Projektnummer/Project no
E72887
Kund/Projektnummer
Försvarsmakten
FoT-område
Operationer i cyberdomänen

Författare/Author
David Lindahl

Datum/Date
2020-12-18
Memo nummer/Number
FOI Memo 7422

Omvärldsbevakning: Statsattribuerade cyberoperationer 2020

Sändlista/Distribution

Enligt separat dokument

1 Inledning

Detta memo innehåller övergripande reflektioner och slutsatser rörande förmodat statssponsrade cyberincidenter som rapporterats i media och andra öppna källor från mitten av oktober 2019 till november 2020. Memot är skrivet som en del av det Försvarsmaktsfinansierade projektet Cyberoperationer som genomförts 2018-2020. Mottagare är Försvarsmakten och de personer kopplade till Försvarsmakten som arbetar med skydd mot, och forskning kring, cyberoperationer. Memot består av ett kapitel med observationer och slutsatser, följt av en bilaga innehållande sammanfattningar av alla ingående incidenter.

2 Reflektioner från omvärldsbevakningen

Detta kapitel innehåller författarens sammanfattande reflektioner kring vad som publicerats i databasen från Council of Foreign Relations[1] och de övriga källorna (artiklar och forskningsrapporter) listade i Bilaga 1.

Enkla angrepp fungerar. Till allra största del är cyberangreppen tekniskt enkla. Nätfiske, riktat nätfiske och social manipulering är angreppsvektorer som fungerar även mot vad som borde vara säkerhetsmedvetna organisationer som myndigheter och militära organisationer. Detta har även bekräftats experimentellt vid flera tillfällen[1].

Snabba angrepp fungerar. Angrepp som bygger på redan kända sårbarheter har visat vara en fungerande metod. Detta då många organisationer inte uppdaterar sina system särskilt snabbt och heller inte isolerar system med nyupptäckta sårbarheter. Detta skapar möjligheter till framgångar för angripare med sämre tekniska förutsättningar, som saknar förmåga att själv ta fram zero-days. De kan ändå få framgång i sina cyberoperationer om de snabbt anpassar sina vapen efter nya publicerade sårbarheter.

Avancerade angrepp fungerar. Parallellt med de tekniskt enkla angreppen förekommer mycket avancerade varianter, som UEFI-hack[2] och zero-days. Om en organisation ska kunna hantera en sådan typ av anfall måste de ha förberett sig noga för att kunna upptäcka avvikelser, hantera incidenter och återställa sina system.

Trendiga angrepp fungerar. Angripare, både stater och kriminella har mycket snabbt anpassat sig till Covid-kopplade aktiviteter. Detta gäller både material för social manipulering, programvara och falska webbplatser. Detta har även noterats tidigare[2].

Grundläggande teknisk säkerhet fungerar. Många av årets cyberangrepp, även de från kompetenta aktörer, har mitigerats eller hindrats av relativt enkla medel. En fungerande rutin för säkerhetskopiering och återställning minimerar i många fall effekterna från gisslanprogram. De organisationer som är systematiska i sin tillämpning av ett kontinuerligt cybersäkerhetsarbete kan drabbas, men angreppen får antagligen lindrigare konsekvenser.

Cyberoperationer associerade med stater är oftast spionage. De huvudsakliga cyberaktiviteter som tillskrivs stater är datorintrång, eller spridning av spionprogramvara, för att få tag på data. Målen är information som är sekretessbelagd eller av ekonomisk betydelse, men också personlig information om individer inklusive aktivitets- och positioneringsdata från mobila enheter. Bredden på

[1] https://www.cfr.org/cyber-operations/

[2] Unified Extensible Firmware Interface (UEFI), firmware för att ladda in operativsystemet i en dator.

informationsinhämtning är omfattande och rör i princip alla myndigheter, militära förband, politiska organisationer och de flesta kommersiella sektorer.

Den breda ansatsen skulle kunna betyda att metoderna trots allt inte är tillförlitliga, och att mängden upptäckta angrepp är resultatet av en ”angrip allt som svarar, se var vi får genomslag”-metod. Men den kan också indikera att cyberangrepp för spionage är en så viktig och effektiv metod att stater har många anställda för att utföra dem.

Angripare går via leverantörer och tredjepartstjänster. Webbplatser, utrustning i nätverkens infrastruktur och uppdateringsmekanismer hos programvara är eftertraktade resurser för en angripare att ha som vektorer för framtida intrång och spionage.

Cyberoperationsmetodiken utvecklas. I flera fall verkar det som att resursstarka aktörer skapar olika enheter med specialiserade förmågor. En hackergrupp specialiserar sig på intrång i vissa branscher, eller mot vissa mål. I ett fall har angripare från olika grupper bytt av varandra så att när ett intrång skett och vägar in i systemet etablerats lämnar den första gruppen över till en annan enhet som specialiserar sig på långvarigt utnyttjande av system och informationsstöld.

Cyberoperationer kommersialiseras. Allt fler företag sätts upp för att tillverka vapen för cyberoperationer. Spionprogramvara, trojanprogram för leverans av skadlig kod och uthyrning av personal för att integrera produkterna i en organisations verksamhet är exempel på produkter och tjänster som nu finns tillgängliga.

Dessa företag rekryterar aktivt före detta cybersoldater som tjänstgjort i statliga militärförband och säkerhetstjänster. Som ett resultat av detta kan nu en aktör med begränsade resurser köpa cyberoperationsverktyg och hyra tränad personal som de annars inte skulle haft tillgång till.

Cyberangrepp har blivit en accepterad del av internationell politik. Under året har ett flertal länder använt cyberangrepp som en respons på fysiska angrepp och öppet erkänt det. I andra fall har cyberangrepp besvarats med cyberangrepp och vem som ligger bakom har betraktats som känt även om erkännande inte har framkommit. I det senare fallet ligger exempelvis angreppen mot Israels vattensektor och Irans hamnresurser, men även Australiens angrepp mot IT-brottslingars cyberresurser. Ingen av dessa händelser verkar föranlett några opinionsproblem, eller ens en diskussion av sanktioner från det internationella samfundet.

Deltidsarbete. Flera länder verkar redan ha hackergrupper som delvis agerar för vinnings skull. Några, som Lazarus verkar systematiskt stjäla som en del av statens aktioner, men andra verkar vara ett slags deltidskriminella som ibland agerar för staten och ibland för egen del.

Åtal och namngivning. Under året har ett antal operatörer blivit åtalade som privatpersoner för brott de anses ha begått på statligt uppdrag. Både amerikanska FBI och Europol har efterlyst ett antal personer för olika brott.

Kinas Great Cannon. Kina har använt denna resurs ytterst sparsamt. Men den är värd att nämna på grund av Kinas ökade betydelse för det internationella dataflödet. Genom att använda sin omfattande censurinfrastruktur som en vapeninjektor kan Kina utnyttja det globala behovet att kommunicera med servrar inne i Kina för att hitta en ständig ström av nya offer som kan fungera som vapenbärare.

Detta placerar företag i en situation där de antingen inte når resurserna de behöver, måste investera i spaning och säkerhetsåtgärder för att stoppa den skadliga koden, eller acceptera att de kan bli ofrivilliga medhjälpare till Kinas angrepp.

Bilaga 1 Förmodat statsstödda cyberoperationer från oktober 2019 till november 2020

Den amerikanska tankesmedjan Council of Foreign Relations har sedan 2005 underhållit en databas[3] över förmodat statssponsrade cyberincidenter som framkommit i öppna källor. 2019 publicerade FOI ett memo som beskrev det årets aktivitet fram till november[3]. Nedan följer kronologiskt de incidenter som registrerats i databasen sedan 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 databasen tagit information som framkommit i media och att attribueringen till stater i flertalet fall är svag eller baserad på rena misstankar.

En annan notering som gjorts är att databasen inte är komplett. Till exempel togs angreppet mot Norges Storting inte upp. Datainsamlingen som utförts kan därför inte anses vara uttömmande.

För varje incident har angetts vilken hackergrupp som anses ligga bakom och vilket land de associerats med. Det finns inget gemensamt namngivningssystem för hackergrupper, utan varje större säkerhetsföretag använder sitt eget. Vi har valt att behålla den namn givning som använts i databasens sammanfattning för respektive incident. För de flesta av fallen stämmer detta med den benämningen källorna till databasen har använt.

Varje incident har getts en beskrivande rubrik följt av en klassificering som anger vilken typ av incident det är. Klassificeringen har tagits från CFR:s databas, men översatts.

- **Underrättelseaktivitet (Espionage)**: Syftet med aktiviteten är att samla in information för senare användning.
- **Dataförstörelse (Data Destruction)**: Syftet med aktiviteten är att radera lagrad information på målsystemen eller göra målsystemen obrukbara. Kan användas för att dölja spår, eller påverka en motståndare.
- **Sabotage:** Definitionen enligt databasens informationssidor är att ”syftet med aktiviteten är att störa eller stoppa en fysisk process”. CFR har inte ändrat definitionen, men har även använt denna term för att klassa incidenter där tjänster som streaming eller tillgång till webbplatser har slagits ut.
- **DDOS:** Distribuerad överbelastningsattack. Syftet med aktiviteten är att paralysera ett datornätverk genom att sända stora mängder data till det från många olika avsändare samtidigt.
- **Vandalism (Defacement):** Obehörig ändring av en webbplats eller konto på sociala media.
- **Vinning (Financial Theft):** Stöld av data eller andra resurser för finansiell vinning.

[3] https://www.cfr.org/cyber-operations/

Några av posterna i databasen saknar klassificering. Dessa har klassificerats som memoförfattaren fann lämpligt.

Ett par incidenter som inte fanns med i CFR-databasen har tagits upp för att författaren ansåg dem tillräckligt väl attribuerade till stater och av intresse för memot. Dessa var angreppet mot Norges Storting, och angreppen som använde UEFI-hack som metod. I det första fallet togs incidenten med på grund av närheten till Sverige och svenska förhållanden. I det andra fallet för att metoden var tekniskt intressant och spridningen av cybervapen från kommersiella aktörer till länder är politiskt intressant.

Oktober 2019

Pegasus[4] **används mot människorättsaktivister i Marocko (Underrättelseaktivitet).** Enligt Amnesty International har den Marockanska regeringen använt spionprogramvaran Pegasus från det israeliska företaget NSO Group[5] för att spionera på människorättsaktivister[6].

KINGDOM-gruppen använder Pegasus mot människorättsaktivister (Underrättelseaktivitet)[4]**.** Gruppen KINGDOM som tros vara associerad med den Saudiska regeringen anklagas av The Citizen Lab[7] för att ha använt Pegasus för att spionera på människorättsaktivister[8] och journalister i Kanada, Mexiko och ett flertal andra länder under flera års tid[9].

USA angriper Iran (Dataförstörelse). Två representanter för USA:s regering berättade för Reuters att USA slagit till mot Iran som vedergällning för drönaranfallen mot Saudi Aramco den 14 september. Enligt källorna skulle angreppet ha slagit ut hårdvara hos datorsystem och skadat den iranska regimens förmåga att sprida propaganda. Irans kommunikationsminister kommenterade angreppspåståendena med att USA måste ha drömt det[10].

Regeringsmål i EU angripna av The Dukes (Underrättelseaktivitet). Enligt Welivesecurity och The Daily Beast har The Dukes, en hackergrupp associerad med Ryssland, angripit flera regeringsdepartement i EU, och minst en ambassad[11].

Turla hackar Oilrig (Underrättelseaktivitet). Turla[12], en hackergrupp associerad med den ryska staten, skaffade sig tillgång till verktyg och program tillhörande Oilrig, en hackergrupp associerad med den iranska staten. Turla använde sedan dessa verktyg, tillsammans med sina egna, för att leta upp och angripa mål som Oilrig hade lyckats angripa och satt upp bakdörrar till. De använde även verktygen för att angripa nya mål. Det är inte känt hur Turla skaffade sig verktygen[13].

Sandworm anfaller Georgien (Sabotage)[5]**.**

Enligt brittiska National Cyber Security Centre (NCSC)[14] har GRU genom gruppen Sandworm angripit webbvärdar i Georgien och slagit ut webbplatser tillhörande

[4] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

[5] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

Georgiens regering, domstolar, medier med flera[15] [16]. Även Polens regering har anklagat Ryssland i ärendet[17].

Uzbekistans säkerhetstjänst spionerar på dissidenter med skadlig kod (Underrättelseaktivitet). Enligt Kaspersky har enhet 02616, en enhet inom den uzbekiska säkerhetstjänsten DXX införskaffat kommersiell skadlig kod från Finfisher, NSO group och Candiru. Dessa användes för att angripa människorättsaktivister, journalister och dissidenter[18]. Spårandet av gruppen som fått namnet SandCat underlättades av att gruppen själva testade sina nyinköpta produkter på egna maskiner med Kasperskys antivirusprogram installerade. Dessa rapporterade in binärerna till Kaspersky som efterhand fick alla nya versioner skickade till sig och kunde spåra mjukvarans spridning[19]. Attribueringen får anses vara en av de mest tillförlitliga memoförfattaren sett eftersom det visade sig att förutom ovanstående tillkom att domänen som gruppen använde registrerats som tillhörande "Military Unit 02616", ett statligt bolag med ägaren till domänen angiven som en offentligt känd DXX-agent.

November 2019

Lazarus angriper indiska myndigheter med riktat nätfiske (Underrättelseaktivitet). Enligt säkerhetsfirman Security Brigade[20] angreps minst fem olika indiska myndigheter, däribland rymdforskningsmyndigheten ISRO och kärnkraftverket Kudankulam, av angripare associerade med Nordkorea[21]. ISRO och Kudankulam förnekar att angriparna lyckades skaffa sig tillträde till styrsystem eller känslig information[22]. Security Brigade kommenterade att angreppet inte varit tekniskt avancerat: ”[…]det var ett nätfiskemejl, en opatchad webbläsare och brist på övervakning”.

APT33 etablerar C&C-servrar[6] för värdefulla mål (Underrättelseaktivitet). Enligt en rapport[23] från Trend Micro[24] har APT33[25, s. 33], en hackergrupp attribuerad till den iranska staten, etablerat en grupp C&C-servrar specifikt för att hantera högvärdesmål som de angripit och tagit kontrollen över. Servrarna styr infekterade datorer i bland annat ett amerikanskt företag med verksamhet relaterad till nationell säkerhet, mål relaterade till USA:s krigsmakt samt mål i Asien och mellanöstern. Dessa servrar i sin tur styrs från datorer skyddade av VPN-uppkopplingar.

Golden Falcon aktiv i Kazakstan (Underrättelseaktivitet). Enligt en rapport[26] från säkerhetsföretaget Qihoo 360[27] har en aktör döpt till Golden Falcon, en hackergrupp attribuerad till Ryssland, använt fjärrstyrnings- och spionverktyg mot ett antal mål i Kazakstan. Målen tillhör många olika kategorier, från militär personal, till myndigheter, journalister, privata företag, representanter för religiösa organisationer, dissidenter och diplomater från olika länder[28]. Intrången verkar ha varierat från nätfiskemejl till fysiskt tillträde till målen. Verktygen som använts varierar från kommersiellt tillgängliga Pegasus från NSO och RCS från HackingTeam[29] till egentillverkade zero-day-sårbarheter.

APT33 spionerar på styrsystemleverantörer (Underrättelseaktivitet). Enligt Ars Technica[30] uttalade sig Microsoft att APT33, en hackergrupp associerad med Iran

[6] Command and Control Servers. Datorer för fjärrstyrning av datorer infekterade med skadlig kod.

börjat angripa leverantörer av styrsystem och styrsystemstjänster[31] med automatiska lösenordsgissare.

Gamaredon spionerar i Ukraina (Underrättelseaktivitet). Enligt säkerhetsfirmorna Anomali[32] och Sentinel Labs[32] har den proryska hackergruppen Gamaredon systematiskt opererat i Ukraina både med att inhämta underrättelser från olika mål i Ukraina, och testat ryska metoder för att utföra cyberkrig[33]. Bland offren finns det ukrainska utrikesdepartementet, polisväsendet, journalister med flera.

Bronze Butler spionerar på japanska företag (Underrättelseaktivitet). Trend Micro har sedan 2008 spårat en hackergrupp[34], BRONZE BUTLER[35], attribuerad till kinesiska staten[36]. Gruppen har inriktat sig på spionage mot olika typer av företag i Sydostasien. Under hösten 2019 drev de en kampanj specifikt mot japanska företag med kontor i Kina, där de stal e-postmeddelanden från ett forskningsföretag och en PR-firma, och använde data från dessa för att konstruera trovärdiga meddelanden för riktat nätfiske. Målen för kampanjen skiljer sig mot tidigare mål för gruppen genom ett snävare fokus. Där tidigare kampanjer inkluderade tillverknings- och ingenjörssektorerna hade alla de nya målen kopplingar till nationellt känslig information: försvarssektorn, delar av kemisektorn, satellit och rymdsektorn.

December 2019

APT34 använder ny skadlig kod (Dataförstörelse). IBM publicerade en rapport[37] där de pekar ut Iran som angripare via APT34 och ytterligare en iransk hackergrupp. Angreppen riktade sig mot olika företag i gas- och energisektorn i mellanöstern. Angreppen var självspridande skadlig kod som raderade hårddiskar. IBM gör bedömningen att angreppen var resultatet av ett samarbete mellan APT34 för att skaffa sig tillträde, och en annan grupp för det förstörande angreppet. De baserar detta på tidigare aktiviteter från APT34 (intrång, ingen förstörelse) och ett tidsgap mellan intrångsdelen av angreppen och att förstörelsen startade.

”The Great Cannon” används mot Hongkong-dissidenter (DDOS). Enligt AT&T[38] har de datacenter som filtrerar trafik till och från Kina, också kända som den kinesiska brandmuren, använts för mannen-i-mitten-angrepp mot LIHKG.com, ett internetforum frekventerat av aktivister för Hongkongs oberoende. Angreppet går till så att datacentren som filtrerar datatrafik ut och in ur Kina lägger till JavaScript i de utgående webbsidorna som passerar. Dessa skript sänder från mottagarens webbläsare förfrågningar till det mål som angreppet riktar sig mot. Resultatet är att en stor mängd trafik dirigeras in mot målet från många olika datorsystem vars ägare är ovetande om angreppet[39]. Angreppet generar en mycket stor mängd trafik, men har använts sparsamt. Endast tre tidigare angrepp är kända, 2015 mot GitHub.org och GreatFire.org[36.] och2017 mot Mingjingnews.com[40].

Ocean Lotus angriper BMW och Huyndai (Underrättelseaktivitet). Tv-kanalen Bayerischer Rundfunk[41] rapporterar att hackergruppen OceanLotus, attribuerad till den vietnamesiska regeringen, har angripit BMW och Hyundai i syfte att stjäla industrihemligheter. Angreppet ska ha skett med verktyget Cobalt Strike i kombination med falska webbplatser som härmade BMW:s och Hyundais webbplatser i Thailand[42].

APT20 går förbi 2-faktor-autenticering (Underrättelseaktivitet). Enligt en rapport från Fox-IT[43] har kinaattribuerade APT20[44] angripit olika myndigheter och tjänsteleverantörer inom bland annat aerotech- finans- och energisektorerna[45]. Angreppet har skett genom att utnyttja sårbarheter i webbservrar och JBOSS-ramverket. Angriparen verkar ha kunnat gå förbi RSA SecurID 2-faktor-autentisering genom att först stjäla en SecurID token (en datafil) från ett offers dator, och sedan modifiera en SecurID-programmet för att få programmet att tro att det är en token som har genererats på den lokala maskinen och därmed får användas för att generera engångskoder[46].

ToTok, social media-app är ett verktyg för UAE:s underrättelsetjänst (Underrättelseaktivitet). Enligt New York Times[47] är programmet ToTok, en social-media-app, skapat för att ge Förenade Arabemiraten underrättelsedata. Företaget Breej Holding som äger appen, kontrolleras i sin tur av DarkMatter[48], en cybersäkerhetsfirma i Dubai bemannad av före detta anställda från USA:s och Israels cybersäkerhetstjänster tillsammans med personal från Förenade Arabemiratens säkerhetstjänst. Appen används för spionage mot interna dissidenter men även globalt. Appen har fått stor spridning i Förenade Arabemiraten där ett antal andra program som WhatsApp och Skype inte är tillåtna.

Januari 2020

Bapco drabbas av Dustman (Underrättelseaktivitet). Bahrains statliga oljebolag Bapco angreps med Dustman[49]. Verktyget är ett raderingsprogram som används för att förstöra data. APT 34, en iranattribuerad hackergrupp, har länkats till angreppet. Användningen av vapnet verkar ha varit ett försök att dölja spionage snarare än rent sabotage.

