**参考消息网11月22日报道**据台湾中时电子报11月19日报道，未来10年，物联网将持续带动数字企业创新的商机，国际研究暨顾问机构Gartner最新公布2018年至2023年引领数字企业创新的十大物联网策略技术趋势。

**趋势一：人工智能（AI）**

Gartner预测2019年全球连网对象数量将达142亿，并在2021年将达到250亿，因此将产生极大量的数据。

Gartner进一步预估，2023年前人工智能的技术分野仍相当复杂，主要是因为许多IT厂商正重金投资人工智能技术，除各种人工智能技术并存外，新的服务及相关投资也不断产生。



11月10日，智能烹饪机器人在进行菜品烹制。当日，首家京东“X未来餐厅”在中新天津生态城正式开业。（新华社）

**趋势二：物联网的社会、法律与道德面向**

随着物联网普及，各种社会、法律与道德层面的相关问题愈来愈重要，包括欧盟《通用数据保护条例》（GDPR）的法规遵循、数据及演绎数据的拥有权、算法偏差、隐私权等。

**趋势三：信息经济学与数据中介（Data Broking）**

Gartner去年的物联网项目调查显示，35%的受访者正在销售或打算销售其产品与服务所搜集的数据，信息经济学理论将这种数据变现的作法，进一步视为应纳入公司账册的策略性商业资产。

至2023年，买卖物联网数据将成为许多物联网系统必要的一环。

**趋势四：从智能边缘转变为智能网格**

物联网领域发展趋势，正从中央及云端转变为边缘运算架构；然而物联网技术的发展并不会就此中断，因为层次分明的边缘架构将逐渐演变为一种较无系统的架构，由各式各样对象与服务以动态网格形式所组成。

这些网格虽然会使整体技术复杂性提升，但也将带来更弹性、更智能、更灵敏的物联网系统，并对IT基础架构、技能与来源带来影响。

**趋势五：物联网管理**

随着物联网范围持续扩展，大众对能确保物联网项目相关信息的创造、储存、使用及删除等行为皆符合标准的管理架构需求日渐提升。管理的范围不只包括装置稽核或韧体更新等单纯的技术性工作，也涵盖装置控管及其产生信息的相关使用等较复杂的问题。

**趋势六：传感器创新**

传感器市场将持续蓬勃发展至2023年，届时新的传感器将可侦测范围更广泛的状况与事件，而目前的传感器价格将变得更为亲民，或被重新包装以支持新应用。

此外，新运算法的问世，也会从现有的传感器技术上演绎出更多信息。



8月16日，一名小朋友在2018世界机器人大会上制作传感器模块。（新华社）

**趋势七：值得信赖的硬件与操作系统**

资安是企业在部署物联网系统最重要的技术考虑。这是因为物联网计划中使用的软件与硬件，其来源和性质通常不是企业所能掌控。

**趋势八：全新物联网使用者体验**

物联网使用者体验（UX）广泛涵盖了各种技术与设计技巧。其影响因素有四项：新的传感器、新的运算法、新的体验设计架构及情境，以及社交感知的体验。

由于大众与不具备屏幕及键盘的对象互动越趋频繁，若企业的使用者体验设计师希望创造能降低阻碍、提升黏着度，并且鼓励持续使用的绝佳使用者体验，就必须运用新的技术、接纳新的观点。



11月6日，参观者在首届中国国际进口博览会上的美国波音公司展台体验“驾驶”波音客机。（新华社）

**趋势九：硅芯片创新**

Gartner预测到了2023年，新的特殊用途芯片将降低运行DNN（深层神经网络）的电力消耗；具备最新边缘架构与嵌入式DNN功能的低功耗物联网终端装置也将诞生，以支持新的应用，例如将数据分析的技术整合在传感器内，或者在低成本的电池供电装置当中加入语音识别技术。



11月7日，华为技术有限公司代表在第五届世界互联网大会上介绍华为昇腾310芯片。（新华社）

**趋势十：针对物联网设计的全新无线网络技术**

物联网网络必须在一系列相互冲突的条件之间取得平衡，如端点成本、耗电量、带宽、延迟状况、联机密度、营运成本、服务质量以及涵盖范围。

没有单一网络技术能同时兼顾这么多条件，不过新的物联网网络技术将可为企业带来一些额外的选择与弹性，尤其是5G网络、新一代低轨道卫星，以及反向散射网络（backscatter networks）。

## **卡巴斯基：2018上半年物联网威胁新趋势**

[vitaminsecurity](https://www.freebuf.com/author/vitaminsecurity" \o "由 vitaminsecurity 发布)2018-10-04共**120289**人围观[安全报告](https://www.freebuf.com/articles/paper)

## **前言**

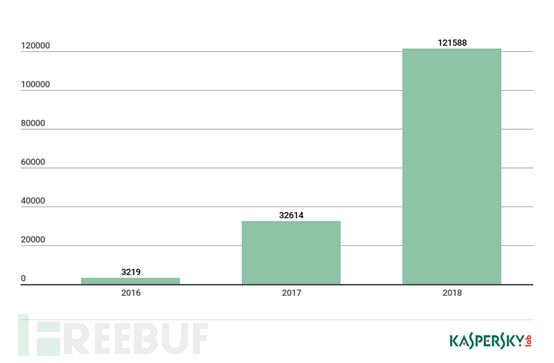
**网络犯罪分子对物联网设备的兴趣一直在增长：在 2018 上半年，我们观察到的 IoT 恶意软件样本的数量是 2017 年全年的三倍。而 2017 年的数字则是 2016 年的 10 倍。这一趋势对于未来而言不容乐观。**

因此在这里我们研究了以下三个问题：

网络犯罪分子感染智能设备的攻击向量；

哪些恶意软件被加载到用户的系统中；

最新的僵尸网络对设备所有者和受害者来说意味着什么。

[](https://image.3001.net/images/20180920/1537426116_5ba342c49dc02.png)

2016 年 – 2018 年，卡巴斯基实验室收集到的 IoT 恶意软件样本的数量

最流行的攻击和感染向量仍然是针对 Telnet 密码的暴力破解攻击。在 2018 年第二季度，我们的[蜜罐](https://encyclopedia.kaspersky.com/glossary/honeypot-glossary/)记录的此类攻击的数量是其它类型攻击数量总和的三倍还要多。

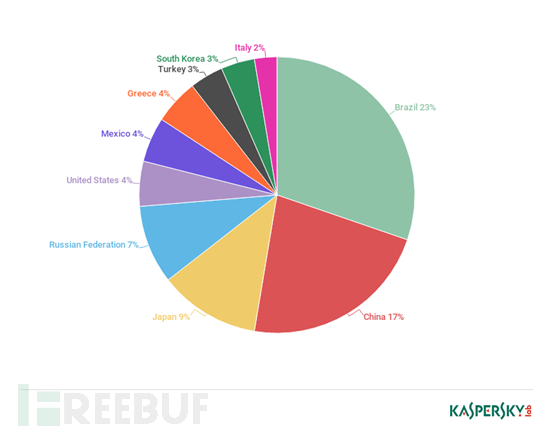
| ****目标服务**** | ****在所有攻击中的百分比%**** |
| --- | --- |
| ****Telnet**** | 75.40% |
| ****SSH**** | 11.59% |
| ****其它**** | 13.01% |

在将恶意软件下载到物联网设备上时，网络犯罪分子的首选项是[Mirai家族](https://securelist.com/is-mirai-really-as-black-as-its-being-painted/76954/)（ 20.9% ）。

| ****#**** | ****下载的恶意软件**** | ****在所有攻击中的百分比%**** |
| --- | --- | --- |
| ****1**** | Backdoor.Linux.Mirai.c | 15.97% |
| ****2**** | Trojan-Downloader.Linux.Hajime.a | 5.89% |
| ****3**** | Trojan-Downloader.Linux.NyaDrop.b | 3.34% |
| ****4**** | Backdoor.Linux.Mirai.b | 2.72% |
| ****5**** | Backdoor.Linux.Mirai.ba | 1.94% |
| ****6**** | Trojan-Downloader.Shell.Agent.p | 0.38% |
| ****7**** | Trojan-Downloader.Shell.Agent.as | 0.27% |
| ****8**** | Backdoor.Linux.Mirai.n | 0.27% |
| ****9**** | Backdoor.Linux.Gafgyt.ba | 0.24% |
| ****10**** | Backdoor.Linux.Gafgyt.af | 0.20% |

