CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport

Phishing uden fangst - Udenrigsministeriet under angreb

Undersøgelsesenheden ved Center for Cybersikkerhed

Januar 2016

CENTER FOR CYBERSIKKERHED

Rapport om APT-angreb mod Udenrigsministeriet

Indhold

Resumé

Denne rapport beskriver et APT-angreb mod Udenrigsministeriet (UM), som er foregået fra december 2014 til juli 2015. Analysen viser, at det via phishing-mails lykkedes angriberne at inficere en enkelt maskine med malware. En af Udenrigsministeriets it-sikkerhedsløsninger stoppede malwaren i at kommunikere udadtil, og angriberne har derfor ***ikke*** haft adgang til maskinen eller data på den. Rapporten beskriver og analyserer angrebet, og forklarer hvordan det blev stoppet.

Rapporten er udarbejdet af Undersøgelsesenheden, der er en del af Center for Cybersikkerhed (CFCS) i Forsvarets Efterretningstjeneste. Undersøgelsesenheden har til opgave at opsamle erfaringer fra sådanne hændelser og stille viden til rådighed for offentligheden for at modvirke fremtidige, lignende hændelser.

I slutningen af rapporten er der med udgangspunkt i erfaringerne fra angrebet samlet en række konkrete anbefalinger henvendt til myndigheder og virksomheder.

Sagen: Et APT-angreb på Udenrigsministeriet

D. 6. juli 2015 får Center for Cybersikkerhed mistanke om, at en pc tilhørende Udenrigsministeriet er inficeret med malware. D. 7. juli 2015 indledes en dialog med UM, som bliver bedt om at identificere den inficerede pc, og 3. august 2015 modtager CFCS maskinen til grundigere analyse. Analysen viser, at maskinen har været inficeret med malware i minimum fire måneder. Analyser viser endvidere, at inficeringen er isoleret til maskinen, og at angriberne ***ikke*** har haft adgang til maskinen eller data på den. Maskinen er blevet kompromitteret via phishing-mails sendt til en medarbejders e-mailkonto. Mailadressen er blandt otte andre UM-mål, som har modtaget i alt 47 phishing-mails i perioden december 2014 - juli 2015. Udover UM har en lang række udenlandske entiteter været mål i kampagnen, heriblandt offentlige organisationer, private virksomheder og privatpersoner.

I det følgende præsenteres en analyse og gennemgang af forløbet omkring phishing-angrebet mod UM. Rapporten indeholder tre kapitler med en teknisk gennemgang af angrebet baseret på: 1) netværksanalyse af trafik i UM-sensoren, 2) malware-analyse af samples taget fra maskinen og 3) forensic-analyse af den kompromitterede maskine.

Efter den tekniske gennemgang gives en kort beskrivelse af den samlede kampagne set i et bredere perspektiv. Endeligt afsluttes rapporten med en række anbefalinger til hvordan et lignende angreb mod myndigheder eller virksomheder kan stoppes.

Målgruppen for rapporten er ledelse og teknikere inden for it-drift og it-sikkerhed. Hensigten med rapporten er derudover, at alle med en vis teknisk indsigt kan få udbytte af at læse om CFCS' virke og se hvordan et større cyberangreb mod Danmark ser ud.

Alle relevante parter, der har været berørt af angrebet, er blevet varslet om sagen.

CFCS' tekniske analysetilgange

CFCS bruger tre typer teknisk analyse til at afdække cyberhændelser:

1. **Netværksanalyse** fokuserer primært på logs fra datasensorerne hos CFCS'kunder samt fra firewalls, og søger at kortlægge kommunikationen mellem maskiner og netværk.
2. **Malware-analyse** kigger på det enkelte stykke malware og beskriver dets funktonalitet og særlige kendetegn.
3. **Forensic-analyse** har fokus på, hvad der er hændt på den enkelte maskine, herunder om der har været ondsindet aktivitet på den.

