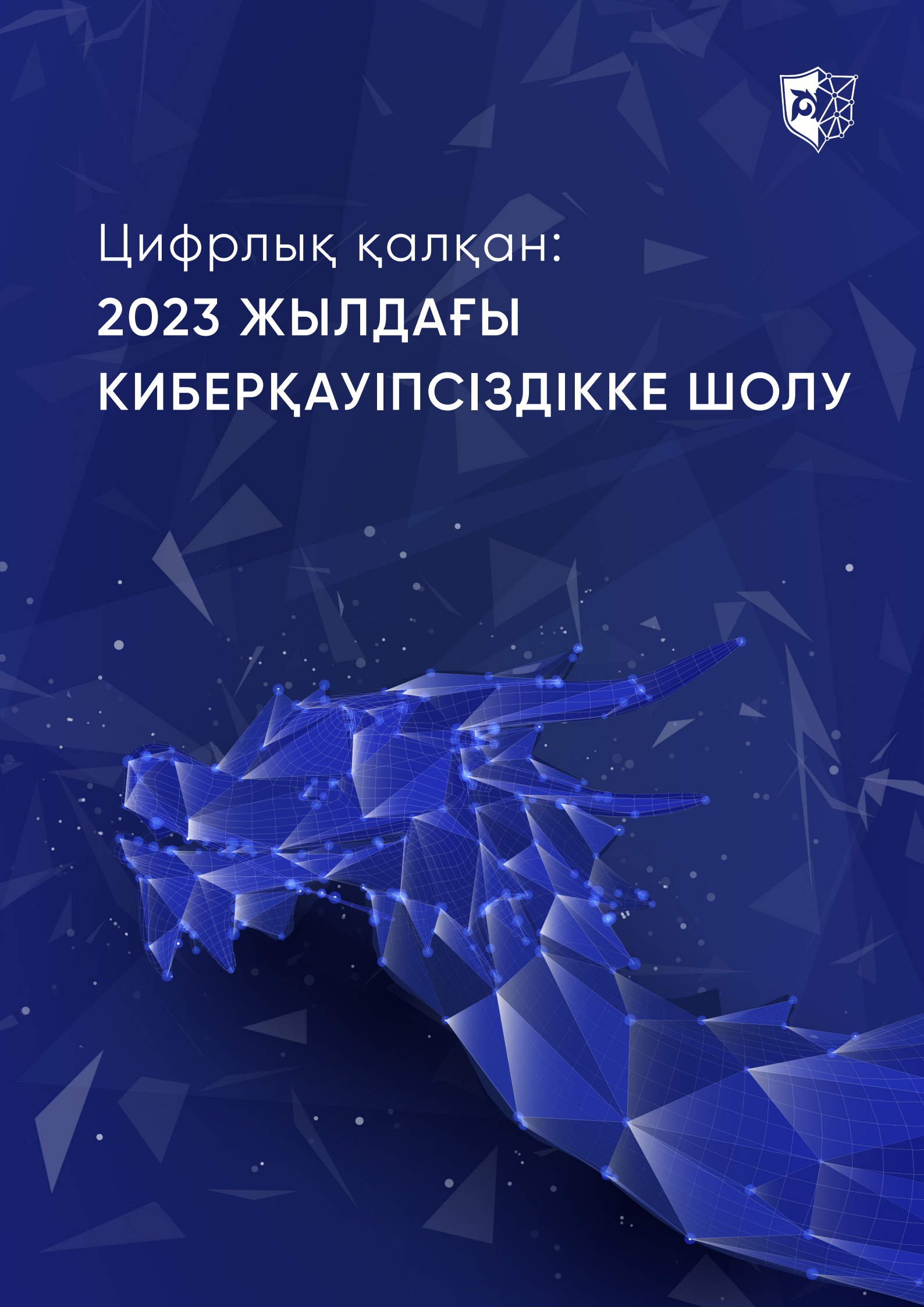
Цифрлық қалқан:

2023 ЖЫЛДАҒЫ КИБЕРҚАУІПСІЗДІККЕ ШОЛУ



Кибердайджест: Мазмұны

Кіріспе 3

Ел ішіндегі компьютерлік инциденттерге шолу 4

Кибергигиена. Пайдаланушылар арасында хабардарлықты арттыру 11

Халықаралық қатерлер және оқиғалар 15

АҚ инциденттері бойынша статистика 28

Осалдықтар мен эксплойттардың талдауы 38

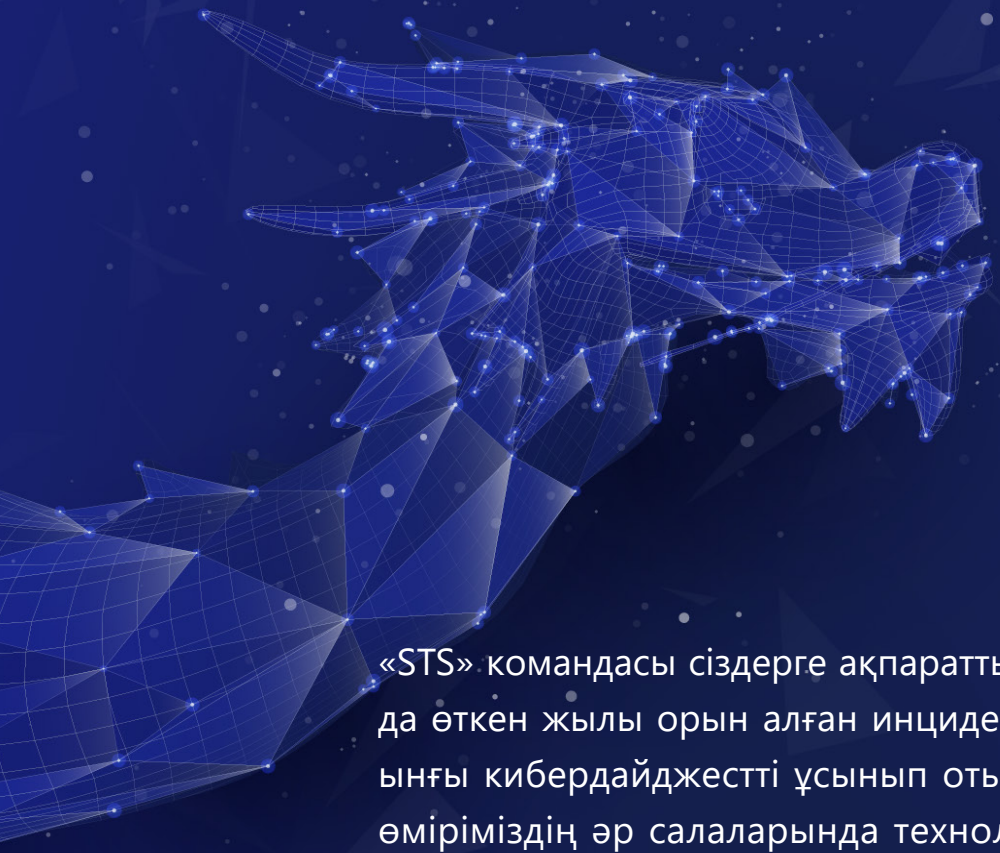
Шабуыл жасау әдістеріндегі үрдістер 43

Қорғау құралдары және ұсынымдар 45

Болашақ үрдістер мен болжамдар 47

Қорытынды 51

Ақпарат көздері және түсіндірмелер 52



Құрметті оқырмандар,

«STS» командасы сіздерге ақпараттық қауіпсіздік (АҚ) саласында өткен жылы орын алған инциденттерге арналған жыл сайынғы кибердайджестті ұсынып отырғанына қуанышты. Біздің өміріміздің әр салаларында технологиялар маңыздырақ рөл атқарып жатқан әлемде ақпараттық қауіпсіздік мәселелері күнделікті өміріміздің ажырамас бөлігіне айналуда.

Өткен жылы мүгедектермен қатар, ұйымдар да тап болатын АҚ саласындағы оқиғалар және сын-қатерлер айтарлықтай көп болды. АҚ қатерлері үнемі дамып, киберқылмыскерлер әсерленгіш ақпаратқа қолжетімділік алу үшін шабуылдардың жаңа әдістерін табуда.

Осы дайджестте біз Қазақстан мен әлемде орын алған АҚ саласындағы ең маңызды және ықпалды инциденттерді қарастырамыз. Біз үрдістердің талдауын ұсынып, өткен оқиғалардан шығаруға болатын қорытындыларды анықтаймыз және алдағы уақытта біздің қоғамның АҚ нығайту стратегияларын талқылаймыз.

Киберқауіпсіздік әлеміндегі соңғы оқиғалардан хабардар болу және өзіңізді өскелең АҚ қатерлерінен қорғау үшін қандай қадамдар жасауға болатынын түсіну үшін біздің әлеуметтік желілердегі аккаунтарымызды қараңыздар.

Қауіпсіздікте болыңыздар!

Ел ішіндегі компьютерлік инциденттерге шолу

Цифрлық кеңістіктегі қауіпсіздік тұрақты ықылас қоюды және талдауды талап ететін ең маңызды мәселеге айналуда. Цифрлық технологиялар санының артуымен қатар ұйымдар және жеке тұлғалар тап болатын ақпараттық қауіпсіздік қатерлерінің деңгейі де жоғарылайды.

Кибердайджесттің осы блогында біз ақпараттық қауіпсіздік саласындағы соңғы оқиғаларға қысқаша шолу ұсынамыз. Киберкеңістік әлеміне еніп, Қазақстандағы ақпараттық қауіпсіздіктің ағымдағы көрінісін айқындайтын басты инциденттерді қарастырамыз.

1 «Спортмастер» дүкенінің 260 мыңнан астам қазақстандық клиенттерінің деректері желіде таралып кетті

Ағымдағы жылдың басында «Спортмастер» спорт дүкендері желісінің ТМД елдеріндегі клиенттерінің дербес деректері таралып кеткені белгілі болды.

Тізімде Қазақстан азаматтарының деректері көрсетілген 260 000 артық жол қамтылған. Деректердің өзектілігі 2012 жылғы 15 қыркүйектен бастап 2018 жылғы 18 мамырға дейінгі кезеңді құрайды.

Файлда есімдер, туған күндер, телефон нөмірлері мен электрондық пошта мекенжайлары көрсетілген. «Спортмастер» компаниясы инцидент пайдаланушылардың логиндері мен парольдерін, төлем ақпаратын, сондай-ақ қызметкерлердің есептік жазбаларын қозғамайтынын атап көрсетіп, деректердің таралғанын растады. Ішкі тексеру басталды. Алдын ала мағлұмат бойынша таралу осы ақпаратқа қолжетімділігі бар мердігерлердің бірі тарапынан орын алғаны ықтимал.

Зиянкестер таралу нәтижесінде алған ақпаратты әлеуметтік инженерияда, атап айтқанда конфиденциалды және банктік деректерді алу мақсатында қоңырау шалу мен фишингтік хабарламаларды таратуды жүзеге асыру кезінде пайдалануы мүмкін.

Бұдан басқа, осы ақпаратты зиянкестер екі факторлық аутентификацияны қоспаған пайдаланушылардың әлеуметтік желілердегі парақшаларын бұзған кезде пайдалана алады.

2 Хакерлер ҚР мемлекеттік ведомствосынан биткойндер талап еткен

ҚР квазимемлекеттік секторы ұйымдарының бірінде желінің шифрлаушы вируспен зақымдалғаны анықталды. Шифрді ашу үшін зиянкестер ақысын биткойнмен төлеуді талап еткен.

Алдын ала талдау ұйым «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» ҚР Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысының талаптарын сақтамағанын көрсетті. Ұйымның барлық желісінен зиянкес домен контроллерін, үш дербес компьютер мен файлдық серверді кедергісіз зақымдаған. Мамандар дербес компьютерлердің біреуі толық шифрланғанын, ал жүйелік логтар тазартылғанын анықтады.

Ұйымның барлық пайдаланушылары үшін бір ғана есептік жазба жасалған – «X». Зиянкес RDP хаттамасын *(Microsoft қашықтағы жұмыс үстелінің хаттамасы)* пайдалана, парольдерді теру арқылы инфрақұрылымға қолжетімділік алып, әрбір жұмыс станциясындағы вирусқа қарсы бағдарламалық қамтылымды жойған. Вирусқа қарсы БҚ жойылғаннын кейін барлық құрылғыларға шифрлаушы жүктелген.

Шифрланған файлдар кеңейту *(CW-WL30486259l7)* алып, Windows операциялық жүйесінде SQL Server, виртуалды дискілер қызметі, Windows томдарын көлеңкелі көшіру қызметі мен брандмауэр сияқты түрлі қызметтерді тоқтатуға және белгілі функцияларды ажыратуға арналған командаларды орындаған. Оған қоса шифрлаушы өзін өзі орнату папкасындағы автоматты жүктеулерге көшірген, ал каталогтарда unlock-info.txt файлын құрған – өтеп алу талап етілген мәтін.

3 Бір білім беру сайтының осалдығы қазақстандық 40 сайттың жария етілуіне себеп болмақ

2023 жылғы наурызда жекеменшік білім беру мекемелерінің интернет-ресурстарының біреуінде веб-шелл айқындалды.

Веб-шелл – қауіпсіздікке күрделі қатер төндіретін, зиянкестер интернет-ресурстарды немесе веб-серверлерді басқару үшін пайдаланатын зиянды скрипт. Скриптті орналастыру үшін жиі жағдайларда сайттың кодындағы осалдықтар немесе парольдерді теру қолданылады.

Веб-шеллді жүктеу веб-қосымшаның осалдықтарына немесе дұрыс емес конфигурацияға байланысты жүзеге асырылады. Ақпараттық қауіпсіздік инцидентін талдау барысында осы веб-серверде орналасқан және әлде қашан жария етілуі ықтимал 40-там астам интернет-ресурс анықталды.

Бұл веб-шелл символдардың 22 әртүрлі жинағын қолдайтынын және жүктеген кезде кілттің (парольдің) көмегімен бастапқы кодты шифрлайтынын, бірақ алынған файлда бұл кілт қамтылмайтынын атап көрсетеміз.

Бұдан басқа, веб-шеллдің жасырын режимі бар және парақшаны қайта жүктеусіз және деректерді жоғалтпай әртүрлі міндеттермен жұмыс істеуге мүмкіндік береді.

Күрделі емес модификацияға байланысты, жиі жағдайларда веб-шеллдерді анықтау қиын. Вирусқа қарсы өнімдер кейде оларды айқындай алмайды. Осы индикаторлардың кейбіреулері рұқсат етілген файлдар үшін ортақ болып табылатынына назар аудару қажет. Күдікті зиянды файлдарды басқа

индикаторлардың мәнмәтінінде қарау және одан әрі тексеру талап етілетінін анықтау үшін іріктеу керек.

Веб-шелл сценарийі құрылған URL-ға зиянкес жиі кіретін белгі де веб-шелдің белсенділігін көрсетуі мүмкін. Қарапайым пайдаланушы байланысты парақтан веб-парақшаны жүктейді немесе қосымша контент, не ресурстар жүктейді. Осылайша, веб-қолжетімділік журналдарының жиілігіне жүргізілетін талдау веб-шеллдің орналасқан орнын көрсете алады. Рұқсат етілген жүгінулердің басым бөлігі әртүрлі пайдаланушылық агенттерді қамтиды, ал веб-шеллге зиянкес қана кіруі мүмкін болып, бұл пайдаланушылық агенттердің шектелген нұсқаларына әкеледі.

4 Geoserver пайдаланатын компанияларға қауіп төніп тұр

2023 жылғы мамырда болжам бойынша CVE-2022-24816 және CVE-2023-25157 сәйкестендіргіштерімен аса маңызды осалдықтарға бейімді 17 IP-мекенжайы анықталды.

Анықталған IP-мекенжайлары Қазақстанның квазимемлекеттік секторының ірі компанияларына тиесілі.

GeoServer стратегиялық шешімдер қабылдау үшін кеңістіктік деректер маңызды компоненттер болып табылатын геология, экология, геодезия, ауыл шаруашылығы, қалаларды басқару сияқты және т.б. әртүрлі салаларда пайдаланылады.

Осалдықтарды жою бойынша уақытылы қабылданбаған шаралар конфиденциалды деректердің жария етілуіне және кейін желіге шабуылдар жасауды жүзеге асыруға, соның ішінде зиянды бағдарламалық қамтылымды басқа да жүйелерге ендіруге әкелуі мүмкін, бұл бүкіл желі инфрақұрылымының қауіпсіздігіне қатер төндіреді.

Осал GeoServer-ге жасалған сәтті шабуыл компания беделіне нұқсан келтіріп, БАҚ пен жұртшылық тарапынан жағымсыз ықыласқа әкеп соғуы ықтимал.

«Бұл оқиға осы салалардың ақпараттық қауіпсіздік бөлімдерінің мамандары жүйе компоненттерін жаңартуға тиісті назар аудармайтынын, бұл конфиденциалды ақпараттың таралу қатерлерінің еселенуіне әкелетінін тағы бір рет дәлелдейді».

Бұған дейін Shadowserver Foundation компаниясы GeoServer бағдарламалық қамтылымындағы осалдықтар туралы ақпарат жариялаған.

** Shadowserver Foundation*
- жазылушыларға күн сайынғы желілік есептерді жіберетін және киберқылмыстарды тексеруде барлық әлем бойынша құқық қорғау органдарымен ынтымақтасатын ақпараттық қауіпсіздікті қамтамасыз ету ұйымы.

5 Қазақстанда 17 мыңнан астам роутер Mikrotik Routeros-тегі осалдыққа ықтимал бейімделген

Қазақстанда 2023 жылғы шілдеде MikroTik осалдығына ықтимал бейімді 17 мың роутер айқындалды. 5 128 роутерде оның бар болуының айқын белгілері бар.

