GIAC Security Essentials Certification Practical
James Fee Langendoen
August 2, 2003
Version 1.4b
Option 1

A Remote Access Conundrum

ABSTRACT

The desire to have easy access to work documents and the advent of Remote Access Services such as ExpertCity's GoToMyPC have provided a potentially hazardous situation to the safety and security of the corporate network. The issue becomes an awareness of the inherent threats incorporated in potentially unmanaged access to the network.

Capable of navigating through a firewall or NAT, and touted as using 128 bit encryption for security, GoToMyPC fulfills many remote workers' needs for a means to access their work without the hassle of those "pesky" IT people. This document also provides some options if the users on your network have taken it upon themselves to utilize this type of access without proper authorization.

GoToMyPC

A client of mine had sustained serious injuries in a bicycle accident which would prevent him from driving to work for a period of 6 weeks. He is a lawyer and while he would be able to function from home, could not do so without access to information that also was required routinely by other members of his firm. The office maintained a small Windows based workgroup network and utilized a cable-modem connection for Internet connectivity. When he contacted me, he was looking for a way to have remote access to his files. I went though several candidate products, but I was very interested in the abilities of GoToMyPC to function through his cable-modem and NAT router, since he had no external IP address. It was also one of the fastest interfaces for a remote control product and they offer a 30 day free trial period.

GoToMyPC from ExpertCity is a hosted service, billed monthly, consisting of a small server application on the Host PC, a Browser (on the client side), a Broker (a matchmaker that listens for connect requests, mapping them to registered computers) and a Communications Server which is an intermediate system that relays an encrypted stream from client to server.[1] Because the server sends out a "ping" to the Broker at regular intervals over HTTP/TCP ports 80, 443 and/or 8200 , it is capable of navigating outwardly through most firewalls, proxy's and NAT routers (the company refers to it as "Firewall Friendly"). The resulting connection is quite workable and has the additional benefits of file transfer and remote printing.

Beside its technical merits, the product is very aggressively marketed. It was noted in a review by Itzhot.com that the top 7 factors that make the GoToMyPC.com website very compelling to a first time user include: Credibility, Easy viewing, Compelling Universal Need, Cost is Acceptable and Affiliate Payout is high, Easy to Use and Implement, and Testimonials.[2] One of the initial challenges of researching for this paper turned out to be the high volume of targeted advertising that the company engages in. Virtually all Network and Administrative websites have hot links to the product demos (most likely due to the affiliate payouts). Consequently, most searches for information involved a significant amount of "wading" though pages with interesting but unrelated information and a GoToMyPC advertisement or link.

There are actually 3 levels of the product, Personal, Pro, and Corporate. The distinction being that the Pro and Corporate versions have increasing levels of Administration available to monitor and manage multiple users. This is done through user control lists and connection logging functions. The Pro version came out during the last revision of this paper, so it is quite a new addition to the product mix.

ExpertCity has gone to great lengths to develop a security model that seems well thought out. It is very well publicized and they capitalize on its strength. It utilizes SSL-authenticated encrypted requests to the Broker. In their documentation, they talk about their Secure Facility, Secure Network, Secure Platform, and Secure Administration. While I commend them for their textbook presentation of their security, I would caution against overconfidence

They have garnered accolades and awards like the PC World World Class Award for Remote Access in 2003[3] and PC Magazine's Editor's Choice for Remote Access as well as a host of other prestigious accolades.[4]

It all seems so good and simple doesn't it?

"Make things as simple as possible, but no simpler" – Albert Einstein

The problem is not of its use, but more of its misuse, whether well intentioned or not. In the example I started off with, GoToMyPC provided a very well suited solution to a remote access problem. In a small office environment, there was no

IT staff and the client machine that would access the system was only in the residence of one of the principles of the firm.

As I continued to research the product, it initially struck me as incongruous that a company like CheckPoint Software would issue a Public Advisory for Corporate Networks with a Severity rating of Medium.[5] However, I came to agree with them that this in fact could constitute a viable security threat.

Somebody smelled a RAT

It turns out that CheckPoint[6] (a company involved in Firewall, VPN, and security technologies) wasn't the only company with concerns. PestPatrol, a company that markets products designed to detect and remove or disable security programs like spyware, DDoS, Trojans and other Hacker tools classifies GoToMyPC as a Commercial RAT (Remote Access Trojan).[7] While I am certain that ExpertCity goes apoplectic over the designation, what is important to keep in mind is that used without consent, the appellation may be appropriate. RS-232C (Co-Founder) of Winforums listed GoToMyPC on his RAT list in his post of 1/20/03[8]

"**Warning** For those downloading Remote control apps for the first time on the net..if you hear of a good one, download *from* the company Site that made it..and it wouldn't hurt to monitor your outgoing/incoming connections either.. there are more than enough proggies out there that are trojaned with these RAT's"

That piece of advice turned out to be quite valuable. A quick Google search using the keywords "crack GoToMyPC" turns up a significant number of links. The same was true of the keywords "warez GoToMyPC". For the uninitiated these terms can be found in places like the Jargon Dictionary[9]. The primary function of a cracked or warez version of the software would be to create a vehicle for later use by someone other than the computer's owner. That means that a user could download a compromised copy of GoToMyPC and the hacker/cracker who had the backdoor credentials could later hijack that PC.

Even if the version were legitimately from the originating company, there are still the potentials of infection from outside attack. SOPHOS, an anti-virus company, lists the W32/Sddrop-B Win32 worm as using GoToMyPC.exe (among others) as a host.[10] This would make it doubly important to insure that all involved PC's have reliable, updated virus protection.

The distinction that needs to be made here is that these references are aimed at the mis-use or subverted use of the program. The point to be addressed is simply; Do you know if this type of product is being used on your network and if so, how is it being used?

In the News

What brings this discussion out of the realm of academic research and into the light of day are some of the current news stories which have circulated. From Security Focus dated March 18 2002, Brian McWilliams in an article entitled “US Military Scours Windows Systems for Hacker Backdoors” [11]

By Brian McWilliams, Newsbytes
ATLANTA, GEORGIA, U.S.A.,
15 Mar 2002, 11:22 AM CST

The United States Army and Navy are conducting a high-priority security review of their Microsoft [NASDAQ:MSFT] Windows systems for the presence of an unauthorized remote-control program, sources familiar with the investigation have confirmed.

An unclassified memo, sent Mar. 6 by the Navy's Computer Incident Response Team (NAVCIRT), warned Navy computer administrators to scan their Windows systems for evidence of a popular commercial software program called RemotelyAnywhere.

"NAVCIRT received several computer incident reports involving the installation of RemotelyAnywhere on compromised computer systems which in turn enables scanning, probing, and compromising of additional DOD systems," said the memo, a copy of which was received by Rob Rosenberger, an independent virus expert who consults to the military on information security matters.

Officials from NAVCIRT, which is part of the Navy's Fleet Information Warfare Center in Virginia, were not immediately available for comment.

A similar message was sent Mar. 13 by the Army Forces Command to computer systems staff at all of its installations.

The Army memo, which was distributed by e-mail and designated High Importance, warned information assurance managers (IAMs) that the remote access tool "may be sitting on our systems, waiting to be launched."

A copy of the Army e-mail obtained by Newsbytes instructed Army system administrators to search all Windows computers for the presence of files that "are evidence of system compromise."

Jack Coffey, an Army Forces Command spokesman in Atlanta, confirmed the authenticity of the memo and said it was based on the advisory from NAVCIRT as well as one from the Department of Defense Computer Emergency Response Team. Coffee said he was unable to immediately provide more information.”

OK, so you say that the program that the Navy and the Army were after was very similar, but not exactly GoToMyPC? Then the July 18, 2003 article by Kevin Poulsen “Guilty Plea in Kinko’s Keystroke Caper”[12].might strike closer to home. In his lead sentence, he states:

"If you used a computer at a Kinko's in New York City last year, or the year before, there's a good chance that JuJu Jiang was watching."

