**Covid-19-pandemins inverkan på skadlig programvara**

Namn: Jens Sabel

Studienummer: 1800143

Handledare: Mats Aspnäs

Inriktning: Datateknik

Åbo Akademi, Informationsteknologi

Referat

I denna avhandling undersöks hur Covid-19 pandemin inverkade på skadlig programvara. Avhandlingen är uppdelad i två olika tidsperioder, före och efter pandemins början, där dessa jämförs med varandra. Avhandlingen är begränsad till sådan skadlig programvara som direkt eller indirekt påverkar företag, skolor och myndighetsinstitutioner.

Efter att ha undersökt tiden före och efter pandemin ser man en tydlig trend av pandemi-inspirerande datorvirus. Själva strukturen på datorvirusen har inte kunnat konstaterat ha ändrats destomera utifrån de rapporter som existerar för tillfället. Det är snarare än förändring hur olika datorvirus sprider sig där man kan notera förändringar som direkt eller indirekt är en biprodukt av coronapandemin. För att hitta rent strukturella förändringar inom 20-talets datorvirustyper behövs mer forskning i ämnet.

Sökord

Covid-19, Skadlig programvara, Datorvirus, Trender, Mobilvirus

Innehållsförteckning:

[1. Inledning 4](#_Toc97236175)

[2. Datorvirus före coronapandemin 5](#_Toc97236176)

[2.1 Samhällssituationen före coronapandemin 5](#_Toc97236177)

[2.2 Trendande datorvirus före pandemin 5](#_Toc97236178)

[2.3 Exempel på datorvirusens uppbyggnad och spridningsmetoder 9](#_Toc97236179)

[3. Trendande datorvirus under coronapandemin 11](#_Toc97236180)

[3.1 Bakgrund 11](#_Toc97236181)

[3.2 Trendande datorvirus för datorer 11](#_Toc97236182)

[3.3 Trendande datorvirus för smarttelefoner 15](#_Toc97236183)

[3.4 Exempel på datorvirusens uppbyggnad och spridningsmetod 16](#_Toc97236184)

[4. Jämförelse mellan före och efter coronapandemins början 18](#_Toc97236185)

[5. Avslutning 18](#_Toc97236186)

[6. Källor 20](#_Toc97236187)

# 1. Inledning

Den samhälleliga förändringen som skedde under åren 2020 och 2021 till följd av coronapandemin har påverkat vardagen på många, mer eller mindre, förutsägbara sätt. Pandemin påtvingade samhälleliga förändringar som ändrade på hur vi kommunicerar, arbetar, sköter våra vardagliga ärenden samt hur vi utövar våra fritidsintressen. Många länder stadfäste lagar och förordningar på hur vi skulle ändra våra levnadssätt för att bäst bekämpa pandemin och säkerställa att så många som möjligt skulle skyddas från pandemin. Parallellt med pandemin utvecklades också en annan typ av virushot, nämligen datorvirus.

Målet med denna avhandling är att försöka hitta en korrelation mellan coronapandemin och dess inverkan på datorvirus. Avhandlingen behandlar några exempel på virustyper som dominerat under de olika tidsperioderna före och efter corona­­pandemin. Avhandlingen begränsar sig till de virustrender som direkt eller indirekt rör arbetslivet, studerande, myndigheter samt de mest populära trenderna inom it.

I denna avhandling undersöks hur coronapandemin påverkade skadlig programvara. Först undersöks vilka trender inom datorvirus och spridningsmetoder som fanns innan 2020. Fokus skiftar sedan till vilka trender som har utmärkt sig under pandemiåren 2020 och 2021. Slutligen kommer dessa båda tidsperioders trender att jämföras med varandra. För att minska på företags jävighet till sina egna produkter och dess möjliga inverkan på deras rapporter har denna avhandling baserat sig mestadels på källor från IEEE samt på rapporter från Europeiska unionens cybersäkerhetsbyrå Enisa. Rapporter från företag används endast för att förtydliga det som redan tagits upp av respekterade källor eller för att få ett annat perspektiv om ämnet i fråga. Förutom detta kan även källor referera till nyhetsartiklar för att förtydliga att en viss trend har varit så påtaglig så att nyheterna runtom världen har skrivit om ämnet.

