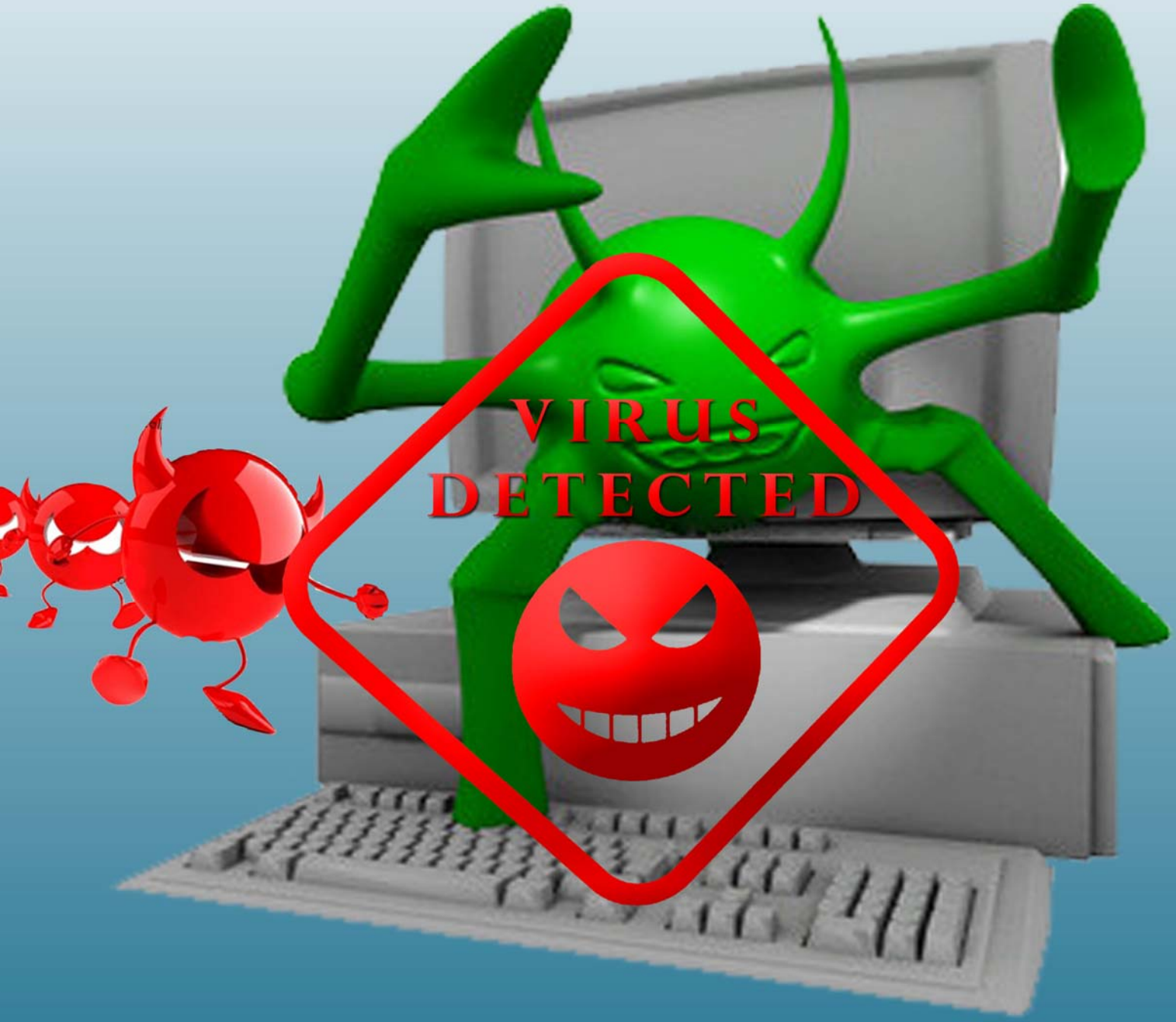
CCC News

Control Computer Crimes

Issue 0007 - 15 September 2009



Message from the Editor

Welcome to the seventh issue of CCCNews Magazine.

We are happy to announce that that download of sixth issue of CCCNews Magazine has crossed 150,000. This is the testimony that CCCNews Magazine is becoming more popular and downloaded by many more readers.

This gives us satisfaction that our efforts are appreciated as more people are taking Computer Security seriously.

Like Information Technology industry, we are constantly evolving and changing. Now, you have more reports, research, analysis, surveys and very little news and related matter. All the news are covered in CCCNews Newsletter, which is published every Monday, Wednesday and Friday.

In this edition, we start with two different analytical reports, presenting you a fashion parade of top computer threats in last 20 years.

We also bring you a article on calculator about – "How much is the worth of your data in Cyber under ground market". This is an extremely interesting topic of research. You may try this calculator yourself. We do not know - how the underground worth is calculated and what have been the assumptions. But, this is a new dimension to estimate the value of the data now, and other IT assets later, which can help in defining the right IT security strategy. May be insurance companies can support researchers to define a model to calculate the value of IT assets before and after loss based on assumptions, statistical, operations research and actuarial sciences.

We also present two articles on "7 reasons – why your websites are not longer safe" and "10 ways to hack into a network". Both these articles provide details on website security issues. So, all website users and developers must keep these in mind when designing security of their websites.

Happy reading.

Rakesh Goyal
Editor

CONTENTS

CCC News
Issue 0007
15 September 2009

Rakesh Goyal
Editor
editor@cccnews.in

Published by
CCC Media
Mumbai, India

Analysis

The most dangerous computer threats of the last 20 years

PandaLabs has issued a ranking of the most insidious malware threats that have surfaced in the past 20 years.

The following threats have been selected for the notoriety they achieved through widespread epidemic and the damage caused:

Friday 13 or Jerusalem

Created in Israel in 1988 and first reported in Jerusalem, this supposedly commemorated the 40th anniversary of Israel. Whenever the date was Friday 13, it would delete all programs run on an infected computer.

Barrotes

The first well-known Spanish virus appeared in 1993. Once on the computer, it would remain hidden until January 5, when it would activate displaying just a series of bars on the monitor.