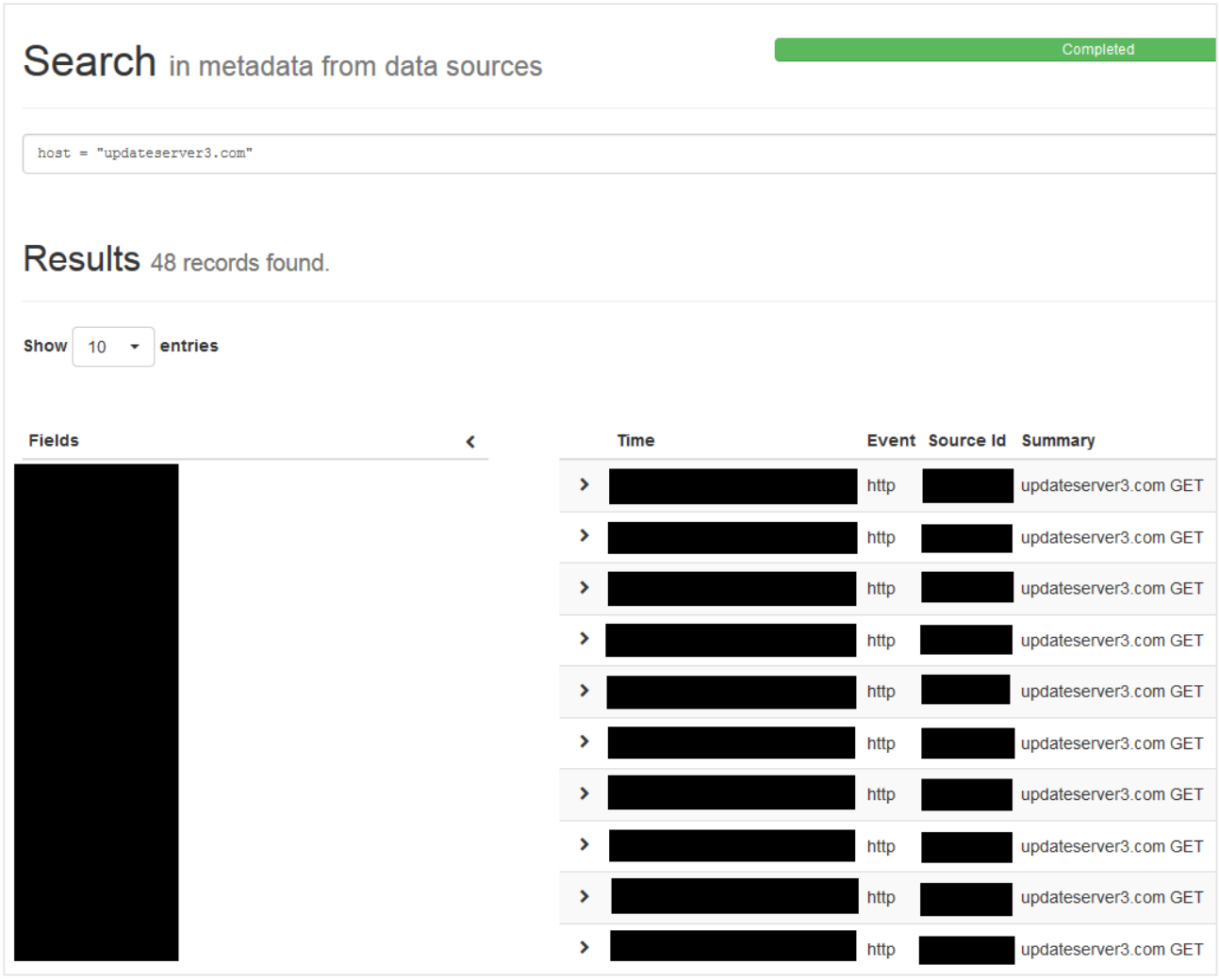
1. Netværksanalyse

Dette kapitel beskriver, hvordan angrebet mod UM blev opdaget af CFCS. Derefter er der en analyse af, hvordan angrebet er foregået, hvor mange phishing-mails, der er blevet sendt, hvornår og til hvem. I slutningen af kapitlet er der en beskrivelse af, hvordan angriberne har brugt kompromitterede afsenderadresser for at få deres phishing-mails til at se mere legitime ud i modtagernes øjne.

Malware-trafik findes i UM-sensoren

Inficeringen af UM-maskinen bliver opdaget som led i en rutinemæssig kontrolgennemgang af nye indicators of compromise (IOC) fra en rapport udarbejdet af et it-sikkerhedsfirma. IOC'er, der blandt andet består af IP-adresser, malware-signaturer og domæne-navne, anvendes til at søge efter ondsindet netværkstrafik gemt i sensorerne, som er installeret hos CFCS' civile og militære kunder. Såkaldt trafikdata fra sensorerne, eksempelvis en e-mails afsender- og modtagerinformation samt emnefelt, gemmes i CFCS datahåndteringssystem (se figur 1). De såkaldte pakkedata, eksempelvis en e-mails indhold og vedhæftede filer, gemmes lokalt hos kunden. Disse data må kun analyseres af CFCS, hvis der er en begrundet mistanke om en sikkerhedshændelse.

I dette tilfælde resulterer en manuel søgning på IOC'er relateret til malwaren i følgende resultat:



Figur 1: Søgning på IOC relateret til malwaren.

Søgningen viser, at der i perioder i 2015 har været netværkstrafik hos UM til domænet 'update-server3[.]com', der ifølge it-sikkerheds-rapporten er ondsindet. Malwaren på den inficerede maskine har altså på dette tidspunkt forsøgt at kommunikere med domænet, der fungerer som command and control-infrastruktur (C2); muligvis med henblik på at stjæle data.

Command and control-infrastruktur

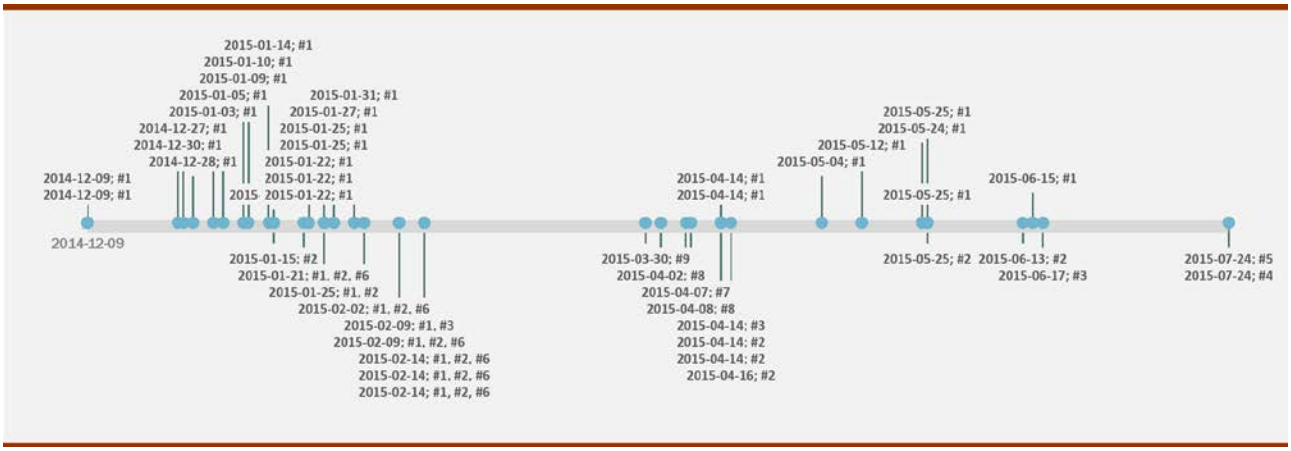
En command and control-server, også kaldet C2-server eller C&C-server, er betegnelsen for den tekniske infrastruktur som en angriber anvender til at kontrollere sin malware. En C2-server kan f.eks. flytte data ind og ud af en inficeret maskine eller et netværk via den malware, den kontrollerer. På den måde kan en angriber inficere en maskine eller et netværk med yderligere malware eller stjæle værdifuld information.

