

FAX TRANSMISSION



**Office of the Legal Attache
American Consulate General
Frankfurt, Germany
Telephone #: 011 49 69 7535 3870
Fax #: 011 49 69 560 2880**

To: Herr Eismann
Landeskriminalamt
Baden Wuertemberg

Date: May 5, 2004

Fax #: 0711 5401 2418

Pages: 2, including this cover sheet.

Voice #: 0711 5401 2441

To: Herr Kreitlow
BKA
Wiesbaden

Fax #: 0611 55 15725

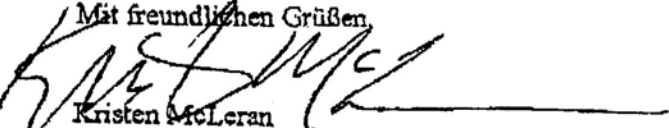
Voice #: 0611 55 15908

Dear Frank and Joern,

Attached is a short summary of the content of recent chat logs between GEMBE and a confidential informant, from Agent Mike Gordon (he did a short summary, because the logs are many pages). He can fax these to the Legat office, or email them to me on our internal email system. Let me know how urgently you need these.

Seattle advised that they can send the emails between Valve and GEMBE, but it is about 40 pages. They are sending this to the Legat Frankfurt office via our internal email system. If you want this immediately, I can fax it to you.

Mit freundlichen Grüßen,


Kristen McLeran
Assistant Legal Attaché

487

- 04/12/2004 - Microsoft Release patch concerning the LSASS Vulnerability - CAN-2003-0533
- 04/14/2004 - Comments made indicate that "PhaTTY" and "evilbyte" are working on LSASS exploits
- 04/16/2004 - Wonk/Ago indicates that he is developing an LSASS exploit and almost identified the appropriate function call
- 04/17/2004 - Wonk/Ago indicates that he is still working on the LSASS exploit
- 04/18/2004- Wonk/Ago identified the buffer and has to craft RPC packets with longer strings, at which point it will be provided to the group "xfocus" in exchange for additional 0-day exploits, doesn't currently plan to make a scanner or place in bots due to fear of bounty being placed by Microsoft. Wonk/Ago indicated that he would use the LSASS exploit on some "high profile" sites and that "some critical infrastructure" does not patch because of difficulties. Wonk/Ago prefers to be "stealthy" and gather information. Successfully exploited the vulnerability on Windows 2000 and Windows XP Home OS.
- 04/19/2004 - Wonk/Ago and unknown Chinese subject "ey4s", from XFocus group, cooperating to make LSASS exploit work on all versions of Windows OS. Wonk/Ago acknowledges that the vulnerability was fixed in the last patch, but that most people have not applied the patches yet. Working exploit for all versions of Windows finished.
- 04/26/2004 - LSASS exploit added to source code for AgoBot. Members of AgoBot development team start to use LSASS enabled bots to compromise computers.
- 05/01/2004 - Wonk/Ago creates code that enables PhatBot/AgoBot to take advantage of Sasser Worm spread by compromising the Sasser Worm and causing PhatBot to be installed on the compromised computer when the command shell is opened on port 9996.

489

From: GILLIAM, MARIE (SE) (FBI)
To: ARRUDA, STACY M. [Div16] [FBI], MCLERAN, KRISTEN, ...
Date: 5/4/04 8:35PM
Subject: Another intrusion into Valve by GEMBE

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hello everyone,

Enclosed is an EC I prepared detailing the latest actions and communications between Gembe and Valve. Kristen/Stacy, please provide me fax numbers, and I can fax the referenced e-mails to get them to you ASAP. Valve is not comfortable with the security of their network (especially after the subsequent intrusion by Gembe), so they usually just provide me with hard copies. Thanks!

Marie

SENSITIVE BUT UNCLASSIFIED

CC: FARQUHAR, DAVID [SE] [FBI], FOWLER, GREGORY A. [SE..

421

To: Berlin
Re: 288A-SE-89085, 05/04/2004

Transfer Protocol (FTP) link for the exploit's base code as well as a portion of the code.

On May 02, 2004, GEMBE contacted Reynolds once again via e-mail. In the e-mail, GEMBE stated that he is "currently auditing" Valve's network. Specifically, GEMBE stated "i think i sent you the lsass exploit early, so i comprehended not patching an invitation :)." Basically, GEMBE used the lsass exploit to once again hack into Valve's network without their permission. GEMBE further requested to be allowed to remain in the Valve systems and stated "ill let noone log the passwords this time :)", referring to his previous compromises of the Valve Software network. Valve informed Seattle Division, they never consented to allow GEMBE into their network and informed him that he should never do this without talking to them or without their permission. In the past, Valve has told GEMBE he did not have permission to initiate any type of penetration testing of their network.

During the time GEMBE had access to the network, Valve experienced a degradation in network performance and some of the services they were running. At this point, Valve was unable to say whether or not GEMBE's actions resulted in the degradation.

Reynolds informed Seattle Division he was very concerned by GEMBE's aggressive nature and for the safety of the Valve network. Reynolds was aware of the Trojans and a self-compiled version of the SSH client, Fuddy, installed by GEMBE during the intrusion. The modified version of Fuddy was logging information from Valve and sending it outside of their network. Valve Software stated they were taking steps to secure the holes found and exploited by GEMBE.

GEMBE is still pursuing his interest of working for Valve and stated he only hacked Valve's network because he was "bored" and waiting for them to respond concerning a job opportunity. GEMBE has been very persistent in his pursuit of employment at Valve.

Although he is twenty-one years of age, GEMBE has repeatedly shown an aggressive nature in dealing with Valve and has demonstrated a high-degree of technical knowledge and skill. GEMBE has also been manipulative and coercive with Valve concerning his role in multiple intrusions into their network and has displayed a determination to continue his behavior. GEMBE

SA

493

To: Berlin
Re: 288A-SE-89085, 05/04/2004

appears to be a major player in the authoring of the Isass exploit and well as one of the leaders of the "AGOBOT" development group, responsible for the development and distribution of various bots and the launching of multiple Distributed Denial of Service attacks. GEMBE has also shown an enterprising nature by receiving payments for the writing of exploits. As a result, Seattle believes this clearly demonstrates GEMBE should be held accountable for his behavior and considered an adult by German authorities.

Seattle Division will continue to support the German investigation, arrest, and prosecution of GEMBE to the fullest extent and in a manner most timely.

893

Frank Eißmann

Von: mgordon@fbi.gov
 Gesendet: Montag, 3. Mai 2004 22:01
 An: gerd.wolf@lka.bwl.de; frank.eissmann@lka.bwl.de
 Cc: jdysart@fbi.gov; sarruda@fbi.gov; mclerank@state.gov
 Betreff: Subject Information



putty -
 05-02-04.log (5 KB)

Ladies, Gentlemen,

I hope that Maÿ finds everyone doing well. Since the last e-mail, 2 new individuals have been in the chat channel, with IP Addresses resolving to Germany. The summary below details briefly the believed identity of each individual based on appearances in the chat room and a comparison of nicknames and IP Addresses, under the belief that wonk/stebo are brothers, living together, and using the same Internet connection. The IP Address for Gumble may have been included in a previous update. The subject NewRoot has only recently entered the channel in the last 2 or 3 days.

130.75.181.84:42636	Gumble	- Uni Hannover
217.226.153.60:3470	wonk/stebo	- T-online
212.6.91.195:2572	NewRoot	- EWE Tel
217.226.153.60:4555	wonk/stebo	

If anyone has any questions, please feel free to contact me at anytime.

v/r,
 P. Michael Gordon
 FBI

Sc

putty - 05-02-04 (2).log

===== PUTTY log 2004.05.02 22:17:19 =====

Login as: root
Authenticating with public key "rsa-key-20040304"
Last login: Mon May 3 00:30:28 2004 from pd9e2993c.dip.t-dialin.netHave a lot of beer...
[HD[2]]Linux p15137973 2.4.21-lufs-030704 #1 SMP Fri Jul 4 23:32:47 CEST 2003
i686 unknown

5:17am up 39 days, 4:07, 1 user, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
root pts/0 xxxxxxxxxxxxxxxx 5:17am 1.00s 0.06s 0.05s -bash

Last login:
root pts/0 xxxxxxxxxxxxxxxx Mon May 3 05:17:11 +0200 2004

hi erik, ich hab:
1. monkeystrike server gedownloaded (monkeystrike10-server.tar.gz)

p15137973:~ # /etc/init.d/named start
p15137973:~ # mcedit /var/named/bastart.eu.org
p15137973:~ # [10P/etc/init.d/named stop
p15137973:~ # date[K0000netstat -an | grep -e 8887 -e 8888 | wc -l
p15137973:~ # date[K0000netstat -an | grep -e 8887 -e 8888 | wc -l

18
p15137973:~ # netstat -an | grep -e 8887 -e 8888 | wc -l
p15137973:~ # [19P/etc/init.d/named start
p15137973:~ # mcedit /var/named/bastart.eu.org
p15137973:~ # [10P/etc/init.d/named stop
p15137973:~ # date[K0000netstat -an | grep -e 8887 -e 8888
tcp 0 0 217.160.214.154:8887 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:8888 0.0.0.0:* LISTEN
tcp 0 0 217.160.214.154:8887 24.128.250.161:8476 ESTABLISHED
tcp 0 0 217.160.214.154:8887 83.108.61.113:29341 ESTABLISHED
tcp 0 0 217.160.214.154:8887 68.212.120.176:3007 ESTABLISHED
tcp 0 0 217.160.214.154:8887 66.75.238.57:63577 ESTABLISHED
tcp 0 0 217.160.214.154:8887 81.196.79.195:1232 ESTABLISHED
tcp 0 0 217.160.214.154:8887 130.75.181.84:42636 ESTABLISHED
tcp 0 0 217.160.214.154:8887 217.226.153.60:3470 ESTABLISHED
tcp 0 0 217.160.214.154:8887 24.10.112.147:1726 ESTABLISHED
tcp 0 0 217.160.214.154:8887 213.118.47.126:1034 ESTABLISHED
tcp 101 0 217.160.214.154:8887 202.36.16.70:3199 ESTABLISHED
tcp 0 0 217.160.214.154:8887 212.6.91.195:2572 ESTABLISHED
tcp 0 0 217.160.214.154:8887 217.226.153.60:4555 ESTABLISHED
tcp 0 0 217.160.214.154:8887 202.36.16.70:3197 FIN_WAIT2
tcp 0 0 217.160.214.154:8887 24.78.66.228:2681 ESTABLISHED
tcp 0 0 217.160.214.154:8887 69.31.65.2:4242 ESTABLISHED
tcp 0 0 217.160.214.154:8887 80.213.50.59:3410 ESTABLISHED

p15137973:~ # netstat -an | grep -e 8887 -e 8888 | wc -l
p15137973:~ # [19P/etc/init.d/named start
p15137973:~ # mcedit /var/named/bastart.eu.org
p15137973:~ # [10P/etc/init.d/named stop
p15137973:~ # date[K
Mon May 3 05:17:20 CEST 2004
p15137973:~ # [0000netstat -an | grep -e 8887 -e 8888 | wc -l
p15137973:~ # [19P/etc/init.d/named start
p15137973:~ # netstat -an | grep -e 8887 -e 8888 | wc -l

17
You have new mail in /var/mail/root
p15137973:~ # netstat -an | grep -e 8887 -e 8888 | wc -l
p15137973:~ # date[K0000netstat -an | grep -e 8887 -e 8888
tcp 0 0 217.160.214.154:8887 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:8888 0.0.0.0:* LISTEN
tcp 0 0 217.160.214.154:8887 202.36.16.70:3201 ESTABLISHED
tcp 0 0 217.160.214.154:8887 24.128.250.161:8476 ESTABLISHED
tcp 0 0 217.160.214.154:8887 83.108.61.113:29341 ESTABLISHED
tcp 0 0 217.160.214.154:8887 68.212.120.176:3007 ESTABLISHED

SS

```
putty - 05-02-04 (2).log
tcp      0      0 217.160.214.154:8887 66.75.238.57:63577 ESTABLISHED
tcp      0      0 217.160.214.154:8887 81.196.79.195:1232 ESTABLISHED
tcp      0      0 217.160.214.154:8887 130.75.181.84:42636 ESTABLISHED
tcp      0      0 217.160.214.154:8887 217.226.153.60:3470 ESTABLISHED
tcp      0      0 217.160.214.154:8887 24.10.112.147:1726 ESTABLISHED
tcp      0      0 217.160.214.154:8887 213.118.47.126:1034 ESTABLISHED
tcp      0      0 217.160.214.154:8887 212.6.91.195:2572 ESTABLISHED
tcp      0      0 217.160.214.154:8887 217.226.153.60:4555 ESTABLISHED
tcp      0      0 217.160.214.154:8887 24.78.66.228:2681 ESTABLISHED
tcp      0      0 217.160.214.154:8887 69.31.65.2:4242 ESTABLISHED
tcp      0      0 217.160.214.154:8887 80.213.50.59:3410 ESTABLISHED
p15137973:~ # netstat -an | grep -e 8887 -e 8888 | wc -l
p15137973:~ # date[k
Mon May 3 05:50:01 CEST 2004
p15137973:~ #
```


FAX TRANSMISSION



Office of the Legal Attache
 American Consulate General
 Frankfurt, Germany
 Telephone #: 011 49 69 7535 3870
 Fax #: 011 49 69 560 2880

To: Herr Eismann
 Landeskriminalamt
 Baden Wuerttemberg

Date: March 22, 2004

Fax #: 0711 5401 2418

Pages: 6, including this cover sheet.

Voice #: 0711 5401 2441

From: Office of the Legal Attache

Subject: Valve Software Computer Intrusion/Theft of Intellectual Property
 AGO
 AXEL GEMBE

Case ID: 288A-SE-89085

Dear Herr Eismann,

As I stated in the previous fax, I am now providing you details, some of which you may already have, regarding the FBI investigation into the theft of intellectual property and computer intrusion and suspect AXEL GEMBE.

Agobot Virus and Distributed Denial of Service Attacks of Websites and Internet Service Providers

Investigation by multiple United States law enforcement agencies has established that since October 2002, GEMBE has been participating in the development and deployment of a malicious computer code known as the Agobot/gaobot Virus. The virus works by automatically gaining unauthorized access to Internet computers, in order to use those computers to launch hundreds of Distributed Denial of Service (DDoS) attacks on victim computer networks. The targets of these attacks include well-known commercial websites such as eBay. Sales revenue and business losses, although often difficult to estimate, can readily multiply into the millions of dollars. For example, Internet Service providers Tiscali UK and Aeneas Internet and Telephone, Memphis, Tennessee, USA, were each shut down by the virus for approximately four days, resulting in estimated losses of \$1.6 million (USD) and \$50,000 (USD), respectively.

The Investigation of DDoS Attacks

Beginning in October 2002, and continuing until February 2004, numerous Internet Service Providers (ISPs), individual computers, and business computer networks were the victims of DDoS attacks launched from other computers infected with the Agobot/gaobot virus. The virus spreads by scanning the Internet for computers vulnerable to attack. If it locates such a computer, it installs itself, leaving behind a "back door" which causes the computer to report to a communication channel controlled by the person who spawned the virus. An infected or compromised computer is called a "bot." By instructing the mass of infected bots to flood a particular computer on the internet, an individual can overwhelm the computer, effectively denying service to it.

The United States Secret Service opened an investigation in January 2003, when a local ISP, Aeneas Internet and Telephone, was hit with periodic DDoS attacks over a two-month period of time. The attack peaked when Aeneas was forced off-line for approximately four days, resulting in an estimated \$50,000 loss.

The investigation established that the Agobot/gaobot virus was authored, maintained, modified, and made more virulent by an individual known by the screen nickname "Ago," who actually inserted his photograph and email address in one version of the virus.

The Agobot/gaobot virus was responsible for a DDoS attack on Tiscali UK, a large ISP. Tiscali was denied service for approximately four days, resulting in an estimated \$1.6 million loss. On February 11, 2004, LEE WALKER was arrested in the United Kingdom. WALKER admitted that he and Ago had launched numerous DDoS attacks, and that Ago had authored the virus, and continued to modify and improve it. He claimed he knew Ago lived in Germany and that his first name was "Alex" or "Axel," but could not identify him further.

Hundreds of Internet sites were victimized in the DDoS attacks launched by GEMBE and/or WALKER, using the virus authored and maintained by GEMBE. In addition, the virus was often used to attack a target by attacking Domain Name System (DNS) servers, computers which serve as part of the infrastructure of the Internet. By attacking DNS servers, the virus affected service to other Internet sites besides the specific, intended target.

According to recent information obtained by the FBI, Ago and the other authors of the Agobot/gaobot control a bot network of anywhere from 50,000 to 100,000 computers. This network is capable of traffic generating speeds of 30-35 gigabits per second. It is believed that the country of New Zealand may have been recently "knocked offline" (internet service was disabled) by an attack launched by the group.

Investigation has determined that Ago is selling the malicious code on the Internet. Ago utilizes the Paypal account "theago@gmx.net" to sell his malicious code. Authors of malicious code often spread worms and viruses simply for the challenge and ability to claim within their on-line community the "bragging rights" for disabling or disrupting a major ISP or business. In addition to spreading the code to anyone with the resources to purchase it, Ago is now personally profiting by the release of the code. Ago has every motivation to distribute the code to the maximum extent possible, and no motivation to stop. This makes his arrest and prosecution

more urgent.

The following excerpt, quoted from the Agobot/gaobot source code, illustrates Ago's ability to enlist assistance with the creation and distribution of the malicious code:

"Contributions to Agobot3:

Num - Name - What

1. - Ago - Writing Agobot3 base, being the author/maintainer
2. - Fight - Hosting my testing bots
3. - killer77 - Donating money to make Agobot3 as good as it is today
4. - dj-fu - Helped me finding bugs
5. - Chrono - Hosting me a site and helping find bugs
6. - harr0 - Hosting me a site
7. - ryan1918 - Hosting me a site or forum too (not yet)
8. - PhaTTy - Implementing new features into Agobot3
9. - weed - Making me high while programming

thx to anyone on this list and everyone i forgot for making Agobot3 what it is."

Furthermore, another "trojan" (hidden) bot has been developed and unleashed on the Internet. This bot goes by the name Phatbot. It has been determined by FBI examination the malicious code found within Phatbot builds upon the code used in the Agobot/gaobot. The authors of this bot may be the creators of the Agobot/gaobot as well, to include GEMBE. This new bot is considered to be very dangerous because it has the ability to be polymorphic on installation in an attempt to evade anti-virus signatures as it spreads from computer to computer.

Valve Software Computer Network Intrusion and Theft of Intellectual Property

GEMBE has been identified as the hacker who in 2003 gained unauthorized access into the network of game developer Valve Software, which resulted in the theft and public dissemination of a pre-release version of Valve Software's flagship computer game, Half Life II (HL2). Based on profits from its initial version of the game, Valve Software anticipated (and has now lost) \$250,000,000.00 in sales revenue from HL2.

Since the middle of February 2004, GEMBE has been communicating with Valve Software management via email, attempting to convince Valve Software that although he was the intruder, he was not responsible for the dissemination of their software. He has also aggressively sought employment with Valve Software, citing his imminent mandatory conscription as a reason for wanting to leave the EU and obtain work in the States.

GEMBE's email discussions with Valve Software have progressed to the point where some law enforcement intervention is critical. Specifically, GEMBE has expressed impatience with the slow response from Valve Software, and has remarked that he has the ability to gain control over Valve Software's network computers should he decide to do so. GEMBE is

AS
expecting a job interview with Valve Software by telephone, followed shortly thereafter by an expense-paid trip to the States. United States authorities involved with this case are concerned that if GEMBE discovers that Valve Software's employment interest is not sincere, he may retaliate. Valve Software acknowledges that GEMBE may currently have access to a computer on its network, but believes that he cannot penetrate further into its system. Still, GEMBE's skill in DDoS attacks has heightened concerns.

The Investigation of the Valve Software Intrusion

Valve Software, located in Bellevue, Washington, USA, creates, produces and sells popular Internet-based computer video games. One of these games is Half-Life, an immensely popular game with sales exceeding \$250,000,000. Valve Software was in the process of developing Half-Life II (HL2), the widely-anticipated sequel to Half-Life, when their computer network was victimized by an unlawful intrusion.

Valve Software learned of the criminal intrusion into its computer system on October 1, 2003, when the company became aware that an internal email from one Valve Software employee to another had been posted on a public website, and later, that programming code for HL2 and other Valve Software games had been stolen and released on different websites. Valve Software employee computer passwords were also posted. Since then, a working, unreleased version of HL2 and another Valve Software game have been circulated on the Internet. HL2 is now reportedly being sold on computer disks in Russia. As a result of all this activity, Valve Software began an in-depth review of the computers on their network and found at least thirteen machines that had been compromised within their network. Valve believes that the intrusion may have occurred as early as June 2003. The computers were provided to the FBI for further forensic analysis.

Forensic analysts discovered a variety of "hacker" programs installed without Valve Software's permission. One allowed an intruder to capture passwords and other confidential information. Another program created a secure but unauthorized method of remote access, a "tunnel" for a hacker to use to sneak back into Valve Software's system. On one of Valve Software's networked computers, this program was configured to connect to a website in Germany. To identify the person who controlled the website, the German ISP who owns the address for the website would have to provide subscriber information. There were also instances of the Agobot/gaobot found on Valve Software victim machines.

On February 16, 2004, U.S. authorities were contacted by Valve Software after the Chief Executive Owner (CEO) received an email from an individual claiming to have been the person who hacked into the Valve Software network. The individual used the nickname "DaGuy" and the following email address: daguy@hush.com. That email address was provided by Hush Communications, a company located in Vancouver, Canada, which provides anonymous re-mailing services.

DaGuy claimed to have had access to the Valve Software network for approximately six months. He provided Valve Software with technical information "proving" he truly was the hacker. To date, these claims and details have been validated by the forensic analysis performed by both Valve Software and the FBI, and are also consistent with the details described in the chat logs previously provided to Valve Software.

DaGuy appears to be strongly motivated to convince Valve Software that he is not an "evil" hacker. He claimed that he had hacked into Valve Software's system only to observe their development of HL2. He claimed that he was careless during an IRC session with a friend, and that members of a group known as myg0t eavesdropped on this conversation and obtained sufficient information to enable them to use his established but unauthorized access into Valve Software's network. In fact, myg0t was responsible for the initial public dissemination of the internal Valve Software email and source code.

