CENTER FOR CYBERSIKKERHED

UNDERSØGELSESRAPPORT

Et wiper-angrebs anatomi

Hvordan wipere fungerer, og hvordan du forsvarer dig mod dem

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave juni 2024

Formål

Destruktive cyberangreb er generelt sjældne, men kan have alvorlige konsekvenser. Den mest udbredte type destruktive cyberangreb er wipere, der anvendes med henblik på at destruere eller afskære offeret fra sin data. Denne rapport har til formål at orientere om formålene med at anvende wiper-angreb, hvordan et typisk angreb forløber, samt hvordan du kan beskytte dig mod dem. Målgruppen for denne rapport er primært it-ledelse og it-teknikere.

1. Indledning

Destruktive cyberangreb har indtil nu oftest været anvendt i konflikter mellem stater. Særligt Ukraine har siden 2014 været udsat for flere destruktive cyberangreb, og antallet af angreb mod ukrainske organisationer steg til et hidtil uset omfang efter Ruslands invasion af landet i februar 2022.

Ruslands krig mod Ukraine har ændret den sikkerhedspolitiske situation i Europa. Danmark står overfor et nyt trusselsbillede, hvor tidligere tydelige grænser mellem fred, krise og krig er blevet erstattet af slørede og overlappende overgange mellem de forskellige stadier. Det er på den baggrund alvorligt, at statslige hackergrupper sandsynligvis forbereder kapaciteten til at kunne udføre destruktive cyberangreb mod dansk kritisk infrastruktur.

Den klart mest udbredte type destruktive cyberangreb er såkaldte wiper-angreb. I et wiper-angreb slettes, overskrives eller krypteres data, så den er utilgængelig eller er umulig at genskabe. Et sådan angreb kan være en alvorlig trussel mod den ramte organisation og, afhængigt af målet, potentielt også det omkringliggende samfund. Ved at destruere kritisk information og systemer kan angriberne besværliggøre eller stoppe en organisations arbejde og derved potentielt afbryde samfundsvigtige funktioner.

Denne rapport belyser, hvilke formål hackere kan have med at anvende wipere, de overordnede faser i et angreb samt forskellige wipingteknikker. Det gøres ved at inddrage konkrete eksempler fra forskellige observerede wipere. Afslutningsvist er der råd og anbefalinger til, hvordan man kan beskytte sig mod wiper-angreb.

Der findes også andre former for destruktive cyberangreb end wiper-angreb. Der er eksempler på, at hackere har udført destruktive cyberangreb, hvor hensigten var at manipulere industrielle kontrolsystemer og dermed få sat systemerne ud af drift og i visse tilfælde endda forårsage fysisk ødelæggelse. Medmindre systemerne har lav sikkerhed, er det typisk kompliceret at udføre sådanne angreb. Det kræver bl.a. omfattende planlægning og forberedelse. Blandt andet derfor er disse angreb sjældne.

2. Formålene med et wiper-angreb

Selvom wiper-angreb er destruktive og angriberen i udgangspunktet har ødelæggelse for øje, kan de også bruges som et led i et mere overordnet mål. Disse mere strategiske hensigter med wiper-angreb har naturligvis indflydelse på, hvilke mål angrebet rettes mod, og hvordan angrebet udføres.

Alle typer organisationer med digitale systemer eller enheder kan i princippet blive ofre for wiper-angreb. I Ukraine er alt fra banker over supermarkeder til statslige myndigheder blevet udsat for wiper-angreb. Formålet med de fleste af angrebene mod Ukraine har sandsynligvis været at stresse og belaste det ukrainske samfund.

Udover at påvirke sin modstanders befolkning og beslutningstagere, kan hackere også bruge wiper-angreb til at sende politiske signaler. Et eksempel på sidstnævnte er wiperen Olympic Destroyer fra 2018, der af amerikanske myndigheder er blevet beskrevet som en russisk protest mod udelukkelsen af russiske atleter fra OL i Sydkorea.

Wiper-angreb kan også udføres i et forsøg på at opnå taktiske militære fordele i en konkret situation. Et eksempel på sådan et angreb er AcidRain, der fandt sted på dagen for Ruslands invasion af Ukraine i februar 2022 og sandsynligvis var målrettet de ukrainske militære styrkers satellitkommunikation. AcidRain-angrebet slettede opsætningen på tusindvis af satellitmodemmer fra den amerikanske virksomhed Viasat og påvirkede også organisationer udenfor Ukraine.

Der er også set eksempler på, at hackere har eksfiltreret informationer fra offerets systemer, inden de ødelagde den resterende data. I disse tilfælde kan det være, at spionageaktiviteten faktisk var det primære formål, og at angriberen ødelagde data for at slette sine spor eller for at skade modstanderen yderligere.

