ЗБОРНИК НА ТРУДОВИ

Трета меѓународна научна конференција
„Науката – подршка на развојот во
Република Македонија“

Скопје 29-30 јануари 2016

ЗБОРНИК НА ТРУДОВИ: Трета меѓународна научна конференција „Науката – подршка на развојот во Република Македонија“

Организатор: Институт за дигитална форензика
Универзитет „Евро-Балкан“ - Скопје

Уредник: Проф.д-р Сашо Гелев

Издавач: Универзитет „ЕВРО-БАЛКАН“ Скопје
Република Македонија
www.euba.edu.mk

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

001.3:330/378(497.7)(062)

МЕЃУНАРОДНА научна конференција (3 ; 2016 ; Скопје)
Науката - поддршка на развојот во Република Македонија : зборник на трудови / Трета меѓународна научна конференција, Скопје 29-30 јануари, 2016 ; [уредник Сашо Гелев]. - Скопје : Универзитет "Евро-Балкан", 2016. - 208 стр. : илустр. ; 30 см

Фусноти кон текстот. - Библиографија кон трудовите. - Abstract

ISBN 978-608-4714-15-6

а) Научен развиток - Општествени науки - Македонија - Собири
COBISS.MK-ID 100693514

Програмски одбор

- Проф. Д-р Митко Панов, Универзитет Евро Балкан - Претседател
- проф. Д-р Сашо Гелев – Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија копретседател
- Проф. Д-р Влатко Чингоски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Проф. Д-р Божо Крстајиќ, Електротехнички факултет - Подгорица, Црна Гора
- Проф. д-р Здравко Скакавац, Факултет за правне и пословне студије, Универзитет УССЕ, Нови Сад;
- Проф. д-р Лада Садиковиќ, Факултет за криминалистика, криминологија и безбедност, Универзитет во Сараево;
- Проф. Д-р Тони Стојановски, Австралија
- Проф. д-р Гордан Калајџиев, Правен факултет, Универзитет Св. Кирил и Методиј – Скопје, Република Македонија
- Д-р Никола Протрка, Полициска академија, Загреб, Република Хрватска
- Проф. Д-р Стефан Сименов, Академија за внатрешни работи на Р. Бугарија
- Проф. д-р Весна Матијашевиќ Покупец, Универзитет Евро Балкан
- Доц. д-р Вангел Ноневски, Универзитет Евро Балкан
- Доц. д-р Роман Голубовски, Електротехнички факултет Радовиш Универзитет Гоце Делчев Штип, Република Македонија
- Д-р Зоран Нарашанов, Винер осигурување, Скопје, Република Македонија
- Проф. д-р Марјан Николовски, Факултет за безбедност, Универзитет Св. Климент Охридски, Битола, Република Македонија
- д-р Дијана Стојановиќ Ѓорѓевиќ, Универзитет Евро Балкан

Организацискиодбор

- Проф. д-р Сашо Гелев, претседател
- Доц. Д-р Мимоза Клековска, член
- Доц. Д-р Снежана Черепналковска-Дуковска, член
- Доц. д-р Вангел Ноневски, член
- М-р Игор Панев, член
- Зорица Каевиќ, член
- Ивана Гелева, член

П Р Е Д Г О В О Р

Конференцијата се организира да се согледа влијанието на науката – како основна подршка во развојот на Република Македонија.

Пред две години за прв пат ја организиравме оваа конференција со цел студентите од вториот и третиот циклус на студии да се оспособат за пишување и презентирање научно-стручни трудови, а останатите учесници да ги пренесат своите најнови истражувања во посочените области.

Втората конференција во однос на првата по бројот на презентирани трудови беше поспешна. Презентирани беа повеќе од 60 труда.

Третата конференција се одржа малку подоцна со помал број на трудови но поквалитетни. Најдобрите трудови од оваа конференција покрај зборникот на трудови од конференцијата, ќе излезат и во наше списание со интенција тоа да прерасне во меѓународно списание.

Проф. Д-р Сашо Гелев

СОДРЖИНА

угд 004.492:004.738.4.056.5

Марјан Крстевски

Министерство за одбрана на

Република Македонија

Сашо Гелев

Електротехнички Факултет, Универзитет Гоце Делчев- Штип, Македонија

RANSOMWARE – КОМПЈУТЕРСКИ ВИРУС НА ДЕНЕШНИЦАТА

Апстракт: *Интернет, глобалната компјутерска мрежа за краток временски период од десетина години еволуира во моќна мрежа без која не може да се замисли животот на современиот човек. Кога оваа компјутерска мрежа би престанала да функционира, дури тогаш би се сфатило нејзиното значење и во колкава мера се има проткаено во сите пори на општественото живеење. Бројот на корисници на интернет од година во година се повеќе се зголемува. Споредбено со развојот и имплементацијата на компјутерската мрежа во систем на глобална мрежа – интернет, раснат и потенцијалните опасности од различни напади од интернет, вклучувајќи многу малициозни програми и напади од човечки фактор како хакери, вандали и компјутерски терористи.*

Денес имаме голем број на различни малициозни програми кои освен со нивната разновидност, се разликуваат и по начинот на кој го инфицираат незаштитениот компјутер.

Во последните две до три години еден од најопасните малициозни програми кој го привлече вниманието на целата интернет популација е ransomware.

Во трудот што следи ќе биде дефинирано што е ransoware, *како напаѓа и неговата историја. Потоа ќе стане збор за CTB-Locker-от, како еден од најпознатите видови од фамилијата на* ransomware *кој бележи драстичен скок на употреба во првото тромесечје од 2015 година, како доаѓа до инфекција со CTB-Locker-от, како истиот функционира и што е потребно да превземете кога ќе откриете дека вашиот компјутер е заразен со CTB Locker. На крај во трудот ќе бидат презентирани неколку методи за враќање на фајловите криптирани со CTB Locker.*

Клучни зборови: *ransomware, CTB Locker, криптирање, откуп, дешифрирање*

RANSOMWARE – COMPUTER VIRUS OF NOWADAYS

Abstract: *Internet, the global computer net, for short period of about ten years has evaluated into powerful net without whom we cannot imagine the life of the contemporary man. When this computer net would stop functioning then would be realized its meaning and in what extent it has woven in every pores of the social living. The number of the Internet users is becoming larger from year to year. Compared to the development and the implementation of the computer net in the system of the global net-the Internet, are growing the potential dangers from different attacks from the Internet, including many malware programs and attacks from the human factor like hackers, vandals and computer terrorists.*

Today we have big number of different malware programs which differ in the way that they infect the unprotected computer besides their diversity.

In the last two to three years, one of the most dangerous malware programs which attracted the attention of the whole Internet population is ransomware.

In the work that will follow it would be defined what is ransomware, how attacks and its history. Then it would be mentioned the CTB-Locker as one of the most famous kinds of the family ransomware which marks drastic leap in the use of the first trimester of 2015, as it comes to infection with the CTB-Locker, how it functions and what it's necessary to take over when you will find out that your computer is infected with the CTB-Locker. In the end, in the work it would be presented several methods for returning the files encrypted with the CTB-Locker.

Keywords: *ransomware, CTB Locker, encrypted, ransom, decoding*

1. ВОВЕД

Малициозниот софтевер е софтвер (скрипта или код) направен со цел да се наруши некоја компјутерска операција, да се соберат чувствителни операции или да се добие неовластен пристап до компјутерските системи. Тоа е општ термин кој се користи од страна на компјутерски професионалци да означи различни форми на непријателски, нападни или досадни програми.

Денес имаме голем број на различни малициозни програми кои освен со нивната разновидност, се разликуваат и по начинот на кој го инфицираат незаштитениот компјутер.

Во последните две до три години еден од најопасните малициозни програми кој го привлече вниманието на целата интернет популација е ransomware.

Ransomware е вид на вирус од поновите генерации, кој има задача да го заклучи вашиот компјутер со порака од типот „Вашиот компјутер е заклучен од страна на FBI/CIA/Interpol… затоа што на 11 Април оваа година, вие или некој друг од овој компјутер, имате посетувано сајтови со детска порнографија“ и да ви понуди прифатлив договор дека вашиот компјутер ќе биде отклучен и дека против вас нема да се води никаква законска постапка ако платите, на пр. 200 долари, во наредните 2-3 дена.

Ransomware на вашиот компјутер ќе инсталира сет на малициозни програми кои во потполност ќе ја оневозможат неговата работа. Освен што може да ви го заклучи компјутерот, постои и опасен вид на ransomware вирус кој може да ги шифрира сите важни за вас фајлови, без можност да ги вратите фајловите дури и по активирање на антивирусната програма и на тој начин ќе ве присили да платите одредена сума на пари и да се надевате дека фајловите ќе бидат дешифрирани и вратени назад.

Ransomware е изведен од англискиот збор Ransom, што во превод значи уцена, а ware е изведен од Software, што отприлика значи компјутерска програма. Буквалниот превод би бил компјутерска програма за уцена, но некои го нарекуваат и полициски малвер, затоа што во голем број на случаеви се закануваат со полиција доколку не платите.

2. ШТО Е RANSOMWARE

Ransomware е вид на малициозна програма или код кој ги краде и шифрира датотеките на жртвата, за да подоцна напаѓачот би изнудил одредена сума на пари во замена за клучот за дешифрирање на кодот. Документирани случаеви на вакви напади се ретки, но истите се во пораст. Еден од првите документирани случаи на ransomware напад е забележан во Мај 2005 година. Самата програма која ги шифрира датотеките често пати не е тешка за решавање, но постојат и комплексни програми кои користат хибридни методи слични на военото шифрирање. Таквата програма се вика Cryptovirus, Cryptotrojan или Cryptoworm.

Ransomware се шири глобално, речиси да не бира жртви, затоа што крајната цел не му е да управува со системот и да има пристап до важните податоци, туку потенцијалната заработувачка од откупувањето, во зависност од тоа колку се податоците важни за жртвата. Цената на откупувањето се движи од 300 до 2000 долари, а бројот на заразени компјутери се движи од десетина илјади и од ден во ден таа бројка се повеќе се зголемува.

3. КАКО НАПАЃА RANSOMWARE

Уценувачкиот напад на ransomware се изведува по пат на посебно изградена програма која се испраќа како attachment на електронската пошта која се праќа на жртвата. Жртвата кога ќе го отвори или активира attachment-от, се покренува програмата и шифрира одреден број на датотеки (или сите датотеки) на хард дискот од компјутерот. Во електронската пошта на жртвата се наоѓа и порака која и кажува на жртвата дека успешното дешифрирање може да се направи само со помош на одговарачкиот клуч за дешифрирање, кој напаѓачот (наводно) ќе и го испрати на жртвата, откако истата ќе му исплати на напаѓачот одредена сума на пари.

Корисникот чии што компјутер е нападнат често пати има само читлив документ во кој е известен за нападот и документ со инструкции како ќе ги врати заклучените датотеки. Меѓутоа кога програмата се ослонува исклучиво на симетричната криптографија, клучот за

дешифрирање често се наоѓа во самата програма и може да се извлече без да се контактира напаѓачот, што од друга страна укажува на неискуството на напаѓачот.

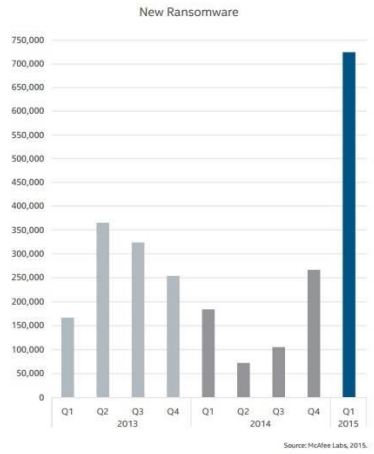
4. ИСТОРИЈАТА НА RANSOMWARE

Во Мај 1996 година Adam Young од Универзитетот во Колумбија презентирал документ Criptovirology-extortion-based security threats and countermeasures на IEEE's Security and Privacy symposium. Тој го опишал развојот на првиот прототип на ransomware. Од моментот на појавата на тој иновативен документ во 1996 година, истражувачите имаат опишано многу сценарија за појавата на овој malware.

Еден од првите познати malware од фамилијата ransomware е Gpcode.ak, кој се појавил во 2008. Malware-от има криптирано огромен број на фајлови на компјутерите на жртвите. Еден од најпознатите malware од фамилијата ransomware е CryptoLocker кој се има појавено во Септември 2013 година.

Дека станува збор за малициозна програма која е во пораст, говорат и статистиките каде активноста на ransomware во првото тромесечје од 2015 година е зголемено за 165%. Особено забележливо е дејствувањето на оние вируси од фамилијата на CTB-Locker, со новите верзии на CryptoWall, TorrentLocker и BandarChor. Исто така во првото тромесечје од 2015 година е забележан и нов вид наречен Teslacrypt. Сето напред наведено може да се забележи од графикон 1.

Графикон 1: Пораст на Ransomware во период од 2013 до првото тромесечје од 2015 година



Извор: McAfee Labs, 2015

Овие видови на ransomware воглавно напаѓаат жртви од богатите земји, затоа што корисниците од овие земји се повеќе подготвени да платат.

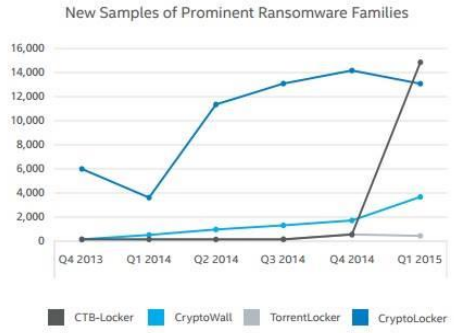
Новата технолигија низ овие неколку години го има направено ransomware многу моќен вирус, што се огледа преку следното:

- Виртуелен начин на плаќање: користејќи виртуелен начин на плаќање, изнудувачите го избегнуваат традиционалниот начин на плаќање со цел да не остават некаква трага при трансферот на парите;
- Tor network: користејќи tor network, напаѓачите можат многу полесно да ја сокријат локацијата од каде го контролираат серверот, од каде и ги продаваат клучевите на жртвата. Овој вид на мрежа овозможува криминалната инфраструктура да се одржува долг период, па дури и да се изнајмува на други напаѓачи;
- Можноста вирусот да се пренесе и на мобилен: Во Јуни 2014 година за првпат е откриен вирус од фамилијата ransomware кој ги има криптирано податоците на уредите со андроид систем. Истиот, со помош на AES енкрипција, ги криптира податоците на мемориската картичка на телефонот и преку Tor, SMS и HTTP се поврзува со напаѓачот;
- Заразување на различни уреди за складирање на податоци: Во Август 2014 година Synolocker почнал да ги таргетира мрежите на кои се имаат приклучено уреди за

складирање на податоци. Malware-от искористувајќи ја ранливоста на овие уреди, од далечина ги криптира податоците користејќи RSA 2,048-bit keys или 256-bit keys.

На следниот графикон можат да се видат едни од најпознатите видови на малвери од фамилијата на ransomware, а од графиконот може да се забележи и енормно високиот раст на CTB-Locker –от во првото тромесечје од 2015 година.

Графикон 2: Видови на малвер од фамилијата на Ransomware



Извор: McAfee Labs, 2015

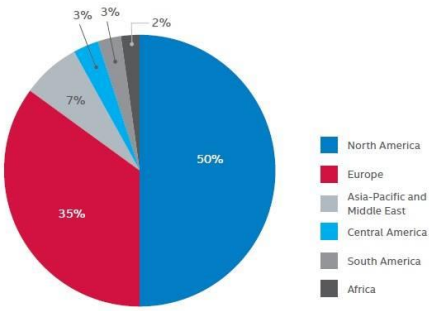
Во понатамошниот дел од овој труд ќе се задржам на CTB-Locker-от, како еден од најпознатите видови од фамилијата на ransomware кој бележи драстичен скок на употреба во првото тромесечје од 2015 година.

5. ЗОШТО Е ВАЖЕН CTB LOCKER-OT

CTB Locker-от е специфична ransomware закана и многу честа тема на дискусија во IT светот. Се шири со спамови на голем број адреси, првенствено во САД и Велика Британија. Често пати се појавува паралелно со backdoor тројанци, downloader-и, massmailer, со вируси кои ги крадат лозинките и слично. Самостојно се инфилтрира или со помош на наведените малвери како додатна компонента. Она по што се разликува од сличните закани, се вредните и упорни создавачи кои држат чекор со промените во технологијата на заштита и континуираното објавување на нови начини на инфекција на различна група на корисници.

Почнувајќи од минатата година кога е забележан, CTB Locker покрај целни групи во САД и Велика Британија се има проширени и низ останатиот дел од светот, затоа што за спам пораките не постои географско ограничување. На почетокот биле напаѓани куќни корисници, потоа малите и средните претпријатија, а сега на мета се и големите компании.

Графикон 3: Присуство на CTB Locker-от по континенти, изразено во проценти



Извор: McAfee Labs, 2015

Уште еден начин на напад кој го користи се отворените RDP портови, а најранливи се оние кои се обезбедени со слаба лозинка. Без разлика дали напаѓа од надвор или од веќе

заразен компјутер во компанијата, овој малвер ќе го провери стандардниот порт 3389 и ќе ги проба најчесто користените лозинки (admin, 12345, password, P@ssw0rd итн). Способен е да ги инфицира популарните формати на фајлови (.doc, .jpg, .pdf, итн.), без разлика дали се наоѓаат на компјутерот, на екстерен хард диск, на USB стикови, на мрежни фолдери, па дури и во cloud, доколку корисникот има подесено перманентен пристап. Ако е да речеме вашиот Dropbox мапиран локално и постојано е online, целните фајлови исто така ќе бидат инфицирани, односно криптирани.

Во овој момент CTB Locker брои над десетина илјади заразени компјутери, иако е проценето дека се испратени милиони спам пораки со овој малвер. Останатите корисници најверојатно, како и што се препорачува, ги имаат избришано овие спам пораки без да ги отворат, а со тоа го имаат решено проблемот од можно активирање на потенцијалната закана.

Погодените корисници завршуваат со огромен број на шифрирани фајлови. Најчесто тоа се Microsoft Office документи, Adobe формати, Tunes и останати видео и аудио записи, вклучувајќи и фотографии.

6. КАКО ДОАЃА ДО ИНФЕКЦИЈА СО CTB LOCKER

Како што веќе претходно рековме, CTB Locker се дистрибуира низ агресивна спам кампања. Спам пораките обично во прилог содржат fax или invoice известување со кое се бара итен одговор. Отворање на прилогот (invoice, pdf, exe или сл.), значи активирање на тројанец Win32/TrojanDownloaderElenoocka, а чија улога е да го контактира командно-контролниот центар и да го превземе главниот дел од инфекцијата, Win32/Filecoder.DA.Gen, познат под името CTB Locker. CTB Locker понатаму ги скенира и криптира сите кориснички документи на компјутерот и бара откуп во замена за клучот за декриптирање. Тука наидуваме на првиот и најголем недостаток на инфекцијата – дури и ако го отвориме прилогот и тројанецот да помине низ антивирусната програма, процесот на превземање на CTB Locker-от од командниот центар може да се прекине доколку имаме firewall, односно т.н. заштитен sид. Во тој случај firewall ќе детектира излезна комуникација на тројанецот и ќе го праша корисникот дали сака тоа да се случи.

7. КАКО ФУНКЦИОНИРА CTB LOCKER ИЛИ CITRONI

CTB Locker (Curve-Tor-Bitcoin Locker), исто така познат и како Citroni, е малвер за криптирање на фајлови пуштен во средината на Јули 2014 година чија што цел се сите верзии на Windows оперативниот систем. Криминалната група која го користи овој вирус, користи нова технологија за криптирање со елиптична крива и комуникација со командниот центар преку TOR мрежи. Овој вирус се дистрибуира со помош на сет алати кои се продаваат online за 3000 американски долари, а во цената се вклучени и инструкциите за поставување и пуштање во оптег.

Кога го инфицира компјутерот CTB Locker-от, незабележливо ги скенира сите фајлови и ги криптира, по што корисникот повеќе не може да им пристапи на истите. Во следниот чекор од инфекцијата на екранот од компјутерот се покажува информација дека вашите податоци се шифрирни и има упатство за плаќање на откупот во крипто валута од 2 BTC (Bitcoin), која во долари зависи од курсот на доларот и моментално изнесува околу 500 долара.

Откако ќе го детектира одговарачкиот фајл, CTB Locker го заклучува користејќи енкрипција со елиптична крива, единствена за овој вид на malware. Кога ќе заврши скенирањето, се прикажува известување со инструкции за плаќање, се менува desktop сликата и се поставува %MyDocuments%/AllFilesAreLocked<userid>bmp фајл кој содржи исти упатства. На крајот креира текстуален фајл %MyDocuments%/DecryptAll Files<user_id>.txt и html фајл % MyDocuments%/<random>.html со упатство за пристап на сајтот на malware-от и плаќање на откупнината.

Уште една необична карактеристика на ваков вид на инфекција е дека за комуникација со командно-контрлниот сервер користи TOR мрежа наместо интернет. Оваа техника на прикривање драстично го отежнува следењето и лоцирањето на командниот сервер.

После restart –от на компјутерот, malware-от прави копија на својот извршен фајл и му издава задача за да се стартува при следното логирање, па затоа не треба да се изненадите ако во %Temp% фолдерот наидете на бројни копии на истиот извршен фајл под различни имиња.

8. ШТО ТРЕБА ДА НАПРАВИТЕ КОГА ЌЕ ОТКРИЕТЕ ДЕКА ВАШИОТ КОМПЈУТЕР Е ЗАРАЗЕН СО CTB LOCKER

Доколку се посомневате дека сте заразени со CTB Locker (го имате отворено прилогот од спам пораката, имате отворено pdf фајл, а Acrobat Reader не е покренат, фајлот се има изгубено после покренувањето), веднаш прекинете ги сите мрежни врски на компјутерот и веднаш направете скенирање со ажурна антивирусна програма. Важно е тука да се напомене, дека компјутерот не треба да се исклучи доколку сакаме одреден форензички експерт со соодветна форензичка алатка да се обиде да го најде клучот во RAM-от. За жал поголем број на корисници не сфаќаат дека се заразени со овој вид на инфекција, се додека не им се појави порака со известување, а тогаш фајловите се веќе шифрирани. Скенирањето ќе ја отстрани инфекцијата и ќе спречи повторно стартување по логирањето на корисникот.

9. CTB LOCKER НУДИ ПРОБНО ДЕШИФРИРАЊЕ НА 5 ОДБРАНИ ФАЈЛОВИ

Варијантата која се има појавено во Август минатата година дава можност за дешифрирање на 5 фајлови. Доколку во главниот прозорец за известување кој се појавува по извршеното криптирање кликнете на Next, ќе ви биде понудено да дешифрирате 5 фајлови бесплатно. Кога ќе кликнете на Search, пребарувањето ќе селектира 5 фајлови и истите ќе ги дешифрира како доказ дека дешифрирањето е можно доколку го платите откупот.

10. ШТО СЕ СЛУЧУВА ДОКОЛКУ НЕ ГО ПЛАТИТЕ ОТКУПОТ НА ВРЕМЕ

После извршената инфекција и извршеното криптирање CTB Locker ќе ве извести дека имате 96 часа (на почетокот ова време било 72 часа) да го платите откупот или ќе ги изгубите вашите фајлови засекогаш. Ова е дел од тактиката на заплашување, затоа што и по изминатите 96 часа ќе можете да го платите откупот, но преку TOR сајтот на malware-от. Кога тајмерот ќе заврши со одбројувањето, ќе ви прикаже Time expired прозор со инструкции како да го платите откупот:

Кога ќе кликнете на Exit, програмата ќе се затвори и malware-от ќе се избрише од системот. После тоа можете да го отворите фјлот под име DecryptAllFiles.txt во Documents фолдерот и да ги следите понатамошните упатства за пристап на сајтот на CTB Locker за дешифрирање.

