The alarming increase in the number of attacks targeted at IoT devices

Along with the explosive growth of globalized internet and especially wireless connectivity, the number of attacks targeted Internet devices and Things (IoT) has escalated 'scary. 'throughout 2018.

Along with the explosive growth of globalized internet and especially wireless connectivity, the number of attacks targeted Internet devices and Things (IoT) has escalated 'scary. 'During the year 2018, a total of 32.7 million unauthorized intrusion into IoT facilities was discovered and recorded by the network security monitoring organization SonicWall, while traditional phishing attacks There are signs of decline again.

In addition, according to statista statistics, by 2020, most of the 31 billion IoT devices connected to the internet will be listed as vulnerable to hackers or non-hackers. Owning appropriate security control barriers.

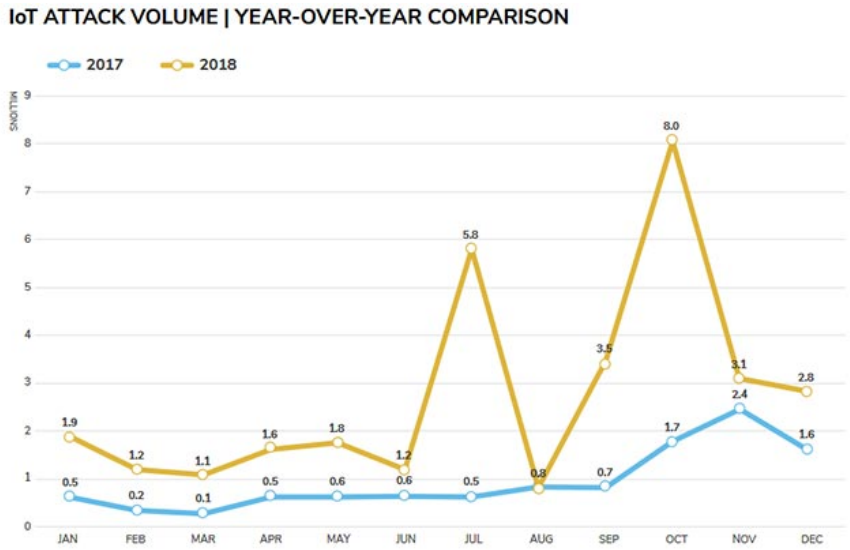
1. Endpoint Detection and Response threats, an emerging security technology

Not being protected by strong security control barriers makes IoT devices easily take control, and hackers will use them to add to the system of large-scale botnets within control. By exploiting security vulnerabilities that impact these IoT devices in large numbers, they can also take control of them by using the default public login information.

Many studies have also shown that the failure of IoT manufacturers to implement adequate security controls to protect this type of device from remote attacks has contributed significantly to the number. The number of attacks targeted at IoT infrastructure increased to a record 217.5% last year, ie from 10.3 million in 2017 to 32.7 in 2018, and is expected to remain this is even higher in 2019 if organizations and businesses do not soon make

reasonable defense measures.

More specifically, most botnets accumulating large amounts of IoT devices last year were tracked by SonicWall originating from the United States, with "more than 46% of global botnets originating from IP addresses based in Chinese flag, followed by China with 13% ".

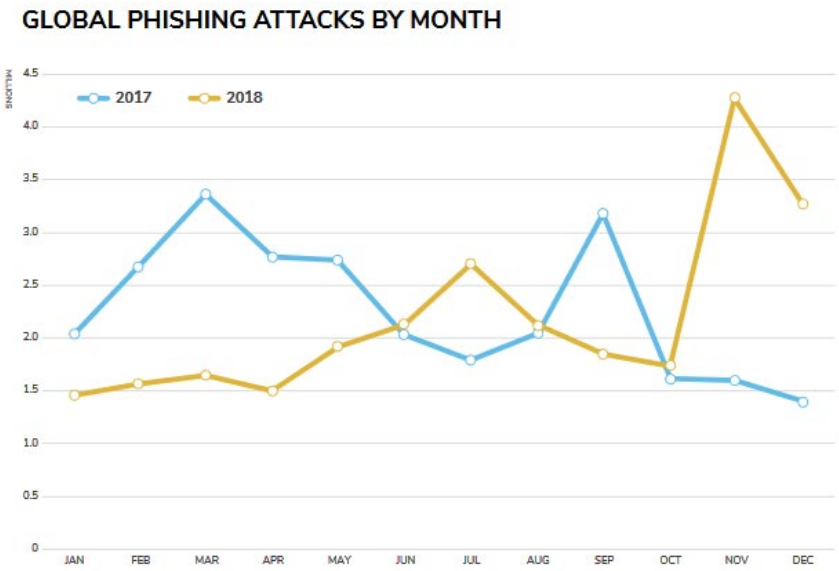


1. Fileless malware - Achilles heel of traditional antivirus software

Fortunately, most DDoS and spam attacks through which bad actors take advantage of botnets can be effectively prevented by using "content filter control tools to block traffic." Unwanted access or malicious access from some IP, country of origin or domain name on certain topics ".

On the other hand, 2018 witnessed a decline in the number of phishing attacks, the most common attack method commonly used by malicious agents, which is in fact the initial infection phase in most of the fraud and data hijacking campaigns. However, despite the decline in quantity, the scale and damage from this type of attack is still quite large.

