Internet zatlar (IoT) - häzirki zaman sanly ösüşiniň iň möhüm bölekleriniň biri bolup, dürli pudaklarda ulanylyp, adamlaryň gündelik durmuşyny we iş proseslerini ýeňilleşdirýär. Akylly öý enjamlaryndan başlap, senagat önümçiligine çenli giň gerimde ulanylýan bu tehnologiýa, maglumat alyş-çalyş arkaly has netijeli we awtomatlaşdyrylan ulgam döretmäge mümkinçilik berýär. Şeýle-de bolsa, IoT enjamlarynyň giňden ýaýramagy bilen olaryň käbir gowşaklyklary hem ýüze çykýar. Esasy meseleler howpsuzlyk, gizlinlik, standartlaşdyrma, programma üpjünçiligi we energiýa sarp ediş bilen baglanyşyklydyr. IoT ulgamyndaky bu ýetmezçilikler, enjamlaryň durnuklylygyny we ygtybarlylygyny pese düşürip, , funksional we dolandyryş taýdan dürli kynçylyklara sebäp bolup, IoT ulgamynyň çäklerini hem kesgitleýär. Şu ýerde IoT enjamlarynyň we ulgamlarynyň esasy gowşaklyklary barada giňişleýin maglumat berler.

### ****IoT Tehnologiýasynyň Esasy Gowşaklyklary:****

### ****1. Standartlaşdyrmanyň we düzgünleşdirmegiň ýetmezçiligi****

IoT enjamlary dürli kompaniýalar tarapyndan öndürilýär we olaryň hemmesi biri-biri bilen utgaşykly işlemeýär. Bu, ulgamlaryň bilelikde işlemegini kynlaşdyryp, enjamlaryň arasynda baglanyşyk kemçiligini döredýär. Standartlaryň bolmazlygy, enjamlaryň dürli programmalary we protokollary ulanmagy sebäpli, olar bilen işleşmekde kynçylyk döreder.

### ****2. Ulgamyň durnuklylygy we çydamlylygy****

IoT enjamlary köplenç internet arkaly işleýändigi sebäpli, internet baglanyşygynyň kesilmegi ýa-da gowşak bolmagy ulgamyň işine uly täsir ýetirýär. Şeýle hem, köp IoT enjamlary uzak möhletleýin ulanylmaga niýetlenmedik bolany üçin, olaryň tiz könelmegi ýa-da näsazlyk ýüze çykmagy mümkin.

### ****3. Maglumatlaryň takyklygyny we hilini dolandyrmak****

IoT enjamlary dürli çeşmelerden maglumat alýar, emma bu maglumatlaryň dogrulygyny we hilini dolandyrmak kyn bolup biler. Sensorlardaky nädogry ölçegler ýa-da programma üpjünçiligindäki ýalňyşlyklar netijesinde, ulanyjylara nädogry maglumat ýetirilip biler. Bu bolsa, IoT ulgamynyň netijeliligini pese düşürýär.

### ****4. Energiýa sarp edilişi we batareýa meselesi****

Köp IoT enjamlary batareýa bilen işleýär we olaryň energiýa sarp edişi ýokary bolup biler. Käbir enjamlaryň çalt zarýadynyň gutarmagy, olaryň dowamly işlemegini kynlaşdyrýar. Bu bolsa, uzak möhletleýin ulanylyşda tehniki hyzmatyň we batareýa çalyşmagyň zerurdygyny görkezýär.

### ****5. Enjamlaryň programmalaşdyryş we täzelenme (update) meseleleri****

IoT enjamlarynyň köpüsi täze täzelenmeleri seýrek ýa-da haýal alýar. Käbir enjamlaryň programma üpjünçiliginiň köne bolmagy, olaryň döwrebaplaşdyrylmagyny kynlaşdyrýar. Täzelenmeler arkaly enjamyň işleýşi gowulaşsa-da, käbir ýagdaýlarda ol ulgam bilen gabat gelmän, täze näsazlyklaryň ýüze çykmagyna sebäp bolup biler.

### ****6. Enjamlar arasynda utgaşmazlyk we çylşyrymly dolandyryş****

IoT ulgamlary köplenç biri-biri bilen sazlaşykly işlemeýär. Bir kompaniýanyň enjamy beýleki kompaniýanyň platformasy bilen utgaşyp bilmän, tehniki kynçylyklara sebäp bolup biler. Mundan başga-da, IoT ulgamlarynyň dolandyryş panelleri we programmalary çylşyrymly bolup, ulanyjylar üçin düşnüksiz bolup biler.

**7. Maglumat alyş-çalyş meseleleri**

IoT enjamlary uly göwrümli maglumatlary ýygnap we saklap bilýär. Emma maglumatlary çalt we ygtybarly alyş-çalyş etmek üçin zerur bolan infrastruktura kähalatlarda ýeterlik bolmaýar. Bu bolsa, maglumatlaryň haýal işlemegine ýa-da ýitmegine sebäp bolup biler.

IoT ulgamlary häzirki zaman tehnologiýasynyň möhüm bölegi bolsa-da, olaryň gowşaklyklary bu tehnologiýanyň gerimini we netijeliligini çäklendirýär. Ulgamlaryň sazlaşygy, durnuklylygy, maglumat hilini dolandyrmak we energiýa tygşytlylygy bilen baglanyşykly meseleler IoT tehnologiýasynyň has kämilleşdirilmelidigini görkezýär. Bu gowşaklyklaryň üstünde işlemek bilen, IoT ulgamlarynyň has ygtybarly we täsirli bolmagy gazanylyp bilner.

**IoT enjamlaryna abanýan esasy howplar**

Olaryň tiz we giňden ulanmagy bilen baglylykda, kiberhüjümler, maglumat ogurlamak, enjamlaryň näsazlyga uçramagy we gizlinlik meseleleri ýaly köpugurly täsirleri döredýär. Aşakda IoT enjamlaryna abanýan esasy howplary sanap geçýäris:

**1. Kiberhüjümler (Hacking)**

* **Düzgünleriň gowşaklygy**: IoT enjamlarynyň köpüsi gowşak parollar ýa-da başga-da goragsyz gorag çäreleri bilen işleýär. Bu, hakerlere enjamlar we ulgamlara girmek üçin mümkinçilik döredýär.
* **Botnetler**: IoT enjamlarynyň köpüsi internet bilen baglanyşýar, şonuň üçin olara girip, botnetler döretmek mümkin. Bu, dürli noýtralardan ýokary dolandyryş üçin ulanylýar, ýagny, IoT enjamlary ulanmak arkaly uly "DDoS" (Distributed Denial-of-Service) hüjümlerini amala aşyrmak mümkin.

**2. Maglumat ogurlamak**

* **Şahsy maglumatlaryň ogurlanmagy**: IoT enjamlary adamlaryň şahsy maglumatlaryny, hereketlerini, saglyk ýagdaýyny we beýleki möhüm maglumatlaryny ýygnap biler. Bu maglumatlar hakerler tarapyndan ogurlanyp, satylyp ýa-da başga maksatlar üçin ulanylyp bilner.
* **Sensorlar arkaly gizlin maglumat almak**: IoT sensorlary ulanyjylaryň fiziki ýagdaýy, ýerleşýän ýeri, hereketi barada maglumat toplap biler. Bu maglumatlaryň ýitmegi ýa-da ogurlanmagy ulanyjynyň gizlinligine we şahsyýetiňe zyýan ýetirip biler.

**3. Fiziki taýdan hatardan çykmak**

* **Enjamyň fiziki ogurlanmagy**: IoT enjamlary köp wagty bilen akylly enjamlar we sensoral bolup, olary fiziki taýdan ogurlamak ýa-da ýeňil we çalt ýerlemek mümkin. Bu ýagdaýda, enjamy yzarlamak we onuň daşyndan maglumat almak başarnykly bolup biler.
* **Enjamlaryň täzelenme zerurlygy**: IoT enjamlarynyň köpüsi täzelenmeleri ýa-da gowşak programmalary ulanýan bolsa, olara goşmaça fiziki ýa-da onlaýn kiberhüjümler bolup biler.

**4. Maglumatlaryň howpsuzlygy**

* **Gizlinlik meselesi**: IoT enjamlary ulanyjylaryň dürli şahsy maglumatlaryny toplamak bilen bagly gizlinlik meselesini döredýär. Bu ýagdaý ulanyjylara rahatlyk bermän, olaryň gizlinligine we hukugyna zyýan ýetirip biler.

**6. Awtomatlaşdyrylan şahsy kararlar**

* **Awtomatiki kararlar we düzgünler**: IoT enjamlary awtomatiki dolandyryşlar we kararlar berip biler. Eger-de bu enjamlar nädogry maglumatlary işläp, ýalňyş kararlar kabul etse, bu ýagdaý iş alyp barmak ýa-da şahsyýet üçin nädogry netijeler döredip biler.

### ****7. Täzelenmeler (Update) we programma täzelenmesi****

* **Täzelenme üstünlikleriniň ýoklugy**: Käbir IoT enjamlary täzelenmeleri ýa-da howpsuzlyk ýagdaýlaryny yzygiderli alyp barmaýar. Bu ýagdaý, enjamlaryň gowşak howpsuzlyga eýe bolmagyna, we kiberhüjümleriň has aňsat we täsirli bolmagyna sebäp bolup biler.

IoT tehnologiýasy durmuşy has amatly we awtomatlaşdyrylan hala getirse-de, onuň önümçiliginde we ulanylyşynda birnäçe howplar bar. Bu howplar, kiberhüjümleriň, maglumat ogurlamagyň, enjamlar arasyndaky utgaşmazlyklaryň, gizlinlik meseleleriniň we fiziki howplaryň öňüni almak üçin aýratyn üns bermegi talap edýär. Howpsuzlyk çärelerini ýokarlandyrmak we IoT ulgamlaryny has ygtybarly we goragly etmek zerur bolup biler.

### ****Shodan arkaraly IoT enjamlary tapmak we olar baradaky gowşaklyklary öwrenmek****

**Shodan** (https://shodan.io), internetdäki açyk ulgamlary we enjamlar barada maglumat berýär. Şeýlelik bilen, Shodan arkaly IoT enjamlarynyň gowşaklyklaryny tapmak we analiz etmek üçin mümkinçilikler döredilýär. Şu makalada, Shodan arkaly IoT enjamlaryny tapmak, olary analiz etmek we gowşaklyklaryny öwrenmek barada maglumat berler.

### ****1. Shodan arkaly IoT enjamlaryny tapmak****

Shodan, internetdäki dürli enjamlar we hyzmatlar hakyndaky maglumatlary ýygnamak üçin döredilen serşirleýiş (search engine) ulgamydyr. IoT enjamlarynyň tapylmagy üçin Shodan, ulanyjylara dürli açyk portlar, IP adresleri, we enjamlar barada maglumat berýär. Aşakdaky usullar, Shodan arkaly IoT enjamlaryny tapmakda kömek eder:

* **Açar Sözü (Keyword) We Taglar**  
  Shodan, belli açar sözler we taglar arkaly enjamlar barada maglumat tapar. Meselem, «webcam», «smart thermostat», «doorbell», «IP camera» we ş.m. ýaly taglar arkaly IoT enjamlary tapyp bolýar. Ulanyjylar bu açar sözlerini serşirlemek arkaly tapylan enjamlar barada maglumatlar alýarlar.
* **Port Skanirlemesi (Port Scanning)**  
  Shodan, enjamlar tarapyndan açyk bolan portlary we olaryň hyzmatlaryny tapmaga kömek edýär. IoT enjamlary, köplenç aýratyn portlardan geçýär we bu portlar ulgama girip bilmek üçin açyk bolup biler. Açar portlar arkaly enjamlar tapylyp, olaryň işleme görnüşi we howpsuzlyk ýagdaýy barada maglumat alyp bolýar.
* **X.509 Sertifikatlary**  
  Shodan, enjamlar üçin X.509 sertifikatlaryny we degişli sertifikat maglumatlaryny tapmaga kömek edýär. Bu sertifikatlar, ulanyjylara enjamyň nädip işledigini we onuň howpsuzlyk ýagdaýyny analiz etmek üçin möhüm maglumatlary berýär.

### ****2. IoT Enjamlarynyň gowşaklyklaryny öwrenmek****

Shodan arkaly bu gowşaklyklary öwrenmek, ulanyjylara enjamlar bilen baglanyşykly howplary ýüze çykarmaga kömek edýär. Aşakdaky ýagdaýlar IoT enjamlarynyň esasy gowşaklyklaryny we howplaryny görkezýär:

* **Goragsyz Parollar (Default Passwords)**  
  Köp IoT enjamlary, olara täze girýän ulanyjylar üçin umumy parollar bilen üpjün edilýär. Bu parollar köplenç üýtgedilmeýär we bu ýagdaý, enjamlara aňsatlyk bilen girilip bilinmegini üpjün edýär. Shodan, bu görnüşli enjamlar barada maglumat alýan wagtda, ulanyjylar üçin girip boljak enjamlar we olaryň parol üpjünçilikleriniň gowşakdygyny görkezýär.
* **Açyk Portlar**  
  IoT enjamlarynyň köpüsiniň portlaryň açykdygy sebäpli ulanmakda gowşaklyga duçar bolýar. Shodan, enjamlar we ulgamlaryň açyk portlaryny tapyp, bu portlaryň nädip işleýändigini görkezýär. Açyk portlar, enjamlar tarapyndan girip bilmek üçin mümkinçilik döredýär we bu kiberhüjümleriň amala aşyrylmagyna ýol açýar.
* **Täzelenme (Update)**   
  IoT enjamlarynyň käbirleri täzelenme alman, olaryň gowşak howpsuzlyk çözgütlerinden peýdalanýar. Shodan arkaly enjamlaryň täzelenme ýagdaýy we programma üpjünçiligi baradaky maglumatlar tapylyp, olaryň ýakyn wagtda täzelenmändigini ýa-da gowşak howpsuzlyk çözgütleri bilen işledilýänligi ýüze çykarylýar.
* **Şahsy Maglumatlaryň Ogurlanmagy**  
  IoT enjamlary, şahsy maglumatlary toplap, olary bulut serwerlerine iberýär. Shodan, bu enjamlar barada maglumat tapyp, şahsyýetiň gizlinligini howp astyna goýýar. Hakerler, bu görnüşli enjamlar arkaly ulanyjylaryň şahsy maglumatlaryny ogurlap bilýär.

**Brute-force hüjümleri**

Ulanyjylaryň parollaryny tapmak üçin ähli mümkin bolan kombinasiýalary synap görmäge esaslanýan tehnologiýadyr. IoT enjamlarynda bu görnüşli hüjümleri amala aşyrmak, adaty däp bolan açyk parollar ýa-da gowşak parol goragyna eýe bolan enjamlarda has uly howplar döredýär. Bu ýerde, brute-force hüjüminiň IoT enjamlaryndaky görnüşleri we onuň amala aşyrmak üçin ulanylýan usullar barada maglumat berler.

Brute-force hüjümi, diňe bir paroly tapmaga niýetlenen tehniki bir metoddyr. Bu usulda, hüjümçi ähli mümkin bolan harp, san we aýratyn simwollar kombinasiýalaryny synap görýär. Brute-force hüjümleri amala aşyrmak üçin dürli tehniki serişdeler we meýilnamalar ulanylyp bilner. Käbir iň giňden ulanylýan usullar:

#### **Hydra**

Hydra, parollar we login maglumatlaryny tapmak üçin iň meşhur we giňden ulanylýan brute-force gurallaryň biridir. Hydra, köp sanly protokollary we şifrleri synap görmek arkaly parol tapmak üçin ulanylýar. IoT enjamlarynda, web interfeyslere, FTP ýa-da SSH ýaly hyzmatlara girip bilýän parollary tapmak üçin ulanylyp bilner. Mysal üçin:

* *hydra -l admin -P /path/to/passwordlist.txt 192.168.1.100 http-get*

Bu mysalda, "admin" login we dürli parollar bilen synanyşyk edilýär.

#### **Brute-****force Skriptler**

Brute-force hüjümlerini geçirmek üçin dürli skriptler we programmalary döredip bolýar. Bu skriptler, belli bir enjamyň ýa-da ulgamyň parollaryny synap görmek üçin döredilýär. Skriptler özbaşdak programmalar bolup, olary şifrlemek we parol tapmak üçin köp sanly ýönekeý tapgyrlara böleýin.

#### **Burp Suite**

Burp Suite, web appliýasiýalaryna garşy hüjümleriň iň meşhur gurallaryndan biridir. Bu gural, HTTP/S trafigini toplamak, modifikasiýa etmek we brute-force hüjümleri etmek üçin ulanylyp bilner.

#### **Nmap (Network Mapper)**

Nmap, ulgamlar we enjamlar barada maglumat almak üçin giňden ulanylýan açyk çeşmeli guraldyr. IoT enjamlarynyň IP adreslerini tapmak we olaryň portlaryny skanirlemek üçin Nmap ulanylyp bilner. **Mysal üçin**:

* *nmap -p 22,80,443 192.168.1.100*

Bu mysalda, 22, 80 we 443 portlaryna seredilip, olaryň açykdygy anyklanýar.

**IoT enjamlaryny nyşana alypn amala aşyrylan kiberhüjümler:**

**Mirai Botneti (2016)** - IoT enjamlaryny nyşana alyp, olary botneta öwürýän zyýanly programma üpjünçiligidir. 2016-njy ýylda Mirai botneti Twitter, Netflix ýaly hyzmatlaryň elýeterliligini bozup, giň gerimli DDoS hüjümlerini amala aşyrdy.

**BrickerBot (2017)** -IoT enjamlaryny nyşana alyp, olary işlemeýän ýagdaýa getirýän zyýanly programma üpjünçiligidir. Bu hüjüm enjamlaryň firmware-ini bozup, olaryň ulanylmazlygyna sebäp bolýar.

**Hajime Botneti (2016)** - Mirai bilen meňzeş bolup, IoT enjamlaryny nyşana alýar. Emma Hajime, zyýanly hereketleriň ýerine, enjamlaryň howpsuzlygyny ýokarlandyrmaga synanyşýar.

**Persirai (2017)** - IP kameralaryny nyşana alyp, olary botneta öwürýän zyýanly programma üpjünçiligidir. Bu hüjümde 120,000-den gowrak kamera täsirlenipdir.

**Bashlite (2016)** - bir milliondan gowrak wideo kamerany we DVR-lary nyşana alyp, DDoS hüjümlerini amala aşyrdy.

**Reaper (2017)** -IoT enjamlarynyň programmalaryndaky gowşaklyklary ulanyp, olary botneta goşýan zyýanly programma üpjünçiligidir. Bu botnetiň 2 milliona golaý enjamy öz içine alandygy çaklanylýar.

Уже было несколько примеров взлома или уязвимости смарт-устройств, в том числе:

* Многие [интеллектуальные медицинские устройства,](http://www.24x7mag.com/2014/08/beware-nine-medical-device-vulnerabilities/) включая инсулиновые помпы и внутренние дефибрилляторы, используют устаревшее программное обеспечение и незашифрованные данные, что создает серьезные уязвимости с точки зрения конфиденциальности и физического благополучия пациентов.
* Миллионы [смарт-телевизоров](https://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it) подвержены риску мошенничества с кликами, бот-сетей, кражи данных и программ-вымогателей.
* [1,4 миллиона автомобилей Fiat Chrysler были отозваны](http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/) после того, как исследователи обнаружили, что с их помощью можно получить доступ к автомобилям и управлять ими удаленно через Интернет, в том числе выключить двигатель и съехать с дороги.
* Обнаружено, что [75% дверных замков с технологией Bluetooth Smart имеют уязвимости, позволяющие легко их взломать.](https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/)
* Недавно была осуществлена [​​крупнейшая в истории DDoS-атака с использованием более 150 000 взломанных смарт-устройств по всему миру, включая камеры, принтеры и холодильники.](http://thehackernews.com/2016/09/ddos-attack-iot.html)

Было обнаружено, что 70% устройств отправляют данные по сети в незашифрованном виде. [Шифрование данных необходимо](https://spin.ai/blog/what-is-the-reason-for-encrypting-data-in-a-backup/) для предотвращения их перехвата неавторизованными лицами, особенно при передаче через Интернет между облаком и устройством или мобильным приложением.

80% протестированных устройств не требовали достаточно длинных и сложных паролей.

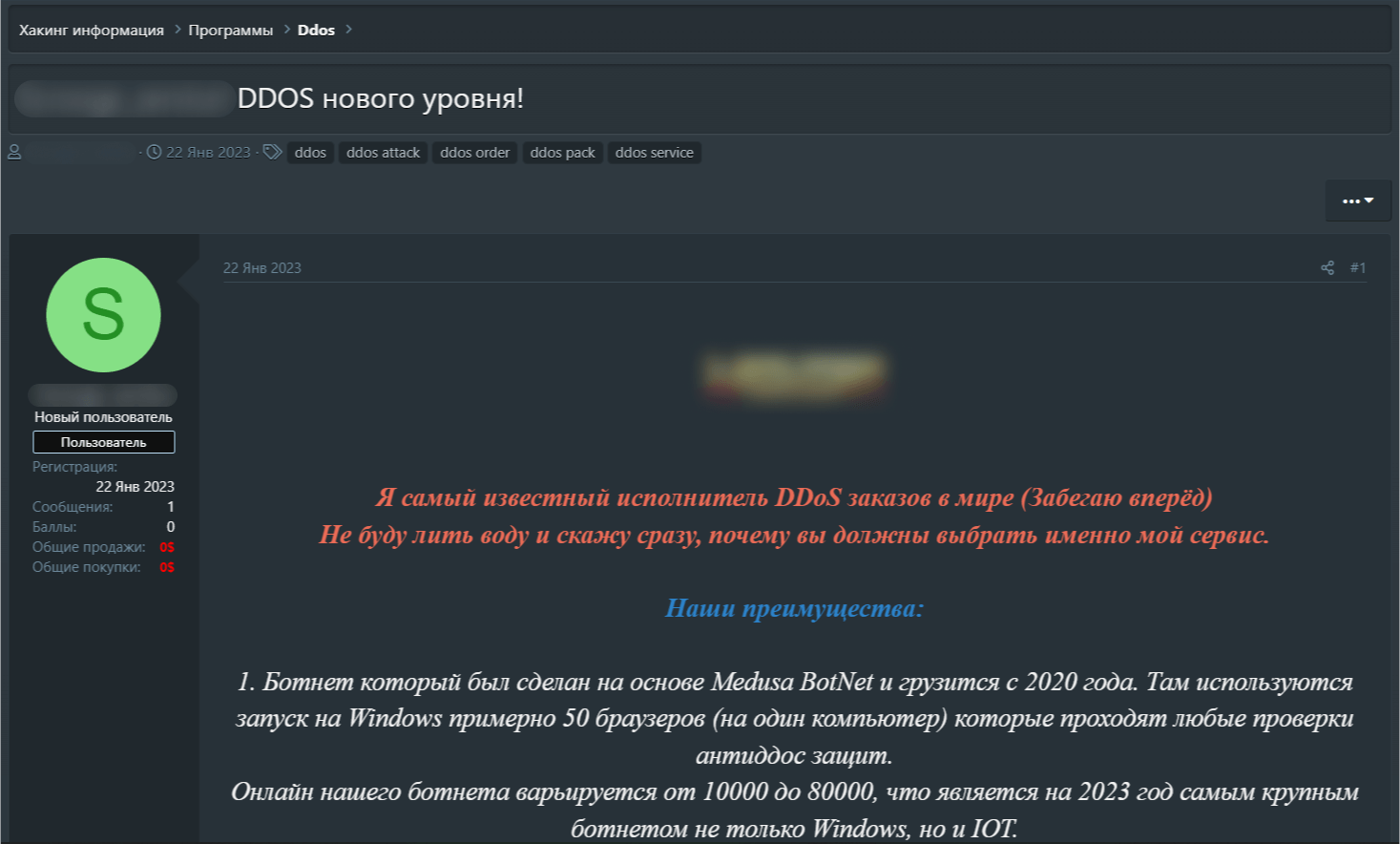
Атаки с перебором паролей довольно распространены, поскольку часто Telnet- и SSH-сервисы на IoT-устройствах защищены широко известными паролями по умолчанию, которые пользователи, как правило, не меняют. Более того, в некоторых случаях на IoT-устройствах установлены несменяемые главные пароли, заданные производителем.

К компрометации устройства также могут приводить и уязвимости работающих на нем сервисов. Самый распространенный тип уязвимостей, которые эксплуатируют злоумышленники, — внедрение вредоносных команд при выполнении запросов к веб-интерфейсу. Ущерб от таких атак может быть весьма значительным, как, например, в случае с [уязвимостью реализации протокола TR-064](https://securelist.com/new-wave-of-mirai-attacking-home-routers/76791/), который интернет-провайдеры используют для автоматической настройки устройства в локальной сети. Уязвимость позволила злоумышленникам отправлять пакеты TR-064 без аутентификации, чем они и воспользовались для распространения зловреда Mirai.

Вне зависимости от метода компрометации, атаковать IoT-устройства могут как злоумышленники со своих серверов, так и сами зловреды за счет так называемого механизма самораспространения — способности вредоносных файлов самостоятельно обнаруживать уязвимые устройства в интернете и устанавливать на них свою копию множеством различных методов. Во втором случае атака может исходить и со стороны зараженного ранее IoT-устройства.

## Услуги в даркнете: DDoS-атаки, ботнеты и уязвимости нулевого дня в IoT

Среди услуг в даркнете, связанных с IoT, в первую очередь стоит рассмотреть DDoS. Ботнеты, построенные на основе IoT-устройств и использующиеся для проведения распределенных DoS-атак, стали чаще встречаться в объявлениях на различных теневых форумах и пользоваться спросом у злоумышленников.

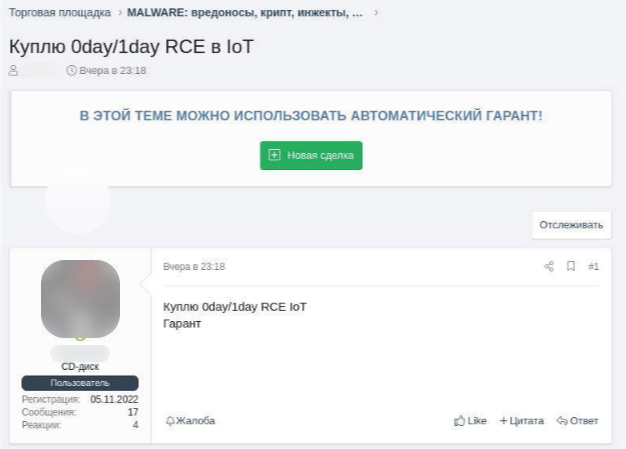
[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21041913/iot-report-2023-01.png)

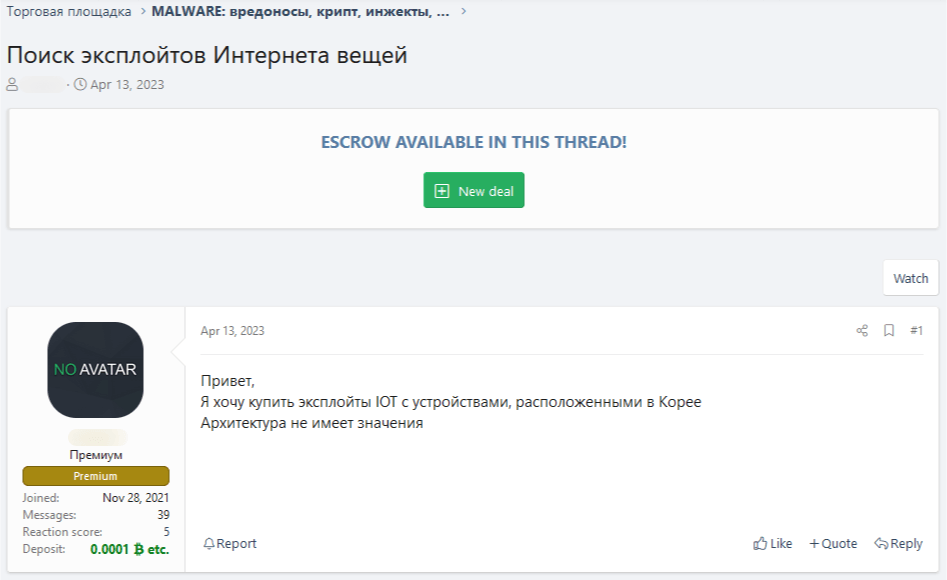
Всего за первую половину 2023 года аналитики сервиса Kaspersky Digital Footprint Intelligence обнаружили более 700 объявлений об услугах по проведению DDoS-атак на различных форумах в даркнете.

**Распределение количества публикаций, связанных с услугами по проведению DDoS-атак, по месяцам, H1 2023 (**[***скачать***](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/20183647/03-ru-iot-charts.png)**)**

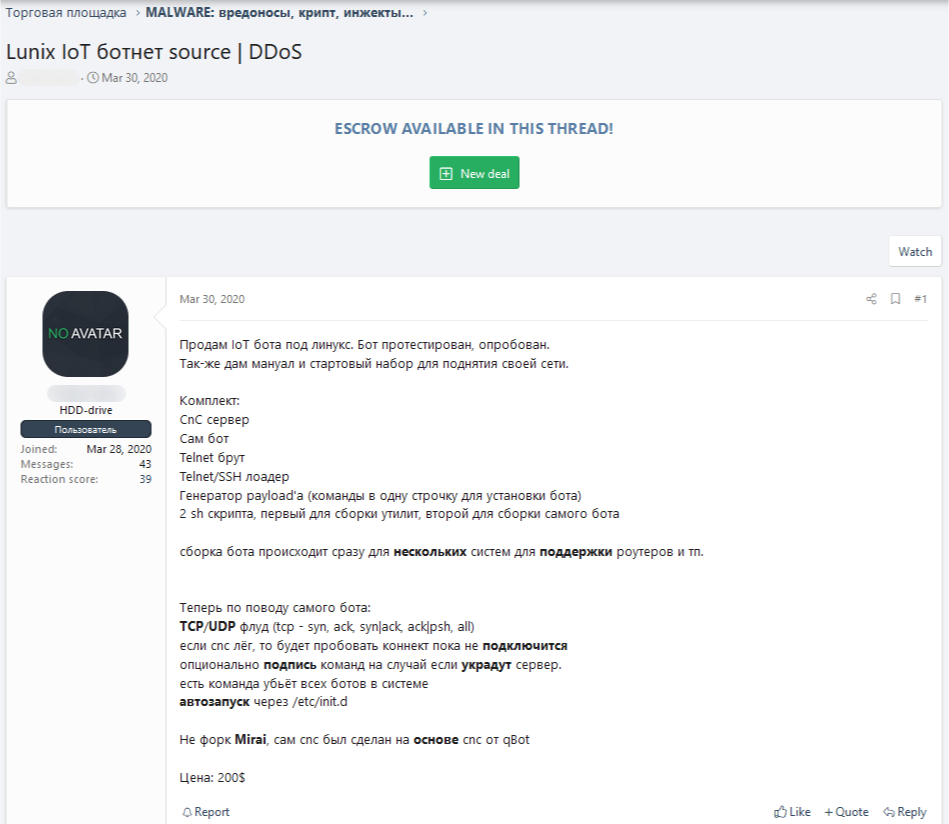
Цена такой услуги зависит от множества факторов, влияющих на сложность атаки, среди которых: наличие у жертвы защиты от DDoS, наличие капчи и JavaScript-верификации. В общей сложности стоимость атаки варьируется от $20 за сутки до $10 000 за месяц, а средняя цена для изученных объявлений составила $63,5 за сутки или $1350 за месяц.

Покупают в даркнете и услуги по взлому IoT. В частности, злоумышленники ищут эксплойты к уязвимостям нулевого дня в устройствах интернета вещей.

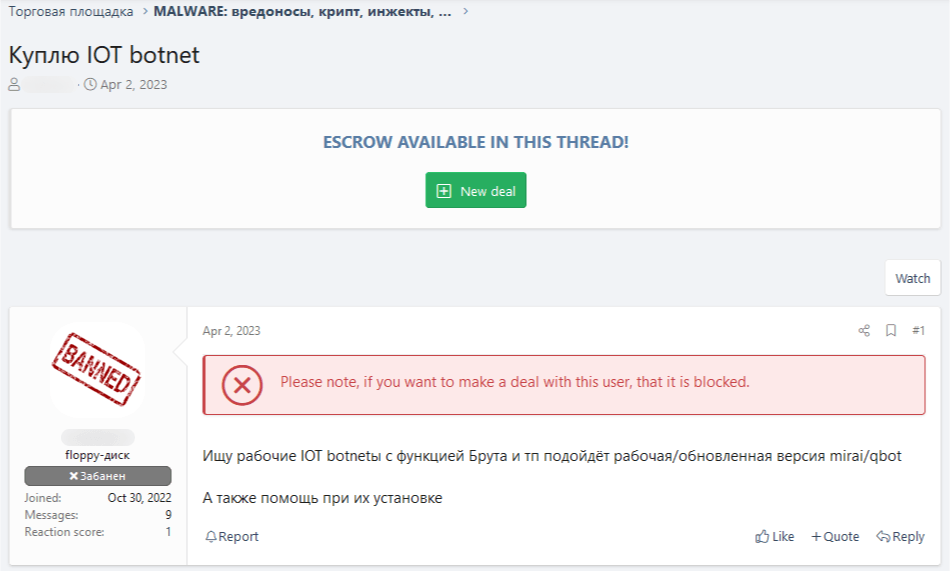
[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042000/iot-report-2023-02.png)

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042031/iot-report-2023-03.png)

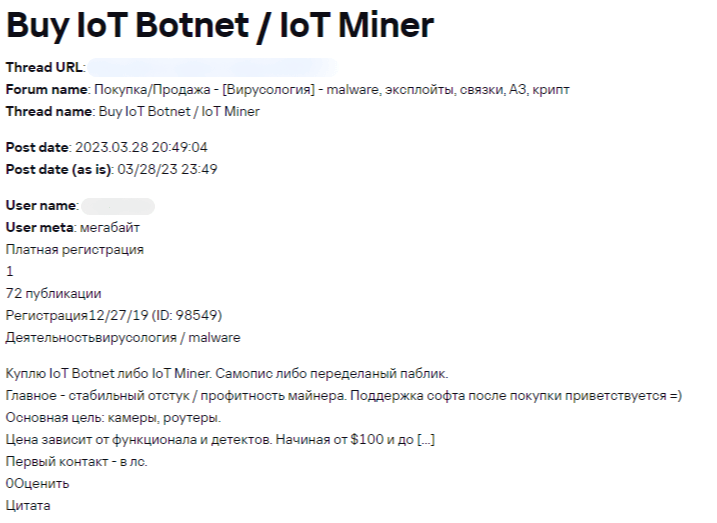
Также на теневых форумах можно найти предложения о продаже и покупке вредоносного ПО для IoT. Иногда к собственно зловреду прилагается инфраструктура и дополнительные утилиты. Так, на скриншоте ниже продавец предлагает самописный DDoS-бот с C2-сервером и ПО для загрузки зловреда через Telnet или SSH:

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042054/iot-report-2023-04.png)

Ниже скриншот объявления, в котором злоумышленник ищет не только вредоносное ПО, но и помощь в его установке.

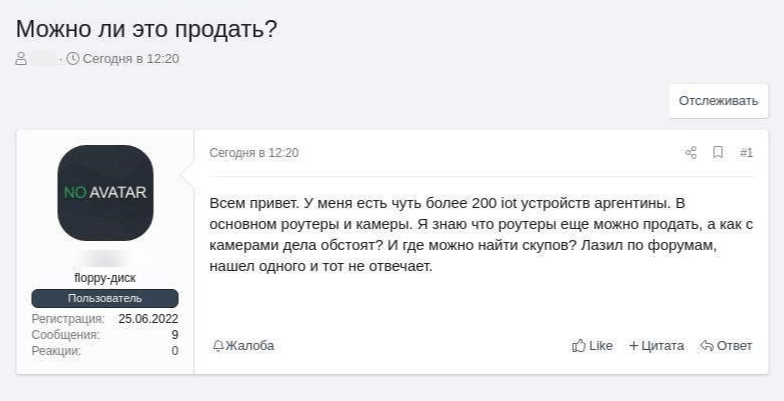
[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042121/iot-report-2023-05.png)

В некоторых случаях злоумышленники обозначают, для каких типов IoT-устройств они ищут или продают зловреды.

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042146/iot-report-2023-06.png)

*Скриншот объявления из потока Kaspersky Threat Intelligence Portal*

Иногда в даркнете продают и сети уже зараженных устройств, хотя такие объявления не очень распространены. Например, пользователь на скриншоте ниже ищет покупателя для ботнета из 200 роутеров и камер, расположенных в Аргентине.

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042447/iot-report-2023-071.png)

## Цели и виды вредоносного ПО, атакующего IoT

Злоумышленники, заражающие IoT-устройства, могут преследовать разные цели. В частности, они могут в дальнейшем использовать зараженную технику как инструмент для проведения кибератак, маскировки вредоносного трафика, использовать мощности устройства для майнинга или требовать выкуп за возвращение доступа к нему. При этом некоторые злоумышленники атакуют любые IoT-устройства, а другие — только технику определенного типа, способную выполнять интересующие их задачи. Ниже мы приводим виды вредоносного ПО для IoT в зависимости от его цели.

### DDoS-ботнеты

Наиболее распространенный вид вредоносного ПО для IoT-устройств — троянские программы, перехватывающие контроль над устройством для ведения DoS-атак на различные сервисы. Для DDoS-зловредов нет разницы, какие устройства атаковать. Функциональностью, которая интересует злоумышленников, — способностью отправлять запросы по сети — обладают все. Значительная часть подобных зловредов — это модификации кода Mirai, но существует и множество других семейств, различающихся методами распространения и закрепления на устройстве.

Так, вредоносное ПО RapperBot, хотя и позаимствовало некоторые части кода Mirai, по большей части состоит из уникального кода. Оно способно на [умный перебор паролей](https://securelist.ru/crimeware-report-uncommon-infection-methods-2/107293/#rapperbot-171-umnyj-podbor-parolej-187), основанный на анализе получаемого от Telnet-сервиса первого сообщения с запросом аутентификационных данных. По этому сообщению зловред может распознать тип устройства и перебирать только пароли к устройствам этого типа, что значительно повышает эффективность его самораспространения.

### Программы-вымогатели

В отличие от DDoS-зловредов, вымогатели атакуют преимущественно IoT-устройства, на которых есть пользовательские данные — NAS-хранилища. Одним из ярких примеров IoT-шифровальщика является DeadBolt, [поразивший тысячи устройств QNAP NAS](https://arstechnica.com/information-technology/2022/09/new-wave-of-data-destroying-ransomware-attacks-hits-qnap-nas-devices/) в 2022 году. Для атаки использовалась уязвимость [CVE-2022-27593](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27593), позволяющая злоумышленникам модифицировать системные файлы на устройстве. В результате пользовательские файлы оказались зашифрованы, а интерфейс устройства заблокировало сообщение о том, что для восстановления данных нужно заплатить выкуп в размере 0.03 BTC. Производитель выпустил обновление, закрывающее уязвимость, но подобные атаки все еще остаются актуальными.

### Майнеры

Несмотря на относительную неэффективность майнинга на IoT-устройствах, связанную с их низкой вычислительной мощностью, злоумышленники предпринимали попытки [добывать криптовалюту Bitcoin](https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/) в ходе кампаний Mirai. Однако эти попытки не получили широкого распространения.

### DNS changer

Атакующие могут использовать скомпрометированные IoT-устройства и для атаки на подключающихся к ним пользователей. Так, в 2022 году в ходе вредоносной кампании Roaming Mantis (также известной как Shaoye) злоумышленники [распространяли](https://securelist.com/roaming-mantis-dns-changer-in-malicious-mobile-app/108464/) приложение для Android, одной из функций которого была смена настроек DNS на Wi-Fi-роутерах через интерфейс администрирования. Зловред получал доступ к роутеру, если на нем использовались учетные данные по умолчанию, например admin:admin. На подходящем устройстве он менял конфигурацию так, чтобы роутер использовал сервер DNS, подконтрольный злоумышленнику. Этот сервер перенаправлял всех, кто подключался к роутеру, на ресурс, определяющий ОС клиента: если устройство работало под управлением Android, ресурс раздавал вредоносные файлы APK, а пользователей iOS перенаправлял на фишинговые страницы.

### Прокси-боты

Также довольно широко распространено использование зараженных устройств в качестве прокси-серверов — промежуточных узлов в сети, перенаправляющих трафик злоумышленника через себя, таким образом затрудняя его отслеживание. Чаще всего такие прокси-серверы используются для рассылки спама, обхода antifraud-систем и совершения различных сетевых атак.

## Вредоносное ПО для IoT: конкуренция и персистентность

Одна из основных особенностей вредоносного ПО для IoT — существование множества различных семейств, основанных на обнаруженном в 2016 году зловреде Mirai, исходный код которого был опубликован на одном из подпольных форумов. Это привело к быстрому развитию сотен модификаций, различающихся способами ведения DoS-атак, словарями для перебора учетных данных и выбором уязвимостей для самораспространения.

Большое количество игроков, в свою очередь, привело к жесткой конкуренции среди киберпреступников, причем не только специализирующихся на DDoS, но и в целом нацеленных на интернет вещей. Поэтому IoT-зловреды постепенно начали включать в себя функции для «нейтрализации» конкурентов непосредственно на зараженном устройстве и предотвращения его повторного заражения.

Наиболее популярная среди злоумышленников тактика закрепления доступа за собой — добавление правил сетевого экрана, блокирующих попытки подключения к устройству; несколько реже используется отключение сервисов удаленного управления устройством. Для борьбы с конкурентами, уже присутствующими на устройстве, обычно применяется ряд методов обнаружения, например проверка имен процессов, используемых ими портов и анализ памяти на «вредоносные» паттерны. Если IoT-зловред что-то обнаружит, он завершает чужие процессы и удаляет чужие файлы. Так злоумышленники борются друг с другом за контроль над устройством.

## Прочие угрозы, связанные с небезопасностью устройств IoT

Как мы видели из объявлений о покупке-продаже доступа к скомпрометированным IoT-устройствам, среди типов устройств, интересующих злоумышленников, встречаются подключенные к интернету видеокамеры. Способы монетизации доступа к камере могут быть разными. Ее могут использовать не только как «компьютер» (например, для майнинга криптовалюты или размещения вредоносного ПО для организации DDoS-атак) или «маршрутизатор» («прокси» или VPN для анонимизации различной вредоносной деятельности), но и (внезапно!) по прямому назначению.

Показателен [недавний инцидент](https://t.me/moscowmi/14898) с жительницей московской области, обнаружившей на китайских вебсайтах материалы приватного характера, сделанные с домашней видеокамеры, которую она приобрела на AliExpress для наблюдения за собакой.

Исследователь безопасности Пол Маррапезе (Paul Marrapese) изучил пользовательский сегмент видеокамер и выяснил, что проблемы информационной безопасности в них присутствуют и, к сожалению, производители устройств их далеко не всегда исправляют. Например, он обнаружил  критические уязвимости в протоколах и прошивках некоторых видеокамер, причем [один из вендоров так и не вышел на связь для устранения уязвимостей](https://hacked.camera/cves/).

Кроме того, хочется отметить, что часто производители подобных видеокамер используют различные реализации P2P-протоколов (peer-to-peer-, пиринговых). Такие, например, как Shenzhen Yunni iLnkP2P и CS2 Network P2P, которые используются на более чем пятидесяти миллионах устройств. Эти реализации, в свою очередь, имеют слабое шифрование трафика или не шифруют его вовсе, что дает злоумышленнику возможность совершить атаку типа MitM (Man-in the-Middle) — прослушивать трафик устройства, чтобы узнать учетные данные пользователя или перенаправить на свои ресурсы видеопоток, идущий с камеры.

Согласно [исследованию коллег из Trend Micro](https://www.trendmicro.com/vinfo/ie/security/news/internet-of-things/exposed-video-streams-how-hackers-abuse-surveillance-cameras), подглядывание за жизнью владельцев видеокамер — далеко не редкость. При этом стоит помнить, что помимо собственно камер инструментом шпионажа могут стать многие другие IoT-устройства, которые, несмотря на то что их основное назначение не связано с видеонаблюдением, также оснащены камерой. В частности, возможность записывать аудио и видео в режиме реального времени есть у большинства умных кормушек для питомцев. Спрос на них растет, число моделей множится, заполняя новый сегмент рынка, однако вендоры не всегда уделяют должное внимание их защите. Так, [исследование кормушки](https://securelist.com/smart-pet-feeder-vulnerabilities/110028/) из популярной линейки показало целый ворох уязвимостей и проблем безопасности, эксплуатация которых превращает устройство в инструмент подглядывания за хозяевами питомца и открывает другие возможности для злоумышленников.

Другой тип IoT-устройств, требующих особого внимания к вопросам безопасности, — умные устройства для детей. К сожалению, не все вендоры серьезно подходят к защите таких устройств. Впервые мы столкнулись с проблемой их небезопасности несколько лет назад, когда один из производителей умных детских часов заказал у нас [сервис по исследованию зрелости безопасности продукта](https://ics-cert.kaspersky.com/services/) по методологии [IoT Security Maturity Model от Industry IoT Сonsortium](https://www.iiconsortium.org/smm/). Аттестацию вендор тогда провалил, и сертификата мы не выдали — проблемы безопасности в продукте превращали его, по сути, в устройство слежения за ребенком и за всем(и), что (кто) находится в его окружении.

Проблема недостаточной защищенности IoT-устройств характерна не только для пользовательского рынка. Системы промышленного IoT могут также содержать тривиальные уязвимости, а рекомендованные вендором настройки — быть небезопасными.

Распространенной ошибкой конфигурации промышленных устройств являются пароли по умолчанию. Так, например, они вместе с весьма небезопасными рекомендациями по подключению и настройке были [приведены в документации](https://ics-cert.kaspersky.ru/publications/blog/2022/03/30/uyazvimosti-v-reshenii-tekon-avtomatika-bez-otvetstvennoe-raskrytie-i-masshtab-bedstviya/) производителя медиаконвертеров  для подключения лифтового оборудования к системам мониторинга в диспетчерских. Кроме того, наши исследователи обнаружили в устройствах уязвимости, эксплуатация которых доступна даже не слишком квалифицированным злоумышленникам и позволяет им получить полный контроль над конвертером. Небезопасные настройки из рекомендаций впоследствии убрали. Однако производитель устройств, вначале продемонстрировавший оперативность в устранении проблем безопасности, растерял по дороге всю ответственность, и многие из обнаруженных нами уязвимостей по сей день остаются неисправленными — спустя более года после того, как мы предоставили вендору информацию о них.

Из приведенных выше примеров может сложиться впечатление, что мы считаем все устройства IoT небезопасными, а их производителей — пренебрегающими культурой безопасной разработки. Однако это не так. Например, компания Bosch успешно [получила наш сертификат зрелости безопасности](https://ics-cert.kaspersky.com/smm-assessment/?item=bosch-ip-video-surveillance-camera-platforms) для умной видеокамеры, предназначенной для использования на промышленных предприятиях. Нам бы очень хотелось, чтобы как можно больше вендоров IoT-устройств, в том числе систем промышленного IoT, включали кибербезопасность своих продуктов в число первых приоритетов.

## Заключение

IoT-устройства интересуют злоумышленников по целому ряду причин: их можно использовать для DDoS-атак, перенаправлять через них трафик или подсматривать за владельцами с помощью встроенных видеокамер. NAS-хранилища также могут быть целью вымогателей, а роутеры привлекательны для злоумышленников, нацеленных на подключенные к ним устройства, например на мобильные устройства в общественной Wi-Fi-сети или на устройства локальной сети жертвы.

Злоумышленники непрерывно атакуют IoT и предлагают в даркнете услуги, связанные с такими атаками. Тем не менее большинство подключенных устройств, в том числе в промышленной среде, по-прежнему остается легкой добычей: для подключения используются пароли по умолчанию, в устройствах находят уязвимости, не все из которых получают патчи от производителя. Вендорам IoT-устройств, как домашних, так и промышленных, следует ответственно подходить к безопасности своей продукции и внедрять механизмы защиты от кибератак на стадии разработки. В частности, мы рекомендуем отказаться от практики использования паролей по умолчанию и генерировать уникальные пароли для каждого конкретного устройства. Также следует регулярно выпускать патчи к обнаруженным уязвимостям.

о есть по сути это экосистема устройств и технологий, подключенных через Интернет, которые постоянно собирают и передают данные. Часто к названию таких устройств добавляют приставку смарт или умный.

На первый взгляд, определение выглядит как обычная сеть. Однако ее специфика заключается в том, что в такой сети нет пользователей, сервисов, баз данных. То есть, принципиально – это изолированные сегменты объединенные через интернет устройств куда «не ступает нога человека».

IoT является очень удобным и полезным набором технологий, что значительно упрощает как нашу повседневную жизнь, так и работу организаций. Однако, к сожалению, идеальных технологий просто нет. Несмотря на безумную популярность и удобство устройств IoT, они имеют свои недостатки. Речь идет о наличии уязвимостей, которые трудно определить и отсутствие стандартизации. Помним, что IoT сети – это комплексы, где крайне редко появляется человек, соответственно – некому отслеживать нетипичную ситуацию и вирусы.

Злоумышленники в такой «не освещенной сети» могут расти и преуспевать очень долго не замеченными. Каждое устройство IoT является потенциально уязвимой точкой входа в сеть и бизнес-процессы. Поэтому такие сети могут стать (и становятся) первым этапом больших взломов, особенно если атака таргетирована именно на вашу организацию.

С развитием технологий, кибербезопасность устройств становится все более критическим вопросом. Особенно это становится очевидным в контексте Интернета вещей, поскольку количество устройств, которые могут получать и отправлять конфиденциальные данные ежедневно растет. Внедрение и обновление мер безопасности устройств должно стать приоритетом на ближайшие годы для технологии IoT.

В группу приборов, подключаемых к [интернету](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82), входят видеокамеры, телевизоры, принтеры, холодильники и другая техника. Большая часть этих устройств неудовлетворительно защищена от хакерских атак. Сами по себе эти устройства могут не представлять интереса для преступников. Однако хакеры взламывают их, чтобы использовать в качестве роботов для создания [ботнетов](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82), посредством которых можно атаковать более серьезные системы. Большинство владельцев взломанных устройств даже не подозревают, как используется их техника.