Осы осалдықты өз мақсаттарында пайдаланып, зиянкес артықшылықтарын қарапайым әкімші деңгейінен super admin-ге дейін *(кіріктірілген әкімшінің есептік жазбасы)* жоғарылатуы мүмкін.

Осалдықты пайдалану үшін аутентификация талап етіледі, алайда тіпті бұл да хакер үшін проблема емес, себебі RouterOS-де әкімшінің стандартты есептік жазбалары әдеттегідей орнатылған. Қауіпсіздік жөніндегі MikroTik нұсқаулықтарында роутерді орнату кезінде әкімшінің деректерін жоюға ұсыным берілген. Былай айтқанда, парольді ауыстыру, бірақ, бұл ұсынымдардың көбі ескерілмейді.

MikroTik RouterOS өнімінің осал нұсқаларын пайдаланатын ұйымдарға ресми ақпарат көзінен жаңартуларды ұйым саясатының қағидаларына сәйкес шұғыл түрде қолдану ұсынылады.

Сонымен қатар, RouterOS-тің 6.49 төмен алғашқы құрастырылымдарында әдеттегідей белгіленген әкімші паролі бос жол түрінде және MikroTik роутерлерінің шамамен 60%-ы әлі де оны пайдаланатыны байқалады.

6 NCALayer-дің жалған жаңартуына байланысты инцидент

Мемқызмет алу туралы сұрау салуға қол қою үшін NCALayer орнату қажет екені белгілі.

Ағымдағы жылғы қыркүйекте ncalayer.info/update.php фишингтік интернет-ресурсы анықталды. Оны ашқан кезде NCALayer-ге арналған жаңарту түрінде «Trojan Downloader» типінің зиянды бағдарламасы жүктеледі де іске қосылады.

GitHub кодының белгілі репозиторийін қамтитын шифрды ашу мен жүктеулер тізбегінен кейін компьютерге бұзылған нұсқасы хакерлік даркнет форумдарда таратылатын Venom RAT v6.0.1 зиянды бағдарламалық қамтылымы орнатылады.

Бұл зиянды бағдарламаның ерекшелігі оның кейлоггер, деректерді ұрлау, компьютерді қашықтан жасырын басқару *(VNC)*, сондай-ақ веб-камераны басқару функционалының иесі болып табылатыны. Түпкілікті нәтижесінде зиянкестің пернетақтада терілетін ақпаратты оқуға, парольдерді, с.і. браузерлерден көруге, сондай-ақ сыртқы қосымшаларды орнатуға мүмкіндігі бар.

7 Хакерлер Citrix өнімдерін пайдаланатын қазақстандық компанияларды бұза алады

Ағымдағы жылғы қазанда Интернеттің қазақстандық сегментінде CVE-2023-3519 сәйкестендіргішінің маңыздылық деңгейі жоғары осалдығына ықтимал бейімді Citrix NetScaler ADC және NetScaler Gateway өнімдерін пайдаланатын 27 IP-мекенжайы анықталды.

CVSSv3.1 (Common Vulnerability Scoring System) сәйкес осалдықтың рейтингі 10-нан 9.8. Ол зиянкеске еркін кодты авторланусыз орындауға мүмкіндік береді. Осалдық SAML хабарламасында каноникализация немесе түрлендіру әдістерінің өте көп саны жіберілген кезде пайда болады.

Ағымдағы жылғы 20 шілдеден бастап CVE-2023-3519-ға жасалған жаппай шабуылдар барысында әлемде 640-қа жуық Citrix Netscaler ADC және Gateway серверлері бұзылып, бэкдорлармен зақымдалғаны белгілі.

Сондай-ақ, бірнеше жыл бұрын REvil және DoppelPaymer бопсалаушы топтар корпоративтік желілерді бұзу үшін өткен шабуылдарда Citrix Netscaler ADC және Gateway ұқсас осалдықтарын пайдаланған.

Зиянкес осалдықты пайдалана отырып, зиянды БҚ ендіруі, конфиденциалды деректерді ұрлауы және кейін желіге шабуылдар жасауы мүмкін екенін, бұл бүкіл желі инфрақұрылымының қауіпсіздігіне қатер төндіретінін атап көрсету қажет.

8 Қазақстандықтардың жеке деректерінің таралып кету себебі – инфостилер

2023 жылғы қарашада дербес деректердің таралуына байланысты ақпараттық қауіпсіздік инциденттерінің саны артқаны тіркелді.

Таралудың себебі зақымдалған компьютерлерден жеке деректер *(парольдерді, банктік деректерді және басқа да әсерленгіш мәліметтер)* ұлауды көздейтін ақпарат жинаушылар, зиянды бағдарламалық қамтылымдар *(бұдан әрі-ЗБҚ)* болып табылады. ЗБҚ бұл түрі жасырын жұмыс істеу және ұрланған деректерді зиянкестерге жіберу үшін шығарылған.

Ақпарат жинаушылар *(немесе ақпараттық трояндар)* - бұл құрбанның ДК конфиденциалды деректерді жинау үшін әзірленген ЗБҚ түрі.

Олар есептік жазбалар, парольдер, кредиттік карталардың нөмірлері сияқты жеке деректерді және басқа да конфиденциалды мәліметтерді ұрлайды.

Ақпарат жинаушылардың кіші түрі – пайдаланушының пернелерді басуын тіркейтін кейлоггерлер бар. Олар да пайдаланушының конфиденциалды ақпаратын жинауға арналған.

Дербес деректердің таралу себебі болған кейбір ақпарат жинаушылар:

ReadLine Stealer

Жабық форумдарда сатылады және зиянкестер оларды деректерді ұрлап, құрбанның комьютеріне басқа вирустар жүктеу үшін пайдаланады. Барлық веб-браузерлерден логиндерді, парольдерді, автотолтыру деректерін, cookie файлдарын және кредиттік карталардың деректерін ұрлай алады. Хакерлер бұл ақпаратты әртүрлі есептік жазбаларға *(мәселен, әлеуметтік желілерге, электрондық поштаға, банктік шоттарға, криптовалюталық әмияндарға)* қол жеткізу үшін құқыққа қайшы пайдалануы мүмкін.

Vidar Stealer

Бұл банктік ақпаратты, сақталған парольдерді, IP-мекенжайларды, браузердің тарихын, криптоәмияндарға кіруге арналған есептік жазбаларды қоса алғанда, құрбанның компьютерінен әсерленгіш деректерді ұрлауға және зиянкестің серверіне жіберуге қабілетті ақпарат жинаушы. Vidar Stealer спам-хаттардың, пираттық БҚ, кілттердің генераторлары және т.б. көмегімен таратылады.

Raccoon Stealer

ДК мен жүйелерден деректерді ұрлауға арналған. Бұл есептік жазбалардың логиндері мен парольдері, банктік карталардың деректері және басқа жеке мәліметтер сияқты конфиденциалды ақпаратты жинауға бағытталған ақпарат жинаушылар санатының үлгілік өкілі. Электрондық поштадағы зиянды ендірмелерді, жария етілген веб-сайттарды қоса, әртүрлі тәсілдермен немесе БҚ-дағы эксплойттар арқылы таратылады. Әдетте, олардың мақсаты өзіне назар тартпай, ақпарат жинау үшін мақсатты жүйелерге ену болып табылады.

Azorult Stealer

Логиндер, парольдер, банктік карталардың деректері, браузердің cookie туралы ақпарат сияқты деректерді және басқа да құнды мәліметтерді жинау үшін жиі пайдаланылады. Зиянды электрондық хаттар, зиянды веб-сайттар, жария етілген бағдарламалар немесе эксплойттар арқылы таратылуы мүмкін. Зақымдаған соң ақпаратты жинап, кейін оны зиянкестердің бақылауындағы қашықтағы серверге жібереді.

Ақпарат жинағышқа байланысты дербес деректердің таралуы туралы айтылған кезде, бұл жиі жағдайларда ақпараттық қауіпсіздікті айтарлықтай бұзу орын алғанын білдіреді.

Әдетте, мұндай жағдайлар күрделі тергеп тексеруді және алдағы уақытта осындай инциденттерге жол бермеу үшін шаралар қабылдауды талап етеді.

Әлемде технологиялар дамуының қарқынына байланысты ақпараттық қауіпсіздікті қамтамасыз ету үздіксіз қарсы шығуға айналуда.

Қазақстандағы ақпараттық қауіпсіздік саласындағы соңғы инциденттерге шолу цифрлық ортаны үнемі мониторингтеу мен жаңа қатерлерге бейімделудің маңыздылығын білдіреді. Фишингтік шабуылдар, зиянды бағдарламалар мен басқа да киберқатерлер күрделеніп, жетілдірілуде.

Ақпараттық қауіпсіздік – бұл естен шығармау мен стратегияларды жаңартуды талап ететін үздіксіз процесс. Үнемі үйрену, инновациялық әдістер және бірлескен зерттеулер цифрлық дәуірде қорғаудың қажет деңгейін қамтамасыз етеді.

Кибергигиена.

Пайдаланушылар арасында хабардарлықты арттыру

Ақпараттық қауіпсіздік туралы хабардарлық біздің Қазақстан ұйымдарының қызметкерлері, қарапайым пайдаланушылар мен жалпы қоғам үшін қауіпсіз цифрлық кеңістікті құруға ұмтылысымыздың басты аспектісі болып табылады.

«STS» командасы **әртүрлі секторлардағы ұйымдардың қызметкерлерін, қазақстандық пайдаланушыларды, соның ішінде оқушылар мен студенттерді қоса, түрлі аудиторияларды қамтып, ақпараттық қауіпсіздік (АҚ) мәдениетінің деңгейін жоғарылату бойынша алуан түрлі іс-шараларды** іске асырады.

«STS» командасы интернетті қауіпсіз пайдаланудың, фишингтен қорғаудың негізгі аспектілерін, АҚ заманауи қатерлеріне шолуды және т.б. қоса алғанда, кибергигиена бойынша түрлі тақырыптарда үнемі дәрістер өткізеді. Дәріс шаралары жапы хабардарлықты арттыруға және пайдаланушыларды цифрлық әлемдегі қауіпсіздіктің практикалық дағдыларына үйретуге бағытталған.

Қазіргі уақытта Қазақстан Республикасының мемлекеттік органдары, квазимемлекеттік және жекеменшік секторлар қызметкерлерінің мекенжайына электрондық пошта бойынша хаттар жіберу арқылы ұйымдастырылатын мақсатты фишингтік шабуылдардың пайыздық үлесі артып келеді.

Қызметкерлер **мұқият әзірленген**, қызметкерді корпоративтік желілерге, немесе Ұйымның конфиденциалды не дербес ақпарат қамтылған дерекқорларына қолжетімділік беретін **конфиденциалды/дербес мәліметтер – логин мен парольді** енгізуге итермелейтін фишингтік[1] хабарламалар алады.

Мақсатты[2] фишингтік хаттарда ЗБҚ болуы мүмкін, көптеген жағдайларда бұл қашықтан қол жеткізуге, зиянды жүктегішке немесе шифрлаушы вирусқа арналған бағдарламалық қамтылым.

Фишингтен қорғаудың **пошталық/веб-трафикті фильтрлеу мен талдау, бағдарламалық ортаны шектеу, ендірмелерді/БҚ іске қосуға тыйым салу** сияқты техникалық шаралары – өте тиімді, алайда, бұл ретте олар **жаңа қатерлерге қарсы тұралмайды және маңыздырағы, адамның білімқұмарлығы мен бейхабардарлығына қарсы тұра алмайды.** Осыған байланысты мақсатты фишингтік шабуылдардан қорғаудың маңызды факторларының бірі - **қызметкерлерді оқыту.**

[1] «Фишинг» (ағыл phishing, fishing — балық аулау, ұстау) — мақсаты пайдаланушылардың конфиденциалды деректері- логиндер мен парольдеріне қолжетімділік алу болып табылатын интернет-алаяқтық түрі.

[2] «Спирфишинг» (ағыл. spear phishing) – зиянкес пайдаланушы туралы бұрын жиналған деректерді пайдалана отырып, нақты пайдаланушыға арнап фишингтік хат қалыптастыртын Фишинг түрі.

Ұйымдардың қызметкерлері арасында кибержаттықтырулар *(фишинг пен шабуылдардың басқа түрлеріне практикалық сынақтар)* өткізу ақпараттық қауіпсіздік мәдениетін және ақпараттық қауіпсіздіктің қатерлері мен инциденттеріне әрекет ету бойынша пайдаланушылардың хабардарлығын арттыруда келесі себептер бойынша маңызды рөл атқарады:

Осал тұстарды сәйкестендіру

Кибержаттықтырулар ақпараттық қауіпсіздікті қамтамасыз ету жүйесіндегі осал тұстарды айқындауға көмектеседі. Егер қызметкерлер фишинг немесе басқа шабуылдар үшін осал болса, бұл зиянкестер үшін ену нүктесі болуы мүмкін. Мұндай тесттерді жүргізу ұйымға қай жерде қорғауды жақсарту керек екенін көруге мүмкіндік береді.

Оқыту және хабардарлық

Кибержаттықтырулар тек қана проблемаларды сәйкестендірмейді, қызметкерлерді ықтимал қатерлерді танып, әрекет етуге үйретеді. Бұл инциденттер жағдайында іс-әрекеттер жасауға оларды барынша даярлап, қызметкерлердің ақпараттық сауаттылық және хабардарлық деңгейін арттыруға көмектеседі.

Әрекет ету стратегияларын тестілеу

Кибержаттықтырулар өткізу ақпараттық қауіпсіздіктің инциденттеріне әрекет ету жоспарлары мен стратегияларының тиімділігін тексеруге мүмкіндік береді. Егер оқу-жаттығу шеңберінде қызметкерлер шабуылды сәтті тауып, әрекет етсе, бұл жоспарлар мен стратегиялар нақты жағдайларда қолдануға дайын екеніне сенімділік тудырады

Ең жақсы тәжірибелерді қалыптастыру

Кибержаттықтырулар өткізу арқылы ұйым ақпараттық қауіпсіздік саласындағы ең үздік тәжірибелерді әзірлеп, өзінің қызметкерлері арасында тарата алады. Бұл электрондық поштаны, сілтемелер мен ендірмелерді тексеру қағидаларын, сондай-ақ парольдерді құру және басқару жөніндегі нұсқаулықтарды қамтуы мүмкін.

Тәуекелдерді азайту

Ақпараттық қауіпсіздікті жоғарылату конфиденциалды ақпараттың таралуына, қаржылық шығындарға әкеп соғуы немесе ұйым беделіне нұқсан келтіруі ықтимал болған инциденттер тәуекелінің төмендегенін білдіреді.

Жалпы, қызметкерлер арасындағы кибержаттықтырулар ұйымның ақпараттық қауіпсіздігін нығайтудың және киберқатерлер кеңінен таралған әрі талғағыш болып келетін әлемде персоналды іс-әрекеттер жасауға даярлаудың маңызды құралы болып табылады.

Қазақстан ұйымдары қызметкерлерінің білімін және хабардарлық деңгейін тексеру үшін «STS» командасы фишингтік хабарламалар мен интернет-ресурстар сияқты кибершабуылдарды ұқсастыруға, сондай-ақ әр түрлі зиянды ендірмелерді ұқсастыруға арналған түрлі құралдарды пайдаланады. Бұл іс-шаралар ұйымдармен келісу бойынша қызметкерлердің реакциясын және ақпараттық қауіпсіздіктің ұқсас инциденттеріне тойтарыс беруге дайындығын бағалау үшін жүргізіледі.

«STS» командасы әртүрлі арналар арқылы пайдаланушылардың өтініштерін қабылдайтынын атап көрсету қажет, мынадай:

«ҚР ақпараттық қауіпсіздігі»
Telegram-арнасы
t.me/kzcert

Электрондық пошта мекенжайлары:
incident@cert.gov.kz
info@sts.kz

Telegram-бот
«KZ-CERT BOT»
t.me/KZ_CERT_chat_bot
Пайдаланушылардан өтінімдер беруді автоматтандыру, сондай-ақ өтінімдерді өңдеу мәртебелерін нақты уақытта қадағалау үшін әзірленген.

Ресми **cert.gov.kz** интернет-ресурсындағы және АҚ инциденттері туралы ақпарат алмасу платформасындағы **misp.sts.kz** **«АҚ инциденті туралы хабарлау»** нысандары.

1400
Ақысыз
call-орталығы

«STS» командасының мақсаты» - орын алатын қатерлерге әрекет ету ғана емес, оқытып -үйрету арқылы олардың туындауына жол бермеу. «STS» командасы қоғамдастығымыздың әр мүшесі ақпараттық қауіпсіздікті қамтамасыз етудегі өзінің рөлін түсініп, АҚ ықтимал қатерлерінен қорғауға белсене қатысатын ақпараттық қауіпсіздік мәдениетін құруға ынталанады.

«STS» командасының мақсатты іске асыруға арналған ұсынымдары

Білім беру іс-шараларына, семинарлар мен вебинарларға қатысу арқылы ақпараттық қауіпсіздік туралы өз хабардарлығыңызды арттырыңыз. Ақпараттық қауіпсіздіктегі соңғы трендтерді қадағалаңыз және өзіңізді желідегі қауіпсіз мінез-құлық негіздеріне үйретіңіз.
Сондай-ақ, АҚ бойынша соңғы оқиғалар трендінде болу үшін командаңың әлеуметтік желілердегі аккаунттарын қараңыз.

Онлайн-аккаунттарыңыз үшін берік парольдерді пайдаланып, өз деректеріңізді қол жеткізуден қорғауды күшейту үшін екі факторлық аутентификацияны іске қосыңыз.

Осалдықтарды түзету үшін операциялық жүйелер мен вирусқа қарсы бағдарламаларды қоса, өз құрылғыларыңызда бағдарламалық қамтылымды үнемі жаңартыңыз.

Электрондық хаттардағы ендірмелерді ашқан және жеке ақпаратты берген кезде абай болыңыз, күдікті сілтемелер бойынша өтпеңіз. Тексерілмеген дерек көздеріне сенбеңіз.

Пайдаланушыларға:

Онлайн-акканутарыңызды рұқсатсыз қол жеткізу және күдікті белсенділік тұрғысынан мерзімді түрде тексеріңіз

Интернеттегі қауіпсіздік бойынша курстардан өтіп, АҚ қатерлерін қалай тануға және аулақ болуға болатынына үйреніңіз.

Өз құрылғыларыңызда вирусқа қарсы бағдарламалық қамтылымды орнатыңыз және үнемі жаңартыңыз.

Әсерленгіш операцияларды орындау үшін ортақ Wi-Fi желілерін пайдаланудан аулақ болыңыз.

Ұйымдардың қызметкерлеріне:

IT/IS-бөлімімен белсенді ынтымақтасыңыз және ұйым ұсынатын қауіпсіздік жөніндегі тұрақты тренингтерге қатысыңыз.

Компанияның қауіпсіздік, әсіресе конфиденциалды ақпаратты өңдеу мен беруге қатысты саясаттарын сақтаңыз.

Вирусқа қарсы бағдарламаларды және бағдарламалық қамтылымды өзекті жай-күйінде қолдап отырыңыз, сондай-ақ жұмыс орындарының физикалық қауіпсіздігін қамтамасыз етіңіз.

АҚ инциденттеріне әрекет ету процедураларын біліңіз және күдікті белсенділік немесе инциденттер туралы IT/IS-бөліміңізге дереу хабарлаңыз.

Ақпараттық қауіпсіздік саласындағы халықаралық қатерлер мен оқиғаларға жыл бойы тұрақты талдау жүргізу бірқатар басты себептер бойынша орынды. Бірінші кезекте, зиянкестер өздерінің шабуыл жасау әдістерін үздіксіз жетілдіретіндіктен, ақпараттық қауіпсіздік қатерлерінің динамикалық болмысы үнемі мониторингтеуді талап етеді. Тек қана жүйелі талдау жаңа қатерлерді анықтауға және оларға тиімді әрекет етуге көмектеседі.

Интернеттің жаһандық сипаты виртуалды кеңістіктегі қатерлердің де халықаралық ауқымын білдіреді. Халықаралық қатерлерді талдау ортақ үрдістерді түсінуге ғана емес, шабуылдардың себептерін айқындауға мүмкіндік беріп, бұл **киберқорғау** стратегияларын әзірлеудің маңызды компонентті болып табылады.

Кибершабуылдардың басым бөлігі нақты мемлекеттік мекемелер, энергетикалық жүйелер мен көліктік желілер сияқты объектілерге бағытталғанына байланысты, аса маңызды инфрақұрылымды қорғау маңыздырақ болып келеді. Қатерлерді тұрақты талдау осалдықтарды анықтауға және оларға талдау жүргізуге, сондай-ақ қауіпсіздік шараларын әзірлеу мен жақсартуға көмектеседі.

Цифрлық ақпарат көлемдерінің артуы мен жеке деректердің таралуы нәтижесінде конфиденциалдылықты қорғау барынша өзекті мәселеге айналуда. Қатерлерді талдау жеке деректерді өңдеу мен сақтауға төнетін ықтимал қатерлерді анықтауға мүмкіндік береді, ал бұл қауіпсіздіктің жоғары деңгейін қолдау үшін қажет.

2023 жылы халықаралық қоғамдастықта ақпараттық қауіпсіздіктің қатерлері мен инциденттерінің келесі түрлері кеңінен таралған:

Түпкілікті нүктелерге шабуылдар жасау *Endpoint-Based Attacks*

Түпкілікті нүктелерге шабуылдар өнеркәсіптің барлық салаларындағы бизнес үшін күрделі қатер төндіреді. Түпкілікті нүктелердің саны көбейіп, қашықтан жұмыс істеу мүмкіндіктері қалыпты болып қала беретіндіктен, түпкілікті нүктелерге шабуылдың шегі кеңейіп, ұйымдарды бірқатар қатерлер үшін осал етеді.

Бұл шабуылдарда бопсалаушы бағдарламаларды, фишингтік шабуылдарды, нөлдік күн эксплойттарын, файлдарсыз зиянды бағдарламаларды және «қызмет көрсетуден бас тарту» түріндегі шабуылдарды қоса алғанда, компьютерлердің, смартфондар мен IoT-құрылғылардың *(заттар Интернеті)* осалдықтары пайдаланылған.

Бопсалаушы бағдарламалар пайдаланылған шабуылдар

Бұл шабуылдар негізінен ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері мен компанияларды көздеді.

Үлкен резонансқа ие болған инциденттер:

Сан-Франциско шығанағы ауданындағы жылдамдықты көлік жүйесі

Vice Society

Сан-Францискодағы BART жүйесі қаңтарда бопсалаушы бағдарламаның шабуылынан зардап шекті, ол үшін жауаптылықты Vice Society тобы өзіне алды. Қызмет көрсетуде іркілістер орын алмағанмен, ұрланған деректер Интернетте орналастырылды. BART қызметтерге немесе ішкі жүйелерге әсердің болмағанын растайды, алайда аса маңызды жүйелерге ықтимал бэкдор-қолжетімділікке байланысты инцидент қорқыныш туғызды.

Reddit

BlackCat Ransomware

ALPHV бопсалаушылар тобы, сондай-ақ BlackCat ретінде белгілі, ақпанда Reddit.-ке жасалған кибершабуыл үшін жауаптылықты өзіне алды. Сәтті **фишингтік кампания** бастамашылық еткен шабуыл ішкі құжаттарды, бастапқы кодты, сондай-ақ қызметкерлер мен жарнама берушілер туралы ақпаратты қоса алғанда, **80 ГБ** деректердің **ұрлануына әкеп соқты**. Ұрланған деректерді жою үшін Reddit-тен 4,5 миллион доллар бопсалап алудың сәтсіз әрекеттерінен кейін топ оларды ашу ниеті туралы жариялады.

Dole Food Company

Dole Food компаниясы ақпанда орын алған бопсалаушы бағдарлама пайдаланылған және оның нәтижесінде қызметкерлер жазбаларының ашылмаған саны жария етілген шабуылды растады. Әсер шектелген болса да, Солтүстік Американдағы өндірістік кәсіпорындар шабуылдың нәтижесінде уақытша жабылды. Инцидент Dole жұмыс күші туралы деректерге ықпал етті, бұл туралы SEC ұсынатын жыл сайынғы есепте хабарланды.

АҚШ маршалдар қызметі

USMS

Бопсалаушы бағдарламаның АҚШ маршалдар қызметіне *(Әділет министрлігі құрамындағы федералды құқық қорғау органы)* шабуылы нәтижесінде сот процестерінің нәтижелерін, әкімшілік деректер мен жеке деректерді қоса, құқық қорғау органдарының конфиденциалды деректері жария етілді. USMS, үшінші тұлғалардың және USMS кейбір қызметкерлерінің тергеп-тексерулеріне байланысты субъектілердің сәйкестендірілетін ақпараты *(PII)*.

Орегон қаласы

Royal Ransomware

АҚШ-тың Орегон қаласында бопсалаушы бағдарламаның шабуылы нәтижесінде округ деректері шифрланды. Сайлау және шұғыл сервистер бақылауда қалды, бірақ үкіметтің барлық басқа операциялары шифрланды. Royal Ransomware мәлімдемесі бойынша, зиянкестер деректерге қолжетімділіктің ақысын өтеуді талап еткен, нақты соманы округ шенеуніктері айтқан жоқ.

Enzo Biochem

Нью-Йорктің биотехнологиялық компаниясы сәуір айында сынақтардың деректерін, сондай-ақ шамамен 2,5 миллион адамның жеке ақпаратын жария еткен бопсалаушы бағдарламаның шабуылына ұшырады. Есімдерге, тестілердің деректеріне және 600 000 әлеуметтік сақтандыру нөміріне қолжетімділік алынды. Enzo-ға жасалған шабуыл мамырда PharMerica фармацевтикалық алпауытқа жасалып, нәтижесінде 6 миллионға жуық адамның конфиденциалды деректері ашылған жеке шабуылдан кейін орын алды.

ESXi және Linux бопсалаушы бағдарламалары

Бопсалаушы бағдарламалардың әртүрлі топтары аса маңызды қызметтердің жұмысын және деректерді бұзып, VMware ESXi серверлері мен Linux жүйелеріне шабуылдарды жалғастырды.

Аргентинаның бағалы қағаздар жөніндегі ұлттық комиссиясы кибершабуылдың құрбаны болды.

2023 жылғы маусымда Аргентинаның бағалы қағаздар жөніндегі ұлттық комиссиясы болжам бойынша бопсалаушы бағдарламаларды әзірлеумен айналысатын Medusa хакерлік тобы жасаған кибершабуылдың құрбаны болды. Хакерлер керсінше жағдайда комиссияның 1,5 Тб құжаттарын және дерекқорларын Интернетте орналастырамыз деп қорқытып, бір аптаның ішінде $500 мың мөлшерінде ақы талап еткен. Аргентинаның қаржы нарықтарына соққы келтіруі ықтимал болған конфиденциалды файлдар мен жазбалар таралып кету қатеріне ұшырады.

Bleeping Computer деректері бойынша, Medusa бопсалау операциясы 2023 жылдың басынан миллиондаған ақы төлеу талаптарымен барлық әлемдегі корпоративтік құрбандарды көздеп, айтарлықтай қарқын алды. Medusa хакерлері 2023 жылғы мамырдан бастап өздерінің блогын іске қосып, қызметін жандандырды. Аталған платформа төлеп алудан бас тартқан құрбандар деректерінің таралуы үшін пайдаланылып, оларға БАҚ жоғары назарын тартуда. Medusa бопсалаушылар тобы 2023 жылғы мамырда Австралияның ірі онкологиялық орталығына жасалып, оның барысында хакерлер $100 мың мөлшерінде ақы төлеуді талап еткен шабуыл үшін жауаптылықты көтерді. Хакерлер сондай-ақ, 2023 жылғы сәуірде Microsoft Bing және Cortana сервистерінің бастапқы кодын Интернетте орналастырды.

Medusa бопсалаушы вирусы 2023 жылғы ақпанда барлық әлем бойынша кем дегенде 18 ұйымға шабуыл жасады. Вирус оның жұмысының негізін өзгертуге қабілетті көптеген тұжырымдарды қолдайды. Әдеттегідей іске қосылған кезде файлдарды шифрлауға ештеңе кедергі болмау үшін бағдарламалық қамтылым 280-ден астам Windows қызметтері мен процестерінің жұмысын автоматты түрде аяқтайды, содан кейін файлдарды қалпына келтіруде олардың пайдаланылуына жол бермеу үшін ОЖ резервтік көшірмелерін іздейді және жояды.

LockBit бопсалаушы бағдарламасының операторлары топ Boeing корпорациясынан ұрланған барлық ішкі файлдарды жария ету туралы шешім қабылдағанын мәлімдеді.

Киберқылмыскерлер бұл қадамға ұшақ жасау алпауыты ақы төлеуден бас тартқан соң барды. MalwareHunterTeam-нің X-аккаунтындағы ақпаратына сәйкес LockBit операторлары файлдарды жария етті. Boeing жүйелерінің жарияланған архивтері мен резервтік көшірмелерінің жалпы салмағы шамамен 50 ГБ. Boeing баспасөз хатшысы киберинцидент Boeing-тің өндірістік процестерін ішінара қозғағанын, бірақ соған қарамастан, ұшақ жасау мен ұшуларға ешқандай қауіп төндірмейтінін атап көрсетті. Lockbit операторлары Boeing-ті Tor желісіндегі таралған мәліметтер сайтындағы құрбандардың тізіміне қосты.

Жоғарыда сипатталған инциденттерде байқалған бопсалаушы бағдарламалардың ең белгілі штаммдары:

Royal

Киберқылмыскерлер 2022 жылғы қыркүйектен бастап американдық және халықаралық ұйымдарға Royal бопсалаушы бағдарламасының көмегімен шабуыл жасауда.

Желілерге енгеннен кейін олар вирусқа қарсы бағдарламаны ажыратып, бопсалаушы бағдарламаны ендіру алдында деректерді ұрлайды. Ақысын төлеп алу жөніндегі нұсқаулықтар шифрлағаннан кейін .onion URL-мекенжайы арқылы түседі және биткондармен 1-ден бастап 11 млн долларға дейін әртүрлі соманы талап етеді.

Royal бопсалаушы бағдарламасы өндіріс, байланыс, денсаулық сақтау мен білім беру сияқты маңызды секторларды көздейтіні байқалды.

LockBit 3.0.

LockBit 3.0 *(сондай-ақ LockBit Black ретінде белгілі)* операциялары «көрсетілетін қызмет ретіндегі бопсалаушы бағдарлама» *(RaaS)* үлгісін сақтайды және өзінің LockBit пен LockBit 2.0 алдыңғы буындарының неғұрлым жалтармалы және модульдік жалғасы болып табылады. LockBit 3.0 пайдаланатын филиалдар инфрақұрылымның аса маңызды секторларындағы кәсіпорындардың кең спектріне шабуылдар жасау үшін түрлі TTP қолданатыны байқалды.

BianLian

BianLian – бұл 2022 жылғы маусымнан бастап бопсалаушы бағдарламаларды пайдалана отырып, АҚШ пен Австралияның аса маңызды инфрақұрылымына шабуылдар жүргізетін киберқылмыскерлер тобы. Осы бопсалаушы бағдарламаларды әзірлеу, енгізу және күшпен алу арқылы белгілі олар барлау үшін қашықтағы жұмыс үстелі хаттамасының *(RDP)* шынайы есептік деректерін, сондай-ақ ашық бастапқы коды бар құралдарды жиі қолданады, ал деректерді шығарып алу үшін FTP, Rclone немесе Mega пайдаланады.

BianLian 2023 жылы қосарланған бапсалау моделінен ақысы төленбесе, деректерді жария етумен қорқытып, эксфильтрация негізіндегі бопсалауға көшті. Алдыңғы кампанияларда олар кәсіптік қызметтер мен жылжымайтын мүлікті дамыту сектрын көздеді.

Cl0p

Өзінің 2019 жылғы ақпанда пайда болу сәтінен бастап CL0P дамып, қазіргі уақытта бұзылған желілерге қолжетімділікті сатып, Ransomware-as-a-Service *(RaaS)* ретінде жұмыс істейді. Алғашқы кезде өзінің қосарланған бапсалауымен белгілі болған олар 2021 жылы тактикасын өзгертіп, деректерді ұрлауға шоғырланды.

Cl0p АҚШ-та 3000 астам ұйымды және бүкіл әлем бойынша 8000 ұйымды жария етті. Cl0p *(сондай-ақ Clop ретінде белгілі)* бопсалаушылар тобы 2023 жылғы мамырда Windows серверлерінде жұмыс істейтін MOVEit файлдарды беру серверінің қосымшасындағы нөлдік күн осалдығын пайдаланып, ерекше әсер тудырды. Эксплойттар тізбегі серверден, сондай-ақ Azure-нің BLOB-объектілерінің іске қосылған қоймасынан файлдарды ұрлайтын Microsoft Internet Information Services *(IIS)* .aspx веб-қабықшасын каталогқа \MOVEitTransfer\wwwroot\ серверлерге жеткізеді. SentinelOne есебінде ұйымдар Cl0p тобы тарапынан ықтимал шабуылдарды анықтау үшін пайдалана алатын сұрау салулар берілген.

Шабуыл айтарлықтай өзгерісті көрсетті: дәстүрлі түпкілікті нүктелерге бағдарланған бопсалаушы зиянкестер кодты бұлтты сақтау қызметтеріне арнайы жазды. Ықпал өте әсерлі болды: 500-ден астам ұйым және 34 миллион адамның деректері жария етіліп, бұл осы кампанияны 2023 жылдың ең ірі қатерлерінің біреуіне айналдырды.

QakBot

Сонымен қатар Qbot, Quackbot, Pinkslipbot және TA750, Qakbot ретінде белгілі 2008 жылдан бастап зиянды БҚ-мен көптеген жаһандық зақымдаулар тудырды. Бастапқыда бұл банктік троян болған, бірақ ол барлау, деректерді ұрлау, көлденең қозғалыс және бопсалаушы бағдарламаны жеткізу үшін пайдаланылатын ботнет пен зиянды БҚ-ның әмбебап нұсқасына айналды. QakBot үлестес зиянкестердің болашақ мақсаттары үшін жария етілген құрылғыларға қолжетімділікті сатып, қаржы және авариялық қызметтерді, коммерциялық объектілерді, сондай-ақ сайлау инфрақұрылымының ішкі секторын қоса, әртүрлі секторларды көздейді.

3CX жеткізілімдер тізбегіне шабуылдар

«SmoothOperator» атауына ие болып, анықталған жеткізілімдер тізбегіне шабуыл барысында солтүстік корея режимімен байланысты субъектілер 3CX Private Automatic Branch Exchange (PABX) платформасының инфрақұрылымын жария етті.

VoIP бағдарламалық қамтылымын әзірлеу компаниясын бүкіл әлем бойынша 600 000 астам адам пайдаланады және автомобиль өнеркәсібінен, тамақ өнеркәсібінен, қонақүй бизнесінен ұйымдарды, басқарылатын ақпараттық технологиялар *(MSP)* мен өңдеу өнеркәсібі қызметтерін берушілерді қоса алғанда, 12 миллионнан артық күнделікті пайдаланушылары бар.