Cascade or Falling Letters

Created in Germany in 1997, this virus would make the letters on the screen fall in a cascade whenever it infected a computer.

CIH or Chernobyl

This virus was produced in Taiwan in 1998, and took just one week to propagate and infect thousands of computers.

Melissa

First appeared on March 26, 1999 in the USA, This ultra-smart malicious code used social engineering to spread, with a message that read "Here is that document you asked for. . . don't show anyone else ;-)"

ILoveYou or Loveletter

So famous, it hardly needs introduction. This romantic virus emerged from the Philippines in 2000. With the subject 'ILoveYou' it infected millions of computers around the world and even hit organizations like the Pentagon.

Klez

Created in 2001 in Germany, it only infected computers on the 13th of odd months.

Nimda

The name is basically 'admin' spelled backwards, as it was able to create administrator privileges on infected computers. It originated in China on September 18, 2001.

SQLSlammer

This was another major headache for companies. It first appeared on January 25, 2003, and affected more than half a million servers in just a few days.

Blaster

This virus, created in the USA on August 11, 2003, contained a message in its code: "I just want to say love you, San!!" (We still don't know who 'San' is), and "Billy gates, why do you make this possible? Stop making money and fix your software".

Sobig

This German virus was famous in the summer of 2003. The F variant was the most damaging, it attacked on August 19 of the same year and generated more than 1 million copies of itself.

Bagle

This emerged on January 18, 2004, and has been one of the most prolific viruses with respect to the number of variants.

Netsky

This worm also came from Germany in 2004 and exploited vulnerabilities in Internet Explorer. Its creator was also responsible for the notorious Sasser virus.

Conficker

Last on the list and most recent, it appeared in November 2008. Oddly enough, if your keyboard is configured in Ukrainian, it won't affect you...

Credits : http://www.net-security.org/

Analysis

Top 10 threats in 40 years of Internet

It's odd but appropriate that an antivirus and internet security company is "celebrating" the 40th anniversary of the interment with a list of the Web's most notorious badware.

To wit, Symantec's Top Web Threats in the History of the Internet:

1. I Love You (2000)
Who wouldn't open an e-mail with "I Love You" in the subject line? Well, that was the problem. By May 2000, 50 million infections of this worm had been reported. The Pentagon, the CIA, and the British Parliament all had to shut down their e-mail systems in order to purge the threat.

2. Conficker (2009)
The Conficker worm has created a secure, worldwide infrastructure for cyber crime. The worm allows its creators to remotely install software on infected machines. What will that software do? We don't know. Most likely the worm will be used to create a botnet that will be rented out to criminals who want to send SPAM, steal IDs and direct users to online scams and phishing sites.

3. Melissa (1999)
Melissa was an exotic dancer, and David L. Smith was obsessed with her and also with writing viruses. The virus he named after Melissa and released to the world on March 26th, 1999, kicked off a period of high-profile threats that rocked the Internet between 1999 and 2005.

4. Slammer (2003)
This fast-moving worm managed to temporarily bring much of the Internet to its knees in January of 2003. The threat was so aggressive that it was mistaken by some countries to be an organized attack against them.

5. Nimda (2001)
A mass-mailing worm that uses multiple methods to spread itself, within 22 minutes, Nimda became the Internet's most widespread worm. The name of the virus came from the reversed spelling of "admin."

6. Code Red (2001)
Websites affected by the Code Red worm were defaced by the phrase "Hacked By Chinese!" At its peak, the number of infected hosts reached 359,000.

7. Blaster (2003)
Blaster is a worm that triggered a payload that launched a denial of service attack against windowsupdate.com, which included the message, "billy gates why do you make this possible? Stop making money and fix your software!!"

8. Sasser (2004)
This nasty worm spread by exploiting a vulnerable network port, meaning that it could spread without user intervention. Sasser wreaked havoc on everything from The British Coast Guard to Delta Airlines, which had to cancel some flights after its computers became infected.

9. Storm (2007)
Poor Microsoft, always the popular target. Like Blaster and others before, this worm's payload performed a denial-of-service attack on www.microsoft.com. During Symantec's tests an infected machine was observed sending a burst of almost 1,800 emails in a five-minute period.

10. Morris (1988)
An oldie but a goodie; without Morris the current threat "superstars" wouldn't exist. The Morris worm (or Internet worm) was created with innocent intentions. Robert Morris claims that he wrote the worm in an effort to gauge the size of the Internet. Unfortunately, the worm contained an error that caused it to infect computers multiple times, creating a denial of service.

Credits : http://news.postbulletin.com

Research

Malware stays on machines for years

In another warning to PC users and IT security managers, new research from security vendor Trend Micro has found that malware lingers on devices much longer than previously thought - for months and sometimes years.

Previous estimates have said the average compromised machine remains infected for around six weeks, but now Trend is saying that many computers are infected or repeatedly infected for more than two years, with a median infection length of 300 days for some countries.

The security vendor analysed around 100 million compromised IP's and found that 80 per cent of all compromised machines have been infected for more than a month - with at least a quarter of these business computers.

With malware becoming increasingly difficult to locate and remove, the message is clear for firms - ensure your systems are running comprehensive scanning and remediation tools alongside any anti-malware technology. Deflecting attacks is only part of the battle.

Courtesy : http://www.security-watchdog.co.uk

Development

How much are you worth on the black market?

Ever wondered how much your online identity is worth to a cyber criminal? A new tool from Symantec Corp. will perform the calculation for you.

The ***Norton Online Risk Calculator**, unveiled within a microsite to coincide with the launch of Norton 2010, calculates your net worth on the black market by asking a few questions about your personal Internet use.

It takes a few minutes to answer the questions, after which you get three results: how much your online assets are worth, how much your online identity would sell for on the black market, and your risk of becoming a victim of identity theft.

The main point isn't to promote software or instill fear, but to spread awareness on cyber crime, said Marian Merritt, Internet security advocate for Symantec.

IT pros can use the consumer-oriented tool to educate employees in their office, as well as advocate Internet security to their family and friends. "IT is in that unique position of bridging both worlds," said Merritt.

