CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport

KingOfPhantom - bagdør til hovedmålet

Undersøgelsesenheden ved Center for Cybersikkerhed

Januar 2016

CENTER FOR CYBERSIKKERHED

Rapport om APT-angreb mod en dansk hostingvirksomhed og en af dens kunder

Indhold

Executive Summary

Denne rapport beskriver et såkaldt APT-angreb[1], som er blevet udført i 2014- 2015 mod en dansk it-hostingvirksomhed og en af virksomhedens kunder. Angrebet vurderes at være gennemført af en statsstøttet aktør med spionage for øje. Med udgangspunkt i de konkrete angreb viser rapporten, hvordan andre virksomheder og myndigheder kan sikre sig bedre mod tilsvarende angreb. Rapporten er udarbejdet af Undersøgelsesenheden[2] i Center for Cybersikkerhed (CFCS) med det formål at opsamle erfaringerne fra hændelsen og stille viden til rådighed for at modvirke fremtidige, tilsvarende hændelser.

Rapporten viser, at angriberne uset havde etableret solidt fodfæste i netværket hos såvel virksomheden som hos en af virksomhedens kunder i en længere periode. Det er ikke muligt at sige hvilke oplysninger, der er blevet kompromitteret eller stjålet fra virksomheden eller virksomhedens kunde, men detaljerede analyser af angrebets modus mv. viser, at angriberne havde mulighed for at navigere uset rundt på netværkene i mere end et år. I den periode kunne angriberne i princippet tilgå alle data i hostingvirksomheden og den berørte kunde.

Hostingvirksomheden blev bekendt med angrebet på baggrund af et tip fra CFCS og havde virksomheden ikke reageret på henvendelsen fra centret, kunne kompromitteringen være fortsat i længere tid.

Med samtykke fra virksomheden delte CFCS IP-adresser og domæner på den identificerede angrebsinfrastruktur med den øvrige del af Forsvarets Efterretningstjeneste. Dette betød, at Forsvarets Efterretningstjeneste identificerede en række udenlandske virksomheder, som var kompromitteret af samme aktør. Samarbejdspartnerne i de lande, hvor virksomhederne var placeret, blev kontaktet med henblik på eventuel videre aktion og udbedring.

For at imødegå tilsvarende angreb er anbefalingen blandt andet, at "top 4" fra publikationen "Cyberforsvar der virker" implementeres, og at der er etableret en sikkerhedsorganisation, som kan indsamle viden om truslerne og gennemføre systematiske analyser af netværkstrafik og brugermønstre samt af logfiler fra anti-virus programmer.

[1] Se bilag 1 for beskrivelse af APT-angreb

[2] Se side 12 for beskrivelse af Undersøgelsesenheden

Indledning
Forsvarets Efterretningstjeneste udgav i november 2015 en trusselsvurdering, der bl.a. konkluderer at: "Spionage mod offentlige myndigheder og virksomheder udgør fortsat den alvorligste cybertrussel mod Danmark og danske interesser. Spionagen udføres primært af statslige og statsstøttede grupper. Gennem de seneste år er omfanget af cyberspionage mod Danmark steget betydeligt, og gruppernes metoder og teknikker er blevet mere avancerede. Truslen fra cyberspionage mod danske myndigheder og virksomheder er meget høj. På langt sigt er det meget sandsynligt, at flere stater vil udnytte internettet offensivt".

"Eksempelvis var der i 2014-2015 en alvorlig it-sikkerhedshændelse, hvor en dansk virksomhed og dennes underleverandør var mål for cyberspionage gennem mere end et år. Den statsstøttede hackergruppe bag hændelsen havde fuld adgang til begge virksomheders netværk og kunne hente forretningshemmeligheder fra diverse computere og servere. Gruppen kunne også optage lyd fra de indbyggede mikrofoner i virksomhedernes computere samt tage skærmbilleder og registrere tastetryk. "[3].

Når CFCS bistår ved en hændelse som ovennævnte, er en vigtig del af arbejdet, at der afslutningsvis udarbejdes en teknisk udredning til den forurettede virksomhed eller kunde, der beskriver, hvilke datakilder der har været inficeret, hvilke typer infektion der har fundet sted herunder beskrivelse af malware, redegørelse for det tidsmæssige forløb og redegørelse for omfanget af og konsekvensen ved angrebet. På baggrund af den tekniske udredning kan CFCS' undersøgelsesenhed udarbejde en offentlig rapport, der kan belyse hvilke faktorer, der gjorde sig gældende ved angrebet og hvilke metoder, der kan anvendes til at imødegå lignende angreb.

Denne rapport gennemgår ovennævnte angreb.

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

Sagen: Et APT-angreb mod en privat it-hostingvirksomhed
I 2014-2015 var der en alvorlig it-sikkerhedshændelse, hvor en dansk virksomhed og en af virksomhedens kunder var mål for cyberspionage gennem mere end et år. Virksomhederne vidste ikke, de var kompromitterede, før de modtog henvendelsen fra CFCS. I den periode virksomhederne var kompromitterede, havde angriberne en lang række muligheder for at spionere og udtrække data fra virksomhederne.

Angrebet opdages
Primo juni 2015 modtog CFCS oplysninger fra en partner, som pegede i retning af et muligt, igangværende APT-angreb rettet mod en dansk it-leverandør af bl.a. hostede it-løsninger (herefter benævnt "*virksomheden*"), og derfor var angrebet også potentielt rettet mod virksomhedens kunder. CFCS kontakter virksomheden og udsender som en konsekvens heraf straks et udrykningshold til virksomheden.

[3] Efterretningsmæssig Risikovurdering, Forsvarets Efterretningstjeneste, november 2015

CFCS alarmeres

Når CFCS får kendskab til angreb, sker det primært på to måder. Enten via en alarm, der indløber fra en af de sensorer, som CFCS har placeret i de tilsluttede kunders infrastruktur, eller på anden vis som fx et tip. Når en alarm indløber via sensorerne, vil der ofte være tilstrækkeligt med data til at kunne vurdere angrebets karakter. Når analyserne viser, at der er tale om en såkaldt ægte positiv, dvs. når det er fastlagt, at et angreb er i gang, vil kunden blive kontaktet, og CFCS vil tilbyde at bistå med at imødegå angrebet. Når CFCS bliver opmærksom på et avanceret angreb på anden vis - som det der er nævnt i casen - kontaktes virksomheden med tilbud om at foretage nærmere analyser i virksomhedens infrastruktur.

