НАРАСТВАЩАТА ЗАПЛАХА ОТ КИБЕРАТАКИ СРЕЩУ НАУЧНИЯ СЕКТОР

Димитър Димитров[1], Евгени Андреев[2]

[1]Висше военноморско училище „Никола Вапцаров“
e-mail: dimitar.infosec@gmail.com; e.andreev@naval-acad.bg

Ключови думи: *Кибератаки, киберсигурността, научния сектор*

Резюме: *В статията се разглежда опасността от кибератаки над различни институции на научния сектор. Представени са главните видове атаки срещу институциите и какви са крайните цели на тези атаки. Направен е преглед на някои от най-сериозните кибератаки в този сектор и са представени основните проблеми и пропуски, които водят до пробивите в самите системи. Подчертава се значението на необходимостта от проактивни мерки, свързани с киберсигурността в научния сектор.*

THE GROWING THREAT OF CYBER ATTACKS AGAINST THE SCIENTIFIC SECTOR

Dimitar Dimitrov[1], Evgeni Andreev[1]

[1]Nikola Vaptsarov Naval Academy
e-mail: dimitar.infosec@gmail.com; e.andreev@naval-acad.bg

Keywords: *Cyber attacks, Cybersecurity, Scientific sector*

Abstract: *The article discusses the threat of cyber attacks on various institutions of the scientific sector. The main types of attacks on institutions are presented and what are the ultimate goals of these attacks. Some of the most serious cyber attacks in this sector are reviewed and the main problems and gaps that lead to the breaches in the systems themselves are presented. The importance of the need for proactive cyber security measures in the scientific sector is highlighted.*

Въведение

Събирането на разузнавателна информация, свързана с научния сектор на противника, е практика, която датира от хилядолетия. Този процес предлага ценна информация за нивото на напредък, постигнато от противниците или конкурентите. Научният сектор обхваща широк спектър от академични институции, лаборатории и хора, занимаващи се с научни изследвания и създаване на наука. Независимо от тяхната принадлежност, тяхната интелектуална собственост, по-специално патентите и научните изследвания, оказва значително влияние върху глобалния пейзаж на развитие на нациите. Когато една нация изостава в научните постижения и не разполага с капацитет да постигне сравними резултати, тя прибягва до неконвенционални методи, включително индустриален шпионаж и атаки от тип "вътрешен човек". Макар че тези стратегии дават резултати, като са известни не малко случая на успешна кражба на патенти и научни разработки, те са свързани със значителни рискове. Агентите, участващи в тези операции, са постоянно изложени на опасност и най-малката грешка може да доведе до тяхното разкриване. Въпреки това ситуацията се промени с дигитализирането на научния сектор. Дигитализацията на научния сектор безспорно носи множество ползи, като например по-добра свързаност, по-лесен достъп до информация и подобрен обмен на идеи. От друга страна, тя също така благоприятства кражбата на научни документи и компрометирането на цели лаборатории и институции. Свързването на различните компоненти на научната общност в мрежа е лесен процес, но защитата на тези компоненти изисква време и специфични

компетенции. Дори когато мерките за сигурност са проектирани с мисъл за защита, неправилната конфигурация и пропускането на критични стъпки за сигурност могат да направят тези мрежи уязвими. Пробивите в сигурността често се случват, когато злонамерените хакери успешно се възползват от тези уязвимости.

