Linnéuniversitetet
Kalmar Växjö

Rapport

Ransomware och WannaCry - Kryptering som Vapen

Att förstå ransomware-attacker, med särskild fokus på WannaCry och dess betydelse för modern cybersäkerhet.

Författare: Ebbe Karlstad
Termin: HT23
Kursnamn: Technical Information and Communication
Kurskod:1DV510

Abstract

The WannaCry ransomware-attack is one of the bigger cyberthreats the world has seen. It released the 12th of May in 2017 and infected over 230 000 computers in over 150 countries across the world. The report will dive deep into the background and history of ransomware-attacks, from the very first one, the so called “AIDS-trojan” to the WannaCry-attack. The report will also study the mechanics of the ransomware itself, its parts and intricacies, what vulnerabilities were used and how it works on the infected computers. Another few big aspects of this report will be how the attack was allowed to happen, what security aspects that could have changed or minimized the outcome of the attack, and what this means for cybersecurity in companies and individuals.

Keywords

WannaCry, Ransomware, Cybersecurity, Malware, Encryption

Sammandrag

Ransomware-attacken WannaCry är ett av de största cyberhot som världen har skådat. Den började spridas den 12e maj 2017 och infekterade över 230 000 datorer i över 150 länder runt om i världen. Rapporten kommer att göra en djupdykning i bakgrunden och historien bakom ransomware-attacker, från den allra första, den så kallade "AIDS-trojanen", till WannaCry-attacken. Rapporten kommer också att studera själva ransomware-attackens mekanik, dess delar och finesser, vilka sårbarheter som utnyttjades och hur den fungerar på de infekterade datorerna. Ytterligare några viktiga aspekter i rapporten kommer att vara hur attacken tilläts att ske, vilka säkerhetsaspekter som kunde ha förändrat eller minskat resultatet av attacken, och vad detta innebär för cybersäkerheten hos företag och privatpersoner.

Nyckelord

WannaCry, Ransomware, Cybersäkerhet, Skadlig kod, Kryptering

Innehåll

1 Inledning

Över 230 000 datorer över hela världen blev i maj 2017 övertagna av cyberattacken ”WannaCry”. Attacken, som utfördes på operativsystemet Microsoft Windows, visade inte bara svagheterna i själva operativsystemet utan också den destruktiva potentialen av en ransomware-attack. Under det senaste decenniet har ransomware-attacker blivit allt vanligare, vilket skapar en stor risk hos företag och individer över hela världen [1]. Denna rapport kommer att ge en översikt på ransomware-attacker som ett cyberhot mot mänskligheten och även ta reda på WannaCry’s mekanik och hur den fungerar. Tidigare forskning finns vad gäller attacken, däremot är de riktade mot en specifik frågeställning, som exempelvis forskning på statisk analys av attacken, gjord av Kao och Hsiao [2], och dynamisk analys av den, även denna gjord av Kao och Hsiao [3].

Genom att undersöka ransomware-attackers bakgrund och historia, samt följande frågor försöker rapporten få fram en djupare förståelse av attacken och vad den betyder för modern cybersäkerhet. Rapporten är därmed väsentlig för att undersöka dessa frågor, samt frågor gällande hur företag och individer i framtiden bättre kan agera för att förbättra sina försvarsmetoder i ett försök att undvika ransomware-attacker.

1.1 Syfte och frågeställningar

Det primära målet med denna rapport är att ta reda på de ursprungliga sårbarheterna som tillät attacken, hur attacken faktiskt fungerar och vilka möjligheter som fanns för att undvika attacken, samt ifall dessa togs eller ej.

