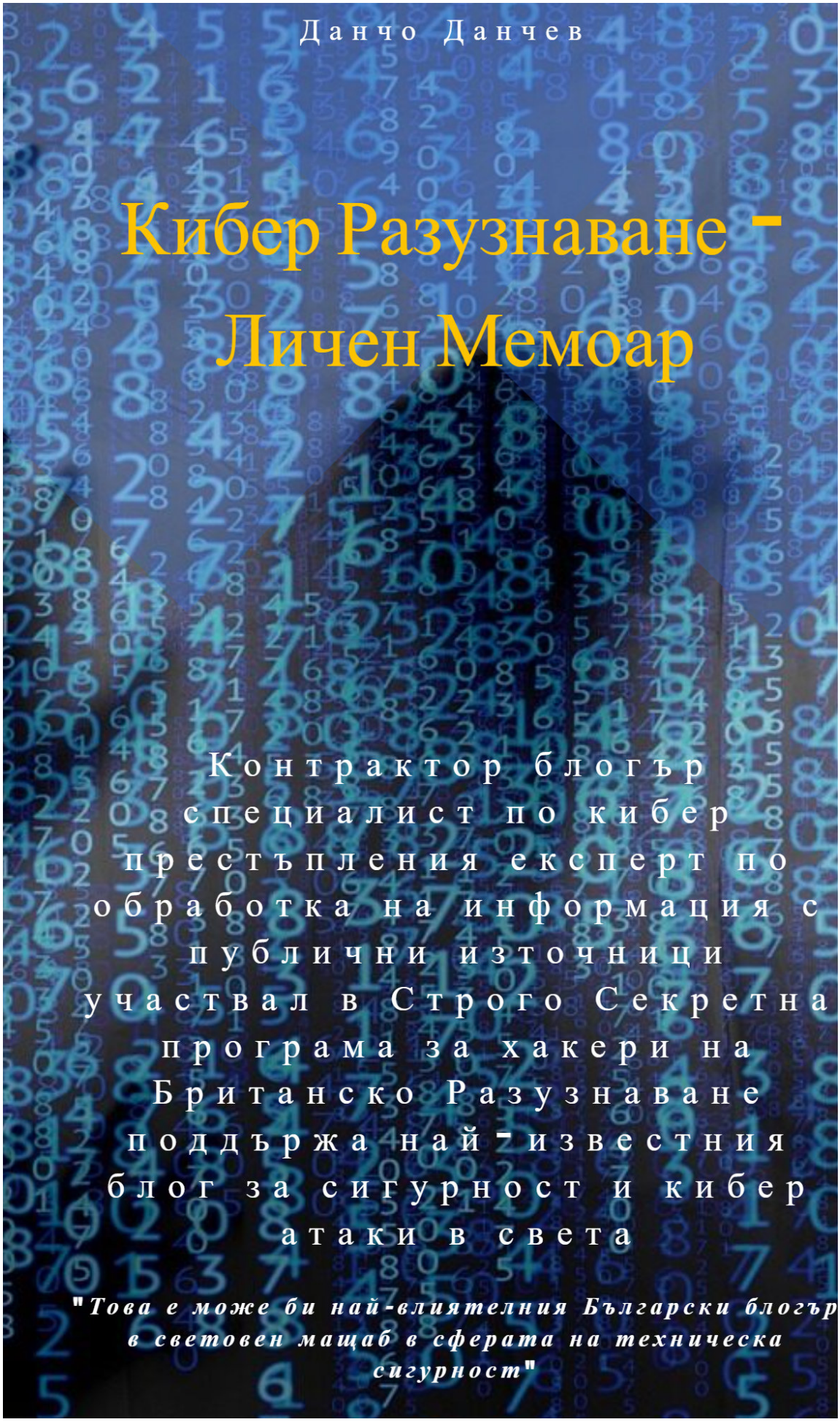


https://ddanchev.blogspot.com Email: dancho.danchev@hush.com

Table of Contents

Съдържание

Във второто издание на моя мемоар "Кибер Разузнаване" ще откриете следната информация и бонус съдържание в следните категорий:

- Преведени на Български интервюта който съм взимал от специалисти от индустрията по информационна сигурност и хора от Сцената по сигурност и хакерство
- Голям избор от лични и непубликувани снимки от конференций и събития както и на моята лаборатория за изледване на кибер атаките и кибер заплахите
- Две интервюта с мен който съм давал на различни онлайн портали
- Компилация от учебни материали в сферата на залавянето и проследяването на кибер престъпници който съм правил и проучвал през годините
- Интересни коментари и преживявания от различни конференции за сигурност
- Историй и преживявания в Astalavista.com
- Историй и преживявания като хакер ентусиаст през 90-те

Предговор

Скъпи читатели,

Това е Данчо и за мен е удоволствие и чест да ви представя моята лична електронна книга, включваща мемоари на хартиен носител и аудио книга която сигурно вече слушате, която има за цел да разкаже подробно моята история като хакерски ентусиаст от 90-те години до наши дни, когато съм един от най-популярните блогъри по сигурността в света разузнавателен анализатор и изследовател на киберпрестъпленията в международен план, където в момента ръководя едно от най-популярните издания за сигурност в индустрията за сигурност, което е моето лично - Блогът на Данчо Данчев - Умствени потоци от знания за информационната сигурност издание, което е успяло да привлече приблизително 5,6 млн. прегледа от първоначалното си стартиране през декември 2005 г., когато учех в Холандия и бях зает с работата и управлението на небезизвестния портал Astalavista, докато бях зает като управляващ директор на портала, където бях зает да отговарям за цялото съдържание и за привличането на нови

рекламодатели.

Кибер Разузнаване е процес на откриване и анализ на информация, която може да се използва в кибернетични цели. Това става чрез сканиране на мрежи, събиране на данни, анализ на тях и генерирането на доклад.Кибернетичното разузнаване е практика за наблюдение и анализ на онлайн активността с цел установяване на злонамерени намерения. То обхваща широк спектър от дейности - от идентифициране и проследяване на кибератаки до разкриване на уязвимости в ИТ инфраструктурата, както и от защитни мерки като тестване за проникване до проактивни изследвания на нововъзникващи заплахи.

Използването на киберразузнаването може да бъде също толкова важно, колкото и традиционните практики за събиране на разузнавателна информация. С развитието на интернет и разширяването на технологичните възможности се увеличават и начините, по които могат да се извършват кибератаки. За организациите, които не са подготвени, последствията могат да бъдат значителни. Киберразузнаването е съществена част от стратегията за готовност за сигурност на всяка организация. Чрез наблюдение на онлайн активността за злонамерени намерения то дава възможност на организациите да идентифицират и предприемат превантивни действия, преди да се стигне до пробив. Освен това то им позволява да идентифицират потенциални кибератаки и да предотвратят по-нататъшни атаки, преди да имат възможност да успеят.

Това е една от основните причина да започна и да продължа да се занимавам с такъв тип разузнаване на кибер заплахи като използвам публични източници на информация.

След успешна кариера на хакерски ентусиаст през 90-те години и успешно управление и функциониране на един от водещите световни портали за хакери и експерти по сигурността, който е Astalavista, за период от три години около 2003-2006 г., когато първоначално реших да стартирам една от водещите публикации в индустрията за сигурност, която е моят личен блог след което успях да постигна успешна кариера като независим консултант в света на блоговете за сигурност, изследванията на киберпрестъпността и разузнаването на заплахите, което ме накара да посетя няколко конференции само с покани, включително да представя събитие на неразкрито място, включително действително да привлека и задържа приблизително 6 милиона показвания на страници, което не е лошо за човек, който работи по отношение на управлението и поддържането на личния ми блог за период от 12 години.

Някои от предишните ми позиций през 90-те като хакер ентусиаст са позиций като член на WarIndustries модератор на списъка в BlackCode Ravers съдружник Black Sun Research Facility модератор на списъка Съдружник на софтуер на DiamondCS Trojan Defense съдружник в LockDownCorp съдружник в HelpNetSecurity консултант по сигурността за Frame4 Security Systems сътрудник на WindowSecurity.com на TechGenix управляващ директор - Astalavista Security Group консултант по сигурността - Wandera Анализатор на заплахи на GroupSense консултант по сигурността - KCS Group Europe анализатор на информация с публични източници на Treadstone71 блогър по сигурността - Armadillo Phone блогър по сигурността за ZDNet блогър по сигурността на Webroot.

Сред основните причини да напиша този личен мемоар от 600 страници е да дам възможност на колеги изследователи и експерти по сигурността, включително и на широката общественост, да се запознаят със задълбочен преглед на личния ми опит в сферата на сигурността като тийнейджър хакер ентусиаст през 90-те години на миналия век, днес най-популярният и често цитиран блогър в сферата на сигурността, анализатор на разузнаването на заплахите и изследовател на киберпрестъпността в международен план, както и да представя разнообразен набор от висококачествени и никога непубликувани и обсъждани преди това казуси и обогатена техническа информация и OSINT данни за настоящи и нови тенденции в кибератаките.

Основната цел на книгата ще бъде да позиционира мемоарите ми като един от най-популярните и често цитирани лични разкази за хакерството и сцената на сигурността около 90-те години през призмата на бившия ми тийнейджър хакер до наши дни по отношение на различни високопоставени и напреднали национални актьори и

злонамерени и измамнически кампании за кибератаки, като крайната цел е да се обсъди задълбочено моят опит в областта на събирането на разузнавателна информация за заплахи в областта на сигурността и изследването на киберпрестъпността през последното десетилетие.

Написах тази книга по две основни причини: Първо, искам да разпространя информация за опасностите от APT атаки. Вярвам, че ако хората са по-наясно със заплахата, те ще бъдат по-добре подготвени да се защитят. Второ, искам да предоставя технически насоки за това как да използват инструментите за сигурност в ежедневието си. Важно е хората да знаят как да се предпазват от сложни кибератаки.

Има многобройни начини, по които хората могат да станат мишена на APT. Един от често срещаните методи е да се подмами човек да кликне върху злонамерена връзка или да се изпрати подозрителен прикачен файл към електронна поща. Тези атаки могат да бъдат много сложни и изискват напреднали познания в областта на компютърната сигурност.

Смятам, че е важно всички, включително предприятията, правителствата и дори обикновените хора, да разберат как да се борят срещу тези заплахи.

Приятно четене!

Представяне

Добре дошли в прекрасния свят на изследването на киберпрестъпленията, събирането на информация за интернет и киберзаплахите с отворен код и блоговете за сигурност във второто издание на личния мемоар на Данчо Данчев "Кибер Разузнаване".

Това е Данчо Данчев и с гордост съобщавам, че най-накрая успях да публикувам второто издание на личните си мемоари, които в общи линии описват историята ми като хакерски ентусиаст през 90-те години до днес, когато съм международно признат изследовател на киберпрестъпността, блогър по сигурността и анализатор на събирането на информация за заплахите, който ръководи едно от най-популярните издания в сферата на сигурността, което е мой личен блог от декември 2005 г., когато учех в Холандия, докато работех по управлението на портала Astalavista, известен още като The Underground, където бях нает като управляващ директор и където отговарях основно за управлението на разделите Security Guide и Security News, включително за изготвянето на бюлетина за сигурност, в който всеки месец публикувах ексклузивно и непубликувано досега интервю за сигурността с ключова фигура от сцената и индустрията за сигурност.

За мен е удоволствие и чест да ви представя моята лична електронна книга, включително мемоарна книга на хартиен носител, която има за цел подробно да разкаже моята история като хакерски ентусиаст около 90-те години на миналия век до наши дни, където съм един от най-популярните блогъри в областта на сигурността, анализатор на разузнавателни заплахи и изследовател на киберпрестъпления в международен план, където в момента ръководя едно от най-популярните издания в областта на сигурността в индустрията за сигурност, което е моето лично - Блогът на Данчо Данчев - “Умствени

потоци от знания за информационната сигурност” издание, което успя да привлече около 5.6 млн. прегледа на страници от първоначалното му стартиране през декември 2005 г., когато учех в Холандия и бях зает да работя и управлявам небезизвестния портал Astalavista, докато бях зает да изпълнявам функциите на управляващ директор на портала, където бях зает да отговарям за цялото съдържание и за привличането на нови рекламодатели.

Основната цел на моя мемоар е да представя моята история в света на изследването на кибер атаки и обработка на информация с публични източници за кибер атаки през последните 10 години и да разкажа моята история като хакер специалист и като днешния световно известен специалнист в сферата на анализ и разпространение на информация за кибер атаки в световен мащаб.

В първата глава ще разкажа и ще направя представяне на книгата и ще споделя различна информация за другите глави от книгата и ще представя и ще дискутирам част от моята биография с цел да запозная читателя с моя опит в индустрията и да разкажа част от мойте преживявания в индустрията.

Изследването на кибератаки е област, която се фокусира върху анализа на кибератаки. За организациите е важно да разберат какво представлява кибератаката, как работи и как могат да я предотвратят. Много хора са загрижени за кибератаките, поради което интересът към тази област нараства.

Хората, които работят в тази област, изучават кибератаките и се опитват да ги разберат по-добре. Те могат да използват компютри и технологии, за да анализират данни от различни източници, за да научат повече за кибератаките. Те могат също така да пишат статии или книги за кибератаките и да споделят знанията си с обществеността.

Работата в тази област има много предимства. Тя може да помогне на организациите да се предпазят от кибератаки. Тя може също така да привлече нови хора в организацията и да повиши осведомеността по въпросите на киберсигурността сред широката общественост.

Моята биография:

Данчо Данчев е експерт в областта на борбата с киберпрестъпността и събирането на разузнавателна информация за заплахите, като активно развива собствена методология за обработка на разузнавателна информация за заплахите, довела до успешен набор от стотици висококачествени анализи и изследователски статии, публикувани във водещия блог за разузнаване на заплахите в индустрията - Zero Day на ZDNet, Dancho Danchev's Mind Streams of Information Security Knowledge и Webroot's ThreatBlog, като негови изследвания са публикувани в Techmeme, ZDNet, CNN, PCWorld, SCMagazine, The Register, NYTimes, CNET, ComputerWorld, H+Magazine, а в момента изготвя разузнавателна информация за заплахи във водещия в индустрията блог за разузнавателна информация за заплахи - Dancho Danchev's - Mind Streams of Information Security Knowledge, който е получил над 5. 6 млн. прегледа на страници от декември 2005 г. насам и в момента се счита за една от най-популярните публикации в индустрията за сигурност.

Основните му постижения включват:
- Представен в GCHQ с проекта Honeynet
- SCMagazine Кого да следвате в Twitter за 2011 г.
- Участие в строго секретна програма на GCHQ, наречена "Прекрасен кон"
- Идентифицирана е основна жертва на атаката на SolarWinds - PaloAltoNetworks
- Открит зловреден софтуер в уебсайта на Flashpoint
- Проследил, наблюдавал и профилирал ботнета Koobface и разкрил един от операторите на ботнета
- Два пъти попадна в Slashdot
- Моят личен блог има 5,6 милиона прегледа на страници от декември 2005 г. насам
- Старият ми акаунт в Twitter има 11 000 последователи

- Средно 7000 RSS читатели на моя блог
- Имам собствен винил "Blue Sabbath Black Cheer / Griefer - We Hate You Dancho Danchev", направен от канадски художник
- В момента управлявам Astalavista.box.sk
- Дадох интервю за DW относно ботнета Koobface
- Дадох интервю за NYTimes относно ботнета Koobface
- Дадох интервю за руския OSINT
- Посочен като основен конкурент от Taia Global на Джефри Кар
- Представен в GCHQ
- Представен в Интерпол
- Представен на InfoSec
- Представен в CyberCamp
- Представен на RSA Europe

За мен е удоволствие и чест да ви представя моята лична електронна книга, включително мемоарна книга на хартиен носител, която има за цел подробно да разкаже моята история като хакерски ентусиаст около 90-те години на миналия век до наши дни, където съм един от най-популярните блогъри в областта на сигурността, анализатор на разузнавателни заплахи и изследовател на киберпрестъпления в международен план, където в момента ръководя едно от най-популярните издания в областта на сигурността в индустрията за сигурност, което е моето лично - Блогът на Данчо Данчев - “Умствени потоци от знания за информационната сигурност” издание, което успя да привлече около 5.6 млн. прегледа на страници от първоначалното му стартиране през декември 2005 г., когато учех в Холандия и бях зает да работя и управлявам небезизвестния портал https://astalavista.com, докато бях зает да изпълнявам функциите на управляващ директор на портала, където бях зает да отговарям за цялото съдържание и за привличането на нови рекламодатели.

Основната цел на моя мемоар е да преставя моята история в света на изследването на кибер атаки и обработка на информация с публични източници за кибер атаки през последните 10 години и да разкажа моята история като хакер специалист и като днешния световно известен специалнист в сферата на анализ и разпространение на информация за кибер атаки в световен мащаб. В първата глава ще разкажа и ще направя представяне на книгата и ще споделя различна информация за другите глави от книгата и ще представя и ще дискутирам част от моята биография с цел да запозная читателя с моя опит в индустрията и да разкажа част от мойте преживявания в индустрията.

Приятно четене!

Коментари от Колеги

"*Работя в сферата на сигурността от много години и през голяма част от тях следя отличната изследователска работа на Данчо по идентифициране на киберпрестъпници и комплексен анализ на съвременни атаки с високотехнологичен зловреден софтуер. Данчо е изключително добре познат в сектора за сигурност с работата, която е свършил и продължава да върши. Когато имахме възможност да си сътрудничим с Данчо в Webroot, не се поколебахме. Данчо е доказал, че непрекъснато постига резултати за нас, а работата му е просто феноменална. Очаквам с нетърпение да работя с Данчо още дълги години.*"

- Жак Еразъм, клиент на Данчо

"*Данчо е опитен изследовател, с когото имах удоволствието да работя по няколко хакерски разследвания за клиенти на Taia Global. Смятам, че Данчо е един от най-добрите и най-проницателни изследователи, работещи в областта на InfoSec днес.*"
- Джефри Кар, главен изпълнителен директор на Taia Global, Inc., управлявал Данчо индиректно в Споразумение за неразкриване на информация

"*Данчо Данчев има поглед върху киберпрестъпната общност. Мога да се сетя за няколко души, които имат неговия опит, умения и разбиране, когато става въпрос за киберразузнаване и разбиране на киберзаплахите. Не мога да препоръчам Данчо.*"

- Ланс Шпицнер, президент на The Honeynet Project, работил с Данчо в Споразумение за неразкриване на информация

"*Данчо е един от онези изключително редки професионалисти в областта на сигурността, които имат не само усет за разкриване на корените на причина за дадена атака и умението да я изследва от различни ъгли, но и да обясни откритията си по начин, който които имат значимо и пряко въздействие върху тези, които са натоварени със защитата срещу такива атаки. Възхищавам се на дълбочината на неговия анализ и упоритата му решимост да проследи кои са престъпните оператори въпреки опасностите, на които може да бъде изложен. Данчо получава два палеца нагоре от мен и бих го наел на мига, ако някога стигне до САЩ. Междувременно ще продължа да следя изследванията му, да чета блоговете му и да търся с нетърпение да си сътруднича с него в бъдещи разследвания на киберпрестъпления.*"

- Гюнтер Олман, вицепрезидент на отдел "Изследвания", Damballa, Inc. е работил в друга компания, когато работи с Данчо в Споразумение за неразкриване на информация

"*Данчо е изключителен професионалист в областта на информационната сигурност; той непрекъснато прави всичко възможно за клиентите и общността по сигурността. Неговите познания и анализи в основни области като анализ на разузнавателни заплахи, контраразузнаване на киберпрестъпления и изследване на конкурентното разузнаване са изключителни. Той се справя с лекота и с най-трудната задача - да предаде това в разбираема и смислена за общността форма. Работата с Данчо в продължение на няколко години е изключително продуктивна и ползотворна.*"

- Джарт Армин, редактор, HostExploit, е бил в друга компания, когато е работил с Данчо в Споразумение за неразкриване на информация

"*За първи път се запознах с Данчо, когато беше току-що завършил колеж, но вече с огромни познания за въпросите на информационната сигурност. Той стана един от експертите в Клиниката по сигурност на ITsecurity.com, сайт, който основах и издавах по онова време; и той с готовност даваше безплатна помощ и съвети за сигурността на посетителите на сайта. Оттогава наблюдавам как кариерата и*

знанията му се развиват скокообразно, докато той вече е сега, без никакво съмнение, е един от водещите световни експерти в сенчестия свят на киберпрестъпността."

- Кевин Таунсенд, основател/редактор на ITsecurity.com, работил директно с Данчо в ITsecurity.com

"*Докато възстановявахме екипа по сигурността на сайта и измамите във водещ онлайн уебсайт, заплахите и бързата еволюция в в областта на онлайн сигурността изискваха от мен да навляза бързо и с повече от малко дълбочина и широта на разбирането на настоящите тенденции и рискове в сферата на киберсигурността. След като прекарах доста време в изграждане на информационна мрежа от най-съществените, релевантни и полезни източници, в разговорите за активност и актуализации се появи една обща нишка - "Данчо Данчев".*

Докато прелиствах публикациите за сигурност, списанията за киберсигурност, блоговете и сайтовете на доставчиците на услуги за сигурност, продължавах да виждам, че Данчо е цитиран и признат като изследователя и експерта по сигурността, който е "разкрил историята" или е "предупредил потребителите за нвуязвимостите", или е "предупредил общността за векторите на заплаха" за важни събития. Данчо доброволно споделяше критична информация за това, което са замислили измамниците, и беше безценен и много ценен източник. Страстта на Данчо към работата му се изразява в искреното му желание да потуши дейността на "лошите момчета" и да сподели колкото се може повече полезна информация. Горещо препоръчвам Данчо на всяка организация, която търси първокласен експерт и страстен популяризатор на практиките в областта на онлайн сигурността."

- Крис Дънкан, директор "Операции с клиенти", CareerBuilder.com, е работил в друга компания, когато е работил с Данчо в ZDNet

Благодарности

Бих желал да благодаря на следните колеги и приятели от индустрията за тяхното приятелство и помощ през годините от гледна точка на борбата с престъпността и споделянето на информация за кибер атаки в глобале мащаб.

- Иван Шмид - за това, че е най-якият шеф на света и че ме прие в един от най-популярните уебсайтове за хакери в мрежата през 2003-2006 г., където имах привилегията да работя като управляващ директор на портала заедно с бившата ми приятелка от 90-те години - Йорданка Илиева, докато учех в Холандия.

- Паскал Митнер - за това, че беше вторият най-готин шеф в света, с когото никога не съм имал възможност да се запозная лично, но който вършеше работата ми както трябва и където всъщност ми плащаха за това, че върша работата си

- Гари Скот - с когото имах привилегията да обменям данни и информация през 90-те години по пътя ми към изготвянето на висококачествен бюлетин и всъщност разузнаване на заплахите за ScanSafe по това време, която по-късно беше придобита от Cisco

- Гади Еврон - за това, че запази хладнокръвие и дух и всъщност ме вдъхнови да правя своите изследвания, докато бях зает да гледам една от неговите лични презентации на голямо събитие в областта на сигурността през 90-те години, на което той имаше възможност да докладва

- Пол Фъргюсън - за това, че запази хладнокръвие и дух и че всъщност ме вдъхнови да правя своите изследвания в областта на изследванията на киберпрестъпността чрез ежедневните му публикации в личния му блог

- Алекс Екълбъри - за това, че запази спокойствие и корпоративност и всъщност ме вдъхнови да правя изследвания в областта на киберпрестъпността, както и за това, че управлява и поддържа Sunbelt Software, който силно ме вдъхнови да правя изследвания в областта на киберпрестъпността

- Марк Раш - за това, че запази спокойствие и ме вдъхнови да се занимавам с изследвания в областта на киберпрестъпността с рубриката си в SecurityFocus

- Джейми Райден - за това, че е добър професионалист и човек, на когото имам доверие и когото познавам, и за това, че ми помогна в няколко случая да направя изследването си и да продължа да го правя

- Стив Санторели - за това, че лично ме покани да присъствам на събитие само с покани, за това, че поддържа връзка с мен, за това, че запазва спокойствие и за това, че лично ми написа лична препоръка въз основа на моите изследвания и опит в индустрията

- Джеймс Маккуейд - за това, че беше сред малкото хора, които действително повишиха осведомеността за съществуването на Руската бизнес мрежа, и за това, че продължи да предоставя високопоставена и ценна разузнавателна информация за заплахите в различни списъци за кореспонденция

- Джефри Бардин - за това, че ме покани да се присъединя към Treadstone71 като анализатор на OSINT и ми позволи да работя с него по няколко проекта, в рамките на които спечелих необходимата сума, за да платя някои от сметките си и да инвестирам правилно в няколко проекта, включително за пускането на един от първите търговски електронни магазини за разузнавателни продукти

- Джефри Кар - за това, че запази хладнокръвие и изрази личната си благодарност и коментира моите изследвания в контекста на "продължавам да го правя". - Кен Дънам - за това, че запази хладнокръвие и за това, че води високопоставен и популярен пощенски списък за тенденциите в областта на сигурността и актуална техническа информация за настоящите и текущите тенденции в областта на кибератаките

- Джарт Армит - за това, че запази хладнокръвие и че се обърна към мен няколко пъти, за да ми каже "здравей" и "продължавай с добрата работа"

- Робърт Макмилън - за това, че е истински професионалист и добър приятел, с когото имах привилегията да говоря и общувам многократно

- Роб Лемос - за това, че е добър професионалист и човек, когото познавам, с когото съм работил и чиято работа съм следил в миналото

- Грег Кийзър - за това, че е истински професионалист и че всъщност си направи труда да ме цитира и да се позове на мен в няколко статии по многобройни поводи - Гари Уорнър - за това, че е истински професионалист и че винаги е на първа линия в борбата с лошите момчета и киберпрестъпността в международен план

- Хорхе Миерес - за това, че е истински професионалист в областта на разузнаването на заплахите и изследванията на киберпрестъпността, че запазва спокойствие по отношение на новите изследвания и че предлага уникален и задълбочен преглед и перспектива за нови и нови тенденции и заплахи в областта на кибератаките

- Маркус Сакс - за това, че запазва спокойствие и е истински професионалист, чиято работа съм следил в миналото

- Гюнтер Олман - за това, че е истински професионалист и добър приятел, с когото всъщност имах възможност да се срещна на RSA Europe 2012 Светът е малък и безкраен и ние определено можем да го направим по-добър, като вършим работата си, следвайки основната методология, че "OSINT, проведен днес, е спестен някъде долар на данъкоплатеца".

Начална Кариера - 90-те

z

Историята отвътре на живота на бившия български хакер Данчо Данчев

Беше привилегия през декември 2005 г., когато първоначално стартирах личния си блог Dancho Danchev'Blog - Mind Streams of Information Security Knowledge, който бързо се превърна в една от най-популярните публикации в сферата на сигурността до днес, когато успях да привлека около 5. 6 млн. прегледа през последното десетилетие и където успях да привлека и задържа висококачествена аудитория, която основно се състои от изследователи в областта на сигурността, членове на разузнавателната общност на САЩ, включително и на правоохранителните органи на САЩ, включително и видни представители на индустрията за сигурност, където моят личен блог се превърна в ежедневно четиво с цел създаване на основите на успешна комуникационна платформа за повечето от изследванията, които публикувам онлайн. След приблизително десет години активна дейност в блоговете за сигурност, OSINT анализи и изследвания, включително изследвания и анализи на разузнавателни заплахи, успях да събера лоялна аудитория, която значително допринесе за броя на последователите ми в 11 000 души в Twitter, използвайки стария ми акаунт включително активното участие на стария ми акаунт в Twitter в строго секретна програма на GCHQ, известна като "Lovely Horse", в която имах привилегията да допринеса със знания и ноу-хау за проекта на разузнавателната общност на САЩ за използване на "Отворен код за сигурност", чиято крайна цел беше да се наблюдават хакери от висок ранг и сигурност експерти по отношение на достъпа до техните изследвания и знания.

Уважаеми читатели,

Това е Данчо и реших да споделя моята лична история от реалния живот около 90-те години, когато бях виден бивш български хакер по време на прословутата хакерска вълна през 90-те години, когато Astalavista.box.sk и Progenic. com бяха моите основни и ежедневно посещавани тип букмаркове, което значително ме провокира да продължа основно 20-годишната си кариера като специалист по информационна сигурност, днес водещ световен експерт в областта на изследването на киберпрестъпленията и събирането на информация за заплахите, който от декември 2005 г. поддържа едно от водещите и най-популярни издания в областта на сигурността, което е моят личен блог, който първоначално стартирах, докато работех като управляващ директор за Astalavista, който по онова време беше един от най-популярните и посещавани с голям трафик портали за информационна сигурност в света, където имах привилегията да работя като управляващ директор, докато учех в Нидерландия.

Искате ли да научите за моята истинска история като бивш български хакер през 90-те години? Интересувате ли се да научите повече за това как поставихме основите на

пазарния сегмент на техническото събиране на данни, включително и на днешния модерен пазарен сегмент на разузнаването на заплахи, и как ги изправихме на крака, използвайки информацията и знанията за данни, които бяха произведени и разпространени? Продължете да четете. Историята се развива в малък град в България през 90-те години в постсъветска и посткомунистическа страна, където модерните технологии започват бавно да навлизат и подтикват един местен хитрец да събере възможно най-много информация от мрежа от свързани компютри, известна като интернет, с цел да търси глобално господство чрез активен и постоянен обмен на информация с колеги от целия свят, включително изключително от САЩ и членове на U. S Security Industry the Scene and prominent members of the U.S. Intelligence Community including hundreds of independent contractors in a post and pre 9/11 World which is where Dancho Danchev originally started his career as a hacker enthusiast today's leading expert in the field of cybercrime research and threat intelligence gathering. Примерна лична снимка на родния град на Данчо Данчев в България - Троян.

Виртуално пространство

КИБЕРТЕРОРИЗМЪТ

ДОКОЛКО РЕАЛЕН Е ПРОБЛЕМЪТ?

ИНФОРМАЦИОННАТА ИКОНОМИКА, в която светът навлезе през последните 20 години, благоприятства развитието на модерните средства за комуникация, разбивайки междуконтиненталните и етнически граници, придавайки нови измерения на понятието информационно общество, а може би точното понятие е информационно-зависимо общество!

Тази статия се стреми да разгледа проблема за информационната война и кибертероризма, който неизменно я съпътства, от различни гледни точки. Тя ще отговори на следните въпроси – какво е кибертероризъм и каква е разликата между него и информационната война? Могат ли действията на информационната война и е кибертероризъм да предизвикат човешки жертви или икономически хаос и какви са възможните сценарии?

Развитието на електронната търговия, отварянето на военните, производствени и корпоративните мрежи, с цел увеличаване на производителността чрез въвеждане на мрежово-базираните комуникации, са основните причини за феноменалното развитие на киберпанди като US и водещ фактор за успеха на армията им. Информационната война като платформа за военни, разузнавателни, пропагандни и дори терористични действия се ползва още от създаването на телевизията, Интернет и първите спътници в космоса. Факторите благоприятстващи за това са :

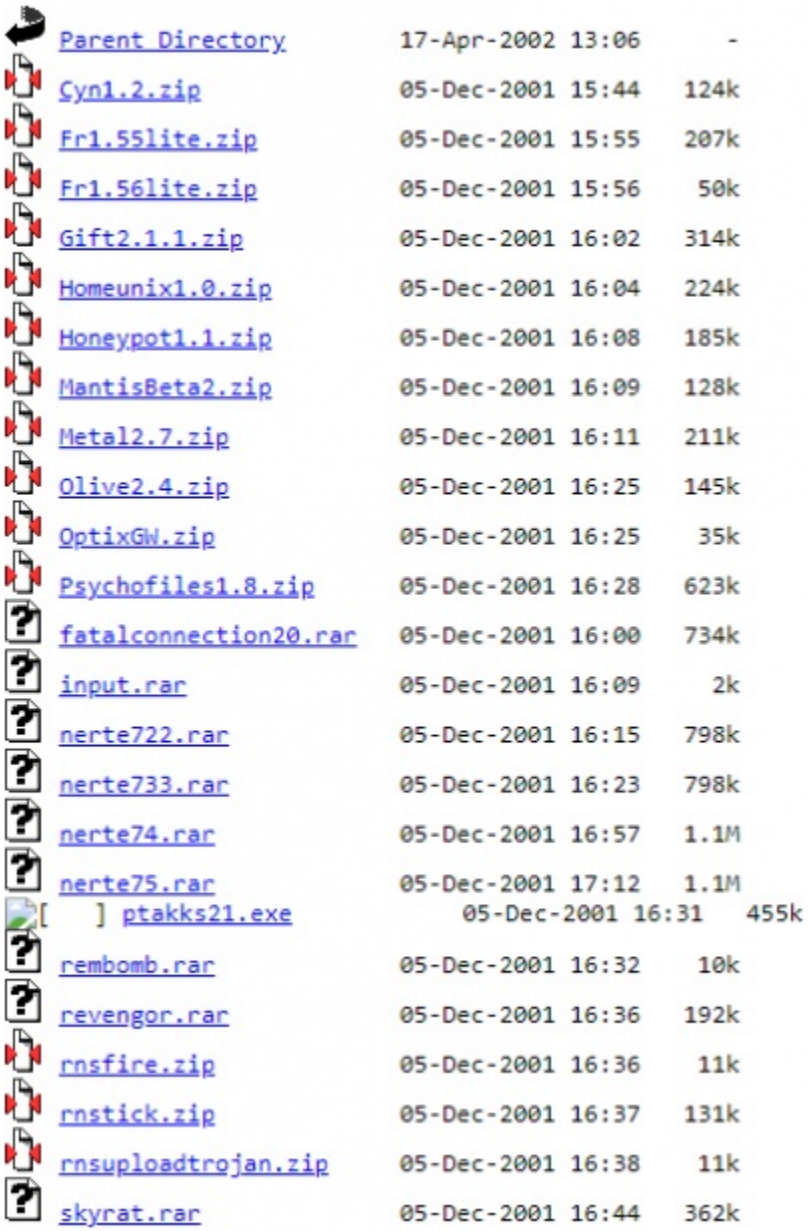
■ **Глобалната световна свързаност, скорост и интерактивност на пренасяната информация.** Докато по времето на Студената война ЦРУ и КГБ са разчитали основно на HUMINT (човешко разузнаване), информационната революция и глобализация допринесе за допълнителното развитие на SIGING (сигнално разузнаване), ELINT (е-разузнаване) и дори CYBERINT (киберразузнаване). Всеки от изброените типове се ползва и за офанзивни, и за защитни цели.

■ **Невиждани до преди 20 г.възможности за събиране и анализиране на разузнавателна информация и водене на военни действия.** Първият американски разузнавателен сателит – CORONA, изпращал събраните сателитни снимки на Съветския съюз чрез капсули, които се катапултирали и били прихващани в океана – процес, който днешните разузнавателни агенции едва ли биха искали да си спомнят. При постоянно намаляващите разходи за съхраняване на информация и при навлизането на новаторите както в публичния,

ДАНЧО ДАНЧЕВ, Astalavista.com
(dancho@astalavista.net) е независим консултант по информационна сигурност. Работи за Frame4 Security Systems (Холандия), а също като изпълнителен директор на Astalavista.com. Член е на ISECA.org – Асоциацията за информационна сигурност. Области, в които авторът има опит, са е-бизнес решения, анализ на злонамерен код и др.

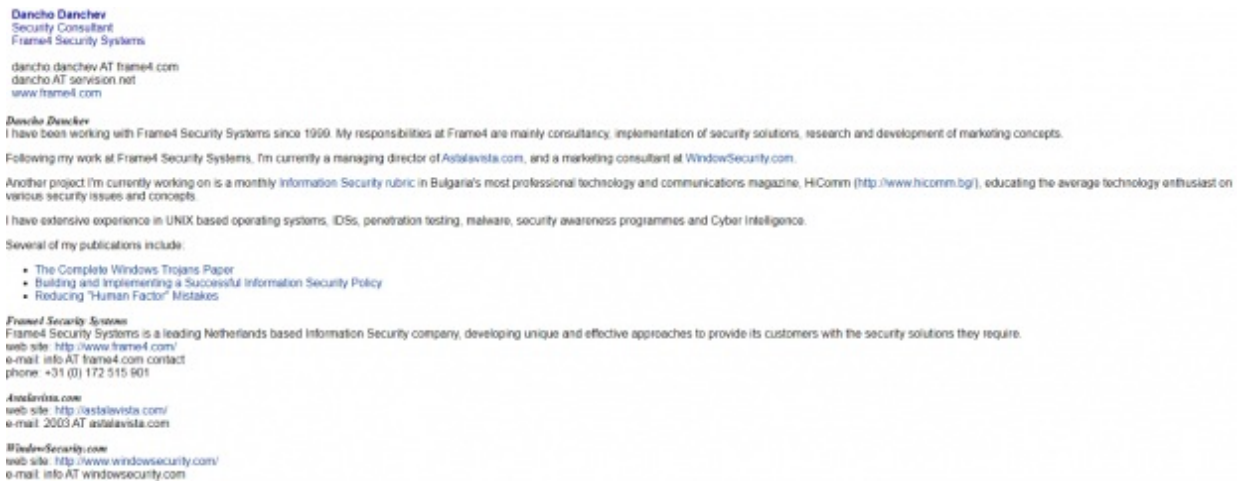
Когато бях в България по време на тийнейджърските си хакерски години, бях зает с работа на свободна практика като консултант по информационна сигурност, докато работех с международни портали за сигурност, където се занимавах с предлагане на съвети и практически препоръки за информационна сигурност и практически решения,

включително работата ми с CIO.bg, където веднъж допринесох със статия за кибертероризма и киберджихада, включително поредица от публикации за HiComm.bg, където водех популярен информационен сигурност и участва с няколко статии в няколко от броевете на списанието. На по-късен етап някак си реших да се занимавам с корпоративна дейност и по някакъв начин да намеря начин да навляза в комерсиалната индустрия за информационна сигурност с моите познания, като потенциално започнах да допринасям със знания и информация, използвайки личните си контакти в различни портали за информационна сигурност по пътя си към евентуална работа, за предпочитане като автор на блог за сигурност или журналист, което очевидно успях да направя, тъй като по това време активно допринасях със собствените си изследвания и знания в различни портали за h/c/p/a (хакерство/пробиване/разбиване/анархия).



По някое време Данчо решава да се обърне към основния оператор на един от любимите си уебсайтове за сигурност по това време - https://net-security.org с цел да допринесе със статия за новостартиралия им проект forbidden.net-security.org. Идеята му беше да допринесе със статия за сигурността за наскоро стартиралия им бюлетин, а въпросната статия беше доброто старо ръководство "Как да използваме троянски коне". В крайна сметка статията беше приета и Данчо се почувства горд от себе си, че е допринесъл за проекта и че статията му е публикувана, така че евентуално повече хора

да я прочетат и да му изпратят имейл с въпроси за троянските коне и за самата статия. Основният уебмастър на net-security.org по това време беше Берислав Кучан и проект все още остава един от любимите и най-популярните ежедневно посещавани уебсайтове за сигурност на Данчо. Примерна снимка на София, България. Снимка с любезното съдействие на Данчо ДанчевНа по-късен етап реших да установя работни взаимоотношения с Frame4 Security Systems, която е холандска компания, с цел написване на подобрена версия на оригиналния документ "Как да използваме троянски коне", който по-късно се превърна в "The Complete Windows Trojans Paper", който бързо се превърна в един от най-популярните и четени документи на Сцената за съвременните троянски коне и как да ги използваме и как да се предпазим от тях.



Dancho Danchev
Security Consultant
Frame4 Security Systems

dancho.danchev AT frame4.com
dancho AT servision.net
www.frame4.com

Dancho Danchev
I have been working with Frame4 Security Systems since 1999. My responsibilities at Frame4 are mainly consultancy, implementation of security solutions, research and development of marketing concepts.

Following my work at Frame4 Security Systems, I'm currently a managing director of Astalavista.com, and a marketing consultant at WindowSecurity.com.

Another project I'm currently working on is a monthly Information Security rubric in Bulgaria's most professional technology and communications magazine, HiComm (http://www.hicomm.bg/), educating the average technology enthusiast on various security issues and concepts.

I have extensive experience in UNIX based operating systems, IDSs, penetration testing, malware, security awareness programmes and Cyber Intelligence.

Several of my publications include:

- The Complete Windows Trojans Paper
- Building and Implementing a Successful Information Security Policy
- Reducing "Human Factor" Mistakes

Frame4 Security Systems
Frame4 Security Systems is a leading Netherlands based Information Security company, developing unique and effective approaches to provide its customers with the security solutions they require.
web site: http://www.frame4.com/
e-mail: info AT frame4.com contact
phone: +31 (0) 172 515 901

Astalavista.com
web site: http://astalavista.com/
e-mail: 2003 AT astalavista.com

WindowSecurity.com
web site: http://www.windowsecurity.com/
e-mail: info AT windowsecurity.com

Примерна лична снимка на моста Еразъм в Ротердам. Снимка с любезното съдействие на Данчо ДанчевС наближаването на края на лятото Данчо получава предложение да започне работа в местния офис на своя интернет доставчик (Internet Service Provider), който по това време е Digital Systems, на позицията офис асистент, където отговаря за запознаването на нови клиенти с предлаганите от интернет доставчика услуги и за обработката на фактури. Сред основните предимства на работата в местния офис на доставчика на интернет услуги е действителната честотна лента, до която има достъп, позволяваща му да влиза в интернет без никакви ограничения, които той използва, за да посещава някои от любимите си уебсайтове за сигурност и хакерство Top50 и Top100, откъдето в крайна сметка сваля някои от най-новите инструменти за хакерство и сигурност, включително троянски коне, които копира на дискета и в крайна сметка носи вкъщи по време на обедната почивка с цел да обменя информация с втория си приятел проект все още остава един от любимите и най-популярните ежедневно посещавани уебсайтове за сигурност на Данчо. Примерна снимка на София, България. Снимка с любезното съдействие на Данчо ДанчевНа по-късен етап реших да установя работни взаимоотношения с Frame4 Security Systems, която е холандска компания, с цел написване на подобрена версия на оригиналния документ "Как да използваме троянски коне", който по-късно се превърна в "The Complete Windows Trojans Paper", който бързо се превърна в един от най-популярните и четени документи на Сцената за съвременните троянски коне и как да ги използваме и как да се предпазим от тях.

Примерна лична снимка на моста Еразъм в Ротердам. Снимка с любезното съдействие на Данчо ДанчевС наближаването на края на лятото Данчо получава предложение да започне работа в местния офис на своя интернет доставчик (Internet Service Provider), който по това време е Digital Systems, на позицията офис асистент, където отговаря за запознаването на нови клиенти с предлаганите от интернет доставчика услуги и за

обработката на фактури. Сред основните предимства на работата в местния офис на доставчика на интернет услуги е действителната честотна лента, до която има достъп, позволяваща му да влиза в интернет без никакви ограничения, които той използва, за да посещава някои от любимите си уебсайтове за сигурност и хакерство Top50 и Top100, откъдето в крайна сметка сваля някои от най-новите инструменти за хакерство и сигурност, включително троянски коне, които копира на дискета и в крайна сметка носи вкъщи по време на обедната почивка с цел да обменя информация с втория си приятел LockDownCorp и да управлява популярен уебсайт за хакерство и сигурност, който след това да включи в класацията на Progenic.com Top100 Hacking and Security Web sites, включително да предлага платени консултации по сигурността, за да открие начини да помогне на хората да защитят домашните си компютри от троянски коне и да ги научи как да използват защитна стена и как да защитят домашните си компютри.

Примерна снимка на екрана на водещия антитроянски скенер на работодателя на Данчо Данчев LockDownCorp около 90-те години на миналия векНа по-късен етап от ранната си кариера в областта на информационната сигурност той посещава и се присъединява към Клиниката за сигурност на https://itsecurity.com, където публикува личната си биография и отговаря на често задавани въпроси за сигурността, които потребителите на уебсайта задават, и отговорът му се появява на първа страница, като по този начин потенциално води до трафик към работодателя му по това време, който е Frame4 Security Systems, и всъщност подобрява знанията и разбирането си за информационната сигурност като цяло. Данчо е известен и с това, че е участвал в хакерската група Blackcode Ravers, която е управлявала популярния по това време уебсайт https://blackcode.com, и всъщност е участвал с два броя на популярен по това време бюлетин за сигурност, които са били представени на началната страница на портала.

```
|-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|         |++++++++++|
|The Complete Trojans Text                       |--------|Written On|
|(Security Related)                              |        |          |
|by tHe MaNiAc                                   |        |3.04.2000 |
|contact me at: themaniac@blackcode.com          |--------|++++++++++|
|maniac@forbidden.net-security.org               |
|-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|

This guide is for educational purposes only I do not take any responsibility about anything
happen after reading the guide. I'm only telling you how to do this not to do it. It's your decision.
If you want to put this text on your Site/FTP/Newsgroup or anything else you can do it but don't
change anything without the permission of the author.I'll be happy to see this text on other pages too.

All copyrights reserved.You may destribute this text as long as it's not changed.

<--=--=--=--=--=--=--=-->
Author Notes:

I hope you like my texts and find them useful.
If you have any problem or some suggestion feel free to e-mail me but please don't send mails like
"I want to hack the US government please help me" or "Tell me how to blind a trojan into a .jpg"
"WHere can I get a portscanner" etc......
Be sure if I can help you with something I will do it.
I've started writing security related tutorials and I hope you like that.I'll try to cover
much more topics in my future texts and I want to thank to all of the people that like my
texts.
<--=--=--=--=--=--=--=-->

Links:
------------------------------ \
Here you can find other texts   \
written by me or other friends:  \
http://www.blackcode.com         /
blacksun.box.sk                 /
neworder.box.sk                /
------------------------------

Table of Contents
<--------------------------------------\
|                                       \
|-1.What Is This Text About?             \
|-2.What Is A Trojan Horse                \
|-3.Trojans Today                          \
|-4.The future of the trojans               \
|-5.Anti-Virus Scanners                      \
|-6.How You Can Get Infected?                 \
|-----From ICQ                                 \
|-----From IRC                                  \
|-----From Attachment                            \
|-----From Physical Access                        \
|-----From Trick                                   \
|-7.How Dangerous A Trojan Can Be?                  \
|-8.Different Kinds Of Trojans                       \
|-----Remote Access Trojans                           \
|-----Password Sending Trojans                         \
|-----Keyloggers                                        \
|-----Destructive Trojans                                \
|-----FTP Trojans                                         \
|-9.Who Can Infect You?                                    \
```

Примерна снимка на екрана на личния модем на Данчо Данчев, с който той разклащаше дъската по време на 90's През славните години на IRC (Internet Relay Chat), когато Данчо е бил зает да виси в няколко IRC мрежи, включително DALNet и IRC мрежата на местната му страна, той успява да получи файла с паролата /etc/shadow за целия си ISP (Internet Service Provider), който по това време е Digital Systems, и споделя копие от него с най-добрия си приятел по това време Георги Кадийски с цел да използва няколко популярни и високо Списък на думи, включително John the Ripper за разбиване на пароли, потенциално получаване на достъп и насилване на целия списък с пароли за стотици активни акаунти в Интернет по това време. В продължение на няколко дни резултатите по онова време бяха изключителни в контекста на действителния успех в процеса на грубото налагане, което потенциално позволи на Данчо и неговия приятел да получат лесен достъп до безплатните интернет акаунти, които по онова време струваха пари и им позволиха да използват интернет безплатно.   Примерна екранна снимка на личната хакерска страница на Данчо Данчев, наречена "Security is Futile", около 90-те години на миналия векНа по-късен етап Данчо успява да получи достъп и до конкурентния доставчик на интернет услуги в местния град, известен като BIANet /etc/shadow, който му е изпратен от негов приятел и той отново го споделя с приятеля си, който отново започва да използва грубото разбиване на файла с пароли, използвайки различни Worldlist и печално известния по това време инструмент за разбиване на

пароли John the Ripper което потенциално позволява на Данчо и неговия приятел лесен достъп до неограничена dial-up свързаност в интернет.

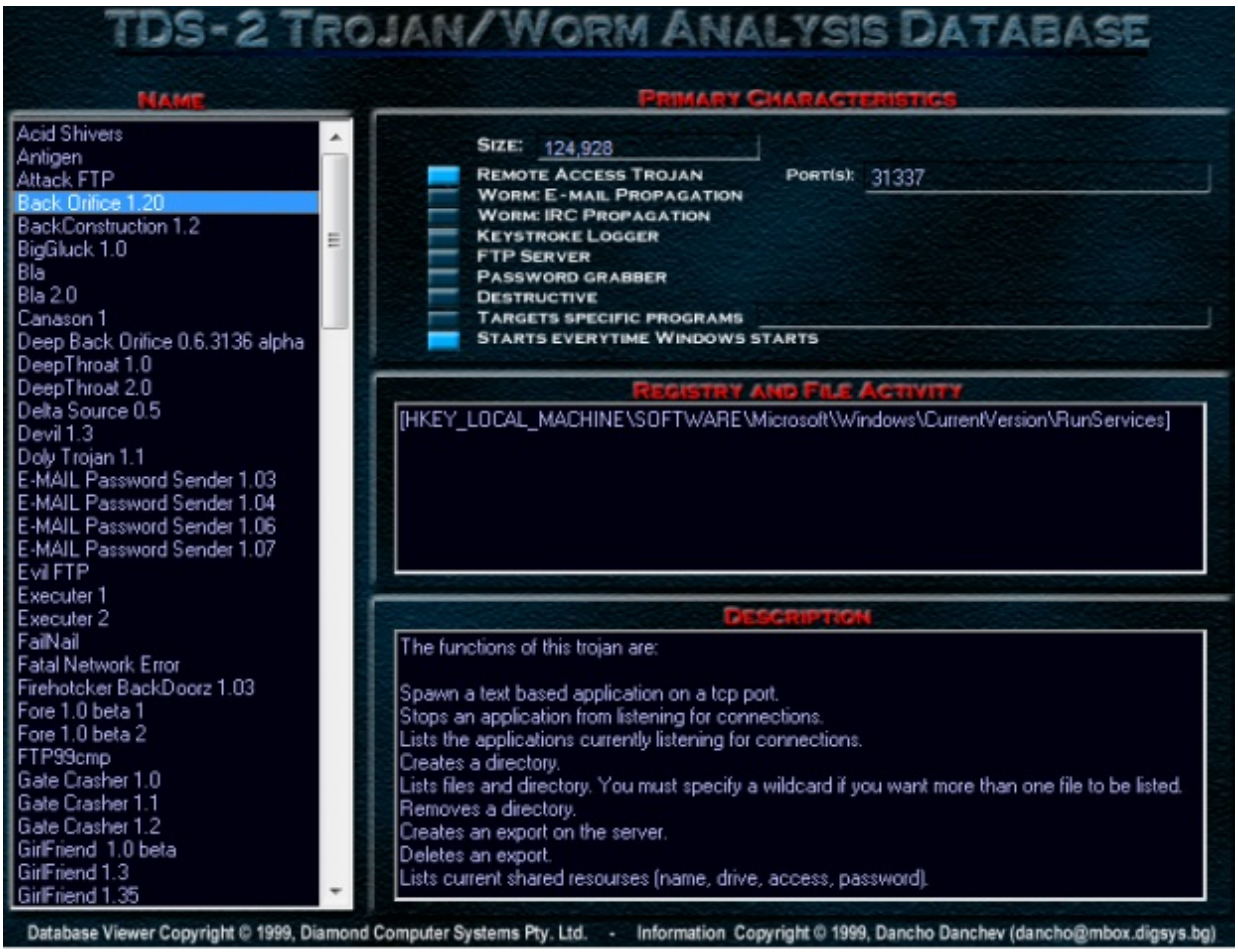
```
          -={ BlackCode Ravers Magazine Issue 2 }=-
             Home page : http://www.blackcode.com
                Editor of the magazine: tHe mAniAc
                        themaniac@blackcode.com
       ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Table of Contents:

-----------------------------------------------------
1.Editorial
2.Mirrors of the magazine
3.Latest News With BlackCode Ravers
4.How to break your school security
5.About Virii
6.Advertising
7.Trojans Section
8.For the newbies
9.Linux Section
10.Interviews
11.Final Words
-----------------------------------------------


1.Editorial
=-=-=-=-=-=-=-=-=-=-=-=-=
It's me again.This is our second issue.I've changed the
design and I've added several new things in the newsletter.
I've also received a lot of e-mails about our magazine.
People like it and they want more information here.
The first issue was short one but of course every new
issue has many new things added in it.
I'm happy people like it and we have MANY new subcribers every day.
Also we have much more visitors than before.
```

Примерна снимка на екрана на личния хакерски сайт на Данчо Данчев около 90-те години на миналия векНастъпи времето да играем една игра. Данчо бързо включил 16-битовия си компютър Правец 2MB RAM и бързо се появил екран, пълен с възможности за избор на компютърна игра, който го подканил да избере игра. Докато зареждаше една сравнително известна игра, известна като Scorch, Данчо реши да играе два часа, а след това да продължи със срещата с приятелите си и да започне дискусия с баба си. Голям почитател на стратегическите игри, Данчо решил, че няма време, което да отдели, за да играе любимата си игра - Sid Meier's Civilization, и вместо това решил, че евентуално ще играе играта по-късно през деня. Играта на Scorch беше доста интересно преживяване и той отдели няколко часа от ценното си учебно време, за да взаимодейства с играта. След това реши да се обърне към най-добрия си приятел по това време и съмишленик в света на НЛО Съветския съюз и компютърните игри, включително хакерската Сцена, за два часа продължителна игра, в която щяхме да изготвим стратегия за това как най-добре да "подходим" към Съветския съюз по отношение на инвазията активно и внимателно да планираме всеки ход по пътя си към нахлуването в Съветския съюз и евентуално във всички околни държави.



Докато аз бях зает с подготовката за нашата няколкочасова игра, Джордж трябваше да се занимава с преглеждането на един диск, който в общи линии беше огледало на Packetstormsecurity и по-специално на раздела E-Zine, за да можем да се подготвим да проведем разговор по отношение на разработването на нашата технологична и военна стратегия по пътя към постигане на глобално господство в оригиналната Civilization на Sid Meier. Това, което по принцип направихме в началото, беше да изготвим стратегия и всъщност да получим по-добър поглед върху технологичното дърво на играта, а докато аз бях зает с придвижването на Империята, Джордж беше зает да води бележки за начина, по който да следим и развиваме военната си стратегия на принципа "пръв дошъл, пръв обслужен". Примерна снимка на екрана от прословутата публикация на Данчо Данчев "Пълният документ за троянците на Windows" около 90-те години на миналия векПровокиран от необходимостта да се свърже с огромната мрежа от компютри, известна като интернет - Данчо бързо реши, че е дошло времето да се свърже - така че реши да потърси подходящ доставчик на връзка в местния си роден град.

Навремето основните доставчици на връзка по онова време бяха българските цифрови системи БИА Нет и водещият доставчик на мобилна свързаност в страната - предплатените dial-up карти на Мтел. Времената бяха различни по отношение на свързаността и DSL и ADSL бяха сбъдната мечта в лицето на корпоративните мрежи, които правилно използваха и използват ISDN тип базирана свързаност. Данчо решава бързо да се сдобие с необходимия dial-up модем, в който в крайна сметка се влюбва, за да достигне до огромната мрежа от компютри, известна като Интернет с помощта на местен доставчик на телефонни услуги, известен като Digital Systems. По онова време - почасовият dial-up достъп означаваше да помислите два пъти какво правите и как го правите онлайн, което означаваше, че по принцип трябваше да подготвя план за нещата, които ще правя онлайн, включително уебсайтове, които ще трябва да посетя, включително набор от имейли, които ще трябва да изпратя на набор от хора, включително приятели и колеги. Минали са години, откакто се е подготвил да се сдобие с персонален компютър и да се свърже, което означава, че е успял да подготви списък с уебсайтове и новинарски групи на тема хакерство и компютърна сигурност, включително общи уебсайтове, които евентуално ще посети.

Сред първите уебсайтове, които посетил, бил NBA.com, където бързо се запознавал с последните събития в любимия си отбор, включително ежедневно разглеждал снимки и евентуално видеоматериали, които да представят любимия му отбор по това време. Сред най-почитаните опитни, които той открива за първи път, преди да се свърже, е да търси снимки на НЛО и информация за КГБ, включително активно възпроизвеждане на звук с помощта на външните си високоговорители в доминирания от MIDI свят по онова време. Най-почтеното и незабравимо преживяване по онова време е фактът, че е имал достъп до електронна поща, която е използвал, за да поддържа връзка със системния администратор на доставчика на интернет услуги, така че да може да поддържа връзка с него, включително активно споделяне на нови връзки към уебсайтове, които той да посещава и да обменя комуникация.

Сред следващите най-значими и ключови характеристики на интернет с помощта на местен доставчик на телефонни услуги, известен като Digital Systems. По онова време - почасовият dial-up достъп означаваше да помислите два пъти какво правите и как го правите онлайн, което означаваше, че по принцип трябваше да подготвя план за нещата, които ще правя онлайн, включително уебсайтове, които ще трябва да посетя, включително набор от имейли, които ще трябва да изпратя на набор от хора, включително приятели и колеги. Минали са години, откакто се е подготвил да се сдобие с персонален компютър и да се свърже, което означава, че е успял да подготви списък с уебсайтове и новинарски групи на тема хакерство и компютърна сигурност, включително общи уебсайтове, които евентуално ще посети. Сред първите уебсайтове, които посетил, бил NBA.com, където бързо се запознавал с последните събития в любимия си отбор, включително ежедневно разглеждал снимки и евентуално видеоматериали, които да представят любимия му отбор по това време. Сред най-почитаните опитни, които той открива за първи път, преди да се свърже, е да търси снимки на НЛО и информация за КГБ, включително активно възпроизвеждане на звук с помощта на външните си високоговорители в доминирания от MIDI свят по онова време. Най-почтеното и незабравимо преживяване по онова време е фактът, че е имал достъп до електронна поща, която е използвал, за да поддържа връзка със системния администратор на доставчика на интернет услуги, така че да може да поддържа връзка с него, включително активно споделяне на нови връзки към уебсайтове, които той да посещава и да обменя комуникация.

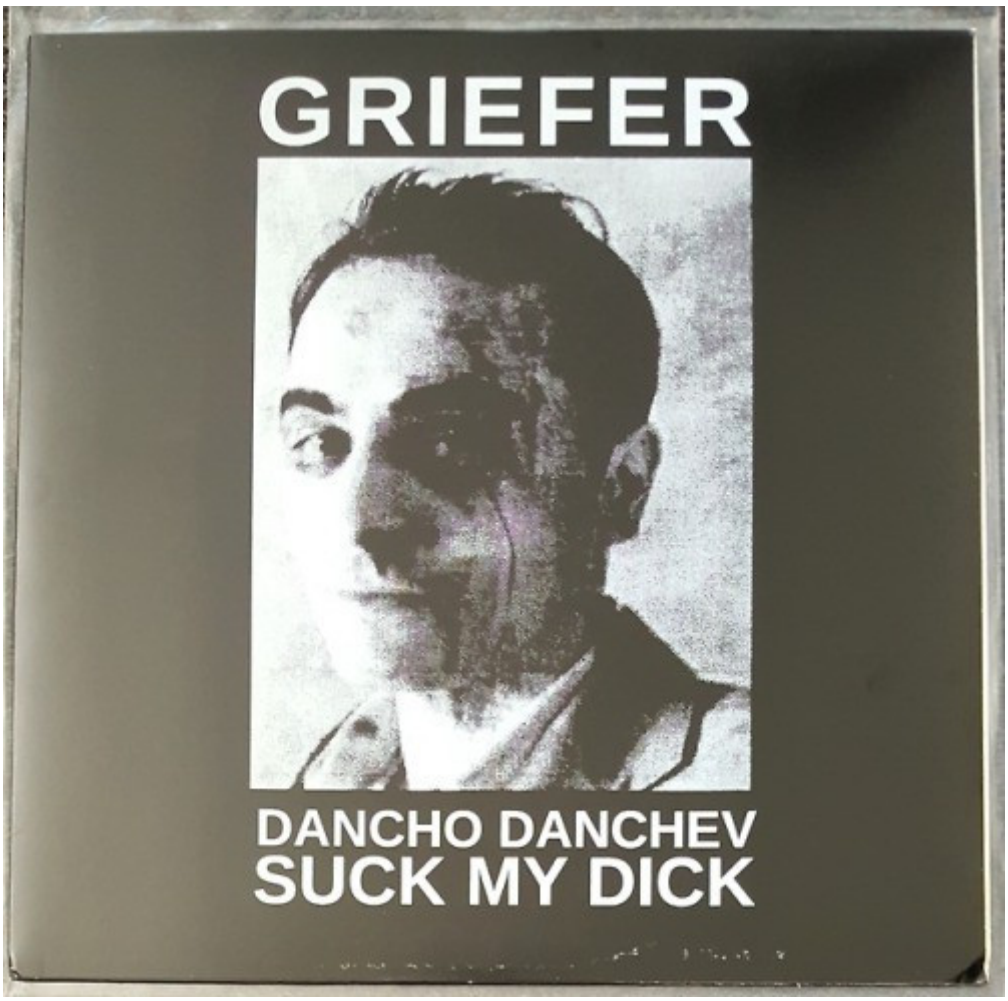
Сред следващите най-значими и ключови характеристики на интернет бързо решава, че трябва да започне да навлиза в света на хакерството, за да трупа знания и да впечатлява приятелите си. Сред първите канали, към които се присъединява по това време, са #gay и #lesbian, където той се представя за друг човек, който основно се стреми да предложи нов и оригинален скрийнсейвър, базиран на снимки, на различни лица с цел да ги подмами да изпълнят скрийнсейвъра на домашните си компютри и в крайна сметка да получат достъп до компютрите си, използвайки популярен по това време клиент за троянски кон, като например Sub7. Би било доста лесно да се предположи как нещата са се усложнили, като Данчо бързо е получил достъп до основното приложение mIRC на Internet Relay Chat, включващо различни IRC-базирани "военни скриптове", включително дузина мейл-бомби и различни други ICQ-базирани тип нукери и флудери по пътя си към демонстриране на подходящо техническо ноу-хау пред своите приятели и колеги в сенчестия свят на хакерството.

Сред първите канали, до които се опита да получи достъп, бяха #hacker #hackers #hacking и прословутият #hackphreak в EFNet, включително за да отвори всъщност няколко лични канала в местните IRC мрежи, включително #drugs #KGB и #linuxsecurity. На по-късен етап той всъщност успява да попита свой приятел за евентуален статут на оператор в местната IRC канала на града, където той основно управляваше бот за онлайн защита 24/7, известен като xploit, включително активното използване на Socks5 сървър, който по това време се предлагаше от неговия работодател LockDownCorp, където той беше зает да действа като технически колектор на троянски коне/червеи/вируси и VBS скриптове с цел подобряване на процента на откриване на антитроянски софтуер на базата на сигнатури.

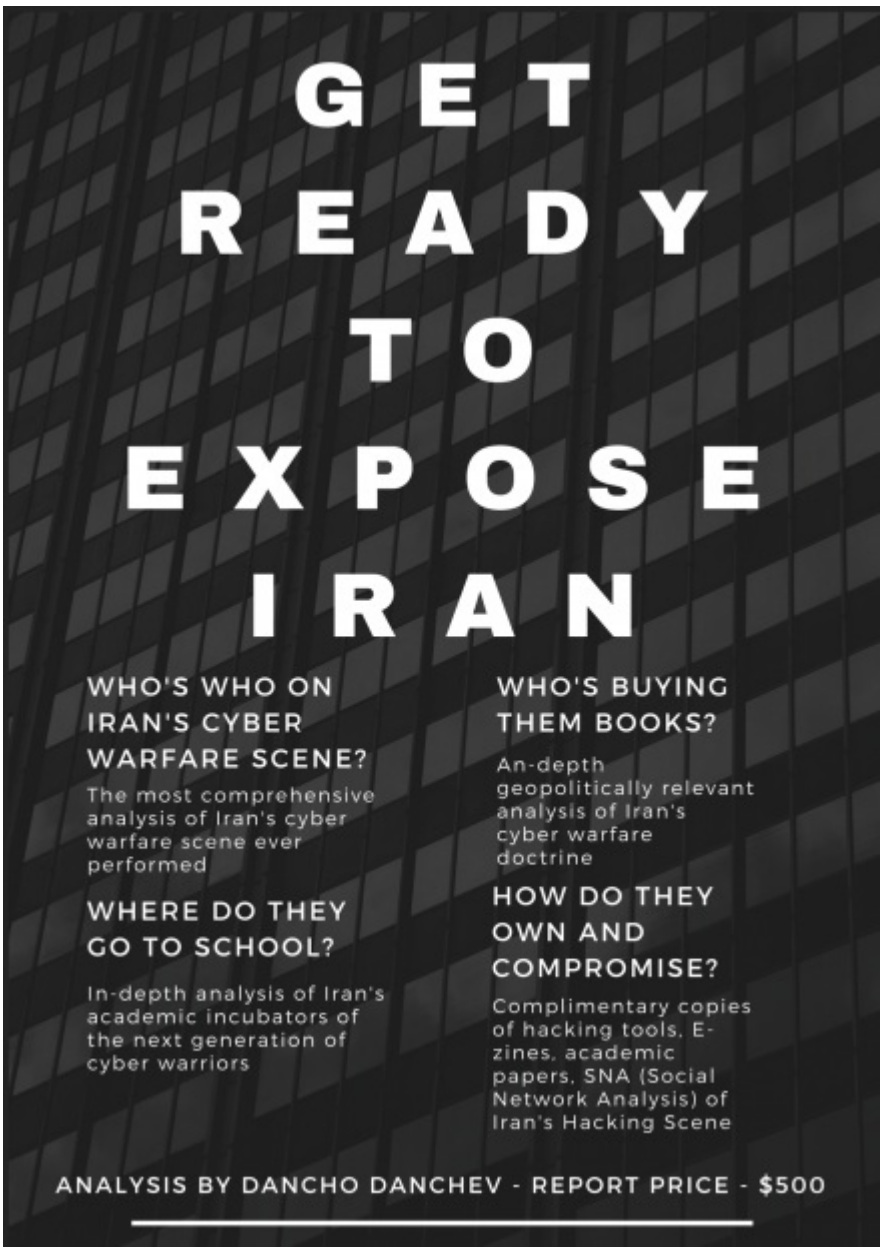
Примерна снимка на 3G USB модем, който Данчо използвал за работа по време на пътуванеЕдно от първите неща, които Данчо решава да направи в свободното си време, е да проучи активно местния уебмастър на официалния уебсайт на родния си град с цел да се опита да извърши социално-инженерна атака срещу официалния уебсайт на местния град, която в общи линии успява и води до появата на "поздравително" съобщение публикувано на официалния уебсайт, без да се извършва реално унищожаване и премахване на данни, което изглежда като професионален подход при компрометирането на легитимен уебсайт с цел да поздрави личните си приятели и да разпространи съобщение от името на "Троянската хакерска група", която по това време основно се състои от един от най-близките му приятели и друг колега хакер ентусиаст. Сред отговорностите му по онова време беше и активното събиране на троянски коне/червеи/вируси и VBS скриптове с идеята да ги сподели с работодателя си, който по онова време беше LockDownCorp - един от водещите световни доставчици на антитроянски програми, с цел подобряване на процента на откриване на тези публично достъпни троянски коне, което по-късно се превръща в успешна операция за техническо събиране, която основно плаща сметките му и всъщност му предлага приличен финансов стимул да продължи да се занимава със сигурност като хакер ентусиаст и всъщност подобрява цялостния процент на откриване на някои от най-разпространените троянски коне по това време от страна на работодателя му.

Примерна снимка на Данчо Данчев по време на пътуване. С любезното съдействие на Данчо ДанчевСъщинското договорно споразумение беше свързано с това, че Данчо притежаваше частен FTP сървър, на който прекарваше часове в качване на събраните троянски коне, използвайки домашната си dial-up връзка, и в крайна сметка получаваше приходи от този процес, използвайки Western Union, където беше щастлив, че е установил директни работни отношения с един от водещите световни доставчици на антитроянски програми, който по това време се намираше на адрес - http://proxy2.stealthedip.com/maniac/incoming/ Всеки път, когато Данчо се опитваше да се свърже с приятелите си, той се опитваше да разбере дали те са онлайн, използвайки популярен троянски кон, включително да провери всъщност имейл акаунта си за техните наскоро сменени пароли и друга свързана информация, включително текущото им IP, за да може правилно да се свърже с домашния им компютър с образователна цел. Като най-забележителният в света изследовател на киберпрестъпността, блогър по сигурността и анализатор на разузнаването на заплахите, изследователят бързо си спечели слава, като систематично и ефикасно профилира и анализира прилична снимка на злонамерени национални и измамни онлайн, което го кара да направи успешна кариера като най-популярния в света изследовател на киберпрестъпността, блогър по сигурността и анализатор на разузнавателни данни за заплахи.

Примерна лична снимка на Данчо Данчев. Imagery Courtesy of Dancho DanchevВ ранната сутрин на понеделник изследователят бързо събира набор от материали за изследване на основния ботнет, който следи - скандалния ботнет Koobface, като използва пасивни и активни виртуални SIGINT методологии, които основно включват активно вземане на проби от злонамерените онлайн дейности на ботнета, използвайки ежедневен набор от прихванати злонамерени и измамни кампании, стартирани, управлявани и оперирани от ботнета Koobface, с цел осигуряване на необходимата техническа оперативна и стратегическа разузнавателна информация от типа OSINT, включително ежедневната партида от домейни и кампании за набиране на парични мулета, с чието профилиране се е занимавал с идеята да помогне на U. САЩ по пътя към издирване и преследване на киберпрестъпниците, които стоят зад тези кампании.

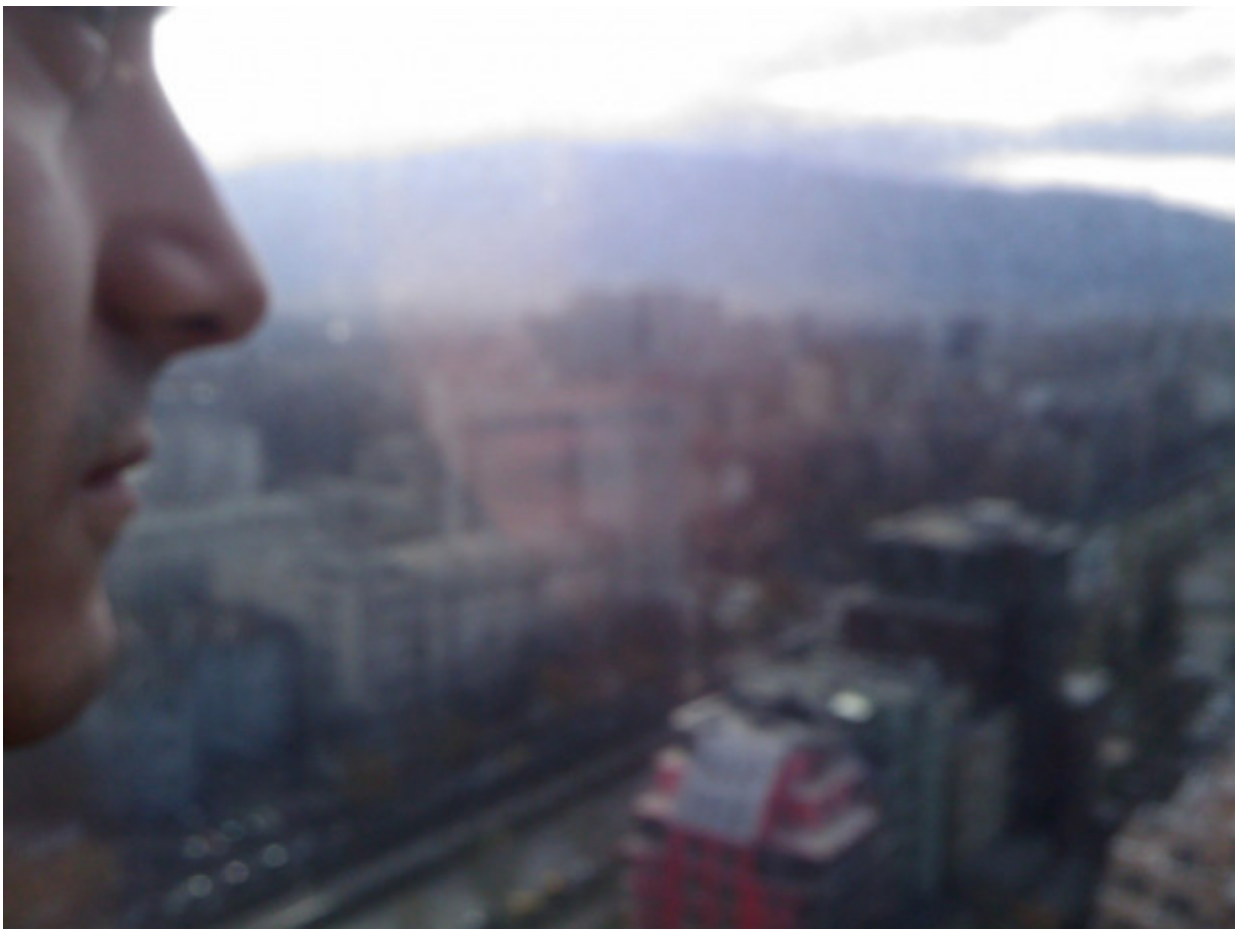


Примерна снимка от програмата на GCHQ "Lovely Horse" за следене на хакери в Twitter, в която е участвал Данчо ДанчевБотнетът Koobface е бил основният ботнет, разпространяван през социалните медии по това време, в частност Facebook и вече е успяла да засегне десетки хиляди потребители в световен мащаб, като потенциално ги е подмамила да взаимодействат с измамни и визуални кампании, базирани на социално инженерство, под формата на фалшиви Adobe Flash плейъри и фалшиви видеоклипове в YouTube, при които крайната цел е да се опитат да засегнат приятелите си във Facebook, като изпращат автоматизирани и легитимно изглеждащи съобщения, включващи връзки към измамно и злонамерено съдържание. Примерна екранна снимка от бюлетина за сигурност на Данчо Данчев за Blackcode.com Около 90-те години на миналия векИзминали са години, откакто се е подготвял да се сдобие с персонален компютър и да се свърже, което означава, че е успял да подготви списък с уебсайтове и новинарски групи на тема хакерство и компютърна сигурност, включително общи уебсайтове, които евентуално би посетил. Сред първите уебсайтове, които посети, беше NBA.com, където бързо щеше да се запознае с последните събития в любимия си отбор, включително ежедневно разглеждане на снимки и евентуално видеоматериали, които да представят любимия му отбор по това време.



Сред най-почитаните опитни, които той открива за първи път, преди да се свърже, е да търси снимки на НЛО и информация за КГБ, включително активно възпроизвеждане на звук с помощта на външните си високоговорители в доминирания от MIDI свят по онова време. Примерна екранна снимка на базата данни за анализ на троянски коне на Данчо Данчев, която той е направил за пакета за защита от троянски коне на своя работодател DiamondCS около 90-те години на миналия векНай- маститият и незабравимо преживяване по онова време беше фактът, че той имаше достъп до електронна поща, която използваше, за да поддържа връзка със системния администратор на доставчика на интернет услуги, така че да може да поддържа връзка с него, включително активно споделяне на нови връзки към уебсайтове, които той да посети и да обмени комуникация.

Минаха години, откакто той се подготви да придобие персонален компютър и да се свърже, което означава, че успя да подготви списък с уебсайтове и новинарски групи на тема хакерство и компютърна сигурност, включително общи уебсайтове, които евентуално ще посети. Сред първите уебсайтове, които е посетил, е бил NBA.com, където бързо е щял да се запознае с последните събития в любимия си отбор, включително ежедневно разглеждане на снимки и евентуално видеоматериали, които да представят любимия му отбор по това време. Сред най-почитаните опитни, които той открива за първи път, преди да се свърже, е да търси снимки на НЛО и информация за КГБ, включително активно възпроизвеждане на звук с помощта на външните си високоговорители в доминирания от MIDI свят по онова време.



Най-почтеното и незабравимо преживяване по онова време е фактът, че е имал достъп до електронна поща, която е използвал, за да поддържа връзка със системния администратор на доставчика на интернет услуги, така че да може да поддържа връзка с него, включително активно споделяне на нови връзки към уебсайтове, които той да посещава и да обменя комуникация. Примерна лична снимка на екрана на личния хакерски уебсайт на Данчо Данчев около 90-те години на миналия век Сред следващите най-значими и ключови характеристики на интернет, които използвах по онова време, беше ICQ, по-специално фактът, че съобщенията от родния ми град пътуваха до столицата на страната в реално време, което беше особено впечатляващо, по-специално фактът, че получавах незабавни отговори на съобщенията си. Съвсем логично беше да се заключи, че активният обмен на съобщения по ICQ и реалните контакти са от решаващо значение за придобиването на популярност и за реалния опит да се владее Сцената.