More complete details can be found at the Department of Justice site for the Indictment of Jiang on December 20, 2002 [13] and his subsequent guilty plea on July 11, 2003 [14].

The long and the short of this story, as you may well imagine, is that Juju Jiang of Queens, New York had hijacked over 450 online banking passwords and user names. Jiang had installed a program called "Invisible Keylogger Stealth", a kernel mode keyboard sniffer. The way in which he was caught was that while he in a stolen GoToMyPC account, the owner of the account noticed the PC's cursor moving on it's own accord and establish a connection with an online money transfer site under the victim's name. It was with the help of GoToMyPC's access logs that the U.S. Secret Service was able to ascertain Jiang's IP address. The frightening aspect of this story is that it took someone whose monitor was still lit to see and realize that something was wrong. In most corporate environments the only folks around at night are the cleaning crew. While I admire the job they perform, I'm not certain that they would understand the implications of a computer cursor moving "on it's own".

The point of relating these stories is not a castigation of GoToMyPC but an attempt at presenting a balanced view of the risks and rewards. In many ways, Remote Access seems to be analogous to nuclear power. It is extremely powerful in its benefits, but can be potentially disastrous if not used in the manner it was designed for. At this point, I would like to state that I do not feel that there has been any attempt on the part of ExpertCity to develop a "black-hat" tool. As I stated earlier, there are actually three levels of the product and each has functions for its own targeted segment. The two levels of corporate licensing try to address the issues I am raising with the basic product.

Even if you have done your best to install an application like this in conformance with your existing Security Policies, are you aware of the additional security issues which can be raised through the use of remote access software and public access computers?

Security

For many small companies the concept of a security policy usually starts somewhat informally. People working from home and/or small offices are more and more concerned with things like Anti-Virus protection and Personal Firewalls than developing security models in active directory. Access control tends to be among a group of people who all know one another. This is their way of mitigating threats and vulnerabilities. As an organization starts growing in size, so too do the vulnerabilities it faces. In response, an organization develops security policies and procedures. They implement this in a variety of ways such as physical and network security. A larger, more mature organization will develop a threat model and calculate vulnerabilities to existing threats. The principles of Confidentiality, Integrity and Availability will form the basis of the security policies and be expressed in physical access control, password policies, and workstation security policies.

The concept of "Defense in Depth" expressed in the Security Essentials course actually takes shape as the organization grows. For a small organization where the administrator can be fairly aware of the activities of all participants, it is difficult to map the structure of a defense in depth program since many of the security attributes overlap. This changes rapidly as the organization grows in size and spans several sites and a diverse population of workers with different needs and responsibilities. A simple concept such as physical access takes on a whole new dimension. More specifically, network access and privilege become a challenge worthy of an entire discipline. The defense in depth graphic depicts a security model with annular rings providing successive layers of protection for the organizational data. In that graphic, the data is surrounded and protected by the applications, the hosts and the networks, each with their own subsystems of protection and documentation.

This security mindset leads to the development of physical access control lists, network access groupings, network firewalls and VPN's, all designed to monitor which machines connect, who is using them and when these connections occur.

Nothing out of the ordinary so far, right? Then why would there be an advisory on this product?

How could a beneficial tool like GoToMyPC be considered a risk, a threat or a vulnerability to a network's Confidentiality, Integrity or Availability?

The issue stems from the unauthorized injection of the basic product into a corporate network. The installation of this type of product without the knowledge and support of the administrator works to subvert several of the defenses used to protect and monitor the corporate data assets. While in and of itself it can be a useful tool, it also can be a platform for attacking the network infrastructure.

However, security policy can be developed for remote access even if it becomes necessary from public access computers. The proviso is that both user and management be aware of the risks and that the methods of authentication be adjusted or augmented accordingly. Even just a password change after such use would help. If it were to be a more common occurrence, a product with a changing number sequence like a SecureID might be of value.