Med udgangspunkt i IOC'erne opretter CFCS' teknikere automatiserede søgeregler som løbende holdes op i mod netværkstrafikken i alle sensorerne. Fremadrettet vil nye angreb med lignende IOC'er på kunder, der er tilsluttet en sensor, derfor automatisk forårsage en alarm i systemet og

give anledning til en nærmere analyse. Det er fast procedure, at IOC'er fra åbne og lukkede kilder jævnligt lægges ind i sensor-systemet.

Angrebsvektor og kompromittering

I denne kampagne mod UM er der fundet 47 phishing-mails. Angrebet varede i mere end syv måneder og ramte ni forskellige e-mail-konti. I figur 2 nedenfor ses en tidslinje over modtagne phishing-mails og hvilke mail-konti, de er sendt til (nummereret #1 til #9). Angrebet strækker sig fra d. 9. december 2014 til d. 24. juli 2015.



Figur 2: Tidslinje over modtagne phishing-mails, inklusiv modtager (nummereret)

Som det ses i figur 2, rammes en enkelt postkasse, #1, i begyndelsen af angrebet med et stort antal forskellige phishing-mails. I januar og februar 2015 tilføjes #2, #3 og – i et enkelt tilfælde - #4 til modtagerlisten. Efter mere end en måneds pause ændrer angriberne taktik i slutningen af marts 2015, og der udsendes derefter færre mails til et bredere udsnit af modtagere.

UM har fanget nogle af de afsendte phishing-mails i deres egen mailscanner, som søger efter ondsindede indkomne e-mails, men et antal e-mails er alligevel sluppet igennem til brugernes indbakker. Grunden til, at nogle phishing-mails er sluppet igennem sikkerhedsnettet, kan muligvis være, at UM's sikkerhedsløsninger er blevet opdateret undervejs med nye signaturer og derfor er blevet bedre i stand til at identificere malwaren. Endeligt viser analysen (se mere s. 11), at der afsendes flere forskellige versioner af malwaren, og at de nyere versioner er krypteret med henblik på at få dem til at se uskyldige ud. Dette kan have gjort det sværere at opsnappe de ondsindede e-mails.

Angribernes vedholdenhed og gentagne forsøg mod postkasse #1 resulterer i en kompromittering af denne enkelte maskine. Det kan ikke bestemmes præcist, hvornår inficeringen er fundet sted. Dette uddybes i afsnittet 'Analyse af den kompromitterede maskine' s. 13.

Der er ikke registreret yderligere inficeringer af UM-maskiner i relation til denne phishing-kampagne.

Phishing og spear-phishing

En phishing-kampagne er generelt karakteriseret ved, at der udsendes en meget stor mængde enslydende mails til en bred personkreds. Hensigten er at manipulere modtagerne til at åbne vedhæftede filer eller klikke på indlejrede links i en fremsendt mail. Målet for angriberen kan være at inficere offerets maskine med malware eller lokke vedkommende til at opgive følsomme informationer.

Spear-phishing-mails er forskellige fra phishing-mails ved at være målrettede enkeltpersoner, og de er typisk lavet, så de virker særlig relevante, overbevisende og tillidsvækkende for offeret.

Kompromitterede afsenderkonti

Et særtræk ved kampagnen er, at angriberne har anvendt kompromitterede e-mail-konti som afsenderadresse med henblik på at få de ondsindede phishing-mails til at fremstå legitime i modtagerens øjne. Modtagerne i UM har således i visse tilfælde haft mail-korrespondance med personen bag den kompromitterede afsenderadresse, som de har modtaget en phishing-mail fra. Det er muligt, at angriberne har stjålet UM-mailadresserne fra mailkartoteket i de selv samme kompromitterede e-mail-konti.

En udenlandsk ambassade og et udenlandsk universitet er to af de fremtrædende kompromitterede afsenderadresser. For de to afsendere er emnefeltet i phishing-mailen afpasset afsenderadressen; igen for at få phishing-mailen til at se mere legitim ud.

Blandt afsenderadresserne er der også anvendt en e-mailkonto fra Danmarks Tekniske Universitet (DTU). Angriberne har muligvis bevidst anvendt en dansk konto til at ramme danske mål.

Angriberne har i alt anvendt 21 afsender-adresser til at sende phishing-mails til UM. Da de resterende afsender-adresser har endelserne: ’mail.com’, ’mail.ru’, ’gmail.com’, ’hotmail.com’, ’outlook.com’ eller ’yahoo.com’, er det ikke muligt at identificere yderligere kompromitterede afsender-konti.

