Internet delle cose (IoT): Benvenuti nel selvaggio West

Luca Pesce, Senior Solutions Engineer, SonicWall

9 novembre 2021 orario 11.20-12.00 - StreamingEdition

#securitysummit #streamingedition

Luca Pesce

SENIOR SOLUTIONS ENGINEER, SONICWALL

SECURITY SUMMIT
Streaming Edition
9-10-11
novembre 2021

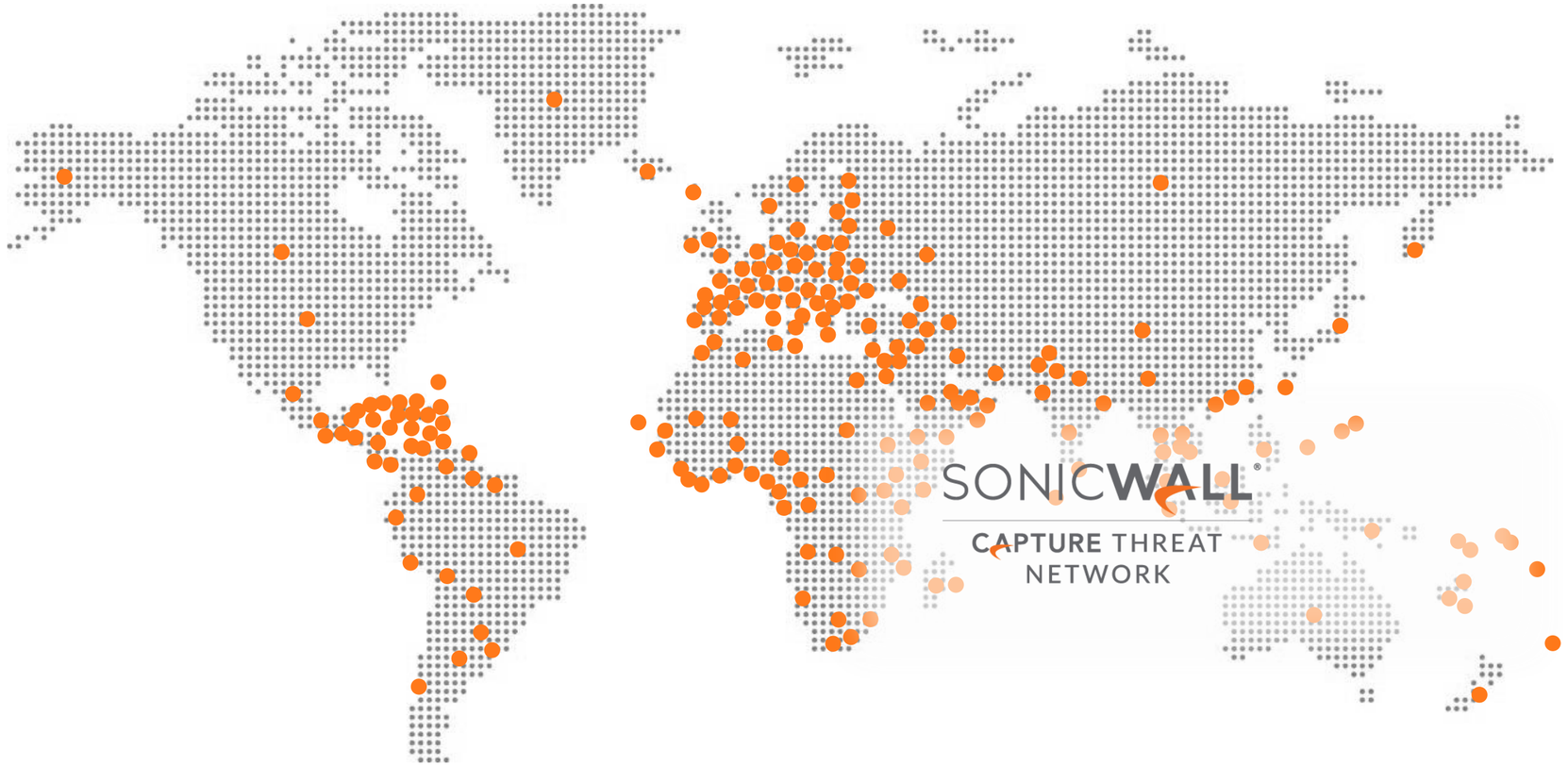
SONICWALL

The pandemic’s work-from-home reality resulted in an unprecedented change for organizations as they fought to defend exponentially greater attack surfaces from cybercriminals armed with powerful cloud-based tools, cloud storage and endless targets.