Det er dog langt fra altid, at motivet bag et wiperangreb er tydeligt. Hackere kan designe angrebet, så det netop skaber forvirring om motivet. Ved at forklæde sit angreb som et økonomisk motiveret ransomware-angreb, kan aktøren sløre sit motiv og ophav. Denne type angreb beskrives mere indgående senere i rapporten.

Wiper-angreb kan både være simple eller komplicerede cyberangreb at udføre. I visse tilfælde kan også de simple angreb forvolde stor skade. Visse angreb har været udført på en måde, der viser, at angriberen har haft dybdegående indsigt i offerets systemer og netværk. Det tager tid, ressourcer og teknisk forståelse at opnå den indsigt, og derfor er det ikke alle typer af hackere, der kan udføre sådanne angreb.

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) følger truslen fra destruktive cyberangreb, herunder wiper-angreb, og udgiver løbende trussels-vurderinger, der beskriver truslen. I disse trusselsvurderinger kan man bl.a. læse mere om aktørerne bag angrebene og sandsynligheden for angreb mod danske organisationer. Vurderingerne kan findes på CFCS' hjemmeside.

Hvem wiper?

Der er flere forskellige hackergrupper, der udfører wiper-angreb, og også forskellige bevæggrunde for at udføre dem. Nogle gør det for at ramme en modstander i en konflikt eller krig, andre for at skabe opmærksomhed om en sag, andre igen for at slette deres spor og endelig - i nogle få tilfælde - sker det måske helt uden, at det var aktørens hensigt. Nedenfor er tre eksempler på aktører, der har udført wiper-angreb.

Sandworm

Sandworm er en hackergruppe, som ifølge amerikanske myndigheder arbejder for den russiske stat. De er anklaget for at stå bag flere alvorlige destruktive cyberangreb, herunder adskillige wiper-angreb. Sandworm er særligt kendt for NotPetya-angrebet i 2017 og Olympic Destroyer-angrebet mod vinter-OL i Sydkorea i 2018. Sandworm er desuden af flere it-sikkerhedsfirmaer attribueret til at stå bag mange af de wiper-angreb, der har ramt Ukraine siden 24. februar 2022. Gruppen bliver kaldt Sandworm, fordi der er fundet referencer i deres malware til science fiction-bogen Dune af Frank Herbert fra 1965, hvor kæmpe sandorme spiller en afgørende rolle.

Lazarus Group

Nogle af de første store wiper-angreb blev udført af en hackergruppe, der bl.a. kendes som Lazarus Group, som senere af amerikanske myndigheder er attribueret til den nord-koreanske stat. Lazarus er af flere it-sikkerhedsfirmaer blevet udpeget som de ansvarlige for DarkSeoul wiper-angrebet, der i foråret 2013 bl.a. ramte flere sydkoreanske tv-selskaber og finansielle virksomheder, og tog titusindvis af computere ud af drift. Allerede igen i november 2014 blev Sony Pictures Entertainment ramt af et meget omtalt wiper-angreb, som Lazarus Group også blev sat i forbindelse med. Endelig er Lazarus også blevet forbundet til WannaCry i maj 2017, der er blandt de mest omfattende cyberangreb hidtil observeret. Selvom WannaCry var en ransomware-kampagne, betød en mulig fejl i udførelsen, at kampagnen reelt endte med at fungere som et wiper-angreb. Senere er Lazarus Group kædet sammen med wipere ifm. cybercrime, sandsynligvis for at besværliggørelse af en evt. efterforskning.

