

物联网小镇

Town of Internet of Things

IOT FTW

BY PASCAL GLOOR

ACCEPTABLE USE POLICY

The Twitter Rules

We believe that everyone should have the power to create and share ideas and information instantly, without barriers. In order to protect the experience and safety of people who use Twitter, there are some limitations on the type of content and behavior that we allow. These limitations are set forth in the Twitter Rules below.

The Twitter Rules (along with all incorporated policies), [Privacy Policy](#), and [Terms of Service](#) collectively make up the "Twitter User Agreement" that governs a user's access to and use of Twitter's services.

All individuals accessing or using Twitter's services must adhere to the policies set forth in the Twitter Rules. Failure to do so may result in Twitter taking one or more of the following enforcement actions:

- requiring you to delete prohibited content before you can again create new posts and interact with other Twitter users;
- temporarily limiting your ability to create posts or interact with other Twitter users;
- asking you to verify account ownership with a phone number or email address; or
- permanently suspending your account(s).

If you attempt to evade a permanent suspension by creating new accounts, we will suspend your new accounts.

Please note that we may need to change these Rules from time to time and reserve the right to do so. The most current version is always available at: <https://twitter.com/rules>.

The policies set forth in these Twitter Rules govern organic content on our platform. To learn more about the rules which govern ads and promoted content, please review our [Ads policies](#).

Content Boundaries and Use of Twitter

Intellectual property

Trademark: We reserve the right to suspend accounts or take other appropriate action when someone's brand or trademark, including business name and/or logo, is used in a manner that may mislead or confuse others about your brand affiliation. Read more about our [trademark policy and how to report a violation](#).

Copyright: We will respond to clear and complete notices of alleged copyright infringement. Our copyright procedures are set forth in our [Terms of Service](#). Read more about our [copyright policy](#).

Graphic violence and adult content

We consider graphic violence to be any form of gory media related to death, serious injury, violence, or surgical procedures. We consider adult content to be any media that is pornographic and/or may be intended to cause sexual arousal. Twitter allows some forms of graphic violence and/or adult content in Tweets marked as containing sensitive media. However, you may not use such content in live video, your profile, or header images. Additionally, Twitter may sometimes require you to remove excessively graphic violence. [Read more](#) about how we define graphic violence and adult content and [how to mark your media as sensitive](#).

Media depicting deceased individuals: We may require you to remove media that depicts the death of an identifiable individual if we receive a request from their family or an authorized representative. Learn more about [how to make such a request](#).

Unlawful use

You may not use our service for any unlawful purposes or in furtherance of illegal activities. By using Twitter, you agree to comply with all applicable laws governing your online conduct and content.

Distribution of hacked materials

We do not permit the use of our services to directly distribute content obtained through hacking that contains personally identifiable information, may put people in imminent harm or danger, or contains trade secrets. Direct distribution of hacked materials includes posting hacked content on Twitter (for instance, in the text of a Tweet, or in an image), or directly linking to hacked content hosted on other websites.

We may suspend accounts which directly distribute hacked materials where the account has made a claim of responsibility for a hack, or where Twitter is able to reliably attribute a hack to the account distributing that content.

Trends

At times, we may prevent certain content from trending. This includes content that violates the Twitter Rules, as well as content that may attempt to manipulate trends. Read more about [what we allow and do not allow to trend](#).

Third-party advertising in video content

You may not submit, post, or display any video content on or through our services that includes third-party advertising, such as pre-roll video ads or sponsorship graphics, without our prior consent.

Misuse of Twitter badges

You may not use badges, including but not limited to the "promoted" or "verified" Twitter badges, unless provided by Twitter. Accounts using unauthorized badges as part of their profile photos, header photos, display names, or in any way that falsely implies affiliation with Twitter or authorization from Twitter to display these badges, may be suspended.

Misuse of usernames

Selling usernames: You may not buy or sell Twitter usernames.

Username squatting: You may not engage in username squatting. Some of the factors we take into consideration when determining whether conduct is username squatting include:

- the number of accounts created;
- the creation of accounts for the purpose of preventing others from using those account names;
- the creation of accounts for the purpose of selling those accounts; and
- the use of third-party content feeds to update and maintain accounts under the names of those third parties.

Please note that Twitter may also remove accounts that are inactive for more than six months. Learn more about [username squatting](#).

Abusive Behavior

We believe in freedom of expression and open dialogue, but that means little as an underlying philosophy if voices are silenced because people are afraid to speak up. In order to ensure that people feel safe expressing diverse opinions and beliefs, we prohibit behavior that crosses the line into abuse, including behavior that harasses, intimidates, or uses fear to silence another user's voice.

Context matters when evaluating for abusive behavior and determining appropriate enforcement actions. Factors we may take into consideration include, but are not limited to whether:

- the behavior is targeted at an individual or group of people;
- the report has been filed by the target of the abuse or a bystander;
- the behavior is newsworthy and in the legitimate public interest.

