ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

Пайдаланылған әдебиеттер тізімі

1. Таненбаум Э., Уэзеролл Д. Компьютерные сети. – 5-е изд. – СПб.: Питер, 2012. – 960 с. [https://kr-labs.com.ua/books/Tenenbaum_KS.pdf]
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. – 2-е изд. – М.: Триумф, 2006. – 816 с. [https://kr-labs.com.ua/books/Bryus_Shnayer_-_Prikladnaya_Kriptografia.pdf]
3. Лапонина О.Р. Основы сетевой безопасности. – Национальный Открытый Университет «ИНТУИТ» , 2014. – 384 с [http://master.cmc.msu.ru/files/Laponina-1.pdf]
4. Kurose J., Ross K. Computer Networking: A Top-Down Approach. – 7th ed. – Pearson, 2017. –912p. [https://www.ucg.ac.me/skladiste/blog_44233/objava_64433/fajlovi/Computer%20Networking%20_%20A%20Top%20Down%20Approach,%207th,%20converted.pdf]
5. Kali Linux операциялық жүйесі [https://www.kali.org/get-kali/#kali-platforms]
6. NMAP утилитасы [https://nmap.org/download]
7. Telegram әлеуметтік желісі [https://web.telegram.org/]

ФИШИНГ: ЖЕЛІДЕГІ BEEF ӘДІСІ АРҚЫЛЫ АЛДАУ ЖӘНЕ ОДАН САҚТАНУ

Таубай М.Е. Раматуллаев Ә.А.
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Астана, Қазақстан.
maditaubay04@gmail.com alimramatullaev@gmail.com

Аңдатпа

Бұл мақалада біз сілтеме арқылы шабуыл жасау түрлерін қарастырамыз. Біздің қарастыратындарымыз фишинг және BeEF (Browser Exploitation Framework), сондай-ақ екеуінің өзара байланысын және осы қауіптерден қорғану әдістерін талдаймыз. Хакерлердің BeEF-ті қалай өздеріне тиімді етіп пайдаланатынын және пайдаланушылар мен ұйымдардың осы шабуылдарға төтеп бере алатындай қандай қадамдар жасайтынын талқылаймыз.

Кілттік сөздер: фишинг, әлеуметтік инженерия, BeEF, интернет қауіпсіздігі, киберқауіп, қорғаныс әдістері.

1. Кіріспе

Интернеттегі қауіптер күн сайын күрделене түсуде, ал киберқылмыскерлер пайдаланушылардың жеке деректерін алу үшін жаңа әдістерді қолдануда. Солардың ішінде ең көп тарағаны – **фишинг**. Бұл – алаяқтықтың кең таралған түрі, оның көмегімен қаскүнемдер логиндер, парольдер, банк карталарының деректері сияқты маңызды ақпаратты қолға түсіреді. Сонымен қатар, **BeEF (Browser Exploitation Framework)** құралы веб-шолғыштардың осалдықтарын пайдаланып, шабуылдаушыларға қосымша артықшылықтар береді.[1]

Фишингтің қаупі

Фишингтің басты қаупі – оның адамдарды алдау арқылы жүзеге асуы, сондықтан одан толық қорғану қиын. Компаниялар ақпараттық қауіпсіздік бойынша оқыту жүргізсе де, алаяқтар өз әдістерін жетілдіріп отырады.

Фишингтің тағы бір қатері – құпия деректердің қолды болуы. Егер **логин мен құпиясөз** ұрланса, қолданушы аккаунтынан айырылуы мүмкін. **Банк картасының мәліметтері** түссе, алаяқтар қаржыны иемденуге тырысады. Ал жеке ақпарат көбіне **үшінші тараптарға сатылады, интернетте жарияланады** немесе **қосымша шабуылдарға қолданылады**.[2]

Бұл мақалада фишинг түрлері, BeEF-тің жұмыс істеу принциптері және осындай шабуылдардан қорғану әдістері қарастырылады.

Фишинг түрлері және әдістері

Фишинг – кибершабуыл түрі, онда зиянкестер пайдаланушыларды құпия сөздер, несие картасы деректері немесе корпоративтік жүйелерге қол жеткізу сияқты құпия ақпаратты беру үшін алдайды. Фишинг әлеуметтік инженерияға негізделген: шабуылдаушылар жалған электрондық хаттар, веб-сайттар немесе әлеуметтік медиа хабарламалар жасау арқылы сенімді адамдар немесе ұйымдар ретінде жасырылады.[3]

1. **Email-фишинг** – Фишерлер жалған электрондық хаттарды жібереді, пайдаланушыларды алдап, оларды зиянды сілтемеге өту сияқты жеке ақпаратты ашуға тырысады. [3]
2. **Spear phishing (нысаналы фишинг)** – бұл әдеттегі фишингтің жекелендірілген нұсқасы. Жаппай жіберудің орнына зиянкестер белгілі бір адамдарды немесе компанияларды таңдайды. Олар өз хабарламаларын мүмкіндігінше сенімді және сенімді ету үшін әлеуметтік желілер немесе басқа қол жетімді көздер арқылы өз мақсаттары туралы ақпаратты алдын ала жинай алады. [3]
3. **Vishing (Voice phishing)** – бұл телефон қоңыраулары арқылы жасалатын фишинг. Алаяқтар пайдаланушыларға қоңырау шалып, банк карталарының құпия деректерін, жүйелерден логиндерді немесе басқа ақпаратты алу үшін банк, қауіпсіздік, техникалық қолдау қызметкерлерімен таныстырады. Көбінесе шабуылдаушылар нөмірлерді ауыстыру технологиясын қолданады, бұл сізге сенімді ұйымдардың қоңырауларына ұқсас қоңыраулар жасауға мүмкіндік береді. [3]
4. **Smishing (SMS phishing)** – бұл алаяқтар SMS хабарламаларын қолданатын фишингтің бір түрі. Электрондық пошта алаяқтығы сияқты, шабуылдаушылар мәселені шешу үшін сілтемеге өтуді немесе нөмірге қоңырау шалуды ұсынатын жалған хабарламалар жібереді. [3]
5. **Whaling** ("үлкен балықты" аулау) – бұл компанияның жоғары лауазымды тұлғаларына бағытталған spear-фишингтің бір түрі: мысалы, бас және қаржы директорлары. Шабуылдар мұқият ойластырылуы мүмкін, өйткені мұндағы ставкалар әлдеқайда жоғары.[3]

Мақалада BeEF және оның қолданылуын қарастырылды, айта кетсек BeEF (Browser Exploitation Framework) – веб-шолғыштардың осалдықтарын анықтау және оларды пайдалану үшін жасалған құрал. Бастапқыда бұл фреймворк ақпараттық қауіпсіздік мамандары үшін тестілеу мақсатында әзірленсе де, кейіннен оны хакерлер мен алаяқтар да белсенді қолдана бастады.

BeEF қалай жұмыс істейді?

1. **Жәбірленушіні шабуылға ұшырату** – пайдаланушы зиянды сілтемеге өтеді немесе шабуылдаушы арнайы код енгізілген сайтқа кіреді.
2. **Шолғыштың осалдығын пайдалану** – BeEF арқылы шабуылдаушы пайдаланушының браузеріне қосылып, оған түрлі командалар жібере алады.
3. **Деректерді ұрлау** – шабуылдаушы құрбанының сессия мәліметтерін, cookie-файлдарын, сақталған парольдерін және басқа да жеке ақпараттарын жинай алады.
4. **Құрылғыны басқару** – кейбір жағдайларда шабуылдаушы жәбірленушінің құрылғысын қашықтан бақылап, веб-камераны қосу, пернетақта әрекеттерін тіркеу және сайттарға автоматты түрде қайта бағыттау сияқты әрекеттерді орындай алады.[4]

Қорғаныс әдістері

Зерттеу барысында келесі қорғаныс әдістері қарастырылды:

1.Браузер қауіпсіздігін қамтамасыз ету

- **Браузерді жаңарту:** зерттеу кезінде браузердің соңғы нұсқасын пайдалану қажеттілігі талданды. Сонымен қатар, осалдықтарды жоятын патчтарды уақытылы орнатудың маңыздылығы атап өтілді.

2.Желілік қауіпсіздікті күшейту

- **VPN және прокси-серверлерді қолдану:** IP-мекенжайды жасыру және қосымша шифрлау деңгейін қамтамасыз ету арқылы желілік қауіпсіздікті арттыру әдістері зерттелді.
- **Қауіпті сайттарды бұғаттау:** желілік әкімшілеу құралдарын пайдалану арқылы белгісіз немесе күдікті сайттарға кірудің алдын алу мүмкіндігі қарастырылды.

3.Зиянды скрипттерден қорғау

- **JavaScript-ті шектеу:** зерттеу барысында белгісіз сайттарда JavaScript-ті өшіру әдістері қарастырылып, тек сенімді көздерден ғана скрипттерді орындауға рұқсат беру қажеттілігі анықталды.
- **Қауіпті браузер сессияларын болдырмау:** HTTPS қосылымдарын ғана пайдалану және белгісіз Wi-Fi желілерінде жұмыс істемеу арқылы қауіпсіздікті қамтамасыз ету жолдары қарастырылды.

4.Қолданушыларды оқыту және қауіпсіздік мәдениетін дамыту

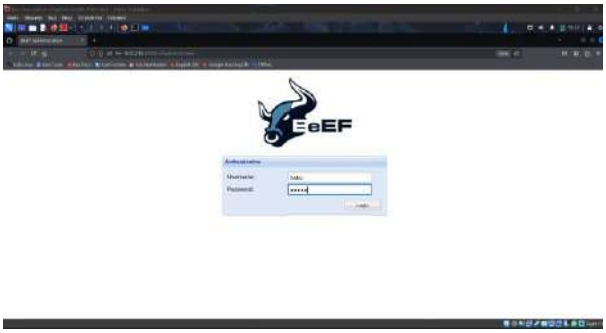
- **Киберқауіпсіздік бойынша оқыту:** BeEF және басқа браузерлік шабуылдар туралы ақпараттандырудың маңыздылығы зерттелді. Сонымен қатар, қауіпсіздік саясатын енгізу қажеттілігі қарастырылды.
- **Ескертулер мен тестілеу:** персоналға әлеуметтік инженерия шабуылдарын анықтау бойынша тренингтер өткізу және браузерлік осалдықтарға тест жүргізу әдістері зерделенді.

Зерттеу нәтижесінде жоғарыда аталған қорғаныс шараларының тиімділігі талданып, оларды тәжірибеде қолдану мүмкіндіктері қарастырылды.[5]

Тәжірибелік жұмыс:

1-сурет: BeEF серверін іске қосу

Бұл суретте біз Kali Linux терминалын ашып BeEF серверін іске қосу процесін көрсетеміз. **Hook URL:** Бұл URL-ге кірген браузер. Бұл браузерге шабуыл жасауға мүмкіндік береді. **UI URL:** Бұл BeeF басқару панеліне кіру үшін қолданылатын сілтеме. **HTTP Proxy:** BeeF басқа жүйелердің трафигін бақылауға арналған прокси қызметін де іске қосады. **RESTful API:** BeeF API арқылы сыртқы қосымшалардан командаларды орындауға мүмкіндік береді. Біз **ctrl** батырмасымен **UI URL деп тұрған сілтемеге басамыз.Содан бізді сайтқа жібереді.**

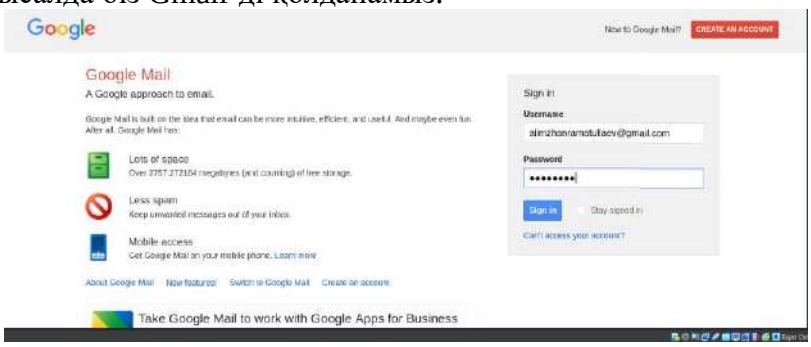


2-сурет: BeEF басқару панеліне кіру

Бұл суретте BeEF басқару панелінің кіру беті көрсетілген.Бұл жерде біз логин мен құпия сөзімізді теріп жүйеге кіреміз.

