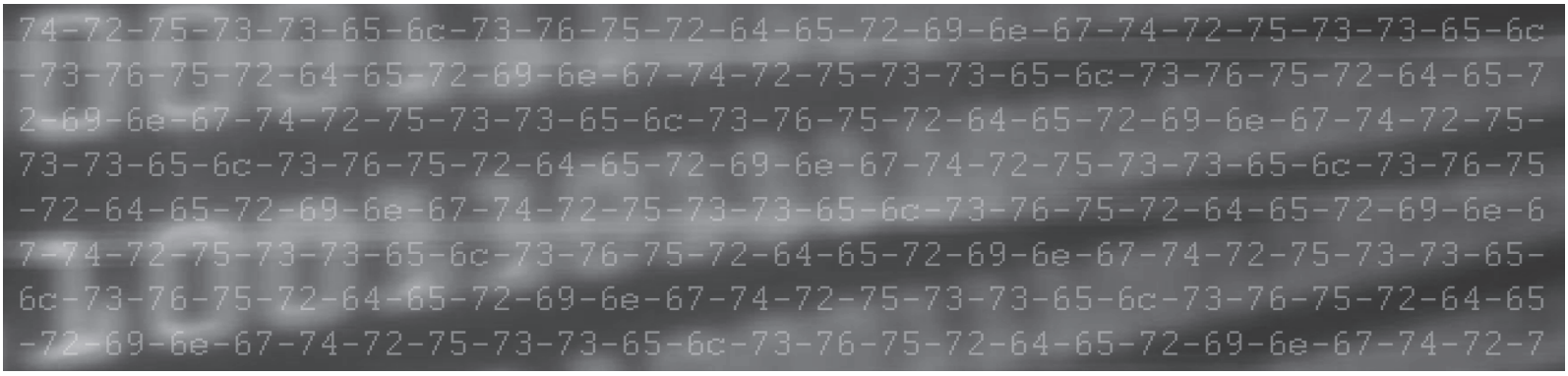
CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport

Målrettede forsøg på hacking af den danske energisektor



Undersøgelsesenheden ved Center for Cybersikkerhed

September 2018

CENTER FOR CYBERSIKKERHED

Målrettede forsøg på hacking af den danske energisektor

Denne undersøgelsesrapport beskriver flere målrettede forsøg på at få uautoriseret adgang til netværk i organisationer i den danske energisektor i 2017. Rapporten indeholder forslag til tiltag, der med udgangspunkt i erfaringerne fra hændelserne kan hjælpe myndigheder og virksomheder til at modvirke lignende forsøg på indbrud.

Hovedvurdering

- Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) har konstateret, at der har været flere målrettede forsøg på at få uautoriseret adgang til organisationer i den danske energisektor i 2017. Trusselsaktøren har brugt spear phishing og vandhulsangreb til at facilitere forsøgene på kompromittering.
- En del af de ramte organisationer driver samfundsvigtig infrastruktur, hvilket vil sige, at de varetager grundlæggende systemer, der er væsentlige for, at det danske samfund kan fungere.
- CFCS vurderer, at hændelserne var forsøg på cyberspionage udført af en statslig aktør med tilknytning til et andet lands efterretningstjeneste. Indhentning af information om samfundsvigtig infrastruktur kan desuden benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren.
- CFCS har samarbejdet med de involverede organisationer for at afdække hændelserne. Der er ikke fundet tegn på, at aktøren har haft succes med at kompromittere netværk, maskiner eller data som en konsekvens af de beskrevne hændelser.

Indledning

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) udgav i maj 2018 trusselsvurderingen Cybertruslen mod Danmark, der bl.a. konkluderer at: "Truslen fra cyberspionage er **MEGET HØJ**. Flere lande har væsentlige cyberkapaciteter, som benyttes til at spionere mod andre lande, herunder mod Danmark. Cyberspionage udgør en sikkerhedspolitisk og samfundsøkonomisk trussel mod Danmark og danske interesser. Der er tale om en særdeles aktiv trussel fra enkelte stater, der løbende forsøger at stjæle informationer fra danske myndigheder og virksomheder."