It's unlikely the average consumer would read an Internet Security Threat Report, she added, but a simply illustrated example might get the same point across. "It's shocking how little value criminals place on your credit card," she said.

IT pros themselves might also benefit from a refresher on cyber crime. "Sometimes those who think they know the most can be even more at risk than others who admit they don't know much and therefore are very cautious," said Merritt.

Even those who consider themselves experts in IT tend to take shortcuts when it comes to online security because they think they aren't at risk, their information isn't really that valuable or

they don't realize how much work it takes to recover a stolen identity, she explained.

IT pros might be familiar with concepts of the underground criminal economy and may even know a self-proclaimed hacker or two, but they may not realize the extent to which cyber crime has grown over the past several years, she said.

Cyber crime is now larger than the international drug trade, Merritt pointed out. Nearly 10 million people have reported identity theft in the U.S. over the last 12 months and one in four households have already been victimized, she said.

Not only is the rate of growth surprising, but how easy it is for criminals with no technical skills to convert themselves into cyber criminal businesses overnight, she said. Build-your-own botnet kits and spam engine systems trade on the black market for about $500, Merritt pointed out.

Cyber crime is well reported in the IT space, but the message doesn't often reach the general public, according to Merritt. "You turn on the news and they are talking about capturing drug dealers going across the border, but they rarely show a hacker in handcuffs," she said.

Michael Calce, who did make popular news headlines back in 2000 for a series of DDoS attacks that brought down major Web sites including Yahoo, eBay and Amazon, is one exception. His 56-charge conviction gained further notoriety due to the fact that he was only 15 years old at the time.

The former hacker is now making an effort to rebuild his reputation as a "white hat" and spreading the message on cyber crime and Internet security. The Internet is broken, threats are exploding and IT community needs to join forces to fix it, warned Calce at the IT360 conference last April.

In a post-conference interview, Calce summed up his main message for those who were unable to attend the event. "We're trying to get a message across that we need to do something about this. Government agencies need to step in, us -- the white hat community -- need to step up our game because this is a very serious issue that is starting to explode," he said.

One of the main problems, according to Calce, is that the Internet was never intended to become a commercial tool. "We have to rebuild certain protocols and basically get a new concept of how the Internet should be with computer security in mind. There's a serious lack of fundamental securities when it comes to the Internet," he said.

Calce's message also addressed consumers. Individual Internet users are increasingly becoming targets, he pointed out. "It's people putting their lives online that is starting to make the difference ... when you put that into perspective, that everybody's life is now online, you can see that they're becoming targets, whereas ten years ago this wasn't really the case," he said.

The best practice for the non-techie is to constantly update software and do some reading, according to Calce. "People are always on Google anyways -- type up Internet security, see what you can figure out. It can definitely be beneficial to your future because the way technology is headed, sooner or later, everybody is going to need to know the fundamentals of security," he said.

Calce suggested average Internet users look at security as a whole. "You may be attempted by hackers, you may be logged by your ISP, you may be this, you may be that ... there's so many factors to factor in. The fact is, you have to expect the worst-case scenario," he said.

Mistakes Internet users continue to make include forgetting to renew their security software subscriptions, not keeping operating system patches up to date and failing to use the latest version of their Internet browser, Merritt pointed out.

Users may also believe they have a comprehensive Internet security package, when in fact, all they are using is anti-virus software without firewall and intrusion protection, said Merritt. Children are easy targets and further increase the risk, especially through their use of peer-to-peer networks.

But even users who do everything right can find their personal information compromised. The biggest security hole problems that lead to this generalized risk for consumers are massive data

breaches that occur at institutions like banks, universities, major retailers and credit card institutions, said Merritt.

The best protection against this further threat is to sign up for a credit card monitoring service and regularly review your credit report, Merritt suggested. Institutions may or may not be required to notify consumers about a breach, she pointed out.

Symantec is introducing real-time, reputation-based security technologies in its latest lineup of Norton consumer products. The new protection model, available in Norton Internet Security 2010 and Norton AntiVirus 2010, is called Quorum.

The addition of Quorum allows Norton to detect 80 per cent of the threats within that one per cent that previously remained undetected, according to Lana Knop, principle product manager for Symantec. The new Norton packages, available online and through retailers in the U.S. on Sept. 9, are coming to Canadian retail locations by the end of September.

One in five users who go online will become a victim of some form of cyber crime, she pointed out. Knop put it into perspective by comparing the rates to street crime.

"Every four and a half minutes, a crime is committed on the streets of Los Angeles. Every three minutes, a crime is committed on the streets of Washington, D.C. In New York, a crime is committed every two minutes ... every three seconds, a crime is committed on the net," she said.

Credits : Jennifer Kavur; http://www.itworld.com

* You may try Norton Online Risk Calculator is available at http://everyclickmatters.com/preloader.html?redirect=/victim/assessment-tool.html

Analysis

7 Reasons Websites Are No Longer Safe

Conventional wisdom is that Web wanderers are safe as long as they avoid sites that serve up pornography, stock tips, games and the like. But according to recently gathered research from Boston-based IT security and control firm Sophos, sites we take for granted are not as secure as they appear.

Among the findings in Sophos' threat report for the first six months of this year, 23,500 new infected Web pages -- one every 3.6 seconds -- were detected each day during that period. That's four times worse than the same period last year, said Richard Wang, who manages the Boston lab. Many such infections were found on legitimate websites.

In a recent interview with CSOonline, Wang outlined seven primary reasons legitimate sites are becoming more dangerous.

1. Polluted ads

Many legitimate sites rely on paid advertisements to pay the bills. But Wang said recent infection statistics gathered by his lab show that they are often hiding malware, without the knowledge of the website owner or the user.

"A lot of sites supported by advertisers, rather than contracting directly with the advertiser, work through ad agencies and network affiliates," Wang said. "Some of these affiliates are less than diligent in reviewing content for flaws and infections."

Ads that incorporate Flash animation and other rich media are often rife with security holes attackers can exploit. When the user clicks on the ad, the browser can be (and often is) redirected to sites that download malware in the background while the user is reading the legitimate site. Someone in the ad-providing supply chain can be the culprit, though tracing a compromise back to them can be exceedingly difficult, Wang said.

Whatever the case may be, a downloaded Trojan is then free to gather up usernames, passwords and other sensitive banking data.

2. SQL injection attacks

SQL injection attacks are among the most popular of tactics and have been used in several high-profile incidents in the last couple of years. For example, see "SQL Injection Attacks Led to Heartland, Hannaford Breaches."

SQL injection is a technique that exploits a flaw in the coding of a Web application or page that uses input forms. A hacker might, for example, input SQL code into a field that is intended to collect email addresses. If the application doesn't include a security requirement to validate that the input is of the correct form, the server may execute the SQL command, allowing the hacker to gain control of the server.

"The hacker essentially takes advantage of flaws related to shoddy site development," Wang said.

3. User-provided content

It doesn't take a genius to write a comment to a blog posting or something they see on a social networking site like Facebook or Twitter. The bad guys know this and are therefore taking the opportunity to pollute discussion threads and other sources of user-supplied content with spam-laden links. (See "Seven Deadly Sins of Social Networking Security".)

"You can get comment spam, completely irrelevant comments including links to sites trying to sell you stuff," Wang said. "They can also try posting full links to malicious sites or work in a little scripting, depending on the filter they are trying to work around."

4. Stolen site credentials

Using the types of malware and social networking tactics described above, as well as other means, attackers can steal the content provider's log-in credentials. From there it's no sweat logging into the site and making changes. It typically is a change so subtle and small that it escapes notice. The tiny bits of code added in can then steal the site visitor's credit card or other data.

5. Compromised hosting service

This one is similar to number 4, where the credentials of the content provider are stolen and hackers log in to make sinister changes. Through this vector, Wang said the bad guys could potentially poison thousands of sites the provider is hosting in one strike.

6. Local malware

The website you visit may be perfectly safe, but if there's malware hidden on your own machine you can unwittingly become part of the attack, Wang said. For example, the user can visit their online banking site, and when typing in a user name and password the Trojan is there to record that information and pass it back to the attacker, allowing him to go in later and empty out your account or that of others.

7. Hacker-engineered fakes

Finally, there's the problem of hackers trying to sell you fake merchandise that includes phony security software. If a box appears warning that your machine may have been infected and that you must immediately download a particular security tool to remove it--a common occurrence if you have visited a site that surreptitiously downloads malware onto your computer--it's a sure sign of trouble.

"You spend your $39.95 and you get a worthless piece of software, and at the same time you have given them your credit card data," Wang said.

What is one to do if their website relies on ads and open access? Wang suggested IT security administrators use security scanners against anything coming in by way of third-party hosts and, for in-house apps and other online property, that developers redouble efforts to write more ironclad code.

Credits : Bill Brenner; http://www.cio.com

Education

10 ways to hack into networks

Spying on voice and data

Attackers seeking to do harm or mischief to networks work with an ever expanding arsenal of tools that sometimes seem to be the stuff of spy fiction, but they are all too real.

Here are 10 cloak-and-dagger ways, legal and illegal, to secretly tap into networks and computers to capture data and conversations.

1. Wireless keyboard eavesdropping

Remote-exploit.org has released an open source hardware design and accompanying software for a device that captures then decrypts signals from wireless keyboards. The device uses a wireless receiver that can be concealed in clothing or disguised as a common object that could be left on a desk near a PC to pick up signals.

Called Keykeriki, the technology targets 27MHz wireless keyboards to exploit insecurities that remote-expoit.org discovered earlier. The company plans to build and sell the hardware.

2. Wired keyboard eavesdropping

Electromagnetic pulses that keyboards make to signal what key is being hit travel through the grounding system of the keyboard and the computer itself as well as the ground for the electrical wiring in the building where the computer is plugged in.

Probes placed on the ground for the electric wiring can pick up these electromagnetic fluctuations, and they can be captured and translated into characters. The potential for this type of eavesdropping has been known for decades, and many experts believe spy agencies have refined techniques that make it practical. Andrea Barisani and Daniele Bianco, researchers for network security consultancy Inverse Path, are presenting their quick-and-dirty research on the topic at this year's Black Hat USA

conference in the hopes of sparking more public research of these techniques.

3. Laptop eavesdropping via lasers

Bouncing lasers off laptops and capturing the vibrations made as keys are struck give attackers enough data to deduce what is being typed. Each key makes a unique set of vibrations different from any other. The space bar makes an even more unique set, Barisani and Bianco say.

Language analysis software can help determine which set of vibrations correspond to which key, and if the attacker knows the language being used, the message can be exposed, they say.

4. Commercial keyloggers

Early keyloggers were devices attached in-line with keyboards, but they advanced to software tools that grab keystrokes and store or send them to an attack server. Commercial versions have the software loaded on memory sticks that can dump the software on a computer and then be reinserted later to download the collected data.

5. Cell phones as remotely activated bugs

Software loaded onto certain models of cell phones can silence the ringers and cut off the light displays that would normally be triggered when calls are made to them. The caller can then listen in on conversations in the room where the phone is located.

According to press reports, the FBI received court permission to use this technique to spy on suspected Mafia members in New York.

6. Cell phone SIM card compromise

If attackers can get possession of a cell phone briefly, they can use commercially available software to download and read SIM cards and their store of phone numbers, call logs, SMS messages, photos and so on.

For instance PhoneFile Pro is software on a USB stick that claims to enable both the download and the display of the data.

7. Law enforcement wiretapping based on voice print

Phone company voice switches include software that can search all conversations going through it for voices that match sets of voiceprints. Whenever the switch makes a match, it can trigger a recording of the conversation and alert law enforcement officials, says James Atkinson, an expert in technical surveillance countermeasures.

The feature is designed to support communications assistance for law enforcement (CALEA) -- the law that requires phone companies to provide wiretapping access under court order to specific communications traffic.

8. Remote capture of computer data

Under a sketchy technique called Computer and Internet Protocol Address Verifier (CIPAV), the FBI has remotely tracked down data about individual computers.