<u>Knock Knock, Who's there?</u>

The basis for protecting an organization's assets revolves around knowing who has access to them and monitoring that access. As companies cultivated knowledge workers who could perform tasks without all being at the same physical location several technologies were implemented to maintain a secure manner for the workers to connect and share data. Initially dial-up and lease lines gave you control over the communications channel in very tangible ways. With the advent of the internet, the VPN became a more realistic approach to having remote corporate computers connect and validate into the corporate networks in a secure fashion. The key was that the hardware as well as the software became components of the security process. It was simply less likely that an end-user would configure a remote dial-up on an unknown machine, even more so with many of the current generation VPN clients. More importantly, the portals for these connections were monitored and logged. The logs would document success and failures for connections and attempts and appropriate actions could be taken if improper events seemed to occur. Those ports could be open during normal (even if extended) work hours or restricted as needed.

And then there were none…

The most significant issue with GoToMyPC standard version is that the audit trail is at best obscured and at the worst almost untraceable.

Kevin Tolly in his NetworkWorld article 'Always On' programs pose an 'always on threat ' stated:

> "Try as they might to secure the enterprise - using firewalls, VPNs, intrusion detection and content filters - network managers are being defeated in droves . . . by their co-workers. .. For network managers, though, such programs can create network performance headaches and set the stage for serious security breaches. "[15]

A worker who connects to their work machine from the outside does not generate the same type of traffic that we are used to logging. Good IT security policy would have the workstation log off after a period of inactivity. That situation would require the remote access to log in, but other than the time of the logon (to the local workstation) there would not be anything extraordinary about the event. Worse, if the user has sufficient rights to install this program, it would also be likely that they would just "leave the workstation on" when they left to facilitate their own connectivity.

Another issue is that with the availability of web based connectivity, there is no control over which computer is connecting to the internal network machine. For the most part it might be the home or personal computer of the worker, but it doesn't have to be. The hard part is getting the security buy in from the users. They need to understand why this like any resource needs monitoring. As Toni Kistner said in her NetworkWorldFusion article A Network manager's nightmare, "Of course, you're thinking: what's the point of even having a firewall when everybody can bust through it without my knowledge or permission? True enough. But don't go blaming the technology or your users' freedom to access it. What you're grappling with is a people problem."[16]

The issue I have with that is the risk is not equally shared by the users and the organization. Rarely is the user in a position to determine what level of risk the organization is willing to accept. When a network is compromised it seems that the end users do not share a proportionate share of the burden that those events visit upon the administrators (of course, that is the view from the position of a system administrator).

What *IS* the risk?

One risk would be the hijacking of the GoToMyPC account.

How is this possible? Chris Lindquist stated it best in his Tech Tact article Remotely Possible for CIO.com:

"Now this wouldn't be a real problem if all your users were cautious and changed their passwords regularly and didn't access their work systems from God-knows-what public access Web café in Prague or Omaha or the like where some 15-year-old miscreant has installed a keystroke-tracking utility. But if someone glances over the proper shoulder one day and gets that username and password (two of 'em actually), your systems could instantly become an open target."[17]

Like most exploits, the likelihood is based on a set of conditions which may or may not readily exist for your organization. But as the Jiang case documents; this is not as far fetched as you might like to believe.

A simple analogy would be to a box cutter. It's a rather simplistic device used by stock clerks at grocery stores all over. It is a single edge razor blade in a holder, usually with a covering. Before September 11th, passengers were prohibited from bringing them on airplanes, but it was still possible to find ways of getting them on board. After the tragedy of that day, it was found that the security rules (which already existed) needed to be more stringently enforced – for everyone's safety. Those very simple devices, used in an unintended manner by very dangerous people created a situation that very few people foresaw.

The danger of an unauthorized version of GoToMyPC being loaded onto your corporate network and then hijacked lies in the hijacker's ability to probe assets as a trusted member of the network with very little notice or logging of that probing. This exposure is real, so I would also rate this as a risk. Combined with the product's ability to upload files, the damage could be considerable owing to a hacker's ability to insert the cracking tools of their choice within the boundary of the network. There is considerable support for the decision of the Army and the Navy to track down an unauthorized remote control program.

