[illegible]

10 [illegible]

[illegible]

[illegible]

[illegible] ...

[illegible]

[illegible] (1 [illegible]).

دستگاه‌های اینترنت اشیا در معرض تهدید، برنامه‌های مخرب اینترنت اشیا را نشانه رفته‌اند.
آمارها نشان می‌دهند بیش از ۶ میلیارد دستگاه هوشمند در سراسر جهان مورد استفاده قرار می‌گیرند. هنگامی که در سال ۲۰۱۶ بدافزار میریا دستگاه‌های اینترنت اشیا را در معرض تهدید قرار داد، همگان آگاه شدند که چگونه این دستگاه‌ها ممکن است تبدیل به ابزاری شوند که هکرها از آن‌ها استفاده می کنند. با این وجود تاریخچه حملات بدافزاری به تجهیزات اینترنت اشیا به خیلی قبل‌تر از ظهور باتنت فوق باز می‌گردد.
HYDRA
The first malware program targeting IoT devices.
TSUNAMI
A cross-platform IRC backdoor with DDoS capabilities.
TROJAN.LINUX.PNSCAN
A Trojan infecting vulnerable devices with the Tsunami backdoor.
BRICKERBOT
A bot infecting IoT devices and rendering them inoperable.
PSYBOT
Emergence of PsyBot, the first in the wild malicious program for the MIPS platform.
GAFGYT
An IRC backdoor capable of scanning IP ranges to find vulnerable devices.
MIRAI
and its clones Hajime, Remaiten, and Moose.
2008
2009
2010
2014
2015
2016
2017
KASPERSKY

-1 [illegible]

[illegible] [illegible] [illegible] [

IoT Analytics

[illegible]

[illegible]: [illegible] - [illegible] [illegible] [illegible]

[illegible]

[illegible]

[illegible]

[illegible] **15** [illegible]

[illegible]

Low-Power, Short-Range IoT Networks

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Low-Power, Wide-Area Networks

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

IoT Processors

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

iOS [illegible]

[illegible]

[illegible] 2025 [illegible]

[illegible]

[illegible]

[illegible] SAP Event Stream Processor [illegible] (Distributed Stream Computing Platforms [illegible]) DSCPs [illegible]

[illegible]

[illegible]

IoT Platforms

[illegible]

[illegible]

[illegible]

[illegible]

IoT Standards and Ecosystems

در حالی که اکوسیستمها و استانداردها در حال حاضر بهعنوان یک فناوری شناخته نمیشوند، اما در اغلب موارد بهعنوان واسطهای برنامهنویسی پیشرفته (API) از آنها نام برده میشود. ما به این استانداردها و واسطهای برنامهنویسی پیشرفته نیاز داریم. بهواسطه آنکه دستگاههای اینترنت اشیا نهتنها برای برقراری ارتباط با یکدیگر به آنها نیاز دارند، بلکه بسیاری از مدلهای تجاری اینترنت اشیا بهمنظور بهاشتراکگذاری دادهها میان دستگاهها و سازمانهای مختلف به این استانداردها محتاج هستند. کارشناسان بر این باورند که ظرف چند سال آینده تعدادی از این اکوسیستمها با یکدیگر ترکیب خواهند شد و شاهد رویارویی جدی در حوزههای تجاری، فنی و صنعتی اکوسیستمها اینترنت اشیا خواهیم بود. این رویارویی حتی به درون خانههای هوشمند، شهرهای هوشمند و صنعت بهداشت و درمان نیز کشیده خواهد شد. بر همین اساس سازمانها ممکن است به فکر طراحی و ساخت محصولاتی باشند که از انواع مختلفی از استانداردها یا اکوسیستمهای مختلف پشتیبانی کنند. این رویکرد نهتنها فرآیند بهروزرسانی محصولات را بهشکل سادهتری مدیریت میکند، بلکه به محصولات اجازه خواهد داد از استانداردها و واسطهای برنامهنویسی چندگانه پشتیبانی کنند. برای طراحی چنین محصولاتی شرکتها بهدنبال متخصصانی خواهند بود که به استانداردها و معماریهای مختلف مرتبط با اینترنت اشیا آشنایی داشته باشند. به طور مثال، تیم IBM Global Business Services نزدیک به 17 روز پیش در زمان نگارش این مقاله آگهی استخدامی را منتشر کرد و اعلام داشت بهدنبال کارشناس اینترنت اشیا ارائهدهنده راه حلهای CoC (سرنام Solution Architect-Center of Competence) است.

منبع :
[IT Business Edge]
دسته بندی:
[اینترنت اشیا]
[پرونده ویژه]
تاریخ انتشار :
10:50 - 06/06/1396
برچسب:
[اینترنت اشیا] - [اینترنت اشیا صنعتی] - [امنیت اینترنت اشیا] - [فناوری اینترنت اشیا] - [اشتغال‌زایی اینترنت اشیا]

نشانی:
https://www.shabakeh-mag.com/information-feature/iot/9000/10-%D9%81%D9%86%D8%A7%D9%88%D8%B1%DB%8C-%D8%AF%D8%A7%D8%AE%D9%84%DB%8C-%DA%A9%D9%87-%D8%AF%D8%B1-%D8%A7%DA%A9%D9%88%D8%B3%DB%8C%D8%B3%D8%AA%D9%85-

%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-
%D8%A7%D8%B4%DB%8C%D8%A7-
%D8%A7%D8%B4%D8%AA%D8%BA%D8%A7%D9%84%E2%80%8C%D8%A2%D9%81%D8%B1%DB%8C%D9%86%DB%8C-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF