Projektnummer/Project no
E72787
Kund/Customer
Försvarsmakten
FoT-område
Operationer i cyberdomänen

Handläggare/Our reference
David Lindahl
Datum/Date
2019-12-06
Memo nummer/number
FOI Memo 6963

Omvärldsbevakning statsattribuerade cyberoperationer 2019

Sändlista/Distribution:

[Sändlistan dold]

1. Inledning

Detta memo innehåller ett urval av cyberincidentbeskrivningar som rapporterats i media och andra öppna källor under 2019.

Memot är skrivet som en del av det Försvarsmaktsfinansierade projektet Cyberoperationer 2019. Mottagare är Försvarsmakten och de personer kopplade till Försvarsmakten som arbetar med skydd mot, och forskning kring, cyberoperationer.

2. Påstådda statsoperationer hittills under 2019

Den amerikanska tankesmedjan Council of Foreign Relations har sedan 2005 uppdaterat en databas över förmodat statssponsrade cyberincidenter som framkommit i öppna källor. Nedan följer de incidenter som registrerats i databasen mellan januari och november 2019 och som vi kunnat verifiera i media. För några poster i databasen fanns inte längre verifierbara källor, andra poster hade beskrivningar av incidenten som inte stämde med källorna. (Källuppgifterna hade uppdaterats eller feltolkats). Vi har valt att inte ta med dessa exempel. Notera att rubrikerna i punkterna nedan är påståenden som framkommit i media och att attribueringen ofta är svag eller baserad på rena misstankar.

Totalt kunde vi verifiera 31 incidenter som i media eller andra öppna källor attribuerats till statsaktörer. Av dessa är 27 troligen informationsstöld eller underrättelseverksamhet[1]. Fyra kan antas haft som mål att skaffa sig tillträde till system för att kunna utföra andra angrepp. Fyra skulle kunna vara utförda för att få en politisk verkan. Två angrepp var enligt medias källor direkt riktade mot att störa tjänst eller verksamhet. Ett hade som syfte att förstöra information, eller datoriserad utrustning. Notera att flera av angreppen faller in under mer än en kategori. Vi har i slutet av incidentbeskrivningarna nedan skrivit ut våra slutsatser kring angriparens syfte(n).

9/1, **DNS Hijacking** (Muks Hirani, 2019). En angripare manipulerade DNS-uppslagningen på Internet för att dirigera om trafik till angriparens egna servrar. Offren var bland annat Libanons finansdepartement, Förenade Arabemiratens Telekommyndighet (Motsvarande svenska PTS) och Libanesiska Middle East Airlines, som alla fick sin inkommande eposttrafik omstyrd. FireEye attribuerar angreppet till Iran baserat på att alla offer hade information som var värdefull för Iran, men andra utredare, som till exempel Talos blogg (Warren Mercer, u.d.) poängterar att inga tekniska bevis länkar Iran till angreppet. Syfte: *Underrättelseverksamhet.*

18/1, **Riktad phishing mot USA:s Demokratiska parti.** (Volz, 2019) Denna händelse skedde under 2018 men offentliggjordes först i januari 2019. Enligt de nya uppgifterna ska angreppen mot Demokraternas parti som skedde under 2016 års valkampanj ha fortsatt under 2017 och 2018 med riktad phishing. Syfte: *Underrättelseverksamhet*.

30/1, **Spionage mot IPhone iMessage service** (NBC, u.d.). Den 30 januari publicerades information av Reuters att en cyberenhet i Förenade Arabemiraten, kallad Raven, hade använt verktyget Karma för att hämta ut information ur hundratals Iphones tillhörande intressanta personer. Spionaget ska ha skett under 2017 och 2018 och rapporterades av före detta anställda från Raven. Bland offren ska bland andra Qatars Emir Sheikh Tamim bin Hamad al-Thani, Omans utrikesminister Yusuf bin Alawi bin Abdullah och Turkiets före detta vice premiärminister Mehmet Şimşek finnas. Raven bemannas enligt bloggen Lawfare (Chesney, u.d.) av amerikansk personal som tidigare arbetat inom USA:s försvar och

[1] Det är viktigt att hålla i minnet att underrättelseverksamhet inte enbart är spionage mot statshemligheter. Det är också insamling av information för att ha som beslutsunderlag eller möjliggöra andra operationer, både cyberoperationer och konventionella. Det är alltså svårt att från en enskild incident avgöra syftet med informationsinsamlingen.

underrättelsemyndigheter och som nu rekryterats på den öppna marknaden. Enligt samma källor ska gruppens vapen, Karma, ha köpts från en privat leverantör snarare än att ha utvecklats internt. Syfte *Underrättelseverksamhet*.

