



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

March 30, 2007

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

2007-008

DATE ISSUED:

March 30, 2007

SUBJECT:

Microsoft Internet Explorer 7 Phishing E-mail

Several states reported receiving emails asking users to download Internet Explorer 7 by clicking on a link embedded in the e-mail. If the user follows the instructions, their computer will be infected with malware. This information Bulletin discusses the characteristics of the e-mail in more detail.

OVERVIEW:

The e-mail appears to originate from admin@microsoft.com asking users to download Internet Explorer 7 contains a graphic of IE 7 and links to various URLs. Clicking on the picture results in a file, IE7.0.exe, being downloaded to the user's machine. Note that currently this file does not auto-execute so at this point the users computer is not yet compromised.

However, if IE7.0.exe is executed by the user, the malware will compromise their computer by copying IE7.0.exe to the user's TEMP directory as 'winlogon.exe' after which it deletes the original IE7.0.exe file. Based on our analysis of the malware, it will then create batch files that it uses to create a registry key:

“HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Firewall auto setup: winlogon.exe” which will auto-execute when the user logs in.

The following registry keys are also created:

HKCU\Software\Microsoft\Internet Explorer\Desktop\host: 66.232.126.138

HKCU\Software\Microsoft\Internet Explorer\Desktop\id: 66232126138

HKCU\Software\Microsoft\Internet Explorer\Security\host: 66.232.126.138.

After a period of time the program will lookup several domain names and try to connect to the SMTP port for those domains. It also attempts to connect to a web server at 72.232.49.214 and reports whether the SMTP connection was successful.

Image sample included in Phishing Email:



RECOMMENDATIONS:

- Advise staff of this situation and inform them not to click on the links in the email.
- Block downloads of MIME-types associated with executable content at the network border.
- Review your security device logs from traffic to the IP address above. Any of your hosts that have attempted connections to these IP addresses should be investigated to determine if they are infected.
- Apply egress filtering on your firewalls. Egress filtering is best explained as a rule set that allows or denies network traffic which is in an out-bound direction. It prevents packets that contain invalid or incorrect addresses from leaving your site, and prevents communications to unauthorized or questionable TCP and UDP ports. Egress filtering makes it harder for attackers or malware to use your system as a relay site, and similarly careful port filtering can render many backdoors ineffective as well. Blocking inappropriate outbound access is critical to containing an infection once a compromise has occurred. Restricting outbound traffic to necessary business functions will make it more difficult for a worm or botnet to use a compromised system to further its propagation.
- Employ outbound proxy services. Some bot and worm variants do not make allowances for the use of proxy servers, thereby making them unable to contact hosts outside of the current network.

In the event that a host or hosts becomes compromised on your network, follow these recommended procedures:

Alaska State Government:

- Disconnect infected host(s) from the network.
- Once an infected host is removed from the network, perform forensics analysis in order to identify the infection. If the malware cannot be identified, you should

provide a sample of the infection files to the State Security Office for further analysis.

- DBAN device prior to reconnecting to any State Government Network.

Non-Government:

- Disconnect infected host(s) from the network.
- Once an infected host is removed from the network, perform forensics in order to identify the infection. If the malware cannot be identified, you should provide a sample of the infection files to the anti-virus vendors for analysis. If the malware has been identified, or when the vendor provides a new signature for removal purposes, apply this to the infected hosts and verify removal of the malware.

File Removal for known malware files:

(Please note that other files may be infected that have yet to be identified.)

- Delete 'winlogon.exe' and remove the registry keys:

HKLU\Software\Microsoft\Windows\CurrentVersion\Run\Firewall auto setup
HKCU\Software\Microsoft\Internet Explorer\Desktop\host: 66.232.126.138
HKCU\Software\Microsoft\Internet Explorer\Desktop\id: 66232126138
HKCU\Software\Microsoft\Internet Explorer\Security\host: 66.232.126.138

If multiple infections occur:

- Shutdown the network segment that the infected hosts reside on. This restricts propagation to other hosts on that segment.
- Provide filters for the network traffic in order to isolate and identify how this infection is spreading and which hosts are infected.
- Monitor all network traffic in order to address possible multifaceted attacks.
- Once an infected host is removed from the network, perform forensics in order to identify the infection. If the malware cannot be identified, you should provide a sample of the infection files to the anti-virus vendors for analysis. If the malware has been identified, or when the vendor provides a new signature for removal purposes, apply this to the infected hosts and verify removal of the malware.

REFERENCES:

Dark Reading:

http://www.darkreading.com/document.asp?doc_id=107732

SANS:

<http://isc.incidents.org/diary.html?storyid=2537>

The Register:

http://www.theregister.co.uk/2006/10/18/hack_site_spoofs_ie7_download/