РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

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 378

ББК 74.58

ISBN 978-9965-31-997-6

ӘОК 004. 056

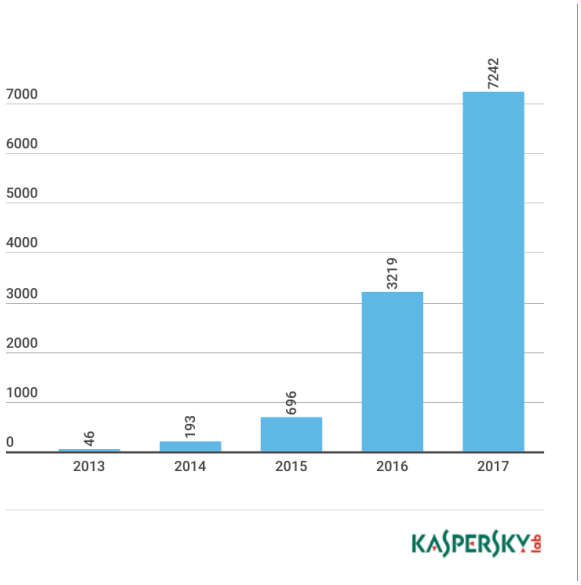
IOT ҚАУІПСІЗДІГІ ЖӘНЕ ШАБУЫЛДАРҒА ШОЛУ

Сисенов Нұрбек Маханбетұлы, Улюкова Гулден Бектемировна
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті, Информатика және ақпараттық қауіпсіздік кафедрасы оқытушылары, Астана, Қазақстан
Оразкелдиев Айболат Жанболатұлы
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті,Ақпараттық қауіпсіздік жүйелері мамандығы студенті, Астана, Қазақстан

Ақпараттық коммуникациялық технологиялар кілтті бағыттарының бірі IoT концепциясы болып табылады. Гартнер (Gartner) компаниясының IT аналитиктері 2020 жылға қарай IoT-құрылғылар саны 20,4 млрд жетеді деп болжайды. Бірақ мамандар IoT құрылғыларын экспоненциялды ендіру ақпараттық қауіпсіздікке талаптарды жоғарылатады деп ескерту жасайды, өйткені оларды құру кезінде бұл аспектке жеткілікті назар аударылмады. Байланыс үшін негізінде бұлтты есептеулерді қолдану да «бұзу» және кибершабуыл қаупін жоғарылатады. 2016 жылы «ақылды құрылғылардың» қауіпсіздігі тақырыбына қызығушылықты біршама арттырған оқиғалар қатары орын алды. Олардың ішінде OVH француз хостинг компаниясына және Dyn американдық DNS-провайдерлеріне қуаттылығы жағынан рекордты DDoS-шабуылдарды атауға болады. Бұл шабуылдардың роутерлер, IP-камералар, принтерлер және басқа да құрылғылардан құралған ірі ботнеттің көмегімен ұйымдастырылғандығы белгілі.

Сонымен қатар 2016 жылдың соңында әлемге роутерлерден тұратын алып ботнет (5 млн.-ға жуық) туралы мәлім болды. Бұл мәселелер желілік құрылғылармен шектеліп қана қойған жоқ: қауіпсіздікпен қиындықтар Miele ыдыс жуғыш машиналарында және AGA асхана плиталарында табылды. Сонымен қатар BrickerBot зиянкесі «әріптестеріне» қарағанда тек жұқтырып қана қоймай, сонымен қатар осал құрылғыларды толықтай істен шығаратын.

Gartner мәліметтері бойынша әлемде қазіргі уақытта ақылды құрылғылардың саны 6 миллиардтан асады. Осал болуы ықтимал құрылғылардың соншалықты көп саны қаскүнемдердің назарынан тыс қалмады: деректер бойынша 2017 жылдың мамыр айында «Касперский зертханасы» топтамасында «ақылды құрылғылар» үшін арналған мыңдаған түрлі зиянкес программалық қамтамалар болды, және де олардың ішіндегә жартысына жуығы 2017 жылда қосылған болатын.



«Ақылды құрылғылар үшін арналған зиянкес программалық қамтамалар нұсқалары санының өсуі, 2013-2017 ж.ж.

IoT үлкен мүмкіндіктер қалыптастырады. Мысалы, ұйқыдан тұрғанда сіздің үй қолайлы температураға дейін жылытылған, ал сіздің кофеңіз дайын – және нақты уақытқа байланысты емес, сіздің оянған сәтке негізделіп дайын болатын әлемді елестетіңіз. Автокөлігіңіз пайда болайын деген ақаулар туралы сізге хабарлап, автоматты түрде жақын кәсіпорынмен байланысып, қосымша бөлшектердің барын тексереді. IoT сонымен қатар көптеген жаңа зияны көбірек болуы ықтимал, тіпті жойқын қауіптер қалыптастырады. Мысалы, қаскүнем сіздің салқындатқышты қыстың ортасында қашықтан басқарып қосты немесе кофе дайындайтын машинаны қыздырып өрт туғызды немесе автокөлігіңіз өздігінен үлкен жылдамдық алып бұғатталып қалса деп елестетіңіз.

Нашар конфигурацияланған немесе осалдықтары бар IoT құрылғысының үй желісінде болуы жайсыз салдарларға алып келуі мүмкін. Ең жиі қолданылатын сценарийлердің бірі - құрылғыны ботнетке қосу. Бұл, мүмкін, оның иесі үшін ең ақаусыз нұсқа; басқа нұсқаларды пайдалану қауіптірек. Осылайша, үй желісінің құрылғылары заңсыз әрекеттерді жасау үшін делдал ретінде пайдаланылуы мүмкін. Сонымен қатар, IoT-құрылғыға қол жеткізе алатын шабуылдаушы кейінгі боспалау үшін - құрылғы иесінің соңынан тыңшылық жасай алады - осыған ұқсас оқиғаларды бүгінге дейін көп мәрте орын алған. Соңында (және бұл ең нашар сценарий емес), қандай да бір тәуекелдіктерді жұқтырған құрылғы жай ғана бұзылуы мүмкін.

«Ақылды» құрылғылардың негізгі мәселелерді атап өтсек олар бағдарламалық жасақтама, құпиясөздер, Telnet және SSH болып табылады. Ең жақсы жағдайда, өндірушілер өздерінің «ақылды» құрылғылары үшін кідіріспен бағдарламалық қамтама жаңартуларын шығарады. Ең нашар (ең жиі жағдайда) - бағдарламалық жасақтама жаңартылмайды, көптеген құрылғыларда жаңартуларды орнату мүмкіндігі де жоқ.

Бағдарламалық жасақтама гаджеттерінде киберқылмыскерлер қолданатын қателер болуы мүмкін. Мысалы, Trojan PNScan (Trojan.Linux.PNScan) келесі осалдықтардың бірін пайдаланып маршрутизаторларды бұзуға тырысты:

– CW-2014-9727 Fritz! Box роутерлеріне шабуыл жасау үшін;

– Linksys маршрутизаторларына шабуылдау үшін HNAP хаттамасындағы (Home Network Administration Protocol) осалдығы және CVE-2013-2678-дегі осалдылық;

– ShellShock (CVE-2014-6271).

Егер ол әрекет сәтті болса, ол құрылғыны Tsunami бэкдорымен жұқтырған.

Persirai трояны IP-камералардың 1000-нан астам түрлі модельдерінде қамтылған осалдығын пайдаланды. Егер ол сәтті болғанда, ол супер қолданушы құқықтарымен құрылғының ерікті кодын орындай алады.

Тағы бір қауіпсіздік саңылауы TP-069 хаттамасының орындалуымен байланысты. Ол оператор жағынан қашықтан басқаруға арналған және SOAP-ге негізделген, ол өз кезегінде командаларды жіберген кезде XML пішімін пайдаланады. Нақты бұл параллельді парсерде осалдық табылған. Инфекцияның бұл әдісі Trojan Mirai-ның кейбір нұсқаларында, сондай-ақ Хаймеде қолданылған. Осылайша Deutsche Telekom құрылғылары зарарланған.

Тағы бір мәселе – өндіруші арқылы белгіленген құпия сөздер. Олар тек бір модельге ғана емес, сонымен бірге бүкіл өнім сызығына арналған болуы мүмкін. Сонымен қатар, бұл жағдай жаңа болып табылмайды, бұл қолданушы аты мен құпия сөздер комбинациялары тізімдерін ғаламторда оңай табуға болатындықтан, ол шабуылдаушылар арқылы пайдаланылады. Олар үшін жеңілдік жасайтын мәселенің бірі ретінде, «ақылды» құрылғылардың маңызды бөлігі Telnet және / немесе SSH порттары арқылы «жарқыратылады».

Мысалға, Gafgyt (Backdoor.Linux.Gafgyt) троян бағдарламасының бір нұсқасының логин-құпиясөз жұптар тізімі 1-кестеде берілген.

Логин	**Пароль**
root	root
root	—
telnet	telnet

!root	—
support	support
supervisor	zyad1234
root	antslq
root	guest12345
root	tini
root	letacla
root	Support1234

1-кесте. Gafgyt (Backdoor.Linux.Gafgyt) троян бағдарламасының бір нұсқасының логин-құпиясөз жұптар тізімі.

Зиянкестердің telnet-портқа қосылуға тырысқанда көбірек қолданатын логин-құпиясөз жұптар тізімі 2-кестеде көрсетілген.