I den konkrete sag var virksomheden ikke tilsluttet CFCS' netsikkerhedstjenestes sensornetværk. Når CFCS går ind i en sag, der ikke relaterer sig til netsikkerhedstjenestens kunder, kan det fx skyldes, at der er tale om et angreb på samfundsvigtig infrastruktur, eller at CFCS kan få ny viden om avancerede angreb, der styrker indsatsen mod angriberne.

Angrebet kortlægges

Virksomheden blev kontaktet og oplyste, at man ikke havde opdaget noget unormalt, men gerne ville have støtte af CFCS til nærmere analyser.

Støtten til virksomheden blev indledt med et møde med ledelsen i virksomheden, hvor den konkrete mistanke blev beskrevet. CFCS redegjorde for de planlagte analysemetoder og behov for adgange til netværk og systemer. Når virksomheden ikke er tilsluttet netsikkerhedstjenesten, er det nødvendigt med et skriftligt samtykke fra virksomheden om adgang til data, før CFCS kan bistå. Samtykket blev givet, og via netværksanalyse fandt analytikerne fra CFCS indikationer på, at der var malware på netværket. Analysen identificerede hurtigt trafik fra en af virksomhedens administrator-pc'er og en af virksomhedens servere mod en fjendtlig command and control server - C2. Memory dumps fra de to maskiner bekræftede, at der var malware på maskinerne. Malwaren blev identificeret som en særlig variant af PlugX.

Teknisk set er varianten hverken mere eller mindre avanceret end andre varianter, men netop denne type er kendetegnet ved kun at blive benyttet af en mindre gruppe hackere. Angrebet kunne på den baggrund identificeres som et statsstøttet cyberangreb.

Command and control server (C2-server eller C&C-server)

En command and control-server er en betegnelse for den server som hackeren anvender til at kontrollere det inficerede netværk. En C2-server kan fx anvendes til at installere ny malware eller flytte data ind og ud af netværket. C2-serveren kan være en server, der fysisk er placeret i det inficerede netværk, men vil ofte være placeret et andet sted. I den konkrete case var C2-serveren placeret uden for virksomhedernes netværk.

Om Plug X

PlugX-betegnelsen dækker over en familie af "remote access tools" (RAT's), der har været i brug af kendte APT-grupper og løbende er blevet udviklet siden 2008. Der findes flere varianter, der alle deler en række funktionaliteter på den inficerede host:

- Indsamling af information om kørende processer
- Indsamling af detaljerede systeminformationer
- Monitorering af netværksforbindelser og ressourcer
- Forbinde- og lave anmodninger til SQL databaser
- Starte og stoppe, loading og rekonfiguration af systemenheder
- Danne og slette filer
- Ændring af systemets registreringsdatabase
- Logning af brugeres tastning
- Kopiering af skærmbilleder

En angriber kan med værktøjerne - og hvis de rigtige forhold er til stede - (fx wake-on lan) blandt andet tænde og slukke maskiner, udføre administrative opgaver, oprette nye brugere, navigere rundt som legitim bruger og få adgang til og udtrække informationer på et inficeret netværk. PlugX-malwaren er designet specifikt til at minimere risikoen for detektion i dens operation og i dens kommunikation med C2-servere. For eksempel er nogle PlugX-rats konfigureret til ikke at lave udgående kommunikationsaktivitet i weekenden for ikke at generere mistænkelig netværkstrafik.

Andre RAT-familier kan have andre kendetegn.

Anvendelsen af RAT's er ikke unikt for APT-grupper, men anvendes bredt af forskellige hackere til forskellige formål.

Efter PlugX blev identificeret, blev det aftalt med virksomheden at igangsætte en række yderligere analyser for at få et bedre billede af inficeringens omfang. Det afgørende fund fra analyserne var konstateringen af, at inficeringerne stammede fra en jump-server, dvs. en server, der kontrollerer adgangene til de forskellige løsninger i det hostede miljø. Denne server var bl.a. inficeret med en keylogger, der indsamlede de brugernavne og passwords, der var anvendt på serveren. Med disse oplysninger har angriberne i princippet kunne navigere uset rundt på netværket inklusiv de dele af netværket, der huser firmaets forskellige kunder. Analyserne viste, at malwaren også var spredt til den del af firmaets infrastruktur, der hoster løsninger for kunderne.

På jump-serveren blev der endvidere fundet et værktøj, der gav angriberen mulighed for at udføre kommandoer på netværket. Sammen med adgangen til brugernavne og passwords gav denne funktion adgang til en række handlemuligheder som fx at oprette nye brugere, redigere i indstillinger som fx at deaktivere antivirus mv. eller udtrække data fra netværket. Der var derfor mistanke om, at angrebet kunne være væsentligt større end de første indikationer angav, så undersøgelserne blev udvidet til at undersøge alle servere i virksomheden. CFCS udviklede et script til at søge efter indikatorer på kompromittering, som blev leveret til virksomhedens teknikere, så de selv kunne undersøge de servere, som CFCS ikke havde kigget på. Resultatet af scriptet viste, at der var

indikationer på malware på flere servere, men at de inficerede servere var en del af den samme kundes hostede miljø. Der ikke var indikationer på, at andre kunder var berørte.

Hvad kunne være gjort for at forhindre den første kompromittering?

Forløbet af den første kompromittering kendes ikke, men CFCS vurderer med en vis sandsynlighed, at angrebet var nøje planlagt, og at spearphishing derfor var en del af angrebet. Om infektionen spredte sig fra en vedhæftet fil i en mail, et link fra internettet eller evt. via et fysisk medie vides ikke. Men flere af de forholdsregler, der er nævnt sidst i denne rapport, kunne have vanskeliggjort eller forhindret kompromittering. Eksempler kunne være:

- Awareness hos medarbejderne ville muligvis have betydet, at man ikke havde åbnet et givent link eller vedhæftning.
- Begrænsede administrative rettigheder og/eller styring af pc'ens trafik kunne muligvis have begrænset skaden til den første pc, der blev angrebet.
- Minimering af aktive services på pc'en ville gøre det sværere for angriberen at kommunikere med resten af netværket og nemmere for virksomheden eller en ekstern sikkerhedskonsulent at opdage unormal trafik.
- Regelmæssige netværks- og trafikanalyser kunne muligvis have opdaget kompromitteringen tidligere.
- Whitelisting af software kunne forhindre, at uønsket software kunne installeres.