11. ДАЛИ Е МОЖНО ДА СЕ ДЕШИФРИРААТ И ОСТАНАТИТЕ ФАЈЛОВИ ОСВЕН 5-ТЕ ПРОБНИ

За жал, се уште нема начин да го пронајдете клучот за дешифрирање на фајловите без да платите откуп на CTB Locker сајтот. Откривање на клучот со brute force методата не е реална опција поради големината и потребното време да се пробие ваков вид на криптирање. Исто така ниедна алатка за дешифрирање искористена од разно разни компании нема да работи за овој вид на инфекција. Единствен начин да ги вратите фајловите без плаќање на откуп, е со помош на backup, file-recovery алатки, или доколку имате среќа од Shadow Volume копијата.

12. КАКО ДА ГИ ВРАТИТЕ ФАЈЛОВИТЕ КРИПТИРАНИ СО CTB LOCKER

Доколку вашите фајлови се шифрирани и не сакате да платите откуп, постојат неколку методи за враќање на фајловите во оригиналната форма.

Метод 1: Backup

Првиот и најдобриот метод за враќање е backup. Доколку практикувате backup вашите податоци, по извршеното чистење на инфекцијата, можете да покренете процедура за нивно враќање (restore).

Метод 2: File-recovery softver

Се претпоставува дека при процесот на криптирање, CTB Locker првин прави копија на фајлот, го криптира, па дури тогаш го брише оригиналот. Недостаток на ваквиот пристап е евентуалната можност да избришаните оригинали ги вратиме со помош на некој file-recovery софтвер, како што е R-Studio или Photorec. Важно е да се напомене дека по извршеното криптирање, потребно е што помалку да се користи компјутерот, затоа што создавањето на нови фајлови го отежнува враќањето на некриптираните, избришаните фајлови.

Метод 3: Shadow Volume копија

Како последно засолниште од каде можете да пробате да ги вратите вашите фајлови е од Shadow Volume копијата. За жал, CTB Locker пред извршување на криптирањето ќе се обиде да ги избрише сите Shadow Volume копии на вашиот компјутер, но меѓутоа не успева секогаш во тоа поради недоволните права на пристап, така да потребно е да ја проверите таа опција. За повеќе информации како се врши враќање на податоците со помош на оваа метода, посетете How to restore files encrypted by CTB Locker using shadow volume copies.

13. ЗАКЛУЧОК

Во иднина ќе се појавуваат нови видови и разни варијанти на веќе постојните на овој вид на malware, со нови техники и начини на функционирање. Во почетокот на оваа година, на пример, истражувачите од Швајцарија имаат откриено нова техника на откуп и енкрипција која ја имаат наречено Ransomweb.

Во секој случај, со примена на соодветни антивирусни софтвери, добар заштитен sид, доволна информатичка обученост и со редовен update на софтверот, можеме да се заштитиме од ransomware. Доколку ова се спроведе создавачите на овој malware не може да сметаат на одредена придобивка од луѓе кои имаат барем малку свест за информатичката безбедност.

Електронските закани засекогаш ќе ги има и секогаш некои луѓе ќе гледаат можност како да ја искористат наивноста на некои корисници или слабоста на софтверот заради некоја своја лична корист.

На секој корисник на интернет останува одговорноста да направи чекор напред за подобро информирање и внимателност при користењето, како сите ние би имале подобри и посигурни web страни.

14. КОРИСТЕНА ЛИТЕРАТУРА

[1] EC – Council, Computer Forensics Evidence Collection & Preservation, USA, 2010

[2] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf

[3] http://kompjuteras.com/

[4] http://www.uridium.rs/virusi-koji-ucenjuju-ransomware-programi/

[5] https://muricmilorad.files.wordpress.com/2011/11/maliciozni-software.pdf

[6] https://www.gsws.com/downloads/knowb4/WhitePaper_Ransomware_KnowBe4.pdf

[7] http://www.removevirustoday.com/hr/Ransomware/Kako-ukloniti-ctb-locker-ransomware-20150305.html