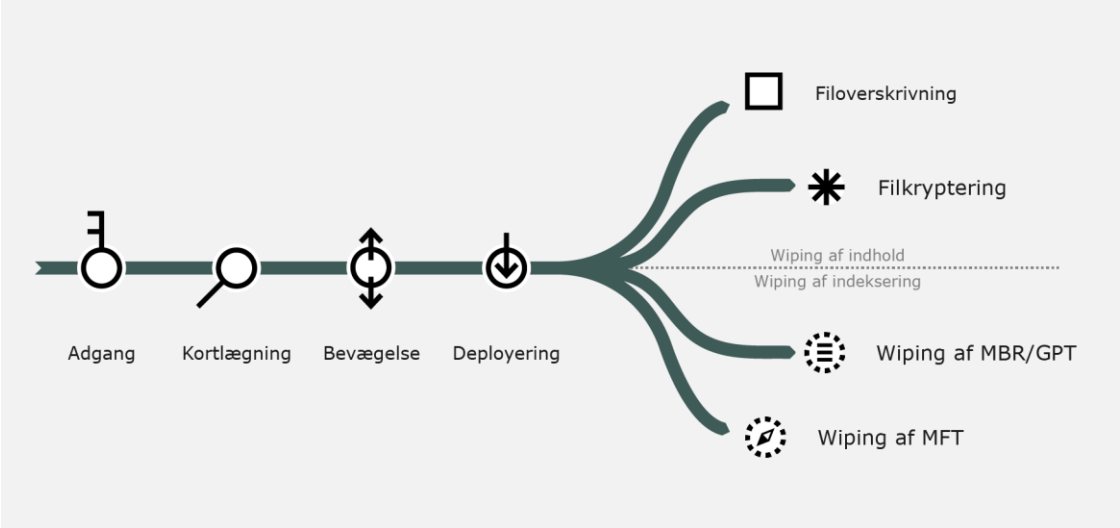
Shamoon

Shamoon-wiperen er observeret i flere versioner i flere forskellige kampagner over tid, som i åbne kilder med forskellige grader af sikkerhed er attribueret til iranske aktører. Første gang den blev observeret var i 2012, hvor den bl.a. blev brugt imod den saudiske olievirksomhed SaudiAramco, hvor mere end 30.000 computere blev ramt. Angrebet var på det tidspunkt et af de mest ødelæggende udført mod en virksomhed. Efterfølgende tog en hidtil ukendt gruppe, der kaldte sig selv Cutting Sword of Justice, ansvaret og udråbte det som et angreb mod det saudiske monarki. Fire år senere dukkede Shamoon-wiperen igen op i 2016, i en ny version. Mellem november 2016 og januar 2017 ramte den mål i forskellige samfundskritiske sektorer i Mellemøsten. I december 2018 blev Shamoon-wiperen endnu engang aktiv i en opdateret form. Målene var organisationer involveret i olie- og gasindustrien i Saudi-Arabien og de Forenede Arabiske Emirater, heriblandt Saipem, en italiensk servicevirksomhed inden for olieindustrien, der havde deres største kunde i Saudi-Arabien. Angrebet ramte specifikt Saipems tilstedeværelse i Mellemøsten, og mere end 300 servere og computere blev wipet.

3. Wiper-angrebets faser

I dette afsnit kortlægges forløbet i et typisk wiper-angreb. Beskrivelsen er inddelt i en række faser, der tilsammen danner det samlede angrebsforløb. Den opdeling kaldes for en Cyber Kill Chain, som betyder, at hver enkelt fase ofte er nødvendig for den næste. Derfor vil angrebet potentielt kunne afværges, hvis hackerne stoppes under én fase i angrebet.

Et wiper-angreb gennemgår generelt de samme overordnede faser, som de fleste andre typer cyberangreb. Selvom wiper-teknikker varierer og løbende bliver udviklet, følger de fleste angreb det samme overordnede forløb. I dette afsnit fremhæves de mest centrale faser i et wiper-angreb.

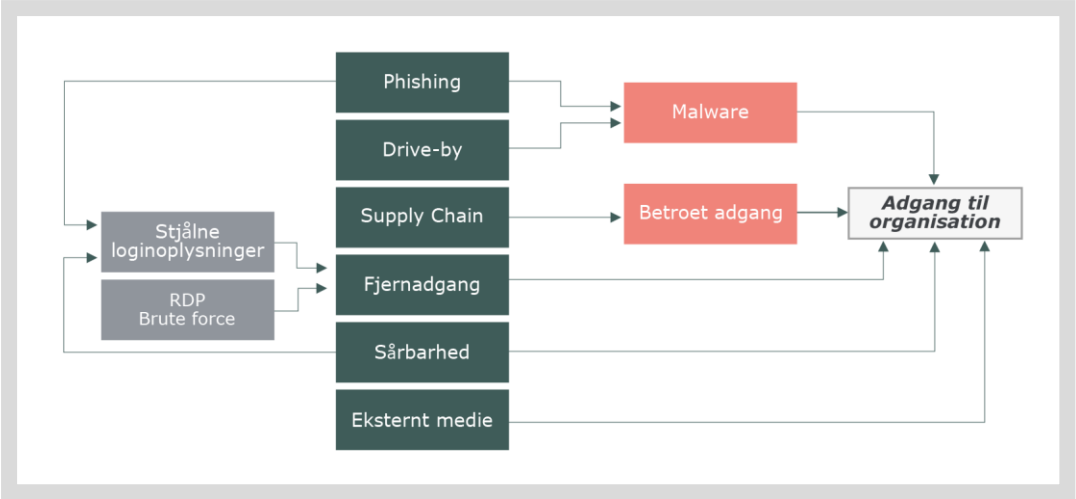


Figur 1: Et wiper-angrebs faser i form af en cyber kill chain. I højre side af figuren, hvor hackerne kan vælge forskellige wiping-teknikker, kan hackerne godt vælge flere af dem på én gang. Flere wipere har eksempelvis både wipet indholdet og indekseringen eller både wipet MBR pg MFT.