Da der var konstateret malware i hostingmiljøet tilhørende en kunde hos virksomheden, var det sandsynligt, at malwaren havde spredt sig til kundens (herefter benævnt "kunden") eget it-miljø. CFCS tilbød derfor at bistå kunden på dennes egen adresse. Efter kunden havde givet skriftligt samtykke om dataadgang til CFCS, blev der som forventet fundet malware på flere maskiner hos kunden. Deriblandt på en Domain Controller og på en lokal administrator-pc. Kunden, der ikke havde set tegn på angrebet før de fik henvendelsen fra CFCS, rekvirerede ekstern assistance fra moderselskabet. I et samarbejde mellem CFCS, virksomheden og dennes teknikere, kunden og teknikerne fra kundens moderselskab blev der identificeret flere inficerede servere hos kunden. CFCS kunne fastslå, at alle servere var inficerede med samme malware fra den identificerede PlugX-familie.

Efter malwaren var identificeret og kategoriseret, begyndte arbejdet med at rense og reetablere infrastrukturen hos de to firmaer. Denne proces skete i samarbejde mellem de respektive firmaers sikkerhedsrådgivere og egne teknikere med råd fra CFCS' analytikere.

Hvad kunne være gjort i forhold til at mindske eller forhindre spredningen af malware?

Efter angriberne havde placeret malware på administrator-pc'en med et af de førnævnte PlugX-værktøjer og derved fik afluret loginoplysninger for den bruger-konto, gav det reelt angriberne ubegrænset adgang til virksomhedens øvrige net-værk. Det var derfor nemt for angriberne at fortsætte med opbygning af en infra-struktur de selv kunne kontrollere med henblik på uset at kunne spionere og herunder udtrække data. CFCS vurderer, at følgende initiativer kunne have minime-ret spredningen af malware:

- Særlige, dedikerede brugerkonti til administrative formål ville have gjort det langt sværere at komme videre på netværket.
- 2-faktor-login til administrative konti. Dette giver mere end dobbelt arbejde for hackeren, og angriberen ville muligvis have stoppet her.
- Segmenterede netværk. Hvis netværkene var opdelt i forskellige sikkerhedszoner med separate passwords, ville arbejdet være langt mere krævende og muligvis have stoppet angrebet.

Samlet set ville disse tiltag gøre arbejdet langt mere besværligt og langt mere tidskrævende for angriberen. Hvis disse tiltag implementeres sammen med øget kontrol af logs og netværkstrafik, vil det give virksomheder og myndigheder gode forudsætninger for at opdage og stoppe tilsvarende angreb.

Yderligere tiltag, der kunne have begrænset angribernes færden, kunne være:
AD-låsning så det ikke var muligt at ændre i ad'et uden særlig autorisation.
Kryptering af særligt sensitive filer ville gøre disse data ubrugelige eller i hvert fald vanskeligere at anvende for angriberen.

Grafisk illustration af angrebet

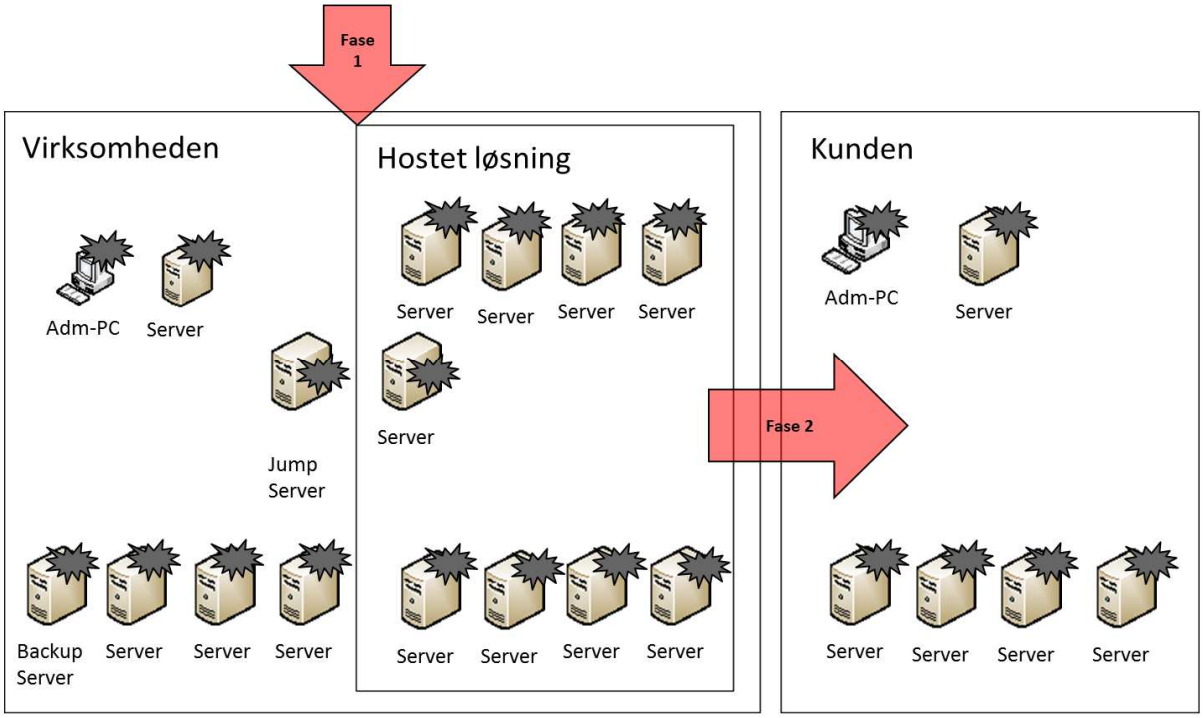


Illustration 1 – angrebets udbredelse

Illustrationen viser angribernes vej ind i begge firmaer. Som tidligere nævnt kender CFCS ikke til, hvordan angriberne er kommet ind i virksomheden, men tegningen viser, at de via "jump-serveren" kunne navigere rundt og installere malware på en række servere og pc'er.

