Bypassing Personal Firewall (Zone Alarm Pro)

By Tr0y (a.k.a Debasis Mohanty)
28th Sep, 2005

Impact:
Circumvention of Zone Alarm Pro (Personal Firewall) Program Control Protection

Description:
While I was testing desktop based firewalls (here it is Zone Alarm Pro) with the firewall evasion kit developed by me, I found that a very old flaw still exists in many latest versions of desktop based firewalls. It is possible for a malicious program to bypass a desktop based firewall by using DDE-IPC (Direct Data Exchange – Interprocess Communications) which enables an un-trusted program to communicate with the attacker or access internet via other trusted programs (Ex: Internet Explorer). This flaw is known since before year 2003.

As per a post by Te Smith (Sr. Director, Corporate Communications, Zone Labs), this issue is resolved in higher version Zone Alarm Pro having Advanced Program Control feature. (Ref # http://seclists.org/lists/bugtraq/2003/Jul/0000.html) However, I find that this issue still exists in higher versions of Zone Alarm Pro and might also exist in other desktop based firewalls.

I didn't find any good PoC around, so I thought of writing a PoC which can demonstrate and explain how an un-trusted program can access internet or establish connection with the attacker via other trusted programs by leveraging over the DDE-IPC design flaw.

Proof-of-Concept
The latest version of Zone Alarm Pro has been installed for this test. This PoC will demonstrate how an un-trusted program can access internet or send victim's information to the attacker by using other trusted programs in the system (Ex: Internet Explorer). The information can be sent to the malicious site by injecting victim's information via Internet Explorer "http" requests.

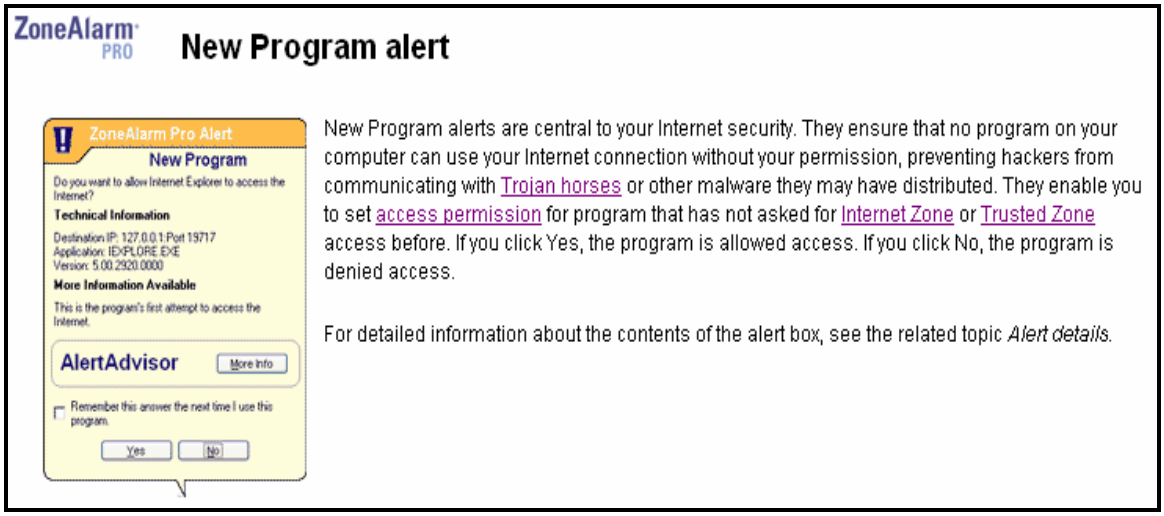
Note: Here it is assumed that Internet Explorer is one among those trusted program in the Zone Alarm program / access control list and has the default setting as "Allow".

The malicious program can communicate with the server using the following Win32 API:

```
void accessinet( char * pszURL )
{
      ShellExecute(NULL, "open", pszURL, NULL, NULL, SW_SHOWNORMAL);
}
```

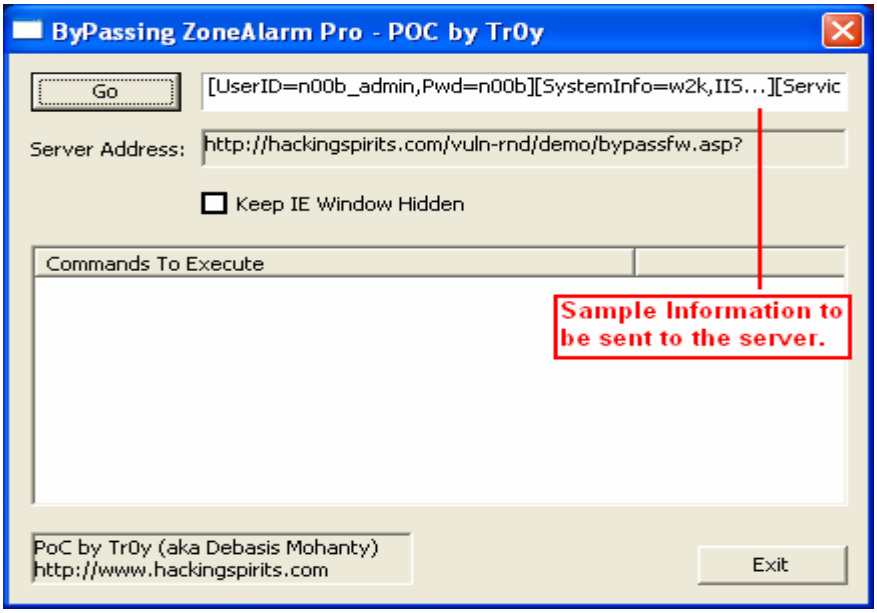
This PoC will try to prove the statement in the screenshot (refer **Screenshot 1**) wrong by demonstrating the hack.

Screenshot 1: Screenshot taken from ZoneAlarm Pro help file



- ☑ Step 1: Run "zabypass.exe"
- ☑ Step 2: The sample information in the text box is meant to be sent to the to the attacker's site. If you want to change the information in the text box then feel free to do that (Note: Only the text which appears in the text box will be sent to the server and no information is logged).

Screenshot 2: zabypass.exe showing the sample information in the text box to be sent to the server



☑ Step 3: Click on "GO" button to send the information to the server.

☑ Step 4: On successful execution, Internet Explorer (or the default browser) will be open up and will try to access the attacker's (here it is my site…..For GOD sake don't think I am attacking you, it is just a demo ;o) without getting blocked by Zone Alarm (refer **Screenshot 3** for details). The firewall will not prevent it as Internet Explorer is a trusted program and will be allowed to access the any site. Here the victim's information can be sent to the server using GET / POST method.

Screenshot 3: Demo site displaying the victim's information received by it from zabypass.exe

Solution:

- **For Users:** Upgrade to the latest version of Zone Alarm (Internet Security Suite) prevent against such attacks. Believe me it's an amazing product, I might need more time to break it ;o).

- **For Firewall Vendors:** Unfortunately there are still many desktop based firewalls which are unable to prevent such attack. The Personal Firewall should be designed such that it checks for the DDE-IPC (Direct Data Exchange – Interprocess Communications) protocol and also monitors for un-authorized attempt to access internet via other process by monitoring the parent & child processes. Hooks should be implemented to identify processes issuing "ShellExecute" or "CreateProcess" and then prevent if there is possibility of breach.

I have listed few FAQs at the end for the readers to clear the doubts (if any). Although I try to reply all valid questions but sometimes it becomes an overhead. So just to save a bit of internet traffic kindly refer the FAQ section and lets not contribute towards those 1 million mails just sent ;o). I shall only reply to those queries which are not clear in this write-up or doesn't appear in the FAQ section.

FAQ (Frequently Asked Questions)

□ Some Weird Questions

a. ***Is this a Window's vulnerability?***
Well you can say YES and NO as well.

"YES" in the sense, the DDE-IPC message exchange is flawed by design. Most often this is exploited by many malicious programs.

"NO" because this PoC is created to demonstrate the inability of personal firewalls to prevent such attacks. Here the exploit is more focused towards demonstrating a firewall hack. Have this answer on high priority in this write-up.

b. ***Is this a fully functional Trojan? Can I have a personal copy of it? Trust me, I will only use it for education purpose… blah blah bala …***
Weird!! For GOD sake this is just a demo copy and not a fully functional Trojan. All the steps are transparent and no information is logged during the demo.

□ Other Questions

a. ***What are the other ways for such attacks?***
There are many other ways of achieving the same result. For Example, instead of "ShellExecute" one can also use "CreateProcess" API to achieve similar result. COM can also be used to achieve similar result.

b. ***How this program has been coded? Can I have the source code of it?***
This program has been coded in pure "C" using VC++ editor. The code is pretty simple and has already been mentioned above. The entire code can't be shared as I don't want to be a registered member in the FBI's or Micro$oft's database for promoting worms & Trojans creations ;o).

c. ***What is the idea behind sharing such information as this can also be used for sophisticated worms?***
The idea behind sharing such information is to keep the security community and the common users aware of such threats. The security community / developers will find this information useful and will try to patch their products to prevent against such attacks.

I am aware that already this method is being used by few malicious programs although they not so well known. Imagine if this issue is not patched and the personal firewall developers keep quite on such issues…..so who will suffer?? Yeah, all common users who blindly rely on such firewalls.

Feel free to mail me your feedbacks, comments, flames etc etc ….:

Tr0y (aka Debasis Mohanty)
debasis@hackingspirits.com

------ + ------
www.hackingspirits.com
------ + ------