

I KNOW WHAT YOU DID LAST LOGON – MONITORING SOFTWARE, SPYWARE AND PRIVACY

Jeff Williams
Microsoft, USA

Email jwill@microsoft.com

ABSTRACT

To some, the thought of keystroke logging and other forms of monitoring bring to mind the Orwellian surveillance society – a view that is reinforced by recent news as well as the increasing presence of monitoring software in spyware and the frequency with which such software is found accompanying botnets. The act of capturing keystrokes on a computer as well as other forms of monitoring can manifest in a range of ways from completely benign to overtly criminal. In cases where the logged party is unaware of the activity there is also the possibility of financial impact through various types of fraud as well as personal endangerment when the monitoring is a component of stalking or domestic violence. However, monitoring also has legitimate commercial uses such as consensual workplace monitoring, parental controls and computer troubleshooting.

We will explore the technical methods employed by both hardware and software-based key loggers, how keystroke loggers are integrated with specific malware threats, the user experience associated with various key loggers installed, and examine the social and legal appropriateness of various use scenarios.

DEFINITIONS

Before entering into a detailed discussion of monitoring software and privacy it seems prudent to provide definitions for several of the terms that will be used within this paper. As, historically, there has not been a general consensus definition for these terms, the author has chosen to use those definitions published by the Anti-Spyware Coalition as these represent the consensus of its membership and, as a result, obviates the need to redefine these terms solely for the purpose of this paper [1].

Spyware

Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use and distribution of their personal or other sensitive information.

Tracking software

Software that monitors user behaviour, or gathers information about the user, sometimes including personally identifiable or other sensitive information, through an executable program.

Keystroke logger

Tracking software that records keyboard and/or mouse activity. Keyloggers typically either store the recorded keystrokes for later retrieval or they transmit them to the remote process or person employing the keylogger. While there are some legitimate uses of keyloggers, they are often used maliciously by attackers to track behaviour surreptitiously and perform unwanted or unauthorized actions including but not limited to identity theft.

Botnet

A type of remote control software, specifically a collection of software robots, or 'bots', which run autonomously. A botnet's originator can control the group remotely. The botnet is usually a collection of zombie machines running programs under a common command and control infrastructure on public or private networks. Botnets have been used for sending spam remotely, installing more spyware without consent, and for other illicit purposes.

A BRIEF DISCUSSION OF PRIVACY

Privacy has been described in many ways by many people. For the purpose of this discussion we will use the following amalgamation of viewpoints borrowed from industry:

The right of individuals to determine if, when, how, and to what extent data about themselves will be collected, used and shared with others.

The fundamental principles within that description that apply to the topic of monitoring software are notice and consent. For monitoring to be appropriate it must be conducted with clear and complete notice provided to the individual prior to the monitoring and informed consent must have been obtained from the person being monitored. Any monitoring done outside of that can be considered inappropriate at best, though many would use considerably stronger and, often, pejorative terminology to describe it.

Other privacy considerations must be taken into account with regard to the data collected during the use of any monitoring software. Is that data stored securely and protected from view or usage outside of what was disclosed when the original notice and consent occurred? Are the people who have access to that data limited only to those with a specific need (a need that is, again, consistent with the notice and consent provided by the individual)? Is the data protected from tampering so as to prevent the attribution of words and deeds to the individual where those words and deeds were not that person's doing? Is the use of the data under the provisions discussed above enforced in some meaningful way with consequences associated with any misuse?

While a full discussion of applicable privacy law is outside of the scope of this document it should be mentioned that there are likely to be numerous legal considerations relating to the use of monitoring software. Such software can capture personal data, sensitive data relating to financial, medical or other protected classes of information such as information relating to children. Further, in some instances an individual may have an expectation of privacy which is also protected. Those seeking to use monitoring software for legitimate purposes may do well to consult with an attorney before conducting the monitoring, and those who choose to monitor maliciously could be violating one or more laws in one or more jurisdictions.

No discussion of privacy law, however brief, would be complete without pointing out that the law is continually changing in response to new trends, new understanding and new social considerations. While there has been considerable press coverage of topics relating to privacy and the law in recent years, this is hardly a new phenomenon. In 1890, Samuel Warren and Louis D. Brandeis wrote in the *Harvard Law Review* [2]:

‘That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been necessary from time to time to define anew the exact nature and extent of such protection.’

This is as true today as it was then – new uses of information (and, in the present day, new uses of information technology) necessarily require that previous conceptions of appropriate and inappropriate use be revisited in some meaningful way. As a result, we should expect that further laws will be introduced, amended or retired as our understanding of this important topic changes over time.

DISCUSSION OF MONITORING SCENARIOS

There are many reasons for monitoring computer activity, some of which are legitimate (or quasi-legitimate, depending on one’s viewpoint). Perhaps the most talked-about reason recently has been the support of law enforcement investigations. While there are decidedly strong opinions relating to this usage both from those with deeply ingrained privacy beliefs as well as from the law enforcement community, the end result of obtaining the evidence necessary to convict a criminal is often positioned as an essential investigation and prosecution tool. In the case of *United States v. Nicodemo Scarfo, Jr.*, keystroke logging was a critical component of the conviction of the defendant [3].

According to court documents, Nicodemo Scarfo, Jr. was engaged in illegal gambling and loan sharking. During the FBI investigation, agents came across a personal computer but were unable to decipher contents of specific files of interest due to the use of encryption. Because the FBI suspected that a file contained evidence supporting their case, the agents received two search warrants – the first to break into the location containing the PC in order to install a hardware-based keystroke-logging system inside the keyboard of the computer and the second to extend the warrant to allow time to collect the data captured by the keystroke logging system and thereby determine the pass phrase of Mr Scarfo as well as the contents of the encrypted file.

By utilizing the hardware-based key logger, the FBI was able to advance its case against Mr Scarfo and obtain key information which was necessary for prosecution. Privacy concerns relating to the Fourth Amendment of the Constitution of the United States were brought up in the case, but because the use of the keylogger took place under properly executed search warrants which constrained the search to only the relevant data, the court found that privacy concerns were not a reason to overturn the evidence. From this we can see that the use of evidence collected by a keylogger can be seen as a useful tool for law enforcement when done within the parameters defined by established law.

Monitoring of employees in a corporate environment is also a regular practice in many industries. This monitoring is often done with consent through the various employment

agreements and policy documents an employee signs as a part of their on-boarding with the company.

Corporate monitoring of employees comes in a number of forms relating to very distinct purposes. In some cases, a help desk will operate most efficiently by having the ability to view or, in some cases, take control of, an employee’s workstation in order to diagnose and troubleshoot system or application problems from a remote location. The efficiency afforded to the technician through this monitoring – especially when working with a novice user – can represent significant cost savings to the company by allowing the support transaction to complete more quickly and often more completely than support conducted either by telephone or requiring a site visit. To ensure that the needs relating to consent and disclosure are met, most, if not all, commercial remote control software provides visible cues that monitoring is taking place as well as some form of consent mechanism to collect consent from the individual before they are monitored.

Another use of monitoring employed by some corporations has to do with helping to ensure policy compliance.

Compliance with regulation and with corporate policy is of critical importance to some businesses and industries. This monitoring often takes place at the server or gateway in the form of keyword searching of documents and email. Monitoring of employee activity can also occur as a component of an internal investigation within the company where the monitoring can be used to show evidence of, or even to refute claims of improper conduct.

Perhaps the most common and best understood type of monitoring is the use of software by a parent to monitor or even restrict the online activities of their children. The goal of such software is to help ensure that the child’s use of the Internet does not stray into areas of risk or areas outside of the family’s view of appropriate use. The data collected by a parental control solution can also serve as a tool for meaningful discussion around that which can be found online and the people with whom the child is interacting. But, for every positive reason for monitoring there are one or more questionable rationales including financial fraud, eavesdropping, stalking and domestic violence.

Brown v. Brown

An interesting case illustrating some of the more questionable uses of monitoring is *Steven Brown v. Patricia Brown* [4]. In September 2001, Steven Brown was charged with installing monitoring software on the computer of his estranged wife Patricia Brown. The software was a commercially available offering which Mr Brown purchased and installed on Ms Brown’s computer at her separate residence without her knowledge. The software collected personal information and tracked computer activity (e.g. the websites visited, emails sent and received) and sent the full details to Mr Brown by email at regular intervals.

Mr Brown was charged with using a computer to commit a crime, eavesdropping, installing an eavesdropping device and unauthorized access. He pled guilty to eavesdropping and using a computer to commit a crime. He received two years’ probation.

Two important elements of this case are the lack of consent from the person being monitored and the lack of visibility of the software running which was collecting personal

information. Ms Brown suspected she was being monitored after Mr Brown taunted her with information he could only have obtained through monitoring of some kind. As a result, Ms Brown did research on many monitoring products and found information on software that was likely installed on her computer (which, in the end, did indeed turn out to be the package used). Ms Brown contacted the manufacturer asking how the software could be detected and removed. She was informed that it was not possible to tell the software was running – since it runs hidden and is designed to look like a legitimate system file even to an experienced technician. She was then informed that it could only be removed by the person who installed it due to the protections included in the software against tampering. The software provider, as one might expect, was unwilling to provide information as to whether or not Mr Brown had purchased a copy of the software, causing Ms Brown to pursue the matter with the state's Attorney General.

