s die onderdeel zijn van een groter SCADA systeem. Sommige protocollen zijn internationaal in gebruik zoals de IEC61850 die vaak wordt gebruikt bij een HMI om samen te werken met digitale relais en andere intelligente elektronische apparaten (IEDs). IEDs zijn microprocessor-georienteerde controle apparaten en worden veelal gebruikt bij stroomonderbrekers. IEDs En RTU’s opereren in master/slave heodanigheid waar de slave devices commandos sturen naar de master devices.

Onderstations onderhouden de doorstroom van elektriciteit door de transmissie of distributielijnen. Het management controleert dus de flow van energie van en naar een onderstation. Als je een breaker opent dan maak je iegenlijk de leiding of toevoer van elektriciteit door die leiding onmogelijk, deze wordt dan letterlijk onderbroken.

Het elektriciteitenet is een goed ontworpen systeem en ondanks re risico’s zijn landen overal ter wereld er zich van bewust dat de taak van electricitetssector is omeen betrwoubaar en veilig systeem te onderhouden met een natuurlijk bijproduct in de vorm van een toename van veiligheidsasrtieklen.

BLACKENERGY2 is een malware met exploits voor specifieke type HMI applicaties waaronder SIEMENS SIMATIC, GE CIMPLICITY, en Advantech WebAccess. De bedoeling was om HMI aan te vallen aangsloten op het internet. Door gebruik te maken van de HMIs konden de aanvallers toegang krijgen tot de centrale locatie van de ICS om inzage te krijgen van het industriele proces en de grafische afbeelding van de ICS. Het aanvallen van een HMI zorgt op zich zelf niet voor fysieke schade, maar het is wel een doelwit voor spionage in een ICS. Een vaste voet in een netwerk dat is aangesloten op talloze componenten van het ICS en controle op toegang tot internet is voor aanvallers geen slechte uitgangspositie.

De aanval op drie oekraiense karachtcentrales op 23 december 2015 was een unieke gebeurtenis in de geschiedenis voor de electricitetesnet operatoren. Het was de eerste digitale aanval die de die de elctriciteitsnetwerken van een bepaalde regio of land heeft verstoord. Bij deze aanval werd BLACKENERGY3 gebruikt. BLACKENERGY3 gebruikt geen ICS componenten in tegenstelling tot BLACKENERGY2. De BLACKENERGY 3 malware werd gebruikt om toegang te krijgen tot bedrijfsnetwerken van de energiebedrijven en dan de SCADA systemen binnen te treden. Terwijl in de omgeving de aanvallers een hun verkenning deden of op enig moment gebruik maakten van de elektriciteitsnet. Zij deden ervaring op met de werkzaamheden en gebruikten legitieme functionaliteiten van het distributiemanagement om onderstations los te koppelen van het net waarmee meer dan 225000+ gebruikers voor meer dan 6 uur zonder stroom kwamen te zitten. Hoe dan ook, door het wissen bestanden met de KillDisk malware en de destructie van serial-to-ethernet devices door middel van malafide software updates waren de Oekraiense net operators niet in staat om hun SCADA omgeving te gebruiken, wat resulteerde in het technisch onvermogen om de geautomatiseerde controle op systemen te managemen. Dit duurde in sommige gevallen een jaar voordat de controle over de system iun handen viel van de net operators. Een belangrijk aspect van de aanval was de focus van de aanvaller om de systemen tegen elkaar uit te laten spelen. Malware maarkte de aanval mogelijk, en malware vertraagde de hersteloperaties, maar het was de directe interactie van de aanvaller op de ICS dat resulteerde in de elektriciteitsstoring, niet de malware.

De crashoverride malware werd gebruikt voor de aanval op een onderstation met een enkel transmissieniveau in Oekraine op 17 december 2016. Het belangrijkste om mee te nemen en te begrijpen is de kwaliteit en schaalbaarheid waarmee de malware is ontwikkeld. De malware ontwikkelde een aanpak om de industriele processen te begrijpen en te coderen op dezelfde manier zoals STUXNET dat deed. Het maakte gebruik van het OPC protocolom de omgeving in kaart te brengen en om een selectie te maken van doeleinden gelijkbaar met HAVEX. De bilbiotheek- en configuratiebestanden van de HMI werden aangevallen om meer over de omgeving te weten te komen en benutte HMI’s om verbinding te maken met Internet-connected-locations waar dat mogelijk is. En het nam dezelfde aanpak bij het leren van net operaties en benutte de zwakheden van het systeem tegen zichzelf. Al deze taken werden zo verfijnd uitgevoerd dat de aanvallers een platform hadden gekregen om aanvallen uit te voeren in verschillende omgevingen en waren dus niet beperkt tot specifiek enkele verkopers platforms. De situatie markeert een ontwikkeling van aanvallers met als doel het verstoren van operaties en het blootstellen van kwetsbaarheden voor de verdedigers die de patch systemen zien als primair mikpunt, gebruikmakend van anti-malware tools om specifieke samples te ontdekken, en ze vertrouwen op een air-gapped netwerk als oplossing.

