Transcript

P. Starte litt opp med litt praktisk angående den statistikken du sendte oss, for der står det jo sånn om ETPRO TROJANER og alt mulig sånt. Er det sånn at dette er malware som er på pcene?
C. Når det står at det er trojaner så er det jo malware, da er det bevist malware
P. Er bevist malware ja, alt er bare en felles betegnelse på malware?
C. Nei men type trojaner, malware type trojaner.
P. har dere noen formening på hvordan disse trojanerne kommer på pcene til folk?
C. Vi har ikke dokumentert det, men sånn tipper det er enten via epost eller waterhole nettsider som sprer de. Stort sett de angrepsvektorene som brukes, uten at vi har registrert det da, men det er utifra hva leverandører og de som forsker på trussel etterretning de sier at det er stort sett sånn de ser de kommer inn. Så vil det jo være rart at de kommer inn på noen annen måte hos oss.
P. hvor lenge ca. er det de pleier å være på pcene før dere oppdager de?
C. Nei så fort de er på merkes de i trafikken som synes i statistikken dere har fått der
P. Og da går dere bare kjapt og sier nå må vi (Philip Lager lyd og tegn signaliserer kastes ut)
C. Hiver de av nett og kontakter brukeren det kommer helt ann på hvordan maskinen er, altså om det er maskin vi har kontroll på eller ikke om det er en server eller om det er en klient. Om det er en bring your own device eller drifta klient. Her er det litt mer komplisert linje å gå
P. Ok så hva er det dere gjør hvis det er en klient liksom, altså booter dere de av nettet liksom eller er det mer?
C. Spørs om det er bring your own device eller om det er drift av klient. Drifta klient har vi mulighet til å gå inn og sjekke det. Bring your own device har vi ikke noen annen mulighet enn kaste de av nett. Men som regel når det er coinmining varsler vi brukeren. Ber de kjøre noe antivirus programmer eller oppdatere maskinen deres

P. Unike signaturer fra dette er signatur fra den malware?
C. Det er forskjellige unike så har du jo de signaturene som har coinminer eller i seg og da er da antall. Så dette er da de unike signaturene vi ser og så har du da antall hver signatur har trigga på.
P. Men de antallet er det antallet med pc liksom eller om det?
C. Nei det er antall ganger den signaturen har trigget
P. men har dere noe tall på hvor mye ofte klienter eller hvor mange klienter som er, stadig blir brukt til mining på en måte?
C. Da må e hent ut ny statistikk, men ja du kan se det. Vi kan ta sortering på unike ip adresser
P. Har dere noe på hvor stort antall privat bruk av det og hvor mye som er liksom dette her er malware som?
C. det kan vi ikke skille på per nå
P. Men har dere noe tanker sånn cirka, sånn cirka hva fordelingen er?
C. Nei ikke per nå som jeg tør å si. Da må jeg sjekke datasettet først

