Linnéuniversitetet
Kalmar Växjö

Rapport

Ransomware och WannaCry - Kryptering som vapen

Att förstå ransomware-attacker, med särskilt fokus på WannaCry.

Author: Ebbe Karlstad
Supervisor: Sergej Ivanov
Semester: HT23
Discipline: Technical Information and Communication
Course code: HT23-1DV510

Linnéuniversitetet
Kalmar Växjö

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 dove 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 also studied 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 were how the attack was allowed to happen, and what security aspects could have changed or minimized the outcome of the attack. It also discusses what this means for cybersecurity in companies and individuals.

Keywords

WannaCry, Ransomware, Cybersecurity, Malware, Encryption

Sammanfattning

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 har gjort en djupdykning i bakgrunden och historien bakom ransomware-attacker, från den allra första, den så kallade "AIDS-trojanen", till WannaCry-attacken. Rapporten har också studerat själva ransomware-attackens mekanik, dess delar och finesser, vilka sårbarheter som utnyttjades och hur den fungerar på de infekterade datorerna. Ytterligare några stora aspekter av denna rapport var hur attacken tilläts ske, och vilka säkerhetsaspekter som kunde ha ändrat eller minimerat utfallet av attacken. Den diskuterar också vad detta innebär för cybersäkerhet i företag och för enskilda individer.

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 bättre kan agera för att förbättra sina försvarmetoder för cyberattacker.

1.1 Syfte och frågeställningar

Det primära målet med denna rapport är att ta reda på de ursprungliga sårbarheterna som tillät attacken. Den kommer också studera hur attacken faktiskt fungerar och vilka möjligheter som fanns för att undvika den.

- Vilka var de första ransomware-attackerna och hur gick de till?
- Vilka var de ursprungliga sårbarheterna som lät hackarna utföra attacken?
- Hur fungerar WannaCry-attacken?
- I efterhand, vilka var de viktigaste missade möjligheterna som kunde ha minskat omfattningen av WannaCry-attacken?

2 Resultat

2.1 Tidiga ransomware-attacker

Enligt Akbanov med flera [4] är 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. Det finns ingen garanti för att en betald lösen leder till att filerna återfås. Detta uppmuntrar ofta bara de som står bakom attacken att fortsätta med sina skadliga aktiviteter [4].

Enligt Drake [5], 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 påbörjades världens första ransomware-attack. Denna krypterade filerna på användarens maskin och bad dem 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 [6], skriver 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 [6].

Enligt Drake [5] är några av dessa tidiga ransomware-attackerna ”Archiveus”-trojanen och ”GPCode”. Archiveus 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 [5] beskriver även att GPCode använde symmetrisk kryptering under de första fem åren av sin existens. Hon skriver även att den år 2010 bytte system till det mer säkra och asymmetriska systemet RSA-1024, som krypterar dokument med särskilda filändelser.

Halvvägs genom 2013 släpptes ”CryptoLocker”, vilket var stort inom ransomware-världen, då det för första gången använde sig av ett ”botnet”. Singh [7] beskriver i en artikel att ett botnet kan ses som ett stort nätverk av värd-datorer som kontrolleras på distans [7]. Drake [4] 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 [5].

Enligt Akbanov med flera [4] 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 [4].

2.2 Ursprungliga sårbarheter

Burdova [8] 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. När de väl gjort det utvecklade de den till det som idag känns till som ”EternalBlue”. I april 2017 hittades EternalBlue av hackergruppen ”The Shadow Brokers” som släppte det på deras Twitter-sida för allmänheten att göra vad de vill med.

Burdova [8] 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 [8].

2.3 WannaCrys mekanik

Enligt Kao med flera [9], följer ransomware-attacker en generell anatomi på fyra steg. Det första steget är ”driftsättningsfasen”. Här använde WannaCry-attacken sårbarheten MS17-010 för att föra in skadlig kod via filen ”launcher.dll” i användarnas datorer. Detta gjordes genom EternalBlue-exploateringen och en bakdörr i Windows-systemet som kallas ”Doublepulsar”. Kao med flera [9] 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 [10] står för ”Local Security Authority Subsystem Service”, och är en process som tar hand om säkerhetspolicy i operativsystemet Windows [10].

Det andra steget i ransomware-attackens anatomi kallar Kao med flera [9] för ”installations-fasen”. Här skickas ransomware-koden till användarens dator. När denna kod når systemet, injekteras launcher.dll filen i lsass.exe processen. 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 en delprocess av attacken att avslutas, annars kommer den att köras och påbörja infektionen.

Hackarnas maskin undersöker därefter 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. Programmet ”taskche.exe” genererar efter det ett unikt ID för en mapp, kontrollerar parametrar för hur programmet ska

köras, och packar upp resursfiler, bland annat.

Kao med flera [9] 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 med flera 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 och AES för att kryptera filerna. Den huvudsakliga nyckeln, som kallas RSA root public key, har endast skaparen av WannaCry tillgång till, vilket enligt Kao med flera gör den svår att hitta och lösa krypteringen för. ”Destruction”-fasen involverar skapandet av två RSA-2048 nycklar som 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 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 med flera [9] 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. Programmet installerar även nödvändiga filer för att kunna fungera med en TOR-tjänst. Enligt Reed med flera [11] är detta en slags infrastruktur som tillåter privat kommunikation över ett offentligt nätverk med hjälp av s.k. onion routing [11]. Kao med flera [9] skriver sedan att servern efter detta kommer att uppdatera en textsträng i filen ”c.wnry” med en unik Bitcoin adress [9].

2.4 Missade möjligheter

Enligt [12] skriver författaren av artikeln att när attacken slog till i maj 2017 började en cybersäkerhetsforskare vid namn Marcus Hutchins att studera WannaCry’s källkod. Han upptäckte att en frågeställning till domänen ”iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com” skickades innan koden utfördes. Vid denna tid var inte denna domän 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. En anledning till att skaparna av WannaCry integrerade frågan till denna domän kan vara för att avgöra om deras attack utfördes i en skyddad sandbox-miljö. Om de fick ett svar från domänen, tolkade attacken detta som att den kördes i en säker testmiljö. Detta gjorde så att attacken stängde ner sig själv för att undvika att bli upptäckt av säkerhetsforskare [12].

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 [12]. Sakib med flera [13] utförde en undersökning bland flera olika organisationer för att försöka komma fram till den största anledningen till att ransomware-attacker lyckas. Deras resultat kan ses i följande bild.

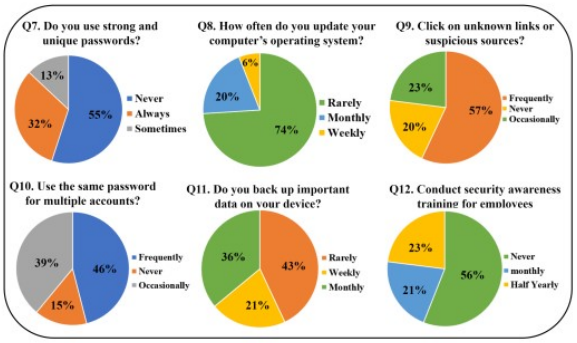

Figure 1: Undersökningsresultat

I fråga Q8 från Sakib med fleras [13] studie, som gjordes på 1260 deltagare, visar det sig att 74% sällan uppdaterar sin dators operativsystem. 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. Detta hade stoppat deras dator från att bli infekterad. Sakib med flera [13] drog slutsatsen att deras studie visar att många människor har dåliga cybersäkerhetsvanor, vilket ökar deras sårbarhet 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 med flera [9] 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 [9].

Rapporten har även studerat sårbarheterna som tillät attacken, främst MS17-010, vilket är en sårbarhet i Microsoft Windows. Enligt [12] 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 [12]. Enligt Sakib med flera [13] 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. Microsofts respons på sårbarheten som tillät WannaCry-attacken skedde exakt en månad innan attacken släpptes. Ifall endast denna studie används skulle alltså runt 20% av deltagarna vars datorer fortfarande hade icke-uppdaterade operativsystem vara mottagliga för attacken [13]. Då denna siffra inte är global, utan bara gäller 1260 deltagare, kan detta påstående inte dras som en allmännelig slutsats. Den 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.

References

[1] Kaspersky. (2020, Jun.) What is wannacry ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. Accessed 13 November 2023.

[2] S.-C. Hsiao and D.-Y. Kao, "The static analysis of wannacry ransomware," 2018.

[3] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of wannacry ransomware," 2018.

[4] V. Vassilakis, M. Akbanov, I. Moscholios, and M. Logothetis, "Static and dynamic analysis of wannacry ransomware," 2018.

[5] V. Drake. (2022, Jul.) The history and evolution of ransomware attacks. https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/. Accessed 6 December 2023.

[6] G. Simmons, "Symmetric and asymmetric encryption," 1979.

[7] R. R. Singh, K. Kamila, and J. Kalaivani, "Neural network based botnet detection," 2021.

[8] C. Burdova. (2020, Jun.) What is eternalblue and why is the ms17-010 exploit still relevant? https://www.avast.com/c-eternalblue. Accessed 27 November 2023.

[9] D.-Y. Kao, S.-C. Hsiao, and R. Tso, "Analyzing wannacry ransomware considering the weapons and exploits," 2019.

[10] GlassWire. What is lsass.exe? 5 ways to see if it's safe. https://www.glasswire.com/process/lsass.exe.html. Accessed 7 December 2023.

[11] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," 1998.

[12] Cloudflare. What was the wannacry ransomware attack? https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/. Accessed 10 December 2023.

[13] S. Sakib, M. A. K. Raiaan, N. M. Fahad, M. S. H. Mukta, A. A. Mamun, and S. Chowdhury, "A review of the evaluation of ransomware: Human error or technical failure?" 2023.