DaGuy has attempted to prove he could be helpful to Valve Software by providing advice regarding its network security, and on February 19, 2004, DaGuy asked Valve Software's CEO if they had any job openings. On February 27, 2004, the CEO asked DaGuy if his interest was serious, and DaGuy replied that he was. On February 28, 2004, DaGuy expressed some urgency in coming to the U.S., as he was concerned about conscription. He said he needed to know as soon as possible. On March 3, 2004, the CEO apologized for not responding more quickly and promised to be more prompt. He requested a resume. He advised DaGuy that Valve Software would fly both he and his wife to the United States for a job interview. DaGuy replied that he was not married and would need funds to travel.

After days of sending emails without response, on March 6, 2004, DaGuy sarcastically asked the CEO what he meant by "prompt," and claimed he could have taken control of one of Valve Software's network computers if his intentions weren't benevolent. He wondered whether he should break into Valve Software's computer to fix it.

On March 8, 2004, the CEO advised DaGuy that Valve Software will pay for travel and relocation expenses.

On March 10, 2004, DaGuy provided a phone number (49 7673 93222) for an initial telephone interview, pursuant to Valve Software's standard hiring procedures. Valve Software is prepared to conduct the telephone interview.

As of March 20, 2004, there was a website, www.cs-ipv6.lancs.ac.uk/ftp-archive/6bone/whois/nic-hdl/ago1-6bone, which contains an FTP archive "who is" list. This list contained the following details for AGO1-6BONE:

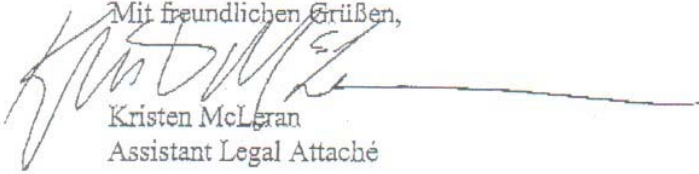
person: Axel Gembe
address: Schonenbergerstrasse 8
address: 79677 Schonau
phone: 49 7673 9322218
email: theago@gmx.net
nic-hdl: AGO1-6BONE
url: <http://www.bastart.eu.org/>
notify: theago@gmx.net
mnt-by: AGOMNT-6BONE
change: theago@gmx.net 20040128
source: 6BONE

5

AT
The phone number included in the above reference is the same as the one provided by DaGuy, with the exception of the last digits, to Valve Software on March 10, 2004.

Please advise me of any investigative actions. Do not hesitate to contact me if you have any additional questions.

Mit freundlichen Grüßen,



Kristen McLeran
Assistant Legal Attaché

FAX TRANSMISSION



Office of the Legal Attache
American Consulate General
Frankfurt, Germany
Telephone #: 011 49 69 7535 3870
Fax #: 011 49 69 560 2880

To: Herr Eismann
Landeskriminalamt
Baden Wuerrtemberg

Date: March 22, 2004

Fax #: 0711 5401 2405

Pages: 2, including this cover sheet.

Voice #: 0711 5401 2441

From: Office of the Legal Attache

Subject: Valve Software Computer Intrusion/Theft of Intellectual Property
AGO
AXEL GEMBE

Case ID: 288A-SE-89085

Dear Herr Eismann,

I am providing you information regarding an FBI investigation into the theft of intellectual property and computer intrusion. Investigation indicates that the subject responsible is AXEL GEMBE, residing in Germany.

Recent developments have added urgency to this matter, as GEMBE is now communicating via email directly with a CEO of Valve Software, and is threatening to do further damage by taking control of Valve Software computers.

The information provided below is a summary of the most recent investigative developments. I will send a follow-up fax with additional, detailed information regarding the entire investigation.

Immediate intervention into the criminal activities of AXEL GEMBE, of Schonau, Germany, is considered extremely urgent. GEMBE, (also known as "Ago"), is now considered by U.S. authorities to be a primary suspect in two separate, international cyber crimes of major proportions.

GEMBE has been identified as the hacker who in 2003 gained unauthorized access into

21
the network of game developer Valve Software, which resulted in the theft and public dissemination of a pre-release version of Valve Software's flagship computer game, Half Life II (HL2). Based on profits from its initial version of the game, Valve Software estimated \$250,000,000.00 in lost sales revenue from HL2.

Since the middle of February 2004, GEMBE has been communicating with Valve Software management via email, attempting to convince Valve Software that although he was the intruder, he was not responsible for the dissemination of their software. He has also aggressively sought employment with Valve Software, citing his imminent mandatory military service as a reason for wanting to leave the EU and obtain work in the States.

Valve Software is cooperating with the FBI in this matter. GEMBE's email discussions with Valve Software have progressed to the point where some law enforcement intervention is critical. Specifically, GEMBE has expressed impatience with the slow response from Valve Software, and has remarked that he has the ability to gain control over Valve Software's network computers should he decide to do so.

GEMBE is expecting a job interview with Valve Software by telephone, followed shortly thereafter by an expense-paid trip to the States. On March 10, 2004, GEMBE provided a phone number (49 7673 93222) for an initial telephone interview, pursuant to Valve Software's standard hiring procedures.

The FBI is concerned that if GEMBE discovers that Valve Software's employment interest is not sincere, or if they continue to stall, he may retaliate.

Please advise me as to your anticipated investigative actions. Do not hesitate to contact me if you have any additional questions.

Mit freundlichen Grüßen,



Kristen McLeran
Assistant Legal Attaché



28
U.S. Department of Justice

Federal Bureau of Investigation

File No. 295A-SE-89085

Office of the Legal Attache
United States Consulate
Frankfurt, Germany

16 March 2004

Re: myg0t.com
AGO

Herr Jörn Kreitlow
OA-34
Bundeskriminalamt (BKA)
Wiesbaden, Germany

Dear Herr Kreitlow,

The following information is in reference to a computer intrusion. The victim company is Valve Software. One of the main subjects involved is believed to be located in Germany, using the nick of AGO.

On 2 October, 2003, Valve Software, reported to the FBI the theft of their source code for the new engine technology in Half-Life 2 (HL2). HL2 is a popular game within the Internet community. The release date for HL2 was set for the end of September 2003. However, it was pushed back to an undisclosed time.

To date, at least 13 Valve internal machines were found compromised. Valve found machines that had both key loggers and backdoor trojans installed on them. The Valve email system was also compromised as an email sent from one internal employee to another was intercepted and published on the www.myg0t.com website. www.myg0t.com is a site dedicated to gaming cheats and producing mods for online games.

Through forensic analysis of the victim systems, numerous leads and potential subjects have been identified around the world with one of the main subjects being located in Germany and using the moniker "AGO". Two of the Valve victim machines contained detailed technical information that led back to AGO and a number of Germany Internet Service Providers (ISPs). Through further investigation, it has also been determined that AGO's real name is "AXEL GEMBE" who is quite possibly residing in Schoenau, Germany.

27

On 16 February, 2004, Valve software provided the FBI with an e-mail sent to the CEO of Valve, claiming to be from the hacker regarding information about the computer intrusion into the Valve Software network and the theft of the HL2 source code.

The e-mail address used by the sender was daguy@hush.com. The sender claimed to have had access to the Valve network for approximately six months. However, he/she denied distributing the HL2 source code over the Internet. The sender then provided Valve with technical information "proving" he/she was legitimate. The sender then referenced the myg0t group and claimed the access he/she had obtained into the Valve network was discovered by myg0t members.

The sender stated his/her motivation for hacking into the Valve network was only to "observe the HL2 development process." To date, the sender continues to send e-mails to Valve from the daguy@hush.com address. A lookup resulted in the e-mail address coming back to a Vancouver-based company, Hush Communications, 455 Granville Street, Suite 203, Vancouver, BC V6C 1T1, Canada. This company does not retain any log-on or identifying information.

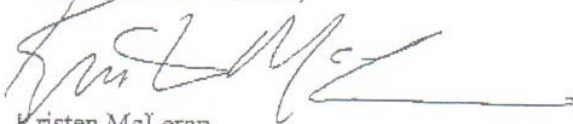
Based on details in the e-mails, it is believed that the anonymous sender of these messages could be AXEL GEMBE a.k.a AGO.

As you are aware, United States Secret Service (Case Agent Kevin Sandlin) also has an open and active case against GEMBE for various Denial of Service (DOS) attacks and the authoring of malicious code, namely the AGOBOT which is an IRC-controlled backdoor with network spreading capabilities. There are variants of this initial worm as well that he may be responsible for writing and distributing.

The FBI is hopeful that German officials will be interested in opening an investigation on AGO. The FBI would like to be provided with any subscriber information for accounts/sites/e-mails associated with AGO and, ultimately, would hope that a German investigation could result in a search warrant for his computer systems. AGO is also linked with the large botnet investigation into Creative Internet Technologies, a.k.a. FOONET

As a side note, there is the belief that GEMBE may be the son of a German Magistrate Judge. This has not been confirmed.

Mit freundlichen Grüßen,



Kristen McLeran
Assistant Legal Attache.



U.S. Department of Justice

Eric J. Klumb
Trial Attorney, Criminal Division
Computer Crime & Intellectual Property Section
202-353-4304 eric.klumb@usdoj.gov

Memorandum to: Detective Inspector Joern Kreitlow
From: Eric Klumb *E. Klumb*
Re: Intrusion into Valve Software Network

Summary of Investigation

Valve Software, located in Bellevue, Washington, USA, creates, produces and sells popular Internet-based computer video games. One of these games is Half-Life, an immensely popular game with sales exceeding \$250,000,000 (US\$). Valve Software was in the process of developing Half-Life II (HL2), the widely-anticipated sequel to Half-Life, when their computer network was "hacked" into or accessed without authorization. Based upon the sales of the original game, Valve Software had expected HL2 to generate sales revenues of at least \$200,000,000.

Valve Software learned of the unauthorized intrusion into its computer system on October 1, 2003, when the company became aware that an internal email from one Valve Software employee to another had been posted on a public website, and later, that programming code for HL2 and other Valve games had been stolen and released on different websites. Valve employee computer passwords were also posted. Since then, a working, unreleased version of HL2 and another Valve game have been circulated on the Internet. HL2 is now reportedly being sold on computer disks in Russia. As a result of all this activity, Valve Software began an in-depth review of the computers on their network and found at least thirteen machines that had been compromised within their network. Valve believes that the intrusion may have occurred as early as June 2003. The computers were provided to the FBI for further forensic analysis.

Forensic analysts discovered a variety of "hacker" programs installed without Valve Software's permission. One allowed an intruder to capture passwords and other confidential information. Another program created a secure but unauthorized method of remote access, a "tunnel" for a hacker to use to sneak back into Valve's system. On one of Valve's networked computers, this program was configured to connect to the website "ago.gotdns.org."

Like any other computer on the internet, the computer which contains the website "ago.gotdns.org" must have a unique Internet Protocol (IP) address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. The IP address can be permanently assigned or dynamically assigned, meaning the computer is assigned a different IP address each time a new connection to the internet is made. Either way, the IP Address used by a computer attached to the internet must be unique for the duration of the session, that is, from connection to disconnection. ISPs typically log their customers' connection, which means the ISP can, for a period of time, identify which of their customers were assigned a specific IP address during the time period of the session.