Lazarus angriper kryptovalutaväxlare (Vinning). Enligt en rapport från Kaspersky[50] har Lazarusgruppen, attribuerad till Nordkorea, sedan 2018[51] angripit mål genom att sprida trojaner i program för att hantera kryptovalutor. Dessa har spridits via webbplatser för påhittade företag dit offren lockats genom e-postkampanjer. Målen verkar ha varit kryptovalutaväxlare och liknande organisationer. Lazarus har använt programmen för att föra ut valuta ur organisationerna.

MAGNALLIUM angriper USA:s elnät (Underrättelseaktivitet). Enligt Dragos Security[52] har MAGNALLIUM, också kända som APT33, en hackergrupp attribuerad till Iran, angripit kraftbolag i USA genom lösenordsgissning i stor skala[53]. Angreppen riktade sig mot kontorsdatornäten och verkade inte vara försök att gå vidare mot styrningen av elnäten.

Burisma angrips av APT28 (Underrättelseaktivitet). Enligt New York Times[54] och BBC[55] har företaget Burisma, ett gasföretag från Ukraina, blivit angripna av Fancy Bear, också kända som APT28, en hackergrupp attribuerad till Ryssland. Angreppet skedde med hjälp av nätfiske och falska webbplatser. Angriparna har inte försökt sabotera eller interagera med styrsystem eller produktion. Angreppet tros var ett försök av GRU att skaffa kompromitterande material att använda för påverkansoperationer mot USA.

Mitsubishi drabbas av datastöld (Underrättelseaktivitet). Enligt Bleeping Computer[56] förlorade Mitsubishi data vid ett intrång som skedde 2019. Data

inkluderade personuppgifter och anställningsuppgifter om närmare 200 anställda. Enligt Cyberscoop[57] stals information om en ny hypersonisk sjömålsrobot. Angriparna sägs enligt insatta källor vara Bronze Butler, en hackergrupp attribuerad till Kina.

Tidningsägare får Spyware på WhatsApp (Underrättelseaktivitet). FN anklagar Saudiarabien för att ha sänt skadlig kod via WhatsApp till Washington Posts ägares telefon i syfte att avlyssna honom[58]. Ärendet tros relaterat till Washington Post-journalisten Jamal Khashoggi som anses ha mördats på order av en prins från landet i fråga [59].

Konni angriper en myndighet i USA med riktat nätfiske (Underrättelseaktivitet)[7]. Hackergruppen Konni, attribuerad till Nordkorea, har sedan flera år[60] använt olika kampanjer av riktat nätfiske mot myndigheter och andra organisationer i USA[61].

DNS-kapning främjar turkiska intressen (Underrättelseaktivitet). Reuters rapporterar[62] att fler än 30 mål, bland annat i Albanien, Grekland, Irak och Cypern har angripits med DNS-kapning. Offren dirigerades om till falska webbplatser och inloggningssidor där angriparna samlade in lösenord och annan trafik. Bland offren finns underrättelsetjänster och andra myndigheter men också privata organisationer och individer.

New York Times angrips av KINGDOM (Underrättelseaktivitet). En journalist vid New York Times fick ett sms med en länk som försökte installera NSO Groups Pegasus-spionprogram på hans telefon. Domänen som länken i sms:et gick till användes vid tillfället av hackergruppen KINGDOM, en hackergrupp som attribuerats till Saudiarabien[63].

Westat angrips av APT34 (Underrättelseaktivitet). Enligt säkerhetsfirman Intezer har APT 34, en hackergrupp kopplad till Iran, angripit det amerikanska företaget Westat och amerikanska myndigheter[64]. Företaget har gjort enkätundersökningar åt amerikanska myndigheter de senaste 16 åren och angriparna har använt riktat nätfiske genom utskick av förfalskade enkäter med skadlig kod till anställda på Westat och andra myndigheter[65].

Journalister angrips av Charming Kitten (Underrättelseaktivitet). Säkerhetsfirman Certfa Lab har rapporterat[66] att Charming Kitten, en hackergrupp med nära band till Irans säkerhetstjänst, har använt social manipulering, bland annat nätfiske-angrepp, för att angripa journalister, människorättsaktivister och politiska dissidenter[67].

Universitet angripna av Winnti (Underrättelseaktivitet). Enligt säkerhetsfirman Welivesecurity angrep Winnti, en hackergrupp med kopplingar till Kinas regering, två universitet i Hong Kong[68]. Angreppen startade i mars 2019 under demonstrationerna för självständighet[69].

Februari 2020

Ukrainas försvars- och säkerhetsmyndigheter angrips av Gamaredon (Sabotage). Säkerhetsfirman Sentinel Labs rapporterar[33] att Gamaredon, en hackergrupp kopplad till Ryssland, har anfallit olika mål i Ukraina. Gamaredon har bedrivit spionage mot

[7] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

militära utbildningscenter och andra mål relaterade till nationell säkerhet. Förutom underrättelseaktiviteterna hävdar SentinelLabs att angrepp har skett mot fysisk infrastruktur och militär utrustning inklusive artilleri[70].

Malaysiska myndigheter angrips av APT40 (Underrättelseaktivitet). Malaysias CERT MyCert rapporterar[71] att anställda vid malaysiska myndigheter utsatts för riktat nätfiske. Enligt ZDNet[72] är angreppet utfört av APT40, en hackergrupp med kopplingar till Kina.

Österrikes utrikesdepartement angrips av Turla (Underrättelseaktivitet). Den österrikiska regeringen anger[73] att angreppet syftade till underrättelseinhämtning och utfördes av en statsaktör[74]. Österrikes statliga radiostation ORF uppger[75] att hackergruppen Turla, som anses ha kopplingar till Ryssland, ligger bakom angreppen och spekulerar i att en politisk schism mellan Ryssland och Österrike ska ha utlöst angreppet.

Fox Kitten angriper företag i Israel, USA (Underrättelseaktivitet). Säkerhetsfirman ClearSky uppger att Iran via hackergruppen APT34, med hjälp av APT33 och APT39 stå bakom angreppen[76]. Angriparna använde one-day-sårbarheter[8] i VPN-tjänster för att få tillträde till offrens nätverk och infiltrerade dessa med intrång och skadlig kod för att stjäla information. Enligt en artikel i ZDNet[77] opererar APT34 med systematiska intrång mot nyckelmål och lämnar sedan över exploateringen och exfiltreringen till APT33 och APT39.

Israeliska soldater utsätts för catfishing[9] **(Underrättelseaktivitet).** Israels säkerhetstjänst ISA meddelade[78] att de och den israeliska militären stoppat en operation utförd av Hamas. Israeliska soldater kontaktades på sociala medier av vad som verkade vara unga kvinnor men som var fiktiva personer skapade genom att modifiera foton av riktiga kvinnor. Soldaterna övertygades att ladda ner programvara på sina telefoner som gav Hamas tillgång till information, bilder och GPS-koordinater från soldaternas telefoner[79].

Mars 2020

APT Tonto angriper Japan, Ryssland och Sydkorea (Underrättelseaktivitet)[10]**.** Talos Intelligence anger[80] att APT Tonto, en hackergrupp attribuerad till kinesiska staten, har använt sin skadliga kod Bisonal i närmare tio år (med uppdateringar). Under denna tid har de anfallit militärtekniska och flygtekniska tillverkare och leverantörer i Sydkorea, Japan, och Ryssland[81].

Vicious Panda utnyttjar Covid-pandemin (Underrättelseaktivitet). Den mongoliska offentliga sektorn angreps med nätfiske[82] där e-postmeddelandena påstods innehålla viktig information om Covid men innehöll skadlig kod som installerade RAT-program[11]

[8] Nyligen publicerade sårbarheter.

[9] Angriparen skapar en fiktiv person på sociala media och använder denna för att lura offren.

[10] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

[11] Remote Access Tools, fjärrstyrningsprogram som installeras via skadlig kod.

på offrets dator. Förövarna har benämnts Vicious Panda och attribuerats till kinesiska staten[83].

Turla anfaller Armenien (Underrättelseaktivitet). Enligt säkerhetsfirman Welivesecurity har hackergruppen Turla tagit över ett antal webbplatser i Armenien och använt dessa för att kartlägga användare och identifiera lämpliga offer. Dessa har sedan fått en uppmaning att uppdatera sin Adobe Flash Player via ett pop-up-fönster som levererade skadlig kod.

Hades angriper Ukraina (Underrättelseaktivitet). Nätfiske-meddelanden som utgav sig för att komma från den ukrainska folkhälsomyndigheten spreds i Ukraina och uppmanade offren att klicka på länkar som laddade ner spionprogramvara. Hades, en hackergrupp attribuerad till ryska staten, påstås ligga bakom kampanjen[84]. Samtidigt spreds e-postmeddelanden med falska påståenden om Covid-spridningen, vilket ledde till upplopp på flera platser i landet[85].

Mythic Leopard använder Covid (Underrättelseaktivitet). APT36, också kända som Mythic Leopard, använde e-postmeddelanden med falsk Covid-information för att lura sina offer i Indien och Pakistan[86].

APT 28 angriper sårbara webbservrar (Underrättelseaktivitet). Enligt Trend Micro har APT28 under lång tid skannat internet för att få tillgång till sårbara servrar med webmail eller MS Exchange[87]. De tog sedan över e-postkonton och använde dessa för nätfiske[88].

WHO angrips av DarkHotel (Underrättelseaktivitet). Världshälsoorganisationen WHO utsattes för nätfiske-försök av DarkHotel, en hackergrupp CFR associerat med Sydkorea[89].

Lotus Blossom använder vattenhålsangrepp[12] **(Underrättelseaktivitet).** Enligt Trendmicro har hackergruppen Lotus Blossom, associerad med kinesiska staten, angripit webbplatser för att kunna spåra och sprida skadlig kod till dissidenter i Hong Kong[90].

APT41 startar en global kampanj (Underrättelseaktivitet). Flera säkerhetsföretag[91] rapporterar att den kinaattribuerade hackergruppen APT41 använde sårbarheter i Citrix-programvaran och Cisco-routrar för att anfalla fler än 75 organisationer[92] i fler än 20 länder. Offren tillhörde olika branscher, från försvarsindustri och myndigheter till hälsovård och ideella föreningar.

DarkHotel spenderar fem zero-days (Underrättelseaktivitet). Googles Threat Analysis Group (TAG) meddelar[93] att de sett en spionagekampanj riktad mot offer i Nordkorea där angriparna under ett år använde fem olika zero-days. Angriparna har identifierats som DarkHotel vilka tros ha kopplingar till Sydkoreanska staten.

Saudier övervakas (Underrättelseaktivitet). Enligt visselblåsare[94] använder Saudiarabiens regering säkerhetshål i telenätsprotokollet SS7 för att övervaka sina medborgare runt om i världen[94].

[12] Angriparen tar över tjänster eller webbplatser som offret förmodas använda och utnyttjar dessa för att angripa. Hen ”väntar vid vattenhålet” på bytet.

Tibetanska organisationer måltavlor för vattenhålsangrepp (Underrättelseaktivitet)[13]**.** Storm Cloud[95] är en hackergrupp som associerats med Kina. De har använt vattenhålsattacker mot tibetanska organisationer och individer för att leverera spionprogramvara[96].

WHO angrips med nätfiske (Underrättelseaktivitet). Världshälsoorganisationen WHO utsattes för en nätfiske-kampanj där förövarna pekades ut som agerande för Iran[97]. Iran förnekade kännedom om angreppet.

April 2020

Australien angriper cyberbrottslingars webbplatser (Dataförstörelse). Australiens försvarsdepartement uppger att landets signalspaningsorganisation ASD har slagit ut webbplatser och kommunikationsvägar tillhörande cyberbrottslingar som försökte utnyttja Covid-pandemin för att angripa mål i Australien[98]. ASD:s chef hävdar att arbetet kommer att fortsätta med utökat samarbete med telebolag för att komma åt cyberbrottslingar som agerar bortom Australiens gränser[99].

Syrian Electronic Army sprider skadlig kod (Underrättelseaktivitet). Enligt Cyberscoop[100] har en hackerkampanj spårats till byggnader som attribuerats till högkvarteret för Syrian Electronic Army, en hackergrupp som tros agera för den syriska staten. Genom bedrägeri relaterat till Covid-pandemin har de fått offer att ladda ner appar med skadlig kod[101].

Ocean Lotus angriper Wuhan (Underrättelseaktivitet). Enligt FireEye[102] har hackergruppen Ocean Lotus, attribuerade till Vietnam, angripit administrationen i den kinesiska Wuhan-provinsen med nätfiske-brev för att få information om Covid-krisen och Kinas hantering av den[103].

Polens militärhögskola angrips av hackare (Vandalism). Den polska militärhögskolan angreps av hackare som använde skolans resurser för att utge sig för att vara polska officerare och postade ett brev som hävdade att USA:s militära närvaro i landet var en ockupation som måste bekämpas. Den polska säkerhetstjänsten beskriver angreppet som "överensstämmande" med rysk desinformationsaktivitet[104].

Ocean Lotus sprider skadlig kod via Google Play (Underrättelseaktivitet). Enligt Kaspersky Labs[105] har hackergruppen Ocean Lotus, attribuerad till Vietnam, använt Google Play för att sprida appar infekterade med spionverktyget Phantom Lance[106].

Maj 2020

Taiwans oljebolag angrips av Winnti Umbrella (Sabotage). CPC, Taiwans statliga oljebolag drabbades av en gisslanprogramvara[107] som Taiwans justitiedepartement angett härstammar från Winnti Umbrella, en hackergrupp som attribuerats till Kina[108]. Angreppet resulterade bland annat i att företagets webbplats slutade fungera under en dag.

APT30 anfaller myndigheter (Underrättelseaktivitet). Enligt New York Times[109] har gruppen APT30, en hackergrupp kopplad till den kinesiska militären, angripit

[13] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

myndighetspersonal och politiker i Australien, Filippinerna, Vietnam, Brunei och Myanmar med skadlig kod.

Cyberangrepp mot Israels dricksvatten får respons (Sabotage). Enligt Times of Israel tog sig angripare från Iran in i styrsystemen för dricksvattenproduktion i Israel i slutet av april och försökte orsaka skada genom att öka klorhalten i dricksvattnet[110]. Generaldirektören för Israels nationella cyberdirektorat beskrev incidenten som ett försök att orsaka förlust av liv, inte data[111]. Några veckor senare utfördes ett cyberangrepp mot hamnen Shahid Rajaee nära Bandar Abbas i Iran. Angreppet orsakade en i det närmaste total nedstängning av hamnen när datorerna som hanterar lastning, lossning och annan logistik plötsligt fallerade. Anonyma tjänstemän har berättat för Times of Israel att Israel slagit ut hamnen som en direkt hämnd för vattenangreppet och att detta innebär att Israels redan befintliga slag-för-slag-strategi som de implementerar för konventionella angrepp nu också gäller för cybersfären[112]. Al Jazeera beskrev angreppet som mycket precist och citerade en anonym amerikansk tjänsteman som sade att Iran hade korsat en gräns med angreppet mot vatteninfrastrukturen som Israel måste besvara[112].

HIDDEN COBRA slår mot banker (Vinning). US-CERT skriver i en rapport[113] att Nordkorea genom hackergruppen HIDDEN COBRA angripit offer med skadlig kod för fjärrstyrning via C&C-servrar i bland annat Danmark. Cyberscoop hävdar att källor inom FBI kopplat angreppen till kryptovalutaväxlare, bankomater och banker men inte velat avslöja vilka incidenterna var[114].

Kina spionerar på Covid-forskning (Underrättelseaktivitet). Enligt FBI[115] och Cybersecurity and Infrastructure Security Agency (CISA) har Kina via cyberangrepp försökt komma över forskningsresultat rörande Covid-vaccin/-behandlingar och information om de som forskar kring dessa områden.

Vicious Panda (Underrättelseaktivitet). Avast Security hävdar att en hackergrupp, Vicious Panda, agerande i Kinas intresse installerade bakdörrar och fjärrstyrningsverktyg i gasbolag, myndigheter och telekomföretag i Centralasien[116].

Greenbug anfaller Telekom (Underrättelseaktivitet). Enligt Cyberscoop[117] har hackergruppen Greenbug, attribuerad till Iran, angripit flera telebolag i Pakistan. Angreppet ska ha syftat inte bara till att få tillgång till företagens kontorsnätverk utan också till telenätverken. Enligt Symantec inleddes angreppen via e-postmeddelanden varefter angriparna traverserade företagens inre nätverk och etablerade krypterade tunnlar som de kunde nå vid senare tillfällen[118].

Spelbolag angrips av Winnti Umbrella (Underrättelseaktivitet). Enligt Welivesecurity[119] har hackergruppen Winnti Umbrella, attribuerad till Kina, angripit spelföretag och försökt skaffa sig långvarigt tillträde till dessa organisationer. Målet ska ha varit att skaffa sig information som skulle användas för att tillverka skadlig kod-uppdateringar till populära spel för framtida intrång[120].

Luftfartsmyndigheter angrips av Chafer (Underrättelseaktivitet)[14]**.** Enligt Bitdefender[121]angrep den iranska hackergruppen Chafer luftfartsmyndigheter i Kuwait och Saudiarabien. De olika ländernas myndigheter angreps något olika där kuwaitiska system angreps direkt men vid de saudiska angreppen användes social manipulering mot personalen.

Berserk Bear anfaller tysk kritisk infrastruktur (Underrättelseaktivitet).

Enligt den tyska säkerhetstjänsten[122] har en rysslandsattribuerad hackergrupp, Berserk Bear, angripit företag inom Tysklands kritiska infrastruktursektor. Angreppen ska ha syftat till att skaffa sig tillträde och underrättelser men också till att få tillgång till styrsystemen för företagens produktionsmiljöer.

Sandworm anfaller Exim (Underrättelseaktivitet). Den amerikanska signalspaningsmyndigheten NSA påstår[123] att den ryska militära underrättelsetjänsten GRU är ansvariga för intrång mot e-postservrar som kör den mycket vanliga programvaran Exim. Inga specifika incidenter nämns.

Juni 2020

Gamaredon anfaller Ukrainska myndigheter (Underrättelseaktivitet). Welivesecurity hävdar i en rapport[124] att hackergruppen Gamaredon, attribuerad till Ryssland, angripit myndigheter och andra organisationer i Ukraina. Intrångsvektorn ska ha varit e-postmeddelanden som när de öppnades laddade ner skadlig kod på offrens datorer.

Lazarus angriper aerospace-företag (Underrättelseaktivitet). Bedragare som utgav sig att vara rekryterare från Collins Aerospace och General Dynamics sände e-postmeddelanden med bilagor som innehöll skadlig kod[125]. Enligt ESET Research tyder de tekniska spåren på att Lazarus, en hackergrupp attribuerad till Nordkorea, låg bakom. Vid minst ett tillfälle kontaktade angriparna offren efter angreppet och använde data från offrens e-postkonto för att försöka tillskansa sig pengar genom en social manipuleringsattack.

Statsaktör angriper Australien (Underrättelseaktivitet). Den australiensiska regeringen meddelade[126] att flera sektorer inklusive alla nivåer av myndigheter, industri, utbildning, politiska organisationer och kritisk infrastruktur var utsatta för en sofistikerad cyberattack utförd av en statlig aktör med stora resurser. Enligt anonyma statstjänstemän var angriparen Kina[127]. Angreppet orsakade stora störningar men det exakta målet är inte känt.

Juli 2020

Ytterligare angrepp mot den israeliska vattenförsörjningen (Sabotage). Angriparna utförde cyberangrepp mot pumpsystem för bevattning i Galiléen och Mateh Yehuda men ingen fysisk effekt uppstod. Enligt den israeliska tidningen Ynet[128] var angriparna iranska hackare som dolde sig genom att använda europeiska och

[14] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

amerikanska servrar. Enligt ZDNET[129] följdes angreppet av en serie olyckor och explosioner som drabbade iransk infrastruktur.

USA anklagar Kina för spionage (Underrättelseaktivitet). USA:s justitiedepartement anklagar två namngivna agenter vid Kinas säkerhetsministerium för cyberangrepp[130] mot "hundratals företag, myndigheter, organisationer, dissidenter och människorättsaktivister". De utpekade ska ha agerat både för den kinesiska statens räkning och för egen vinning. Under sitt arbete ska de ha stulit immateriell egendom till ett värde av hundratals miljoner dollar[131].

Kina anklagas för vatikanspionage (Underrättelseaktivitet)[15]. Enligt säkerhetsfirman Recorded Future ska hackare kopplade till den kinesiska staten ha angripit Vatikanens datorsystem inför ett toppmöte mellan representanter för de båda staterna[132]. Enligt en senare rapport från samma firma ska hackergruppen Red Delta, också kopplad till kinesiska staten, ha angripit katolska organisationer med verksamhet i Kina för att få in spionprogramvara i deras utrustning[133].