To be more precise, while phishing is an almost constant contributor to malware-based attacks, companies and household users are increasingly aware of more clearly about the danger as well as its consequences. In addition, email-based attacks have also grown subtly as many security researchers find that "instead of deploying large, purposeless campaigns, cybercriminals tend to launch attacks on highly feasible systems, such as corporate email fraud (Business Email Compromise - BEC) ".



1. What is cybercrime? How to prevent cybercrime?

According to the information stated in 2019 Cyber ??Threat Report, "2018, SonicWall has recorded 26 million phishing attacks worldwide, a 4.1% decrease compared to 2017. During that time, the average customer of each customer SonicWall faces 5,488 phishing attacks ".

"The interest of getting security and privacy is becoming more urgent than ever. The network security and government teams in each country must work together closely and effectively to build a safer internet environment, reduce risks and at the same time build people's trust in the government and consumers for businesses, 'said Michael Chertoff, Executive Chairman and co-founder Chertoff Group, and former US Secretary of Homeland Security share.

In addition, "this report also provides important analysis on the development of security tactics and methods in cyberspace. In the context that organizations are increasingly relying more In analyzing data to understand and predict risk, this information will be very helpful for businesses and also the government in making wise decisions in investing in security systems. my honey '.

The data behind the statistics presented in SonicWall's 2019 Electronic Threat Report (2019) comes from the efforts of SonicWall Capture security intelligence researchers. Labs. Specifically, they had to analyze "more than 200,000 facts and samples of malware recorded daily to perform comparisons, analysis and record online criminal activity".

1. There were 12,449 serious data breaches recorded in 2018, an increase of 424% compared to 2017

SonicWall Capture Threat Network has been used to collect and record malware events and patterns with the help of about 1 million security sensors, from about 215 countries and territories around the world. .

Besides the information mentioned on SonicWall's Cyber ??Threat Report 2019 also includes the following important findings:

1. 10.52 billion malware attacks were blocked in 2018, the highest ever recorded by SonicWall.
2. More than 2.8 million encrypted malware attacks were blocked in 2018, up 27% from 2017 compared to 2017.
3. The number of ransomware attacks has increased by 11% over the previous year.
4. The number of web application attacks has increased by 56% compared to 2017.
5. 3.9 trillion times attempted to gain unauthorized access to network systems, the database has been recorded.

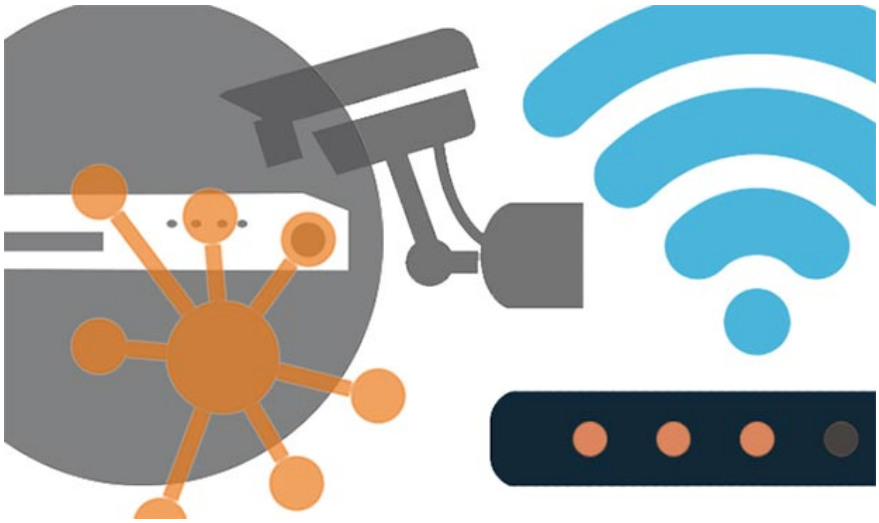
Calculations will still be difficult to predict in 2019

In related news, according to Avast's report last February, 40.8% of smart home systems come with at least one IoT device vulnerable to remote attacks, 33% of which are easy. Injured by using outdated software with unpatched security issues, while about two-thirds are hacked by a weak security system.

In addition, IoT medical devices (Medical IoT - IoMT) are considered as the top favorite of hackers because they often use outdated operating systems or contain too many security holes. More worrisome, according to an analysis of Check Point Research, in many cases, these devices are easily compromised and thus reveal sensitive data of many patients. This data is then often sold by crooks on the black market.

In addition, according to research conducted by SafeBreach's Dor Azouri security analyst in early March, many Windows 10 IoT Core devices were found to be victims of remote command-line attacks, Allows malicious agents to run arbitrary code with system privileges and not undergo authentication.

Not only that, Trend Micro also pointed out in its security report that software is obsolete on UPnP-enabled devices that allows an attacker to exploit a series of hidden vulnerabilities in messages. UPnP is used by many different server and utility systems that can be accessed via the Internet.



1. Supercomputers can completely detect cyber threats

Thus, it can be seen that 2019 will still be a challenging year for ensuring the network security situation on IoT devices in particular and on the entire global internet network in general.