Avhandlingen är skriven med hypotesen att datorvirus har ändrat hur de attackerar, hur de sprids samt vad som själva datorviset riktar in sig på. Hypotesen finner stöd i det förändrade samhällsläget som ändrade på arbetsmiljön för många miljontals människor. Detta ämne är av högsta relevans i dagens samhälle där vi förlitar oss mer och mer på olika tekniska hjälpmedel för att fungera i samhället. Pandemin påtvingade även att vi tvingades förlita oss mera på kommunikation via tekniska hjälpmedel i stället för

Avhandlingen är strukturerad så att liknande kategorier tas upp både före och efter coronapandemins början. I fall där nya datorvirushot har uppenbarat sig under pandemin påpekas saken tydligt för att uppmärksamma en tydlig skillnad. Efter att rapporter från de senaste fyra åren har blivit undersökta jämförs de trender som existerat under denna tidsperiod med varandra.

# 2. Datorvirus före coronapandemin

## 2.1 Samhällssituationen före coronapandemin

Värt att komma ihåg före pandemins början var att människor hade i genomsnitt mer kontakt ansikte mot ansikte. Arbetsmiljön var koncentrerad till företagens egna utrymmen. På fritiden kunde man gå till restaurangen för att äta mat på plats samt så kunde man ta sig en kopp kaffe på sitt lokala café. De nyaste filmerna visades på biografer runtom i världen till fullsatta biosalonger.

På den ekonomiska sidan ser man en tydlig trend på kryptovalutors popularitet. I en rapport [1] skriven av forskare vid ett australienskt universitet syns det redan 2018 en ökning i användningen av kryptovalutor för illegala ändamål. Kryptovalutors popularitet har förutom i illegala syften också blivit populärare bland legitima företag. Idag finns det många företag i väst som använder sig av kryptovalutor som godkänd betalningsmetod [2]. Som exempel hittar man några av de stora IT-jättarna Microsoft, Amazon och PayPal. I samma rapport hittas även att de som värnar om dess anonymitet gärna använder kryptovalutor för att investera med för att säkerställa att investeringen inte kan kopplas till sig själv.

## 2.2 Trendande datorvirus före pandemin

Enligt Europeiska unionens cybersäkerhetsbyrå Enisa var den vanligaste typen av cyberattacker gentemot företag och individer datorvirusattacker [3]. Dessa stod för 30% av alla attacker som orsakade dataförlust. I samma rapport ser man en tabell över de topp 15 vanligaste typerna av datorvirus för året 2018. Enligt Enisa har majoriteten av de topp 15 vanligaste virustyperna stigit i användning eller hållit sig på en stabil nivå. Endast ett fåtal attacktyper konstaterades falla i antalet upptäckta fall. Dessa var datorvirus som installeras via en så kallad insider på ett företag, gisslanprogram samt cyberspionage. Den enda nya kategorin på virushot som introducerades 2018 var kryptokapning.

Kryptokapning definieras enligt den svenska ordboken IT-ord som ”det att en angripare i hemlighet använder andras webbläsare för att bryta kryptovaluta”. I andra ord kan man säga att kryptokapning går ut på att man i hemlighet använder sig av en del av en annan persons dator i hens ovetskap för att kunna bryta kryptovaluta för sin egen vinst. Enligt Enisas rapport [3] ökade denna typ av datorvirus med 629 % under det första kvartalet av 2018. En orsak som tas upp i en rapport [4] av Symantec, publicerad samma år, kan denna trend förklaras av virustypens enkelhet. Enligt rapporten behövs endast ett par rader med kod för att producera ett välfungerande kryptokapningsvirus. Rapporten antyder också att orsaken till denna drastiska ökning är att värdet på kryptovalutor har ökat betydligt. ”Coin Mining: A modern gold rush”, eller på svenska ”Kryptokapning, en modern guldrush”, är det som rapporten vill framföra. I grafen nedan visas värden på den populära kryptovalutan bitcoin från oktober 2013 till februari 2022. Grafen visar på att Bitcoin ökade markant i värde redan i slutet av 2017, början av 2018. Eftersom datorvirus även följer trender inom samhället och ”går dit pengarna finns”, så stöder denna graf rapportens utlåtande.