P. Ja men. Ja men det er fult lovlig det ja
T. Ja det var hpc clusterne
C. Ja
T. Hvordan var det dere fant ut den ble misbrukt?
C. Kombinasjon av at hpc som lurte om vi kunne se på det og det var signatur som var trigga.
P. Ja ok, Hvordan fant derre ut at det var noen interne?
C. Det var jo lett, det er jo scheduling og det er jo logg på hpc cluster som kjører. Så da kan se hvem som starta prosess og da spore tilbake hvilken node den prosessen har gått på og så videre og videre
P. Og da har vedkommende sagt jeg gjorde det eller lignende?
C. Det utaler meg ikke noe om
P. Er det noe måte for dere å blokkere folk annet enn kaste de av nettet, fra kunne kjøre cryptominer på pc sine?
C. Kan gjøre grep i nettet, blokkere f.eks dns adresser som brukes til å rapportere ting og så videre også videre. Ting vi kan gjøre, men når det gjelder private utstyr så det jo litt begrensa. Annet enn å begrense nette deres
P. Hva er grunnen til at dere ikke har implementert noe slike tiltak?
C Fordi det er andre ting som brenner mer
P. Ja ok
C Så miner litt bitcurrent, det er ikke høyest på lista over problemmer
P. Hva tror du er oppfatningen blant dine kollega angående mining, er det folk vet det er ulovlig på en måte eller er det har ikke tenkt så mye over det og miner bare fordi det?
T. Trend eller?
C. Tro det er en trend folk hiver seg på ja, ihvertfall når det gjelder de som setter opp sjølv. Det er jo ikke ulovlig etter når du snakker ulovlig så er jo norsk lover, men brudd på regelverk tror jeg det ikke er mange som har tenkt over
P. Hva er måten dere for du snakket tidligere om at dere så mange av de walletsa som ble brukt var fra mørke siden av nettet?
C. der har du jo de som går etter trojan
P ja og der fordi hvordan ser dere at de går til disse walletsa. Er det bare fordi disse kjente malware sender til?
C. Altså du kan jo se hvilken wallet det sendes til og innholdet denne walleten er jo offentlig informasjon i hvert fall på bitcoin. Så kan se alle transaksjoner som går inn og ut av en wallet
P. Ja ok har dere noen tanker hvordan dere skal implemiter kryptomining i neste IT-reglement?
C. ja det er allerede, det er ikke spesifikt sagt noe om det, men det står svart på hvitt i reglement at det ikke får lov til å bruke NTNU infrastruktur til kommersiell virksomhet. Så lenge du tjener penger på det er det kommersiell virksomhet.
P. Er det noe folk tenker over?
C. Nei må må nok kjøre en liten innsida sak eller noe sånt få en liten kampanje rundt det på awarensen. Så reglemente dekker det det skal dekke
P. Har dere noen tiltak på mining på nettsider. Det er jo noe som ser ut som blir brukt en del?
T. Hvis du liksom stopper med reklame og så begynner med mining istedenfor

C. Der kan man gjøre ting på klienten og blokkere de javascriptene, selv en drifta client er det mange måter vi kan gjøre det på. Selve nettet kan blokkere de filene som lastes ned. Så får ikke kjørt den javascript fil på klienten
P. Igjen det blir nedprioritert fordi de ikke såpass spennende?
C Per nå ja
P. Er det like stor økning nå som det var før jul eller har det dabba en del av?
C. Det fortsetter
P. Det gjør det?
C Det øker ikke så veldig mye mer, men det fortsetter
T. Den økninga er det da gjort av den profesjonelle aktørene eller det folk setter frivillig opp minere?
C. Det er jo mest på den profesjonelle du ser den da, men ja det er nok en litt økning på som setter opp sjølv på grunn alt alle vg artiklene kan man vel si da. Hvordan bli rik på cryptomining, merker at folk prøver.
P. Dere hadde ikke sett noe tilfeller av brutforce på pc og server som ble installert cryptominere på etter de ble brutforca?
C Ikke som jeg kan huske nei
T. Ja er det noen regler på hva ansatt får lov å legge på serverne de f.eks har stående på kontoret sitt slike ting?
C. Nei ikke spesifikt som jeg kommer på så du har et sett med retningslinjer, men de er ikke ferdig vedtatt av styre enda. Og så er det da
P. Kommersiell bruk biten
T. Så det er liksom forsker på crypto
C. Vi har folk som forsker på crypto
T. Men det er sann at de satt de opp av nysgjerrighet og så glemte de at den var satt opp?
C. det skjer hele tiden, det er ikke bare med kryptominere
P. Har dere hadd noen tilfeller av type pcer på ciscolab at studenter har slengt cryptominere på de og bare latt de stå og gå?
C. Kan ikke huske at det har hvert noen på ciscolabe, men det er eksempel på det
P. Det er det ja
T. Har du lyst å komme med et eksempel eller?
C. Trenger ikke henge ut noen faggrupper
P. Sykepleierne?
C. Spesielt de, nei da
P. Fungerer adgangskontroll på de forskjellige clusterene deres bare visse folk som kan bruke det?
C. Må få en konto på de av de som administrer dette
P. Har du noe estimat på hvor mye penger det har kostet skolen?
C. Nei