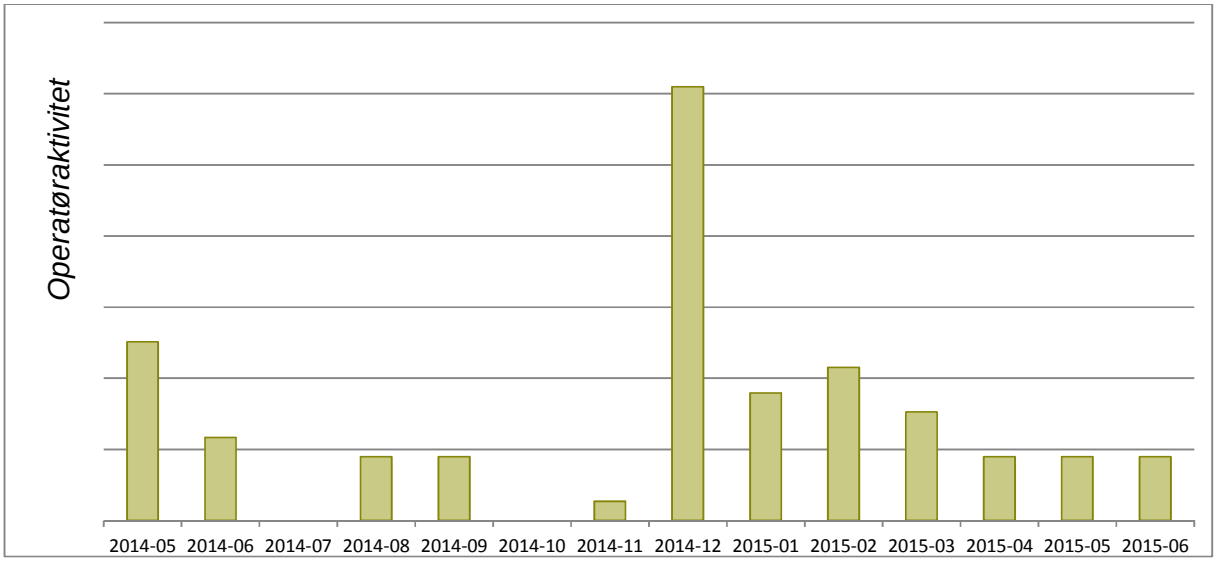


Illustration 2 - fordeling af angrebets operatøraktivitet over tid

Illustrationen viser den relative fordeling af den operatøraktivitet, der har styret angrebet. Operatøren er den eller de hackere, der teknisk har styret angrebet. Det er forholdsvis tydeligt, at an-

grebet centrerer sig omkring maj 2014, hvor de fik den første adgang, og så omkring årsskiftet 2014/15, hvor de fik adgang til kundens data og infrastruktur. Det er normalt, at angreb foregår i bølger. Er der perioder uden aktivitet (som fx i juli eller oktober 2014), er det ikke et udtryk for, at angrebet er stoppet. Der kan være forskellige årsager til pauserne. Fx at angriberne afventer, om de er opdaget, at de samler data fx via en key-logger eller noget helt tredje.

Analyse

Den tekniske analyse i den konkrete sag viste dels, at malwaren var spredt til en stor del af virksomhedens infrastruktur, og dels at malwaren var spredt fra virksomhedens infrastruktur til en af dens kunders infrastruktur. Det stod også hurtigt klart, at den malware, der var fundet på de forskellige maskiner, kunne henføres til den såkaldte PlugX-familie, hvilket igen indikerede, at der var tale om et APT-angreb. Endvidere viste analysen, at infektionen med malwaren var sket mere end et år tidligere, hvorfor hackerne teoretisk har haft adgang til data i samme tidsrum.

Analyser af de logs mv., der var til rådighed, gav ikke mulighed for at identificere indholdet af de data, som angriberen har været i kontakt med og evt. har ekstraheret. Et ofte tilbagevendende problem er, at it-afdelingerne sletter logs efter relativt kort tid. Nogle gange efter blot en uge, nogle gange efter en måned. Det er de færreste, der gemmer logs i flere år. Havde de relevante historiske logs været til rådighed, vurderer CFCS, at det ville have været muligt at identificere indholdet af de data, som angriberne havde været i kontakt med.

Analyserne viste ikke, hvordan angrebet startede, eller hvordan malwaren kom ind i virksomheden, men CFCS antager, at det sandsynligvis var en spear-fishing mail med en inficeret vedhæftning eller et inficeret link, der gav hackerne adgang. Også her ville historiske logs have givet et mere detaljeret billede.

CFCS' tekniske analysetilgange

CFCS har 3 tekniske tilgange til den slags udredninger:

1. **Netværksanalyse**, er en type analyse, der primært fokuserer på logs fra firewalls mv. og kortlægger den kommunikation, der har været mellem de ramte maskiner og øvrige adresser.
2. **Forensic analyse**, er en type analyse, der har fokus på, hvordan malwaren har fungeret og evt. spredt sig på den enkelte maskine
3. **Malware-analyse**, er en type analyse, der kigger på de enkelte typer malware og beskriver særlige kendetegn mv.

Hvad var konsekvensen af angrebet?

Hvis en virksomheds eller en offentlig myndigheds data kompromitteres eller stjæles, har det som regel alvorlige konsekvenser. For den private virksomhed kan konsekvenserne eksempelvis være tab af markedsandele, produktionstab, videnstab, dårlig branding mv. For den offentlige myndighed kan angrebet yderligere føre til tab af tillid.

I den konkrete sag er det svært at sige, hvad konsekvensen præcist var, da analyser af logs mv. ikke gav mulighed for at identificere indholdet af de data, som angriberen har været i kontakt med og evt. har ekstraheret. Men da både virksomheden og dens kunde via it-systemerne antageligvis ligger inde med en række forretningskritiske oplysninger, er det CFCS' vurdering, at der er sket en vis skade for virksomheden og kunden.

Virksomheden har oplyst, at de har brugt over 3 mio. kr. i direkte omkostninger på bl.a. re-konfiguration af deres netværk og rensning og analyse af deres maskiner mv. Kunden har ikke opgjort de økonomiske omkostninger, men det er CFCS' vurdering, at de også har haft store omkostninger. Såvel hos virksomhed og kunde er endvidere brugt mange – og dyre - arbejdstimer – også uden for alm. arbejdstid – hos interne og eksterne ressourcer.

