New Security Threats over IM and VoIP Software

Tedo Vrbanec, B. S.
Teacher Training College Čakovec
Dr. Ante Starčevića 55, 40000 Čakovec, Croatia
E-mail: tedo.vrbanec@gmail.hr

Professor Željko Hutinski, Ph. D.
Faculty of Organization and Informatics
Pavlinska 2, 42000 Varaždin, Croatia
E-mail: zeljko.hutinski@foi.hr

Abstract – Instant-messaging and Voice over IP software are more and more becoming targets of virus and malware writers. They are attempting to bypass security-system updates and to collect user's confidential personal and financial data. In their nature, those threats are different from usual threats, e.g. those affecting e-mails. Updating virus definitions and antivirus software components is not efficient enough because of high mutating level of those kinds of viruses. The main cause of the success of those threats is in speed of inter-infecting between users.

I. INTRODUCTION

High productivity enabled by the instant messages carries high risk for those organizations which do not take adequate care about the security. The increase of the number of exchanged instant messages is constant, and at the beginning of 2006 [1] 12 billion messages were exchanged every day. As many as 300 million people use instant messages every day. With the increase of the number of users, the risk of the security incident is also increasing.

The security measures for the information–communication assets which protect the organizations from the threats from Internet are increasingly more sophisticated, but at the same time, the frequency of the common thefts of the computers which contain the confidential data about the employees or the clients of the organization is increasing [2].

The technology of the VoIP telephony contains significant security omissions [3], and with the increased use, the risk is also higher. It is estimated [3] that this technology has reached a critical number of the users, and a higher number of hackers is now oriented to the abuse of its security omissions. The same is true for the smart mobile telephones and palmtops. The confirmation for this is the appearance of the *CommWarrior* worm, which was spreading among the mobile phones in Europe at the end of 2005 [3].

The writers of the malign code use methods of social engineering; they send a code packed in an innocent or officially looking packages, to the addresses of the target group, with preliminary research of the organizations, people and their businesses [3], in the form of time-bombs etc.

II. FORMS OF COMPUTER THREATS

In this paper, we will use the term "threat" or "malign code" to refer to every form that endangers the computers and their users. The most common threats are: viruses, worms, trojans, spyware and *phishing*. Spyware is software whose aim is spying of work, habits and behaviour of infected users. *Phishing* is mass sending of specially designed e-mails which direct the addressee to specially designed fake web sites in order to gather confidential data, mostly financial ones, as for example numbers of credit cards, etc. On the electronic black market [3], the data about a person, from the ID number to the mother's surname, can be bought for 13 €, and there are cases of the price being lower than 1€.

One of the threats is the software whose goal is to turn the computer into *zombi*, and creation of *BotNet* – the computer network under alien, malign "control", as well as the activation of the DDoS or other attack to the any goal in any moment, without knowledge of the owner/user. In most cases, the *zombi* computers which make *BotNet* are controlled by system of the instant messages, which are desired target for criminal activities.

The threats are also unauthorized or unwanted changes of the settings of operational and software systems because of the advertising, increasing the hits of certain web sites, or attracting the users to the specially designed web sites which are used as a vehicle for installation of some form of the malign code to the user computer, or are used to offer pornographic contents to the user.

Instant messages software usually has the possibility for script making. This possibility is under the scrutiny of the hackers, which search the vulnerabilities they can use.

The worms specialized for the instant messages are activated and installed to user computers directly, by the careless activation of the hyperlinks in the false instant messages.

There is a new notion, *spim*, which is a derivate of the notion *spam*, unwanted e-mail. *Spim* is an unwanted instant message that is sent through instant message networks.

There are three basic threats in VoIP telephony: firstly, the hackers can reach the confidential personal and financial data, secondly, by launching DoS attacks, they can prevent the legitimate users to reach the resources/services, and thirdly, the users can spread malign VCards (electronic visiting cards).

III. APPEARANCE AND INCREASE OF THE NUMBER OF THREATS IN THE SYSTEM OF INSTANT MESSAGES AND VoIP TELEPHONY

In the October of 2005, the number of attacks through the software support for instant messages increased for 30% [4] compared to September, and more than 70% of the discovered threats were capable of disabling the updating

of the security protection and the virus detection. These tendencies are disturbing, because in November, the number of the threats increased for 226% [5]. Furthermore, as many as 36% [5] of the threats from the instant messages were able to endanger the users of more than one system of the instant messages, and 13% of them have been spreading through all of the major systems: *Microsoft MSN Messenger* and *Windows Messenger* (which share the same network [19]), *AOL Instant Messenger* (AIM), *Yahoo! Messenger*, *ICQ* and *Google Talk*. All these numbers confirm that Internet villains perceive this medium for real time communication as a wide open security hole in corporative networks. On the other hand, it is interesting that the attacks through the P2P networks in November decreased for 36% in comparison to the situation in October [5]; this is certain signal of redirection of the threats from P2P to IM.