Figur 1: Värde på Bitcoin under åren 2013–2022 Länk: https://www.statista.com/statistics/326707/bitcoin-price-index/

Före pandemiåret 2020 fanns det även en tydlig ökande trend för datorvirus som riktar in sig på mobiltelefoner eller smarttelefoner. Enligt flertalet rapporter [3,4,5] ökade antalet skadlig programvara för mobiltelefoner stadigt varje år före 2020. Enisas rapport [3] tar bland annat upp att denna trend amplifieras på grund av att många väljer att använda sina telefoner så länge att smarttelefonens operativsystem inte längre underhålls med nya säkerhetsuppdateringar. Hit kan man dra paralleller med när Windows bestämde sig för att avsluta sina säkerhetsuppdateringar till äldre operativsystem så som exempelvis Windows 7 och Windows XP. Ett operativsystem som inte underhålls med säkerhetsuppdateringar medför logiskt sett med tiden en större och större risk för användaren.

Enligt rapporten från Symantec [4] designades hälften av alla mobilvirus att se ut som applikationer från tre olika kategorier: Livsstil, Musik & Ljud samt Böcker & Referenser. Totalt stod dessa för 56,9 % av alla mobilvirustyper med påstådda livsstilsapplikationer som största andel av dessa. En högst relevant statistik som rapporten även har tar upp är att 2017 använde endast 20 % av alla Android telefoner den senaste uppdaterade operativsystems-versionen [4]. Samma siffra var 77,3 % för telefoner som körde på Apples operativsystem IOS. Med dessa siffror kan man se att Androidanvändare har i genomsnitt en betydligt högre risk för att bli infekterade med virus som använder sig av äldre androidversioners sårbarheter.

Enligt rapporten från Enisa [4] var 2018 det år då virus inriktade på säkerhetskritiska system blev ett hot. Triton-viruset blev det första observerade datorviruset som specifikt riktade in sig på säkerhetsinstrument. De flesta säkerhetsinstrument är designade så att de direkt stoppar en process när systemet upplever att något är utanför det normala. Eftersom viruset riktar in sig på att ändra på något systemkritisk så tvingar därmed viruset systemet att helt stoppa. Detta kan då i sin tur leda till en finansiell börda för företag ifall dess produktion blir avstannad för längre perioder. Enligt en rapport publicerad av Black Hat USA [7] användes denna typ av attack gentemot ett Saudi arabiskt oljeraffinaderi för att stänga ner hela företagets produktion. Själva datorviruset riktade in sig på de säkerhetssystem som övervakade raffinerandet av olja. Efter att säkerhetssystemet upptäckte en drastisk förändring av säkerhetskritiska värden stängde systemet som väntat ner produktionen och fick hela produktionslinjen att stoppa. Vid en första granskning såg det ut som vilken som helst nedstängning men efter att man forskat i vad som orsakade produktionsstoppet såg man klart och tydligt att det var ett datorvirus som orsakade nedstängningen.

Enligt Enisa [3] var ”Githubifieringen” av IT-säkerhetsbranschen en noterbar trend som har fortsatt att öka för varje år framtill 2018. Med ”Githubifiering” menas att allt fler verktyg som används för olika säkerhetstester överförs till olika plattformar som är tillgängliga för alla. Dessa säkerhetsprogram blir då allt mera öppen mjukvara. Enligt en undersökning [8] publicerad av två forskare vid Dalhousie universitet i Kanada kunde några av dessa öppna mjukvaruapplikationer stoppa mellan trettio och fyrtio procent av alla virustyper som ett system utsattes för. I rapporten framkommer dock att dessa applikationer kräver mera utveckling för att bli effektivare. En rekommendation som rapporten [8] också framhäver är att i kombination med annan säkerhetsprogramvara blir säkerhetsgraden högre. Förutom dessa antivirusprogram finns även verktyg för utnyttjande av säkerhetsbrister. Metasploit är ett exempel som syns i Enisas rapport [3]. Metasploit [9] är ett öppet mjukvaruprogram som tillåter användaren att leta efter och utnyttja säkerhetsbrister i olika typ av programvara. Själva programmet ägs av det amerikanska säkerhetsföretaget Rapid7 men användningen av programvaran är öppen för alla. Enligt Enisas rapport [3] använder många cyberbrottsgrupper just dessa typer av programvara för att genomföra sina attacker.

I en vetenskaplig artikel [6] som publicerades 2018 undersöktes de totala trenderna över antalet datorvirusattacker och hur stor andel av dessa som var nya virustyper. Resultatet finns åskådliggjort i grafen nedan.



