

**United States District Court**

**STATE AND DISTRICT OF COLORADO**

UNITED STATES OF AMERICA,

v.

JOHN DOE,  
a/k/a RAFAEL NUNEZ  
a/k/a "RaFa"

**CRIMINAL COMPLAINT**

CASE NUMBER: 03-1129M

I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief:

On or about June 10, 2001, in the State and District of Colorado, defendant JOHN DOE, a/k/a RAFAEL NUNEZ, a/k/a "RaFa" knowingly caused the transmission of a program, information, code or command, and as a result of such conduct, intentionally caused damage, without authorization, to a protected computer in violation of Title 18 United States Code, Section 1030(a)(5)(A)(i).

I further state that I am Special Agent Joseph Diebert, Defense Criminal Investigative Service and that this complaint is based on the following facts: See affidavit attached hereto and incorporated herein.

Continued on the attached sheet and made a part hereof:  Yes  No

*Joseph Diebert*

Signature of Complainant

Sworn to before me, and subscribed in my presence

5-12-03 5:05 PM at Denver Colorado  
Date City and State

**Craig B. Shaffer, United States Magistrate Judge**

Name and Title of Judicial Officer

*[Signature]*  
Signature of Judicial Officer

## **AFFIDAVIT OF JOSEPH DIEBERT**

I, Joseph Diebert, being duly sworn, hereby declare and state:

1. I am a Special Agent for the Department of Defense (DoD), Office of Inspector General, Defense Criminal Investigative Service (DCIS), assigned to the Denver Resident Agency. I have been employed by the DCIS for over 8 years, and I have been assigned to the Denver, CO office since 1998. During my career as a Special Agent with the DCIS, I have been assigned to investigate numerous crimes involving DoD interests, including computer crimes. I have participated in investigations involving the execution of search and seizure warrants, which have resulted in the seizure of computer-related equipment, media and data files evidencing fraud and other criminal activities. I have received specialized training in the investigation of computer, telecommunications, and other “high technology” crimes directed at the DoD. I have also received computer investigative training at the Federal Law Enforcement Training Center and the Defense Computer Investigations Training Center.

2. As a DCIS Special Agent, I am conducting an investigation into violations of Title 18, United States Code, Section 1030(a)(5)(A)(i) (Intentionally doing damage to a protected computer) arising from intrusions into the computer system at the Defense Information Systems Agency in Denver, CO, which occurred in June 2001, and is further described below. Based on the information below, probable cause exists to believe that, on or about June 11, 2001, JOHN DOE, aka “Rafael Nunez” aka “RaFa” violated 18 U.S.C. § 1030(a)(5)(A)(i) by intentionally causing the transmission of a program, information, code or command, and as a result of such conduct, intentional intentionally causing damage, without authorization, to a protected computer.

3. The information contained in this affidavit is based on my investigation and training, and/or from information relayed to me by DCIS agents or other law enforcement agents. Because this affidavit is being submitted for the limited purpose of providing probable cause

regarding the criminal offense listed above, I have not included every detail regarding my investigation.

### **DISA Computer Intrusions**

4. On June 11, 2001, personnel of Defense Information Systems Agency (DISA) in Denver, CO discovered that the web-based server network that provides computer based training (CBT) for thousands of U.S. Air Force personnel per day was inaccessible. All related services on the DISA CBT servers were stopped. Upon restart of the servers, a new home web page was displayed on the DISA CBT web site. The new unauthorized web page read, in part, "woh is Back...and kiss my ass cause I just Owned yours! – America's Air Force Department of Defense computer system Own3d by [RaFa] [woh@world-of-hell.com](mailto:woh@world-of-hell.com) – <http://www.world-of-hell.com>". Analysis of the DISA Denver CBT log files by the DISA Regional Computer Emergency Response Team (RCERT) indicated that on June 10, 2001, an unknown individual(s) gained unauthorized access to the DISA CBT servers using a vulnerability "hack".

5. On June 15, 2001, I met with, Robert Blanchard, who at that time was a contract DISA systems administrator at the DISA MegaCenter, Denver, CO, who told me the following:

(a) A review of the defaced server's logs indicated that on June 10, 2001, at approximately 8:37 p.m. (MT) an unknown individual gained unauthorized access to two DISA CBT servers using a vulnerability attack directed at the virtual address of two shared servers at the DISA Denver Mega Center. Since the servers were operating as a group, the commands sent during the intrusion by the unknown individual were divided between the two DISA servers based on the load of each server at the time each command was sent during the intrusion.

(b) The server logs indicated that the unknown individual was possibly using a "script" or set of commands pre-programmed to execute and perform a certain function during the intrusion. The unknown individual also attempted to alter the computer logs to hide his unauthorized access into the DoD system. This attempt was not totally successful, again due to the network sharing aspects of the clustered servers.

