Global Information Assurance Certification Paper

The Search for "Kozirog"

GIAC Certified Incident Handler Course
Attack Analysis and Response

Greg A. Weaver

TABLE OF CONTENTS

Executive Summary:

Incident handling for any major organization poses significant and complicated management challenges. If all of the incident handlers assets and resources are centrally located, crisis response and investigation can be relatively straightforward. Appropriately documented and resourced, the incident handler can quickly get to the scene of the potential intrusion and respond to the crisis with all available assets in hand. Additionally, the incident handler can rely on easy access to any additional tools, resources, or other expert personnel to augment his capabilities or shortcomings. This response would be the ideal solution for any organization, however all to often; this scenario is not the norm.

As a manager for a global response CERT, the challenges that face the individual incident handlers can quickly overwhelm the incident handler or the CERT response team capabilities, especially if multiple events are occurring. The Incident Handler at this level requires a unique skill set that not only taxes his own capabilities, but those of his team. He must be able to draw upon his own technical expertise, manage the crime scene remotely and rely on the capabilities of system and network administrators that possess unknown or questionable skills and resources. The incident handler at this level cannot physically go to the crime scene and document the connectivity, resources available, or the accessibility of the suspect system to physical or remote access. Additionally, the incident handler cannot assume that the individual with whom he must rely upon has the technical capabilities or more importantly, the integrity and honesty to approach the situation with the same level of dedication that an incident handler on site would possess.

Incident handling at the global response level must rely on a tiered and coordinated response plan. This plan, as a minimum, includes the resources of local law enforcement or investigative agencies, competent and trustworthy system administrators that have been identified either from previous incident handling or established through direct personal contacts and finally, technical expertise that understands the importance of forensic evidence gathering.

Incident handlers have on hand documented emergency action plans and procedures that can be quickly accessed and passed to subordinate agencies for implementation. These standard-operating procedures, widely disseminated, allow all individuals to quickly ascertain the immediate CERT requirements and the long-range goals of reestablishing the integrity of the compromised network. The incident handler of this global CERT response team follows standard commercial “best practices”, however the environment of this CERT team encompasses more than “correcting and reconnecting” the compromised system. The CERT team of this organization is acutely cognizant that every suspected event or potential intrusion could result in national level criminal investigations, potential terrorism, or nation-state sponsored intelligence gathering entities. This

CERT team has the added benefit of enforceable policies and regulations that set regulatory requirements, and emphasis from CEO level personnel that supports their efforts.

All of this however, is quickly circumvented by one careless user who prefers to ignore the regulatory requirements and opens an email attachment that was sent to him anonymously.

Preparation:

The events that led up to the unfortunate incident could have been easily prevented. The network on which this user had access permission had clearly published access restrictions and warning banners presented at the user's login. Access to the network gave implicit consent to monitoring of all activities. System administrators have standard configurations and the use of anti-virus software is a requirement on all systems capable of having it installed.

All of the networks associated in the incident are monitored by an Intrusion Detection System (Real Secure). These can be augmented as necessary, by the capabilities of the CERT's intrusion detection section and the utilization of more specialized intrusion detection capabilities and tools. The utilization of the intrusion detection section's capabilities is strictly monitored and utilized in mission critical networks in support of criminal or investigative situations.

The CERT is a manned 24X7 operation. The CERT's current standard response to network security events and intrusions is to isolate the suspect system, evaluate the extent of the intrusion, eradicate the intruder, rebuild the compromised system(s), evaluate the potential threat to the remainder of the network and correct other identified vulnerabilities. This standardized response ensures that all incident handlers apply the appropriate response procedures event after event. Training in these procedures is critical to ensure the timely and accurate response of CERT team members. This response is a pre-coordinated effort between the CERT team, law enforcement investigators, intelligence investigators, and CEO level personnel.

The authority to investigate an intrusion is a shared responsibility, and the CERT routinely defers to the law enforcement investigators as part of the shared response. The CERT teams initial response is concentrated in forensic preservation of the evidence. This coordination is critical in an effort to ensure that all evidence that is potentially available is preserved for any future criminal prosecution. Additionally, the CERT team coordinates and interacts with other similar CERT organizations with similar missions and security criteria.

In retrospect, users that circumvent security policies and procedures often times allow this CERT team the capability and authority to examine the entire network structure in detail and provide a more comprehensive response plan. Unlike commercially structured corporations whereas the CERT can take more pro-active actions in actively scanning internal hosts and identifying associated vulnerabilities, this CERT must normally rely on requests for these types of activities from the leadership of the organizations. Security violations or compromised systems provide the CERT the opportunity to fully ascertain the potential for other security vulnerabilities, identify additional suspect systems, and recommend corrective requirements. The capability of the CERT to dedicate

the necessary resources for these corrective actions, however, must be planned in advance and exercised frequently. The difficulty for the CERT managers in these roles is focused on making a competent decision as to when these limited resources are to be utilized.

Identification:

Identification of a potentially compromised system can be difficult, but a proactive response plan can be instrumental in responding to the initial intrusion and identifying similar exploited systems. In this scenario, the CERT team received notification from an email exchange of personnel. The CERT teams standard procedures include the monitoring and review of intrusion detection, firewall, system, and router logs. Additionally, analysis is conducted over greater periods of time focusing on activity that initially is unremarkable for a given day, but poses a potential threat over several weeks or months.

The CERT received notification encompassing an email exchange between a supporting CERT and an educational facility. This email identified two internal host suspected of attempted connection events. The following information was provided to the CERT team as the source of the initial investigation. Fortunately, as with many notifications, the CERT was notified by a system administrator that was aware of legitimate traffic for his network and suspicious of the source of this incident.

- ----- ORIGINAL MESSAGE FROM "EDUCATIONAL FACILITY" -------

CERT POC-

(I've cc'd "network administrator", just to keep her in the loop)

I thought I had a great many .xxx hosts for you, but it was only 2 out of the 183 hosts we caught trying to access xxxxx.xxx.edu:

Host	IP Address	# flows since midnight
ws136203.yyy.yyy.yyy	aaa.aaa.aaa.203	3400
ws136192.yyy.yyy.yyy	aaa.aaa.aaa.292	3284

(Where a flow is a completed TCP connection)

We can assume these hosts are infected with the virus.
Their were no .xxx sites observed during this time, between midnight and ~2pm today.
These are hosts attempting to talk to xxx.xxx.EDU as a result of a virus. (Sidebar: xxxx.xxx.net maps to xxx.xxx.EDU. Apparently, their DNS servers were compromised)

What we know about this virus is in the attached log entry. I called McAfee yesterday, and was unable to get more info. If you have better contacts at their lab, perhaps you can shake something loose...

We will probably end up retiring the name/address used by this host after this event is concluded.

- victim bob

Upon receipt of this information, the CERT team implemented their initial standard response plan. This process confirms that the suspected targets are active or assigned and whether to investigate the incident further. The incident handler performs a simple nslookup and whois search on the targeted IPs. The use of "ping" to confirm active hosts is prohibited across the internal internet boundaries and would be unsuccessful. Secondly, inquiries are made to contact the system administrator to verify that the sources are active. The CERT teams initial results indicated that the hosts were active and legitimate.

Of special note, the CERT team standard procedures also document the requirements for the incident handler in the event that the CERT team encounters or receives inquiries following the normal business hours of most network and system administrators. If the incident handler cannot accurately verify the targeted host as active, the CERT team will conduct a non-intrusive scan of the system to determine the operating system and system status. No scans are conducted that could potentially contaminate the potential evidence on the destination system. If the host is active, and the indicators of the information available support the potential source as being compromised, the CERT team will direct that the targeted IP address be blocked at the perimeter security routers as a precautionary security measure until the next work day or system administrator notifications are confirmed. The CERT team attempts notification of the system administrator through traditional e-mail and telephonic procedures.

