Hacking

DDoS attack that disrupted internet was largest of its kind in history, experts say

Dyn, the victim of last week's denial of service attack, said it was orchestrated using a weapon called the Mirai botnet as the 'primary source of malicious attack'

RECORDED FUTURE BLOG

Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018

By Priscilla Moriuchi and Sanil Chohan on April 5, 2018

WIRED SUBSCRIBE

ANDY GREENBERG SECURITY 10.20.17 05:45 PM

THE REAPER IOT BOTNET HAS ALREADY INFECTED A MILLION NETWORKS

7 Variants (So Far) of Mirai

Mirai is an example of the newest trend in rapidly evolving, constantly improving malware. These seven variants show how threat actors are making bad malware worse.

root xc3511	user user	guest 12345	root ikwb
root vizxv	admin (none)	admin1 password	root dreambox
root admin	root pass	administrator 1234	root user
admin admin	admin admin1234	666666 666666	root realtek
root 888888	root 1111	888888 888888	root 00000000
root xmhdipc	admin smcadmin	ubnt ubnt	admin 1111111
root default	admin 1111	root klv1234	admin 1234
root juantech	root 666666	root Zte521	admin 12345
root 123456	root password	root hi3518	admin 54321
root 54321	root 1234	root jvbzd	admin 123456
support support	root klv123	root anko	admin 7ujMko0admin
root (none)	Administrator admin	root zlxx.	admin 1234
admin password	service service	root 7ujMko0vizxv	admin pass
root root	supervisor supervisor	root 7ujMko0admin	admin meinsm
root 12345	guest guest	root system	tech tech

> ***MIRAI was able to infect over 600,000 IoT devices by simply exploiting a set of 64 well-known default IoT login/password combinations.***

From July to September 2017, SecurityScorecard identified 34,062 IPv4 addresses on the public internet that showed symptoms expected from an embedded device infected with the Mirai IoT malware. This contrasts with 184,258 IPv4 addresses of IoT devices infected with Mirai IoT malware from August 1, 2016, to July 31, 2017.

MOTHERBOARD Moveable Hacking Environment

NEWS | By Lorenzo Franceschi-Bicchierai | Aug 7 2016, 7:00am

Hackers Make the First-Ever Ransomware for Smart Thermostats

White hat hackers have made the first proof of concept for malware that locks a smart thermostat and demands a ransom.

WIRED The Untold Story of NotPetya, the Most Devastating Cyberattack in SIGN IN | SUBSCRIBE

MIKE MCQUADE

ANDY GREENBERG SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Victoria

Traffic cameras in Victoria infected by WannaCry ransomware

State government says 55 cameras were affected after a contractor introduced the virus to the system by mistake

CSO FROM IDG INSIDER Sign In | Register

Report: IoT is the next frontier for ransomware

The growth of the Internet of Things will offer new ransomware opportunities for cybercriminals, according to a report released Thursday by Symantec

THE COST OF NOTPETYA

In 2017, the malware NotPetya spread from the servers of an unassuming Ukrainian software firm to some of the largest businesses worldwide, paralyzing their operations. Here's a list of the approximate damages reported by some of the worm's biggest victims.

$870,000,000

Pharmaceutical company Merck

$400,000,000

Delivery company FedEx (through European subsidiary TNT Express)

$384,000,000

French construction company Saint-Gobain

$300,000,000

Danish shipping company Maersk

$188,000,000

Snack company Mondelez (parent company of Nabisco and Cadbury)

$129,000,000

British manufacturer Reckitt Benckiser (owner of Lysol and Durex condoms)

$10 BILLION

Total damages from NotPetya,