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 щети по репутацията 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 кражба 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.

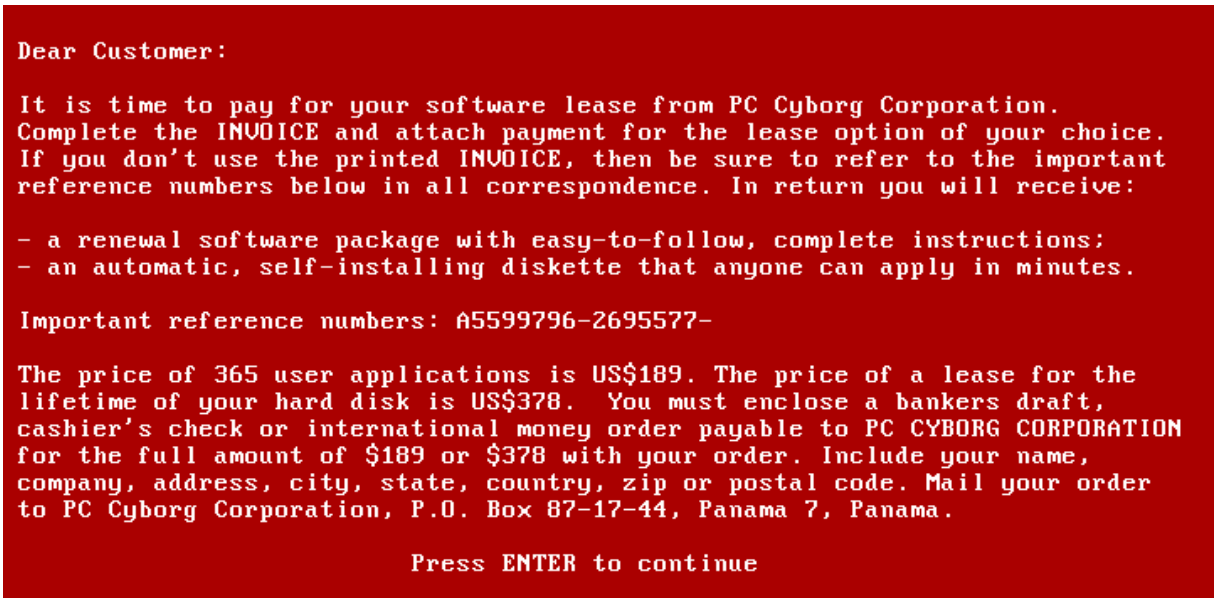
Ransomware става широко разпространен чак през ранните две хилядни – вероятно поради трудността хакера да си получи откупа. Появата на биткойна и криптовалутите променят това. Лесен и удобен начин е за получаване на крупната сума от потърпевшия като остават незабелязани. При традиционното банкиране участниците 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.

Еволюция на Ransomware

1. Ранна фаза на Ransomware

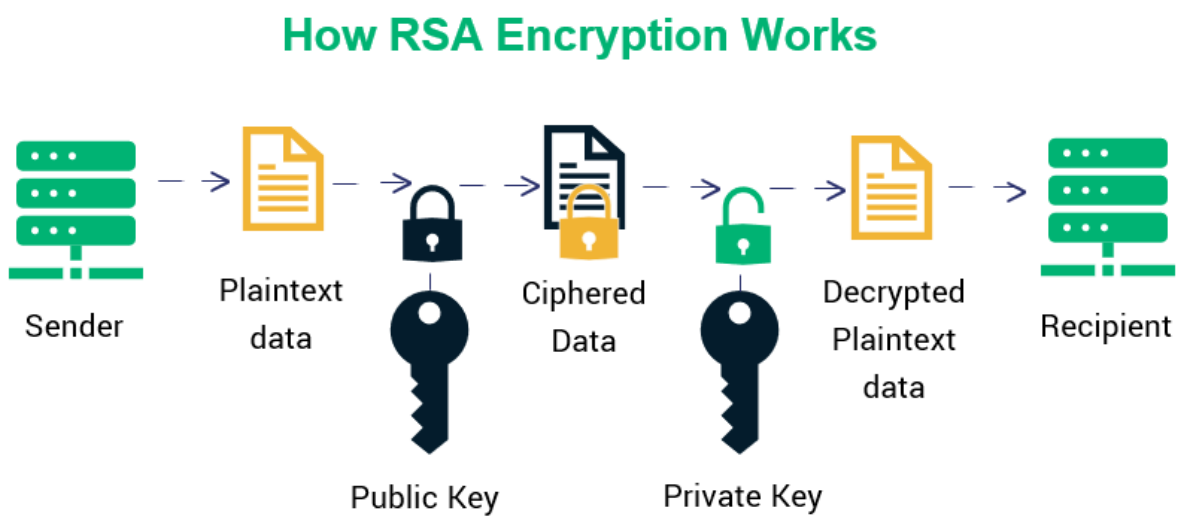
Първичната форма на софтуера за изнудване е, както вече споменахме, инфектирани флопидискове. На фигура 1 е показано, съобщението, което се визуализира на системата афектирана от троянския кон - AIDS trojan (PC Cyborg Virus). AIDS заменя AUTOEXEC.BAT файла, който по-късно се използва да преброи колко пъти компютъра е стартиран. Когато стигне до 90, AIDS скрива всички директории и криптира имената на всички файлове намиращи се на **C:**. Съответно се появява и съобщението за откуп.



(Фиг. 1 – съобщението за откуп на AIDS trojan)

2. Ransomware използващ RSA криптиране

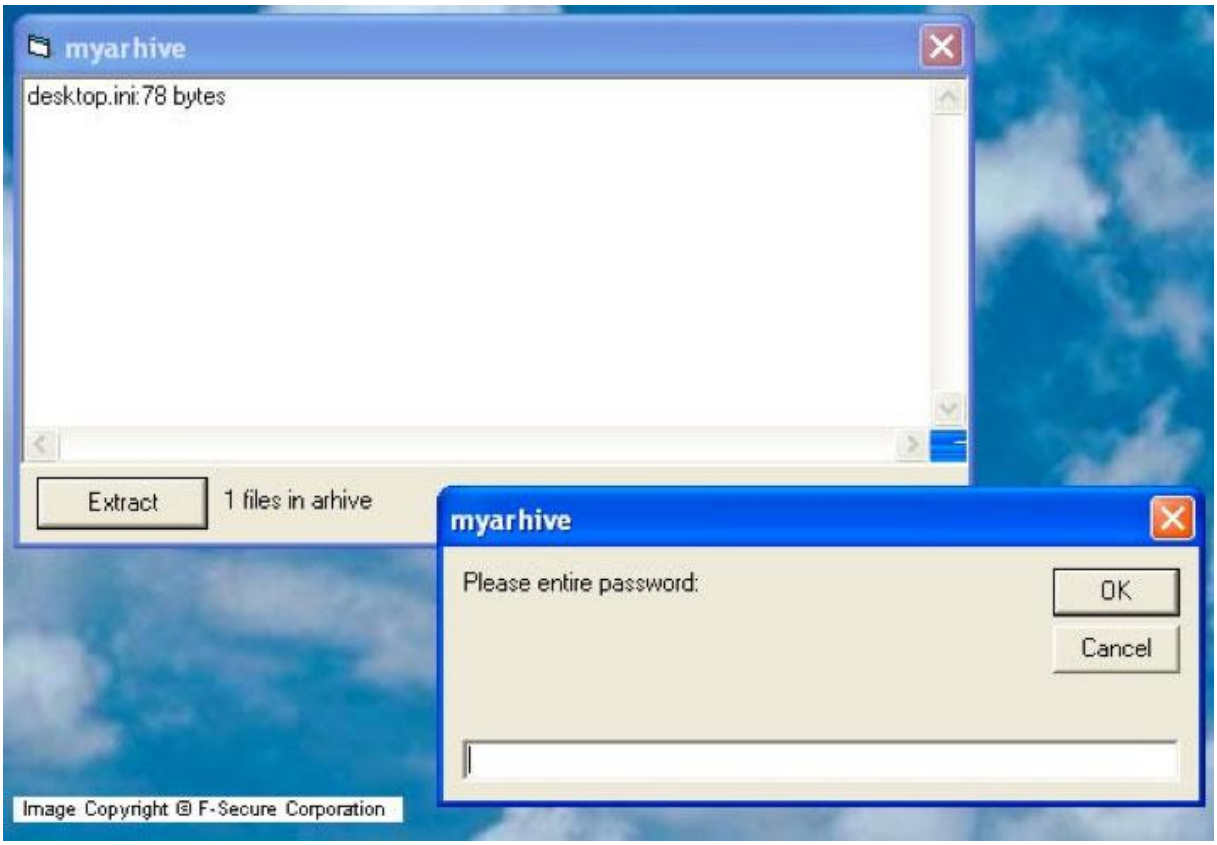
През 2004-2005 г. се появява нова форма на ransomware. Към вирусите се прилагат по-силни криптиращи алгоритми. Archiveus Trojan е първият вирус да използва асиметричен алгоритъм за криптиране на данни – RSA (фиг. 3).



(Фиг. 2 – архитектура на RSA криптиране)

Алгоритъмът използва два ключа, с които се криптира и декриптира информация. 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.

Archiveus Trojan криптира всичко в MyDocuments директорията (фиг. 4) и изисква от потърпевшия да закупи артикули от онлайн аптека, в замяна ще получи 30 символен код, за да възстанови всичките си файлове. Известен „недостатък“ на вируса, е че дори жертвата да заплати откупа, някои от файловете остават коруптнати.



(Фиг. 3 – Изглед на Archiveus Trojan вирус.)

3. Spear phishing Ransomware

Spear phishing е вид phishing атака, при която се таргетира точно определен човек, група или организация. Обикновено целта им е извличане на лична информация, сваляне и инсталация на вируси или изпращане на определена сума капитал на хакера. Постигат го чрез изграждане на фалшиви истории или сценарии. Често фишинг заплахите са прикачени в имейли, социални мрежи, текстови съобщения или телефонни разговори. Spear phishing атаките е най-ефективната форма на атака, понеже измамата е пригодена да бъде максимално убедителна за конкретно лице.

През 2006 година се появява първия spear phishing ransomware. GPCode се разпространява през електронни пощи като прикачен файл под формата на заявление за работа. Променя се desktop background, като е изписано съобщението, че системата е пробита и че е прикачен файл с инструкции (фиг. 5 и 6).

По-новите версии (2010 г.) използват алгоритъм за криптиране RSA-1024, който за времето си е непосилен да бъде разбит чрез brute force. Първите версии на GPCode използват симетрично криптиране, където ключът за криптиране и декриптиране е един и същ. Това го прави лесен за разбиване. Друг недостатък на първоначалния GpCode, е че файловете, които се криптират се запазват на нова локация, а некриптираните се изтриват. Undeletion utility може да възстанови част от файловете.

(Фиг. 4 – Пробита система от GPCode.)

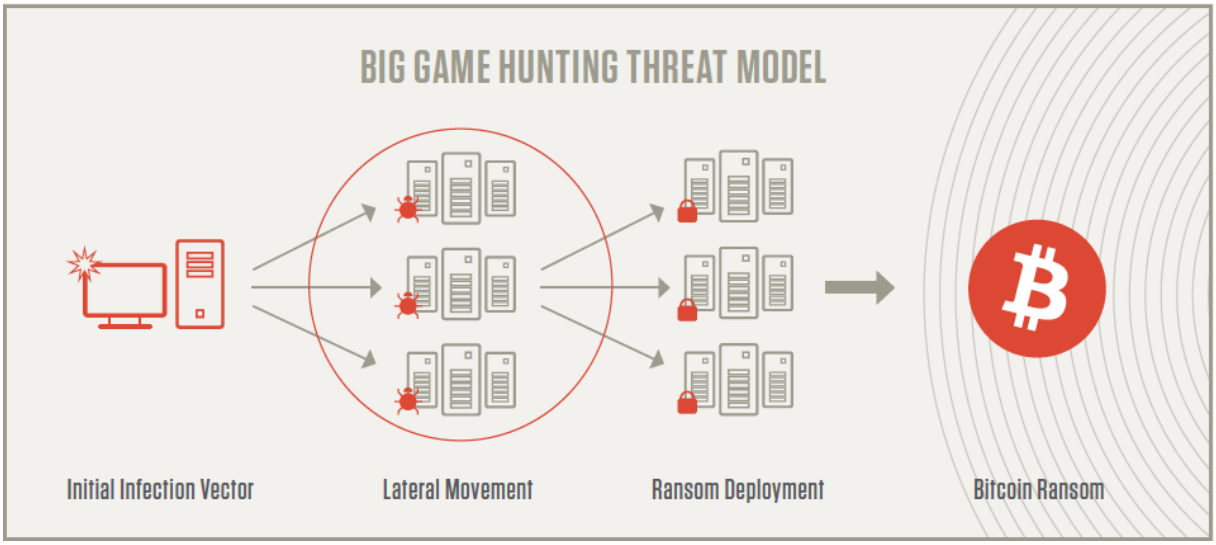
(Фиг. 5 – Инструкции за откуп, GPCode.)

4. Ransomware в Android базирани системи

LockerPin е първият malware, който атакува мобилни системи. Потребителят обикновено инсталира приложения от пиратски сайтове, но се промъква и троянския кон – LockerPin. Опитва да достъпи административни правомощия маскирайки се като софтуерен ъпдейт на телефона, виж фигура 7. Ако потребителят се подведе и изпълни указанията, се сменя PIN на телефона. Единственият начин да си възстанови достъпа е, ако телефона се върне до фабрични настройки. Това означава пълно изтриване на личните данни. Ако реши да плати откупа, пин кодът е неизвестен дори и на хакера, понеже е случайно генерирано число.

(Фиг. 6 – Троянски код маскиран като софтуерен ъпдейт.)

5. Big Game Hunting (BGH) и Ransomware



(Фиг. 7 – Модел на заплахите в Big Game Hunting)

За да оптимизират атаките си, ransomware операторите променят стратегията си. Те се отказват от метода „spray and pray“, при който зловреднният софтуер се разпространява масово, без конкретен избор на жертва. Вместо това започват да таргетират конкретни организации и потребители, или известно още като Big Game Hunting. Идеята е проста, вместо да се надяват някой да се хване и да получат малко сума откуп – стандартно са искали по 300 USD, компанията изложи на подобна атака стават жертва на откупи в суми достигащи десетки хиляди. Такива жертви са River Beach и TravelEx, заплатили съответно 600 000 USD и 2.3 млн. USD. В двата примера атаката е една и също, изтегляне на неверифицирани файлове през phishing имейл.

На фигура 7 е показан модела на атаката в BGH. Започва през едно инфектирано устройство и се разпространява към всички възможни системи в мрежата. Процесът се повтаря, докато се заразяват възможно най-много системи. После се деплойва ransomware-ът и се изисква откуп в биткойни.

Стратегии и защита от ransomware

Настоящите препоръки за превенция и реакция при ransomware атаки се базират на оперативния опит на организации като CISA, NSA, FBI и MS-ISAC. Насоките са предназначени както за ИТ специалисти, така и за лица, участващи в изготвянето на полици и процедури за реакция при киберинциденти.

1. Подготовка за Ransomware и Data Extortion инциденти

Поддръжка на офлайн криптирани backups на критично важната информация и често проверка на изправността на backup-а. От съществено значение е резервният вариант да се поддържа офлайн, понеже повечето ransom атаки опитват да намерят и изтрият или криптират резервни копия на системата. Така се принуждава жертвата да плати откупа.

Поддръжка и ъпдейт на “golden” images на системата. Поддържането на “image”, които имат специфична преконфигурирана операционна система и свързаните с нея софтуерни приложения е важно, понеже по-лесно ще може да бъде възстановена системата и деплойната, виртуална машина или сървър.

Поддържане на резервен хардуер, който да бъде използван при необходимост от възстановяване на системите. Това позволява по-бързо възстановяване на дейността, ако възстановяването на основната инфраструктура не е желано или не е възможно.

Използване на multi-cloud solution е подходящо, понеже може да се съхранява важна информация или резервни копия на системата, като същевременно се добавя още един слой защита. Multi-cloud е препоръчителен, тъй като се намалява риска от vendor lock-in или с други думи организацията не зависи само от един доставчик на cloud. В случай че всички акаунти или услуги при даден облачен доставчик бъдат компрометирани, наличието на резервна инфраструктура при алтернативен доставчик позволява по-бързо възстановяване на системите.

Имплементация на Zero Trust Architecture (ZTA) за превенция на неоторизиран достъп до данни и услуги. Достъпът до данните трябва да бъде възможно най-гранулярен. Тоест https://www.educative.io/answers/what-is-granular-access-control

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.

[8] „archiveus-trojan,“ Knowbe4, [Онлайн]. Available: https://www.knowbe4.com/ransomware-knowledgebase/archiveus-trojan.

[9] Matthew Kosinski, „Spear phishing,“ Ibm, [Онлайн]. Available: https://www.ibm.com/think/topics/spear-phishing.

[10] „Gpcode,“ Knowbe4, [Онлайн]. Available: https://www.knowbe4.com/ransomware-knowledgebase/gpcode.