Ransomware
[CERT-BG]

[TLP-WHITE]

CERT.BG
COMPUTER EMERGENCY RESPONSE TEAM
BULGARIA

Съдържание

Въведение

Неведнъж сме говорили за RANSOMWARE и ще продължим да го правим, заради сериозността на заплахата. С тази брошура ще се опитаме да направим бърз преглед на характеристиките на този тип зловреден софтуер, какво можем да направим, за да предотвратим инцидент, и какво да направим, когато сме вече заразени.

Нека да се спрем на термина „откуп“? Обикновено това означава голяма сума пари, поискана в замяна на някого или нещо. Най-често се използва в случаи на отвличане, когато похитителят изисква откуп в замяна на заложника.

Ransomware е вид зловреден софтуер, който блокира потребителите от използване на собствените им компютърни системи и криптира техните файлове, като дава на нападателите контрол над всяка информация, съхранявана на устройствата на жертвите. След това киберпрестъпниците заплашват да изтрият данните на жертвите, докато не бъде платен откуп. Корените на този тип зловреден софтуер могат да бъдат проследени до края на 80-те години. Първият такъв зловреден софтуер е написан от Джоузеф Поп през 1989 г. и е известен с името „PC Cyborg“.

CERT България НЕ съветва жертвите на ransomware атаки да заплащат искания откуп, защото това не гарантира декриптиране на вече криптираните файлове или отключването на устройството, дори напротив – може дори да доведе до допълнителни бъдещи атаки.

Видове Ransomware

Има безброй видове ransomware, повечето атаки попадат в две основни категории: **`crypto ransomware`** и **`locker ransomware`**.

- Crypto ransomware работи, като криптира чувствителните компютърни файлове на жертвите и изисква откуп, преди файловете да могат да бъдат възстановени.
- Locker ransomware не криптира файлове. Той компрометира основните компютърни функции и заключва изцяло устройството, докато не бъде платен откуп.

Тежестта на заплахата, произтичаща от една такава атака с ransomware, ще зависи от използвания вариант на ransomware, а методите за възстановяване от инцидента се различават в зависимост от конкретния вид на използвания зловреден софтуер.

CERT България препоръчва, за да идентифирате с кой ransomware сте заразен и има ли декриптор за него, да посетите следните сайтове:

ID Ransomware

No More Ransom

Как протича една ransomware атака?

Въпреки че има различни видове ransomware, повечето атаки следват един от няколко предвидими пътища. Това означава, че има определени превантивни стъпки, които всеки бизнес може да предприеме, за да се предпази от атака. Най-популярните от тези стъпки са надграждането до последните версии на ползваните от Вас софтуерни приложения и прилагането на двуфакторна автентификация (2FA).

Както може би сте забелязали диаграмата е разделена на три фази, показващи от входните точки на атакуващите до крайният етап, където атаката е успешна и се поиска откуп.

Първата фаза показва как нападателят търси начини да проникне в мрежата. Най -често срещаните начини използвани от нападателите са:

- получаване на потребителски имена и пароли за влизане в компютъра чрез фишинг кампания;
- използване на слабости в системи, които са свързани с интернет, като например имейл сървър или системи за отдалечен достъп;
- изпращане на зловреден софтуер чрез файлове, заразени със зловреден софтуер, прикачени към имейл.

Втората фаза показва как атакуващият се стреми да получи администраторски права върху всички възможни устройства във Вашата мрежа.

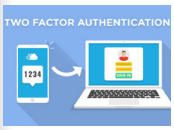
Третата фаза започва след като нападателят е получил достъп до системите във Вашата мрежа и вече е готов да извърши същинската част от атаката – криптирането на системи и данни.

Фаза I

Най -доброто място за спиране на една атака е преди тя дори да е започнала, а именно Фаза 1:

-Нападателите най-често използват фишинг.

Бъдете внимателни, когато щракнете директно върху връзки в имейли, дори ако изпращачът е някой, когото познавате. Опитайте се независимо да проверите адресите на уебсайтове. Обърнете внимание на адресите на уебсайта, върху които кликвате, както и на тези, които въвеждате сами. Зловредните адреси на уебсайтове често изглеждат почти идентични с легитимни сайтове, като често се използват леки вариации в правописа или различен домейн.



-Налучкване на парола (т. нар. password guessing).

За да получат валидни комбинации от потребителско име и парола и да използват тази информация за влизане в имейли или системи за отдалечен достъп. За да се предпазите от влизане на нападател във вашата система за отдалечен достъп, използвайте дълги, силни и уникални пароли или включете 2FA (двуфакторна автентификация).

-Използване на уязвимости в софтуерни приложения.

Поддържайте всичките си операционни системи и софтуерни приложения чрез обновяване до последни актуални версии. Така Вие ограничавате броя на слабостите, които атакуващ може да използва, за да получи неоторизиран достъп до Вашите компютри.

-Чрез имейл.

Друг често използван от нападателите метод е изпращането на документ или електронна таблица, прикачени към имейл, които при отваряне се опитват да заредят зловреден софтуер на Вашия компютър. Бъдете изключително внимателни с .exe или .dmg (изпълними) файлове, както и файлове с разширения, които не познавате. Мрежовите устройства за сигурност, като например някои защитни стени (firewall), могат да идентифицират тези файлове, когато те преминават през мрежата и да ги блокират или карантинтиннират. Това няма да спре всички ransomware атаки, но ще попречи на много от тях и е добра първа стъпка за защита. Ако в огранизацията Ви не използвате Macros-и за работа с Doc или xls файлове, може да забраните активирането на macros-и, чрез групова политика или локално за работните станции и никога да не се разрешава ползването на макроси при отваряне на прикачен DOC файл, особено ако при отваряне на документа на началната страница има указания и стрелки за позволяване на съдържание (Enable Content).Също така никога да не се отварят прикачени към e-mail-и JSE, .VBS, .VBE, .WSF, .WSH ,.SCT и .HTA и подобни script файлове.

Фаза II

Във Фаза 2 нападателят ще се опита да използва първоначалния компютър, който е компрометирал, и да получи административен достъп до всички компютри и устройства във вашата мрежа.

Командния сървър (C&C) е мястото, откъдето нападателят ще зареди допълнителен зловреден софтуер на компрометирания компютър. Това ще му позволи да превърне достъпа си в постоянен (например, ако рестартирате компютъра) и да команва Вашият компютъра да атакува други устройства във Вашата мрежа. За пореден път антивирусните системи с последни дефиниции са едни от най -добрите защитни средства за спиране на атаката на този етап.

След като нападателят вече има контрол над конкретно устройство, той се стреми да разшири достъпа си и да получи пълен административен достъп до всички устройства във Вашата мрежа. Използването на защитни стени за разделяне на мрежата на отделни сектори (компартментализация) може да ви помогне да спрете нападателя да се разпространи и да зарази и други устройства.

Фаза III

Стигаме до Фаза 3, където нападателят вече е получил достъп до множество различни системи във Вашата организация и вече е готов да извърши най-увреждащата част от атаката.

На този етап нападателите са изтрили Вашите архиви и са криптирали и/ или откраднали Вашите данни и вече Вие разбирате, че имате компютърен инцидент.

Тук вече си задавате въпроса- Как мога да изляза от тази ситуация?
Вашия процес за архивиране и възстановяване на данни (backup) работи правилно. Ако можете да възстановите криптираните файлове от архивите, ще бъдете в състояние да се възстановите от успешна ransomware атака с малко или никакво влияние върху Вашата организация. За тази цел архивите трябва да се съхраняват на място, което не е достъпно за ransomware атакуващият (например ако устройството, на което са архивите е офлайн или не е свързано към заразената машина). Имайте предвид, че атакуващите обръщат особено внимание на архивите като част от усилията за криптиране на всички ценни файлове.

“Подгответе се за най-лошото”

Плащането на откуп за извличане на файлове трябва да бъде последната крайна мярка за всяка организация. Плащанията помагат за забогатяване на криминалните организации и подхранват по-нататъшни атаки, включително и срещу Вас самите. Дори ако нямате резервни копия на вече криптираните данни, трябва да разгледате възможностите си, преди да платите:

- Може ли да се пресъздадат откраднатите данни?
- Имате ли по-стара версия на файловете, които могат да бъдат обновени / редактирани с нова информация?
- Съществуват ли някъде другаде данните ви, като система на друго място, която не е била компрометирана?
- Потърсете мнение на специалист дали криптираните файлове могат да се разкриптират, без да плащате на атакуващият? Понякога използваните зловредни кодове съдържат слабости в криптирането, които могат да бъдат използвани.

Ако всичко друго се провали и сте решили да платите откупа, трябва да сте готови да направите плащането своевременно. Почти всички ransomware атаки изискват плащане чрез криптовалута. Част от всеки рансъмуер план трябва да включва информация за това как да се улесни плащането в най-лошия случай.

Имайте предвид, че дори да платите откупа и атакуващите наистина да Ви предоставят ключ за декриптиране, нямате защита от последващи изнудвания. Много често след първото плащане, атакуващите се свързват отново с Вас и искат пари отново – този път, за да не публикуват всички Ваши данни, които те вече са откраднали. Понякога атакуващите се опитват да вземат пари трети път, като се свързват с Вашите клиенти и партньори, чиито данни са откраднали от Вас и изнудват тях.

CERT България НЕ съветва жертвите на ransomware атаки да заплащат искания откуп, защото това не гарантира декриптиране на вече криптираните файлове или отключването на устройството, дори напротив – може дори да доведе до допълнителни бъдещи атаки.

Think before you click!

Traffic Light Protocol (TLP):

[TLP-RED] – Само за определени получатели: в контекста на една среща, например, информацията се ограничава до присъстващите на срещата. В повечето случаи, тази информация се предава устно или лично.
[TLP-AMBER] – Ограничено разпространение: получателят може да споделя тази информация с други хора от организацията, но само ако е спазен принципът "необходимост да се знае". Честа практика е източникът на информацията да уточни веднага след маркировката на кого може да се споделя или да предвиди ограничения на това споделяне. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.
[TLP-GREEN] – Широка общност: информацията в тази категория може да бъде разпространявана широко в рамките на дадена общност. Въпреки това информацията не може да бъде публикувана или поствана в Интернет, както и изнасяна извън общността.
[TLP-WHITE] – Неограничено: предмет на стандартните правила за авторско право; тази информация може да се разпространява свободно, без ограничения.

CERT Bulgaria

E-mail: cert@govcert.bg
Tel: +359 2 949 22 12
Mobile: +359 878 908 546
Web: www.govcert.bg