Some companies and organizations have services which process the cases of threats to their users. Analyzing these threats [4], they came to the conclusion that as much as 88% of instant message threats (most often, the worms) are prone to mutation. For example, during 11 months of 2005, the worm *Kelvir* mutated as much as 123 times. The most common threats during 2005 were [4] the worms *Kelvir*, *Bropia* and *Opanki*. In the domain of instant message exchange [4], 62% of the mutated threats spreading through the messages are connected to the *Microsoft MSN* network, 25% to *AOL* and 8% to *Yahoo!*

In the sphere of the computer criminal, the criminals have started to join forces, and through the common effort, they are erasing the barriers to the threats. There are more and more coordinated attacks of the viruses, worms, through *phishing*, spyware and instant messages. We are here no longer dealing with persons whose intentions are evil and who have plenty of time at disposal, but with people, whose goal is a large (criminal) profit, measured in hundreds of millions of US dollars. [6].

The experts from MIT [7] have discovered the security hole in practically all VoIP applications, which enables the criminals from Internet to hide their identity during the starting of the DoS attacks or sending the unwanted messages. It is only the matter of time [7] when this technique will become widespread. The researchers from Cambridge have discovered the scenario through which the hackers use VoIP to hide the commands for controlling the computers in which malign software (like trojan) which has already been previously installed. Until now, the preferred vehicle of control have been instant messages, but they can be traced, i.e. their starting and target point can be revealed, while this is very hard to do with VoIP messages, in fact it is almost impossible.

IV. SYSTEMS OF PROTECTION

The firewall has long ago become the part of the software support of every computer, as well as the part of network of every organization which is even remotely aware of the dangers which stem from the Internet. Hiding and copying the real, local addresses into the outer addressed visible to other computers (NAT) has for a long time been a standard factor of security. A time has come for the systems of analysis of the network traffic and network intrusions to take such standard place. Such systems point to the anomalies and traffic of the local network, alarming the network administrator to the possible attacks in progress. It is easy to imagine the next phase of development of the security systems: every software product will be connected with the community established by the manufacturer, so the users will be able to exchange the information about the newly found viruses and other threats for their product or the product group.

The talks transmitted through the Internet should be protected by the cryptographic procedures [8]. Namely, during the telephone order of the groceries, the consumer is dictating the number of his credit card to the seller. In classical telephony this is not a problem, because the interception of such number requires physical contact with the telephone wire or the access to the public or private telephone switch office. Since in VoIP telephony these talks are transformed into the data packages, which move through Internet to their destination via many of the other machines out of the control of the communication participants, it is obvious why the messages should be encrypted. *The American National Institute for Standardization and Technology* (NIST) is also aware of the importance of the issue of security and VoIP telephony. In January 2005 it has issued a special publication SP800-58 which contains detailed security considerations for the VoIP systems [8].

The organisations that can afford it are introducing instant messages gateways. In such way, they can introduce another level of the protection, described in Table 1.

Table 1. Types, levels and sites of protection through the instant messages [4]

Name/description	**Level of protection**	
	AV protection of e-mail and computers	**Protection on the level of IM gateways**
Attacks on IM networks - viruses and worms spreading through IM networks - the degree of threats – from harmless to very dangerous	- stopping e-mail attachments - AV inspection of e-mail attachments - regular scanning of computers against unwanted applications	- prevention of passing of instant messages - stopping of IM files - making the list of known *spimers*
Attacks to the IM client vulnerable spots - viruses and worms which use vulnerable spots of IM clients - not necessarily spread through IM		- stopping client variants which are known to be vulnerable - stopping of IM files - AV check of IM files

V. RESEARCH OF THE CURRENT SECURITY CONDITION

It is not unusual that the e-mail traffic in organizations is mostly covered by security measures – according to some research [1] from 62% to 73% organizations and 81% of private users [9], but the big problem is the lack of security measures for instant messages. As many as 50% of the respondents in the same research [1] stated that the thought about the security protection of instant messages never occurred to them, and only 11% of the respondents said they have in-built system for checking of instant messages

in their organisation. This difference is explained by the expectation that the organisation that cares about the safety of e-mail will also take care about instant messages. Still, the tools that protect the e-mail are often inadequate for protection from the threats that come through instant message clients. It is also one of the causes of the increasing number of viruses which are typically spreading through the system of instant messages.