Атаките, насочени към академичния сектор, могат да бъдат категоризирани като разузнавателни атаки, които оценяват противника, нападателни атаки, насочени към кражба на данни, и разрушителни атаки. В съвременните военни доктрини кибершпионажът играе ключова роля по време на фазата на разузнаване, която често се изпълнява без официална военна офанзива. Освен от грешките в конфигурацията често се възползват и от липсата на киберхигиена в изследователските институти и академиите. Тенденцията за нападателни атаки за извличане на данни се засилва, особено в секторите на здравеопазването и военните иновации. Тази тенденция е обусловена от факта, че някои държави нямат капацитет да развият необходимата наука и им е по-лесно да я откраднат. Целите на тези атаки се простират отвъд правата на интелектуална собственост и патентите, те обхващат и събраните данни, като например ДНК информацията, съхранявана от компании като 23andMe [1]. В крайния случай офанзивните атаки с разрушителни намерения целят да направят дадена система неизползваема. Такива атаки могат да включват криптиране на данни и изнудване за откуп или унищожаване на конкретната система. Методите, използвани при тези атаки, често са сложни и трудни за изпълнение, като изискват значителни ресурси. Само няколко хакерски синдиката разполагат със средствата за осъществяване на такива атаки срещу научни институции. Останалите участници в заплахата, които разполагат с тази способност, са държавно спонсорирани хакерски групи (APTs). За разлика от типичните рансъмуер атаки, които засягат конкретен сегмент от системата, спонсорираните от държавата хакерски групи проникват в цялата система и я правят неработоспособна. Техните операции могат да продължат месеци преди началото на офанзивната фаза, като в крайна сметка водят до това, че системата е или криптирана, или невъзстановима.

Грешки в процеса на конфигуриране. JCA на CISA и NSA в контекста на MITRE ATT&CK.

В координирани усилия за намаляване на рисковете, свързани с кибератаки, експлоатиращи уязвимостите на неправилно конфигурирани системи, агенции от Алианса "Пет очи" си сътрудничиха при публикуването на нова Съвместна препоръка за киберсигурност (Joint Cybersecurity Advisory) [2]. Специалисти в сферата на redteaming и blueteaming операциите, част от Агенцията за национална сигурност (NSA) и Агенция за киберсигурност и сигурност на инфраструктурата (CISA), анализираха и представиха десетте най-често използвани слабости и пропуски, открити в процесите на конфигуриране на различни системи. Обърнато е внимание върху проблемите на:

1. Конфигурирането по подразбиране на софтуер и приложения

Много от наличните програми и приложения са от типа off-the-shelf (COTS). Те се предлагат с предварително конфигурирани пароли, зададени от производителя, предимно с цел тестване преди внедряване. Критичният проблем възниква, когато тези пароли по подразбиране и свързаните с тях акаунти останат непроменени след интегрирането им в системата. Този пропуск представлява значителен риск за сигурността, който може да доведе до редица заплахи, описани в рамката MITRE ATT&CK [3, 4], включително T1078.001, T1589.001, T1098, T1133, T1072 и T1078.002. Основната опасност тук е, че запазването на пароли по подразбиране и административни данни в системата създава уязвимости, които отварят вратата за неоторизиран достъп. Злонамерените хакери могат да се възползват от тези пропуски в сигурността, за да влязат в различни сегменти на вътрешната мрежа, което в крайна сметка им позволява да извършват различни действия и да установят постоянно присъствие.

Освен проблема с паролите и администраторските акаунти, друг често срещан проблем се крие в разрешенията за услуги и настройките на конфигурацията по подразбиране в системите, системните логове и приложенията. Някои услуги могат да имат слаб контрол на достъпа или да се предлагат с несигурни конфигурации по подразбиране. Дори тези услуги да не са първоначално разрешени, ако потребителите или администраторите решат да ги активират, те стават потенциални цели за експлоатация. В рамките на MITRE ATT&CK тези проблеми са категоризирани в T1649, T1557, T1558.001, T1557.001 и T1110.002. Основната опасност е, че незащитените настройки и услуги по подразбиране могат да бъдат използвани от злонамерени участници, за да компрометират сигурността на мрежата, да получат неоторизиран достъп и потенциално да увеличат привилегиите си в рамките на организацията.

2. Неправилно разпределение на привилегиите на потребителите и администраторите

Администраторите на системата или мрежата често задават множество роли на отделни потребителски акаунти, като им предоставят достъп до различни устройства и услуги в мрежата на организацията. Въпреки че този подход цели да улесни управлението на потребителите, той несъзнателно създава значителен риск за сигурността. В такива ситуации, ако злонамерен участник в заплахата компрометира един от тези многофункционални акаунти, той може да действа като канал за бързо странично движение в цялата мрежа. Така същевременно може и да избегне методите за откриване на странично движение и повишаване на привилегиите, използвани при фазата на добиване на контрол, част от Cyber kill chain [5]. Типични грешни конфигурации при разпределение на привилегиите на потребителите и администраторите са Прекомерни привилегии на акаунта, Повишени права на акаунта за услуги и Неоснователно използване на повишени акаунти.

Привилегиите на акаунта контролират достъпа на потребителя до ресурсите на хоста или приложението, като осигуряват ограничен достъп до чувствителни данни и налагат сигурност с най-малки привилегии. Когато са прекалено разрешаващи, те водят до проблеми със сигурността, като увеличават излагането на риск и разширяват повърхността на атаките. С разрастването на организациите промените в управлението на акаунтите, персонала и изискванията за достъп често водят до прекомерен достъп. Анализирайки групите в Active Directory (T1078), злонамерените участници идентифицират акаунти с ненужни привилегии, като потенциално предоставят неоторизиран достъп в рамките на домейна. Приложенията използват служебни акаунти с повишени привилегии и компрометирането им предоставя на нападателите еквивалентен достъп. Това може да доведе до неоторизиран контрол върху критични системи, което прави служебните акаунти привлекателни цели. Те могат да се използват за kerberoasting [6] (T1558.003). ИТ персоналът често използва повишени администраторски акаунти за рутинни задачи, което увеличава тяхната уязвимост. Злонамерените участници търсят валидни идентификационни данни за домейна след достъп до мрежата, като ги използват за проучване на домейна и се насочват към повишените акаунти, улеснявайки ескалацията на домейна и разширявайки повърхността на атаката.

3. Недостатъчно наблюдение на вътрешната мрежа

Неоптимална практика за конфигуриране на хост и мрежови сензори за събиране на трафик и регистриране на крайни хостове е сериозен проблем пред много организации. Тези неадекватно настроени конфигурации създават притеснителен пропуск в сигурността, като потенциално позволяват компрометирането от страна на злонамерения хакер да остане незабелязано. TA008 по рамката MITRE ATT&CK.

4. Липса на мрежова сегментация

Сегментирането на мрежата е основна практика в областта на сигурността, насочена към създаване на отделни дялове за сигурност в мрежовата инфраструктура на организацията. Когато мрежовото сегментиране не е ефективно приложено, то води до липса на добре дефинирани граници на сигурността, които да разграничават потребителските, производствените и критичните системни мрежи. На практика този недостатък на мрежовото сегментиране предоставя на неоторизирани лица, които успешно са компрометирали мрежов ресурс, свободата да се придвижват сравнително лесно през множество системи, срещайки минимални препятствия по пътя си. Липсата на правилно сегментиране на мрежата повишава уязвимостта на организацията, създавайки среда, в която потенциалните атаки с цел получаване на откуп и тактиките след експлоатиране могат да бъдат осъществени с по-голям успех. Без ясно разграничаване на зоните за сигурност злонамерените участници могат да се движат по-свободно в мрежата, което увеличава вероятността от сериозни пробиви и компрометиране на данни. T1199 по рамката MITRE ATT&CK.

5. Слабо управление на актуализациите и KEV

Системните сегменти, услугите и приложенията често се обновяват и получават пачове с цел отстраняване на уязвимости в сигурността. Въпреки това често срещана практика е организациите да отменят тези актуализации, като по този начин неволно създават възможности за потенциалните нападатели да открият отворени зони за достъп и да се възползват от критични слабости. Пренебрегването на прилагането на най-новите пачове излага системите на потенциална хакерска атака чрез публично достъпни експлойти. Такива

уязвимости често са лесно откриваеми чрез методи и инструменти за сканиране на уязвимости и изследване на отворени източници. Допускането на значителни уязвимости в производствените системи, без да се въведат необходимите пачове, значително разширява повърхността на атака, като по този начин повишава риска от успешна кибератака. Освен това възниква и друг проблем, когато организациите продължават да използват софтуер или хардуер, който вече не се поддържа от производителя. В такива случаи липсата на актуални актуализации на сигурността и пачове прави тези системи силно уязвими за експлоатация. Злонамерени участници могат лесно да се възползват от уязвимостите в тези неподдържани системи, за да получат неоторизиран достъп, да компрометират чувствителни данни и да нарушат оперативните дейности. T1595.002, T1592, T1190 и T1220 по рамката MITRE ATT&CK.

6. Избягване на контрола на достъпа до системата

Неправилно конфигурираният контрол на достъпа до системата може да изложи на опасност уязвимости, които злонамерени хакери могат да използват, използвайки техники като pass-the-hash[7] и kerberoasting. Тези методи позволяват на злонамерения хакер да се представи за определен потребител, като използва събраните негови хешове. Възможно е да се увеличат привилегиите, без да се задейства откриването им от системите за киберсигурност. T1550.002 по рамката MITRE ATT&CK.

7. Слаби или неправилно конфигурирани методи за многофакторно удостоверяване

Неправилните конфигурации на изискванията за многофакторно удостоверяване (MFA) могат да доведат до ситуации, при които хешовете на паролите за потребителски акаунти остават статични с течение на времето. Дори ако действителната парола вече не се използва постоянният хеш на паролата за акаунта може по невнимание да послужи като алтернативно удостоверение за неоторизирано удостоверяване. Дори ако организацията е приела MFA за повишаване на сигурността, остатъчният хеш на паролата може да се превърне в потенциално слабо място, ако не се управлява или актуализира правилно. TA008 по рамката MITRE ATT&CK.

8. Неефективни ACL на мрежови ресурси и услуги

Споделените данни и архиви са силно уязвими към киберзаплахи. Злонамерените хакери често се насочват към тези ресурси. Един от често срещаните начини за това е, когато мрежовите администратори е конфигурирал неправилно списъците за контрол на достъпа (ACL). Това може да позволи на неоторизирани потребители да получат достъп до чувствителни или администраторски данни, съхранявани в споделените дискове. При експлоатиране на слабо конфигурирани ACL злонамерените хакери получават достъп до споделени дискове и папки. От там те могат да събират и изнасят чувствителни данни. Тези данни могат да бъдат използвани за различни злонамерени цели, включително за изнудване на организацията или за събиране на разузнавателна информация за планиране на по-нататъшни мрежови прониквания. Екипите за оценка на сигурността често откриват чувствителна информация в тези споделени мрежови файлове, която може да подпомогне последващи злонамерени действия. T1135, T1083,TA0010,T1018,T1046 и T1552 по рамката MITRE ATT&CK.

9. Лоша киберхигиена

Пренебрегването на подходящи практики за киберсигурност може да доведе до тежки последици за организацията. Неспазването на тези основни правила може да доведе до уязвимости като лесно разбиване на пароли, ставане на жертва на фишинг и атаки със социален инженеринг, както и загуба или неправилно разполагане на важни данни. T1110.002, T1555 и T1552.001 по рамката MITRE ATT&CK.

10. Неограничено изпълнение на код

Ако на програмите им е дадена неограничени права за изпълнение, злонамерените хакери могат да използват това за да изпълнят злонамерен код в системата. Както екипите за оценка, така и злонамерените участници често използват неограничено изпълнение на код, включващ изпълними файлове, библиотеки за динамични връзки (DLL), HTML приложения и макроси. е използват тези методи, за да установят първоначален достъп, да поддържат устойчивост и да улеснят страничното движение в мрежата. Освен това тези участници могат да зареждат уязвими драйвери и след това да използват известните уязвимости на тези драйвери, за да изпълняват код в ядрото, придобивайки най-високо ниво на системни

привилегии и ефективно компрометирайки устройството. Това подчертава изключителната важност на надеждните практики за сигурност и внимателното наблюдение за защита от неограничено изпълнение на код. T1059.005, T1059, T1027.010 и T1068 по рамката MITRE ATT&CK.

Космическия сектор и хакерите

Ролята на космическия сектор в сферата на научните изследвания, промишлените предприятия и военните операции се развива с всяка изминала година по безпрецедентен начин и придобива все по-голямо значение. Този сектор се е превърнал в централна точка за различни заинтересовани страни, включително правителствени организации и частни корпорации. Изключение не правят и злонамерени държавно спонсорирани APT групи.

През август 2023 г. Националният център за контраразузнаване и сигурност (NCSC), който функционира към Службата на директора на националното разузнаване на САЩ, издаде бюлетин [8, 9], в който се посочват данни за дейностите на чуждестранни агенти и злонамерени хакери, насочени към космическия сектор на САЩ. Тези дейности са многоаспектни и пораждат многобройни опасения в областта на сигурността и разузнаването. Основната цел на тези атаки е събирането на разузнавателна информация. Чуждестранните организации активно участват в събирането на високочувствителна информация, свързана с космическия сектор на САЩ и възможностите му. Тази информация включва технически спецификации, възможности на спътниците и уязвимости. Целта е да се изгради подробна и изчерпателна карта на възможностите и потенциалните слабости на американския космически сектор, според NCSC. Тези злонамерени участници съсредоточават усилията си както върху частни, така и върху военни спътници. Като се насочват към широк кръг спътници, те се стремят да идентифицират уязвимостите в различни системи, като по този начин придобиват представа как да използват тези слабости за бъдещи атаки. В допълнение към събирането на разузнавателна информация злонамерените участници организират и разрушителни атаки. Тези атаки имат за цел да нанесат вреди и да нарушат функционирането на спътниковите комуникации и космическите способности на САЩ. Те могат да доведат до влошаване на състоянието на критичната инфраструктура, като потенциално забавят възможностите за реагиране по време на бедствия или други извънредни ситуации. Нападателите използват сателитните мрежи като допълнително стъпало за по-напреднала кибервойна. Чрез проникването в тези мрежи те могат да получат достъп до други цели с висока стойност и да извършват по-сложни кибератаки, което представлява значителна заплаха за сигурността както на националните, така и на международните интереси. Освен това атаките срещу космическия сектор надхвърлят проблемите на сигурността. Ресурсите, предоставяни от спътниковите услуги, са дълбоко обвързани с различни сектори на икономиката. Много системи, приложения и услуги разчитат на точни и непрекъснати спътникови данни, поради което тези атаки нарушават не само националната сигурност, но и по-широката икономическа екосистема.

Освен уязвимостите в сателитния сектор, наземните обсерватории все по-често стават обект на кибератаки, което представлява сериозно предизвикателство за астрономията. Само за десет месеца няколко от най-модерните и ценни обсерватории, използвани от астрономите, станаха жертва на хакерски атаки, които доведоха до сериозни смущения в работата им и повдигнаха въпроси относно естеството и обхвата на тези атаки. През ноември 2022 година обсерваторията ALMA в Чили беше подложена на кибератака [10, 11], което доведе до значително намаляване на научните ѝ дейности. Въпреки че ALMA направи изявление, в което твърди, че заплахата е била овладяна и не са били компрометирани чувствителни данни, някои съществени въпроси остават. В изявлението липсваше подробна информация за стандартите и процедурите, които трябва да се следват в случай на кибератака, което оставя открита възможността чувствителни данни да са изтекли, без да бъдат открити. Тази ситуация напомня на случаите, когато компании като LastPass първоначално омаловажаваха нарушенията, само за да могат хакерите по-късно да публикуват откраднатите данни. Друг пример за наземен компромат се случва през август 2023 година, когато Националната лаборатория за оптични и инфрачервени астрономически изследвания (NOIRLab) става жертва на хакерска атака [12]. Тази атака имаше сериозни последици, като доведе до спиране на работата на телескопите Gemini North в Хавай и Gemini South в Чили. Освен това бяха засегнати и по-малките телескопи, разположени в Cerro Tololo в Чили. За разлика от инцидента с ALMA, операцията по възстановяването на тези обсерватории е продължителен процес, продължаващ няколко седмици, през които телескопите не работят, което води до значителни смущения в научните наблюдения и изследвания.

Тези кибератаки срещу наземни обсерватории не само засягат областта на астрономията, но и повдигат по-широки въпроси относно сигурността на критичната научна

инфраструктура. Те подчертават необходимостта от строги мерки за киберсигурност, прозрачност при докладването на киберинциденти и международно сътрудничество, за да се защити работа, извършвана в тези обсерватории, и да се запази целостта на научните данни и изследвания.

Заключение

В постоянно променящия се пейзаж на киберпространството научният сектор и свързаните с него области се намират в нова реалност, изпълнена с непрестанни предизвикателства. Утопичната концепция за сигурност в цифровата епоха е под постоянна заплаха. Този сектор, чието значение нараства с всяка изминала година, се утвърди като ключов за разнообразни заинтересовани страни, включително правителствени организации и частни корпорации. Но и дори за злонамерените APT групи. За да се защити този ключов домейн, е от съществено значение да се разберат основните проблеми, с които той се сблъсква. Сред най-критичните предизвикателства NSA и CISA са установили неправилно конфигурирани и управлявани системи. Като разгледаме реални случаи на хакерски атаки, които се възползват от тези неправилни конфигурации, можем да проправим пътя за по-сигурна и устойчива мрежа, съобразена с научните занимания. Това налага проактивна позиция, при която се предприемат мерки за укрепване на нашата защита.

В този динамичен кибернетичен пейзаж осигуряването на сигурността на научния сектор не е само въпрос на защита на интелектуалната собственост и данните; става въпрос за запазване на самата същност на прогреса и иновациите в цифровата ера. Тъй като секторът продължава да се развива, значението на укрепването на неговите мерки за киберсигурност не може да бъде надценено. Това е колективна отговорност, която се разпростира върху държавните структури, частните предприятия и общността за киберсигурност като цяло.

Литература:

1. Toulas, B., 23andMe hit with lawsuits after hacker leaks stolen genetics data,https://www.bleepingcomputer.com/news/security/23andme-hit-with-lawsuits-after-hacker-leaks-stolen-genetics-data/
2. Joint Cybersecurity advisory, CISA, NSA., NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations, https://media.defense.gov/2023/Oct/05/2003314578/-1/-1/0/JOINT_CSA_TOP_TEN_MISCONFIGURATIONS_TLP-CLEAR.PDF
3. Trellix, What Is the MITRE ATT&CK Framework?, https://www.trellix.com/security-awareness/cybersecurity/what-is-mitre-attack-framework/
4. MITRE ATT&CK, MITRE ATT&CK, https://attack.mitre.org/
5. SantinelOne, What Is The Cyber Kill Chain? Steps, Examples, & How To Use It, https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/
6. SantinelOne, What Is Kerberoasting Attack?, https://www.sentinelone.com/cybersecurity-101/what-is-kerberoasting-attack/
7. Netwrix, Pass the Hash Attack, https://www.netwrix.com/pass_the_hash_attack_explained.html
8. Director of national intelligence, Safeguarding the US space industry, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL%20FINAL%20Safeguarding%20the%20US%20Space%20Industry%20-%20Digital.pdf
9. Greig, J., FBI, Air Force warn of cyberattacks on space industry by ‘foreign intelligence operations’, https://therecord.media/fbi-warns-of-space-cyberattacks
10. ALMA, ALMA Services Affected by Cyberattack, https://almascience.nrao.edu/news/alma-services-affected-by-cyberattack
11. ESO, ALMA Update on the Recovery from the Cyber-attack, https://www.eso.org/sci/facilities/alma/news/announcements/alma-ann1507121111.html
12. NOIRLab, Cybersecurity incident at NSF’s NOIRLab, https://noirlab.edu/public/announcements/ann23022/