Логин	**Пароль**
User	Password
root	xc3511
root	vizxv
admin	admin
root	admin
root	xmhdipc
root	123456
root	888888
root	54321
support	support
root	default
root	root
admin	password
root	anko
root	
root	juantech
admin	smcadmin
root	1111
root	12345
root	pass
admin	admin1234

2-кесте. Telnet-портқа қосылуға тырысқанда көбірек қолданатын логин-құпиясөз жұптар тізімі

Ең қауіптісі, шабуыл жасалатын IP-мекенжайлар арасында өнеркәсіп пен қауіпсіздікпен байланысты құрылғыларды мониторинг және басқару жүйелері кездеседі:

- Дүкендер, мейрамханалар мен жанармай құю станциялары үшін POS-терминалдар;
- Сандық хабар тарату жүйесі;
- Қауіпсіздікті қамтамасыз ету және қол жетімділікті бақылау жүйесі;
- Қоршаған ортаны мониторингінің қондырғылары;
- Бангкок сейсмикалық станциясының мониторингі;
- Өнеркәсіпте қолданылатын програмаланатын микроконтроллерлер;
- Электро қуатты басқару жүйесі.

Internet of Things үшін зиян келтіруші программалар санының көбейуі және олармен байланысты оқиғалардың іске асуы, «ақылды» құрылғылардың қауіпсіздік проблемасына қаншалықты маңызды. 2016 жылы жай ғана мүмкін екендігін көрсетіп қана қоймай өте шынайы қауіпті екенін көрсетті. DDoS-шабуыл жоғары бәсекелестік нарығында зиянкестерді әлдеқайда күшті, қуатты шабуыл жасауға көмектесетін, оларды қанағаттандыратын жаңа ресурстарды іздеуге итермелейді. Ботнет Mirai «ақылды» құрылғылардың ресурстары қандай болу керектігін көрсетті, және қазіргі уақытта олардың саны миллиардтқа жетіп отыр. Ал 2020 жылға қарай әртүрлі копания сарапшылары құрылғылардың саны 20 мен 50 миллиардқа дейін өсуі мүмкін деп болжам жасап отыр.

Қорытындылай келе, сіздің құрылғыларыңызды зиян келтіруші программалардан қорғауға көмектесетін бірнеше ұсыныс бергіміз келіп отыр:

Егер құрылғыда ашу талап етілмесе, оған сыртқы желіге қол жетімділік бермеңіз;

Сізге керек болмаған барлық құрылғыларды желілік қызметтерден ажыратыңыз.

Егер құрылғыда өзгертуге келмейтін стандартты немесе әмбебап құпия сөз, немесе ажыратуға келмейтін алдын ала орнатылған тіркеу жазбасы болса, олар қолданылып желілік қызметтерді өшіріңіз немесе оларға ішінен желіге қол жетімділікті жабыңыз.

Қолданар алдында үнсіз келісім құпия сөзін тікелей іздеуге төзімді жаңа құпия сөзге өзгертіңіз.

Құрылғыңызды жүйелі түрде соңғы нұсқаға жаңартып отырыңыз (егер жаңа нұсқалары бар болса).

Осы қарапайым ұсыныстарды орындау IoT-зиянкес программалардың шабуылының көпшілігіне жол бермейді.

Қолданылған әдебиеттер тізімі:

1. Нил Ходж, The-Internet-of-Risks, 28 Июля 2017
2. Earl Perkins, Securing the Internet of Things, 13 September 2017
3. https://securelist.ru
4. Alasdair Gilchrist, IoT Security Issues Paperback – January 23, 2017
5. Lawrence Miller, IoT Security for Dummies, 2016

УДК 004.4 (075.8)

«ҚАШЫҚТЫҚТАН ОҚЫТУДЫҢ АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРДЫ ҚОЛДАНУ ЖОЛДАРЫ»

Смаилова Эльвира Маратовна

Информатика мамандығының 4 курс студенті

Қостанай мемлекеттік педагогикалық институты, Қостанай, Қазақстан

Ғылыми жетекшісі-З.Ерсултанова

Қоғамның және білім беру саласын ақпараттандыру жаңа технологиялардың туындауына әкеледі. Осындай технологиялардың бірі, ақпараттануды бейнелейтін ашық білім беру болып табылады. Ал кеңейтілудің және ашық білім беру саласының аукымдылығы қашықтықтан білім беру технологиялары әсерлі тәсілдердің бірі болып табылады. Ақпараттық және телекоммуникациялық орталары мен тәсілдері алуан түрлі бола тұра мынадай мүмкіндік береді:

- дамуды, білім алуын және беруін өзгертеді;
- оқытудың мазмұны мен тәсілін жаңартуына мүмкіндіктер ашады;
- жалпы және мамандандырылған білім саласына кіруін кеңейтеді;
- оқытушы қажеттілігінсіз, оқу үдерісінде олардын рөлін өзгертеді (ақпаратты білім мен түсінушілікке аударатын тұрақты диалог). Оқушыларды тұрмыстық, қоғамдық және