In particular, I would like to point out that the services mentioned did NOT castigate Remote Access programs across the board, but to limit the advisory to the “unauthorized” versions. While it is difficult to read much into that, it is conceivable that they experienced a “cracked” version. However, it is equally likely that they just decided to reassert access control over their network, if they felt that it was possible for it to be compromised. Either way, the decision process would not be significantly different for a network admin of any network of moderate or better size. The fundamental question is what your tolerance to exposure is.

Jay Heiser detailed the problem in his May 2002 InfoSecurity Magazine article “Combating Nonviral Malware” He talks about the huge category of unwanted code. In that grouping, you find things like unauthorized remote access software, the latest P2P offerings as well as the more traditional electronic burglar tools.

“The formal definition of malware is "malicious software." The only safe assumption is to treat all unwanted code as "malicious." While viruses and worms are the most visible forms of malware, "unwanted code" describes a broad range of software that potentially violates an organization's security policy.”[18]

Ultimately that is the basic problem, isn’t it? Has your security policy been breached? The issue starts to become clearer as we evaluate what it is we wish to allow on our networks and what we choose to prevent. Also, if we have no policy, we have very little defense to the user community for denying them. Not only must we defend our networks, but through policy we must defend our actions.

Another potential risk comes in the form of having an unknown machine connect to and transfer files into the network. The exposure is trusting that there is an antiviral agent updated and actively working on the unknown machine and that the machine does not have a Trojan or worm for which your corporate software has no protection yet.

As I stated, ExpertCity does indeed have corporate type products. And those products do have User logging and management features, but that is not true of the basic product. So how do you secure against it?

First Steps…

The first step is actually to see if any of the types of software we have been discussing exist on our network. The more you view the problem and the larger your network, the more you begin to appreciate that we are talking about a nontrivial task. What’s worse is that with all the high profile risks that assail us daily, this is a tough one to add to the list of things to get done. For argument’s sake, let’s just stick with the Remote Access program I started with, GoToMyPC

(though you have seen that the list rapidly expands to other products and categories)

While I might be inclined to see if this were a viable means of connectivity for my organization, I would like to insure that the discussion happened on my terms. So a quick trip to the firewall and block the host poll.gotomypc.com. You should also block traffic to port 8200 as well. For a complete shutdown, block access to GoToMyPC Broker servers poll.gotomypc.com and static.gotomypc.com on the firewall ports 80,443, and 8200. This would allow time for a discussion without compromise.

Personally, I subscribe to Mike Olsson's post in the Netsys.com Intelligent Hacker's Choice! Firewalls Archives regarding GoToMyPC,

> "try to block access to their servers, to prevent dumb users from ... well.. being dumb…In any case, I'd _never_ allow anything like this in a high-security environment, the same way I never allow ANY logons from external sources in such environments."[19]

But as they say, your mileage may vary.

In conjunction with managing the firewall, you will also need to review your standard security practices.

Review your documentation for workstation and password security. No, it won't specifically stop the problem, but in many ways this is a Social Engineering type of problem. As an administrator you will need to be able to justify your company's position to the users. Having current documentation can only help (as do periodic reviews).

Also, go through your group policies. While it may be seen by some as Draconian, perhaps it *isn't* a particularly good idea to allow users to indiscriminately load software brought in from wherever. A review in light of a new vulnerability will often bring out exposures that were not considered to be as pressing previously. What makes all security policy reviews valuable is that (hopefully) we learn from the iterative process. Organizations are by nature dynamic and as such their security needs and challenges change over time. In this paper I am documenting a challenge to remote access, but you can see how it rapidly touches most of the areas of security that an administrator must address.

The best way to respond to a challenge is through the tried and true methods of falling back on sound security implementation.

Try frequent logging and monitoring of port traffic with particular attention to the outbound 80, 443 and 8200. This particular situation is one in which you are looking for what is essentially non-HTTP data through the HTTP port.