В качестве примера приведена масштабная [DDoS-атака](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:DDoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) на [интернет](https://www.tadviser.ru/index.php/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82)-ресурс Krebs On Security, в сентябре 2016 года.

|  |  |  |
| --- | --- | --- |
| « | Интенсивность запросов от ботсети во время атаки достигла 700 Гб/с. В составе [ботсети](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82) более 1 млн камер, видорегистраторов и других подключенных к [интернету вещей](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA)) устройств. Это не первый резонансный случай, когда подобные устройства становятся частью [ботнета](https://www.tadviser.ru/index.php/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82), однако впервые сеть состояла почти полностью из таких приборов.  **Брайан Кребс (Brian Krebs), владелец ресурса** | » |

<https://www.sentinelone.com/cybersecurity-101/data-and-ai/iot-security-risks/>

https://sber.pro/publication/bezopasnost-iot-ustroystv-interneta-veshei/

<https://www.youtube.com/watch?v=PrIwGos7vHM&ab_channel=SamsungInnovationCampus>

<https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9,_IoT,_M2M_(%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%80%D1%8B%D0%BD%D0%BE%D0%BA)>

IoT (Internet of Things) enjamlaryna edilýän atakalar, uly zyyanlara we howpsuzlyk meselelerine sebäp bolup biler. Aşakda IoT enjamlaryna edilip bilinýän atakalaryň sowly amala aşyrylyp, ýitirilýän we döredilen zyyanlar barada maglumat berilýär:

### 1. ****DDoS (Distributed Denial of Service) Atakasy****

* **Zyyanlar**:
  + **Hyzmatlaryň elýeterliliginiň ýitirilmegi**: DDoS atakasy, IoT enjamlarynyň aragatnaşygy arkaly bir web hyzmatyny ýa-da ulgamy çykarmak üçin giňden ulanylýar. Bu atakalar web serwerlerine ýa-da bulut hyzmatlaryna elýeterliligi çäklendirip, şol hyzmatlary ýa-da ulgamly serwisleri dowamly işlemeýän hala getirip biler.
  + **Maliýe ýitgileri**: Web sahypalarynyň ýa-da hyzmatlarynyň elýeterliliginiň bozulmagy müşderileriň we işiň ygtybarlygyny we mahabatyny ýitirmäge sebäp bolup biler. Bu bolsa maliýe ýitgilerine we ygtybarlylygyň bozulmagyna getirýär.

### 2. ****Brute Force Atakasy****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň çalşygy**: IoT enjamlarynyň parollaryny tapmak üçin ulanylan brute force atakasy, enjamyň hasaplarynyň gowşaklyklaryny peýdalanyp, şahsy maglumatlary ýa-da kontentleri çalyp almak üçin mümkinçilik döredýär.
  + **Enjamyň basyp alynmagy**: Şahsy parollaryň ýa-da login maglumatlarynyň tapylmagy, enjamy basyp almak ýa-da ulanmak üçin hakerlere ýol açýar. Bu ýagdaýda enjamdan şübheli maksatlar üçin peýdalanmak mümkin.

### 3. ****Man-in-the-Middle (MITM) Atakasy****

* **Zyyanlar**:
  + **Maglumatlaryň aldanmagy**: MITM atakasy, aragatnaşykda bolan maglumatlary okap ýa-da üýtgedip, bu maglumatlaryň aldanmagyny döredýär. Hakerler şahsy maglumatlary, şifrlenmedik aragatnaşyk arkaly üýtgedip ýa-da öňünden alyp bilýärler.
  + **Şahsyýetiň ýoluna çykmagy**: Aragatnaşykda şahsy maglumatlaryň (şifrler, kart maglumatlary) çalyşylmagy, hakerleriň bu maglumatlary giňden peýdalanyp, başga biri hökmünde hereket etmegine sebäp bolup biler.

### 4. ****Firmware Atakalary****

* **Zyyanlar**:
  + **Enjamyň işini bozmak**: IoT enjamlarynyň firmware'ine edilýän atakalar, enjamyň işini basyp almak ýa-da bozmak üçin ulanylyp biler. Bu, enjamyň doly işini ýerine ýetirip bilmezlige getirer.
  + **Enjamyň gurnama mümkinçiliginiň ýok edilmegi**: Firmware'ine edilýän hüjümler, enjamy özgerdýän kodlary goýup, ulgamyň işine täsir eder. Bu ýagdaýda, enjamyň doly gurnama ýa-da täzelenme işleriniň ýerine ýetirilmegi mümkin däl bolup biler.

### 5. ****Sosial Injenerçilik (Social Engineering)****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň açylmagy**: Sosial inženerlik, ulanyjynyň ynamyny gazanmak arkaly, onuň şahsy maglumatlaryny (parollar, maglumatlar) almak üçin ulanylyp bilner. Bu, enjamyň ýa-da ulgamyň hasaplaryna girmäge mümkinçilik döredýär.
  + **Zäherli linkleriň ýa-da kodlaryň täsir etmegi**: Hakerler ulanyjyny şübheli linkleri basmaga mejbur edip, bu link arkaly enjamda zäherli programma üpjünçiligini ýerleşdirip bilerler.

### 6. ****Cross-Site Scripting (XSS) Atakasy****

* **Zyyanlar**:
  + **Web interfeýsiniň bozulmagy**: XSS atakasy, web interfeýsine zäherli kod ýerleşdirip, enjamyň web sahypasyna täsir edip biler. Bu, ulanyjylaryň we maglumatlaryň howpsuzlygyny ýok eder.
  + **Şahsy maglumatlaryň çalyşylmagy**: XSS atakasy arkaly, şahsy maglumatlar (login maglumatlary, şifrler) çalynyp, şübheli maksada ýüklenip bilner.

### 7. ****SQL Injection Atakasy****

* **Zyyanlar**:
  + **Maglumat bazasynyň bozulmagy**: SQL injection atakasy, enjamyň maglumat bazasyna girmäge mümkinçilik berýär we bu maglumat bazasyny üýtgedip, adatça goýberilmedik maglumatlary alyp biler.
  + **Enjamdan we maglumatlardan peýdalanmak**: Hakerler, SQL injection arkaly, enjamdaky maglumatlary, şahsy maglumatlary ýa-da biznes maglumatlaryny almaga mümkinçilige eýe bolup bilerler.

### 8. ****Botnetler****

* **Zyyanlar**:
  + **Hyzmatyň elýeterliliginin bozulmagy**: Botnetler, IoT enjamlarynyň köpüsi bir arada bolanda, ulgamyň we hyzmatyň çäklendirilmegine ýa-da basyp alynmagyna sebäp bolup biler.
  + **Zäherli maksatlar üçin ulanylyp bilner**: IoT enjamlary botnetlere goşulyp, şübheli maksatlar üçin, mysal üçin, DDoS hüjümlerini amala aşyrmak üçin ulanylyp biler.

### 9. ****Zero-Day Atakalary****

* **Zyyanlar**:
  + **Enjamyň gowşaklygyny peýdalanmak**: Zero-day atakasy, enjamda ýa-da ulgamda öňünden ýüze çykmadyk gowşaklykdan peýdalanmagy mümkin edýär. Bu, enjamda howpsuzlyk gowşaklyklaryny tapyp, bu gowşaklygy ulanyp enjamyň basyp almagyna sebäp bolup biler.
  + **Täzelenmeleriň we aragatnaşyklaryň täsir etmegi**: Zero-day atakasy, täzelenme ýa-da enjamdaky gowşaklyklar zerarly, hakerlere enjamyň içindäki maglumatlary ýitirmäge ýa-da täsir etmäge mümkinçilik döredýär.

### 10. ****Physical Attacks (Fiziki Atakalar)****

* **Zyyanlar**:
  + **Enjamyň fiziki taýdan bozulyşy**: Fiziki atakalar, enjamyň fiziki taýdan kesilmegine ýa-da işiniň bozulmagyna sebäp bolup biler. Bu, enjamyň işini çäklendirip, ulgamdan çykmagyna sebäp bolup biler.
  + **Maglumatlaryň aşkar edilmegi**: Fiziki atakalar arkaly, enjamlar arkaly toplanan maglumatlar fiziki ýagdaýda olýalyp, olaryň gizlinligi we howpsuzlygy bozulýar.

Bu atakalar sowly amala aşyrylýan ýagdaýlarda, IoT enjamlary we olaryň sistemy üçin uly zyyanlar döredip biler. Hakerler, bu atakalar arkaly enjamlar ýa-da ulgamlara, olaryň işini basyp almak, şahsy maglumatlary almak we hasaplary basyp almak ýaly howplary döredýärler. Howpsuzlyk çärelere we täzelenmelere yzygiderli üns bermek, bu görnüşli atakalary peseltmekde we olaryň yzyna galmagyna garşy durmakda möhüm rol oýnaýar.

IoT (Internet of Things) enjamlaryna edilýän atakalar, uly zyyanlara we howpsuzlyk meselelerine sebäp bolup biler. Aşakda IoT enjamlaryna edilip bilinýän atakalaryň sowly amala aşyrylyp, ýitirilýän we döredilen zyyanlar barada maglumat berilýär:

### 1. ****DDoS (Distributed Denial of Service) Atakasy****

* **Zyyanlar**:
  + **Hyzmatlaryň elýeterliliginiň ýitirilmegi**: DDoS atakasy, IoT enjamlarynyň aragatnaşygy arkaly bir web hyzmatyny ýa-da ulgamy çykarmak üçin giňden ulanylýar. Bu atakalar web serwerlerine ýa-da bulut hyzmatlaryna elýeterliligi çäklendirip, şol hyzmatlary ýa-da ulgamly serwisleri dowamly işlemeýän hala getirip biler.
  + **Maliýe ýitgileri**: Web sahypalarynyň ýa-da hyzmatlarynyň elýeterliliginiň bozulmagy müşderileriň we işiň ygtybarlygyny we mahabatyny ýitirmäge sebäp bolup biler. Bu bolsa maliýe ýitgilerine we ygtybarlylygyň bozulmagyna getirýär.

### 2. ****Brute Force Atakasy****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň çalşygy**: IoT enjamlarynyň parollaryny tapmak üçin ulanylan brute force atakasy, enjamyň hasaplarynyň gowşaklyklaryny peýdalanyp, şahsy maglumatlary ýa-da kontentleri çalyp almak üçin mümkinçilik döredýär.
  + **Enjamyň basyp alynmagy**: Şahsy parollaryň ýa-da login maglumatlarynyň tapylmagy, enjamy basyp almak ýa-da ulanmak üçin hakerlere ýol açýar. Bu ýagdaýda enjamdan şübheli maksatlar üçin peýdalanmak mümkin.

### 3. ****Man-in-the-Middle (MITM) Atakasy****

* **Zyyanlar**:
  + **Maglumatlaryň aldanmagy**: MITM atakasy, aragatnaşykda bolan maglumatlary okap ýa-da üýtgedip, bu maglumatlaryň aldanmagyny döredýär. Hakerler şahsy maglumatlary, şifrlenmedik aragatnaşyk arkaly üýtgedip ýa-da öňünden alyp bilýärler.
  + **Şahsyýetiň ýoluna çykmagy**: Aragatnaşykda şahsy maglumatlaryň (şifrler, kart maglumatlary) çalyşylmagy, hakerleriň bu maglumatlary giňden peýdalanyp, başga biri hökmünde hereket etmegine sebäp bolup biler.

### 4. ****Firmware Atakalary****

* **Zyyanlar**:
  + **Enjamyň işini bozmak**: IoT enjamlarynyň firmware'ine edilýän atakalar, enjamyň işini basyp almak ýa-da bozmak üçin ulanylyp biler. Bu, enjamyň doly işini ýerine ýetirip bilmezlige getirer.
  + **Enjamyň gurnama mümkinçiliginiň ýok edilmegi**: Firmware'ine edilýän hüjümler, enjamy özgerdýän kodlary goýup, ulgamyň işine täsir eder. Bu ýagdaýda, enjamyň doly gurnama ýa-da täzelenme işleriniň ýerine ýetirilmegi mümkin däl bolup biler.

### 5. ****Sosial Injenerçilik (Social Engineering)****

* **Zyyanlar**:
  + **Şahsy maglumatlaryň açylmagy**: Sosial inženerlik, ulanyjynyň ynamyny gazanmak arkaly, onuň şahsy maglumatlaryny (parollar, maglumatlar) almak üçin ulanylyp bilner. Bu, enjamyň ýa-da ulgamyň hasaplaryna girmäge mümkinçilik döredýär.
  + **Zäherli linkleriň ýa-da kodlaryň täsir etmegi**: Hakerler ulanyjyny şübheli linkleri basmaga mejbur edip, bu link arkaly enjamda zäherli programma üpjünçiligini ýerleşdirip bilerler.

### 6. ****Cross-Site Scripting (XSS) Atakasy****

* **Zyyanlar**:
  + **Web interfeýsiniň bozulmagy**: XSS atakasy, web interfeýsine zäherli kod ýerleşdirip, enjamyň web sahypasyna täsir edip biler. Bu, ulanyjylaryň we maglumatlaryň howpsuzlygyny ýok eder.
  + **Şahsy maglumatlaryň çalyşylmagy**: XSS atakasy arkaly, şahsy maglumatlar (login maglumatlary, şifrler) çalynyp, şübheli maksada ýüklenip bilner.

### 7. ****SQL Injection Atakasy****

* **Zyyanlar**:
  + **Maglumat bazasynyň bozulmagy**: SQL injection atakasy, enjamyň maglumat bazasyna girmäge mümkinçilik berýär we bu maglumat bazasyny üýtgedip, adatça goýberilmedik maglumatlary alyp biler.
  + **Enjamdan we maglumatlardan peýdalanmak**: Hakerler, SQL injection arkaly, enjamdaky maglumatlary, şahsy maglumatlary ýa-da biznes maglumatlaryny almaga mümkinçilige eýe bolup bilerler.

### 8. ****Botnetler****

* **Zyyanlar**:
  + **Hyzmatyň elýeterliliginin bozulmagy**: Botnetler, IoT enjamlarynyň köpüsi bir arada bolanda, ulgamyň we hyzmatyň çäklendirilmegine ýa-da basyp alynmagyna sebäp bolup biler.
  + **Zäherli maksatlar üçin ulanylyp bilner**: IoT enjamlary botnetlere goşulyp, şübheli maksatlar üçin, mysal üçin, DDoS hüjümlerini amala aşyrmak üçin ulanylyp biler.

### 9. ****Zero-Day Atakalary****

* **Zyyanlar**:
  + **Enjamyň gowşaklygyny peýdalanmak**: Zero-day atakasy, enjamda ýa-da ulgamda öňünden ýüze çykmadyk gowşaklykdan peýdalanmagy mümkin edýär. Bu, enjamda howpsuzlyk gowşaklyklaryny tapyp, bu gowşaklygy ulanyp enjamyň basyp almagyna sebäp bolup biler.
  + **Täzelenmeleriň we aragatnaşyklaryň täsir etmegi**: Zero-day atakasy, täzelenme ýa-da enjamdaky gowşaklyklar zerarly, hakerlere enjamyň içindäki maglumatlary ýitirmäge ýa-da täsir etmäge mümkinçilik döredýär.

### 10. ****Physical Attacks (Fiziki Atakalar)****

* **Zyyanlar**:
  + **Enjamyň fiziki taýdan bozulyşy**: Fiziki atakalar, enjamyň fiziki taýdan kesilmegine ýa-da işiniň bozulmagyna sebäp bolup biler. Bu, enjamyň işini çäklendirip, ulgamdan çykmagyna sebäp bolup biler.
  + **Maglumatlaryň aşkar edilmegi**: Fiziki atakalar arkaly, enjamlar arkaly toplanan maglumatlar fiziki ýagdaýda olýalyp, olaryň gizlinligi we howpsuzlygy bozulýar.

Bu atakalar sowly amala aşyrylýan ýagdaýlarda, IoT enjamlary we olaryň sistemy üçin uly zyyanlar döredip biler. Hakerler, bu atakalar arkaly enjamlar ýa-da ulgamlara, olaryň işini basyp almak, şahsy maglumatlary almak we hasaplary basyp almak ýaly howplary döredýärler. Howpsuzlyk çärelere we täzelenmelere yzygiderli üns bermek, bu görnüşli atakalary peseltmekde we olaryň yzyna galmagyna garşy durmakda möhüm rol oýnaýar.

Häzirki wagtda IoT enjamlaryna edilýän atakalar we olaryň amala aşyran zyyanlary baradaky hakykatdaky köp sanly wakalar we kynçylyklar bar. IoT ulgamynyň dünýäde giňden ulanylmagy, bu enjamlaryň howpsuzlyk gowşaklyklaryny we potensial zorluklary açyp görkezdi. Aşakda IoT enjamlaryna edilen uly atakalar we olaryň döredýän zyyanlary barada birnäçe hakykatlyk wakany we meseleleri ýatlap bileris:

### 1. ****Mirai Botnet Hüjümi (2016)****

* **Hüjüm**: Mirai botneti, 2016-njy ýylda IoT enjamlary arkaly amala aşyrylan iň uly DDoS hüjümlerinden biri bolup, enjamlar (kamera, routerler, TV'ler we beýleki IoT enjamlar) botnetleriň bir bölegine öwrüldi. Bu botnet, «Internet of Things» enjamlaryny ulanmak arkaly, internete bagly web serwislerine we serverlere uly basyş edip, olaryň işini basyp aldy.
* **Zyyanlar**:
  + **Hyzmatlaryň çäklendirilmegi**: Mirai botneti, Dyn (bir internet provayderi) we beýleki kompaniýalara garşy DDoS hüjümlerini amala aşyrdy. Bu hüjümler, onlarça şübheli ulgam we servisi basyp aldy.
  + **Maliýe Ýitgileri**: Şeýle hüjümler birnäçe kompaniýalaryň we hyzmatlaryň ýitirişine sebäp boldy. Ekranda ýüze çykýan hyzmatlaryň wagtynda işlemek üçin ähli hyzmatlaryň bozulmagy, ulanyjylara we kompaniýalara uly maliýe ýitgilerini getirýär.

### 2. ****Stuxnet (2010)****

* **Hüjüm**: Stuxnet, IoT we senagat ulgamyna garşy edilýän ilkinji giňden tanalan hüjümlerden biridir. Bu zäherli programma, Iran döwletiniň yklym energiýasy pudagyndaky natriýum merkezi we beýleki senagat enjamlaryny nygtap, olaryň işini hasaplap, fizik taýdan zoýun çykarmak üçin amala aşyryldy.
* **Zyyanlar**:
  + **Fiziki Zyyan**: Stuxnet, senagat ulgamlaryny çalt ýitirmäge we giňişleýin fiziki zyyanlara sebäp boldy. Bu hüjüm, öňki döwürde fiziki ulgamlara edilýän iň uly we tehnologik taýdan ösüşi ulanyp edilýän ataklaryň biri boldy.
  + **Maliýe Ýitgileri**: Senagat ulgamyndaky wagtyň geçmegi, tebigy gaz we gazada işlere bolan ykdysady ýitirişleri döretdi.

### 3. ****Target DDoS Atakasy (2013)****

* **Hüjüm**: 2013-nji ýylda ABŞ-nyň Target kompaniýasyna DDoS atakasy edilip, web serwisiniň ýa-da IoT enjamlarynyň ulanylyp, müşderi maglumatlarynyň giňişleýin açylmagyna sebäp boldy.
* **Zyyanlar**:
  + **Şahsy Maglumatlaryň Çalynmagy**: Bu atakalar müşderileriň şahsy maglumatlaryny, kredit kartalaryny we beýleki möhüm maglumatlary çalyşmaga sebäp boldy.
  + **Reputasiýa We Maliýe Ýitgileri**: Target kompaniýasy bu hüjüme garşy dürli jogapkärçilikleri almak we uly maliýe ýitgileri ýüze çykdy. Şeýle hüjümler kompaniýalaryň itibarını çalt ýitirmäge sebäp bolýar.

### 4. ****WannaCry Ransomware (2017)****

* **Hüjüm**: WannaCry, IoT we beýleki ulgamlara gurallary arkaly edilýän ransomware hüjümleriniň biri bolup, botnet ulgamlaryndan peýdalanylyp, dünýä boýunça ähli ulgamlara girmäge mümkinçilik berýärdi.
* **Zyyanlar**:
  + **Maglumatlaryň ýitirilmegi**: WannaCry hüjümi bilen, köp sanly kompýuterlere we ulgamlara gurallary şifrlemek we ondan maglumatlary almagy maksat edinmek üçin ulanyldy.
  + **Işleriň basylmagy**: Hüjüme sezewar bolan kompaniýalar we guramalar, öz ulgamyny we maglumatlaryny açmak üçin bölek-bölek tölegler we dolandyryşlarynda güýçli kynçylyklar görýärdi.

### 5. ****Hackerler tarapyndan IoT Enjamlarynyň Basyp Alnmagy****

* **Hüjümler**: 2017-nji ýylda, hakerler IoT enjamlary arkaly Wi-Fi-routerlere, kameralara, öýdeki awtomatlaşdyrylan ulgamlara we beýleki IoT enjamlaryna girmäge başladylar. Bu atakalar, şahsy maglumatlary almak we enjamdan şübheli maksatlar üçin peýdalanmak üçin amala aşyryldy.
* **Zyyanlar**:
  + **Şahsy Maglumatlaryň Çalynmagy**: Enjamlar fiziki ýa-da aragatnaşyk arkaly şübheli peýdalanyldy, bu bolsa ulanyjylaryň maglumatlarynyň ýitirilmegine sebäp boldy.
  + **Aşkar Edilen Ulgamlar**: Enjamlar, howpsuzlyk gowşaklyklary we parol sowadyşlary arkaly ulanyldy, olardan ýüzlerçe adam, IoT enjamlarynyň işine täsir edip, hasaplaryna girmäge mümkinçilik tapdy.

### Netije

IoT enjamlary we ulgamlary üçin atakalar dünýäde dürli uly zyyanlary döretdi. Bu zyyanlar diňe sanly dünýäde däl, eýsem fiziki we maliýe taýdan-da uly täsirler galdyrdy. Netijede, IoT enjamlary üçin howpsuzlyk çärelere degişli esaslykly ulaglar we tejribeler (şifrlenme, parol üpjünçiligi, täzelenmeler) gurnalan. Bu hüjümler, ýönekeý adamlaryň we kompaniýalaryň IoT ulgamlaryna bolan ynamynyň azalmagyna sebäp boldy. Howpsuzlyk derejesi ýokarlandyrylmadyk ýagdaýda, täze atakalar has giňişleýin zyyan döredip biler.

## Типы рисков Интернета вещей

Разнообразие устройств, приложений и сетей Интернета вещей порождает множество потенциальных рисков, в том числе:

* **Конфиденциальность данных:**  устройства Интернета вещей часто собирают и передают огромные объемы конфиденциальных данных, что делает их привлекательными целями для киберпреступников, стремящихся использовать личную или конфиденциальную информацию.
* **Перехват устройств:**  злоумышленники могут взломать устройства IoT, получить контроль над их функциями и использовать их для запуска дальнейших атак или срыва операций.
* **Атаки типа «отказ в обслуживании» (DoS):**  крупномасштабные ботнеты, состоящие из взломанных устройств Интернета вещей, могут быть использованы для подавления и отключения критически важной инфраструктуры и онлайн-сервисов.
* **Атаки «человек посередине» (MitM):**  злоумышленники могут перехватывать сообщения между устройствами Интернета вещей и их предполагаемыми получателями, что позволяет осуществлять прослушивание и манипулирование данными.
* **Уязвимости прошивки:**  недостатки в программном обеспечении, управляющем устройствами IoT, могут стать для злоумышленников возможностью использовать уязвимости и получить несанкционированный доступ.
* **Атаки на цепочку поставок:**  Взлом цепочки поставок устройств Интернета вещей может привести к внедрению вредоносного кода или компонентов, что сделает устройства уязвимыми для атак.
* **Риски физической безопасности:**  Физическая доступность устройств Интернета вещей может сделать их уязвимыми для взлома, кражи или несанкционированного доступа к конфиденциальным данным.

Интернет вещей (IoT) — это термин, используемый для описания сети взаимосвязанных электронных устройств с «умной» технологией. В то время как смартфоны теперь стали обычным явлением, другие умные устройства все еще находятся в зачаточном состоянии, но их использование постоянно растет, и в настоящее время [к Интернету подключено около 6,4 млрд «вещей»](http://www.gartner.com/newsroom/id/3165317) , что на 30% больше, чем в 2015 году. Ожидается, что в 2020 году это число вырастет до [ошеломляющих 20,8 млрд.](https://www.symantec.com/content/dam/symantec/docs/infographics/istr-iot-en.pdf)

К таким интеллектуальным устройствам относятся автомобили, бытовая техника, системы зданий, такие как освещение и отопление, телевизоры, медицинские приборы, производственное оборудование и многие другие типы систем, используемых как в потребительских, так и в промышленных условиях.

Умные устройства призваны сделать нашу жизнь проще и удобнее. Например, системы домашней автоматизации позволяют домовладельцам включать термостат по пути домой с работы зимой или немедленно получать оповещения о предполагаемом вторжении в дом, пока их нет дома.

Однако все это дополнительное оборудование и программное обеспечение, подключенное к Интернету и потенциально доступное любому человеку (при наличии соответствующих учетных данных или через уязвимость программного обеспечения), представляет огромную угрозу безопасности предприятий и частных лиц, которые его используют.

## Риски безопасности устройств Интернета вещей

Любое используемое вами оборудование и программное обеспечение, подключенное к Интернету, может быть потенциально доступно киберпреступникам. С появлением каждого нового устройства растет число потенциальных точек доступа для хакеров.

Уже было несколько примеров взлома или уязвимости смарт-устройств, в том числе:

* Многие [интеллектуальные медицинские устройства,](http://www.24x7mag.com/2014/08/beware-nine-medical-device-vulnerabilities/) включая инсулиновые помпы и внутренние дефибрилляторы, используют устаревшее программное обеспечение и незашифрованные данные, что создает серьезные уязвимости с точки зрения конфиденциальности и физического благополучия пациентов.
* Миллионы [смарт-телевизоров](https://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it) подвержены риску мошенничества с кликами, бот-сетей, кражи данных и программ-вымогателей.
* [1,4 миллиона автомобилей Fiat Chrysler были отозваны](http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/) после того, как исследователи обнаружили, что с их помощью можно получить доступ к автомобилям и управлять ими удаленно через Интернет, в том числе выключить двигатель и съехать с дороги.
* Обнаружено, что [75% дверных замков с технологией Bluetooth Smart имеют уязвимости, позволяющие легко их взломать.](https://www.cnet.com/news/have-a-smart-lock-yeah-it-can-probably-be-hacked/)
* Недавно была осуществлена [​​крупнейшая в истории DDoS-атака с использованием более 150 000 взломанных смарт-устройств по всему миру, включая камеры, принтеры и холодильники.](http://thehackernews.com/2016/09/ddos-attack-iot.html)

Эксперты по безопасности предупреждают, что многие смарт-устройства уязвимы для атак, поскольку они не проходят достаточного тестирования безопасности, часто используют устаревшее программное обеспечение, и на них невозможно установить брандмауэр или другое защитное программное обеспечение, как это можно сделать на обычном компьютере.

Поскольку компьютерное программное обеспечение становится все более надежным и устойчивым к вредоносным атакам, хакеры обращаются к новому поколению интеллектуальных устройств как к более простому варианту, часто добиваясь большого успеха.

## Почему умные устройства так уязвимы?

Есть несколько причин, по которым Интернет вещей представляет такую ​​угрозу нашей цифровой безопасности. [Исследование, проведенное HP,](https://www.scribd.com/document/263392568/IOT-Research-Study-by-HP) рассмотрело некоторые из самых популярных устройств IoT, чтобы оценить их общий уровень безопасности, и обнаружило несколько проблемных моментов:

### 1. Отсутствие защиты личных данных

Большинство потребительских смарт-устройств (90% из тех, которые были оценены в исследовании) хранят персональные [конфиденциальные данные пользователя](https://spin.ai/blog/sensitive-data-protection/)  либо на самом устройстве, либо в облаке, либо через мобильное приложение, которое интегрируется с устройством. Эти данные часто не защищены должным образом и часто передаются в незашифрованном виде по сетям.

### 2. Небезопасное программное обеспечение

Поскольку интеллектуальные технологии развиваются так быстро, производители вынуждены как можно быстрее выводить свою продукцию на рынок. Это означает, что важные части жизненного цикла программного обеспечения, такие как безопасность и тестирование, часто выполняются в спешке.

Хотя обновления для таких устройств, как правило, выпускаются регулярно, 60% опрошенных загружали эти обновления автоматически без шифрования. Это означает, что существует вероятность перехвата и изменения загрузки хакерами.

Во многих случаях уязвимости не могут быть устранены немедленно, поскольку компания не хочет беспокоить своих пользователей, заставляя их обновлять прошивку.

### 3. Недостаточная процедура аутентификации

Небезопасные пароли и [управление облачной идентификацией](https://spin.ai/blog/sensitive-data-protection/) являются распространенной уязвимостью во всех видах цифровых систем. Хотя большинство компьютерных программ теперь заставляют пользователей создавать надежный пароль, это не относится ко всем смарт-устройствам.

Кроме того, пользователи часто используют пароли для нескольких аккаунтов. Если безопасность подключенного устройства недостаточна и хакеры получают доступ к паролю, они могут использовать этот пароль для доступа к другим, более конфиденциальным аккаунтам, принадлежащим пользователю.

80% протестированных устройств не требовали достаточно длинных и сложных паролей.

### 4. Отсутствие шифрования данных

Было обнаружено, что 70% устройств отправляют данные по сети в незашифрованном виде. [Шифрование данных необходимо](https://spin.ai/blog/what-is-the-reason-for-encrypting-data-in-a-backup/) для предотвращения их перехвата неавторизованными лицами, особенно при передаче через Интернет между облаком и устройством или мобильным приложением.

80% протестированных устройств не требовали достаточно длинных и сложных паролей.

### 5. Плохо закодированный пользовательский интерфейс

Более половины протестированных устройств имели плохо закодированные веб-интерфейсы, что приводило к уязвимостям безопасности из-за таких проблем, как плохая обработка сеансов, слабые учетные данные по умолчанию и постоянный межсайтовый скриптинг.

Эти уязвимости безопасности позволяют хакерам легко получить доступ к веб-интерфейсу с помощью таких уловок, как использование функции сброса пароля, и таким образом получить доступ к данным и управлению самим устройством.

## Как сделать Интернет вещей более безопасным?

Безопасность Интернета вещей начинает восприниматься все серьезнее, и [даже ФБР](https://www.ic3.gov/media/2015/150910.aspx) выпустило предупреждения о рисках безопасности, которые могут возникнуть при использовании таких устройств.

Несколько советов безопасности и альянсов также были созданы различными технологическими организациями с целью разработки передовых методов и предоставления образования по надлежащей защите интеллектуальных устройств. К ним относятся [Совет безопасности Интернета вещей](http://www.smartcardalliance.org/activities-councils-internet-of-things-security/) и [Фонд безопасности Интернета вещей.](https://iotsecurityfoundation.org/)

В то время как производители должны брать на себя большую ответственность за создание защищенных устройств и выпуск исправлений безопасности сразу после обнаружения уязвимостей, частные лица и компании, использующие устройства Интернета вещей, также должны убедиться, что они приняли собственные меры безопасности.

Одним из возможных решений являются интегрированные в облако панели управления безопасностью, которые отслеживают подключенные интеллектуальные устройства и информируют пользователя о рисках и компрометациях безопасности с помощью [интеллектуальных](https://spin.ai/blog/cloud-insider-threats-control-for-google-workspace/)[инструментов](https://spin.ai/blog/data-loss-prevention-tools-advantages/) обнаружения угроз   и предотвращения потери данных.

Также важно, чтобы облачные сервисы, используемые устройствами для хранения пользовательских данных, были безопасными, чтобы предотвратить серьезные [утечки данных](https://spin.ai/blog/how-to-implement-data-leak-prevention-in-google-workspace/) .

Чтобы обеспечить достаточный уровень цифровой безопасности в корпоративной среде, ИТ-отделы должны полностью интегрировать интеллектуальные устройства в [общие процессы мониторинга](https://spin.ai/blog/spin-ai-releases-google-workspace-security-policies/) и тестирования безопасности.

Перед покупкой компаниям также следует [учитывать риски безопасности,](https://spin.ai/blog/cybersecurity-awareness-importance-and-purpose/) связанные с интеллектуальными устройствами, и сопоставлять эти риски с преимуществами, которые они предоставляют компании.

Под давлением конечных пользователей производители, скорее всего, будут уделять больше внимания безопасности, начиная с первоначального производства и заканчивая обновлениями и исправлениями программного обеспечения.

Aşakda IoT (Internet of Things) enjamlaryna edilýän iň möhüm 10 atak, olaryň getiren zyyanlary we nämäniň ýaly ataklaryň haýsy ýagdaýlarda ýerine ýetirildigi barada maglumatlar berilýär:

### 1. ****Mirai Botnet Atakasy (2016)****

* **Näme edilendir?**: Mirai botneti, IoT enjamlarynyň (kamera, routerler, printerler we ş.m.) gurnalmagy arkaly, hakerler bu enjamlary botnetlere öwürdüler we soňra bu botnetlerden DDoS (Distributed Denial of Service) hüjümleri üçin peýdalandylar.
* **Zyyanlar**:
  + **Web hyzmatlarynyň we serwisleriň bozulmagy**: Mirai, Dyn, Twitter, Reddit, GitHub ýaly birnäçe uly web serwislerine DDoS hüjümleri düzen we olaryň çäklendirilmegine sebäp boldy.
  + **Maliýe ýitgileri**: Serwisleriň işlemeýän wagty, milyardlarça dollar maliýe ýitgi döredildi.
* **Ýerine ýetirilýän ýer**: ABŞ, Ýaponiýa, we beýleki ýurtlarda dürli internet hyzmatlaryna garşy hüjümler.