3-сурет: BeEF басқару панелі

BeeF басқару панелінің негізгі интерфейсі көрсетілген.Осы жерде бізге жүйеге кірген адамның **IP** адресі көрсетіледі.Содан кейін біз браузерге қосылған модулі бар терезені басып, Командалар және әлеуметтік инженерия қалтасынан Pretty Theft табыңыз және Орындау батырмасын басыңыз. Фишингтің әртүрлі әдістері бар, мысалы Facebook, LinkedIn және басқалары. Бұл мысалда біз Gmail-ді қолданамыз.



4-сурет: Фишинг (Pretty Theft модулі)

Бұл суретте жалған Google Gmail беті көрсетілген. Браузерде gmail почтасына кіру терезесіне ұқсайтын жалған форма пайда болады.Пайдаланушыдан электрондық пошта мен құпия сөзді енгізу сұралады.Бұл BeeF-тің **"Google Phishing"** модулі арқылы жасалған.Егер пайдаланушы логин мен құпия сөзін енгізсе, олар BeeF басқару панеліне жіберіледі.

5-сурет: Командалар және ұрланған деректер

BeeF басқару панеліндегі **Командалар** қойындысын көрсетеді.**"Module Tree" :** Мұнда браузерге жіберуге болатын әртүрлі шабуыл модульдері бар. Мысалы, "Pretty Theft," "TabNabbing," "Google Phishing" және т.б.

Қорытынды

Менің ойымша, қазіргі таңда фишинг – ең қауіпті кибершабуылдардың бірі болып табылады. Оны BeEF сияқты құралдар одан әрі күшейтіп, жеке адамдарға ғана емес, ірі ұйымдарға да зор зиян келтіруі мүмкін. Қорытындылай келе BeEF – браузер осалдықтарын пайдаланып, құрылғыны қашықтан басқаруға мүмкіндік беретін қауіпті құралдардың бірі. Бұл әдіспен шабуылдаушылар пайдаланушының сеансын бақылап, зиянды әрекеттерді орындай алады. Сондықтан BeEF шабуылдарынан қорғанудың ең тиімді жолы – үнемі қырағылық танытып, қауіпсіздік шараларын дер кезінде қолдану. Әрбір қолданушы өз құрылғылары мен жеке деректерінің қауіпсіздігін қамтамасыз ету үшін интернеттегі қауіпсіздік ережелерін сақтап, қауіпсіздік жүйелерін жаңартып отыруы қажет.

Қолданылған әдебиеттер тізімі:

1. Митюков Е. А., Затонский А. В. Модель обнаружения фишинговых атак на основе гибридного подхода для защиты автоматизированных систем управления производством // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2020. №2 https://cyberleninka.ru/article/n/model-obnaruzheniya-fishingovyh-atak-na-osnove-gibridnogo-podhoda-dlya-zaschity-avtomatizirovannyh-sistem-upravleniya-proizvodstvom

2. Фишинг: ловись рыбка большая и маленькая [электронный источник, дата просмотра 19.05.2021] https://habr.com/ru/companies/pentestit/articles/558138/

3. https://blog.skillfactory.ru/chto-takoe-fishing/ Какие бывают типы фишинга?

4. Ronak Sharma, Phishing Attack Sample [электронный источник, дата просмотра 19.03.2025] \\ https://medium.com/@ronak.d.sharma111/phishing-attack-sample-8ff1260c680c

5. Фишинговые письма: как их распознать и не стать их жертвой //https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips