翻訳トライアル実践講座　第 4 回

＜問題 1＞　全文を訳して提出してください。

Spam Methods

Almost everyone is aware of the nuisance caused by spam email. When we get to work in the morning we have to delete a bunch of useless messages from our Inbox before we can start the day. When we get home we have to do the same thing before getting around to reading messages from friends and family. Do you ever wonder how these spammers came by our email addresses in the first place?

There are several ways for spammers to gather email addresses to send their messages to. One of the oldest techniques involves sending a “bot” to crawl around on different Web sites, Usenet groups, and other similar Internet resources searching for email addresses. While this method works, it is time-consuming and prone to gathering addresses that are outdated and no longer in use. Another popular method involves generating email addresses using a technique called brute forcing. This method tries sending spam to addresses composed of every possible combination of letters and numbers (for example, a@victim.com, b@victim.com, c@victim.com, etc.). Again, this method produces many invalid addresses and wastes the poor spammer’s time and resources.

So, what's a spammer to do? Earlier this week a worm called JS.Yamanner@m propagated through the Yahoo! Mail Web mail service. Details of JS.Yamanner@m have already been discussed at length, but one significant action of the worm has been overlooked somewhat. When the worm runs it uploads the list of email addresses in the affected user's address book to a Web site. The most likely reason for this upload is so that the addresses can be added to databases used by spammers and phishers. Since the addresses are contained in an active user account it is more likely that the majority of addresses are valid and current, therefore increasing their value.

While this is not the first piece of malicious code to gather email addresses, it does demonstrate that this is an ongoing concern. As spam becomes more profitable the spammers are, in turn, becoming more sophisticated because after all, time is money.

＜問題 2＞　全文を訳して提出してください。

Internet Infrastructure Security

The Internet's crucial role in modern life, commerce, and government underscores the need to study the security of the protocols and infrastructure that comprise it. For years,we've focused on endpoint security and ignored infrastructure weaknesses. Recent discoveries and initiatives highlight a simple fact: the core is just as vulnerable as the edge.

In the past few years, attackers have increasingly targeted infrastructure. Internet protests,vigilantism, nation-state attacks, distributed denial of service for hire, public-key infrastructure lapses, and the market for 0-day exploits have shifted our attention to the increased risk in which we place not only our data but also our livelihood. The Internet s infrastructure, protocols, and processes are therefore getting attention from researchers, not just practitioners.

Infrastructure Vulnerabilities

The Internet is one of world's largest, most complex human-engineered distributed systems ever devised and deployed. It comprises multiple, often interdependent, subsystems. When an endpoint or user of this massive system is threatened, one or more subsystems are often called on to help contain the threat. However, when Internet subsystems themselves come under fire, how do we manage system threats from the system itself or its otherwise trusted subsystems?

The Internet security community tends to consider only the ramifications of availability or integrity loss at one host or organization at a time. Recently, people have been examining, and in some cases exploiting, vulnerabilities that threaten Internet subsystems—the protocols and equipment that move data around. When these subsystems come under attack, statistics on compromised Secure Shell servers and monetary losses owing to credit card fraud seem almost quaint. When infrastructure is at risk, the upper limits of those statistics are boundless.

In addition, the Internet infrastructure is currently undergoing significant changes. As the available IPv4 address pool winds down,

widespread deployment of IPv6 is becoming a reality. Is it any surprise that after one large network provider adopted IPv6, its first inbound email message was spam? More than a decade in the making, the Domain Name System (DNS) root zone was recently signed with DNS Security Extensions. With it generally comes larger DNS answers, which adversaries can use to turn the system against itself in amplification and reflection attacks. The Inter-net Engineering Task Forces Secure Inter-Domain Routing working group is trying to bring assurance to Internet routing where currently even relatively simple router configuration errors can mistakenly reroute huge swaths of address space. In summary, the Internet Protocol—the glue that holds the entire system together—is undergoing a major deployment upgrade while two of its biggest core subsystems, DNS and Border Gateway Patrol, are adding some not-so-trivial security mechanisms.

以上