CENTER FOR CYBERSIKKERHED

MALWAREANALYSE:

CFCS-Sinkhole sladrer om Sodinokibi ransomware

Der er en vedvarende trussel fra målrettede angreb, hvor et firmas filer krypteres og hvor virksomheder afpresses til at betale løsesum for at få dekrypteret deres egne filer. Såkaldt Big Game Hunting er en stigende tendens blandt hackere. Her går de målrettet efter at kompromittere større virksomheder og organisationer, hvor der kan være en stor økonomisk gevinst ved at ramme dem med ransomware-angreb. Det kræver en betydelig indsats og brug af tekniske resurser at ramme sådanne mål, men gevinsten for et vellykket ransomware-angreb af denne kaliber kan opveje den nødvendige og tidskrævende indsats.

Netop fordi det kræver teknisk indsigt og et stort tidsforbrug at planlægge, tilrettelægge og udføre sådanne angreb, bliver de udført af resursestærke organiserede kriminelle. Kriminelle organisationer, har gennem en årrække tilegnet sig de nødvendige færdigheder, midler og alliancer til både at udvikle sofistikeret malware samt udføre angreb med stor økonomisk gevinst for øje.

Det betyder, at danske firmaer kan lide store økonomiske tab, hvis de udpeges som mål af hacker-grupperne. Danske virksomheder bør derfor tage denne trussel alvorligt og sikre deres netværk efter bedste praksis.

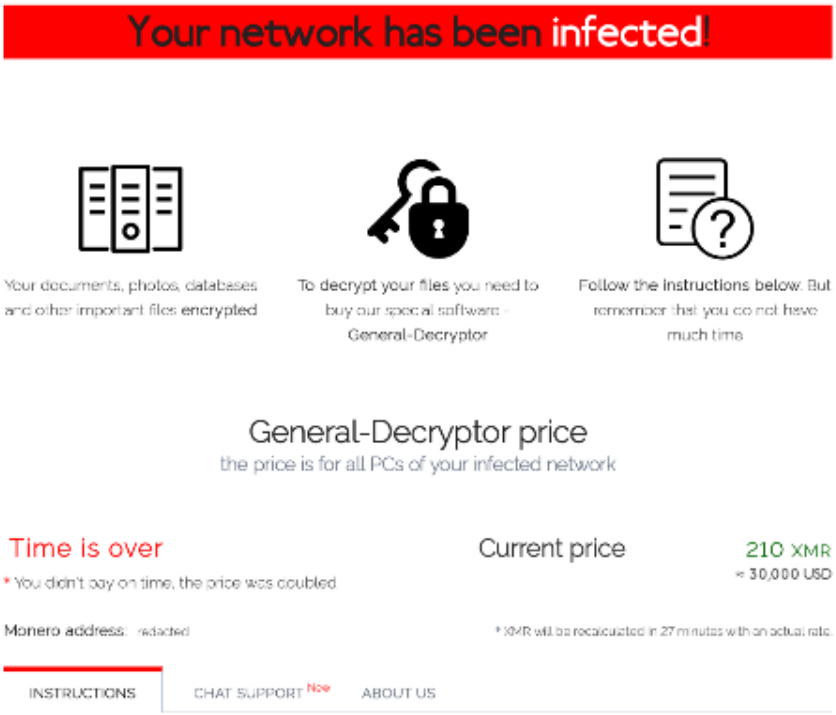
LÆSEVEJLEDNING

Målgruppen for denne artikel er primært it-teknikere, som ønsker en dybere teknisk forståelse for ransomware. Artiklen tager udgangspunkt i en velkendt ransomware-familie, Sodinokibi, som Center for Cybersikkerhed (CFCS) har analyseret samt tilvejebragt statistisk information om. Artiklen supplerer derved tidligere publikationer udgivet af CFCS vedrørende ransomware.

For en bredere forståelse af ransomware anbefales det særligt at læse to øvrige publikationer fra CFCS: "Anatomien af målrettede ransomware-angreb" og "Reducér risikoen for ransomware". De giver indblik i, hvordan ondsindede aktører opbygger deres angreb, og hvordan man forvarer sig mod disse. Publikationerne kan læses uafhængigt af hinanden og i vilkårlig rækkefølge.