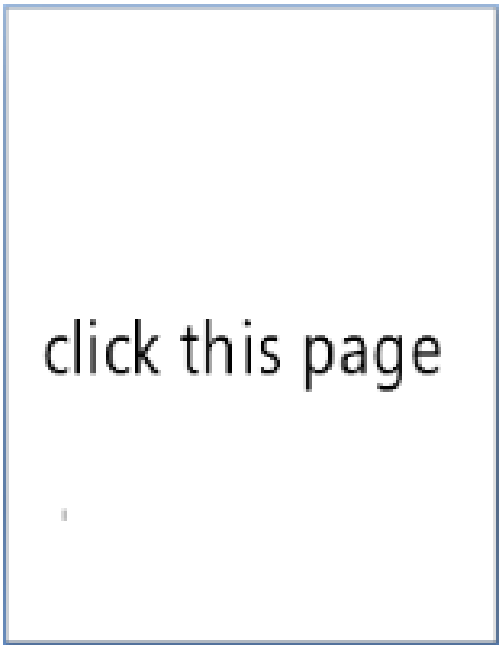
2. Malware-analyse

Dette kapitel beskriver, hvordan angriberne forsøger at manipulere deres mål til uden deres viden at inficere deres maskiner via ondsindede fil-vedhæftninger. Derefter er der en forklaring på, hvordan malwaren installerer sig på maskinen, hvilke funktioner den har og hvordan den skjuler sig fra at blive opdaget. Endeligt er der en analyse af forskellige tegn på organisationen bag angrebet fundet i malwaren.

Levering af malwaren

De 47 phishing-mails er vedhæftet enten en PowerPoint-fil (*.pps), en PowerPoint slide-show-fil (*.ppsx) eller et Worddokument (*.docx). Klikkes der på den vedlagte fil i phishing-mailen, åbnes det tilsvarende Office-program.

I Word-dokumentet er der indlagt et stort ikon, hvorpå der står 'click this page'. Et eksempel kan ses nedenfor:



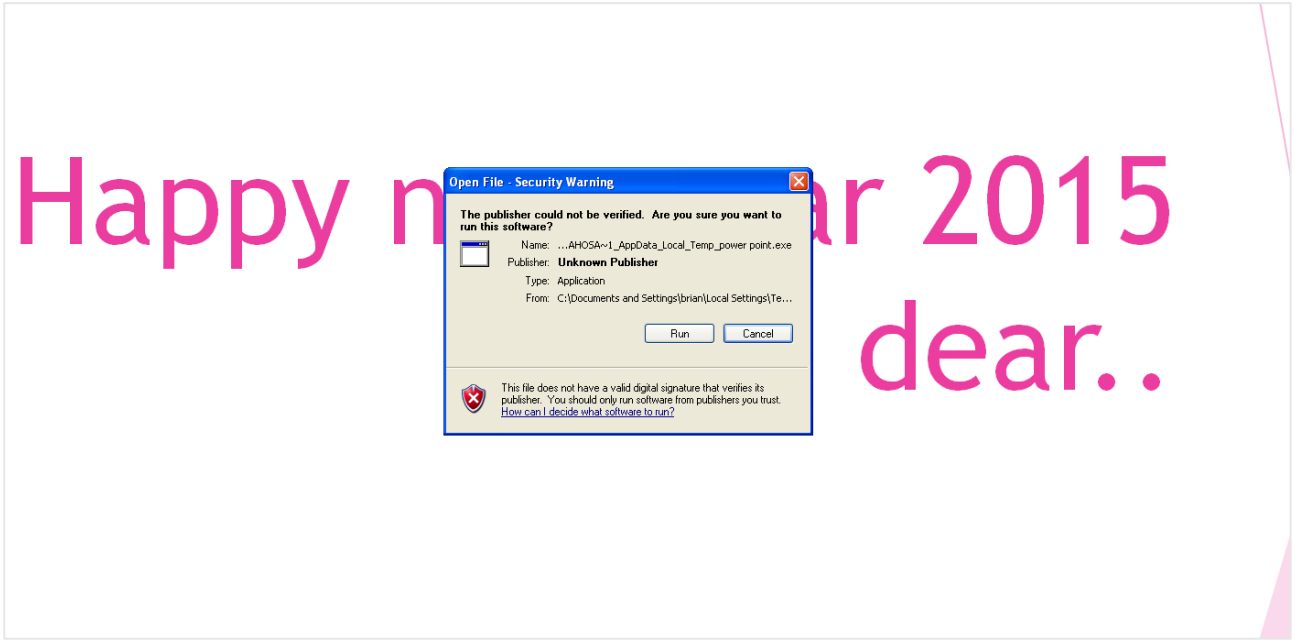
Figur 3: Word-dokument med indlagt ikon/exe-fil

Ved klik eksekveres den indlagte ondsindede exe-fil ved navn 'power point.exe', og malware-installationen begyndes. Teknikken er anvendt, for at et potentielt offer ikke skal mistænke, at der er tale om eksekvering af en exe-fil.

I PowerPoint-præsentationerne er 'power point.exe' indlagt i skjul, og forsøges automatisk eksekveret, hvis brugeren prøver at se præsentationen.

I de tilfælde, hvor den vedhæftede fil er i .ppsx-format, køres præsentationen med det samme, når brugeren har klikket på den i sin mail-klient. Herefter forsøges 'power point.exe' igen automatisk eksekveret.

I alle tre tilfælde vil Windows dog typisk (alt efter brugerens Windows-sikkerhedsindstilling) præsentere brugeren for en advarsel og bede om en bekræftelse på, at filen skal køres. Et eksempel kan ses nedenfor:



Figur 4: Windows sikkerhedsadvarsel ved afspilning af PowerPoint-præsentation med indlagt exe-fil

Visse PowerPoints indeholder op til tyve slides med tilfældigt - og nogle gange ganske underholdende - materiale som f.eks. tegninger og videoer. Hensigten er at få præsentationen til at se legitim ud, sådan at den ikke vækker offerets mistanke om, at han eller hendes maskine netop er blevet inficeret med malware.