Denne undersøgelsesrapport omhandler konkrete eksempler på denne trussel. Rapporten beskriver, hvordan en trusselsaktør har forsøgt at tiltvinge sig adgang til netværk i organisationer i energisektoren. En del af de ramte organisationer driver samfundsvigtig infrastruktur, hvilket vil sige, at de varetager grundlæggende systemer, der er væsentlige for, at det danske samfund kan fungere.

Målgruppen for rapporten og dens anbefalinger er ledelse og teknikere inden for it-drift og it-sikkerhed.

CFCS har varslet eller samarbejdet med alle berørte organisationer i sagen.

CFCS' Netsikkerhedstjeneste

CFCS' Netsikkerhedstjeneste monitorerer løbende netværkstrafikken til og fra de myndigheder og virksomheder, der frivilligt er tilsluttet sensornetværket. Når CFCS har en begrundet mistanke om, at der er foregået en sikkerhedshændelse, udfører centerets teknikere analyser af netværktrafikken for at afgøre, om der er tale om ondsindet aktivitet.

Kunder, der er tilsluttet Netsikkerhedstjenesten, opnår en styrket beskyttelse mod cyberangreb, der udføres af statsstøttede eller statslige aktører.

CFCS bistår dertil både tilsluttede og ikke-tilsluttede organisationer med blandt andet varslinger, analysearbejde og rådgivningstiltag.

Forsøg på tyveri af loginoplysninger

CFCS har konstateret, at aktøren målrettet har forsøgt at stjæle loginoplysninger fra medarbejderes arbejdsstationer i de ramte organisationer. Det er gjort via spear phishing-mails med vedhæftninger og via vandhulsangreb.

Formålet med de afsendte spear phishing-mails har været at lokke modtagerne til at åbne vedhæftninger deri, så vedkommende bliver kompromitteret. Mailene og de vedhæftede dokumenter imiterer legitime henvendelser for at narre modtagerne. Aktøren har sendt en del af phishing-mailene til funktionspostkasser, som bl.a. bruges af jobansøgere, der er offentligt tilgængelige på visse af organisationernes hjemmesider. Når det vedhæftede dokument åbnes, igangsættes tyveriet automatisk, medmindre relevante sikkerhedsforanstaltninger er implementeret.

Spear phishing
Hensigten med spear phishing er at manipulere modtagere til at åbne vedhæftede filer eller klikke på indlejrede links i en fremsendt mail. Afsenderens hensigt kan være at inficere offerets maskine med malware eller lokke vedkommende til at opgive følsomme informationer. Spear phishing-mails er målrettet, så de virker særlig relevante, overbevisende eller tillidsvækkende for modtageren.

Sådan stopper du kompromittering via spear phishing
Se CFCS' sikkerhedsvejledning Spear-phishing – et voksende problem for mere information om, hvordan du opdager og stopper spear phishing.

Yderligere har aktøren strategisk udvalgt en række legitime hjemmesider og kompromitteret dem for at misbruge dem som platform for angreb på udvalgte besøgende. En del af de hjemmesider, aktøren har udnyttet som vandhuller, er relateret til og normalt anvendt i energisektoren. Det øger sandsynligheden for, at en medarbejder fra energisektoren besøger hjemmesiden og bliver kompromitteret. Når vandhullet besøges, indlæses et indlagt ondsindet script derfra, og tyveriet igangsættes automatisk, medmindre relevante sikkerhedsforanstaltninger er implementeret.