成功破解 Telnet 密码后下载到 IoT 设备上的恶意软件 Top10

以下是我们记录到的 Telnet 攻击最多的国家的 Top 10 ：

[](https://image.3001.net/images/20180920/1537426176_5ba343009055d.png)

2018 年第二季度，受感染设备数量的地理分布

如图所示， 2018 年第二季度发起 Telnet 攻击的 IP 地址（唯一）数量最多的国家是巴西（ 23% ），第二名是中国（ 17% ）。俄罗斯排名第四（ 7% ）。在整个 2018 年 1 月至 7 月期间，我们的 Telnet 蜜罐共记录到来自 86560 个 IP 地址（唯一）的超过 1200 万次攻击，并且从 27693 个 IP 地址（唯一）下载了恶意软件。

由于一些智能设备的所有者修改了默认的 Telnet 密码并使用复杂的密码，而许多小工具根本不支持这种协议，因此网络犯罪分子一直在寻找新的感染向量。这一情况还受到恶意软件开发者之间的竞争所推动（他们之间的竞争导致了暴力破解攻击效率越来越低）：一旦成功破解了 Telnet 密码，攻击者就会更改设备的密码并阻止对 Telnet 的访问。

僵尸网络 Reaper 就是一个使用“替代技术”的很好的例子，它在 2017 年底感染了约 200 万个 IoT 设备。该僵尸网络并没有采用 Telnet 暴力破解攻击，而是利用已知的软件漏洞进行传播：

[D-Link 850L路由器固件中的漏洞](https://blogs.securiteam.com/index.php/archives/3364)

[GoAhead网络摄像机中的漏洞](https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html)

[MVPower CCTV摄像机中的漏洞](https://www.pentestpartners.com/security-blog/pwning-cctv-cameras/)

[Netgear ReadyNASSurveillance中的漏洞](https://blogs.securiteam.com/index.php/archives/3409)

[Vacron NVR中的漏洞](https://blogs.securiteam.com/index.php/archives/3445)

[Netgear DGN设备中的漏洞](http://seclists.org/bugtraq/2013/Jun/8)

[Linksys E1500/E2500路由器中的漏洞](http://www.s3cur1ty.de/m1adv2013-004)

[D-Link DIR-600和DIR 300 – HW rev B1路由器中的漏洞](http://www.s3cur1ty.de/m1adv2013-003)

