Issue Number: 43 December' 12 - January' 13

IT UNLIMITED

KONGU ARTS AND SCIENCE COLLEGE

NANJANAPURAM, ERODE

DEPARTMENT OF COMPUTER SCIENCE[UG]

CYBER CREWS ASSOCIATION

CONTENTS

BOTNET

What is a botnet?

The term *bot* is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the Internet, without you knowing it.

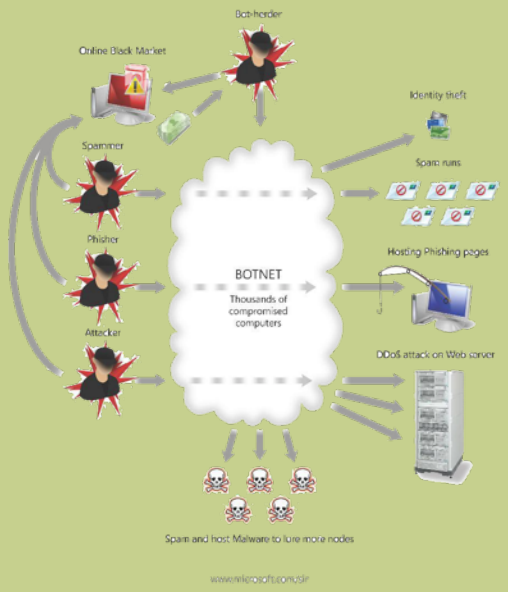
Criminals typically use bots to infect large numbers of computers. These computers form a network, or a *botnet*.

Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If your computer becomes part of a botnet, your computer might slow down and you might inadvertently be helping criminals.

Zombie Army

A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion.

Computers that are co opted to serve in a zombie army are often those whose owners fail to provide effective firewalls and other safeguards. An increasing number of home users have high speed connections for computers that may be inadequately protected. A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation.



Top 5 biggest botnets

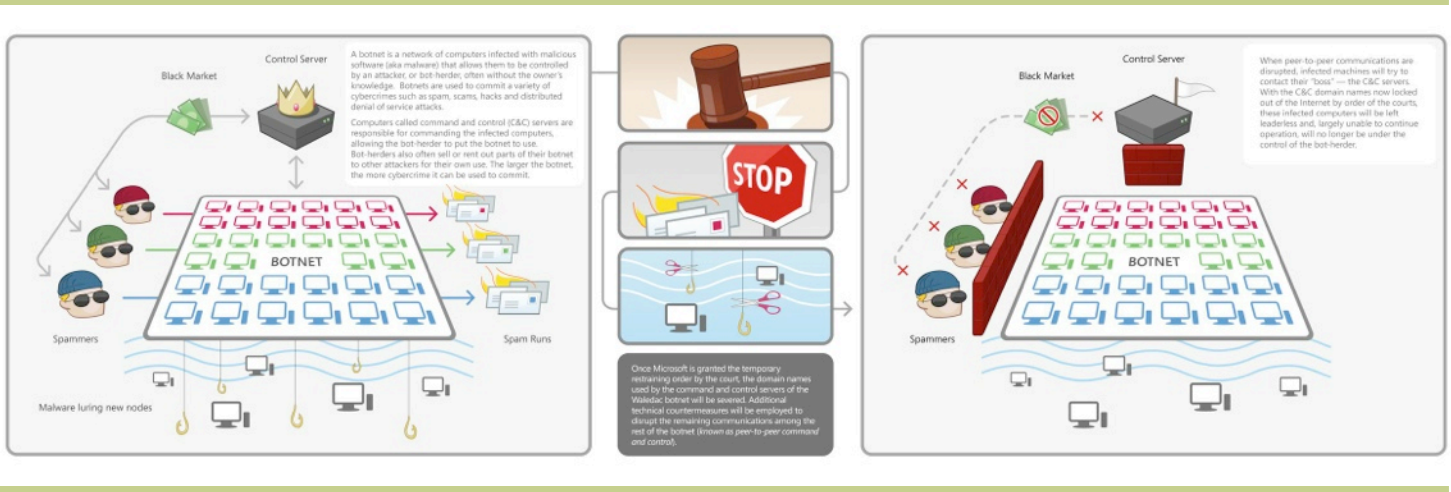
1. Rustock (generating 43% of all spam)

The current king of spam, its malware employs a kernel-mode rootkit, inserts random text into spam and is capable of TLS encryption. Concentrates solely on pharmaceutical spam.

BOTNET

2. Mega-D (10.2%)

A long-running botnet that has had its ups and downs, owing to the attention it attracts from researchers. Concentrates mostly on pharmaceutical spam.



3. Festi (8%)

A newer spambot that employs a kernel mode rootkit and is often installed alongside Pushdo on the same host.

4. Pushdo (6.3%)

A multi-faceted botnet or botnets, with many different types of campaigns. A major distributor of malware downloaders and blended threat emails, but also sends pharma, replica, diploma and other types of spam.

5. Grum (6.3%)

Also employs a kernel-level rootkit. A wide range of spamming templates changes often, served up by multiple web servers. Mostly pharma spam.