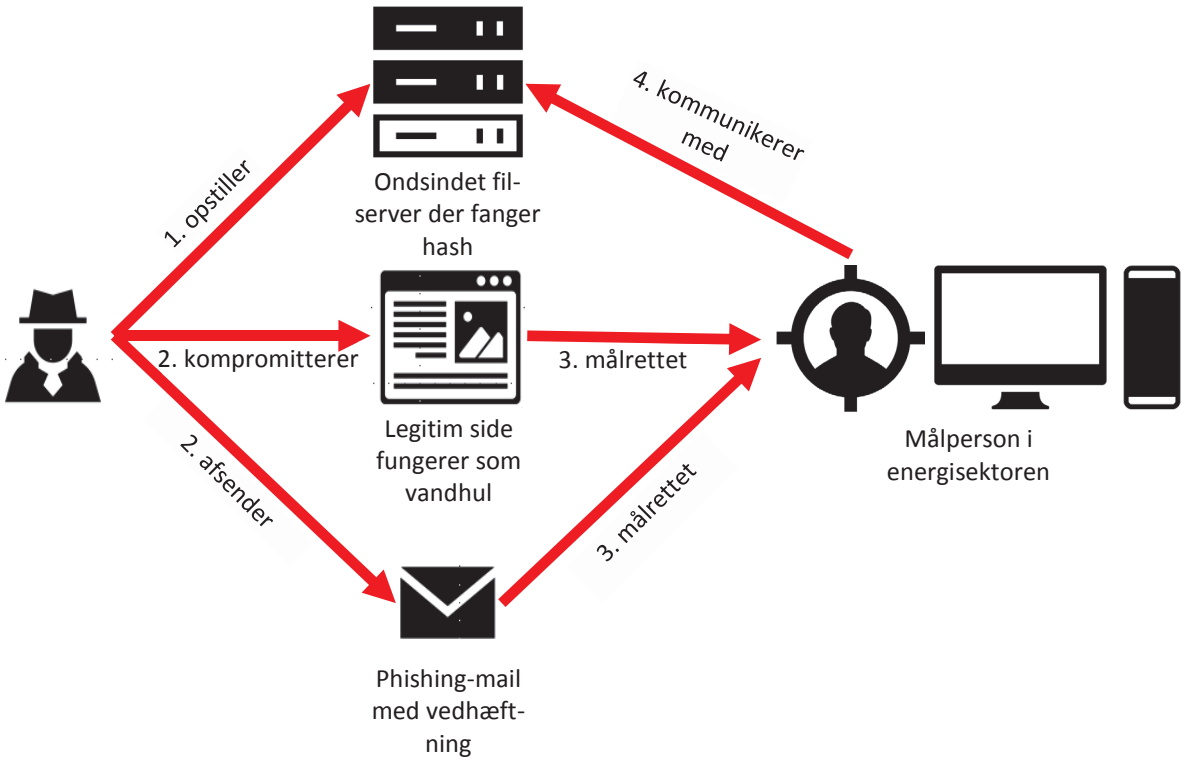
Vandhulsangreb
I et vandhulsangreb kompromitteres og misbruges en legitim hjemmeside som platform til at kompromittere et eller flere mål, der forventes at besøge siden.

Sådan stopper du kompromittering via vandhulsangreb
Vandhulsangreb kan designes til at udnytte mange forskellige sårbarheder, og der findes derfor ikke en enkelt løsning til at stoppe dem. Risikoen for at blive kompromitteret kan reduceres ved at følge rådene i CFCS' sikkerhedsvejledning Cyberforsvar der virker.

Det vedhæftede dokument i phishing-mailen og scriptet i vandhullerne udløser den samme teknik til at stjæle loginoplysninger. Offerets maskine lokkes til automatisk at spørge efter en fil fra en server på internettet kontrolleret af aktøren. Dette sker uden offerets viden eller godkendelse. Kommunikationen foregår via server message block (SMB) og web-based distributed authoring

and versioning (WebDAV). De to protokoller anvendes begge legitimt til bl.a. fjernadministration af filer og dokumenter.