De crashoverride malware is een modulair framework dat bestaat uit een initiele backdoor, een loader module, enkele support en payload modules.

De belangrijkste items zijn de backdoor deze verschaffen toegang tot het geinfecteerde systee,, de loader module, maakt acties mogelijk op de doelcomputer, en de individuele payload modules.

Er werden bij de aanval twee samples verzameld van malware gerelateerd aan de effecten op een aangevallen industrieel controle systeem. Een sample was een IEC 104 protocol module en de ander was een data wiper. Beide samples hebben karakteristieke eigenschappen die een indicatie geven dat ze onderdeel zijn van een breeduitgemeten ICS aanval en manupulatie framework.

Onderzoek toonde aan dat beiden module samples een functie hadden genaamd Crash met als functie het in staat stellen om additionele modules inladen en uitvoeren.

De backdoor van de RAT Module eigenschappen:

* Authenticeren met een locale proxy via een intern netwerk die al is vastgesteld voordat de backdoor is geinstalleerd
* Na aiuthenticatie word een HTTP kanaal geopend naar een extern controle server (C2) via een interne proxy
* Ontvangen van instructies via een externe instructie en controle server
* Maakt een file aan op het lokale systeem
* Overschrijft een bestaande service point naar de backdoor zodat de malware blijft werken bij een reboot

In detail:

Toegang tot het ICS netwerk verloopt via de backdoor module. Het dragos instituut verkreeg 4 samples met een vergelijkbare functionaliteit. Bij het uitvoeren ervan bleek dat de malware pogingen deed om een hard-gecodeerde proxy-address te localiseren in het lokale netwerk. ELECTRUM moet een interne proxy bewerkstelligen voor de installatie van de backdoor.

De malware verwacht te kunnen communiceren met een interne proxy die luistert naar TCP 3128. Deze poort is een default poort geassocieerd met de Squid proxy. Vanaf het moment dat er een verbinding is wordt er een HTTP POST request gedaan met het GUID van het slachtoffer. Deze informatie authenticeert de aangevallen machine met de command en control (C2) server. Als de C2 server niet antwoord, dan zal de backdoor afsluiten.

Als de authenticatie succesvol is op de interne proxy, dan zal de malware proberen een HTTP CONNECT actie uitvoeren naar een externe C2 server via de interne proxy.

Bij alle vier samples werden drie verschillende C2 addressen gevonden die waarschijnlijk onderdeel waren van de aanval op Oekraine in december 2016.

Bij het uitvoeren van een HTTP CONNECT, probeert de malware de default user agent te identificeren. Als deze niet kan worden vastgesteld of gewoonweg niet bestaat dan zal een hard-coded default voor de malware worden gebruikt.

De malware kan geconfigureerd worden via een hard-coded configuratie waarde. De malware kan dan de volgende instructies ophalen van de C2 server:

\* • Create a new process as logged in user • Create a new process as specified user via CreateProcessWithLogon • Write a file • Copy a file • Execute a command as logged in user • Execute a command as specified user • Kill the backdoor • Stop a service • Specify a user (log in as user) and stop a service • Specify a user (log in as user) and start a service • Alter an existing service to point to specified process and change to start at boot

Uitvoer resulteert in enkele artefacten die worden achtergelaten op de host. Tijdens de executie, kijkt de malware naar de aanwezigheid van een MUTEX waarde. MUTEXES zijn programma objecten die het mogelijk maken om resources te delen tussen verschillende threads. In dit geval kijkt CRASHOVERRIDE naar \SESSIONS\1\Windows\ApiPortection

De backdoor mag ook een nieuwe mutex aanmaken en controleren. Een review tijdens de uitvoer en de analyse van andere modulen in de malware geeft een indicatie dat SESSIONS\1\Windows\ meerdere keren voorkomt, wat impliceert dat waarschijnlijk een check zal worden uitgevoerd.

De backdoor schrijft een bestand weg naar C:\Users\Public\ of C:\Users\<Executing User>

De service manipulatie proces is de enige persistente mechanisme voor de malware. Wanneer deze wordt gebruikt dan kan de aanvaller willekeurig een systeem service kiezen, deze door te verwijzen naar de CRASHOVERRIDE, en ervoor zorgen dat het wordt geladen bij een systeem boot. Als dit mislukt dan zal de malware hetzij op disk weggeschreven niet starten bij een machine reboot.

Wanneer de opties voor de aanvaller worden gegeven, is een belangrijk deel van de functionaliteit geassocieerd met de remote acces tool afwezig: een commando voor het extrafilteren van data. Terwijl deze functional aangemaakt zou kunnen zijn via de commando uitvoer opties, is het te verwachten dat deze optie expliciet is gegeven het feit dat de gegeven opties om files te downloaden en kopieren op de host als de aanvaller als doel heeft de tool te gebruiken als een allesomvattend backdoor voor spionage activiteiten. Integendeel de functionaliteit van deze tool is expliciet ontwikkeld voor het facilitetren van toegang tot de machine en uitvoeren van instructies op het systeem an kan niet worden gezien als een spionage platform, data stealer of iets in die richting.

Launcher module

Details

Data wiper module

Key features

Details

IEC 104 module

Key features

Details

Iec 101 module

IEC 61850 module

OPC DA module

SIPROTEC Dos Module

Capability conclusies

Implicaties van capability

Aanvals optie: de-energize substation

Aanvals optie: force islanding event

Adding Amplification attacks

Using OPC to create a Denial of Visibility

Using CVE-2015-5374 to Hamper Protective Relays

Defense Recommendations

<https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/>

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

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

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

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

<https://www.virusbulletin.com/virusbulletin/2019/03/vb2018-paper-anatomy-attack-detecting-and-defeating-crashoverride/>

<https://www.nixu.com/blog/crashoverride-threat-electricity-networks>

<https://www.youtube.com/watch?v=TH17hSH1PGQ>

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

<https://thecyberwire.com/stories/f0c289436fff6d87ec93227b77dd3d88/crashoverride-its-aftermath-and-its-implications>

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

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

<https://www.accenture.com/us-en/blogs/blogs-crashoverride-malware-alert>

<https://www.incibe-cert.es/en/blog/crashoverride-malware-ics-back-again>

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

<https://www.csoonline.com/article/3200828/crash-override-malware-that-took-down-a-power-grid-may-have-been-a-test-run.html>

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

<https://www.belden.com/blog/industrial-security/crashoverride-first-malware-platform-designed-to-take-down-electric-grids>

<https://www.cyberbit.com/blog/ot-security/industroyer-crashoverride-ot-malware/>

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

<https://blog.claroty.com/crashoverride-a.ka.industroyer-detection-and-alerting-in-claroty-platform>

<https://www.tenable.com/in-the-news/crashoverride-ics-attack-targets-vulnerable-electrical-grid>

<https://www.powermag.com/why-crashoverride-is-a-red-flag-for-u-s-power-companies/>

Volgens Dragon, een bedrijf gespecialiseerd in industriele cybersecurity, is CrashOverride een modulair framework dat bestaat uit een backdoor, een loader module, enkele ondersteunende en payload modules. Bij een ICS aanval, moet de aanvaller eerst een proxy server instellen om een backdoor te kunnen plaatsen. Vervolgens download de CrashOverride een datawiper module, deze verwijderd registry keys, bestanden en onderbreekt prcessen die draaiten op het systeem.

De functionaliteit in de CrashOverride framework heeft als enige doel om aanvallen uit te voeren die leiden tot een electrische storing. In het rapport van Dragos komt naar voren dat er scenarios denkbaar zijn waarbij de malware kan worden ingezet om netoperaties te verstoren die resulteren in urenlange storingen op aangecallen locaties die op meerdere plekken dagenlang kunnen duren. Het is echter geen worst-case scenario; waarbij een aanveel meerder locaties simultaan worden aangevallen wat zou kunnen leiden tot een storing voor hooguit enkele dagen.

Een andere reden voor een ICS aanval met gebruik van CrashOverride zou zijn om een IEC 104 module te gebruilken waarmee de aanvaller bepaalde functionaliteiten van het systeem naar zijn hand kan zetten.