The Future of Botnets

A lot of people in the security industry are paid to think like attackers: pen testers, security consultants, software security experts. But some of these people have never met an actual black hat, so much of their work is necessarily based on what they *think* attackers might do in a given situation. Considering the stakes in today's security game, gleaning intelligence from professional attackers is an invaluable experience for researchers on the other side of the ball. Robert Hansen, a security researcher and CEO of SecTheory, has been doing just that in recent months, having a series of off-the-record conversations with spammers and malicious hackers in an effort to gain insight into their tactics, mindset and motivation. He's not the type to hack randomly, he's only interested in targeted attacks with big payouts. Sure, if you really work at it for days or weeks you'll get in, almost always, but it's not like it used to be where you'd just run a handful of basic tests and you were guaranteed to break in. The risk is that now when he

BOTNET

sends his mules to go cash out, there's a chance they'll get nailed. Well, the more I thought about it the more I thought that this is a very solvable problem for bad guys. There are already other types of bad guys who do things like spam, steal credentials and DDoS.

For that to work they need a botnet with thousands or millions of machines. The chances of a million machine botnet having compromised at least one machine within a target of interest is relatively high.

Hansen's solution to the hacker's problem provides a glimpse into a busines model we might see in the not-too-distant future. It's an evolutionary version of the botnet-for-hire or malware-as-a-service model that's taken off in recent years. In Hansen's model, an attacker looking to infiltrate a specific network would not spend weeks throwing resources against machines in that network, looking for a weak spot and potentially raising the suspicion of the company's security team.

Instead, he would contact a botmaster and give him a laundry list of the machines or IP addresses he's interested in compromising.

If the botmaster already has his hooks into the network, the customer could then buy access directly into the network rather than spending his own time and resources trying to get in.

This model makes sense on a number of levels and may well have been implemented already. The value of a large botnet for executing DDoS attacks or extracting valuable data from the compromised machines could be multiplied hundreds or thousands of times using this model.

ETHERNET

Ethernet is a family of computer networking technologies for local area networks (LANs). Ethernet was commercially introduced in 1980 and standardized in 1985 as IEEE 802.3. Ethernet has largely replaced competing wired LAN technologies.The Ethernet standards comprise several wiring and signaling variants of the OSI physical layer in use with Ethernet. The original 10BASE5 Ethernet used coaxial cable as a shared medium. Later the coaxial cables were replaced by twisted pair and fiber optic links in conjunction with hubs or switches. Data rates were periodically increased from the original 10 megabits per second, to 100 gigabits per second.

History

Ethernet was developed at Xerox PARC between 1973 and 1974. It was inspired by ALOHAnet, which Robert Metcalfe had studied as part of his PhD dissertation. The idea was first documented in a memo that Metcalfe wrote on May 22, 1973. In 1975, Xerox filed a patent application listing Metcalfe, David Boggs, Chuck Thacker and Butler Lampson as inventors. In 1976, after the system was deployed at PARC, Metcalfe and Boggs published a seminal paper.

Standardization

In February 1980, the Institute of Electrical and Electronics Engineers (IEEE) started project 802 to standardize local area networks (LAN). The "DIX-group" with Gary Robinson (DEC), Phil Arts (Intel), and Bob Prints (Xerox) submitted the so-called "Blue Book" CSMA/CD specification as a candidate for the LAN specification. In addition to CSMA/CD, Token Ring (supported by IBM) and Token Bus (selected and henceforward supported by General Motors) were also considered as candidates for a LAN standard. Competing proposals and broad interest in the initiative led to strong disagreement over which technology to standardize.

Evolution

Ethernet evolved to include higher bandwidth, improved media access control methods, and different physical media. The coaxial cable was replaced with point-to-point links connected by Ethernet repeaters or switches to reduce installation costs, increase reliability, and improve management and troubleshooting. Many variants of Ethernet remain in common use.

Shared media

Repeaters and hub

Bridging and switching

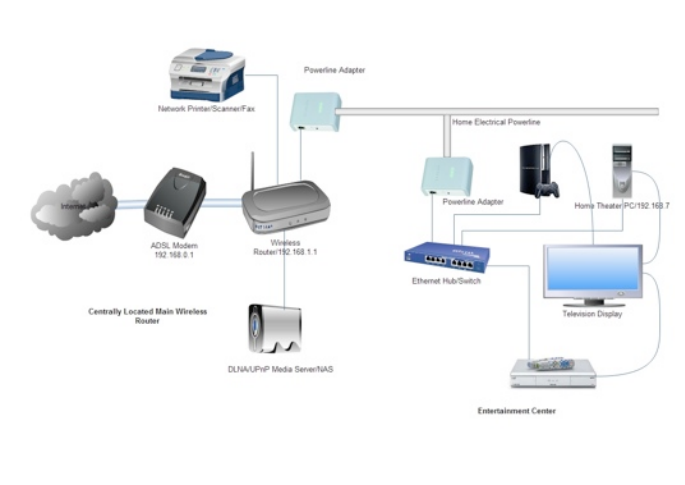
Advanced networking

ETHERNET

Varieties of Ethernet

The Ethernet physical layer evolved over a considerable time span and encompasses coaxial, twisted pair and fiber optic physical media interfaces and speeds from 10 Mbit to 100 Gbit. The most common forms used are 10BASE-T, 100BASE-TX, and 1000BASE-T.

All three utilize twisted pair cables and 8P8C modular connectors. They run at 10 Mbit/s, 100 Mbit/s, and 1 Gbit/s, respectively. Fiber optic variants of Ethernet offer high performance, electrical isolation and distance (tens of kilometers with some versions). In general, network protocol stack software will work similarly on all varieties.



Ethernet frames

A data packet on the wire is called a frame. A frame begins with preamble and start frame delimiter, followed by an Ethernet header featuring source and destination MAC addresses.