As working situations evolved, so did the methods of threat actors and motivated perpetrators.

SONICWALL

About the SonicWall Capture Labs Threat Network



1.1m+
Global Sensors

215+
Countries & Territories

24x7x365
Monitoring

<24hrs
Threat Response

140k+
Malware Samples Collected Daily

28m+
Malware Attacks Blocked Daily

Your new research destination

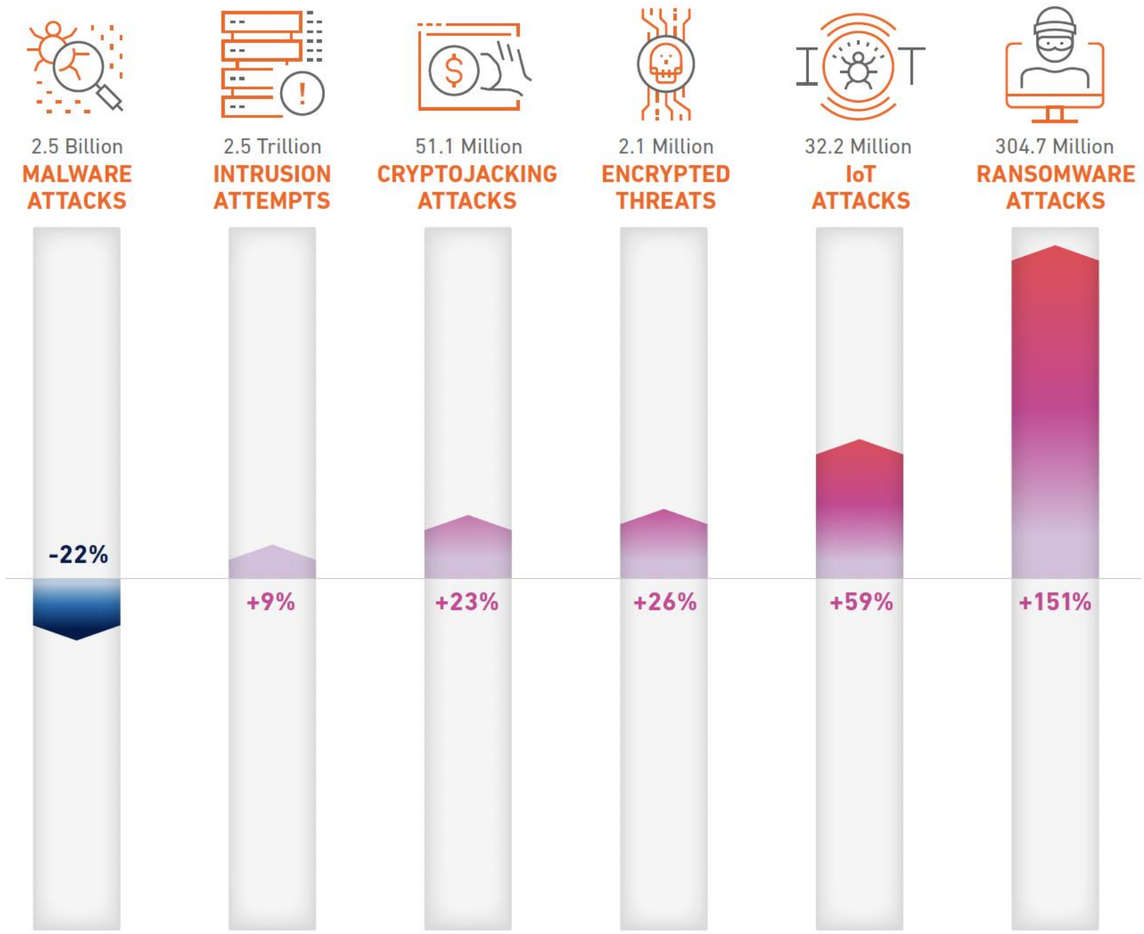
- With threats of almost every type on the rise, SonicWall in June introduced the Capture Labs Portal, a **free-to-use centralized repository for comprehensive research**.
- It offers direct access to information gathered by SonicWall's Capture Threat Network which includes:
  - SonicWall's internal malware analysis framework
  - Shared threat intelligence and exploits from industry groups and research organizations
  - Information from thirdparty researchers