Details of the technology have never been publicly revealed, but they were used to track down high-school students who sent e-mail bomb threats. CIPAV grabs IP and MAC addresses, running processes, visited Web sites, versions of operating systems, registered owner and logging of computers the target computers connect to. It is believed the software that does this is dropped in via exploiting instant messaging.

9. Cable TV as an exploitable network

Because most cable TV networks are essentially hubbed, any node can monitor any other node's traffic, says James Atkinson, an expert in technical surveillance countermeasures. By and large security is rudimentary and the encryption used could be hacked by someone with basic technical skills and readily available decryption tools, he says.

10. Cell phone monitoring

Commercially available software claims to capture cell phone conversations and texting. Attackers need to get physical access to the phone to upload the software that enables this.

There are several commercial brands on the market, but there are also online complaints that the software doesn't work as advertised or is more complicated to use than the vendors let on.

Credits : Tim Greene; http://features.techworld.com

Report

Cyber safety data hard to come by

A report commissioned by the Federal Government on cyber safety has shed light on the scarcity of local data on online dangers, such as cyber-bulling and cyber-stalking, to children.

The Review of Existing Australian and International Cyber-safety Research report, undertaken by the Edith Cowan University, found there were significant gaps in Australian research, with only very preliminary Australian research being conducted on the effects of exposure to pornography on children and cursory examination of areas such as cyber-stalking.

"Therefore, it is necessary to extrapolate from overseas research findings to estimate the prevalence and consequences associated with some cyber safety risks to Australian youth," the report reads.

The report, which the government is using to support its $125.8 million cyber-safety plan, argues that while cyber-grooming and sexual solicitation are potentially the most serious cyber-safety risks for children, cyber-bullying occurs at a rate far lower than overseas.

"Whereas rates of up to 50 per cent of [students] being cyber bullied have been reported among young people in the US and Europe, prevalence rates in Australia are much lower (less than 10 percent)," the report reads.

Despite the anonymity offered by the Internet and mobile phone, the report also found that the majority of students were aware of the identity of the cyber-bullying perpetrator.

While exact prevalence data were not available on cyber-stalking, overseas estimates of the proportion of young people in Australia affected by cyber-stalking was about seven per cent, according to the report.

About 84 per cent of boys and 60 per cent of girls in Australia are estimated to have been accidentally exposed to pornography

online, while 38 per cent and two per cent of boys and girls respectively have been deliberately exposed.

In related news, the Federal Government is also claiming a cyber-safety win with the signing on of several IT industry heavyweights to promote its children's Internet safety initiative, CyberSmart.

According to the communications minister Stephen Conroy, Google and YouTube Australia, MySpace and Telstra have signed on to promote the Cybersmart.gov.au Web site.

The companies, along with welfare organisations such as Bravehearts, Child Wise, and The Alannah and Madeline Foundation, will promote the CyberSmart website by prominently displaying links on their own websites, according to the government.

The CyberSmart site seeks to educate young children, teenagers, teachers and parents about potential online risks such as cyber-bulling, sexually explicit, violent, prohibited or illegal content and scams and identity theft.

Conroy said the need for a central source of information about cyber-security was borne out by meetings with the Youth Advisory Group on cyber-safety, and through the government-commissioned cyber-safety report.

Credits : Tim Lohman; http://www.computerworld.com.au

Research

Cyber criminals targeting small businesses

Cyber criminals are increasingly targeting small and medium-sized businesses that don't have the resources to keep updating their computer security, according to federal authorities.

Many of the attacks are being waged by organized cyber groups that are based abroad, and they are able to steal not only credit card numbers, but personal information — including Social Security numbers — of the card holders, said Michael Merritt, assistant director of the U.S. Secret Service's office of investigations.

Merritt, in testimony prepared for the Senate Homeland Security and Governmental Affairs, said that as larger companies have taken on more sophisticated computer network protections, cyber criminals have adapted and gone after the smaller businesses who do not have such high-level security.

Phil Reitinger, the deputy under secretary at the Department of Homeland Security said there are many simple steps that businesses can take to protect themselves.

"Securing the entrances of one's factory or store is second nature to any business owner and so cyber security protections must become," he said in his testimony to the panel. He added that a recent study suggested that as many as 87 percent of data breaches could be avoided by installing simple to intermediate preventative measures.

Reitinger and Merritt said government agencies are working to coordinate more both with each other and with the private sector to improve cyber security.

But lawmakers working on cyber security legislation in several committees across Capitol Hill are pressing for the administration to do more.

"Security cannot be achieved by the government alone," said Sen. Joseph I. Lieberman, I-Conn. and chairman of the homeland security panel. "Public-private partnership is essential. Together,

business, government, law enforcement, and our foreign allies must partner to mitigate these attacks and bring these criminals to justice."

Credits : LOLITA C. BALDOR; http://tech.yahoo.com

Report

Hackers Better Organized Than Government

US DHS Official Says Foundation Exists to Battle Attackers

Hackers are better organized to attack critical government and business IT systems than the government and business are structured to defend their cyber assets, the Department of Homeland Security's top cybersecurity official told a US Senate panel Monday.

"Hackers, in some way, have remained better in information sharing than we in government have been, so that's an area of growth for us," Philip Reitinger, US DHS deputy undersecretary, National Protection and Programs Directorate, told the Senate Committee on Homeland Security and Governmental Affairs, which held a hearing on protecting industry against growing cyber threats.

Another witness from DHS, Assistant Director Michael Merritt of the Secret Service's Office of Investigations, explained that using so-called carding portals - sort of a Craig's List for cyber attackers - criminals link up anonymously, exchanging hacking tools and information such as stolen credit card numbers. Unlike traditional families of organized criminals, Merritt said, teams of virtual criminals are a loose hierarchy in which members don't know one another; a hacker in the Ukraine can buy stolen credit card numbers from someone in the Baltic through a carding site anonymously. With anonymity, he said, it's laborious to identify these criminals.

Despite the challenges, Reitinger said government and business are partnering to come up with solutions to battle cyber criminals. He cited work on new ways to authenticate users without requiring a username or password, noting it's hard to steal personal identifiable information if usernames aren't employed to access systems.