Deze functionaliteit biedt naast diverse tools voor het instellen van automatische manipulatie, ook specifieke functionaliteiten. De functies voor een malware operator zijn beperkt door de opties in het configuratiebestand.

Maar het communicatie-protocol dat de CrashOverride gebruikt is niet per se een mankement. Volgens een medewerker van Nazomi networks maakt de aanvaller alleen gebruik van legitieme instructies om incorrecte informatie te versturen naar de control units van de onderstations

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

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

<https://cyberx-labs.com/glossary/industroyer-crashoverride-crash-override/>

<https://tehtris.com/en/egambit-endpoint-security-versus-crashoverride/>

De auteur van deze blog biedt enkele oplossingen:

WildFire

Threat prevention

AutoFocus

Minemeld

Traps Advanced Endpoint Protection

ICS Protocol Visibility and Control

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

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

<https://www.msspalert.com/cybersecurity-breaches-and-attacks/u-s-dept-of-homeland-securitys-crashoverride-malware-warning-to-utilities/>

De reden dat de Industroyer/CrashOverride malware moeilijk te traceren is omdat het werkt met industriele protocollen in plaats van “zero-day”software om een doelwit mee te infecteren. De Industroyer malware is in staat de controle over te nemen van elektriciteits onderstations en stroomonderbrekers wat een stroomuitval veroorzaakt.

Het is belangrijk een bewustzijn te kweken onder secutity-experts dat er onder veiligheidsmedewerkers geen andere aanpak nodig is voor zulke bedreiginen als er al een werkmothodiek is waarbij dagelijks systemen worden doorgelicht.

Zowel overheden en private sectoren moeten investeren in het opschalen van kennis van software, hardware en protocollen in gebruik. Er moet geinvesteerd worden en prioriteiten moeten worden gesteld. Waarbij de boventoon wordt gevoerd door een aanpak van risico-management gericht, schalen van een defensielaag, implementeren van nieuwe technieken en uitvoeren van proactief beleid. De uitdaging is om aanvallen te verzachten om meer schade te voorkomen.

Chief Information Security Officers

<https://iiot-world.com/ics-security/cybersecurity/five-cybersecurity-experts-about-crashoverride-malware-main-dangers-and-lessons-for-iiot/>

Wat doet de malware

Wat doet de malware juist niet

Hoe deze bedreiging te detecteren?

Hoe kan silentdefense helpen?

<https://www.forescout.com/company/blog/crashoverride-protect-your-ics-network-against-the-newest-malware/>

<https://search.abb.com/library/Download.aspx?DocumentID=9AKK107045A1003&LanguageCode=en&DocumentPartId=&Action=Launch>

De CrashOverride malware is een uitbreidbaar raamwerk dat kan worden ingezet om kritische infrastructuur aan te vallen; systemen met de volgende protocollen IEC-101,IEC 104 en IEC1850 kan de volgende schade worden aangericht:

* Commandos versturen naar een RTU
* Kan DNP3-protocol aanvallen, een protocol dat wordt gebruikt in de VS en west-europese landen
* Is inzetbaar om op een Siemens SIPROTEC relais een Dos aanval uit te voeren, waarmee de relais kon worden uitgeschakeld

Er zijn ook mogelijkheden om je tegen de malware te beschermen namelijk:

* Check Points Application Control voor commandVisibility en baselining. Er kunnen verschillende bestaande en nieuwe protocollen mee worden geidentificeerd nl: IEC-104, DNP3 en IEC-6150 commando’s
* Er zijn ook patches beschikbaar voor de Siemens SPIROTEC Dos vulnerability

<https://blog.checkpoint.com/2017/06/21/crashoverride/>

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

Firewals en segmentatie zijn niet langer voldoende om de dreiging van doelgerichte geavanceerde malware op ICS/SCADA systemen af te weren.

Een actieve cyber defense is de volgende fase in het ontwikkelen van een volwassen cyver secrity model. Volgens SANS gaat het om een proces waarin continu veiligheidsoperaties worden opgezet om bdreigingen te identificeren en tegen te gaan. Een actief defensie-cyclus bestaat uit vier fasen die continu op bezig zijn met identificatie van onderdelen en het monitoren van netwerk security monitoren; incident response; bedreiding en omgevingsanalyse; en het verkrijgen van inlichtingen over bedreigingen in het algemeen.