Violence and physical harm

Violence: You may not make specific threats of violence or wish for the serious physical harm, death, or disease of an individual or group of people. This includes, but is not limited to, threatening or promoting terrorism. You also may not affiliate with organizations that – whether by their own statements or activity both on and off the platform — use or promote violence against civilians to further their causes.

Suicide or self-harm: You may not promote or encourage suicide or self-harm. When we receive reports that a person is threatening suicide or self-harm, we may take a number of steps to assist them, such as reaching out to that person and providing resources such as contact information for our mental health partners.

Child sexual exploitation: You may not promote child sexual exploitation. Learn more about our zero-tolerance [child sexual exploitation policy](#).

Abuse and hateful conduct

Abuse: You may not engage in the targeted harassment of someone, or incite other people to do so. We consider abusive behavior an attempt to harass, intimidate, or silence someone else's voice.

Unwanted sexual advances: You may not direct abuse at someone by sending unwanted sexual content, objectifying them in a sexually explicit manner, or otherwise engaging in sexual misconduct.

Hateful conduct: You may not promote violence against, threaten, or harass other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease. Read more about our [hateful conduct policy](#).

Hateful imagery and display names: You may not use hateful images or symbols in your profile image or profile header. You also may not use your username, display name, or profile bio to engage in abusive behavior, such as targeted harassment or expressing hate towards a person, group, or protected category.

Private information and intimate media

Private information: You may not publish or post other people's private information without their express authorization and permission. Definitions of private information may vary depending on local laws. Read more about our [private information policy](#).

Intimate media: You may not post or share intimate photos or videos of someone that were produced or distributed without their consent. Media depicting sexual violence and/or assault is also not permitted. Note: limited exceptions may apply if there is clear context that the interaction is consensual. Read more [about intimate media](#) on Twitter.

Threats to expose / hack: You may not threaten to expose someone's private information or intimate media. You also may not threaten to hack or break into someone's digital information or attempt to incentivize others to do so (e.g., through setting a bounty or reward on such actions).

Impersonation

You may not impersonate individuals, groups, or organizations in a manner that is intended to or does mislead, confuse, or deceive others. While you may maintain parody, fan, commentary, or newstfeed accounts, you may not do so if the intent of the account is to engage in spamming or abusive behavior. Read more about our [impersonation policy](#).

Spam and Security

We strive to protect people on Twitter from technical abuse and spam.

To promote a stable and secure environment on Twitter, you may not do, or attempt to do, any of the following while accessing or using Twitter:

- Access, tamper with, or use non-public areas of Twitter, Twitter's computer systems, or the technical delivery systems of Twitter's providers (except as expressly permitted by the Twitter Bug Bounty program).
- Probe, scan, or test the vulnerability of any system or network, or breach or circumvent any security or authentication measures (except as expressly permitted by the Twitter Bug Bounty program).
- Access or search, or attempt to access or search, Twitter by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by Twitter (and only pursuant to the applicable terms and conditions), unless you have been specifically allowed to do so in a separate agreement with Twitter. Note that crawling Twitter is permissible if done in accordance with the provisions of the robots.txt file; however, scraping Twitter without our prior consent is expressly prohibited.
- Forge any TCP/IP packet header or any part of the header information in any email or posting, or in any way use Twitter to send altered, deceptive, or false source-identifying information.
- Interfere with or disrupt the access of any user, host or network, including, without limitation, sending a virus, overloading, flooding, spamming, mail-bombing Twitter's services, or by scripting the creation of content in such a manner as to interfere with or create an undue burden on Twitter.

Any accounts engaging in the following activities may be temporarily locked or subject to permanent suspension:

- **Malware/Phishing:** You may not publish or link to malicious content intended to damage or disrupt another person's browser or computer or to compromise a person's privacy.
- **Fake accounts:** You may not register or create fake and misleading accounts. While you may use Twitter pseudonymously or as a [parody, commentary, or fan account](#), you may not use misleading account information in order to engage in spamming, abusive, or disruptive behavior, including attempts to manipulate the conversations on Twitter. Some of the factors that we take into account when determining whether an account is fake include:
 - Use of stock or stolen avatar photos
 - Use of stolen or copied profile bios
 - Use of intentionally misleading profile information, including profile location
- **Spam:** You may not use Twitter's services for the purpose of spamming anyone. Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or the experience of users on Twitter to drive traffic or attention to unrelated accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is considered to be spamming include:
 - if you have followed and/or unfollowed a large number of of accounts in a short time period, particularly by automated means (aggressive following or follower churn);
 - if your Tweets or Direct Messages consist mainly of links shared without commentary;
 - if a large number of people have blocked you in response to high volumes of untargeted, unsolicited, or duplicative content or engagements from your account;
 - if a large number of spam complaints have been filed against you;
 - if you post duplicative or substantially similar content, replies, or mentions over multiple accounts or multiple duplicate updates on one account, or create duplicate or substantially similar accounts;
 - if you post multiple updates to a trending or popular topic with an intent to subvert or manipulate the topic to drive traffic or attention to unrelated accounts, products, services, or initiatives;
 - if you send large numbers of unsolicited replies or mentions;
 - if you add users to lists in a bulk or aggressive manner;
 - if you are randomly or aggressively engaging with Tweets (e.g., likes, Retweets, etc.) or users (e.g., following, adding to lists or Moments, etc.) to drive traffic or attention to unrelated accounts, products, services, or initiatives;
 - if you repeatedly post other people's account information as your own (e.g., bio, Tweets, profile URL, etc.);
 - if you post misleading, deceptive, or malicious links (e.g., affiliate links, links to malware/clickjacking pages, etc.);
 - if you sell, purchase, or attempt to artificially inflate account interactions (such as followers, Retweets, likes, etc.); and
 - if you use or promote third-party services or apps that claim to get you more followers, Retweets, or likes (such as follower trains, sites promising "more followers fast", or any other site that offers to automatically add followers or engagements to your account or Tweets).