As part of his job, Reitinger heads DHS's National Cybersecurity Division - charged with safeguarding federal communications networks - and he testified that the unit plans to more than double its payroll, to 260 from 111 people, in the coming year. "That's a heavy lift in government," he said.

Reitinger said unlike in the past, when the government would invite business participation after it developed policy to protect private-sector cyber assets, it included business participation at the get-go to create National Incident Cyber Response plan.

"I've seen incredible commitment from people in both the private sector and public sector," Reitinger testified. "I believe we have a real opportunity here. ... We built the framework to work together. Now we need to drive toward outcomes. We need to worry less about having a partnership and more that we can achieve with the partnership."

Credits : Eric Chabrow; http://www.govinfosecurity.com

Survey

Three out of four administrators don't trust anti-virus software

In a recent study, a total of 226 administrators, CIOs and security specialists were asked what they thought of signature and blacklist-based solutions. Three out of four administrators consider signature-based enterprise anti-virus protection unreliable. For zero day attacks in particular, two thirds of the administrators surveyed did not believe that standard anti-virus products helped to prevent attacks.

The study was commissioned by CoreTrace, which produces security software that uses whitelists to decide whether applications may be executed. Users are able to run previously defined programs only, so that it's not possible to run executable email attachments or infected programs from USB memory sticks. Vista implements a similar protection mechanism, which it calls Software Restriction Policies (SRP), but the administration function, via the Microsoft Management Console (MMC), is somewhat rudimentary. Microsoft has made SRP more fine tuneable in Windows 7, but administration still requires the use of MMC.

Nevertheless, 89 per cent of those questioned in the CoreTrace study still use a standard anti-virus product, with half of the respondents citing the fact that it's "better than nothing" as their rationale for doing so. The other half felt compelled to use an anti-virus product due to compliance and company guidelines. Around 40 per cent had thought about getting rid of their anti-virus protection, one reason being that it reduces system performance.

According to the survey, 40 per cent of users were not aware of alternatives to blacklisting and signature-based approaches. 43 per cent considered the absence of system scans when using a whitelisting approach, to be a positive factor. However, 66 per cent had concerns about adding new applications for users, wanting the process to be as quick and simple as possible.

Traditional anti-virus software vendors are also working on adding whitelist-based solutions to their existing products. The daily

flood of variants of a large numbers of viruses is making production and distribution of signatures ever more impractical. As an initial remedy, many vendors have implemented cloud-based solutions that check file hashes to see whether a file has already been recognised as malicious on another system.

Credits : http://www.h-online.com

Analysis

Clients are weakest links in cybersecurity

Unpatched applications on Web servers

Hackers — whether criminal or apparent agents of foreign governments — are exploiting unpatched applications on Web servers and client computers to infect entire networks, according to report released today on predominant cybersecurity risks.

"Attackers have long picked up on this opportunity and have switched to different types of attacks in order to take advantage of these vulnerabilities, using social engineering techniques to lure end-users into opening documents received by e-mail or by infecting Web sites with links to documents that have attacks for these vulnerabilities embedded," according to the Top Cyber Security Risks list, released today by the SANS Institute.

On average, major organizations being monitored by Qualys, a company that provides patch-management services, take at least twice as long to patch client-side application vulnerabilities as operating-system vulnerabilities, the report states. This can leave client computers open to targeted attacks delivered via socially engineered e-mail.

"Waves of targeted e-mail attacks, often called 'spear phishing,' are exploiting client-side vulnerabilities in commonly used programs such as Adobe PDF Reader, QuickTime, Adobe Flash and Microsoft Office," the report states. "This is currently the primary initial infection vector used to compromise computers that have Internet access."

These targeted attacks are the primary threat faced by government organizations and by top executives with access to sensitive data, said Rob Lee of Mandiant, an incident-response company and the SANS faculty leader in forensics.

"They predominantly use spear-phishing attacks which they have socially engineered" to deliver client-side application exploits, Lee said. He called the threats advanced and persistent. "These are not hobbyists who are doing this. There's a big payoff here."

But the same client applications are being exploited by malicious code that is delivered by trusted third-party Web sites. These Web sites frequently host publicly posted content but have been compromised, often by SQL injection techniques.

"Despite the enormous number of attacks and despite widespread publicity about these vulnerabilities, most Web site owners fail to scan effectively for the common flaws and become unwitting tools used by criminals to infect the visitors that trusted those sites," the report states.

Whatever the delivery mechanism being used, a successful attack against a client computer can give the attacker a foothold within an organization.

"Once the client gets exploited, the attack pivots through the organization," ultimately giving access to servers housing sensitive data, noted Ed Skoudis, who works with the Internet Storm Center, in comments on the release of the report.

The report urged organizations to better protect DMZ-based Web applications from SQL injection attacks and to pay more attention to keeping application patches up-to-date, even on clients that do not contain or have direct access to sensitive data. "There is no single silver bullet here," Skoudis said. Attention must be paid to security at different locations to build up adequate layers of security.

The report was based on attack data gathered by TippingPoint from 6,000 organizations, in addition to vulnerability data from 9,000 organizations monitored by Qualys. The study was undertaken to update a list of the Twenty Critical Controls for Effective Cyber Defense, which is maintained by the Center for Strategic and International Studies.

The information included in the report is enlightening, said Alan Paller, SANS Institute's director of research.

"For the first time, they have taken the cover off the attack space and the vulnerability patch space, so you can see inside and see what is happening."

The findings are not surprising, however. Cybersecurity vendors and industry organizations have been reporting the trend toward exploitation of applications rather than operating systems for several years.

"People heard about it, but they didn't do anything about it," Paller said. What the report provides that is new is specific data that should allow IT security professionals to focus priorities. "I think we failed because we didn't prioritize. If you're security people aren't fixing these things, you have to get new security people."

The patch cycle for applications now is much slower than for operating systems, with a decrease in the number of vulnerable systems of only about 20 percent over 60 days from the release of a patch, said Wolfgang Kandek, the top technologist at Qualys.

"Applications that are widely installed are not being patched at the same speed as operating systems," Kandek said. The same tools often can be used to patch both applications and operating systems, he said. The reason they are not is cultural. "It is a fear of breaking the applications that makes the IT staff reluctant to patch the applications. It is critical for organizations to realize this is becoming an attack vector."

The United States is overwhelmingly the top target for server-side HTTP attacks, the study found. "For years, attack targets in the United States have presented greater value propositions for attackers, so this statistic really comes as no surprise." This country is also the overwhelming top source of such attacks.

The threats are being compounded by a growing pool of researchers who are discovering vulnerabilities before they are known to and fixed by application vendors, so called zero day vulnerabilities.

"The skill set of people who are discovering the vulnerabilities is sharper now than ever," said Rohit Dhamankar, the top scientist at TippingPoint and a principal author of the report.

Unfortunately, the study found that this pool is growing faster among the bad guys than among the good guys. "There is a corresponding shortage of highly skilled vulnerability researchers

working for government and software vendors," he said. "So long as that shortage exists, the defenders will be at a significant disadvantage in protecting their systems against zero-day

Credits : William Jackson; http://gcn.com

RESEARCH

How to measure security?

NIST maps out the emerging field of IT metrology

Information technology security is a hot topic, but attention usually focuses on the lack of it. What is missing is an objective, quantifiable way to effectively measure it.

"Security can be looked at in different ways by different people," said Wayne Jansen, a computer scientist at the National Institute of Standards and Technology's IT Laboratory. There is quality control for code developers, the process of deploying a system, and its maintenance by users. "These are all different aspects," and they do not lend themselves to traditional methods of measurement used in physical science, he said.

Jansen has examined the status of efforts to develop security metrics, identified challenges and suggested a course for future research in a recent NIST report, "Directions in Security Metrics Research."

There have been a number of efforts to establish metric systems for security, including the international Common Criteria, the Defense Department's Trusted Computer System Evaluation Criteria, the European Communities' Information Technology Security Evaluation Criteria, and the International Systems Security Engineering Association's Systems Security Engineering Capability Maturity Model.

"Each attempt has obtained only limited success," Jansen wrote. "Compared with more mature scientific fields, IT metrology is still emerging."

The issue is complicated because security means different things to different people and organizations. "Security is risk- and policy-dependent from an organizational perspective; the same platform populated with data at the same level of sensitivity, but from two different organizations, could be deemed adequate for one and inadequate for the other," he wrote. "The implication is that establishing security metrics that could be used for meaningful system comparisons between organizations would be extremely difficult to achieve."

There is no standardized terminology for discussing or describing security, Jansen said. The Federal Information Security Management Act's criteria for rating systems as low, medium or high impact is subjective, and assigning them numerical rankings can blur the distinction between qualitative and quantitative measures.

It is difficult to remove subjectivity from IT security. Security measures can be correctly implemented yet still not be effective. "Effectiveness requires ascertaining how well the security-enforcing components tie together and work synergistically, the consequences of any known or discovered vulnerabilities, and the usability of the system," the report states. In other words, what is effective for one system might not be for another.

Are meaningful security metrics even achievable?

"The answer is yes," Jansen said, "but they might not be as satisfying as you want."

He identified two broad areas of research — process and organizational maturity — that focus on the care and maintenance of IT systems, and the intrinsic characteristics or properties of the systems. "I think we can make good progress on the maturity aspect," he said. Research on security characteristics is not as far along.

There is not likely to be a single system of security metrics anytime soon because of the need to address different elements of security separately. Jansen cited the Federal Information Processing Standard 140 for cryptographic modules as a workable metric "because it bites off a manageable chunk." The much broader Common Criteria, on the other hand, is less effective, he said.

"The issue of how to do this is going to be with us for the foreseeable future," he said.

Challenges to effective security metrics identified in the report include:

- The lack of good estimators of system security.

- The entrenched reliance on subjective, human, qualitative input.
- The protracted and delusive means commonly used to obtain measurements.
- The dearth of understanding and insight into the composition of security mechanisms.

Promising lines of research for improved metrics include:

- Formal models of security measurement and metrics.
- Historical data collection and analysis.
- Artificial intelligence assessment techniques.
- Practicable concrete measurement methods.
- Intrinsically measurable components.

Credits : William Jackson; http://gcn.com

Education

How to Recover Your Firefox Master Password

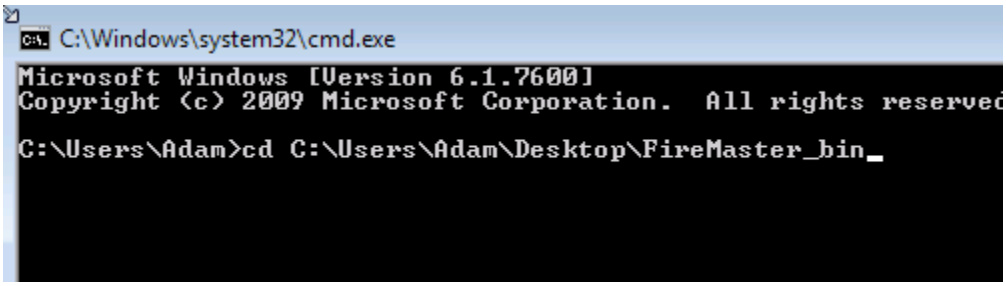
If you're using Firefox's built-in password management, you should also be using its master password feature to protect your saved passwords from prying eyes. But what happens if you lose your master password?

Since the master password prevents anyone from accessing your saved passwords, you're out of luck if you lose your master password—that is, you can't access any of your saved credentials without it.

That's where the free, open source tool FireMaster comes in. FireMaster is a command line tool designed specifically to recover your master password from Firefox. Here's how to use it:

1. Download FireMaster and extract it to a folder on your desktop.

2. Open a command prompt. (Shortcut: Hit Win+R, type cmd, then hit Enter.)



3. At the command prompt, change the FireMaster folder to your active directory. The quickest way to do this is to type cd , then drag and drop the FireMaster folder from your Desktop onto the command prompt—which will automatically fill in the path to that folder. Then just hit Enter.

4. Construct your FireMaster crack command. FireMaster supports a lot of different options, but you can speed up the process if you can narrow down a few points to customize your password cracking. For example, if you know you've only used alphabet characters (a through z), adding the following to your command can speed up a brute force attack significantly: -c "abcdefghijklmnopqrstuvwxyz" For the purpose of testing and providing an example, I wanted to see how long it would take for FireMaster to crack a password containing only letters (a through z) that I knew was exactly six characters long. The resulting command looks like this:
FireMaster.exe -b -q -l 6 -c "abcdefghijklmnopqrstuvwxyz" -p "??????"%appdata%\Mozilla\Firefox\Profiles\1sq2zzh2.default

   As you can see, I'm telling FireMaster to try a brute force crack on a 6-character master password using only the letters a through z. (You should read through the usage information to get a better idea of what options you've got for customizing the process to what you know about your password to speed things up.)

   In the last part of the command, I'm pointing FireMaster to my Firefox profile folder, where the key3.db file exists (this is the file that contains the encrypted password information). The last folder in that path will differ for you, but everything up to that folder (i.e., %appdata%\Mozilla\Firefox\Profiles\ will get you most of the way there. (If you only have one

Firefox profile, you should just see one folder inside Profiles; use that folder.)

5. After you've constructed your command, just hit Enter to get cracking. Using the command constructed above, FireMaster took roughly 23 minutes to crack my Firefox password. If I didn't know how long the password was, it would take significantly longer (you can offer a minimum and maximum password size to help narrow things down a little further). That said, it clearly wasn't all that difficult to crack my password given all I knew about it. It gets much harder the more secure your password is (think unusual characters and long passwords).

Every time we post something about, say, how to crack a Windows password, we have to address the privacy issue. Password cracking tools like FireMaster can, like most things, be used for both good and evil. If you've forgotten your master password and you're desperate to get the keys back to Firefox, it can be extremely useful. If you just like testing how secure your current password is, it's a handy tool. (I always love testing my passwords against these sorts of things.) It would also, obviously, do the trick if you're trying to steal someone else's information. Don't use it for that, jerk.

If you're really serious about your passwords, we'd recommend securely managing them with KeePass.

FireMaster is a free, open-source download. It works on Windows, but it can crack the master password from any Firefox installation—you just need to copy the key3.db file to a folder on a Windows computer and point FireMaster at that folder. If you give it a try, let's hear how crackable your master password is in the comments.

Credits : Adam Pash; http://lifehacker.com

EVENTS

iT'S Bengaluru

Location : Hotel Chancery Pavilion, Bangalore
email : jairaj@totalesp.org
Website : http://www.totalesp.org/

Date	Themes	Tracks
22 August, 2009	Information & Communication Technology applications	Banking, Insurance, Finance Sector(NSE, BSE, Commodity Exchanges,NSDL & SEBI)
29 August,2009	Information & Network Security	Non IT Sector (Manufacturing,Services, Academics)
5 September, 2009	Technology & Management	Telecom Sector
12 September, 2009	Information Security Strategy Management	Core IT Sector
19 September, 2009	Technology Management	Hardware Network and BPO Sector

Media Partners : CCC News Control Computer Crimes

HITB Security Conference 2009

Date : October 5, 2009
Location : Malaysia
Website : http://conference.hackinthebox.org/hitbsecconf2009kl/?page_id=292

"Bangalore Cyber Security Summit- 2009"

a National Conference on Cyber Security

Date : 8-9 October, 2009
Location : Hotel Ashok, Bangalore, India
email: osd@bangaloreitbt.in, kulkarnitr@gmail.com

Gitex Technology Week

Date : October 18, 2009
Location : Dubai International Conventional Exhibition Centre, Dubai

Website : http://www.gitex.com/

fourth annual eCrime Researchers Summit (eCRS)

Date : October 20, 2009
Location : Tacoma, WA, USA
Website : APWG <http://www.antiphishing.org/>
http://www.ecrimeresearch.org/2009/cfp.html

The 3rd International conference on IPRs

Personal Data Protection and National Security

Date : October 20-22, 2009
Location : Beirut, Lebanon
Website : http://www.cybercrime-fr.org/index.pl/cyberlaw2009

OWASP AppSec Brasil 2009

Date : October 27, 2009
Location : Câmara dos Deputados in Brasília, DF
Website : https://www.owasp.org/index.php/AppSec_Brasil_2009

T2'09

Date : 29 October, 2009
Location : Câmara dos Deputados in Brasília, DF
Website : http://www.t2.fi/

New age cyber crime – by Marcusevans

Date: 29 & 30 October 2009
Location: Le Royal Meridian, Mumbai, India
Email: leec@macrusevanskl.com

Media Partners : CCC News Control Computer Crimes

Answers to Quiz 0006

1. Facebook is also called a ***SOCIAL*** networking site.

2. Indian competitor of Google earth is called ***BHUVAN***.

3. In reporting bugs / errors, reporting a non-existing bug / error is called false ***NEGATIVE***.

4. A program downloaded with limited features for evaluation, which can be purchased later, if liked, is called ***SHAREWARE***.

5. An IP address (in IPv4 or IP version 4) has 4 dot-***DASH*** notations.

Winners for Quiz no 0006

Grand Prize

Bhupati Seth, Mumbai, India

Three consolation prizes

1. Ashwin Bhavsar, Thane, India
2. Nirmala Jacob, Kolkata, India
3. Riddhi Sharma, Chandigarh, India

Congratulations to all winners and others with correct answers.

This edition of the magazine is brought to you courtesy

Sysman Computers Private Limited

Sysman is

1. **Pioneer in IT Security since 1991**
2. **Empanelled with CERT-In**
3. **Done over 2000 IT Security assignments**
4. **Provide Research Support**
5. **Create Public Awareness**
6. **Published 6 Books / 50 papers**
7. **An associate consultant to BSI to implement ISO 27001-ISMS**

Contact –

Sysman Computers Private Limited, Mumbai

sysman@sysman.in

+91-99672-48000

www.sysman.in