



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

The Inside-Out Firewall Vulnerability

Richard Hammer – hammer@lanl.gov

My subnet is located behind 2 firewalls so I don't worry about a lot of the dangers that Network Administrators directly exposed to the internet worry about. The institutional firewall limits incoming connections and our firewall limits them even more as well as most outgoing ports. My policy has been to not open a port in either direction unless there is a very good programmatic reason. Scanning my network for known vulnerabilities and password sniffing from the outside is almost impossible. In the past I had pondered the concept of hackers having our clients connecting out to sites, but dismissed it as unlikely. I was actually feeling pretty safe until the PrettyPark Trojan/Worm visited a month ago. In this paper I will walk you through my PrettyPark experience and discuss the possibility of hackers targeting your systems from the inside of your firewall.

PrettyPark

A full description of PrettyPark can be found at the following sites:

<http://www.symantec.com/avcenter/venc/data/pretypark.worm.html>

&

<http://vil.nai.com/vil/wm98500.asp>

This was the first time that we had a known instance where one of our machines was infected with a Trojan that actually tried to make connections out of our firewalls. We were fortunate to have tcp port 6667 (out bound) closed at our firewall. I played around with the infected machine and actually opened our outgoing firewall port 6667 for about 1 minute and was able to capture the infected machine connecting to IRC sites. Listed below is a screen capture from SessionWall3 showing a successful connection:

```
Client IP = 172.16.164.60
Server IP = 207.152.95.10
Client physical address = 00:A0:24:D5:B2:4F
Server physical address = 00:A4:C0:91:D2:9C
Client port = 4155
Server port = 6667 TCP
```

Client -> Server

NICK Fzi`Vb|

USER zl|e[c_oPWq eehg_VW :cMGNpnXT

You can get an evaluation copy of SessionWall3 at the following site:

http://www.cai.com/solutions/enterprise/etrust/intrusion_detection/

Here is a NetStat Capture of the Client trying to connect when the outgoing port is closed.

The screenshot shows the X-NetStat application window. The main window displays a table of active connections. The table has columns for #, Proto, Local Port, Remote Addr, Remote Port, and Status. The connections are as follows:

#	Proto	Local Port	Remote Addr	Remote Port	Status
1	TCP	0	MUSTANG	0	LISTENING
2	TCP	0	MUSTANG	0	LISTENING
3	TCP	5679	MUSTANG	0	LISTENING
4	TCP	1401	MUSTANG	0	LISTENING
5	TCP	1401	banana.irc.easynet.net	6667	SYN_SENT
6	TCP	137	MUSTANG	0	LISTENING
7	TCP	138	MUSTANG	0	LISTENING
8	TCP	nbssession	MUSTANG	0	LISTENING
9	UDP	nbname	*	*	*
10	UDP	nbdatag...	*	*	*

Below the table, there are buttons for 'Get Connections', 'Tray', 'About', and 'Close'. There are also checkboxes for 'Numeric format', 'All connections' (checked), and 'Show time passed in tray'. The status bar shows 'Done.', 'Last update: 00:00:17', and 'Elapsed: 1.245 s'.

An 'Connection Info' dialog box is open, showing details for the connection to banana.irc.easynet.net:

- Protocol: TCP
- Local Port: 1401
- Remote Address: banana.irc.easynet.net
- Remote port: 6667
- Connection status: SYN_SENT
- Message: Actively trying to establish connection.

The dialog box has an 'OK' button at the bottom.

In a little over a minute the infected machine connected to 3 of the 8 known IRC sites that

PrettyPark makes connections to. Here is a listing from my firewall showing one of the connections:

```
Mar 30 16:34:56 2000 f_rgeneric_tcppproxy a_server t_nettraffic p_major
pid: 1878 ruid: 2115 euid: 2115 pgid: 200 fid: 2000001 cmd: 'tcpgsp'
domain: RGnx edomain: RGnx srcip: 172.16.164.60 srcport: 4155 srcregion: NIS6A
dstip: 207.152.95.10 dstport: 6667 dstregion: BLUE-YELLOW protocol: 6
service_name: Internet Relay Chat acl_id: outgoing rules:SERVICE:0 result: 1
encrypted: 0 netsessid: 38e3e4a000066129
```

```
Mar 30 16:34:56 2000 f_rgeneric_tcppproxy a_server t_nettraffic p_major
pid: 1878 ruid: 2115 euid: 2115 pgid: 200 fid: 2000001 cmd: 'tcpgsp'
domain: RGnx edomain: RGnx srcip: 172.16.164.60 srcport: 4155 srcregion: NIS6A
dstip: 207.152.95.10 dstport: 6667 dstregion: BLUE-YELLOW protocol: 6
bytes_client_written: 0 bytes_server_written: 51
service_name: Internet Relay Chat reason: closing connection
netsessid: 38e3e4a000066129
```

According to Norton and McAfee, PrettyPark will send info to these sites to stay connected and will retrieve any commands received from the IRC channel. I did not allow this machine to stay connected long enough to get some sniffer output of someone sending commands to our infected machine. I noticed that PrettyPark cycles through the 8 sites quit rapidly. When one fails to connect it tries the next site almost immediately.

