Списание „Математика, компютърни науки и образование“ Том 5, кн. 1, 2022
Journal of Mathematics, Computer Science and Education Vol. 5, No. 1, 2022

DOI: 10.54664/VFLF8577

Основни заплахи за киберсигурността

Антоанета Цветанова, Милена Стефанова

Key Cybersecurity Threats

Antoaneta Tsvetanova, Milena Stefanova

Abstract: *The report presents popular cyber threats targeting the financial and banking sectors. It presents the main steps, stages, and characteristics of known cyberattacks carried out in the last decade, as well as an assessment of the damage caused by them. A comparison is made between the attacks examined. Emphasis is placed on key elements targeted by cyber threats today. Possible ways are summarized in which users can protect themselves from cyber threats or prevent them.*

Keywords: *cyberattack; cyber threat; malware; Dyre Wolf; cryptojacking.*

ВЪВЕДЕНИЕ

За да продължи да съществува по време на пандемията от Covid-19, пазарът трябваше бързо и успешно да се адаптира към промените, наложени от ограничителните мерки, изразени в това да бъде намален контактът между хората. Частта от малкия и среден бизнес, която оцеля, адаптира предлагането на стоки и услуги чрез платформи за онлайн пазар и социални мрежи. Много организации и компании, за да предпазят своите служители, преместиха работния си процес онлайн, с което промениха и техния живот. По данни на Националния статистически институт, разликата между закупените стоки и услуги по Интернет преди 2020 г. и след това е близо 10 % [3].

На практика пазарът и работата на компаниите се преместват все повече в дигиталното пространство. По този начин обективно се увеличава степента на уязвимост на личните данни и потенциалните заплахи онлайн.

ИЗЛОЖЕНИЕ

Кибератака е акт за повреда или унищожаване на компютърна мрежа, компютърна система или уебсайт чрез тайно променяне на информация за нея без разрешение [10].

През последните две години процентът на кибератаките реализира скок от 600 %, независимо от техния тип. Те могат да бъдат насочени към различни сфери, като според статистиката, един от най-засегнатите сектори в глобален мащаб е социално-икономическият. Средната стойност на загубите, до които може да доведе една атака за последната година е между $3,86 милиона и $4,24 милиона [6].

В рамките на Европа, проучвания на Европейската агенция за информационна сигурност (ENISA) сочат, че заплахата върху финансите на гражданите е най-малка. Независимо от това, никога не трябва да се подценява риска от загуба на средства и информация.

1. Кибер заплахи във финансовия сектор. Известни са множество заплахи, като обект на изследването са някои от най-често срещаните:

– *Зловреден софтуер* (malware) – вирусен софтуер, специално предназначен да повреди или да получи достъп до компютърна система, без знанието на потребителя.

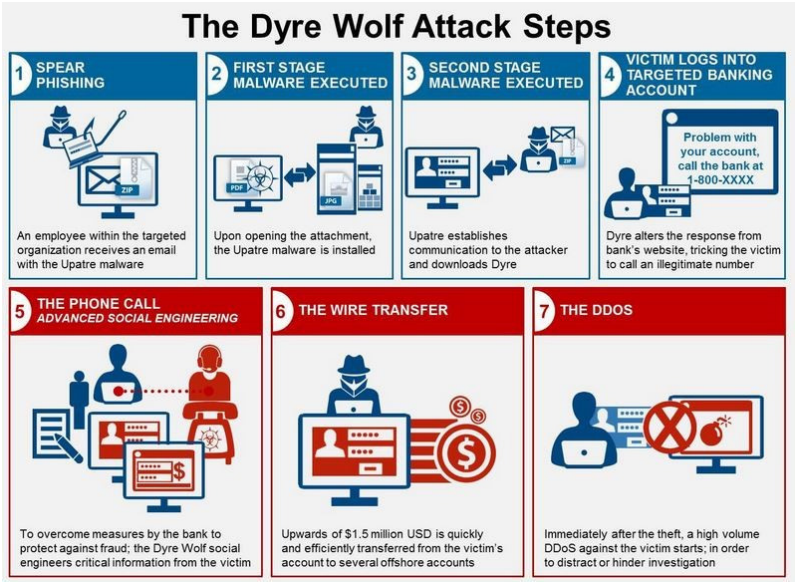
– *Рансъмуер* (ransomware) –вид злонамерен софтуер, който може да блокира достъпа до системата или да криптира потребителските файлове. Обичайно действието е придружено от съобщение с искане за откуп – според хакерите, като единствен начин за възстановяване на достъпа до системата или за получаването на декриптиращ ключ. Оттук е и наименованието на този вид зловреден код – "*ransom*", което в превод от английски език означава откуп.