Figur 2: Grafen visar virustrenderna före 2018. Bilden hämtad från: https://www.researchgate.net/profile/Anitta-Patience-Namanya/publication/327665678\_The\_World\_of\_Malware\_An\_Overview/links/5ba1ef8e299bf13e603bd0fe/The-World-of-Malware-An-Overview.pdf

Från grafen kan man avläsa att den totala mängden virustyper som förekommit under åren 2007 till 2018. Under de senaste tre åren, sedan rapporten fastställdes, kan man se en sjunkande trend i antalet nya virustyper som förekommit. Överlag har antalet virus som förekommit ökat för varje år, med högst ökning mellan 2013 och 2018.

## 2.3 Exempel på datorvirusens uppbyggnad och spridningsmetoder

En av de vanligaste virustyperna som förekom 2017 var Wannacrypt0r-viruset, mer känt som ”WannaCry”. Både Enisas och Symantecs rapporter [3, 4] för 2017 och 2018 bekräftar att detta virus dominerat marknaden till andelen upptäckta fall. WannaCry-viruset var uppbyggt som ett normalt utpressningsvirus [10]. När användaren laddat ner utpressningsviruset krypterades mer eller mindre hela datorn. För att få tillbaka sina filer, eller få sina filer dekrypterade, var man tvungen att betala en viss summa i Bitcoin som lösensumma. Enligt samma rapport [10] behöver denna typ av virus följande tre grundsteg: Viruset ska kunna läsa in all data, viruset ska kunna kryptera eller skriva över den befintliga data och viruset ska kunna ta bort all data helt och hållet. Fungerar alla dessa steg har man uppnått ett välfungerande utpressningsvirus.

En typ av datorvirus som utmärkte sig under 2018 var utvecklingen av så kallade fillösa datorvirustyper [3]. Med dessa menas virus som inte direkt existerar fysiskt på en användares maskin utan virus som åberopar något kommando som i sin tur förutsätter datorn för något godtyckligt virushot. Dessa virustyper har varit extra svåra att för antivirusprogram att förhindra [10]. Detta på grund av att dessa virustyper oftast sprider sig tillsammans med ett annat program. Ett exempel på en virusfamilj som rapporten från Financial Technology [10] tar fram är PoshCoder. PoshCoder är helt och hållet skriver i PowerShell vilket betyder att viruset endast existerar i arbetsminnet och inte skrivs till lagringsminnet. Rapporten [10] tar även upp att man från PowerShell kan ladda över dessa skript till en USB-sticka. Därefter kan man sätta in denna USB-sticka i en dator som sedan snabbt exekverar de kodrader som finns färdigt inställda. Denna spridningsmetod förutsätter att man fysiskt tar sig till den plats som man vill attackera och är därmed något begränsad till spridningssättet.

En annan populär spridningsmetod som datorvirus har börjat använda sig mer av är sårbarheter i produkter från Microsoft. Ett botnätprogram vid namn Emotet, som enligt Enisas rapport [3] användes ofta under 2018, använde sig just av denna spridningsmetod. Europeiska unionens byrå för brottsbekämpning Europol släppte i början av 2021 en artikel [15] över hur Emotet hade blivit stoppat tack vare ett internationellt samarbete mellan flertalet länder. I artikeln beskrivs det att Emotet spred sig via word-dokument. Genom att helt automatisera processen från att man först installerar word-dokumentet på sin dator till att ens dator blivit del av ett större botnätverk så blev Emotet ett datorvirus som fick stor spridning under åren före 2021. Många olika sätt användes för att lura användaren till att öppna dessa dokument, exempelvis kunde dessa skadliga dokument maskera sig som fakturor eller som fraktsedlar. När användaren öppnade dokumentet blev de mötta med ett meddelande som bad användaren att aktivera makron för dokumentet. Aktiverade man dessa makron kunde den medföljande skadliga koden köra och datorn blev då infekterad av Emotet-viruset.