Hackerne skaffer sig adgang til offeret

Hackernes første mål er at opnå indledende adgang til deres mål. Metoderne til det er de samme som i andre typer cyberangreb. Forud for selve kompromitteringen af et bestemt mål vil hackerne typisk have lavet måludvælgelse og rekognoscering mod netværket. På baggrund af denne indledende undersøgelse vil hackerne kunne tilpasse deres værktøjer til at få adgang til organisationen. Hvis hackerne ønsker at ramme mange ofre eller har en mere opportunistisk tilgang til, hvilke ofre de rammer, vil de i stedet kunne lave brede sårbarhedsscanninger eller forberede brede phishing-kampagner.

Nedenstående figur illustrererer forskellige muligheder for hackere til at opnå en indledende adgang på offerets netværk. En mere dybdegående behandling af disse forskellige teknikker kan findes i CFCS' undersøgelsesrapport: Anatomien af målrettede ransomware-angreb.



Figur 2: Typiske metoder hackere opnår indledende adgange på.

Nogle metoder giver hackerne direkte adgang til offerets systemer uden bruger-interaktion. Det kunne eksempelvis være, hvis hackerne udnytter sårbarheder i internetvendte systemer, protokoller eller tjenester. Hackerne kan også have købt loginoplysninger til offerets systemer fra cyberkriminelle. Brute force-angreb er endnu en angrebsmetode, der ofte er effektiv. Her bryder hackerne svage adgangskoder.

Andre angrebsmetoder forudsætter, at ofrene først interagerer med hackerne. Det kan eksempelvis være via phishing-mails, hvor modtageren får leveret malware eller får franarret loginoplysninger.

En anden angrebsmetode er såkaldte supply chain-angreb, hvor hackere har angrebet en anden organisation og så misbruger den legitime adgang, som organisationen har til sine kunder eller samarbejdspartnere. Ved det omfattende NotPetya-angreb fra 2017 skete den indledende adgang ved et supply chain-angreb. Hackere kompromitterede en ukrainsk software-leverandør og fik derved distribueret en manipuleret software-opdatering, der indeholdt NotPetya-malwaren, til leverandørens kunder.

Hackerne kortlægger offerets systemer og netværk

Når hackerne har opnået adgang til offeret, står de grundlæggende set med et valg mellem hastighed og grundighed. Vælger hackerne grundigt at undersøge og kortlægge netværket, vil det give dem mulighed for at planlægge en omfattende og styret sletning. Samtidig øger det dog risikoen for, at de bliver opdaget grundet sikkerhedstiltag. Prioriterer hackerne derimod at udnytte deres adgang med det samme og foretage en hurtig sletning, kan det være at offeret kan genskabe sin data, da destruktionen typisk vil være mindre grundig.

Hvis hackerne prioriterer at undersøge offerets netværk, kan de gøre det på forskellige måder. Hackerne kan eksempelvis skanne computerens filer og system- og netværks-rettigheder for at undersøge, om den kompromitterede bruger er administrator eller ej. Har den kompromitterede bruger administratorrettigheder, vil vedkommende sandsynligvis også have adgang til alle mapper på de tilknyttede drev, hvilket kan give hackeren mulighed for at sprede malwaren og slette større mængder data.

Lateral bevægelse
Med en kortlægning af netværket vil hackerne ofte forsøge at bevæge sig lateralt på tværs i netværket. Det gør de bl.a. ved at forsøge at logge ind på andre klienter eller servere som lokaladministrator.

Når en administrator opretter forbindelse til en klient eller en server, skal de validere deres identitet med et kodeord. Det er dog tit en udfordring for administratorer, som skal holde styr på samtlige kodeord for alle enheder i et netværk, hvilket kan dreje sig om hundrede- eller tusindvis af individuelle kodeord afhængigt af netværket. Derfor er der en tendens til, at kodeordene er ens eller meget forudsigelige på tværs af klienter og servere. Det udgør imidlertid en stor sikkerhedsrisiko, hvis hackerne kan bryde, gætte eller på anden vis få fat i kodeordene. Hvis dét sker, kan hackerne frit oprette forbindelse til klienterne eller serverne på netværket med administratorrettigheder.

Domæneadministrator
Domæneadministratoren er en gruppe af særligt priviligerede brugere i Active Directory, der har fuld control over hele organisationens netværk. Gruppen kontrollerer, hvem der har adgang til hvilke dele af netværket og kan tildele adgang til brugere på netværket.

Group Policy Objects (GPO)
GPO'er er en samling indstillinger, der gør det muligt for en domæneadministrator at implementere specifikke konfigurationer for brugere på netværket, f.eks. krav til kodeordskompleksitet, eller hvilke mapper og drev forskellige brugere har adgang til.