Sammenfatning

De kriminelle bagmænd bag Sodinokibi-malwaren udviser både evne og vilje til at skjule deres aktiviteter og har således god operationssikkerhed. De besidder endvidere solid forståelse for korrekt implementering af krypteringsalgoritmer. Det er derfor ikke er muligt for offeret at dekryptere deres filer uden først at have betalt løsepengene.



"All your base are belong to us"

Sodinokibi

Denne artikel omhandler ransomware-familien Sodinokibi også kendt under navnet REvil. Sodinokibi-malwaren er ransomware specifikt målrettet Windows-computere. De kriminelle bagmænd bag Sodinokibi har været banebrydende på ransomware-markedet siden 2018. De har været med til at starte konceptet RaaS (Ransomware as a Service) ved at stille deres platform til rådighed for et netværk af udvalgte samarbejdspartnere. Størrelsen af netværket gør, at der kan rammes langt flere mål, end hvis de kriminelle opererede som små adskilte individuelle grupper, der hver især måtte varetage alle aspekter af en kriminel forretning med store tekniske udfordringer. Det vurderes, at det samlede netværk har en årlig omsætning på flere hundrede millioner danske kroner.[1]

De enkelte kriminelle samarbejdspartnere i netværket er selvstyrende og opererer almindeligvis uafhængigt af hinanden. De kvalificerer sig ved at have den fornødne viden om, hvordan man kompromitterer virksomheders it-infrastruktur og besidder stor operationel forsigtighed. Sodinokibi-bagmændene stiller til gengæld en sofistikeret ransomware-platform til rådighed, som samarbejdspartnerne kan bruge, når de skal inficere et offer med ransomware. Ved at undersøge individuelle udgaver af Sodinokibi-malwaren anser vi det for meget sandsynligt, at der i starten af 2020 var mindst 32 unikke samarbejdspartnere, hvilket stemmer overens med åbne kilder. [2]

Sodinokibi-platformen understøtter ransomware-operationer ved at tilbyde nødvendig infrastruktur, herunder brugergrænseflade til administration og generering af individuelt konfigurerede udgaver af

[1] https://www.bleepingcomputer.com/news/security/ryuk-ransomware-bitcoin-wallets-point-to-150-million-operation/ & https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/
[2] CrowdStrike Global Threat Report 2020

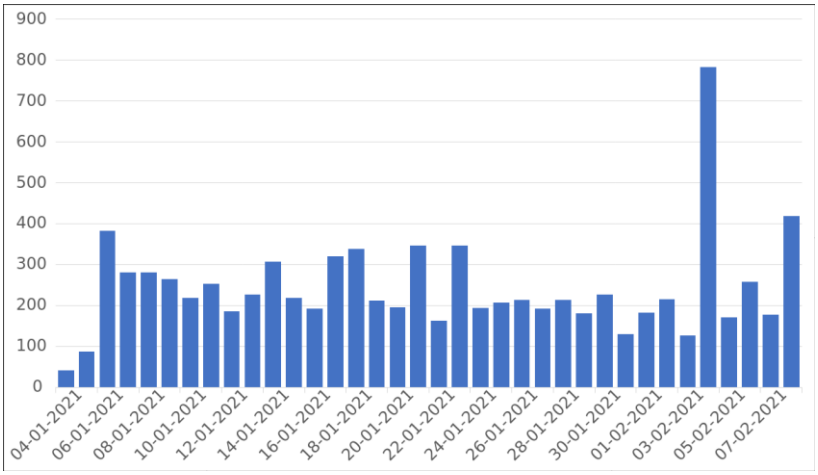
Sodinokibi-malwaren. Desuden håndteres også den økonomiske side, herunder modtagelse af løsesum fra ofrene, samt fordelingen af den økonomiske fortjeneste mellem Sodinokibi-bagmændene og samarbejdspartnere. Der er set opkrævning af løsesum af en størrelse op mod 10 millioner dollars, men den gennemsnitlige løsesum ligger ifølge åbne kilder på 233.817 dollars.[3]

Platformen er designet således, at bagmændene bag ransomwaren kan dekryptere alle filer, som er blevet krypteret med Sodinokibi-malwaren. Det kan de ved brug af deres egen private hovednøgle. Samarbejdspartnere er dog begrænset til kun at kunne dekryptere filer hos ofre, de selv har inficeret. Ofrene får ligeledes også kun mulighed for at dekryptere deres egne filer – forudsat at de har betalt løsesummen.

DOBBELT AFPRESNING

Flere virksomheder har som en foranstaltning mod ransomware-angreb fået styr på deres backup-løsninger. Dette var tidligere tilstrækkeligt. Men en stigende tendens er afpresning, hvor kriminelle forud for krypteringen af ofrets sensitive filer downloader data fra det kompromitterede netværk. De kriminelle får dermed yderligere "vægt" i forhold til forhandling af løsesum, når de er i besiddelse af data, som samtidig er gjort utilgængelig for ofret. På den måde kan de true med at frigive eller sælge disse data, hvis offeret ikke betaler. Det betyder i praksis, at en fungerende backup-løsning kun er det halve forsvar. Afpresning ses i halvdelen af de optalte ransomware-angreb.[4]

Man bør desværre som offer antage, at de stjålne data muligvis sælges til tredjepart eller bruges i fremadrettede afpresningsforsøg - uagtet om man har betalt den forlangte løsesum. Netop derfor er det vigtigt at prioritere sit it-forsvar mod ransomware-angreb.



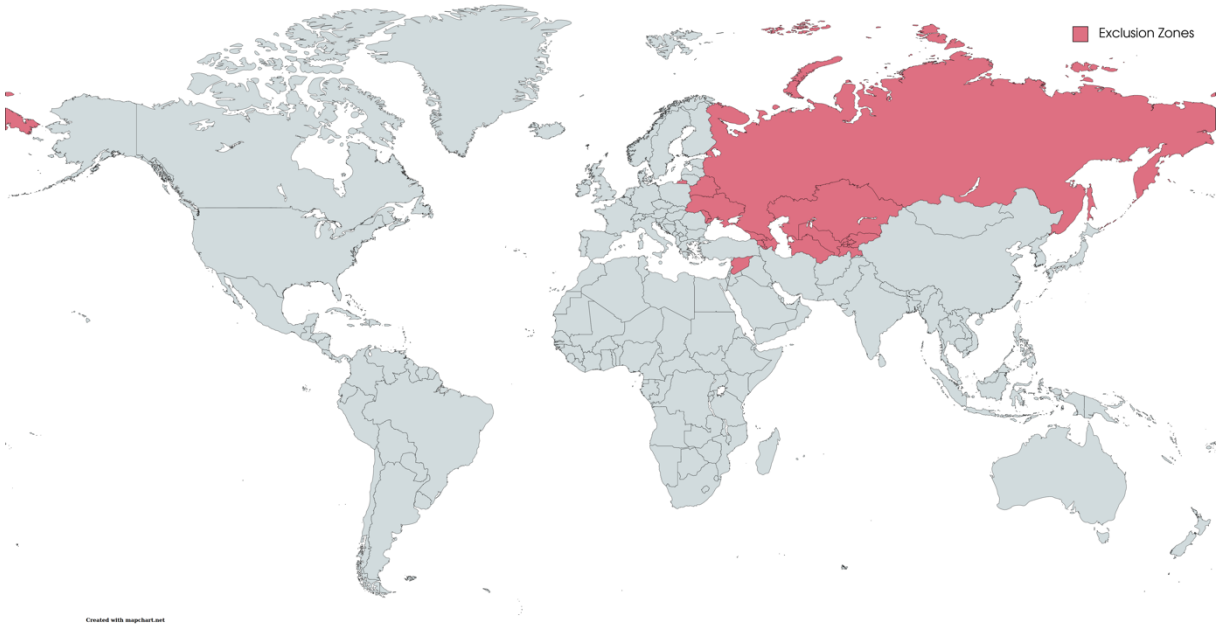
Infektionsfrekvens pr. dag med Sodinokibi på verdensplan i januar 2021