Това, което направих на практика по онова време, беше да помоля няколко от моите приятели, за които се знаеше, че са участвали в Сцената по онова време, да препратят и обменят приличен набор от ICQ контакти на колеги от Сцената, което бързо ме снабди с необходимите контакти, за да се присъединя към няколко хакерски групи, по-специално HackHouse и Social Engineering Project, на които се гордеех, че съм член. Примерна снимка на екрана на примерен етичен компрометиран уебсайт около 90-те години. Снимка с любезното съдействие на Данчо ДанчевСред следващите най-значими и ключови характеристики на интернет, които използвах по онова време, беше ICQ, по-специално фактът, че съобщенията от родния ми град пътуваха до столицата на страната в реално време, което беше особено впечатляващо, по-специално фактът, че получавах незабавни отговори на съобщенията си. Съвсем логично беше да се заключи, че активният обмен на съобщенията в ICQ и действителните контакти е от решаващо значение за това да станете популярни и да се опитате да притежавате Сцената.

Това, което направих на практика по онова време, беше да помоля няколко мои приятели, за които се знаеше, че са участвали в Сцената по онова време, да препратят и обменят приличен набор от ICQ контакти на колеги от Сцената, което бързо ми даде необходимите контакти, за да се присъединя към няколко хакерски групи, по-специално към HackHouse и Social Engineering Project, на които се гордеех, че съм член. Примерна екранна снимка на частно психеделично транс парти в Second Life. Снимка с любезното съдействие на Данчо ДанчевСред следващите най-значими и ключови характеристики на интернет, които използвах по онова време, беше ICQ, по-специално фактът, че съобщенията от родния ми град пътуваха до столицата на страната в реално време, което беше особено впечатляващо, по-специално фактът, че получавах незабавни отговори на съобщенията си. Съвсем логично беше да се заключи, че активният обмен на съобщения по ICQ и реалните контакти са от решаващо значение за придобиването на популярност и за реалния опит да се владее Сцената. Това, което направих на практика по онова време, беше да помоля няколко мои приятели, за които се знаеше, че са участвали в Сцената по онова време, да препратят и обменят приличен набор от ICQ контакти на колеги от Сцената, което бързо ме снабди с необходимите контакти, за да се

присъединя към няколко хакерски групи, по-специално HackHouse и проекта "Социално инженерство", на който се гордея, че съм член.

Proxy Server Name	HTTP Port	SOCKS Port	Network #	Machine	IP BLOCK
BLACKCODEPROXY.COM	8080	1080	Network # 1	Machine # 1	216.41.20.82
TLPROXY.COM	8080	1080	Network # 2	Machine # 2	12.148.163.141
PROXY1.THEPROXYCONNECTION.COM	8080	1080	Network # 1	Machine # 3	216.41.20.120
PROXY2.THEPROXYCONNECTION.COM	8080	1080	Network # 1	Machine # 4	216.41.20.13
PROXY3.THEPROXYCONNECTION.COM	8080	1080	Network # 1	Machine # 5	216.41.20.37
HIDDEN-INPHERNO.NET	8080	1080	Network # 2	Machine # 6	199.105.112.152
DSL-NET.ORG	8080	1080	Network # 2	Machine # 7	63.127.192.136
ONTARIO-CA.NET	8080	1080	Network # 2	Machine # 8	199.105.112.163
GERMANY-DE.NET	8080	1080	Network # 2	Machine # 9	199.105.112.170
SHAWCABLE-CA.NET	8080	1080	Network # 2	Machine # 10	199.105.112.182
MODEM-LINK.NET	8080	1080	Network # 2	Machine # 11	199.105.112.186
CA-CABLE.NET	8080	1080	Network # 2	Machine # 12	63.127.192.178
INTERNET-PIPELINE.NET	8080	1080	Network # 2	Machine # 13	199.105.112.190
WIRELESS-INET.NET	8080	1080	Network # 1	Machine # 14	216.41.20.175
STAR-TRAVEL.ORG	8080	1080	Network # 1	Machine # 15	216.41.21.20
POPULAR-PEOPLE.ORG	8080	1080	Network # 2	Machine # 16	12.148.163.51

Примерна снимка на екрана на личната външна батерия на Данчо Данчев, която той използваше за пътувания, докато работеше за ZDNetЕдна от първите групи, към които наистина се присъединих по това време, беше Toxic Crisco, която по принцип представляваше група от лица, занимаващи се с различни онлайн дейности, включително евентуално хакерство, включително проекта SCR, който по принцип беше хакерска група за социално инженерство, в която се гордеех, че членувам, по-специално с активното си участие в четенето на различни високопрофилни психологически книги по това време. За целите на използването на IRC, по-специално DALnet, Данчо бързо събра копие на популярния mIRC, включително няколко военни скрипта ICQ Bombers Nukers и Mail Bombers, включително троянски коне, и бързо реши, че трябва да започне да придобива опит в света на хакерството с цел придобиване на знания и впечатляване на приятелите си. Сред първите канали, към които всъщност се присъединява по това време, са #gay и #lesbian, където основно се представя за друг човек, който се стреми да предложи нов и оригинален скрийнсейвър, базиран на снимки, на различни лица с цел да ги подмами да изпълнят скрийнсейвъра на домашните си компютри, като в крайна сметка получат достъп до компютрите си, използвайки популярен по това време клиент за троянски коне, като например Sub7.

Сред първите групи, към които наистина се присъединих по онова време беше Toxic Crisco, която по принцип представляваше група от хора, занимаващи се с различни онлайн дейности, включително хакерство, включително проекта SCR, който по принцип беше хакерска група, управлявана от социалното инженерство, в която се гордеех, че членувам, и по-специално с активното си участие в четенето на различни високопрофилни психологически книги по онова време. В един прекрасен четвъртък следобед Данчо реши да поиграе на прилична компютърна игра, докато майка му беше заета с гладене в детската стая, и реши да предприеме пътуване, с което успешно да отърве Света от враждебни извънземни.

Играта, наречена Duke Nukem, в общи линии отвеждаше Данчо на пътешествие в друг Свят, където той прекарваше по-голямата част от следобеда, отървавайки се от враждебни извънземни, докато водеше дискусия с майка си за местонахождението си през деня, включително за активната подготовка за занятията на следващия ден и евентуалния разговор за вечеря. Докато мама беше заета с гладене, Данчо пое на друго пътешествие в далечен Свят, където се грижеше и защитаваше Земята от зли извънземни и реши, че е дошло време за почивка. Някои от най-запомнящите се спомени на Данчо от онова време са свързани с играта на пълен работен ден на една от най-добрите стратегически игри през 90-те години, а именно Sid Meier's Civilization. Прекарвайки прилична част от времето си основно по четири часа дневно, Данчо бързо придобива необходимите умения, за да изведе цивилизацията си на ново ниво, като води войни, развивайки и обменяйки нови технологии и водейки войни с конкурентни и противникови цивилизации.

След като вече е овладял силата на играта "Цивилизация", Дancho бързо попада в свят на политика, технологии и войни и успешно картографира и оставя опора в света по начина, по който го познава и владее, след като успешно прекарва прилична част от времето си в игра на най-добрата стратегическа игра през 90-те години - Civilization на Сид Майер. Game World е нещо различно. Всеки път, когато Данчо решаваше да поиграе на някоя игра, Светът спираше, а Данчо играеше и научаваше основите и вътрешните механизми на всяка игра, до която успяваше да се добере през 90-те години. Преодолявайки границите на играта, в един момент Данчо решава да разгледа по-

задълбочено как всъщност можеш да накараш компютърния играч да стане по-напреднал и по-сложен и всъщност се опитва да обучи изкуствения интелект на играта и евентуално да измисли начин да научи да използва усъвършенствани военни тактики. Би било доста лесно да се предположи как нещата са се усложнили с това, че Данчо бързо е получил достъп до основното приложение mIRC на Internet Relay Chat, включващо различни "военни скриптове", базирани на IRC, включително дузина пощенски бомбардировачи и различни други базирани на ICQ тип Нукери и Флудери по пътя си към демонстриране на подходящо техническо ноу-хау на своите приятели и колеги в сенчестия свят на хакерството.

Сред първите канали, до които се опита да получи достъп, бяха #hacker #hackers #hacking и прословутият #hackphreak в EFNet, включително за да отвори всъщност няколко лични канала в местните IRC мрежи, включително #наркотици #КГБ и #линукссигурност. На по-късен етап той действително успява да поиска от свой приятел евентуален статут на оператор в IRC канала на местния град, където по принцип управлява 24/7 бот за онлайн защита, известен като xploit, включително активно използване на Socks5 сървър, който по това време се предлага от неговия работодател LockDownCorp, където той се занимава с това да действа като технически колектор на троянски коне/червеи/вируси и VBS скриптове с цел подобряване на процента на

откриване на антитроянския софтуер на базата на сигнатури. Образец Socks5 в търговската мрежа. налични сървъри с любезното съдействие на LockDownCorp един от настоящите работодатели на Данчо по това време, които той използва, за да повиши репутацията си в местната IRC мрежа и всъщност да скрие истинското си IP Сред първите неща, които Данчо решава да направи в свободното си време, е да проучи активно местния уебмастър на официалния уебсайт на родния си град с цел да се опита да извърши социално-инженерна атака срещу официалния уебсайт на местния град, който в общи линии успя и доведе до публикуване на "поздравително" съобщение на официалния уеб сайт без да се извършва реално унищожаване и премахване на данни, което изглеждаше като професионален подход при компрометиране на легитимен уеб сайт с цел да поздрави личните си приятели и да разпространи съобщение от името на "Троянската хакерска група", която по това време в общи линии се състоеше от един от най-близките му приятели и още един колега хакер ентусиаст.

Примерни примери за увреждане на уебсайтове с любезното съдействие на Данчо през 90-те години, които основно доведе до лично съобщение и личен поздрав до всички негови приятели по това време с любезното съдействие на "Trojan Hacking Group" Сред отговорностите му по това време включваше активното събиране на троянски коне/червеи/вируси и VBS скриптове с идеята да ги сподели с работодателя си, който по това време беше LockDownCorp един от водещите в света анти троянски коне с цел подобряване на процента на откриване на тези публично достъпни троянски коне, което по-късно се превърна в успешна операция за техническо събиране, която основно плащаше сметките му и всъщност му предлагаше приличен финансов стимул да продължи да се занимава със сигурност като хакер ентусиаст и всъщност подобри общия процент на откриване на някои от най-разпространените троянски коне по това време от страна на работодателя му.

Действителното договорно споразумение се отнасяше до това, че Данчо използваше частен FTP сървър, където с часове качваше събраните троянски коне, използвайки домашната си dial-up връзка, и в крайна сметка получаваше приходи от този процес, използвайки Western Union, където беше щастлив, че е установил директни работни отношения с един от водещите световни доставчици на антитроянски програми, който по това време се намираше на адрес - http://proxy2.stealthedip.com/maniac/incoming/. Когато Данчо се опитваше да се свърже с приятелите си, той се опитваше да разбере дали са онлайн, използвайки популярна троянски кон, включително да провери имейл акаунта си за наскоро променените им пароли и друга свързана информация, включително текущото им IP, за да може да се свърже правилно с домашния им компютър с образователна цел. В качеството си на най-известния в света изследовател на киберпрестъпността, блогър по сигурността и анализатор на разузнаването на заплахите, изследователят бързо придобива известност, като систематично и ефективно профилира и анализира прилична снимка на злонамерената дейност на националните държави и измамниците онлайн, което го кара да направи успешна кариера като най-популярния в света изследовател на киберпрестъпността, блогър по сигурността и анализатор на разузнаването на заплахите.

Примерна брошура, създадена от Данчо Данчев за предстоящо изследване на хакерската екосистема на ИранПрез 2007 г. получих директна покана да присъствам на частна конференция, организирана само с покани от проекта Honeynet в британската GCHQ, на която всъщност присъствах и представих различни теми, включително настоящи и нови тенденции в киберпрестъпността, и всъщност имах възможност да се срещна с хората от проекта Honey net. Примерна снимка на екран от презентацията на Данчо Данчев, проведена в британския GCHQ през 2007 г. С любезното съдействие на Данчо Данчев Примерна карикатура, създадена от Данчо Данчев за презентация.

С любезното съдействие на Данчо ДанчевПрез 2008 г. получих изненадваща покана да се присъединя към екипа на ZDNet - уебсайт портал, на който силно се възхищавах, докато бях зает с работа за https://astalavista.com и бях в действителност посещавам ежедневно мястото, където прекарвам високопрофесионални и продуктивни 4 години като блогър по сигурността в блога Zero Day на ZDNet, което ме доведе до хиляди публикации, включително действителна награда Jessy H. Neal Award за работа в блога Zero Day на ZDNet. Примерна екранна снимка от блога Zero Day на ZDNet. Снимка с любезното съдействие на Данчо ДанчевРаботата за ZDNet до голяма степен оформи професионалното ми благосъстояние по начин, по който основно работех с първокласни технологични експерти от целия свят и всъщност имах възможност да допринасям с лично съдържание и изследвания за период от четири години, което беше незабравимо преживяване и все още е удоволствие и чест да се докосна до тях и всъщност да намеря начин да допринеса и да поздравя хората, с които работех през 2008 г.

В някакъв момент в крайна сметка ме поканиха да участвам в частна конференция само за поканени, където представих практики за набиране на парични мулета и в крайна сметка получих привилегията да се срещна с повечето от хората, с които работя, лице в лице, където се срещахме и всъщност общувахме и обсъждахме различни горещи теми и тенденции в киберпрестъпността в международен план. Пример за личен скрийншот на частна вечеря. Снимка с любезното съдействие на Данчо ДанчевДанчо започва кариерата си в света на разузнавателните изследвания, силно провокиран от изследванията, публикувани и разпространявани от американската компания iDefense, която основно е специализирана в профилирането на онлайн хактивистки дейности и е в състояние да изготвя висококачествени и никога непубликувани досега разузнавателни данни за заплахи и общи разузнавателни справки.

Сред ключовите доклади, до които Данчо е успял да се добере, е сблъсъкът между САЩ и Китай, който по същество се състои от различни групи, базирани в САЩ и Китай, които активно си взаимодействат онлайн, като извършват DDoS (Distributed Denial of Service) атаки срещу тяхната инфраструктура и участват в кампании за нарушаване на целостта на уебсайтове. След това проучва и активно посещава официалния уебсайт на CIA.gov, включително FAS.org и NSA.gov, за да търси наръчници и изследователски материали за разузнаване с отворен код (OSINT), които по-късно значително допринасят за превръщането му в един от водещите световни експерти в областта на изследването на киберпрестъпността и събирането на разузнавателни данни за заплахи. Примерна лична снимка на визитната картичка на Данчо Данчев около 2012 г. С любезното съдействие на Данчо ДанчевВ една ранна понеделнишка сутрин изследователят бързо събира набор от материали за изследване на основния ботнет, който е наблюдавал - скандалния ботнет Koobface.

Основната му мотивация за проследяването и наблюдението на един от най-плодовитите ботнети, който се разпространяваше във Facebook по това време, беше да помогне на индустрията за сигурност и изследователи от цял свят, включително американските правоприлагащи органи, за да проследят дейностите на ботнета и евентуално да се опитат да го изключат от мрежата, както и да проследят някои от авторите, които стоят зад него. Образцова винилова обложка на албум на Данчо Данчев, издаден онлайн от канадски индустриален артистДневната рутина на Данчо се състоеше в това да проверява най-новите кампании, стартирани от бандата, и всъщност да предлага задълбочен технически анализ на последните кампании, като публично разпространява и профилира кампаниите в личния си блог, което го довежда до специфичен набор от подробни и задълбочени анализи на ботнета Koobface, един от малкото публично достъпни ресурси за анализ по темата по това време.