The user of the infected machine was pretty good about updating his virus definition files. He was using McAfee Viruscan with 2/23/2000 dat files. The time stamp on FILES32.VXD was 3/1/2000 and this version of the virus definition files did not detect PrettyPark. A week later I installed Computer Associate's SessionWall3 Intrusion/Virus detection program. SessionWall3 is a pretty good, easy to use program for scanning your network. SessionWall actually caught two other cases of PrettyPark entering our network. One evening I cleared the SessionWall scanner and noticed IRC connect attempts to a site that rang a bell in my brain (banana.irc.easynet.net:6667). I was lucky that I had cleaned a system infected with PrettyPark and one of the sites was named banana something.

Even if you can get your users to update their virus protection your machines are vulnerable to this type of attack until the dat files include the Trojan signature. Mass distributed worms like PrettyPark will always be relatively easy to detect and clean. Writers of this type of Trojan will not have our machines connect to machines that can be traced to them. Only opening outgoing ports that are required for business will stop most of these mass distributed Trojans.

Scary Stuff

Selective targeting of my subnet is the vulnerability that I worry about the most right now. PrettyPark tells us a lot about how to do these things:

- 1) Deliver the code to the target.
- 2) Execute the code
- 3) Create outgoing connection to hacker's machine.
- 4) Get the information
- 5) Trash/disable the infected system and cover tracks.

I have been thinking about selective targeting for some time now and have discussed it recently with a fellow colleague. It seems far fetched but I found a paper on the internet, "Placing Backdoors Through Firewalls" by van Hauser / [THC] - The Hacker's Choice, that gives instruction, lists dangers, and supplies scripts to do exactly what I listed above.

I can think of two low tech ways to deliver and execute the code. One would be to have an insider install the code, another would be to use e-mail and let the double click syndrome install the code. My experience tells me that the average user will double click on anything that looks funny, interesting, business related, or comes from someone they know. I would guess that the double click syndrome is the most popular way to execute malicious code. Making the outgoing connection look legitimate is important, van Hauser offers several suggestions, tunnel from Phrack 52, ssh, netcat, ack-telnet, and http (example script supplied). Once the code is executed getting data from a targeted machine looks easy. With a legitimate looking connection there is a real good chance that this kind of attack will not even be noticed. Virus protection will not work unless the hacker uses a known piece of malicious code and since the traffic will look legitimate so our network scanners won't detect it. The smart hacker will then get the info and start covering his/her tracks. Deleting the malicious code and corrupting a couple system files will look like just another system failure.

Possible Solutions

- 1) Closing unneeded outgoing ports. Better have strong support before you do this, because users will start to whine when they can't chat with their aol buddies during work hours.

Sites with Good port lists:

<http://home2.freegates.be/bchicken/index2.html>

<http://www.dark-e.com/lowfi.html>

<http://www.sans.org/y2k/ports.htm>

- 2) Use Personal firewall programs, port scanners and port blockers. I use one of these at home and it works pretty well. Host based protection should be able to stop and detect these types of attacks. Getting users to accept and understand these types of solutions will be difficult since most double clickers can barely update their virus dat files.

Personal Port Scanners, Blockers and Firewalls:

<http://www.agnitum.com/products/jammer/jtour1.phtml>

<http://home2.freegates.be/bchicken/index2.html>

<http://net-security.org/various/download/>

<http://davidovv2.homestead.com/freetoolsservices.html>

<http://www.zonelabs.com/>

<http://grc.com/su-firewalls.htm>

<http://www.symantec.com/sabu/nis/>

3) Scan and delete known Viruses/Trojans/Worms at your gateway. Do not allow them to get to the double clickers of the world! I use SessionWall3 and it works pretty well for me.

http://www.cai.com/solutions/enterprise/etrust/intrusion_detection/

4) Train users NOT to DOUBLE CLICK on attachments that are not business related.

Clearly critical data should not be stored on networks that have liberal outgoing connection policies and no personal protection.

Resources

You can find van Hauser's Paper at:

<http://www.anticode.com/cgi-bin/showdsc.anticode?cat=backdoors-and-rootkits.html>

Much thanks to Richard Kandarian – He was the first person that I ever heard actually talk about selective targeting! He has other Solutions that I will not go into here!

Good Sites for information on Trojans:

<http://anti-trojan.virtualave.net/page6.html>

<http://home2.freegates.be/bchicken/index2.html>

<http://www.commodon.com/threat/threat-all.htm>

<http://www.dark-e.com/lowfi.html>

© SANS Inst.

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event