Ghostwriter härmar NATO-personal (Underrättelseaktivitet)[16]. Enligt Mandiant Threat Intelligence[134] har en grupp kallad Ghostwriter angripit webbplatser och e-postkonton tillhörande media och individer associerade med NATO. Dessa har sedan använts för att publicera nyhetsartiklar och brev från påhittade och äkta personer i syfte att föra fram ett anti-NATO-narrativ för de som läser dem. Det förfalskade materialet har sedan använts som referens och källmaterial i ytterligare ett steg genom att falska artiklar baserade på materialet publicerades med påhittade och verkliga personer angivna som författare[135]. Säkerhetsfirman IronNet attribuerar gruppen till rysk säkerhetstjänst[136].

Augusti 2020

Storbritanniens handelsministers e-postmeddelanden läckta (Underrättelseaktivitet). Enligt anonyma källor har hackare med kopplingar till ryska staten läckt dokument som de tillskansat sig från handelsministerns e-postkonto[137].

TAIDOOR angriper myndigheter och tankesmedjor (Underrättelseaktivitet). Enligt US-CERT[138, s. 1029] har Kina genomfört cyberangrepp via hackergruppen TAIDOOR mot myndigheter, tankesmedjor och andra organisationer som har samröre med Taiwan. Huvuddelen av angreppen sker genom riktat nätfiske[139] där offret luras att ladda ner skadlig kod. I en ny version av taktiken laddas blogginlägg med krypterade delar ner från Yahoo Blogs och dekrypteras för att få fram den skadliga koden.

Fox Kitten angriper nätverksutrustning (Underrättelseaktivitet). FBI uppger att en grupp iranska hackare angripit nätverksutrustning av märket F5 genom att utnyttja nyligen kända säkerhetshål innan offrens organisationer hunnit säkra upp sårbar utrustning. Enligt anonyma källor är angriparna Fox Kitten, en hackergrupp som attribueras till Iran[140] [77].

[15] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

[16] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

USCYBERCOM stänger ner IRA (Sabotage). Under de amerikanska valen 2018 angrep det amerikanska cyberkrigsförbandet USCYBERCOM den ryska trollfabriken Internet Research Agency i Sankt Petersburg och stängde tillfälligt ner den för att förhindra att Ryssland skulle påverka valet[141][142].

Lazarus angriper försvarsföretag (Underrättelseaktivitet). Lazarusgruppen fortsatte med sin kampanj där de utgav sig för att vara rekryterare från olika företag[143] men nu i Israel och USA[144, s. 10295].

Kina angriper Taiwan (Underrättelseaktivitet). Enligt Taiwans säkerhetspolis har hackare med kopplingar till den kinesiska staten angripit taiwanesiska myndigheter i underrättelsesyfte[145]. Angreppen ska ha utförts av minst fyra av Kinas hackergrupper, Blacktech, TAIDOOR, MustangPanda och APT40, enligt den biträdande direktören för den taiwanesiska säkerhetspolisens cybersäkerhetskontor[146].

Ryssland angriper Stortinget (Underrättelseaktivitet). Enligt den norska regeringen utförde Ryssland cyberangrepp mot Stortingets e-postsystem[147]. **Denna incident fanns inte i CFR:s databas men memoförfattaren valde att ta upp den på grund av närheten till Sverige.**

Lazarus angriper bankomater (Vinning). Enligt amerikanska FBI[148]har nordkoreanska hackare systematiskt angripit banker i mer än trettio länder för att utföra olagliga uttag i bankomater över hela världen. De har också i samma operation angripit postanvisningssystemen för att kunna genomföra falska överföringar.

Kimsuky angriper FN-anställda (Underrättelseaktivitet). Enligt FN[149] har den nordkoreanska regimen använt hackare för att utföra cyberangrepp mot FN-personal för att sprida skadlig kod till deras datorer. Angriparna har skickat falska "Security-Alert"-meddelanden för att få offren att öppna e-postmeddelanden med skadlig kod.

September 2020

NSO Groups skadlig kod-program mot används WhatsApp (Underrättelseaktivitet). Enligt WhatsApp[150] har programvara från NSO Group använts för att angripa användare och leverera spionprogramvara till mobiltelefoner och andra mobila enheter bland annat i Togo. FN:s särskilda rapportör fördömde i sin rapport[151] att övervakningsprogramvara exporterades och användes mot journalister och människorättsaktivister och nämner specifikt incidenterna i Togo. Citizen Lab uppger[152] att målen för angreppen var religiösa företrädare och oppositionspolitiker. Förövarna uppges vara en hackergrupp som fått namnet REDLIONS, och misstänks företräda Togos regering.

USA:s presidentval angrips från flera länder (Underrättelseaktivitet). Microsoft rapporterar[153] att det amerikanska presidentvalet angripits av hackergrupper från flera länder. Bland annat Ryssland (Strontium), Kina, (Zirconium) och Iran (Phosphorous). Förutom ett stort antal individer har fler än tvåhundra organisationer, konsultfirmor och påtryckningsgrupper drabbats. Båda presidentkandidaternas kampanjer och företrädare har angripits. Microsoft noterar specifikt att angreppen nu också riktar sig mot rådgivare och konsulter som inte representerar politiska organisationer.

Pioneer Kitten angriper molntjänster (Underrättelseaktivitet)[17]**.** Enligt den amerikanska cybersäkerhetsmyndigheten CISA[154] och säkerhetspolisen FBI har Pioneer Kitten angripit ett stort antal mål i USA inom myndighets-, sjukvårds- finans-, och mediesektorerna. Pioneer Kitten anses vara en privat aktör i Iran som utför uppdrag åt den iranska regeringen men även agerar för egen vinnings skull. Förövarna har angripit offren via tidigare kända sårbarheter som offren underlåtit att skydda sig mot. Tillgång till några av offrens nätverksresurser har sedan sålts på hackerforum.

Pioneer Kitten angriper dissidenter i exil (Underrättelseaktivitet). Checkpoint Research hävdar i en rapport[155] att Pioneer Kitten under flera år ska ha spionerat på olika organisationer av intresse för den iranska regimen däribland dissidenter i exil och människorättsorganisationer som företräder iranska minoriteter.

APT28 anfaller Azerbajdzjan (Underrättelseaktivitet). Säkerhetsfirman Qi'anxins Red Raindrop Team upptäckte[156, s. 28] att APT28, en hackergrupp attribuerad till Ryssland, hade spridit spionprogramvara till opinionsledare och politiker i Azerbajdzjan. Enligt säkerhetsfirman Quintelligence[157] var en specifik myndighet målet för kampanjen. Förövarna använde förfalskade dokument rörande NATO-övningar som trojaner.

APT28 angriper en amerikansk myndighet (Underrättelseaktivitet). Cybersäkerhetsmyndigheten CISA och säkerhetspolisen FBI uppger[158] att en av USA:s myndigheter utsattes för ett framgångsrikt intrång. Wired Magazine skriver att spåren tyder på att förövarna var APT28[159].

Oktober 2020[18]

Diplomaters datorer hackade med UEFI-kod (Underrättelseaktivitet). Kaspersky Security skriver[160] i en rapport att de hittat skadlig kod som de tentativt kopplar till Winnti Umbrella. Koden har hittats i utrustning tillhörande diplomatmål i östra Asien. Angriparna använder den firmware som laddar in operativsystemet (Unified Extensible Firmware Interface, UEFI) för att lagra skadlig kod. Den skadliga koden verkar vara baserad på den information som 2015 läcktes från den italienska firman Hacking Team[161]. **Denna incident fanns inte med i CFR:s databas men inkluderades eftersom den är både tekniskt intressant och visar på hur cybervapen kan spridas mellan olika aktörer.**

November 2020

Cybersäkerhetsmyndigheten CISA pekar ut Kina (Underrättelseaktivitet). CISA och FBI pekar ut Kina som ansvariga för angrepp de senaste tio åren mot många sektorer inom myndigheter och industri[162]. De anger att Kinas statssäkerhetsministerium har ett antal olika organisationer aktiva med pågående spaning och cyberintrång mot andra länder. Några av grupperna arbetar både för egen vinning och för den kinesiska staten.

---

[17] Denna incident har klassats av memoförfattaren då den saknade klassning i databasen

[18] Oktober och november har endast en post vardera i databasen vilket troligen är ett resultat av förseningar i databasunderhållet och bör därför inte ses som en indikation att staters cyberaktiviteter plötsligt skulle ha minskat.

Titel/Title
Omvärldsbevakning: Statsattribuerade cyberoperationer 2020

Memo nummer/Number
FOI Memo 7422

Referenslista

[1] T. Sommestad och H. Karlzén, ”När luras personer av nätfiske?”, FOI-rapport FOI-R--4951--SE, apr. 2020.

[2] D. Lindahl, ”Cyberattacks in the healthcare sector during the first three months of the Covid-19 pandemic”, FOI, Memo 7062.

[3] D. Lindahl, ”Omvärldsbevakning statsattribuerade cyberoperationer 2019”, FOI Memo 6963, 2019.

[4] ”Pegasus: The ultimate spyware for iOS and Android”. https://www.kaspersky.com/blog/pegasus-spyware/14604/ (åtkomstdatum nov. 15, 2020).

[5] T. Brewster, ”Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text”, *Forbes*. https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/ (åtkomstdatum nov. 15, 2020).

[6] ”Morocco: Human Rights Defenders Targeted with NSO Group’s Spyware”. https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/ (åtkomstdatum nov. 15, 2020).

[7] ”About the Citizen Lab”, *The Citizen Lab*. https://citizenlab.ca/about/ (åtkomstdatum nov. 15, 2020).

[8] ”The Million Dollar Dissident: NSO Group’s iPhone Zero-Days used against a UAE Human Rights Defender”, *The Citizen Lab*, aug. 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (åtkomstdatum nov. 15, 2020).

[9] B. Marczak, J. Scott-Railton, A. Senft, B. Abdul, och R. Deibert, ”THE KINGDOM CAME TO CANADA”, s. 19.

[10] I. A. Stewart Phil, ”Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials”, *Reuters*, okt. 16, 2019.

[11] K. Poulsen, ”Russian Cyber Unit That Went Dark After Hacking DNC Is Still Spying”, *The Daily Beast*, okt. 17, 2019.

[12] ”Turla Group (Threat Actor)”. https://malpedia.caad.fkie.fraunhofer.de/actor/turla_group (åtkomstdatum nov. 15, 2020).

[13] ”Advisory: Turla group exploits Iranian APT to expand coverage of victims”. https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims (åtkomstdatum nov. 15, 2020).

[14] ”What we do”. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do (åtkomstdatum nov. 15, 2020).

[15] ”UK condemns Russia’s GRU over Georgia cyber-attacks”, *GOV.UK*. https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (åtkomstdatum nov. 15, 2020).

