УНИВЕРИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

ФАКУЛТЕТ ПО ИНФОРМАЦИОННИ НАУКИ

М А Г И С Т Ъ Р С К А Т Е З А

На тема:

КИБЕРСИГУРНОСТТА В ПУБЛИЧНАТА АДМИНИСТРАЦИЯ В БЪЛГАРИЯ - СЪСТОЯНИЕ, ЗАПЛАХИ И ПРЕДИЗВИКАТЕЛСТВА

Дипломант: Владимир Димитров Фак. №: 0086-имд	Научен ръководител: проф. д-р Ирена Петева

гр. София, 2018 г.

Р Е З Ю М Е

Владимир Николов Димитров; Киберсигурността в публичната администрация в България - състояние, заплахи и предизвикателства; научен ръководител: проф. д-р Ирена Петева; София; 2018 г.; Факултет по информационни науки; Специалност – Информационни технологии; Университет по библиотекознание и информационни технологии; 63 страници; 7 броя използвани източници, 22 броя снимки.

Целта на магистърската теза е провеждането на опит за обхващане и фиксиране актуалното състоянието на киберсигурността в публичната администрация в страната и региона; отбелязване на най-важните киберзаплахи, въздействащи върху нея; детерминиране на бъдещи предизвикателства в тази сфера; извеждане на политики, методи и похвати за неутрализиране на деструктивните кибервъздействия върху публичната администрация в страната, региона и света. Засегнати са значими компютърно-информационни инциденти, получили гласност в страната и света, като примерен измерител за нивото, състоянието и тенденциите на киберсигурността в публичната администрация. Проведен е частичен анализ на състоянието на важни държавни сайтове и уеб базирани ресурси. Изведени са бъдещи подходи и конкретни практически примери, при чието използване и имплементиране е възможно повишаване киберсигурността на публичната администрация в България и региона.

Ключови думи: киберсигурност, публична администрация, интернет, компютри, информационни технологии, компютърни заплахи, компютърни вируси, хакерски атаки, компютърни престъпления.

С Ъ Д Ъ Р Ж А Н И Е:

УВОД

Дигитализирането на света през последните няколко десетилетия поставя редица важни предизвикателства пред нашия начин на живот и бъдещо развитие. Общуването ни с компютрите и киберсвета започва от ранна детска възраст. Голяма част от децата в детската градина редовно ползват таблети, компютри или мобилни телефони за забавление, обучение или комуникация. Процентът на интернет потребителите пазаруващи онлайн постоянно расте и Интернет-на-нещата/IoT започва бавно да се превръща в реалност. Компютрите и контролиращият ги софтуер все повече улесняват живота ни във всички сфери на нашия бит и съществуване. Наред с всички киберулеснения светът е поставен пред невиждани до сега предизвикателства, резултат от мащабната дигитализация. Киберсигурността на този дишащ дигитален свят е крехка, но ограничен брой посветени в спецификата на тези проблеми са наясно с това. Зад забавния и весел образ на интернет пространството, в което общуваме, забавляваме се и пазаруваме виртуално, се прокрадват множество тъмни сенки на злонамерени групи от хакери, политически мотивирани субекти, джихадисти, специализирани правителствени служби и други играчи, чиито възможности, потенциал и намерения са обвити в мистерия.

Благодарение на усърдния и продължителен труд на екип английски криптографи успяли да разкодират част от съобщенията предавани с легендарната германска машина Енигма, Втората световна война е съкратена с няколко години, а броя на жертвите е намален с милиони. Специализирани разузнавателни служби на няколко държави са сключили тайни споразумения, по силата на които прихващат и четат милиарди телефонни разговори, имейли, съобщения, снимки, видео материали и други.

Подобни факти радко стават обществено достояние в детайли и на практира разкриват една малка част от сложната и тревожна ситуация, в който се намира кибер пространството в наши дни.

ГЛАВА ЕДНО. Киберсигурността като понятие

Общото понятие сигурност се разглежда, като свойство на дадена система да противодейства на външни или вътрешни деструктивни фактори, които могат да доведат до нейното нежелателно състояние, поведение, срив или неправилна работа. Това важи и за сигурността на компютърно-информационните системи и мрежи. Целта на всяка компютърно-информационна система е доставяне на пълна, достоверна и своевременна информация. Тази информация е уязвима както поради случайни, така и поради злонамерени влияния, което налага да се предприемат редица мерки за нейната защита, контрол и верификация. Кибер сигурността не може и не бива да се възприема като отделен и самостоятелен елемент от сигурността като цяло. Тя е един все по-важен в съвременния живот компонент, играещ понякога решаваща роля в общата картина на надеждното функциониране на цялото общество, и в частност на публичаната администрация.

1.1 Защита на информацията

Под защита на информацията трябва да се разбира постоянно използване на средства, методи и подходи с цел:

1. Защита на конфиденциалността/тайната - да не се допуска разкриването на информация от неоторизирани лица;

2. Защита на цялостността — недопускане на неоторизирана преднамерена или случайна модификация на информацията;

3. Защита на достъпността - да не се допуска срив или отказ от достъп до информация или компютърно-информационния ресурс.

Компютърната и мрежова сигурност е специфично свойство на компютърните системи и мрежи да противодействат на опитите за несанкциониран достъп до обработваната и съхраняваната у тях информация, водещи до деструктивни въздействия и получаване на неточна, лъжлива или заблуждаваща информация.

1.2 Политики за киберсигурност

Компютърно-информационната сигурност се гради върху редица концепции, политики и мерки, както следва:

1. Идентификация - потребителите използват компютърните приложения и ресурси, чрез потребителски идентификатор/обикновено потребителско име/username;

2. Автентификация - доказване на самоличността на потребителя/обикновенно чрез парола;

3. Оторизация - присвояване на права за достъп на всеки потребител /например за запис, четене и/или изпълнение на файл/;

4. Контрол на достъпа - присвояване на права за достъп до мрежови ресурси и предпазване на ресурсите, чрез ограничен достъп /кой, как, кога и при какви условия има достъп до конкретна дигитална папка, файл или друга информация/;

5. Конфиденционалност - защита на данните, чрез контрол на достъпа и прилагане на криптографски средства, методи и похвати;

6. Цялостност/интегритет на данните – механизъм за откриване на несанкционирана модификация на данните, обикновено при предаване на съобщението;

7. Доказване източника на данните;

8. Управление на отказ или срив в услуги (предимно при DoS и DDoS атаки) — понятието е известно с английската дума mitigating и най-общо обхваща дейности по предотвратяване препълването на лентата на пропускане на канала или блокирането на достъпа, чрез филтриране и ограничаване на заявки, както и други специализирани мерки за защита на информацията — ограничавене на достъп до допълнителни /обикновено банкови/ ресурси;

Уязвимо място е слабост, пропуск или неточност в компютърната информационна система и/или в мерките за нейната сигурност, която може да доведе до компрометиране сигурността на системата или важни части от нея. То е всяка точка на компютърните и комуникационните системи и на системата за тяхната защита, където те са слабо защитени срещу атаки, свързани с тяхната сигурност. Уязвимите места в една система зависят от конкретната й реализация. Заплахата е процес, явление, човек, обект или друго събитие, които могат да предизвикат вреда на компютърните системи, мрежи и ресурси.

1.3 Видове кибер заплахи към публичната администрация

Примери за заплахи са използване на общодостъпен/известен способ за достъп/exploit до системата с цел извършване на неправомерни действия; маскиране като оправомощен потребител; използване на служебно положение с цел достъп до информация; физическо разрушаване на системата или нейни компоненти и комуникационни канали; изключване на системата за защита, архивиране или нейни компоненти; изключване на подсистемите, обезпечаващи работата на системата /електроснабдяване, охлаждаща, вентилационна, комуникационна и тн./; промяна на режима на работа на устройства и програми; подкуп и изнудване на персонала или отделни потребители; кражба и несанкционирано копиране на информационни носители; незаконно използване на пароли, пропуски, магнитни карти и тн.; разкриване на криптографски средства за защита на информацията; включване на апаратни средства и програми, позволяващи несанкциониран достъп; заразяване с вируси и друг злонамерен софтуер; неправомерно включване към комуникационните линии с цел подмяна на законен потребител и предаване на лъжлива информация от негово име; неправомерно включване към комуникационните канали с цел прехващане на поверителна информация; неправомерно включване към комуникационните линии с цел анализ на протоколите за връзка и последващото им имитиране за достъп до системата; използване на подслушвателни устройства и устройства за дистанционно видеонаблюдение; прихващане на паразитни електромагнити явления; четене на остатъчна информация от оперативната памет и външни носители на информация; незаконно използване на терминали и компютри оставени без надзор и други.

Според източника заплахите могат да бъдат външни и вътрешни. Външни са дейността на разузнавателни и специални служби, различни политически, икономически и други структури, насочени срещу интересите на организацията, и най-често престъпни действия на отделни групи и лица. Вътрешни са нарушаване на правилата за събиране, обработка и предаване на информацията,

незаконна дейност на групировки и лица за прикриване на закононарушения и нанасяне на вреди на интересите на физически и юридически лица на базата на тази информация.

Визираните заплахи обикновено се проявяват при провеждането на кибер атака.

Атаката е целенасочено действие на злонамерен нарушител, състоящо се в изследване и използване на слаби страни с цел пробив в сигурността на информационна система.

Формите на организиране на атаките са разнообразни, но като цяло се включват в една от следните категории:

- отдалечено или локално проникване в компютърна система или мрежа чрез програми, които получават неоторизиран достъп до друг компютър през интернет или друга мрежа;

- отдалечено блокиране на компютърна система или мрежа чрез програми, които през интернет блокират работата на отдалечен компютър или на отделна негова програма;

- чрез мрежови или други скенери - програми, които събират информация за мрежата за да определят кои от компютрите и програмите работещи на тях, са потенциално уязвими за атаки. Най-използваният мрежови скенер към 2018 г. е Nmap – https://nmap.org/. Използването на мрежови скенери се явява начален/подготвителен етап на атаката, при който се събират данни за атакувания обект или система;

- чрез скенери за слабите страни, наречени exploit scanners или vulnerability scanners - програми, които проверяват големи групи от компютри в търсене на слаби места към конкретен вид атаки. Най-известните и използвани скенери са Acunetix Web Vulnerability Scanner - https://www.acunetix.com/ и Nessus – hhttps://www.tenable.com/products/nessus/nessus-professional. В голяма част от функционалността на тези скенери е включена възможността не само за налучкване/откриване, но и използване на уязвимост и последващ нерегламентиран достъп до компютърно-информационната система;

- чрез разбивачки/bruteforce на пароли - програми, които налучкват пароли, чрез множество опити за вписване с потребителски имена по подразбиране и пароли от предварително зададен списък;

- чрез мрежови анализатори/sniffers - програми, прослушващи мрежови трафик, с възможност за автоматично отделяне на имена на потребители, пароли, номера на кредитни карти и друга специфична информация от общия трафик;

- модификация на предаваните данни или подмяна на информацията – подобен вид атаки се извършват най-вече чрез специализирани софутерни приложения /като прогарамата Cain&Abel/ в условията на Човек-по-средата/Man-in-the-middle атаки;

- подмяна на доверен с лъжлив обект – типичен пример за подобна атака е подмяната на линка за изтегляне на най-известната в света линукс дистрибуция Линукс Минт на 20 февруари 2016. При инцидента, неизвестен извършител е осъществил нерегламентиран достъп до интерент сайта на Линукс Минт на адрес linuxmint.com, като е публикувана препратка за сваляне на заразен инсталационен ISO файл с новата версия на операционната система към български интернет протокол адрес 5.104.175.212. Линукс Минт е най-известната и използвана в света дистрибуция от крайни домашни потребители.

Форма на атака срещу сигурността на системата е и социално инженерство - получаването на несанкциониран достъп до информация по друг начин, без разбиване на програмното обезпечаване. Целта е да се надхитрят хората, за да се получат паролите за достъп до системата или друга информация, помагаща да се наруши сигурността й. Основният използван принцип е — попитай правилно и правилния човек и ще ти се отговори, поискай правилно и правилния човек и ще ти се даде.

Киберсигурността на публичаната администрация е възможно да бъде разглеждана и като състояние, при което са налични базова информационна сигурност и кибер хигиена, с тенденция за постигане на стособност за резистентност на кибер и хибридни заплахи от различен калибър. Тъй като е невъзможно постигането на сто процентова сигурност и тя на практика не съществува, е необходимо провеждането на задълбочен анализ на риска и набелязване на точно необходимите мерки за обезпечаване на стабилно ниво на резистентност от кибер инциденти на публичната администрация. Пробиви, изтичане на служебна информация, унищожени бази данни, обезобразени

публични сайтове и други подобни компютърно-информационни инциденти е имало и ще има. Набелязването на точни, конкретни и навременни мерки, както и въвеждането на специфични методи, политики и планове за реакция, са категоричен гарант за постигане на надеждно ниво на киберсигурност на публичната администрация в страната, отговарящо на съвременните световни тенденции.

ГЛАВА ВТОРА. Атаки към компютърно-информационните ресурси на публичната администрация

Както беше споменато по-горе съществуват различни класификации на заплахите, в зависимост от техния източник, времетраене, сложност, размер на нанесените щети, степен на въздействие и други.