Har hackerne held med at placere sig på domæneadministratorens konto, har de adgang til hele infrastrukturen og kan hurtigt kortlægge organisationens data-infrastruktur. Den er ofte allerede kortlagt af organisationen selv med henblik på at udrulle opdateringer. Her kan hackerne f.eks. udnytte de såkaldte Group Policy Objects (GPO'er). GPO'er kan også bruges til at beslutte, hvilke programmer der automatisk skal starte, når styresystemet tændes på den enkelte computer. På den måde kan hackere placere malware på alle netværkets brugere og vælge, at malwaren skal sætte gang i sletningen, så snart de enkelte brugere logger på.

Domain control servere er hjertet i de fleste organisationers netværk. Den giver adgang til hele organisationens domæne, hvorfra de kan styre store dele af organisationens it-infrastruktur. Disse funktioner er guld værd for hackere, der ønsker at udføre et wiper-angreb. I stedet for at skulle opnå adgang til hver eneste klient og server i netværket giver en administratoradgang til en Domain Controller mulighed for at udrulle en wiper til hele domænet på én gang. Domæne-administratorer med adgang til Domain Controllere er derfor meget attraktive for hackerne, og deres konti bør være særligt beskyttede.

Hackerne opretter i nogle tilfælde en ny domæneadministratorkonto, når de har adgang til Domain Controlleren. Det gør de dels i forsøget på at omgå logning, men også for at undgå at miste adgangen igen, i tilfælde af at den kompromitterede domæneadministrator skulle ændre kodeord.

Caddywiper - wiperen der ikke vil slette alt

Denne wiper har ad flere omgange ramt adskillige organisationer i Ukraine. CaddyWiper tjekker som det første, om den kører på en domænecontroller. Er det tilfældet, stopper den al aktivitet og lukker ned. Hvis malwaren er landet på en almindelig bruger, vil den indlede sletningen. Det er bemærkelsesværdigt, fordi det i et typisk angreb netop er domænecontrolleren, der interessant at kompromittere, så der er mulighed for at fordele malwaren ud i hele netværket.

En mulig grund til at hackerne ikke ønskede at wipe via domænecontrolleren kunne være, at man ønskede at bevare adgang til netværket, f.eks. i form af en bagdør til eksfiltrering af data eller som en platform til at udføre yderligere angreb.

Deployering af wiper-malware

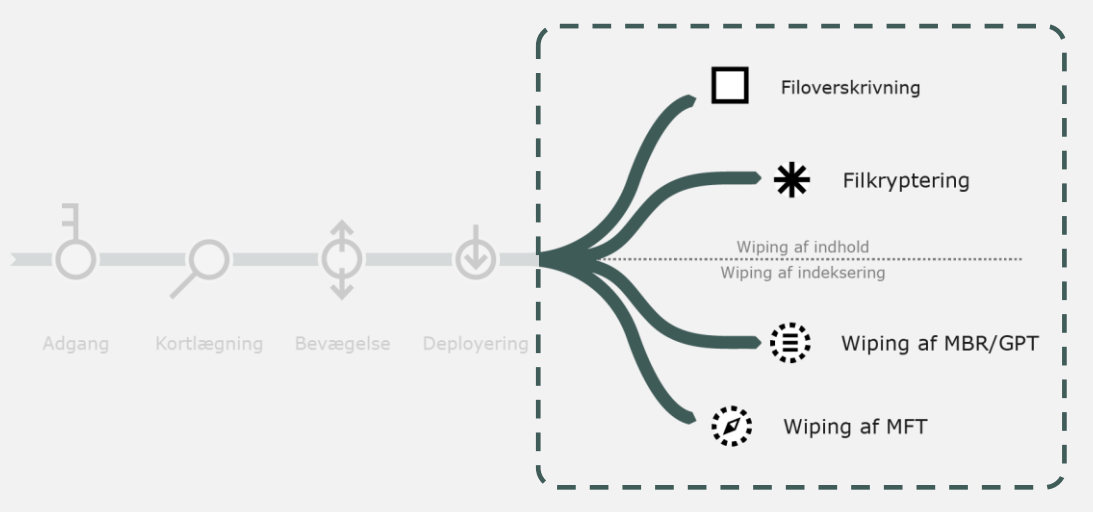
Afdækningen af offerets system, adgange og netværk danner grundlag for beslutningen om, hvordan angrebet skal designes. Som led heri vil hackerne kunne programmere malwaren mere specifikt. Hackeren kan f.eks. opliste mapper og filer i den rækkefølge, de skal slettes i, for at holde systemet stabilt så længe som muligt. Det kan gøres ved, at wiperen konfigureres til enten at prioritere eller springe over forskellige filplaceringer eller -typer. Dette kan eksempelvis være Windows' systemmapper og programfiler såsom .EXE, .SYS og .LIB. Wiperen vil typisk først overskrive de ikke-kritiske filer såsom dokumenter, billeder og zip-filer og først til sidst overskrive systemkritiske filer.

Det er dog ikke altid, at hackere har brug for manuelt at gennemgå deres ofres systemer for at skabe et meget ødelæggende angreb. Hackere kan f.eks. have programmeret deres malware til at sprede sig automatisk på et offers netværk via nogle kritiske sårbarheder. Det var bl.a. NotPetya-malwarens evne til sprede sig på ofrenes netværk, der gjorde den særligt ødelæggende.

Wiping påbegyndes

Som nævnt tidligere, findes der forskellige typer wiping-teknikker. Wipere kan for forståelsens skyld opdeles ift., om de ødelægger selve indholdet, eller om de ødelægger fortegnelsen over, hvor forskellige filer er på harddisken. Sidstnævnte er i figuren nedenfor kaldt wiping af indekseringen. Den ene wipingteknik udelukker ikke den anden - flere wipere har både wipet indholdet og indekseringen. I det følgende beskrives de dog hver for sig, da der er visse specifikke nuancer ved de to wiping-teknikker, der er værd at dykke ned i, bl.a. fordi de ikke ødelægger data lige effektivt.

Uanset om hackerne ønsker at wipe indholdet eller indekseringen, kan de derudover vælge enten at slette, overskrive eller kryptere data.



Figur 3: Figuren fremstiller faserne i et wiper-angreb. Vi er nu nået til at data wipes. Angriberne kan vælge forskellige tilgange til dette. Blandt andet kan de vælge at gå efter at wipe indholdet eller indekseringen på harddisken.

Wiping af indhold

Vil hackerne sikre en grundig sletning af data, kan de gå efter at ødelægge indhold gemt på harddisken, så filerne ikke kan genskabes. Det er mere tids- og ressource-krævende end kun at ødelægge indekseringen af filer, hvilket beskrives senere.

Diskens indhold kan som sagt destrueres ved enten at slette, overskrive eller kryptere de enkelte filers data på deres fysiske placeringer på harddisken. I resten af rapporten er fokus på overskrivning og kryptering, da det typisk ikke er særligt effektivt kun at slette data.

Når filer på en harddisk slettes, fjernes de ikke umiddelbart fra disken med det samme. Pladsen, hvor filen var gemt, bliver i stedet markeret som ledig til at gemme nye filer på. Når nye filer så gemmes, overskrives den data, der tidligere befandt sig på pladsen, og derfor er den oprindelige data først nu reelt slettet. Derfor kan man ofte genskabe en fil, der er blevet slettet ved en fejl. Der er enkelte eksempler på wipere, der kun har slettet data, men de har typisk også været forholdsvis nemme at udbedre. Oftest sletter wiper-malware derfor ikke bare, men overskriver også med ny og ubrugeligt data, for netop at sikre sig, at den oprindelige data er helt væk.

Den mest effektive måde at gøre dette er at overskrive harddiskens forskellige clusters med tilfældigt genererede bytes, så filerne erstattes med ulæselige data. I mange tilfælde designes malwaren til at overskrive filer i en bestemt rækkefølge for at holde systemet stabilt, indtil angrebet er færdigt. Malwaren kan desuden programmeres til også at slette sig selv som det sidste trin i processen. Det vanskeliggør den efterfølgende analyse af angrebet.

En anden måde hackerne kan wipe indholdet er ved at kryptere data på harddisken. Det er typisk mere kompliceret at lave angreb, som anvender kryptering end ren overskrivning af filer med ulæselig data. Det gælder både selve konstruktionen af malwaren, samt den computerkraft, der skal bruges på offerets systemer til at udføre denne sidste del af angrebet. Når hackere derfor anvender kryptering i wiper-angreb er det typisk, fordi hackerne vil skabe forvirring om, hvem der står bag angrebet og hvad deres motiv er.

Forvirringen kan opstå, fordi kryptering af data oftest bruges i kriminelle ransomware-angreb. I kriminelle ransomware-angreb bliver krypteringen af data fulgt af et krav om at betale en løsesum for at få udleveret en nøgle, der kan dekryptere dataen. Hvis de rigtige krypteringsalgoritmer bruges og implementeres korrekt, vil det være så godt som umuligt for offeret at dekryptere filerne uden dekrypteringsnøglen. Ved wiper-angreb, hvor formålet er destruktion frem for økonomisk vinding, har hackerne imidlertid ingen intention om at give dekrypteringsnøglen til offeret.

Det er dog ikke altid, at kryptering bruges for at skabe tvivl om formålet og aktøren bag angrebet. Selvom kryptering som udgangspunkt er mere ressourcekrævende end overskrivning, kan hackerne spare nogle af disse ressourcer ved at bruge offentligt tilgængelig ransomware, som eksempelvis kan være lækket på kriminelle fora. På den måde kan de spare egenudviklingen af malware, og dermed kan de hurtigt iværksætte flere angreb.