31/1, **Riktad phishing mot tankesmedjor** (Maza, 2019). Fancy Bear, också kända som Strontium, är en hackergrupp som länkats till Ryssland. Enligt medieuppgifter använde de sig av riktad phishing och falska webbsidor för att lura tankesmedjemedlemmar i USA och Tyskland att lämna ut sina inloggningsuppgifter. Syfte: *Underrättelseverksamhet*.

6/2, **Cloudhopper, Informationsstöld från Visma** (Stubbs, Reuters, 2019). Konsultfirman Visma i Norge blev angripna av APT10, en hackergrupp associerad med Kina, under kampanjen som fick namnet Cloudhopper. Målet tros ha varit att komma åt Vismas kunduppgifter, men angreppet upptäcktes på ett tidigt stadium och kunde stoppas. Cloudhopper drabbade även svenska företag men endast det norska angreppet har tagits med i databasen (Campanello, Reuters: Ericsson drabbades av Kinas hackerattack Cloud Hopper, 2019) (Campanello, USA åtalar två kineser för cyberattacken Cloud Hopper som drabbade Sverige, 2018). Syfte: *Underrättelseverksamhet*.

22/2, **Babyshark-angrepp, riktad phishing mot tankesmedjor och University of California**. Angriparen använde en falsk identitet som tillhör en kärnfysiker för att kontakta personer som sysslade med Nordkoreafrågor. Palo Alto Networks Unit 42 anser att angreppet är en del av kampanjen Stolen Pencil och att modus operandi tyder på att den utförts av nordkoreanska angripare (New BabyShark Malware Targets U.S. National Security Think Tanks, 2019). Syfte: *Underrättelseverksamhet*.

27/2, **USA medger angrepp mot Internetforskningsmyndigheten** (Nakashima, 2019). Under valet 2018 ska USA:s Cyber Command med hjälp av underrättelsedata från NSA ha stängt ner internetförbindelserna för det ryska företaget Агентство интернет-исследований, ”Internetforskningsmyndigheten”, en organisation som via Internet utövar olika typer av dold politisk påverkan[2]. Den finansieras av oligarken Yevgeny Prigozhin som har nära band till Putins administration. USA ska ha agerat för att förhindra att ryska intressen skulle kunna blanda sig i USA:s val. Syfte: *Störning av verksamhet*.

5/3, **Leviathan angriper 27 universitet** (Price, 2019). Leviathan, en hackergrupp som associerats med Kinas regim, angrep 27 universitet i USA, Kanada och Sydostasien, däribland University of Hawaii, Massachusetts Institute of Technology (MIT) och University of Washington. Angriparna letade efter information om marinteknisk forskning kopplad till militära ändamål. Syfte: *Underrättelseverksamhet*.

12/3, **Indonesiens röstdatabas utsatt för hackerangrepp** (Jessica Damiana, 2019). Arief Budiman, chef för Indonesiens nationella valkommission uttalade sig i en rapport att kinesiska och ryska hackare hade angripit databasen över röstberättigade för att ”modifiera och manipulera” den för att skapa falska röstberättigade identiteter. Senare meddelade han att det ”inte handlade om Ryssland eller Kina” utan att angrepp hade kommit både utifrån och inifrån landet. Syfte: *Underrättelseverksamhet och möjligen påverkansoperation*.

2/4, **Storbritanniens postverk och företag angrips** (Hughes, 2019). Iran anklagas av brittiska National Cyber Security Centre för att ha angripit företag och myndigheter i Storbritannien och stulit persondata och kontouppgifter för tusentals anställda. Syfte: *Underrättelseverksamhet*.

4/4, **Bayer Pharmaceuticals angrips av Wicked Panda** (Stone, German drug giant Bayer breached by Chinese hacking group Wicked Panda: report, 2019). Den tyska läkemedelskoncernen Bayer Pharmaceuticals hittade skadlig kod inne i sina nätverk. Vid undersökning visade sig denna kunna kopplas till Wicked Panda, en hackergrupp som tidigare slagit till mot spelbolag och mot företag vars information har intresserat Peking. Företaget hävdar att trots intrånget fanns inga spår av informationsstöld. Syfte: *Underrättelseverksamhet*.