<https://www.sans.org/webcasts/notpetya-dragonfly-20-crashoverride-time-active-cyber-defense-ics-scada-networks-105955>

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

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

<https://keybase.io/crashoverride>

De auteur gaat in zijn artikel uit van slachtovffer-capability-infrastructuur-adversary oftewel het Diamond model.

<https://medium.com/@sroberts/the-crash-override-chronicles-overall-8389ef178fdf>

Carshoverride was een doelgericht, semi-modulair malware framework gebruikt.

De malware is uitbreidbaar met andere protocol modules om in te zetten in andere industrien. De tool kan veel impact hebben op electrische transmissie operaties.

Het platleggen van de SCADA systemen beperkte inzicht in de controlesystemen met daarbovenop remmende herstelmogelijkheden. Daarbovenop implementeerde de aanvallers een denial-of-service tegen SIPROTEC relais. Een motief om dit te doen is waarschijnlijk om roterende onderdelen te beschadigen.

<https://www.oilandgaseng.com/articles/the-most-infamous-cyber-attacks-on-industrial-systems/>

Waarschijnlijk is volgens ESET en Dragos CrashOverride de malware achter de aanval op oekraiene in december 2016 omdat de malware in staat is om direct controle switches en stroomonderbrekers bij elektriciteitsnet van onderstations. Een ander aspect dat in de richting wijst van Industroyer/CrashOverride is dat er een ‘activation timestamp’ is gevonden op 17 december 2016, dezelfde dag als de stroomuitval.

De malware wordt niet gezien als een simple fix die weg te patches is of met een ander architectuur ontwerp onschadelijk kan worden gemaakt.

Een jaar eerder op 23 december 2015 was er ook een stroomuitval in oekraien waarbij gebruik werd gemaakt van malware om schakelaars te openen. Uit een security-analyse is gebleken dat een malware genaamd BlackEnergy en een component KillDisk werden gebruikt in 2015. Volgende de onderzoekers is er wel een vergelijkbaar concept maar is er geen link tussen de aanval en de code.

Voorkomen kan door middel van whitelisting.

Industroyer/CrashOverride maakt misbruik van ICS protocolles met een laakbare authenticatie en autorisatie.

<https://www.bankinfosecurity.com/power-grid-malware-platform-threatens-industrial-controls-a-9987>

<https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/CrashOverride.C!dha&ThreatID=2147726161>

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

<https://thehill.com/policy/cybersecurity/337877-crash-override-malware-heightens-fears-for-us-electric-grid>

<https://choice.npr.org/index.html?origin=https://www.npr.org/2017/09/08/548661962/in-crash-override-zoe-quinn-shares-her-boss-battle-against-online-harassment>

<https://pylos.co/2018/11/03/crashoverride-when-advanced-actors-look-like-amateurs/>

<https://www.inguardians.com/dhs-fbi-warn-of-attacks-against-us-energy-manufacturing-companies-and-employees/>

<https://blog.emergeits.com/alert-homeland-security-finds-u-s-power-grid-vulnerable-to-crashoverride-malware-3>

<https://www.cyberthreatalliance.org/member-share/stuxnet-to-crashoverride-to-trisis-evaluating-the-history-and-future-of-integrity-based-attacks-on-industrial-environments/>

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

<https://electricenergyonline.com/energy/magazine/1104/article/Security-Sessions-Combating-ICS-Threats.htm>

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

<https://securityaffairs.co/wordpress/59989/malware/industroyer-malware.html>

<https://isssource.com/crashoverride-designed-for-grid-takedown/>

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

<https://www.ethicalhacker.net/members/crashoverride/>

<https://www.theglobeandmail.com/arts/books-and-media/book-reviews/review-zoe-quinns-crash-override-and-ellen-paos-reset-explore-the-sexism-of-tech-culture/article36431282/>

<https://www.forbes.com/sites/kalevleetaru/2017/06/24/crash-override-and-how-cyberwarfare-is-bringing-conflict-to-the-homefront/#42eb8984277c>

<https://www.computerworld.com/article/2883732/crash-override-network-combats-online-harassment.html>

<https://fticybersecurity.com/2017-11/crashoverride-red-flag-u-s-power-companies/>

<https://www.publicpower.org/periodical/article/e-isac-offers-special-webinar-june-16-crashoverride-malware>

<https://blogs.dnvgl.com/energy/industroyer-and-industrial-control-systems>

<https://www.theverge.com/2015/1/17/7628567/crash-override>

<http://digitaleragroup.com/blog/industry-reactions-to-crashoverride-malware-feedback-friday/?style=turquoise>

## 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