Særlige forhold ved angrebet og efterfølgende skadesbegrænsning

Det er som tidligere nævnt CFCS' vurdering, at det pågældende angreb var et dygtigt udført APT-angreb. Anvendelsen af PlugX-rats kombineret med angrebets modus er et klassisk eksempel på udførelsen af denne type angreb. Det kan muligvis undre, at angriberne - som via adgangen til helt centrale elementer i virksomhedens infrastruktur har haft muligheden for at sprede sig til andre af virksomhedens kunder - ikke benyttede sig af denne mulighed. Analyserne viser, at angriberne gik målrettet efter den ene kunde. CFCS tolker dette på to måder: Enten at angriberne ikke var opmærksomme på yderligere kompromitteringsmuligheder, eller også havde angriberne kun denne kunde som mål for angrebet.

Bortset fra denne iagttagelse er det ikke CFCS' antagelse, at angrebet fraveg de gængse standarder for PlugX-baserede APT-angreb.

En væsentlig forudsætning for, at det lykkedes at rydde op i malwaren og få reetableret virksomhedens og kundens infrastruktur, var samarbejdet mellem virksomhed, kunde og CFCS omkring adgang til relevante data. Dette muliggjorde en hurtig afdækning af angrebets kompleksitet og omfang herunder FE's erkendelse af, at samme aktør ligeledes havde kompromitteret flere udenlandske virksomheder.

Anbefalinger

Der findes mange muligheder for at reducere risikoen for at blive udsat for et vellykket APT-angreb. De fire mest gængse tiltag, der i øvrigt vurderes at kunne dæmme op for mere end 85 % af alle angreb, er beskrevet i publikationen "Cyberforsvar der virker" fra 2013. Publikationen blev udgivet som et fælles tiltag af CFCS og Digitaliseringsstyrelsen. Disse tiltag bør gennemføres under alle omstændigheder.

Med udgangspunkt i den konkrete sag falder anbefalingerne i to dele: organisatoriske og tekniske anbefalinger. Det bemærkes, at der ikke er tale om en udtømmende liste af mulige tiltag, men at der er fokuseret på de tre vigtigste tiltag i ovenstående kategorier. Alle tiltag, som kan anvendes til at imødegå APT-angreb, øger den generelle cybersikkerhed i virksomheden. Ingen tiltag kan dog

forhindre et APT-angreb fra en målrettet, statsstøttet aktør, men omkostningen ved at gennemføre og vedligeholde angrebet kan øges i en sådan grad, at angriberen søger mod svagere beskyttede mål. Derfor nytter det at styrke den generelle robusthed i organisationen.

I forhold til den konkrete sag er observationen, at cybersikkerhed blev set som en del af it-driften, og selvom såvel kunde som virksomhed har dygtige og kompetente medarbejdere, er erfaringen fra sagen, at cybersikkerheden kan styrkes ved at forbedre de eksisterende sikkerhedsprocesser og dedikere ressourcer til sikkerhedsarbejdet.

Top tre organisatoriske tiltag:

- **Indhent viden om trusler og sikkerhed**
  Hav en del af organisationen, som løbende indhenter viden om trusler og sikkerhedstiltag og formidler disse til topledelsen, og organiser sikkerhedsarbejdet efter veldefinerede processer ligesom it-driftens ITIL-processer.
- **Foretag analyser af logs**
  Hav en del af organisationen, der har tid til og mulighed for at analysere logs fra firewalls, antivirus og lignende systemer med henblik på at opdage tegn på angreb.
- **Etabler en sikkerhedskultur og styrk opmærksomheden**
  Øg medarbejderopmærksomheden omkring trusselsbillede, og styrk sikkerhedskulturen på arbejdspladsen generelt, så mistænkelige mails eller underlig aktivitet på pc'en registreres og rapporteres til en sikkerhedsorganisation.

Den konkrete sag viste, at adgangen til administrative funktioner kun var beskyttet af et password. Det gjorde det enkelt for angriberne at optræde som administrator. Da netværkene ikke var segmenterede, var det derfor let for angriberne med en enkelt administratoradgang at bevæge sig rundt i netværket og sprede malwaren. Endeligt anvendte angriberne servere til at kommunikere med internettjenester, som serverne ikke havde behov for adgang til. Dette lettede angribernes mulighed for at etablere C2-infrastrukturen.

Top tre tekniske tiltag:

- **Separate konti til administrative formål og anvendelse af 2-faktor login**
  Det anbefales, at de systemadministrative brugere skal anvende separate konti til e-mail og websurfing, og det anbefales også, at der anvendes 2-faktor-login til de centrale systemer.
- **Segmenter netværket**
  Netværket bør opdeles i forskellige sikkerhedszoner. Dette gør det langt sværere for hackeren at navigere rundt og flytte data.
- **Bloker for servereadgang til internettet**
  Der bør blokeres for serveradgang til internettet. Kun deciderede web- og mailservere skal kunne tilgå internettet. Disse skal til gengæld være omgivet med fornøden sikkerhed.

I tilfælde af angreb

Ved mistanke om at et netværk er inficeret med PlugX eller anden APT-lignende malware, skal man tage sig tid til at danne overblik over situationen og undgå at foretage handlinger, der kan have karakter af "panik-handlinger". Det er en god ide at entrere med eksterne analysefirmaer i denne fase og eventuelt kontakte politiet og/eller CFCS. Det kan være svært ikke at foretage sig noget i en sådan krisesituation, men det er vigtigt at huske på, at angriberne måske har været til stede i flere måneder, så et par dage fra eller til gør næppe skaden værre. CFCS' anbefaling er at undlade at foretage mitigerende handlinger på netværket, før der er lagt en plan for håndteringen, evt. i samarbejde med CFCS. Informationer af efterforskningsmæssig eller analysemæssig relevans kan gå tabt og derved gøre den efterfølgende skadesbegrænsning og genoprettelse vanskeligere.

Ligeså vigtigt er det, at man har en overordnet beredskabsplan, som indeholder en disaster-recovery plan, der kan anvendes ved cyberangreb. Det siger sig selv, at denne plan skal testes løbende. Det kan også ske ved såkaldte "skrivebords-øvelser". Planen bør forholde sig til de forskellige typer angreb, som man vurderer, man kan blive ramt af, men også til intern og ekstern kommunikation, herunder til myndigheder og presse. Der er fx forskel på, hvordan man håndterer DDoS-angreb, ransomware angreb eller APT-angreb, og dette bør afspejles i disaster-recovery planen.