Suffolk County v. Michael Valentine

More recently there are cases which demonstrate that the courts are gaining a deeper understanding of this problem space. This is well illustrated by the case of *Suffolk County v. Michael Valentine* [5]. In this case, in what might be referred to as a classic example of 'Type II Cybercrime' [6], a police officer in Suffolk County, New York had met a woman through an online dating service. The couple dated for approximately six weeks, after which the woman broke off relations.

Following the breakup Mr Valentine is alleged to have broken into the woman's email account by guessing that her password was the name of her favourite pet. He is said to have sent email from that account to his own email address (posing as her), stating that her friends would 'come out of the bushes with a baseball bat and beat [his] brains in'. According to the press, Mr Valentine also posed as her in chat rooms and in other emails making statements reflecting on her in ways that did not match her character.

Mr Valentine was charged with 197 counts of stalking, computer trespass, official misconduct and tampering with evidence. Mr Valentine pled not guilty and the results of the trial are pending at the time of this writing. If these allegations are true it would represent a different form of monitoring than the case previously discussed, in that it does not involve the use of any software, but instead is primarily the result of a compromise of weak credentials on a web service accessible to all.

Setting aside the charges relating to Mr Valentine's employment in law enforcement which aggravate the situation, this would essentially be a case of run-of-the-mill (and not particularly impressive) hacking. In such a case, even existing anti-malware software – software which may be designed to target monitoring software – cannot protect the individual.

US v. Carlos Enrique Perez-Melara

In a third case, commonly referred to in the press as 'Lover Spy' [7], we extend the traditional method of software-based keylogging to include an element of social engineering. The software was marketed for \$89 to individuals wishing to spy on someone else's online activities. The people behind Lover Spy describe what happens next as:

'Through our service, you compose and send your lover a normal-looking "Greeting Card" saying "I Love you" or a similar message. Because the email appears to be a regular greeting card, the recipient will open the ecard and LoverSpy will be automatically and silently installed!

'The program begins monitoring them IMMEDIATELY, there is no delay. It records and sends you all emails they view, including *Hotmail*, *Yahoo*, and *Outlook* emails.' [8]

More than 1,000 copies of this software were sold between 2003 and 2005 and the operator of Lover Spy was charged with 35 counts of 'manufacturing, sending and advertising a surreptitious interception device' and 'unauthorized access to a computing device'. The charges totalled 175 years in prison. Four others who purchased the software were also charged with multiple counts of hacking. The hacking charges each carried consequences of up to five years in prison and up to a \$250,000 fine. Looking at the charges filed we can see again that a key element differentiating appropriate from inappropriate use of monitoring software revolves around the consent of the individual being monitored.

METHODS OF MONITORING

As we've seen, there are many approaches to monitoring an individual's computer activities. These techniques include the use of commercial software as well as more rudimentary spying techniques such as password-guessing. There are also hardware-based attacks such as the use of a small camera overlooking a keyboard or ATM PIN entry keypad [9] as well as hardware devices designed either to be installed in series with the keyboard or soldered inside the keyboard itself (such as the one used by the FBI in the Scarfo case). These hardware solutions boast capacities of as many as 2 million keystrokes (more than 600 typewritten pages).

Hardware-based keystroke logging is nearly impossible to detect through the use of software, as even advanced techniques, such as monitoring for voltage variances in the hardware path, require foreknowledge of what keyboard is being used and what is 'normal' for that keyboard in all use scenarios. In addition to the methods described previously there are also a growing number of instances of malicious software which include monitoring components.

MONITORING AS A COMPONENT OF MALICIOUS SOFTWARE

Case study – TrojanSpy:Win32/Banker

One example of malware which contains a monitoring component is seen in the variant *TrojanSpy:Win32/Banker* trojan reviewed for this discussion [10].