Included in the forwarded email chain of message was the original text from several commercial hosts to the system administrator of the educational institution. This message also provided the incident handler with information that potentially identified the cause of the suspect traffic and other indicators that could be used to identify additional suspect systems.

The text of the mail began:

>Sent: Tuesday, December 06, 2000 5:17 PM
>To Whom It May Concern:
>
> We received this file yesterday evening. You probably are aware of it but
> if not, this is for your info. The virus identified below is apparently
> targeting one of your systems.
>
> The host being hit is registered to you at xx.xx.x.225
> (xxx.xxxx.net). The file has been sent to McAfee's AVERT labs
> (California) and AVP (Chile) for analysis.

Additional information provided in the mail identified still more useful information to the incident handler and the virus support person.

>Subject: RE: [Virus submission via avp.ch] require additional
> information regarding the DDos.Win32.Kozog virus
>
> that is NOT ZIP file - if you look at the name more attently, you'll see
> that it is "OFFER2001.ZIP many spaces EXE" file
> That is DDoS tool - by a command from remote hacker it will attack
(original text and spelling not corrected)

And finally, getting to the end of the message, the potential source of the infestations that may have occurred by email.

> >Here is the email that was sent, we detect the following
> > virus with your product: DDos.Win32.Kozog virus as an executable file within
> > the zip file.
> > Could you please give me some information on this virus, I
> > search your web site for some info on this virus with a negative result.
> > The infected file is zip and password protected (password is
> > "infected").
> > Thank you in advance.

_____

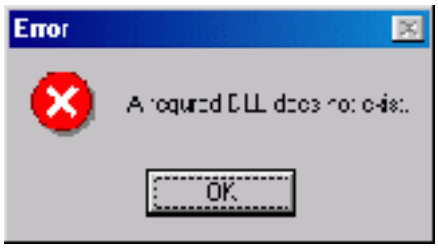
> > From: World Travel Agency Ltd. [office4@worldtravel.com]
> > Sent: November 21, 2000 5:31 PM
> > To: All tourists and vacationist
> > Subject: Celebrate the New Millenium!
> > World Travel Agency Ltd.
> > 359 BTC Drive
> > P.O. Box 134108
> > Seattle, WA 98108-23
> > USA
> >
> > Dear Sir/Madam
> > Celebrate the New Millenium! Discover the Paradise!
> > We offer the most attractive package for the New Millenium
> > celebrations you
> > have ever seen.
> > Pure nature, modern architecture and high technologies are
> > fused to create
> > the perfect resort.
> > Reasonable prises, correctness, high quality services.
> > Click on the zip-file below to see our offer!
> > Make your neighbours envy!
> >
> > Best Regards,
> > **********

_____

(original text unchanged, note the spelling and grammatical errors within the message.)

Fortunately, this incident handler had many consecutive pieces of information that would be useful for him to develop a containment plan and take action.

Infected systems also display the following text box and icon:



CONTAINMENT and ERADICATION

While awaiting the confirmation from the targeted addresses, the incident handler continues to work the incident. Initial notifications are made to the CERT team manager and agency leadership. This notification outlines the basic facts available, the actions of the incident handler, the system administrator response, and the incident handlers evaluation. Additional resources, personnel, and guidance may be identified and resourced by the manager, dependent on the nature of the information and the extent of the possible intrusion. Usually, no additional personnel assets are committed to the investigation until the system administrator can verify the intrusion.

The incident handler makes the initial notifications to the CERT law enforcement support agent. Though no intrusion has been confirmed, this step allows for the early notifications of law enforcement agencies and subsequently, notifications of their deployed investigative personnel located near the intrusion site. This step is critical in getting a qualified individual on site that has the interest of preserving criminal evidence as a priority if needed. Since the provided information suggested a virus or trojan horse program, the CERT manager tasked specialized virus personnel to begin preliminary support to the incident handler.