Undersøgelsesenheden

Den tidligere regering udgav i december 2014 den første nationale strategi for cyber- og informationssikkerhed, og beskyttelsen mod cybertrusler er også et element i den terrorpakke, der blev vedtaget af Folketinget i foråret 2015. Fælles for de to tiltag er, at det er besluttet at forankre og styrke indsatsen mod cybertrusler i CFCS. Et af initiativerne er at etablere en undersøgelsesenhed, der med udgangspunkt i konkrete større cyberhændelser undersøger, hvad der gik galt – og hvorfor. På baggrund af undersøgelserne er det CFCS's hensigt at udsende relevant information og vejledning, så myndigheder og virksomheder kan drage nytte af erfaringerne 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."[4]

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

Henvisninger

Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift 2014 (CSC-sagens 3. rapport)

Cyberforsvar der virker, 2013

Den nationale strategi for Cyber og Informationssikkerhed, 2014

Trusselsvurderingen om APT-angreb, FE, 2014

Efterretningsmæssig Risikovurdering, Forsvarets Efterretningstjeneste, 2015

Bilag 1 - Hvad er et APT-angreb?

Som nævnt ovenfor vurderer CFCS, at angrebet mod de to virksomheder var et såkaldt 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 netværk 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 indenfor udvikling og produktion af avanceret elektronik, telekommunikation og it-sikkerhed eller fra virksomheder 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 1: Grafisk fremstilling af 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.

Brute force

Brute force er en metode, som hackere kan bruge til at dekryptere en datanøgle, eksempelvis et password tilhørende et brugernavn. Selve metoden består i, at hackerne ved hjælp af særlige programmer eller særlig hardware forsøger at gætte sig frem til det rigtige kodeord.

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.

Phishing og spear-phishing

Inden for it-sikkerhed betyder begrebet phishing, at en angriber forsøger at skaffe sig information om et offer, såsom brugernavn, kodeord eller kreditkortoplysninger, ved at udgive sig for at være en legitim modtager af disse oplysninger. Phishing foregår oftest ved, at offeret modtager en e-mail og gennem social engineering manipuleres til selv at indtaste disse oplysninger. Ved spear-phishing anvendes samme fremgangsmåde, men her er offeret særligt udpeget og angrebet derfor målrettet.

Social engineering

Social engineering er en angrebsteknik, hvor offeret manipuleres til at udføre bestemte handlinger eller til at videregive klassificeret information uden selv at være klar over det. I forbindelse med it-sikkerhed bruges termen til at beskrive eksempelvis e-mails eller hjemmesider, der på overfladen ser legitime ud, men som i virkeligheden rummer malware. Social engineering kræver et vist kendskab til offeret for at være effektivt.