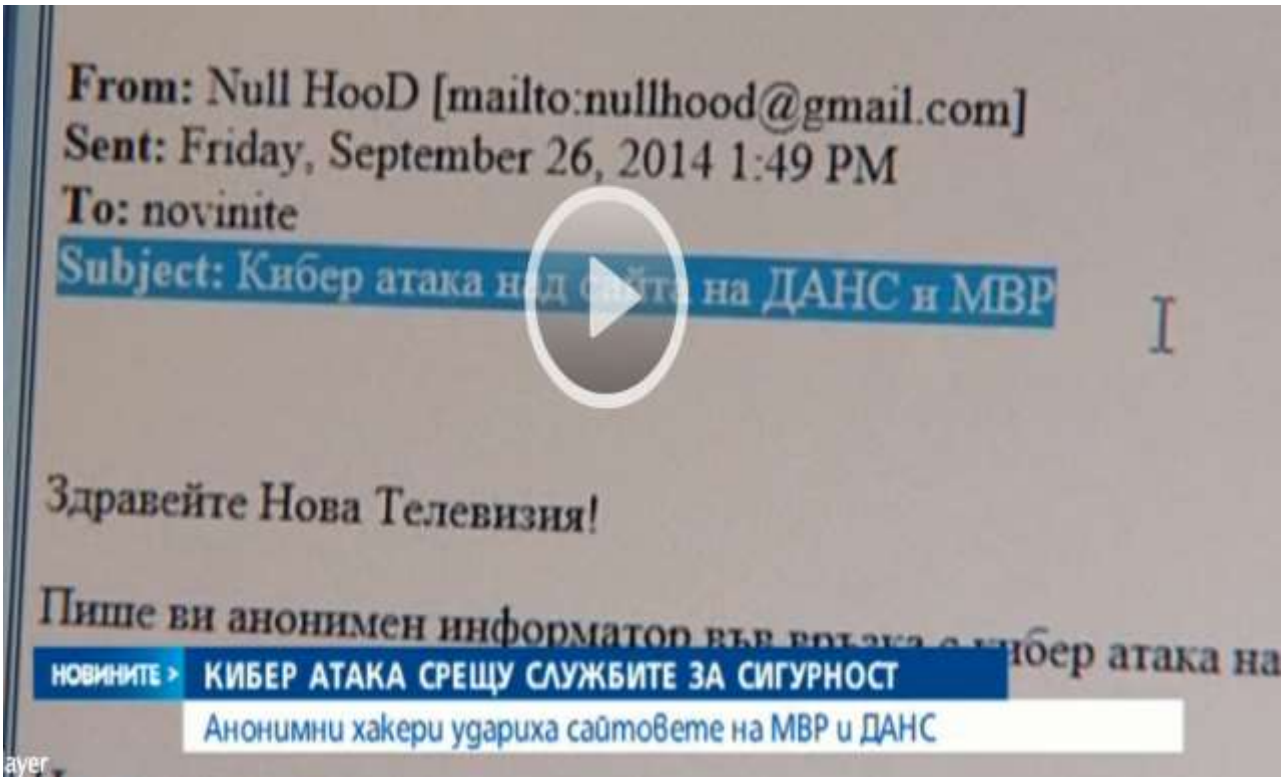
Въпреки това могат да бъдат изведени следните основни похвати, използвани от компютърни престъпници и злонамерени лица през последните години:

2.1 Атаки за отказ от услуга/DDoS

Изключително използван похват за нанасяне на поражения върху компютърно-информационни ресурси през последните години. Принципа на действие е опростен и изключително ефикасен. Към онлайн ресурс се изпращат хиляди/милиони/милиарди «нелегитимни» заявки, които изчерпват мрежовите и хардуерните му ресурси, като за времето на атаката същия не може да бъде използван по предназначение от целевите си потребители. Обекти на подобни атака са предимно банкови сайтове, сървъри за онлайн компютърни игри, онлайн казина, мрежи на конкурентна фирма, правителствен сайт и тн. Едни от най-мащабните атаки от този вид са атаката срещу Spamhaus през 2013 г., атаката срещу GitHub през март 2015 г., атака към най-големия френски хостинг доставчик OVH, CloudFlare и други сайтове за онлайн игри от февруари 2014 г.

Ресурсите за осъществяването на подобен вид атаки са използването на бот-нет мрежи, SYN и ICMP Flood атаки, Application-level flood, SMURF атаки, NTP Reflection атаки и тн. През последните три години се утвърждава нов по своята характеристика вид атака за отказ от услугата, получил названието Extortion DDoS/Атака за изнудване. Най-яркият представител на този вид атака в средите на кибепрестъпниците през 2016 г. се явява хакерската групировка DD4BC/ДдосЗаБиткойни/. Нейни представители изпращат до атакуваната фирма, банка или друга мишена, мейл съдържащ кратко представяне на хакерската групировка, нейни минали операции и пострадали, Биткой адрес за превод и искане за превеждане на 3 Биткойна, за да не предприемат атака към съответния сайт/ресурс. Междувременно се предприема кратка/демонстративна атака за отказ от услугата. Един от най-използваите видове DDoS от тази хакерска групировка е наличието на десетки хиляди уязвими интернет сайтове, създадени с безплатната платформа WordPress, които при инсталация и по подразбиране притежават XML-RPC PingBack уязвимост в себе си. Най-общо XML-RPC PingBack уязвимостта е свързана с посещаването и откопирането на препратка/link в самата WordPress платформа. Когато сайт, създаден с WordPress установи, че в неговата структура е наличен или «прясно» публикуван линк към друг сайт — той ще го посети и изтегли съдържанието зад този линк. Чрез използването на специализирани скенери за наличието на тази уязвимост е възможно придобиването на актуална листа със сайтове, които притежават недоконфигурирана PingBack опция. В последствие, към тези сайтове се изпраща специфична XML-RPC PingBack заявка, указваща им да посетят многократно атакувания ресурс.

По подобен начин в България през септември 2014 г. интернет сайтовете на Министерството на вътрешните работи и Държавна агенция «Национална сигурност» бяха атакувани и недостъпни за няколко десетки часа, като отговорност за хакерската атака е поета от анонимен български хакер с псевдоним nullhood.



Методите за защита от DDoS атаки са ограничен брой действия, обикновенно свеждащи се до помощ от локалния доставчик на интернет услуги за организацията, с цел ограничаване на заявките по геолокационен принцип, забраняване на определени протоколи към атакувания сървър на ниво рутери на доставчика, мигриране на друга критична инфраструктура в отделна мрежа, доконфигуриране на атакуваните програмни ресурси, пренасочване на целия трафик и отделяне на «мръсния» такъв, при специализиран доставчик на анти-DDoS решения. Световен лидер в смегчаването/mitigation на подобни атаки са американските корпорации CloudFlare, Incapsula, Amazon AWS, Akamai, Level3 и други. В регионален за България мащаб множество родни IT организации използват решения предлагани от румънската фирма Voxility или хардуерните продуктите на израелската фирма Radware или американската Fortinet.

2.2 Заразяване с компютърни вируси

Най-общо, от практическа гледна точка, заразяването с компютърни вируси се осъществява по следните четири примерни сценария:

2.2.1 Криптолокър

Този вид зловреден компютърен код обикновено се доставя до афектираната компютърна конфигурация чрез прикачен файл към фишинг имейл. Чрез вградени в операционната система Windows инструменти се извършва бързо и надеждно криптиране на наличните потребителски данни — офис документи, снимки, видео, бази данни и други. На потребителя се извежда съобщение с искане за откуп в рамките на около 500 евро, за това подобни вируси са известни и под името Ransomeware.

Едни от най-ярките представители на този зловреден код са ИскаПлаче/WannaCry от месец май 2017, Петя/НеПетя от месец юни и Лошия Заек/BadRabbit от откомври. За изготвянето на тези зловредни програми са използвани „тайни“ хакерски инструменти, разработени от Националната агенция за сигурност на САЩ, които през лятото на 2016 г. са откраднати и частично разпространени от неизвестна хакерска групировка “БрокеритеВСянка” - вероятно свързани с руски разузнавателни структури.

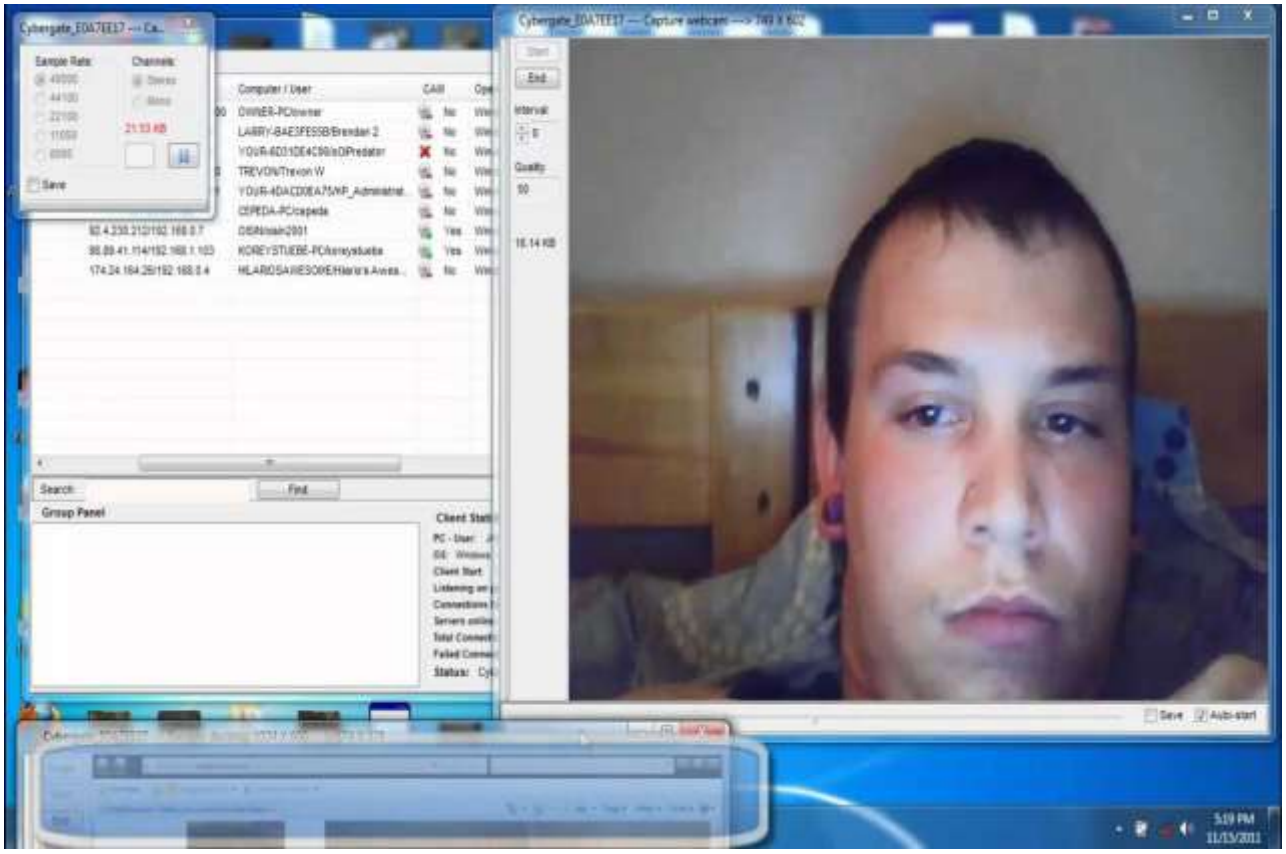
Поради високото ниво на латентност при този вид престъпления /пострадалите организации, фирми и лица не докладват, че са жертва на крипто вирус/ в България официално са известни само няколко стотици подобни случая. По неофициални данни от представители на големи фирми, публикации в социални мрежи и становища на лица с познания в тази сфера, е възможно да се заключи, че за 2017 година от крипто вируси в страната са пострадали наколко десетки хиляди крайни интернет потребители.

2.2.2 RAT

RAT/Remote Administration Tool е наименованието на група «специализиран» софтуер с неизвестен създател, който най-общо притежава функционалност по: създаване/генериране на файл /инсталационен, картинка, видео, документ и тн./, който се използва за заразяване на компютърна

конфигурация; при стартиране на заразата се инициира невидим за обикновенния потребител процес; процеса извършва допълнителни операции за да се «скрие» и изпрати «съобщение до вкъщи» за своята готовност за комуникация; при необходимост се запускат допълнителни процеси, които позволяват отдалечен достъп до файловата структура на атакуваната система, запускане на нейния микрофон, камера, извличане и добавяне на файлове, откопиране на потребителски имена и пароли, промяна на системни настройки, «предпазване» от антивирусно сканиране и тн. RAT-а притежава специфичен интерфейс, подпомагащ гореописаните дейности. Едни от най-известните и използвани RAT програми са Blackshades, DarkComet, CyberGate, NjRAT, XtremeRAT и други. Например «прохождащ» хакер се снабдява с един от изброените RAT-ове, генерира зловреден файл, изпраща го като прикачен файл в мейл, чат съобщение до познат или го използва за да заради компютърна конфигурация до която има физически достъп. В последствие е възможно неправомерно придобиване на почти всякаква информация от атакуваната система — въвеждани потребителски имена и пароли в социални мрежи, пощенски услуги и най-вече — в банкови сайтове. Голяма част от така наречените прохождащи хакери използват подобни инструменти от любопитство, за да «хакнат» съученик или познат, или за получаване на незаконни облаги. Друг вариант е генерирането на заразен файл и последващото му публикуване в торент тракер, като «хак/крак» за популярна игра, софтуер, материали с порнографско съдържание, музика, филми или други подобни.

Част от интерфейса на CyberGate RAT:



2.2.3 Ботнет

Заразяването с компютърни вируси е широко понятие, което включва в себе си редица разнопосочни действия и усилия — намиране на пролука в операционна система, софтуер или друго приложение; намиране на подходящия начин за използването на тази пролука, доставката и активирането на вируса до мишената; последащи мероприятия по «скрита» комуникация със заразата и редица други. В световен мащаб най-голямата част от гореописаните дейности по заразяване с компютърни вируси е възможна и се провежда от стройно организирани престъпни групи от хакери. Тази дейност приритетно се извършва в «защитени» хакерски форуми или чрез криптирани канали за комуникация /най-вече в джабър сървъри или ICQ комуникация/. На хакерските

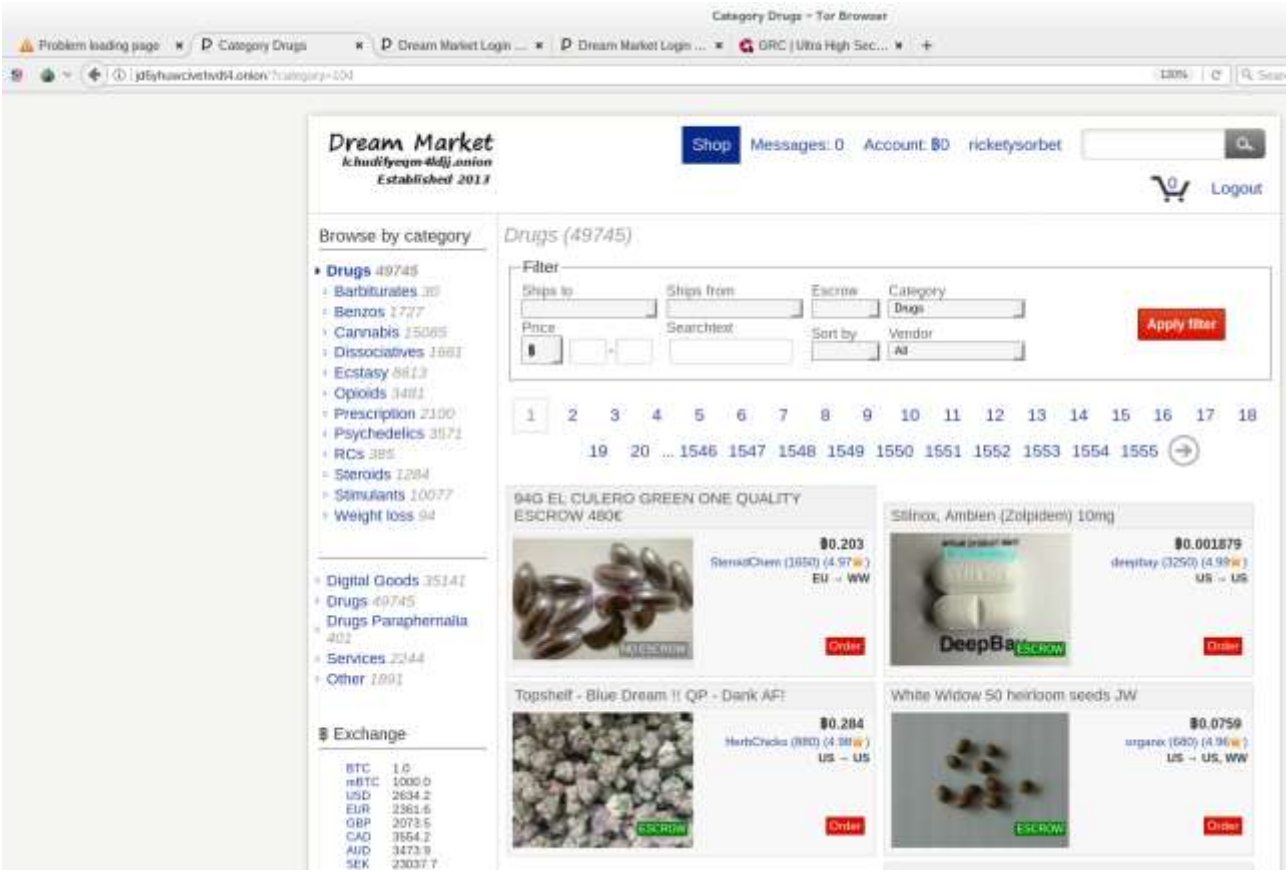
форуми се търгува с: незаконно придобити данни от платежни инструменти /данни от кредитни карти и данни за онлайн банкиране/; мрежи от мулета; бот-нет мрежи или техни части; услуги по изпиране на незаконно придобити парични средства; други съпътстващи дейности.

Двигателят на заразяването с компютърни вируси са пакетите за експлоатиране/exploit pack. Те представляват набор от методи, похвати и пролуки в операционни системи и общоприет софтуер, чието експлоатиране довежда до заразяване на компютърни конфигурации с вируси. Едни от най-известните и използвани пакети за експлоатиране през 2015 г. са BlackholeExploitKit, Nuclear, Sakura, Fiesta и редица други «затворени» и безименни. Една от най-качествените функционалности на пакетите за експлоатиране е тяхната възможност за «принуждаване» на потребителски браузъри да изпълнят определено действие. Хакерска групировка закупува в закрит форум един от изброените пакети и въвежда в експлоатация интернет сайт с видео или снимки. Софтуерната платформа зад сайта използва функционалността на пакета за експлоатиране, като принуждава браузъра на посещаващия да «свали» и активира определен файл-вирус. В последствие се популяризира посещаването на сайта чрез агресивни кампании в социални мрежи с публикации от вида «СКАНДАЛНО! Щракни тук за да видиш новите голи снимки на фолк звездата XXX», публикации с шокиращи актуални новини и други подобни. В резултат на дейността на сайта и експлоатиращия пакет зад него хакерската групировка изгражда бот-нет мрежа с десетки хиляди жертви. В последствие тази бот-нет мрежа се отдава под наем в същия хакерски форум, от който е закупен пакета за експлоатиране. Незаконно придобитите данни на невинните жертви, част от бот-нет мрежата се препродават и в крайна сметка използват за генериране на «мръсни» пари.

Едни от най-известните и посещавани закрити хакерски форуми към 2018 г. са www.exploit.in, www.zloy.bz, www.rescator.cc, www.probiv.cc и други. Част от посочените сайтове са често достъпни със специфичен криптографски

сертификат на определен коменикационен порт, потребителско име и парола предоставени от администратора срещу няколко хиляди евро и след референции от най-малко трима доверени други потребители на сайта.

Голяма и важна част от подобни закрити хакерски форуми са налични в лучената мрежа TOR. Най-известният хакерски форум в мрежата TOR към 2018 г. е с наименование Dream Market и е достъпен на адрес 4fli55dqu7k6p5cz.onion. Dream Market е интернет базирана платформа/магазин за търгуване, с раздели - Дигитални Стоки, Наркотици, Принадлежности за наркотици, Услуги и Други. Над 80 процента от предлаганите за продажба стоки са различни видове наркотични вещества, като най-често се предлагата т.нар. дизайнерска дрога. За изпращане на наркотичните вещества приоритетно се използват пощенски автомати, където не си изисква пряк контакт с пощенски служител.



2.2.4 Кибер армии

Обществена тайна е съществуването на специализирани държавни формирования /киберармии/, чиято основна цел е осъществяването на операции в киберпространството с разузнавателни, контраразузнавателни или други специфични цели. За изпълнението на тези цели се използват кибероръжия нарочно създадени и потребителски донастроени за специфичната цел. Цели на тези операции и киберинструменти обикновенно са други държави, чужди държавни организации, нации, територии или отделни личности.

През месец май 2013 г. бившият служител на Централното разузнавателно управление на САЩ Edward Joseph Snowden напуска страната си и в последствие публикува хиляди секретни документи на американското правителство. Съдържанието на тези документи разкрива тайното съглашение UKUSA между САЩ, Англия, Австралия, Канада и Нова Зеландия известно като «ПЕТТЕ ОЧИ», по силата на което различни специализирани служби от тези държави обединяват силите си с цел прихващане, съхранение и анализ на различен вид комуникации в световен мащаб — милиарди телефонни разговори, мейли, чатове, сателитни и други комуникаци, спътникови, позициониращи и други данни.

Структурата на това съглашение е многопластова, като основни нейни компоненти са:

PRISM — проект на Националната агенция за сигурност на САЩ, чрез който се събира и обработва информация от базите данни на IT гигантите Microsoft, Yahoo, Google, Facebook, YouTube, Skype, Apple и други;

XKEYSCORE — специализирана софтуерна платформа на Националната агенция за сигурност на САЩ, чрез която се прихваща и анализира телекомуникационен и интернет трафик, като е възможно

установяване и следене в реално време на дигитален отпечатък, идентичен със самоличността на организация или отделно физическо лице;

Tempora — проект на Департамента за правителствени комуникации на Англия GCHQ, чиято основна функционалност позволява извличане, съхранение и анализ на огромен обем от данни, събирани от най-големите възли/сборни пунктове на оптичната мрежа, върху която се крепи киберпространството.

Наред с гореизброените проекти за прихващане и анализ на комуникацията на стотици милиони интернет потребители по цял свят, са налични и функционират набори от киберинструменти, създадени от няколко разузнавателни държавни структури. По-голямата част от тези инструменти са изключителна държавна тайна и техните имена са неизвестни, но функционалността им се свежда основно до «превземане» на чужди компютърни системи, чрез използване на набор от уязвимости /0-day/ и последващо прихващане и анализ на постъпващата информация.

През 2007-2008 г. иранският президент по онова време Махмуд Ахмадинеджад посещава град Натанц, в чиито покрайнини функционира огромно подземно съоражение с няколко хиляди газови центруфуги за обогатяване на уран U-235. Визитата е отразена в официалния сайт на президента с прессъобщение и няколко десетки снимки от вътрешността на комплекса. В няколко регионални телевизии са публикувани репортажи от събитието и други подобни посещения на президента в други правителствени обекти от ядрената програма на Иран. Върху една от публикуваните снимки е запечатана визията от екраните на работещите в съоръжението инженери.

Тази малка част от интерфейса, с който боравят иранските инженери и допълнителните материали в интернет, преса и телевизия се явяват ключови за предстоящата кибератака, забавила иранската ядрена програма с няколко години. Няколко седмици по-късно до информационните системи на ядрената централа е «доставен» зловреден код — повратен момент в Операция Олимпийски Игри — специализирана кибероперация на американски и израелски разузнавателни служби. Основно оръжие на операцията — StuxNet - световно известен вирус /набор от вируси/ заразяващ SCADA индрустриални системи, за първи път открит от почти безизвестната беларуска антивирусна компания VirusBlokAda през 2010 г.

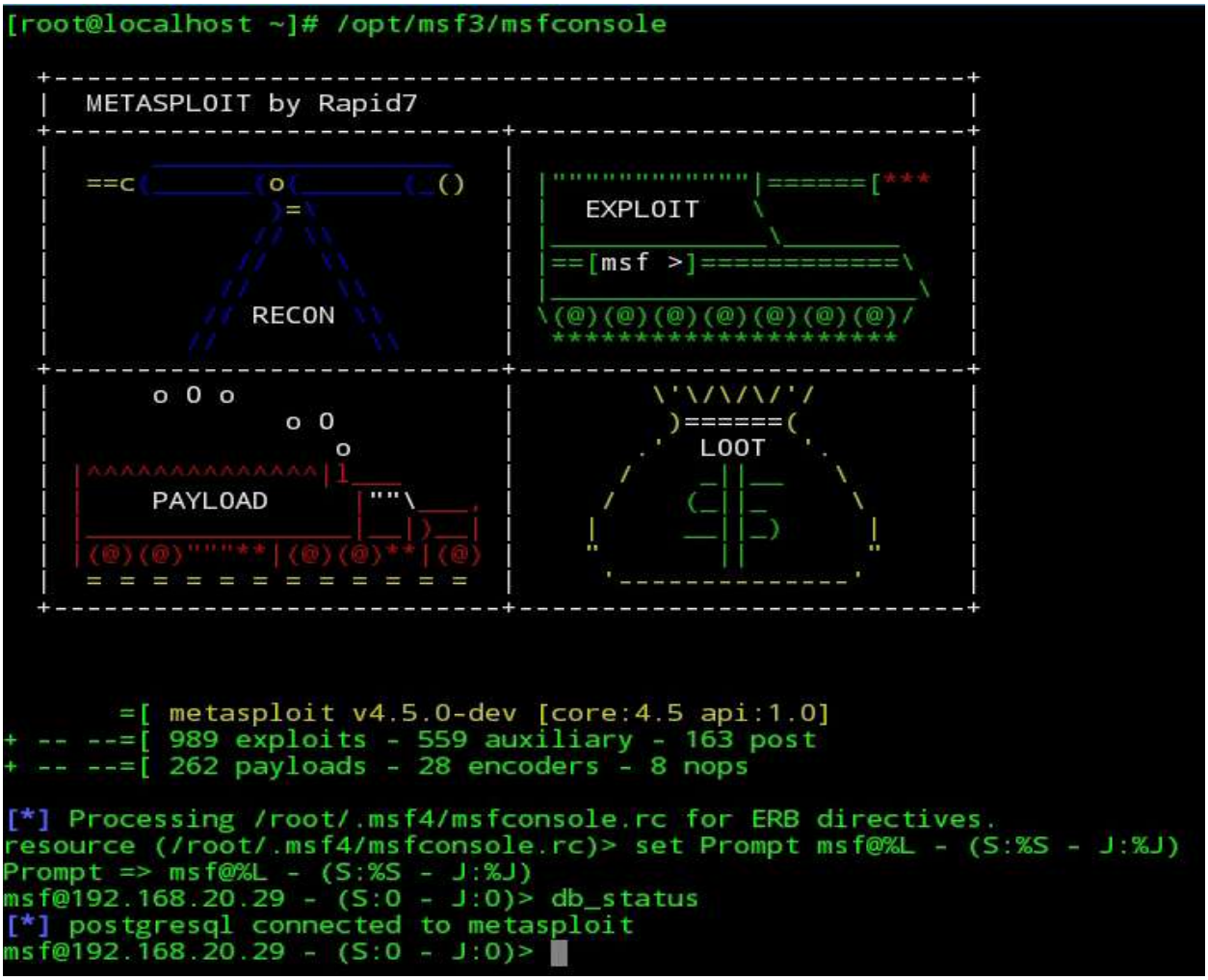
Други представители на тези тайни организации са PLA UNIT 61398 — специализирано звено за кибер операции на Народната освободителна армия на Китай; UNIT 8200 — звено за кибер операции на Израелските отбранителни сили ЦАХАЛ; тайни групи към Федералната служба за безопасност и Главното

разузнавателно управление на Русия, тясно свързани с руската кибер мафия; кибер армия на Северна Корея и други.

Подобни кибероперации на специализирани държавни организации се планират и провеждат продължително и включват редица други разузнавателни и контраразузнавателни способи и съпътстващи мероприятия. Способност за подобни прояви в световен мащаб притежават само няколко държави!

