

PRESSEMEDDELELSE

PRESSEMEDDELELSE - Sådan ser et APT-hackerangreb ud

Pressemeddelelse · Udgivelse og medieindhold



Cybersikkerhedsfirmaet Bitdefender har efterforsket et hackerangreb af en APT-gruppe rettet mod en sydøstasiatisk regering. APT-grupper, Advanced Persistent Threat, er nogle af klodens mest kompetente hackere, og deres angreb gør brug af nogle ret så avancerede værktøjer. For at give en forståelse af, hvordan APT-grupperne arbejder, giver Bitdefender her et indblik i, hvordan et APT-angreb ser ud ud med den nye efterforskning som eksempel.

APT-grupper er nogle af de mest kompetente hackere i verden. Nogle af grupperne udfører deres kriminelle gerninger for profit, mens andre er statssponsorerede og angriber med et politisk motiv. Bitdefenders eksperter holder hele tiden øje med grupperne og deres ofre overalt på kloden, og efterforsker angreb for at opnå mere viden om de yderst kompetente grupper. Det er sådan en efterforskning, Bitdefender giver et indblik i her.

Beviser indsamlet af Bitdefenders eksperter viser, at et angreb blev indledt mod en sydøstasiatisk regering i november 2018. Beviserne er indsamlet fra ofrets computere og en række af dem peger på, at det var en kinesisk APT-gruppe, der stod bag angrebet.

En bagdør der giver fri adgang

Eksperterne kan ud fra beviserne se, at det første af hackernes værktøjer, *Chinoxy*, dukker op på ofrets systemer i november 2018. Der er ingen beviser for, hvordan hackerne har fået adgang, men da *Chinoxy* er en trojansk hest, er det ikke usandsynligt, at det er sket gennem et phishing-angreb, hvor det er lykkedes APT-gruppen at franske en person sine loginoplysninger, uden at vedkommende har opdaget det. Det kunne eksempelvis ske ved, at hackerne sendte en mail til personen med et link til en loginside til systemerne, der ligner den ægte vare. Forskellen er blot, at det er hackernes side, hvor de kan læse det brugernavn og kodeord, der bliver tastet ind. Personen ville derefter få enten en troværdig fejlmeddelelse og blive sendt videre til den rigtige loginside, eller med de indtastede oplysninger blive sendt videre og logger ind på den ægte side. På den måde undgår hackerne, at personen fatter mistanke.

Chinoxy blev brugt af hackerne til at lave en bagdør i ofrets systemer, der gjorde det muligt for APT-gruppen at få adgang uden ofrets viden og uden at være afhængig af det første, ukendte, adgangspunkt. Hvis det f.eks. var en persons loginoplysninger, så ville et opdateret kodeord betyde, at hackerne igen skulle franske en person sine loginoplysninger for at få adgang. Med en bagdør fik hackerne deres egen vej ind i systemerne. Adgang på hackernes egne vilkår er nødvendigt for dem, for at de kan opretholde et vedvarende angreb (*persistent*), som i dette tilfælde.

Det er blandt andet i *Chinoxy*, at eksperterne kan se, at programmets sprog er sat til kinesisk, hvilket peger på, at det er en kinesisk APT-gruppe, der står bag.

De første komponenter implementeres

Kort tid efter, at APT-gruppen havde fået *Chinoxy* installeret, brugte de bagdøren til at køre et andet stykke malware, *PcShare*, som injicerede processen *PcMain* ind i den legitime proces *logagent.exe* på computeren. Dette er en metode til at skjule malwaren, da *logagent.exe* normalt skaber trafik ved at sende logfejl fra *Windows Media Player*. Det gør det sværere at opdage hackernes lyssky aktiviteter, da trafikken fra den injicerede *logagent.exe* proces umiddelbart vil se normal ud. Dette er én af metoderne, der blev brugt

til at skjule hackerens tilstedeværelse. En anden metode var f.eks., at *PcShare* udgav sig for at være en del af *Microsoft Windows Update*.

PcShare kunne derefter bruges af hackerne til at udføre en lang række angreb, bl.a. fjernkontrol af den inficerede enhed, upload og download af filer og muligheden for at slette malware fra enheden. Med *PcShare* blev hackerne derfor i stand til at udføre kompleks cyberspionage.

Den 29. januar 2019 intensiverede hackerne deres angreb med malware-værktøjet *Ccf32*, der primært blev brugt til at indsamle data. *Ccf32* var kodet til at lave en skjult folder til sig selv, lede efter specifikke typer af filer, som malware derefter kopierede, komprimerede og gemte i den skjulte folder.

***FunnyDream* - en ubehagelig sofistikeret værktøjskasse**

Under arbejdet med at spore *Ccf32* igennem systemerne opdagede eksperterne endnu en bagdør, ud over *Chinoxy*. Bagdøren viste sig at være en del af den større malwareværktøjskasse *FunnyDream*. Beviserne peger på, at *FunnyDream* blev installeret i april 2019, hvorefter hackerne i de efterfølgende fem måneder fik kontrol med omkring 200 forskellige maskiner, som de kunne udføre en række komplekse angreb på vha. *FunnyDream*.