AVTech 设备中的漏洞

与暴力破解相比，这种传播方法具有以下优点：

能更快地感染设备；

对用户而言，打补丁远比修改密码或禁用服务要难得多。

尽管这种方法的实施难度更高，许多恶意软件作者已经开始青睐这种方法。很快就会出现利用智能设备软件中的已知漏洞的新木马。

## **一、新的攻击，旧的恶意软件**

为了观察恶意软件针对了哪些漏洞，我们分析了企图连接到我们蜜罐的不同端口的数据。下表是 2018 年第二季度的数据：

| ****服务**** | ****端口**** | ****所占比例%**** | ****攻击向量**** | ****恶意软件家族**** |
| --- | --- | --- | --- | --- |
| ****Telnet**** | 23, 2323 | 82.26% | 暴力破解 | Mirai, Gafgyt |
| ****SSH**** | 22 | 11.51% | 暴力破解 | Mirai, Gafgyt |
| ****Samba**** | 445 | 2.78% | 永恒之蓝, 永恒之红, CVE-2018-7445 | – |
| ****tr-069**** | 7547 | 0.77% | [TR-069实现中的RCE漏洞](https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/) | Mirai, Hajime |
| ****HTTP**** | 80 | 0.76% | 利用web服务器中的漏洞或破解管理控制台密码 | – |
| ****winbox (RouterOS)**** | 8291 | 0.71% | [针对RouterOS(MikroTik)的攻击中获得的凭据](https://xakep.ru/2018/03/29/hajime-hunts-mikrotik/)和[基于WinBox的攻击](https://threatpost.ru/mikrotik-patched-zero-day-vulnerability-in-record-time/25811/) | Hajime |
| ****Mikrotik http**** | 8080 | 0.23% | 版本低于6.38.5的MikroTik RouterOS中的远程代码执行漏洞 [Chimay-Red](https://github.com/BigNerd95/Chimay-Red) | Hajime |
| ****MSSQL**** | 1433 | 0.21% | 版本2000、2005、 2008中的任意代码执行漏洞；修改管理员密码；数据窃取 | – |
| ****GoAhead httpd**** | 81 | 0.16% | [GoAhead网络摄像机中的远程代码执行漏洞](http://blog.netlab.360.com/a-new-threat-an-iot-botnet-scanning-internet-on-port-81-en/) | Persirai, Gafgyt |
| ****Mikrotik http**** | 8081 | 0.15% | [Chimay-Red](https://github.com/BigNerd95/Chimay-Red) | Hajime |
| ****Etherium JSON-RPC**** | 8545 | 0.15% | [身份认证绕过漏洞（CVE-2017-12113）](https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0465) | – |
| ****RDP**** | 3389 | 0.12% | 暴力破解 | – |
| ****XionMai uc-httpd**** | 8000 | 0.09% | [一些中国制造的设备的XionMai uc-httpd 1.0.0中的缓冲区溢出漏洞（CVE-2018-10088）](https://www.bleepingcomputer.com/news/security/all-that-port-8000-traffic-this-week-yeah-thats-satori-looking-for-new-bots/) | Satori |
| ****MySQL**** | 3306 | 0.08% | 版本2000、2005、 2008中的任意代码执行漏洞；修改管理员密码；数据窃取 | – |

绝大多数攻击仍然是针对Telnet和SSH密码的暴力破解攻击。第三大最常见的攻击是针对SMB服务（文件远程访问服务）的攻击。我们还没有观察到针对该服务的IoT恶意软件。 无论如何，某些版本的SMB中包含严重的已知漏洞，如永恒之蓝（Windows）和永恒之红（Linux）。举个例子，臭名昭著的勒索软件 [WannaCry](https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/)和门罗币矿工 [EternalMiner](https://securelist.com/sambacry-is-coming/78674/)就利用了这些漏洞。

下表是 2018 年第二季度攻击我们蜜罐的受感染 IoT 设备的类型分布：

| ****设备**** | ****所占比例%**** |
| --- | --- |
| ****MikroTik**** | 37.23% |
| ****TP-Link**** | 9.07% |
| ****SonicWall**** | 3.74% |
| ****AV tech**** | 3.17% |
| ****Vigor**** | 3.15% |
| ****Ubiquiti**** | 2.80% |
| ****D-Link**** | 2.49% |
| ****Cisco**** | 1.40% |
| ****AirTies**** | 1.25% |
| ****Cyberoam**** | 1.13% |
| ****HikVision**** | 1.11% |
| ****ZTE**** | 0.88% |
| ****Miele**** | 0.68% |
| ****Unknown DVR**** | 31.91% |
|  |  |

我们可以看到，运行 RouterOS 的 MikroTik 设备在列表中一骑绝尘，其原因应该是 Chimay-Red 漏洞。有趣的是，列表中还包括 33 个美诺洗碗机（占攻击总数的 0.68% ）。它们很可能是通过其固件中的 PST10web 服务器漏洞 [CVE-2017-7240](https://nvd.nist.gov/vuln/detail/CVE-2017-7240)被感染的（该漏洞于 2017 年 3 月公开）。

### **端口7547**

针对端口 7547 上的远程设备管理服务（ [TR-069](https://en.wikipedia.org/wiki/TR-069) 协议）的攻击十分常见。根据 Shodan 的查询结果，全世界有超过 4000 万台设备的这个端口是打开的。这还是在该漏洞最近导致约 100 万德国电信路由器被感染，更不用说用于分发恶意软件家族 Mirai 和 Hajime 之后。

另一类攻击则是利用了运行 RouterOS 版本 6.38.4 之下的 MikroTik 路由器中的漏洞 [Chimay-Red](https://wikileaks.org/ciav7p1/cms/page_16384604.html)。在 2018 年 3 月，该攻击被积极用于分发 Hajime 。

### **网络摄像机**

网络犯罪分子也没有忽视网络摄像机。 2017 年 3 月研究人员在 GoAhead 设备的软件中发现了几个严重的漏洞。在相关信息被披露的一个月后，利用这些漏洞的 Gafgyt 和 Persirai 木马新变体出现了。仅在一周内，这些恶意程序就积极感染了 57000 个设备。

2018 年 6 月 1 日， XionMaiuc-httpd web 服务器中的漏洞（ CVE-2018-10088 ）的[相关PoC](https://encyclopedia.kaspersky.com/glossary/poc-proof-of-concept/)被公开。该产品被用于一些中国制造的智能设备之中（如 KKMoonDVRs ）。一天之内，针对这些设备的有记录的扫描尝试增至三倍。这一激增的罪魁祸首就是 Satori 木马，其以之前针对[GPON路由器](http://blog.netlab.360.com/gpon-exploit-in-the-wild-ii-satori-botnet-en/)的攻击而闻名。

## **二、终端用户面临的新恶意软件和威胁**

### **DDoS攻击**

与以前一样，物联网恶意软件的主要目的是进行 DDoS 攻击。受感染的智能设备成为僵尸网络的一部分，根据相关命令攻击一个指定的地址，耗尽该主机用于处理真实用户请求的资源和能力。木马家族 Mirai 及其变体（尤其是 Hajime ）仍在部署此类攻击。

这可能是对终端用户危害最小的情况了。最坏情况（很少发生）也就是受感染设备的拥有者被 ISP 拉黑。而且通常情况下简单地重启设备就可以“治愈”该设备。

### **加密货币挖掘**

另一类有效荷载与加密货币有关。例如， IoT 恶意软件可以在受感染设备上安装恶意矿工。但是鉴于智能设备的算力很低，这种攻击的可行性还是一个疑问，即使它们的数量可能很大。

Satori 木马的创建者发明了一种更为狡猾和可行的获取加密货币的方法。他将受感染的 IoT 设备作为访问高性能计算机的一种钥匙：

第一步，攻击者首先试图利用已知漏洞感染尽可能多的路由器，这些漏洞包括：

[CVE-2014-8361](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8361)–Realtek SDK 的 miniigd SOAP 服务中的远程代码执行漏洞

[CVE 2017-17215](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE 2017-17215)– 华为 HG532 系列路由器固件中的远程代码执行漏洞

[CVE-2018-10561](https://nvd.nist.gov/vuln/detail/CVE-2018-10561), [CVE-2018-10562](https://nvd.nist.gov/vuln/detail/CVE-2018-10562)–Dasan GPON 路由器中的身份认证绕过漏洞和任意代码执行漏洞

[CVE-2018-10088](https://nvd.nist.gov/vuln/detail/CVE-2018-10088)–XiongMai uc-httpd 1.0.0 中的缓冲区溢出漏洞，该产品被用于部分中国制造的路由器和智能设备的固件中

第二步，利用受感染的路由器和以太坊挖矿软件 [Claymore](https://www.dualminer.ru/) 的远程管理工具中的漏洞 [CVE-2018-1000049](https://reversebrain.github.io/2018/02/01/Claymore-Dual-Miner-Remote-Code-Execution/)，将钱包地址替换成自己的。

### **数据窃取**

在 2018 年 5 月检测到的 [VPNFilter](https://securelist.com/vpnfilter-exif-to-c2-mechanism-analysed/85721/)木马则追求其它的目标。它首先拦截受感染设备的流量，然后从中提取重要的数据（用户名、密码等）并发送到网络犯罪分子的服务器。下面是 VPNFilter 的主要功能：

模块化架构。该恶意软件的创建者可随时添加新的功能。例如， 2018 年 6 月初检测到一个用于向截获的网页注入 JavaScript 代码的新模块。

自启动机制。该木马将自己写入标准 Linux 计划任务程序 crontab ，还可以修改设备的非易失性存储器（ NVRAM ）中的配置设置。

使用 TOR 与 C&C 服务器进行通信。

能够自毁并使设备“变砖”。一旦接收到相关命令，该木马就会自我删除并用垃圾数据覆盖固件的关键部分，然后重启设备。

该木马的传播方法仍然未知：其代码中没有包含自我传播机制。无论如何，我们倾向于认为它通过利用设备软件中的已知漏洞来感染设备。

[第一份关于VPNFilter的报告](https://blog.talosintelligence.com/2018/05/VPNFilter.html)称其感染了约 50 万个设备。从那时起，更多的设备被感染了，并且易受攻击的设备厂商列表大大加长了。到六月中旬，其目标包括以下品牌的设备：