[2] Organisationen beskrivs regelbundet i media och av säkerhetsfirmor som ”en trollfabrik”

15/4, **Amnesty Internationals Hong Kong-kontor angrips** (International, 2019). Enligt Amnesty International försökte angripare från kinesiska staten ta sig in i deras nätverk och hämta ut information. Syfte: *Underrättelseverksamhet.*

6/5, **Gothic Panda, använder NSA-tillverkade vapen** (Symantec, 2019). Enligt en Symantecrapport hade Gothic Panda, en hackergrupp kopplad till kinesiska staten, tillgång till de vapen som Shadow Brokers[3] stal från Equation Group[4] minst ett år innan vapnen läcktes i samband med att Microsoft släppte säkerhetspatchar för dem (Dobos, 19). I rapporten avslöjar Symantec inte vem som var målet för angreppen, som ska ha ägt rum i september 2016, närmare än att det rör sig om en ”educational institution in Hong Kong” (Symantec, 2019). *Okänt syfte.*

13/6, **Demonstranters kommunikationsappar hackas eller störs** (Paul Mozur, 2019). Under demonstrationerna i Hong Kong har kommunikations- och sociala medieappar blivit utsatta för olika typer av angrepp och störningar vid flera tillfällen. (Inte enbart under den 13/6). LIHKG, ett socialt forum, drabbades av flera utdragna DDOS-angrepp från datorer inifrån fastlandskina (Banjo, 2019), Även Telegram, en krypterad meddelandetjänst, har störts ut vid flera tillfällen och WhatsApp har använts för att sända skadlig kod till demonstranter innehållande spionprogramvara. Council of Foreign Relations har listat Kina som angripare i sin databas, men vi har inte hittat någon annan referens till Kina som angripare. Syfte: *Påverkansoperation, störning av verksamhet.*

22/6, **USA:s Cyber Command angriper Iran** (Julian E. Barnes, 2019). Enligt flera nyhetsmedier utförde USA ett cyberangrepp mot Iran som en respons på att Iran skjutit ner en UAV som tillhörde USA. Enligt flera medier slog angreppet ut de missiler och ledningssystem som hade använts för att skjuta ner UAV:n (The Guardian, 2019). Syfte: *Påverkansoperation, sabotage*.

25/6, **Operation Soft Cell angriper telebolag och kinesiska dissidenter** (Mor Levi, 2019). Sedan 2017 har en angripare som identifierats som APT10, en hackergrupp länkad till Kinas regim, infiltrerat åtminstone tio teleoperatörer och stulit information. Angriparen har hämtat ut metadata om olika abonnemang och koncentrerat sig på specifika individers samtalslistor, cellanslutningar, SIM-kort och hårdvara (Greenberg, 2019). Angreppet var enligt media så avancerat och framgångsrikt att de vid åtminstone ett tillfälle lyckades skaffa sig tillräckliga rättigheter för att konfigurera ett eget VPN inom teleoperatörens nät utan dennas vetskap. Syfte: *Underrättelseverksamhet.*

27/6, **Yandex angrips med Regin** (Christopher Bing J. S., 2019). Yandex, ett företag som driver ett antal Internettjänster, från epost till internetsökningar, angreps med hjälp av Regin. Ett cybervapen som länkats till underrättelsetjänster som samarbetar i det så kallade FiveEyes-samarbetet bestående av USA, Storbritannien, Australien, Nya Zeeland och Kanada. Enligt Yandex försökte angriparna leta upp information kring hur Yandex verifierar användarkonton, men lyckades inte med angreppet. Syfte: *Underrättelseverksamhet.*

24/7, **Tyska företag angrips med Winnti** (Schuetze, 2019). BASF, Siemens, och Henkel är några av företagen angrips under incidenten. Winnti används av en del källor som ett verktygsnamn (Medium , 2019) och av en del källor som namnet på den hackergrupp som använder det (Tartare, 2019). Angreppet var ett försök att infiltrera offrens datornät i syfte att hämta ut information. Enligt tyska medier visade utredningen att angriparna sannolikt arbetade för Kina (Von Hakan Tanriverdi, 2019) Syfte: *Underrättelseverksamhet.*

26/7, **Fancy Bear angriper Bellingcat via phishing** (Threatconnect Research Team, 2019). Angripare skickade epost-meddelanden till Bellingcat-anställda från vad som såg ut som Protonmail-adresser. Angriparna hade etablerat en falsk domän, protonmail.ch, där de satt upp en kopia av Protonmails webbplats. I e-postmeddelandena blev Bellingcats anställda ombedda att logga in och verifiera sina

[3] En hackergrupp som har erbjudit stulna cybervapen på den svarta marknaden. De har också läckt information och vapen öppet, däribland de sårbarheter som användes för att utföra angreppen WannaCry och NotPetya.

[4] En hackergrupp som länkats till NSA, eventuellt att täcknamn för TAO, NSA:s avdelning för datorintrång

konton mot den falska domänen. Angreppet misslyckades på grund av en kombination av vaksamhet från Bellingcat-personalens sida och antiphishing-mekanismer hos Protonmail (Chapman, 2019). Attribueringen till Fancy Bear görs på grund av likheter i metodik, och för att Bellingcat arbetat med att avslöja Fancy Bears aktiviteter. Syfte: *Underrättelseverksamhet, förberedelse för andra angrepp*.

1/8, **Stone Panda angriper företag inom samhällsviktig verksamhet med riktad phishing** (Godin, 2019). Tre företag i USA drabbades av phishingkampanjer från en angripare som sägs vara APT10, också kända som Stone Panda, en hackergrupp med kopplingar till Kinas regim, kända för underrättelseverksamhet mot kritisk infrastruktur. Syfte: *Underrättelseverksamhet.*

5/8, **Fancy Bear använder IoT som angreppsvektor** (Vavra, 2019). Microsofts Threat Intelligence Center meddelade att Fancy Bear, en hackergrupp kopplad till Ryssland lyckades hitta sårbarheter som tillät dem att koppla upp sig mot skrivare, VOIP-telefoner och videoavkodare och placera skadlig kod i dem. Angreppet möjliggjordes av att användare inte ändrat defaultlösenord, eller underlåtit att uppdatera programvaran i enheterna. Syfte: *Underrättelseverksamhet.*

7/8 **Bahrains kontrollsystem hackade** (Keyser, 2019). Bahrains Myndighet för Nationell Säkerhet, Inrikesdepartement och vice premiärministers kontor utsattes för datorintrång. Enligt Wall Street Journal låg Iran bakom dåden (Bradley Hope, 2019). Myndigheten för El och Vatten angreps vid samma tillfälle, och en källa hävdade att angriparna ”tog kontroll över några av systemen”. Vilka system som drabbades har inte offentliggjorts. Syfte: *Underrättelseverksamhet, förberedelse för andra operationer*.

22/8 **Falska webbplatser på Kimsuky-domän** (Stone, Hacking group targets organizations focused on North Korea's missile program, 2019). Säkerhetsforskare hittade ett antal webbplatser vars IP-nummer och kontrollservrar matchar de som användes i Kimsuky, en underrättelseoperation riktad mot sydkoreanska datornät vilken har attribuerats till Nordkoreas underrättelsetjänst. Webbplatserna som nu hittats är dock kopior av europeiska organisationers webbplatser, minst tre utrikesdepartement, flera universitet och tankesmedjor (Anomali Labs, 2019). Alla webbplatserna tillhör organisationer med anknytning till stater eller organisationer som intresserat sig för Nordkoreas kärnvapenprogram. Det har dock inte framkommit några data som pekar på att de falska webbplatserna skulle ha använts av någon, eller att någon drivit en kampanj för att lura dit användare. Syfte: *(Förberedelse för) Underrättelseverksamhet*.

3/9 **Vattenhålsattacker[5] mot uigurer** (Stone, Researchers uncover malicious sites targeting China's Uighur population, 2019). Elva webbplatser med anknytning till folkgruppen uigurer i Kina angreps och infekterades med skadlig kod. Om en Android-enhet användes för att besöka platserna registrerades enhetens ID-nummer, telefonnummer, geografisk plats, användarnamn med mera. Säkerhetsfirman Volexity anger hackergrupper kopplade till Kina som förövarna och noterar att alla de angripna platserna är spärrade för åtkomst inifrån Kina, vilket i så fall skulle innebära att operationen var riktad mot uigurer bosatta utanför Kina, alternativt användare i Kina som kringgår Kinas åtkomstspärrar. Syfte: *Underrättelseverksamhet*.

5/9 **Asiatiska teleoperatörer angripna av Kina** (Stubbs, China hacked Asian telcos to spy on Uighur travelers: sources, 2019). Enligt Brittiska underrättelsetjänsten har Kina hackat sig in i ett antal teleoperatörer i Asien för att komma åt loggar och abonnemangsdata för kunder som tillhör folkgruppen uigurer. Syfte *Underrättelseverksamhet*.

11/9 **Cobalt Dickens angriper 60 universitet** (Secureworks, 2019). Mabna-institutet, en iransk organisation som tros vara en del av Irans statliga säkerhetstjänst, också kallade Cobalt Dickens, har tidigare angripit mer än hundra universitet med hjälp av riktad phishing och falska inloggningssidor för

[5] Angriparen letar upp webbplatser målgruppen använder och angriper dessa för att komma åt målen när de ansluter vid ett senare tillfälle.

att stjäla lösenord och identiteter tillhörande forskare (US Department of Justice, 2018). Under juli och augusti 2019 utförde de ytterligare en serie angrepp, även denna gång mot universitet. Målen finns i USA, Australien, Kanada, Hong Kong och Schweiz. Totalt har Cobalt Dickens angripit minst 380 universitet och högskolor i minst 30 länder. Syfte: *Underrättelseverksamhet*.