Bilag 2 - Malware analyse rapport

Malware analysis

Contents

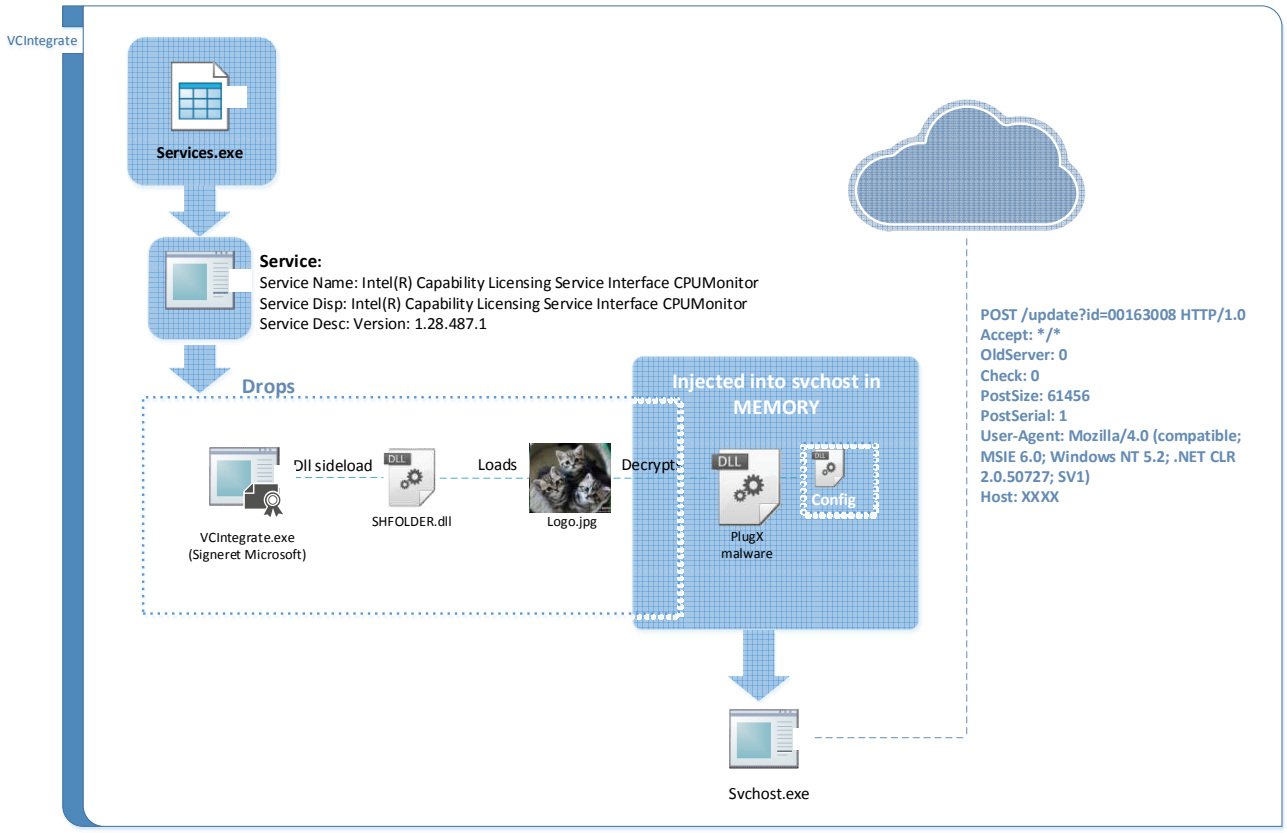
Rules

Yara Rules

```
rule known_plugx_loader
{
        meta:
                SHFOLDER_dll_md5 = "766f7fe95e9dfeee03561255f49f2a84"
                WINMM_dll_md5 = "6f101db7b074e0303d6a1e877b9ab3dc"
                mpsvc_dll_md5 = "9496d5b1a26527ef302564b37d8ffa03"
                WTSAPI32_dll_md5 = "be59ff05b96b7bb251dd77932b71bbc1"
        strings:
                $a1 = {E8 ?? 0? 00 00 83 C4 0C 8B 45 ?? FF D0 6A FF FF 15 ?? ?? 00 10}
// memcpy, call eax, sleep

        condition:
                all of them
}
```

```
rule plugx_jpg_mal_image
{
strings:
                $a1 = {ff d8}
                $a2 = {ff d9 e8 3e 33 03 00 da}

        condition:
                $a1 at 0 and $a2
}
```

Overview



Installation

On execution the following files are then dropped into the Install Dir: "%ALLUSERSPROFILE%\ Intel(R) Capability Licensing Service Interface CPUMonitor" directory

File Name	VCIntegrate.EXE
File Size	42720 bytes
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	64787351f8dd15fa642b37d2e3d023c8
SHA1	62406876a635d5c6f5fa9376fc67a5c2e4af9ed2
SHA256	84cce1726ebd16f31bbf2d8209e76d54c49404686b8b8c5c094650c5b9fb4bf0

File Name	SHFOLDER.dll
File Size	4096 bytes
File Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	766f7fe95e9dfeee03561255f49f2a84
SHA1	73310ceea38ab3195dc782dbf0b11b61249fb10b
SHA256	65f55f680e9390c6f9b9cb3da95fa7c0e55276288812ecc4ad8e5c06bc8412fc

File Name	Logo.jpg
File Size	251206 bytes
File Type	JPEG image data, JFIF standard 1.01
MD5	d571bd6cdbcead9b1ea1b3312db4e149
SHA1	cf479054a1ed0c2345f45096ce33be01e1b29859
SHA256	b3e6b575bbb6ace1ac5c5ee63457a25f5a6130bfe3a2ed85e40666cc1bc20608

Filename:	Trend2013.dat
File Type:	data

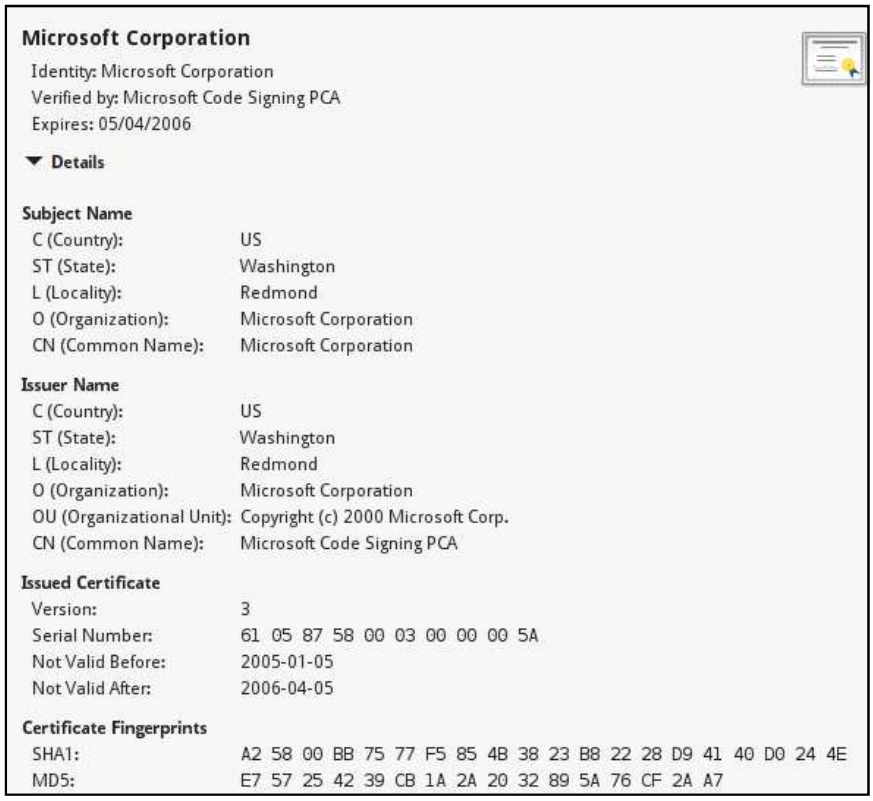
Filename:	Boot.cfg
File Type:	data
Comment:	Extra encrypted configuration file

1. File description

1.1 VCIntegrate.EXE

A benign file with an outdated but valid digital signature signed from “Microsoft Corporation” and is a common Windows file which is responsible for loading and processing the settings of related application or Windows function.

The file has a dll side-loading vulnerability that loads the malicious SHFOLDER.dll



Microsoft Corporation

Identity: Microsoft Corporation
Verified by: Microsoft Code Signing PCA
Expires: 05/04/2006

▼ Details

Subject Name

C (Country):	US
ST (State):	Washington
L (Locality):	Redmond
O (Organization):	Microsoft Corporation
CN (Common Name):	Microsoft Corporation

Issuer Name

C (Country):	US
ST (State):	Washington
L (Locality):	Redmond
O (Organization):	Microsoft Corporation
OU (Organizational Unit):	Copyright (c) 2000 Microsoft Corp.
CN (Common Name):	Microsoft Code Signing PCA

Issued Certificate

Version:	3
Serial Number:	61 05 87 58 00 03 00 00 00 5A
Not Valid Before:	2005-01-05
Not Valid After:	2006-04-05

Certificate Fingerprints

SHA1:	A2 58 00 BB 75 77 F5 85 4B 38 23 B8 22 28 D9 41 40 D0 24 4E
MD5:	E7 57 25 42 39 CB 1A 2A 20 32 89 5A 76 CF 2A A7

1.2 SHFOLDER.dll

An auxiliary dll, which has fake exports which are required by VCIntegrate.EXE is malicious and will be side-loaded by VCIntegrate.EXE.

It reads the file “Logo.jpg” into memory and starts execution after 41422 bytes of the jpeg file.