Skype – the most popular (because it's free) product for VoIP telephony in the world uses on purpose port 80 for communication. Port 80 is primarily used for web traffic. Therefore, it is very hard to close down, although such software solutions already exist. Many organizations, from universities to international corporations and national governments (for example, France), prohibit the use of *Skype* or recommend the clients not to use it (although it already has over 61 million of registered users). This is reinforced by the recommendation of the *Info-Tech Research Group* [10], which recommends the same for the system of instant messages. What makes *Skype* a potential risk? The same things which make it so popular: even an unskilled person can download it from Internet and install it, without the control of the administrator, it is extremely easy to adjust, firewalls are not a barrier for its communication, and it leaves almost no traces of its presence, except significant increase in traffic. The software works terrifically, but the hole made by the phone talks can be used for the theft of data or for virus installation.

The research made for the members of *Info-Tech Research Group* [10] resulted in five conclusions, i.e. reasons for prohibition of the use of the most popular software for VoIP telephony in the business environment:

- *Skype* is not in accordance with the standards, because it allows the communication through the organizational firewalls, making and revealing the vulnerabilities of the organization.

- Encryption used in *Skype* is not open coded, therefore it is open for the attacks by those who designed the system of encryption or those who have knowledge of it, and who were compromised later. Besides, it is not clear how to manage the keys.

- The organizations which use *Skype* risk the communication barrier with the states, organizations and institutions which prohibited *Skype*.

- *Skype* is impossible or very hard to detect, track or assess, which creates risk for the organizations which are obliged to do these things.

- There is an open question whether the VoIP telephone talks have to be recorded according to the legal regulations.

Even a mediocre hacker has a potential to use vulnerability of *Skype*.

VI. EXAMPLES OF NEW THREATS

The worms can spread very fast through instant message networks [11]. They introduce themselves falsely as messages from *buddies* with a hyperlink that looks innocent, but is in fact the link toward a malign code placed somewhere on the Internet. When a user activates hyperlink, a malicious code is installed and started in his computer. The worm spreads, sending messages to every address from the address book of the user of the infected computer. The example [11] is the worm which, in the pre-Christmas days, easily passed through instant message networks, presenting itself as the file whose content is related to Santa Claus. Opening the file, the users saw the figure of Santa Claus, but an undetected *rootkit* installed onto their computer, which took over the control over the computer, and is invisible for the security system. Very similar threats occurred in the form of Christmas greeting card.

Through instant message networks, *phishing* attacks are also appearing, like the attack [12] on *Yahoo! Messenger*, when some of the users were deceived with fake message, which told them they were breaking the terms of the use of that service, and directed them to the fake web site, similar to the official web site for the applications. During the application, the other side really stole the basic user data: user name and password.

Instant message networks like *AOL Instant Messenger* [13] are also confronted with the worms which talk to potential victims, convincing them that the attachment does not contain a virus. If the user asks whether the attachment is a virus, the worm answers negatively. After the activation, the malicious code disables the security systems, changes the system files and opens the front door of the computer. In the second phase, it sends its copies to new users whose identifying data it finds on the victim's computer. The outgoing messages are invisible to the user.

In the December of 2005, *Symantec* and F-*Secure* published [14] that some ftp and web servers were infected and that they were spreading the infection to the user computer which were accessing them. In the same month *PandaLabs* warned about many e-mails whose attachments were infected by trojans. *Akonix Systems Inc*. warned about the trojan which was spreading through the direct hyperlink contained in instant messages (most often from the domain *hometown.aol.com*). Trojan [14] has the task to monitor user activities on financial web sites because of the theft of the user names and passwords, which it sends afterward through an e-mail without the knowledge of the user. The trojan *Banbra-BOK* is hard to detect, since it does not announce its presence in the infected computer through message or warning.

In December of 2005, the worm *Dasher* was spreading through the use of the security omission in the Windows which the Microsoft patched two months earlier (*Microsoft Windows Distributed Transaction Coordinator*) *Memory Corruption vulnerability*); the family of the worms and trojans called *Bagle*, reinforced its activity; the trojan *Banbra* was spreading through the software support for the instant messages [14]. These are just some examples of such disturbing phenomena.

