Threat STOP

Most Infamous Botnets

of the 21st Century

2000

GTbot

Based on an mIRC-client, GTbot was the first Denial of Service botnet.

Earthlink Spammer

Built by Khan K. Smith, this botnet sent over 1.25M phishing emails, earning Khan over $3M USD.

2007

ZeuS/Zbot

This banking botnet is notorious for its size (3.6M PCs by 2009) and famous heists - one heist raked in $70M USD from US banks.

Storm

One of the first known P2P botnets, Storm got up to 1M bots partaking in an array of criminal activity. The botnet was taken down in 2008.

Cutwail

Boasting 2M bots, this botnet sent out 74 billion spam emails a day at its peak, making up 46.5% of the world's spam volume at the time.

Bayrob

Active between 2007-2016, Byrob's activity varied from eBay scams, to spam and cryptomining.

Srizbi

In 2007/2008, Srizbi was responsible for 60% of all spam worldwide, until botnet's hosting server was taken offline in 2008

2008

Grum

Specializing in spam, mainly pharmaceutical themed, Grum sent out up to 39.9 billion emails a day before it was shut down in 2012.

Kraken

Kraken is best known for infecting 10% of all Fortune 500 companies.

Mariposa

Mariposa botnet used malvertising to recruit over 10M bots before being taken down by Spanish law enforcement.

Conficker

This extremely famous computer worm created a botnet by spreading to millions of computers worldwide.

2009

ZeroAccess

Built using the ZeroAccess rootkit, this botnet made money in many ways until its takedown in 2013 - click-fraud, web ads and bitcoin mining.

Bamital

Also taken down in 2013, Bamital is believed to have infected 1.8M computers, luring victims to download malware.

Bredolab

Bredolab used its 30M bots to send out massive quantities of spam until Dutch law enforcement took down its C&C servers in 2010.

2010

Gameover ZeuS

Built on the leaked source code of the ZeuS trojan, this botnet stole banking information and was the primary distributor of CryptoLocker ransomware.

Kelihos

It took four attempts for authorities to take this botnet down, which distributed tons of spam for years.

Ramnit

Another botnet based on the ZeuS trojan source code. Authorities sinkholed the first version, but the botnet resurfaced and is still active today.

2011

Andromeda

Many criminal gangs operated Andromeda botnet over the years, whose source code was leaked online, creating networks with up to 2M bots.

Dridex

One of the most infamous today, this P2P botnet has a variety of info stealing and keylogging functions.

2012

Necurs

This spam botnet reach over 6M devices by 2016. Rumored to have been created by TA505, Necurs is a main distributor of the Dridex trojan.

2014

Bashlite

Created by members of the Lizard Squad hacking group, this IoT malware and botnet is primarily used to carry out DDoS attacks.

Emotet

Emotet is the world's leading Malware-as-a-Service. Boasting an extravagant variety of capabilities and modules, it has been claimed to be the most dangerous botnet today.

Windigo

This botnet, which went undetected for 3 years, infected over 10,000 Linux servers, allowing it to send out 35 million malicious emails per day.

2015

Methbot

The largest ad-fraud botnet in history, Methbot generated between $3-6 million per day in PPC advertising schemes. The botnet was taken down in 2016.

2016

Mirai

This extremely famous IoT botnet exploits devices like air-quality monitors, surveillance cameras, etc., and has temporarily taken down huge companies such as OVH, Dyn and Krebs on Security using DDoS attacks.

Trickbot

Trickbot was built upon the Dyre Banking Trojan, yet it quickly developed in to a malware installer and botnet, at the same time as Emotet started similarly shifting focus.

2017

Hajime

The first IoT botnet to use P2P architecture, this botnet is believed to be used to proxy malicious traffic and carry out credential stuffing attacks.

Smominru

Also called MyKings or Hexmen, this is the biggest solely-cryptomining botnet active today. Smominru has already mined millions of dollars worth of Monero.

2018

3ve

3ve is said to be the most advanced click-fraud botnet ever assembled. The botnet ran three simultaneous operations, and its takedown is considered historic.

2020

Dark Nexus

Boasting advanced features and evasion techniques, some say Dark Nexus puts other IoT botnets to shame. Researchers are on the lookout for this botnet's next move.

Threat STOP