Malware-installation og funktionalitet

Den indlagte ondsindede fil 'power point.exe' er et selvudpakkende arkiv, der lægger følgende tre filer i brugerens %TEMP%/ -bibliotek i en folder kaldet tmp{4 tilfældige tal}, f.eks. "tmp5291":

- **ins{2-4 tilfældige tal}.exe**
- **mpro842.dll**
- **readme.txt**

ins{2-4 tilfældige tal}.exe (f.eks. "ins211.exe") giver den installerede malware vedholdenhed på den kompromitterede maskine. Dette gøres på forskellige måder. For at skjule tilstedeværelsen af malware på computeren, flytter denne fil de to andre malware-filer til mappen C:\ProgramData\Adobe. Malwaren imiterer PDF-programmet Adobes mappe, der ikke almindeligvis giver anledning til mistanke. Dertil dannes en registreringsnøgle, der tilsvarende imiterer Adobe AIR plugin med passende filbeskrivelse.

mpro842.dll: indeholder alle malwarens remote access tool (RAT)-funktionaliteter. Analysen viser, at malwaren indeholder typiske RAT-funktioner, der blandt andet kan lave systeminformations-indhentning, og som kan give operatørerne af malwaren fjernadgang til maskinen.

Dertil danner malwaren logfiler i mappen '%APPDATA%/Adobe,' ved navn mpro842,.ini og mpro842,.dat (bemærk, at kommaerne ikke er en fejl). I den sidste logfil indsamles information om, hvilke programmer brugeren anvender, indtastninger i søgefelter og kodeordsfelter samt em-nefeltet i e-mails. Der er altså tale om en keylogger-funktion. I afsnittet 'Kampagnen bredere set', s. 14, diskuteres hvordan disse bidder af information kan have nytte for en angriber.

Det har været muligt at identificere malware-versionsnummeret, f.eks. "00022 CPL (systm11)", hvoraf de fem første cifre afsendes, når malwaren kommunikerer med sin C2. Malware-designerne og operatørerne anvender versionsnumre for at holde styr på hvilken udgave af deres malware, der kommunikerer hjem ved en kompromittering. Ligesom der jævnligt laves opdateringer til legi-tim software for at forbedre et produkt, kan malware-designerne videreudvikle på malware og tilføje nye funktionaliteter eller beskyttelses-mekanismer.

Remote access tool (RAT)
Et "remote access tool", eller fjernstyringsværktøj, er et stykke software, der giver fjernadgang til en maskine. Sådanne værktøjer anvendes ofte helt legitimt i forbindelse med f.eks. it-support eller til opsætning af fjern-arbejdspladser. Et RAT kan også være en del af et stykke malware, der i skjul giver en angriber uretmæssig adgang til en maskine eller netværk.

readme.txt: er ikke en nødvendig del af malware-funktionaliteten, men indeholder uskyldigt ud-seende tekst relateret til "Aptana Studio", der har til hensigt at få malwaren til at se legitim ud. Aptana Studios er ikke relateret til Adobe, der ellers er søgt imiteret. Se eksempel nedenfor:

> Welcome!
>
> If you are reading this, we'd like to thank you for your interest Aptana Studio. Please read through this guide carefully. For Aptana Studio 2 Upgraders […]

Anti-detektionsteknikker

Efter registreringsnøglen er dannet af ins{2-4 tilfældige tal}.exe, pauser malwaren, indtil maskinen genstartes. Ved opstart tjekker malwaren for tilstedeværelsen af en række almindelige antivirus-programmer og stopper eksekveringen af malwaren, hvis de findes. Dette forhindrer potentielt, at malwaren fanges og registreres af maskinens antivirus. Formålet med dette kan være at undgå at gøre offeret opmærksom på inficeringen. En anden grund kan være at undgå, at det installerede antivirus-program får mulighed for at indsamle og hjemsende samples af malwaren, hvis inficerin-

gen skulle blive opdaget. Dette mindsker antivirus-virksomhedernes viden om malwaren og derved også evnen til at fange denne specifikke malware under andre angreb og kompromitteringer.

Designerne af malwaren har forsøgt at kryptere og skjule en del af RAT-funktionaliteterne for at gøre det sværere for sikkerhedsanalytikere at afdække, hvad malwaren kan. Krypteringen kan også have den funktion at gøre det sværere for mailscannere at opdage malwaren i indkomne ondsindede mails.

Brugen af kommaer i mappe- og filnavne, f.eks. 'mpro842,.ini,' (se afsnittet om mpro842.dll), kan muligvis være et lavpraktisk forsøg på at omgå korrekt registrering af fil-signaturer til brug i antivirusprogrammer. Brugen af tilfældige cifre i filnavne f.eks. "ins{2-4 tilfældige tal}.exe" kan spille samme rolle.

Endeligt er malwaren designet til at skjule sig for teknisk analyse. Når malware analyseres af it-teknikere, indsættes og køres det i et kontrolleret miljø - en "sandbox". Efter malwaren er eksekveret, registreres alle følgende ændringer på systemet af sandbox-programmet. På den måde kan teknikerne afdække, hvorledes malwaren agerer og virker på en inficeret maskine. Malwaren er designet til først at begynde sin installation fem minutter efter eksekvering. På den måde vil sandbox-programmet ikke registrere ændringer, medmindre det er sat til at diagnosticere i mere end fem minutter.

Flere versioner af malware

Der kan identificeres en række versioner af den malware, der har været anvendt i kampagnen. Ændringerne i malwaren ser dog ikke ud til at tilføje megen ny funktionalitet men er primært fokuseret på at kryptere og skjule stadig flere dele af malwarens RAT-karakteristika.

