International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 8
(12/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1205 – Supplement on best practices against botnet threats

ITU-T X-series Recommendations – Supplement 8

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Supplement 8 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on best practices against botnet threats

Summary

Supplement 8 to ITU-T X-series Recommendations provides practical solutions as best practices for countermeasures against botnet threats. These best practices can be utilized by network operators in implementing countermeasures against botnet threats. The best practices are applicable to management, control, and user activities to mitigate security incidents caused by botnet. This Supplement features two best practices.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 8	2010-12-17	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 8 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on best practices against botnet threats

1 Scope

This Supplement provides practical solutions as best practices for countermeasures against botnet threats. These best practices can be utilized by network operators in implementing countermeasures against botnet threats. The best practices are applicable to management, control, and user activities to mitigate security incidents caused by botnet. This Supplement features two best practices.

2 References

[ITU-T X.1205] Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity*.

3 Definitions

For purposes of this Supplement, the definitions given in [ITU-T X.1205] apply. Additionally, the following definitions apply:

3.1 **bot**: An automated software program used to carry out specific tasks designed for malicious purposes. It is interchangeable with a robot.

3.2 **botmaster**: An individual responsible for controlling and maintaining a botnet.

3.3 **botnet**: Remotely controlled malicious software robots (bots) that are run autonomously or automatically on compromised computers together with a command-and-control server owned by botmasters.

3.4 **command-and-control server**: A host that allows the botmaster to control indirectly a sub-group or a group of bots in the botnet to forward an attack instruction to launch attacks.

3.5 **DNS sinkhole**: A scheme for countering bot threats that is designed to block communication between the bots and a command-and-control server by using the sinkhole scheme; it may render the bots dormant or inactive.

3.6 **sinkhole**: A scheme for redirecting specific IP traffic to a sinkhole device (e.g., sinkhole router) for the purpose of traffic analysis, diversion of attacks, and detection of anomalous behaviours on a network.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

C&C	Command and Control
CCC	Cyber Clean Center
DDoS	Distributed Denial of Service
DNS	Domain Name System
IRC	Internet Relay Chat
ISP	Internet Service Provider
PC	Personal Computer
URL	Unique Resource Locator

5 Conventions

None.

6 Overview

A botnet can be regarded as a remotely controlled network consisting of compromised computers by a botmaster for possibly criminal purposes. Any infected computer is referred to as a bot or a zombie, and it serves as an agent following the instruction of the botmaster without the knowledge of its owners.

The unique feature of a botnet lies in having a control communication network. Most botnets have a common centralized architecture, i.e., bots in the botnet connect directly to some special hosts (called "command-and-control" servers or "C&C" servers). These C&C servers receive commands from their botmaster and forward them to the other bots in the network.

The following illustrates how a botnet is created and used to send e-mail spam:

1) An attacker sends out viruses or worms with the intention of infecting ordinary users' computers whose payloads are malicious applications – the bot.

2) An ordinary user's computer turns into a bot-infected computer if the bot is successfully installed on the user's computer.

3) The bot on the infected computer logs into a particular C&C server (often an IRC server, but in some cases a web server) to inform the latter of its infection.

4) A spammer purchases access to the botnet from the attacker. The spammer sends instructions via the IRC server to the infected PCs, causing them to send out spam messages to mail servers.

Figure 1 illustrates a typical botnet working scenario. The attacker indirectly controls the botnet through the control servers that work as a bridge between the botmaster and the bots to convey the attacker's instructions. This instruction could include launching DDoS attacks, sending spam e-mails, distributing malwares, etc.

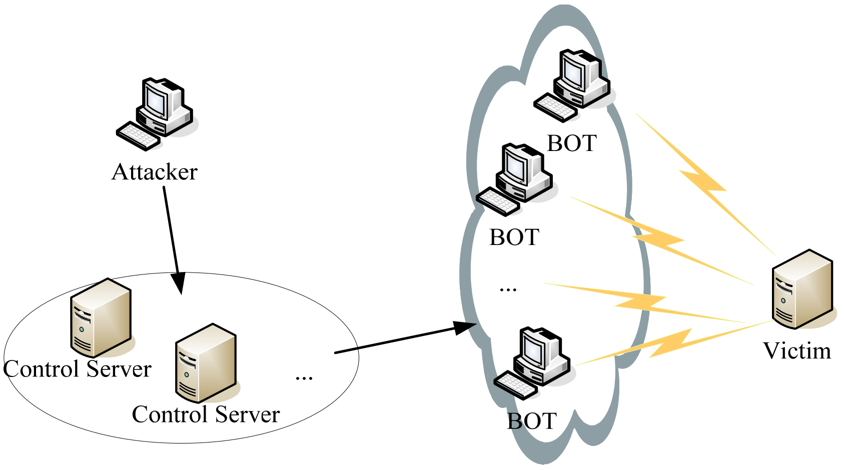

Figure 1 – Typical botnet working scenario

7 Best Practice 1: Alert operation based on the detection of bot-infected PCs (project name: Cyber Clean Center (CCC))

7.1 Introduction

Best practice 1 provides an example of a successful best practice for bot countermeasures operated in Japan. The project name of the best practice is Cyber Clean Center (CCC) [b-CCC]; it has the purpose of reducing the number of bot-infected users' computers in Japan.

7.2 Purpose of CCC

As a type of fraudulent program characterized by augmented infection in recent years, bot has a tremendous number of variants. This makes cleaning bots using a conventional type of elimination means against computer viruses difficult. Since attack and infection activities of bots occur in constrained portions of programs and are unseen to the outside, users do not realize what is going on in their computers. For a safe Internet environment, this is a serious situation.

Given the circumstances above, CCC has been established with the aim of providing botnet countermeasures as an integrated base organization to coordinate among related institutions, ISPs (Internet service providers), and security vendors. The primary purpose of CCC is to investigate the mechanisms of bots' attack and infection in an effective, safe manner and to encourage users to remove bots from their once-infected computers by providing countermeasures (bots removal tool) against bots.

Another important purpose of CCC is to detect and remove new types of bots – which may not be detected by the existing antivirus software – and to share the new bot malware executables with antivirus software companies to allow updating their virus patterns at the earliest opportunity.

7.3 Basic operation flow: Public awareness activities in collaboration with ISPs

According to the CCC investigation of bot, as one of the factors of bot proliferation, a bot infection – unlike earlier viruses – advances in a secret, undetectable manner; the infection route is also unknown to Internet users.

To detect bot, the Cyber Clean Center provides decoy machines, "honeypots", obtains the IP addresses of the infected users' computers, and also draws the attention of the infected users in collaboration with the supported ISPs in this project.

Unlike the conventional notification of procedure for removing viruses by e-mail, this CCC alerting method uses e-mail and website in combination. This method directly sends e-mails to an infected user together with a URL of the "bot countermeasure website" that shows how to disinfect bots. In other words, this method can directly give the infected users easy-to-understand explanations on how dangerous bots are and how to remove bots from their computers. Figure 2 shows the conceptual diagram and operational flow of CCC activity.

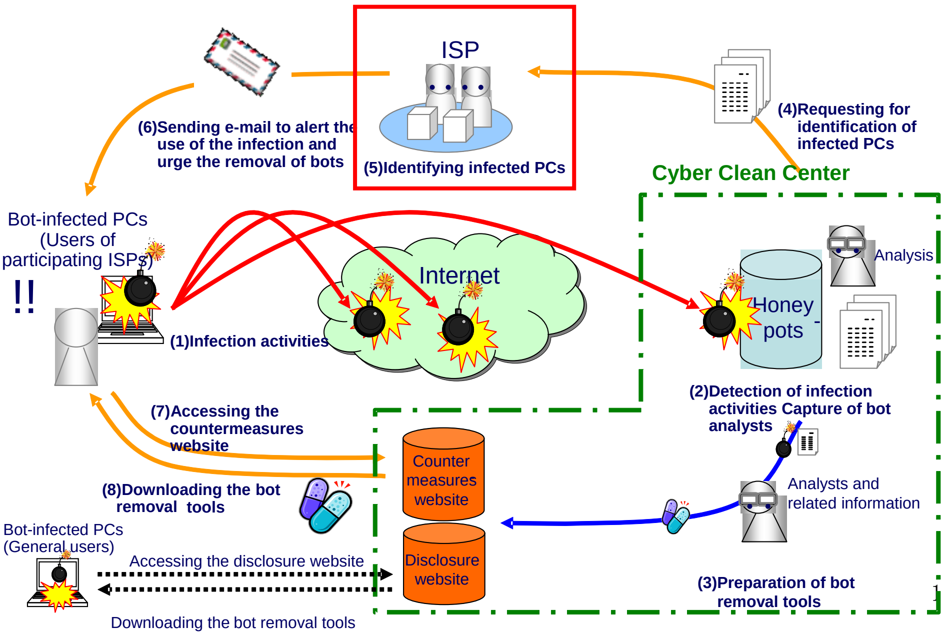
ISP
(5)Identifying infected PCs
(6)Sending e-mail to alert the use of the infection and urge the removal of bots
(4)Requesting for identification of infected PCs
Cyber Clean Center
Bot-infected PCs (Users of participating ISPs)
!!
Internet
(1)Infection activities
Honey pots
Analysis
(2)Detection of infection activities Capture of bot analysts
(7)Accessing the countermeasures website
Counter measures website
(8)Downloading the bot removal tools
Analysts and related information
Bot-infected PCs (General users)
Accessing the disclosure website
Disclosure website
Downloading the bot removal tools
(3)Preparation of bot removal tools

Figure 2 – Workflow of bots detection and response in CCC

1) Capturing bots

The Cyber Clean Center has designed and implemented many "decoy" machines (Honeypots) to efficiently capture bots executables which are attacked by users' infected computers in Japan (Steps (1), and (2) in Figure 2). In this bot capturing phase, several "logs" such as the infected PC's IP addresses and time stamps (date and time) of the infection are collected to correctly identify the infected user PC for the corresponding ISPs.

2) Analysis of bots and generation of removal tools

The bot executables obtained in 1) above are carefully analysed by analysts. These executables are appropriately managed and uniquely identified by means of Hash values. Furthermore, based on the result of analysis that carefully considers the priority of the processes, removal tools against bots executables are generated for use in later process. These removal tools are stored in a bot countermeasures website (Step (3), Figure 2).

In addition to the above, captured bots executables are to be distinguished carefully as to the new types from the existing types and are carried out by means of dynamic behaviour analysis for further research and studies. The new types of bots executables are also shared with several antivirus companies to allow updating virus patterns for their use.

3) Identifying infected users

Based on the collected logs at 1) above containing the corresponding IP address and date and time, the Cyber Clean Center identifies an ISP to which the infected PC users are subscribed to and informs the identified ISP of related data. The ISP further identifies the infected PC user by means of log information (Steps (4), and (5), Figure 2).

The relevant ISP above sends the infected PC user an alerting e-mail containing the URL of the bot countermeasure website (see 2) above). The URL contains a user-specific character string (tracking ID) that enables the ISP to monitor and track the progress of the removal activity at the user's PC (Step (6) in Figure 2). The alerting e-mail above, as a communication media, may be an e-mail and/or a postal letter depending on the country and ISP.

4) Accessing the bot countermeasure website

In response to the alert mail to the user (4), the infected PC user is expected to access the indicated URL (bot countermeasures website) to make the user become aware of botnet threat in his/her computer environment and to download the bot removal tool (Step (7) in Figure 2).

The infected user downloads the free bot removal tool and executes it to disinfect bots. The removal tool should be usable without any pre-installation, and it should not conflict with the existing antivirus software already operating in the PC.

The user is strongly recommended to perform Windows Update and to install an antivirus software. Likewise, the user is requested to issue a notice of completion of bot cleaning using the communication items on the website. Through this notice, the Cyber Clean Center would be able to confirm that the user's removal activity is complete (Step (8) in Figure 2).

7.4 Effectiveness of CCC

CCC has been operating since March 2007. For nearly three years, according to the statistical data summarized in January 2010, the total number of bots executables captured through CCC was 15'808'843, with 472'481 alert e-mails sent to 96'771 infected PC users in Japan. The average rate of downloading removal tools was 31.1%. Furthermore, CCC has been operating a public website that is freely downloadable from any PC user, and 1'152'689 hits have been recorded in this open website among PC users because of CCC security awareness activities.

According to statistical data obtained on CCC operations, before the commencement of CCC activities, the bot infection rate was around 2.0~2.5% (as of 2005) among Japanese broadband users. After the CCC operation was carried out, however, the infection rate plummeted to as much as 0.6% (as of 2010). Therefore, CCC activities can be said to be of great help to decrease the number of bot-infected PC users in Japan.

8 Best Practice 2: DNS sinkhole

8.1 Introduction

The DNS (domain name system) sinkhole scheme has been developed and operated by Korea Internet and Security Agency (KISA) [b-KISA] to counter or combat attacks by bot-infected computers in Korea.

The DNS sinkhole scheme is designed to block communication between bot-infected computers and a bot C&C server to render bot-infected computers dormant.

There are three players in the botnet context: a botmaster, a command-and-control (C&C) server, and a group of bot-infected computers. Once infected with a bot agent, a bot-infected computer attempts connection with a C&C server to inform the latter of its infection and to become a member of the botnet maintained by a C&C server.

A botmaster wishing to launch massive DDoS attacks, scanning the network to find computers with vulnerabilities, or forwarding massive spam e-mails issues the attack commands forwarded to the group of bot-infected computers via a C&C server. Therefore, blocking the communication channel between a bot-infected computer and the C&C server is very critical in rendering a bot-infected computer dormant.

Bot-infected computers use a URL or a domain name instead of a direct IP address, making changing the IP address of a C&C server easy. For the DNS sinkhole to work well, information on the URLs of C&C servers is a prerequisite. The following describes how to get a list of URLs or domain names of C&C servers:

A honeynet operated by KISA collects information on bot agents including the URL of the C&C server and an example of a bot agent. As a type of honeypot designed to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems, a honeynet is a high-interaction honeypot designed to capture extensive information on threats. High interaction means that a honeynet provides real systems, applications, and services for attackers to interact with, as opposed to low-interaction honeypots that provide emulated services and operating systems. A honeynet has a name server and a collection of computers.

A collection of trap computers in the honeynet gathers extensive information on bot agents by performing functions such as data capture and data analysis in a contained environment.

When attacked by malware, trap computers in the honeynet obtain information on the malware and analyse the behaviour of the malware; thus obtaining knowledge of the URL of the C&C servers controlling this malware.

When a computer receives a malware, the malware will be installed, beginning its malicious activity as a bot. When the malware in the trap computer attempts connection with the C&C server, it has to query a local name server in the honeynet. This query will be forwarded to the domain name system. This activity of querying itself may be regarded as malicious activity from malware. The local domain name system will receive the URL of a C&C server included in the request. This particular domain name is added to a list of bot C&C servers.

Upon obtaining the domain names of the URL of C&C servers, this information will be shared by the relevant administration agents responsible for operating the ISP's DNS. The transfer can be performed by using the DNS RR (resource record) update. Generally, a DNS RR record contains a set of domain names and their relevant real IP. In this DNS RR record, the real IP addresses of the C&C servers are changed to the IP addresses of the sinkhole systems in KISA. Once local ISPs complete the update of their own domain name system, bot-infected computers never succeed in completing the connection with a C&C server.

8.2 Operation of the DNS sinkhole

When establishing connection with a C&C server, a bot-infected computer makes a DNS query for an ISP's DNS system. Note, however, that the domain system contains the IP address of the sinkhole system instead of the real IP address of the C&C server.

Figure 3 describes the operation of the DNS sinkhole scheme as follows: When a newly bot-infected computer tries to make a connection with its C&C, it queries the ISP's DNS server; the DNS server then returns the IP address of a DNS sinkhole system, not the IP address of a C&C server.

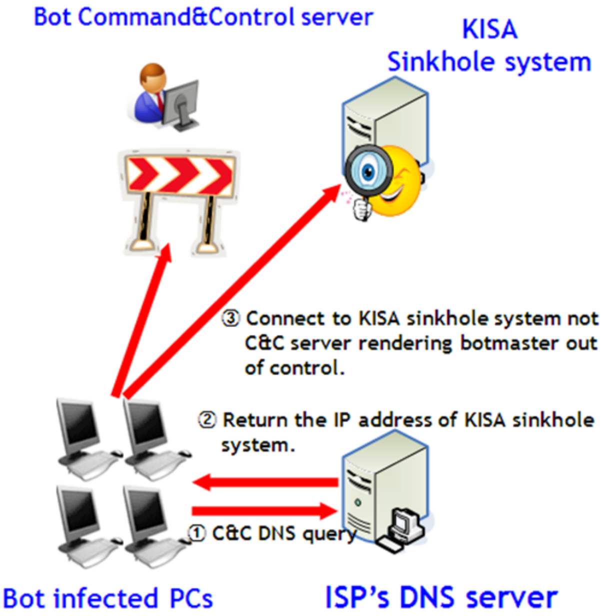
Bot Command&Control server
KISA
Sinkhole system
③ Connect to KISA sinkhole system not C&C server rendering botmaster out of control.
② Return the IP address of KISA sinkhole system.
① C&C DNS query
Bot infected PCs
ISP's DNS server

Figure 3 – DNS sinkhole operation

As a consequence, this connection of a bot-infected computer with a C&C server never succeeds, i.e., communication is blocked.

8.3 Effectiveness of the DNS sinkhole

Figure 4 describes the effectiveness of the DNS sinkhole scheme. Before employing the DNS sinkhole, the infected bot systems are connected with the C&C server, which in turn is controlled by the botmaster to launch the DDoS attacks to the target website. After employing the DNS sinkhole scheme, however, the DNS RR originating with the bot-infected computer is modified so that communication with the DNS server may be redirected to the sinkhole server instead of its C&C server. This way, the botmaster never gets a chance to control a group of bot-infected computers; thus keeping them dormant or inactive.

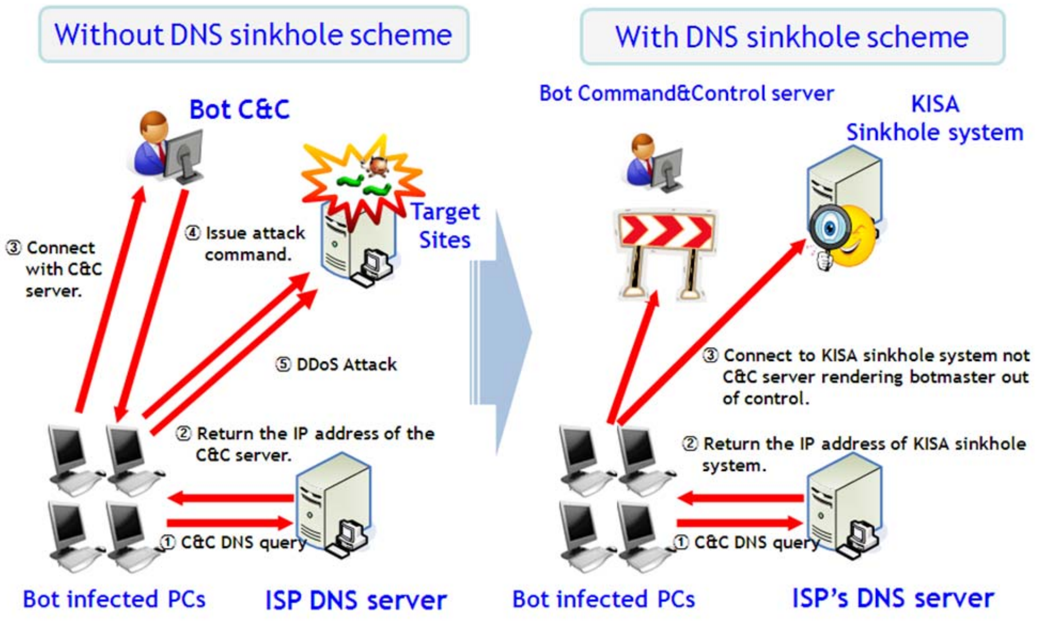
Without DNS sinkhole scheme
Bot C&C
Target Sites
③ Connect with C&C server.
④ Issue attack command.
⑤ DDoS Attack
② Return the IP address of the C&C server.
① C&C DNS query
Bot infected PCs
ISP DNS server
With DNS sinkhole scheme
Bot Command&Control server
KISA Sinkhole system
③ Connect to KISA sinkhole system not C&C server rendering botmaster out of control.
② Return the IP address of KISA sinkhole system.
① C&C DNS query
Bot infected PCs
ISP's DNS server

Figure 4 – Effectiveness of the DNS sinkhole scheme

Bibliography

[b-CCC] Cyber Clean Center, https://www.ccc.go.jp/en_ccc/.

[b-KISA] Korea Internet & Security Agency, http://www.kisa.or.kr/eng/main.jsp.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011