[16] ”U.S. and Allies Blame Russia for Cyberattack on Republic of Georgia - The New York Times”. https://www.nytimes.com/2020/02/20/world/europe/georgia-cyberattack-russia.html (åtkomstdatum nov. 15, 2020).

[17] ”Statement of the Polish MFA on cyberattacks against Georgia - Ministry of Foreign Affairs Republic of Poland - Gov.pl website”, *Ministry of Foreign Affairs Republic of Poland*. https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia (åtkomstdatum nov. 15, 2020).

[18] J. S. Bing Christopher, ”Uzbek spies attacked dissidents with off-the-shelf hacking tools”, *Reuters*, okt. 03, 2019.

[19] S. Gallagher, ”Kaspersky finds Uzbekistan hacking op… because group used Kaspersky AV”, *Ars Technica*, mar. 10, 2019. https://arstechnica.com/information-technology/2019/10/kaspersky-finds-uzbekistan-hacking-opbecause-they-used-kaspersky-av/ (åtkomstdatum nov. 15, 2020).

[20] ”Cyber Attack on ISRO: ISRO warned of a possible cyberattack when Dtrack came calling”. https://economictimes.indiatimes.com/tech/internet/isro-warned-of-a-possible-cyberattack-when-dtrack-came-calling/articleshow/71964232.cms (åtkomstdatum nov. 16, 2020).

[21] B. W. Desk, ”India plays down ISRO breach by suspected North Korean hackers”, *Brecorder*, nov. 07, 2019. http://www.brecorder.com/news/542425 (åtkomstdatum nov. 16, 2020).

[22] ”Assessment of Reported Malware Infection at Nuclear Facility | Dragos”, nov. 01, 2019. https://www.dragos.com/blog/industry-news/assessment-of-reported-malware-infection-at-nuclear-facility/ (åtkomstdatum nov. 16, 2020).

[23] ”Obfuscated APT33 C&Cs Used for Narrow Targeting”, *Trend Micro*. https://www.trendmicro.com/en_us/research/19/l/more-than-a-dozen-obfuscated-apt33-botnets-used-for-extreme-narrow-targeting.html (åtkomstdatum nov. 16, 2020).

[24] ”About Us”, *Trend Micro*. https://www.trendmicro.com/en_us/about.html (åtkomstdatum nov. 16, 2020).

[25] ”APT33 (Threat Actor)”. https://malpedia.caad.fkie.fraunhofer.de/actor/apt33 (åtkomstdatum nov. 16, 2020).

[26] ”盘旋在中亚上空的阴影-黄金雕（APT-C-34）组织攻击活动揭露”. (Läst via Google Translate), https://blogs.360.cn/post/APT-C-34_Golden_Falcon.html (åtkomstdatum nov. 16, 2020).

[27] ”关于 - 360 核心安全技术博客”. (Läst via Google Translate), https://blogs.360.cn/about (åtkomstdatum nov. 16, 2020).

[28] C. Cimpanu, ”Extensive hacking operation discovered in Kazakhstan”, *ZDNet*. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/ (åtkomstdatum nov. 16, 2020).

[29] ”Italian spyware company Hacking Team allegedly sold surveillance systems to repressive govts., emails leak reveals - Business & Human Rights Resource Centre”. https://www.business-humanrights.org (åtkomstdatum nov. 16, 2020).

[30] ”About Us | Ars Technica”. https://arstechnica.com/about-us/ (åtkomstdatum nov. 16, 2020).

[31] WIRED, ”A notorious Iranian hacking crew is targeting industrial control systems”, *Ars Technica*, nov. 23, 2019. https://arstechnica.com/information-technology/2019/11/a-notorious-iranian-hacking-crew-is-targeting-industrial-control-systems/ (åtkomstdatum nov. 16, 2020).

[32] ”About”, *SentinelLabs*. https://labs.sentinelone.com/about/ (åtkomstdatum nov. 16, 2020).

[33] ”Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting”, *SentinelLabs*, feb. 05, 2020. https://labs.sentinelone.com/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/ (åtkomstdatum nov. 16, 2020).

[34] ”Operation ENDTRADE: Multi-Stage Backdoors that TICK”, *Trend Micro*. https://www.trendmicro.com/en_us/research/19/k/operation-endtrade-finding-multi-stage-backdoors-that-tick.html (åtkomstdatum nov. 16, 2020).

[35] ”BRONZE BUTLER, REDBALDKNIGHT, Tick, Group G0060 | MITRE ATT&CK®”. https://attack.mitre.org/groups/G0060/ (åtkomstdatum nov. 16, 2020).

[36] ”BRONZE BUTLER | Secureworks”. https://www.secureworks.comhttp://www.secureworks.com/research/threat-profiles/bronze-butler (åtkomstdatum nov. 16, 2020).

[37] ”OAJ4VZNJ.pdf”. Åtkomstdatum: nov. 16, 2020. [Online]. Tillgänglig vid: https://www.ibm.com/downloads/cas/OAJ4VZNJ.

[38] ”The “Great Cannon” has been deployed again”. https://cybersecurity.att.com/blogs/labs-research/the-great-cannon-has-been-deployed-again (åtkomstdatum nov. 23, 2020).

[39] ”ChinasGreatCannon.pdf”. Åtkomstdatum: nov. 23, 2020. [Online]. Tillgänglig vid: https://citizenlab.ca/wp-content/uploads/2009/10/ChinasGreatCannon.pdf.

[40] ”security - What is randomly replacing Baidu TongJi (Analytics)’s Javascript code to make DDOS attack on websites on browser?”, *Stack Overflow*.

https://stackoverflow.com/questions/45874555/what-is-randomly-replacing-baidu-tongji-analyticss-javascript-code-to-make-dd (åtkomstdatum nov. 23, 2020).

[41] ”Autoindustrie im Visier von Hackern: BMW ausgespäht | BR24”. https://www.br.de/nachrichten/wirtschaft/fr-autoindustrie-im-visier-von-hackern-bmw-ausgespaeht,RjnLkD4 (åtkomstdatum nov. 23, 2020).

[42] ”Reputed Vietnamese APT group OceanLotus hacks BMW, Hyundai: report”, *SC Media*, dec. 09, 2019. https://www.scmagazine.com/home/security-news/apts-cyberespionage/reputed-vietnamese-apt-group-hacks-bmw-hyundai-report/ (åtkomstdatum nov. 23, 2020).

[43] ”About us - Fox-IT”, *Fox-IT (EN)*. https://www.fox-it.com/en/about/about-us/ (åtkomstdatum nov. 24, 2020).

[44] ”Advanced Persistent Threat Groups (APT Groups)”, *FireEye*. https://www.fireeye.com/current-threats/apt-groups.html (åtkomstdatum nov. 24, 2020).

[45] C. Cimpanu, ”Chinese hacker group caught bypassing 2FA”, *ZDNet*. https://www.zdnet.com/article/chinese-hacker-group-caught-bypassing-2fa/ (åtkomstdatum nov. 24, 2020).

[46] M. van Dantzig och E. Schamper, ”Shining a light on one of China’s hidden hacking groups”, s. 41.

[47] M. Mazzetti, N. Perlroth, och R. Bergman, ”It Seemed Like a Popular Chat App. It’s Secretly a Spy Tool.”, *The New York Times*, dec. 22, 2019.

[48] ”DarkMatter - Smart and Safe Digital | Safe and Smart Digital UAE | Cyber Security Specialists UAE | Cyber Solutions for Business| Network Defence Services | DarkMatter”. https://www.darkmatter.ae/ (åtkomstdatum nov. 24, 2020).

[49] C. Cimpanu, ”New Iranian data wiper malware hits Bapco, Bahrain’s national oil company”, *ZDNet*. https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/ (åtkomstdatum nov. 25, 2020).

[50] ”Operation AppleJeus Sequel”. https://securelist.com/operation-applejeus-sequel/95596/ (åtkomstdatum nov. 25, 2020).

[51] ”Operation AppleJeus: Lazarus hits cryptocurrency exchange with fake installer and macOS malware”. https://securelist.com/operation-applejeus/87553/ (åtkomstdatum nov. 25, 2020).

[52] ”North American Electric Cyber Threat Perspective”, s. 17, 2020.

[53] ”Iranian Hackers Have Been ‘Password-Spraying’ the US Grid”, *Wired*.

[54] N. Perlroth och M. Rosenberg, ”Russians Hacked Ukrainian Gas Company at Center of Impeachment”, *The New York Times*, jan. 13, 2020.

[55] ”Burisma: US firm says Russia hacked company at heart of Trump impeachment”, *BBC News*, jan. 14, 2020.

[56] ”Mitsubishi Electric Warns of Data Leak After Security Breach”, *BleepingComputer*. https://www.bleepingcomputer.com/news/security/mitsubishi-electric-warns-of-data-leak-after-security-breach/ (åtkomstdatum nov. 25, 2020).

[57] ”Japan investigates Mitsubishi Electric breach amid national security concerns”, *CyberScoop*, maj 20, 2020. https://www.cyberscoop.com/mitsubishi-japan-missile-data-breach/ (åtkomstdatum nov. 25, 2020).

[58] B. Hubbard och M. Schwirtz, ”Bezos Phone Hack Tied to Saudi Crown Prince Puts New Pressure on Kingdom”, *The New York Times*, jan. 22, 2020.

[59] ”OHCHR | UN experts call for investigation into allegations that Saudi Crown Prince involved in hacking of Jeff Bezos’ phone”. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25488&LangID=E (åtkomstdatum nov. 25, 2020).

[60] P. Rascagneres, ”KONNI: A Malware Under The Radar For Years”. http://blog.talosintelligence.com/2017/05/konni-malware-under-radar-for-years.html (åtkomstdatum nov. 25, 2020).