Wiper eller ransomware?

Der er flere eksempler på wiper-angreb mod Ukraine, hvor data er blevet krypteret. Angrebene har i forskellig grad forsøgt at efterligne ransomware-angreb, hvor nogle af dem har indeholdt den fulde pakke med reel kryptering af data, ransom notes med krav om løsesum, mailadresser til kommunikation med angriberne, samt bitcoin-wallets, hvor løsesummen kunne overføres til.

Efter analyser af angrebene står det dog klart, at der har været tale om såkaldte false flag-operationer, og at angrebene reelt var destruktive cyberangreb. Der er f.eks. analyser, der viser, at krypteringen har været udført på en sådan måde, at det reelt ikke er muligt at dekryptere, eller at de bitcoin-wallets, som løsesummen kræves udbetalt til, ikke eksisterer. Yderligere oplysninger kan i visse tilfælde også forbinde angrebene til fremmede staters efterretningstjenester og dermed styrke vurderingen af, at der er tale om destruktive cyberangreb. Denne type gråzoneangreb medfører økonomisk og samfundsmæssig skade og kan også bidrage til forvirring og usikkerhed om, hvordan stater skal reagere.

HermeticWiper og HermeticRansom

Hermetic-angrebet blev udført mod ukrainske mål i januar 2022 og altså før Ruslands invasion af Ukraine. Selve wiperen Hermetic var et klassisk wiper-angreb, der gik efter at wipe indekseringen. Det bemærkelsesværdige var, at der sideløbende blev udført et andet angreb, hvor malwaren indeholdt et såkaldt ransomwaremodul. Modulet blev af IT-sikkerhedsvirksomheder døbt HermeticRansom. Malware-analytikere kunne hurtigt konkludere, at malwaren med stor sandsynlighed ikke var reel ransomware, da det ikke var muligt at dekryptere filerne. Den tilsyneladende lighed med ransomware bidrog til at skabe forvirring om formålet med angrebet.

Wiping af indeks eller opstartsproces

I bl.a. Ukraine og Saudi Arabien har flere wiper-angreb været rettet mod de strukturer, der gør computere i stand til at indlæse sit styresystem ved opstart eller at ødelægge den oversigt, der gør det muligt at finde filer på harddisken. Denne form for angreb er tidseffektivt og gør systemet utilgængeligt for brugeren. Det kan dog i flere tilfælde være muligt at genskabe systemet, da data stadig er til stede på harddisken.

I angreb mod indekseringen kan hackerne også vælge mellem at overskrive eller kryptere data.

Master Boot Record (MBR) og GUID Partition Table (GPT): Computerens udgangspunkt
MBR bruges under computerens opstartsproces til at identificere, hvor på disken operativsystemet fysisk er gemt og skal indlæses fra ved opstart. Hvis MBR er korrumperet, så vil computerne crashe ved opstart.

I flere af de mest kendte wiper-angreb, såsom Shamoon, NotPetya og HermeticWiper, har malwaren ødelagt computerens mulighed for at indlæse sit styresystem i opstartsprocessen. Det gøres ved at overskrive eller kryptere harddiskens Master Boot Record (MBR), som i nyere systemer er erstattet af GUID Partition Table (GPT). MBR'en kan eksempelvis overskrives med data, der fører til, at en bestemt besked eller et billede bliver vist på offerets skærm. I Shamoon-angrebet mod olieselskabet Saudi Aramco i 2012 overskrev malwaren MBR, så der blev vist et billede af et brændende amerikansk flag på de inficerede computeres skærme. I falske ransomware-angreb bliver der typisk vist en ransom note.

Filsystemets Master File Table (MFT) holder styr på, hvor data fysisk er lagret på harddisken. En hacker kan udnytte det og vælge at angribe MFT'ens strukturering af harddiskens indhold. Ødelægges eller beskadiges MFT'en, bliver den lagrede data i praksis gjort utilgængelig for systemet og brugeren, da filsystemets oversigt over de lagrede filer på harddisken er væk.

Master File Table (MFT): Harddiskens indholdsfortegnelse
Alle filer og mapper på harddisken bliver skrevet ind i MFT'en i en såkaldt FILE record. Ud over at rumme metadata om filer, indeholder den også en henvisning til, hvor på harddisken filens data er fysisk lagret.

Når MTF'en er væk, ved systemet ikke længere, hvilke filer der er lagret, og hvor de fysisk er placeret på harddisken. Filernes data er dog fortsat intakte, indtil de bliver overskrevet.

