ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

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 и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

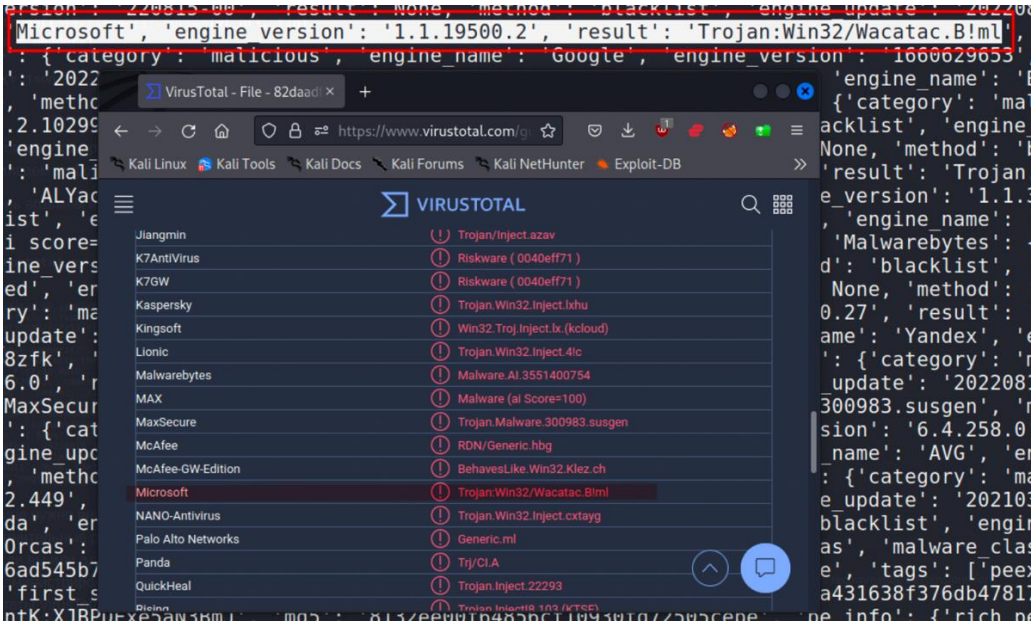

Figure 5. The result of API request

This program in python can be modified and improved, for example, by adding the calculation of other hashes of the test sample: MD5 and SHA-1 calculations. We believe that our program, written for educational and research purposes, will help novice Malware Analyst specialists and will also serve as a good foundation for more advanced and complex programs to automate routine processes of static malware sample research in the future.

References

1. https://www.virustotal.com
2. https://www.python.org/downloads/windows/
3. https://samples.vxunderground.org/APTs/2022/2022.09.07(2)/Samples/f6827dc5af661fb b4bf64bc625c78283ef836c6985bb2 bfb836bd0c8d5397332.7z

ӘОЖ 004.056.55

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ ИНЦИДЕНТТЕРДІ ТЕРГЕУ ҚҰРАЛДАРЫН САЛЫСТЫРМАЛЫ ТАЛДАУ

Мырзақұл Жансая Нұрматуллақызы
Zhansaya.myrzakul@mail.ru
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, ақпараттық технологиялар факультеті, ақпараттық қауіпсіздік кафедрасының студенті
Астана, Қазақстан
Ғылыми жетекші – Ахметова Ж.Ж., PhD, доцент

Қазіргі әлем цифрлық технологияларға көбірек көшуде, бұл ақпараттық қауіпсіздік инциденттерінің көбеюіне әкеледі. Әртүрлі ұйымдар, соның ішінде мемлекеттік органдар, компаниялар және жеке тұлғалар киберқауіпсіздік қаупіне және оқиғаларды тергеу үшін қажетті әрекеттерге тап болады.

Ақпараттық қауіпсіздік оқиғаларын тергеу үшін осы саланың мамандары қолдана алатын көптеген құралдар бар. Бұл құралдарға қауіпті анықтау және алдын алу бағдарламалық құралы, желілік трафикті талдау құралдары және ақпараттық жүйелердің қауіпсіздігін физикалық тексеруге арналған арнайы жабдық кіреді.