Please see our support articles on [following rules and best practices](#) and [automation rules and best practices](#) for more detailed information about how the Rules apply to those particular account behaviors. Accounts created to replace or mimic suspended accounts may be permanently suspended. We may also remove accounts which Twitter is able to reliably attribute to entities known to violate the Twitter Rules.

Content Visibility

Accounts under investigation or which have been detected as sharing content in violation of these Rules may have their account or Tweet visibility limited in various parts of Twitter, including search. To learn more about situations in which content may be restricted on Twitter, please see our support article on [search rules and restrictions](#).

ACCEPTABLE USE POLICY

The Twitter Rules

We believe that everyone should have the power to create and share ideas and information instantly, without barriers. In order to protect the experience and safety of people who use Twitter, there are some limitations on the type of content and behavior that we allow. These limitations are set forth in the Twitter Rules below.

The Twitter Rules (along with all incorporated policies), [Privacy Policy](#), and [Terms of Service](#) collectively make up the "Twitter User Agreement" that governs a user's access to and use of Twitter's services.

All individuals accessing or using Twitter's services must adhere to the policies set forth in the Twitter Rules. Failure to do so may result in Twitter taking one or more of the following enforcement actions:

- requiring you to delete prohibited content before you can again create new posts and interact with other Twitter users;
- temporarily limiting your ability to create posts or interact with other Twitter users;
- asking you to verify account ownership with a phone number or email address; or
- permanently suspending your account(s).

If you attempt to evade a permanent suspension by creating new accounts, we will suspend your new accounts.

Please note that we may need to change these Rules from time to time and reserve the right to do so. The most current version is always available at: <https://twitter.com/rules>.

The policies set forth in these Twitter Rules govern organic content on our platform. To learn more about the rules which govern ads and promoted content, please review our [Ads policies](#).

Content Boundaries and Use of Twitter

Intellectual property

Trademark: We reserve the right to suspend accounts or take other appropriate action when someone's brand or trademark, including business name and/or logo, is used in a way that is abusive, defamatory, or otherwise violates the Rules.

Affiliation: Read more about our [trademark policy and how to report a violation](#).

Copyright: We will respond to clear and complete notices of alleged copyright infringement. Our copyright procedures are set forth in our [Terms of Service](#). Read more about our [copyright policy](#).

Graphic violence and adult content

We consider graphic violence to be any form of gory media related to death, serious injury, violence, or surgical procedures. We consider adult content to be any form of sexually explicit or suggestive content. Twitter allows some forms of graphic violence and/or adult content in Tweets marked as containing sensitive media. However, you may not post content that is excessively graphic, violent, or sexually explicit. We may require you to remove media depicting sexual violence and/or assault is also not permitted.

Media depicting deceased individuals: We may require you to remove media that depicts the death of an identifiable individual, including but not limited to a person's face, body, or remains, if the media is excessively graphic, violent, or sexually explicit. Read more about our [media policy](#).

[request](#).

Unlawful use

You may not use our service for any unlawful purposes or in furtherance of illegal activities.

Distribution of hacked materials

We do not permit the use of our services to directly distribute content of others without their permission. The distribution of hacked materials includes posting hacked content on Twitter (for instance, by retweeting or replying to it) or sharing it on other platforms. We may suspend accounts which directly distribute hacked materials.

Trends

At times, we may prevent certain content from trending. This is to protect the integrity of the trending feature.

Third-party advertising in video content

You may not submit, post, or display any video content on Twitter that contains third-party advertising.

Misuse of Twitter badges

You may not use badges, including but not limited to the "p" (protected) badge, in a way that is abusive, defamatory, or otherwise violates the Rules. This includes, but is not limited to, using a badge to falsely imply affiliation with Twitter or authorization from Twitter.

Misuse of usernames

Selling usernames: You may not buy or sell Twitter usernames.

Username squatting: You may not engage in username squatting, which is the creation of accounts for the purpose of preventing others from using a particular username.

- the number of accounts created;
- the creation of accounts for the purpose of preventing others from using a particular username;
- the creation of accounts for the purpose of selling those accounts;
- the use of third-party content feeds to update and maintain accounts;

Please note that Twitter may also remove accounts that are inactive for a period of time.