2.3 Нерегламентирано проникване/hack

В съвременната литература, специализирана в сферата на компютърно-информационната сигурност е широко разпространено виждането, че «хакването» е изкуство. Нивото и сложността на осъществяването на нерегламентиран достъп до компютърни системи зависи от познанията и степента на мотивираност на атакуващия/атакуващите. Основната методология използвана при осъществяването на нерегламентиран достъп до информационни системи най-общо следва цикличността по 1 — опознаване; 2 — сканиране; 3 - придобиване на нерегламентиран достъп; 4 - жътва/извличане или въвеждане на данни в компрометираната система; 5 - скриване на следите и подсигуряване на възможност за допълнителен достъп при необходимост. Как практически се осъществява това? Как го правят хакерите? - със специфични софтуерни инструменти като Metasploit. Към 2018 г. над 70-80 процента от хакерите използват този инструмент. Той е набор от общоизвестни и известни за закрит кръг хора уязвимости, методи и подходи за хакване, събирани и комбинирани от американската фирма Rapid7. Работата с приложението са извършва в команден режим и изисква познания над средно ниво, за работа с компютърни системи и мрежи.



За по-удобна работа с приложението са налични допълнителни модули — Armitage и CobaltStrike, предоставящи визуална среда на потребителя.

Друг изключително използван при осъществяване на нерегламентиран достъп инструмент е Sqlmap – автоматизиран софтуер за манипулиране на бази данни.

2.4 Обезобразяване/deface на интернет сайт

Осъществяването на нерегламентиран достъп до компютърно-информационни данни и последваща промяна на първоначалния изглед на интернет сайт или интернет базиран ресурс /deface/ се постига основно, чрез използване на пропуски и неточности при изграждането и функционирането на

компютърно-информационна инфраструктура. Основните начини за осъществяване на deface са:

2.4.1. Symlink

Този метод използва неправилното и неточно интерпретиране на файлово местоназначение в операционна система, основно при споделения метод за изграждане на интернет сайтове /shared hosting/. При споделения метод за изграждане на интернет сайтове, върху една операционна система е налично съдържанието на десетки и/или стотици интернет сайтове, разделени в отделни дигитални папки, но в пределите на една и съща файлова структура. Атакуващ придобива нерегламентиран достъп до потребителско име и парола за достъп до заделеното място за определен сайт или атакуващия се абонира сам за услугите на хостинг фирма. В заделеното място само за един от множеството интернет сайтове върху тази файлова и операционни система, атакуващия обикновенно добавя “зловередно” съдържание под формата на автономна работна среда /shell/, чрез която изпълнява отдалечено компютърни команди върху атакуваната система. Неправилното и неточно конфигуриране на последната, позволява на атакуващия да достъпи и променя дигиталните папки, съдържащи другите интернет сайтове върху тази система. Идентичен метод на атака е използван от българската хакерска групировка “Cyber Warrior Invasion” неутрализирана през лятото на 2012 г., в резултат на което са “обезобразени” около 500 интернет сайта в България и по света. Друга разновидност на този метод за deface е първоначално осъществяване на нерегламентиран достъп до неточно конфигуриран сайт и последащо “повишаване” /privilege escalation/ на права и/или symlink.

2.4.2. **DNS hijacking**/Неправомерно манипулиране на записите в системата за имената на интернет сайтове

Domain Name System представлява унифициран метод за преобразуване на имената на интернет сайтове в интернет протокол адреси. Интернет

браузърите, които се използват за достъпване и разглеждане съдържанието на интернет сайтове изпращат и приемат заявки от интернет протокол адреси /IP адреси/ – те не “познават” имената на интернет сайтовете. За това е въведена единна система за преобразуване на имената на интернет сайтовете в интернет протокол адреси - Domain Name System. Най-общо тя представлява хиляди сървъри из цял свят, които съдържат листа с различни имена на интернет сайтове и кореспондиращия интернет протокол адрес /къде може да бъде намерен съответния сайт/. Данните в тези DNS сървъри се синхронизират постоянно и е налична йерархична структура в зависимост от окончанието на съответното интернет име на сайт. В същото време имената на интернет сайтовете в световен мащаб са географски разделени, като за отделните държави са налични един или няколко регионални “отговорници”. За имена на интернет сайтове завършващи с .bg например, единствен и оправомощен субект е варненската фирма “Цифрови системи” ООД. Всеки, който желае да регистрира интернет сайт с окончание .bg задължително трябва да го направи, чрез функционалността предлагана от сайта на тази фирма – www.register.bg. След регистрация на сайт с окончание .bg /например/, фирмата регистратор предоставя възможност, чрез специализиран интерфейс за указване на кореспондиращ със сайта сървър за интернет името и сървър за пощенски услуги. В тази връзка, притежаващият потребителското име и парола за достъп до административния панел на интернет сайт у домейн регистратора /register.bg например/ има възможността да настройва и задава местонахождението на сайта и пощенския сървър зад определен интернет протокол адрес. Независимо, че легитимния собственик и създател на определен интернет сайт има контрол върху неговото физическо местонахождение в хостинг фирма, атакуващ можеш да придобие нерегламентиран достъп до административния панел у фирмата домейн регистратор и да промени сървъра, който се грижи за преобразуването на името в интернет протокол адрес. Този нерегламентиран достъп до административния панел у фирмата домейн регистратор често се придобива, чрез предварителен нерегламентиран достъп до пощенска кутия, посочени при

регистрирането на сайт. По този начин, през месец май 2014 г. DNS записите на интернет сайта на Българската църква /www.bg-patriarshia.bg/ са променени в административния панел у фирмата домейн регистратор, в резултат на което всички заявки към този сайт са препращани към сървър в САЩ, на който е нарочно поставено “хвалебствено” съобщение с послание на фона на турско знаме. С две думи – който контролира администраторския панел на съответното име на интернет сайт, у домейн регистратора – той указва къде /зад кой IP адрес/ е сайта.

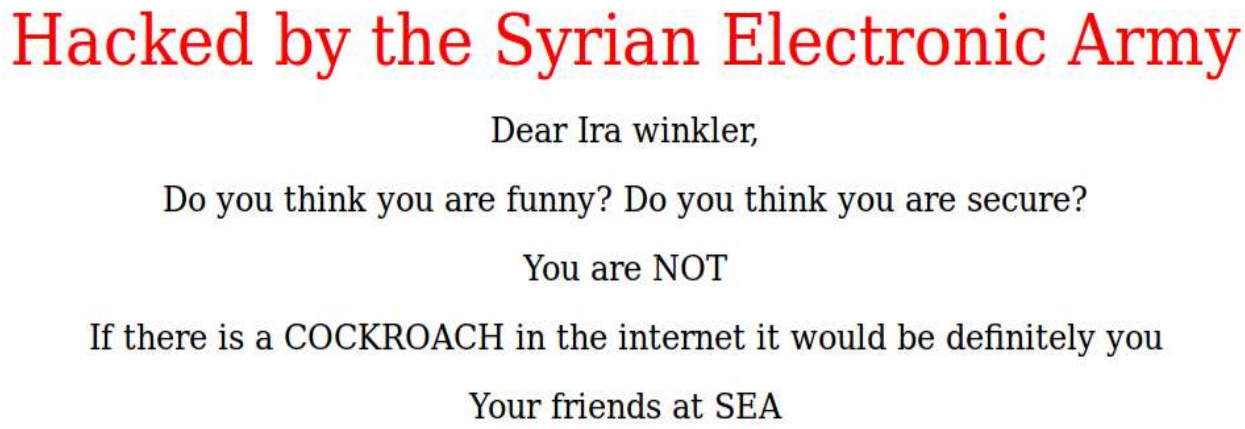
В световен мащаб са известни /но рядкост в българското киберпространство/ още два метода за осъществяване на промяна на първоначалния изглед на интернет сайт /deface/:

2.4.3. **Server exploit**/Нерегламентиран достъп до сървърни ресурси

При този метод, атакуващ използва пропуски и неточности в конфигурацията на операционната система, в чиято файлова структура е съдържанието на интернет сайта, и в последствие осъществява незаконната промяна на първоначалната страница. Метода е сложен и се прилага от изключително подготвени и опитни субекти със специфични познания в областта на компютърно-информационната сигурност. Метода се използва най-вече за придобиване на нерегламентиран достъп до компютърно-информационни данни и използването им с други цели - “събиране” на потребителски имена и пароли, “заразяване” на други компютърни системи, осъществяване на DDoS атаки, нерегламентиран “майнинг/добиване” на виртуални криптографски валути и тн.

2.4.4. **Third-party provider exploit**/Използване уязвимостите на друг доставчик на услуги/

При този метод, се осъществява нерегламентиран достъп до компютърно-информационни ресурси на фирма, която от своя страна изпълнява определени доставки на информационни ресурси за интернет сайта, който е атакуван. Метода е сложен и изключително рядко прилаган. Чрез него, през месец март 2014 г., визията на един от интернет сайтовете на световно известна фирма, специализирана в компютърно-информационната сигурност – RSA, беше променен от “Сирийската електронна армия”. При инцидента не е осъществяван нерегламентиран достъп до информационните ресурси на самия сайт, а е променен модул, който интернет сайта при зареждане “извиква” от сървъри на друга фирма, доставяща информационни услуги:



2.5 Индустриален шпионаж

Основна цел, преследвана от придобиващия нерегламентиран достъп — придобиване на конфиденциална фирмена информация за продукти, клиенти, цени, чертежи, спецификации, ноу-хау, бъдещи фирмени планове и тн. Проникването в чужда фирмена компютърно-информационна система и извличането от там на подобна информация е сложен и продължителен процес, които изисква съществени ресурси и познания, характерни за организирани хакерски групи по-горе, а също и за описаните предходно специализирани правителствени организации. През 2014 г. Федералното бюро за разследване на САЩ обявява за издирване петима служители на секретно звено 61398 от Народната освободителна армия на Китай. Същите са обвинени в провеждането на кибершпионаж срещу над 70 различни компании от САЩ и Европа.

През януари 2016 г. Федералното бюро за разследване на САЩ по идентичен начин обявява за издирване седем ирански граждани по подозрение в осъществяването на координирани DDoS атаки срещу американски финансови институции.

2.6 Кибер операции, спонсорирани от държави/State sponsored

Информацията за подобни операции е оскъдна, тъй като те се провеждат в условията на изключителна конфиденциалност. Фрагментирани данни са налични от бивши служители на разузнавателни структури, които са арестувани по повод разгласяването или пък са обявени за издирване — Edward Snowden, Bradley/Chelsea Manning и други. Провеждането на подобни операции най-често е свързано с дейността на предходно описаните киберармии, като често техните мероприятия се отъждествяват с термина «хибридни войни» — нестандартни действия, инкорпориращи в себе си бойни действия, диверсии, фалшиви новини, кибервойна и други.

Често тези операции се водят паралелно с провеждането на локални военни операции, сложни политически ходове, анексиране на чужди територии, икономически санкции и техните контрамерки, както и други стратегически съревнования в световен мащаб, напомнящи за «Студената война».

В сложната световна карта на провежданите подобни кибер операции, спонсорирани от отделни държави и пряко реализирани от техните киберармии се открояват основите фигури на американската Агенция за национална сигурност и ЦРУ, руските Федерална служба за сигурност /правоприемник на КГБ/ и Главното разузнавателно управление, китайската киберармия — част от Народната освободителна армия на Китай, израелската МОСАД и други не по-малко значими регионални играчи.

Засегнатите по-горе основни атаки към онлайн базирани ресурси през последните години изключително рядко могат да се разглеждат или провеждат поотделно, тъй като между тях съществуват изключително сложни взаимовръзки, обусловени от динамиката на съвременното киберобщество. Осъществяването например на нерегламентиран достъп до вътрешна корпоративна мрежа на голяма фирма много често е предхождано от заразяване на персоналния компютър на неин служител от средния или висок мениджърски клас. Този служител използва стара версия на операционна система, небрежно позволява на своето дете — тинейджър да използва служебния му лаптоп за компютърни игри; използва компютъра за достъп до «мръсни» сайтове — порнография, онлайн хазарт, тракери с нелизенциран софтуер и други. В последствие този служебен компютър /който е заразен с троянски кон от крак на компютърна игра, инсталирана от детето/ попада във фирмената мрежа, където може да послужи за «разширяване» вектора на атаката, чрез препращане на вируси във фирмения пощенски сървър, чрез използване на запазени в компютъра пароли за достъп до фирмените ресурси, чрез прихващане на корпоративна информация от микрофона, камерата и тн. От друга страна, хиляди заразени по гореописания начин компютърни конфигурации са

основните градивни единици на бот-нет мрежата. Сложно организирана международна престъпна група от хакери може да създаде бот-нет мрежа от милиони, дори десетки милиони заразени домашни компютърни конфигурации. Функционалността на тази бот-нет мрежа носи на своите създатели и собственици хиляди евро доходи всеки ден. Бот-нет мрежите обикновенно се отдават под наем с цел атаки за отказ от услуга, разпращане на нежелани електронни съобщения СПАМ, извличане на потребителски имена и пароли за достъп до социални мрежи, комуникатори и други.

ГЛАВА ТРЕТА. Състояние на киберсигурността на публичната администрация в света

Обхващането на състоянието на компютърно-информационната сигурност в световен мащаб е изключително предизвикателство и едва ли съществува личност, корпорация или правителствена организация, която да е осъществила подобно начинание. Редица водещи фирми с сферата на компютърно-информационната сигурност като Kaspersky, BitDefender, Dell, HP, CloudFlare, Symantec и Cisco, регулярно издават доклади за регистрираните от тях кибер заплахи, тяхната динамика и тенденции.

Във връзка с целите на настоящата магистърска теза, обхващането на състоянието на киберсигурността на публичната администрация в България е необходимо да се разглежда в контекста на регионалните и световни тенденции в тази насока.