Angriber-brugernavne og bagvedliggende organisation

Analysen viser, at Windows-brugernavnet for de personer, der har lavet de ondsindede vedhæftede filer, er gemt i selve dokumentet. Dette er sandsynligvis utilsigtet fra malware-designernes side. Som eksempel kan følgende information udtrækkes fra vedhæftningen "director.docx":

> Creator: fedora
> Last Modified By: fedora
> Create Date: 2014:05:09 04:37:00Z
> Modify Date: 2014:05:09 04:37:00Z

Ud fra analyse af malwaren, der er blevet sendt til UM, har det været muligt at opstille følgende tabel med information om de ti forskellige vedhæftninger, der er brugt i phishing-angrebet:

Dato	Brugernavn	navn på vedhæftning	Filtype	malware-versionsnummer	Command and control
30 Dec 2014	payan	11.pps	.pps	00009	updateserver1.com bestupser.awardspace.info
30 Dec 2014	ya hosain	year 2015.pps	.pps	00019	us1s2.strangled.net updateserver3.com
15 Jan 2015	ya hosain	happy new yaer.pps	.pps	00019	us1s2.strangled.net updateserver3.com
22 Jan 2015	mofajeho	ksa event.pps	.pps	00007	updateserver1.com bestupser.awardspace.info
----------	135133128 YAHOSA	i.ppsx	.ppsx	00011	updateserver1.com bestupser.awardspace.info
----------	ya hosain	why.pps	.pps	00019	us1s2.strangled.net updateserver3.com
14 Feb 2015	payan	salam.pps	.pps	00007	updateserver1.com bestupser.awardspace.info
14 Apr 2015	fedora	director.docx	.docx	00022	us1s2.strangled.net updateserver3.com
24 Maj 2015	salazar	message.docx	.docx	00022	us1s2.strangled.net updateserver3.com
15 Jun 2015	mofajeh	dunya.pps	.pps	00024	us1s2.strangled.net updateserver3.com

Tabel 1: Brugernavn, filvedhæftningsnavn, filtype, malware-versionsnummer og C2 for ti ondsindet vedhæftninger brugt i angrebet.

Tabellen giver et indtryk af organisationen bag angrebet. For det første findes der syv forskellige brugernavne i metadata i de ondsindede vedhæftninger. Dette giver muligvis en indikation på antallet af malware-designere og operatører bag angrebet. Det er dog her vigtigt at understrege, at der ikke nødvendigvis er tale om dårlig operationssikkerhed fra angribernes side, og at disse informationer nemt kan manipuleres til at sløre de virkelige angribere. For det andet indikerer brugen af forskellige versioner af malware i perioden en lettere ukoordineret organisation, der ikke benytter sig af den seneste opdaterede udgave af deres "våben". F.eks. anvender brugeren 'payan' i en phishing-mail fra den 14. februar 2015 version 00007 af malwaren til trods for, at vi kan konstatere, at en nyere version, 00019, er i brug 16 dage før, den 28. januar 2015. Dette kan reducere sandsynligheden for en succesfuld kompromittering. Grunden er, at ældre versioner af malwaren kommunikerer med en tilsvarende ældre C2-infrastruktur (se tabellens højre kolonne "Command and control"). Jo længere den samme C2-infrastruktur anvendes, desto større er sandsynligheden for, at den anvendte IP-adresse er blevet opdaget og registreret som en IOC med tilsvarende højere sandsynlighed for, at malwaren bliver stoppet af ofrenes sikkerhedsforanstaltninger.

Endvidere er der i en og samme mail (30. december 2014) to vedhæftninger med malware med forskellige versioner (00009 og 00019). For angriberne har det den negative konsekvens, at den bagvedliggende associerede C2-infrastruktur med sikkerhed kan sammenkobles og konstateres ondsindet: updateserver1[.]com og bestupser.awardspace[.]info med us1s2.strangled[.]net og updateserver3[.]com.

3. Forensic-analyse

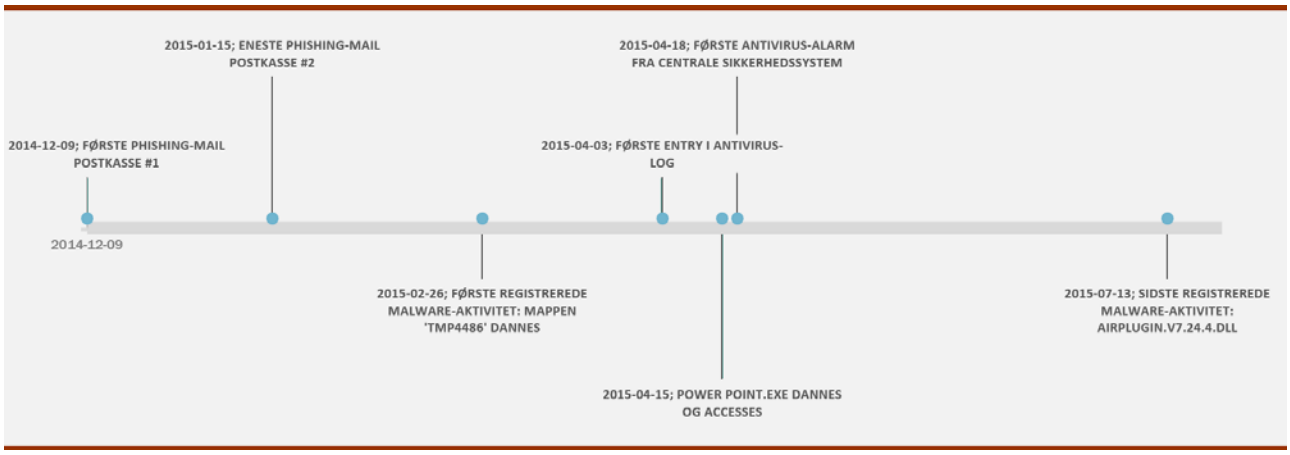
Dette kapitel beskriver hvad der er sket på den kompromitterede maskine hos UM. Der er derefter en beskrivelse af, hvordan malwaren blev stoppet i at kommunikere med sin C2 af UM's proxyserver og derved hindrede angriberne i at få adgang til maskinen eller data på den.

Analyse af den kompromitterede maskine

En analyse af harddisken fra den kompromitterede maskine viser, at den første phishing-mail ankommer i #1s postkasse den 9. december 2014. I perioden frem til den sidste ankomne phishing-mail 15. juni 2015 modtager #1 i alt 18 ondsindede mails. Derudover bliver nogle phishing-mails slettet undervejs af UM's centrale sikkerhedsløsning (mailscanner).

En enkelt phishing-mail er den 15. januar 2015 indgået til maskinen via en bruger, der har åbnet postkassen #2 på computeren.

Det tidligst registrerede tidspunkt for malware-aktivitet på maskinen (mappen 'tmp4486' dannes) er den 26. februar 2015, mere end to måneder efter den første phishing-mail. Blandt andet på grund af det store antal phishing-mails er det sandsynligt, at maskinen har været kompromitteret før dette tidspunkt. Den sidste malware-aktivitet registreres den 13. juli 2015, syv dage efter CFCS har konstateret, at der er ondsindet trafik i UM-sensoren.



Figur 5: Tidslinje med udgangspunkt i forensic-analyse af den kompromitterede maskine

Det er sandsynligt, at maskinen er blevet kompromitteret ad flere omgange, da der er fundet flere forskellige versioner af malwaren på maskinen. Dertil er der registreret flere tegn på, at malwaren er blevet slettet og geninstalleret. Forskellige log-filer fra maskinen indikerer, at malwaren har forårsaget ukendte fejl i systemet i perioden marts til april 2015. Det er derfor sandsynligt, at malwaren har kørt i denne periode. "Power point.exe" ses og køres første gang på systemet 15. april 2015, hvilket indikerer, at der er blevet klikket på en ondsindet vedhæftning igen på dette tidspunkt, og at systemet er blevet kompromitteret endnu engang.

I det omfang malwaren har forsøgt at kommunikere med sin C2, er trafikken blevet blokeret af UM's proxyserver. Proxyservere kan konfigureres til at skanne al indgående-, eller som i dette tilfælde, udgående netværkstrafik og filer. Fordelen ved en proxyserver er, at den fungerer som et

sidste forsvar mod udtrækning af følsomme data, hvis det lykkes angribere at undvige mailscannere samt lokale antivirusløsninger.

Kampagnen bredere set

Som nævnt i afsnittet 'Malware-installation og funktioner' anvender malwaren en keylogger, som indsamler information om, hvilke programmer brugeren anvender, indtastninger i søgefelter og kodeordsfelter samt emnefeltet i e-mails. Samlet set giver oplysningerne et sæt interessante oplysninger og muligheder. Stjålne kodeord kan anvendes til at kompromittere brugeren yderligere og til at få adgang til følsomme informationer. De kan også bruges til at afsende e-mails fra den kompromitterede bruger, som det er beskrevet i afsnittet 'Kompromitterede afsenderkonti'. Dette kan kombineres med information om brugerens emnefelter i e-mails til at skræddersy spear-phishing-mails til andre ofre (ofre, der f.eks. kan findes i kontoens adressekartotek), som den kompromitterede bruger måske allerede har haft korrespondance med. For offeret vil phishing-mailen komme fra en kendt person og omhandle et relevant emne og derfor ikke give anledning til mistanke. På denne måde kan én kompromittering skabe en sneboldseffekt og skabe fundament for yderligere inficeringer.

Informationen fra keyloggeren kan også anvendes til at danne et bredere indtryk af, hvem den kompromitterede bruger mailer med og om hvad, og på den måde afdække netværk og interesser. En fordel for angriberne ved denne type indhentning er, at det ikke afsløres, hvad der specifikt søges efter.

I forbindelse med analysen er det blevet klart, at en lang række organisationer og enkeltpersoner i lande både i og uden for EU har været involveret i angrebet og har modtaget de samme phishing-mails. Op til 68 postkasser i et enkelt land har været mål i samme bølge af phishing-mails.

Kompromitterede konti er anvendt til at sprede malwaren yderligere, hvilket indikerer at ét mål kan være et springbræt til et andet. UM har således ikke nødvendigvis været det primære fokus for angriberne.

Opsamling på sagen

Angriberne har afsendt et stort antal phishing-mails over en længere periode. Det betyder, at bagmændene er vedholdende og højt motiverede. Det lykkedes angriberne at kompromittere en enkelt maskine, men UM's sikkerhedsforanstaltninger forhindrede den installerede malware i at kommunikere med C2-serveren. Angriberne har derfor *ikke* haft adgang til maskinen, og der er ikke blevet kompromitteret data i forbindelse med angrebet.

Anbefalinger

På baggrund af den beskrevne hændelse har CFCS en række anbefalinger til, hvorledes organisationer har mulighed for at reducere risikoen for at blive udsat for et vellykket APT-angreb.

Angrebet mod UM viser, at indsatsen imod APT-angreb bør ske på både ledelsesniveau, på teknisk niveau og på brugerniveau.

Det er af afgørende betydning, at informationssikkerheden er forankret i ledelsen og at trusselbilledet er kendt, således at organisationen kan agere på den baggrund. Ledelsen skal ligeledes sikre, at organisationen har adgang til de nødvendige ressourcer, herunder kompetencer til at iværksætte de fornødne sikringstiltag.

På det tekniske niveau vurderer CFCS, at de fire generelle sikringstiltag, der er beskrevet i publikationen "*Cyberforsvar der virker*" fra 2013, forsat kan dæmme op for mere end 85 % af alle angreb. CFCS vurderer dog, at den aktuelle hændelse tydelig viser effektiviteten af at iværksætte tiltag på flere fronter og dermed implementere forsvar "i dybden". UM's løsning sikrede i den aktuelle sag, at en del af de indkomne phishing-mails blev opdaget og stoppet af UM's mailsscanner, men nogle slap igennem. Et udvalg af disse blev fanget af den lokale eller den centrale antivirusløsning og for så vidt angår de resterende stoppede UM's proxyserver malwaren i at kommunikere med sin C2. Samlet set var resultatet, at angriberne aldrig fik adgang til en kompromitteret maskine.