[61] ”Hackers spearphished U.S. government agency with North Korea-related content last year”, *CyberScoop*, jan. 23, 2020. https://www.cyberscoop.com/government-agency-spearphishing-unit-42/ (åtkomstdatum nov. 25, 2020).
[62] J. S. Menn Christopher Bing, Joseph, ”Exclusive: Hackers acting in Turkey’s interests believed to be behind recent cyberattacks - sources”, *Reuters*, jan. 27, 2020.
[63] ”Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator”, *The Citizen Lab*, jan. 28, 2020. https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/ (åtkomstdatum nov. 26, 2020).
[64] ”Intezer - New Iranian Campaign Tailored to US Companies Uses Updated Toolset”, *Intezer*, jan. 30, 2020. https://www.intezer.com/blog/apt/new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/ (åtkomstdatum nov. 26, 2020).
[65] C. Cimpanu, ”Iranian hackers target US government workers in new campaign”, *ZDNet*. https://www.zdnet.com/article/iranian-hackers-target-us-government-workers-in-new-campaign/ (åtkomstdatum nov. 26, 2020).
[66] C. Lab, ”Fake Interview: The New Activity of Charming Kitten - Certfa Lab”, *Certfa*. https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/ (åtkomstdatum nov. 26, 2020).
[67] R. S. Bing Christopher, ”Exclusive: Iran-linked hackers pose as journalists in email scam”, *Reuters*, feb. 05, 2020.
[68] ”Winnti Group targeting universities in Hong Kong”, *WeLiveSecurity*, jan. 31, 2020. https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/ (åtkomstdatum nov. 26, 2020).
[69] ”Winnti Group Infected Hong Kong Universities With Malware”, *BleepingComputer*. https://www.bleepingcomputer.com/news/security/winnti-group-infected-hong-kong-universities-with-malware/ (åtkomstdatum nov. 26, 2020).
[70] ”Gamaredon APT Improves Toolset to Target Ukraine Government, Military”. https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/ (åtkomstdatum nov. 26, 2020).
[71] ”MyCERT : Advisories - Espionage campaign targeting Malaysia government officials”. https://www.mycert.org.my/portal/advisory?id=MA-770.022020 (åtkomstdatum nov. 26, 2020).
[72] C. Cimpanu, ”Malaysia warns of Chinese hacking campaign targeting government projects”, *ZDNet*. https://www.zdnet.com/article/malaysia-warns-of-chinese-hacking-campaign-targeting-government-projects/ (åtkomstdatum nov. 26, 2020).
[73] ”Cyber attack on the Foreign Ministry is over – BMEIA, Außenministerium Österreich”. https://www.bmeia.gv.at/en/the-ministry/press/announcements/2020/02/cyber-attack-on-the-foreign-ministry-is-over/ (åtkomstdatum nov. 26, 2020).
[74] G. Corfield, ”Austrian foreign ministry: ’State actor’ hack on government IT systems is over”. https://www.theregister.com/2020/02/14/austria_foreign_ministry_hack_turla_group_allegs/ (åtkomstdatum nov. 26, 2020).
[75] ”Noch immer Cybergefechte im Netz des Außenministeriums”, *fm4.ORF.at*, jan. 19, 2020. https://fm4.orf.at/stories/2997349/ (åtkomstdatum nov. 26, 2020).
[76] ”ClearSky-Fox-Kitten-Campaign-v1.pdf”. Åtkomstdatum: nov. 26, 2020. [Online]. Tillgänglig vid: https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign-v1.pdf.
[77] C. Cimpanu, ”FBI says an Iranian hacking group is attacking F5 networking devices”, *ZDNet*. https://www.zdnet.com/article/fbi-says-an-iranian-hacking-group-is-attacking-f5-networking-devices/ (åtkomstdatum nov. 26, 2020).
[78] ”Hamas Android Malware On IDF Soldiers-This is How it Happened”, *Check Point Research*, feb. 16, 2020. https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/ (åtkomstdatum nov. 26, 2020).

[79] ”IDF stops Hamas ’honeypots’ from trapping soldiers”, *The Jerusalem Post | JPost.com*. https://www.jpost.com/israel-news/idf-foils-hamas-operation-targeting-soldiers-operation-rebound-617744 (åtkomstdatum nov. 26, 2020).

[80] P. Rascagneres, ”Bisonal: 10 years of play”. http://blog.talosintelligence.com/2020/03/bisonal-10-years-of-play.html (åtkomstdatum nov. 27, 2020).

[81] ”cds19-executive-s08-achievement-unlocked.pdf”. Åtkomstdatum: nov. 27, 2020. [Online]. Tillgänglig vid: https://www.fireeye.com/content/dam/fireeye-www/summit/cds-2019/presentations/cds19-executive-s08-achievement-unlocked.pdf.

[82] ”Vicious Panda: The COVID Campaign”, *Check Point Research*, mar. 12, 2020. https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/ (åtkomstdatum nov. 27, 2020).

[83] ”An APT exploits the coronavirus pandemic to spread malware”, *Panda Security Mediacenter*, mar. 23, 2020. https://www.pandasecurity.com/en/mediacenter/news/apt-coronavirus-malware/ (åtkomstdatum nov. 27, 2020).

[84] C. Cimpanu, ”State-sponsored hackers are now using coronavirus lures to infect their targets”, *ZDNet*. https://www.zdnet.com/article/state-sponsored-hackers-are-now-using-coronavirus-lures-to-infect-their-targets/ (åtkomstdatum nov. 27, 2020).

[85] ”A Viral Email About Coronavirus Had People Smashing Buses And Blocking Hospitals”, *BuzzFeed News*. https://www.buzzfeednews.com/article/christopherm51/coronavirus-ukraine-china (åtkomstdatum nov. 27, 2020).

[86] ”Operation C-Major (Threat Actor)”. https://malpedia.caad.fkie.fraunhofer.de/actor/operation_c-major (åtkomstdatum nov. 27, 2020).

[87] C. Cimpanu, ”APT28 has been scanning vulnerable email servers for more than a year”, *ZDNet*. https://www.zdnet.com/article/apt28-has-been-scanning-and-exploiting-vulnerable-email-servers-for-more-than-a-year/ (åtkomstdatum nov. 27, 2020).

[88] ”Pawn Storm in 2019: A Year of Scanning and Credential Phishing on High-Profile Targets”, s. 15.

[89] R. S. Bing Jack Stubbs, Christopher, ”Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike”, *Reuters*, mar. 24, 2020.

[90] ”Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links - TrendLabs Security Intelligence Blog”, mar. 24, 2020. https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/ (åtkomstdatum nov. 27, 2020).

[91] ”This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits”, *FireEye*. https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html (åtkomstdatum mar. 31, 2020).

[92] ”Chinese hackers hit Citrix, Cisco vulnerabilities in sweeping campaign - CyberScoop”. https://www.cyberscoop.com/apt-41-citrix-cisco-zoho-china-cyber-espionage-fireeye/ (åtkomstdatum nov. 27, 2020).

[93] ”Identifying vulnerabilities and protecting you from phishing”, *Google*, mar. 26, 2020. https://blog.google/threat-analysis-group/identifying-vulnerabilities-and-protecting-you-phishing/ (åtkomstdatum nov. 27, 2020).

[94] ”Saudi spies tracked phones using flaws the FCC failed to fix for years”, *TechCrunch*. https://social.techcrunch.com/2020/03/29/saudi-spies-ss7-phone-tracking/ (åtkomstdatum nov. 27, 2020).

[95] ”Targeted attacks using Fake Flash against Tibetans | Volexity”. https://www.volexity.com/blog/2020/03/31/storm-cloud-unleashed-tibetan-community-focus-of-highly-targeted-fake-flash-campaign/ (åtkomstdatum nov. 27, 2020).

[96] ”Holy water: ongoing targeted water-holing attack in Asia”. https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-asia/96311/ (åtkomstdatum nov. 27, 2020).

[97] J. M. Stubbs Christopher Bing, Raphael Satter, Jack, ”Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus - sources”, *Reuters*, apr. 02, 2020.
[98] D. of Defence, ”On the offensive against COVID-19 cyber criminals”, apr. 06, 2020. https://www.minister.defence.gov.au/minister/lreynolds/media-releases/offensive-against-covid-19-cyber-criminals (åtkomstdatum nov. 28, 2020).
[99] CISOMAG, ”Australia Launches Cyber Offence to Bring Down COVID-19 Scammers”, *CISO MAG | Cyber Security Magazine*, apr. 09, 2020. https://cisomag.eccouncil.org/how-the-australian-government-is-fighting-the-war-against-covid-19-scammers/ (åtkomstdatum nov. 28, 2020).
[100] ”Syrian government surveillance campaign turns to spreading malware in coronavirus apps”, *CyberScoop*, apr. 16, 2020. https://www.cyberscoop.com/coronavirus-syria-surveillance-apps-lookout/ (åtkomstdatum nov. 28, 2020).
[101] ”Nation-state Mobile Malware Targets Syrians with COVID-19 Lures”. https://blog.lookout.com/nation-state-mobile-malware-targets-syrians-with-covid-19-lures (åtkomstdatum nov. 28, 2020).
[102] ”Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage”, *FireEye*. https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html (åtkomstdatum nov. 28, 2020).
[103] ”Vietnamese hackers go after Beijing entities managing China coronavirus response”. https://www.cyberscoop.com/vietnam-coronavirus-china-apt32-fireeye/ (åtkomstdatum nov. 28, 2020).
[104] ”Atak dezinformacyjny na Polskę [PL/EN] - Służby specjalne - Portal Gov.pl”, *Służby specjalne*. https://www.gov.pl/web/sluzby-specjalne/atak-dezinformacyjny-na-polske (åtkomstdatum nov. 28, 2020).
[105] ”PhantomLance Android backdoor on Google Play”. https://www.kaspersky.com/blog/phantomlance-android-backdoor-trojan/35234/ (åtkomstdatum nov. 28, 2020).
[106] ”Kaspersky researchers catch Vietnamese hackers using Play Store to distribute apps”, *CyberScoop*, apr. 28, 2020. https://www.cyberscoop.com/vietnamese-hackers-google-play-kaspersky-apt32/ (åtkomstdatum nov. 28, 2020).
[107] ”Taiwan suggests Winnti group is behind ransomware attack on CPC Corp”, *CyberScoop*, maj 18, 2020. https://www.cyberscoop.com/cpc-ransomware-winnti-taiwan-china/ (åtkomstdatum nov. 28, 2020).
[108] ”Taiwan’s state-owned company CPC Corp. suffers ransomware attack”, *CyberScoop*, maj 05, 2020. https://www.cyberscoop.com/cpc-corp-ransomware-attack-taiwan-trend-micro/ (åtkomstdatum nov. 28, 2020).
[109] R. Bergman och S. L. Myers, ”China’s Military Is Tied to Debilitating New Cyberattack Tool”, *The New York Times*, maj 07, 2020.
[110] T. O. I. staff, ”Israel aghast at Iran cyberattack on civilian water infrastructure — TV report”. https://www.timesofisrael.com/israel-aghast-at-iran-cyberattack-on-civilian-water-infrastructure-tv-report/ (åtkomstdatum nov. 28, 2020).
[111] AP and TOI staff, ”‘Cyber winter is coming,’ warns Israel cyber chief after attack on water systems”. https://www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/ (åtkomstdatum nov. 28, 2020).
[112] T. O. I. staff, ”Israel behind cyberattack that caused ‘total disarray’ at Iran port – report”. https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/ (åtkomstdatum nov. 28, 2020).
[113] ”MAR-10288834-1.v1 – North Korean Remote Access Tool: COPPERHEDGE | CISA”. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-133a (åtkomstdatum nov. 28, 2020).
[114] ”US to call out another round of North Korean hacking”, *CyberScoop*, maj 12, 2020. https://www.cyberscoop.com/north-korea-hacking-hidden-cobra-dhs-fbi/ (åtkomstdatum nov. 28, 2020).