Алайда, ақпараттық қауіпсіздік саласындағы оқиғаларды тергеудің барлық құралдары бірдей емес. Олардың артықшылықтары мен кемшіліктері бар және белгілі бір құралды таңдау

оқиғаның түрі, бюджет, қызметкерлердің біліктілік деңгейі және т.б. сияқты көптеген факторларға байланысты.

Бұл мақалада біз ақпараттық қауіпсіздік саласындағы оқиғаларды тергеудің ең танымал құралдарына салыстырмалы талдау жасалды және олардың артықшылықтары мен кемшіліктерін анықталып көрсетілді. Бұл ақпараттық қауіпсіздік мамандарына белгілі бір мәселені шешудің ең қолайлы құралын анықтауға және олардың жұмысының тиімділігін арттыруға көмектеседі.

Ақпараттық қауіпсіздік инциденті (АҚ инциденті) - құпия деректердің ағып кетуіне немесе жоғалуына, жүйенің бұзылуына, ұйымның беделінің нашарлауына және басқа да жағымсыз салдарға әкелуі мүмкін ақпарат қауіпсіздігінің бұзылуына байланысты жағымсыз оқиға. АҚ инциденттерінің бірнеше мысалдарын 1-кестеде көрсетілген:

АҚ инцидент түрі	**Сипаттамасы**
Кибершабуылдар	-құпия ақпаратқа қол жеткізу немесе жүйенің жұмысын бұзу мақсатында шабуылдаушылардың ұйымның немесе жеке тұлғаның компьютерлік жүйесіне шабуылы.
Деректердің бұзылуы	-клиенттердің жеке деректері, қаржылық деректер және т. б. сияқты құпия ақпаратты байқаусызда немесе қасақана ашу.
Компьютерге немесе құрылғыға жұқтыруы мүмкін вирустар мен зиянды бағдарламалар	бұл құпия деректердің ағып кетуіне, жүйенің бұзылуына және деректердің жоғалуына әкелуі мүмкін.
Фишинг	-алаяқтық әдісі, онда шабуылдаушы жеке ақпаратқа қол жеткізу үшін ресми электрондық пошта жіберушісі болып көрінеді.
Желі қауіпсіздігінің бұзылуы	-бұл құпия деректердің ағып кетуіне және жүйенің қауіпсіздігіне қауіп төндіретін желі қауіпсіздігінің бұзылуы.
Рұқсатсыз кіру	-бұл иесінің рұқсатынсыз жүйеге кіру, бұл құпия ақпараттың ағып кетуіне немесе жоғалуына әкелуі мүмкін.
Әлеуметтік инженерия	-бұзушы құпия ақпаратқа қол жеткізу үшін әлеуметтік манипуляцияны қолданатын бұзу әдістері.

1-кесте. АҚ инциденттерінің түрлері

Сондай-ақ, мұнда әлемдегі ақпараттық қауіпсіздік статистикасының бірнеше мысалдары келтірілген:

2021 жылы әлемдегі кибершабуылдардың жалпы саны 2020 жылмен салыстырғанда 22% - ға өсті (check point деректері).

2020 жылы әлемде 5 млрд-тан астам деректердің бұзылуы тіркелді, бұл өткен жылмен салыстырғанда 273% - ға ұлғайды (Risk Based Security компаниясының деректері).

Әлемдегі компаниялар үшін деректерді бұзудың орташа құны 3,86 миллион долларды құрайды (IBM компаниясының деректері).

2021 жылы әлемдегі компаниялардың 90%-дан астамы COVID-19 пандемиясына байланысты үйде жұмыс істеу кезінде қауіпсіздікке қауіп төндірді (check point деректері).

2021 жылы әлемдегі ірі компаниялардың 80% - дан астамы қауіпсіздік деңгейін жақсарту үшін мультифакторлық аутентификацияны енгізді (Microsoft корпорациясының деректері).

2021 жылы әлемдегі ұйымдардың 50% - дан астамы бірнеше күн немесе тіпті апта ішінде деректердің бұзылуын анықтай алмайды (Varonis деректері).

