Hvordan kinesiske etterretningsoffiserer styrer sine kilder

Hvordan kinesiske etterretningsoffiserer styrer sine kilder: Innsidetrusselen i praksis

I en stadig mer kompleks og globalisert verden står selskaper overfor utfordringer knyttet til industriell spionasje og innsidetrusler. Sikkerhetsselskapet Árvakr ønsker med denne artikkelen å belyse hvordan kinesiske etterretningsoffiserer opererer for å kontrollere sine kilder og hvilken betydning dette har for virksomheter. Vi bruker her saken om Xu Yanjun, en etterretningsoffiser fra det kinesiske Ministry of State Security (MSS), for å illustrere disse metodene og risikofaktorene.

Rekruttering og relasjonsbygging

Historien om Arthur Gau, en flyingeniør fra Honeywell International Inc., viser hvordan kinesiske etterretningsaktører systematisk utvikler relasjoner over tid. Det startet med en tilsynelatende uskyldig kontakt fra en administrator ved Nanjing University of Aeronautics and Astronautics (NUAA), kjent som "Little Zha." Over årene sørget Zha for at Gau fikk betalte reiser og eksklusive opplevelser, noe som etablerte en uformell gjensidig forståelse.

Dette er en klassisk metode brukt av etterretningstjenester: oppbygging av tillit og gjentatt kontakt over tid. Så lenge ingeniøren kun holdt akademiske foredrag, virket det harmløst. Men da Zha foreslo at Gau kunne tjene penger på å dele spesifikk teknologi, avslo han, og kontakten opphørte.

Da Zha dukket opp igjen i 2014, hadde han med seg en ny aktør: Xu Yanjun, en MSS-offiser som spesialiserte seg på flyteknologi. Sammen bygget de videre på den tidligere etablerte relasjonen for å manipulere Gau til å dele sensitiv informasjon.

Motivert til å samarbeide

En viktig del av hvordan kinesiske etterretningsoffiserer styrer sine kilder er gjennom incentivstrukturer som skaper forpliktelser. I Gaus tilfelle startet det med gaver og betalte turer, men det utviklet seg raskt til penger. Xu overleverte ham 40.000kr i kontanter etter et møte, og Gau følte seg deretter forpliktet til å dele tekniske PowerPoint-presentasjoner med sensitive algoritmer og designinformasjon fra Honeywell.

Dette er en vanlig strategi. Ved å gi en kilde en mindre sum penger først, etableres en psykologisk kontrakt hvor kilden føler en gradvis økende forpliktelse. Dette kombinert med langsiktig relasjonsbygging og sosial manipulasjon gjør det vanskelig for individet å trekke seg ut av situasjonen.

Teknisk og menneskelig utnyttelse

Xu benyttet seg ikke bare av tradisjonell menneskebasert innhenting (HUMINT), men også av tekniske metoder for å innhente informasjon. Dette kom tydelig frem i hans

forsøk på å infiltrere Safran Aircraft Engines i Frankrike. Han instruerte sin medhjelper, Tian Xi, om å plante et trojansk virus på en fransk ingeniørs datamaskin.

Dette samspillet mellom HUMINT og cyberoperasjoner er karakteristisk for kinesisk etterretning. De opererer ikke i siloer, men kobler sammen menneskelige kilder med tekniske angrep for å maksimere informasjonsinnhenting.

Håndtering og kontroll av kilder

Xu Yanjun benyttet flere metoder for å styre sine kilder, inkludert:

- Falske akademiske invitasjoner: Han brukte universiteter som en front for etterretningsarbeid, hvor inviterte forskere og ingeniører ble utsatt for manipulasjon.
- Identitetsendringer: Han opererte under aliaser som "Qu Hui" og brukte falske visittkort for å skape en tilsynelatende legitim fasade.
- Gradvis eskalering av forespørsler: Han startet med generelle akademiske spørsmål, men beveget seg sakte mot spesifikke tekniske forespørsler for å unngå å vekke mistanke.
- Bruk av WeChat og Gmail: Xu kommuniserte med kilder via personlige e-poster og kinesiske meldingstjenester for å omgå vestlige sikkerhetstiltak.

Indikasjoner på innsidetrussel

Denne saken gir unike innsikter i hvordan kinesiske etterretningsoffiserer styrer sine kilder. Viktige indikasjoner som bedrifter bør være oppmerksomme på inkluderer:

- Endret atferd hos ansatte: Plutselige endringer i arbeidstider, økt interesse for sensitiv informasjon eller uklar kommunikasjon med eksterne aktører kan være røde flagg.
- Reiser til høyrisikodestinasjoner: Gjentatte, uoffisielle reiser til land med kjente etterretningsaktiviteter, spesielt der dekkhistorier om "akademiske foredrag" eller "samarbeid" brukes.
- Mottak av uventede gaver eller pengeoverføringer: Små summer eller gaver kan være tidlige forsøk på å bygge en forpliktelsesrelasjon.
- Deling av ikke-offentlige dokumenter: Selv "ikke-sensitive" dokumenter som deles utenfor normale arbeidsrutiner kan være en del av en større informasjonsinnhentingsstrategi.

Hvordan bedrifter kan beskytte seg

For å minimere risikoen for innsidetrusler er det avgjørende at bedrifter etablerer proaktive sikkerhetstiltak:

- Opplæring og bevisstgjøring: Ansatte bør regelmessig informeres om risikoene ved etterretningsoperasjoner og sosial manipulasjon.
- Sterk tilgangskontroll: Strenge begrensninger på hvem som har tilgang til sensitive data og teknologi kan redusere eksponeringen for potensielle innsidetrusler.

- Sikkerhetsklareringer og bakgrunnssjekker: Regelmessige sikkerhetsgjennomganger av ansatte, spesielt de med tilgang til kritisk informasjon.
- Samarbeid med myndigheter: Nært samarbeid med nasjonale sikkerhetstjenester og spesialiserte sikkerhetsselskaper kan gi verdifull innsikt og støtte i å avdekke og forhindre innsidetrusler.

For virksomheter er dette en viktig påminnelse om at innsidetrusler ikke bare kommer fra opportunistiske ansatte, men ofte er resultatet av langvarige og sofistikerte operasjoner utført av statlige aktører. Ved å forstå disse metodene og implementere effektive sikkerhetstiltak kan bedrifter bedre beskytte sine verdier mot fremtidige trusler.