This software attempts to collect online banking credentials. At present there are literally thousands of variants of this threat [11]. To better illustrate the techniques used by this family, a detailed analysis of one variant was conducted by *Microsoft* anti-spyware analysts for this paper. This and similar variants are targeted specifically at online financial institutions. The variant analysed consists of two components – a randomly named executable which loads *APWIZ.DLL* then exits, and the *DLL* itself, which is a Browser Helper Object which intercepts URLs entered in the *Internet Explorer* process watching for specific key-phrases such as:

- Banco ITA – Feito Para Voc
- Caixa Economica Federal
- Real Internet Bank
- Real Internet Empresas
- Banco Bradesco
- Bradesco S/A
- Bradesco Internet Banking

Once it identifies one of these keywords, it starts to capture keystrokes – presumably those relating to logon at one of those banks. The threat stores information about itself in HKEY_LOCAL_MACHINE\Software\Windows including a timestamp derived from visiting a specific website in the UK, and a unique identifier representing the specific installation of the malware. When it captures information, the details are logged to c:\windows\system32\form.txt (see Figure 1).

Details logged include the date and time the site was visited, full URL of the site and user IDs, passwords and credit card numbers entered in clear text using a number of API calls, most of which are common to Internet access across all versions of *Microsoft Windows*, but several of which are specific to *Microsoft Windows XP* and newer systems. This information is captured in the browser window during form entry and so is captured whether or not the user submits the data through the form. The information is then sent to several email addresses where the attacker can collect the files for further (mis)use.

```

----- Wed Apr 19 18:41:20 2006
URL: https://bank11ne.itaun.com.br/Lqnet/Itaunbank11nePF.htm
----- Wed Apr 19 18:47:47 2006
URL: http://internetcaixa.caixa.gov.br/nasapp/s11bc/
----- Wed Apr 19 18:47:52 2006
URL: https://internetcaixa.caixa.gov.br/NASApp/SIIBC/index_verif.processa
Grabbed from form...
GXHC_GX_jst: 5a6f681b66116166GXHC_3SESSIONID: eef17f131f1e0542
GXHC_3SESSIONID: eef17f131f1e0542
REQ:
GXHC_GX_jst=5a6f681b66116166GXHC_3SESSIONID=eef17f131f1e0542&x=
URL: https://internetcaixa.caixa.gov.br/NASApp/SIIBC/index_verif.processa
Action: principal.processa
Method: post
token(hidden): a37b2941e864715e4d109b9ca2671c
serv(hidden):
Navegue(select): [checked]
Action: login.processa
Method: post
token(hidden): a37b2941e864715e4d109b9ca2671c
Combo(select): 001 [checked]
Campo1(text): 123
Campo2(text): 153
----- Wed Apr 19 18:51:09 2006
URL: https://internetcaixa.caixa.gov.br/NASApp/SIIBC/index_verif.processa#ancora
Action: principal.processa
Method: post
token(hidden): a37b2941e864715e4d109b9ca2671c
serv(hidden):
Navegue(select): [checked]
Action: login.processa
Method: post
token(hidden): a37b2941e864715e4d109b9ca2671c
Combo(select): 001 [checked]
Campo1(text): 0223
Campo2(text): 000000153
----- Wed Apr 19 18:51:15 2006
URL: https://internetcaixa.caixa.gov.br/NASApp/SIIBC/index_verif.processa#ancora

```

Figure 1. Sample of form.txt file.

Some variants of the TrojanSpy:Win32/Banker family also attempt to disable *Microsoft Windows AntiSpyware* (beta 1). The technique used by these variants to disable beta 1 has no effect on *Windows Defender*, *Windows Live OneCare* or *Microsoft's* enterprise anti-malware offering and, as such, this approach is not present in a number of current variants of this family of malware. The large number of variants of this trojan, coupled with statistics relating to each variant's prevalence in the wild, suggests that the author(s) of this family are using a small number of each variant in the hopes of avoiding detection by anti-malware software.

Case study – commercial software

The simplistic approach used by the TrojanSpy:Win32/Banker trojan stands in stark contrast to the richer set of monitoring features in the most prevalent commercial offerings of monitoring software. This difference speaks to the targeted use of malware versus the myriad of uses one might suppose for a commercial package that is aimed at a broad audience.

One such commercial offering, for purposes of comparison, allows its user to install it in stealth or non-stealth mode – depending on the intent of the user. When installed, the software can capture email conversations (both inbound and outbound), chat and IM sessions, websites visited, the programs which have been run, peer-to-peer downloads through programs such as *KaZaA*, as well as keystrokes. Some versions have even added the capability of taking screenshots at various resolutions and colour depths and at predetermined intervals to capture information beyond those data described.

Again, as contrast between malicious and commercial monitoring software, we can refer back to our earlier discussion of privacy and the importance of consent and visibility. In the case of commercial software, one will often find disclaimers either in the packaging or during setup clarifying appropriate use considerations such as only running the software on one's own computer and that any user of that computer should be informed of its presence. This places the burden of appropriate use on the user and not the software provider which, in many cases, will also provide a mode in which the software can run in a stealth configuration where its processes are masked in various ways as was true in the *Brown v. Brown* case discussed earlier.

