Global Information Assurance Certification Paper

The W32.HLLW.Bymer Worm
John Bartolick
February 10, 2001

Introduction

Begin with a non-profit organization dedicated to the promotion of distributed computing. Introduce multi-national projects designed to utilize brute-force code cracking techniques in response to challenges issued by various information security organizations, throw in some prize money and prestige for contest winners, and combine this with a few nefarious individuals and some common and well-known vulnerabilities in the world's most popular desktop operating systems. The result is the W32.HLLW.Bymer worm.

The W32.HLLW.Bymer worm is not a particularly destructive worm. Symantec has categorized the damage associated with the worm as "low"[1], although the worm has been packaged with more destructive viruses (e.g., there are reports that the destructive W32/Kriz.4050 virus has been distributed using the worm[2]). ZDNet claimed that after the first few reports of the worm in the early Fall of 2000, much more frequent reports were observed in December[3]. At that same time Symantec upgraded the worm to a "top threat"[1]. The worm is relatively easy to prevent and eliminate, and although it has spread somewhat rapidly it did not have the distribution speed of other, more notorious worms, probably because it does not exploit electronic mail for distribution. It is also rather straightforward from a technical perspective. I find the worm interesting not because of its uniqueness or because of any groundbreaking characteristic, but because of its genesis as part of worldwide challenges to achieve progress in the areas of cryptography and distributed computing.

Background: The distributed.net Organization

The distributed.net organization (also known as Distributed Computing Technologies, Inc.) is a worldwide effort organized to harness the power of excess processing cycles of thousands of computer clients scattered throughout the world and connected through the Internet. A key component of the organization's Mission Statement well illustrates the group's goals:

"We will deploy our software to form an immense, globally distributed computer that solves large-scale problems and provides an accessible pool of computational power to projects that need it."[4]

In order to promote the organization and to demonstrate "the real-world utility of both distributed computing in general and our software in particular"[4], the organization has initiated several special projects that leverage the group's core competency – the employment of distributed computing resources to solve extremely difficult,

computational-intensive projects. These projects include the decryption of messages encoded with RSA Labs' 56-bit RC5 encryption algorithm as well as the government's 56-bit DES encryption algorithm. This concept of harnessing the horsepower of thousands of distributed clients is also practiced by several competing organizations, including decypher.net, whose projects include a simulation of radiation around an encapsulated radioactive source in an effort to build a safer vessel for containing radioactive materials[5], and SETI, an organization dedicated to using distributed computing as a tool in the "Search for Extra Terrestrial Life"[6,12].

The distributed.net organization's latest project is focused on cracking the RSA 64-bit RC5 key. RSA Labs is offering an award of US$10,000 for winning the contest, of which a minimum of US$1,000 would go to the winning individual[7]. As of February 5, 2001, there were 283,747 individuals and 11,001 distributed.net teams that had participated in the RC5-64 challenge. The distributed.net team has been working on this problem for slightly over three years. Approximately 40% of the keyspace has been checked so far, and at the current rate the problem should be solved some time in the next 872 days. The group has two other projects also active at this time – the Optimal 24-Mark Golomb Ruler (OGR-24) and OGR-25[4].

As individuals harness more and more machine processing cycles, they are able to check a larger portion of the keyspace. In order to supplement the cycles under their direct control, many individuals and teams reach out to recruit associates willing to contribute their processing power toward the effort. Other individuals have chosen a less ethical approach by stealing the machine cycles of unwitting individuals through the use of the W32.HLLW.Bymer worm.

I cannot emphasize enough that the distributed.net project is perhaps the greatest victim of this worm. As detailed later in this paper, the organization itself is not associated with the creation of the worm and had in fact taken all steps in its power to eradicate the worm and prevent future occurrences. The relationship of the worm to the group and its efforts is extremely unfortunate and undeserved.

The distributed.net Client

Distributed.net draws it's massive computing power from thousands of discrete computers running their client software, the current version of which is called dnetc. The dnetc client is designed to utilize "wasted" processing cycles in the client machine; that is to say machine cycles that are required for use by other tasks. The client uses round robin DNS to communicate across the Internet to one of a number of "keyservers" to either download work or to upload results. The client is specifically engineered to make use of idle time and is intended to work on a variety of client architectures, regardless of the speed of the client.

It is important to note again that distributed.net is a well-respected, legitimate organization. The group specifically reinforces that their client software should only be

used with the explicit permission of the owner of the client processor and they have disavowed the use of worms to distribute their software. There is nothing inherently malicious in the dnetc client itself.

The Nature of the Worm

In their widely distributed paper The Not So Friendly World of Cyberspace – Know Your Enemy: Worms at War[8], the Honeynet Project described the characteristics of one derivative of the W32.HLLW.Bymer worm. The Honeynet Project is an organization of security professionals that specializes in the use of honeypots for the purpose of "learning the tools, tactics, and motives of the blackhat community"[9], then sharing the information they learn from these exercises with the security community in the form of a web site and several published papers. Their "Honeynet" was subjected to an abnormally high number of scans against UDP port 137 (NetBios Naming Service) and TCP port 139 (NetBios Session Service). The group correctly guessed that these scans were randomly searching the Internet for Windows-based systems with file sharing enabled. In order to study this condition, the group placed a monitored Windows 98 machine on the Internet with no firewall and with file sharing enabled. Within 24 hours the system was subjected to its first scan. As predicted, the honeypot was scanned by a host which first determined the operating system and then determined the fact that file sharing was enabled. The system was then scanned for the presence of specific files, including dnetc.ini, a component of the distributed.net client. The purpose of this scan was to determine whether or not the worm was already installed. Once the worm determined that neither the dnetc client nor the worm were not present it proceeded to install itself on the subject system. The dnetc client was pre-configured with the address of the individual that would be "using" the machine's cycles as part of the RC5-64 challenge. In addition to installing the distributed.net client, the worm also installed itself on the system. In this example the worm binary was called msi216.exe. Next, the worm replaced the system's win.ini file with a modified version that autoloads the dnetc client. Finally, two keys were added to the registry (HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Bymer.scanner and HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Bymer.scanner).

Once an attacked system is subjected to the above changes and rebooted, the dnetc client executes, taking direction from the specified keyserver and reporting results back on a regular basis. The worm also begins using the new host to conduct further scans of the Internet in order to continue its self-replication. This is a classic example of how it is unwise to jump to conclusions when tracing the source of a malicious Internet scan. In this case, the owner of the scanning machine is totally unaware that their computer has been "hijacked" and is being used as a platform for further distribution of an Internet worm.

As an illustration of the pervasiveness of this worm and its derivatives, the same honeypot was scanned again within a day of the initial attack. This time, the worm efficiently packaged all of its components into one single executable called wininit.exe. This file name was specifically chosen since Windows systems already come with a legitimate file name wininit.exe. In the days that immediately followed, multiple probes for each of the described versions of the worm were recorded by the honeypot. Amazingly, a struggle between competing versions of the worm ensued, with one derivative replacing the name of the controlling distributed.net contest participant with that of the competing party. Some time later the process was reversed as the battle for machine cycles continued.

Aliases and Variants

The W32.HLLW.Bymer worm is also commonly known as dnet.dropper, Trojan.win32.bymer, VBS/NetLog.worm.c, and w32/msinit[1,10]. In addition, the Symantec AntiVirus Research Center (SARC) has issued a report of a related hoax in which perpetrators have attached pre-configured distributed.net clients to an email message that warns the recipient of a new virus that can be easily corrected by running the attached file (the pre-configured dnetc client)[1]. In this example, gullible users play into the hands of the contest cheaters by unknowingly installing dnetc on their own machines.

The Anti-Virus Industry's Reaction

Within hours of the discovery of the initial versions of the W32.HLLW.Bymer worm, the major anti-virus software vendors developed facilities to combat the infection. Since the distributed.net client is legitimate software, anti-virus software will not necessarily identify it as a "virus" nor will it necessarily automatically clean it up. Most products will identify the msinit.exe and bogus wininit.exe binaries as viruses. Most of the remedial activity associated with worm removal is manual.

The worm was initially considered to be a minor annoyance, but has risen rapidly on many virus and worm-related "top 10" lists.

How to Avoid the W32.HLLW.Bymer Worm

It is disconcerting that this worm is normally distributed without the user having to take any action (i.e., the user does not have to open an email message, run an EXE, etc.). As with many other worms, this worm thrives on unprotected systems. The authors have clearly targeted the home user community. The use of a Personal Firewall, such as BlackIce, is a must for any "always on" Internet client, such as those utilizing cable modems and DSLs for connecting to the World Wide Web. Of course, disabling file sharing on Windows systems is a simple protection that should be an essential part of any

Internet-attached Windows client. According to Network Ice, developers of the popular BlackIce personal firewall, 10% of all Internet users leave their hard disks exposed on this port[11]. In fact, they refer to port 139, the NetBIOS Session (TCP), Windows File and Print Sharing as "the most dangerous port on the Internet"[11]. Finally, the use of an established anti-virus utility with updated virus definitions rounds out the "defense-in-depth" approach to avoidance of this and other worms.

The distributed.net Response

The use of a worm to cheat in the RSA contest is clearly not in the best interest of distributed.net. The distributed.net organization reacted quickly to the news that participants in their project were parties to the development, intentional distribution and/or exploitation of an Internet worm. The organization immediately disavowed any relationship with parties involved with the development, distribution, or intentional exploitation of the worm. In a clear message to such individuals, distributed.net announced that guilty individuals and their teams have been permanently removed from the project and are no longer eligible for any prizes associated with the RSA contest. Distributed.net has said, however, that any contest team that is banned because of the action of a specific team member can be reinstated if they demonstrate that the individual's actions were conducted without the knowledge or authorization of the team organizers[4].

The group also initiated an awareness campaign through their website. This campaign included an acknowledgement of the existence of the worm and it's relationship with the distributed.net project, information on identification and removal of the worm, links to related industry information, and a reiteration of the group's mission statement, usage policies, and worm-specific interventions. In addition, the group has established a vehicle for individuals to report abuse of the distributed.net client[4].

Conclusion

The study of the W32.HLLW.Bymer worm encompasses a veritable smorgasbord of topics that virtually mirrors the SANS GIAC Level One Security Essentials curriculum. The introduction to IP and the IP behavior modules were well reinforced by the detailed descriptions of the initial attacks documented by the Honeynet project in their case study of the worm. The value of the "defense in depth" principle espoused in the Information Assurance Foundations section was well illustrated by the fact that multiple security practices are required to totally protect a client computer from being susceptible to the worm. The need for sound policies was illustrated both on the client side (a demonstration of the application of good anti-virus, firewall, and system configuration policy) and on the part of distributed.net (including an excellent example of an appropriate use policy). The value of an excellent perimeter defense was again illustrated by the good people of the Honeynet project, who showed not only the value of an effective firewall, but also a classic example of how to use a honeypot to analyze the

ways and means of the hacker community. Their case study was an excellent demonstration of the practical concepts outlined in the Host Perimeter Defense and Internet Threat modules. The Encryptions courses provided an excellent background into the RSA technology that was at the heart of the contest that eventually spawned the worm. Finally, the whole case provided an excellent synopsis of the course section on malicious code.

References

1) Symantec Anti-Virus Research Center, 12/7/00 URL: http://www.symantec.com/avcenter/venc/data/w32.hllw.bymer.html (January 19, 2001), http://service1.symantec.com/sarc/sarc.nsf/html/W32.HLLW.Bymer.html (February 9, 2001)

2) On-Line Services Web Site, URL: http://www.on-line-services.com/Advisories.htm (February 5, 2001)

3) Vamosi, Robert. "Bymer Spreads Through Open Network Shares" ZDNet US. 12/11/00 URL: http://www.zdnet.co.uk/news/2000/49/ns-19604.html (February 5, 2001)

4) Distributed.net Home Page, URL: http://www.distributed.net/ (January 29, 2001)

5) Decypher.net Web Site, URL: http://www.dcypher.net/newsandprojects.asp (February 9, 2001)

6) SETI Web Site, URL: http://www.seti.org/ (February 10, 2001)

7) RSA Labs, URL: http://www.rsasecurity.com/rsalabs/challenges/secretkey/links.html (January 29, 2001)

8) The Not so Friendly World of Cyberspace - Know Your Enemy: Worms at War Written by the Honeynet Project, Last Modified: 11/9/00 URL: http://packetstorm.securify.com/papers/general/kye-worm.txt (February 1, 2001)

9) Honeynet Project home page, URL http://project.honeynet.org (February 1, 2001)

10) McAfee Home Page, URL: http://vil.mcafee.com/dispVirus.asp?virus_k=98844& (February 1, 2001)

11) Network Ice, URL: http://www.networkice.com/advice/Exploits/Ports/139/default.htm (February 5, 2001)

12) Bedell, Doug. "Search for Extraterrestrials – or Extra Cash, Users Let Home PCs Crunch Scientific Data in Downtime" Dallas Morning News, 12/2/99, URL: http://www.dallasnews.com/technology/1202ptech9pcs.htm (February 9, 2001)