It is not surprising that products are beginning to appear that address issues like this. Vericept™ is offering a product tailored to these specific (as well as other) threats in their product Vericept™ View for Network Security:

"Logs in this group can be generated by unusual system administrator activity, non-RFC compliant client software or hack activity. GoToMyPC activity could be legitimate, but is often disallowed by organizations, as it enables remote access to internal machines, bypassing the firewall. Categories include hacker research, GoToMyPC client and server activity and suspicious IMAP, POP, shell and VNC activities."[20]

This is most helpful in this in dealing with the high volumes of traffic for the ports under scrutiny.

As noted earlier, PestPatrol also offers a product to detect and disable the GoToMyPC server application. As the notion of "Nonviral Malware" expands, so too will the tools to address the problem.

Address the Needs

If this type of activity has been occurring or the users are attempting it the fact is that the users believe that they need better access. While that may or may not be sufficient to drive the organization into a solution, it is certainly an indication that as an administrator you should re-evaluate the potentials, both good and bad of current state of remote access.

Perhaps your organization would be well suited to one of the Corporate offerings of ExpertCity, or possibly to one of the newer VPN clients used in conjunction with independent validity checking (biometric or SecureID).

The point is, if this issue arises, it will not likely go away but more likely come back in a different form. Already there are other products appearing that wish to capitalize on the success of GoToMyPC. Examples of this would be If & Then's TravelingPC or the Remotely Anywhere product detailed in the NAVCIRT advisory. The number of products is likely to grow as their popularity increases.

The goal is to be able to serve the organization securely. Providing users with secure access while maintaining a secure facility is the challenge we face. I cannot say that I believe that this particular vulnerability will last for an extended period of time, though it might. As I had stated in the beginning, I do not believe that ExpertCity had any evil intentions when it developed their product. But what they did develop has been a rapid success and keeping up with that initial success has not allowed more mature features to have been developed for it yet as has happened to its predecessors like Symantec's PCAnywhere. I fully expect to see this product develop and mature.

But, that being said, the problem I have is to secure my networks now. While I can admire the design aspects of this product and in fact have implemented it successfully in an appropriate environment, I must understand that it has significant potential for harm in an inappropriate environment in its current basic form.

In a story that broke on CBSNEWS.com on July 22, 2003 entitled “Cybercafes Pose Security Problems”[21] relating to the Jiang/Kinko affair it becomes apparent that the root of the problem for this type of exposure is in the unsecured nature of public terminal access. As long as an administrator cannot guarantee the security of that access, the network will be at risk. Even with Kinko’s, a company who attempts to maintain a measure of security for the public access machines there is a demonstrated risk.

“Last year, Kinko's security measures became an issue in the pre-trial arguments in the Zacarias Moussaoui terrorism prosecution. Defense attorneys sought information on Moussaoui's 2001 use of a public access PC at a Minnesota Kinko's store, but were foiled by what the FBI said was Kinko's national policy of completely reimaging public access machines on a weekly basis.”[22]

The most significant challenge is to know what products are installed on your network and how educated your users are to the fundamentals of security. While the “Holy Grail” of users may well be to access the corporate information from “anywhere”, the process needs to be managed for the protection of all concerned parties. Products like GoToMyPC without management have the capacity for “flattening” out a well crafted defense in depth.

I would like to finish up by quoting Law 9 of the Ten Immutable Laws of Security Administration (but you really should check out all 10)…

Law #9:
Security isn't about risk avoidance; it's about risk management.
One of the most often-cited truisms in computer security is that the only truly secure computer is one buried in concrete, with the power turned off and the network cable cut. It's true – anything less is a compromise. However, a computer like that, although secure, doesn't help your company do business. Inevitably, the security of any useful network will be less than perfect, and you have to factor that into your planning.