[115] ”People’s Republic of China (PRC) Targeting of COVID-19 Research Organizations — FBI”. https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations (åtkomstdatum nov. 28, 2020).

[116] L. Camastra, ”APT Group Planted Backdoors Targeting High Profile Networks in Central Asia”, *Avast Threat Labs*, maj 14, 2020. https://decoded.avast.io/luigicamastra/apt-group-planted-backdoors-targeting-high-profile-networks-in-central-asia/ (åtkomstdatum nov. 28, 2020).

[117] ”’Greenbug’ hacking group hits three telecom firms in Pakistan”, *CyberScoop*, maj 19, 2020. https://www.cyberscoop.com/greenbug-symantec-iran-hacking-pakistan/ (åtkomstdatum nov. 28, 2020).

[118] ”Sophisticated Espionage Group Turns Attention to Telecom Providers in South Asia”. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/greenbug-espionage-telco-south-asia (åtkomstdatum nov. 28, 2020).

[119] ”No “Game over” for the Winnti Group”, *WeLiveSecurity*, maj 21, 2020. https://www.welivesecurity.com/2020/05/21/no-game-over-winnti-group/ (åtkomstdatum nov. 28, 2020).

[120] M. Hill, ”Winnti Group Targets Video Game Developers with New Backdoor Malware”, *Infosecurity Magazine*, maj 21, 2020. https://www.infosecurity-magazine.com:443/news/winnti-video-game-developers/ (åtkomstdatum nov. 28, 2020).

[121] ”Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf”. Åtkomstdatum: nov. 28, 2020. [Online]. Tillgänglig vid: https://www.bitdefender.com/files/News/CaseStudies/study/332/Bitdefender-Whitepaper-Chafer-creat4491-en-EN-interactive.pdf.

[122] ”German intelligence agencies warn of Russian hacking threats to critical infrastructure”, *CyberScoop*, maj 26, 2020. https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/ (åtkomstdatum nov. 28, 2020).

[123] ”Exim Mail Transfer Agent Actively Exploited by Russian GRU Cyber Actors”, *National Security Agency Central Security Service*. https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/ (åtkomstdatum nov. 28, 2020).

[124] ”Gamaredon group grows its game”, *WeLiveSecurity*, juni 11, 2020. https://www.welivesecurity.com/2020/06/11/gamaredon-group-grows-its-game/ (åtkomstdatum nov. 28, 2020).

[125] ”Operation In(ter)ception: Starting with a LinkedIn message, threat actors went after both secret information and money”. https://www.eset.com/us/about/newsroom/press-releases/operation-interception-starting-with-a-linkedin-message-threat-actors-went-after-both-secret-inf/ (åtkomstdatum nov. 28, 2020).

[126] ”’Sophisticated state-based’ cyber attack hits Australia”. https://www.9news.com.au/national/cyber-attack-australia-scott-morrison-government-private-sector-breach-of-security/e621ae47-f810-4fa7-9c11-3caa3b09f4dc (åtkomstdatum nov. 28, 2020).

[127] ”Australia blames a state actor for major disruptions. China is already denying it.”, *CyberScoop*, juni 19, 2020. https://www.cyberscoop.com/australia-cyber-attack-china-trade-scott-morrison/ (åtkomstdatum nov. 28, 2020).

[128] ”ישראל מים מתקני על סייבר מתקפת :שוב”, (Läst via Google Translate), *ynet*, juli 16, 2020. https://www.ynet.co.il/news/article/rJrCqmAkw (åtkomstdatum nov. 28, 2020).

[129] C. Cimpanu, ”Two more cyber-attacks hit Israel’s water system”, *ZDNet*. https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/ (åtkomstdatum nov. 28, 2020).

[130] ”Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research”, juli 21, 2020.

https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion (åtkomstdatum nov. 28, 2020).
[131] ”f.pdf”. Åtkomstdatum: nov. 28, 2020. [Online]. Tillgänglig vid: https://www.politico.com/f/?id=00000173-76e6-d36e-abff-7ffe63dc0000.
[132] C. Cadell, ”U.S. cybersecurity firm says Beijing-linked hackers target Vatican ahead of talks”, *Reuters*, juli 29, 2020.
[133] ”Chinese State-Sponsored Group ’RedDelta’ Targets the Vatican and Catholic Organizations”, s. 21.
[134] ”Ghostwriter-Influence-Campaign.pdf”. Åtkomstdatum: nov. 28, 2020. [Online]. Tillgänglig vid: https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/Ghostwriter-Influence-Campaign.pdf.
[135] ”’Ghostwriter’ Influence Campaign: Unknown Actors Leverage Website Compromises and Fabricated Content to Push Narratives Aligned With Russian Security Interests”, *FireEye*. https://www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html (åtkomstdatum nov. 28, 2020).
[136] ”Russian cyber attack campaigns and actors”. https://www.ironnet.com/blog/russian-cyber-attack-campaigns-and-actors (åtkomstdatum nov. 28, 2020).
[137] J. S. Faulconbridge Guy, ”Exclusive: Papers leaked before UK election in suspected Russian operation were hacked from ex-trade minister - sources”, *Reuters*, aug. 03, 2020.
[138] ”MAR-10292089-1.v2 – Chinese Remote Access Trojan: TAIDOOR | CISA”. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a (åtkomstdatum nov. 28, 2020).
[139] ”Evasive Tactics: Taidoor”, *FireEye*. https://www.fireeye.com/blog/threat-research/2013/09/evasive-tactics-taidoor-3.html (åtkomstdatum nov. 28, 2020).
[140] ”FBI warns about Iranian hacking group attacking F5 networking devices | Cybersafe News”, aug. 10, 2020. https://www.cybersafe.news/fbi-warns-about-iranian-hacking-group-attacking-f5-networking-devices/ (åtkomstdatum nov. 28, 2020).
[141] ”US Hackers’ Strike on Russian Trolls Sends a Message—but What Kind?”, *Wired*.
[142] M. A. Thiessen, ”Opinion | Trump confirms, in an interview, a U.S. cyberattack on Russia”, *Washington Post*.
[143] ”Dream-Job-Campaign.pdf”. Åtkomstdatum: nov. 28, 2020. [Online]. Tillgänglig vid: https://www.clearskysec.com/wp-content/uploads/2020/08/Dream-Job-Campaign.pdf.
[144] ”MAR-10295134-1.v1 – North Korean Remote Access Trojan: BLINDINGCAN | CISA”. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-232a (åtkomstdatum nov. 28, 2020).
[145] Y. Lee, ”Taiwan says China behind cyberattacks on government agencies, emails”, *Reuters*, aug. 19, 2020.
[146] ”Mainland hackers attacked government agencies to steal data, Taiwan says”, *South China Morning Post*, aug. 19, 2020. https://www.scmp.com/news/china/diplomacy/article/3098012/mainland-chinese-hackers-attacked-government-agencies-steal (åtkomstdatum nov. 28, 2020).
[147] Utenriksdepartementet, ”Datainnbruddet i Stortinget”, *Regjeringen.no*, okt. 13, 2020. https://www.regjeringen.no/no/aktuelt/pm_inbrudd/id2770135/ (åtkomstdatum nov. 28, 2020).
[148] ”FASTCash 2.0: North Korea’s BeagleBoyz Robbing Banks | CISA”. https://us-cert.cisa.gov/ncas/alerts/aa20-239a (åtkomstdatum nov. 28, 2020).
[149] ”pdf.pdf”. Åtkomstdatum: nov. 28, 2020. [Online]. Tillgänglig vid: https://undocs.org/pdf?symbol=en/S/2020/840.
[150] ”WhatsApp FAQ - Protecting our users from a video calling cyber attack”, *WhatsApp.com*. https://faq.whatsapp.com/general/security-and-privacy/protecting-our-users-from-a-video-calling-cyber-attack/?lang=sv (åtkomstdatum nov. 29, 2020).
[151] ”A_HRC_41_35.odt”. .
[152] ”Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware”, *The Citizen Lab*, aug. 03, 2020. https://citizenlab.ca/2020/08/nothing-sacred-nso-sypware-in-togo/ (åtkomstdatum dec. 01, 2020).

[153] ”New cyberattacks targeting U.S. elections”, *Microsoft On the Issues*, sep. 10, 2020. https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/ (åtkomstdatum nov. 29, 2020).
[154] ”Iran-Based Threat Actor Exploits VPN Vulnerabilities | CISA”. https://us-cert.cisa.gov/ncas/alerts/aa20-259a (åtkomstdatum nov. 29, 2020).
[155] ”Rampant Kitten - An Iranian Espionage Campaign”, *Check Point Research*, sep. 18, 2020. https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign/ (åtkomstdatum nov. 29, 2020).
[156] ”APT28 新动向：针对阿塞拜疆国内政治、社会知名人士进行定向攻击”. (Läst via Google Translate), https://www.secrss.com/article/24798 (åtkomstdatum nov. 29, 2020).
[157] ”APT28 Delivers Zebrocy Malware Campaign Using NATO Theme as Lure”, *QuoIntelligence*, sep. 22, 2020. https://quointelligence.eu/2020/09/apt28-zebrocy-malware-campaign-nato-theme/ (åtkomstdatum nov. 29, 2020).
[158] ”Federal Agency Compromised by Malicious Cyber Actor | CISA”. https://us-cert.cisa.gov/ncas/analysis-reports/ar20-268a (åtkomstdatum nov. 29, 2020).
[159] ”Russia’s Fancy Bear Hackers Likely Penetrated a US Federal Agency”, *Wired*.
[160] ”MosaicRegressor: Lurking in the Shadows of UEFI”. https://securelist.com/mosaicregressor/98849/ (åtkomstdatum nov. 29, 2020).
[161] ”A China-Linked Group Repurposed Hacking Team’s Stealthy Spyware”, *Wired*.
[162] ”Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity | CISA”. https://us-cert.cisa.gov/ncas/alerts/aa20-258a (åtkomstdatum nov. 29, 2020).