Abusive Behavior

We believe in freedom of expression and open dialogue, but that means everyone has the right to be free from harassment, abuse, and other harmful behavior. Our beliefs, we prohibit behavior that crosses the line into abuse, including but not limited to the following:

Context matters when evaluating for abusive behavior and determining a response. The following factors may be considered:

- the behavior is targeted at an individual or group of people;
- the report has been filed by the target of the abuse or a bystander;
- the behavior is newsworthy and in the legitimate public interest.

Violence and physical harm

Violence: You may not make specific threats of violence or wish for the serious harm or death of another person, including but not limited to threats or wishes directed at individuals, groups, or organizations that — whether by their own statements or activity both on and off Twitter — have been involved in violence or physical harm.

Suicide or self-harm: You may not promote or encourage suicide or self-harm. We may remove content that promotes or encourages suicide or self-harm, including but not limited to content that provides resources such as contact information for our mental health partners.

Child sexual exploitation: You may not promote child sexual exploitation. Learn more about our [child sexual exploitation policy](#).

Abuse and hateful conduct

Abuse: You may not engage in the targeted harassment of someone, or incite other people to harass someone. This includes but is not limited to the following:

Unwanted sexual advances: You may not direct abuse at someone by sending unwanted sexual messages or images.

Hateful conduct: You may not promote violence against, threaten, or harass other people based on their race, ethnicity, national origin, ancestry, language spoken, sex, sexual orientation, gender identity, or religion. Read more about our [hateful conduct policy](#).

Hateful imagery and display names: You may not use hateful images or symbols in your profile picture, header image, or bio. You may not use a display name that promotes abusive behavior, such as targeted harassment or expressing hate towards a person, group, or protected category.



Definitions of private information may vary depending on local laws. Read more about our [privacy policy](#).

Media depicting sexual violence and/or assault is also not permitted.

Unauthorized access to digital information: You may not attempt to hack or break into someone's digital information or attempt to access someone's digital information without their permission.

Impersonation: You may not impersonate another person or entity, including but not limited to a person, group, or organization, or create a fake account.

Parody, fan, commentary, or newsfeed: You may maintain parody, fan, commentary, or newsfeed accounts, but they must be clearly identifiable as such. Read more about our [parody policy](#).

Technical delivery: You may not use technical delivery methods to deliver content to users, except as expressly permitted by the Twitter Bug Bounty program.

Security or authentication measures: You may not use security or authentication measures to access or use our services, except as expressly permitted by the Twitter Bug Bounty program.

Other than through our published interfaces: You may not use our services other than through our published interfaces that are provided by Twitter (and our partners). Note that crawling Twitter is permissible if done in a way that does not interfere with the service.

Expressly permitted: Content is expressly permitted if it is used in a way that is consistent with the spirit of the Rules. Note that crawling Twitter is permissible if done in a way that does not interfere with the service.

Deceptive, or false source-identifying information: You may not use deceptive, or false source-identifying information, including but not limited to, using a fake name, address, or phone number.

Spam: You may not use our services to promote spam, including but not limited to, sending unsolicited direct messages, mail-bombing Twitter's services, or by scripting the service.

Computer or computer program: You may not use a computer or computer program to access or use our services, except as expressly permitted by the Twitter Bug Bounty program.

Parody, fan, commentary, or fan account: You may not use misleading information, including but not limited to, using a fake name, address, or phone number.

Conversations on Twitter: Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

• the nature of the activity;

• the timing of the activity;

• the location of the activity;

• the identity of the accounts, products, services, or initiatives.

Spam is generally defined on Twitter as bulk or aggressive activity that attempts to manipulate or disrupt Twitter or its services, including but not limited to the following:

• the creation of accounts, products, services, or initiatives. Some of the factors that we take into account when determining what conduct is acceptable on Twitter include:

• the volume of the activity;