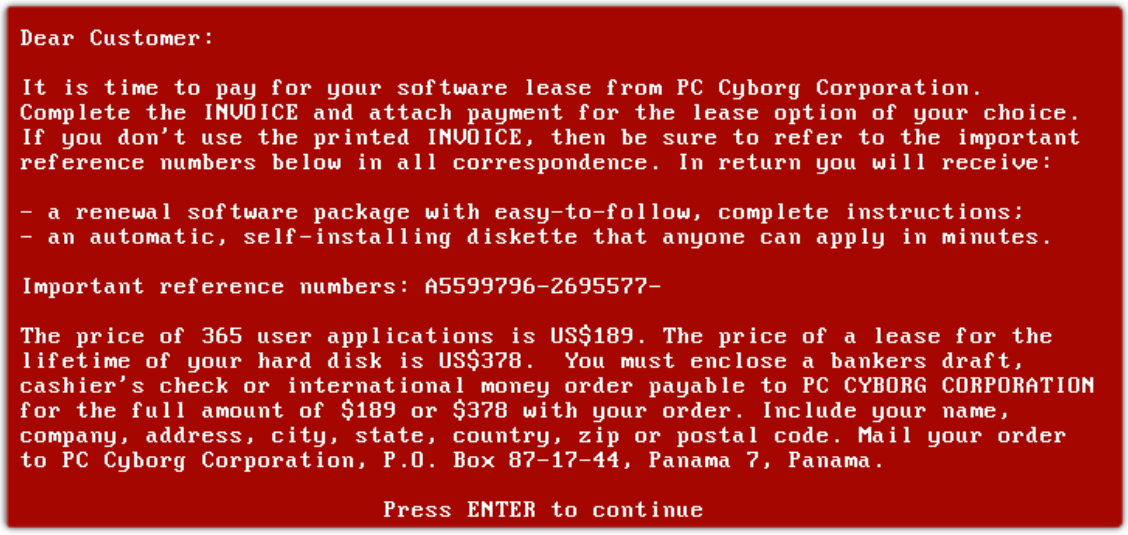
- Vilka var de ursprungliga sårbarheterna som tillät attacken sig för hackarna?
- Hur fungerar WannaCry-attacken?
- I efterhand, vilka var de viktigaste missade möjligheterna som kunde ha minskat omfattningen av WannaCry-attacken?

Bilden som visades på användarnas datorer när de tagits över av WannaCry [4].

2 Resultat

Enligt Akbanov et al. [5], ransomware är en sorts skadlig programvara som låser användare ute från sina egna system tills en lösensumma betalats. Det är som en form av digital kidnappning där filer krypteras och användaren hindras från att få tillgång till dem. Inom ransomware-världen finns två huvudtyper: cryptors och lockers. Lockers är enklare och verkar genom att låsa användargränssnittet på det infekterade systemet. Cryptors däremot är mer avancerade och svårare att knäcka eftersom de använder starkare krypteringsalgoritmer för att låsa viktiga filer på användarens enhet. När användaren drabbas av ransomware informeras de oftast om att de kan få tillbaka sina filer genom att betala en lösensumma. Det finns ingen garanti för att betala lösen faktiskt leder till att filerna återfås och detta uppmuntrar bara de som står bakom attacken att fortsätta med sina skadliga aktiviteter [5].

Enligt Drake [6], brukar den första ransomware-attacken allmänt betraktas som ”AIDS trojanen”, som skapades 1989 och döptes efter World Health Organization’s AIDS konferens som hölls samma år. Under denna konferens delade biologen Joseph Popp ut 20 000 infekterade disketter till deltagarna. När dessa deltagare hade suttit in disketterna i sina datorer och startat upp de 90 gånger visades det allra första ransomware-meddelandet på deras skärmar:



AIDS trojanen krypterade filerna på användarens maskin och bad de att betala en lösensumma på 189 amerikanska dollar emot en upplåsning av filerna.

År 2005 verkar ransomware-attacker ha blivit mer populära igen, tack vare förstärkta och förbättrade teknologier inom filkryptering och algoritmer. En av dessa teknologier är ”secure asymmetric encryption”, eller ”säker asymmetrisk kryptering”. Simmons [7], beskriver i sin artikel att en ”vanlig”, eller symmetrisk kryptering finns en nyckel, som alltid är gömd, för att kryptera/dekryptera digitala data. I en asymmetrisk kryptering, finns det i stället två nycklar, en sändare och en mottagare, som är olika från varandra.