Som en del af kommunikationen afsender maskinen sine Windows-loginoplysninger i kryptografisk form, en hash, til aktørens server. Serveren opfanger og gemmer denne hash, som nu kan udnyttes af aktøren til at få adgang til organisationens netværk.



Figur 1: Tyveri af loginoplysninger via spear phishing og vandhulsangreb

Sådan stopper du tyveri af loginoplysninger via SMB-kald

En måde at stoppe uønsket netværkstrafik i at forlade et internt netværk er ved at implementere egress-filtrering. Filtreringen bør implementeres så tæt på netværkets perimeter som muligt, f.eks. på en router der forbinder til organisationens internetudbyder. Egress-filtreringen kan blokere udgående trafik, f.eks. i forbindelse med tyveri via SMB-kald, der benytter særlige porte ved at lukke dem i routerens firewall.

I dette tilfælde anbefaler CFCS, at det overvejes, at der i internetvendte routere blokeres for trafik over TCP port 139 (NETBIOS) og 445 (SMB) samt UDP port 137-138 (NETBIOS). Dertil bør det overvejes at blokere for WebDAV-forbindelser samme sted. Bemærk at filtreringen risikerer at forstyrre legitim trafik til internettet.

Efter hashen er stjålet, kan den potentielt udsættes for offline forcering af aktøren. I et forcerings-angreb forsøges på automatiseret vis at gætte kodeordet, der matcher den stjålne hash-værdi. Hvis forceringen lykkes, vil offerets loginoplysninger fremgå i klar tekst.

Med de stjålne loginoplysninger kan aktøren derefter potentielt logge ind i organisationens net-værk over internettet, f.eks. via et almindeligt fjernstyringsprogram, og fremstå som en legitim bruger. Aktøren kan også forsøge at udnytte en sårbarhed i Windows' håndtering af kodeord, der gør det muligt at logge ind blot med hash'en i et pass-the-hash-angreb. CFCS har ikke set tegn på, at disse ting er sket.

Sådan stopper du fjernlogin med stjålne loginoplysninger

Brug af to-faktor-autentificering vil ofte forhindre fjernlogin med stjålne loginoplysninger i at virke. Grunden er, at der ved to-faktorautentificering kræves et separat tidsbaseret kodeord for at logge på. Dette ekstra kodeord kan angriberen ikke opsnappe ved den metode, der er beskrevet her.

Organisationen bør samtidig implementere kodeordspolitikker for alle ansatte, der sikrer regelmæssige kodeordsskifte, samt at der anvendes lange kodeord, der kan modstå forcering.

For mere information om god praksis i brugen af kodeord, se CFCS' Passwordvejledning.

Hvis en trusselsaktør har succes med at logge ind i et netværk som legitim bruger, kan det potenti-elt udnyttes til at trænge længere ind i organisationens interne netværk. Det kan f.eks. gøres via installation af malware eller ved at opnå administratorrettigheder, der giver adgang til større dele af netværket.

CFCS har ikke set tegn på, at det er lykkedes for aktøren at stjæle loginoplysninger eller få adgang til de ramte organisationers netværk i forbindelse med de hændelser, der er beskrevet her.

Truslen

CFCS vurderer, at der i omtalte hændelser er tale om forsøg på cyberspionage udført af en statslig aktør med tilknytning til et andet lands efterretningstjeneste.

Cyberspionage mod energisektoren er både politisk og økonomisk motiveret. Spionagen kan bl.a. skaffe viden, der kan bruges til at komme i besiddelse af nye teknologier, fremme egne energisel-skabers interesser eller undergrave forsyningssikkerheden i forbindelse med en eventuel politisk eller militær konflikt.

Indhentning af information om kritisk infrastruktur kan desuden benyttes i forberedelsen af destruktive cyberangreb eller fysiske angreb rettet mod sektoren. Cyberspionagen er derfor ikke kun en økonomisk og politisk trussel, men udgør også en potentiel trussel mod forsyningssikkerheden i Danmark. CFCS vurderer imidlertid, at det på kort sigt er mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod samfundsvigtig infrastruktur i Danmark, herunder i energisektoren. Truslen kan dog ændre sig i forbindelse med en skærpet politisk eller militær konflikt med visse lande.

Anbefalinger

Følgende anbefalinger kan reducere risikoen for eller konsekvensen ved kompromitteringer som her beskrevet.

- Bloker for trafik over TCP port 139 (NETBIOS) og 445 (SMB) samt UDP port 137-138 (NETBIOS) i internetvendte routere. Alle versioner af SMB er sårbare. Dertil bør det overvejes at blokere for WebDAV-forbindelser samme sted. Bemærk at filtreringen risikerer at forstyrre legitim trafik til internettet. Overvej dertil at lukke for alle ubrugte porte.
- Begræns rettighederne på nettet for den enkelte bruger til kun det, som brugerens jobfunktion kræver.
- Undgå at standardbrugere er lokaladministrator på deres arbejdsstation.
- Begræns antallet og brugen af privilegerede konti.
- Begræns privilegerede kontis adgange til Internettet og brug af mailservice.
- Udfør kun IT-administrative opgaver fra dedikerede og gerne ekstra hærdede arbejdsstationer.
- Anvend Microsoft Management Console (MMC) værktøjer i stedet for værktøjer baseret på Remote Desktop Protokollen. Derved undgås det, at hash-værdier fra privilegerede konti efterlades i lageret på ikke-relevante arbejdsstationer i netværket.
- Skift password på privilegerede konti ofte. Det kan eksempelvis være én gang om måneden.
- Anvend to- eller flerfaktorautentifikation.
- Opdater løbende operativsystemer og applikationer.
- Fjern muligheden for at brugerens password-hash gemmes ved at sætte Group policy ”Network security: Do not store LAN Manager hash value on next password change” til ”Enable” på Actice Directory-serveren.
- Segmenter netværket, således at kritiske dele ikke umiddelbart er tilgængelige fra alle steder i netværket. Eksempelvis kan man begrænse adgangene til visse dele af netværket, hvis

brugeren logger på netværket hjemmefra. Vær opmærksom på, at alle brugere efterfølgende skal skifte password, og at nogle ældre ikke–Microsoftapplikationer kan stoppe med at fungere korrekt.

- Følg de syv trin i CFCS' sikkerhedsvejledning Cyberforsvar der virker

Ovennævnte anbefalinger er i stor udstrækning rettet imod it-miljøer baseret på Microsoft, men mange af anbefalingerne kan med fordel også indarbejdes i it-miljøer, der er baseret på andre styresystemer.

CFCS' Undersøgelsesenhed

I december 2014 udkom den første nationale strategi for cyber- og informationssikkerhed. Et af initiativerne i strategien var etableringen af en Undersøgelsesenhed i CFCS, hvis opgave det er at undersøge og afdække større cybersikkerhedshændelser. På baggrund af disse udredninger udsender CFCS rapporter, så myndigheder og virksomheder kan drage nytte af erfaringerne fra tidligere hændelser og beskytte sig bedre.

Uddrag fra National strategi for cyber- og informationsstrategi 2014:
"Regeringen har indført, at alle statslige myndigheder skal underrette Center for Cybersikkerhed ved større cybersikkerhedshændelser. Blandt de cybersikkerhedshændelser, som indrapporteres, vil der være hændelser, der er særlige alvorlige. Regeringen ønsker, at der sker relevant udredning og analyse af sådanne hændelser. Samtidig skal det sikres, at erfaringerne fra hændelserne opsamles og i størst muligt omfang stilles til rådighed for andre myndigheder og virksomheder, således at erfaringerne kan anvendes aktivt i arbejdet med at forebygge fremtidige hændelser."

FE bruger denne skala for sandsynlighed i analyser: