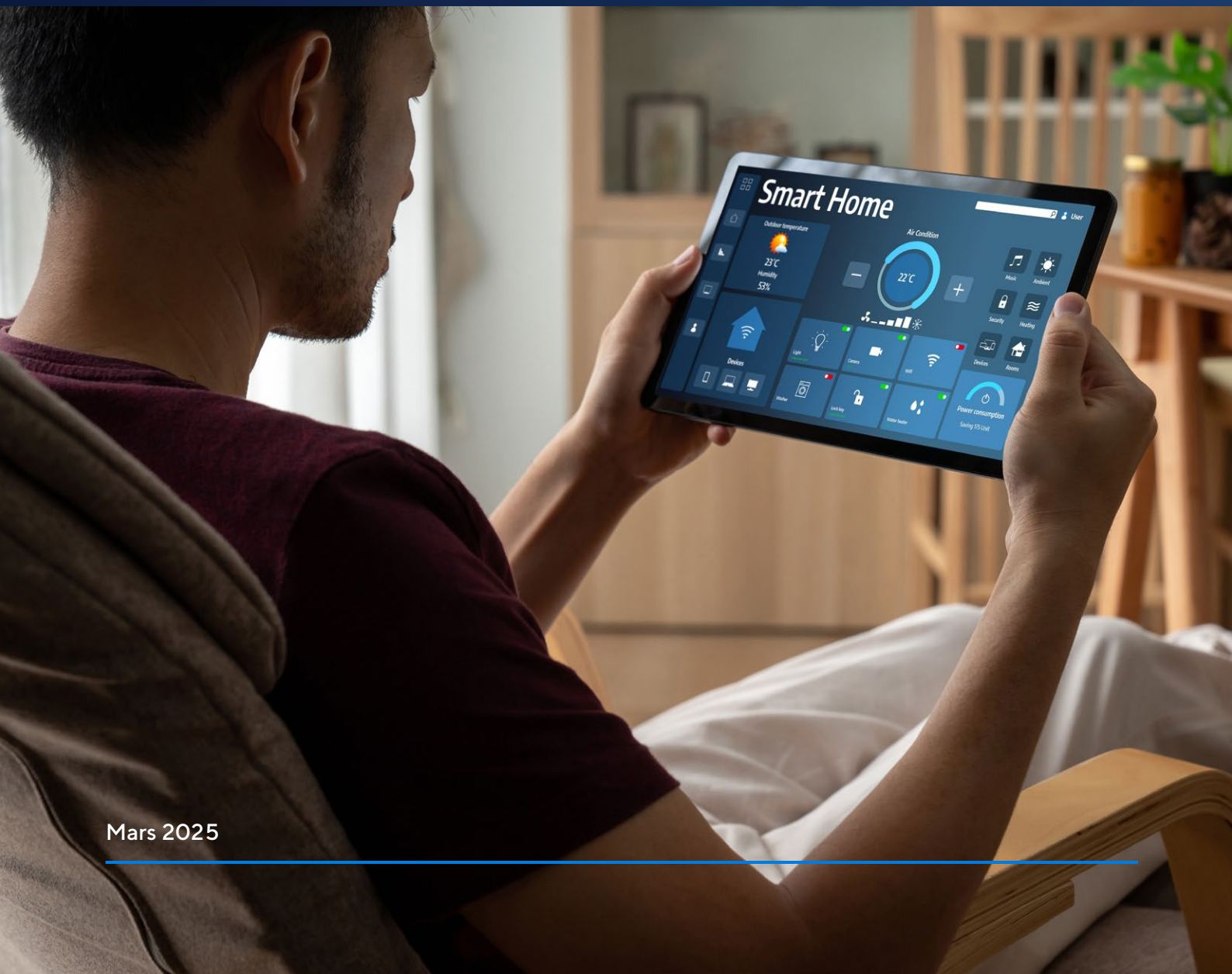
NATIONELLT CYBERSÄKERHETSCENTER

Hotaktörers dolda agerande på nätet



Mars 2025

Innehåll

Nationellt cybersäkerhetscenter NCSC

www.ncsc.se ncsc@ncsc.se

Hotaktörers dolda agerande på nätet

Metoder och tillvägagångssätt hos hotaktörer på cyberarenan förändras och utvecklas ständigt. Denna publikation syftar till att uppmärksamma ett tillvägagångsätt där statsstödda hotaktörer använder komprometterad infrastruktur för att bygga anonymiseringsnätverk. Dessa kan sedan utnyttjas för att agera i det fördolda i syfte att exempelvis genomföra kartläggning samt intrång och andra typer av cyberangrepp.