За различните региони и държави, както и за техните публични администрации съществуват различни рискове от настъпване на кибер инциденти, които най-общо се обуславят от широк спектър влияния - ниво на развитие на обществото, неговата кибер информираност и резистентност,

политическата обстановка, нивото на дигитализация, степен на индустриализация, регионални военни конфликти, хибридни войни и други.

С цел опита за обхащане и отразяване нивото на киберсигурността на публичната администрация в страната, в настоящата глава е проведено изследване на значими кибер инциденти в регионален и световен мащаб.

Състоянието на компютърно-информационната сигурност към 2018 г. в световен мащаб може да бъде частично фиксирано, чрез отразяване на следните по-съществени информационни инциденти за последните месеци.

3.1 Операционната система Windows

Огромна част от дейността на публичната администрация в България и света физически се осъществява върху компютърни конфигурации с инсталирана операционна система Windows.

Операционната система Windows на американската корпорация Microsoft е най-разпространената платформа, използвана от домашни потребители, банкови институции, държавни органи, военни организации и други. Тя предоставя лесен и интуитивен интерфейс, и за нея са налични хиляди допълнителни приложения, улесняващи ползвателите при забавления, отдих и бизнес.

Предвид своята изключително широка популярност и използване, тази операционна система за съжаление е една от най-уязвимите в света и в сферата на компютърно-информационната сигурност е наложено мнението, че нейното използване е изключително рисково. За операционна система Windows са налични множество програмни средства, позволяващи нейното съществено компрометиране.

Описаните безплатни RAT инструменти създадени от неизвестни хакери, предоставят възможност за отдалечено манипулиране на всички дейности, извършвани на заразения компютър. Налични са опции за преглед, добавяне и изтриване на файлове върху превзетата машина, скрито запускане на видео камерата, микрофона, извличане на потребителските пароли, инжектиране на допълнителен компютърен код при сърфиране и тн. В специализирани хакерски форуми са налични подобни платени инструменти с разширена функционалност, която гарантира продължително скрито наблюдение на заразения компютър.

От друга страна на европейския и световен бизнес пазар за инструменти, свързани с компютърно-информационната сигурност са налични няколко водещи фирми, предлагащи специализирани инструменти за манипулиране на всякакви Windows базирани устройства. Представители на тези субекти са германската фирма Gamma Group с техния продукт FinFisher, италианската фирма Hacking Team предлагащи Remote Control System, френския лидер в тази

насока Vupen, както и няколко израелски частни фирми, водени от бивши служители на разузнавателната общност.

На трето място, след хакерските общности и частните фирми, предлагащи специализирани инструменти за тотално компрометиране на операционната система Windows, се нареждат тайните правителствени организации и кибер армии, които са снабдени със секретни набори от подобни платформи на световно ниво. Най-яркия пример е американската Национална агенция за сигурност/NSA, която годишно използва милиарди долари и десетки хиляди служители, за разузнавателни и контраразузнавателни мероприятия. С няколко кликвания на мишката, служител на тази агенция може да изследва и анализира съдържанието на милиони мейли, телефонни разговори, снимки, видео и тн. За защита на американската национална сигурност е възможно и предприемането на целенасочени военни действия, позициониране на мобилни телефони, заснемане от сателит на обекти, превозни средства и лица, както и тяхното физическо унищожаване, чрез ракетни удари.

Всички тези субекти таргетират предимно операционната система Windows, предвид нейното изключително широко разпространение. Друга изключително актуална и атакувана система е Android, тъй-като нейния дял е изключително висок сред мобилните устройства.

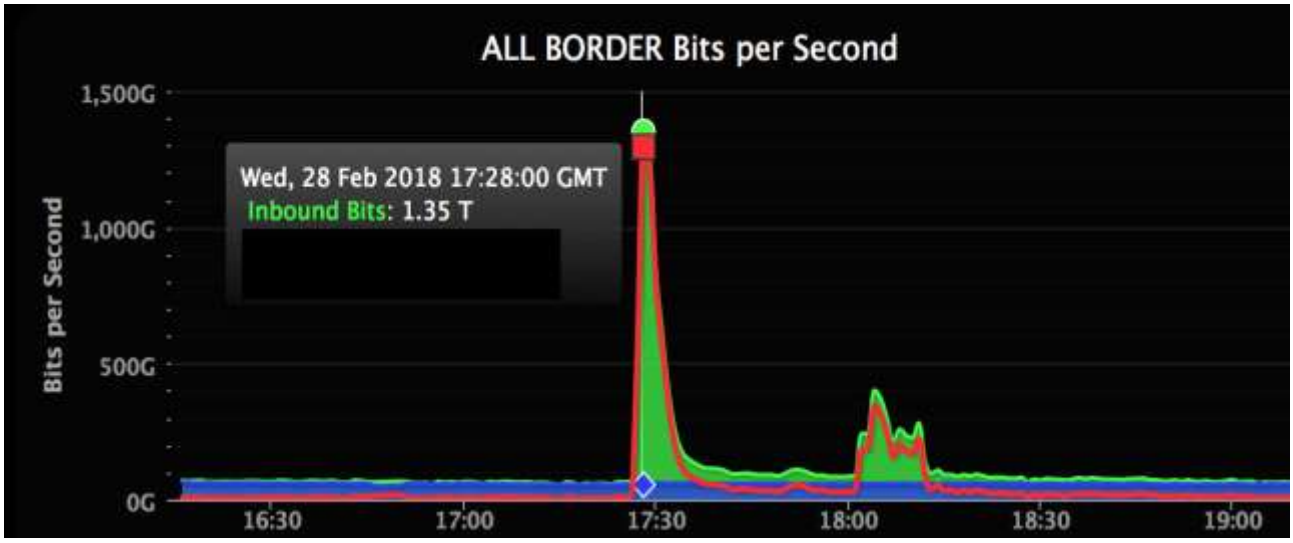
Всяка публична администрация, загрижена за своята кибер сигурност е необходимо да преосмисли и минимизира използването на ненадеждни или уязвими операционни системи, с цел недопускане на компютърно-информационни инциденти.

3.2 Най-голямата атака за отказ от услугата/DDoS

На 28 февруари 2018 г. около 17:21 часа UTC е регистрирана най-голямата атака за отказ от услугата/DDoS до момента. Жертва на атаката е

американския интернет сайт за хостване на компютърен код GitHub, а размера на изпращаните към него заявки са от порядъка на 1,35 Терабита в секунда, което се равнява на над 1300 Гигабита в секунда. Пострадалата фирма разяснява, че този огромен обем от данни е реализиран, чрез атакуването им с над 127 милиона пакета в секунда, чиито източник са били над хиляда отделни автономни мрежи от интернет пространството. За осъществяването на този вид компютърна атака са използвани няколко хиляди неправилно или неточно конфигурирани сървъри, използващия Memcached – дистрибутирана система за съхранение на данни в кеш-паметта, използвана най-често за съхранение на динамични бази от данни. Чрез изпращане на шалфива/spoofed заявка към уязвим memcached сървър на UDP порт 11211, се генерира няколко хиляди пъти по-голям обем от данни, които се насочват към жертвата.

Подобни хакерски атаки представляват съществен риск за правилното функциониране на представители на публичната администрация от всякакъв калибър. Предотвратяването и борбата с DDoS атаките е предизвикателна дейност, която често предполага сериозен финансов или човешки ресурс.



3.3 HackingTeam от Милано

Италианската фирма HackingTeam развива своята дейност от началото на 2003 г., като предлага на правителствени правоохранителни организации специализиран софтуер за „проникване“. Платформата с наименование RCS — Remote Control System предоставя множество способи за „придобиване“ на достъп до компютърни конфигурации и мобилни телефони, както и потребителски интерфейс за боравене с придобитата информация. На практика, клиент на фирмата закупил платформата притежава възможността да «контролира» отдалечено компютърни конфигурации и мобилни телефони на обект/и на разследване или друг интерес, като функционалността включва — пълни данни за «заразената» система — модел, MAC, IMEI, размер на памет и други; извличане на всякакъв вид комуникация — скайп, мейли, криптирани канали и други комуникатори.; отдалечено наблюдение и запис около обекта, чрез включване на камера и микрофон, изследване на файловата система на обекта, извличане на листи с абонати, SMS-и, мейли и тн.

На 5 юли 2015 г. неизвестен извършител публикува от официалния Туитър акаунт на фирмата съобщение, че същата е компрометирана, като е посочен линк за сваляне на над 400 гигабайта конфиденциална информация на HackingTeam. Инцидента получава изключително широк отзвук в средите на компютърно-информационната сигурност в световен мащаб, не само заради установените три броя 0-day уязвимости за Adobe Flash Player в изтеклите фирмени данни. От публикуваната информация се установява, че миланската фирма е продала своята специализирана платформа на полицейски и разузнавателни структури от Италия, Испания, Сингапур, Унгария, Мароко, Саудитска арабия, Турция, Узбекистан, САЩ, Нигерия, Русия, Полша, Уганда и други. Малко над 52 милиона евро общо е заплатила угандийската армия за използването на споменатия софтуер, като средните общи приходи от всичките около 70 клиента са били над 1 милион евро на клиент. Най-вероятният субект, осъществил атаката срещу HackingTeam е специализирана разузнавателна

служба със сериозен потенциал от Европа или Америка. При преглед и анализ на част от изтеклата информация се установява, че служителите на „пострадалата“ италианска фирма широко са използвали уязвимата операционна система Windows, използвали са недостатъчно сигурни пароли и не са защитавали мейл комуникацията си с криптографски средства и похвати.

В кореспонденцията на миланската фирма са налични и имената на няколко служители на ДАНС – Милко Миленов, Асен Куманов и Мирослав Цветков, които през 2014-2015 г. са проучвали възможностите за закупуване на подобен специализиран софтуер и са провеждали срещи с представители на фирмата.

3.4 Американските корпорации Target и Home Depot

Това са огромни вериги от магазини и офиси на територията на САЩ и Канада за потребителски стоки от всякакво естество — техника, хранителни стоки, оборудване, инструменти и тн. През 2013 г. и 2014 г. по идентичен начин са незаконно придобити от хакери данни от кредитни карти, мейли, пароли и друга информация за десетки милиони потребители на двете фирми. Компютърните мрежи на фирмите са компрометирани като крайните устройства за разплащане на касите на магазините са заразени със специфичен зловреден софтуер с наименование BlackPOS, известен и с имената reedum и Kaptoxa. Това приложение е създадено на компютърния език VBScript от Сергей Тарасов с псевдоним ree4 и Ринат Шабаев от Русия, по специфична заявка в хакерски форум. За целта Тарасов и други негови сподвижници са изследвали функционалността на софтуера за разплащане на двете атакувани компании. В последствие BlackPOS е конфигуриран да краде/откопира данни от кредтни карти от RAM паметта на компютърната кофигурация, находяща се на касата в съответния магазин. Въпреки, че в процеса на плащане се използат криптирани канали за одобрение на сделката, чрез комуникация в специална банкова

компютърно-информационна система, софтуера на Тарасов извлича информацията преди тя да бъде преконвертирана, защитена и изпратена.

Визираните четири съществени компютърно-информационни инциденти или заплахи за информационната сигурност на публичната администрация в света са само малка част от свободно наличната информация в кибер пространството. Стотици са подобните инциденти, които са осъществени, но закрити за широката публика. Банкови и корпоративни мрежи са инфилтрирани от злонамерени хакери, като загубите се равняват на милиони евро. От съображения за техния имидж и страх от загуба на клиенти много от афектираните организации не желаят публично разгласяване на подобни кибер инциденти. Те предпочитат да покрият възникналите загуби от техните гаранционни фондове, да заплатят откуп, да преустановят конкретна услуга временно или да предприемат други превантивни мерки, за защита на техните корпоративни или частни интереси.

ГЛАВА ЧЕТВЪРТА. Състояние на киберсигурността на публичната администрация в България

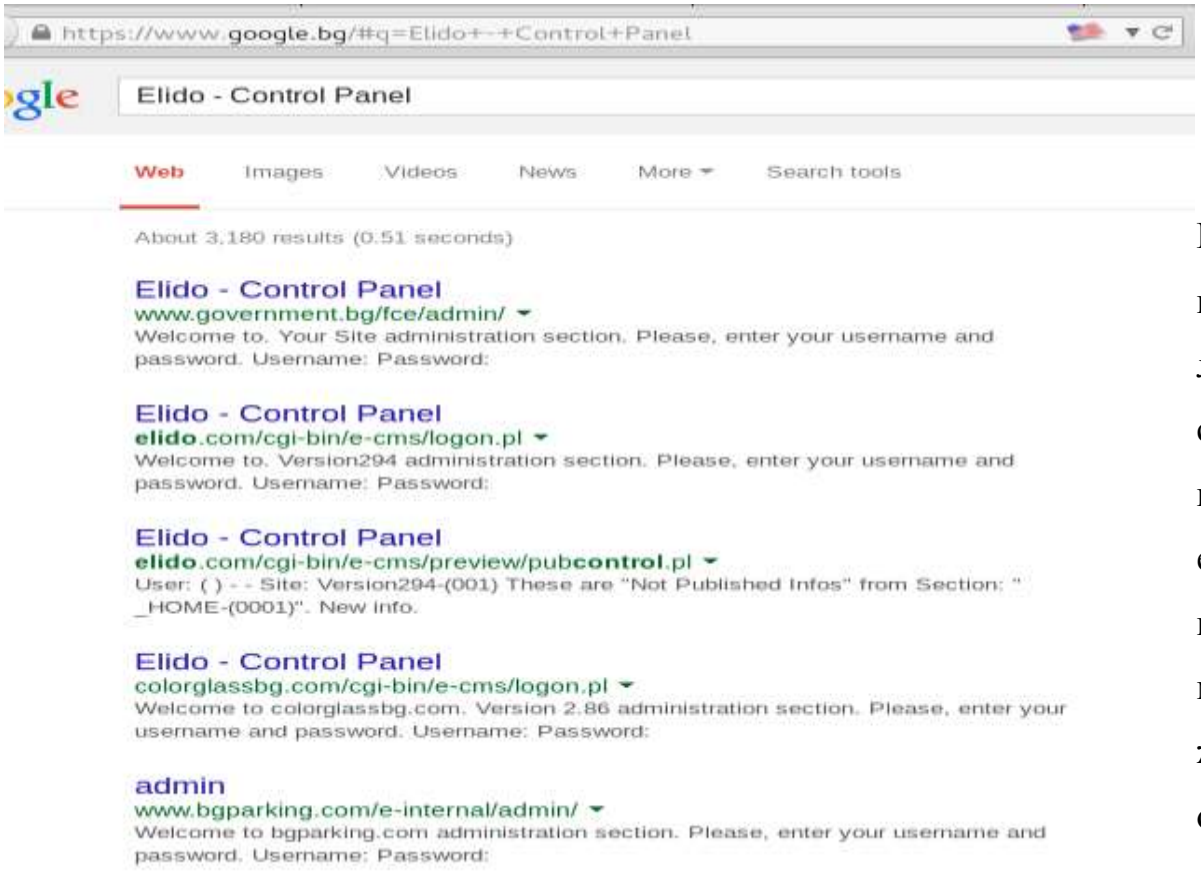
Фрагментирани данни за нивото на компютърно-информационната сигурност в страната е възможно да бъдат придобити при изследване на следните обекти:

4.1 Министерски съвет

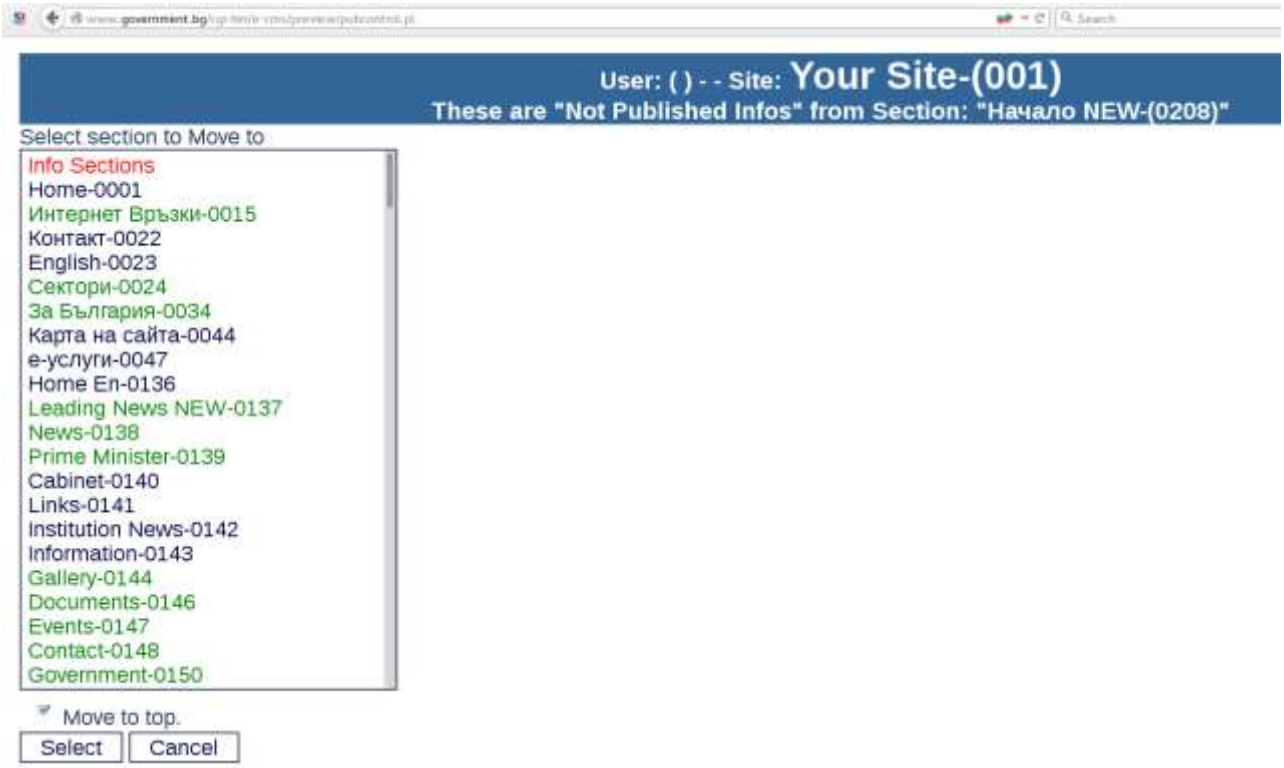
Интернет сайтът на правителството на Република България на интернет адрес www.government.bg е лицето на държавата пред останалия кибер свят. Нивото на неговата реализация, поддръжка и сигурност е изключително важен показател за цялостното ниво на компютърно-информационната сигурност в страната. В тази връзка, при посещение и изследване на част от ресурсите на сайта се установява, че той е реализиран основно на програмния език Perl, като

за менажиране на съдържанието му се използва CMS с наименование Elido — Control Panel. В изходния html код на страницата са налични данни за потребителско име mitko и дата 05 април 2007 г., през която най-вероятно са извършвани последни поправки по изходния код на страницата. Тази дата може да бъде приета и за последната, при която са извършвани други софтуерни конфигурации и донастройки по сайта. Отдалечеността във времето на тези промени е категоричен показател на липса на регулярно и качествено одитиране и персонализиране/донастройка на тези компютърно-информационни ресурси. В съвременният киберсвят, където се случват ежеминутно важни промени по отношение на сигурност и тенденции, е наложително навременно и качествено реагиране и донастройка на каквито и да е компютърно-информационни ресурси.

При търсене в открити източници на използваната платформа за менажиране на съдържанието на сайта www.government.bg с наименование Elido Control Panel е достига до други подобни ресурси, използващи този софтуер:



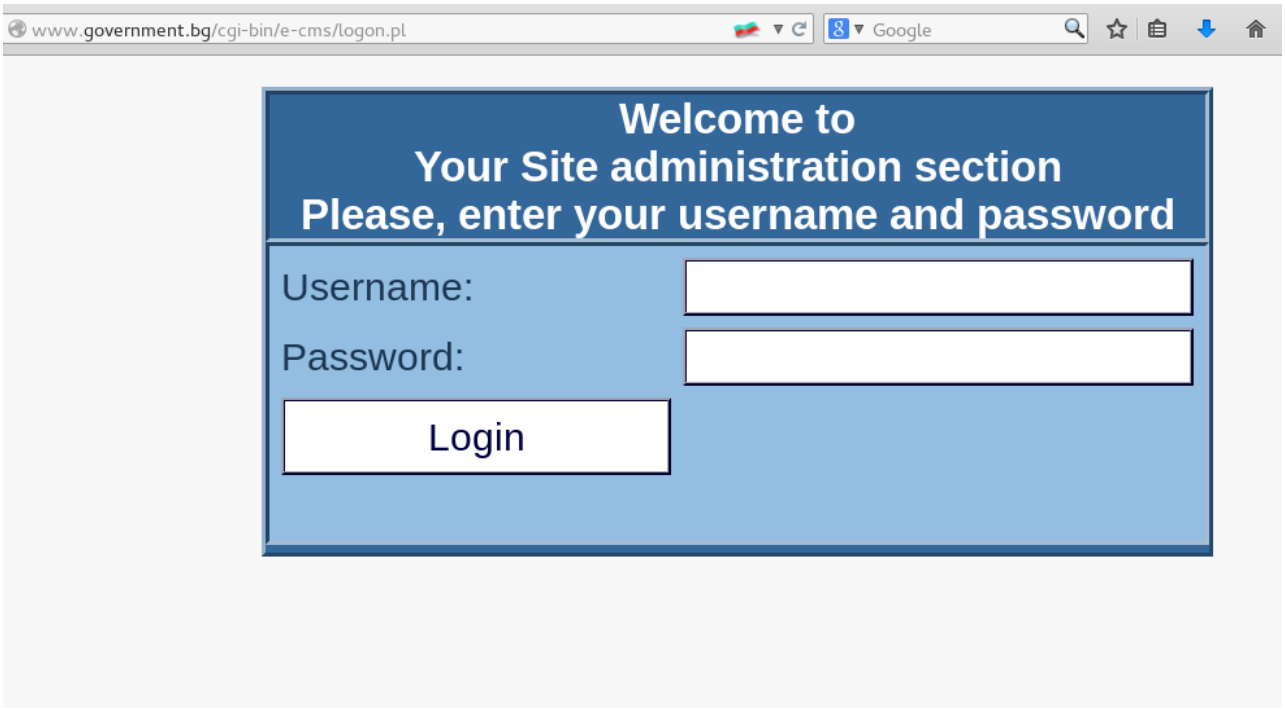
В последствие е възможно използването на индексирани от търсачка Google ресурси /като http://elido.com/cgi-bin/e-cms/preview/pubcontrol.pl/ за да се достигне до http://www.government.bg/cgi-bin/e-cms/preview/pubcontrol.pl – част от администрацията на сайта, предоставяща определена специфична функционалност.



Подобна функционалност е немислимо да е налична за интернет потребители, без администриращи или други функции.

От друга страна, след допълнително изследване на ресурсите се установява, че уеб частта за вписване в администраторския панел на сайта www.government.bg е налична за достъп от всеки интернет протокол адрес в света! Това обстоятелство противоречи на общоприетите добри практики в сферата на компютърно-информационната сигурност за ограничаване на достъпа по интернет протокол адрес, използване на допълнително потребителско име и парола да достъп до този ресурс /обикновено чрез .htaccess и .htpasswd файлове/ и други похвати, за предпазване от брут-форс атаки/налучкване на пароли и допълнителни методи за нерегламентиран достъп.

При изследване се установява, че административната част на сайта е възможна за достъп на адрес http://www.government.bg/cgi-bin/e-cms/logon.pl



Допълнителен пропуск в изграждането на този важен правителствен сайт е липсата на криптографски сертификат при осъществяване на достъп до администраторската му част. Всеки застанал на пътя на трафика администратора/ите на този сайт може с минимални усилия да прихване потребителските имена и пароли за достъп до админ панела, поради простата причина, че същите се предават в некриптиран и напълно четим вид/plaintext.

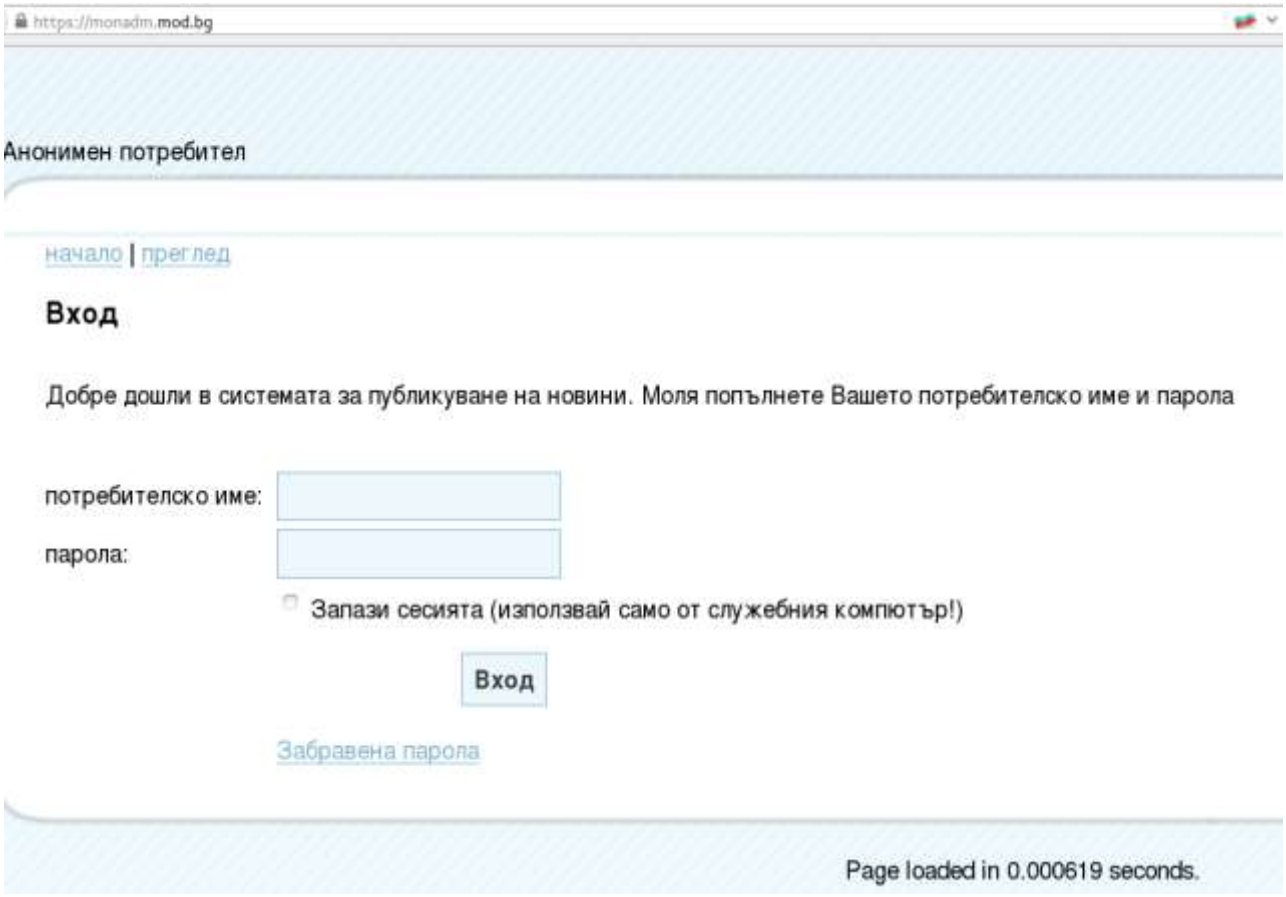
Не на последно място, чрез допълнително изследване на ресурсите на сайта се установява, че компютърния код на ресурса http://www.government.bg/fce/index.shtml е уязвим на XSS заявки и чрез манипулиране на входните данни по подобен начин http://www.government.bg/fce/index.shtml?s=001&p="'--></style>******** е възможно въвеждането на какъвто и да е текст за визуализиране, както и извеждане на допълнителен екран със съобщение:

Наличните неточности в изграждането и поддръжката на сайта www.government.bg са на пръв поглед нищожен, но в същото време категоричен показател за незадоволителното ниво на компютърно-информационната му сигурност, както и за нивото в регионален мащаб на други подобни ресурси!

