基于选择性监测的蠕虫预警技术

何雪煜　卿斯汉
（中国科学院软件研究所信息安全技术工程研究中心　北京100080）

摘　要　首先分析现有的三种蠕虫监测方法：(1)监听、搜集、分析网络中的ICMP-T3信息，由此来判断蠕虫是否在传播。(2)对网络中主机的TCP，或者UDP的连接活动进行监视，对网络中的“水平”扫描活动加以分析。(3)在每个主机上设立微型蠕虫防范系统，对被动和主动的连接数据报进行比较分析。这三种方法各有优点。但同时也存在不足之处，对蠕虫的预警有漏报和错报的可能。我们所设想的蠕虫预警系统是把这三种方法综合利用起来，发挥各自的优势，对各自的不足进行互补，形成更有效、更节约资源的蠕虫预警系统。

关键词　ICMP-T3，水平扫描，微型监测器，触发值

Selective-Monitoring Based Worm-Warning System

HE Xue-Yu　QING Si-Han
(Engineering Research Center for Information Security Technology, Institute of Software, Chinese Academy of Sciences, Beijing 100080)

Abstract　To start, we introduce three ways that to monitor the network for warning of worm. The first way: monitoring the network, collect and analyze ICMP-T3 data packets to see whether there are active worm in the network. The second way: monitoring the TCP or UDP requests from hosts that belong to the local network to see if there exists anomaly “horizontal scan”. And the last way, set up a micro Anti-Worm-System on every hosts to analyze data in and out the host to judge if there are active worm on the host. These three ways all have virtues and shortages respectively. We integrate all these ways to devise a system that keep those virtues and complement shortages of each other, and a system more effective and costs less resources.

Keywords　ICMP-T3, Horizontal scan, Micro monitoring component, Threshold value

1　引言

自从第一条蠕虫开始在互联网上肆无忌惮地快速传播以来，蠕虫，或者恶意代码已经成了互联网上非常重要的危害。蠕虫的传播速度越来越快，发生时间也越来越突然、毫无征兆，再加上人们脆弱的防范意识，它的爆发常常让人猝不及防。蠕虫在利用各种漏洞进入主机之后所潜在的危险足以让所有的计算机所有者心惊胆战。随着各种网络的应用程序的日益增多，蠕虫的种类有增无减。防范蠕虫的最好的方式就是及时地给系统打好补丁(很多广泛传播的蠕虫利用的漏洞已经公布很长时间，而且已有了相应的补丁)，同时还要严格、及时做好网络的各项安全措施，但是这往往需要非常敬业的网络管理员，还有大量的人力。蠕虫的传播很多时候是很难避免的。尽管防范于未然是重要的，但是把蠕虫传播所造成的损失减小到最小同时也是非常重要的补救措施之一。所以在这里我们把注意力集中到蠕虫成功地进行传播之后，如何及时、准确地发现蠕虫的传播迹象。

如果单纯地依靠人工来发现蠕虫的传播，那么造成的损失很可能不堪设想。既然蠕虫是利用计算机来进行动传播，人们也应该充分利用计算机来进行蠕虫的监测。现有的蠕虫预警技术往往都是相互独立的。每项技术都有其独特的用处，但其不足也是非常明显的，这样就会造成蠕虫传播的漏报和误报。本文大概介绍一下三种蠕虫的检测技术，分别分析其优点和不足。然后构建出一个综合利用这三种技术的蠕虫预警系统。

本文第2节介绍蠕虫的传播方式；第3节分别介绍三种蠕虫的预警技术；第4节介绍根据这三种独立的技术构建出的新的蠕虫预警系统。最后是总结。

2　蠕虫的传播

2.1　蠕虫传播的四个阶段

从蠕虫选择感染目标主机到已经被感染的主机就开始新一轮的感染活动这个角度来看，蠕虫的传播活动可以分为下面四个阶段，而第一个阶段和最后一个阶段本质上是一样的。

1　*目标选择*　一个没有被感染的易感染主机很不幸地被选择为入侵对象。从被入侵者的角度来看，这仅仅是一个网络的扫描活动。

2　*攻击漏洞*　蠕虫通过主机上未加防范的漏洞，攻陷主机，使得主机处于蠕虫控制之下。

3　*感染主机*　感染阶段的活动是所有的蠕虫都需要经历的阶段。蠕虫把自己拷贝到处于控制之下的主机里。有的蠕虫“攻击漏洞”阶段和“感染主机”阶段是合二为一的，没有明显的界限。

4　*传播阶段*　往往这是蠕虫非常重要的一个过程，因为它要达到快速传播的目的，又要不至于被发现。在这个阶段，存在着很多传播手段。在这里，简要地介绍一下蠕虫的IP地址选择技术，这对于我们及时地发现蠕虫有着密切的关系。

2.2　蠕虫的地址选择技术

何雪煜　硕士生，研究方向：网络安全。卿斯汉　研究员，博导，研究方向为信息安全理论与技术。

选择性随机扫描 和扫描整个IP地址空间相比，选择性地随机扫描试图选择更有可能存在的IP地址。蠕虫携带地址列表进行传播。地址列表可能来自全域列表，或者本地列表。在传播的过程中根据携带的列表进行选择性的感染。这样就避免了扫描没有分配的地址，减少了扫描时间和因为网络产生ICMP-T3信息而被发现的可能。

可路由扫描 通过BGP来了解可路由的IP地址。BGP是"globally routing protocol"用来连接各个独立的网络。有些BGP列表在网络上是可以得到的。这样就减小了蠕虫的代码携带量。

DNS扫描 蠕虫可以从DNS服务器上得到IP地址来进行传播。

随机扫描 这种扫描方式不用费工夫得到可路由的IP地址，完全根据网络的特点来开发算法。比如，先扫描局域网内的主机，再扫描局域网外的主机，采用完全随机生成不重复的IP地址来达到广泛传播的目的。相应地，各种随机生成IP地址的技术的不断更新和蠕虫检测技术的不断升级就成了蠕虫制造者和蠕虫防范者之间猫捉老鼠的游戏。

3 相互独立的蠕虫预警技术

3.1 基于行为的蠕虫预警方式

一个Behavior-based Anti-Worm System，其主要方法就是根据潜在的受害主机在受到攻击的时候所收到的数据报和已经受了蠕虫感染之后再去感染别的主机所发出的数据报是"一模一样的"这一特点来设计蠕虫的预警系统。因为要比较数据报所包含的"payload"的内容，所以资源消耗比较大。这个系统还有一个特点就是把原本集中于一点的预警机制进行了分散，在所有的主机上都建立微型的预警系统，在本地进行蠕虫的预警活动。

监测规则：在主机上有一个"解析器"，负责解析所有的从外界网络收到的请求，并且把请求内容发送到"Input Buffer"，同时把往外界发送的请求内容发送到"Output Buffer"。为了避免不必要的资源浪费，解析器要把非常明显的安全的请求排除在外。"分析"模块比较接收到的和发送的内容。如果两者匹配，就把比配的内容送到防火墙的模块里面；如果在连续的T(根据情况具体定制)时间内，收到了超过一定数量的相匹配数据报，就认为收到了蠕虫的感染。

防范规则：当防火墙从分析部分收到了攻击的代码之后，就可以通知所有的微型防火墙，过滤掉这样的请求。

弱点：①漏报。如果主机的网络活动十分频繁，缓存不能储存足够的数据报的内容；蠕虫选择在感染了一台主机之后，潜伏一段时间；或者干脆蠕虫在设计的时候把无关紧要的垃圾填充字节设计为某一随机变量的函数结果，就完全颠覆了这个系统的设计基础。出现这些情况就有可能漏掉蠕虫的入侵活动。②错报。现在有的应用程序在网络上的活动和蠕虫很相似设计的目的就是为了充分利用网络的分布式的运算能力和储存能力，这些应用程序不断地发出和接收内容相同的数据报，比如BitTorrent。有了这些应用程序的干扰，就可能引起错误的警报。

防火墙的分散，也许会引起管理的混乱，加重非计算机安全专家用户的负担。

3.2 根据ICMP消息来监测蠕虫

ICMP的目的是提供IP层的通信和路由产生的问题和反馈。对于蠕虫检测来说，最有用的信息就是"目的不可达"信息。它表示了不可达的主机、网络、端口、服务等等。主机不可达的信息在ICMP数据报的"type"域表示为"3"，也称之为ICMP-T3。

蠕虫在大量传播过程中，采用的是随机选择IP的方式。由于蠕虫并不知道这些IP地址是否有效，或者具有有效的IP地址主机并没有开机或连接到网络上，这样在蠕虫的快速传播中，就会产生一定数量的ICMP数据报。利用这个特点，我们可以基于分析ICMP数据报来设计蠕虫预警系统。

有两种信息对于蠕虫监测是很有用的。一是"主机不可达"，二是"目的网络不可达"。"主机不可达"是本地网络路由器产生的。"网络不可达"是路由器之间的路由器产生的。在这两种信息里面，有着非常有用的信息：部分原始的数据报会被ICMP数据报封装在里面。根据RFC792，至少原始的IP头和8字节的数据会被封装在里面。这就意味着原始的目的和源IP地址、目的和源端口、采用的协议和所封装的数据的大小都是可以得到的。