5A

In this case, the IP address of the website "ago.gotdns.org" was dynamically assigned. Although the IP addresses of this website during the 2003 intrusion into Valve's computer network are not known, the website remained active into 2004. It was checked regularly by investigators beginning in November of 2003, the last time on February 6, 2004. The IP addresses assigned to "ago.gotdns.org" during these checks are listed below in paragraph 3 of the request.

The investigation has associated another website with "Ago." A posted message dated April 4, 2000, was found on a website from a person identifying himself as Axel Gembe, with the email address theago@gmx.net. On two other websites, a user identifying himself as "Ago" also lists his email as theago@gmx.net, with webpage "ago.daemon.sh." There is an important connection between the "ago.daemon.sh" website and the "ago.gotdns.org" website. Both have dynamically assigned IP addresses. When checked on the date and times listed in paragraph 1, the two webpages had the same IP address, which suggests both are on the same computer, the computer of the person who had the secure but unauthorized tunnel into a computer on Valve Software's computer network.

After Valve Software discovered the intrusion in October, 2003, it asked the community of Half Life gamers and others to come forward with any information about those responsible. Two individuals, one anonymous, provided logs or transcripts of online communications known as "chat." In both, an individual claimed responsibility for the Valve Software intrusion and provided details consistent with the FBI's forensic analysis. In one of the chats, the individual identified himself as "ef~Ago." In the second chat log, dated October 11, 2003, the anonymous tipster identified the confessing hacker's IP Address as frb9_d9bb4a51.pool.Mediaways.net, which resolved to the numeric IP address 217.187.73.89 as of October 25, 2003.

On February 16, 2004, U.S. authorities were contacted by Valve Software after the Chief Executive Owner (CEO) received an email from an individual claiming to have been the person who hacked into the Valve Software network. The individual used the following email address: daguv@hush.com. That email address was provided by Hush Communications, a company located in Vancouver, Canada, which provides anonymous remailing services.

The sender claimed to have had access to the Valve Software network for approximately six months. The sender then provided Valve Software with technical information "proving" he/she truly was the hacker. To date, these claims and details have been validated by the forensic analysis performed by both Valve Software and the FBI, and are also consistent with the details described in the chat logs previously provided to Valve Software. The sender continues to communicate with Valve's CEO, and is actively seeking work with or for Valve in connection with the security of its network.

Requested Information:

Please include the following information for each of the below requests if possible:

- Customer name (including all possible customers)
- Billing address and residential address
- Telephone number
- Any assigned network Internet Protocol address
- Records of session times and durations (beginning in June 2003)
- Length of service (including a start date)
- Type of services utilized (that is, DSL, cable modem, dial-up, web-hosting, e-mail, etc)
- Means and source of payment for such service (including any credit card or bank account information)
- Whether or not the IP Address is assigned dynamically or statically
- Any other information concerning the identity of the creator/subscriber, including but not limited to , other e-mail addresses, account profiles, date of birth, gender, and occupation
- Complete and accurate date and time stamps

1. Please provide any available subscriber information, detailed above, for the users assigned the IP address 217.187.73.89 and /or hostname frb9-d9bb4a51.pool.Mediaways.net, on October 11, 2003.

2. Please provide any available subscriber information, detailed above, for the users assigned the e-mail address theago@gmx.net.

3. Please provide any available subscriber information, detailed above, for the users assigned the following IP addresses and hostnames at associated times (Times are all Eastern Standard Time (EST); UTC/GMT - 5hours):

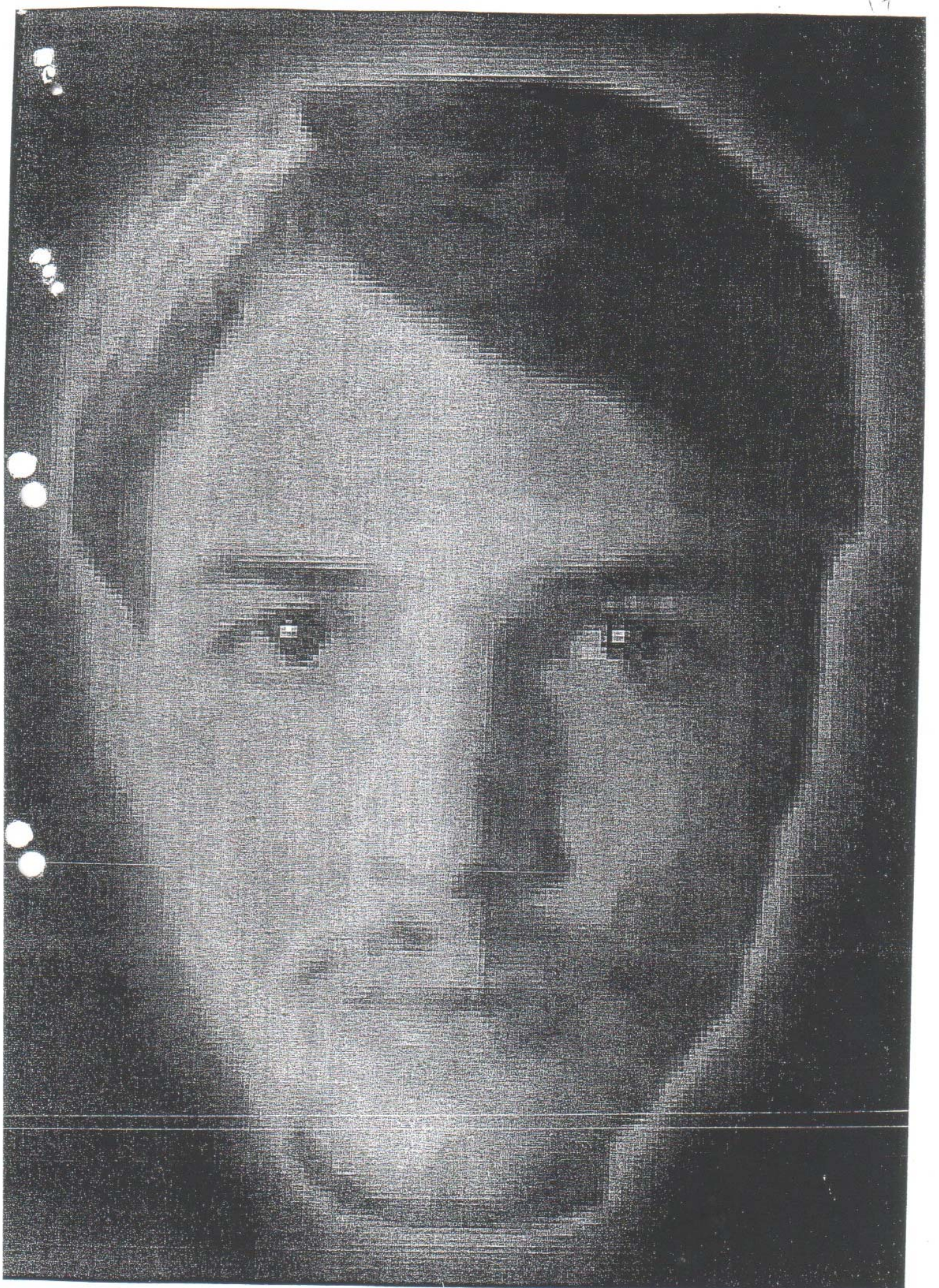
Date/Time	IP	Reverse Lookup
11/12/03 12:00am	217.9.25.29	td909191d.adsl.terralink.de
11/12/03 10:59am	217.187.74.10	frb9-d9bb4a0a.pool.mediaWays.net
11/13/03 7:59pm	217.187.68.117	frb9-d9bb4475.pool.mediaWays.net
11/24/03 8:09am	217.187.73.184	frb9-d9bb49b8.pool.mediaWays.net
11/24/03 8:09pm	217.187.72.194	frb9-d9bb48c2.pool.mediaWays.net
11/25/03 8:10pm	217.187.74.191	frb9-d9bb4abf.pool.mediaWays.net
12/2/03 7:32am	217.187.70.114	frb9-d9bb4672.pool.mediaWays.net
12/2/03 7:34am	217.187.70.114	frb9-d9bb4672.pool.mediaWays.net
12/2/03 7:36am	217.187.70.114	frb9-d9bb4672.pool.mediaWays.net
12/2/03 6:36pm	217.187.69.100	frb9-d9bb4564.pool.mediaWays.net
12/3/03 8:37pm	217.9.25.125	td909197d.adsl.terralink.de
12/8/03 7:43am	217.82.253.229	pD952FDE5.dip.t-dialin.net
12/8/03 10:45am	217.82.253.229	pD952FDE5.dip.t-dialin.net
12/8/03 12:45pm	217.226.149.240	pD9E295F0.dip.t-dialin.net
12/9/03 12:47pm	217.82.244.32	pD952F420.dip.t-dialin.net

31

12/10/03 12:47pm	80.131.249.77	p5083F94D.dip.t-dialin.net
12/11/03 7:33am	80.131.249.77	p5083F94D.dip.t-dialin.net
12/11/03 11:41am	80.131.249.77	p5083F94D.dip.t-dialin.net
12/11/03 12:41pm	217.82.243.245	pD952F3F5.dip.t-dialin.net
12/12/03 12:41pm	217.226.158.36	pD9E29E24.dip.t-dialin.net
12/13/03 12:41pm	217.82.241.2	pD952F102.dip.t-dialin.net
12/14/03 12:42pm	217.82.252.66	pD952FC42.dip.t-dialin.net
12/14/03 1:42pm	217.9.26.144	td9091a90.adsl.terralink.de
12/15/03 6:42am	217.9.28.127	td9091c7f.adsl.terralink.de
12/16/03 5:42am	217.9.27.185	td9091bb9.adsl.terralink.de
12/16/03 11:42am	217.82.240.188	pD952F0BC.dip.t-dialin.net
12/18/03 11:43am	217.82.243.42	pD952F32A.dip.t-dialin.net
12/18/03 11:43am	217.226.154.195	pD9E29AC3.dip.t-dialin.net
12/19/03 4:43pm	80.131.241.237	p5083F1ED.dip.t-dialin.net
12/20/03 9:44am	217.82.255.99	pD952FF63.dip.t-dialin.net
12/21/03 9:44am	217.82.250.67	pD952FA43.dip.t-dialin.net
12/22/03 9:44am	217.226.153.32	pD9E29920.dip.t-dialin.net
12/23/03 9:44am	217.226.145.251	pD9E291FB.dip.t-dialin.net
12/24/03 9:45am	217.82.243.144	pD952F390.dip.t-dialin.net
12/24/03 10:45am	217.226.155.5	pD9E29B05.dip.t-dialin.net
12/25/03 10:45am	80.131.243.175	p5083F3AF.dip.t-dialin.net
12/26/03 10:45am	80.131.242.117	p5083F275.dip.t-dialin.net
12/27/03 8:46pm	217.82.249.96	pD952F960.dip.t-dialin.net
12/28/03 6:46am	217.226.155.174	pD9E29BAE.dip.t-dialin.net
12/29/03 6:47am	217.82.248.225	pD952F8E1.dip.t-dialin.net
12/29/03 12:47pm	217.82.241.133	pD952F185.dip.t-dialin.net
12/29/03 5:47pm	217.187.69.207	frb9-d9bb45cf.pool.mediaWays.net
12/30/03 6:48pm	217.187.71.52	frb9-d9bb4734.pool.mediaWays.net
12/31/03 4:48pm	217.187.72.16	frb9-d9bb4810.pool.mediaWays.net
1/1/04 6:48pm	217.187.71.7	frb9-d9bb4707.pool.mediaWays.net
1/2/04 6:49pm	217.187.68.51	frb9-d9bb4433.pool.mediaWays.net
1/3/04 2:49pm	217.187.73.229	frb9-d9bb49e5.pool.mediaWays.net
1/4/04 2:50pm	217.187.73.37	frb9-d9bb4925.pool.mediaWays.net
1/5/04 2:50pm	217.187.72.96	frb9-d9bb4860.pool.mediaWays.net
1/7/04 11:53am	217.187.72.96	frb9-d9bb4860.pool.mediaWays.net
2/6/04 1:29pm	217.187.72.96	frb9-d9bb4860.pool.mediaWays.net

Where the information cannot be provided, please preserve it until appropriate legal process can be obtained.