### 2. ****Stuxnet (2010)****

* **Näme edilendir?**: Stuxnet, IoT we senagat ulgamyny nygtap, atom reaktoryndaky enjamlar üçin ýörite döredilen zäherli programma (worm) bolup, Senagat we nebitgaz pudaklaryny nygtap, enjamda fiziki zeperler ýetirdi.
* **Zyyanlar**:
  + **Fiziki zeperler**: Stuxnet, Iranyň Natanzdaky urany aýyrmak üçin ulanylýan merkeziyini we beýleki enjamları nygtap, olaryň işini bozdy.
  + **Senagat ulgamynyň howpsuzlyk gowşaklygy**: Stuxnet, täze enjamlaryň we tehnologiyalaryň gowşaklygyny açyp, şunuň ýaly ataklaryň käbiriniň fiziki ulgamlara degişli bolandygyny görkezdi.
* **Ýerine ýetirilýän ýer**: Iran (Natanz), dünýäde beýleki senagat we tehnologik ulgamlara täsir etdi.

### 3. ****DDoS Atakasy (Dyn, 2016)****

* **Näme edilendir?**: Dyn kompaniýasyna edilýän DDoS hüjümi, IoT enjamlary (kamera, router, printerler) arkaly, bu enjamlary botnetlere öwürüp, neteň web serwislerine we internete serwerlerine saldırmak üçin ulanyldy.
* **Zyyanlar**:
  + **Web hyzmatlarynyň elýeterliligi ýitirilýär**: Dyn hyzmatynyň bozulmagy, bir gämi hyzmatyny (GitHub, Twitter, Reddit) çäklendirip, malyýedäki ýitgiler bolup geçdi.
  + **Reputasiýa we maliýe ýitgi**: Ulgam bozulmasy sebäpli internet ulgamynyň hasaplamasyna zäherli täsirler ýetdi.
* **Ýerine ýetirilýän ýer**: ABŞ, beýleki dünýä ýurtlary.

### 4. ****WannaCry Ransomware (2017)****

* **Näme edilendir?**: WannaCry, şifrlenmedik we öňki Windows ulgamyny ulanýan IoT enjamlar üçin ýagny şifrlenmedik we gowşak ulgamlara görnüşde girýär we global derejesinde şifrlemäge sebäp boldy.
* **Zyyanlar**:
  + **Maglumatlaryň ýitirilmegi**: Ransomware, şifrlenen maglumatlary almaýar, bu enjamda maglumatlary ýitirýär.
  + **Maliýe ýitgileri**: Kompaniýalar, guramalar üçin resminamalary, ähli maglumatlary we maliýe hyzmatlary çalyşylýar.
* **Ýerine ýetirilýän ýer**: Dünýäniň dürli ýerlerinde, hususan-da, Britaniýa, Fransiýa, Russiýa, Hindistan ýaly ýurtlarda.

### 5. ****Brute Force Atakasy****

* **Näme edilendir?**: Brute force atakasy, IoT enjamynyň şifrini ýa-da login maglumatlaryny tapmak üçin ähli mümkin bolan kombinasiýalary synap görýär. Bu atakalar, enjamyň gowşak şifrlendirilmiş parollaryny tapmak üçin amala aşyrylýar.
* **Zyyanlar**:
  + **Enjamyň basyp alynmagy**: Parollar tapylandan soň, enjam ulanyjynyň hasaplaryna girip, maglumatlary alyp bilýär.
  + **Şahsy maglumatlaryň ýitirilmegi**: Şahsy maglumatlar, kamera, router, öý awtomatlaşdyrylyşy ýaly enjamlar ulanylar.
* **Ýerine ýetirilýän ýer**: Dünýäniň ähli ýerlerinde, esasanam ulanyjylaryň gowşak parollary ulanýan ýerlerde.

### 6. ****Man-in-the-Middle (MITM) Atakasy****

* **Näme edilendir?**: MITM hüjümi, iki enjam arasynda aragatnaşygyň gözegçilik edilmegini aňladýar. Hakerler, şifrlenmedik maglumatlary okap ýa-da üýtgedip bilýärler.
* **Zyyanlar**:
  + **Maglumatlaryň aşkar edilmegi**: Şahsy we gizlin maglumatlar üýtgedilip ýa-da okalyp bilner.
  + **Enjamyň we maglumatlaryň howpsuzlygynyň bozulmagy**.
* **Ýerine ýetirilýän ýer**: Dünýäniň dürli ýerlerinde, esasanam şifrlenmedik Wi-Fi jaýlarynda.

### 7. ****SQL Injection****

* **Näme edilendir?**: SQL injection atakasy, IoT enjamlarynyň arka plandaky maglumat bazasyna SQL kodlary ýazylyp, ulanyjylaryň maglumatlaryna ýa-da ulgam resminamalaryna girmäge mümkinçilik berýär.
* **Zyyanlar**:
  + **Maglumatlaryň çalynmagy**: Hakerler, maglumat bazasyna girip, şahsy maglumatlary ýa-da iş maglumatlaryny alyp bilýärler.
  + **Ulgamyň işiniň bozulmagy**: Ulgamda SQL soraglaryny üýtgedip, tizligi ýa-da hyzmaty bozulýar.
* **Ýerine ýetirilýän ýer**: Ulgamlar we IoT enjamlary web aragatnaşyk protokollary arkaly.

### 8. ****Zero-Day Atakasy****

* **Näme edilendir?**: Zero-day atakasy, öňünden kesgitlenmedik gowşaklykdan peýdalanyp, enjamyň howpsuzlygyny bozup, ýalňyş programmalary girizip, enjamy basyp alýar.
* **Zyyanlar**:
  + **Enjamyň işini bozmak**: Enjamlar, onuň ykjam işlerini bozmak ýa-da özbaşdak hereket etmek üçin ulanylyp bilner.
  + **Enjamyň fiziki zeperleri**.
* **Ýerine ýetirilýän ýer**: Dünyada her bir täze gowşaklyk ýüze çykan ýerlerde.

### 9. ****Cross-Site Scripting (XSS)****

* **Näme edilendir?**: XSS atakasy, web interfeýsine zäherli kod ýerleşdirip, ulanyjylara seredilen sahypa ýa-da çemeleşmeler arkaly hakerleriň enjamy basyp almagy üçin işleýär.
* **Zyyanlar**:
  + **Şahsy maglumatlaryň alnanlygy**: Şahsy maglumatlar, loginler we şifrler çalyşylýar.
* **Ýerine ýetirilýän ýer**: IoT enjamlarynyň web interfeýsi ulanylan ýerlerde.

### 10. ****Botnet Atakasy****

* **Näme edilendir?**: Botnetler, IoT enjamlarynyň köpüsini bir arada gurup, zäherli maksatlar üçin ulanylan botneteri düzýär.
* **Zyyanlar**:
  + **Enjamlaryň we ulgamlaryň işiniň bozulmagy**: DDoS hüjümleri we enjamlaryň basyp alynmagy.
* **Ýerine ýetirilýän ýer**: Dünyada IoT enjamlarynyň köpçülikleýin ulanylandygy ýerlerde.

Bu atakalar we zyyanlar, IoT enjamlarynyň gowşaklyklarını we howpsuzlyk gowşaklyklaryny görkezýär. Howpsuzlyk çärelerine, şifrlenmäge, täzelenmelere we parol howpsuzlygyna üns bermek, IoT ulgamlarynyň howpsuzlygyny güýçlendirmäge kömek eder.

Количество IoT-устройств — роутеров, камер, NAS-хранилищ, компонентов «умного дома» — растет с каждым годом. Портал Statista [прогнозирует](https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/), что к 2030 году оно превысит 29 миллиардов. С увеличением числа подключенных устройств растет и необходимость их защищать. Первые массовые атаки на IoT-устройства с использованием вредоносного ПО [были зафиксированы](https://securelist.com/heads-of-the-hydra-malware-for-network-devices/36396/#hydra-an-open-source-prototype-of-router-malware) еще в 2008 году, и с тех пор подобных атак становится только больше. Мы проанализировали ландшафт угроз, актуальных для IoT-устройств в 2023 году, а также товары и услуги в даркнете, связанные со взломом подключенных устройств. В этой статье мы приводим основные результаты нашего исследования.

## Векторы атаки

Существует два основных пути заражения IoT-устройств: перебор слабых паролей и эксплуатация уязвимостей в сетевых сервисах.

В первом случае наиболее распространенным методом является перебор паролей к сервисам, использующим протокол Telnet — крайне популярный в IoT-среде нешифрованный текстовый протокол. Успешный перебор пароля позволяет киберпреступникам выполнять произвольные команды на устройстве и запускать на нем вредоносное ПО. Аналогичные результаты дает и перебор паролей к сервисам, использующим SSH — более современный протокол, предусматривающий шифрование трафика. Однако атака на SSH требует больших ресурсов, а доступных из интернета сервисов меньше, чем в случае с Telnet.

За первую половину 2023 года 97,91% попыток перебора паролей, зафиксированных нашими ханипотами, были связаны с протоколом Telnet и 2,09% — с SSH. Больше всего инфицированных устройств, совершавших эти атаки, находилось в Китае, Индии и США, а по количеству атак лидируют Китай, Пакистан и Россия.

**TOP 10 стран и территорий, в которых находилось большинство устройств, атаковавших ханипоты «Лаборатории Касперского», H1 2023 (**[***скачать***](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/20183526/02-ru-iot-charts.png)**)**

**TOP 10 стран и территорий — источников атак на ханипоты «Лаборатории Касперского», H1 2023 (**[***скачать***](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/20183617/01-ru-iot-charts.png)**)**

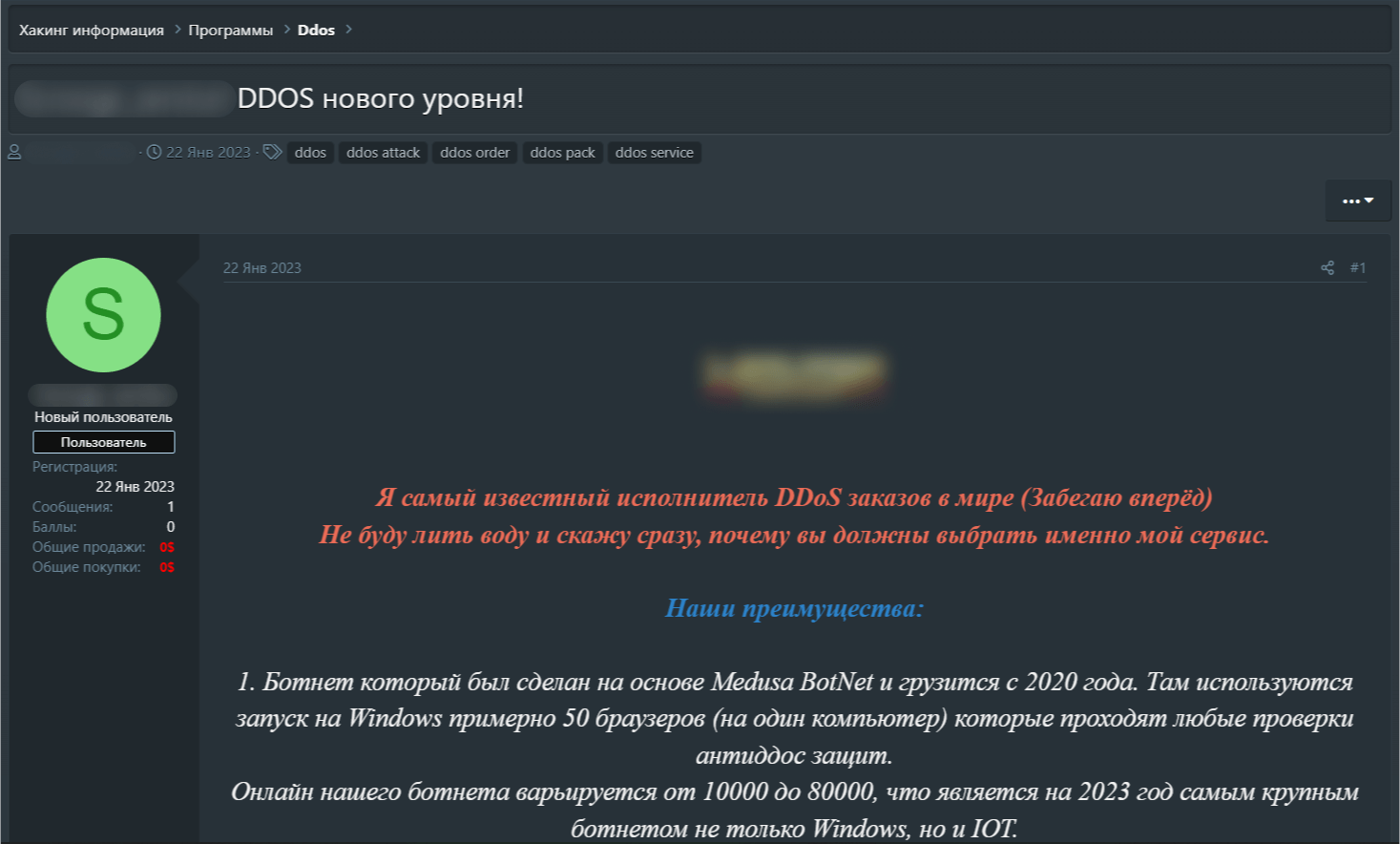
Атаки с перебором паролей довольно распространены, поскольку часто Telnet- и SSH-сервисы на IoT-устройствах защищены широко известными паролями по умолчанию, которые пользователи, как правило, не меняют. Более того, в некоторых случаях на IoT-устройствах установлены несменяемые главные пароли, заданные производителем.

К компрометации устройства также могут приводить и уязвимости работающих на нем сервисов. Самый распространенный тип уязвимостей, которые эксплуатируют злоумышленники, — внедрение вредоносных команд при выполнении запросов к веб-интерфейсу. Ущерб от таких атак может быть весьма значительным, как, например, в случае с [уязвимостью реализации протокола TR-064](https://securelist.com/new-wave-of-mirai-attacking-home-routers/76791/), который интернет-провайдеры используют для автоматической настройки устройства в локальной сети. Уязвимость позволила злоумышленникам отправлять пакеты TR-064 без аутентификации, чем они и воспользовались для распространения зловреда Mirai.

Вне зависимости от метода компрометации, атаковать IoT-устройства могут как злоумышленники со своих серверов, так и сами зловреды за счет так называемого механизма самораспространения — способности вредоносных файлов самостоятельно обнаруживать уязвимые устройства в интернете и устанавливать на них свою копию множеством различных методов. Во втором случае атака может исходить и со стороны зараженного ранее IoT-устройства.

## Услуги в даркнете: DDoS-атаки, ботнеты и уязвимости нулевого дня в IoT

Среди услуг в даркнете, связанных с IoT, в первую очередь стоит рассмотреть DDoS. Ботнеты, построенные на основе IoT-устройств и использующиеся для проведения распределенных DoS-атак, стали чаще встречаться в объявлениях на различных теневых форумах и пользоваться спросом у злоумышленников.

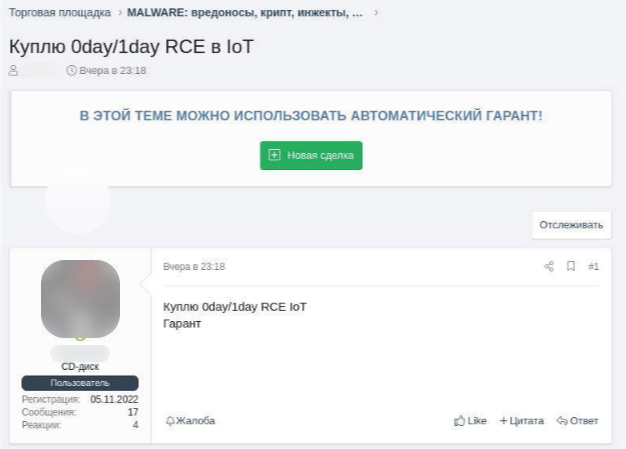
[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21041913/iot-report-2023-01.png)

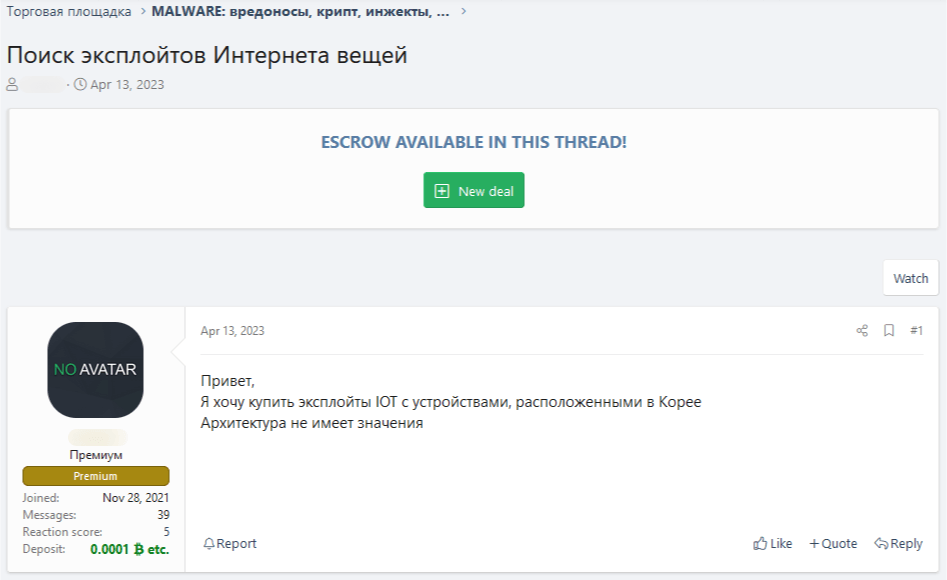
Всего за первую половину 2023 года аналитики сервиса Kaspersky Digital Footprint Intelligence обнаружили более 700 объявлений об услугах по проведению DDoS-атак на различных форумах в даркнете.

**Распределение количества публикаций, связанных с услугами по проведению DDoS-атак, по месяцам, H1 2023 (**[***скачать***](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/20183647/03-ru-iot-charts.png)**)**

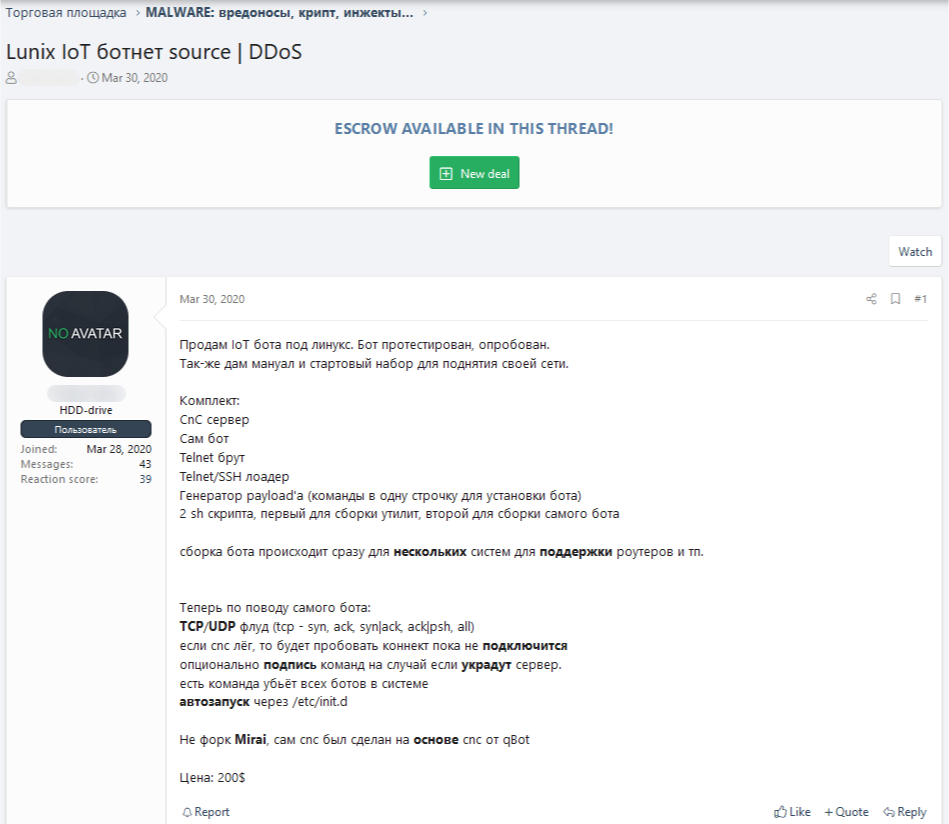
Цена такой услуги зависит от множества факторов, влияющих на сложность атаки, среди которых: наличие у жертвы защиты от DDoS, наличие капчи и JavaScript-верификации. В общей сложности стоимость атаки варьируется от $20 за сутки до $10 000 за месяц, а средняя цена для изученных объявлений составила $63,5 за сутки или $1350 за месяц.

Покупают в даркнете и услуги по взлому IoT. В частности, злоумышленники ищут эксплойты к уязвимостям нулевого дня в устройствах интернета вещей.

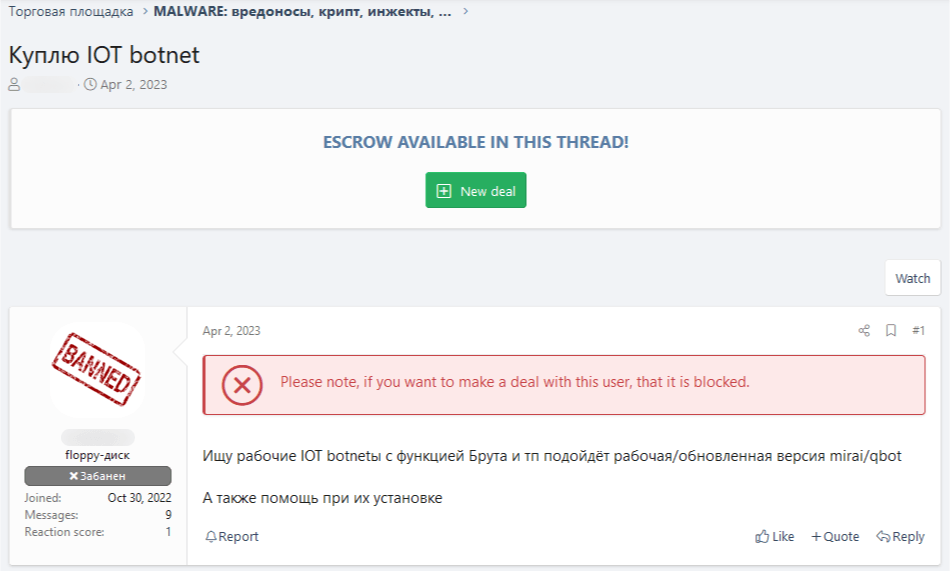
[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042000/iot-report-2023-02.png)

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042031/iot-report-2023-03.png)

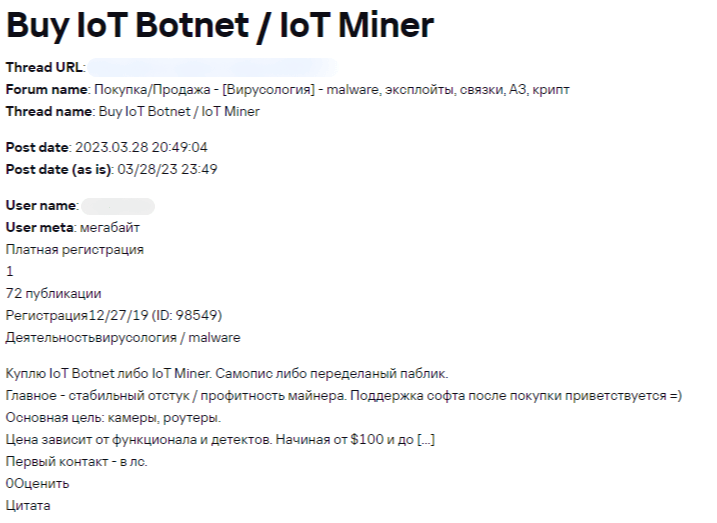
Также на теневых форумах можно найти предложения о продаже и покупке вредоносного ПО для IoT. Иногда к собственно зловреду прилагается инфраструктура и дополнительные утилиты. Так, на скриншоте ниже продавец предлагает самописный DDoS-бот с C2-сервером и ПО для загрузки зловреда через Telnet или SSH:

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042054/iot-report-2023-04.png)

Ниже скриншот объявления, в котором злоумышленник ищет не только вредоносное ПО, но и помощь в его установке.

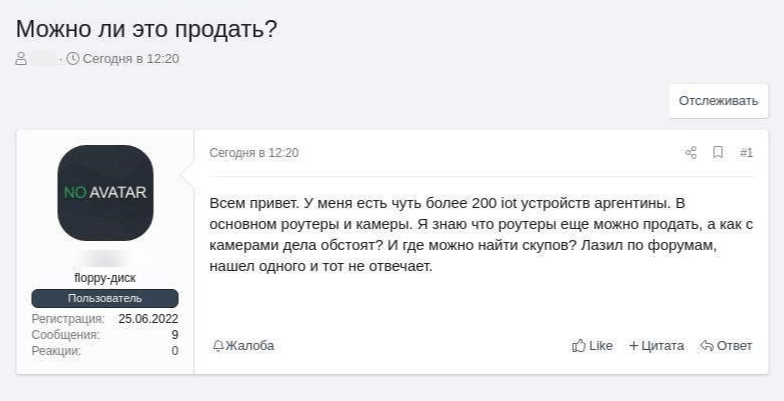
[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042121/iot-report-2023-05.png)

В некоторых случаях злоумышленники обозначают, для каких типов IoT-устройств они ищут или продают зловреды.

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042146/iot-report-2023-06.png)

*Скриншот объявления из потока Kaspersky Threat Intelligence Portal*

Иногда в даркнете продают и сети уже зараженных устройств, хотя такие объявления не очень распространены. Например, пользователь на скриншоте ниже ищет покупателя для ботнета из 200 роутеров и камер, расположенных в Аргентине.

[](https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2023/09/21042447/iot-report-2023-071.png)

## Цели и виды вредоносного ПО, атакующего IoT

Злоумышленники, заражающие IoT-устройства, могут преследовать разные цели. В частности, они могут в дальнейшем использовать зараженную технику как инструмент для проведения кибератак, маскировки вредоносного трафика, использовать мощности устройства для майнинга или требовать выкуп за возвращение доступа к нему. При этом некоторые злоумышленники атакуют любые IoT-устройства, а другие — только технику определенного типа, способную выполнять интересующие их задачи. Ниже мы приводим виды вредоносного ПО для IoT в зависимости от его цели.

### DDoS-ботнеты

Наиболее распространенный вид вредоносного ПО для IoT-устройств — троянские программы, перехватывающие контроль над устройством для ведения DoS-атак на различные сервисы. Для DDoS-зловредов нет разницы, какие устройства атаковать. Функциональностью, которая интересует злоумышленников, — способностью отправлять запросы по сети — обладают все. Значительная часть подобных зловредов — это модификации кода Mirai, но существует и множество других семейств, различающихся методами распространения и закрепления на устройстве.

Так, вредоносное ПО RapperBot, хотя и позаимствовало некоторые части кода Mirai, по большей части состоит из уникального кода. Оно способно на [умный перебор паролей](https://securelist.ru/crimeware-report-uncommon-infection-methods-2/107293/#rapperbot-171-umnyj-podbor-parolej-187), основанный на анализе получаемого от Telnet-сервиса первого сообщения с запросом аутентификационных данных. По этому сообщению зловред может распознать тип устройства и перебирать только пароли к устройствам этого типа, что значительно повышает эффективность его самораспространения.

### Программы-вымогатели

В отличие от DDoS-зловредов, вымогатели атакуют преимущественно IoT-устройства, на которых есть пользовательские данные — NAS-хранилища. Одним из ярких примеров IoT-шифровальщика является DeadBolt, [поразивший тысячи устройств QNAP NAS](https://arstechnica.com/information-technology/2022/09/new-wave-of-data-destroying-ransomware-attacks-hits-qnap-nas-devices/) в 2022 году. Для атаки использовалась уязвимость [CVE-2022-27593](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27593), позволяющая злоумышленникам модифицировать системные файлы на устройстве. В результате пользовательские файлы оказались зашифрованы, а интерфейс устройства заблокировало сообщение о том, что для восстановления данных нужно заплатить выкуп в размере 0.03 BTC. Производитель выпустил обновление, закрывающее уязвимость, но подобные атаки все еще остаются актуальными.

### Майнеры

Несмотря на относительную неэффективность майнинга на IoT-устройствах, связанную с их низкой вычислительной мощностью, злоумышленники предпринимали попытки [добывать криптовалюту Bitcoin](https://securityintelligence.com/mirai-iot-botnet-mining-for-bitcoins/) в ходе кампаний Mirai. Однако эти попытки не получили широкого распространения.

### DNS changer

Атакующие могут использовать скомпрометированные IoT-устройства и для атаки на подключающихся к ним пользователей. Так, в 2022 году в ходе вредоносной кампании Roaming Mantis (также известной как Shaoye) злоумышленники [распространяли](https://securelist.com/roaming-mantis-dns-changer-in-malicious-mobile-app/108464/) приложение для Android, одной из функций которого была смена настроек DNS на Wi-Fi-роутерах через интерфейс администрирования. Зловред получал доступ к роутеру, если на нем использовались учетные данные по умолчанию, например admin:admin. На подходящем устройстве он менял конфигурацию так, чтобы роутер использовал сервер DNS, подконтрольный злоумышленнику. Этот сервер перенаправлял всех, кто подключался к роутеру, на ресурс, определяющий ОС клиента: если устройство работало под управлением Android, ресурс раздавал вредоносные файлы APK, а пользователей iOS перенаправлял на фишинговые страницы.

### Прокси-боты

Также довольно широко распространено использование зараженных устройств в качестве прокси-серверов — промежуточных узлов в сети, перенаправляющих трафик злоумышленника через себя, таким образом затрудняя его отслеживание. Чаще всего такие прокси-серверы используются для рассылки спама, обхода antifraud-систем и совершения различных сетевых атак.

## Вредоносное ПО для IoT: конкуренция и персистентность

Одна из основных особенностей вредоносного ПО для IoT — существование множества различных семейств, основанных на обнаруженном в 2016 году зловреде Mirai, исходный код которого был опубликован на одном из подпольных форумов. Это привело к быстрому развитию сотен модификаций, различающихся способами ведения DoS-атак, словарями для перебора учетных данных и выбором уязвимостей для самораспространения.

Большое количество игроков, в свою очередь, привело к жесткой конкуренции среди киберпреступников, причем не только специализирующихся на DDoS, но и в целом нацеленных на интернет вещей. Поэтому IoT-зловреды постепенно начали включать в себя функции для «нейтрализации» конкурентов непосредственно на зараженном устройстве и предотвращения его повторного заражения.

Наиболее популярная среди злоумышленников тактика закрепления доступа за собой — добавление правил сетевого экрана, блокирующих попытки подключения к устройству; несколько реже используется отключение сервисов удаленного управления устройством. Для борьбы с конкурентами, уже присутствующими на устройстве, обычно применяется ряд методов обнаружения, например проверка имен процессов, используемых ими портов и анализ памяти на «вредоносные» паттерны. Если IoT-зловред что-то обнаружит, он завершает чужие процессы и удаляет чужие файлы. Так злоумышленники борются друг с другом за контроль над устройством.

## Прочие угрозы, связанные с небезопасностью устройств IoT

Как мы видели из объявлений о покупке-продаже доступа к скомпрометированным IoT-устройствам, среди типов устройств, интересующих злоумышленников, встречаются подключенные к интернету видеокамеры. Способы монетизации доступа к камере могут быть разными. Ее могут использовать не только как «компьютер» (например, для майнинга криптовалюты или размещения вредоносного ПО для организации DDoS-атак) или «маршрутизатор» («прокси» или VPN для анонимизации различной вредоносной деятельности), но и (внезапно!) по прямому назначению.

Показателен [недавний инцидент](https://t.me/moscowmi/14898) с жительницей московской области, обнаружившей на китайских вебсайтах материалы приватного характера, сделанные с домашней видеокамеры, которую она приобрела на AliExpress для наблюдения за собакой.

Исследователь безопасности Пол Маррапезе (Paul Marrapese) изучил пользовательский сегмент видеокамер и выяснил, что проблемы информационной безопасности в них присутствуют и, к сожалению, производители устройств их далеко не всегда исправляют. Например, он обнаружил  критические уязвимости в протоколах и прошивках некоторых видеокамер, причем [один из вендоров так и не вышел на связь для устранения уязвимостей](https://hacked.camera/cves/).

Кроме того, хочется отметить, что часто производители подобных видеокамер используют различные реализации P2P-протоколов (peer-to-peer-, пиринговых). Такие, например, как Shenzhen Yunni iLnkP2P и CS2 Network P2P, которые используются на более чем пятидесяти миллионах устройств. Эти реализации, в свою очередь, имеют слабое шифрование трафика или не шифруют его вовсе, что дает злоумышленнику возможность совершить атаку типа MitM (Man-in the-Middle) — прослушивать трафик устройства, чтобы узнать учетные данные пользователя или перенаправить на свои ресурсы видеопоток, идущий с камеры.

Согласно [исследованию коллег из Trend Micro](https://www.trendmicro.com/vinfo/ie/security/news/internet-of-things/exposed-video-streams-how-hackers-abuse-surveillance-cameras), подглядывание за жизнью владельцев видеокамер — далеко не редкость. При этом стоит помнить, что помимо собственно камер инструментом шпионажа могут стать многие другие IoT-устройства, которые, несмотря на то что их основное назначение не связано с видеонаблюдением, также оснащены камерой. В частности, возможность записывать аудио и видео в режиме реального времени есть у большинства умных кормушек для питомцев. Спрос на них растет, число моделей множится, заполняя новый сегмент рынка, однако вендоры не всегда уделяют должное внимание их защите. Так, [исследование кормушки](https://securelist.com/smart-pet-feeder-vulnerabilities/110028/) из популярной линейки показало целый ворох уязвимостей и проблем безопасности, эксплуатация которых превращает устройство в инструмент подглядывания за хозяевами питомца и открывает другие возможности для злоумышленников.

Другой тип IoT-устройств, требующих особого внимания к вопросам безопасности, — умные устройства для детей. К сожалению, не все вендоры серьезно подходят к защите таких устройств. Впервые мы столкнулись с проблемой их небезопасности несколько лет назад, когда один из производителей умных детских часов заказал у нас [сервис по исследованию зрелости безопасности продукта](https://ics-cert.kaspersky.com/services/) по методологии [IoT Security Maturity Model от Industry IoT Сonsortium](https://www.iiconsortium.org/smm/). Аттестацию вендор тогда провалил, и сертификата мы не выдали — проблемы безопасности в продукте превращали его, по сути, в устройство слежения за ребенком и за всем(и), что (кто) находится в его окружении.

Проблема недостаточной защищенности IoT-устройств характерна не только для пользовательского рынка. Системы промышленного IoT могут также содержать тривиальные уязвимости, а рекомендованные вендором настройки — быть небезопасными.

Распространенной ошибкой конфигурации промышленных устройств являются пароли по умолчанию. Так, например, они вместе с весьма небезопасными рекомендациями по подключению и настройке были [приведены в документации](https://ics-cert.kaspersky.ru/publications/blog/2022/03/30/uyazvimosti-v-reshenii-tekon-avtomatika-bez-otvetstvennoe-raskrytie-i-masshtab-bedstviya/) производителя медиаконвертеров  для подключения лифтового оборудования к системам мониторинга в диспетчерских. Кроме того, наши исследователи обнаружили в устройствах уязвимости, эксплуатация которых доступна даже не слишком квалифицированным злоумышленникам и позволяет им получить полный контроль над конвертером. Небезопасные настройки из рекомендаций впоследствии убрали. Однако производитель устройств, вначале продемонстрировавший оперативность в устранении проблем безопасности, растерял по дороге всю ответственность, и многие из обнаруженных нами уязвимостей по сей день остаются неисправленными — спустя более года после того, как мы предоставили вендору информацию о них.

Из приведенных выше примеров может сложиться впечатление, что мы считаем все устройства IoT небезопасными, а их производителей — пренебрегающими культурой безопасной разработки. Однако это не так. Например, компания Bosch успешно [получила наш сертификат зрелости безопасности](https://ics-cert.kaspersky.com/smm-assessment/?item=bosch-ip-video-surveillance-camera-platforms) для умной видеокамеры, предназначенной для использования на промышленных предприятиях. Нам бы очень хотелось, чтобы как можно больше вендоров IoT-устройств, в том числе систем промышленного IoT, включали кибербезопасность своих продуктов в число первых приоритетов.

## Заключение

IoT-устройства интересуют злоумышленников по целому ряду причин: их можно использовать для DDoS-атак, перенаправлять через них трафик или подсматривать за владельцами с помощью встроенных видеокамер. NAS-хранилища также могут быть целью вымогателей, а роутеры привлекательны для злоумышленников, нацеленных на подключенные к ним устройства, например на мобильные устройства в общественной Wi-Fi-сети или на устройства локальной сети жертвы.

Злоумышленники непрерывно атакуют IoT и предлагают в даркнете услуги, связанные с такими атаками. Тем не менее большинство подключенных устройств, в том числе в промышленной среде, по-прежнему остается легкой добычей: для подключения используются пароли по умолчанию, в устройствах находят уязвимости, не все из которых получают патчи от производителя. Вендорам IoT-устройств, как домашних, так и промышленных, следует ответственно подходить к безопасности своей продукции и внедрять механизмы защиты от кибератак на стадии разработки. В частности, мы рекомендуем отказаться от практики использования паролей по умолчанию и генерировать уникальные пароли для каждого конкретного устройства. Также следует регулярно выпускать патчи к обнаруженным уязвимостям.

о есть по сути это экосистема устройств и технологий, подключенных через Интернет, которые постоянно собирают и передают данные. Часто к названию таких устройств добавляют приставку смарт или умный.

На первый взгляд, определение выглядит как обычная сеть. Однако ее специфика заключается в том, что в такой сети нет пользователей, сервисов, баз данных. То есть, принципиально – это изолированные сегменты объединенные через интернет устройств куда «не ступает нога человека».

IoT является очень удобным и полезным набором технологий, что значительно упрощает как нашу повседневную жизнь, так и работу организаций. Однако, к сожалению, идеальных технологий просто нет. Несмотря на безумную популярность и удобство устройств IoT, они имеют свои недостатки. Речь идет о наличии уязвимостей, которые трудно определить и отсутствие стандартизации. Помним, что IoT сети – это комплексы, где крайне редко появляется человек, соответственно – некому отслеживать нетипичную ситуацию и вирусы.

Злоумышленники в такой «не освещенной сети» могут расти и преуспевать очень долго не замеченными. Каждое устройство IoT является потенциально уязвимой точкой входа в сеть и бизнес-процессы. Поэтому такие сети могут стать (и становятся) первым этапом больших взломов, особенно если атака таргетирована именно на вашу организацию.

С развитием технологий, кибербезопасность устройств становится все более критическим вопросом. Особенно это становится очевидным в контексте Интернета вещей, поскольку количество устройств, которые могут получать и отправлять конфиденциальные данные ежедневно растет. Внедрение и обновление мер безопасности устройств должно стать приоритетом на ближайшие годы для технологии IoT.

## Почему важно защищать устройства IoT?

Защита устройств Интернета вещей является жизненно важным компонентом безопасности современной сети в организациях. Даже такие, казалось бы, невинные устройства, как, к примеру, обыкновенные датчики света, могут создавать опасности для безопасности. ИТ-команды должны включать эти риски в свои протоколы кибербезопасности и работать над сведением их к минимуму.

Без надлежащих практик по безопасности IoT, компании могут столкнуться с новыми угрозами, поступающими из киберпространства. Например, злоумышленники, нацеленные на умные устройства, могут получить доступ к критическим ресурсам компании далеко за пределами их начальной точки входа в сеть (из-за того, что уязвимые умные устройства подключены к ним). Это позволит им собирать конфиденциальные данные или устраивать утомительные для системы кибератаки.

Риски IoT действительно легко не заметить, если не использовать предназначенные для этого инструменты. Иногда специалисты по информационной безопасности пренебрегают инвентаризацией конечных точек, поэтому легко можно пропустить потенциально уязвимое к атакам устройство, не уделив ему достаточно внимания. Сегодня существуют программные продукты для проведения инвентаризации и мониторинга всех подключенных IoT девайсов. Такой тип решений по безопасности значительно снижает риски, анализируя всю поверхность потенциальных атак.

## Распространенные атаки на IoT

Чтобы предотвратить атаки на устройства IoT, прежде всего нужно знать, какие распространенные виды атак могут использовать киберпреступники для достижения своих целей.:

* **DDoS-атака:**происходит когда ботнет – зараженная сеть компьютеров – непрерывно посылает огромное количество запросов в систему. Аномально высокая активность может привести к значительным задержкам в работе системы или вообще к ее остановке. Удачно скорректированная и настроенная DDoS-атака может вызвать системную ошибку компонента безопасности, скрывая реальные вредные действия. Более того, зараженные устройства IoT также могут стать частью ботнета и помогать злоумышленникам проводить еще более разрушительные атаки внутри локальной сети, у которой обычно больше доверия у систем информационной безопасности.
* **Эксплойт программного обеспечения:**многие киберпреступники используют уже известные уязвимости в программной части устройства для проведения атаки. Разработчики обычно закрывают найденные «дыры» безопасности в обновлениях. Однако далеко не всегда свежие версии ПО вовремя загружаются на устройстве. Именно это делает их уязвимыми к атакам с использованием эксплойтов. Дополнительной угрозой является то, что далеко не все производители устройств информируют своих пользователей о реальном технологическом стеке ПО устройства, мотивируясь рыночными стимулами (использование определенной библиотеки, которая в открытом доступе может быть конкурентным преимуществом, если другие игроки рынка не догадались ее использовать).
* **МІТМ-атака (атака посредника):**хакеры могут перехватить сетевой трафик (встав посреди канала передачи между устройством отправителем и устройством получателем) и получить учетные данные или конфиденциальную информацию, которую устройства IoT передают через корпоративные сети. Из-за того, что многие смарт-устройства обычно даже не зашифрованы, злоумышленнику будет очень легко использовать полученные данные для несанкционированного доступа в систему.
* **Физическое вмешательство:** простого подключения киберпреступником USB флешки с вредоносным кодом, к внешнему устройству IoT может быть достаточно, чтобы распространить вредоносное программное обеспечение через сеть и шпионить по проходящим в ней коммуникациям.
* **Брутфорс атаки:**тот факт, что в компаниях обычно не уделяется достаточно внимания парольной безопасности устройств IoT, делает их уязвимыми к потенциальным атакам грубой силой или «Брутфорс». Часто пароли устройств IoT остаются неизменными после установки просто используя базовый пароль, что позволяет злоумышленникам очень просто их подбирать.
* **Перехват прошивки:**если обновление микропрограммы устройства не было криптографически подписано или прошивка передается по не защищенному каналу связи – это позволяет злоумышленникам перехватить ее и загружать вредоносное ПО на устройстве под видом апдейтов. Также с помощью украденной прошивки у киберпреступников появляется возможность получить учетные данные устройства. Используя учетные данные, они могут получить доступ к корпоративным сетям или другим системам, хранящим конфиденциальную информацию. Таким образом атака на, казалось бы, невинное устройство может превратиться в полномасштабную утечку данных.

## Защита устройств IoT

Из вышеупомянутых векторов атак на IoT можно заключить, что основные компоненты систем Интернета вещей достаточно уязвимы к атакам злоумышленников. Вне зависимости от масштаба и типа среды, в которую встраивается система IoT, безопасность должна рассматриваться еще на этапе проектирования, чтобы улучшить ее интегрирование. Особым вызовом для инженеров и специалистов информационной безопасности является то, что из-за технологических особенностей IoT не разрешается установить агент для проверки наличия заражений или уязвимостей.

Вот несколько основных рекомендаций, чтобы предотвратить кибератаки на устройстве и в целом уменьшить риски для безопасности компании:

## 1. Управление поверхностью атаки, инвентаризация и мониторинг всех устройств

При планировании защиты IoT одной из главных задач должно быть создание карты подключенных устройств для их инвентаризации. Команды безопасности должны знать точное количество используемых устройств, а также идентификаторы производителей, серийные номера, версии оборудования и прошивки. Мониторинг, анализ и отчетность в режиме реального времени крайне важны для организаций, чтобы иметь возможность управлять рисками Интернета вещей. Однако традиционные решения безопасности конечных точек обычно используют технологию так называемых программных агентов, не подходящих для устройств IoT. К счастью существуют лучшие современные подходы – безагентные решения (например [DeviceTotal](https://corewin.ua/ru/security/arcusteam/)) мониторинга поверхности атаки. Они обеспечивают оценку уровня риска в режиме реального времени, непрерывно анализируя поведение и состояние всех подключенных устройств Интернета к вещам. Некоторые решения такого плана даже позволяют управлять поверхностью прекогнитивных атак, учитывая риски потенциальных «атак нулевого дня». Эти инструменты безопасности позволяют организациям использовать все преимущества технологии IoT, исправив ее основной недостаток – недостаточный уровень безопасности.

## 2. Сегментация сети

В случае успешной кибератаки злоумышленник может получить доступ ко всей сети организации. Сегментация предотвращает это, ограничивая поверхность атаки и минимизируя ущерб. Сегментация сети – это процесс разделения внутренней сети на несколько отдельных подсетей. Хотя сегменты могут время от времени общаться между собой, они обычно независимы и изолированы друг от друга. Этот метод позволяет сосредоточить больше внимания на отдельных частях сети, содержащих наиболее критические данные, для их усиленной защиты.

## 3. Установка надежных паролей для IoT

Многие устройства IoT поставляются со слабыми предварительно установленными паролями, которые очень легко подобрать. Как только IoT устройство впервые регистрируется в вашей сети, для начала, лучшей методикой будет изменить его предустановленный пароль на более сложный. Новый пароль должен быть устойчивым для подбора, уникальным для каждого защищенного устройства и соответствовать политикам управления паролями вашей команды по ИТ-безопасности.

## 4. Защита всех устройств IoT на физическом уровне

Физическая защита устройств имеет очень большое значение, поскольку девайсы, доступные извне, могут подвергнуться физическому вмешательству злоумышленников с целью получения несанкционированного доступа или загрузки в систему вредоносного ПО. Поэтому следует обеспечить надежное место дислокации устройства, чтобы к нему не было открытого доступа.

## 5. Своевременные обновления прошивок

Новые версии прошивок могут исправить существующие программные уязвимости устройства. Поэтому их регулярное обновление значительно улучшит общую безопасность IoT. Однако обновления также следует проверять на подделки, поскольку злоумышленники могут под видом обновления загрузить на устройство вредоносное программное обеспечение. Другая сторона обновлений – это уязвимости в официальных обновлениях. Нужно контролировать версионность и держать новейшую из безопасных версий прошивки, в этом помогут автоматизированные системы анализа прошивки устройств.

## Вывод

Выполнение, приведенных выше рекомендаций, поможет вам безопасно пользоваться устройствами IoT в вашей организации, используя их пользу в полную и при этом минимизировать риски, которые они могут создавать. Но следует помнить, что кибератаки постоянно развиваются и усложняются. Поэтому важно быть в курсе новых событий в киберпространстве и регулярно обновлять меры безопасности, используя [передовые решения для обеспечения мониторинга устройств](https://corewin.ua/ru/security/arcusteam/) и анализа поверхности атаки.

**IOT (Internet of Things) ulgamynyň esasy howplary we howply ýagdaýlar:**

IoT ulgamlar köp üstünlikleri getirýär, ýöne howpsuzlyk boýunça uly çökgünlikleri hem ýüze çykarýar. Esasy howplar şulardan ybarat:

### \*\*1. ****Botnet we DDoS howplary****

* **Näme?** Köp sanly IoT enjamlary (kamera, router, smart enjamlar) birleşdirilip, ululy howp ediji botnet döredilýär.
* **Netije?** Ululy trafik (DDoS) ýa-da maglumat ogurlanylyar.
* **Mysal:** **Mirai botnet** (2016) 600 Gbit/s trafik bilen DNS servisleri çökdirdi.

### \*\*2. ****Maglumat ogurlama (Data Breach)****

* **Näme?** Şifrelenmedik maglumatlar (wideo, sensor maglumatlary, şahsy maglumatlar) ogurlanýar.
* **Netije?** Şahsy maglumatlaryň sypdyrylmagy, şantaj we firma reputasiýasyna zyýan.
* **Mysal:** **Ring smart kameralary** (2020) – hackerlar kameradaky sahnalary gören.

### \*\*3. ****Ransomware (Fidýe howpy)****

* **Näme?** IoT enjamy blokirlenýär we açmak üçin töleg talap edilýär.
* **Netije?** Smart jaý ýa-da fabrik ulgamy işlemez ýagdaýa düşýär.
* **Mysal:** **Samsam ransomware** (2018) – smart binalary we IoT sensorlaryny basyp aldy.

### \*\*4. ****Fiziki howplar****

* **Näme?** Enjama fiziki giriş (USB, debug portlary) arkaly zyýan ýetirilýär.
* **Netije?** Enjam dolandyrylyar ýa-da maglumatlary öçürilýär.
* **Mysal:** **Smart howpsuzlyk kameralarynyň flash belgisi** üýtgedilip, zyýanly kod ýerleşdirildi.

### \*\*5. ****Man-in-the-Middle (MITM) howplary****

* **Näme?** IoT enjam bilen server arasyndaky aragatnaşyk gözegçilige alnyp, maglumat üýtgedilýär.
* **Netije?** Parollar, sensor maglumatlary ogurlanýar.
* **Mysal:** **Smart jaý termostatlaryna hüjüm** – temperaturany üýtgetmek üçin howp edijiler giriş edip bilýär.

### \*\*6. ****Zaharly Firmware / Malware****

* **Näme?** Enjamyň işleýş programmasy (firmware) üýtgedilip, arka gapy goýberilýär.
* **Netije?** Uzakdan dolandyrmak, botnet-e goşmak.
* **Mysal:** **VPNFilter malware** (2018) – routerlary infekirleşdirdi.

### \*\*7. ****Default Parollar we Zäweak Awtentifikasiýa****

* **Näme?** Enjamyň giriş paroly "admin:admin" ýa-da "12345" ýaly bolup, aňsatlyk bilen düşürilýär.
* **Netije?** Dolandyryş paneli ele geçirilýär.
* **Mysal:** **Mirai botnet** default parollary ulanýardy.

### ****IOT HOWPLARYNYŇ ÖŇÜNI ALMAK ÜÇIN NÄMELER ETMELI?****

✅ **Parollary üýtgetmek** – default logini ýok etmek.  
✅ **Firmware täzelenmeleri** – iň soňky howpsuzlyk ýamalaryny ýükläp almak.  
✅ **TLS/SSL ulanyp maglumatlary şifrlemek**.  
✅ **IoT enjamlary aýratyn tor bölüminde (VLAN) saklamak**.  
✅ **Fiziki girişi çäklendirmek** (USB portlaryny ýapmak).  
✅ **Network gözegçiligi (IDS/IPS)** – gerek däl aragatnaşygy ýapmak.