Datorexperten i grå hatt – både polis och skurk

Gråhattarna arbetar i gränslandet mellan laglig och kriminell datorverksamhet

ILLUSTRATION: CAMILLA LAGHAMMAR

Under våren utspelades ett ordkrig mellan amerikanska myndigheter och den multinationella datorjätten Apple. I det uppmärksammade fallet beordrades Apple av den amerikanska federala utredningsbyrån FBI att utveckla en så kallad bakdörr för att låsa upp en I-Phone som tillhörde Rizwan Farook, den avlidna förövaren av terrordådet i San Bernardino i Kalifornien i december förra året.

Apple vägrade dock att hjälpa FBI, då det skulle innebära att Apple var tvunget att kringgå säkerhetsåtgärderna i sin egen produkt för att låsa upp mobilen. Flera andra IT- och datorleverantörer slöt upp på Apples sida och hävdade att om regeringar skulle kunna beordra leverantörer att kringgå sina säkerhetssystem, så skulle det innebära allvarliga kränkningar av den personliga integriteten för övriga användare världen runt.

För att tvinga Apple att samarbeta, stämde FBI företaget inför domstol. Fallet kom dock aldrig så långt. Precis innan rättegången skulle börja, gick FBI ut med information att man lyckats bryta sig in i den låsta mobilen med hjälp av en hemlig tredje part. Sedan dess har spekulationer florerat om vem denna tredje part kan ha varit. Flera insatta analytiker menar att det rör sig om så kallade gråhattar.

Sammanfattat

- Gråhattar, grey hat hackers, är datorexperter som arbetar i gränslandet mellan laglig och kriminell verksamhet.
- De känner den underjordiska delen av branschen och kan hjälpa till att komma åt brottslingar.
- Man misstänker att de också begår egna brott
- Sannolikt använder FBI gråhattar för att komma åt verksamhet de vill stoppa.

Datorexperter i gråzonen

Några har kanske hört uttrycket, men vad är egentligen en gråhatt? Inom datasäkerhetsvärlden används begreppen vithatt och svarthatt för att särskilja mellan datorexperter som håller sig till den lagliga ”vita” sidan, och deras ▶

kriminella motparter som håller på med ljusskygga verksamheter. Mellan båda dessa miljöer finns dock en stor grupp av hackare. Dessa kallas för gråhattar (grey hat hackers).

Cyberkrigets legosoldater

Definitionen av vad som är en gråhatt varierar en del. Det kan handla om en datorexpert som sköter säkerheten för en bank eller ett företag på dagarna men är delaktig i idealistiskt motiverade datorintrång på fritiden, så kallad hacktivism. Andra betraktar gråa hattar som cyberkrigets legosoldater som tar emot uppdrag från vem som helst som erbjuder intressanta utmaningar med tillräckligt mycket betalt.

”Det som förut var löst sammansatta grupper av idealister och småkriminella, har vuxit till välorganiserade verksamheter som i många fall har kopplingar till stater och globala storbolag.”

Datasäkerhetsvärlden är något av vilda västern och det är inte bara hattfärgen som skiljer hjältarna från skurkarna. Det är väldigt svårt att mäta säkerhet i ett datorsystem, och det är nästan omöjligt för uppdragsgivare att bedöma kompetensen och erfarenheten bland säkerhetsexperter. Dessutom förändras tekniken så fort att det är väldigt lätt att halka efter kunskapsmässigt. Det är just detta som gör gråhattar så värdefulla. De kan verka i framkant av den lagliga marknaden men har samtidigt bra insyn och kontakter i den underjordiska delen av branschen.

En bra affär

Ett franskt företag som heter Vupen visade sig vara en enfant terrible när de 2011 för första gången visade upp hur de kunde bryta sig in i Google Chromes webbläsare, men samtidigt vägrade lämna över information till Google om hur attacken fungerade.

Vupen har specialiserat sig på att sälja datorattacker, så kallade zero-dag attacker, fast med en tveksam affärsstrategi. Metoden för attackerna som de utvecklar hemlighålls och säljs till högstbjudande, oavsett om det är till den leverantör som har blivit utsatt för attacken eller till någon annan aktör med andra agendor.

NSA en av kunderna

Vupen har haft både den amerikanska nationella säkerhetsmyndigheten NSA och den tyska motsvarigheten BND som kunder. Företaget har varit helt öppet med att de sålt zero-dag attacker till kunder inom underrättelseverksamhet, storbolag och försvarsindustrin.

Under 2015 ansökte Vupen om konkurs men ombildades till den lite mer rumsrena nyskapelsen Zerodium. Företaget köper numera upp programkod för att kunna utföra attacker för lukrativa ”hittelöner”,och sedan sälja dessa vidare till uppdragsgivare.

Zerodium är långt ifrån den enda aktören på marknaden. Andra kända zero-dagmäklare är Netragard och Endgame. På bara ett fåtal år har stämningen i datasäkerhetsvärlden förändrats en hel del. Det som förut var löst sammansatta grupper av idealister och småkriminella, har vuxit till välorganiserade verksamheter som i många fall har kopplingar till stater och globala storbolag.

Anlitas i brottsbekämpning

I ett uppmärksammat fall 2013 fällde amerikanska FBI den anonyma svartmarknadstjänsten Silk Road. Denna underjordiska marknad fanns tillgänglig från anonymiseringstjänsten Tor, och blev känd för att tillhandahålla en helt laglös försäljning åt världens största nätdrogshandel för sin tid. En del av Silk Roads framgång låg i att de till skillnad ifrån andra liknande verksamheter inte blåste sina kunder på pengar och dessutom motarbetade brott som ansågs ha direkta offer. Succén slutade dock abrupt när

Intressanta länkar

FBI betalar miljoner för att bryta sig in I-Phone.
www.reuters.com/article/us-apple-encryption-fbi-idUSKCNoXI2IB

Företaget Netragard har som slogan ”Vi skyddar dig från sådana som oss”.
www.netragard.com

Rumsrena datorattacker på beställning.
https://www.zerodium.com/

Sveriges militära underrättelse- och säkerhetstjänst Must utvecklar offensiv datasäkerhetsförmåga.
www.svt.se/nyheter/inrikes/sverige-far-nytt-militart-cyberkommando

Vissa betraktar gråhattarna som cyberkrigets legosoldater som tar emot uppdrag från vem som helst som erbjuder intressanta utmaningar med tillräckligt mycket betalt.”

mannen som tros vara grundaren till Silk Road, Ross Ulbricht, spårades upp och dömdes till livstids fängelse.

Men metoderna som användes för att spåra upp Ulbricht har varit omtvistade och kontroversiella. Kända säkerhetsexperter som tidningen Wireds Andy Greenberg och forskaren Nicolas Weaver har uttalat misstankar om att FBI, för att kunna få fast Ulbricht, måste ha anlitat hackare utanför USA för att bryta sig in i tjänstens servrar. Det skulle vara på det sättet FBI lyckades identifiera kopplingen mellan tjänsternas servrar och Silk Roads huvudman samt hans innersta krets.

Mer organiserat

I Sverige har den militära underrättelse- och säkerhetstjänsten Must börjat utveckla möjligheten att bedriva offensiva insatser mot datorsystem. Man kan lätt ana att rekryterings- och utbildningsprocesser för sådana grupper och förband måste vara knepig då den troligen kunskapsmässigt mest intressanta kandidaten skulle passa bra i en grå hatt.

Att staten kan ha en god förmåga att möta datorattacker anses viktigt idag, inte minst eftersom oförutsägbara länder som Nordkorea lägger betydande resurser på offensiva datorförband, så kallade cyberkommandon.

I dagens samhälle är vi som individer beroende av att ständigt vara uppkopplade. Detsamma gäller tjänsterna vi använder och i ännu högre grad den kritiska infrastrukturen. Sannolikt kommer denna utvecklingstrend bara bli starkare i framtiden. Därför är det viktigt att våra samhällsfunktioner och lagstiftningen inte halkar efter vad gäller datasäkerhet, utan istället prioriteras för att kunna öka beredskapen för det myrornas krig som utspelar sig i etern omkring oss. I den kampen är de verkliga hjältarna antagligen minst sagt grå eminenser.

Nicholas Honeth
Industriella informations- och styrsystem, KTH