DET GEOGRAFISKE ASPEKT

Det er forventeligt at Sodinokibi-bagmændene ønsker at inficere så mange enheder som muligt med deres ransomware for i sidste ende at opnå maksimal økonomisk gevinst. Sodinokibi-malwaren

[3] https://coveware.com/blog/q3-2020-ransomware-marketplace-report & https://coveware.com/blog/q2-2020-ransomware-marketplace-report
[4] https://coveware.com/blog/q3-2020-ransomware-marketplace-report & https://coveware.com/blog/q2-2020-ransomware-marketplace-report

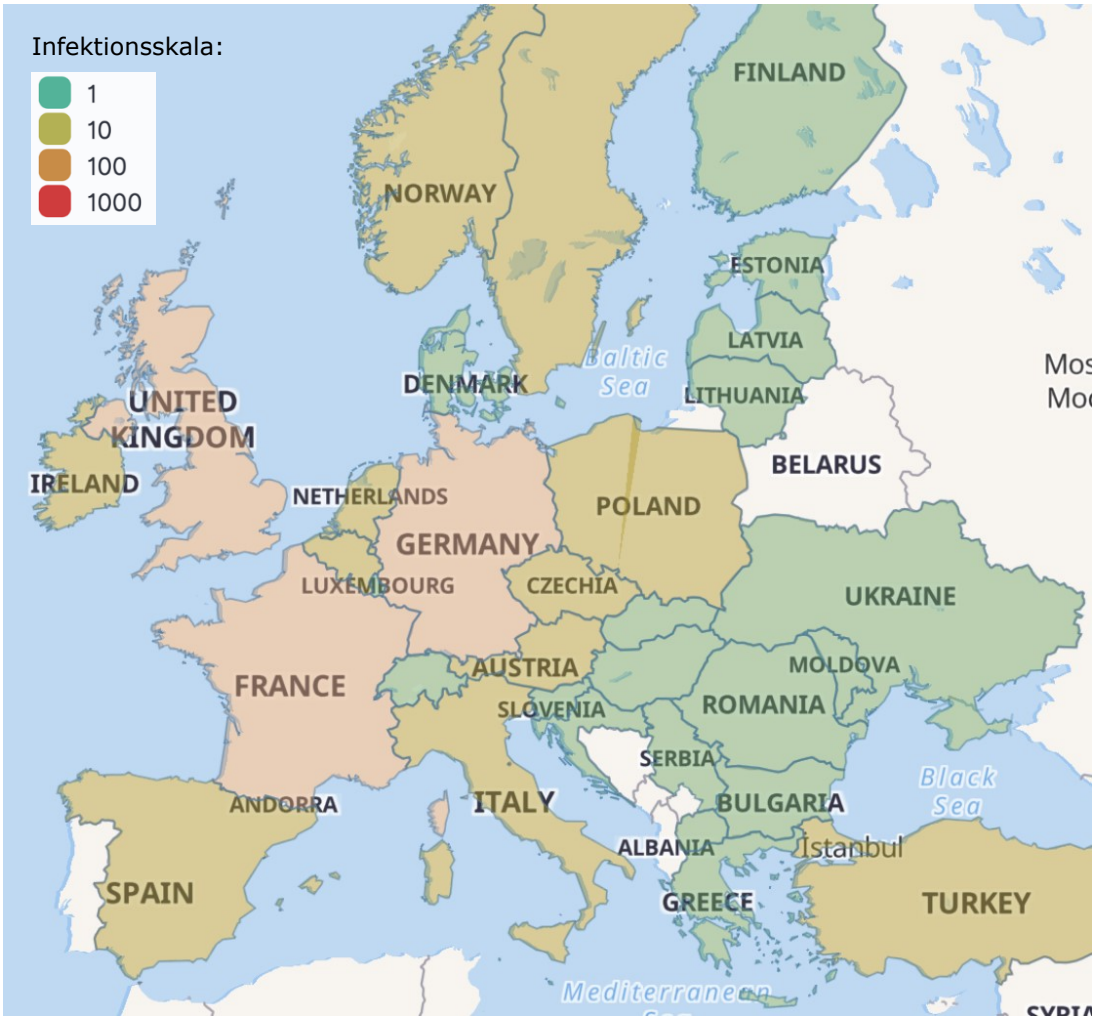
afbryder dog infektionen af systemet, såfremt operativsystemets sprog og tastaturlayout passer på et af følgende lande: *Armenien, Aserbajdsjan, Georgien, Hviderusland, Kasakhstan, Kirgisistan, Moldova, Rusland, Syrien, Tadsjikistan, Turkmenistan, Ukraine eller Usbekistan.*