An unfortunate side effect of allowing the person installing the software to make decisions about disclosure of its presence is that it allows for a number of potential misuse scenarios such as spying on a family member, housemate or co-worker. Such misuse can contribute to or facilitate instances of domestic violence. Consider the following scenario:

1. Abuser installs a commercial monitoring package in stealth mode on the computer of their spouse due to feelings of mistrust.
2. The mistrust contributes to further difficulties in the relationship driving the couple further apart. The abusive spouse attempts to exert more and more dominance in the relationship trying to control the actions of the victim.
3. The victim becomes afraid of the increased control and abuse and makes a decision to leave the relationship.
4. The victim sets up a new bank account and credit card and starts moving money into this account to facilitate departure.
5. The victim seeks help using the monitored PC first looking for support from family or friends via email and later seeking a shelter or making travel arrangements to get away from the abuse.
6. The abuser reviews all of the captured information which includes every website visited for research, online banking information including credentials for the private accounts, details of any tickets purchased or

maps/directions to local shelters and correspondence with family and friends describing any plans or concerns.

It does not take a great deal of imagination to predict any number of negative outcomes to such a scenario. This is particularly true when one considers that someone is three times more likely during a separation and 25 times more likely during a divorce to be victims of violence at the hands of an intimate partner than a married person would be [12].

Such scenarios have caused providers of parental controls (another form of monitoring software) to consider whether or not it is appropriate for that software to have stealth capability at all.

Case study – Win32/Gaobot

The Win32/Gaobot variant we analysed for this discussion is a worm which propagates using a scan/exploit architecture [13]. Specifically, once the bot has infected a system it begins to scan the local subnet to find neighbouring hosts to infect. When it finds a host IP present it uses exploits relating to several different vulnerabilities in *Microsoft* software for which patches are available. The vulnerabilities targeted are:

- MS03-026 (an issue with RPC/DCOM most commonly associated with Win32/MSBlast)
- MS04-011 (a vulnerability in the LSA Service which was targeted by the Win32/Sasser worm)
- MS01-059 (a vulnerability in UPnP targeted by a number of variants of Win32/Rbot, Gaobot, and Win32/Spybot)
- MS02-039 (a vulnerability in *SQL Server* and MSDE – most commonly associated with the Win32/SQLSlammer worm)
- MS03-007 (a vulnerability in ntdll.dll targeted by the Win32/Nachi and Win32/Welchia worms as well as various bots)

Exploit code for each of these has been published on the Internet for some time in a wide variety of forums and, as can be noted by the year in which each of the patches was released, so has protection from each of these vulnerabilities.

Not content to attack these vulnerabilities alone, the bot's author also targets known vulnerabilities in *Dameware Mini-Remote* (a piece of commercial software that is also seen distributed with various malware packages) as well as backdoors left by other, previous worms and trojans including: Win32/MyDoom, Win32/Bagle, Win32/Netdevil, Win32/Optix, Win32/Subseven, and Win32/Kuang. The malware also attempts to disseminate itself through network shares using both the credentials of the logged-on user as well as a brute force attack using a short list of approximately 40 words which are used in combination for username and password. During the analysis for this report, systems in the US, Brazil, Spain, Argentina, Australia, and Korea were seen to join the control channel of this bot.

An infected system is capable of updating itself via FTP by connecting to a specific site and downloading a file called BLING.EXE. The name of the file suggests to the author of this report that this Gaobot variant is distributed with a personal profit motive for the attacker. The update capability is not limited to simply updating the bot itself, it can also be used to install additional malware or utilities depending on the needs of the botnet's controller.

In addition to the self-update component, the malware also sniffs network traffic searching for specific text indicating a logon session for Unix/*Linux* command shells, logon scripts, HTTP, FTP, IRC, IM, other bots, P2P applications and *PayPal* in order to capture the credentials associated with those sessions. The code used for this is similar to the publicly available code for the Carnivore library.

The bot scans the system for the presence of various specific pieces of software – mostly games – and pulls the key from the registry for each of them. The software in question includes more than three dozen titles including *Neverwinter Nights*, *Command & Conquer (Red Alert, Red Alert 2, Tiberian Sun and Generals)*, various *Electronic Arts* titles, *Unreal Tournament*, *Battlefield 1942*, *Battlefield Vietnam*, *Medal of Honor*, *Need for Speed*, *Counter-Strike*, *NOX*, *Chrome*, *Half Life* as well as the product activation codes for *Microsoft* software. The activation details for these software titles are almost assuredly to be used as currency in the warez underground.