En forudsætning for at ovennævnte tiltag fungerer effektivt er, at organisationen løbende monitorerer de anvendte it-sikkerhedsløsninger, og at man reagerer på de kritiske hændelser på baggrund af indarbejdede retningslinjer for, hvorledes disse kritiske hændelser skal håndteres.

CFCS mener, at organisationen, med ovennævnte tiltag, vil være godt rustet i beskyttelsen imod APT-angreb, men den aktuelle hændelse illustrerer også vigtigheden af en høj og konstant sikkerhedsbevidsthed hos alle brugere i en organisation. En infektion kan, i den aktuelle situation, kun gennemføres ved, at malware i en phishing-mails blev aktiveret af en bruger. CFCS har i oktober 2015 udgivet sikkerhedsanbefalingen "*Spear-phishing – et voksende problem*". I denne publikation beskriver CFCS phishing grundigt, og hvad organisationerne kan gøre for at beskytte sig mod spear-phishing. Publikationen beskriver også, hvorledes brugeren kan opdage ondsindede mails, og hvad organisationen kan gøre for at begrænse skaden, hvis en bruger kommer til at åbne en vedhæftning eller trykke på et indlagt link.

Samlet set vil anbefalingerne derfor være:

- Forankring af informationssikkerhed i topledelsen
- Kendskab i topledelsen til det aktuelle trusselbillede
- Adgang til de nødvendige ressourcer
- Implementering af de fire tiltag fra "Cyberforsvar der virker"
- Forsvar i dybden
- Løbende monitorering
- Høj og konstant sikkerhedsbevidsthed i organisationen.

Undersøgelsesenheden

I december 2014 udkom den første nationale strategi for cyber- og informationssikkerhed. Forsvaret mod cybertrusler blev yderligere styrket i 2015 i forbindelse med regeringens styrkede indsats mod terror. Fælles for de to tiltag er målet med at forankre indsatsen mod cyberangreb i CFCS og gøre den mere effektiv. Et af initiativerne i de to tiltag var at etablere en særlig enhed, der med udgangspunkt i større cyberhændelser har til opgave at undersøge, hvad der hændte og hvorfor det eventuelt gik galt. På baggrund af disse udredninger udsender Undersøgelsesenheden 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:

"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. Derfor vil Center for Cybersikkerhed: Etablere en enhed til undersøgelse af større cybersikkerhedshændelser. Enheden består som udgangspunkt af medarbejdere fra Center for Cybersikkerhed. Andre myndigheder – fx Digitaliseringsstyrelsen og PET – inkluderes afhængig af hændelsen. Enheden etableres i 1. kvartal 2015."[1]

[1] National strategi for cyber- og informationsstrategi, Regeringen 2014, side 23

Bilag 1 – Hvad er et APT-angreb?

APT, eller Advanced Persistant Threat, er en betegnelse for en trussel eller et angreb, hvor angriberen forsøger at opnå uautoriseret adgang til en udvalgt virksomheds eller myndigheds net-værk med det formål i al ubemærkethed at opnå adgang til netværket gennem længere tid. Hensigten vil typisk være at spionere og udtrække data fra netværket. Ofte er det virksomheder inden-for udvikling og produktion af avanceret elektronik, telekommunikation og it-sikkerhed eller fravirksomheder i medicinal-, forsvars- og luftfartsindustrien, der er målene for denne type angreb, men også offentlige myndigheder er i farezonen.

Herunder beskrives en mulig fremgangsmåde ved et APT-angreb.

Modus – overordnet beskrivelse af de metoder, som hackerne benytter sig af

Et APT-angreb begynder med, at angriberne bag udfører en ofte omfattende rekognoscering og undersøgelse af det netværk, der skal kompromitteres. Det er i denne fase, at angriberne opnår en viden, som kan bruges til at tilpasse den malware, der skal bruges i angrebet. Det er også under rekognosceringsfasen, at angriberne gør sig begreb om, hvordan de bedst kan bruge social engineering. Efterfølgende forberedes og afsendes malwaren. Denne er ofte enten vedhæftet til en e-mail som en legitimt udseende fil eller indlagt i e-mailen som et link. Når offeret klikker på den vedhæftede fil eller linket i e-mailen, kan vedkommendes computer blive inficeret.

Figur 6: Fem trin i et APT-angreb

Når angriberne har fået etableret fodfæste i det kompromitterede netværk, bestræber de sig på, at deres aktiviteter ikke bliver bemærket. Et af kendetegnene ved APT-angreb er eksempelvis, at angriberne ofte forsøger at gemme sig i netværkstrafikken inden for normale kontortider. Endvidere gør angriberne brug af VPN-forbindelser, hvor de ved hjælp af legitime brugernavne og passwords får fjernadgang til et kompromitteret netværk.

CFCS er bekendt med, at angribere i en række tilfælde har skaffet sig adgang til samtlige passwords i den angrebne organisation via angreb på password-databasen i de kompromitterede netværk. Denne database downloades til servere, som angriberne kontrollerer. Her bliver de krypterede passwords brudt ved hjælp af såkaldte brute force-metoder eller opslag i tabeller over gængse passwords. Når angriberne har adgang til brugernavne og passwords, kan de bevæge sig forholdsvist ubemærket og tilsyneladende legitimt rundt på det kompromitterede netværk. Endeligt vil angriberne forsøge at fastholde deres adgang til det ønskede netværk. Dette betyder eksempelvis, at de vil forsøge at installere særligt malware, skjult dybt i systemet på den enkelte computer, som kan vækkes til live, hvis APT-gruppens oprindelige bagdør opdages og lukkes.