Зиянкестер бұл қолжетімділікті 3CX түпкілікті нүктелерінің клиенттеріне зиянды кодты енгізу үшін пайдаланған, құрбандар оны жаңартулар түрінде жүктеген. Бэкдорға байланысты нұсқасында github[.]com/IconStorages/images мекенжайы бойынша орналасқан жалпыға қолжетімді код репозиторийінде орналастырылған .ico суреті файлындағы пайдалы жүктеме түтігін кодтау жолымен жасырын стенография қолданылып, бұл зиянды БҚ-ға C2 белсенді серверінің мекенжайын алуға мүмкіндік берген.

Деректердің таралуы
Data leak

Capita-ға шабуыл

Ең ірі аутсорсинг қызметтерін көрсетушілердің бірі Capita компаниясы 2023 жылғы наурызда күрделі кибершабуылға тап болды. Бұл инцидент Microsoft Office 365 қосымшаларын қоса алғанда, компанияның ішкі жүйелерінің жария етілуіне әкеп соқты.

Шабуыл нәтижесінде арасында жергілікті өкімет, Британия әскері мен Ұлттық денсаулық сақтау қызметін *(NHS)*, BBC қоса, мемлекеттік ұйымдар болған Capita көптеген клиенттерінің деректеріне, сондай-ақ Ұлыбританиядағы ең ірі университет зейнетақы қорының 470 000 жуық мүшесінің деректеріне әсер тиді.

WH Smith-ке шабуыл

Ұлыбританиядағы белгілі сауда маркасы WH Smith 2023 жылғы наурызда қызметкерлердің конфиденциалды деректерінің таралуына әкелген кибершабуылға тап болды. Шабуыл нәтижесінде ағымдағы және бұрыңғы қызметкерлердің аттары, мекенжайлары, ұлттық сақтандыру нөмірлері мен туған күндері жария етілді.

Клиенттік аккаунттар жеке жүйеде сақталғанның нәтижесінде, оларға қол жеткізілмеген. WH Smith инцидент туралы Лондон қор биржасын дереу хабардар етіп, қауіпсіздік жүйесін нығайту бойынша шаралар қолданды.

37 млн абоненттер деректерінің таралуы

2023 жылғы 19 қаңтарда T-Mobile америка ұялы байланыс операторының шамамен 37 млн. абонентінің деректерін хакерлер ұрлағаны белгілі болды. Оператордың жүйелері 2022 жылдың қараша айында хакерлік шабуылға ұшырағаны, алайда бұл туралы тек 2023 жылғы қаңтарда белгілі болған.

Зиянкестер туған күндерін, телефон нөмірлерін және мекенжайларын қоса, абоненттердің жеке деректеріне қолжетімділік алған. Бұл ретте парольдер, құпия кодтар, банктік ақпарат, сондай-ақ мемлекеттік құжаттардың деректері қол тимеген болып шықты. T-Mobile ұялы байланыс операторы сыртқы киберқауіпсіздік жөніндегі сарапшылардың көмегімен таралуды келесі күні тоқтатқанын компания хабарлады.

Киберқылмыскерлер Air Europa авиакомпаниясы клиенттерінің кредиттік карталары туралы ақпаратқа қолжетімділік алды

Air Europa 2023 жылғы 10 қазанда клиенттерге кибершабуыл нәтижесінде зиянкестер олардың төлем деректеріне қолжетімділік алуы ықтимал болғаны туралы хаттар жіберді.

Киберқылмыскерлер кредиттік карталардың нөмірлеріне, олардың жарамдылық мерзімдері мен CVV/CVC-ға қолжетімділік алғаны белгілі. Бұл ретте CVV/CVC кодтарының сақталуы осы төлем карталарының *(PCI DSS)* қауіпсіздік стандарты қағидаларына қайшы келеді. Компанияның өкілдері 28 тамызда мамандар ішкі жүйелерде күдікті белсенділікті айқындағанын хабарлады.

Зардап шеккен клиенттерді аваиакомпания орын алған инцидент туралы 41 өткен соң ғана хабарландырды. Air Europa өзінде ұрланған деректерге байланысты алаяқтықтың расталған оқиғалары жоқ екенін мәлімдейді, алайда, бұл ретте егер кредиттік карталар билеттерге ақы төлеу үшін пайдаланылған болса, клиенттерді оларды жоюға шақырады.

ChatGPT Plus-ке шабуыл

OpenAI-дың ChatGPT Plus сервисі 2023 жылғы наурызда жазылуышалрдың төлем деректерінің күрделі таралуына тап болды.

Проблеманы пайдаланыстағы кітапханалардың біреуіндегі осалдық тудырған. Осы осалдықтың нәтижесінде кейбір пайдаланушылар тоғыз сағат бойы басқа пайдаланушылардың аттарын, электрондық пошта мекенжайларын, төлем мекенжайларын, кредиттік карта нөмірлерінің соңғы төрт санын және олардың жарамдылық мерзімдерін қоса, төлем деректерін көре алған. OpenAI проблеманы шұғыл жойып, оқиға туралы пайдаланушыларды хабарландырды.

Рұқсатсыз қол жеткізу
Кибератаки

Австралияда 4 порт кибершабуылға байланысты жұмысын тоқтатты

Австралияның ең ірі порт операторы DP World компаниясы 2023 жылғы 10 қарашада ақпараттық инфрақұрылымының жұмысын тоқтатқан маңызды кибершабуылға тап болды. DP World Сидней, Мельбурн, Брисбен және Фримантледегі терминалдар арқылы Австралия контейнерлік тасымалының 40% басқарады. Хакерлік енудің нәтижесінде 30 мыңнан астам контейнердің келуі мен кетуі кідіртіліп, бұл сарапшылардың пікірі бойынша, елде әртүрлі тауарлар бағаларының өсуіне әкеліп соғады.

Хакерлердің Qulliq Energy-ге шабуылы

Канада

Канададағы ірі электр энергиясын жеткізуші Qulliq Energy 2023 жылғы қаңтардың ортасында кибершабуылдан зардап шегіп, оның нәтижесінде компьютерлер істен шықты, ал оның клиенттері көрсетілген қызмет үшін банктік карталардың көмегімен төлеу мүмкіндігінен айырылды.

Qulliq Energy компаниясының өкілдері шабуыл 2023 жылғы 15 қаңтарда басталғанын және электр станцияларының жұмысы қалыпты режимде жалғастырылғанына қарамастан, корпорацияның клиенттерді қолдау қызметі мен әкімшілік кеңселеріндегі компьютерлік жүйелер қолжетімсіз болғанын хабарлады. Компания кредиттік карталар бойынша төлемдерді қабылдай алмай, клиенттер шоттарды тек қана қолма-қол ақшамен немесе банктік аударымдармен төлей алды.

Blind Eagle

Check Point Research (CPR) сарапшылары 2023 жылғы 5 қаңтарда Blind Eagle тобы Оңтүстік Америкада шабуылдар ұйымдастыру үшін пайдаланатын кибершабуылдар тарихындағы зақымдаудың ең күрделі тізбектерінің бірі туралы айтты. Зиянкестер Колумбия мен Эквадорда испантілді нысаналарға шабуыл жасайды.

Пайдаланушыға Колумбияның мемлекеттік ведомствосынан, атап айтқанда Сыртқы істер министрлігінен фишингтік электрондық хат келуі мүмкін. Онда егер алушы «бюрократия мәселесін» шешпесе, оны елден шығу кезіндегі проблемалармен қорқытады. Хаттар сілтеме мен құрбанды сол сілтеме бойынша жіберетін PDF-файлды қамтиды. Өтуге әрекет жасалған кезде кіріс HTTP-сұрау салуға талдау жүргізіледі: ол Колумбия аумағынан тыс жасалған болса, сервер зақымдау тізбегін үзіп, пайдаланушыны Колумбия CIM көші-қон бөлімінің нақты сайтына қайта жібереді. Алайда сұрау салу Колумбиядан түссе, шабуыл жалғастырылады.

SMS-шабуылының көмегімен биржа қызметкерін бұзу

Coinbase криптовалюталық биржасы 2023 жылғы 17 ақпанда оның қызметкерлерінің бірін көздеген кибершабуыл туралы хабарлады. Бейтаныс зиянкес компанияның ИТ-инфрақұрылымына қашықтан қолжетімділік алуға әрекеттеніп, Coinbase жұмыскерінің жүйеге кіруге арналған есептік деректерін ұрлады.

Coinbase ақпараты бойынша шабуыл 2023 жылғы 5 ақпанда басталды: зиянкес белгілі бір маңызды хабарлама алу үшін өз компаниясының есептік жазбаларына кіруге шақырып, Coinbase бірнеше қызметкерлеріне SMS-хабарламалар жіберді.

Қызметкерлердің біреуі айлаға түсіп, сілтеме бойынша өтті, фишингтік парақшаға тап болып, онда өзінің есептік деректерін енгізді. Содан кейін алаяқ ұрланған ақпаратты пайдалана, Coinbase ішкі жүйелеріне кіруге әрекет жасады, бірақ қолжетімділік көп факторлық аутентификациямен қорғалғандықтан, бұл қолынан келген жоқ. Жүйеге қолжетімділік ала алмай, киберқылмыскер өзін Coinbase-нің ИТ-маманы ретінде таныстырып, криптовалюта биржасының сол қызметкеріне қоңырау шалды.

Зиянкес қызметкерді өзінің жұмыс станциясына кіріп, кейбір іс-қимылдарды жасауға сендірді. Coinbase-нің CSIRT қауіпсіздік командасы күдікті белсенділікті 10 минуттың ішінде анықтады және қызметкермен шұғыл байланысып, ол алаяқтық схеманың құрбанына айналғанын түсініп, зиянкеспен байланысты үзді.

WordPress арқылы ауқымды SEO-шабуыл

2023 жылғы ақпанда зиянкестер «WordPress» сайтының мазмұнын басқару жүйесінде жұмыс істейтін скайттарға маңызды кибершабуылды жүзеге асырды. Шабуылдың мақсаты іздеуді оңтайландырумен айла-шарғы жасау болды (SEO). Зиянкестер мақсатты сайттарға зиянды жарнамалық хабарландыруларды ендіру үшін WordPress-тегі осалдықтарды пайдаланды.

Бұл хабарландырулар кірушілерді сауалдар мен жауаптар берілген жалған парақшаларға жіберіп отырды. Жалған парақшалар зинкестер сайттарының SEO-позицияларын жақсарту үшін құрылды. Пайдаланушылар осы парақшаларға өткен кезде алдаудың құрбандары ғана болмай, зиянкестерге олардың іздеу жүйелеріндегі сайттарының рейтингін жақсартуға аңғарусыз көмектескен. Бұған осы парақшаларда трафикті ұлғайту және жасырын SEO-техникаларды пайдалану арқылы қол жеткізілгені ықтимал.

Осымен, бұл шабуыл киберзиянды ғана болмай, іздеу жүйелерінің тұтастығы мен дұрыстығына қауіп төндіріп, бизнес пен пайдаланушылардың іздеу технологияларына өскелең тәуелділігі аясында ерекше алаңдатарлық болып табылады.

Royal Mail-ге шабуыл

Ұлыбританияның ұлттық почта қызметі Royal Mail 2023 жылғы қаңтарда LockBit ресей тобы жүзеге асырған кибершабуылдың мақсатына айналды. Бұл инцидент посылкалар мен хаттарды ел аумағынан тыс жеткізуде едәуір кідірулер тудырып, олардың халықаралық пошта операцияларын шындап қиындатты.

Ұлттық пошта қызметтері де белгілі бұзушылықтарды бастан өткерді. Компания «киберинцидент» туралы мәлімдеді. Кейін зиянкестер ақысын төлеу мақсатында компанияға қысымды күшейту үшін Royal Mail қызметкерлерінің деректерін жариялады.

ABB-ға шабуыл

Автоматтандыру және энергетика саласындағы жетекші жаһандық компания ABB 2023 жылғы мамырда Black Basta тобы бастамалаған кибершабуылға ұшырады. Аталған шабуылдың нәтижесінде компьютерлер мен серверлерді қоса, компанияның жүздеген құрылғылары жария етілді. Шабуыл компанияның Windows Active Directory-іне зиянды бағдарламалық қамтылымды ендіруден басталып, бұл хакерлерге корпоративтік деректер мен жүйелердің елеулі санына қолжетімділік алуға мүмкіндік берді.

Ішкі операциялармен қатар, клиенттік ақпаратқа қатер төндіріп, маңызды файлдарға және жүйелерге қолжетімділікті бұғаттау үшін хакерлер шифрлау техникаларын қолданды. Компания шабуылдың одан әрі тарауын болдырмау және қалған жүйелерді қорғау үшін барлық VPN-қосылуларды уақытша ажыратуға мәжбүр болды. Бұл инцидент кибершабуылдар ірі өнеркәсіптік және технологиялық кәсіпорындарға төндіретін өскелең қатерге ерекше назар аудартуда.

The Guardian-ға шабуыл

Ұлыбританияның The Guardian атты күнделікті газеті 2022 жылғы желтоқсанның соңында және 2023 жылғы қаңтардың басында олардың ішкі операцияларының маңызды бұзылуына әкелген күрделі фишингтік кампанияға ұшырады. Әлеуметтік инженерия әдістерін пайдалана отырып, зиянкестер алдау арқылы қызметкерлердің біреуінен қолжетімді деректерді алды.

Содан кейін олар конфиденциалды ақпаратқа қолжетімділік алып, басылым желісіне енді. Шабуыл нәтижесінде редакция екі айға қашықтан жұмыс істеуге ауысуға мәжбүр болды, бұл материалдарды дайындау мен шығару процесін айтарлықтай күрделендірді. Жария етілген деректердің арасында қызметкерлердің жалақыларын, банктік деректемелерін және паспорт нөмірлерін қоса, жеке деректері болды.

Lacroix-қа шабуыл

Электрондық компоненттерді шығарумен айналысатын Lacroix компаниясы 2023 жылғы 12 мамырда аса маңызды кибершабуылға тап болды. Шабуыл нәтижесінде шифрлаушы вирус компанияның виртуалды инфрақұрылымын шифрлап, бұл жұмыстағы күрделі бұзушылықтарға әкеп соқты.

Нәтижесінде бір аптаның ішінде компанияның сегіз зауытының үшеуі жабылды. Бұл зауыттар алдыңғы жылдағы сатылымдардың жалпы көлемінің шамамен 19% үшін жауапты болып, компания сатылымдарының жалпы көлемінде маңызды рөл атқарған. Бұл оқиға кибершабуылдар өндірістік кәсіпорындарға төндіретін өскелең қатерге ерекше назар аудартуда.

Осалдықтар

Microsoft Exchange Online және Azure AD

Ағымдағы жылғы жазда STORM-0558 қытай тобы АҚШ-тың бірнеше үкіметтік мекемесіне жасаған шабуылдардың егжей-тегжейліктері белгілі болды.

Шабуылдар барысында Microsoft-тың бірқатар компонентке, соның ішінде ұрланған қол қою кілтіне және оны қолданудың ауқымды шеңберіне қол жеткізу құқықтары бұзылды, бұл зиянкестерге әсер еткен ұйымдардың Microsoft қызметтері үшін сеанстардың токендерін құруға мүмкіндік берді.

Зерттеушілер жеке есептік жазбалардың аутентификациясын қолдайтын барлық қосымшаларды қоса алғанда, осалдық Azure Active Directory қосымшаларының басқа түрлерін де қозғағанын анықтағанына қарамастан, алғашқы есептерде тек қана Exchange Online әсерге ұшырағаны айтылды. BingBang — бұл Azure Active Directory (AD) қосымшалары аясындағы проблема, мұнда әдеттегідей конфигурациясы қосымшаларға жағымсыз қолжетімділік бере алады.

Зерттеушілер Azure көптеген қосымшалары үшін «әдеттегідей» конфигурациясы Azure AD кез келген пайдаланушысы қосымшаларға қолжетімділік ала алатынын білдіретінін анықтады. BingBang-та сипатталған проблемаларды жою үшін Azure AD аутентификациясын пайдаланатын ұйымдар назарды бірінші кезекте конфиденциалды және аса маңызды қосымшаларға аударып, қосымшаларға қолжетімділіктің қандай деңгейлері берілгенін тексеруге тиіс.

Google Chrome әрбір пайдаланушысына SymStealer қауіп төндірді

2023 жылғы 13 наурызда Imperva Red командасы 2022 жылдың соңында Google Chrome браузерінде CVE-2022-3656 сәйкестендіргіші арқылы қадағалау жүргізілетін осалдықты анықтағаны белгілі болды. Осалдық белсенді болған сәтте ол 2,5 миллиардтан астам Chrome пайдаланушыларына ықпал етіп, зиянкестерге криптоәмияндар мен бұлтты провайдердің есептік деректері сияқты конфиденциалды файлдарды ұрлауға мүмкіндік берген.

Зиянкес, мәселен, криптоәмиян қызметін ұсынатын жалған веб-сайт құруы ықтимал болды. Ал әмиянды жасау процесінде компьютерге «қалпына келтіру кілттері» деп аталатындарды жүктеуді сұрай алды. Ivc жүзінде бұл кілттер пайдаланушының компьютеріндегі конфиденциалды файлға немесе папкаға символдық сілтемені қамтитын zip-файл болады, мәселен, бұлтты провайдердің есептік деректері. Пайдаланушы қалпына келтіру кілттерін архивтен шығарып, веб-сайтқа қайта жүктеген кезде символдық сілтеме өңделеді де зиянкес керек конфиденциалды файлға қолжетімділік алады. Веб-сайт заңды болып көрінетіні, ал қалпына келтіру кілттерін жүктеу және көшіру процесі – криптовалюталық әмияндар үшін қалыпты тәжірибе болғандықтан, пайдаланушы бірдеңе дұрыс емес екенін түсінбеуі де мүмкін.

Google 108 нұсқадағы Chrome символдық сілтемелерінің осалдығын толық жойды. Өз криптоактивтеріңізді қорғау үшін бағдарламалық қамтылымды өзекті жай-күйінде қолдап отыру, күмәнді файлдарды жүктеуден немесе сенімсіз дереккөздерінен сілтемелер бойынша өтуден аулақ болған маңызды.