Contacting system administrators provide the CERT team the initial opportunity to ensure that the correct steps are taken to preserve the evidence on the system. The host was identified as a Windows NT operating system, service pack 5, with no current hot fixes installed. Additionally, the host had an anti-virus product installed; yet disabled by the user. Unfortunately, the system administrator for these systems had already started to reformat and reload the operating system prior to contacting the CERT team.

The CERT teams initial contact provided the system administrator with enough details to identify and verify the systems integrity were compromised, and he implemented his standard policy for virus infections. This overzealous system administrator's good intentions prevented the CERT from obtaining any evidence to support the traffic that was reported by the educational facility.

Additionally, he took no actions to confirm the type of virus or the actions of the individual user. The only assumptions that could be made was that an unknown virus or trojan generated the traffic, yet no other details could be gathered, effectively terminating any opportunities of the CERT to gather the necessary evidence to assist the remainder of the organization or law enforcement personnel.

The incident handler provided the system administrator of the compromised host, a templated response plan via email that outlined his specific requirements to conduct a system backup and the evidence preservation steps.

As with any incident, the CERT maximizes the opportunity to train system administrators in incident response and forensic evidence preservation. The CERT also works to ensure that there are policies and procedures in place that help prevent future occurrences. The system administrator is given detailed instructions on resources available from the CERT team that can be leveraged to assist him in securing this particular system, and the network.

The CERT teams response policy includes a comprehensive vulnerability assessment of the compromised system after it has been rebuilt. The use of commercial vulnerability assessment scanning tools such as ISS Scanner and Cybercop, and other scanning tools such as nmap and whiskers, provide for a comprehensive assessment for the administrator.

Additionally, the administrator is passed to the virus support team to help him in installing and configuring the new anti-virus detection software. This new software, configured correctly, will assist the administrator in preventing future incidents based on the user deliberately circumventing policy. An added benefit to this particular incident is that the user lost his access for the time necessary to rebuild and secure this system.

The incident handler begins a systematic review of all publicly available information concentrating on potential sources of the intrusion based on the potential exploit type, port designations, hacker methodology, and tools capable of the exploit. The CERTs incident handler teams share a common knowledge database that will aid them in future exploit identification as well. This search resulted in no new notable events or information to assist in this incident.

Although the investigation of this particular system had been abruptly halted, the incident handler continues the action plan, conducting an extensive search of internal historical databases on computer incidents for both the identified source and targeted IP addresses. This review provides the CERT team with a historical perspective, if any, of the hosts and may indicate to the CERT manager and leadership that a more proactive response may be indicated in the event that the host was identified in other incidents.

A review of compiled intrusion detection databases identified three more potential systems that may have been infected with the Denial of Service Trojan. The following shows the type of traffic that was captured.

DATE	EVENT NAME	SOURCE PORT	DEST PORT	SOURCE ADDRESS NAME	DESTINATION ADDRESS NAME
11/21/00	Port_Scan	1103	113	mm.mm.mm.164	zz.zz.zz.117
11/22/00	Port_Scan	1111	37	mm.mm.mm.164	zz.zz.zz.117