The experienced hackers use the methods of social engineering with ease [15], by presenting themselves in instant messages as someone else, someone whom the victim trusts. The message can contain only a small malign part, or a link toward a malign file.

According to [16], it is only a question of time before whole networks collapse because of the instant messages or P2P applications. Some worms which spread through instant messages [17], copy themselves into shared maps of popular P2P applications, as to ensure their spreading. Furthermore, [18], there are examples of checking the language settings of the computer; they are able to send the

messages on some of the (presently ten) most widely spread languages.

In this moment, in USA, [9], over 52% of the phone business communication is being conducted through VoIP telephony. The major service providers are: *Vonage*, *CallVantage* (AT&T), *Lingo*, *Packet8* (8X8), *VoiceWing* (Verizon) and *Skype*. At the same time, 3 million of home users use VoIP, and their number doubles every year.

VII. SECURITY POLICY

John Penrod [15]: "The existing messages are not the safe method of communication and should not be used for transfer of the files or sensitive information." Instant messages have become valuable tool that managing structures use for sending routine messages and to link with the remote colleagues in real time. As was the case with almost every new method of communication through the computer, this method also created the whole set of problems and security challenges. Many of them can be significantly reduced if their users follow the instructions of the security policy of the organization in which they work.

The security policy related to instant messages already has the best practice, which is visible in the following points [15]:

1. The hazards which stem from the use of the instant messages cannot be ignored. Namely, their use is constantly increasing. It is necessary for organizations to recognize not only the uses, but also the hazards and dangers of their use. Instant messages can be valuable tools if used in the proper manner.

2. The key of success or failure is the education of users. The employers which allow the use of instant messages have to educate the employees constantly about what content can be sent through the system of instant messages, and what content cannot.

3. The security policy that relates to instant messages has to be publicly announced. It should prevent the damage that occurred because of the potential abuse of instant messages.

4. It is simple to check whether some content can be sent through instant messages: anything that would make any problems if published in newspapers headlines or which would be embarrassing in a court of law should not be sent through instant messages.

5. The control of an instant message system has to include definition and control of the possibilities of the instant messages system that the users can use, monitoring of the messages in search for sensitive information, and the archiving of instant messages. Such policy should be stated clearly to everyone who uses an instant message system.

6. The updated security systems are necessary. Instant messages can expose the holes in the network security to the potential attacker.

Here are recommendations for the integration of the security policy of organizations:

- Attachments should never be opened or web sites visited through the hyperlinks sent by the unknown sender.

- The constant user updates of the patches for the operational and software systems are necessary.

- Every computer has to have installed applications against viruses, espionage software, and unwanted e-mails; also, it has to have personal firewall and the application for protection of the privacy, as well as the automated update of these.

- Playing on-line games with unknown players is careless and dangerous.

- The computer protection should be checked often through *eicar* file.

VIII. CONCLUSION

Instant messages are the fastest adopted means of communication in the history and a strong supporting factor of the organizational procedures. However, every new opportunity of the communication through information-communication technology sooner or later leads to the abuse, i.e. to new security threats, and the security measures are not being adopted in the same pace. The failure to adopt these measures increases the risk to the information assets of the organizations.

The solution lies in the multi-layer security. Namely, although network security is the theme of many conversations, and firewalls, antivirus systems and anti-spyware software are standard in function of the protection of gateways and workstations, this is not enough. Despite all levels of protection, the frequency of compromising of the servers, workstations and the end network points – terminals, leads to the conclusion that the implementation of the multilevel security is a necessary procedure for the insurance of the all-encompassing security network.

To ensure the security of the data in VoIP telephony, it is necessary to have the possibility for blocking and encryption of VoIP messages in the real time, while they travel the network, and to define and strictly implement the organization of the security policy.

REFERENCES

[1] IT Observer Staff, *Instant Messaging Security Still Lags Behind Email*, http://www.ebcvg.com/articles.php?id=1039, January, 2006

[2] J. M. Germain, NewsFactor Business: *The Worst-Case Hack Scenario*, http://business.newsfactor.com/story.xhtml?story_id=41047, January, 2006

[3] B. Grow, BussinesWeek online: *Coming to Your PC's Back Door: Trojans*, http://www.businessweek.com/technology/content/jan2006/tc20060123_003410.htm, January, 2006

[4] A. Gonsalves, *IM Worms Mutating At An Alarming Rate*, TechWeb News, http://www.techweb.com/wire/173603062, November, 2005

[5] Messaging Pipeline Staff, *IM worms up again in November*, http://www.securitypipeline.com/174403031, November, 2005

[6] J. P. Mello Jr., TechNewsWorld: *Security Firm Reports Malware Threats Jump 48 Percent*,

http://www.technewsworld.com/story/47694.html#, June, 2005

[7] TelecomWeb, *Warning: Beware Of The VoIP Zombies*, http://www.telecomweb.com/news/1138308006.htm, January, 2006

[8] National Institute of Standards and Technology (NIST), *Security Considerations for Voice Over IP Systems*, http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf, January, 2005

[9] O. Kharif, BussinesWeek online: *VoIP Providers: Heeding the Call?*, http://www.businessweek.com/technology/content/nov2005/tc20051128_964764.htm, January, 2006

[10] R. Armstrong, Info-Tech Research Group: *Ban corporate Skype usage immediately, says Info-Tech Research Group*, http://www.infotech.com/Press%20Releases/Skype%20Security.aspx, November, 2005

[11] D. Kawamoto, News.Com: *Santa IM worm hits AOL, MSN and Yahoo*, http://news.com.com/2102-7349_3-6002790.html?tag=st.util.print, December, 2005

[12] E. Oswald, BetaNews: *New Yahoo IM Phishing Attack Surfaces*, http://www.betanews.com/article/print/New_Yahoo_IM_Phishing_Attack_Surfaces/1134409339, December, 2005

[13] M. Santo, RealTechNews: *Instant Messaging Worm Talks You Into Infecting Yourself*, http://www.realtechnews.com/posts/2284, December, 2005

[14] B. Brenner, *Trio of trouble: Malcode targets Windows, IM users* http://searchwin2000.techtarget.com/originalContent/0,289142,sid1_gci1152680,00.html, December, 2005

[15] L. Hall, *Danger: Don't wile away your career on IM*, http://atlanta.bizjournals.com/atlanta/stories/2005/11/21/smallb3.html, November, 2005

[16] W. Eazel, *Hackers up pressure on P2P networks*, http://www.scmagazine.com/uk/news/article/525411/hackers-pressure-p2p-networks/, November, 2005

[17] E. Larkin, *Online safety threats lurk in instant messages*, October, 2005

[18] J. Leyden, *Polyglot IM worm targets MSN*, http://www.theregister.co.uk/2005/08/25/kelvir_im_worm/, July, 2005

[19] M. Miller, *Absolute PC Security and Privacy*, Sybex, London, 2002

[20] Akonix Systems, Inc., *Solutions for Enterprise IM: Defense in Depth*, http://www.akonix.com/solutions/defense_in_depth.asp, January, 2006

[21] McClure, S., J. Scambray, G. Kurtz, *Hacking Exposed: Network Security Secrets and Solutions*, McGraw-Hill, 1999

[22] W. Dworakowski, WindowSecurity.com: *Why is a firewall alone not enough? What are IDSes and why are they worth having?*, http://www.windowsecurity.com/pages/article_p.asp?id=466, August, 2002

[23] L. Greenemeier, InformationWeek: *Put Up A Strong Defense - Emerging security technologies monitor and encrypt data to defend against internal threats as well as outside ones*, http://www.informationweek.com/story/showArticle.jhtml?articleID=177102288, January, 2006

[24] M. Navrathna, *A heavy price of vulnerability*, http://www.deccanherald.com/deccanherald/jan252006/cyberspace1356422006124.asp, January, 2006

[25] R. Lemos, CNET News.com: *Skype plugs hole in VoIP software*, http://techrepublic.com.com/5100-22_11-5454452.html, November, 2005

[26] Network World, *Executive guide: The REAL World of VoIP*, http://ad.doubleclick.net/click%3Bh=v5|337a|3|0|%2ale%3B23268784%3B0-0%3B1%3B11302073%3B2-120|90%3B13219796|13237692|1%3B%3B%7Esscs%3D%3fhttp://www.networkworldpartners.com/register.do?pdfid=79&tdcode=D4, January, 2006

[27] Sicker D. C., T. Lookabaugh, *VoIP Security: Not an Afterthought*, http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=209, September, 2004

[28] O. Poole, *Network Security, A practical guide*, Butterworth-Heinemann, Oxford, 2003