Asymmetrisk kryptering gör att meddelanden kan kontrolleras av någon som inte behöver se själva meddelandet. Denna sorts kryptering låter, till skillnad från symmetrisk kryptering, de privata nycklarna hållas privata, vilket leder till att de är mycket svårare att dekryptera [7].

Enligt Drake är några av dessa tidiga ransomware-attackerna ”Archiveus”-trojanen och ”GPCode”, där den förstnämnda krypterade alla filer i användarens mapp med namnet ”Mina Dokument” som med ett trettiosiffrigt lösenord sedan kunde dekrypteras efter en lösensumma blivit betald. GPCode däremot, attackerade datorer med operativsystemet Windows direkt. Drake beskriver även att GPCode använde symmetrisk kryptering under de första fem åren av sin existens, men att den år 2010 bytte system till det mer säkra och asymmetriska systemet RSA-1024, som krypterar dokument med särskilda filändelser.

Mellan åren 2009 och 2013 släpptes, enligt Drake, tre till stora ransomware program, Ett utav dessa var Vundo, som attackerade datorer vars webbläsare var sårbara och skrivna i programmeringsspråket Java, eller genom att användaren klickade på bilagor i skadliga epost-meddelanden. Kort därefter släpptes ”WinLock”-trojanen, som skapades av ett tiotal ryska cyberbrottslingar, dessa använde programmet för att låsa användarnas datorer och spela upp pornografi till dess att användarna skickat ungefär 10 amerikanska dollar i ryska rubel. Den sista ransomware-attacken för denna tidsperiod som Drake nämner är ”Reveton”, som kom ut 2012 och som låste användarens webbläsare, som visade ett meddelande som låtsades vara från USA:s FBI (Federal Bureau of Investigation). Meddelandet skrämde användaren genom att säga till den att den innehav illegal pornografi, och uppmanade hen att betala en lösensumma för att undvika att bli åtalade.

Halvvägs genom 2013 släpptes ”CryptoLocker”, vilket var stort inom ransomware-världen, då det för första gången använde sig av ett ”botnet”. Singh [8] beskriver i en artikel att ett botnet kan ses som ett stort nätverk av värd-datorer som kontrolleras på distans [8]. Drake skriver att det botnet som användes kallades ”Gameover Zeus” och använde mer traditionella hacking-tekniker, som phishing. CryptoLocker använde sig även av en krypteringsteknik som kallas 2048-bit RSA, som gjorde den ännu svårare att knäcka.

År 2016 blev ransomware ännu vanligare, och den första ransomware-as-a-service (RaaS) varianten släpptes. Ransomware kunde nu köpas från grupper som ofta arbetade med varandra, en grupp som skrev ransomware-koden, och en hacker-grupp som hittade sårbarheter i diverse system. Några av dessa är ”Ransom32”, som var den första ransomware-attacken skriven i JavaScript, ”shark”, som uppladdades på en publik WordPress sida, och ”Stampado”, som var tillgänglig för endast $39.

Under åren 2016 och 2017 släpptes större ransomware-attacker, som Petya, LeakerLocker och WannaCry [6].

Enligt Akbanov et al. [5] släpptes den sistnämnda av dessa, WannaCry, i maj 2017 och är även känd som Wana Decrypt0r, WCry och WannaCrypt. Den här attacken spred sig snabbt och tog kontroll över omkring 300 000 system i över 150 länder. Särskilt drabbades sjukvården när WannaCry slog till. Det som gjorde WannaCry så svårstoppbar var dess användning av mask-teknik, vilket gjorde att den kunde kopiera sig själv till andra datorer och nätverk utan användarens medgivande [5].

2.1 Ursprungliga sårbarheter

Burdova [9] skriver; säkerhetssårbarheten som hittades av Microsoft fick beteckningen ”MS17-010” och var en kritisk sårbarhet i Microsofts operativsystem Windows. Sårbarheten hittades av USA:s National Security Agency (NSA). NSA hade letat efter denna sårbarhet i Windows programvara i nästan ett år innan de hittade den, och utvecklade den till det som idag känns till som ”EternalBlue”, vilket i april 2017 hittades av hackergruppen ”The Shadow Brokers” som släppte det på deras Twitter-sida för allmänheten att göra vad de vill med.

Burdova skriver även att själva verktyget fungerar genom att utnyttja fildelnings-protokollet ”SMBv1” (Server Message Block version 1) som finns i äldre Microsoft-operativsystem. SMB är ett sätt för Windows system att kommunicera med varandra och med andra system. En månad innan The Shadow Group släppte EternalBlue till allmänheten släppte Microsoft patchen ”Bulletin MS17-010” då det tros att de blivit tipsade om sårbarheten i deras system av NSA. Patchen som släpptes fungerade på uppdaterade datorer och stängde helt ner sårbarheten och alla attacker som eventuellt skulle kunna göras på den, trots detta blev över 230 000 Windows-maskiner låsta av ransomware-attacken i maj 2017 då företag och privatpersoner tenderar att inte uppdatera sina system tillräckligt ofta [9].

2.2 WannaCry’s mekanik

Enligt Kao et al. [10], följer ransomware-attacker en generell anatomi på fyra steg. Det första steget är ”driftsättningsfasen”, där WannaCry-attacken använder sårbarheten MS17-010 för att föra in skadlig kod via filen ”launcher.dll” i användarnas datorer genom EternalBlue-exploateringen och en bakdörr i Windows-systemet som kallas ”Doublepulsar”. Kao et al. beskriver vidare att WannaCry utnyttjar drivrutinen för SMB (Server Message Block) under namnet ”srv2.sys” för att få åtkomst till andra infekterade enheter och injektera skadlig kod även i dessa. Filen launcher.dll injekteras sedan även i system-processen lsass.exe, vilket enligt [11] står för ”Local Security Authority Subsystem Service”, och är en process som tar hand om säkerhetspolicy i operativsystemet Windows [11]. Kao et al. skriver även att lsass.exe nu fungerar som en ”lastare” för filen mssecsvc.exe, som enligt Henderson [12] är en fil som gör att ransomware-infektionen fungerar korrekt [12].

Kao et al.’s rapport studerade lsass-processens minne från minnesdumpar och kom fram till att ifall minnesdumpen laddas in i ett program som kallas ”IDA Pro”, kan den tidigare nämnda DLL filen fungera med ett program som heter ”PlayGame”, vars uppgift i detta fall är att starta ransomware-attacken.

Det andra steget i ransomware-attackens anatomi kallar Kao et al. för ”installationsfasen”, som i sig innehåller de tre stegen; ’dropper’, ’infection’, och ’resource loader’. Här skickas ransomware-koden till användarens dator. När denna kod når systemet, injekteras launcher.dll filen i lsass.exe processen där denna process startar programmet mssecsvc.exe. Efter detta används två Windows API:s för att skicka en förfrågan till domänen ”www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”, vilket är en så kallad ”kill-switch URL”. Ifall denna förfråga godkänns kommer mssecsvc.exe att avslutas, annars kommer den att köra mssecsvc.exe och påbörja infektionen.

I det första del-steget, dropper, börjar mssecsvc.exe sina uppgifter utan några specifika instruktioner. Den sätter upp en service under namnet ”mssecsvc2.0” och ett annat program som heter ”tasksche.exe” och skickar in dessa i systemet.

Kao skriver att i det andra del-steget i installationsfasen, ”infection”, körs mssecsvc servicen, som använder sårbarheten i MS17-010 systemet för att infektera användarens dator. Hackarnas maskin undersöker i detta steg SMB-protokollet och porten 445. Ifall anslutningen lyckas kommer ett specialpaket att överföras för att se om Doublepulsar-bakdörren finns. Om denna inte är installerad startas i stället EternalBlue-attacken.