Följande datorvirus följde även en så kallad ”virus-som-en-service”-modell. Efter att en dator blev infekterad med Emotet-viruset försattes den infekterade datorn med i ett nätverk med andra infekterade datorer. Dessa datorer byggde tillsammans ett kraftfullt nätverk som kunde utföra olika uppdrag [15]. Enligt en rapport publicerad i ScienceDirect [16] cirkulerar dessa nätverk runt på djupwebben som vilken aktör som helst kan betala för att använda. Rapporten konstaterar dock att denna typ av service inte har kunnat etablera sig på en större skala då dessa typ av datorvirusattacker inte kan autentiseras vara verkliga på förhand. Denna typ av virusservice finns även noterad i Enisas rapport [3].

En annan spridningsmetod som riktade in sig på mobiltelefoner var DNS-attacker. Dessa attacker blev vanliga under åren före coronapandemin och enligt Enisas rapport [3] skulle bli vanligare för varje år. I en artikel publicerad av cybersäkerhetsföretaget Kaspersky beskrivs hur denna typ av attack genomförs [17]. Först infekteras en valfri router, förslagsvis en router på ett café dit många kunder kopplar upp till caféets wi-fi. När en användare kopplar upp sig till den infekterade routern och försöker koppla till någon URL-adress blir man genast förd till en annan sida som innehåller något godtyckligt virus.

”Roaming Manits”-datorviruset som tas upp i Kasperskys artikel [17] skickar användaren vidare till en hemsida som ber användaren att uppdatera telefonens webbläsare. Då användaren laddar ner denna påstådda uppdatering tar datorviruset och erhåller de nödvändiga behörigheter och information som krävs för att stjäla användarens uppgifter till Google. Under 2018 fanns det en ökande trend av denna typ av datorvirusattacker som dels berodde på den generella ökande trenden inom datorvirus inriktade på mobiltelefoner [3].

# 3. Trendande datorvirus under coronapandemin

* 1. Bakgrund

Efter att coronapandemin spred sig globalt från och med början av 2020 ändrades vår vardag markant. Uppgifter som förut gjordes på en fysisk plats var nu tvungna att övergå till att skötas digitalt. Arbetsmiljön övergick från en företagens egna arbetsutrymmen till hemmakontor, detta som en del av den strategi som de flesta länder införde för att försöka stoppa coronavirusspridningen. Anställda tvingades nu mer eller mindre stå själva för att säkra deras hemnätverk och ta tillräckliga steg för att förebygga datorvirusspridning, en uppgift som nätverksadministratörer och it-personal skötte när arbetsmiljön var centrerad till företagets egna lokaler.

Den omställning som skedde på arbetsplatserna var tvungen att ske snabbt och många företag var inte beredda för en sådan stor omställning. Flertalet rapporter [12,13,14] berättar om att det dels var på grund av denna snabba omställning som flertalet virus försökte ta vara på chansen och utnyttja denna nya osäkerhet i samhället. I följande kapitel undersöks datorvirus under tiden efter coronapandemins start.

Noterbart är att cyberattacker kontinuerligt ökar vartefter tillgängligheten till internet och teknologi ökar. Enligt en rapport publicerad till IEEE [18] bidrar följande fenomen till denna ökning: ökning av antalet internetanvändare, ökning av antalet internet­uppkopplade enheter, ökande komplexitet av internettjänster, ökande digitalisering samt skiftande fokus för kriminella. Rapporten tar upp det faktum att brott gjorda över nätet kommer med en betydligt lägre risk än brott som sker fysiskt på plats.

* 1. Trendande datorvirus för coronapandemin

Den Europeiska unionens cybersäkerhetsbyrå Enisa har valt att klassificera in de mest trendande datorvirushoten i åtta olika kategorier för år 2021[13]: gisslanprogram, skadeprogram, kryptokapningsvirus, mejl-relaterade virus, dataläckor, överbelastnings­attacker, desinformationsattacker och icke-skadliga virushot. Till de icke-skadliga virushoten hör sådana program som inte direkt orsakar någon direkt skada för användaren. Exempel på sådana virus är så kallade reklamvirus vars enda uppgift är att visa extra reklam på användarens dator.

Enligt en rapport [14] publicerad 2020 har coronapandemin orsakat stora ekonomiska bördor för både privatpersoner, myndigheter och företag. Enligt rapporten orsakade coronavirusrelaterade datorvirusskador till ett värde av 12 miljoner dollar mellan januari och april 2020. Samma rapport har även undersökt rapporter från Singapore och Australien som indikerar på att coronapandemin har gett inspiration till nya coronavirusrelaterade bedrägerier. Redan under första kvartalet av 2020 upptäcktes 394 nya coronavirusrelaterade bedrägerier.



Figur : Sektorer som blev attackerade per nummer av upptäckta fall (april 2020 till juli 2021). Bilden är tagen från Enisas datorvirusrapport för 2021: [https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport](https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/%40%40download/fullReport), Hämtad 19.3.2022

I figuren ovan syns andelen attacker gentemot olika sektorer i samhället. En trend som Enisas rapport [13] tar upp är att antalet attacker gentemot myndighetstjänster har ökat märkbart. Grafen visar även på att leverantörer av digitala tjänster samt hälsovårdsinstitutioner också varit målet för många av de cyberattacker som skedde under 2021. Överlag noterade rapporten [13] att andelen cyberincidenser gentemot enskilda användare ökade medan cyberincidenser gentemot hela sektorer minskade något. Detta fenomen kan förklaras med det distansarbete som coronapandemin påtvingade. Den internationella organisationen för kriminalpoliskårer Interpol varnade redan 2020 [18] för att det kaos som blev påtvingat på grund av den nya samhällsbilden kunde signifikant öka antalet utpressningsattacker gentemot olika samhällsaktörer, speciellt hälsovårds­institutioner.

I en rapport som publicerades juni 2020 [14] undersöks de första effekterna av coronapandemin på datorvirus. Redan i början av pandemin fann rapporten fyra olika kategorier av virusattacker där en tydlig trend uppvisats redan i början av coronapandemin. Till första kategorin hör attacker som stör servicetjänster. Hit hör DDoS-attacker samt spionprogramattacker. Samma rapport påstår även att denna utveckling är ett direkt resultat av de restriktioner som coronapandemin påtvingade. Samma uppåtgående trend av DDoS-attacker tas även upp av Enisas datorvirusrapport för 2021 [13]. Denna rapport tar även upp att denna ökning sker i samband med att IoT, sakernas internet, i kombination med mobilnätverk har skapat en ny våg med DDoS-attacker.

Den andra kategorin av attacker som ökat [14] är datorvirus som riktar in sig på ekonomisk vinning. Hit hör utpressningsprogram och digitala bedrägeri som tagit inspiration av coronavirusrelaterade applikationer. De digitala bedrägerierna som spelade på folks rädslor för pandemin var bland annat hemsidor som påstod sig sälja personlig skyddsutrustning, exempelvis ansiktsmasker och övriga produkter för att skydda sig mot pandemin. Samma fenomen rapporteras även i en nyhetsartikel från Interpol [19], där man redan i mars 2020 varnade för denna typ av bedrägerier. I nyhetsartikeln från Europol [19] skriver man att den stora efterfrågan på personlig skyddsutrustning i början av pandemin banade vägen för kriminella att utnyttja denna situation. I den rapport som undersöker coronavirusrelaterade datorvirus [14] skriver man även att under en veckas period i mars månad av 2020 fann 2000 länkar som ledde till sidor som påstod sig sälja covid-19-relaterade produkter. Bland dessa sidor fanns legitima försäljare som sålde dessa produkter till skyhöga priser samtidigt som det fanns sidor som helt enkelt försökte komma över kortnummer och personlig information [14,19].

Till den tredje kategorin hör datorvirusattacker som riktat in sig på informationsstöld och dataläckor [14]. Denna kategori går lite in på den förra kategorin gällande informationsstöld. I denna kategori som rapporten från 2020 [14] tar upp finner man tre olika kategorier på cyberrelaterade risker som ökade markant under coronapandemin. Dessa var: nätfiske över nätet både via dator och telefon samt utnyttjande av säkerhetsbrister i de redan, vid pandemins början, existerande kommunikationsmedel. Enligt Enisas rapport för 2021 [13] är nätfiske via mejl eller nätfiske via telefon fortfarande en av de större säkerhetsriskerna som finns i dagens läge.

Till den andra delen av denna tredje kategori hör de brister i kommunikationsprogram som man blev tvungen att börja använda till följd av de restriktioner som tillkom på grund av corona­pandemin. En sektor som speciellt drabbades hårt av denna omställning var utbildningsinstitutioner. I en rapport som publicerades i samband med IEEE International Conference on Computing (ICOCO) [20] undersökte man olika brister inom de digitala läroutrymmena. Rapporten går igenom säkerhetsbrister inom läroplattformerna Docebo, Blackboard och Moodle samt kommunikationsplattformarna Cisco Webex Meetings, Skype for Business och Zoom. I rapporten skriver man att samtidigt som efterfrågan på dessa tjänster markant ökade så utsattes även dessa program för fler datorvirusattacker. Samma rapport säger också att säkerheten för dessa program inte han fullständigt kontrolleras och uppdateras innan efterfrågan blev så stor som den blev.

Till den fjärde kategorin hör skrämselprogram eller program vars uppgift är att sprida desinformation [14]. Rapporten tar upp exempel på desinformationskampanjer som utspelade sig på populära sociala medier, exempelvis Facebook, WhatsApp och LinkedIn. Många av dessa artiklar förde även vidare användaren till hemsidor som idkade nätfiske. Enligt Enisas rapport för 2021 [13] står två större grupper bakom dessa informations­attacker: statligt sponsorerade aktörer och cyberkriminella. Samma rapport tar även upp att man sett en ökning av tjänster som gör desinformation som en service. Dessa tjänster kan i sin tur köpas av någon enskild grupp för att sprida sin agenda eller för att skapa ett missförtroende gentemot någon eller någonting.

Den kryptokapningstrend som började redan före coronapandemin är enligt Enisas rapport [13] ännu växande. I rapporten skrivs även att år 2021 var ett nytt rekordår när det kommer till antalet upptäcka fall. Som man kan se på figur 1, vid kapitel 2.2, så ser man att värdet på bitcoin toppade under 2021 i juni och oktober månad. Denna värdeökning har gjort denna typ av datorvirusattacker väldigt lönsamma och det är därför inte heller svårt att förstå varför cyberkriminella satsar på denna typ av virus [13]. Samma rapport konstaterar även att man ser en tydlig ökning av kryptokapningsvirus som riktar in sig på själva datorn istället för endast datorns webbläsare. Filbaserade kryptokapningsvirus var till antalet upptäckta fall sju gånger fler än de webbaserade varianterna.

* 1. Exempel på trendande datorvirus för smarttelefoner

\*Hit ska exempel om olika dominerande virustyper under covidpandemin för smarttelefoner sättas\*

* 1. Exempel på datorvirusens uppbyggnad och spridningsmetod

\*Samma som rubriken ovan fast inriktat på datorvirus för datorer\*

#

# 4. Jämförelse mellan före och efter coronapandemins början

# *\*I detta kapitel ska jag ta å jämföra tiden före och efter coronapandemin för att se på vilka skillnader jag hittar, en snabb sammanfattning hittas redan i referatet\**

# Viktigt att ta i åtanke när jämförelsen mellan dessa tidsperioder blev gjorda är att mängden datorvirus som blir detekterade ökar hela tiden vartefter allt fler får tillgång till internet i utvecklingsregioner. Vartefter teknologin utvecklas har man kunnat skapa allt billigare smarta enheter som fler och fler får tillgång till att använda vartefter samhället utvecklas.

# 5. Avslutning

\*Avslutning som binder ihop hela avhandlingen och presenterar de tydligaste trendskillnaderna\*

# 6. Källor

[1] David Lord, Donald Maxim, Hannah Woodford-Smith, Corey Johnson, Ho Woon Chung, Samara Carroll, Harshit Trivedi, Bianca Sabol. [https://www.researchgate.net/profile/Roderic-Broadhurst/publication/326436666\_Malware\_Trends\_on\_'Darknet'\_Crypto-markets\_Research\_Review/links/5b9091f192851c6b7ec645c6/Malware-Trends-on-Darknet-Crypto-markets-Research-Review.pdf](https://www.researchgate.net/profile/Roderic-Broadhurst/publication/326436666_Malware_Trends_on_%27Darknet%27_Crypto-markets_Research_Review/links/5b9091f192851c6b7ec645c6/Malware-Trends-on-Darknet-Crypto-markets-Research-Review.pdf) Hämtad 20.02.2022

[2] Saman Adhami, Giancarlo Guidici och Srefano Martinazzi. Publicerades: 9.5.2018, Uppdaterades 4.12.2018. Länken är hämtad 20.2.2022: <https://moodle.epfl.ch/pluginfile.php/2721162/mod_resource/content/1/1-s2.0-S0148619517302308-main.pdf>