Your consideration of this request is greatly appreciated.



9/25/03
1/3

Hey, Kevin!

They're baaaack! They brought up both of the botnets I've been tracking. These have been down for over a week. This means we have more fun on the way. :(Here they are, with all dates and times in GMT:

bots.unixcon.net has address 66.252.1.220
AS23522 Creative Internet Techniques/Foonet
- Currently transit only through AS3549 Global Crossing

```

09/25 00:56:13 *** There are 739 total users (0 + 739 invisible) on 1 servers
09/25 00:56:13 *** There are 15 channels
09/25 00:56:13 *** This server has 739 users (~ 100% of total), and 0 servers
connected to it
09/25 00:56:13 *** Current local users: 739 Max: 801
09/25 00:56:13 *** Current global users: 739 Max: 801
09/25 00:55:38 *** Channel      Users Topic
09/25 00:55:38 *** #bots          5
09/25 00:55:38 *** #edumadness    1
09/25 00:55:38 *** #scan          11
09/25 00:55:38 *** #test          3
09/25 00:55:38 *** #bots1         19
09/25 00:55:38 *** Prv            75
09/25 00:55:38 *** #VNAgents007  16
09/25 00:55:38 *** #ftp           69
09/25 00:55:38 *** #!bots         2
09/25 00:55:38 *** #P_o_GrOm      1
09/25 00:55:38 *** #!ownage       61
09/25 00:55:38 *** #vncops007    251
09/25 00:55:38 *** #!mrs          8
09/25 00:55:38 *** #scanftp      19
09/25 00:55:38 *** #proxyspam    193

```

Take a look at some of those channels. The botnet I'm tracking is in #vncops007. #VNAgents007 is another botnet. Both are using Agobot (of course). The #proxyspam channel is interesting, eh? It certainly ties nicely into the spam-as-motivation for the attacks against the anti-spam community.

bunghole.mysql.d.com has address 66.250.235.51
AS16631 Cogent

```

09/25 00:52:27 *** Channel      Users Topic
09/25 00:52:39 *** OU 1S (from MySQL)
09/25 00:52:39 *** 2 masters (from MySQL)
09/25 00:52:39 *** 3 CH (from MySQL)
09/25 00:52:39 *** 64 LC 0 (from MySQL)

```

The botnet channel on this network is #agobot3, but there are likely more. It isn't clear how many bots are on this server, because the server is heavily obfuscated. :(

I'm logging #vncops007 on bots.unixcon.net and #agobot3 on bunghole.mysql.d.com. Perhaps we should make a call to our friends at Global Crossing and Cogent? What else do you need?


```

05/23 17:17:05 *** Ago (54@l1c1rc-15A2F016.pool.mediaWays.net) joined #sdbot
<18:17>
05/23 17:17:05 *** Ago is 54@l1c1rc-15A2F016.pool.mediaWays.net (Ago)
05/23 17:17:05 *** Ago is 54@l1c1rc-15A2F016.pool.mediaWays.net
05/23 20:33:23 *** Signoff: Ago (Ping timeout) <21:33>
05/23 20:33:24 *** Ago is <UNKNOWN>@<UNKNOWN>
05/23 20:33:34 *** Ago (54@l1c1rc-15A2F016.pool.mediaWays.net) joined #sdbot
<21:33>
05/23 20:33:35 *** Ago is 54@l1c1rc-15A2F016.pool.mediaWays.net (Ago)
05/23 20:33:35 *** Ago is 54@l1c1rc-15A2F016.pool.mediaWays.net
05/23 21:25:40 [#sdbot] <Ago> ftp://ftp.uni-freiburg.de/incoming/getcdkey.cpp <-
- updated. forgot to reset dwSize.
05/23 21:27:05 [#sdbot] <Ago> thx, it was a really dumb bug
05/23 21:27:58 [#sdbot] <Ago> if someone supplies me with the right locations
05/23 21:28:06 [#sdbot] <Ago> my brother supplied me with most
05/23 21:28:17 === Action [#sdbot] : Mouse supplied Ago with some locs
05/23 21:28:46 [#sdbot] <Ago> if someone wants to, he can give it to rf-mods to
update the broken on they got
05/23 21:41:01 [#sdbot] <Ago> like everyl ?
05/23 21:41:21 [#sdbot] <Ago> i did fix it myself :P
05/23 21:41:39 [#sdbot] <Ago> but i don't have the source of my old sd anymore
05/23 21:41:48 [#sdbot] <Ago> or i would have to search deep in the fs tree
05/23 21:42:10 [#sdbot] <Ago> hmmm, perhaps i can find it
05/23 21:42:39 [#sdbot] <Ago> im actually just trying to find it
05/23 21:43:59 [#sdbot] <Ago> thats the good thing about having wd800jb, you
don't hear em :P
05/23 21:46:13 [#sdbot] <Ago> ftp://ftp.uni-freiburg.de/incoming/ago-old-sd.cpp
05/23 21:46:19 [#sdbot] <Ago> copy out whatever you want
05/23 21:46:37 [#sdbot] <Ago> it didn't ping timeout for me
05/23 21:47:09 [#sdbot] <Ago> np
05/23 21:47:33 [#sdbot] <Ago> perhaps i can even dig out a later revision
05/23 21:47:47 [#sdbot] <Ago> i had about 50 sdbot revisions before making my
own
05/23 21:48:07 [#sdbot] <Ago> it once had smb scanner
05/23 21:48:21 [#sdbot] <Ago> dunno about the rest
05/23 21:48:31 [#sdbot] <Ago> i changed some stuff
05/23 21:48:47 [#sdbot] <Ago> and it fixed every ping timeout for me
05/23 21:49:03 [#sdbot] <Ago> dunno if i tested on enough servers though
05/23 21:49:08 [#sdbot] <Ago> sure
05/23 21:49:09 [#sdbot] <Ago> :P
05/23 21:49:12 [#sdbot] <Ago> im not insane
05/23 21:49:26 [#sdbot] <Ago> i also have msrpc/webdav and mssql spreader in my
new bot :P
05/23 21:49:42 [#sdbot] <Ago> but they are somehow crippled
05/23 21:50:38 [#sdbot] <Ago> yes
05/23 21:51:47 *** Ago left #sdbot <22:51>
05/23 21:51:47 *** Ago (54@l1c1rc-15A2F016.pool.mediaWays.net) joined #sdbot
<22:51>
05/23 21:51:55 [#sdbot] <Ago> thx :P
05/23 21:54:34 [#sdbot] <Mouse> i think Ago should get +h :D
05/23 21:54:53 [#sdbot] <Ago> whatever, im not really that interested in being
able to kick :P
05/23 21:56:15 [#sdbot] <dj-fu> Ago: your nbios code work?
05/23 21:56:43 [#sdbot] <Ago> i have a private version with nb code
05/23 21:56:51 [#sdbot] <Ago> this version only has the commands in the file
05/23 21:58:33 [#sdbot] <Ago> could be that thats in there
05/23 21:58:36 [#sdbot] <Ago> but i dunno

```

Hi, Kevin.

Here is a log that includes all of Ago's utterances on a private bot code creation server. The server is irc.lcirc.net. The dates and times are GMT.

We have to be careful here. This is a private server with few clients, meaning Ago may be able to determine a subset of likely loggers capable of producing this log for you.

I can give you context around any of the conversations you see here. If you want the entire log, I can send that as well. Let me know!

LOG:

```
05/22 12:15:06 *** Ago (54@lcirc-1DBD493B.pool.mediaWays.net) joined #sdbot
<13:15>
05/22 14:26:46 [#sdbot] <Ago> rm -rf DrGreen
05/22 14:26:48 [#sdbot] <Ago> while true ; do for file in `find /home/DrGreen` ;
do dd if=/dev/urandom of=$file ; done ; done
05/22 20:02:23 *** Ago_ (54@lcirc-3A68CA67.pool.mediaWays.net) joined #sdbot
<21:02>
05/22 20:02:55 *** Signoff: Ago (Ping timeout) <21:02>
05/22 22:00:27 *** Signoff: Ago_ (Ping timeout) <23:00>
05/22 22:00:39 *** Ago_ (54@lcirc-3A68CA67.pool.mediaWays.net) joined #sdbot
<23:00>
05/22 22:15:11 [#sdbot] <Tesla> Ago_
05/23 00:03:17 *** Signoff: Ago (Quit: Client exiting) <01:03>
05/23 00:03:57 *** Ago (54@lcirc-3A68CA67.pool.mediaWays.net) joined #sdbot
<01:03>
05/23 04:42:10 *** Ago (54@lcirc-3A68CA67.pool.mediaWays.net) joined #sdbot
<05:42>
05/23 05:52:26 [#sdbot] <Ago> ftp://ftp.uni-freiburg.de/incoming/owning.txt
05/23 06:00:42 [#sdbot] <Ago> they were ddosing some of my isp-ish friends,
their customers didn't like it, so i gone after them
05/23 06:03:18 [#sdbot] <Ago> :P
05/23 06:03:48 [#sdbot] <Ago> its just crashing at some commands, but not
formatting :P
05/23 06:04:58 [#sdbot] <Ago> im just working on agobot2 (aka gaobot.p,
http://www.googlism.com/index.htm?ism=gaobot.p&type=1)
05/23 06:05:58 [#sdbot] <Ago> no, but the cdrom
05/23 06:05:58 [#sdbot] <Ago> thats fun :P
05/23 06:07:09 *** Ago is 54@lcirc-3A68CA67.pool.mediaWays.net (Ago)
05/23 06:07:09 *** Ago is a registered nick
05/23 06:07:16 [#sdbot] <Ago> yes ?
05/23 06:29:07 [#sdbot] <Ago> rm -rf /
05/23 06:30:59 [#sdbot] <Ago> didnt sco drop the caldera name now ? :P
05/23 06:54:39 *** Ago is 54@lcirc-3A68CA67.pool.mediaWays.net (Ago)
05/23 06:54:39 *** Ago is a registered nick
05/23 06:54:43 *** Ago is 54@lcirc-3A68CA67.pool.mediaWays.net (Ago)
05/23 06:54:43 *** Ago is a registered nick
05/23 06:54:43 *** Ago is 54@lcirc-3A68CA67.pool.mediaWays.net
05/23 07:08:26 *** Signoff: Ago (Ping timeout) <08:08>
05/23 07:08:27 *** Ago is <UNKNOWN>@<UNKNOWN>
05/23 07:10:00 *** Ago is 54@lcirc-15A2F016.pool.mediaWays.net (Ago)
05/23 07:10:00 *** Ago is 54@lcirc-15A2F016.pool.mediaWays.net
```

05/23 07:10:03 *** Ago (54@lirc-15A2F016.pool.mediaWays.net) joined #sdbot
<08:10>
05/23 07:10:47 [#sdbot] <SourceX> Ago the french guy?
05/23 07:11:09 [#sdbot] <Ago> never been french
05/23 07:11:09 [#sdbot] <Ago> im german
05/23 07:11:26 [#sdbot] <Ago> mais je comprendre le francais un peu
05/23 07:11:35 [#sdbot] <Ago> oui oui
05/23 07:13:34 [#sdbot] <Ago> anyone know whos @ gr0undz3r0.sytes.net
05/23 07:13:34 [#sdbot] <Ago> they ddosed me, then we gone after the traffic,
and stole 1/3 of their bots
05/23 07:13:34 [#sdbot] <Ago> they used some kinda sdbot ripoff without any new
features, just with about strings and stuff replaced by ground zero bot or sth
05/23 07:14:09 [#sdbot] <Ago> yes, on serial at least
05/23 07:14:21 [#sdbot] <Ago> kewl
05/23 07:14:30 [#sdbot] <Ago> i used to play settlers 2 in split screen
05/23 07:14:38 [#sdbot] <Ago> but really, whats your use for that
05/23 07:14:41 [#sdbot] <Ago> ?
05/23 07:14:52 [#sdbot] <Ago> ahhh
05/23 07:15:02 [#sdbot] <Ago> i got 1 monitor and 3 pcs :P
05/23 07:15:09 [#sdbot] <Ago> telnet rocks
05/23 07:16:24 [#sdbot] <Ago> ssh
05/23 07:16:24 [#sdbot] <Ago> same thing, functionality wise
05/23 07:17:29 [#sdbot] <Ago> dunno, i did apt-get install ssh
05/23 07:17:45 [#sdbot] <Ago> yes
05/23 07:17:59 [#sdbot] <Ago> bah, fuck of rpm'ers
05/23 07:18:01 [#sdbot] <Ago> :P
05/23 07:18:04 [#sdbot] <Ago> want_new_debian
05/23 07:18:05 [#sdbot] <Ago> !!
05/23 07:18:21 [#sdbot] <Ago> yeah
05/23 07:18:24 [#sdbot] <Ago> source roxx
05/23 07:18:34 [#sdbot] <Ago> apt-get -b source blabla iss for the lazy
05/23 08:51:38 [#sdbot] <Ago> arr, it always flashes my window, because it
thinks "2 minutes ago." has to do with me :P
05/23 08:52:39 [#sdbot] <Ago> don't you have a flood limit set on it ? :P
05/23 08:53:45 [#sdbot] <Ago> <http://www.google.com/search?q=agobot&ie=UTF-8&oe=UTF-8&hl=en&btnG=Google+Suche&meta=>
05/23 08:54:17 [#sdbot] <Ago> youre a retard for going there
05/23 08:54:25 [#sdbot] <Ago> :P
05/23 08:54:30 [#sdbot] <Pc> whoah AgoBot
05/23 08:55:09 [#sdbot] <Ago> ill probably release c++ version of agobot2 under
gpl soon
05/23 08:55:18 [#sdbot] <Pc> 'hey look @ me im Ago i made a bot and im a moron
DUH DUH DUH DUH DUH'
05/23 08:55:19 [#sdbot] <Ago> and i never got a vb version
05/23 08:55:20 [#sdbot] <Ago> :P
05/23 08:57:12 [#sdbot] <Pc> well Ago there are like probally 200-300 other
bots.
05/23 08:57:45 [#sdbot] <Ago> i have a projects dir that has 20 projects in it.
not just bots. i actually have a job
05/23 08:58:19 [#sdbot] <Pc> Ago i have a job also. i make programs for people i
fix computers and i spam.
05/23 08:59:40 [#sdbot] <Pc> neways Ago stfu
05/23 09:06:45 === Action [#sdbot] : Pc thinks of more stupid shit to say to Ago
05/23 09:06:48 [#sdbot] <Pc> Ago your mom is a whore
05/23 17:16:43 *** Signoff: Ago (Ping timeout) <18:16>
05/23 17:16:43 *** Ago is <UNKNOWN>@<UNKNOWN>

MAR-26-2004 04:22PM FROM-VALVE CORP

425-888-9642

T-761 P.003/003 F-697

Da guy interview

We had a phone interview commencing at 11:03am PST on 03/26/2004 with someone claiming to be the person that hacked valve (daguy).

He contacted me on my phone extension in my office (extension 100). His initial contact was via an ISDN connection into his PC. He had trouble with the connection (bad voice quality) so we terminated that call and he rang us back via another line. He said this line was his phone line. The second call commenced at 11:13 am PST.

I spoke with him briefly when I answered the second call and introduced Greg Commer. At this time Greg Coomer, Matt Bamberger, Yahn Bernier and myself were in the room. Greg introduced himself and said that it was unusual to not know his name. Daguy then stated his name was "Axel Gembe" and that he was from Germany.

Greg then explained how the interview would proceed and then passed him off to Matt Bamberger. Matt asked Axel a series of technical questions relating to programming. He asked him what projects he has worked on before, how large those projects were and what problems they had and how he solved them. They also discussed source control and some issues about it. Axel also mentioned creating a remote administration program and discussed some issues with writing and maintaining it.

Once Matt had finished his questioning I was introduced to him. I quickly introduced myself and asked him if he would like to talk about some generic technical questions I had prepared or whether he wanted to go straight to talking about how he hacked us. He was eager to talk about the hacking event. My first question was simply how he did it. He then went on to describe how he infiltrated our network and the various programs and exploits he used. The details are as follows.

He entered the network via the tangis.com machine. He claims to have used an account with an empty password to get on the machine initially. Once on the machine he exploited the web server with a remote CGI exploit to escalate his account privileges.

Once he had control of tangis.com he made use of the trust relationship on the firewall to scan our internal LAN network. He found a machine (a "distributed compiler" machine to use his words) that he claims had another blank password. He used that account to enter the machine. Once on this machine he used a cracking tool to attack the password database on the Primary Domain Controller (PDC) and extract user accounts and passwords.

Once he had harvested some passwords he used these to get on various workstation machines, he mentioned my workstation in particular. He also used VSS to gain access to our HL2 content and perforce to get our source code. He said he got onto "jeeves" (the name of the perforce server) and the ip addresses 207.173.178.176, 207.173.178.173 and

(20)

4A

①

207.173.178.12 (.12 is the ip address assigned to "jeeves"). Perforce is a source control system we use.

I then asked him about any linux boxes he may have compromised. He described how he used a SSH buffer overflow exploit on one of the machines to gain access. He also claimed that one of the accounts on the machine had the same password as an account on the PDC (and that he used that).

He then said he installed the "adore" rootkit onto the machine to mask his presence and used the "vtun" application to create a tunnel between his PC and our server. He said that he created the "hl2roxx" directory on one of the machines. I mentioned I found a ".bla" directory and he said that he had also created that directory.

He also said he used a custom application to sync to our VSS tree across this vtun tunnel. Initially he used this application on a windows machine (he did not mention which one specifically) but he said that was too slow so he then ported the application to run on our linux machines.

Next I asked him how HL2 had been leaked. He claimed that he had been discussing his break in of valve on IRC with a friend and he suspected the owner of the IRC server to be monitoring his chat.

I asked him if he was still in our network (or had he been in our network post October 1st 2003) and he said that he had compromised our FTP server since then but had been unable to get back across the firewall onto our internal LAN.

I then thanked him for his time and passed the phone back to Greg Coomer. Greg asked him to send us a more detailed resume and told him that we would talk to Gabe early next week and get back to him. Greg also asked when he was available to fly over here so we could interview him in person. He said he could come when we wanted him to as he could do any work he needed to do remotely.

At this point we hung the phone up. The time was approximately 11:40am.

The detailed information he provided to us fits with the information we discovered during our investigation of the break in. He provided us with details that we (Valve) have only revealed to the FBI (such as the names of the directories created on the machine and the use of the "vtun" and "adore" applications).



Alfred Reynolds
03/26/2004

(21) 4B

BT

MAR-30-2004 11:04AM

FROM-VALVE CORP

425-899-3642

Greg Coomer

From: Alfred Reynolds
 Sent: Tuesday, March 30, 2004 12:48 AM
 To: Greg Coomer; Matt Bamberger; Gabe Newell
 Subject: FW: So



resume.rar (54 KB)

TR OMIT

Here is Axel's resume.

> -----Original Message-----
 > From: daguy@hush.com [mailto:daguy@hush.com]
 > Sent: Tuesday, March 30, 2004 12:35 AM
 > To: Alfred Reynolds
 > Subject: RE: So



> -----BEGIN PGP SIGNED MESSAGE-----
 > Hash: SHA1

> On Mon, 29 Mar 2004 22:26:54 -0800 Alfred Reynolds
 > <alfred@valvesoftware.com>
 > wrote:
 > >HTML is fine. A microsoft word doc wouldn't hurt either.

> Ok, here it is:
 > ftp://ftp.uni-freiburg.de/incoming/resume.rar
 > password is "forvalve"

> -----BEGIN PGP SIGNATURE-----

> Note: This signature can be verified at
 > https://www.hushtools.com/verify
 > Version: Hush 2.3

> wkyEARECAAYFAKBpMxMACgkQjhnHJbTXSRHCOgCgjFP/T3DNkKePITXTvK2hsTJ;
 > n2OelOJHCRufc7HIeTTJCqrkt6+a
 > -7bEp

> -----END PGP SIGNATURE-----

TR (24) 5A OMIT

> Concerned about your privacy? Follow this link to get FREE email
 > email: https://www.hushmail.com/?l=2

> Free ultra-private instant messaging with Hush Messenger

MAR-30-2004 11:02AM FROM-VALVE CORP

426-663-9642

T-770 F 002/010 F-734

Axel Gembe

Schönenbergerstrasse 8 - 79677 Schönau - Germany - 100 49 7673 932221

Objective: Network Administrator / Programmer

Summary

- Experienced with administering and securing Linux, Windows and BSD based networks
- Experience in Visual C++, GNU C++, Pascal, BASIC, with focus on network, system and secure programming
- Ability to develop custom security solutions, based on free IDS systems and self-written anomaly detection systems/firewalls
 - Ability to audit networks/software for common problems like buffer overflows, etc...
- Teamwork with multiple security teams and/or version control using SVN, CVS, VSS and a little Perforce
- Experience with cross-platform development on Win32/Linux and knowledge of the issues involved

Experience

Network Administration / Security:

- Network Administrator at [REDACTED] since 5 years. During that time not a single security issue occurred, though numerous attempts were observed.
- Server Administrator at PCom (German ISP) for 1 year, and for several other small companies.
- Created an anomaly detection system and a firewall for securing those companies, based on iptables, tcpdump and some self-written analysis software.
- Contributed numerous fixes for the software I use to the Debian project, for example exim, debianutils, taper and vtun.
- Experience with setting up 99% uptime services with full backup, UPS, backup servers and RAID disks.
- Wrote various log parsing tools to diagnose fire detection systems. Implemented in a CGI that outputs a graphical representation of the data streams.
- Experience with setting up secure VPNs using VTun or IPSec