Det sista del-steget i ”infection”-processen kallar Kao et al. för ”resource loader”. Det huvudsakliga ransomware-programmet, ”taskche.exe” startas av ”mssecsvc.exe” i den första, dropper-fasen. Nu extraheras komprimerade XIA-resurser som innehåller WannaCry-relaterade filer. Programmet ”taskche.exe” genererar här ett unikt ID för en mapp, kontrollerar parametrar för hur programmet ska köras, skapar en ”autorun-registreringsnyckel” som låter programmet köras automatiskt, packar upp resursfiler till WannaCry-attacken, väljer en Bitcoin-adress för överföring av användarens kryptovaluta, ändrar mappattribut och dekrypterar filer för att förbereda för kryptering.

Kao et al. skriver att det tredje steget för WannaCry-attacken är ”Destruction Phase”, där alla filer på användarens maskin börjar bli infekterade, krypterade, eller låsta, av attacken. WannaCry använder en serie steg och speciella nycklar för att kryptera dessa filer. Kao et al. skriver att attacken kan delas upp i två steg; hur krypteringen sker och hur de speciella nycklarna hanteras. Attacken använder sig av olika nyckeltyper, som RSA (som skapades av Ron Rivest, Adi Shamir och Leonard Adleman, därav dess namn) och AES (Advanced Encryption Standard), för att kryptera filerna. Den huvudsakliga nyckeln, som kallas RSA root public key, har endast skaparen av WannaCry tillgång till, vilket enligt Kao et al. gör den svår att hitta och lösa krypteringen för. ”Destruction”-fasen involverar skapandet av två RSA-2048 nycklar som sparas med filnamnen 00000000.pky och 00000000.eky.

Innan RSA nyckeln sparas till 00000000.eky krypteras den med hjälp av rot-nyckeln som tidigare nämndes. För alla filer som krypteras av attacken skapas också en slumpmässig AES-128 nyckel med hjälp av rot-nyckeln. När en fil har blivit krypterad läggs bäddas den unika krypterade AES-nyckeln in i filens ”header”, följt av 8-byte värdet ”WANACRY!” och 4-byte längden på själva AES-nyckeln.

Kao et al. skriver att det fjärde och sista steget i en WannaCry-attack kallas ”Command-and-Control Phase”, där alla åtgärder kräver en s.k. kommando- och kontroll process för att bestämma vilka åtgärder som härnäst ska vidtas. Bland filerna i WannaCry-attacken finns ”@WanaDecryptor@.exe”, som är ett program som kontrollerar attacken, kommunicerar med filer och enheter, och tar bort vissa filer. Detta program används på tre olika sätt; ”fi”, ”co”, eller ”vs”. Programmet installerar även nödvändiga filer för att kunna fungera med en TOR-tjänst, vilket enligt Reed et al. [13] är en slags infrastruktur som tillåter privat kommunikation över ett offentligt nätverk med hjälp av s.k. onion routing [13]. Kao et al. skriver sedan att ifall ”@WanaDecryptor@.exe” körs med ”fi” parametern kommer den att försöka ansluta till onion servern, men ifall den körs med ”co” parametern kommer den i stället köra filen ”taskhsvc” som en slags delprocess för att försöka ansluta till onion servern. Efter detta kommer servern att uppdatera en textsträng i filen ”c.wnry” med en unik Bitcoin adress. Serverdomänerna listas i "c.wnry" enligt följande: ”gx7ekbenv2riucmf.onion”, ”57g7spgrzlojinas.onion”, ”xxlvbrloxvriy2c5.onion”, ”76jdd2ir2embyv47.onion” och ”wwnhwhlz52maqm7.onion”.