[3] ENISA Threat Landscape Report 2018, Publicerad 28.1.2019, Länken hämtad 20.2.2022: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>

[4] Symantec ISTR Internet Security Treath Report Volume 23: <https://docs.broadcom.com/doc/istr-23-2018-en>, Länken hämtad 20.2.2022

[5] R. Srivastava, R. P. Mishra, V. Kumar, H. K. Shukla, N. Goyal and C. Singh, "Android Malware Detection Amid COVID-19," *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 2020, pp. 74-78, <https://ieeexplore.ieee.org/document/9337105>, Hämtad 27.2.2022

[6] Namanya, Anitta Patience, et al. "The world of Malware: An overview." 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2018. <https://www.researchgate.net/profile/Anitta-Patience-Namanya/publication/327665678_The_World_of_Malware_An_Overview/links/5ba1ef8e299bf13e603bd0fe/The-World-of-Malware-An-Overview.pdf>, Hämtad 03.03.2022

[7] DI PINTO, Alessandro; DRAGONI, Younes; CARCANO, Andrea. TRITON: The first ICS cyber attack on safety instrument systems. In: *Proc. Black Hat USA*. 2018. p. 1-26. <https://scadahacker.com/library/Documents/Cyber_Events/Nozomi%20-%20TRITON%20-%20The%20First%20SIS%20Cyberattack.pdf>, Hämtad 04.03.2022

[8] KAYACIK, Hilmi Günes; ZINCIR-HEYWOOD, A. Nur. A case study of three open source security management tools. In: IFIP/IEEE Eighth International Symposium on Integrated Network Management, 2003. IEEE, 2003. p. 101-104. https://link.springer.com/content/pdf/10.1007/978-0-387-35674-7\_10.pdf , Hämtad 06.03.2022

[9] Github, Metasploit Wiki: <https://github.com/rapid7/metasploit-framework/wiki>, Hämtad 06.03.2022

[10] N. Scaife, P. Traynor and K. Butler, "Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward)," in *IEEE Potentials*, vol. 36, no. 6, pp. 28-31, Nov.-Dec. 2017, doi: 10.1109/MPOT.2017.2737201. <https://ieeexplore.ieee.org/document/8103104>, Hämtad 06.03.2022

[11] K. P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis and S. Shiaeles, "Understanding and Mitigating Banking Trojans: From Zeus to Emotet," *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, pp. 121-128, doi: 10.1109/CSR51186.2021.9527960. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9527960> Hämtad: 17.3.2022

[12] Malwarebytes, State of Malware Report 2021: https://www.malwarebytes.com/resources/files/2021/02/mwb\_stateofmalwarereport2021.pdf , Hämtad 19.3.2022

[13] ENISA Treath Landscape 2021: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>, Hämtad 19.3.2022

[14] S. Hakak, W. Z. Khan, M. Imran, K. -K. R. Choo and M. Shoaib, "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies," in *IEEE Access*, vol. 8, pp. 124134-124144, 2020, <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9129700>, Hämtad 19.3.2022

[15] Europol, World’s most dangerous malware EMOTET disrupted by global action, <https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>, Hämtad 20.3.2022

[16] MELAND, Per Håkon; BAYOUMY, Yara Fareed Fahmy; SINDRE, Guttorm. The Ransomware-as-a-Service economy within the darknet. Computers & Security, 2020, 92: 101762. <https://www.sciencedirect.com/science/article/pii/S0167404820300468>, Hämtad 20.3.2022

[17] Kaspersky, Roaming Mantis infects smartphones trough Wi-Fi routers: <https://www.kaspersky.com/blog/roaming-mantis-malware/22427/>, Hämtad 20.3.2022

[18] L. Caviglione *et al*., "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," in *IEEE Access*, vol. 9, pp. 5371-5396, 2021: <https://ieeexplore.ieee.org/document/931115>, Hämtad 20.3.2022

[19] Interpol, News 2020, Interpol warns of financial fraud linked to Covid-19: <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19>, Hämtad 28.3.2022

[20] E. DJEKI, J. DEGILA, C. BONDIOMBOUY and M. H. ALHASSAN, "Security Issues in Digital Learning Spaces," *2021 IEEE International Conference on Computing (ICOCO)*, 2021, pp. 71-77, <https://ieeexplore.ieee.org/document/9673575>, Hämtad 28.3.2022