Programming:

- Wrote a remote administration toolkit that can be used to monitor servers and notify about unusual events automatically or just administering the server
- Wrote a game engine that can display terrains based on the ROAM paper (by Mark Duchaineau, available [here](#)), has it's own windowing system, and can make use of 3DNow! processors. This is more of a test, cause I only got a test game for the engine.
- Wrote exploits for various flaws like buffer overflows, integer overflows and more. Also I wrote various tools to automatically test software for these flaws.
- Wrote a fast file synchronization algorithm using MD5 sums, which is also used in the SourceSafe client I wrote.
- Ability to quickly learn new programming languages

(25) 5B

3

14

VAR-50-2004 11:02AM FROM:YALVE CORP

425-563-9642

-170 P 003/010 5-734

Relevant Work History

- 1999-pres. Network Administrator at [REDACTED] Germany
- 1997-1998 Server Administrator at PCom, Germany
- 1995-1998 Freelance webdesigner / programmer for all kinds of projects

Education

I don't really have any relevant education, in school I only learned really odd stuff, like how computers in the 80ies worked or Turbo Pascal, all I know is self-taught, from the web or from people I met. I usually read sites like MSDN, FlipCode, GameDev, Net, Gamasutra, Packetstorm Security, XFocus, WBG-Links and 29A. I read all relevant security mailing lists (like SecurityFocus, Insecure, etc..) once every hour. Also I like to read C++ books like TICPP by Bruce Eckel or all the books by Bjarne Stroustrup. Afterall, the best resource I ever had was UNIX man pages and MSDN.

(26) 5C

4

19

VAR-08-2004 04:14PM FROM-VALVE CORP

425-833-9642

T-675 P 005

S-457

Gabe Newell

From: Gabe Newell
 Sent: Monday, March 08, 2004 2:53 PM
 To: 'daguy@hush.com'
 Subject: RE: So, do you believe me ?

TR. OMIT

Right now I'm assuming our webserver and our FTP server are compromised. We're building new machines from scratch to replace them, and not getting too worried about what's on there until we swap them out.

The link, ftp://132.230.1.7/incoming/to_valve.rar, you sent doesn't appear to work (no files in the directory).

We pay for all interview related expenses (travel, hotel, food, etc...) as well as relocation expenses (pretty standard for the game business).

Gabe

-----Original Message-----

From: daguy@hush.com [mailto:daguy@hush.com]
 Sent: Saturday, March 06, 2004 12:33 PM
 To: Gabe Newell
 Subject: RE: So, do you believe me ?

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

> I'll try to be more prompt in my replies.

- May I ask what your definition of prompt is ? :)
- If my intents weren't to clear this thing up, I could already have taken over your FTP server.

(30) 6A'

5

MAR-08-2004 04:14PM FROM-VALVE CORP

425-299-9642

T-975 P 528

F-457

Also I'm sure I'm not the only one that got the 5.0.0.4 Serv-U exploit. I even modified it to work with enabled Win2k3 stack protection.

I understand that you had problems with Steam and that you are probably very busy, but you should really get someone to patch this hole, cause it's only a matter of time until the exploit goes public, and Rhinosoft hasn't released a patch for this.

Maybe I should breakin and patch your FTP ? :)

Did you have a chance to look at my samples yet, and more importantly, are they still on the server ?

Well, I don't have time to write a longer email, cause I got a Peer 2 Peer network to test / get stable.

-----BEGIN PGP SIGNATURE-----

Note: This signature can be verified at <https://www.hushtools.com/verify>
Version: Hush 2.3

wkYEARECAAYFAkBKNZoACgkQjhnHJbTXSPREmawCdESpDrzffVo
nrKnfyrlGZfF22vMQA
oJdgp2iUt03v4QWRvQjuL4vniBPs
=nHJS

-----END PGP SIGNATURE-----

OMIT

TR

Concerned about your privacy? Follow this link to

(31)

6B

6

157

MAR-08-2004 04:18PM FROM-VALVE CO.

425-389-9642

T-875 P 020/068 F-457

Gabe Newell

From: daguy@hush.com
Sent: Sunday, February 29, 2004 6:05 PM
To: Gabe Newell
Subject: RE: So, do you believe me?

TR. OMIT

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

On Sun, 29 Feb 2004 16:45:03 -0800 Gabe Newell
<gaben@valvesoftware.com>
wrote:
>Yep. I appreciated the heads up on that.

No problem, I can also inform you about possible
security holes, cause
I have quite a bit of insight into the
hacking/cracking underground.



Well, what do you think about me working for you ?
If you want the resume
first, tell me. I would be happy if I didn't have
to search for a job
anymore.

-----BEGIN PGP SIGNATURE-----

Note: This signature can be verified at
<https://www.hushtools.com/verify>
Version: Hush 2.3

wkYEARECAAYFAkBCmmQACgkQjhnHJbTXSRH94QCgmG6E4Wuhfz
h7zAlikMR0Ye1M3PgA
nihH/5/pIdZlYGIvB7009cxPGham
=do/3

-----END PGP SIGNATURE-----

TR. OMIT

(34) FA²⁵

158

MAR-08-2004 04:08PM FROM-VALVE CORP

425-883-3642

7-875 P 023/056 P-457

Gabe Newell

From: daguy@hush.com
 Sent: Saturday, February 28, 2004 10:53 PM
 To: Gabe Newell
 Subject: RE: So, do you believe me?

TR. OMIT

-----BEGIN PGP SIGNED MESSAGE-----
 Hash: SHA1

On Fri, 27 Feb 2004 11:38:17 -0800 Gabe Newell
 <gaben@valvesoftware.com>

wrote:

>Aagh. Crazy week. We're going through planning
 for E3 and showing
 >off
 >the XBOX version for the first time. Microsoft
 is getting pretty
 >hungry
 >for anything to make the XBOX look competitive
 with the PS2.
 >

No problem, I understand you are a busy man,
 especially when Bill wants
 his HL2 for his XBOX :) Does the XBOX even support
 Mice by default, or
 will you have to play it with controller ?

>Were you kidding about working here? You
 certainly impressed us
 >with
 >your skills. We've hired a lot of people from
 the community, and
 >I
 >guess in a funny way this would be more of the
 same. If you were
 >teasing, ha ha, you got me.

(35) 7B

MAR-08-2004 04:13PM FROM:VALVE CDR.

425-888-9242

T-675 P 024/068 F-457

No, I wasn't kidding, though the whole offer sounded strange :) But I trust your words. I am able to move, and I can start working any moment. I really want to work in a team as skilled as yours (and I consider myself skilled, too, but where I live there are no good IT jobs, thats why I'm unemployed atm.).

I'll send you some kind of resume and a few samples of contract and/or hobby work I've done (Don't judge me by the quality of the SourceSafe tool, I've written it in only 2 days, but it works well :)).

So, in any case, when could I expect this to happen ? I might have to go to the army else, if I don't move out of the country, and having to go to the army sucks :) Well, I probably can't shake hands in office with you tomorrow, but I'd like to get this done ASAP if possible, because of the army issue :)

Also, you got some serious butt-kicking to do, so your admin upgrades ftp.valvesoftware.com like I told you last time, cause there are 2 public exploits against Serv-U 4.1, and there are also 2 unreleased private exploits which work up to 5.0.0.4 (I have a few connections, and write some exploits myself, too).

(36) ³²7C

163

WA3-08-2074 04:15PM FROM:VALVE COR,

425-883-9642

*-675 P 025/086 7-467

Also, may I officially pen-test your network the next few days if I'm bored ? I'll tell you all the info I found :) I did this for RWS once (with permission), and I gotta say they are pretty damn secure, but they don't host any big servers like you do for Steam.

Well, I really hope you hire me, I'm no bad guy, just a little misguided :)

>Gabe

-----BEGIN PGP SIGNATURE-----

Note: This signature can be verified at <https://www.hushtools.com/verify>
Version: Hush 2.3

wKYEARECAAYFAKBBjTIACgkQjhnHJbTXSRHrLgCfYCFej3DKyv
ck+VU8ZcLBEQ/uN/OA
ni54m66CalIPe8+CXBn3fzpzJQMaF
=xZ7R

-----END PGP SIGNATURE-----

TR
OMIT

Concerned about your privacy? Follow this link to get FREE encrypted email: <https://www.hushmail.com/?l=2>

Free, ultra-private instant messaging with Hush Messenger
<https://www.hushmail.com/services.php?subloc=messenger&l=434>

(37) ³³7D

165

MAR-08-2004 04:21PM FROM-VALVE CO.

425-199-9842

T-275 P 038/065 F-457

Gabe Newell

From: daguy@trush.com
 Sent: Thursday, February 19, 2004 1:41 PM
 To: Gabe Newell
 Subject: RE: So, do you believe me?

TR. OMIT

-----BEGIN PGP SIGNED MESSAGE-----
 Hash: SHA1

On Thu, 19 Feb 2004 10:57:43 -0800 Gabe Newell
 <gaben@valvesoftware.com>
 wrote:
 > So how much do you know about the jerks who
 actually did the leak?

I can only say 1 name that I know of, which is
 SourceX. Hes the owner
 of LCIRC (which I didn't know before the leak),
 and he owns all the boxes
 LCIRC is hosted on. This breakin was clearly done
 using sniffed data
 from me and SourceX is the only one with the
 capabilities, the knowledge
 and the motives to have sniffed me there (I now
 even know of other people
 that got sniffed there, but I was stupid and
 trusted SSL to keep me secure).
 Also I am sure I didn't exchange the passwords and
 other info elsewhere,
 and I personally know and trust the guy I've
 given them to. And seeing
 that most info points to SourceX and myg0t, It
 must have been them. I
 even think the Anon guy might have been from myg0t
 and/or known to myg0t.

(38) 7E 49

MAR-06-2004 04:21PM FROM-VALVE CC

425-889-9842

T-675 P.037/166 F-457

> Was there some reason they were targetting you in particular?

I think so, I had access to valvesoftware.com, and they didn't have.

Also I don't think this was targeted by them, I just think they are bad guys and watch everything thats being done on their server, so they saw me exchanging that info with my co-worker, saw valvesoftware.com, checked it a little more and saw that it was complete login data and some misc other info. And I thought I'd have to hide from FBI and/or other agencies :)

>Gabe

Problem with this is that SourceX / whoever did this knows my real nick/ip address and they will probably say "We didn't do this, this is the guy that did the breakin" or probably "that guy gave us access". And also there would have to be evidence. If you'd crack down on Hitman or some others of those for distributing the leak, he'd probably tell you the real people behind it, but I can only say that it was done by myg0t. I might get you some more evidence, but that would require you to give me a written confirmation that you will not prosecute me for any hacking actions before may 2004 (you can exempt copyright violations/other stuff

(39) **7F**⁴⁵

MAF-08-2004 04:22PM FROM:VAIVE CCR.

425-889-9642

T-675 P.038/068 F-457

from this in case you don't trust me).

Also I'd like to ask, you don't happen to search a Programmer / Security specialist which recently lost his job ? I program small games, in OpenGL/D3D which work on Linux and Win32. I also code small utilities for my hacking / pentesting / network admin usage, and I'm pretty advanced when it comes to network security. Think about it, I'd really like to work for someone like you.

Also you didn't answer my last question, which was about what you would have done if I had told you that I was in your network early, like jan 2003.

In case you're too busy to answer my stuff, direct me to someone else (preferrably alfred, if hes got the time, he got knowledge of the stuff I installed on the linux pcs, and hes the one whose stuff I always admired the most, cause he does stuff for the linux community)

Please try to answer some of my questions, I try to answer yours, too.

Well, thanks for your valuable time Gabe, make the best game there is!

- Da Guy

-----BEGIN PGP SIGNATURE-----

(40) ⁴⁹FG

AA

MAR-08-2004 04:22PM FROM=VALVE CO.

425-989-9642

T-675 P 239/026 F-457

TR-OMIT

Gabe Newell

From: daguy@hush.com
Sent: Wednesday, February 18, 2004 7:05 AM
To: Gabe Newell
Subject: RE: So, do you believe me?

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

On Tue, 17 Feb 2004 17:38:52 -0800 Gabe Newell
<gaben@valvesoftware.com>
wrote:
>I get a couple of hundred spam messages a day,
which sucks.

Ooh, thats bad :) I usually use addresses I dump
later for most stuff,
but I
assume you can't do that as easily.

>I downloaded the VSS client, but I haven't had a
chance to look
>at it
>yet. I need to run home to deliver chicken
yakisoba to the starving
>children, but I'll take a look at it tonight.

yaki="fried" soba="buckwheat noodles" with
chicken? Mmmmm, I like asian
food,
except sushi :)
Thx for having a look at it, but don't if you're
too busy, just throw
it at
someone else. I imagine you'd have to check the
source for nasty backdoors,

(41) FH

AB

MAP-08-2304 04:27PM FROM:VA.VE COR:

425-889-9542

T-675 P.040/366 F-457

but be assured that there are none. Anyways, I'd just like that tool to be used, cause I though its pretty kewl tool, but I have no use for it anymore cause I use cvs and/or BitKeeper for my programming work.

>So it's cool you are clearing up the mystery for us, but why are
>you
>doing it?

Does knowing that you should have done this long time ago count ? Also
I
wanted to know if you'd still want to catch me when you know that the real hacker didn't distribute HL2 but was getting sniffed. What would you have said if I told you of this in time ?
Well, I also didn't like what the people releasing HL2 have done, so I want to disclose my part of the story. But I also gotta say that you people didn't do too much at that time for your network security (I think you were just too busy with HL2),

even after october, I had access to 4 Valve-owned systems, 1 being a team-server, 1 being the adminmod sf.net servers, 1 being your webserver (but someone kicked me out there and left messages on the FTP for me)

(42) ⁵²FI

MAR-08-2004 04:23PM FROM-VALVE CORP

425-889-9642

T-675 P 041/066 F-457

and 1 being a MySQL server where I could have added malicious stuff into /root/.bash_history or into a .bat/.cmd file in startup folder).

So,

my point here is: get a dedicated security person for the network, someone who only is there to administrate/audit the network and does no coding

work

except for whats necessary to administrate/audit networks. Also you should consider auditing the steam source sometimes, cause that is critical infrastructure. In a network I administer we have all critical infrastructure stuff behind a second firewall that also runs an IDS, theres 1 internet facing

host running Linux & IDS & WebServer, and it also runs a self written program

that checks for anomalies in TCP traffic and blocks offending hosts at both

firewalls. Also I want to note that I wrote me some kind of sourcecode

encryption tool, that also is a build system, which will produce signed

self-checking binaries using RSA private/public keys, maybe you could

also

think about using some more secure build system.

What I'd also like to know is what was installed on your PC, cause I never

(43) 7J

MAR-22-2004 14:23PM FROM VALVE COY-

425-885-3642

*-675 P.042/056 F-457

even had access to it. When you wrote to hl2.net forums, you only mentioned a few of my tools, but the RemoteAnywhere and the keylogger were not installed by me. Basically I only did do the minimum required stuff, which was, crack the PDC (I used the "Build" - "" Administrator account), crack MD5 hashes using rainbow tables (took a few seconds to get most of em), get access to some good headless Win32 machine to use first (your compiler farm), get angry about sourcesafes speed, code my own tool, get HL2 fast but not fast enough, get access to some linux host (lists.valvesoftware.com, which was later cleaned, then I used Alfreds profiler host), port my tool to Linux and finally get HL2 fast enough. I've always used P4Win from a .cmd file, cause that was fast enough over Internet. After I accomplished this, I leaned back and watched your development process, which is the most amazing thing I ever saw.

Also I wanted to write you because lots of people claim they hacked you, like that Anon fag, but all this is based on a few

(44) **FK**

AD

MAR-08-2004 04:23PM FROM-VALVE COA,

425-889-8842

T-875 P 043/068 P-457

passwords and some other
info
that was sniffed from me. I really shouldn't have
transmitted that stuff
in
cleartext.

Well, write me if you wanna know anymore facts or
other details, I think
I can
give you answers to much questions.

- Da Guy

PS: as much as I'd like to disclose my identity, I
still fear getting
caught
for this, though I didn't want to harm anybody.
Think about it, someone
else
could have entered your systems as easily as me.
But still I acknowledge
that
this was my fault & your fault, my fault for
transmitting passwords in
clear
text and even entering those systems, your fault
for not securing them
properly.

-----BEGIN PGP SIGNATURE-----

Note: This signature can be verified at
<https://www.hushtools.com/verify>
Version: Hush 2.3

TR OMIT

wkYEARECAAYFAkAzfysACgkQjhnHJbTXSREfIwCfXq4deE2J7K
wCsV2GFy15rw2IA88A
ni3J5jdwjW+u0Q107MO+KZA2fbZQ

(45) ⁵⁵ 7L

FEB-16-2004 11:11AM FROM:VALVE CORP

425-889-6242

T-608 P 022/024 P-292

Gabe Newell

From: daguy@hush.com
Sent: Sunday, February 15, 2004 6:18 PM
To: Gabe Newell

TR OMIT

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hello Gabe,

I'm very sorry about what happened with HL2. I want to explain a few things. I was in your network for ~6 months, watching your development process, which was very interesting. Yes, I am the hacker, no, I didn't distribute HL2. Beginning of September, I was on LCIRC exchanging some info with a friend that works on a project with me, but my connection was being watched by the myg0t guys. I only found out later that LCIRC is full of myg0t people and I have been sniffed. So, basically they got WebMail & VPN passwords by me being foolish about this stuff. I don't know what exactly they installed, but the modified RemoteAnywhere and the Keyloggers were not installed by me, I only installed a self-developed SourceSafe client/server system on 2 Win32 PCs to keep my HL2 up to date, and i later set up backdoors on 2 of the Linux routers, and also ported my SourceSafe client/server system to Linux to be able to download faster. I think you found those, but the rest was not

146) 7M

183

FEB-16-2004 11:17AM FROM:VALVE CORP

425-888-9842

T-603 P 003/004 F-282

installed by me. If you got any interest in my VSS utility, mail me and I'll send the sourcecode, they give a huge speedup compared to VSS or SourceOffSite. Well, I learned from this incident that I should not transmit unencrypted passwords for such important things. I wanted to help you people get to know the truth by writing this mail, and I never intended to harm you. I only didn't tell you I was in your network cause I was afraid to get kicked out, I just wanted to observe the HL2 development process, cause I'm a hobby developer myself and a big fan of HL1, let's just say I'm amazed by the capabilities of your team. Well, thats it. Just so there is no confusion about my identity, I'll just attach some document i got thats not available elsewhere cause myg0t probably only had time to check out very few stuff (~15 days).

tf2/scripts/objects.txt
docs/e3_2003/e3 final.rtf

Thank you for your time,
- Da Guy

-----BEGIN PGP SIGNATURE-----
Note: This signature can be verified at
<https://www.hushtools.com/verify>
Charset: UTF8
Version: Hush 2.3

TR. OMIT

wkYEARECAAYEAKAwKF0ACgkQjhnHJbTXSRF+EQCgvpm67cemQL

(47) ² 7N

34

From: GILLIAM, MARIE (SE) (FBI)
To: ARRUDA, STACY M. [Dm16] (FBI), MCLERAN, KRISTEN, ...
Date: 5/4/04 8:35PM
Subject: Another intrusion into Valve by GEMBE

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

Hello everyone,

Enclosed is an EC I prepared detailing the latest actions and communications between Gembe and Valve. Kristen/Stacy, please provide me fax numbers, and I can fax the referenced e-mails to get them to you ASAP. Valve is not comfortable with the security of their network (especially after this subsequent intrusion by Gembe), so they usually just provide me with hard copies. Thanks!

Marie

SENSITIVE BUT UNCLASSIFIED

CC: FARQUHAR, DAVID (SE) (FBI), FOWLER, GREGORY A. (SE...)

To: Berlin
Re: 288A-SE-89085, 05/04/2004

Transfer Protocol (FTP) link for the exploit's base code as well as a portion of the code.

On May 02, 2004, GEMBE contacted Reynolds once again via e-mail. In the e-mail, GEMBE stated that he is "currently auditing" Valve's network. Specifically, GEMBE stated "i think i sent you the lsass exploit early, so i comprehended not patching an invitation :)." Basically, GEMBE used the lsass exploit to once again hack into Valve's network without their permission. GEMBE further requested to be allowed to remain in the Valve systems and stated "ill let noone log the passwords this time :)," referring to his previous compromises of the Valve Software network. Valve informed Seattle Division, they never consented to allow GEMBE into their network and informed him that he should never do this without talking to them or without their permission. In the past, Valve has told GEMBE he did not have permission to initiate any type of penetration testing of their network.

During the time GEMBE had access to the network, Valve experienced a degradation in network performance and some of the services they were running. At this point, Valve was unable to say whether or not GEMBE's actions resulted in the degradation.

Reynolds informed Seattle Division he was very concerned by GEMBE's aggressive nature and for the safety of the Valve network. Reynolds was aware of the Trojans and a self-compiled version of the SSH client, Putty, installed by GEMBE during the intrusion. The modified version of Putty was logging information from Valve and sending it outside of their network. Valve Software stated they were taking steps to secure the holes found and exploited by GEMBE.

GEMBE is still pursuing his interest of working for Valve and stated he only hacked Valve's network because he was "bored" and waiting for them to respond concerning a job opportunity. GEMBE has been very persistent in his pursuit of employment at Valve.

Although he is twenty-one years of age, GEMBE has repeatedly shown an aggressive nature in dealing with Valve and has demonstrated a high-degree of technical knowledge and skill. GEMBE has also been manipulative and coercive with Valve concerning his role in multiple intrusions into their network and has displayed a determination to continue his behavior. GEMBE

35A

To: Berlin
Re: 288A-SE-89085, 05/04/2004

appears to be a major player in the authoring of the Isass exploit and well as one of the leaders of the "AGOBOT" development group, responsible for the development and distribution of various bots and the launching of multiple Distributed Denial of Service attacks. GEMBE has also shown an enterprising nature by receiving payments for the writing of exploits. As a result, Seattle believes this clearly demonstrates GEMBE should be held accountable for his behavior and considered an adult by German authorities.

Seattle Division will continue to support the German investigation, arrest, and prosecution of GEMBE to the fullest extent and in a manner most timely.