– *Фишинг* (phishing) – кибератака, при която хакерите изпращат имейли до широка група хора, като с това злонамерено действие целта е заблуда и прихващане на чувствителни данни като потребителско име, парола или детайли за кредитна карта.

В потвърждение на опасността от тях и реалните икономически загуби, до които те могат да доведат, е направен обзор на популярни кибератаки от последното десетилетие, които са причинили мащабни финансови загуби.

2. Dyre Wolf е зловреден софтуер, базиран на троянския кон Dyre, който е насочен към кражба на пари от корпоративни банкови сметки, тъй като през тях редовно се осъществяват транзакции на големи суми. Пикът на тази кибер заплаха е през първото тримесечие на 2015 г., като за този период е изчислено, че с реализирането на Dyre Wolf заплахата са откраднати повече от $1 милион, с което този malware заема челните позиции в списъка на „Топ зловредни софтуери, атакуващи в глобален мащаб".

На Фиг. 1. е представена последователността от стъпки, по които протича Dyre Wolf атаката. Следва детайлно обяснение на всяка от стъпките [5].



Фиг. 1. Dyre Wolf – стъпки, по които се реализира [5]

Стъпка 1. (Spear Fishing) Имейлът, получен от служителя, съдържа архивиран, най-често zip файл, представляващ някакъв документ с генериран случаен номер. Файлът в архива е с PDF икона, но всъщност е с формат EXE или SCR.

Стъпка 2. (Първи етап на атака) Изпълнението й протича през следните фази:

– Зловредният софтуер Upatre използва "checkip.dynds.org", за да определи публичния IP адрес на атакуваната машина. Върнатият IP-адрес се използва, за да бъде инициализирана жертвата.

– Следващ sTUN (Session Traversal Utilities for NAT) сървър се свързва за определяне на публичния IP адрес и вида на NAT (Network Address Translation).

– Проверява се връзката с Интернет, за да се определи дали се използва прокси сървър.

– Осъществява се контакт с Command & Control (C&C) сървър, за да бъде изтеглен Dyre файл от разнообразен списък с домейни, наподобяващи файлови имена.

Стъпка 3. (Втори етап на атака) Последователно се изпълняват следните активности:

– Настойчивост: Като част от инсталацията на Dyre, злонамереният софтуер се налага, като създава “Google Update Service” (googleupdaterr.exe) или услуга „Актуализация на потребителските данни“ (userdata.dat). Тя е настроена да се изпълнява автоматично при всяко рестартиране на системата. След като се стартира и е инжектиран злонамерен код в легитимния sVCHOST.EXE процес, тя спира.

– Установяване на Darknet: Dyre прави връзки с няколко възела, за да установи pear-to-pear тунелна мрежа.

– Прихващане на уеббраузър: веднъж инсталиран и установил връзка с мрежата, злонамереният софтуер Dyre се „закача“ за браузъра на жертвата, за да прихване идентификационните данни, които могат да бъдат въведени в целевите сайтове на банките.

– Разпространение на имейл: ако Dyre открие, че outlook имейл клиентът е инсталиран, той ще се опита да изпрати имейл съобщения до различни получатели с DYRE полезни данни като zip файл.

Стъпка 4. (Жертвата влиза в банковия си профил): Dyre заменя истинския номер на банката с фалшив.

Стъпка 5. (Телефонно обаждане – социално инженерство): злонамереният софтуер може да управлява своите схеми за социално инженерство по различен начин, като постоянно следи дейността на жертвата в банковите сайтове, в рамките на Dyre. Възможни са следните сценарии:

– Класическото инжектиране (The classic injection): в момента, когато засече дейност, злонамереният софтуер заменя стойностите на записаните данни, като не спира да събира идентификационните данни на жертвата.

– Прокси и уебфалшификати: при засечена активност, злонамереният софтуер пренасочва заявката през прокси сървъра към C&C сървър, от където очаква копие на страница на банката, вече адаптирана към оригиналната.

– Инжектиране от страна на сървъра (Server-Side-Injections): прихванатата ли е дейност от страна на жертвата, Dyre прихваща и отговора от сървъра на банката. Когато оригиналният отговор от банката е представен на PHP сървъра, той се преобразува и се изпраща нов отговор на браузъра на жертвата, само че в него са включени и адаптирани кодове. Те се показват в отговора на банката, преди да бъдат изпратени на жертвата.

Стъпка 6. (Мрежов трансфер): след получаване на достъп до данните на жертвата, хакерът влиза в сметката и прехвърля известна сума пари.

Стъпка 7. (DDoS): веднага след като заявеният трансфер се случи, нападателят издава DDoS атака срещу жертвата, използвайки атаки към NTP и DNS, като операторите на Dyre Wolf са в състояние да завладеят всеки ресурс надолу по веригата [5].

2.1. Техники за справяне с кибер заплахата **Dyre Wolf**

На базата на информацията, известна за заплахата Dyre Wolf, от страна на компаниите могат да бъдат предприети следните мерки, за да защитят средствата си или да намалят риска от тяхната кражба:

– Ограничаване на изпълнението на файлове от temp папки;

– Използване на максималните функции за защита при работа в сайта на дадена банка;

– Разграничаване на изпълнимите файлове, които са част от архив, прикачен към имейл съобщения и забрана за тяхното стартиране.

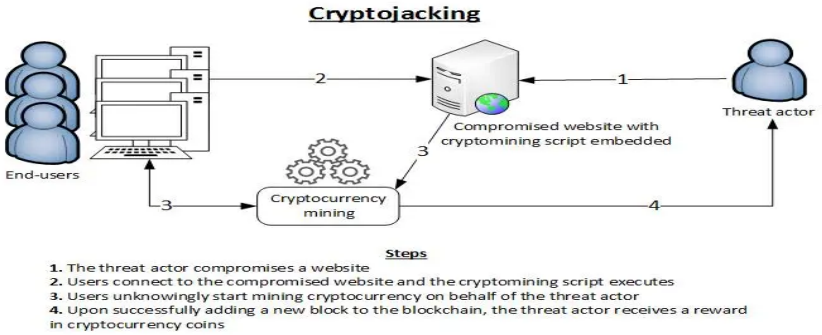
3. Cryptojacking представлява вид киберпрестъпност, при която тайно се изземва изчислителната мощност на дадено устройство, за да се генерира криптовалута. Отнася се също до законни уебсайтове, които не искат съгласието на посетителите преди изпълнение на crypto mining скриптове в браузъра, нито им предоставят възможност да се откажат.

Cryptojacking не изисква значителни технически умения, затова се смята, че рискът хакерите да бъдат и идентифицирани е значително по-малък, отколкото при рансъмуер, а атаките им остават незабелязани за дълго време [7].

Хакерите имат два начина да накарат устройството на жертвата „да копае“ криптовалута:

– *Зареждане на crypto mining код* – по подобие на фишинг атака, жертвата получава имейл с връзка, която изпълнява съответния код на заразеното устройство;

– *Инжектиране на скрипт в уебсайт или реклама* – след посещаване на уебсайта или когато заразената реклама „изскочи“ в браузъра, скриптът автоматично се изпълнява, без да се запазва върху устройството.



Фиг. 2. Cryptojacking – схема на действие [7]

Вредителите често използват и двата метода за по-голяма възвръщаемост на ресурси.

3.1. Техники за справяне с кибер заплахата **Cryptojacking**

За разлика от Dyre Wolf, Cryptojacking е съсредоточена към устройствата на обикновените потребители, затова на базата на информацията за тази киберзаплаха, могат да бъдат обобщени следните мерки за защита или намаляване на риска от повреда:

– *Блокиране на страници и ограничаване на браузъри*, за които е известно, че използват скриптове за Cryptojacking;

– *Използване на приложения за ограничаване на реклами*, които са фокусирани върху поверителността;

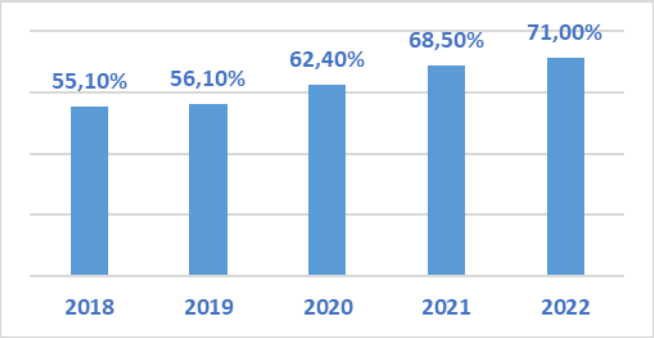
– *Непрекъснато наблюдение на работата на компютърната система* – като скорост на обработване на данните, натовареност на процесора, захранване на устройството.