Geografiske eksklusionszoner

Det er desværre ikke muligt direkte at udlede årsagen til disse eksklusionszoner.

CFCS har lavet et såkaldt *sinkhole* på et afregistreret domæne og på den baggrund uddraget statistiske infektionsdata. Herunder ses et uddrag af disse for januar 2021, hvori der ses hvilke lande samt med hvilken frekvens de er blevet angrebet.



Europæisk infektionskort for januar 2021

Globalt infektionskort for januar 2021

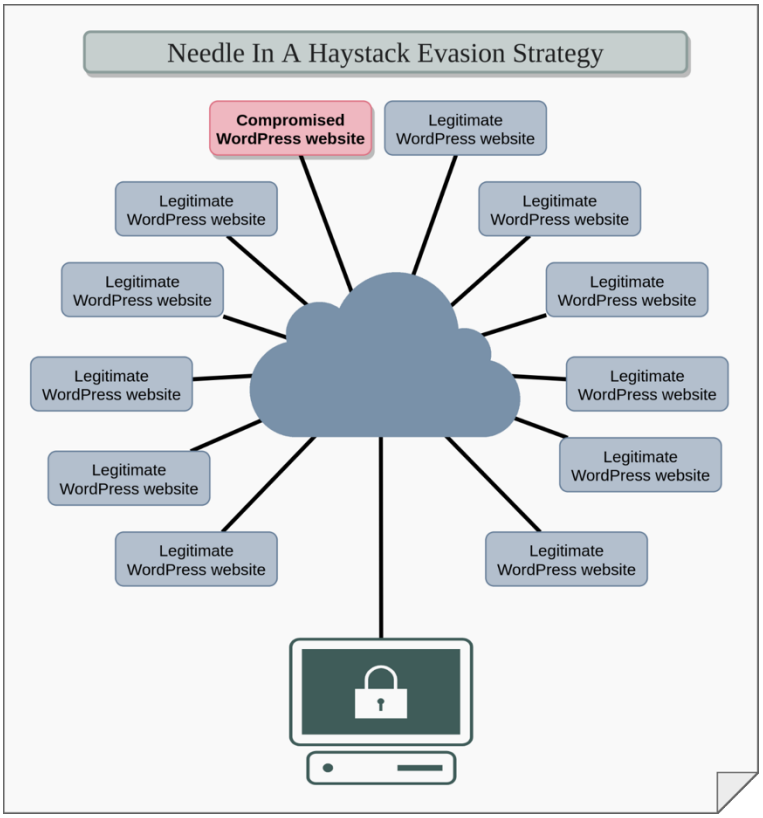
DET INDLEDENDE ANGREB

Angrebene påbegyndes ofte ved kompromittering af internetvendte fjernskriveborde (RDP), SMB services samt målrettede phishing e-mails, hvorfor det er vigtigt at prioritere disse i virksomhedens forsvar. [5] Alle internetvendte systemer er dog potentielle angrebsflader, og både den offentlige og private sektor er udsatte mål.

KONTAKTEDE DOMÆNER

Når ransomwaren har krypteret offerets filer, sender den et såkaldt "beacon". Det afsendte beacon er en datapakke, som indeholder information omkring det inficerede system samt benyttede kryptografiske nøgler. Dette beacon sendes til en lang række internetdomæner via HTTPS. Mængden af legitime internetdomæner er interessant. Ofte har malware blot ét enkelt eller et lille antal domæner der kontaktes, men i dette tilfælde kontaktes over 1.200 domæner.