ASUS

D-Link

Huawei

Linksys

MikroTik

Netgear

QNAP

TP-Link

Ubiquiti

Upvel

ZTE

由于这些厂商的设备不仅在公司网络中使用，而且常被用作家用路由器，这使得情况变得更糟。

## **三、结论**

智能设备正在崛起， [有人预测](https://www.statista.com/statistics/764026/number-of-iot-devices-in-use-worldwide/)称 2020 年智能设备的数量将超过世界总人口数量的好几倍。然而厂商们还是没有重视设备的安全性：在设备初始化设置过程中，他们没有提醒用户去修改默认密码；他们也没有向用户发布关于新固件版本的通知；甚至更新过程本身对普通用户而言都显得十分复杂。这使得物联网设备成为网络犯罪分子的主要攻击目标，甚至比个人计算机更容易受到感染。物联网设备通常在家庭基础设施中扮演了一个重要的角色：有些用于管理网络流量，有些用于拍摄监控视频，还有一些用于控制家用设备（如空调等）。

针对智能设备的恶意软件不仅在数量上增长，而且在质量上也在增长。越来越多的 exploits （漏洞利用程序）被网络犯罪分子开发出来。而除了传统的 DDoS 攻击之外，被感染的设备还被用于窃取个人数据和挖掘加密货币。

下面是一些可以帮助减少智能设备感染风险的小技巧：

除非绝对必要，否则禁止从外部网络访问设备；

定期重启有助于清除已感染的恶意软件（尽管大多数情况下还存在再次感染的风险）；

定期检查是否存在新版本的固件并进行更新；

使用复杂密码（长度至少为 8 位，包含大小写字母、数字和特殊字符）；

在初始设置时更改出厂密码（即使设备未提示您这样做）；

如果选项存在，则关闭 / 禁用不使用的端口。例如，如果您不打算通过 Telnet （占用 TCP 端口 23 ）连接到路由器，则最好禁用该端口以降低被入侵的风险。

## **2019年物联网发展的六大趋势**

IMG_256

资本实验室

01-0109:01

**资本实验室·今日创新观察**

**聚焦前沿科技创新与传统产业升级**

**张珂**

在人类发展史上，通讯技术的每次革命性突破，都会让我们离完全的数字化社会越来越近。

当现金变成微信和支付宝；当逛商场变成逛淘宝；当叫出租车变成叫滴滴；当“您好”变成“您家WIFI密码是什么？”时，现实中的我们每个人都在不知不觉中成为万物连接的一个节点。

数字化，已经成为现代社会发展的重要推动力；连接，已经成为未来社会的主旋律；物联网，则让一切变得简单而强大。那么，在2019年甚至更长的未来几年中，物联网会呈现出怎样的发展趋势，其中又包含了哪些商业机会？

**1.更严格的合规性**

当某项新技术诞生时，业界的兴奋、激进与政策和监管的滞后往往会形成鲜明的对比。在新技术初期，低水平监管意味着行业的技术力量几乎都在专注于创新。一旦这种创新与应用开始普及时，新技术所带来的各种风险也就突显出来。



2018年，数据隐私成为网络社会的一个关键词，各种用户数据泄露或被滥用的事件频发，特别是Facebook的丑闻引发了全球担忧。

所有的互联网公司和商家都收集了大量的用户数据。当“千人千面”、“个性化推荐”等词语已然成为互联网公司技术实力的代言人时，这也意味着我们每一个人都在这些互联网公司的注视下“裸奔“。

2019年，各种立法和监管机构将提出更加严格的用户数据保护规定，用户的敏感数据可能会随着时间的推移而受到更严格的监管。这种监管或许会与互联网行业的发展有一定冲突，例如2018年欧盟GDPR政策的出台，不得不让全球互联网巨头调整策略。

2019年，物联网法规或许将创造一个有利可图的商业机会——用户数据合规管理和咨询。

**2.更安全的防护措施**

随着物联网设备和基础设施的价格持续降低，企业对各种物联网设备的应用就越来越普及。这也意味着，企业需要更加关注物联网的安全。



2019年，安全软件将成为物联网产品的关键组成部分，同时，硬件级安全措施将也受到关注，特别是对于处理特别敏感数据的应用程序。

通过硬件本身执行受信任的操作系统和应用程序可以帮助缓解网络攻击和威胁。但是，物联网硬件和软件的开放性却更容易受到网络攻击。

以安全为重点的物联网设施将受到更多的关注，特别是某些特定的基础行业，如医疗健康、安全安防、金融等领域。

**3.更普及的智能消费设备**

2018年是智能家居设备快速发展的一年，各种智能化电子设备正在让我们的家庭生活变得越来越简单，扫地机器人让我们从基础家务中摆脱出来；智能音箱可以帮我们自动下购物订单。

2019年，各种外观和尺寸的物联网家居设备将会出现进一步的强劲增长。



2019年，更多的智能化技术将融入到日常家庭生活中，智能化厨房会让做菜做饭更加轻松，智能监控会让家庭安全系统更加强大，智能办公桌、智能墙壁有望走进生活。我们将获得越来越多的自由时间，而这都是物联网技术带来的变革。

**4.更加关注人工智能**

随着数据处理能力的提升，边缘计算将成为物联网的重要力量，因为它可以实现更高效的操作和更快捷的响应，而混合的物联网技术将变得更加普及。



2019年，我们将看到人工智能带来新物联网技术的重大进步。随着越来越多的企业使用物联网设备与技术，收集到的数据量呈现指数级增长，传统的计算方式已经无法满足数据处理需求。而AI则能填补数据收集和数据分析之间的空白，此外，AI可以实现更好地图像处理、视频分析，创造更多的应用场景和商机。

对企业而言，投资人工智能比投资更多的传感器更有意义。

**5.更专业的知识和人才**

2019年，将有越来越多的技术人员花时间提升物联网技能，这也将推动物联网技术培训的普及。



物联网专业知识的需求，将推动企业雇用更加专业的技术人员，一些大型企业或许将出现一个相对较新的高级角色——首席数据官。

随着数据分析变得越来越复杂、越来越强大，企业也越来越意识到需要能在更宏观的角度来进行数据分析和管理。

**6.移动访问更加轻松**

智能手机的普及直接影响着物联网的普及。移动连接、传感器、导航芯片等成本的下降，以及零部件的快速小型化，将推动智能手机的功能越来越强大，越来越集成化。



物联网不再是未来的技术，已经成为当今数据驱动型经济的基础和支柱。随着5G的到来，移动设备对物联网网络的访问将大幅增加，越来越多的物联网数据将掌握在更多人的手中。

对于技术人员，物联网专化化数据非常重要，但对于非技术人员在2019年也将获得更多的物联网衍生数据。

以智能手机为代表的移动设备将让每个人成为物联网社会中的一个连接点，从而共享物联网社会的便利性。

未来，物联网的发展将更多转移到更好地利用所收集数据的处理技术上，而不再只是关注物联网技术本身。

当每个人、每个设备都连接到一个大型网络中，人与人、人与设备、设备与设备之间将会产生更多的联系，而这也意味着将出现无尽的新的机会与可能性。

2018年趋势：AI 和物联网的未来将会如何？

作者：本站收录 来源：IT技术之家 2017-11-29 10:05:38 填写您的邮件地址，订阅我们的精彩内容：

摘要：提到人工智能，最流行也是最早被大众熟知的一个例子非深蓝(Deep Blue)莫属，深蓝是由 IBM 开发的超级计算机。

关键词：物联网[18870篇] 人工智能[756篇] 传感器[2533篇]

目前最火热的两个领域 —— 物联网和人工智能之间将会产生怎样的化学反应

人工智能和物联网的世界显然是令人兴奋的，但目前看来，依然有一些关键的技术问题需要解决，特别是关于开发者方面的问题。在这篇文章中，大家将会了解到在这些热门领域，有哪些值得我们期待的事情。

现在人造机器、工具和技术还不够成熟，人工智能和物联网是目前最热门的趋势。但它们到底是什么?它们的效果如何?2018 年我们又应该期待什么?大家不妨继续往下看。

　　人工智能

提到人工智能，最流行也是最早被大众熟知的一个例子非深蓝(Deep Blue)莫属，深蓝是由 IBM 开发的超级计算机。

那么人工智能在 2018 年将如何改变人们的生活?根据 Narrative Science 的报告，2016 年只有 38% 的公司使用人工智能，但到 2018 年这一比例预计将上升到 62%。

AI 已经使我们的生活变得更好：

1. 便捷的生活。人工智能让我们的生活变得更方便。这里可以列举一些例子：Siri 和 Cortana 的语音辅助服务、亚马逊的 Echo、GPS 等。

2. 更好的客户互动服务。AI 被越来越多地用于创建聊天机器人。这些聊天机器人可以在更短的时间内处理更多的客户问题，并及时提供解决方案。客户也可以获得即时的解决方案，从而提升对服务方的满意度。

3. 重构业务流程。AI 在商业决策中起着关键的作用。AI 可通过使用大数据和其他分析工具来识别业务中存在的浪费情况和额外处理。

4. 节省成本。人工智能使得数字化能够代替人类的工作，节省了部分人力资源的使用成本。机器不需要像人一样休息，因此可以提供更好更多的生产力。

5. 医疗应用。AI 用于在更短的时间内提供深入的诊断结果，这有助于医生迅速开始用药和治疗。机器人甚至可以帮助精神病患者摆脱抑郁症、进行关键的手术并监测神经紊乱的情况。

　　AI 的最新趋势：

人工智能将在 2018 年大幅增长。可以预见到，即将到来的一年会出现的人工智能技术包括：

1. 语音识别。不仅仅是输入命令，你将可以直接提问并从超级计算机中获得想要的东西。

2. 自然语言的生成。这将使得计算机具有人一样的表达和写作的功能，深度学习的发展是如此的迅猛，语言知识与深度学习模型的有机融合相信会带来更好的前景。使用 AI 业务可以生成报告，或在客户服务中使用商业智能洞察。

3. 智能家居。人工智能在 2018 年将用于智能家居管理。从确定您在家中的存在，到锁门和关闭空调、电器，AI 能确保节省更多的能量消耗和提升舒适度。

4. 机器学习平台。人工智能将于设计、训练和部署应用程序。构建在线训练工具包并提供算法。

5. AI 对硬件的兼容。人工智能目前不能在市场上可用的标准硬件上运行，因此将会出现专有的设备带来新的设计和架构以满足人工智能的高级需求。

　　物联网

2018 年物联网又将如何改变人们的生活?

1. 保险行业的快速增长。保险公司现在可以通过物联网获得实时数据。这将有助于他们分析风险、进行产品细分、改善对损失的控制，并获得更多的保险费。

2. 更好的产品。随着物联网的逐渐普及，用户使用的不再是独立的设备，而是提供一系列服务的设备，例如像 Siri 和 Cortana 这样的语音服务或其他服务。

3. 即时的健康服务。物联网已经催生了一些数字疗法的诞生，包括可以治疗失眠、抑郁症、生育和背痛的设备。

4. 零售转型。物联网意味着基于传感器的分析以及存在与客户偏好相关的大量数据。使用这些数据，零售部门能够识别出潜在客户，并更好地销售他们的产品。

　　物联网最新趋势

那么物联网的未来到底会如何?研究人员相当有把握确定物联网在 2018 年将会以更快的速度增长。一些关于物联网未来的发展的看法：

到 2020 年，将有超过 240 亿个电子设备通过物联网连接

未来几年将花费大约 6 万亿美元用于物联网

边缘分析计算和云分析计算将在决定物联网投资的过程中发挥至关重要的作用

物联网和人工智能会产生怎样的化学反应?

AI 和 IoT 是两个不同的趋势，不过在 2018 年，它们将会被一起使用，以在商业和日常生活中获得最佳结果。物联网将会产生大量的数据，人工智能将帮助跟踪并深入分析这些数据。

不妨在 2018 年里使用这两种技术吧，你的生活和业务也将会获得更多的收益。