The middle section of the frame consists of payload data including any headers for other protocols (e.g., Internet Protocol) carried in the frame. The frame ends with a 32-bit cyclic redundancy check, which is used to detect corruption of data in transit.

MALWARE

Malware, short for **malicious** (or malevolent) **software**, is software used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. 'Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.

Malware includes computer viruses, worms, trojan horses, spyware, adware, and other malicious programs. In law, malware is sometimes known as a **computer contaminant**, as in the legal codes of several U.S. states. Malware is not the same as defective software, which is software that has a legitimate purpose but contains harmful bugs that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official company website. An example of this is software used for harmless purposes that is packed with additional tracking software that gathers marketing statistics.

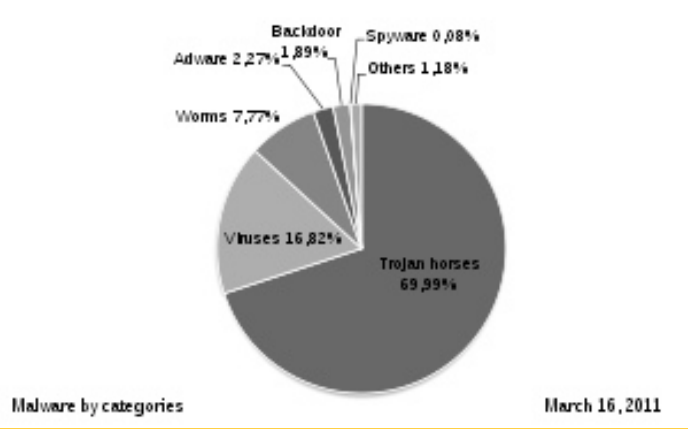
Malware has caused the rise in use of protective software types such as anti virurs, anti-malware, and firewalls. Each of these are commonly used by personal users and corporate networks in order to

History of viruses and worms

Before Internet access became widespread, viruses spread on personal computers by infecting the executable boot sectors of floppy disks. By inserting a copy of itself into the machine code instructions in these executables, a virus causes itself to be run whenever a program is run or the disk is booted. Early computer viruses were written for the Apple II and Macintosh, but they became more widespread with the dominance of the IBM PC and MS-DrOS system. Executable-infecting viruses are dependent on users exchanging software or boot-able floppies, so they spread rapidly in computer hobbyist circles

Purposes

Many early infectious programs, including the first Internet Worm, were written as experiments or pranks. Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others.



Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general. However, malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on. Left un-guarded, personal and networked computers can be at considerable risk against these threats. (These are most frequently counter-acted by various types

MALWARE

of firewalls, anti virus software, and network hardware).

Since the rise of widespread broadband Internet access, malicious software has more frequently been designed for profit. Since 2003, the majority of widespread viruses and worms have been designed to take control of users' computers for black-market exploitation. Infected "zombie computers" are used to send email spam, to host contraband data such as child pornography, or to engage in distributed denial-of-service attacks as a form of extortion.

Vulnerability to malware

Use of the same operating system

An oft-cited cause of vulnerability of networks is consistent use of the same operating system. For example, Microsoft Windows or Mac OS X have such a large share of the market that concentrating on either could enable an exploited vulnerability to subvert a large number of systems.

Instead, introducing diversity, purely for the sake of robustness, could increase short-term costs for training and maintenance. However, having a few diverse nodes would deter total shutdown of the network, and allow those nodes to help with recovery of the infected nodes. Such separate, functional redundancy could avoid the cost of a total shutdown.

Anti-malware strategies

Website security scans

As malware also harms the compromised websites (by breaking reputation, blacklisting in search engines, etc.), some websites offer vulnerability scanning. Such scans check the website, detect malware, may note outdated software, and may report known security issues.

Eliminating over-privileged code

Over-privileged code dates from the time when most programs were either delivered with a computer or written in-house, and repairing it would at a stroke render most antivirus software almostredundant. It would, however, have appreciable consequences for the user interface and system management.

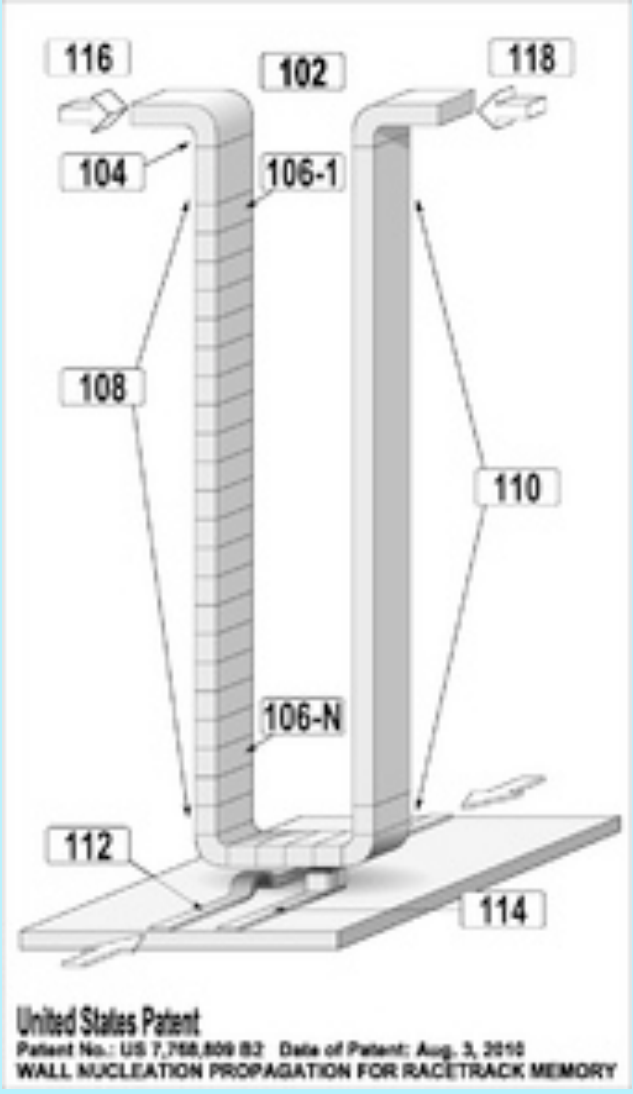
The system would have to maintain privilege profiles, and know which to apply for each user and program. In the case of newly installed software, an administrator would need to set up default profiles for the new code.