Ud over bagdøren, indeholdte *FunnyDream* en række specifikke malware-værktøjer:

- *FilePak* – malware udviklet til automatisk at indsamle filer efter en række specifikke forudsætninger. *FilePak* blev brugt til at finde og indsamle bestemte typer af filer, som hackerne var interesserede i, hvorefter den komprimerede de indsamlede filer til én samlet fil. Derefter tilslørede *FilePak* denne fils eksistens, så den ikke blev opdaget. Hackerne kunne så hente *FilePaks* indsamling gennem *FunnyDream*-bagdøren, når det passede dem.
- *ScreenCap* – er som navnet angiver et værktøj, der blev brugt til at tage skærbilleder. *ScreenCaps* skærbilleder blev gemt i et arkiv, der, ligesom med *FilePak*, tilslørede sig selv, for at undgå at blive opdaget. Hvert femte sekund tog *ScreenCap* et billede af ofrets skærm i et uendeligt loop, hvilket ganske enkelt betød, at skærmen var under konstant overvågning.
- *Keyrecord* – er en såkaldt *keylogger*, som hackerne brugte til at registrere alle tastaturanslag på ofrets system. Også *Keyrecord* overvågede konstant ofrets system.

- *FilePakMonitor* – en mere kompleks udgave af *FilePak*, der gav hackerne mulighed for selv at kontrollere indsamlingen af filer. Derudover scannede *FilePakMonitor* hele ofrets system, inkl. eksterne drev, igennem hver 12. time. Hvis en fil var blevet ændret siden sidste scanning, blev den indsamlet. Derudover sendte *FilePakMonitor* en besked til hackerne om, at der var indsamlet nye filer, hvorefter de kunne hentes.
- *TcpBridge* – blev brugt til at få adgang til ofrets interne netværk. TCP, *Transmission Control Protocol*, er en internetprotokol og er en fast del af nutidens internet. Igennem TCP er det muligt for forskellige maskiner at oprette forbindelse til hinanden gennem internettet, og med *TcpBridge* kunne hackerne selv styre, hvordan de ville forbinde deres egne *Command & Control*-servere (C&C), hvorfra de udførte deres angreb, med ofrets maskiner.
- *TcpTransfer* – gjorde det muligt for hackerne at forbinde deres C&C-servere med maskiner på ofrets interne netværk, der ikke havde adgang til internettet. Dvs. at hackerne kompromitterede ikke-internetforbundne maskiner ved at hacke en maskine, der var forbundet med internettet, hvorfra de kunne skabe forbindelse til maskiner på det interne netværk.
- *Md_client* – en bagdør, der gav hackerne endnu en mulighed for at få adgang til ofrets systemer.

Hackernes infrastruktur peger imod Kina

Bitdefenders eksperter har i beviserne fundet domæner og IP-adresser til hackernes C&C-servere. Derfor ved vi, at størstedelen af hackernes servere er placeret i Hong Kong (16), mens de resterende findes i Kina (1), Vietnam (1) og Sydkorea (1).

Normalt er C&C-servere i samme region som ofret ikke et tegn på, at hackerne nødvendigvis befinder sig samme sted. Men da denne regions internet er relativt restriktivt, så vil det være en stor fordel for hackerne at have deres egen infrastruktur placeret i samme region som ofrets for at undgå, at deres servers forbindelse til ofrets systemer vil blive set som suspekte. Var C&C-serverne placeret uden for regionen, ville det med al sandsynlighed have udløst ofrets sikkerhedsalarmer.

Dette, samt de fundne filer med kinesisk sprog og det faktum, at *Chinoxy* er kendt for at blive brugt af kinesiske hackere, betyder, at Bitdefenders eksperter har grund til at tro, at APT-gruppen har kinesisk oprindelse.

Angreb aktivt i næsten to år

Bitdefenders efterforskning fandt, at hackerne var aktive på ofrets systemer indtil september 2020, omend en stor del af C&C-serverne var inaktive på dette tidspunkt. De komplekse værktøjer, som hackerne har brugt, peger på omfattende færdigheder og opfindsomhed, når det kommer til at bruge et alsidigt værktøjssæt.

Ved at offentliggøre denne efterforsknings resultater håber Bitdefender at give et indblik i, hvor veludviklede og komplekse denne type angreb er, samt at kontekstualisere hvad det kan have af konsekvenser for organisationer at blive ramt af et angreb i denne skala.

Læs Bitdefenders whitepaper om efterforskningen her:

<https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf>

Online: <https://pressemeddelelse.dk/pressemeddelelser/pressemeddelelse-saadan-ser-et-apt-hackerangreb-ud/>

Pressemeddelelsen er videreformidlet af Pressemeddelelse.dk. Pressemeddelelse.dk er ikke ansvarlig for indholdet. Spørgsmål til indholdet rettes til Bitdefender.