Analyse af forskellige udgaver af Sodinokibi-malwaren, hvori debug informationer ikke var fjernet, viser, at disse domæner kaldes for "stat"-domæner. Måske en hentydning til, at de primært benyttes til opsamling af statistik om inficerede systemer. Domænerne peger på legitime sider på servere, der geografisk er fordelt over hele verden. Det er ofte mindre sider, som benytter sig af CMS-systemet WordPress. Det kan være vanskeligt at bedømme, hvilken netværks-infrastruktur Sodinokibi-bagmændene reelt har adgang til, når den samme trafik sendes til mere end 1.200 domæner.



Den berømte nål i en høstak

[5] CrowdStrike Global Threat Report 2020 og coveware

Hele listen af domæner skiftes endvidere i omtrent halvårlige intervaller. En anden interessant observation er, at beacons sendes som en "HTTPS POST" forespørgsel til et billede, hvis navn delvist er tilfældigt genereret. Det er fordelagtigt for bagmændene, da indholdet (BODY) af POST-forespørgsler almindeligvis ikke opsamles i webserver-logs. Anvendelsen af kompromitterede WordPress sider stemmer desuden overens med den stigende tendens CrowdStrike rapporterer om i deres årlige Global Threat Report.[6]

Analyse af koden

KODEBASENS KVALITET OG KOMPLEKSITET

Først og fremmest er kodebasen solid. Dette kan blandt andet ses i de korrekt implementerede kryptografiske algoritmer. Disse algoritmer tvinger offeret til at betale, såfremt de ønsker deres data tilbage. For at højne sikkerheden for en vellykket kryptering, forsøger Sodinokibi-malwaren desuden at stoppe programmer og services således at de filer, de arbejder med, frigives. Dermed kan de efterfølgende krypteres på en sikker måde. Disse faktorer har medvirket til, at netop Sodinokibi-bagmændene er blevet en af de største aktører i ransomware-branchen med en estimeret andel af markedet på lidt over 16%.[7]

INDLÆSNING AF AFHÆNGIGHEDER

Sodinokibi-malwaren gør kun begrænset brug af den almindelige importtabel for derved at skjule interessante afhængigheder, der ellers kan fortælle noget om dens kapabiliteter. Under opstart indlæses i stedet en liste af slørede afhængigheder.

INDLEJRET KONFIGURATION

Sodinokibi-malwaren indeholder en konfiguration, som er krypteret med RC4, hvorfor der ligeledes er indlejret en statisk dekrypteringsnøgle. Selve konfigurationen bruger JSON-indkodning, og nedenfor er vist et udsnit af et eksempel.

```
{
    "sub": "1234",
    "prc": ["excel", "sql", "winword", (forkortet)],
    "dmn": "https://some-wordpress-site[.]unknown; (forkortet)",
    "img": "(forkortet)",
    "pid": "123",
    "svc": ["sql", "backup", (forkortet)],
    "fast": true,
    "wht": {
        "ext": ["dll", "ps1", (forkortet)],
        "fls": ["boot.ini", (forkortet)],
        "fld": ["windows", (forkortet)]
    },
    "dbg": false,
    "exp": true,
    "pk": "(forkortet)",
    "net": true,
    "wipe": true,
    "nname": "{EXT}-readme.txt",
    "nbody": "(forkortet)"
}
```

Reduceret eksempel på en konfiguration

[6] CrowdStrike Global Threat Report 2020

[7] https://coveware.com/blog/q3-2020-ransomware-marketplace-report & https://coveware.com/blog/q2-2020-ransomware-marketplace-report

Ved at undersøge konfigurationen og den kompilerede kode, kan vi drage en række konklusioner omkring virkemåden.