1982

GENESIS

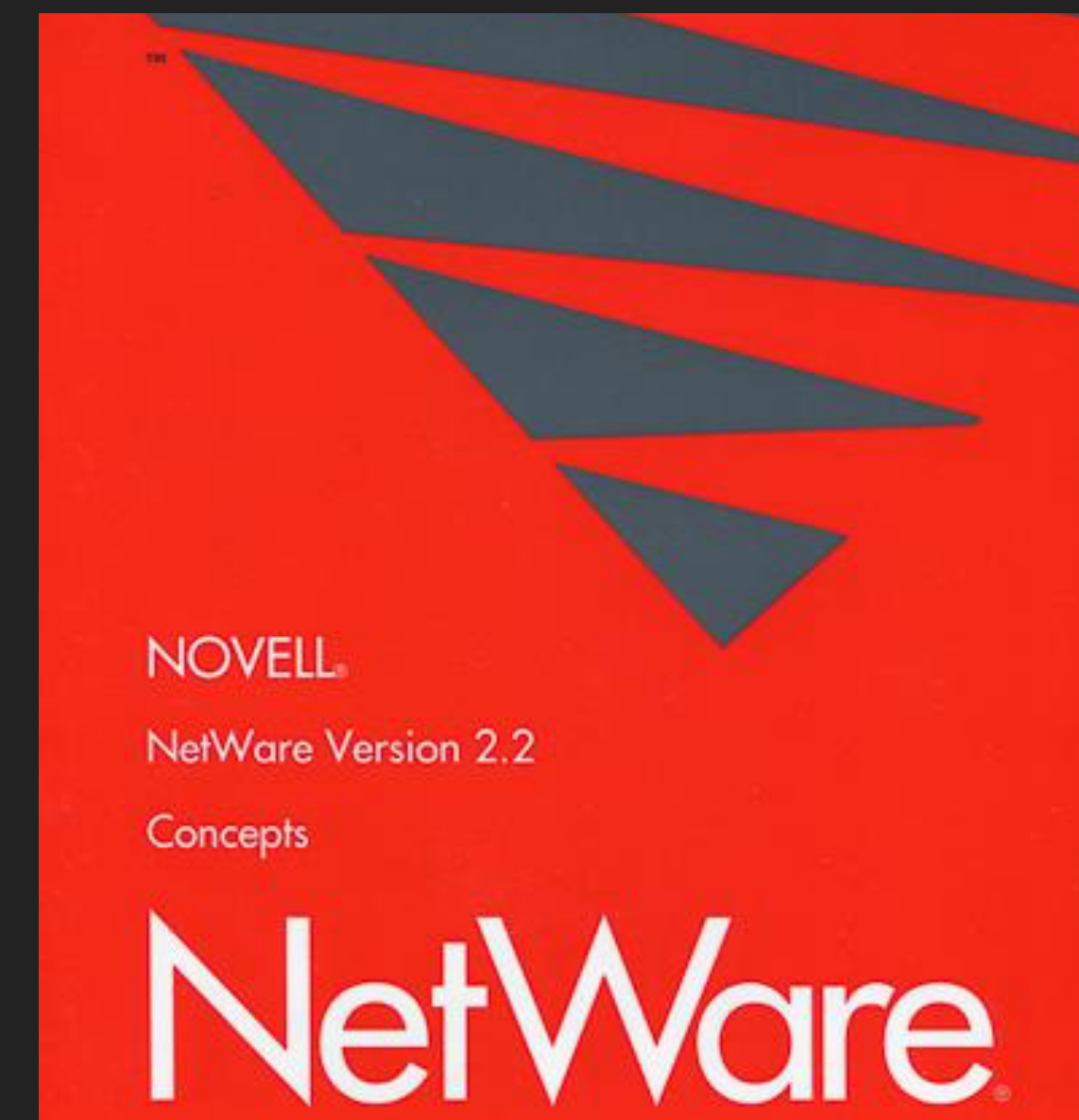
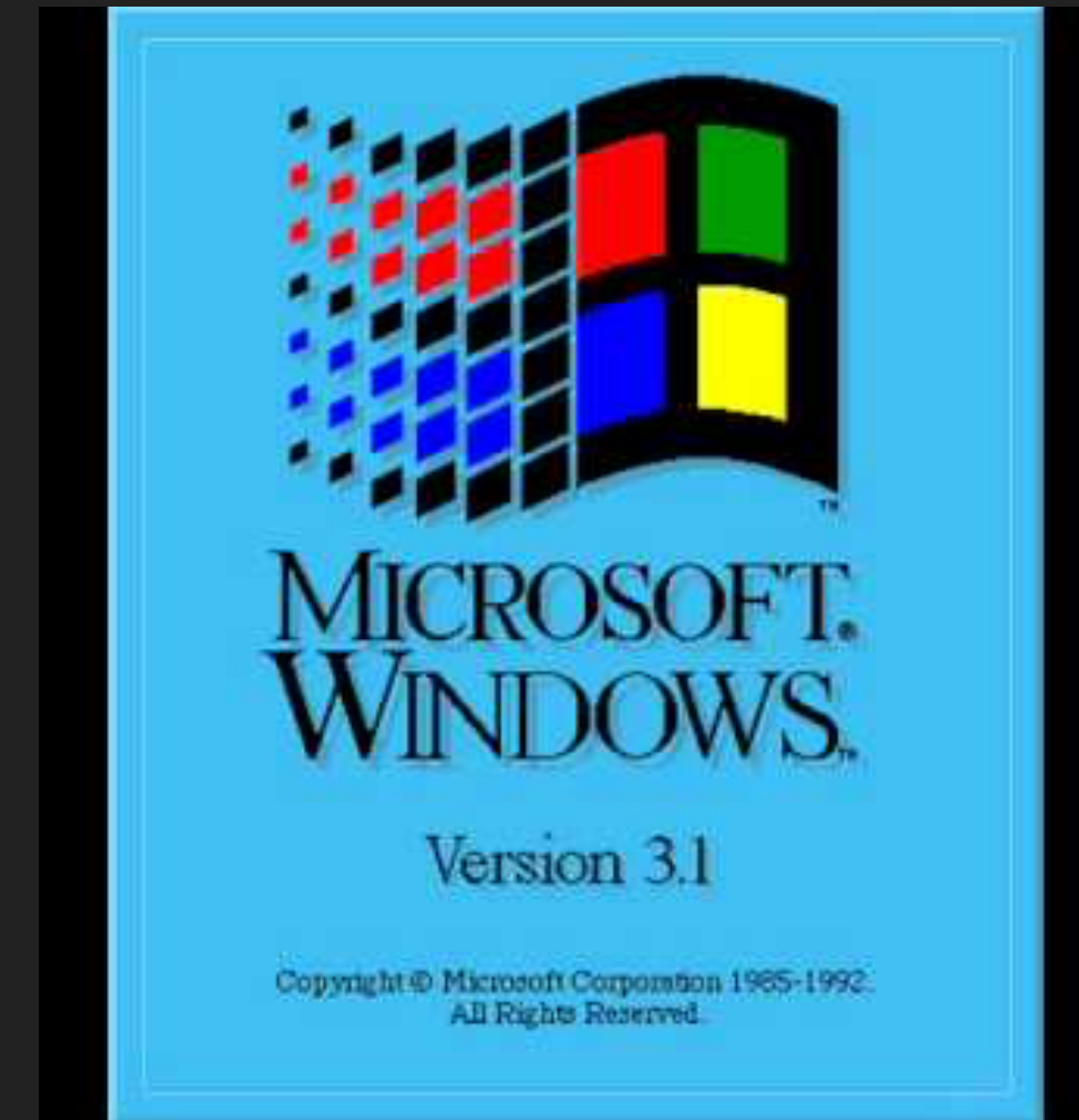
- ▶ Months only after IPv4 deployment
- ▶ Coke machine at Carnegie Mellon University, Pittsburgh, Pennsylvania, United States
- ▶ Lookup content and temperature



1990-2000

STANDARDISATION

- ▶ Microsoft "at Work"
- ▶ Novell "NEST"
- ▶ ...



2000-2010

POST STANDARDISATION WORLD

2000-2010

POST STANDARDISATION WORLD

- ▶ MESS (Media Enhancement for Security Standard)

POST STANDARDISATION WORLD

- ▶ MESS (Media Enhancement for Security Standard)

FAKE



2010-2020

ROM

- ▶ AKA the Rise of the Machines



GFYSS

- ▶ Wide implementation and acceptance of GFYSS for IoT (Go Fuck Yourself with your Stupid Standards)
- ▶ Common Sense became totally overrated



This Thermometer Tells Your Temperature, Then Tells Firms Where to Advertise



Kinsa says its smart thermometers are in more than 500,000 American households.

Tony Cenicola/The New York Times



Mashable ✓

@mashable

Follow



If you ever wanted a flying robot in your home, you're in luck



Flying robot

Aire is a new type of home security. Instead of multiple cameras covering different rooms, it's one camera flying throughout your home.

Every minute for three months, GM secretly gathered data on 90,000 drivers' radio-listening habits and locations



It turns out that Facebook could in fact use data collected from its Portal in-home video device to target you with ads

Who you call and what apps you use could determine what ads you see.

By [Kurt Wagner](#) | Oct 16, 2018, 1:45pm EDT



SHARE





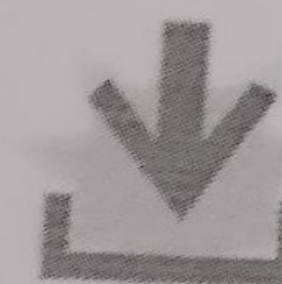
1 Insert key into the key channel.



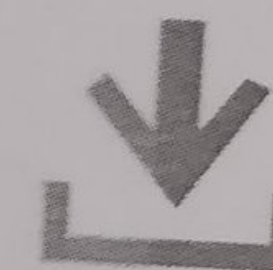
2 The key connects to the server.



3 Upgrade begins. Do not remove the key during the upgrade which takes about **1-2 minutes** depending on the network speed.



4 The key has been upgraded when the key gives two beep sounds between 4 seconds and the light is solid.



5 Remove the key from the device. Upgrade is now completed and you can continue using your key with a normal manner.



NOTICE:

If the key is removed from the device during the upgrade process, the key will be reset to the factory default. Red X sign will appear on the screen.



285

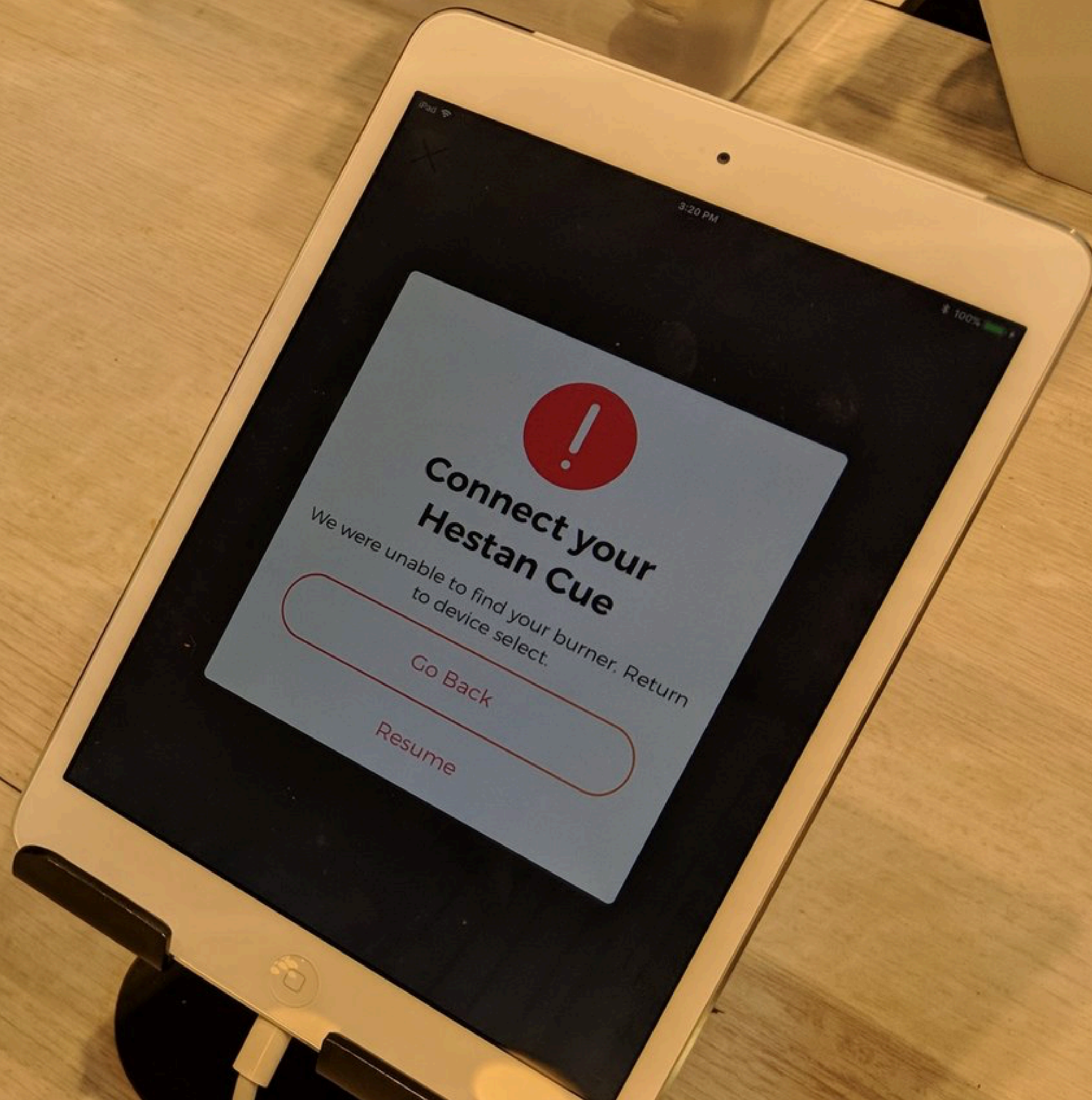



Negs S

---○F



Software update required
Contact Tesla Service





**The thermostat is
restarting. Back in a bit.**

juan @juanbuis · Aug 28

i'm in san francisco, the city where I can't use the restroom as it requires me to sign up for an app with a US phone number

Unlimited access to all Good2Go locations FREE for a limited time

GOOD2GO
www.good2go.global

Download your key today ▶
iOS users - open your camera to scan QR code

Download on the App Store
GET IT ON Google Play

Need access to the restroom?
Here's your key ▶

USE THE APP TO:

- Find a Good2Go location
- Join the virtual queue
- Get notified when it's your turn
- Unlock and open the door with your smartphone!

San Francisco's newest must-have app!



549



4.5K



11K



NEWS | By [Lorenzo Franceschi-Bicchierai](#) | Sep 2 2015, 3:45pm

Baby Monitors Are Still Really Easy to Hack

Despite media attention, several devices have serious vulnerabilities.

SHARE



TWEET



Image: [Piotr Adamowicz](#)/Shutterstock

Samsung's smart fridge could be used to steal your Gmail login



A connected fridge from Samsung. Image courtesy of Samsung.

Pura Scents: Smart Air Freshener Meets Smart Nightlight



Customize the aroma of any space from a smartphone + a multi-colored smart nightlight that you control.

Created by

Team Pura Scents

633 backers pledged \$57,760 to help bring this project to life.

This guy's light bulb performed a DoS attack on his entire smart house



Kashmir Hill

3/03/15 9:41am • Filed to: REAL FUTURE ▾

6.0K Save



Andy Dubbin

[Home](#) » [Cybersecurity](#) » [IoT & ICS Security](#) » [Hacker creates seven new variants of the Mirai botnet](#) | [Avast](#)



Hacker creates seven new variants of the Mirai botnet |

Avast



by [Avast Blog](#) on October 25, 2018

In September 2016, Twitter, CNN, Spotify, and many others were knocked offline by the biggest DDoS attack in history. Today we know it by the name Mirai, but no one would have imagined at the time that this attack was coming from a herd of Internet of Things (IoT) devices cobbled together to form a botnet.

Mirai was discovered by [MalwareMustDie](#) researchers in August 2016 . Although it was not the first IoT malware to be [discovered](#), it is certainly the most prominent.

After taking down much of the internet on the east coast of the US, things got worse when the malware creator self-dubbed Anna-Senpai released the source code. Since then, motivated hackers around the world have used it as a framework to create their own variants of botnets. Eventually, the original malware creators were arrested and [pleaded guilty in court](#), but the impact of the code release significantly sped up botnet creation. New variants started to appear, adding new functionality and exploiting a variety of vulnerabilities in unsecured IoT devices.

Torii IoT Botnet Takes Mirai to the Next Level



Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine

Email Phil Follow @philmuncaster



Security experts are warning of a new IoT botnet far more stealthy, persistent and advanced than Mirai and designed to compromise a wide range of device architectures.

Researcher [@VessOnSecurity](#) first tweeted about his discovery last week after detecting the threat via a honeypot. Although it spreads via Telnet and targets weak credentials on devices, “it’s not your run-of-the-mill Mirai variant or Monero miner,” he warned.

“It does not (yet) do the usual stuff a botnet does like DDOS, attacking all the devices connected to the internet, or, of course, mining cryptocurrencies,” [explained Avast](#) in a follow-up analysis.

“Instead, it comes with a quite rich set of features for exfiltration of (sensitive) information, modular architecture capable of fetching and executing other commands and executables and all of it via multiple layers of encrypted communication.”

Dubbed “Torii” by the firm, the threat first finds out the architecture of the targeted device, and downloads an appropriate payload — with MIPS, ARM, x86, x64, PowerPC, SuperH and more supported.

This payload is a dropped for the second stage. Meanwhile, Torii uses at least six methods to make sure the file remains on the device and always runs.

“The second stage payload is a full-fledged bot capable of executing commands from its master (CnC),” said Avast. “It also contains other features such as simple anti-debugging techniques, data exfiltration, multi-level encryption of communication, etc.”

Sean Newman, director at [Corero Network Security](#), said Torii is “cashing in on the rapidly expanding global pool of IoT devices.”

Why Not Watch?



25 MAY 2017

From Targeted to Distributed - Raise your Defenses Against Ransomware and Modern Malware



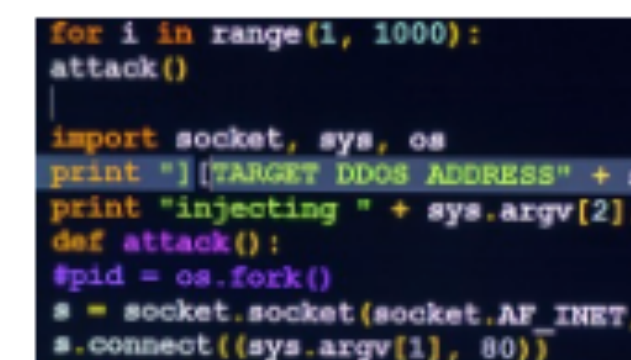
10 MAR 2016

Out Think Mobile Malware - Learn How to Protect Your Mobile Devices



2 FEB 2017

Securing the Internet of Unnecessary Things



9 MAR 2017

How IoT Enabled a DDoS, and How to Avoid Being Part of It

Don't forget the devices that bring the internet right to your pants. i.Con, a "smart condom" that's actually more like a cock ring, aims to tell men exactly how shit they are in bed. Maybe, I don't know, ask your girlfriend?



A \$100 [Bluetooth toaster](#) by Griffin that can send you a notification when your toast is done to your desired level of crispness. Which is fine, except toast takes like three minutes. And it's \$100. My toaster was \$8 and works almost all the time.



Welcome Home

Griffin Home smart appliances and chargers connect to handle daily routines effortlessly.



Do we really need an Alexa-powered toilet?

Jennifer Jolly | Special for USA TODAY

Published 1:37 PM EST Jan 12, 2018



This toilet from Kohler can flush by voice command

Kohler

PRIVACY

- ▶ gathering any data
- ▶ selling wildly data to the best bidder



PRIVACY

- ▶ gathering any data
- ▶ selling wildly data to the best bidder

NOBODY GIVES A SHIT



SECURITY

- ▶ H4X0rZ gathering any data
- ▶ H4X0rZ use data to blackmail
- ▶ H4X0rZ use YOUR device for DDoS
- ▶ and...



SECURITY

- ▶ H4X0rZ gathering any data
- ▶ H4X0rZ use data to blackmail
- ▶ H4X0rZ use YOUR data
- ▶ and...

NOBODY GIVES A SHIT