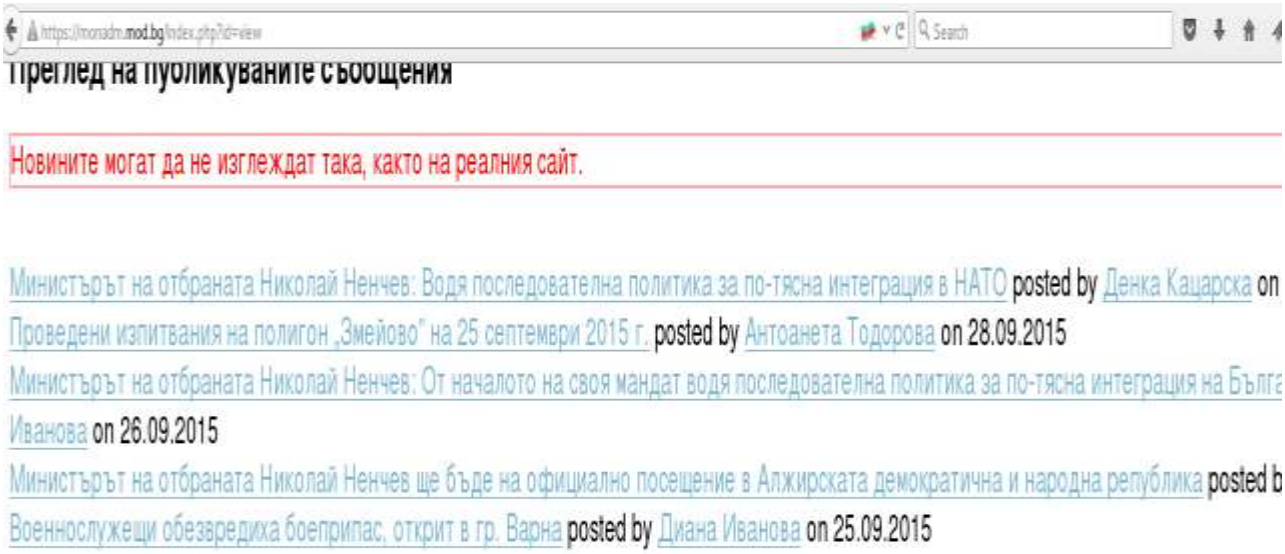
От началото на 2018 г. интернет сайта на Министерски съвет е обновен и е въведена нова визия, функционалност и софтуерна система за менажиране на съдържанието, като предходно описаните пропуски би трябвало да са заличени. Въпреки това те остават показател за нивото на киберсигурност в национален и регионален мащаб.

4.2 Министерството на отбраната

При повърхностно изследване ресурсите на сайта на Министерството на отбраната на Република България се установява, че ресурса http://www.mod.bg/bg/fn/ препраща към административен модул за публикуване на новини на същия сайт на адрес https://monadm.mod.bg/, чиято възможност за достъп от всеки интернет протокол адрес в света е само неточност на пръв поглед.



Опцията за преглед на новините, без вписване в административната част, разкрива имейл адреси и имена на три служителки — Антоанета Тодорова, Денка Кацарска и Диана Иванова, които от години се грижат за публикуване на новини на сайта на Министерството на отбраната. Наличието на подобна информация /общодостъпна/ е индикатор за пропуски в компютърно-информационната сигурност на този ресурс. Имена и мейли на служители на Министерството на отбраната, заедно с допълнителни данни и съобщение до тях от вида Spear Phishing в прецизно избран момент и при специфични обстоятелства са отправна точка за настъпването на многослоен и продължителен компютърно-информационен инцидент.



4.3 Атакувани сайтове на МВР и МОН през 2016

През месец февруари 2016 г. неизвестни лица използват пропуск в изграждането на сайтовете на Министерството на вътрешните работи и Министерството на образованието, като чрез манипулиране на полетата за търсене се извиква външно съдържание, което се визуализира на атакуваните сайтове.

На сайта на МВР е визуализиран текст и снимки, според които главния прокурор на страната е обвинен в корупция и се издирва от полицията. Подобни съобщения са изведени и за други политици, представители на парламентарно представени партии.

На сайта на МОН е визуализирана снимка на тогавашната министърка Кунева, представена в непличен танц върху маса пред погледа на важни български политици и на фона на турски флаг.

Двата инцидента намират изключително широк обществен отзвук в медийното пространство и социалните мрежи, като са нанесени непоправими морални щети на афектираните представители на публичната администрация.

Описаните неточности и пропуски при изграждането и поддръжката на тези важни правителствени сайта са на пръв поглед несъществени и могат да бъдат пренебрегнати като неопасни от практическа гледна точка за осъществяване на атака. Самото им наличие обаче, в съвкупност с други подобни пропуски /които е възможно да бъдат установени при задълбочено проучване/ съставя стройна логическа верига водеща до извода, че нивото на компютърно-информационната сигурност не е на необходимото ниво. Във всички сектори от администрацията на държавата са налични пропуски и неточности при изграждане и функциониране на компютърно-информационни ресурси, но настоящото ниво в България може да се определи под средното за Европа. Това състояние е резултат от редица обществено-политически, структурни, финансови, човешки и множество други фактори.

4.4 Кибератаки по време на изборите през октомври 2015

По време на провежданите избори за местна власт през периода 25 октомври до 1 ноември 2015 г. нормалното функциониране на редица държавни сайтове и информационни ресурси е затруднено или спряно, в резултат на масирана хакерска атака от вида Атака за отказ от услугата/DDoS.

Атакувани са сайтовете на Централната избирателна комисия, ДАНС, МВР, Информационно обслужване, НАП, Президентството и други важни държавни администрации.

За осъществяване на атаката са използвани хиляди зомбирани компютърни конфигурации, част от ботнет мрежа, които са принудени да изпращат множество заявки към целите, като по този начин изтощят техните хардуерни и софутерни ресурси. Тази атака е проведена на няколко етапа, като нейната интензивност се повишава след изказване на Президента на страната, в подкрепа на възможността за провеждане на електронно гласуване. След това изявление, сайта на президентската институция става недостъпен или частнично достъпен за период от няколко часа, като отново имижда на тази институция е сериозно увреден.

Поради специфични обществено-политически влияния по време на провеждането на изборите, от редица медии в страната са изказани твърдения, че зад тези атаки стоят представители на опозиционните партии в парламента и техните «тролове».

В крайна сметка, визираната атака оказва неблагоприятно въздействие върху публичната администрация в цялата страна, тъй като е нарушена нормалната работа на редица междуведомствени мрежи за финансови разплащания, затруднен е процеса по преброяване на гласовете, вътрешно-ведомствената комуникация в Избирателната комисия, нейните регионални звена и задгранични преставителства.

4.5 Фейсбук страницата на Президента през януари 2018

В ранните часове на 21 януари 2018 г. до официалната страница на Президента на Република България в социалната мрежа Фейсбук е осъществен нерегламентиран достъп от неизвестно лице, като е публикуван текст на турски език и препратка към турски интернет сайт за бързи кредити. Инцидента е широко отразен от редица водещи български медии, а неговото осъществяване е категоричен индикатор за незадоволителното ниво на киберсигурността на цялата публична администрация в страната.

Вероятно турския хакер, който е публикувал материалите не е осъзнавал важността на превзетия от него ресурс и просто е желал рекламирането на финансовия сайт пред хилядите последователи на профила на българския Президент. В конкретно избран момент подобна публикация, но с политическо изявление или дори фалшиво твърдение за обявяване на война, би могло да дискредитира и непоправимо накърни интересите на президентската институция или на цялата държава.

4.6 Безпрецедентна SPAM атака към България

Типичен пример за заразяване с компютърни вируси и създаване на ботнет мрежа и нейното разрастване е безпрецедентната атака към български интернет потребители, започнала през есента на 2016 г. Множество интернет потребители получават на електронните си пощенски кутии съмнителни имейли с предупреждение за плащане на просрочени задължения, предупреждения за завеждане на съдебно дело, промяна в регламента на институция или други подобни.

Визираната мащабна СПАМ кампания може условно да се раздели на следните шест/или повече вълни:

1. СПАМ от Националната агенция по приходите – първи мейли през октомври-ноември 2016 г. и в последствие през април-май 2017 г.

2. СПАМ от Частен съдебен изпълнител Радомир Стоянов – януари-февруари 2017 г.

3. СПАМ от Николай Лазаров с прикачен файл, именован “сметката” - февруари 2017 г.

4. СПАМ с искова молба и предупреждение за завеждане на съдебно дело от Добринка Дойнова – март 2017 г.

5. СПАМ с предупреждение за плащане на просрочени задължения от името на фирма Кредисимо АД – ноември 2017 г.

6. СПАМ с предупреждение за неплатени задължения към ЕНЕРГО-ПРО – декември 2017 г.

Заразяването на компютърната конфигурация се извършва сложно, на различни етапи. Първоначално към СПАМ съобщенията е прикачен зловреден файл, който заставя компютъра да извърши заявка да интернет сайт, който е

временно изграден върху вече съществуваща ботнет мрежа, която се цели да се разрастне. За целта се използват т.нар. „стабилни точки“ от нея – компрометирани компютри, които са с надеждни хардуерни и мрежови показатели, и които рядко се изключват от техните потребители. От така изградения върху няколко стабилни точки сайт се хоства и сваля допълнителен файл с характеристики на RAT инструмент, който компрометира компютърната конфигурация на потребителя, като извлича неправомерно лични данни, пароли за социални мрежи, пощенски кутии, банкови ресурси и други.

Така заразения компютър е възможно да бъде използван от кибер престъпници и за други кибер атаки – разпращане на нови фишинг мейли и DDoS мрежови атаки.

Описаната мащабна СПАМ кампания към България, която и към началото 2018 г. продължава на различни вълни е категоричен индикатор за вложен солиден информационен, времеви и човешки ресурс от хакерска или чужда правителствена организация. На фона на световната, европейска и регионална картина на кибер инцидентите е възможен е извода, че тази кампания е ключов компонент от хибридни войни, провеждани от противници на ЕС и НАТО.

ГЛАВА ПЕТА. Бъдещи тенцендиции и предизвикателства в сферата на киберсигурността в публичната администрация в България, региона и света

В съвременното дигитално общество са налични и ще се развиват нови и непознати заплахи към критичната инфраструктура на публичната администрация, фирми и отделни граждани. С появата и развитието на интернета на нещата - Internet of Things /IoT/, където всяко устройство, автомобил, машина, стая, бюро, хладилник и тн., ще бъде включено в световната мрежа, ще се родят нови видове и подходи за компрометиране на

човешкия живот извън киберпростанството. В близките години е възможно да сме свидетели и на първото кибер убийство на човешко същество. Подобни проявления за сега са само щрихи от сюжетните линни на съвременните научно-фантастични филми, но настоящите тенденции загатват предстоящото.

5.1 Стратегия за киберсигурност

На 13 юли 2016 г. с постановление на Министерски съвет е приета Националната стратегия за киберсигурност, която изразява колективния ангажимент и отговорност на всички заинтересовани страни и волята на ръководството на страната за осигуряване на модерна рамка и стабилна среда за развитие на националната система за кибер сигурност и постигане на отворено, безопасно и сигурно кибер пространство.

В стратегията е залегнала основна визия за постигане на „Кибер устойчива България 2020“, като са очертани етапите на развитие за израстване от базова информационна сигурност и кибер хигиена до зряло информационно общество, способно да противодейства на кибер и хибридни заплахи в различните сфери. При постигане на целите е планирано страната ни да бъде надежден и устойчив партньор и участник в общите мрежи и системи и колективната сигурност с евро-атлантическите ни партньори, с иновативно и изпреварващо технологично развитие, съответно на приоритетите за развитие на икономиката и обществото, и с капацитет и способности да участва в предотвратяването и преодоляването на променящите са кибер заплахи, кризи и инциденти.

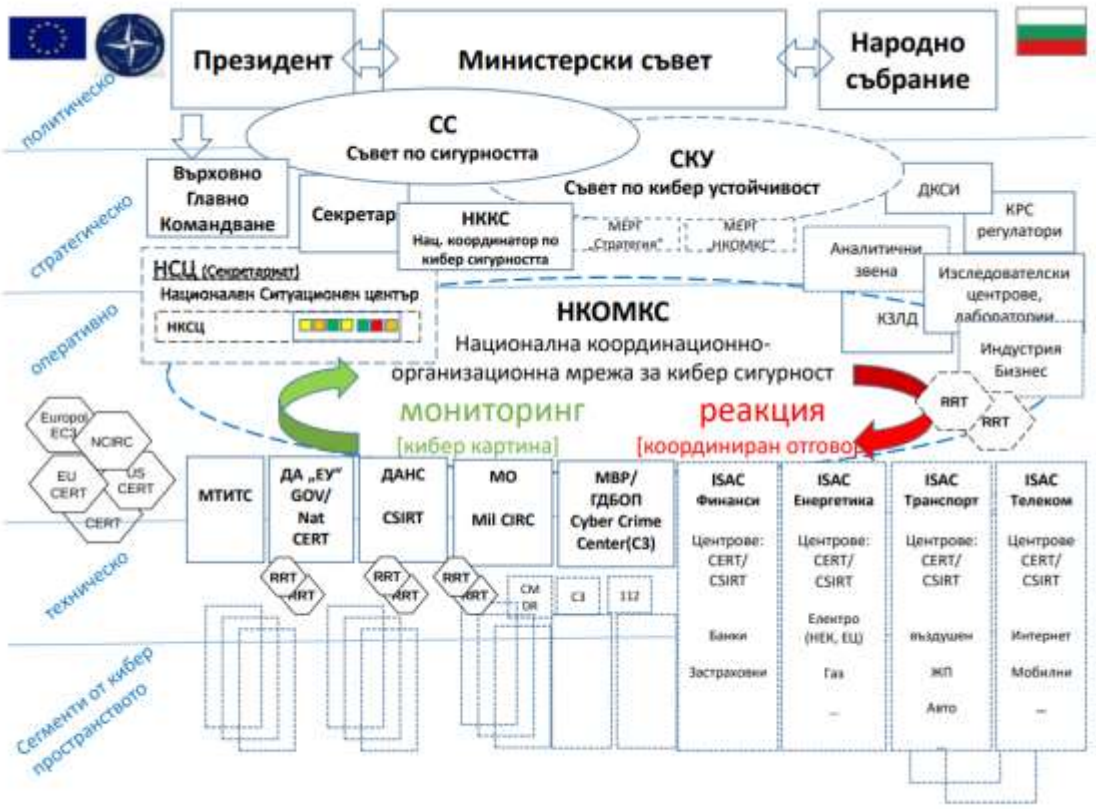
Набелязани са мерки и цели за развитие в няколко ключови области, като са детермининари основните фактори за успешното им и ускорено постигане.

Засегнати са три основни последователни и надграждащи се фази – инициираща фаза, при която ще се целят кибер сигурни институции; втора фаза на развитие от капацитет към възможности за постигане на кибер устойчиви

институции и кибер сигурно общество; фаза три – зрялост на кибер стойчивото общество.

В стратегията пожелателно е засегната необходимостта и възможността за създаване на Национална координационно-организационна мрежа за кибер сигурност, Национален ситуационен център от Националната система за управление на кризи, Национален кибер ситуационен център, Оперативен център за кибер отрбана при Министерството на отбраната, Съвет по кибер устойчивост към Министерски съвет и други специализирани звена.

Представен и модел на националната система за кибер сигурност и устойчивост, в който всички заинтересовани страни, стейкхолъдъри, държавни органи, фирми и граждани ще взаимодействат правилно за посигане на набелязянати цели:



Фигура 2. Модел на националната системата за кибер сигурност и устойчивост.

За съжаление тази сложна плетеница от различни правителствени и частни субекти, които е необходимо по свой почин и на принципа на доброволно споделяне на информацията да постигнат заложените в стратегията цели е практически неприложима. Когато към това се добави и липсата на конкретно държавно финансиране в тази насока картината се влошава. Бизнеса от своя страна преследва приоритетно своите корпоративни интереси и реалното му ангажиране в тази национална стратегия е по-скоро немислимо. Единици са фирмите, които са готови да заделят от своя бюджет конкретни финансови ресурси за участие например в отраслов център за реакция при кибер инциденти/CERT/.

Качественото и навременно постигане на набелязаните в стратегията цели е по-скоро немислимо в обозримо бъдеще за публичната администрация в страната. Това най-вече се обуславя в липсата на целенасочена държавна политика в сферата на компютърно-информационната сигурност. Обществена тайна е, че служителите при звената за информационна поддръжка на отделните публични администрации са недостатъчно платени, некачествено и неточно обучени и слабо мотивирани.

Приетата през 2016 г. стратегия е по-скоро досаден ангажимент, от който висшето ръководство на страната е трябвало да се избави, за да бъдат поне формализирани поетите пред международните партньори и целия Европейски съюз интеграционни, икономически и обществено-политически ангажименти.

5.2 Безплатни антивирусни програми

В условията на ограничени бюджетни ресурси на регионално ниво е възможно възприемането на диференциран подход при избора и използването на антивирусни решения в държаваната администрация на страната. Широко използваното към момента антивирусно решение с наименование Microsoft Security Essentials познато и под името Security Center Endpoint Protection, което на практика се използва във всички правителствени организации в България,

като част от операционната система на Microsoft, е познато като крайно ненадеждно и неефективно. В сферата на информационната сигурност в световен мащаб е широко залегнало виждането, че това антивирусно решение е на дъното на почти всички съпоставяния на антивирусни продукти от всякакъв калибър. Липсата на „добра“ антивирусна програма, която да защитава крайните потребители от публичната администрация е една от най-честите причини за заразяването на компютри с вируси. През последните две-три години в страната, огромен брой компютърни заразявания с последващ Криптолокер и загуба /чрез криптиране/ на хиляди важни документи и други данни са в резултат на липсата или недостатъчната наличност на недеждно антивирусно решение.

В тази връзка е възможно въвеждането на единственото в света безплатно за корпоративни или лични нужди антивирусно решение на мултинационалната корпорация Comodo.

Продуктът Comodo Internet Security предлага относително надеждни нива на антивирусна защита, като притежава редица приемущества в сравнение с широко използваното към момента ненаджедно решение Microsoft Security Essentials. В лицензионните споразумения на това софтуерно приложение е отразено, че то може да бъде използвано без ограничения, както от крайни домашни потребители, така и от корпорации, организации и публични администрации от всякакъв калибър. Подобна стъпка би била правилна и навременна, като би повишила /дори и слабо/ нивото на компютърно-информационна сигурност на публичаната администрация в България и региона.

През последните две-три години редица водещи фирми, световни лидери в антивирусната защита, предоставят безплатни антивирусни решения за крайни интернет потребители. Фирмите Kaspersky, BitDefender, F-Secure, Simantec и други от техния калибър са публикували за свободно изтегляне

безплатни версии, осигуряващи надеждна кибер хигиена. Съгласно лицензионните споразумения, тези продукти е възможно да бъдат използвани от домашни потребители, като се изключва корпоративната употреба. Въпреки това, безплатните антивирусни решения на тези регионални лидери могат да обезпечат надеждно ниво на кибер защита за крайни некомерсиални интернет портребители, като част от цялостната картина на киберсигурността на публичната администрация в страната.

5.3 Използване на Линукс

Линукс базираните операционни системи са създадени и се поддържат от широк кръг лица, а най-често от общности, където всеки отделен участник може да одитира и коригира компютърния код, върху който е изградено програмното обезпечаване. Често екипите поддържащи конкретна линукс дистрибуция са хора от различни държави и дори континенти. За разлика от другите операционни системи, почти всички линукс дистрибуции са безплатни, като се отличават с високо ниво на защита от компютърни вируси и други кибер заплахи. Конвенционалните компютърни вируси за операционната система Windows са практически неизползваеми срещу която и да е Линукс система. Изключително редки са случаите на компрометиране на подобна компютърна система, използвана от краен интернет потребител. Само дузина са зловредните кодове, таргетиращи линукс операционните системи и дори след тяхното доставяне до атакуваната конфигурация, те имат ограничено и оскъдно практическо действие.

Докато широко използваната в публичната администрация по света операционна система Windows и нейния задължителен компонент Word са с обща цена около 400 /четиристотин/ български лева за базисно използване /без допълнителните програмни компоненти/ Линукс системите са напълно безплатни и предоставят значително по-високо ниво на защита, от гледна точна на компютърно-информационната сигурност.

Резистентността на линукс базираните опирационни системи към конвенционалните компютърни вируси е важна предпоставка за тяхното продължително и надеждно внедряване и употреба. RAT инструментите, криптолокъра и другите зловредни компютърни кодове практически не могат да афектират компютърна конфигурация, използваща каквато и да е Линукс базираната операционна система.

Друга ключова причина за използването на Линукс операционните системи е проблема с конфиденциалността. Широко известен е факта, че Windows тайно събира и изпраща на сървърите на компанията статистически данни за активността на потребителите, използвани от тях софутерни продукти, натискани клавиши, посещавани сайтове, извършени търсения и друга лична информация за крайните ползватели.

Всяко звено от публичната администрация в страната е възможно значително ще повиши своята кибер резистентност при въвеждане в експлоатация за крайните потребители на Линукс базирана операционна система, особено ако компютърната конфигурация е свързана към интернет пространството. Това обстоятелство се улеснява и от все повече позиционирането на различните услуги в онлайн среда. Множество приложения, имейл комуникация, чат програми и други важни за бизнеса и администрацията приложения са интернет или мрежово базирани и тяхното достъпване е възможно само с използането на интернет браузър.

ЗАКЛЮЧЕНИЕ

В настоящата магистърска теза са описани основните заплахи за компютърно-информационната сигурност на публичната администрация в регионален и световен мащаб. Засегнати са основните похвати използвани най-често от външни за организацията влияния и лица, които се използват за осъществяване на нерегламентиран достъп до компютърни мрежи и друга критична онлайн инфраструктура.

Чрез частично представяне на някои от най-значимите и обществено известни кибер инциденти в страната, региона и света е проведен опит за обзор и фиксиране на състоянието на киберсигурността на публичната администрация в България към 2018 г.

Множеството хакерски похвати, хилядите компютърни вируси, ботнет мрежи, дейности на хакерски групи, тайни правителствени кибер армии и отделни индивиди, оказват своето деструктивно влияние върху цялостната картина на киберсигурността във всичките и аспекти.

Според изследване на Обединените нации от 2016 г., налично на адрес https://publicadministration.un.org/egovkb/en-us/Data-Center България е поставена на 52-то място от 192 държави /след Бразилия и преди Коста Рика/ според индекса на развитие на електронното правителство и нивото на дигитализация в страната. По показателите в същото изследване за предходни години се наблюдава стабилна тенденция, страната ни да повишава и подобрява своята обща резистентност на кибер заплахи, както и да затвърждава поетите евроатлантически и европейски ангажименти за дигитализиране на публичната администрация.

Визираните в настоящата теза компютърно-информационни инциденти обаче са категоричен индикатор на нивото на киберсигурността в страната и региона. През последото десетилетие в почти всички отрасли на публичната

администрация в България приоритетно се въвежда дигитална инфраструктура по почина на обществените поръчки. Това е непреодолимо законово изискване, което за съжаление носи редица отрицателни негативи върху цялостното състояние на киберсигурността. След избор на фирма изпълнител за доставка и въвеждане в експлоатация на нова компютърна техника, софтуер или конкретна виртуална услуга се пристъпва към нейното имплементиране. Това се осъществява от външни за организацията фирми, които настройват заплатеното одобурдване и първоначално го конфигурират за експлоатация. Изключително рядко се провеждат независими тестове за оценка на така въведеното в действие оборудване и нерегулярно се обновяват към новите версии отделните мрежови или други дигитални ресурси. В начилните отдели за поддръжка на тази техника липсват качествено и надеждно обучен персонал, който планово и регулярно да преглежда и анализира множеството хронологични събития в служебната компютърна мрежа. Не се осъществява мониторинг на логове от операционни системи, уеб сървъри, домейн контролери, защитни стени и друга критична кибер инфраструктура. Рядко действащата техника и софтуер се донастройват и специфично конфигурират за нуждите само и единствено на конкретната единица на публичната администрация. Служители и администратори от IT отделите използват едни и същи, кратки и ненадеждни пароли и ключове за достъп до конфиденциална информация. В страната са налични цели местни администрации, чиито компютърни конфигурации функционират без надлежно лицензирани операционни системи и допълнително програмно осигуряване. Кибер хигиената за отговорно сърфиране в интернет пространството, игнориране на съмнителни съобщения от неизвестен източник, неизползване на служебна техника за сваляне на нелицензирани филми, музика и софутер, за много представители на публичаната администрация са непознати понятия.

Приетата през 2016 г. Национална стратегия за киберсигурност на страната е отчаян опит на държавно ниво за впрягане на администрация, бизнес и академия, за постигане на базисни нива на информационна сигурност в

страната и надграждане нивото на дигитализацията на обеществото за постигане на кибер устойчива България 2020.

Към 2018 г. нивото на киберсигурност на публичната администрация в страната може да бъде определено като незадоволително, а тенденциите в негоото развитие са тревожни. Това най-вече се обуславя от липсата на ясна държавна и политическа воля в посока инвестиции, иновации и дигитализиране на обществения живот. Поради нестабилната обществено-политическа и социално-икономическа картина в страната, хиляди млади и изключително надарени специалисти в сферата на компютърно-информационната сигурност предпочетоха да работят за частни корпорации в Европа и САЩ, лишавайки България от надежден човешки потенциал.

Предизвикателства пред страната през следващите години ще бъдат и изключително сложните политически и обществени промени в европейски и световен мащаб, произтичащи от провеждщите се съвременни кибервойни, като част от т. нар. хибридни войни. В тази връзка, компютърно-информационната структура на цялата държава е под сериозна заплаха от евентулни кибератаки, подобна на естонската от 2007 г. Предвид незадоволителното ниво на киберсигурност, България за съжаление е лесна мишена за финансово или политически мотивирана хакерска групировка или кибер армия, като последиците от евентуална мащабна кибер атака вероятно ще бъдат пагубни.

В настоящата магистърска теза бяха засегнати основните заплахи за киберсигурността на публичната администрация, фиксирания бяха значими компютърно-информационни инциденти и пропуски при изграждане на важни публични сайтове, и бяха посочени бъдещи предизвикателства в тази насока, с което считам, че целта на магистърската теза е постигната!

ИЗПОЛЗВАНА ЛИТЕРАТУРА И ИЗТОЧНИЦИ

https://www.wikipedia.org/ - свободна, уеб-базирана енциклопедия;

http://thehackernews.com/ - новинарски сайт за компютърно-информационни инциденти и новости;

http://krebsonsecurity.com/ - новинарски сайт/блог на Брайън Кребс – изследовател на деструктивни влияния, процеси и инциденти в киберпространството;

http://www.wired.com/ - новинарски сайт за компютърно-информационни инциденти и новости;

https://securelist.com/ - новинарски сайт/блог на световно известната руска антивирусна компания Касперски;

http://www.cybercrime.bg/ - сайт на отдел „Киберпрестъпност“ при ГДБОП-МВР;

http://www.zone-h.org/ - информационна платформа с публикувани deface на интернет сайтове;