Konfigurationen indeholder blandt andet en positivliste af filendelser samt specifikke filnavne og mapper, som ikke må blive krypteret. Dette gøres for at bibeholde operativsystemet i en minimal, men stabil tilstand for derved at kunne vise offeret en vejledning i, hvordan man betaler for at få dekrypteret filerne igen.

Konfigurationen indeholder desuden en liste med over 1.200 domæner.

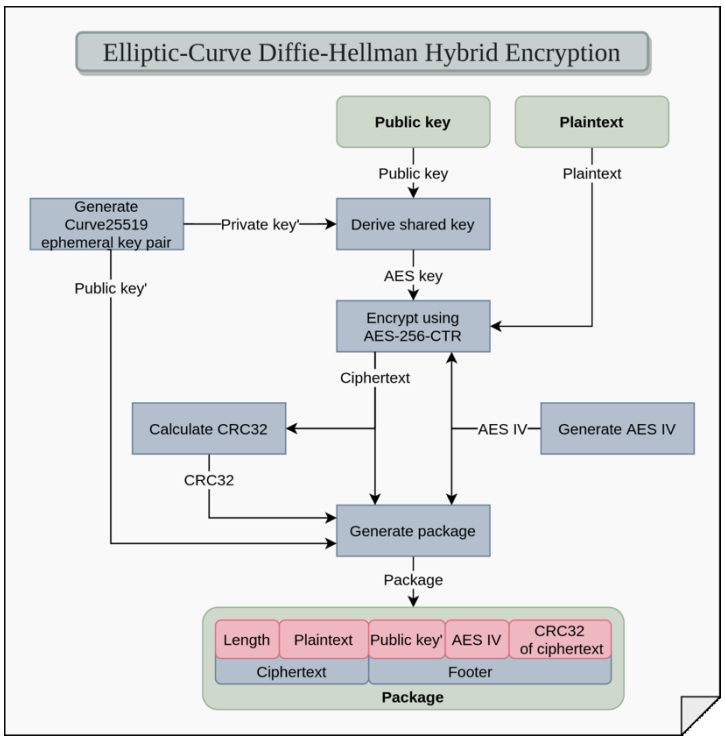
KRYPTOGRAFISKE ALGORITMER

CFCS konkluderer, at der benyttes sikre algoritmer til at generere og udveksle kryptografiske nøgler samt kryptering af data.

Der laves én kryptografisk nøgle til symmetrisk kryptering (AES-256-CTR), der benyttes når beacons sendes til Command and Control domænerne. Denne unikke nøgle er bundet til den specifikke installation.

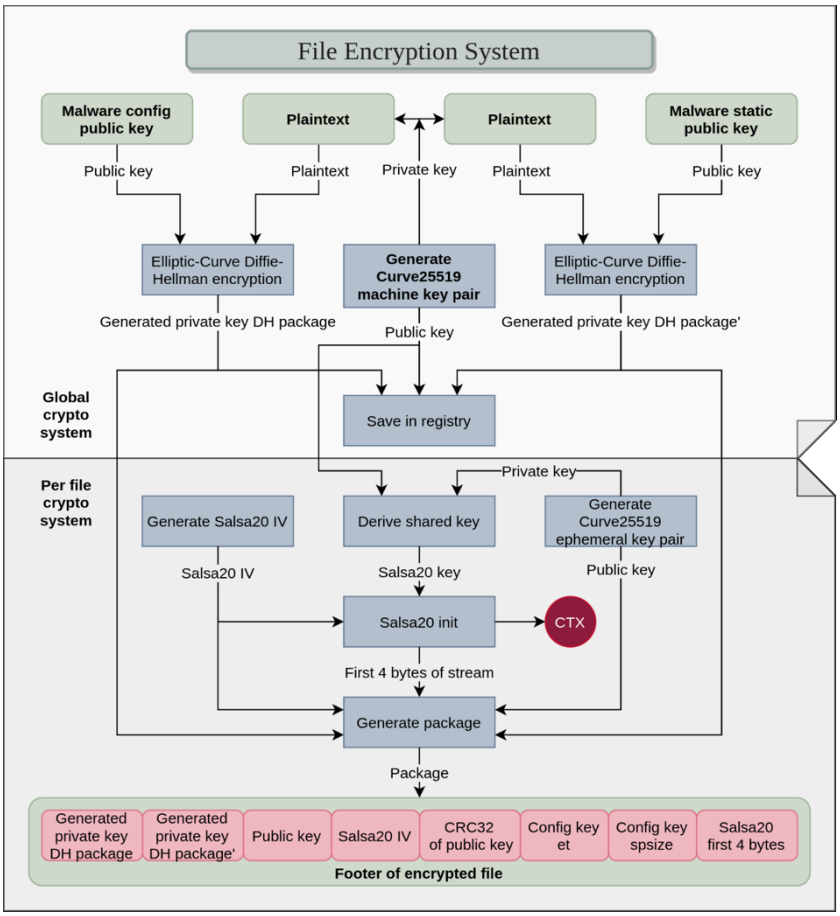
Derudover laves der en unik kryptografisk nøgle for hver eneste fil der krypteres. Filerne krypteres med Salsa20 algoritmen.

Udveksling af nøglepar og kryptering sker blandt andet via et Elliptic-Curve Diffie Hellman (ECDH) hybridkrypteringssystem med Curve25519. Efter at have modtaget en offentlig nøgle, krypteres klartekst ved brug af AES-256-CTR. ECDH-delen er illustreret i diagrammet nedenfor.



Benyttet krypteringssystem til beacons og delvist til filer

ECDH-delen indgår desuden i filkrypteringssystemet. Dette system er inddelt i to hoveddele. Et system som afvikles én gang per installation, og et andet der afvikles for hver enkelt fil der krypteres.



Benyttet krypteringssystem til filer

Hver krypteret fil får tilføjet ekstra data. Vigtigst er, at dette data indeholder to krypterede privatnøgler, som hver især kan bruges til at beregne fil krypteringsnøglen. Det forudsætter naturligvis, at man er i besiddelse af mindst én af de private nøgler, der hører til de offentlige nøgler, der blev brugt som parametre til ECDH-delen i det globale krypteringssystem. Kun Sodinokibi-bagmændene kan derved lave et program, der dekrypterer offerets filer, hvilket netop er den service, de tager sig så velbetalt for.

Malwareanalyser bidrager med viden

Ved at analysere malware kan man få indsigt i dens funktionalitet. Når man forstår, hvordan den virker, kan man bedre lave modforanstaltninger og beskytte sig mod de teknikker malwaren benytter. Har man for eksempel gennem sin analyse fundet de IP-adresser eller “Command and Control" domæner, som malwaren kommunikerer med, kan man blokere for disse i sin firewall og proxy. Analytikeren kan også finde unikke byte-mønstre der kan bruges til detektering af den specifikke malware i antimalware-løsninger.

Malware-udviklere er naturligvis bekendt med analytikernes arbejdsmetoder og prøver ofte at vanskeliggøre denne analyse. Malware-analyse kræver derfor specialiseret viden og kan være en langsommelig og resursekrævende proces. Derfor besidder mange virksomheder almindeligvis ikke selv de fornødne resurser til at udføre denne opgave.

CFCS modtager ofte filer fra virksomheder, der oplever sikkerhedsbrud. Når CFCS modtager en mistænkelig fil, vil den ofte blive grundigt analyseret af en analytiker. På baggrund af denne analyse dokumenterer analytikeren interessante aspekter med henblik på at hjælpe den ramte virksomhed samt bedre fremadrettet at kunne detektere og mitigere angreb. Det kan blandt andet være i form af rådgivning eller anonymiserede undersøgelsesrapporter.

REFERENCER

- https://www.bleepingcomputer.com/news/security/ryuk-ransomware-bitcoin-wallets-point-to-150-million-operation/
- https://www.bleepingcomputer.com/news/security/revil-ransomware-gang-claims-over-100-million-profit-in-a-year/
- https://coveware.com/blog/q3-2020-ransomware-marketplace-report
  https://coveware.com/blog/q2-2020-ransomware-marketplace-report
- https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave marts 2021.