Алайда, ақпараттық қауіпсіздік статистикасы көптеген факторларға байланысты өзгеруі мүмкін екенін атап өткен жөн, мысалы, географиялық орналасуы, ұйымның түрі мен мөлшері, әртүрлі қорғаныс әдістері мен құралдарын қолдану және т. б. Бірақ осы деректердің статистикасының өзі ақпараттық қауіпсіздік инциденттерді құралдардың көмегімен де дұрыс анықтай алмау мүмкіндіктерін қарастырады.

АҚ-инциденттер туындаған жағдайда ақпараттың қауіпсіздігін қалпына келтіру, қайталанған инциденттердің алдын алу және жағымсыз салдарларды барынша азайту жөнінде шаралар қабылдай отырып, оларға тез және тиімді әрекет ету маңызды. Сондай-ақ, қорғаныс жүйелерін орнату, бағдарламалық жасақтаманы үнемі жаңартып отыру және қызметкерлерге ақпаратты қауіпсіз пайдалану ережелерін үйрету сияқты ықтимал АҚ оқиғаларының алдын алу шараларын қабылдау қажет. Төменде қазіргі таңдағы ақпараттық қауіпсіздік салсындағы әлемдік статистикалар мен зерттеулер бойынша 2-кесте құрылды. Кестеде ең танымал 5 құрал атаулары және нақты артықшылығы мен кемшілігі бар құралдарға анықтамалар көрсетілген.

Құрал атауы	Сипаттамасы	Артықшылығы	Кемшіліктері
SIEM (Security Information and Event Management)	Қауіпсіздік туралы ақпаратты басқару жүйесі және оқиғаларды басқару	Нақты уақыттағы оқиғаларды бақылау, деректерді орталықтандырылған сақтау, ережелер мен модельдерге негізделген оқиғаларды талдау	Жоғары шығындар, іске асырудың күрделілігі және теңшеу
EDR (Endpoint Detection and Response)	Периметрлік қорғаныстан өткен қауіптерді анықтауға және оларға жауап беруге арналған құрал	Қауіптерді анықтаудың жоғары дәлдігі, нақты уақыттағы қауіптерге жауап беру қабілеті	Іске асыру және теңшеу қиындықтары
Forensic Toolkit (FTK)	Компьютерлер мен мобильді құрылғылардағы деректерді анықтау, талдау және қалпына келтіру құралы	Жоғары сканерлеу жылдамдығы, қуатты деректерді іздеу және талдау, жойылған деректерді қалпына келтіру мүмкіндігі	Жоғары құны, әрқашан жасырын қауіптерді анықтай бермейді
Wireshark	Желілік трафикті талдау құралы	Тегін, әртүрлі деңгейдегі деректер пакетін талдау мүмкіндігі	Белгілі бір дағдылар мен білімді қажет етеді, шифрланған трафикті талдауда әрдайым тиімді бола бермейді
Nmap	Желілерді сканерлеу және осалдықтарды анықтау құралы	Тегін, әртүрлі деңгейдегі желілерді сканерлейді, осалдықтарды анықтайды	Белгілі бір дағдылар мен білімді қажет етеді, қорғалған желілерді сканерлеу кезінде әрдайым тиімді бола бермейді

2-кесте. Ақпараттық қауіпсіздік инцидентттерін тергеуге арналаған танымал 5 құрал

Белгілі бір құралды таңдау көптеген факторларға байланысты екенін және ұйымның нақты қажеттіліктері мен қызметкерлердің біліктілік деңгейіне негізделуі керек екенін ескеру маңызды.

Төменде ақпараттық қауіпсіздік ұйымдарында қолданылатын бес танымал SIEM жүйесінің тізімі берілген:

- Splunk Enterprise Security
- IBM QRadar
- McAfee Enterprise Security Manager (ESM)
- LogRhythm NextGen SIEM Platform
- Elastic GYM

Бұл тізім ақпараттық қауіпсіздік саласындағы сарапшылар мен пайдаланушылардың пікірлері мен отзывтарына негізделген және әр ұйымның нақты қажеттіліктері мен қалауына байланысты өзгеріп отырады.