Ақпаратты бұлттық ұрлаулар

2023 жылы дұрыс бапталмаған немесе осал бұлтты сервистерден есептік деректерді сұрататын бұлтты ақпарат ұрлаушылардың таралуының тұрақты артуы байқалды.

Кейбір белгілі үлгілер мыналарды қамтиды: AlienFox – бұл Androxgh0st кодының фрагменттері негізінде жасап шығарылған және Telegram арналары арқылы сатылатын кешенді құрал. Зиянкестер ашық бұлтты сервистермен жұмыс істеу үшін Python негізіндегі құралдардың модульдік жинағын қашықтан іске қосады. AlienFox бірінші кезекте зиянкестер спам-шабуылдар жүргізу үшін теріс пайдалана алатын есептік деректерді, API кілттерін және AWS SES пен Microsoft Office 365 қоса алғанда, белгілі сервистердің құпияларын көздейді.

Мақсатты сервистердің егжей-тегжейлі бөлінуін SentinelLabs толық есебінде табуға болады. Сол кодтың AlienFox тәрізді Legion тармағының спамға бағдарланған көптеген ұқсас функциялары бар. AlienFox сияқты Legion да Telegram арналарына жиі кіретін сатып алушылар арасында таратылады.

Ақпараттық қауіпсіздіктің халықаралық қатерлерін жүйелі түрде талдау ұйымдарға тек қана инсайттар емес, ақпараттық қауіпсіздіктің ықтимал инциденттеріне әрекет етуде өзінің дайын болуы мен тиімділігін арттыруға мүмкіндік туғызып, маңызды мәнге ие болуда. Бұл тәсіл дайындықтың, сондай-ақ хабардарлықтың жоғары деңгейін қолдап отыруға мүмкіндік береді.

Қорғау саласындағы стратегиялар мен әдістерді үнемі жаңарту тұрақты киберқауіпсіздіктегі түйінді элементке айналуда. Қатерлер туралы өзекті деректер және аналитика ұйымдарды өз стратегияларын бейімдеу мен жетілдіру үшін қажет ақпаратпен қамтамасыз етеді. Үнемі жаңарту мен талдаудың осы циклі кибершабуылдарға байланысты тәуекелдерді барынша азайтуға және цифрлық ортада қауіпсіздіктің жоғары стандартын қолдап отыруға мүмкіндік беретін механизмді құрады.

Осымен, халықаралық қатерлерді үнемі талдау ұйымдар киберқауіпсіздік саласындағы ұдайы өзгеріп отыратын сын-қатерлерге сәтті қарсы тұра алатын неғұрлым қорғалған киберкеңістікті құрудың басты құралына айналуда.

Ақ инциденттері бойынша статистика:

Ақпараттық қауіпсіздіктің өңделген инциденттеріне талдау жүргізе отырып, «STS» командасы негізгі трендтер мен ерекшеліктерді бөлектеуге тырысады, бұл бізге тек қана алдыңғы тәжірибелерден тәлім алуға емес, болашақ киберқатерлерден қорғау бойынша неғұрлым тиімді стратегияларды әзірлеуге мүмкіндік береді.

Біздің статистикалық деректер инциденттер мен кибершабуылдардың алуан түрлі аспектілерін қамтиды. Осы деректерді ұсыну ашықтықты ғана көрсетуге арналмай, сондай-ақ жұртшылық пен біздің серіктестерге цифрлық кеңістіктегі қатерлердің динамикасын жақсырақ түсінуге мүмкіндік береді.

АҚ-ның өңделген инциденттері бойынша статистиканы ұсынудың осы процесі хабардарлықты арттыру үшін маңызды. Біз кездесетін нақты сценарийлер мен сын-қатерлердің негізінде алдағы уақыттағы зерттеулердің, біздің АҚ стратегияларымызды талдау және жетілдірудің берік іргетасын құруға ынталанамыз.

«STS» командасы 2023 жылғы қаңтардан бастап ақпараттық қауіпсіздіктің қатерлері мен инциденттері бойынша шамамен **35 мың өтінім** тіркеді

ЗБҚ 21 940

ЖАО-да ағымдағы жылы ең таралған ЗБҚ түрлері:

- Malicious-url - **5 277**
- HTTP2.RST_STREAM.Rapid.Reset.DoS - **2 885**
- TCP.Split.handshake - **1 316**
- HTTP2.RST_STREAM.Rapid.Reset.DoS.Rate - **354**
- Memcached.try_read_command_binary.Stack.Buffer.Overflow - **185**

МО-да ағымдағы жылы ең таралған ЗБҚ түрлері:

- Malicious-url - **1 517**
- HTTP2.RST_STREAM.Rapid.Reset.DoS - **492**
- TCP.Split.handshake - **222**
- HTTP2.RST_STREAM.Rapid.Reset.DoS.Rate - **126**
- Expat.Libexpat.XML.Paser.DOS - **76**

ТОП-5 МО

ЗБҚ-ға байланысты оқиғалардың саны бойынша ТОП – 5 МО:

- ҚР ІІМ - **493**
- ҚР ҚМ - **414**
- ҚР ЦДИАӨМ - **396**
- ҚР ОСК - **231**
- ҚР ТЖМ - **189**

Ботнет
4 040

ЖАО-да ағымдағы жылы ең таралған ботнет түрлері:

- Mozi.botnet - **1 036**
- njRAT.Botnet - **304**
- Andromeda.botnet - **303**
- Lethic.Botnet - **267**
- Mariposa.Botnet - **217**

МО-да ағымдағы жылы ең таралған ботнет түрлері:

- Mozi.botnet - **200**
- Lethic.Botnet - **66**
- njRAT.botnet - **66**
- andromeda.Botnet - **63**
- AAEH.Botnet - **35**

ТОП-5
МО

Ботнеттерге байланысты оқиғалардың саны бойынша ТОП – 5 МО:

- ҚР ЦДИАӨМ - **130**
- ҚР ІІМ - **109**
- ҚР ТЖМ - **36**
- ҚР АШМ - **30**
- ҚР ҚМ - **28**

Осалдықты пайдалану - 2 726 АҚ инциденті

Фишингтік шабуыл – 2 160 АҚ инциденті

Фишингті ұқсастыру түрлері

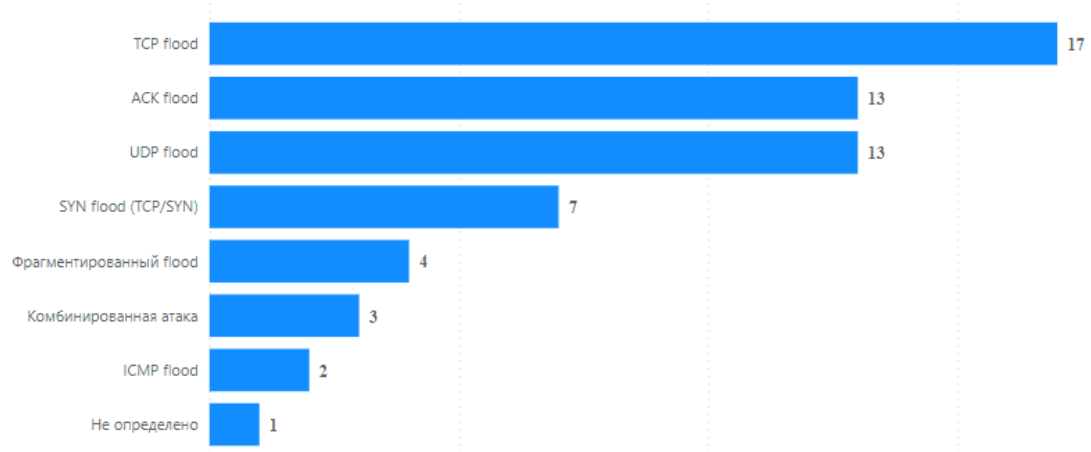
Интернет-ресурсқа қолжетімділіктің болмауы - 1 090 АҚ инциденті

Жалпы қолжетімсіз болу ұзақтығы бойынша ТОП-5 ИР:

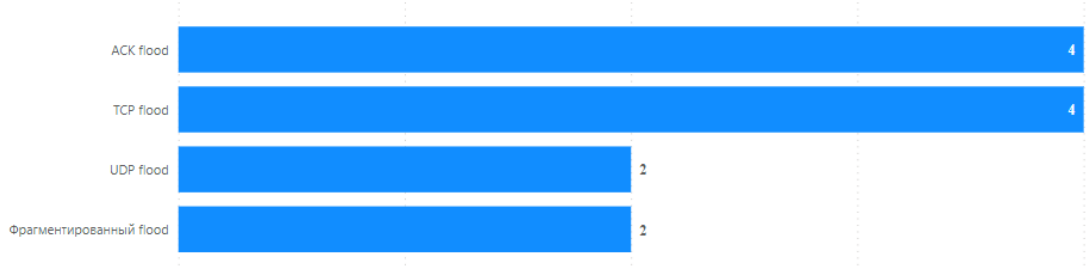
ИР атауы	Қолжетімсіздікті тіркеулер саны	Жалпы қолжетімсіз болу уақыты *күндер*	Жалпы қолжетімсіз болу уақыты *сағат*
spon.energo.gov.kz	10	48,3	1 161
pkrezerv.gov.kz	2	25,8	620
election.gov.kz	67	16,1	388
sud.gov.kz	154	14	337
dot.saylau.kz	24	12,3	295

С 2023 жылдың басынан **DDoS – шабуылдарға** байланысты **272** оқиға тіркелді.

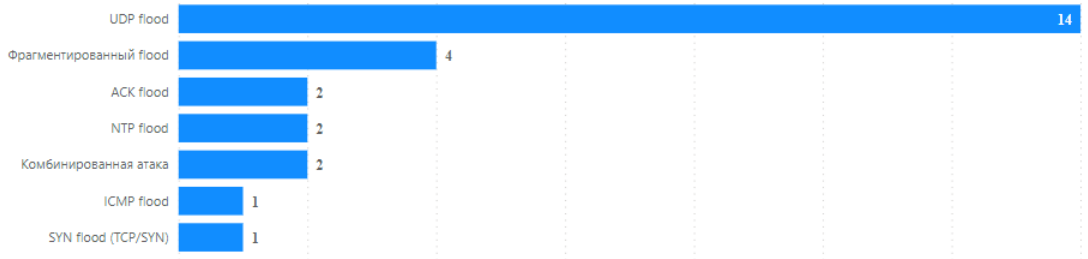
ҚР ЕДБ-ға бағытталған DDoS – шабуылдардың түрлері:



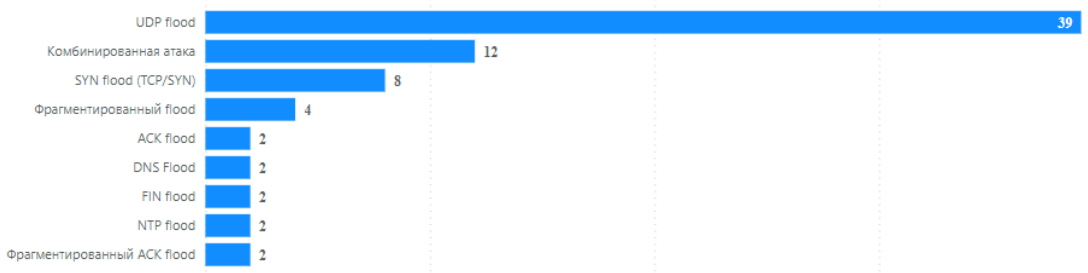
ҚР МО-ға бағытталған DDoS – шабуылдардың түрлері:



Квазимемлекеттік секторға бағытталған DDoS – шабуылдардың түрлері:



АКИАМО-ға бағытталған DDoS – шабуылдардың түрлері:



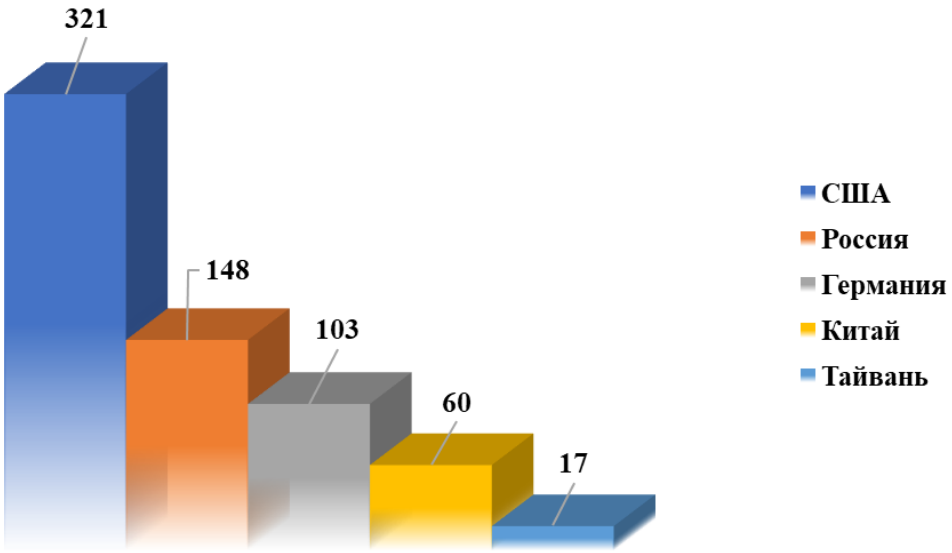
272 оқиғаның 152 инциденті тіркеліп,
пысықталғанын атап көрсеткіміз келеді.

Анықталған ақпараттық қауіпсіздік қатерлері мен компьютерлік инциденттер бөлігінде халықаралық ақпарат алмасу жөніндегі іс-шаралар:

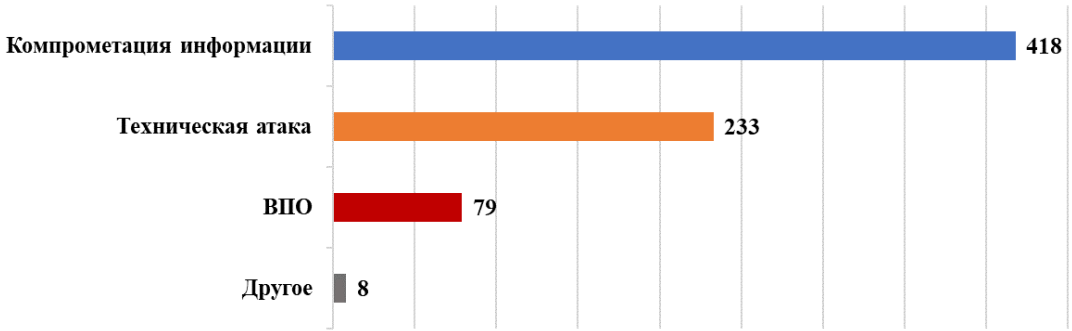
2023 жылы АҚ оқиғалары мен инциденттерін пысықтау нәтижелері бойынша АҚҰҰО 78 мемлекеттің шетелдік ұйымдарына 1832 хабарлама жіберді *(Интернетке қол жеткізудің бірыңғай шлюзі мен Электрондық поштаның бірыңғай шлюзі жабдығынан алынған мәліметтер (IPS/IDS).*

32 мемлекеттің шетелдік ұйымдарынан АҚҰҰО мекенжайына 738 хабарлама келіп түсті.