Примерна снимка на екрана от презентацията на Данчо Данчев за Koobface, представена на CyberCamp 2016. По онова време се знаеше, че майсторите на ботнета следят изследванията на Данчо и в крайна сметка оставят съобщение, вградено в реалната C&C инфраструктура, с което основно поздравяват изследователя за неговите изследвания, включително второ и трето съобщение по време на коледния сезон, включващо реален отговор точка по точка на неговите "Топ 10 неща, които и изследователи от цял свят, включително американските правоприлагащи органи, за да проследят дейностите на ботнета и евентуално да се опитат да го изключат от мрежата, както и да проследят някои от авторите, които стоят зад него.

Image 4 : Electronic Warfare (ELINT) 2

Image 6 : NCW Attack Formation

Образцова винилова обложка на албум на Данчо Данчев, издаден онлайн от канадски индустриален артистДневната рутина на Данчо се състоеше в това да проверява най-новите кампании, стартирани от бандата, и всъщност да предлага задълбочен технически анализ на последните кампании, като публично разпространява и профилира кампаниите в личния си блог, което го довежда до специфичен набор от подробни и задълбочени анализи на ботнета Koobface, един от малкото публично достъпни ресурси за анализ по темата по това време. Примерна снимка на екрана от презентацията на Данчо Данчев за Koobface, представена на CyberCamp 2016По онова време се знаеше, че майсторите на ботнета следят изследванията на Данчо и в крайна сметка оставят съобщение, вградено в реалната C&C инфраструктура, с което основно поздравяват изследователя за неговите изследвания, включително второ и трето съобщение по време на коледния сезон.

Преживявания в Astalavista.com

През 2003 когато започнах да уча в Холандия се опитах да си намеря работа в един от най-известните портали за хакери и специалисти по сигурност в света и реално успях да си намеря работа за позицията Изпълнителен Директор където основната ми задача е да отговарям за съдържанието на портала като нови програми новини и документи и презентации за сигурност който посетителите ще могат да свалят и да обогатяват знанията си в света на компютърната сигурност.

Позицията ми на портал-а беше от 2003 до 2006 където също така бях отговорен за публикуването на 32 издания от месечната ни публикация която включва интересно интервю с някой известен от сцената или от индустрията където за момента съм взел интервюта от следните хора от сцената и индустрията:

- Proge
- Джейсън Скот
- Кевин Таунсенд
- Ричард Мента
- MrYowler
- Prozac
- Candid Wuest

●Anthony Aykut
●Dave Wreski
●Mitchell Rowtow
●Eric (SnakeByte)
●Бьорн Андреасон
●Брус
●Николай Недялков
●Roman Polesek
●Джон Йънг
●Ерик Голдман
●Robert
●Джон Б. Улрих
●Даниел Брандт
●Дейвид Ендлер
●Владимир, ЗАРАЗА

За мен беше привилегия да интервюирам някои от хората който съм успял да интервюирам включително един от създателите на Progenic.com включително LinuxSecurity и Cryptome.org където основната цел е да задавам интересни въпроси и да публикувам отгорите на портала с цел повече хора да могат да ги видят.

Една от основните причини поради която успях да се справя и да продължа образованието си в Холандия беше заплатата и усилията които полагах портала да работи което се отрази върху моята заплата като студент и Изпълнителен Директор на портала тогава за което бих желал лично да благодаря на собствениците на портала за възможността на направя промяна и да покажа на какво съм способен от гледна точка на съдържание.

Докато бях студент и учех в Холандия с моята приятелка Уорданка Илиева която отговаряше за проверка за грешки на месечната публикация която публикувах на портала получавах заплатата си всеки месец което ми позволи да уча и да продължа да уча в Холандия и като цяло ме мотивира да работя над портала и също така спечелихме и награда за най-популярен сайт от PCMagazine.

Друго основно нещо за което бих искал да благодаря на собствениците на портала е възможността да работя и да публикувам нови секций и рубрики на портала и истинските моменти който всички сме имали заедно когато публикувахме Коледните и Новогодишни Поздравления и рубриката относно потребители който ни изпращаха снимки на техните работни станций като фенове и почитатели на портала.

Бонус Съдържание - Интервю с Мен

sOpen Source Intelligence (OSINT) е тактика, използвана за научаване на информация, свързана с защитата на организация от външни и вътрешни заплахи, като се използват публично достъпни данни. Способността да се идентифицира информация, която потенциално може да бъде използвана срещу организация, предоставя полезна информация, която може да намали риска, пред който организацията може да се изправи. Това е система за ранно предупреждение, използвана за прогнозиране и сигнализиране на потенциална заплаха.

Редакторите на LinuxSecurity сметнаха, че би било интересно да обсъдим темата за разузнаването с отворен код, разузнаването на заплахите и как да започнем работа с OSINT с нашата аудитория, както и да говорим с Данчо Данчев, известен бивш хакер и изследовател на разузнаване на сигурността от България . Данчо е лидер в областта на текущите и нововъзникващите изследвания на киберпрестъпленията и разузнаването на заплахи и плодовит блогър по темите.

Данчо Данчев, български хакер, изследовател по сигурността

Решихме, че би било интересно да зададем на Данчо няколко въпроса за неговия произход, разузнаването с отворен код, текущите тенденции в общността за киберсигурност, тъмната мрежа, правителствената сигурност, заплахите от нулевия ден и усилията му, довели до свалянето на Koobface , най-големият ботнет в света по това време.

Бивш блогър на ZDNet Zero Day повече от четири години, Данчо също работи като блогър по сигурността за Webroot. През 2011 г. той беше избран от SCMagazine за тяхната награда за социални медии като финалист за неговия акаунт в Twitter по това време. Данчо също представи в GCHQ на Обединеното кралство, включително централата на канадската разузнавателна служба, и основна презентация на тема „Разкриването на Koobface – най-голямата ботнет в света“.

През 2016 г. Данчо представи на CyberCamp RSA Europe и InfoSec Europe актуални тенденции в киберпрестъпността и киберджихада. Преди това той също беше един от основните разработчици на подземната мрежа, известна като Astalavisita.

Данчо е често цитиран и често споменаван изследовател на киберпрестъпления, блогър по сигурността и анализатор на разузнаване на заплахи с повече от десетилетие в борбата с киберпрестъпленията и активното реагиране на настоящи и нововъзникващи заплахи от киберпрестъпления.

Данчо също е работил като технически колектор за прословутото анти-троянско софтуерно решение LockDown2000, включително работа като мениджър на троянски бази данни за водещия на пазара антитроянски доставчик на Trojan Defense Suite. Съобщава се, че неговият изследователски блог, Mind Streams of Information Security Knowledge, има над 5,6 милиона активни показвания на страници и посетители, откакто е стартиран през 2005 г.

Данчо започва да се занимава с компютърна сигурност през 90-те, като проучва троянски коне и инструменти за хакване и пише за тях за софтуерна компания, която разработва анти-троянски решения.

Тези, които използват тези инструменти, определено трябва да вземат основни предпазни мерки, за да защитят собствената си поверителност, като например използването на VPN и защитени тунели.

„По-скоро бих казал, че хората трябва да търсят каква информация предоставят публично, включително социални медии, тъй като хората, включително шпиони и лоши момчета, често са склонни да си пишат домашното преди и преди стартирането на кибератаки, които включват и шпионски кампании.“ Мъдър съвет от опитен OSINT изследовател.

Вие сте блогър или изследовател по сигурността и бихте искали да имате профил тук? Споделете вашата история с нас и ние ще се радваме да я обсъдим с вас. Разузнаването на заплахи е проучване и изследване на това кой може да ви атакува, каква е тяхната мотивация и способности и какви индикатори за компрометиране във вашите системи да търсите, за да помогнете да вземете информирани решения относно вашата сигурност. Квалифицираният изследовател на разузнавателните данни за заплахите трябва да може да премахне външната информация и фалшивите аларми и да се съсредоточи само върху действащите разузнавателни данни, които пряко засягат нейните интереси.

Данчо ни каза, че „разузнаването на заплахи е неделима част от моята кариера и е нещо, което правя и практикувам ежедневно. Най-ранният ми опит с Threat Intelligence е като технически колекционер на троянски коне/вируси/червеи и VBS скриптове за LockDownCorp през 90-те години, което в комбинация с моя опит в OSINT ми позволи да създам някои от най-признатите изследователски статии в индустрията. Също така проучвам източноевропейски киберпрестъпници, както и международни и глобални спам фишинг кампании и злонамерен софтуер и информация за участниците зад тях.“

Threat intelligence и OSINT е изследване и анализ само на публични данни. LinuxSecurity беше любопитно дали Данчо някога е бил blackhat хакер. „В целия си опит като тийнейджър като бивш хакер ентусиаст съм компрометирал само един уебсайт, който беше официалният уебсайт на моя град“, пише Данчо. Той успя да получи счетоводните данни за сайта чрез социално инженерство на tripod.com по това време, за да премине през ICQ профила на системния администратор, за да получи достъп до сайта с цел промяна на началната страница, за да разпространи съобщение и всъщност да каже „здравей“ и поздравете местни приятели.

Какво е Open Source Intelligence (OSINT)?
Разузнаването с отворен код или OSINT е данни, събрани от публично достъпни източници, които да се използват в контекст на разузнаване. Въпреки че не се отнася непременно до софтуер с отворен код, OSINT вместо това се отнася повече до информация, която е отворена и достъпна за всички, като тази, която е публично достъпна в Интернет.

OSINT изследователят е опитен техник, способен да анализира бързо големи количества данни, използвайки сложни инструменти и знания за това как работят подземните мрежи в Интернет, за да разбере киберпрестъпниците и как действат.

OSINT може също да се използва за проследяване на потенциален нападател преди тази атака да се случи, както и да анализира необработени данни, за да определи кой може да бъде засегнат от атака.

В правителството на САЩ ЦРУ отговаря за събирането, производството и популяризирането на разузнавателна информация с отворен код чрез управлението на DNI Open Source Center (OSC).

В разузнавателната общност терминът "отворен" се отнася до свободно достъпна информация, обикновено в нейната сурова форма, като например в база данни. OSINT данните са полезни за получаване на информация като част от разследване - използването на OSINT не означава непременно, че данните също са лесно достъпни.

Това не се отнася непременно до информация, която може да бъде намерена с помощта на обикновени търсачки - огромна част от интернет не може да бъде намерена с помощта на основните търсачки. Вместо това „дълбоката мрежа“ се отнася до множество страници или платени стени, които не могат да бъдат индексирани от Google, но въпреки това са публично достъпни.

Например инструменти като Shodan и Censys могат да се използват за намиране на IP адреси, мрежи, отворени портове, уеб камери, принтери и почти всичко друго, което е свързано с интернет. Тези отделни части от информация могат да се комбинират с други публично достъпни части от информация, за да се разработи профил за конкретна тема, която представлява интерес от опитния анализатор.

Има и тъмна страна на OSINT - всичко, което може да бъде открито от изследователите по сигурността, може да бъде открито и от участниците в заплахите. Всъщност в края на миналата година Данчо идентифицира стотици гигабайти сурова OSINT информация в подземни форумни общности за киберпрестъпления от повече от милион уебсайтове и ги претърси за измамнически действия в опит да затвори общността.

Първи стъпки с OSINT
LinuxSecurity попита Данчев как е започнал с OSINT. Данчев пише: „През 2008 г. спечелих привилегията да бъда поканен на конферентно събитие само с покана в GCHQ, на което присъствах с проекта Honeynet. Оттогава направих многобройни ценни приноси към разузнавателната общност на САЩ като независим изпълнител и чрез изследванията, които публикувах в моя личен блог по отношение на висококачествени и никога непубликувани досега OSINT анализи като независим изпълнител.”

Данчо ни разказва за момент, когато разглеждал искания за FOIA и по-специално публично публикувана и класифицирана информация, посещавайки и преглеждайки официалния уебсайт на ЦРУ, и се натъкнал на следния цитат от любезното съдействие на президента Никсън по онова време - „Каква е ползата от тях? Имат над 40 000 души, които четат вестници." Той казва, че това го е заинтересувало от OSINT и му е помогнало да оформи бъдещето на кариерата си като разузнавателен анализатор и OSINT анализатор, работещ по NDA като независим изпълнител.

За този проект Данчо се опита да събере възможно най-много лична информация, включително уебсайтове на IoC (индикатори за компромис), включително информация за лични акаунти и имейл адреси.

Неговото изследване доведе до публикуване на списък с хиляди имейл адреси и ICQ номера на киберпрестъпници, отговорни за кражба на кредитни карти и CVV номера, наред с друга лична информация (PII).

Данчев каза, че е научил в началото на моята кариера, че най-добрият начин да се научиш в света на разузнаването за сигурност е да се присъединиш към местна общност за хакерство и сигурност. Общността за сигурност възнаграждава упоритата работа и усърдието. Докажете, че можете да говорите авторитетно по тема за сигурността, да управлявате проект и да изградите общност около него и ще бъдете признати за вашите усилия.

Анонимна комуникация чрез Tor
Един от най-полезните инструменти в арсенала на хакера за разузнаване на сигурността е Tor, безплатният софтуер с отворен код за позволяване на анонимна комуникация. Името произлиза от съкращението за името на оригиналния софтуерен проект, "The Onion Router". Първоначално Tor беше световна мрежа от сървъри, изградена за американския флот, която позволяваше на хората да сърфират в интернет анонимно.

Tor прикрива самоличността ви, като прехвърля трафика ви между различни Tor сървъри, криптирайки този трафик, така че да не се проследява обратно към вас.

Достъпът до мрежата Tor изисква използване на браузъра Tor. Обикновено се използва в

среди, в които се притеснявате да не бъдете проследени, като например ако живеете под диктатура или хакер, който иска да остане скрит от правителството.

„Вярвам, че беше около 2006 г., когато бях зает да проучвам няколко програми на правителството на САЩ, включително SPAWAR. Тогава реших да го използвам, включително няколко други инструменти за скрита комуникация, за да попреча на моя местен интернет доставчик да прихване това, което правя онлайн“, пише Данчо.

Той продължава: „По-специално по това време през 90-те много източноевропейски страни, част от Съветския съюз по това време, бяха под технологично ембарго, което беше известно като COCOM, като персоналните компютри по това време бяха нещо в линията на лукс и само организации и компаниите наистина биха могли да си ги позволят.“

Данчо също така говори за Командването на системите за космическа и военноморска война, известно като SPAWAR, и изследванията, които са направили за чуждестранното разузнаване и други US Правителствените програми като ценен ресурс.

Заплахи от нулев ден и блогове за сигурност
Данчо беше блогър по сигурността в блога Zero-Day на ZDNet в продължение на четири години, като обхващаше теми, включително най-новите кибер заплахи, киберпрестъпления, злонамерен софтуер и ботнет мрежи, както и уязвимости на операционната система и експлойти.

Данчев пише: „През този период отразявах стотици значими събития в областта на сигурността, включително уязвимости, засягащи Adobe, Apple, Google и Facebook, както и ботнет мрежи и зловреден софтуер, засягащ стотици милиони потребители. Преди доста време бях награден и с престижната награда Jesse H. Neal за най-добър блог.

В една публикация Данчо обсъди как процесът на разработване и управление на такъв ботнет е напълно автоматизиран, ефективен и най-важното - достъпен като услуга чрез злонамерен подземен доставчик на Cybercrime-as-a-Service.

Сигурен съм, че ще научим повече за това как работи в бъдещ доклад.

Асталависита, бебе
През 2003-2006 г. Данчо беше оператор на сайта за astalavista.box.sk – подземния хакерски уебсайт, докато действаше като управляващ директор, където отговаряше за управлението на съдържанието на портала и изготвянето на бюлетин за сигурност, където интервюира хора от сектора на сигурността .