Ақпараттық қауіпсіздік инциденттерін тергеу құралдарын салыстырмалы талдаудан және зерттеулерден кейінгі тұжырымдар мен қорытындылар келесідей болып қалыптасты:

1. Ақпараттық қауіпсіздік оқиғаларын тергеудің көптеген құралдары бар, олардың әрқайсысының өзіндік артықшылықтары мен кемшіліктері бар.
2. SIEM жүйелері ақпараттық қауіпсіздік оқиғаларын анықтауға және тергеуге арналған ең танымал құралдардың бірі болып табылады.
3. SIEM жүйелері оқиғаларды тергеу үшін айтарлықтай ақпарат пен контекст бере алады, бірақ оларды орнату және пайдалану үшін белгілі бір білім мен дағдыларды қажет етеді.
4. Оқиғаларды қолмен тергеу ақпараттың қауіпсіздігін қамтамасыз етуде әлі де маңызды рөл атқарады, бірақ бұл өте көп уақытты қажет етеді және ресурстарға үлкен шығындарды қажет етеді.
5. Әрбір ұйым өзінің инфрақұрылымы мен бизнес-процестерінің ерекшеліктерін ескере отырып, оның қажеттіліктері мен мүмкіндіктеріне сәйкес оқиғаларды тергеу құралдарын таңдауы керек.

Осылайша, ақпараттық қауіпсіздік инциденттерін тергеу құралдарын таңдағанда, ұйымдар көптеген факторларды, соның ішінде сараптама деңгейін, ресурстардың қолжетімділігін және ақпарат қауіпсіздігінің нақты қажеттіліктерін ескеруі керек.

Пайдаланылған әдебиеттер тізімі

1. Бриц, М.Т. Компьютерная криминалистика и киберпреступность: Введение / М.Т. Бриц. – СПб.: Питер, 2015. – 448 с.
2. Le-Khac, N.-A. Digital Forensics and Cyber Crime: First International ICST Conference, ICDF2C 2009, Albany, NY, USA / N.-A. Le-Khac, M.S. Olivier, G. Peterson. – Berlin: Springer, 2009. – 223 p.
3. Davidoff, S. Network Forensics: Tracking Hackers through Cyberspace / S. Davidoff, J. Ham. – Upper Saddle River, NJ: Prentice Hall, 2012. – 576 p.
4. EC-Council. Computer Forensics: Investigating Network Intrusions and Cyber Crime. – Cengage Learning, 2014. – 640 p.
5. Sammons, J. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics / J. Sammons. – Burlington, MA: Syngress, 2014. – 216 p.
6. Carrier, B. File System Forensic Analysis / B. Carrier. – Upper Saddle River, NJ: Addison-Wesley, 2005. – 592 p.
7. Carvey, H. Windows Forensic Analysis Toolkit, Fourth Edition: Advanced Analysis Techniques for Windows 8 / H. Carvey. – Burlington, MA: Syngress, 2014. – 744 p.
8. Национальный институт стандартов и технологий. Карманный справочник по реагированию на инциденты: краткое руководство для реагентов / НИСТ. – Москва: Третий Рим, 2019. – 64 с.
9. Malin, C.H. Real-World Incident Response: Behind the Keyboard / C.H. Malin, E. Casey, J.M. Aquilina. – Indianapolis, IN: Syngress, 2018. – 544 p.

10. Altheide, C. Digital Forensics with Open Source Tools / C. Altheide, H. Carvey. – Burlington, MA: Syngress, 2011. – 288 p.
11. Casey, E. The Handbook of Computer Crime Investigation: Forensic Tools and Technology / E. Casey. – Amsterdam: Elsevier, 2001. – 762 p.
12. Shipley, T.G. Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace / T.G. Shipley, A. Bowker. – Amsterdam: Elsevier, 2013. – 336 p.
13. Anson, S. Mastering Windows Network Forensics and Investigation / S. Anson, S. Bunting. – Indianapolis, IN: Wiley, 2012. – 696 p.
14. Fichera, J. Network Intrusion Analysis: Methodologies, Tools, and Techniques for Incident Analysis and Response / J. Fichera, S. Bolt, T. Layton. – Rockland, MA: Syngress, 2012. – 280 p.

ӘОЖ 004.056+332.1

«АҚЫЛДЫ КӨЛІК ЖҮЙЕСІНІҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІ»

Нұрғалиқызы Маржан
nurgalikyzy_m@mail.ru
Ақпараттық технологиялар факультетінің 2 курс магистранты
«Л. Н. Гумилев атындағы Еуразия ұлттық университеті» КеАҚ,
Астана, Қазақстан
Ғылыми жетекшісі – Қонырханова Асем

Аңдатпа: Ақпарат дамып, күннен-күнге жаңа технологиялар қолданылып жатыр. Бізді қоршаған орта ақпаратпен тығыз байланысты. Кез-келген мәліметті интернеттен қарап тауып жатамыз. Үлкен алпауыт компаниялар да адамдардың жұмыс күшінің орнына түрлі технологияларды ойлап тауып, қолданысқа енгізуде. Соның бірі, ақылды көлік жүйесі. Адамдардың қажеттілігіне орай қазіргі кезде көлік транспорты күннен-күнге жақсарып келе жатыр. Қоғамдық көлік аялдамалары, жеке тұрақтар, жаяу жүргіншілер өткелдері және бағдаршамдар секілді бірқатар мәселелер ақылды көлік жүйесімен байланысты болуда. Мысалы, әртүрлі сандық көздерден үздіксіз келетін гетерогенді ақпараттың массивін gps сенсорлары, камералар, пайдаланушылардың мобильді қосымшаларда іске асып жатады.

"Ақылды көлік" жүйесінің аналитикалық рөлі, жол қозғалысын ұйымдастырудағы өзгерістерді бақылаудан тұрады. Демек, бағдаршамдар реттеледі, көшелердің кеңейтілуі, бір жақты қозғалысты ұйымдастыру туралы шешімдер қабылданады, жаяу жүргіншілер аймақтары реттеледі. Көлік аналитикасының өнімі ақпараттық қолдау іске асырылады. бұл тек электрондық таблолар ғана емес,өз елімізде қолданысқа ие Яндекс , индрайвер секілді барлық қызметтер мен қолданушы қосымшалары және карталар, навигаторлар. Мысалы, көліктің бақылау тақтасындағы дисплей қардың салдарынан жұмысқа әдеттегі жолмен жету қиын болатындығы туралы ескертеді және маршрутты қайта құруды ұсынады. "Ақылды көлікке" арналған аналитикалық жүйелер туралы айтатын болсақ, нарық мамандары бірінші кезекте 1970 ж Артур Симстің жұмысы негізінде жасалған австралиялық Сиднейдегі scats (Sydney Coordinated Adaptive Traffic System) жол қозғалысын басқарудың адаптивті жүйесін еске түсіреді. Қазір SCAT әлемнің 27 еліндегі 37 мың қиылысқа қызмет көрсетеді. Ақылды көлік тек жүргізушісіз көлік қана емес, сонымен қатар көптеген салалар мен компанияларды қамтитын бүкіл экожүйе десек те болады.

Түйінді сөздер: ақылды көлік, қауіптер, карталар, қосымшалар, аналитикалық жүйе

Кіріспе

Ақылды көлікті дамыту бағыттарының бірі-пилотсыз көлік. Қазіргі уақытта пилотсыз көлік негізінен әуе кеңістігінде және метрода кедергілер мен штаттан тыс жағдайлардың аздығына байланысты қолданылады. Автокөлік жүргізушісіз көлік жайлы, автомобиль электроникасына жасанды интеллектті енгізу бойынша зерттеулер мен сынақтар жүргізілуде Мысалы, Nissan, Mercedes-Benz, Audi, Tesla, Volvo, Google, Apple.

Жол қозғалысына ықпал ететін: көлік құралдары, жол белгілері, бағдаршамдар, бақылау және қауіпсіздік жүйелері және 3G, 4G, LTE ұялы желілері, Wi-Fi, Bluetooth, LoRa, NB-IoT сияқты