The keys are sent as an IRC PRIVMSG to the bot's control channel. The channel logon credentials are encrypted in the source code of the bot. One particularly interesting behaviour of this bot is that it has a list of IRC connect strings which it uses when it connects to an IRC channel to make the channel appear more legitimate. This is, presumably, to counter the increased prevalence of researchers who look for bot-related channels in order to take down those hosts as a prophylactic measure.

Finally, the bot attempts to steal administrator logon credentials on *Microsoft Windows 2000* and *Microsoft Windows NT* through MSGINA.DLL and does keylogging within the foreground window through user32.dll.

Microsoft's Malicious Software Removal Tool (MSRT) has removed Gaobot variants from more than 260,000 unique computers between January 2005 and March 2006 with a total of more than 794,000 removals. The Win32/Gaobot family of malware is the fourth most prevalent family removed by the *MSRT* [14].

Case study – Win32/Rbot

So far we have seen an array of monitoring methodologies ranging from commercial software with disclosure, to commercial software with stealth capability, and both malware that is targeted in its approach as well as malware whose broad approach is more opportunistic – taking whatever credentials or information it can find (presumably for sale or trade). The final case study in this report is a piece of malware called Win32/Rbot [15]. This particular threat displays the behaviours discussed in all of the previous examples as well as some additional advanced techniques worthy of discussion.

This variant of Win32/Rbot is an advanced bot which, in addition to capturing information from the infected host, is also designed to slow or prevent analysis in a debugger, to degrade the security of the infected host and to provide additional functionality to the controller.

The threat propagates in a manner similar to Win32/Gaobot using a scan/exploit methodology. A key difference with this threat is that the vulnerabilities targeted are less well known than those used in Win32/Gaobot. This provides the attacker with a larger pool of potential target systems since some

companies and individuals choose to apply only those patches relating to specific threats which they hear about in the mass media, rather than staying completely up to date as is recommended by *Microsoft* and others in the software and security businesses.

The specific vulnerabilities targeted by this Win32/Rbot variant are:

- MS01-059 (Internet Connection Sharing on *Microsoft Windows 98, 98SE, ME* and *XP* systems)
- MS03-049 (Workstation Service)
- MS03-0043 (Messenger Service)
- MS02-061 (*SQL Server* and MSDE)

It is worth noting that the functions targeted by each of these threats are present on most or all versions of *Microsoft Windows* in common usage. The bot also scans a much broader address space covering the full address space of the Internet and not simply the local subnet. Like our Win32/Gaobot variant, this particular Win32/Rbot attempts to spread via available network shares but it also searches for mapped drives (C:-Z:) and both the ADMIN\$ and IPC\$ administrative shares.

To prevent detection, the malware drops itself in the *Microsoft Windows* directory with a filename that is visually similar to the legitimate *Microsoft Windows* file SVCHOST.EXE. Once loaded into memory, the original file dropped during infection is deleted from the file system and a kernel mode driver, RDRIV.SYS, is installed. This driver is a rootkit known as the Virtool:WinNT/FURootkit [16], it masks the presence of the running process from Task Manager and other system tools. The bot then makes a number of changes to the registry which prevents access to Automatic Updates, Windows Update and Microsoft Update, prevents the installation of *Microsoft Windows XP SP2* on an *XP* system where SP2 is not already present, blocks the Windows Security Center from loading and disables various services thereby preventing administrative updates of the system using Group Policy. It also blocks remote administration and remote editing of the registry and disables various anti-virus products and firewalls which may be running on the system.

The bot's author has also predicted that others (anti-malware researchers, competing criminals) will try to disassemble the bot and so has included logic to detect and prevent this. The malware attempts to detect whether it is being run within *VMware* and, if it is, the software terminates. The bot itself is also packed with *ASProtect* in an effort to raise the bar for anyone attempting to determine its contents. Further, when the software is loaded into a common debugger, it displays the following dialog box, taunting the analyst (Figure 2).



Figure 2: Anti-debugging dialog box.

This variant of Win32/Rbot also captures a good deal of information about the computer and its user. For starters, the bot collects information about the system configuration including CPU speed, amount of RAM, operating system and service pack level, computer name, user name, type of Internet connection, IP addresses for internal and Internet-facing networks, as well as upstream and downstream bandwidth. It is likely that this information is used by the attacker to determine their capabilities across the entire botnet with regard to the ability to mount sustained distributed denial of service attacks, host files such as pirated software, movies, music, pornography or similar purposes.

The bot also attempts to steal personal information including POP3 credentials (servername, username, password), HTTPMail credentials (URL, username, password), *Hotmail* credentials (username, password), account information from the Internet Account Manager, contents of protected storage (pstore.dll), *Outlook Express* data (including deleted email), *MSN* credentials, *Internet Explorer* AutoComplete data, and credentials for password-protected *Internet Explorer* sites.

This Win32/Rbot includes its own Internet proxy, thereby acting as a man-in-the-middle for online transactions. To verify connectivity, it connects to Windows Update before attempting to update itself with a configuration file from one of six different sites on the Internet. This malware also tests the capability and configuration of the system by checking for the presence and version of a number of system DLLs.

The IRC component of this bot is customized and has the ability to upload and download additional files, manipulate the DNS cache and ARP cache, conduct a multi-threaded port scan (with the ability to throttle the scan to reduce the possibility of detection), as well as the ability to scan for vulnerabilities and to exploit vulnerable systems. Finally, there is a command within the bot to secure or unsecure the system by enabling or disabling DCOM – presumably in an effort to prevent a competing botherder from capturing nodes in the botnet while still allowing the possibility of using DCOM when needed.

The breadth of capability in monitoring and attacks shown by Win32/Rbot illustrates some of the numerous ways in which a criminal can make money on the Internet through the use of a botnet. Theft of personal information is still very much present in this bot – to a degree not seen in our previous examples in addition to the other areas targeted by this threat.

The Win32/Rbot family is the most prevalent of the threats removed by *Microsoft's Malicious Software Removal Tool*, representing more than 4.4 million removals from more than 1.9 million unique computers in the *MSRT's* first 15 months [14]. Additionally, the FU rootkit employed by Win32/Rbot accounts for more than 762,000 removals from more than 386,000 unique machines and represents the fifth most prevalent threat and the most frequent rootkit removed by the *MSRT* [14].

FURTHER PRIVACY CONSIDERATIONS

This paper has covered a wide variety of monitoring software, ranging from parental controls, to commercial spy software, to malicious software with monitoring capability. The methods and rationales behind the monitoring differ widely in each of these categories. A key component of the legitimacy of monitoring in each of the cases revolves around the consent

experience, with an aspirational practice being full, clear and conspicuous disclosure (such as with the most consumer-friendly parental control software) through the wholly malicious (and often criminal) collection of data carried out by malware such as Win32/Gaobot, Win32/Banker and Win32/Rbot.

It is hoped that makers of commercial software will continue to follow and to refine best practices around consent and disclosure. At the same time, it is clear that even should this occur there is a growing threat of monitoring through the use of malicious software and that the malicious software used for this is growing in capability.

SUMMARY

Keystroke logging and other forms of monitoring represent benefit or risk depending on the technique used by the software and create complex legal and social questions. From a privacy perspective the main points to consider with regard to the appropriateness of monitoring relate to the consent experience of the person being monitored and the disclosure provided by the software as to what it will do. Additional privacy concerns of access to and security of the data collected, as well as the integrity of the data, are also worth noting, though these are secondary to the considerations around consent and notice. Legal considerations such as a person's expectation of privacy as well as other laws also come in to play but vary widely depending on the specific jurisdiction involved. The law is also in a state of continuous flux due to ongoing refinements in the understanding of data use.

While there are privacy concerns relating to monitoring there are also legitimate uses for technology capable of such intrusions including use in support of law enforcement, technical support and as a tool for parents. In law enforcement use it is essential that the scope of monitoring be limited to the minimum required to support the case and the monitoring must also be conducted in accordance with all applicable laws. Monitoring in the course of employment must also be respectful of boundaries – something that takes place both through employment agreements and with controls within most technologies used for this purpose. Use of monitoring software within a family can range from an educational and parenting tool to one designed to limit risk faced by the child.

Monitoring also occurs for reasons which have little or no social benefit including stalking, online bullying, as a manifestation of a broken relationship and of the online equivalent of eavesdropping. In the last several years we have also seen a marked rise in the use of monitoring software as a component of malware given that the information collected can be used both for direct fraud as well as for a currency amongst those in the underground. The methods used by the authors of malicious software vary from those targeted approaches singling out some small number of financial institutions to the more opportunistic collection of information with intent that is less clear.

Both legitimate and illegitimate use of monitoring shows widespread use, and trends indicate that this will continue. This can be mitigated to some degree through education as well as through the availability of tools such as the *Microsoft Malicious Software Removal Tool*, *Windows Defender* and other security products, adherence by independent software

vendors not only to practices which meet the minimum legal bar, but also those which address social considerations around consent and disclosure, and broader enforcement against those who break the law or facilitate these crimes.

THANKS

The author would like to acknowledge and thank the following people whose efforts contributed tremendously to this work. Aaron Hulett and Jaime Wong of *Microsoft's* anti-spyware analysis team conducted the detailed analyses of the threats highlighted in the case studies. Jason Geffner, a Reverse Engineer in *Microsoft's* anti-virus team, provided advanced analysis assistance on the stealth and anti-analysis components of Win32/Rbot. Cindy Southworth, Director of the National Network to End Domestic Violence (NNEDV.ORG), provided statistics and examples relating to the domestic violence threat and also served as an early reviewer of this work. The author is grateful for the cooperation and support of everyone who contributed to this paper through the various review cycles, early presentation run-throughs and data gathering.

REFERENCES AND END NOTES

- [1] AntiSpyware Glossary. <http://antispwarecoalition.org/documents/GlossaryJune292006.htm>.
- [2] Warren, S. D., Brandeis Harvard, L. D. The Right to Privacy. *Law Review* 193 (1890).
- [3] United States v. Scarfo, *et al.*, Criminal No. 00-404 (D.N.J.). <http://www.epic.org/crypto/scarfo/opinion.html>.
- [4] Michigan v. Steven Paul Brown (Warren, Michigan; Sept. 2001) (unofficial case citation).
- [5] Suffolk County v. Michael Valentine (D.N.Y. 2006). <http://www.theglobeandmail.com/servlet/story/RTGAM.20060404.gtstalkapr4/BNStory/Technology/>.
- [6] Gordon, S., Ford, R. Computer Crime Revisited: The Evolution of Definition and Classification. In *Papers and Presentations of the 15th Annual EICAR Conference*, Paul Turner and Vlasti Broucek (eds). Hamburg, Germany, 2 May 2006.
- [7] U.S. v. Carlos Enrique Perez-Melara, *et al.* (Southern District of CA; Case Numbers 05CR1264LAB, 05CR1486LAB, 05CR1487LAB, 05CR1488LAB, 05CR1485LAB). <http://www.webpronews.com/news/ebusinessnews/wp-45-20050829ItSeemedLikeAGoodIdeaAtTheTime.html>.
- [8] LoverSpy. http://george.hotelling.net/90percent/linkage/lover_spy.php.
- [9] <http://www.ci.ventura.ca.us/newsmanager/templates/?a=436&z=5>.
- [10] TrojanSpy: Win32/Banker variant.
SHA1: 2414b6727519b4ec116c7e873ddd46bbd4be2c5c
MD5: ea99aceb5d472a141ce7c5cc2938bbca
SHA1: e3bd0d0c4a4d4b6177284dc64209e8b15b800490
MD5: 62b635b70de8a80c60ea01d1db13ed22
SHA1: 01d89bf0fe313e882a60b9f1a892287bc3e90065

- MD5: 785e4ec04aec79b8552b240dfea76246
Microsoft Malicious Software Encyclopedia,
Banker family. <http://www.microsoft.com/security/encyclopedia/details.aspx?name=TrojanSpy:Win32/Banker>.
- [11] Microsoft Anti-Virus telemetry (unpublished).
- [12] Bureau of Justice Statistics. Violence Against Women: Estimates From the Redesigned Survey 1, Ronet Bachman and Linda Salzman, (January 2000).
- [13] Win32/Gaobot variant.
MD5: 05BE8E296E77FD92E3AF86B14A4BB932
SHA1:
4047E0F324FAC607EF4F8CB9312968DB51AAB9CB
Microsoft Malicious Software Encyclopedia,
Gaobot family. <http://www.microsoft.com/security/encyclopedia/details.aspx?name=Win32/Gaobot>.
- [14] Braverman, M., *et al.* The Windows Malicious Software Removal Tool: Progress Made, Trends Observed. Microsoft, June 2006.
- [15] Win32/Rbot variant.
MD5: 036b94eb0600d867f32bde7de309e35d
SHA1:
D9D775355479268890CD9E34CCEB80A462ECF32C
Microsoft Malicious Software Encyclopedia,
Rbot family. <http://www.microsoft.com/security/encyclopedia/details.aspx?name=Win32/Rbot>.
- [16] Microsoft Malicious Software Encyclopedia,
W32/FURootkit. <http://www.microsoft.com/security/encyclopedia/details.aspx?Name=Virtool:WinNT/FURootkit>.