В началото на 2000-те години порталът Astalavista беше един от най-широко известните и посещавани уебсайтове в света, използвани за търсене на ресурси за хакерство и сигурност с хиляди потребители, които го посещаваха ежедневно. Въпреки че първоначално е създаден като ресурс за изследователи по сигурността, той също така се превърна в популярна търсачка за експлойти за сигурност, софтуер за хакване, кракване и различни генератори на ключове и софтуерни кракове.

В днешно време - в момента той управлява проект с висок профил в оригиналния домейн Astalavista.box.sk, все още един от най-посещаваните уебсайтове в света за хакери и експерти по сигурността, включително популярен форум за сигурност.

Botnet Koobface и компрометиращи сайтове за социални мрежи
Ботнетът Koobface (анаграма за Facebook) се разпространи изключително във Facebook и успя да зарази стотици хиляди потребители в световен мащаб, използвайки кампании за социално инженерство, за да ги подмами да разкрият лични данни за себе си и своите приятели.

„В продължение на две години и половина активно наблюдавах дейностите на ботнета и

публикувах подробностите в моя личен блог. В крайна сметка научих за една-единствена грешка, допусната от един от майсторите на ботнет зад кампанията, което в крайна сметка ме накара да намеря действително идентифицираща лична информация за него, което в крайна сметка доведе до затварянето на целия ботнет Koobface по това време“, пише Данчо в своя съдействие за отстраняване на ботнет с правителството на САЩ.

Данчо работи цели дни, за да осигури действена информация за начина, по който работи ботнетът Koobface, включително действителна информация за някои от текущите и най-новите кампании, стартирани от операторите на Koobface по това време. След това той направи тази информация достъпна за по-широката индустрия за сигурност, включително правоприлагащите органи, така че те да могат действително да проследят и преследват някои от ботнет майсторите зад нея.

Бил Бренер от CSO Online съобщи в статията си „Данчо Данчев разкрива човека зад ботнета Koobface“ по времето, когато Koobface „подкани приятели да изтеглят актуализация на своя Flash player, за да гледат видео. Актуализацията е копие на вируса. Доста невероятни неща.

Стартирането на действително усилие за сваляне срещу инфраструктурата на ботнета, включително основните командни и контролни (C&C) сървъри, доведе до разпространение на лично съобщение до всички заразени хостове в международен план, което ме поздрави лично и включваше препратка към моя личен блог, последвано от друго съобщение по време на коледния сезон, включително действителни отговори точка по точка на моите „Топ 10 неща, които не знаете за Koobface Botnet“, които публикувах в блога Zero Day на ZDNet по това време, вградени във всяка заразена със зловреден софтуер хост част от ботнетът.

Това беше невероятен успех и изключително възнаграждаващо за разузнавателната общност.

Еволюцията на събирането на разузнавателна информация
Американската армия за първи път измисли термина OSINT в края на 80-те години на миналия век като начин за предоставяне на своевременно, обективно разузнаване, без пристрастия, въз основа на всички източници, достъпни за разузнавателната общност на САЩ, публични и непублични.

Когато се случиха 11 септември, бяха създадени правителствени агенции, за да се гарантира, че OSINT е основен източник за сливане и консолидиране на съответните разузнавателни данни в продукти, които могат да се предприемат.

Правителството се научи да си сътрудничи с академичните среди - университетите са идеалното място за улавяне на експертния опит, необходим за извършване на анализа.

OSINT анализаторите сега обработват огромни количества публични данни, като тези в социалните мрежи, за да открият нововъзникващи тенденции и да идентифицират ценна информация.

Инструментите, използвани за OSINT, също са се развили значително. За еволюцията на използваните инструменти Данчев пише, че „по-голямата част от инструментите, за които съм запознат, разчитат на API, включително активното използване на публични източници. Потребител Тези, които използват тези инструменти, определено трябва да вземат основни предпазни мерки, за да защитят собствената си поверителност, като например използването на VPN и защитени тунели.

„По-скоро бих казал, че хората трябва да търсят каква информация предоставят публично, включително социални медии, тъй като хората, включително шпиони и лоши момчета, често са склонни да си пишат домашното преди и преди стартирането на кибератаки, които включват и шпионски кампании.“ Мъдър съвет от опитен OSINT изследовател.

Вие сте блогър или изследовател по сигурността и бихте искали да имате профил тук? Споделете вашата история с нас и ние ще се радваме да я обсъдим с вас.

Бонус Съдържание - Интервю с Мен 02

Данчо, може ли да представиш себе си и най-новия проект на Box.sk? Можете ли да разкажете повече за опита си в борбата с киберпрестъпността, включително за приноса ви към общността за събиране на разузнавателна информация за заплахи и индустрията за сигурност на САЩ?

Казвам се Данчо Данчев. Бил съм независим създател, занимаващ се с OSINT борба с киберпрестъпленията и събиране на разузнавателна информация за заплахите повече от десетилетие и в момента ръководя една от водещите публикации за сигурност в индустрията за сигурност, която е моят личен блог, в който съм поставил основите за ефикасно и подходящо OSINT и методологията на правоприлагането по отношение на борбата и прекъсването на киберпрестъпленията в международен план, което ме накара да преследвам успешна кариера с няколко високопоставени компании и организации, базирани в САЩ през последното десетилетие след успешна кариера като бивш хакер през 90-те години. Ежедневната ми рутина се състои от копаене дълбоко в сферата на киберотбраната в контекста на реагиране и проследяване на високопоставени кампании за злонамерен софтуер, спонсорирани или насочени към националната държава, и инциденти с киберпрестъпления и следене на лошите, както обикновено, с идеята да допринеса за цялостното унищожаване на киберпрестъпността в международен мащаб и действително да допринесе за разузнавателната общност на САЩ с оперативно и тактическо разузнаване, включително активно да подкрепя правоприлагащите органи на САЩ по пътя им да проследяват и реагират на събития, свързани с киберпрестъпления в световен мащаб.

Основната ми мотивация за повторно стартиране на проект на оригиналния Astalavista.box.sk е да им „покажа как се прави“ в контекста на достигането до по-широка аудитория в контекста на предлагането на практически тактически и оперативни съвети в света на кибервойна операции информационна война и да представи хардкор и никога непубликуван преди потенциално класифициран и чувствителен материал в света на разузнавателната общност на САЩ и правоприлагащите органи на САЩ и действително да намери конструктивен и уместен начин да каже „здравей“ и „ние сме обратно" към лоялна база от потребители в световен мащаб и действително да намерим начин да "запазим духа" на Сцената така, както я познаваме. Планирал съм набор от нови високопоставени проекти, които възнамерявам да съобщавам на нашата публика на систематична и периодична основа с идеята да предложа проницателен и уникален поглед в Сцената по начина, по който я познаваме.

Кои са някои от текущите проекти на Box.sk и какво планирате за бъдещето?

В момента поддържаме високопоставен и изключително популярен блог на Wordpress, включващ форумна общност за киберсигурност и хакерство, и наскоро стартирахме изключително популярен Call for Papers и Call for Innovation част от франчайза WHGDG (World Hacker Global Domination Group). където в момента събираме съдържание в различни области и по различни теми, включително наскоро стартиран IRC сървър, включително изключително популярна търсачка за хакери и експерти по сигурността, включително предстоящото стартиране на нашия водещ публично достъпен продукт, наречен Project Cybertronics VR за Хакери и експерти по сигурността, включително предстоящо високопрофилно предаване в YouTube с участието на хора и експерти от индустрията за сигурност и сцената.

Ние също така сме подредили разнообразие от високопоставени и предстоящи управлявани от общността и обществено достъпни продукти и услуги и определено ще очакваме с нетърпение да издаваме периодични актуализации за тяхната публична и

собствена наличност. „Ако ще бъде масово, по-добре да е добро“ в контекста на възкресяването и повторното стартиране на най-популярния уеб сайт на Scene и индустрията за сигурност за хакери и експерти по сигурността в международен план.

Какво мислите за националната сигурност на САЩ в света след Сноудън?

Аз съм твърдо убеден, че изграждането на общности около изтекли и класифицирани данни може да не е най-добрият начин действително да се съобщи тяхната стойност и действително да се достигне до по-широка аудитория, която потенциално раздухва информацията за понастоящем активното и чувствително и класифицирано кибернаблюдение и тип киберразузнаване на програми, част от портфолиото от услуги, предоставени от Разузнавателната общност на САЩ. Също така съм убеден, че в крайна сметка ще се появи нов набор от подражатели, опитващи се потенциално да откраднат оперативно и тактическо ноу-хау от изтеклите данни, потенциално поставяйки основите за тяхното собствено частно и патентовано кибернаблюдение и продукти за киберразузнаване.

По отношение на националната сигурност на САЩ в свят след Сноудън, аз вярвам, че определен набор от международна фен база или действителни клъстери от поддръжници не може наистина да навреди, освен да повиши осведомеността относно действителното състояние на програмите за кибернаблюдение и киберразузнаване и техния мащаб и да достигне в международен план.

Как можете най-добре да опишете опита си в проследяването и наблюдението на ботнет Koobface?

Отне ми две години и половина активно ежедневно наблюдение на ботнета Koobface, за да изляза действително и правилно да осигуря необходимите технически изследвания и анализи зад ttой действително работи на ботнета и всъщност ми позволи да проследя и публично да разпространя разнообразна лична информация за един от ключовите членове на групата, което в даден момент доведе до пренасочване на IP блока на мрежата на Facebook към моя личен блог, включително всъщност да имам лично съобщение, вградено в десетки хиляди заразени хостове в световен мащаб, което лично да ме поздравява за моето изследване на ботнета Koobface. В един момент проучването ми за местонахождението на групата се превърна в основен източник на информация за дейностите на групата в международен план, което доведе до поредица от публикации в блогове по темата и силно ме мотивира да продължа проучването си за начина, по който ботнетът работи по това време чрез систематични и ежедневно публикуване на високопрофилни и никога непубликувани преди технически анализи и изследвания на ботнет ла

Какво е текущото състояние на борбата с киберпрестъпността в световен мащаб?

Въпреки че в момента наблюдаваме много новопоявили се доставчици и организации, които всъщност са добри в проследяването и реагирането на инциденти и дейности с киберпрестъпления, трябва ясно да се отбележи, че високопоставени мозъчни тръстове, включително независими изследователски организации и доставчици, които имат Проследявайки инциденти с киберпрестъпления и профилирайки киберпрестъпни дейности в продължение на десетилетия, трябва лесно да се считат за препоръчително четиво по отношение на техните наскоро и исторически публикувани изследвания в тази област.

Трябва също така ясно да се отбележи, че вече се провеждат широко разпространени кампании за сътрудничество между академичния търговски и частния сектор, които потенциално подкопават и допринасят за цялостното намаляване на киберпрестъпността в световен мащаб.

Това, което трябва да се направи в по-широкия контекст на борбата с киберпрестъпността в международен план, е текуща OSINT и операция на правоприлагащите органи, подобна на моята наскоро стартирана масова OSINT и

операция на правоприлагащите органи, наречена „Чичо Джордж“, включително моята най-скоро публикувана високопрофилна и достъпна онлайн безплатно Набор от данни за форума за киберпрестъпления за 2019 г., който можете да изтеглите и обработите и потенциално да се свържете с мен по отношение на действителното обогатяване и проследяване и процес на спиране.

Как можете най-добре да опишете продължаващото пресичане между правоприлагащите органи и разузнавателната общност на САЩ в контекста на стартирането на обидни законни кампании за наблюдение? Пример за това е скорошното сваляне и отвличане на основния домейн за Encrochat, собствено криптирано мобилно решение? Смятате ли, че холандските правоприлагащи органи основно са злоупотребили с технологичното си „ноу-хау“ и опит, за да се насочат към комерсиален доставчик на криптирани мобилни решения?

Една основните идей през последните няколко години е факта че различни правораздавателни органи от страни като например Холандия започват да използват техники и методологий от типа на разузнавателна агенция в борбата срещу онлайн престъпността като например се стремят да компрометират цялостно инфраструктурата на кибер престъпниците като реално погледнато имитират дейността на разузнавателна агенция като се получава ситуация на изтичане на информация за различни възможности на агенцията и правораздавателните органи което не е хубаво нещо.

Мислите ли, че стартирането на Кибер командването на САЩ е стъпка в правилната посока? Смятате ли, че публичното споделяне на патентовани версии на зловреден софтуер на VirusTotal е нарушение на OPSEC? Как мислите, че киберкомандването на САЩ може да се представи по-добре в контекста на днешната надпревара във въоръжаването в съвременната офанзивна кибервойна?

Мнението ми е че създаването на Кибер Командването на САЩ е стъпка в правилната посока от гледна точка на юриздикция в Кибер Пространството и от гледна точка на взимането на правилни решения в Кибер Пространството от страна на САЩ което включва събирането на разузнавателна информация за кибер атаки и даване на съвети както и взимане на мерки срещу тази заплахи. От гледна точка на споделянето на злонамерен код на VirusTotal мнението ми е че това е важно от гледна точкна на привличането на повече последователи който да следят актовността на Кибер Командването но като цяло не мисля че злонамерения код който се споделя е важен от гледна точкна на класифициран и такъв какъвто вече го няма.

Това което Кибер Командването може да направи евентуално публичния сектор никога няма да разбере но основно това което може да направи е да поддържа ритъма в борбата срещу кибер атаки направени от други държави и други атакуващи от типа на целенасочени атаки срещу инфраструктурата и интелектуалната собственост на фирми и организации в САЩ.

Работихте за Astalavista.com, един от основните конкуренти на Box.sk през 2003-2006 г.? Какви са вашите впечатления от работата и управлението на портала?

Това е един много важен момент от моя живот в който постигнахме много като екип с моята приятелка и групата от хора с които работехме и основно един от основните източници на приходи който имах за качествената си работа тогава и искренно се надявам хората с който работех да се доволни от гледна точка на съдържнието за което бях отговорен тогава и всички с които работех да продължават да бъдат същите професионалисти като тогава.

През периода 2003-та и 2006-та това беше един от най-популярните портали за сигурност и хакери в света и се гордея че съм работил на него и че съм имал възможност да работя с истински екип и професионалисти тогава.

Вярно ли е, че ръководите една от най-популярните публикации за сигурност в индустрията за сигурност? Как първоначално стартирахте проекта? Какво е текущото състояние на проекта?

Мисля че това е факт да. Проекта за моя личен блог беше стартиран през Декември 2005-та година докато още работех за Astalavista и основната цел беше да намеря нови читатели за мойте проучвания и също така да публикувам съдържание по темата за информационна сигурност и кибер престъпления всеки ден. В момента това е един от най-известните блогове в индустрията и искренно се надявам това да продължава да бъде така.

Какво е отношението ви към "4th party collection"?

Мисля че процеса по събиране на информация за атакуващи и кибер атаки от такъв тип сорт е процес в правилната насока където един от най-важните фактори за успех е този тип информация да бъде споделен с колкото се може повече хора и организаций с цел да може информацията да достигне до повече хора и евентуално да се изградят по-добри защити и да може хората който се занимават с този тип дейност да бъдат по-лесно проследени.

Вярвате ли, че пренаселената индустрия за сигурност означава по-нисък OPSEC за високопрофилни операции?

Мисля че съм съгласен. Основната идея е че когато много компаний от частния сектор се занимават с такъв тип дейност и реално погледнато не споделят своите знания с правителството може да се получи ситуация в която разузнавателна агенция може да работи по случеи по който вече са работили фирми от индустрията и това може да се отрази върху качеството на операцията за залавянето и следенето на кибер престъпници.