Det innebär att uppkopplade enheter såsom en hemmarouter, kan vara en del av ett stort anonymiseringsnätverk utan att ägaren är medveten om det. För den enskilda användaren är skillnaden knappt märkbar trots att enheten har blivit komprometterad eftersom routern, det uppkopplade kylskåpet, eller den smarta högtalaren fungerar som vanligt. Utåt blandar sig illegitim trafik från dessa komprometterade enheter med legitim trafik. Därför är detta ett problem som är svårt att identifiera och ger hot aktören stora möjligheter att agera dolt.

Bakgrund

I dagens uppkopplade samhälle har fler och fler elektroniska enheter (kylskåp, dammsugare, kameror med mera) fått funktioner för att kunna kommunicera via internet.

I takt med att fler enheter kopplas upp ökar risken för att tekniska sårbarheter upptäcks som kan utnyttjas för angrepp. Dessutom förblir många enheter uppkopplade långt efter det att tillverkaren slutat att erbjuda säkerhetsuppdateringar. Det gör att många sårbarheter aldrig åtgärdas och kan därför utnyttjas för angrepp.

De senaste åren har statsaktörer i ökande utsträckning använt komprometterade servrar, routrar och IoT-enheter för att skapa storskaliga anonymiseringsnätverk i syfte att kunna agera på dolt på internet.

Anonymiseringsnätverk

Vad är det?

Stora anonymiseringsnätverk är inget nytt fenomen och nyttjas idag av många användare världen över. Exempelvis har anonymisteringsnätverket TOR (The Onion Router) funnits sedan millennieskiftet. TOR låter användare surfa och kommunicera anonymt och används för både lagliga och olagliga aktiviteter. Medborgare i länder som tillämpar censur av internet är till exempel en stor användargrupp.

De anonymiseringsnätverk som är föremål för denna publikation byggs upp av statsunderstödda hotaktörer i syfte att genomföra cyberoperationer. Anonymiseringsnätverken består av ett antal olika noder. Första noden i kedjan är hotaktörens enhet, denna kopplas till en nod som fungerar som en sluss in i anonymiseringsnätverket och utgörs typiskt av en hyrd, virtuell server. Därpå följer ett stort antal noder som utgör lejonparten av anonymiseringsnätverket. Trafiken transporteras via ett urval av noderna vilket gör det svårt att följa trafiken tillbaka till ursprungskällan. Dessa noder kan utgöras av komprometterad infrastruktur eller hyrd infrastruktur. En av dessa noder fungerar som utgångsnod från nätverket. Sista noden i kedjan är offrets enhet.

I dessa anonymiseringsnätverk, finns det två utsatta parter, dels den som äger den hackade infrastrukturen, dels den som utgör det slutgiltiga målet. Majoriteten av de komprometterade enheterna finns hos privata användare och små- och medelstora företag som oftast är omedvetna om att deras enheter utnyttjas på detta sätt.

Hur används det?

Anonymiseringsnätverken används främst för att upprätta ett lager av förnekbarhet mellan aktören och aktörens mål. Trafiken som döljs i nätverken består framförallt av trafik för kartläggning, skanning och exploatering.

Ett vanligt tillvägagångssätt är att enheterna blir infekterade med skadlig kod som signalerar tillbaka till en kontrollserver. Från kontrollservern kan enheterna sedan administreras för att användas som noder i anonymiseringsnätverket. När det behövs kan kontrollservern skicka kommandon till de komprometterade enheterna för att exempelvis få information eller uppdatera programvaran.

Dessa tillvägagångssätt används troligen dels för att aktivera enheten som en nod för att slussa trafik i nätverket, men även för att infektera andra enheter och därmed utöka nätverket. Ofta används kända sårbarheter för att installera skadlig programvara på den komprometterade enheten.

Nätverken är designade för att skydda användarnas anonymitet genom att trafiken dirigeras med metoder som gör det komplicerat att följa in- och utgångsnoder. Nätverkens uppbyggnad gör det även enklare för aktörerna att smälta in med normal trafik, vilket stärker hotaktörernas möjlighet att dölja sina aktiviteter.

Exempel från verkligheten

Mellan 2020 och 2021 utfördes omfattande cyberangrepp mot mål över hela Europa med hjälp av sådana nätverk. Även om komprometterad infrastruktur har använts tidigare, var detta den första större kampanjen där främmande makt nyttjade denna metod. Angreppen var en del av en större kampanj som bedrevs av en kinesisk cybergruppering. Den använde ett nätverk av komprometterade routrar som i första hand tillhörde privatpersoner i hela Europa. En del av den infrastruktur som gruppen byggde upp fanns i Sverige, och i vissa fall skedde angrepp mot andra länder från routrar i Sverige.

Förebyggande arbete

Myndigheters agerande och relevant lagstiftning

Internationellt har brottsbekämpande myndigheter, privat sektor och cybersäkerhetsmyndigheter agerat för att möta hotet som dessa anonymiseringsnätverk utgör. Åtgärderna faller inom två huvudsakliga kategorier.

Den första är tekniska motåtgärder, där framför allt amerikanska myndigheter efter domstolsbeslut på stor skala oskadliggjorde den skadliga programvaran som angriparna använde sig av. Amerikanska myndigheter uppdaterade även brandväggsregler för att försvåra liknande angrepp.

Den andra kategorin är medvetandehöjande åtgärder där svenska och internationella myndigheter gått ut med information kopplat till hotaktörernas agerande samt teknisk information som kan nyttjas av it-säkerhetsteam för att söka igenom sin it-miljö efter tecken på intrång (eng. indicators of compromise, IoC).

Två EU-regleringar av särskild relevans för området är Cybersäkerhetsakten (2019/881) och Cyberresiliensakten (2024/2847). Dessa regleringar kan bidra till att möta hotet från de anonymiseringsnätverk som beskrivs i denna publikation. De innebär exempelvis krav på tillverkare av hård- och mjukvara att hantera sårbarheter under produktens livscykel och underlättar för konsumenter och verksamheter att avgöra vilka produkter som håller en tillfredsställande cybersäkerhetsnivå.

Det viktigaste förebyggande arbetet utförs dock av dig som äger en produkt som kan riskera att komprometteras och användas i ett anonymiseringsnätverk av den typ som beskrivs ovan.

Upphandling och inköp

En nyckel i att hantera hotbilden som beskrivs i denna publikation är livscykelhantering för uppkopplade produkter i den egna it-miljön eller i hemmet. Det innebär i praktiken att redan i samband med upphandling och inköp göra en bedömning av hur produkten ska hanteras funktions- och säkerhetsmässigt under dess livslängd. En sådan bedömning och hanteringsplan har många aspekter och behöver anpassas utifrån sammanhanget.

För verksamheter bör grunden för att bedöma detta vara den egna riskbedömningen och informationsklassningen. När ny it-utrustning köps in behöver upphandlingsprocessen inkludera livscykelperspektivet där leverantörens plan för support, uppdateringar och uppgraderingar kontrolleras för att stämma överens med verksamhetens behov.

Privatpersoner bör endast köpa utrustning från tillverkare och återförsäljare som är etablerade. Undersök om tillverkaren har en historik av regelbundna uppdateringar. Privatpersoner bör även sträva efter att köpa uppkopplade enheter med anpassningsbara säkerhetsfunktioner.

Rekommendationer

För större organisationer med utvecklad förmåga att hantera olika former av hot inom cyberdomänen, kan de anonymiseringsnätverk som beskrivs i denna publikation kräva ett nytt förhållningssätt i säkerhetsarbetet. Detta blir tydligt i fråga om IoC:er. Dessa utgörs inte sällan av ip-adresser som använts av angriparen. I fallet med anonymiseringsnätverken så omsätts noderna regelbundet, vilket gör att en ip-adress snabbt blir inaktuell i exempelvis blocklistor. Istället behövs en bredare ansats som innefattar en större uppsättning av indikatorer.

För mindre organisationer och privatpersoner kan det vara utmanande att hantera denna hotbild. En bra utgångspunkt för detta kan vara de säkerhetsåtgärder som NCSC-SE tillhandahåller på sin webbplats. Det handlar dels om rekommenderade säkerhetsåtgärder för organisationer, dels om åtgärder för ett säkrare, digitalt privatliv.

Bland dessa är vissa åtgärder mer relevanta för organisationer för att hantera den aktuella hotbilden. Att installera säkerhetsuppdateringar och att säkerställa förmågan att upptäcka it-säkerhetsincidenter är grundläggande. Att förvalta behörigheter genom att exempelvis byta standardlösenord samt att inaktivera oanvända funktioner är också relevanta åtgärder. Om tillverkaren av en produkt aviserar att den inte längre kommer att ta emot säkerhetsuppdateringar bör den bytas ut som en del av verksamhetens livcykelhantering.

Som privatperson bör fokus ligga på att hålla uppkopplade enheter uppdaterade genom automatiska uppdateringar, att överväga om alla smarta enheter i hemmet behöver vara uppkopplade mot internet samt att säkra identifiering och lösenord. Överväg att koppla bort eller byta ut en smart enhet om en sårbarhet blir känd i dess programvara som tillverkaren inte erbjuder en säkerhetsuppdatering för. Byt även ut standardlösenord på smarta enheter samt namn på trådlösa nätverk och smarta enheter.

För mer information och kontakt
www.ncsc.se och ncsc@ncsc.se

Nationellt cybersäkerhetscenter NCSC

NATIONELLT CYBERSÄKERHETSCENTER