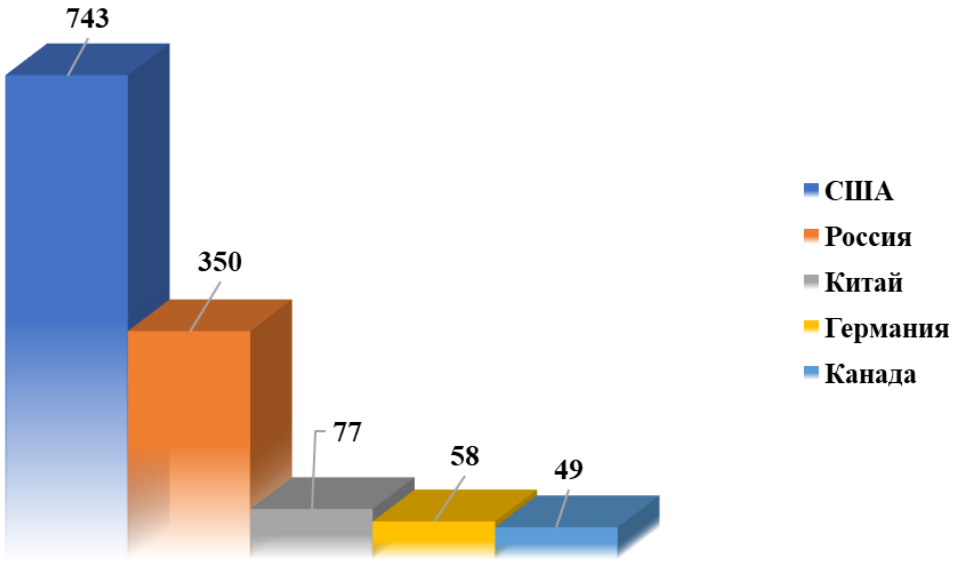
2023 жылдағы кіріс халықаралық хабарламалардың елдер бөлінісіндегі саны (ТОП-5):



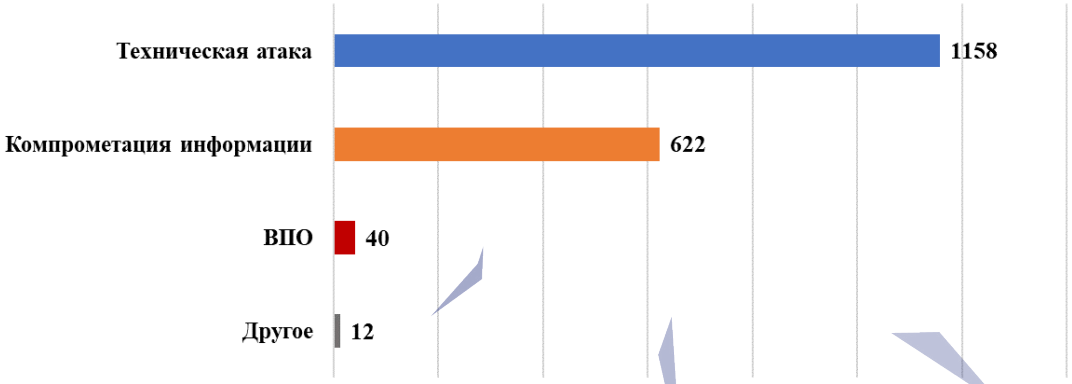
2023 жылдағы кіріс халықаралық хабарламалардың АҚ оқиғалары/қатерлері/инциденттері санаттары бөлінісіндегі саны:



2023 жылдағы шығыс халықаралық хабарламалардың елдер бөлінісіндегі саны (ТОП-5):



2023 жылдағы шығыс халықаралық хабарламалардың АҚ оқиғалары/қатерлері/инциденттері санаттары бөлінісіндегі саны :

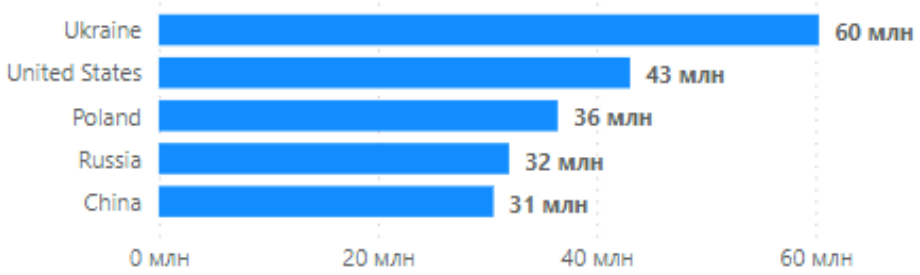


ИҚБШ клиенттеріне шабуылдар туралы мәліметтер

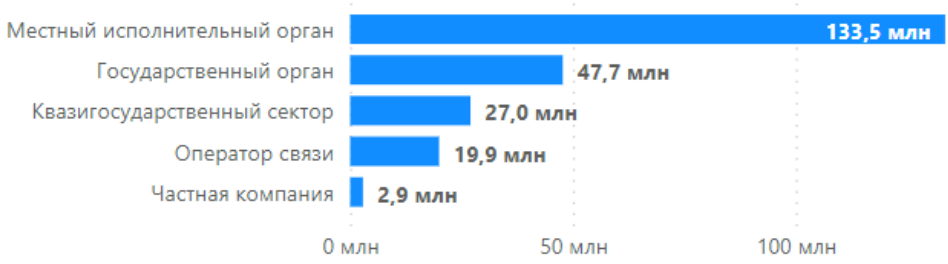
2023 жылы ИҚБШ клиенттерінің қорғауында осалдық табу әрекеттерінің саны кестелерде көрсетілген елдердің инфрақұрылымы пайдаланылып тіркелді.

2023 жылы CVE-2023-28771 осалдығын пайдалану мақсатында ИҚБШ клиенттеріне бағытталған зиянды белсенділік туралы мәліметтер - 223 млн. шабуылдан астам:

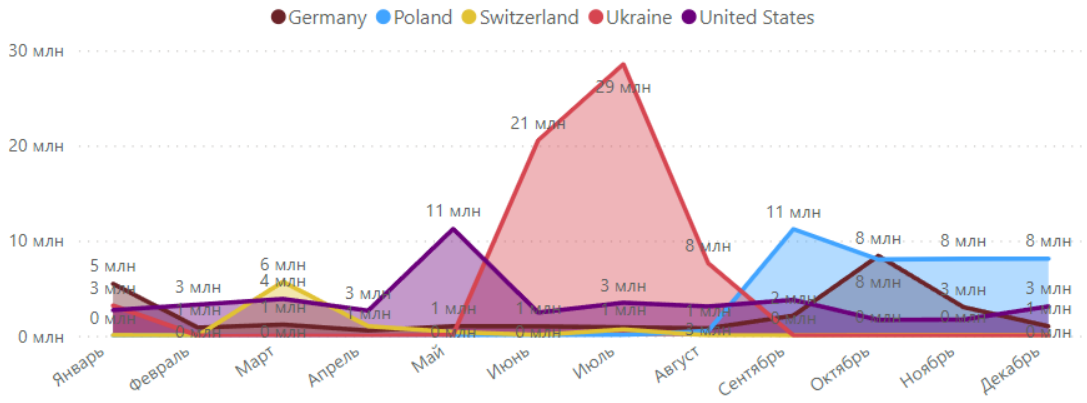
ТОП-5 шабуыл жасаушы елдер



Шабуылдар бағытталған ТОП-5 сектор



ТОП-5 шабуыл жасаушы елдерден шыққан шабуылдар санының өзгеру динамикасы

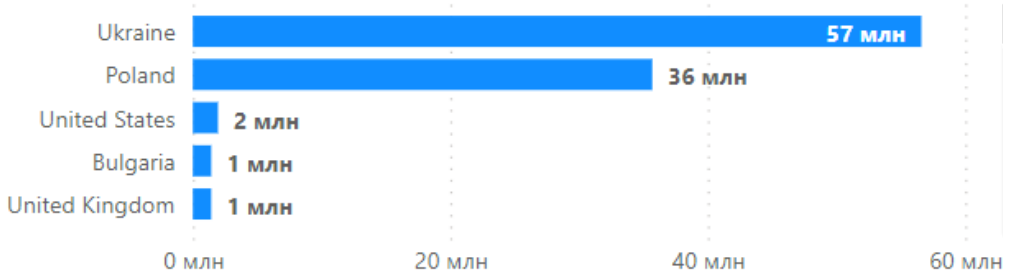


Осалдық туралы ақпаратпен мына сілтеме бойынша танысуға болады: *https://www.fortiguard.com/encyclopedia/ips/53203.*

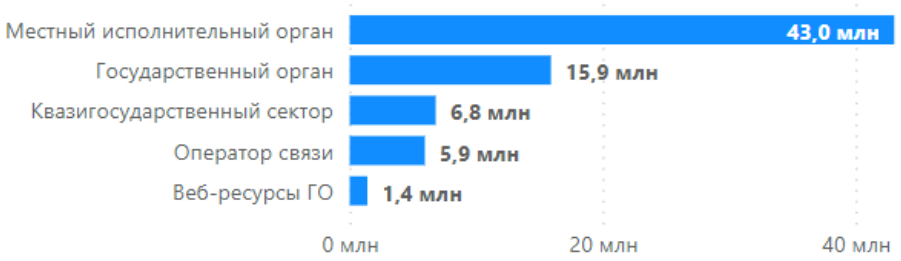
Forti мәліметтері бойынша, осалдық өнеркәсіптік жүйелерді *(SCADA -Supervisory Control And Data Acquisition)* қорғау үшін пайдаланылатын Zyxcel жабдықтарын қозғайды. Мемсекторға бағытталған шабуылдың үлесі 62% құрады *(ЖАО-44%, МО-18%)*. Шабуылдар негізінен ҚР солтүстік өңірлеріне *(Солтүстік Қазақстан облысы, Ақмола облысы, Қостанай облысы)* бағытталды.

ИҚБШ клиенттеріне бағытталған зиянды белсенділік туралы мәліметтер – ТОП-5 шабуыл жасаушы елдер (инфрақұрылымды пайдаланып):

ТОП-5 шабуыл жасаушы елдер

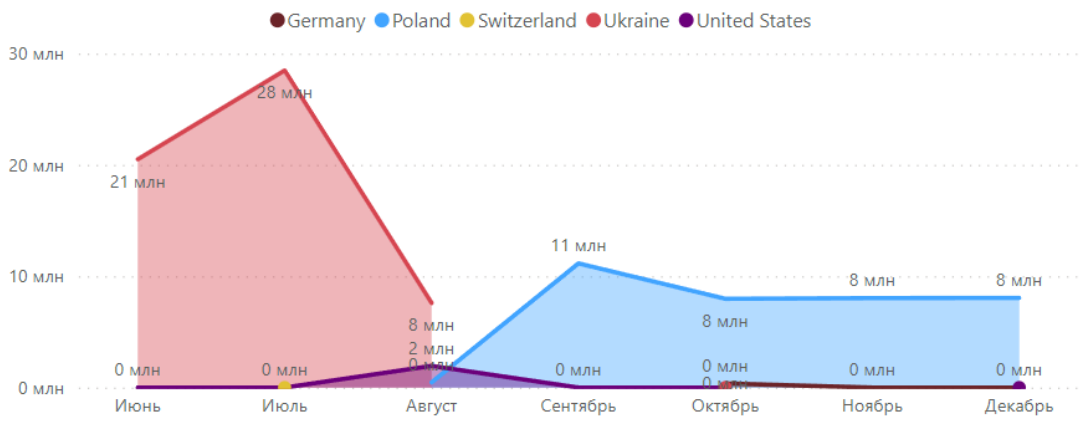


Шабуылдар бағытталған ТОП-5 сектор



Қатерлер

ТОП-5 шабуыл жасаушы елдерден шыққан шабуылдар санының өзгеру динамикасы

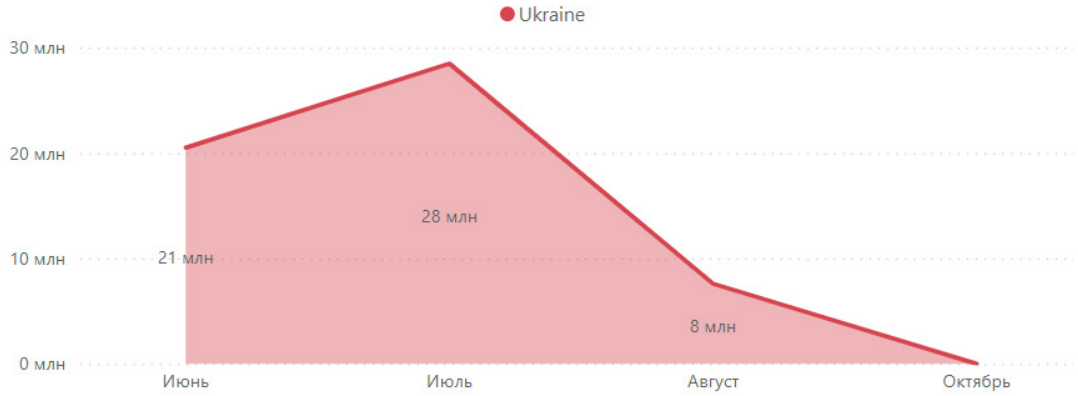


ТОП-3 шабуыл жасаушы елдер: Украина инфрақұрылымын пайдаланып

Зиянды белсенділік бағытталған секторлар жөніндегі мәліметтер

Қатерлер

Айлар бойынша статистика



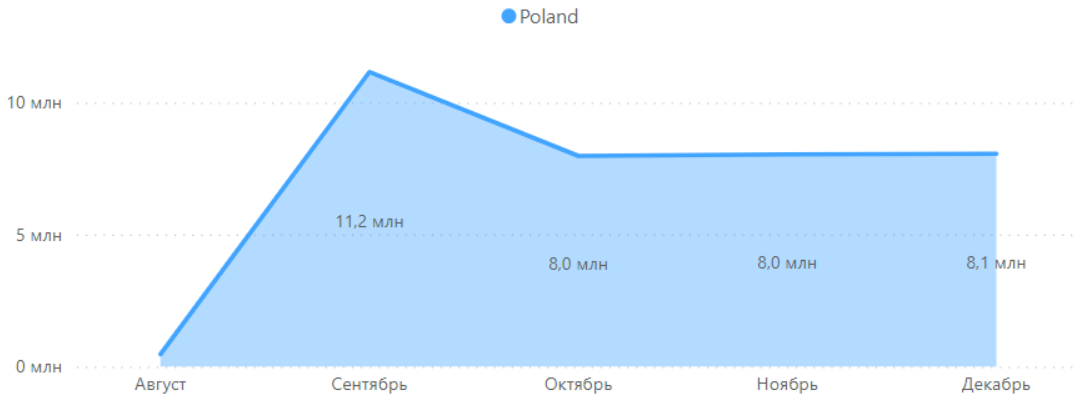
Шабуылдар бағытталған ҚР өңірлерінің ТОП-5

ТОП-3 шабуыл жасаушы елдер: Польшаның инфрақұрылымын пайдаланып

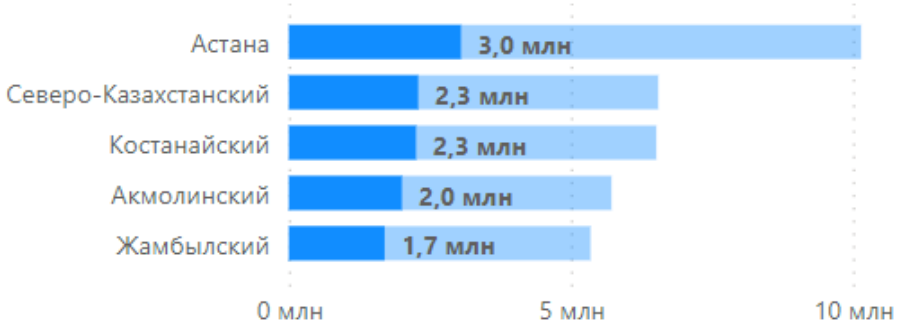
Зиянды белсенділік бағытталған секторлар жөніндегі мәліметтер

Қатерлер

Айлар бойынша статистика



Шабуылдар бағытталған ҚР өңірлерінің ТОП-5

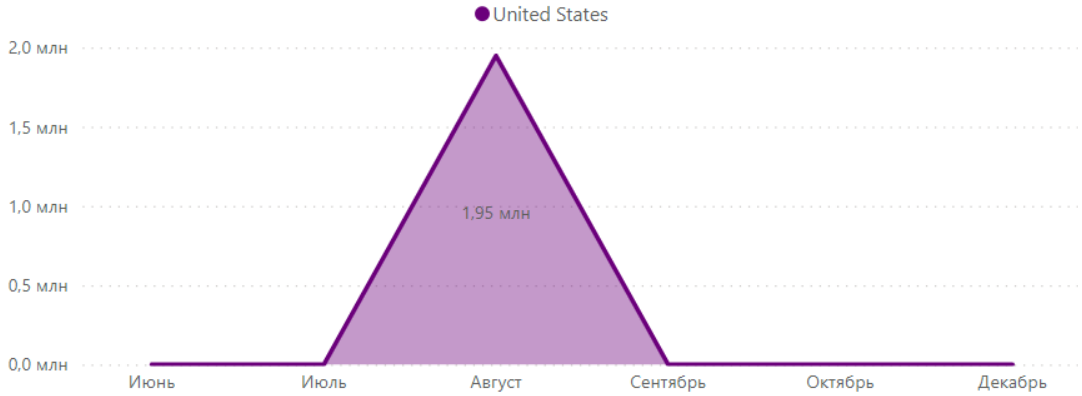


ТОП-3 шабуыл жасаушы елдер: АҚШ инфрақұрылымын пайдаланып

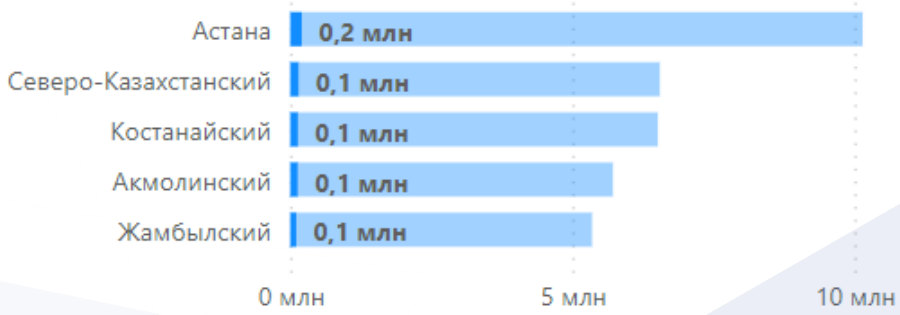
Зиянды белсенділік бағытталған секторлар жөніндегі мәліметтер

Қатерлер

Айлар бойынша статистика



Шабуылдар бағытталған ҚР өңірлерінің ТОП-5



«STS» командасы ақпараттық қауіпсіздік саласындағы өзекті осалдықтарға және бүкіл ел бойынша әртүрлі ақпараттандыру объектілеріне ықпал ететін эксплойттарға белсенді түрде талдау жүргізеді. Бұл тәжірибе қарапайым азаматтардың қауіпсіздігін және олардың цифрлық кеңістігін қорғауды қамтамасыз етуге бағытталған.

Осалдықтарды талдау бізге зиянкестер рұқсатсыз қол жеткізу немесе шабуылдар жасау үшін пайдалана алатын жүйелер мен бағдарламалық өнімдердегі ықтимал осал тұстарды жедел анықтауға мүмкіндік береді. Өзекті қатерлерді қадағалап, біз қоғамдық ресурстардың деңгейімен қатар, жеке веб-сайттардың деңгейінде ақпараттық қауіпсіздік дәрежесін жоғарылату үшін анықталған проблемаларды жою жөнінде ұсынымдар және кеңестер береміз.

Біздің мақсатымыз – ақпараттық қауіпсіздіктің қатерлері туралы ақпаратты барлығына неғұрлым қолжетімді және түсінікті ету. Біз қарапайым азаматтарға оларға өз конфиденциалдығы мен цифрлық әлемдегі қауіпсіздігін қорғауға көмектесетін ақпарат пен құралдарды ұсынуға тырысамыз. Өзекті ұсынымдар мен эксплойттардың талдаулары біздің қоғамға ақпараттық қауіпсіздіктің және онлай-кеңістікте сенімділіктің жоғарырақ деңгейін қамтамасыз ететін «цифрлық қалқан» ретінде қызмет етуге арналған.