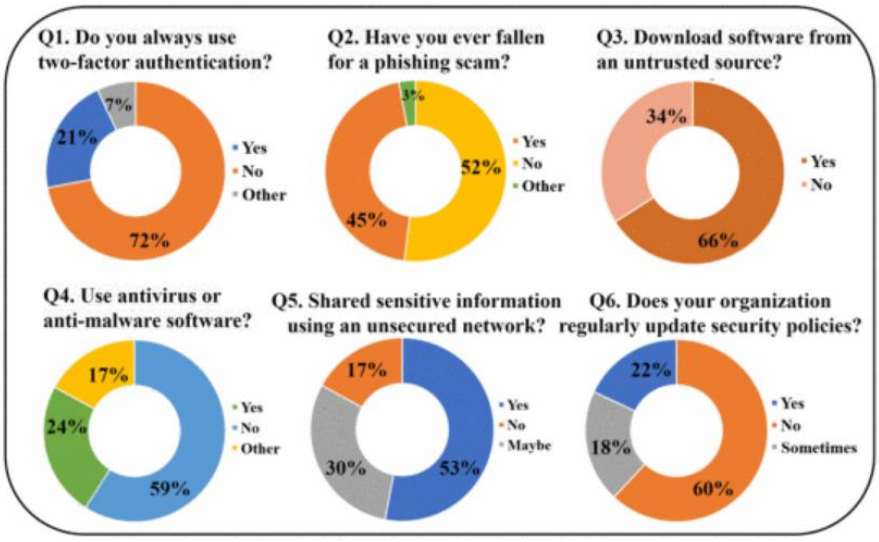
Enligt Kao et al. är dessa fyra stegen anatomin av en ransomware-attack. Allt börjar med driftsättningen av attacken, som utnyttjar sårbarheterna i Windows systemet MS17-010 via EternalBlue och Doublepulsar. Efter detta installeras ransomware-programmet på användarnas dator, här startas tjänster och program samt infekterar datorn med skadlig kod. I tredje steget krypteras filer med RSA och AES-nycklar, denna fas hanterar krypteringsprocesser. Till slut kontrolleras attacken med hjälp av ”@WanaDecryptor@.exe” och ansluter till en TOR-tjänst för kommunikation [10].

2.3 Missade möjligheter

Enligt [14] skriver författaren av artikeln att när attacken slog till i maj 2017 började Marcus Hutchins, en cybersäkerhetsforskare, att studera WannaCry's källkod och hittade en underlig funktion, som rapporten nämnde tidigare. Innan koden utfördes, skickade den en frågeställning till domänen ”iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”, vilket vid den tiden inte var registrerad. Hutchins registrerade domänen för runt 11 amerikanska dollar, vilket ledde till att kopior av WannaCry fortsatte att spridas, men utan att utföras.

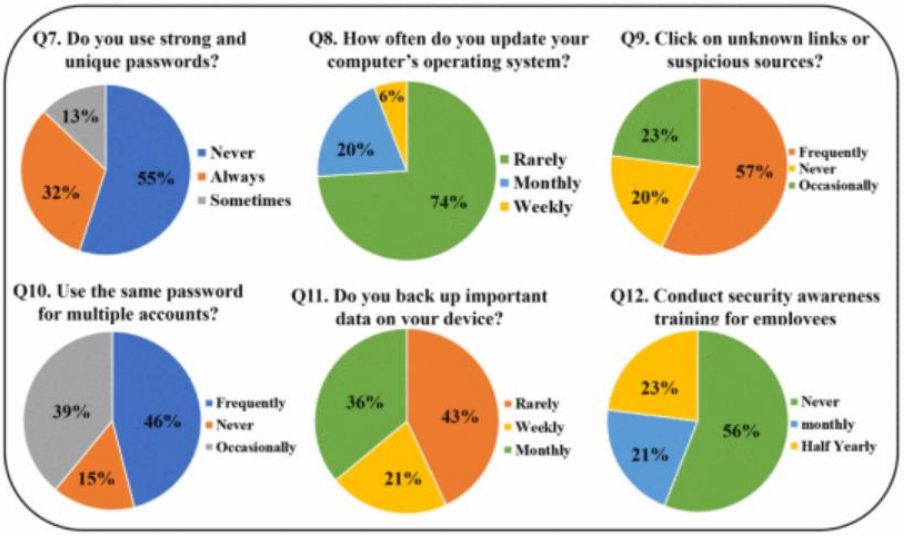
Anledningen till att skaparna av WannaCry programmerade in denna fråga till domänen är fortfarande inte känd, men vissa säger att den var inkluderad så att attacken kunde se om den existerade i ett ”sandbox environment”. En sandbox är en virtuell maskin som körs separat från andra system och nätverk på användarens dator. Detta skapar ett säkert område där filer och program kan testköras, utan att förstöra datorn de körs på. Då en sandbox inte är kopplad till internet, utan i stället försöker att imitera en riktig dator, kan en anledning till att skaparna av attacken lade in denna funktion vara för att attacken skulle kunna kolla om den fanns i en sandbox-miljö genom att skicka förfrågan till domänen. Ifall förfrågan skulle fått ett svar från domänen (som egentligen bara genererades av sandbox-miljön), visste den att den var i en sandbox och kunde efter det stänga ner sig själv, så att säkerhetsforskare inte skulle detektera den som skadlig i sina testmiljöer. Enligt vissa är detta alltså hur attacken stoppades, runt om i världen blev kopior av WannaCry lurade till att tro att den fanns i en sandbox-miljö och därmed även avstängda [14].

Rapporten nämnde tidigare att Microsoft släppte en patch till attacken innan den släpptes och började ta över datorer, trots detta tog attacken över runt 230 000 maskiner runt hela världen [14]. Sakib et al. [15] utförde en undersökning bland flera olika organisationer för att försöka komma fram till den största anledningen till att ransomware-attacker lyckas, och kom fram till att 72% av alla intervjuade personer inte använder tvåfaktorsauktorisering (Q1), 66% laddar ner programvara från osäkra platser på internet (Q3) och att 60% av företagen som intervjuades sällan uppdaterar deras säkerhetspolicys (Q6).



Fråga Q8 i bilden nedan från Sakib et al.’s studie, som gjordes på 1260 deltagare, visar att 74% sällan uppdaterar sin dators operativsystem, medan 20% gör det en gång i månaden och 6% gör det en gång i veckan. Då Microsoft släppte Windows-patchen Bulletin MS17-010 för allmänheten att ladda ner resulterar detta i en en-månads lucka för allmänheten att uppdatera sina operativsystem, vilket hade stoppat deras dator från att bli infekterad. Q12 visar även att 56% av företagen som blev intervjuade aldrig hållt en träning om säkerhet för sina anställda och att endast 21% gör det en gång i månaden.

Dessa två och många andra anledningar, som delning av känslig information, nedladdning av osäker programvara och användning av osäkra lösenord leder Sakib et al. till att dra slutsatsen om att deras studie visar att många människor inte har bra vanor inom cybersäkerhet och att detta gör de mer mottagningsbara för cyberattacker.



3 Diskussion och Slutsats

Den här rapporten har studerat ransomware som ett cyberhot, deras bakgrund och historia, samt djupare utforskat de tekniska detaljerna hos WannaCry ransomware-attacken. Detta för att kunna förstå hur den fungerar, vad som tillät den att ske samt hur den kunde stoppats. WannaCry-attacken var komplex, med många delar och steg i sig. Attacken följer enligt Kao et al. [10] en struktur på fyra steg, först sätts attacken i drift, här används sårbarheten MS17-010 för att föra in skadlig kod i användarens dator genom sårbarheterna EternalBlue och Doublepulsar. Efter detta kommer bland annat en förfrågan att skickas till kill-switch domänen ”www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”, som kommer att köra WannaCry-attacken ifall ingen respons från domänen ges ut. Till sist kommer alla filer på användarens dator att bli krypterade, vilket kräver en lösensumma för att bli upplåsta [10].

Rapporten har även studerat sårbarheterna som tillät attacken, främst MS17-010, vilket är en sårbarhet i Microsoft Windows. Enligt [14] släppte Microsoft en patch till problemet, som helt skulle lösa sårbarheterna och stoppa WannaCry-attacken. Trots detta blev över 230 000 datorer övertagna av attacken [14]. Enligt Sakib et al. [15] blir attacker som denna så stora inte på grund av deras tekniska komplexitet, utan på grund av mänskliga fel. I deras studie kom de fram till att 74% av deltagarna sällan uppdaterade sina operativsystem, vilket i WannaCry’s fall, helt skulle stoppat attacken på den användarens dator.

