ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ

ФАКУЛТЕТ ПО КОМПЮТЪРНИ СИСТЕМИ И ТЕХНОЛОГИИ

КОМПЮТЪРНО И СОФТУЕРНО ИНЖЕНЕРСТВО

Програмни технологии за сигурен код

Курсов проект

„Какво представлява ransomware? Стратегии и защита от ransomware.“

Съставил: Ангел Любомиров Стойнов

Факултетен номер: 121222150

Група: 40

Съдържание

Въведение

Рансъмуерът е вид зловреден софтуер, който криптира файлове и ограничава достъпа до дадена система. Хакерът изисква откуп от ощетения, обикновено парична сума (в биткойн), в замяна откраднатите данни. Най-често се използва биткойн или друга криптовалута, понеже е много трудна да бъде проследена. Ако жертвата откаже да заплати, всички файлове ще бъдат унищожени. Дори потребителят да заплати сумата не е сигурно, че хакерът няма да изтрие всичко въпреки това.

В зависимост от откраднатата информация, жертвата може да бъде притиснат допълнително, като бъде заплашван, че цялата му лична информация ще бъде разпространена в интернет – местожителство, членове на семейство, банкова информация, документи, фирмена информация, работно място и др. Прилагането на двете тактики заедно е известно като: „double extortion”. Колкото е по-силен мотивът, толкова е по-вероятно потърпевшият да се пречупи. Друга тактика, която често се прилага е блъф, хакерът има частичен достъп до дадена система, но е неспособен да й навреди. Тогава хвърля безпочвени закани и разчита потребителя да изпълни наредбите.

Тези атаки с изнудващ зловреден софтуер (ransomware) могат сериозно да нарушат бизнес процесите. Организациите често губят достъп до важна информация, необходима за нормалната им работа и предоставяне на критични услуги. Икономическите и репутационните щети са значителни. Възстановяването след подобна атака е трудно и скъпо. Засегнати могат да бъдат организации от всякакъв мащаб. Последиците се усещат както по време на първоначалното прекъсване, така и дълго след това.

От съществено значение е, компаниите често да прилагат задължителни обучение на служителите си, понеже ransomware може да бъде свален през имейл, attachments, реклами, линкове, уеб страници с вложени злокачествени софтуери. В реферата, ще бъдат разгледани стратегии и защити от ransomware.

История на Ransomware

Въпреки че Ransomware е нашумял последните 10 години, идеята за кражда на потребителска информация или за заложник чрез криптиране на файлове, отграничаване на достъпа или чрез други методи и по-късно откуп е доста стара.

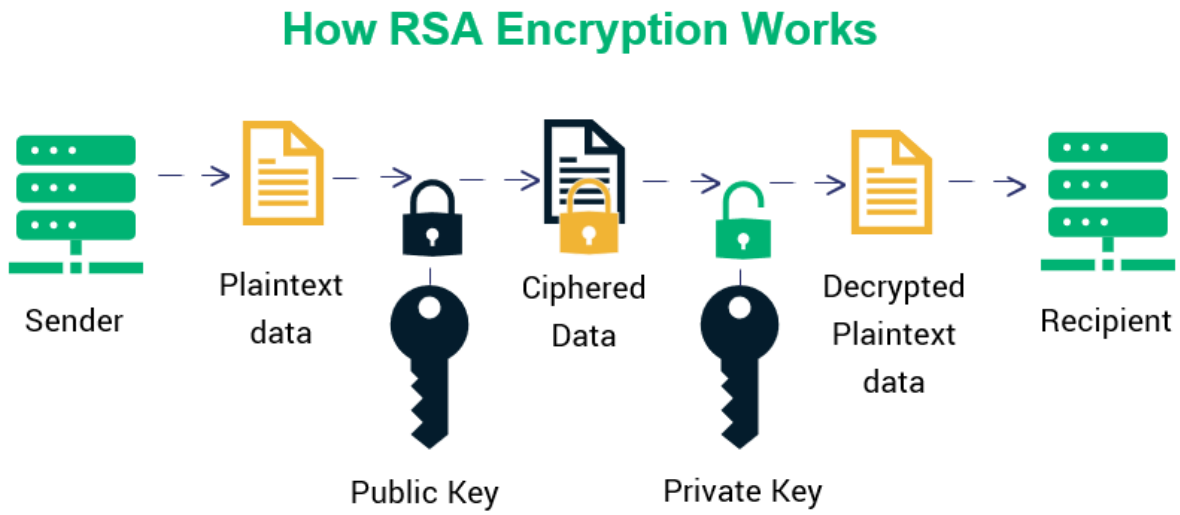
В края на 80-те години, престъпниците са можели да криптират файлове и са искали валута изпратена през пощенски услуги за откуп. Една от първите документирани ransomware атаки е: “AIDS trojan (PC Cyborg Virus)”. Разпространяван е чрез флопи дискети през 1989 година. Потърпевшите са накарани да изпратят 189$ през пощенска кутия в Панама, за да възстановят достъпа до системите си, въпреки че методът за криптирани е бил сравнително прост – чрез симетрично криптиране. Симетричното криптиране е техника, където един и същи ключ се използва за криптиране и декриптиране на данните.

Ransomware става широко разпространен чак през ранните две хилядни – вероятно поради трудността хакера да си получи откупа. Появата на биткойна и криптовалутите променят това. Лесен и удобен начин е за получаване на крупната сума от потърпевшия като остават незабелязани. При традиционното банкиране участниците са ясно идентифицирани – име, банка, държава, регулации и т.н. При криптовалутите адрес на сметката не съдържа директна лична информация. Липсва и централизиран контролен орган. Преводите са почти невъзможни да бъдат спрени, замразени, върнати или проследени от институциите. Изпирането на валутата е сравнително лесно – чрез т.нар. chain hopping (прехвърляне между различни криптовалути) и използване на privacy coins. Минус на биткойна, е че не всяка жертва е достатъчно запознат как да го предостави и да се откупи. Някои от хакерите са заловени, понеже са пускали видеоконференции, за да покажат как да го направят.

През 2013 г. се появява CryptoLocker, което бележи повратен момент в развитието на ransomware. Този нов вид изнудващ зловреден софтуер използва плащания чрез Bitcoin и прилага по-съвременни криптографски методи. Той използва 2048-bit RSA key pairs, генерирани от командно-контролен сървър и изпращани към жертвата. През 2005 г., е използван 56-bit RSA протокол за криптиране, което днес е незащитен и силно не препоръчван. Всичко под 1024-бита може да бъде разбито с brute force.

RSA е алгоритъм за асиметрично криптиране на данни (фиг. 1). Използват се два ключа, с които се криптира и декриптира информация. Използва се за електронни

подписи и в интернет протокола TLS. Основната идея е имайки единия ключ да е математически много трудно да бъде изчислен какъв е другия. По този начин става възможно свободното използвана на единия от ключовете като "публичен", а другия да остане "таен" (само собственика го притежава и никой друг не може в разумно време да го намери). Хакерът притежава частния ключ. На практика файловете се криптират по начин, който не позволява възстановяване без заплащане на откуп от около 300 щатски долара.



(Фиг 1. – архитектура на RSA криптиране)

Еволюция на Ransomware

Стратегии и защита от ransomware

Цитирани източници

[1] „#StopRansomware Guide,“ Americas Cyber Defense Agency, [Онлайн]. Available: https://www.cisa.gov/stopransomware/ransomware-guide.

[2] „Ransomware,“ FBI, [Онлайн]. Available: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware.

[3] K. Baker, „History of Ransomware,“ CrowdStrike, 09 10 2022. [Онлайн]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/history-of-ransomware/.

[4] „Botnet,“ Eset, [Онлайн]. Available: https://help.eset.com/glossary/bg-BG/botnet.html.

[5] „CC Server,“ Eset, [Онлайн]. Available: https://help.eset.com/glossary/bg-BG/cc_server.html.

[6] Ф. Петров, „RSA,“ 16 02 2020. [Онлайн]. Available: https://www.cphpvb.net/network-security/10840-rsa-with-example/.

[7] „What is RSA Asymmetric Encryption? How Does it Work?,“ Secure W2, 15 09 2025. [Онлайн]. Available: https://www.securew2.com/blog/what-is-rsa-asymmetric-encryption.