11/22/00	Port_Scan	2154	49	bbb.bbb.bbb 164	zz.zz.zz.117
11/27/00	Port_Scan	1111	7	bbb.bbb.bbb.164	xx.xx.x.225
11/27/00	Port_Scan	3436	153	bbb.bbb.bbb.164	xx.xx.x.225
11/27/00	Port_Scan	1247	163	bbb.bbb.bbb 164	xx.xx.x.225
11/28/00	Port_Scan	1124	49	bbb.bbb.bbb 164	xx.xx.x.225
11/28/00	Port_Scan	1124	49	bbb.bbb.bbb.164	xx.xx.x.225
11/29/00	Port_Scan	1116	79	bbb.bbb.bbb 164	xx.xx.x.225
11/30/00	Port_Scan	1096	59	bbb.bbb.bbb.164	xx.xx.x.225
12/4/00	Port_Scan	1210	185	bbb.bbb.bbb.164	xx.xx.x.225
12/4/00	Port_Scan	1098	77	bbb.bbb.bbb.164	xx.xx.x.225
12/6/00	Port_Scan	1116	23	bbb.bbb.bbb.164	xx.xx.x.225
12/7/00	Port_Scan	1164	113	bbb.bbb.bbb.164	xx.xx.x.225

The incident handler moves to the next phase and notifies the global operations support personnel to have the targeted IP address and the victims, blocked at the internet security routers, and log any attempts to connect to this address. This proactive measure is implemented for a set time frame to help identify potentially compromised hosts as a result of the same activity.

Logs from one of the security routers identified the following:

snipped
Nov 27 02:48:49 routerx 465940: Nov 27 12:04:25: %SEC-6-IPACCESSLOGP: list xxx denied tcp bbb.bbb.bbb.164(3775) -> xx.xx.x.225(9), 1 packet
Nov 27 02:48:53 routerx 465942: Nov 27 12:04:29: %SEC-6-IPACCESSLOGP: list xxx denied tcp 147.248.140.164(3845) -> xx.xx.x.225(79), 1 packet
Nov 27 02:48:54 routerx 465943: Nov 27 12:04:30: %SEC-6-IPACCESSLOGP: list xxx denied tcp bbb.bbb.bbb.164 (3863) -> xx.xx.x.225 (7), 1 packet
Nov 27 02:49:08 routerx 465945: Nov 27 12:04:44: %SEC-6-IPACCESSLOGP: list xxx denied tcp bbb.bbb.bbb.164 (3989) -> xx.xx.x.225 (7), 1 packet
Nov 27 02:49:11 routerx 465946: Nov 27 12:04:47: %SEC-6-IPACCESSLOGP: list xxx denied tcp bbb.bbb.bbb.164 (4045) -> xx.xx.x.225 (9), 1 packet
Nov 27 02:49:17 routerx 465947: Nov 27 12:04:52: %SEC-6-IPACCESSLOGP: list xxx denied tcp bbb.bbb.bbb.164 (4104) -> xx.xx.x.225 (19), 1 packet
Events snipped…..

These events continued throughout the day with over 8,300 connection attempts from the source IP address to the targeted IP address as identified in the original message provided by the respective CERT. Of note here is that the logs reflect traffic on the 27th of November, nine days before the targeted educational site notified the CERT. The security routers are configured to block

outbound traffic on ports 7, 9, 19, and 79. The CERT investigation determined that the logs of this security router were not being reviewed on a regular basis, as this traffic continued unhindered since the compromised host was infected. Recommendations were made to enforce a more strict review policy for the security logs of the operations center and investigate and report suspicious activity.

The virus incident handler continued research to identify additional information on the suspected Trojan. The information available verified the "virus" was indeed a distributed denial of service tool and not a virus. The tool was sent as outlined above as an email, and the available forensics from the commercial lab provided the following details:

> The attached file intends to be displayed as ZIP archive, but it is Windows EXE file with the name:
> "OFFER2001.ZIP [many spaces] .EXE"
> This is trojan's "installer" that will affect computer if it is run. Because of "[spaces]" trick it will be displayed as .ZIP file in many cases, and that can tempt a user to open it. When the EXE file (trojan's installer) is run, it extracts from itself two more executable files and copies them to Windows system director with names:
> MRE.DLL
> SOUNDV.EXE
> Under Win9x and WinNT these files are registered then in auto-run sections in different ways:
> Under WinNT the trojan registers SOUNDV.EXE file in system registry:
> SOFTWARE\Microsoft\Windows\CurrentVersion\Run soundv.exe
> Under Win9x the DLL file is registered in SYSTEM.INI file in [boot] section:
> drivers=mre.dll
> The trojan then displays fake error message:
> Error
> A requred DLL does not exist.
> (original spelling from a trojan's messagebox).
>
> The SOUNDV.EXE file is the DoS trojan itself. The MRE.DLL is a small program that just executes the SOUNDV.EXE on each run. As a result under both Win9x and WinNT the SOUNDV.EXE component will be activated.
> When this file is run (on next Windows restart) it will stay active as hidden application (service), then it enables auto-dial option in Internet settings, then performs DoS attack on the Bulgarian server "kozirog.netissat.net". [Analysis: Kaspersky Labs and F-Secure Teams; November 2000]

The incident handler was provided the information for the case as supporting evidence. Two of the three remaining system administrators were contacted and apprised of the events leading up to the compromises and their required actions for remediation. Since they were unaware of the intrusions, the incident handler was able to provide the necessary details and steps to recover. The final system was geographically close to the CERT team, and the opportunity to acquire the appropriate logs, information, and or the system was more realistic.

Coincidentally, there was a criminal investigator already at the site of the fourth system compromised. The investigator was gathering information and evidence from another system as part of another investigation. The incident handler contacted the investigator and requested that he obtain a complete backup of the system for forensics review. The investigator was given the details of the intrusion to date, and the points of contact for the system administrator. The investigator, with legal authority, arrived on site, and proceeded to process the crime scene. Since this investigator has extensive experience in computer evidence gathering, the incident handler was assured that the evidence gathered would be complete and accurate.

Typically the hard drive of any compromised system is removed and forwarded to the CERT and the law enforcement investigators for review and detailed analysis. Since this intrusion focused entirely on the actions of the user, the agent conducted a backup of the system to disk and a detailed review of the logs available on the system. The investigator used "ghost" and wrote to a CD. This evidence was verified as complete and the system administrator was instructed to remove the system from the network and begin the rebuilding process. Additionally, the user was counseled on his actions and the threats imposed by opening unsolicited email attachments.

The criminal investigator and the CERT team incident handler conducted a combined research and review effort. The incident handlers keyed on a review of the initial indicators of the information found on the kozirog denial of service tool.

A search for the mre.dll file confirmed the following strings:

```
USER
mre.DLL
]MYY
Portions Copyright (c) 1983,92 Borland
```

And from other strings from the soundv.exe file verified that this was the kozirog Trojan:

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
EnableAutodial
Ph~f
f=3't
f=A't     f
kozirog.netissat.net
```

The final verifications were made from the access logs obtained from the workstation. These provided the time of the actual compromise and times and date of subsequent events. The logs have been significantly reduced as there were multiple attempts reflected during each minute of time in the logs.

TELNET: Session	11/22/2000 16:52
TELNET: Session	11/22/2000 16:51
TELNET: Session	11/22/2000 16:51
<SNIPPED LOG>	
TELNET: Session	11/22/2000 7:12
TELNET: Session	11/22/2000 7:12
TELNET: Session	11/22/2000 7:11
TELNET: Session	11/22/2000 7:11
Total Accesses : 10264 (11/22/00)	

The review of the available data indicated the system was compromised on the morning of the 22 of November, less than one day after the initial release of the infected mail message. Additionally, the logs reflected the times the system was turned off during the vacation periods and the weekend. The logs have been reordered for ease of reading.

TELNET: Session	11/27/2000 7:09
TELNET: Session	11/27/2000 16:27
TELNET: Session	11/28/2000 7:13
TELNET: Session	11/28/2000 15:13
TELNET: Session	11/29/2000 7:09
TELNET: Session	11/29/2000 14:36
TELNET: Session	11/30/2000 7:13
TELNET: Session	11/30/2000 13:05
TELNET: Session	12/04/2000 9:47
TELNET: Session	12/04/2000 15:10
TELNET: Session	12/06/2000 13:05
TELNET: Session	12/06/2000 13:52
TELNET: Session	12/07/2000 7:01
TELNET: Session	12/07/2000 10:19
Total Accesses : 40882	

(The final connection identified when the investigator disconnected the system.)

Interestingly enough, no one identified the enormous amount of outbound traffic from the system or the performance hit that the system must have been undergoing. Evidence within the access logs indicated that the user accessed the “free offer” through a commercial mail account and opened the attachment. The mail did not arrive in his work email address. The system did have an anti-virus product, however it was disabled.

Before the investigator departed the scene, the system administrator was tasked to notify the CERT for additional information. Since the criminal

investigator collected the evidence from the crime scene, the chain of custody for this incident was already verified. The initial intent for this investigation was to gather the evidence, and restore the system. The investigators' initial interview process indicated the user was the cause of the event, and unless the collected evidence proved otherwise, would not be prosecuted in court. As before, the administrator was provided updated information and coordination to conduct a vulnerability scan once the compromised host was rebuilt.

RECOVERY

The incident handler, in conjunction with the system administrator and the network operations center personnel conducted a collaborative effort to continue to identify any additional host that may become infected. Fortunately, no additional hosts were identified with this Trojan installation. All four systems that were initially compromised were scanned with ISS and nmap and the results were provided to the system administrator for corrective actions.

The operations center maintained the IP block on each of the systems until the CERT verified that all corrective actions were taken. The CERT also verified the installation of an anti-virus vendor product with current updates and operating system updates.

The network operations center continued to block of the destination host for a period of seven days with negative results.

FOLLOW-UP

The incident handler, in conjunction with the investigator, conducted a risk assessment with the leadership of the CERT to ascertain the threat posed by this denial of service Trojan and the impact to the networks. Guidance provided the CERT manager directed that the CERT would continue to monitor the intrusion detection and router security logs for the next 24 hours to determine the immediate threat. The virus section would work with the vendors to obtain and disseminate the appropriate definition updates to their products. The destination address was already aware of the attack and had taken steps to reassign the IP of the host associated in the attack, thereby preventing any additional successful attacks.

By blocking the destination IP address of the educational facility the configuration of the security routers prevented any additional systems from actively attacking, and logging provided the capability to actively identify additional systems. Logs revealed no additional systems compromised with this attack.

During the follow up phase of the intrusion and investigation the CERT identified several issues that would be addressed in the formal after actions reports and the subsequent messages that would be released to the general community.

The initial alert message was structured to re-emphasized the importance of an active and installed anti-virus products, and provided the details of the Trojan and the immediate actions that could be taken to circumvent the threat. Fortunately, the vendor provided solution would become available and distributed with the message.

Though there was no immediate solution and no protection was offered at the time by the current anti-virus software, user training and awareness of the opportunities available through “unsolicited” or “free” emails would have helped prevent an intrusion based upon the dangers associated and a recommendation of additional user training should be conducted on those compromised networks.

The CERT also addressed the lack of training and active monitoring of suspicious traffic with the focus on detailed and periodic reviews of router security logs and the timely notification procedures. Had the logs been reviewed more accurately, the suspicious traffic would have been identified as either legitimate or not, much earlier in the intrusion.

An internal review of CERT procedures and policies revealed that the CERT response was appropriate and that the follow-on scheduling of the system vulnerability assessments would need to be conducted. Closing of the incident

can only be accomplished once all involved personnel within the CERT and investigative team have provided their portion of the investigation, and the manager reviews the data for any additional actions that may be needed.

References:

Kaspersky Lab http://www.kaspersky.com

F-Secure: http://www.europe.f-secure.com/v-descs/kozog.shtml

NAI: http://vil.nai.com/villib/dispVirus.asp?virus_k=98916