Your goal cannot be to avoid all risks to the network – that's simply unrealistic. Instead, accept and embrace these two undeniable truths:

There will be times when business imperatives conflict with security. Security is a supporting activity to your business rather than an end unto itself. Take considered risks, and then mitigate them to the greatest extent possible.
Your network security will be compromised. It may be a minor glitch or a bona fide disaster, it may be due to a human attacker or an act of God, but sooner or later your network will be compromised in some fashion. Make sure you have made contingency plans for detecting, investigating and recovering from the compromise.
The place to deal with both of these issues is in your security policy. Work with corporate management to set the overall guidelines regarding the risks you're willing to take and how you intend to manage them. Developing the policy will force you and your corporate management to consider scenarios that most people would rather not think about, but the benefit is that when one of these scenarios occurs, you'll already have an answer. [23]

Conclusions

Remote Access tools in general and GoToMyPC in particular definitely have a place in the arsenal of IT tools. They leverage the ability to geographically disperse workers while maintaining centralized corporate data stores. In doing so, they bring a somewhat unique problem into the mix. They have an ability of providing access to the corporate network by virtue of being able to access a specific piece of that network from anywhere that has internet access. That has an ability to compromise the network in a couple of ways.

Even as sanctioned manner of connection since you have no verification of Virus or other malware protection if a public terminal is used. Then too there is the possibility of a Jiang like hijacking. The problem with that is the open ended exposure. If a user loses a laptop computer, there may be some files compromised but generally it does not entail access to the network (assuming the loss is noted to IT) since its privilege would be revoked. The difficulty with this class of remote access tools lies in its inability to monitor itself (again, I am using the basic product for example).

I believe that the key is in knowing where your assets are deployed and accessed from. In the opening story, the computer in the lawyer's house did not pose a risk to his Law Office. Similarly, arranging for responsible members of an organization to access their computers from their homes can indeed be structured to the satisfaction of all parties concerned, particularly with the logging versions and sound security procedures.

The key is in sound security policy administered sensibly with the knowledge and understanding of the entire organization.

[1] Expertcity® GoToMyPC: A Secure Remote Access Solution, Introduction https://www.gotomypc.com/downloads/pdf/m/GoToMyPC_Personal_Security_White_Paper.pdf

[2] Itzhot Review http://www.itzhot.com/gotomypc.html

[3] http://www.pcworld.com/reviews/article/0,aid,110653,pg,12,00.asp

[4] http://www.asp.com/Archive/gotomypc2122002.htm

[5] http://www.checkpoint.com/securitycenter/advisories/2002/cpai-2002-14.html

[6] http://www.checkpoint.com/

[7] http://www.pestpatrol.com/pestinfo/db/g/gotomypc.asp

[8] http://www.winforums.org/viewthread.php?tid=1751

[9] http://info.astrian.net/jargon/terms/w/warez_d00dz.html

[10] http://www.sophos.com/virusinfo/analyses/w32sddropb.html

[11] http://www.securityfocus.com/archive/12/262528/2002-03-13/2002-03-19/0

[12] http://www.securityfocus.com/news/6447

[13] http://www.usdoj.gov/criminal/cybercrime/jiangIndict.htm

[14] http://www.usdoj.gov/criminal/cybercrime/jiangPlea.htm

[15] NetworkWorldFusion, Kevin Tolly 'Always On programs pose 'always on' threat 09/30/02 http://www.nwfusion.com/columnists/2002/0930tolly.html

[16] NetworkWorldFusion, Toni Kistner A Network manager's nightmare 08/20/01 http://www.nwfusion.com/net.worker/columnists/2001/0820kistner.html

[17] CIO.com Chris Lindquist , Remotely Possible 02/04/2002 http://www.cio.com/online/techtact_020402.html

[18] http://infosecuritymag.techtarget.com/2002/may/combatingmalware.shtml
[19] http://www.netsys.com/firewalls/firewalls-2001-08/msg00673.html
[20] http://www.vericept.com/products/view_security.shtml
[21] http://www.cbsnews.com/stories/2003/07/22/tech/main564568.shtml
[22] http://www.securityfocus.com/news/6447
[23] Microsoft TechNet, The Ten Immutable Laws of Security Administration
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10salaws.asp