Mikrotik

MikroTik

MikroTik (officially SIA "Mikrot?kls") is a Latvian network equipment manufacturing company. MikroTik develops and sells wired and wireless network routers

MikroTik (officially SIA "Mikrot?kls") is a Latvian network equipment manufacturing company. MikroTik develops and sells wired and wireless network routers, network switches, access points, as well as operating systems and auxiliary software. The company was founded in 1996, and as of 2023, it was reported that the company had 367 employees.

With its headquarters in Riga, Latvia, MikroTik serves a diverse array of customers around the world. The company's products and services are utilized in various sectors, such as telecommunications, government agencies, educational institutions, and enterprises of all sizes.

In 2022, with a value of €1.30 billion, Mikrotik was the 4th largest company in Latvia and the first private company to surpass €1 billion value in Latvia.

List of TCP and UDP port numbers

docs". "Neighbor discovery

RouterOS - MikroTik Documentation". "Manual:IP/Services - MikroTik Wiki". wiki.mikrotik.com. Retrieved 2024-02-22. "NCPA Configuration" - This is a list of TCP and UDP port numbers used by protocols for operation of network applications. The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) only need one port for bidirectional traffic. TCP usually uses port numbers that match the services of the corresponding UDP implementations, if they exist, and vice versa.

The Internet Assigned Numbers Authority (IANA) is responsible for maintaining the official assignments of port numbers for specific uses, However, many unofficial uses of both well-known and registered port numbers occur in practice. Similarly, many of the official assignments refer to protocols that were never or are no longer in common use. This article lists port numbers and their associated protocols that have experienced significant uptake.

Dynamic frequency selection

(Nov 16, 2016). "Radar Detection and DFS on MikroTik" (PDF). Radar Detect and DFS on MikroTik. MikroTik. Retrieved 4 December 2019 – via YouTube. Decision

Dynamic Frequency Selection (DFS) is a channel allocation scheme specified for wireless LANs, commonly known as Wi-Fi. It is designed to prevent electromagnetic interference by avoiding co-channel operation with systems that predated Wi-Fi, such as military radar, satellite communication, and weather radar, and also to provide on aggregate a near-uniform loading of the spectrum (uniform spreading). It was standardized in 2003 as part of IEEE 802.11h.

Notre Dame University (Philippines)

University has become a MikroTik Academy in the Philippines. This opportunity means the College of Computer Studies can offer MikroTik Certified Associate

Notre Dame University (NDU) is a private Catholic research basic and higher education institution run by the Missionary Oblates of Mary Immaculate in Cotabato City, Philippines. It was founded by the Oblates in 1948 and has been a member of the Notre Dame Educational Association, a group of schools in the Philippines named Notre Dame. The Association is under the patronage of the Blessed Virgin Mary.

Notre Dame University has academic programs in graduate school, law, liberal arts, arts and sciences, engineering, nursing, accountancy, business administration, computer studies and education, as well as secondary, elementary, and preparatory education.

Denial-of-service attack

pipelining DDoS attack on Sept. 5. 2021 that originated from unpatched Mikrotik networking gear. In the first half of 2022, the Russian invasion of Ukraine

In computing, a denial-of-service attack (DoS attack) is a cyberattack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. The range of attacks varies widely, spanning from inundating a server with millions of requests to slow its performance, overwhelming a server with a substantial amount of invalid data, to submitting requests with an illegitimate IP address.

In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. More sophisticated strategies are required to mitigate this type of attack; simply attempting to block a single source is insufficient as there are multiple sources. A DDoS attack is analogous to a group of people crowding the entry door of a shop, making it hard for legitimate customers to enter, thus disrupting trade and losing the business money. Criminal perpetrators of DDoS attacks often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways. Revenge and blackmail, as well as hacktivism, can motivate these attacks.

List of file signatures

23 40 7E 5E #@~^ 0 vbe VBScript Encoded script 0D F0 1D C0 ?ð?À 0 cdb MikroTik WinBox Connection Database (Address Book) 23 45 58 54 4D 33 55 #EXTM3U

A file signature is data used to identify or verify the content of a file. Such signatures are also known as magic numbers or magic bytes and are usually inserted at the beginning of the file.

Many file formats are not intended to be read as text. If such a file is accidentally viewed as a text file, its contents will be unintelligible. However, some file signatures can be recognizable when interpreted as text. In the table below, the column "ISO 8859-1" shows how the file signature appears when interpreted as text in the common ISO 8859-1 encoding, with unprintable characters represented as the control code abbreviation or symbol, or codepage 1252 character where available, or a box otherwise. In some cases the space character is shown as ?.

Internet of things

infected devices were identified as Dahua, Huawei, ZTE, Cisco, ZyXEL and MikroTik. In May 2017, Junade Ali, a computer scientist at Cloudflare noted that

Internet of things (IoT) describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communication networks. The IoT encompasses electronics, communication, and computer science engineering. "Internet of things" has been considered a misnomer because devices do not need to be connected to the public internet;

they only need to be connected to a network and be individually addressable.

The field has evolved due to the convergence of multiple technologies, including ubiquitous computing, commodity sensors, and increasingly powerful embedded systems, as well as machine learning. Older fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), independently and collectively enable the Internet of things. In the consumer market, IoT technology is most synonymous with "smart home" products, including devices and appliances (lighting fixtures, thermostats, home security systems, cameras, and other home appliances) that support one or more common ecosystems and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. IoT is also used in healthcare systems.

There are a number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of privacy and security, and consequently there have been industry and government moves to address these concerns, including the development of international and local standards, guidelines, and regulatory frameworks. Because of their interconnected nature, IoT devices are vulnerable to security breaches and privacy concerns. At the same time, the way these devices communicate wirelessly creates regulatory ambiguities, complicating jurisdictional boundaries of the data transfer.

VPNFilter

DSR-1000N Huawei HG8245 Linksys E1200 E2500 E3000 E3200 E4200 RV082 WRVS4400N Mikrotik CCR1009 CCR1016 CCR1036 CCR1072 CRS109 CRS112 CRS125 RB411 RB450 RB750

VPNFilter is malware designed to infect routers and certain network attached storage devices. It is estimated to have infected approximately 500,000 routers worldwide at its peak, though the number of at-risk devices is larger. It can steal data, contains a "kill switch" designed to disable the infected router on command, and is able to persist should the user reboot the router. The FBI believes that it was created by the Russian Fancy Bear group. In February 2022, the CISA announced that a new malware called Cyclops Blink produced by Sandworm had replaced VPNFilter.

List of networking hardware vendors

by HPE Linksys

acquired by Belkin Meraki - acquired by Cisco Systems MikroTik Mitsubishi Motorola NEC Netgear Nokia Nokia Networks Open Mesh - acquired - Networking hardware typically refers to equipment facilitating the use of a computer network. Typically, this includes routers, switches, access points, network interface cards and other related hardware. This is a list of notable vendors who produce network hardware.

Electromagnetic interference

(Nov 16, 2016). "Radar Detection and DFS on MikroTik" (PDF). Radar Detect and DFS on MikroTik. MikroTik. Retrieved 4 December 2019 – via YouTube. Decision

Electromagnetic interference (EMI), also called radio-frequency interference (RFI) when in the radio frequency spectrum, is a disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction. The disturbance may degrade the performance of the circuit or even stop it from functioning. In the case of a data path, these effects can range from an increase in error rate to a total loss of the data. Both human-made and natural sources generate changing electrical currents and voltages that can cause EMI: ignition systems, cellular network of mobile phones, lightning, solar flares, and auroras (northern/southern lights). EMI frequently affects AM radios. It can also affect mobile phones, FM radios, and televisions, as well as observations for radio astronomy and atmospheric science.

EMI can be used intentionally for radio jamming, as in electronic warfare.

https://www.onebazaar.com.cdn.cloudflare.net/$15712194/eadvertiser/pregulatey/zparticipatek/volvo+penta+stern+d
https://www.onebazaar.com.cdn.cloudflare.net/$86500846/ntransferx/sregulateq/tattributef/dahleez+par+dil+hindi+e
https://www.onebazaar.com.cdn.cloudflare.net/!40583839/ltransferf/videntifyh/zparticipatey/the+boy+who+harnesse
https://www.onebazaar.com.cdn.cloudflare.net/=23350002/zdiscovert/ncriticizeh/uorganisec/honda+st1300+abs+serv
https://www.onebazaar.com.cdn.cloudflare.net/^92051994/lapproachd/fregulatez/kparticipateg/navistar+internationa
https://www.onebazaar.com.cdn.cloudflare.net/@58899065/uprescribez/arecogniser/wattributeo/chapter+12+stoichio
https://www.onebazaar.com.cdn.cloudflare.net/^96926995/lcontinueg/tdisappeary/jovercomez/literature+in+english+
https://www.onebazaar.com.cdn.cloudflare.net/-16081159/atransferk/brecognisef/srepresentj/parts+manual+for+kubota+v1703+engine.pdf
https://www.onebazaar.com.cdn.cloudflare.net/-92022753/ytransfert/vwithdrawj/oorganisef/dynamics+11th+edition+solution+manual.pdf
https://www.onebazaar.com.cdn.cloudflare.net/=66098519/uexperiencex/adisappears/iovercomet/21+century+institu