2021 CYBER THREAT REPORT

2021 GLOBAL CYBERATTACK TRENDS

The 2021 SonicWall Cyber Threat Report highlights how COVID-19 provided **threat actors with ample opportunity to launch more powerful attacks**, thriving on the uncertainty of remote workforces navigating corporate networks from home.

These **trends** provide a glimpse into how cybercriminals operated as they brought the security industry to a critical tipping point in 2020.

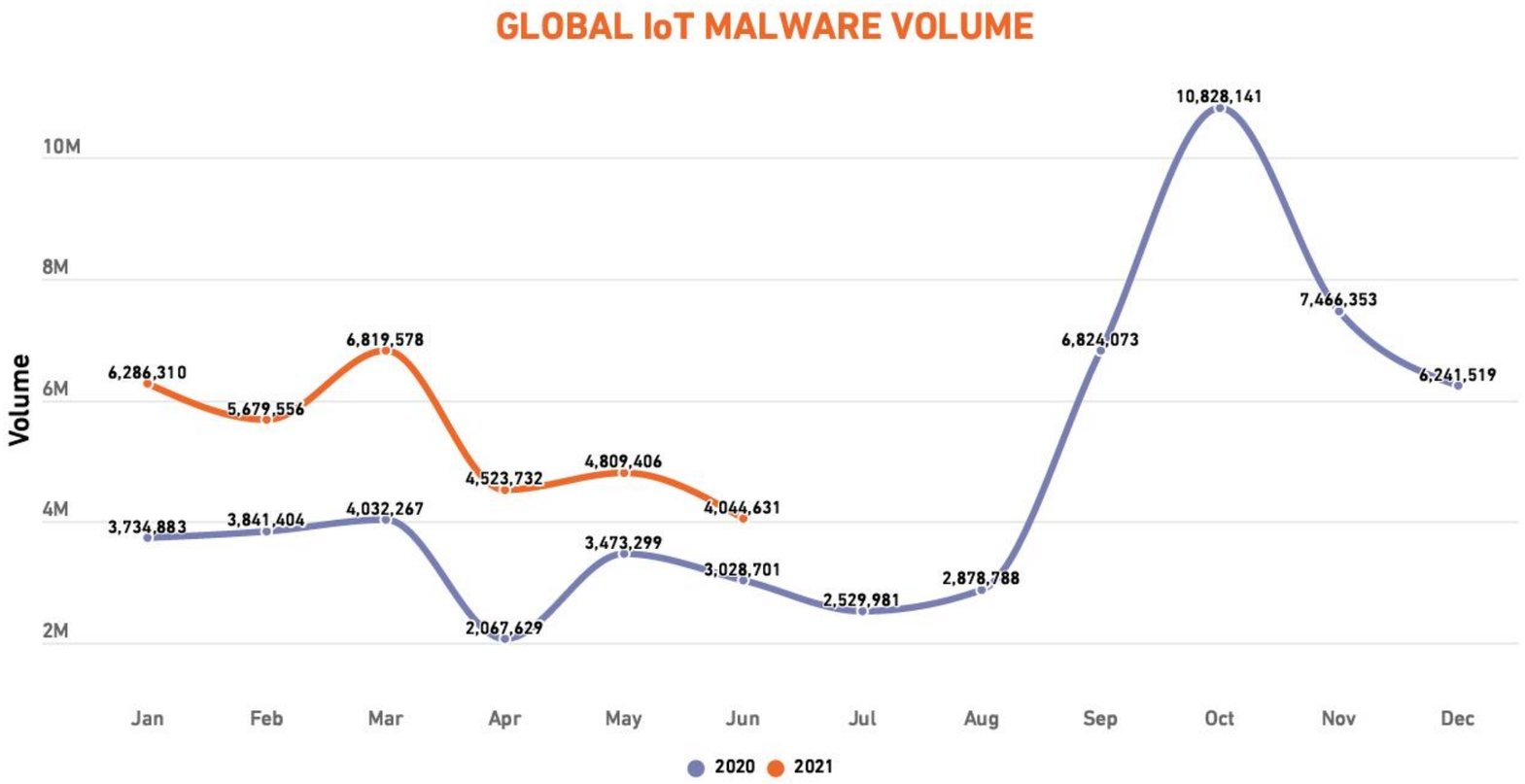


IoT Attacks Jump 59%

IoT malware has shown continued growth since 2018.

But in the first half of 2021, these attacks have increased even faster. IoT attack volume **in the first six months of 2021 rose 59%** over the first six months of 2020 — a period which itself showed a 50% increase over the same time in 2019.

In all, **32.2 million IoT attacks have been recorded so far this year**, compared with 20.2 million during the same time period last year.



Regulation to the rescue?

With the spectre of IoT attacks continuing to grow, **many legislative bodies opted to consider legislation strengthening cybersecurity** on these devices in 2021:

- **U.K.:** The U.K. Department for Digital, Culture, Media and Sport announced a new law that would ban the use of easy-to-guess default passwords in IoT devices. Manufacturers would be required to disclose the length of time they planned to continue offering security updates for these devices.
- **AUSTRALIA:** Due to a lack of response from manufacturers of lower-cost goods, the Australian government announced it is considering making mandatory a suite of voluntary regulations introduced last September.
- **U.S.:** In late March, legislation known as the Cyber Shield Act was reintroduced in Congress. If passed, the law would create security standards for IoT devices based on recommendations from an advisory committee made up of cybersecurity experts from the government, academia and the private sector.

Internet of Things (IoT)
Welcome to The Wild West

What Counts as an IoT Device?

The Problem with IoT Devices

- No Security on the IoT Device
- Insecure Deployment Choices
- Lack of Patching & Updates
- Poor IoT management – Shadow IT

Recent IoT News

MSSP Alert
IoT Hackers Target Millions of Devices in Pandemic, Report ...
Technology, manufacturing, retail, and healthcare industries accounted for 98 percent of IoT malware attack victims.
3 days ago

Ars Technica
Thinking about selling your Echo Dot—or any IoT device? Read this first
Most IoT devices, the Echo Dot included, use NAND-based flash memory to ... didn't save or use any of it to demonstrate additional attacks, ...
3 weeks ago

IT PRO
Critical supply chain flaw exposes IoT cameras to cyber attack
Critical supply chain flaw exposes IoT cameras to cyber attack. Hackers can exploit the vulnerability in ThroughTek's P2P SDK to spy on video ...
1 month ago

Infosecurity Magazine
Smart Home Experiences Over 12000 Cyber-Attacks in a Week
'Smart homes' could experience more than 12,000 cyber-attacks in a single week, ... in which a home was filled with numerous IoT devices, ...
3 weeks ago

SecurityBrief
Ransomware-as-a-service rising as cyber threats grow at alarming rates
... with attacks driven largely by the emergence of Ransomware as a ... dive into IoT security cameras highlights how quickly the attack ...
2 days ago

Softpedia News
New Botnet Dubbed Mirai Compromised Over 300,000 IoT ...
Cybercriminals used compromised IoT devices in order to launch massive DDoS attacks all around the world. Jul 6, 2021 12:49 GMT · By George Dascalu ...
2 weeks ago

Infosecurity Magazine
Smart Home Experiences Over 12000 Cyber-Attacks in a Week
'Smart homes' could experience more than 12,000 cyber-attacks in a single week, ... in which a home was filled with numerous IoT devices, ...
3 weeks ago