11/9 **Malware inbäddad i obskyra filtyper** (Danny Adamitis, 2019). Angripare som tros tillhöra hackergruppen Kimsuky, som eventuellt har kopplingar till Nordkorea, har bäddat in skadlig kod i MS Office-dokument genom att lägga dem i filer med obskyra format, till exempel Kodak FlashPix, vilka så sällan används att antivirusprogram ofta saknar signaturer för dem. Angriparna har bland annat tagit dokument från konferenser, lagt till skadlig kod i dem och sedan sänt ut dem till konferensdeltagarna, och andra sätt att få filerna att verka rimliga att öppna för offren. Syfte: *Underrättelseverksamhet.*

24/9 **Social engineering mot Tibetaktivister** (Stone, A cyber-espionage effort against Tibetan leaders leveraged known Android, iOS vulnerabilities, 20419). Angripare som kopplats till den kinesiska säkerhetstjänsten kontaktade medlemmar i grupper som arbetar för Tibets rättigheter, bland dem medlemmar av Tibets parlament. Efter att via kommunikationsappen Whatsapp ha utgett sig för att vara journalister, representanter för Amnesty International eller andra förtroendeingivande grupper sände de länkar som tillät skadlig kod att laddas ned på offrens telefoner. Kampanjen, som döptes till Poison Carp ledde inte till några rapporterade resultat då den skadliga koden var beroende av redan kända sårbarheter och alla de kontaktade hade uppdaterat sina telefoner. Syfte: *Underrättelseverksamhet, förberedelse för andra operationer*.

26/9 **Underleverantörer till Airbus angripna av Stone Panda** (AFP Paris, 2019). Airbus har rapporterat fyra cyberangrepp mot sina underleverantörer det senaste året. Anledningen anses vara att Airbus egna system är väl skyddade, men att underleverantörerna är lättare att komma åt. Angreppet i september riktade sig mot de VPN[6] som användes mellan Airbus och dess underleverantörer. Angreppen tidigare under året har attribuerats till Stone Panda, en hackergrupp med kopplingar till Kina (Delahaye, 2019). Syfte: *Underrättelseverksamhet, förberedelse för andra operationer*.

4/10 **Phosphorous angriper Trumps presidentkampanj** (Sebenius, 2019). Enligt Microsoft har en hackergrupp kopplad till Iran under augusti och september utfört angrepp mot konton som har anknytning till en presidentkandidats valkampanj, men också myndighetspersoner, journalister och exiliranier. Angreppet sägs inte ha varit särskilt tekniskt sofistikerat, men har visat att angriparna har lagt ner stora resurser på att kartlägga sina tilltänkta offer. Enligt Reuters källor är den sittande presidenten Donald Trump kandidaten som är målet (Christopher Bing R. S., 2019). Syfte: *Underrättelseverksamhet, påverkansoperation*.

14/10, **Sammanställning över Turbine Pandas industrispionage** (Kozy, 2019). Utredare hos Crowdstrike har sammanställt utredningar från USA:s justitiedepartement och andra källor för att visa hur Kina systematiskt använt hackergrupper, konventionella underrättelsemetoder och sin egen industri i samverkan för att nå framgångar i sin flygplansutveckling genom att stjäla industrihemligheter (Konstantin, 2019). Syfte: *Underrättelseverksamhet*

3. Observationer från omvärldsbevakning

Huvuddelen av alla angrepp som rapporteras är fortfarande tekniskt enkla. Riktad phishing är en ofta använd metod.

Sidomål är attraktiva. Teleoperatörer, underleverantörer och andra som en organisation är beroende av måste betraktas som hotvektorer.

[6] Virtuella privata nät, krypterade kommunikationsförbindelser

Politiska kampanjer och politiska påtryckningsgrupper verkar bli allt mer attraktiva. Effekten av operationer mot dessa mål är okänd. Eventuellt är syftet att faktiskt bli upptäckt snarare än att lyckas med operationerna för att å ena sidan markera att man har förmåga att påverka motståndare, och å andra sidan att så tvivel om makthavares legitimitet oavsett vem som vinner val.

Veteraner från cyberkrigsförband har nu börjat arbeta på den globala marknaden, enligt uppgift till mycket höga löner. Privata firmor rekryterar amerikanska och israeliska experter för att sälja deras tjänster till diktaturer. (Chesney, u.d.) (Staff, 2019)

Attribueringsproblematiken kvarstår oförändrad. Det är nästan omöjligt att via öppna källor avgöra vem som faktiskt ligger bakom en viss attack. Den metod som kan användas praktiskt är att söka efter tillförlitliga källor som säkerhetsföretag med gott rykte och försöka kombinera data från flera av dessa.

Ett problem är att media publicerar artiklar och nyhetsberättelser utan vare sig förståelse eller noggrann efterforskning. USA påstod i juni att de utfört cyberangrepp mot Iran som vedergällning för en nedskjuten UAV. I CFR:s databas är sammanfattningen av operationens utfall ”U.S. Cyber Command hackade Irans raket- och missilavfyrningssystem som vedergällning för nedskjutning av en av USA:s UAV:er och angrepp på oljetankers i Hormuz-sundet” och i flertalet medier rapporterades detta som fakta. Men under hösten kom ett antal förtydliganden som inte fick spridning i samma utsträckning. Angreppets omfattning minskade successivt: I augusti rapporterades i stället att angreppet hade haft en förödande effekt på Irans underrättelsesystem (Doffman, 2019), men att angreppet skulle ha riktats mot luftvärnet nämndes inte längre. Senare framkom i stället att angreppet hade riktats mot ”en databas som Irans paramilitära gren använt för att planera angrepp” (Barnes, 2019). I dagsläget har det fortfarande inte framkommit annat än anonyma påståenden som belägg för att operationen över huvud taget har ägt rum.

Utvecklingen för svensk del är svårförutsägbar. Jämfört med USA (CISA, 2018) och Tyskland (Stolton, 2018) verkar Sverige upptäcka mycket färre angrepp. Det kan å ena sidan bero på att vi är ett så mycket mindre land att vi inte är ett prioriterat mål för den här typen av aktiviteter, men det kan också bero på att vi inte har resurser, eller kompetens, hos privata företag för att upptäcka aktiviteterna. Om så är fallet löper vi risken att upptäcka omfattningen av infiltrerade styrsystem i samhällsviktig infrastruktur först när en motståndare slår mot oss.

Referenser

AFP Paris. (den 26 09 2019). *Airbus hit by series of cyber attacks on suppliers*. Hämtat från France24: https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

Anomali Labs. (den 22 08 2019). *Suspected North Korean Cyber Espionage Campaign Targets Multiple Foreign Ministries and Think Tanks*. Hämtat från Anomali: https://www.anomali.com/blog/suspected-north-korean-cyber-espionage-campaign-targets-multiple-foreign-ministries-and-think-tanks

Banjo, S. (den 31 08 2019). *Hong Kong Cyber Attack Briefly Disrupts Key Protester Forum*. Hämtat från Bloomberg: https://www.bloomberg.com/news/articles/2019-08-31/hong-kong-cyber-attack-briefly-disrupts-key-protester-forum

Barnes, J. E. (den 28 08 2019). *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*. Hämtat från The New York Times: https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html

Bradley Hope, W. P. (den 07 08 2019). *High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran* . Hämtat från High-Level Cyber Intrusions Hit Bahrain Amid Tensions With Iran : https://www.wsj.com/articles/high-level-cyber-intrusions-hit-bahrain-amid-tensions-with-iran-11565202488

Campanello, S. (den 21 12 2018). *USA åtalar två kineser för cyberattacken Cloud Hopper som drabbade Sverige*. Hämtat från Ny Teknik: https://www.nyteknik.se/sakerhet/usa-atalar-tva-kineser-for-cyberattacken-cloud-hopper-som-drabbade-sverige-6943257

Campanello, S. (den 26 06 2019). *Reuters: Ericsson drabbades av Kinas hackerattack Cloud Hopper*. Hämtat från Ny Teknik: https://www.nyteknik.se/sakerhet/reuters-ericsson-drabbades-av-kinas-hackerattack-cloud-hopper-6963178

Chapman, C. (den 29 07 2019). *Bellingcat journalists dodge spear-phishing attempt*. Hämtat från The Daily Swig: https://portswigger.net/daily-swig/bellingcat-journalists-dodge-spear-phishing-attempt

Chesney, R. (u.d.). *Lawfare*. Hämtat från Lawfare: https://www.lawfareblog.com/project-raven-what-happens-when-us-personnel-serve-foreign-intelligence-agency

Christopher Bing, J. S. (den 27 06 2019). *Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts - sources*. Hämtat från Reuters: https://www.reuters.com/article/us-usa-cyber-yandex-exclusive/exclusive-western-intelligence-hacked-russias-google-yandex-to-spy-on-accounts-sources-idUSKCN1TS2SX

Christopher Bing, R. S. (den 4 10 2019). *Exclusive: Trump campaign targeted by Iran-linked hackers - sources*. Hämtat från Reuters: https://www.reuters.com/article/us-cyber-security-iran-trump-exclusive/exclusive-trump-campaign-targeted-by-iran-linked-hackers-sources-idUSKBN1WJ2B4

CISA. (den 15 03 2018). *Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* Hämtat från US-CERT: https://www.us-cert.gov/ncas/alerts/TA18-074A

Council of foreign Relations. (12 2014). *Steel Mill Attack on a german steel plant*. Hämtat från CFR: https://www.cfr.org/interactive/cyber-operations/search?keys=steel+mill

Danny Adamitis, E. W. (den 11 09 2019). *Insights and analysis from the Prevailion Team*. Hämtat från Blog.prevaillion: https://blog.prevailion.com/2019/09/autumn-aperture-report.html

Delahaye, J. (den 5 02 2019). *Airbus cyber attack believed to be conducted by hackers in China*. Hämtat från the Mirror: https://www.mirror.co.uk/travel/news/breaking-airbus-cyber-attack-believed-13955680

Dobos, L. (den 09 05 19). *NSA:s supervapen läckte 14 månader innan Shadow Brokers*. Hämtat från IDG.se: https://techworld.idg.se/2.2524/1.718634/nsa-supervapen-lackte

Doffman, Z. (den 29 08 2019). *Secret U.S. Cyber Mission Devastated Iran's Attack Capabilities, Officials Say*. Hämtat från Forbes: https://www.forbes.com/sites/zakdoffman/2019/08/29/secret-cyber-mission-devastated-irans-attack-capabilities-us-officials-say/#4e72e75cb354Godin, D. (den 2 08 2019). *New advanced malware, possibly nation sponsored, is targeting US utilities*. Hämtat från Ars Technica: https://arstechnica-com.cdn.ampproject.org/c/s/arstechnica.com/information-technology/2019/08/new-advanced-malware-possibly-nation-sponsored-is-targeting-us-utilities/?amp=1

Greenberg, A. (den 25 06 2019). *A Likely Chinese Hacker Crew Targeted 10 Phone Carriers to Steal Metadata*. Hämtat från Wired: https://www.wired.com/story/chinese-hackers-carrier-metadata/

Hughes, C. (den 3 4 2019). *Major cyber attack on UK infrastructure and organisations 'carried out by Iran'*. Hämtat från the Mirror: https://www.mirror.co.uk/news/uk-news/major-cyber-attack-uk-infrastructure-14226055

ICS-CERT. (den 23 08 2018). *ICS Alert (IR-ALERT-H-16-056-01)*. Hämtat från US-CERT: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01

International, A. (den 25 05 2019). *State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack*. Hämtat från Amnesty International: https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

Jessica Damiana, F. P. (den 13 03 2019). *Indonesia says cyber attacks won't disrupt elections*. Hämtat från Reuters: https://www.reuters.com/article/us-indonesia-election/indonesia-says-cyber-attacks-wont-disrupt-elections-idUSKBN1QU135

Julian E. Barnes, T. G.-N. (den 22 06 2019). *U.S. Carried Out Cyberattacks on Iran*. Hämtat från The New York Times: https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

Keyser, Z. (den 10 08 2019). *Wall Street Journal reports Bahrain targeted by Iranian cyber attacks*. Hämtat från The Jerusalem Post: https://www.jpost.com/Middle-East/Wall-Street-Journal-reports-Bahrain-targeted-by-Iranian-cyber-attacks-598190

Konstantin, L. (den 14 10 2019). *Report: China supported C919 airliner development through cyberespionage*. Hämtat från CSO United States: https://www.csoonline.com/article/3445230/china-supported-c919-airliner-development-through-cyberespionage.html

Kozy, A. (den 14 10 2019). *Huge Fan of Your Work: How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet*. Hämtat från Crowdstrike: https://www.crowdstrike.com/blog/huge-fan-of-your-work-part-1/

Maza, C. (den 13 1 2019). *Newsweek*. Hämtat från Newsweek: https://www.newsweek.com/russian-military-intelligence-hackers-dnc-washington-1313036

Medium . (den 15 05 2019). *Winnti: More than just Windows and Gates*. Hämtat från Medium: https://medium.com/chronicle-blog/winnti-more-than-just-windows-and-gates-e4f03436031a

Mor Levi, A. D. (den 25 06 2019). *Operation Soft Cell: A Worldwide Campaign Against Telecommunications Providers*. Hämtat från Cybereason: https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers

Muks Hirani, S. J. (2019). *Global DNS Hijacking Campaign: DNS Record Manipulation at Scale.* FireEye.

Nakashima, E. (den 27 02 2019). *U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms*. Hämtat från Washington Post: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.htmlNBC. (u.d.). Hämtat från NBC: https://www.nbcnews.com/tech/security/how-uae-used-u-s-mercenaries-cyber-super-weapon-spy-n964436

New BabyShark Malware Targets U.S. National Security Think Tanks. (den 22 02 2019). Hämtat från Palo Alto Networks Unit 42: https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/

Packham, C. (den 16 09 2019). *Exclusive: Australia concluded China was behind hack on parliament, political parties – sources* . Hämtat från Reuters: https://www.reuters.com/article/us-australia-china-cyber-exclusive/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-parties-sources-idUSKBN1W00VF

Paul Mozur, A. S. (den 13 06 2019). *Chinese Cyberattack Hits Telegram, App Used by Hong Kong Protesters*. Hämtat från The New York Times: https://www.nytimes.com/2019/06/13/world/asia/hong-kong-telegram-protests.html