4. Кибер хигиена. Независимо от типа на заплаха, на първо място е добре потребителят да има умения за защита на своите лични данни. Важно е да има практически познания за това как неговите действия и файлове могат да бъдат защитени – както от страна на местата, които посещава при сърфиране в Интернет, така и реалната среда извън глобалната мрежа – работно място, частни и държавни институции.

4.1. Мотиви за необходимостта от мерки за защита във фирми и организации

Някои от най-големите кибератаки в световен мащаб са от рансъмуер. Популярни такива вируси са CryptoLocker, CryptoWall, Petya, NotPetya и WannaCry, който поразява над 200 хил. компютри в над 150 страни през 2017 година [4]. Този вид кибер заплаха може да бъде криптираща данните или не, може да засегне цялата система или само определени файлове, като целта е

изнудване на засегнатите. Жертвите биват подложени на изнудване от страна на атакуващите, за да получат отново достъп до данните си.



Фиг. 3. Процент на организациите, засегнати от ransomware [9]

Процентът на компаниите, станали жертва на ransomware през последната година бележи скок (Фиг. 3.). Този показател се е увеличил от 55,1% в доклада за защита от киберзаплахи на Netwrix от 2018 г. до 62,4% през 2020 г., до 68,5% за миналата година и до 71% през 2022 [9].

4.2. Насоки за предпазване от рансъмуер

Могат да бъдат обобщени следните мерки за избягване на опасността от *ransomware*:

– Инсталиране на надеждна *антивирусна програма*, която е лицензирана и разполага с механизъм за откриване на подобен тип злонамерен код.

– *Сканиране на всички външни носители* на данни, които се ползват– USB флаш памети, карти памет, компакт дискове и др. – с подходящ антивирусен софтуер

– *Актуални версии на операционната система*, както и на инсталираните приложения. Обновяването на операционната система и приложното програмно осигуряване често е с цел „закърпване“ на пропуски в сигурността, както и отстраняване на установени проблеми [4].

– Периодичното *създаване на резервно копие* (back-up) на най-важните файлове върху външен носител – преносим твърд диск, който не е постоянно свързан или флаш памет. В последните години облачните услуги, които са отлична алтернатива са популярни, като все пак не е препоръчително използването им за запис на строго конфиденциална информация. Практиката показва, че компакт дисковете и DVD дисковете са едни от най-надеждните носители на данни, що се отнася до създаване на периодични резервни копия. Записаните данни на диск (CD или DVD, без опция за повторен запис) не могат да бъдат неволно изтрити, модифицирани, като на практика не могат да бъдат заразени от вируси или друг зловреден код [4].

– Внимание към *имейл кореспонденцията*, особено към такава с прикачени файлове или линкове. Да не се отварят прикачени файлове от непознати податели, като се проверяват имейл адресите, дори и да изглеждат надеждни.

4.3. Умения за безопасност при ползване на мобилни устройства

Защитата на мобилните устройства също е важна, макар че те обикновено са по-безопасни, особено устройствата, базирани на системата IOS. В наши дни мобилните телефони служат също за пазаруване и разплащане, поради което е препоръчително инсталирането на антивирусно приложение, както и управление на идентификационните данни за кредитна /дебитна карта, потребителски имена и пароли, без те да бъдат запаметявани или записвани. От съществено значение са информираността и уменията, тъй като никоя антивирусна програма не предлага сто процентова защита.

5. Мерки за увеличаване на сигурността във фирми и организации

При управление на данните, от голямо значение е спазването на действащото европейско и национално законодателство [8]. Могат да бъдат обобщени няколко водещи насоки при реализиране на политиката за сигурност от страна на компаниите – както във финансовата, така и в сферата на здравеопазването.

Известен е т. нар. подход за сигурност „*нулево доверие*“ – означава, че предприятията не следва да се доверяват автоматично на всяка информация – не само от външни източници, но също от вътрешни [1]. Преди предоставянето на достъп, от бизнес секторите се очаква да проверят идентификационните данни на всеки, който прави опит за връзка с техните системи.