I nämnd undersökning konstaterades det även att 6% av deltagarna uppdaterade sin dators operativsystem en gång i veckan och att 20% gjorde det en gång i månaden. Då Microsofts respons på sårbarheten som tillät WannaCry-attacken och själva attacken i sig skedde med exakt en månads mellanrum skulle, ifall endast denna studie används, alltså runt 20% av deltagarna vars datorer fortfarande hade icke-uppdaterade operativsystem vara mottagliga för attacken [15]. Då denna siffra inte är global, utan bara gäller 1260 deltagare, kan detta påstående inte dras som en allmännelig slutsats, utan ger i stället en övergripande bild på hur uppdatering av operativsystem och programvara eventuellt skulle kunna ha ändrat storleken och allvarligheten på WannaCry-attacken.

Rapporten har fördjupat sig i ransomware-attacker med fokus på WannaCry och belyser bakgrunden av den, dess tekniska aspekter, samt vad som tillät den att växa och sprida sig. Rapporten har även diskuterat hur attacken stoppades och hur användare och företag med hjälp av bättre cybersäkerhetsvanor eventuellt kunde minskat attackens omfattning och gjort den mindre allvarlig.

Referenser

[1] ”What is WannaCry ransomware?,” Kaspersky, 8 Juni 2020. [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. [Använd 13 November 2023].

[2] S.-C. Hsiao och D.-Y. Kao, ”The static analysis of WannaCry ransomware,” Chuncheon, 2018.

[3] D.-Y. Kao och S.-C. Hsiao, ”The dynamic analysis of WannaCry ransomware,” Chuncheon, 2018.

[4] K. Selvaraj, E. Florio, A. Lelli och T. Ganacharya, ”WannaCrypt ransomware worm targets out-of-date systems,” Microsoft, 20 Juni 2017. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/. [Använd 3 December 2023].

[5] V. Vassilakis, M. Akbanov, I. Moscholios och M. Logothetis, ”Static and Dynamic Analysis of Wannacry Ransomware,” 2018.

[6] V. Drake, ”The History and Evolution of Ransomware Attacks,” Flashpoint, 29 Juli 2022. [Online]. Available: https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/. [Använd 6 December 2023].

[7] G. Simmons, ”Symmetric and Asymmetric Encryption,” Sandita Laboratories, New Mexico, 1979.

[8] R. R. Singh, K. Kamila och J. Kalaivani, ”Neural Network Based Botnet Detection,” International Conference on Intelligent Technologies, Hubli, 2021.

[9] C. Burdova, ”What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?,” Avast Academy, 18 Juni 2020. [Online]. Available: https://www.avast.com/c-eternalblue. [Använd 27 November 2023].

[10] D.-Y. Kao, S.-C. Hsiao och R. Tso, ”Analyzing WannaCry Ransomware Considering the Weapons and Exploits,” International Conference on Advanced Communication Technology (ICACT), PyeongChang, 2019.

[11] ”What is lsass.exe? 5 ways to see if it’s safe.,” GlassWire, [Online]. Available: https://www.glasswire.com/process/lsass.exe.html. [Använd 7 December 2023].

[12] J. H. Henderson, ”What is Mssecsvc.exe & How to Delete it,” WindowsReport, 4 Oktober 2023. [Online]. Available: https://windowsreport.com/mssecsvc-exe/. [Använd 2023 December 2023].

[13] M. Reed, P. Syverson och D. Goldschlag, ”Anonymous connections and onion routing,” 1998.

[14] ”What was the WannaCry ransomware attack?,” Cloudflare, [Online]. Available: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. [Använd 10 December 2023].

[15] S. Sakib, M. A. K. Raiaan, N. M. Fahad, M. S. H. Mukta, A. A. Mamun och S. Chowdhury, ”A Review of the Evaluation of Ransomware: Human Error or Technical Failure?,” Dhaka, 2023.