RACETRACK MEMORY

Racetrack memory (or domain-wall memory (DWM)) is an experimental non-volatile memory device under development at IBM's Almaden Research Center by a team led by Stuart Parkin. In early 2008, a 3-bit version was successfully demonstrated. If it is developed successfully, racetrack would offer storage density higher than comparable solid-state memory devices like flash memory and similar to conventional disk drives, and also have much higher read/write performance. It is one of a number of new technologies trying to become a universal memory in the future.

Description

Racetrack memory uses a spin-coherent electric current to move magnetic domains along a nanoscopic permalloyr wire about 200 nm across and 100 nm thick. As current is passed through the wire, the domains pass by magnetic read/write heads positioned near the wire, which alter the domains to record patterns of bits. A racetrack memory device is made up of many such wires and read/write elements. In general operational concept, racetrack memory is similar to the earlier bubble memory of the 1960s and 1970s. Delay line memory, such as mercury delay lines of the 1940s and 1950s are a still earlier form of similar technology, as used in the UNIVAC and EDSAC computers. Like bubble memory, racetrack memory uses electrical currents to "push" a magnetic pattern through a substrate. Dramatic improvements in magnetic detection capabilities, based on the development of spintronic magnetoresistive-sensing materials and devices, allow the use of much smaller magnetic domains to provide far higher bit densities.



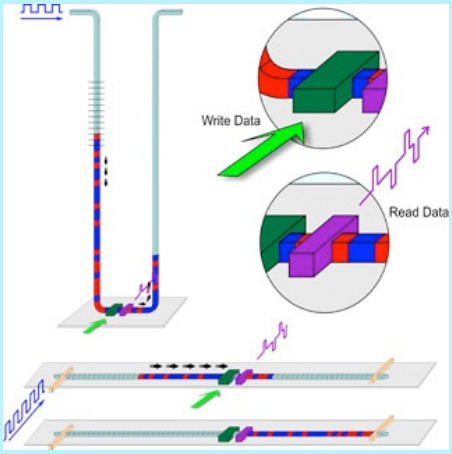
Principle Racetrack Memory

In production, it is expected that the wires can be scaled down to around 50 nm. There are two ways to arrange racetrack memory. The simplest is a series of flat wires arranged in a grid with read and write heads arranged nearby. A more widely studied arrangement uses U-shaped wires arranged vertically over a grid of read/write heads on an underlying substrate.

RACETRACK MEMORY

This allows the wires to be much longer without increasing its 2D area, although the need to move individual domains further along the wires before they reach the read/write heads results in slower random access times.

This does not present a real performance bottleneck; both arrangements offer about the same throughput. Thus the primary concern in terms of construction is practical; whether or not the 3D vertical arrangement is feasible to mass produce.



Comparison to other memory devices

Current projections suggest that racetrack memory will offer performance on the order of 20-32 ns to read or write a random bit.

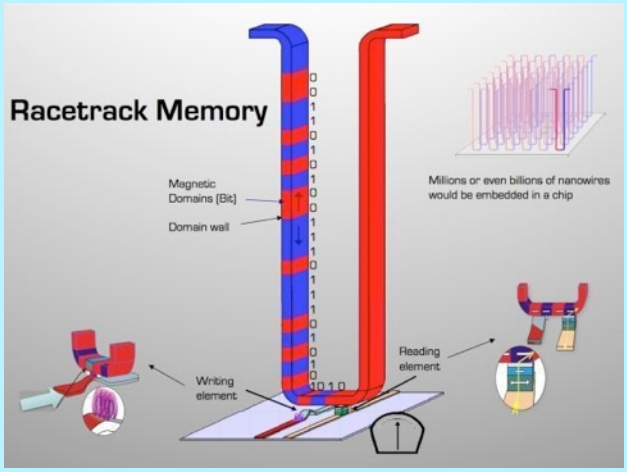
This compares to about 10,000,000 ns for a hard drive, or 20-30 ns for conventional DRAM. The authors of the primary work also discuss ways to improve the access times with the use of a "reservoir," improving to about 9.5 ns.

Aggregate throughput, with or without the reservoir, is on the order of 250-670 Mbit/s for racetrack memory, compared to 12800 Mbit/s for a single DDR3 DRAM, 1000 Mbit/s for high-performance hard drives, and much slower performance on the order of 30 to 100 Mbit/s for flash memory devices.

The only current technology that offers a clear latency benefit over racetrack memory is SRAM, on the order of 0.2 ns, but is more expensive and has a feature size of about 45 nm currently with a cell area of about 140 F

Flash memory, in particular, is a highly asymmetrical device. Although read performance is fairly fast, especially compared to a hard drive, writing is much slower. Flash memory works by "trapping" electrons in the chip surface, and requires a burst of high voltage to remove this charge and reset the cell.

In order to do this, charge is accumulated in a device known as a charge pump, which takes a relatively long time to charge up. In the case of NOR flash memory, which allows random bit-wise access like racetrack memory, read times are on the order of 70 ns, while write times are much slower, about 2,500 ns.



Blazer is a web browser available for Palm handhelds running Palm OS 3.1 or higher with 8MB of free memory available.

The original version of Blazer was developed by Bluelark Systems and was released in November 2000. Bluelark Systems was acquired by Handspring a month later, in December 2000. Version 1.0 supported HTML, WAP, and the markup language used in i-Mode.

Version history

Blazer 1

Blazer 1 was released in November 2000, and differentiated itself from other PalmOS web browsers at the time by its fast performance, progressive rendering, and support of WAP and i-Mode in addition to HTML. It utilized a proxy server which provided transcoding and image conversion optimized for small, underpowered handheld devices. Blazer 1 was available for free download.

Blazer 2

Blazer 2 was released in early 2002. Blazer 2 added the ability to use proxy servers, SSL, 16 bit color, and an improved user interface. Blazer 2 was available both as product bundled with the Treo 180, and as a paid download.

As of September 22, 2005, all copies of Blazer 1 and 2 were rendered inoperable as the proxy server for these browsers was taken offline by Palm.

Blazer 3

Blazer 3 was a significant upgrade in the series. Palm, Inc. dumped the original code for Blazer and started fresh with the NetFront Browser Engine (most notably used in the Sony Clie) as the core of the Blazer browser. It is bundled with Treo 600.

Blazer 4

Next came Palm Blazer 4.0/4.1. It is currently bundled with the Tungsten E2, the Tungsten T5, and the Treo 650 and 680. New Features included faster loading, an improved UI, VPN with an extra plugin, the saving of image and HTML files to a memory card or the device, homepages, bookmarks, and the ability to start on your last viewed page. Blazer 4 also features support for web standards including HTML 4.01, XHTML 1.0, WML 1.3, SSL 3.0, cHTML, JavaScript 1.5, CSS 1.0 and 2.0 (partial),

GIF (both still and animated, along with transparency), JPEG, PNG, BMP and Cookies. The use of some advanced features may cause the browser to crash if it is not in Wide Page Mode.

Soon after, Blazer 4.3 browser came available on the Treo 650, TX and LifeDrive. The most significant addition to 4.3 is the fast mode option, which removes images and/or disables cascading style sheets.

Streaming video

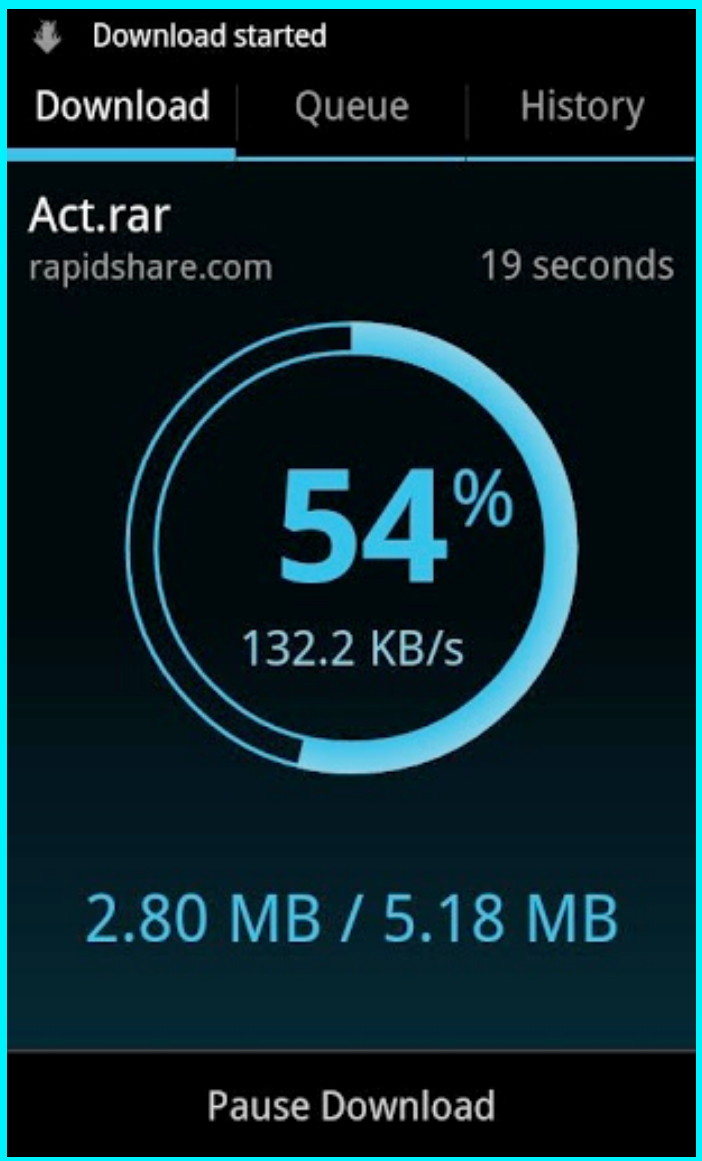
Video is streamed via the Kinoma Video Player. It supports many formats, including Windows Media.