Төменде қазақстандық ақпараттандыру объектілеріне қолдану мүмкін болған ең өзекті осалдықтар мен эксплойттар келтіріледі:

GeoServer CVE-2022-24816 и CVE-2023-25157

KZ-CERT компьютерлік инциденттерге ұлттық әрекет ету қызметі CVE-2022-24816 және CVE-2023-25157 сәйкестендіргіштері бар аса маңызды осалдықтарға ықтимал бейімді GeoServer пайдаланатын IP-мекенжайларын анықтады.

GeoServer – геокеңістіктік деректерді жариялау мен өңдеуге арналған ашық бағдарламалық қамтылым. GIS (Geographic information system) басқа қосымшаларымен үйлесімділікті қамтамасыз етіп, ол деректер мен хаттамалардың WMS (Web Map Service), WFS (Web Feature Service), WCS (Web Coverage Service) қоса алғанда, деректер алмасуға арналған көптеген форматтарды қолдап отырады. GeoServer шешімдер қабылдау үшін кеңістіктік деректер маңызды компоненттер болып табылатын геология, экология, геодезия, ауыл шаруашылығы, қалаларды басқару сияқты және т.б. әртүрлі салаларда пайдаланылады.

CVE-2022-24816 JAI-EXT – мақсаты API Java Advanced Imaging (JAI) кеңейтуі болып табылатын ашық бастапқы коды бар жоба. Желілік сұрау салу арқылы

Jiffle скриптін ұсынуға мүмкіндік беретін бағдарламалар кодтың қашықтан орындалуына әкелуі ықтимал, себебі Jiffle скрипті Janino арқылы Java-кодқа орнатылып орындалады.

Атап айтқанда, бұл GeoServer жобасын қозғайды. CVE-2023-25157 бірқатар функциялар мен фильтрлерде PostGIS және Oracle сияқты белгілі деректер қоймаларымен пайдаланған кезде SQL-инъекцияларының осалдықтары анықталды. Бұл осалдықтар PropertyIsLike, strEndsWith, strStartsWith фильтрін, FeatureId фильтрін, jsonArrayContains функциясын және DWithin фильтрін қамтиды. Осы осалдықтар жүйеге рұқсатсыз қолжетімділік алу үшін ықтимал пайдаланылуы мүмкін.

Kvant.edu.kz интернет-ресурсында анықталған веб-шелл

KZ-CERT компьютерлік инциденттерге ұлттық әрекет ету қызметі kvant.edu.kz интернет-ресурсындағы веб-шеллді анықтады. Веб-шелл (web-shell) — бұл зиянкестер веб-серверге қашықтан әкімшілендіру және командаларды орындау үшін жүктей алатын зиянды скрипт. Зақымдалған веб-серверлер Интернет желісінде де, ішкі желіде де болуы мүмкін. Бұл кейінгі уақытта ішкі хосттарға қосу үшін веб-шелл қай тұста пайдаланылатынына байланысты болады. Веб-шелл мақсатты веб-сервер қолдайтын кез келген тілде жазылады.

Жиірек кездесетін веб-шеллдер ең қолдаулы PHP және ASP сияқты тілдерде жазылған. Сонымен қатар, Perl, Ruby, Python және Unix қабықшаларының сценарийлері қолданылады. Веб-шеллдің мүмкіндіктері 4.1.0 және одан жоғары нұсқасындағы PHP-да жұмыс істеуді, сондай-ақ AJAX-ке ұқсас синхронды емес сұрау салуларды пайдалануды қамтиды. Бұл құрал POST және GET сұрау салуларының әдістерін қолдана алады және олармен обфускация жүргізуі, сондай-ақ пайдаланушылар ортасында жұмыс істеуі мүмкін.

Ол символдардың 22 әртүрлі жинағын қолдайды және жүктеген кезде сіздің кілтіңіздің (парольдің) көмегімен бастапқы кодты шифрлайды, бірақ бұл кілтті алған файлда қамтымайды. Бұдан басқа, веб-шеллдің жасырын режимі бар және парақшаны қайта жүктеусіз және деректерді жоғалтпай әртүрлі міндеттермен жұмыс істеуге мүмкіндік береді.

CVE-2023-3519C Citrix NetScaler ADC және NetScaler Gateway осалдығы

KZ-CERT компьютерлік инциденттерге ұлттық әрекет ету қызметі CVE-2023-3519 сәйкестендіргішінің маңыздылық деңгейі жоғары осалдығына ықтимал бейімді Citrix NetScaler ADC және NetScaler Gateway өнімдерін пайдаланатын IP-мекенжайларын анықтады.

NetScaler Application Delivery Controller (ADC) – бұл серверлерге жүктемені теңдестіруді, трафикті басқаруды, деректерді шифрлау мен шабуылдардан нақты уақытта қорғауды қамтамасыз ететін бағдарламалық-аппараттық желілік контроллер. Ол сұрау салулардың тең бөлінуін қамтамасыз етіп және

артық жүктемелерді болдырмай, бірнеше серверге жүктемені бөлуге мүмкіндік береді. Бұл қосымшалардың өнімділігін және пайдаланушылар үшін қолжетімділігін арттырады.

Citrix NetScaler Gateway — қосымшалар мен деректер деңгейінде егжей-тегжейлі бақылау құралдарын қамтамасыз етіп, сонымен бірге пайдаланушыларға кез келген орыннан қашықтан қол жеткізу мүмкіндігін қамтамасыз ететін қосымшаларға қауіпсіз қол жеткізуге арналған шешім. Осалдық зиянкеске еркін кодты авторланусыз орындауға мүмкіндік береді. Пайдалана алу үшін әсер етілген құрылғылар шлюз (мәселен, VPN, ICA Proxy, CVPN, RDP Proxy виртуалды сервер) немесе аутентификация, авторлану және аудиттің (AAA) іске қосылған SAML бар виртуалды сервері ретінде конфигурацияланған болу керек. Осалдық SAML хабарламасында каноникализация немесе түрлендіру әдістерінің өте көп саны жіберілген кезде пайда болады.

MikroTik RouterOS CVE-2023-30799

KZ-CERT компьютерлік инциденттерге ұлттық әрекет ету қызметі Интернеттің қазақстандық сегментін мониторингтеу барысында ИҚБШ клиенттерінің әдеттегідей парольдері бар және CVE-2023-30799 сәйкестендіргіші осалдығының аса маңызды деңгейіне ықтимал бейімді MikroTik RouterOS-ты пайдаланатын IP-мекенжайларын анықтады.

CVE-2023-30799 осалдығы әкімшінің есептік жазбаларын пайдалана отырып, құрылғының Winbox немесе HTTP-интерфейстері арқылы артықшылықтард Super Admin»-ге дейін жоғарылатуға мүмкіндік береді. Шектелген артықшылықтар беретін admin есептік жазбасына қарағанда, RouteOS операциялық жүйесіне Super Admin толық қолжетімділік береді. Артықшылықтар «Super Admin» деңгейіне дейін жоғарлаған кезде функцияларды шақырту мекенжайын бақылауға мүмкіндік беретін кодтың жолын қолға түсіруге болады.

CVE-2023-36845 Juniper Networks Junos осалдығы

KZ-CERT компьютерлік инциденттерге ұлттық әрекет ету қызметі SRX сериясының брандмауэрлерінде ОЖ-ның J-Web интерфейсі мен EX коммутаторларында CVE-2023-36845 сәйкестендіргішінің маңыздылық деңгейі жоғары осалдығына ықтимал бейімді Juniper Networks Junos өнімдерін пайдаланатын 28 IP-мекенжайын анықтады.

Junos — бұл желілік операцияларды автоматтандыруға арналған операциялық жүйе. Операциялық жүйе Juniper маршрутизаторлары мен коммутаторлары сияқты желілік жабдықта кеңінен қолданылады және ол компьютерлік желілердің сенімді әрі тиімді жұмысын қамтамасыз ету үшін көптеген функциялар ұсынады. Junos компьютерлер мен желідегі басқа құрылғылар арасында байланысты қамтамасыз ету үшін корпоративтік желілерде және интернет-провайдерлерде пайдаланылады. J-Web – бұл Junos құрылғыларын баптау үшін пайдаланылатын графикалық интерфейс. J-Web интерфейсі

HTTP немесе HTTPS хаттамасының қолдауымен веб-браузердің көмегімен маршрутизация платформасын қадағалауға, баптауға, жөнсіздіктерін жоюға және басқаруға мүмкіндік береді. SRX сериясының Juniper брандмауэры – бұл желілерді рұқсатсыз қол жеткізуден, вирустардан, интернеттен жасалатын шабуылдардан және басқа да қатерлерден қорғау үшін пайдаланылатын интеграцияланған брандмауэр және құрылғы. EX сериясының Juniper коммутаторлары – корпоративтік және филиалдық желілерге, сондай-ақ деректерді өңдеу орталықтарына арналған бөлу деңгейінің/ядроның өнімділігі жоғары бұлтты қолжетімділік коммутаторлары. EX сериясының коммутаторлары сымды желілерге қол жеткізуді оңайлатады.

CVE-2023-36845 осалдығы зиянкестерге EX және SRX серияларында Juniper Networks Junos ОЖ-ның J-Web-де осалдықтар тізбегін құруға мүмкіндік беріп, тұтастықтың ішінара жоғалуына әкелетін PHP ортасының белгілі ауыспалы мәнін өзгертуге мүмкіндік береді.

CVE-2023-46604 Apache ActiveMQ осалдығы

KZ-CERT компьютерлік инциденттерге ұлттық әрекет ету қызметі CVE-2023-46604 сәйкестендіргішінің маңыздылық деңгейі жоғары (CVSS 10-нан 10) осалдығына бейімді Apache ActiveMQ хабарламалар алмасудың осал сервистерін анықтады.

Apache ActiveMQ — бұл ашық бастапқы коды бар, Java Message Service (JMS) іске асыратын және MQTT, AMQP, REST пен WebSocket сияқты әртүрлі хаттамаларды қолдайтын хабарламал алмасу жүйесі. Бұл жүйе бөлінген жүйелерде олардың интерациясын, масштабталуы мен өнімділігін қамтамасыз етіп, асинхронды деректер алмасу үшін пайдаланылады.

ActiveMQ қаржы, телекоммуникациялар, денсаулық сақтау мен бөлшек сауданы қоса алғанда, әртүрлі салаларда транзакцияларды өңдеу, желілік трафикті басқару, медицина мекемелері арасында деректер алмасу және туарлар мен тапсырыстарды басқару жүйелерін интеграциялау үшін пайдаланылады. Apache ActiveMQ бағдарламалық платформасындағы CVE-2023-46604 сәйкестендіргіші осалдығының жадта дұрыс емес деректерді қалпына келтірумен байланысы бар. Осалдықты пайдалану қашықтан іс-қимыл жасайтын зиянкеске OpenWire хаттамасы бойынша класс құру арқылы еркін кодты орындауға мүмкіндік береді.

CVE-2023-33466 Orthanc Explorer осалдығы

KZ-CERT компьютерлік инциденттерге ұлттық әрекет ету қызметі DICOM хаттамасы бойынша пайдалана отырып, **ҚР азаматтарының медициналық мәліметтері және дербес деректері қамтылған** желілерде медициналық бейнелерді сақтауға, алуға және жіберуге арналған сервистердің IP-мекенжайларын анықтады. Orthanc Explorer — бұл Orthanc серверін, DICOM хаттамасы бойынша пайдалана отырып, желілерде **медициналық** бейнелерді

сақтау, алу және жіберу үшін пайдаланылатын DICOM еркін және ашық серверін басқаруға арналған веб-интерфейс. Пайдаланушылар Orthanc Explorer көмегімен пациенттердің мәліметтерін, зерттеулер мен бейнелерді көре, жүктей және жоя алады, сондай-ақ сервисті басқарудың басқа да операцияларын жүзеге асыра алады.

1.12.0 нұсқасына дейінгі Orthanc-те CVSS шәкілі бойынша 10-нан 8.8 бағасына ие CVE-2023-33466 сәйкестендіргіші бар аса маңызды осалдық айқындалды. Бұл осалдық API Orthanc-ға қолжетімділігі бар авторланған зиянкеске қоймадағы еркін файлдарды қайта жазуға мүмкіндік беруі ықтимал. Өрістетудің белгілі сценарийлерінде осы да зиянкеске жүйенің конфигурациясын қайта жазуға мүмкіндік беріп, бұл кодты қашықтан орындауды *(RCE)* жүзеге асыру үшін пайдаланылуы мүмкін.

Бұдан басқа, анықталған Orthanc жүйелері өрістетілген IP-мекенжайларының ешқандай авторлану нысандары жоқ. Бұл жүйелерде CVE-2023-33466 осалдығы ықтимал түрде күрделі қатер төндіреді. Авторланудың болмауы осы жүйелерді сыртқы шабуылдарға толығымен ашық етеді және зиянкестер файлды қайта жазу мен еркін кодты орындау үшін осалдықты оңай пайдалана алады.

Мақсатты шабуылдар

«STS» командасы біз STA-2201 ретінде қадағалау жүргізетін хакерлік топтың белсенділігін бақылауды жалғастыруда. Аталған топ жария, бірақ белгілі бола қоймаған эксплойттарды пайдаланады, сондай-ақ түбегейлі жаңа функционал жасап, әртүрлі көздерден алынған кодтың фрагменттерін өзара құрастырады. Бұдан басқа, GitHub репозиторийлерден қосып, шамалы өзгерістер енгізіп, шабуыл жасаушылар ашық бастапқы коды бар құралдарды қайта компиляциялау жүргізеді.

Жүйеде бекітілу және инфрақұрылым бойынша бүйірлік қозғалу бөлігінде зиянкестер қашықтан әкімшілендіру құралдарының мүмкіндіктерін пайдаланады, сондай-ақ Living off the Land (LotL) техникасын қолданады. Шабуылдаушылар SYSTEM артықшылықтарын қолға түсіруге тырысады, бұл оларға жоғары артықшылықтарымен инфрақұрылым элементтерімен, соның ішінде домен контроллерімен және Exchange пошта сервисімен өзара іс-қимыл жасауға мүмкіндік туғызады.

Microsoft Exchange пайдалану кезінде зиянкестер, егер олар бұған дейін «web.config» конфигурациялау файлынан «validationKey», «decryptionKey» параметрлерінің мәндерін алса, оларға еркін кодты іске қосуға мүмкіндік беретін ViewState механизмін пайдаланады. Exchange серверінде бекітілгеннен кейін зиянкестер оларға командалық жолдың командаларын орындау мен файлдарды дискіде сақтауға мүмкіндік беретін басқа зиянды кодты жүктейді.

Сонан соң, қойылған мақсаттарға байланысты, зиянкестер келесі зиянды бағдарламалардың біреуін немесе бірнешеуін орнатады:

1. Файлдық тыңшы, пернетақта тыңшысы функционалы бар, сондай-ақ командаларды орындау мен қосымша зиянды модульдерді жүктеу мүмкіндігіне ие PlugX/ShadowPad көп функциялы бэкдор

2. PowerShell/WMI командаларын орындау, файлдық тыңшы, желіде алдын ала барлау, сондай-ақ DCSYNC түріндегі шабуылды жасау функционалына ие файлсыз бэкдор

3. Арнайы қалыптастырылған электрондық хаттар арқылы басқарылатын және командаларды орындау мен зиянды модульдерді іске қосу мүмкіндігіне ие Transport Agent'а түріндегі бэкдорды орнату

Бұдан басқа, «STS» командасы байланыс операторына жасалып, оның барысында STA-2201 хакерлік топтың мүшелері инфрақұрылымды бақылауда ұстап қалуға арналған қарапайым, бірақ өте алуан түрлі құралдарды пайдаланған кибершабуылды анықтады.

Зиянкестер Microsoft Exchange серверін тестілеу режиміне ауыстырған кездегі техника үлкен қызығушылық тудырады, бұл оларға зиянды драйверді жарамсыз цифрлық қолтаңбамен іске қосуға мүмкіндік берген. Бұдан басқа, зиянкестер екінші сатыдағы файлы «scansts.dll» деген атауға ие PlugX бэкдорын пайдаланған. Зиянкестер «STS» командасы жүргізетін жұмыстарға ұқсастыруға тырысқаны әбден мүмкін.

Ақпараттық қауіпсіздіктің неғұрлым жоғары деңгейін қамтамасыз ету үшін мыналарды қамтитын кешенді әдісті қолдану ұсынылады:

1 Ұйымдастырушылық қорғау шаралары

Заңнамалық, әкімшілік және ұйымдастырушылық-техникалық қорғау шараларын қамтиды.

ҚР ұйымдары олардың талаптарын орындауға тиіс «Ақпараттандыру туралы» Қазақстан Республикасының Заңы, «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы, Қазақстан Республикасы Ұлттық Банкінің нормативтік актілері, «Қазақстан Республикасындағы банктер және банк қызметі туралы» 1995 жылғы 31 тамыздағы № 2444 Қазақстан Республикасының Заңы, «Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін бекіту туралы» Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы № 48 қаулысы және т.б. заңнамалық қорғау шараларының негізгі көздері болып табылады.

Әкімшілік шараларға ұйымның ақпаратты қорғау бойынша іс-қимылдарды жалпы үйлестіруге бағытталған ішкі құжаттары жатады. Мұндай құжаттарға ақпараттық қауіпсіздік жөніндегі техникалық құжаттама, тәуекелдерді басқару, ТЖ кезінде іс-әрекеттерді жоспралау, лауазымдық нұсқаулықтар және т.б. жатады.