蠕虫预警系统所控制的网络里面，所有的路由器都会把自己产生的，或者外网产生的全部ICMP数据报发送一份给预警中心。预警中心对收到的ICMP数据报进行分析。由收到的ICMP数据报可以分析出和ICMP数据报有关的主机可能处于以下几种情况：

1)在一定的时间内，一个主机主动和一定数量的其它主机在相同的端口用相同的协议进行连接。这种情况可能就直截了当地表明很可能是蠕虫在传播。

2)在一定的时间内，一个主机在同样的端口，被一定数量不同的主机用同样的协议连接一定的次数。这种情况可能是一个活跃的蠕虫传播的现象，但是很可能在蠕虫开始传播了相当一段时间之后才会出现。而且更可能的是一个从网络断开的服务器。失败的连接会很多，但是在一段时间之后会减少(人们开始意识到这个服务器已经关闭了)。也可能是一个D-DOS攻击，在服务器被成功地瘫痪或者隔离之后，就会出现这种现象。

3)在一定的时间内一个主机在同样的端口，被另一个主机用同样的协议连接一定次数。这种情况下可能是系统中一个断开的主机。

4)在一定的时间内一个主机被另外一个主机在不同的端口扫描一定的次数。这种情况可能是一个单个主机的恶意垂直的端口扫描。

对ICMP消息进行分析得出的结果，我们可以判断蠕虫是否在传播。

弱点：现在网络的IP-V4地址的分配已经呈饱和状态，而且蠕虫往往都首先对局域网内部的主机进行感染，而往往是同一个局域网里面的用户在同一个时段使用电脑。所以，在一个大型的网络内部，在计算机使用率较高的时候，如果有蠕虫已经开始活动了，ICMP数据报的产生怕满足不了触发蠕虫预警需要的ICMP数据报的数量。而如果开始产生大量的ICMP数据报，可能蠕虫的传播已经比较严重了。或许它已经完成了内部网络的传播任务，开始向外界传播。如果满足触发蠕虫警告的ICMP数据报的触发值设计过低，恐怕又和一般的应用程序没有什么区别。这就增加了对蠕虫的错报。

3.3 根据蠕虫的"水平"扫描行为来监测蠕虫

大多数蠕虫利用的只是一个计算机系统的漏洞，所以在传播的时候，数据报的源IP地址和目的端口都是一样的。也就是"水平扫描"。利用这个特点，可以在网络内部设置监测机

构，监测网络内部的所有的 TCP SYN 或者 UDP 活动。如果在一定的时间内，发现有主机进行了一定数量的“水平扫描”，那么就判定已经有主机感染了蠕虫。并且能够方便地确定感染蠕虫的主机，及时地方便管理员采取活动。

弱点：在大型的网络里面，特别是网络活动繁忙的网络里面，要对每一个计算机进行网络活动的监测是非常耗费资源的。一是，尽管计算机的性价比越来越高，但是应用程序也越来越丰富，这样就对预警系统的资源提出了更高的要求。二是，路由器要把每台主机的每一个 TCP SYN 或者 UDP 都要发送一份到预警中心，这对网络本身也形成了新的负担。

大型的、活动频繁的网络里面在监测每一个主机活动的时候，限于蠕虫预警系统的资源，对每一个主机的活动监测是有资源限制的。就像上面说的那样已经有了应用程序，在运行的时候，网络活动类似于蠕虫的水平扫描。要把蠕虫的活动和这样的应用程序区分开来，就需要能够对水平扫描的主机进行更一步的监测。这样就很有可能漏报。而正是大型的、有着大量的网络活动的组织需更要及时地对蠕虫的活动进行监测，保证在感染蠕虫的时候能够尽量地减少损失。

4 复合的相互协调的蠕虫预警技术

4.1 蠕虫预警系统的结构

上面的三种蠕虫预警方式都各自有着优缺点。我设想把三种预警方式集成起来，保留各自的优点，并且对各自的缺点进行互补。

系统构成：微型监测器；复制、发送 TCP SYN、UDP 的路由器；预警中心。

预警系统如图1所示。

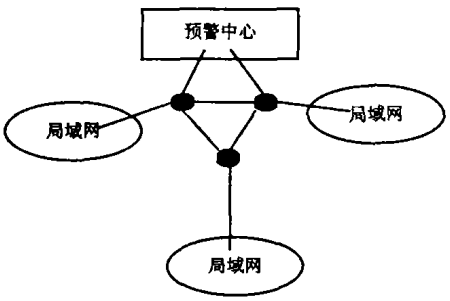

图1

预警机制概述 每台主机上有微型的流量监测器(但是没有微型防火墙，这样可减少用户和管理员的负担)，主机上设置有一定大小的“Input Buffer”和“Output Buffer”。微型流量监测器负责把流入和流出的数据内容进行比较，并且把匹配的数据报发送给预警中心。

每台路由器负责把所有的 ICMP 数据报和 TCP SYN 和 UDP 数据报发送一份到预警中心。

预警中心负责整个网络的蠕虫预警。预警中心分析的数据报有三种。第一种是所有的 ICMP 数据报。预警中心不对这种数据报进行更一步的分析。而是对引起这种数据报的、在监测范围内的“源主机”进行“水平扫描监测”。监测的端口可以是引起 ICMP 数据报的端口，也可以是所有的端口。

第二种是每台主机上传来的流出和流入数据相匹配的数据。一旦收到这种数据，预警中心就选择对发送这种数据报的主机进行“水平”扫描监测。

最后整个网络的 TCP SYN 和 UDP。据预警中心还有富余资源的时候，预警中心还对网络内部的其他流量进行监测。不过，为了提高蠕虫监测的准确性，这种对主机的连接活动的监测是有选择性的。比如轮流监测主机，或者重点监测等等。

判断机制 设单个主机在某个端口，用同样的协议“在一定时间内水平扫描的次数”= N 为蠕虫传播预警的“触发值”。

最终确定有蠕虫在监测范围内传播，是基于该预警系统对蠕虫传播的“水平扫描”特征的。当“N”达到或超过一定数值的时候，就发出蠕虫传播警告。“N”需要根据经验来设置。而在选择监测对象的时候，或者有赖于各个主机、路由器提供监测对象；或者由预警中心来选择监测对象。

对于有的应用程序有着类似于蠕虫传播的网络活动特性，可以针对特有的端口设置不同的“触发值”，或者在重点保护的主机上禁止这类应用程序的运行。

4.2 综合说明

这样的集成式的设计方式使得前三种蠕虫预警方式相互补充，避免了可能出现的漏报、错报。

对于“微型预警系统”，在蠕虫随机改变传播内容，或者蠕虫选择在侵入主机之后潜伏一段时间的时候，由 ICMP 分析和“水平扫描”监测来保证蠕虫检测的及时性。

对于“基于分析 ICMP”的预警方式，当 IP 地址分配趋于饱和，ICMP 数据报产生量不足的时候，由“选择性的水平扫描”来保证检测的及时性。

对于“水平扫描监测”，在网络庞大到一定的数量，预警中心资源不足的时候，由有选择性的“水平扫描”来保证蠕虫预警的及时性。

而“基于 ICMP”和“流出流入数据的匹配”来选择监测对象则一定程度上弥补了“选择性的水平扫描”的没有对整个网络进行监测的不足。

针对有的应用程序在运行的时候，有“水平扫描”的特征，可以对这种应用程序使用的端口进行放宽报警触发条件，或者在重点监测的主机上不准使用这种应用程序。

总结 随着网络的应用程序越来越丰富，这样一方面给蠕虫提供了更为丰富的漏洞；另一方面，这些应用在网络上表现出来的特性，又让蠕虫的预警变得更有挑战性。如何有效地对蠕虫的传播进行预警，是一个需要更多探讨的课题。

参 考 文 献

1 Hung J C, Lin K-C, et al. A Behavior-based Anti-Worm System. 2003. http://csdl. computer. org/comp/proceedings/aina/2003/1906/00/19060812abs. htm

2 Wu J, Vangala S, Gao L, et al. An Effective Architecture and Algorithm for Detecting Worms with Various Scan Techniques. 2004. http://www-unix. ecs. umass. edu/~lgao/ndss04. pdf

3 Berk V, Balos G. Designing a Framework for Active Worm Detection on Global Networks. 2003. http://people. ists. dartmouth. edu/~vberk/papers/iwia03. pdf

4 The CERIAS Intrusion Detection Research Group Center for Education and Research in Information Assurance and Security Purdue University West Lafayette, IN. Digging For Worms, Fishing For Answers 2002. http://www. acsac. org/2002/papers/68. pdf

5 Bakos G, Berk V H. Early Detection of Internet Worm Activity by Metering ICMP Destination Unreachable Messages. 2002. http://www. ists. dartmouth. edu/IRIA/projects/early-worm-detection. htm

6 Zou C C, Gao L, et al. Monitoring and Early Warning for Internet Worms. 2003. http://www. megasecurity. org/papers/monitoringEarlyWarning. pdf

7 Berk V H, Gray R S, Bakos G. Using Sensor Networks and Data Fusion for Early Detection of Active Worms. 2003. http://www. ists. dartmouth. edu/IRIA/projects/d-dibs. htm