At this time, Blazer does not support Adobe Flash Player - meaning you cannot view popular videos on sites such as ESPN or YouTube. This issue has never been addressed by Palm. A relatively small number of phones have the ability to use Flash.

The new Centro has demonstrated the ability to play YouTube videos on its browser using a high speed internet connection. This is demonstrated on the mobile version of You Tube which does not use Flash Technology.

Previous Palm phones with the current version of Blazer can also play these videos. This is the same version of YouTube accessed by the application of the same name on the Apple iPhone

Kinoma has released an upgrade to the Video Player, which can be purchased for many Palm phones, that has support for Flash Video, but is not part of the Blazer web browser itself.



The videos must be searched for via the Kinoma media guide. This guide acts as a browser for many popular video sites, like You Tube and Google Video. Many Palm users can get a discount on this upgrade.

NORTON 360

Norton 360, developed by Symantec, is marketed as an "all-in-one" computer security suite. The package includes an antivirus, a personal firewall, a phishing protection program and a backup program. What distinguishes this suite from Norton Internet Security is the inclusion of file backup and PC maintenance capabilities.

The package is distributed as a download, a box copy, or is preinstalled on computers as OEM software. Additional functions, including parental controls and e-mail spam filtering, are available as extensions developed also by Symantec.

Norton 360 is compatible with Windows XP (excluding 64-bit editions), Windows Vista and Windows 7.

Version history

Version 1.0

Version 1.0 was released on February 26, 2007. This version was the first Symantec product to use SONAR to detect zero-day viruses.

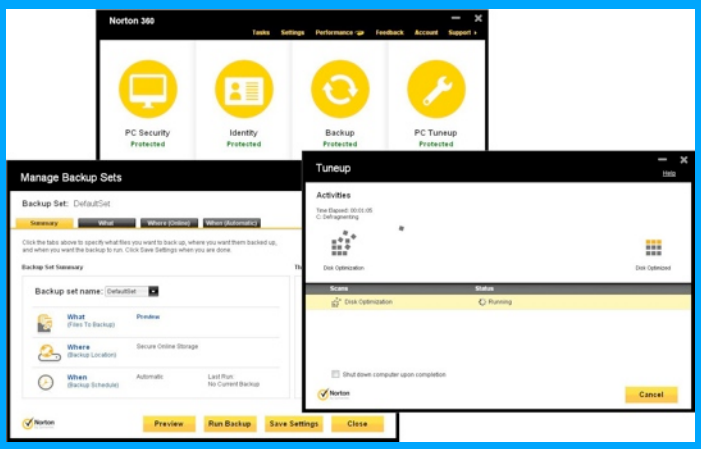
It monitors applications for malicious behavior, taking action as needed. The backup and restore functionality allowed users to back up files online or to a hard drive, CD, or DVD. PC maintenance tools allowed users to clear web browser history and temporary files. A disk defragmenter was bundled as part of the PC maintenance tools. Phishing protection integrates with Internet Explorer, warning users of fraudulent sites.

Version 2.0

Version 2.0 was released March 3, 2008. The backup feature can now inscribe data to Blu-ray and HD DVD discs. Multiple installations of Norton 360 can also to a centralized location. When backing up files online, the user can control the amount of bandwidth Norton uses.

A registry cleaner is bundled with the PC maintenance tools, allowing the user to remove invalid entries. Phishing protection for Firefox was added.

Supplementing the phishing protection is the Norton Identity Safe, which stores login credentials to websites. A network map allows users to view the status of other Norton installations on networked computers and view basic information about each computer. System requirements remain the same as version 1.0.



Version 3.0

Version 3.0 was released on March 4, 2009. This version uses the same codebase as Norton Internet Security 2009. For earlier versions, Symantec rewrote code specifically for Norton 360. Version 3.0 incorporates Norton Safe Web, offered as a standalone service earlier.

Version 4.0

Version 4.0 was released on February 17, 2010. This version adds many new security features found in Norton Internet Security 2010. Version 4 also features a GUI change. The prominent colors now match the gold and black sunburst of Norton Internet Security. Also, the weak SPAM filter has been replaced with the far more effective Symantec BrightMail, which according to Symantec gives 20% better results and require no training.

Version 5.0

Version 5.0 was released in February 2011 and offers improved performance and virus detection. It also provides updated versions of SONAR (version 3) and System insight.

Version 6.0

Version 6.0 was released on February 15, 2012. It adds some new features to this popular all-in-one suite including parental controls, better protection and performance, enhanced local and secure online backups, laptop and netbook users can now save battery and data charges with Power Saving and Metered Broadband modes, and easily remembers logins and other personal info while protecting against online identity theft.

Version-Less (unofficially 7.0)

This is the Norton's latest security suite. It was released on September 5, 2012, together with the newest Norton AntiVirus and Norton Internet Security products. It was described as Version-Less in Symantec's press release alluding to automatic updates that always keep the software to its latest version. There is no specific version reference anywhere in the description of the software.

MS WORD SHORTCUT

MICROSOFT WORD SHORTCUT KEYS

Shortcut Keys	Description
Ctrl + A	Select all contents of the page.
Ctrl + B	Bold highlighted selection.
Ctrl + C	Copy selected text.
Ctrl + X	Cut selected text.
Ctrl + P	Open the print window.
Ctrl + F	Open find box.
Ctrl + I	Italic highlighted selection.
Ctrl + K	Insert link.
Ctrl + U	Underline highlighted selection.
Ctrl + V	Paste.
Ctrl + Y	Repeat the last action performed.
Ctrl + Z	Undo last action.
Ctrl + L	Aligns the line or selected text to the left of the screen.
Ctrl + E	Aligns the line or selected text to the center of the screen.
Ctrl + R	Aligns the line or selected text to the right of the screen.
Ctrl + M	Indent the paragraph.
Ctrl + Shift + F	Change the font.
Ctrl + Shift + >	Increase selected font +1.

DATA MINING

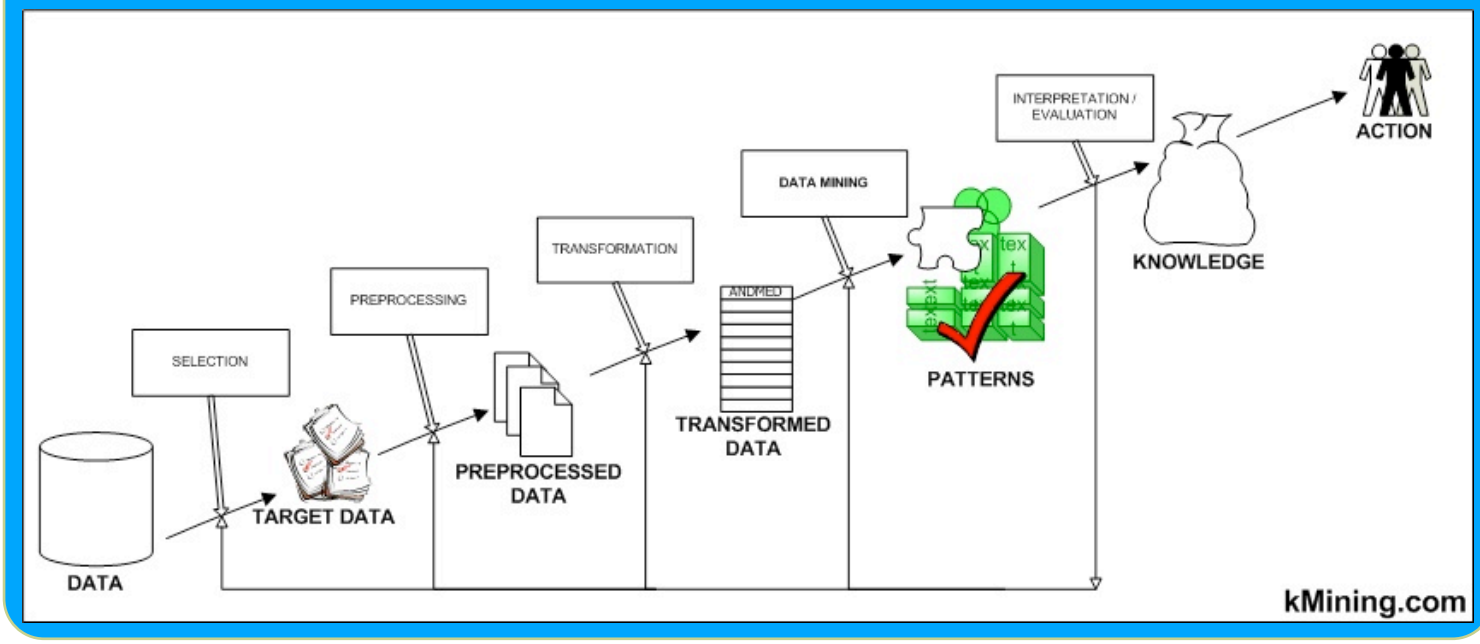
Data mining (the advanced analysis step of the "Knowledge Discovery in Databases" process, or KDD), a field at the intersection of computer science and statistics, is the process that attempts to discover patterns in large data sets. It utilizes methods at the intersection of artificial intelligence, machine learning, statistics, and database systems.

The overall goal of the data mining process is to extract information from a data set and transform it into an understandable structure for further use. Aside from the raw analysis step, it involves database and data management aspects, data preprocessing, model and inference considerations, interestingness metrics, complexity considerations, post-processing of discovered structures, visualization, and online updating.

The term is a buzzword, and is frequently misused to mean any form of large-scale data or information processing (collection, extraction, warehousing, analysis, and statistics) but is also generalized to any kind of computer decision support system, including artificial intelligence, machine learning, and business intelligence.

Etymology

In the 1960s, statisticians used terms like "Data Fishing" or "Data Dredging" to refer to what they considered the bad practice of analyzing data without an a-priori hypothesis. The term "Data Mining" appeared around 1990 in the database community. At the beginning of the century, there was a phrase "database mining"™, trademarked by HNC, a San Diego-based company (now merged into FICO), to pitch their Data Mining Workstation; researchers consequently turned to "data mining".Other terms used include Data Archaeology, Information Harvesting, Information Discovery, Knowledge Extraction, etc. Gregory Piatetsky-Shapiro coined the term "Knowledge Discovery in Databases" for the first workshop on the same topic (1989) and this term became more popular in AI and



DATA MINING

and Machine Learning Community. However, the term data mining became more popular in the business and press communities. Currently, Data Mining and Knowledge Discovery are used interchangeably..

Background

The manual extraction of patterns from data has occurred for centuries. Early methods of identifying patterns in data include Bayes' theorem (1700s) and regression analysis (1800s). The proliferation, ubiquity and increasing power of computer technology has dramatically increased data collection, storage, and manipulation ability.

As data sets have grown in size and complexity, direct "hands-on" data analysis has increasingly been augmented with indirect, automated data processing, aided by other discoveries in computer science, such as neural networks, cluster analysis, genetic algorithms (1950s), decision trees (1960s), and support vector machines (1990s). Data mining is the process of applying these methods with the intention of uncovering hidden patternsin large data sets. It bridges the gap from applied statistics and artificial intelligence (which usually provide the mathematical background) to database management by exploiting the way data is stored and indexed in databases to execute the actual learning and discovery algorithms more efficiently, allowing such methods to be applied to ever larger data sets.

Data mining involves **4 common classes of tasks**:

- **Anomaly detection** (Outlier/ change/deviation detection) – The identification of unusual data records, that might be interesting or data errors and require further investigation.
- **Association rule learning** (Dependency modeling) – Searches for relationships between variables. For example a supermarket might gather data on customer purchasing habits.
- **Clustering** – is the task of discovering groups and structures in the data that are in some way or another "similar", without using known structures in the data.
- **Classification** – is the task of generalizing known structure to apply to new data. For example, an e-mail program might attempt to classify an e-mail as "legitimate" or as "spam".

Notable uses

- **Games & Business**
- **Science and engineering**
- **Human rights**
- **Medical data mining**
- **Spatial data mining**
- **Sensor data mining**

CERTIFIED ETHICAL HACKER

The *Certified Ethical Hacker* is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council.)

An ethical hacker is usually employed by an organization who trusts him or her to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and fixing computer security vulnerabilities. Unauthorized hacking (i.e., gaining access to computer systems without prior authorization from the owner) is a crime in most countries, but penetration testing done by request of the owner of the targeted system(s) or network(s) is not.

A Certified Ethical Hacker has obtained a certification in how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a hacker. The exam code for C|EH is 312-50. The certification is in Version 7.1 as of 14 June 2011. A version 8 has later been added. The EC-Council offers another certification, known as Certified Network Defense Architect (C|NDA). This certification is designed for United States Government Agencies, and is available only to members of selected agencies. Other than the name, the content of the course is exactly the same. The exam code for C|NDA is 312-99.

Examination

Certification is achieved by taking the C|EH examination after having either attended training at an ATC (Accredited Training Center) or done self-study. If a candidate opts for self-study, an application must be filled out and proof submitted of 2 years of relevant information security work experience.

In case you do not have two years of information security related work experience, you can send them a request detailing your educational background and request for consideration on a case basis.

The current version of the C|EH is V8 uses EC-Council's exam 312-50, as did the earlier versions. Although the new version V8 has recently been launched. This exam has 125 multiple-choice questions, a 4 hour time limit, and requires at least a score of 70% to pass.

The earlier v7 had 150 multiple-choice questions and a four hour time limit. The version 7 and version 8 exams costs US$500 for the actual test and US $100 as a nonrefundable fee if you have done selfstudy only Prices apply in the United States (prices in other countries may differ), and is administered via computer at an EC-Council Accredited Training Center, Pearson VUE, or Prometric testing center (in the United States).

CERTIFIED ETHICAL HACKER

Recertification

EC-Council Continuing Education (ECE) points serve to ensure that all certified professionals maintain and further their knowledge. Professionals must meet ECE requirements to avoid revocation of certification. Members holding the C|EH/C|NDA designation (as well as other EC-Council certifications) must recertify under this program every three years for a minimum of 120 credits (at least 20 credits per year).

Controversy

Certain computer security professionals have objected to the term ethical hacker: "There's no such thing as an 'ethical hacker' - that's like saying 'ethical rapist' - it's a contradiction in terms." Part of the controversy may arise from the older, less stigmatized, definition of hacker, which has since become synonymous with computer criminal.

MIND PUNCH

1. If two painters can complete two rooms in two hours, how many painters would it take to do 18 rooms in 6 hours?

2. What letter comes next?

A D H K O?

3. Which five–letter word can be placed in front of each of these words to make new words?

– – – – – RUNNER
– – – – – AGE
– – – – – LINE
– – – – – RANK
– – – – – MAN

1.Answer: 6 Painters

2.Answer : R(Skip two letters then three)

3.Answer: FRONT

THE EDITORIAL BOARD

Patron

Thiru. A Venkatachalam, B.Sc. — Correspondent

Editorial In Chief

Dr. N. Raman, B.Ed, M.Com, MBA, M.Phil,PGDCA, PhD., — Principal

Staff Advisor

Mr. P. Ramesh M.Sc., M.Phil, — Head of the Department

Staff Editor

Mr. R. Sundar Raj, MCA — Assistant Professor

Student Editors

B. Mohamed Muzamil	III B.Sc. CS[A]
M. Sanjay Kumar	III B.Sc. CS[A]
S. Balaji	III B.Sc. CS[A]
K. Sudhakar	III B.Sc. CS[A]
B. Jeevanandham	III B.Sc. CS[B]
R. Kavithra	II B.Sc. CS[A]
C. Raja	II B.Sc. CS[B]
S. Praveen Kumar	I B.Sc. CS[B]
R.B. Thenmozhi	I B.Sc. CS[B]
M. Manoj Kumar	I B.Sc. CS[A]
D. Boobalan	I B.Sc. CS[B]
P. W. Joe Alfred	I B.Sc. CS[C]

The Editorial Board Express its sincere gratitude to all those who are responsible either by being on stage or behind the screen.. .. ..

KONGU ARTS AND SCIENCE COLLEGE
Nanjanapuram, Erode
DEPARTMENT OF COMPUTER SCIENCE(UG)

E-Mail: itunlimitedmagazine@gmail.com Web: www.kasc.ac.in