1.3 Logo.jpg

Actually a valid jpeg file that can be viewed and contains the picture below, but it contains code at an offset of 41422 bytes.
SHFOLDER.dll reads the file into memory and jumps into the jpeg data.
At that offset the code for a decryption algorithm starts to unpack the the main PlugX implant.

1.4 Trend2013.dat

The Trend2013.dat file is a log for keylogging, and the active windows.
Example log file

```
2015-02-02 16:24:00 |  | Command Prompt
ipconfig &all
2015-02-02 16:25:10 |  | Command Prompt
ipconfig /all
2015-02-02 16:26:10 |  | Run
services.msc
```

1.5 Boot.cfg

Boot.cfg is an encrypted configuration file that can update file location, C&C domains/IP, ports, timetables, service names etc.
Plugx tries to read the file boot.cfg on execution, and if found it will decrypt it and update itself.
If the file is not found it will use the default configuration it was configured with.
Boot.cfg can be decrypted with the python method seen below.
The encryption key is the first 4 bytes of the file.

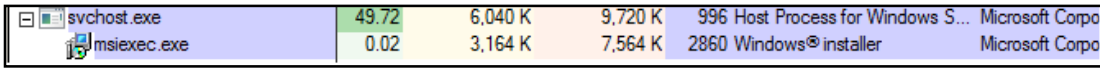
Python decryption

```
def getkey(data):
   return unpack('<I',data[:4])[0]

def decrypt(data,key):
                v1=v2=v3=v4=key
                i=0
                out=""
                while i<len(data):
                                v1 = (v1 + (v1 >> 3) - 0x11111111)&0xffffffff;
                                v2 = (v2 + (v2 >> 5) - 0x22222222)&0xffffffff;
                                v3 = (v3 + 0x33333333 - (v3 << 7))&0xffffffff;
                                v4 = (v4 + 0x44444444 - (v4 << 9))&0xffffffff;
                                mysum=(v1+v2+v3+v4)&0xff
                                out=out+chr(ord(data[i])^mysum)

                                i=i+1

                return out
```

2 PlugX version information

There are multiple ways of trying to describe the version of plugx.
Below are som indications of which version this sample is

Version Indicators

1	This version of PlugX is what some call a “Type 1” sample. Based on the injection into svchost and then msiexec we can draw reference to the following opensource information: https://www.blackhat.com/docs/asia-14/materials/Haruyama/Asia-14-Haruyama-I-Know-You-Want-Me-Unplugging-PlugX.pdf 
2	The string: “KingOfPhantom0308_20140826” is found in this version of PlugX
3	d:\fast\20140927 shellcode dbg\shellcode\XPlug.h
4	Config size: 170c bytes

3 Command set

PlugX has modular plugins which, rather than having their own routines for tasks such as external communication, use functionality provided by PlugX internal APIs. This design choice allows plugins or APIs to be updated independently and in a backward-compatible way, without interrupting the execution of the malware or requiring it to be reinstalled.
Below is the commandlist and RAT functionality:

Command	Description
Disk	Create, read, delete files, change env strings, create/write new files from C&C to disk, run .exe/tools
KeyLog	keylogger
bootProc	Initialize variables and inject shellcode into svchost.exe process
Shell, ShellT1, ShellT2	Create a new cmd.exe process; communicate with it via named pipes; relay input from/output to the C&C connection
Telnet	Create new cmd.exe process with /Q option, turning off echo; communicate with process via sockets; relay input from/output to the C&C connection
Screen, ScreenT1, ScreenT2	Take screenshots
Process	Create, kill, enum processes
Service	Create, change, enum, start, delete services
Nethood	Enumerate computers and shared resources in the local network
Netstat	Collect some network usage statistics
Option	Reboot, logoff, shutdown the system
PortMap	Perform port map
RegEdit	Create, change, enum, delete registry keys
LdrLoadShellcode	Shellcode to unpack and install main code in an injected process
SiProc	Create elevated process and inject code
OlProc OlProcManager OlProcNotify	Injects into services.exe

4 Functions and Plugins

The following references where found to source code functions

XPlugProcess.cpp
XPlug.cpp
XPlugSQL.cpp
XPlugNetstat.cpp
XPlugShell.cpp
XPlugNethood.cpp
XPlugKeyLogger.cpp
XPlugTelnet.cpp
XPlugRegedit.cpp
XPlugPortMap.cpp
XPlugDisk.cpp
XPlugService.cpp
XPlugScreen.cpp
XPlugOption.cpp

5 Persistence

In this sample persistence is maintained by creating a service that points to VCIntegrate.EXE
The service has the following parameters

Service Name	Intel(R) Capability Licensing Service Interface CPUMonitor
Service Disp	Intel(R) Capability Licensing Service Interface CPUMonitor
Service Description	Version: 1.28.487.1

Besides a service, it can also be set to add an autorun entry in the registry.

Command and Control

After the malware has established persistence on a system (copied files and creates itself as service, or added an autorun entry in registry), it tries to establish a network connection with the C&C.

It can communicate with a server using TCP, UDP, or HTTP protocols. It sends broadcast UDP packets to devices on the same subnet as the victim, and listens for a broadcast response, in an attempt to establish connections with other bots in the same local network.

When running HTTP this example uses the custom headers OldServer, Check, PostSize and PostSerial which can be seen below.

Headers	POST /update?id=00163008 HTTP/1.0 Accept: */* OldServer: 0 Check: 0 PostSize: 61456 PostSerial: 1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2; SV1) Host: {host} Content-Length: 0 Pragma: no-cache

It also has the possibility to download its C2 information from another site if wanted.
examples

1. http://dl.dropboxusercontent.com/s/eg3qusm8pl4iz49/index.txt
2. http://TIEBA.BAIDU.COM/F?KZ=866965377

Here it will download data from the above URL's and decode a string between "DZKS" and "DZJS" which will be its command and control servers.

Assessment

A version of the well documented PlugX RAT.

OSINT references

- http://labs.lastline.com/an-analysis-of-plugx
- https://www.blackhat.com/docs/asia-14/materials/Haruyama/Asia-14-Haruyama-I-Know-You-Want-Me-Unplugging-PlugX.pdf
- http://blog.cassidiancybersecurity.com/post/2014/01/plugx-some-uncovered-points.html