Ұйымдастырушылық-техникалық шаралар аумаққа кіруді бақылауға, АЖ мен мүлікті зақымдаулардан физикалық қорғауға, сондай-ақ АЖ жұмысқа қабілеттігін қолдап отыруға бағытталған.

Ақпараттық қауіпсіздік жөніндегі техникалық құжаттаманы үнемі өзектілендіріп отырыңыз, тәуекелдерге талдау жүргізіңіз, қызметкерлерді кибергигиена бойынша оқытуды өткізіңіз. Ақпараттандыру объектісіне, күзет және өрт сигнализация жүйелеріне, ауаны үздіксіз баптау, электрмен жабдықтау жүйелеріне қол жеткізудің қажет деңгейін қамтамасыз етіңіз. АЖ компоненттерін резервтік көшіруді орындаңыз *(сақтау, өңдеу, беру)*.

2 Бағдарламалық-техникалық қорғау құралдары

Бағдарламалық, бағдарламалық-аппараттық және аппараттық қорғау құралдарын қамтиды.

Оларға XDR жүйелері (вирусқа қарсы бағдарлама+EDR+SIEM+SPAN), желіаралық экрандар, DLP жүйелері жатады. Ұйым желісіндегі барлық жұмыс станциялары мен серверлерге сенімді вирусқа қарсы бағдарламалық қамтылымды орнатыңыз және зиянды бағдарламаларды анықтау мен жою үшін оны үнемі жаңартыңыз, желіаралық экрандарда қолжетімділіктерді «рұқсат етілгеннен басқа барлығына тыйым салынған» әдісі бойынша баптаңыз, DLP жүйесін баптауды жүргізіп, деректердің таралу арналарын бақылаңыз.

Желі ішінде шабуылдардан қорғауды қоса, мақсатты шабуылдарды анықтау және болдырмау үшін мамандандырылған шешімдерді ендіруді қарастыру қажет. Сонымен қатар, оқиғаларды нақты уақытта талдау мен мониторингтеу, қалыптан тыс іс-қимылды айқындау және ақпараттық қауіпсіздік инциденттеріне әрекет ету үшін SIEM/SOAR енгізу керек.

3 Криптографиялық қорғау әдістері

Маңызды ақпаратты мамандандырылған БҚ көмегімен шифрланған түрінде сақтауды, беруді қамтамасыз етіңіз. Құпия кілттерді сенімді жерде сақтаңыз.

4 Техникалық қорғау құралдары

Техникалық барлау құралдарын пайдалана отырып, ақпаратты рұқсатсыз қол жеткізуден қорғауға арналған.
Ақпараттың конфиденциалдық деңгейіне сәйкес арнайы құралдарды пайдалана отырып, ақпараттың қорғалуын қамтамасыз етіңіз.

Жасанды интеллект (ЖИ) және машиналық оқыту

2024 жылы ЖИ дамуы айтарлықтай ілгерілеп, көптеген мүмкіндіктер мен сын-қатерлер туғызатыны күтіледі. Сонымен қатар, ЖС өзін үлкен сәттілікпен әлдеқашан танытып жатқан басты салалардың бірі медицина екенін атап көрсету қажет. ЖИ негізіндегі дәрігерлік бағдарламалар ауруларды жоғары дәлдікпен диагностикалауға және емдеудің оңтайлы әдістерін ұсынуға қабілетті. Бұл әртүрлі ауруларды дер кезінде анықтауға және олармен күресуге мүмкіндік береді, сондай-ақ медицина мекемелері жұмысының тиімділігін арттырады.

ЖИ-ден ауқымды өзгерістер күтілетін бағы бір бағыт экономиканың түрлі салаларындағы процестерді автоматтандыру болып табылады. ЖИ көмегімен өндірісті басқарудың ақылды жүйелерін құру, логистикалық процестерді оңтайландыру, бақылау сапасын жақсарту және көптеген басқа мүмкіндіктер болады.

Бұл кәсіпорындар жұмысының тиімділігін едәуір арттырып, шығыстарды азайтуға жол береді. Ақпараттық қауіпсіздікте жасанды интеллект пен машиналық оқытуды пайдалану көптеген артықшылықтар әкелуде.

Бұл технологиялар адам мүмкіндіктерін жақсарту, деректердің ауқымды көлемдеріне тез талдау жүргізу, күрделі заңдылықтар мен өзара байланыстарды табу, сондай-ақ ақпараттық қауіпсіздіктің жаңа қатерлеріне тиімді бейімделу қабілеттеріне ие.

Бұдан басқа, жасанды интеллект пен машиналық оқыту мамандарды күрделі және стратегиялық міндеттерге тереңірек назар аудару үшін босатып, кертартпалыққа негізделген міндеттерді автоматтандыра алады. Алайда, жоғары сапалы және алуан түрлі деректердің, ЖИ модельдерінің анықтығы және түсіну қажеттілігі, зиянкестер тарапынан ықтимал шабуылдар, сондай-ақ конфиденциалдық пен теріс түсінікке қатысты әдеп мәселелері сияқты белгілі қиындықтар орын алады.

Сондай-ақ, ЖИ пайдаланудың әдепке негізделген спектісі басты проблемалардың бірі болып табылады. Деректердің құпиялылығы, қауіпсіздігі мен ЖИ қабылдайтын шешімдер үшін жауаптылық туралы мәселелер туындайды. Сондықтан ЖИ-ді қауіпсіз және әдепке негізделе отырып, пайдалануды қамтамасыз ету үшін тиісті құқықтық және реттеуші механизмдерді әзірлеу маңызды.

Алдағы уақытта машиналық оқытумен қолдау көрсетілетін жасанды интеллекттің ақпараттық қауіпсіздігі «маңызды» құралға айналады. Көптеген басқа салалардағыдай, адамдардың өзара іс-қимылы қауіпсіздікті қамтамасыз етуде бұрыннан бері басты және ажырамас рөл атқарып келеді. Қазіргі сәтте ақпараттық қауіпсіздіктің тиімділігі айтарлықтай дәрежеде адамның қатысуына байланысты екеніне қарамастан, адамдардың мүмкіндіктерімен салыстырғанда, технологиялар белгілі бір міндеттерді неғұрлым сәтті меңгеруде.

Генеративті ЖИ-ді қарсылас тараптардың екеуі де пайдалануда

Жасанды интеллекттің (ЖИ) жеделдетілген қарқынмен дамуына байланысты, ЖИ басқаратын күрделенген және интеллектуалды шабуылдардың таралуына қатысты алаңдаушылық жоғарылап келеді.

Қатерлер спектрі әлеуметтік инженерияның «дипфейк» әрекеттерін, сондай-ақ әртүрлі қорғау құралдарымен айқындауды ескермеуге мүмкіндік беретін интеллектуалды іс-әрекеттерді көрсететін автоматтандырылған зиянды бағдарламаларды қамтиды.

Сонымен бірге бұл технология ауытқуларды нақты уақытта айқындауды пайдалану, интеллектуалды аутентификация мен ақпараттық қауіпсіздік инциденттеріне автоматты әрекет ету механизмдері есебінен ықтимал тәуекелдерді анықтауға, оларды болдырмауға немесе барынша төмендетуге көмектеседі.

Зиянды бопсалаушы бағдарламалар

Зиянды бопсалаушы бағдарламалар жиі жағдайларда ақпараттық қауіпсіздікке төнетін ең белгілі және жойқын қатер ретінде қабылданады. Бұл қатер маңызды болып қалуда және келесі жылы да оның маңыздылығы сақталатыны күтілуде.

Киберқылмыскерлер барынша күрделенген және айлалы әдістерді, соның ішінде жасанды интеллектке негізделген бопсалаушы бағдарламаларды ендіруді қолданатын болады. Бұл бағдарламалар қауіпсіздік ортасындағы өзгерістерге бейімделуге және дәстүрлі қорғау шараларын ескермеуге қабілетті болады.
Зиянкестер бірінші конфиденциалды деректерді ұрлап, кейін оларды шифрлайтын кездегі қос бопсалау тактикасы әлеуетті құрбандарға қосымша қысым жасап және оларды ақы төлеуге мәжібүрлеп, одан әрі дамитынын атап көрсету қажет.

Көрсетілетін қызмет ретіндегі киберқылмыс

Киберқылмыстың көрсетілетін қызмет ретінде дамуы *(Cybercrime-as-a-Service)* типті тәжирибесі жоқ зиянкестер де шабуылды жүзеге асыру үшін ілгерінді құралдарға қолжетімділік ала алатынын білдіреді. Бұл зиянды БҚ-ны жалға алудан бастап дайын кибершабуылдарды қара базарда сатып алуға дейін бәрін қамтиды. Нәтижесінде киберқылмысқа кіру кедергісі төмендеп, бұл шабуылдар саны мен әртүрлілігінің артуына әкелуі мүмкін. Ұйымдар қатерлердің неғұрлым кең спектріне дайын болып, олардың кешенді қорғау құралдары болу керек.

IoT құрылғыларына кибершабуылдар

Заттар интернеті *(IoT)* қазіргі уақыттағы ең жан-жақты технологиялардың бірі болып табылады. Интернет-желінің кеңеюі, қолайлы ақылды құралдардың өткізу қабілетінің ұлғаюы мен олардың алуан түрлі болуы нәтижесінде IoT барлық әлем бойынша танымалдығының ерекше жылдам артуын бастан кешуде.

2024 жылы IoT танымалдығының өсу қарқыны өскелең болып қалатынын болжамданады. Заттар интернеті *(IoT)* күнделікті өмірді, сонымен қатар ұйымдардың операциялық қызметін айтарлықтай жеңілдететін өте ынғайлы және пайдалы технологиялар кешенін білдіреді. Дегенмен, өкінішке орай, мінсіз технологиялар болмайды. IoT құрылғыларының асқан танымалдығы мен ынғайлығына қарамастан, оларда қиын анықталатын осалдықтардың болуы және стандарттарудың жоқтығы сияқты өз кемшіліктері бар. IoT құрылғысы желіге кірудің ықтимал осал нүктесі болып табылады.

Сол себепті бұл желілер ауқымды бұзулардағы, әсіресе шабуыл нақты ұйымға бағытталған кезде, бірінші кезең болуы мүмкін.

Заттар интернетінің негізгі элементтері зиянкестер тарапынан шабуылдарға жеткілікті бейімді. IoT жүйесі енгізілетін қоршаған ортаның көлемі мен түріне байланыссыз, оны енгізуді жақсарту, деректерді қорғау және кибершабуылдарға жол бермеу үшін қауіпсіздік жоспарлау кезеңінде қарастырылуы тиіс.

Бұлтты қауіпсіздік

Бұлтты технологияларға көшу қарқын алуды жалғастыруып, ұйымдардан бұлтты қауіпсіздікке ерекше назар аударуды талап етеді. Бұл жағдай бұлтта сақталатын деректерді қорғауды, API қауіпсіздігін қамтамасыз етуді, сондай-ақ бұлтты ортадағы қолжетімділік пен сәйкестендіруді басқаруды қамтиды. Сонымен қатар, дұрыс бапталмаған бұлтты ресурстар шабуылдардың мақсатына жиі аналатындықтан, бұлтты сервистер конфигурациясының қауіпсіздігі маңызды аспект болып табылады.

Аса маңызды инфрақұрылымды қорғау

Энергетикалық желілер, көлік жүйелері және қаржы мекемелері сияқты аса маңызды инфрақұрылымдарға кибершабуылдар ұлттық қауіпсіздік пен экономикаға елеулі қатер төндіреді. 2024 жылы осы жүйелерді қорғау бойынша шаралардың күшейтілуі күтіледі.

Бұл шабуылдарды анықтау мен болдырмауға арналған мамандандырылған шешімдерді дамытуды, мемлекеттік және жекеменшік ұйымдар арасында ынтымақтастықты нығайтуды, сондай-ақ маңызды салалардағы инциденттерге дайын болу деңгейін арттыруды қамтуы мүмкін.

Ішкі қатерлерге қарсы іс-қимыл

Ішкі қатерлер – айқындау үшін ең күрделі тәуекелдер түрлерінің бірі. Олар қызметкерлердің қасақана іс-әрекеттерін ғана емес, деректердің таралуына немесе қауіпсіздіктің басқа да проблемаларына әкелетін кездейсоқ қателерді де қамтуы мүмкін. 2024 жылы қызметкерлердің іс-қимылдарын технологиялық бақылау мен мониторингтеуден басқа, ықтимал қатерлер және оларды болдырмау әдістері туралы хабардарлықты арттыру үшін персоналды тұрақты оқытуды жүргізу маңызды болады.

Фишинг

Адам психологиясымен айлалы әрекеттер жасай алу қабілетіне байланысты, фишингтік шабуылдар мен әлеуметтік инженерия шабылдары тиімді болып қалуда. Фишингтік шабуылдар пайдаланушыларды алдау мақсатында электрондық хаттарды немесе веб-парақшаларды пайдалануды қамтиды.

Кейінгі он екі ішінде аталған шабуылдар неғұрлым күрделі, мақсатты және сенімдірек болатыны күтілуде. Зиянкестер өздерін сенімді тұлғалар ретінде көрсету немесе бейне/аудио контентпен айлалар жасау үшін жанжақты ұқсату технологиясын қолдануы мүмкін, бұл түпнұсқалы контентті жасандыдан ажыратуды одан әрі қиындатады.
Қызметкерлердің хабардарлығы мен оларды ақпараттық қауіпсіздік негіздеріне оқыту фишинг қатерімен күресуде қолдануға болатын маңызды тактика болып табылады.

Кадрларды оқыту және даярлау

Киберқауіпсіздік саласында білікті мамандардың жеткіліксіздігі ұйымдардың басым бөлігі үшін проблема болып қалуда. Осы салада даярланған кадрларға сұраныс артатыны күтіледі. Ұйымдарға ақпараттық қауіпсіздік қатерлеріне тиімді әрекет етуге даярлау үшін өз қызметкерлерін оқыту мен дамытуды инвестициялау қажет. Бұл мамандандырылған курстарды, воркшоптарды, кибершабуылдарды ұқсастыруларға қатысуды және ақпараттық қауіпсіздік саласындағы хабардарлықты арттыру бойынша тұрақты тренингтерді қамтуы мүмкін.

Бұдан басқа, мамандарға өскелең сұранысты қанағаттандыру үшін университеттер мен білім беру мекемелері өздерінің ақпараттық қауіпсіздік бойынша бағдарламаларын кеңейуі және тереңдетуі мүмкін.

2024 жылы киберқауіпсіздік саласында орын алатын үрдістер ұйымдар жаңа және күшейіп келетін бірқатар қатерлерге тап болатынын көрсетеді. Бұл технологиялық инновацияларды, персоналды оқытуды, заңнаманы сақтау мен халықаралық ынтымақтастықты қамтитын кешенді тәсілді талап етеді. Білім мен дағдыларды үнемі жаңарту, сондай-ақ өзгермелі жағдайларға бейімделу ақпараттық қауіпсіздік қатерлерінен ойдағыдай қорғалудың басты факторы болады.

Қазақстанда соңғы жылы орын алған ақпараттық қауіпсіздік саласындағы инциденттер тек ағымдағы жағдайды бағалауға емес, біздің цифрлық кеңістіктеріміздің қауіпсіздігін жақсарту үшін күш-жігерді шоғырлау қажет салаларды айқындауға да бізге мүмкіндік береді. Осы оқиғалардан алған тәжірибе алдағы уақытта АҚ қатерлерінен қорғалудың тиімдірек стратегияларын дамыту үшін бағалы ресурстар болып табылады.

Соңғы оқиғаларға талдау жүргізіп, біз күрделілік пен алдаудың жаңа биіктіктеріне ұмтылып, киберқылмыскерлер жеке деректерге шабуылдар жасаудан бастап корпоративтік желілерге шабуылдауға дейін өз әдістері мен тактикаларын әлі де дамытып келетінін көріп отырмыз. Әрбір инцидент қауіпсіздік шараларымызды нығайту және АҚ қатерлеріне қарсы тұру дағдыларын жетілдірудің маңыздылығы туралы ескертуге айналады.
Алайда, сын-қ
атерлермен бірге бірлескен күш-жігер, лайықты білім және озық технологияларды енгізу арқылы ғана біз киберқылмыскерлерге қарсы қорғалу шегін күшейте алатынымызды түсінеміз. Ақпараттық қауіпсіздіктің тиімді стратегиялары үнемі назарды, оқытуды және қоғамдастықтың, бизнес пен мемлекеттің белсенді өзара іс-қимылын талап етеді. Бірлескен күш-жігер ғана біздің цифрлық болашағымызды барынша қауіпсіз әрі тұрақты ете алады.

Келесі жыл Қазақстанды киберқауіпсіздікті қамтамасыз етудегі жаңа жетістіктер мен бірлескен табыстар кезеңге айналатынына сенім артамыз. Біздің кибердайджестке назар аударғандарыңызға алғыс айтып, сіздерді келесі баслымда күтеміз.

Ізгі ниетпен, «STS» командасы

Ақпарат көздері және түсіндірмелер

www.tadviser.ru
технологияларды және өнім берушілерді таңдау порталы.

www.ixbt.com
Компьютерлік технологиялар туралы ресей ақпараттық-талдау интернет-басылымы.

www.sentinelone.com
Маунтин-Вью-де (Mountain View), Калифорния штаты *(California)*, орналасқан киберқауіпсіздік саласындағы америка стартапы.

www.anti-malware.ru
Ресей тәуелсіз ақпараттық-талдау орталығы, ақпараттық қауіпсіздікті қамтамасыз ету және зиянды бағдарламалық қамтылымға қарсы іс-қимыл мәселелеріне арналған Интернет-жоба.

www.sts.kz
«Мемлекеттік техникалық қызмет» акционерлік қоғамының ресми интернет-ресурсы.

www.cert.gov.kz
KZ-CERT Компьютерлік инциденттерге ұлттық әрекет ету қызметінің ресми интернет-ресурсы.