Softpedia News
IoT Attacks Increased 700% in just over Two Years
About 98% of IoT attack victims worked in the healthcare, retail & wholesale, manufacturing, and technology sectors.
5 days ago

SwordsToday.ie
Among the epidemics, the intensity of attacks on the Internet of ...
During the two weeks of last December, there were approximately 300,000 infiltration attempts using malicious software for IoT platforms. This ...
4 days ago

Security Intelligence
Poison in the Water: The Physical Repercussions of IoT ...
An Internet of things (IoT) security incident moved into the physical ... If consumed, this cyber-physical attack could have caused loss of ...
1 month ago

Softpedia News
IoT Attacks Increased 700% in just over Two Years
About 98% of IoT attack victims worked in the healthcare, retail & wholesale, manufacturing, and technology sectors.
5 days ago

designnews.com
Fierce Cyber Attacks Demand Enhanced IoT Security. But how ...
With all the ongoing ransomware and cyber-attacks, connected IoT devices need an extra layer of security. New legislation in both Europe and ...
1 month ago

Information Age | ACS
Industrial cyber-attacks will kill someone by 2025
In an Internet of Things (IoT) era where such systems are being connected to online and cloud systems faster than ever, however, ...
13 hours ago

CSO Online
Remote work raises threats from consumer IoT devices
Every consumer device an employee connects to their router or smartphone increases the potential attack surface for a company now that many ...
2 Feb 2021

designnews.com
Fierce Cyber Attacks Demand Enhanced IoT Security. But how ...
With all the ongoing ransomware and cyber-attacks, connected IoT devices need an extra layer of security. New legislation in both Europe and ...
1 month ago

Types of IoT Attack

- Physical Attacks
- DDoS/DoS
- Firmware Hijacking
- Privilege Escalation
- Man-In-The Middle
- Ransomware
- Eaves Dropping
- Botnets

Mirai Botnet – The DDoS Monster

- Mirai grew exponentially, doubling infections every 76 minutes
- 65,000 devices were compromised by day 2
- Deutsche Telekom had over 900,000 routers taken offline by Mirai
- Mirai's two most compromised IoT devices types were **IP Cameras** and **Routers**

The Case of The Internet Connected Fish Tank

- A US based, unnamed, casino was successfully hacked
- High levels of security. Both network and physical were present
- The casino was breached by a smart thermometer in the lobby fish tank
- Cybercriminals used the thermometer to exfiltrate the casino’s high-roller database

The Problems With Printers

- Auto firmware update is often off by default
- Firmware vulnerabilities allow easy remote rooting
- The Treck TCP/IP library has 19 serious vulnerabilities (Ripple20)
- Printer Job Language (PJL) scripts, embedded in documents, can execute code on a printer
- 56% of enterprise companies ignore printers in their endpoint security strategy – Ponemon Institute

Food For Thought

By 2025, forecasts suggest that there will be more than **75 billion Internet of Things (IoT) connected devices in use**. – Statista Research Department

A survey of 540 security pros found that **84% of organizations have IoT devices on their corporate networks**. This survey also showed that over 50% of these organisations didn't have the necessary security measures in place beyond default passwords – Extreme Networks

More than 90% of enterprises, surveyed by Quocirca, reported experiencing at least one data loss through unsecured printing

Out of 1000 organisations surveyed 43% of respondents reported that they had "unprotected devices" accessing corporate data – Innovate MR

Households experience, on average, **104 cybersecurity threats a month**. – Comcast

The Awkward Truth

- There are always more important and more pressing issues that need to be dealt with first
- Some IoT devices are not even considered IoT until it’s too late
- IoT device functionality always comes before security
- Reporting fatigue

How to Protect Your Organisation

- **Plan for IoT in your endpoint strategy** – don’t forget printers!
- **Don’t have a flat network** – segmentation is key
- **Firmware update and patch your IoT devices regularly**
- **Apply firewall policies to your IoT devices and their subnets**
- **Be aware of Shadow IT and monitor for it** – monitor effectively

Q&A

Luca Pesce, Senior Solutions Engineer, SonicWall
italy@sonicwall.com – www.sonicwall.com

Vieni a trovarci al nostro virtual desk!