Price, E. (den 05 03 2019). *Chinese Hackers Targeted 27 Universities to Steal Maritime Research, Report Finds.* Hämtat från Fortune: https://fortune.com/2019/03/05/chinese-hackers-targeted-27-universities-to-steal-maritime-research-report-finds/

Schuetze, A. (den 24 07 2019). *BASF, Siemens, Henkel, Roche target of cyber attacks.* Hämtat från Reuters: https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

sebenius, A. (den 22 06 2019). *Iran Increases Cyberattacks on the U.S. Amid Tensions, DHS Says*. Hämtat från Bloomberg: https://www.bloomberg.com/news/articles/2019-06-22/iran-increases-cyberattacks-on-the-u-s-amid-tensions-dhs-says

Sebenius, A. (den 04 10 2019). *Microsoft Says Iran Tried Hack of U.S. Presidential Campaign*. Hämtat från Bloomberg: https://www.bloomberg.com/news/articles/2019-10-04/microsoft-says-iran-tried-to-hack-a-u-s-presidential-campaign

Secureworks. (den 11 09 2019). *COBALT DICKENS Goes Back to School…Again*. Hämtat från Secureworks: https://www.secureworks.com/blog/cobalt-dickens-goes-back-to-school-again

Staff, T. (den 18 10 2019). *UAE-based intelligence firm said recruiting IDF veterans from elite cyber unit*. Hämtat från The Times of Israel: https://www.timesofisrael.com/uae-based-intelligence-firm-said-recruiting-idf-veterans-from-elite-cyber-unit/

Stolton, S. (den 30 11 2018). *Germany: Critical cyberattacks target government and military networks*. Hämtat från Euractiv: https://www.euractiv.com/section/cybersecurity/news/germany-critical-cyberattacks-target-government-and-military-networks/

Stone, J. (den 04 04 2019). *German drug giant Bayer breached by Chinese hacking group Wicked Panda: report*. Hämtat från cyberscoop: https://www.cyberscoop.com/bayer-breached-china-wicked-panda/

Stone, J. (den 21 08 2019). *Hacking group targets organizations focused on North Korea's missile program*. Hämtat från cyberscoop: https://www.cyberscoop.com/north-korean-hacking-espionage-phishing/

Stone, J. (den 03 09 2019). *Researchers uncover malicious sites targeting China's Uighur population*. Hämtat från CyberScoop: https://www.cyberscoop.com/china-uyghur-hacking-china-android-iphone/

Stone, J. (den 24 09 2019). *A cyber-espionage effort against Tibetan leaders leveraged known Android, iOS vulnerabilities*. Hämtat från CyberScoop: https://www.cyberscoop.com/tibet-citizen-lab-spyware-espionage/

Stubbs, J. (den 05 09 2019). *China hacked Asian telcos to spy on Uighur travelers: sources*. Hämtat från Reuters: https://www.reuters.com/article/us-china-cyber-uighurs/china-hacked-asian-telcos-to-spy-on-uighur-travelers-sources-idUSKCN1VQ1A5

Stubbs, J. (den 6 02 2019). *Reuters*. Hämtat från Reuters: https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

Symantec. (den 07 05 2019). *Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak*. Hämtat från Symantec: https://www.symantec.com/blogs/threat-intelligence/buckeye-windows-zero-day-exploit

Tartare, M. (den 21 10 2019). *Winnti Group's skip-2.0: A Microsoft SQL Server backdoor*. Hämtat från WeLiveSecurity: https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

The Guardian. (den 23 06 2019). *US launched cyber attack on Iranian rockets and missiles – reports* . Hämtat från The Guardian: https://www.theguardian.com/world/2019/jun/23/us-launched-cyber-attack-on-iranian-rockets-and-missiles-reports

Threatconnect Research Team. (den 26 07 2019). Hämtat från ThreatConnect: https://threatconnect.com/blog/building-out-protonmail-spoofed-infrastructure/

US Department of Justice. (den 23 03 2018). *Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps*. Hämtat från Justice Department: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

Warren Mercer, P. R. (u.d.). Hämtat från Talos Intelligence: https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

Vavra, S. (den 05 08 2019). *Russian government hackers used office technology to try to breach privileged accounts*. Hämtat från Cyberscoop: https://www.cyberscoop.com/russian-apt-iot-device-security/

Volz, D. (den 18 01 2019). DNC Says Russia Tried to Hack Into its Computer Network Days After 2018 Midterms . *Wall Street Journal*.

Von Hakan Tanriverdi, M. Z. (den 24 07 2019). *Industriespionage Hacker greifen mehrere Dax-Konzerne an* . Hämtat från Tagesschau: https://www.tagesschau.de/investigativ/ndr/winnti-101.html