Dette er en hurtig wipingmetode, men ikke den mest ødelæggende. Selv om filsystemet ikke længere kan se, hvor filerne er placeret, vil filernes data typisk fortsat være til stede. Det gør, at offeret har mulighed for at genskabe sine filer med specialsoftware.

Flere wipere anvender også en kombination af de to måder at ødelægge strukturen på. På den måde kan hackerne programmere wiperen til at gennemtvinge nedlukning af computeren, når wipingprocessen er overstået, hvilket i kombination med en ødelagt MBR betyder, at computeren ikke kan indlæse sit styresystem. Den gennemtvungne nedlukning kan anvendes i kombination af ødelæggelse af MFT'en, samt i kombination med wiping af filindhold.

Efter wiping af MBR/GPT eller MFT kan det altså som sagt være muligt at genskabe data. Det kan dog være tids- og ressourcekrævende, og i mange tilfælde vælger de ramte organisationer at udskifte det ramte hardware i stedet.

4. Beskyt dig mod wiper-angreb

Udgangspunktet for et effektivt cyberforsvar, der også reducerer risikoen for destruktive wiper-angreb, beror på implementering af en række grundlæggende sikkerhedstiltag. Sikkerhedstiltagene er også effektive overfor andre trusler som cyberspionage og -kriminalitet, hvor angrebsteknikkerne ofte er de samme. For nærmere beskrivelse af disse sikkerhedstiltag, henvises til CFCS' vejledninger "Cyberforsvar der virker" og "Reducér risikoen for ransomware" på CFCS' hjemmeside, og til de tekniske minimumskrav for statslige myndigheder på sikkerdigital.dk.

For at **forebygge** wiper-angreb, bør man bl.a.:

- have et opdateret overblik over sin organisations enheder, der er tilgængelige fra internettet.
- sikre at alle internetvendte systemer og tjenester holdes sikkerhedsopdateret.
- sikre at al fjernadgang sker med flerfaktor-beskyttede logins.
- etablere logning på alle internetvendte systemer og tjenester, og centrale interne tjenester.
- Segmentere klienter og systemer, så de kun tillader den nødvendige trafik, hvilket kan modvirke spredning af malware på organisationens netværk
- uddanne medarbejderne til bedre at kunne identificere og håndtere mistænkelige mails.
- beskytte særligt privilegerede konti og adgange med ekstra sikkerhed.
- sikre at alle klienter har en lokal firewall og opdateret end-point beskyttelse (antivirus/antimalware).
- sikkerhedsopdatere klienter og software.
- sikre at medarbejdere ikke har adgang til data eller systemer, der ikke er nødvendige for deres arbejde.
- tage backup af data, konfigurationer og systemer, som opbevares separat fra produktionsmiljøet. En kopi bør opbevares offline.
- teste genetablering af data og systemer.
- opdatere it-beredskabsplaner og øve dem. Vær i den sammenhæng opmærksom på, om it-beredskabsplanen tager højde for, at retablering efter et wiperangeb kan tage lang tid, såfremt mange klienter eller systemer skal retableres eller nyanskaffes.

For at **opdage** forsøg på wiper-angreb bør man bl.a. aktivt monitorere og handle på alarmer fra sikkerhedsprodukter og centrale logsystemer. IDS-systemer og netværks-monitorering kan yderligere supplere monitoreringen. Tegn på igangværende angreb kan f.eks. være:

- Phishing-mails
- Afvikling af malware på en klient
- Forsøg på udgående kommunikation til kendt skadeligt domæne
- Sletning af shadow copies
- Sletning af lokale logs
- Større antal filtransaktioner (sletning, skrivning, omdøbning)
- Ændringer til group policies
- Tilføjelse af scheduled task
- Forsøg på klient til klient kommunikation

Skulle skaden ske, er det vigtigt at **håndtere** hændelsen velovervejet og struktureret ved at:

- Isolere ramte klienter og netværkssegmenter fra det øvrige netværk, for at begrænse skadens omfang. Det gøres bedst ved at fjerne netværksforbindelsen fysisk eller logisk. Undgå at slukke ramte systemer, da det kan begrænse muligheden for at sikre beviser og analysere hændelsen.
- Aktivere beredskabsplanen, hvis nødvendigt, og følge dens procedurer.
- Søge ekstern assistance fra it-sikkerhedsfirma, hvis de nødvendige kompetencer til analyse, udbedring og genetablering ikke findes i egen organisation.
- Sikre at de udnyttede sårbarheder er afdækket og mitigeret, og at angrebets omfang er tilstrækkeligt afdækket, inden der påbegyndes gentablering fra backup. Det bør ligeledes sikres, at der kun retableres fra en backup fra før kompromitteringen fandt sted, så evt. sårbarheder eller adgange ikke også retableres.
- Indberette hændelsen til relevante myndigheder og i henhold til gældende lovgivning.