Заразяването със зловреден софтуер би могло да се избегне посредством *комбинирането на превенция* с надежден *антивирусен софтуер* [8]. По отношение на браузърите, препоръчително е добавянето на приложение за премахване и блокиране на нежелани реклами, съобщения, изскачащи прозорци и ограничаване на зловредния софтуер [1]. Друга практическа насока е да се подхожда с особено внимание към инсталирането на безплатен софтуер – понякога е възможно да бъде придружен от скрит софтуер за пренасочване или хакерски инструменти, с които потребителите се съгласяват по време на инсталация. Подобни инструменти биха изложили на опасност компютърната или операционната система.

Прилага се и подходът на т. нар. *мрежови пръстен*. Предназначен е да ограничи щетите, които хакерите могат да нанесат, дори ако могат да влязат в мрежата, тъй като те ще останат затворени в рамките на този пръстен. Осигуряването на обучен IT персонал, който е в крак със съвременните заплахи и начините за справяне с тях също е значим водещ елемент в политиката за киберсигурност. От особена важност е фирмите да не използват стари версии на операционни системи, както и такива, които не се актуализират – в съответствие с актуалните заплахи.

Полезна мярка от политиката за превенция на кибер заплахи е *регулярното провеждане на тестове за защитеност*, чиято основна цел е симулиране на кибер атаки. Те следва да се извършват поне два пъти годишно [8]. Подобряването на кибер хигиената е насочено към предотвратяването на катастрофални атаки от зловреден софтуер и нарушения на сигурността на данните.

Значима полза за ръководителите на фирми и ведомства е да организират периодично обучения на служителите относно безопасното използване на мрежовите услуги. Създаването на определен вид „интернет култура“ е най-добрата превенция срещу загубата на данни, резултат от вируси и друг злонамерен софтуер [4].

ЗАКЛЮЧЕНИЕ И БЪДЕЩА РАБОТА

С развитието на социално-икономическия свят, кибер заплахите се видоизменят и придобиват нов облик. Затова гражданите и бизнесът трябва да предприемат необходимите мерки, за да гарантират както защитата на личните данни, така и поверителността на бизнес информацията. На базата на проучването са обобщени мерки за повишаване на културата за противодействие срещу кибер заплахите – не само на работното място, а също и в личното кибер пространство.

ЛИТЕРАТУРА

[1.] **Akhtar, S. et al.** 2021. “Cyber Security Solutions for Businesses in Financial Services: Challenges, Opportunities, and the Way Forward.” *International Journal of Business Intelligence Research (IJBIR)*, vol. 12, no. 1, pp. 82–97. http://doi.org/10.4018/IJBIR.20210101.oa5.

[2.] **Cornish, P. (ed.).** 2021. *The Oxford Handbook of Cyber Security*. Oxford, UK: Oxford University Press.

[3.] https://nsi.bg/bg/content/2831/лица-които-са-купували-стоки-и-услуги-по-интернет-за-лични-цели-през-последните-12-месеца

[4.] https://pcguide.bg/kakvo-e-ransomware-i-kak-da-se-predpazim/

[5.] https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Dyre_Wolf_MSS_Threat_Report.pdf

[6.] https://purplesec.us/resources/cyber-security-statistics/

https://www.interpol.int/Crimes/Cybercrime/Cryptojacking

https://www.netlaw.bg/bg/a/zashhitete-kibersigurnostta-na-vasata-kompaniya

https://www.netwrix.com/2022_cyberthreat_defense_report.html

https://www.oxfordlearnersdictionaries.com/definition/english/cyberattack

ИНФОРМАЦИЯ ЗА АВТОРИТЕ

Антоанета Цветанова – студент спец. „Компютърни науки“, ФМИ, Великотърновски университет „Св. св. Кирил и Методий“, e-mail: S1909010521@sd.uni-vt.bg

Милена Стефанова – главен асистент, доктор, Факултет „Математика и информатика“, Великотърновски университет „Св. св. Кирил и Методий“, e-mail: m.stefanova@ts.uni-vt.bg

ABOUT THE AUTHORS

Antoaneta Tsvetanova – student in Computer Science, Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, e-mail: S1909010521@sd.uni-vt.bg

Milena Stefanova – Senior Lecturer, PhD, Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, e-mail: m.stefanova@ts.uni-vt.bg