(c) The logs indicated that the unknown individual had succeeded in placing several files on the DISA servers.

(d) Actions from this unauthorized access into the DISA systems caused one of the two DISA servers to “crash” at approximately 8:54 p.m. (MT) on June 10, 2001.

(e) Approximately one hour later, an individual again gained unauthorized access into the second DISA server, which had remained operating after the first attack. This unauthorized access succeeded, and the server logs were altered to hide the unauthorized activity. The actions from this unauthorized access into the second DISA system caused the second DISA server to crash.

6. The DISA systems administrator then explained to me that a review of the logs and files left by the unauthorized intruder located a file named “default.htm,” which appeared to have been placed on both DISA servers by the unauthorized intruder. Both files contained the following: “woh is Back...and kiss my ass cause I just Owned yours! – America’s Air Force Department of Defense computer system 0wn3d by [RaFa] – [woh@world-of-hell.com](mailto:woh@world-of-hell.com) – <http://www.world-of-hell.com>.”

7. Robert Blanchard also advised me that the domain name of the affected server is [www.afcbt.den.disa.mil](http://www.afcbt.den.disa.mil).<sup>1</sup>

**DCIS Denver Resident Agency World-of-Hell Investigative Efforts:**

8. On June 27, 2001, I initiated an investigation into the unauthorized access and web page defacement of the DISA Denver, CO servers on approximately June 10, 2001 by the World-of-Hell hacker group. As part of my investigation, I located the World-of-Hell web site on the Internet and I reviewed it on numerous occasions after the unauthorized computer intrusion into the DISA Denver servers. From my multiple reviews of this web site, I learned the following:

---

<sup>1</sup>Based on my training and experience in investigating computer crimes, I have learned that a domain name is the common alpha-numeric name associated with a corresponding Internet protocol address for a web site or other place on the Internet.

(a) The World-of-Hell web site, [www.world-of-hell.com](http://www.world-of-hell.com), indicated that the group began its exploits in March of 2001. According to the web site, members of the World-of-Hell group included: Cowhead2000, Sybek, dawgyg, Messiah-X, TheSlacker, FonE\_TonE, RaFa, Rubix, n0|d, Virulent and vandal.

### **Cowhead2000 Investigative Efforts<sup>2</sup>**

9. My further review of the World-of-Hell web site disclosed that at least one individual claiming to be a member of the World-of-Hell group allegedly witnessed an incident of vandalism at the Alexis Park Hotel and Resort during a hacker's convention in Las Vegas, NV, in July 2001. In or about July 2001, I had a copy of this vandalism incident report forwarded to me from Alexis Park Hotel & Resort's security department. I reviewed the incident report, and I learned that there was a member of the World-of-Hell hacker group who used the alias Cowhead2000. Cowhead2000 was identified as a fifteen-year-old juvenile who resides in Bartlett, TN. I then conducted Internet searches, and I found eight web page defacements attributed to Cowhead2000.

10. Thereafter, at my request, on November 27, 2001, DCIS Special Agents (SAs) G. Kyle Fach, Nashville, TN, and Mark Hollomon, New Orleans, LA, interviewed Cowhead2000 at his home in Memphis, TN. SA Mark Hollomon then advised me, in part, of the following regarding the interview of Cowhead2000 on November 27, 2001:

(a) Cowhead2000 was interviewed in the presence of his mother and his stepfather. Cowhead2000, a juvenile and a member of the hacker group World-of-Hell, is exclusively known within the group as Cowhead2000.

(b) The DCIS SAs asked Cowhead2000's parents for permission to image the material from their son's computer hard drives. Cowhead2000's parents signed a DCIS consensual search authorization form, and the DCIS SAs began the imaging process on one of

---

<sup>2</sup>If requested by the Court, I will divulge the true identity of "Cowhead2000." However, because Cowhead2000 is a juvenile, his hacker nickname is used herein.

three hard drives. The initial drive took 2.5 hours to image, so the DCIS SAs asked Cowhead2000's mother for permission to remove the other two hard drives and take them to the DCIS lab for duplication. Cowhead2000's mother gave her permission for the DCIS SAs to remove the hard drives with the understanding that the hard drives would be returned when duplicated.

(c) Cowhead2000 stated to the agents that he had not hacked or defaced any web sites since the spring of 2001. When the DCIS SAs confronted him with a list of web site defacements, which I had provided to them to question Cowhead2000 about, he admitted to those web page defacements but did not admit to any others. Cowhead2000 stated to the agents that the World-of-Hell group, of which he is a member, targets large corporations' web sites to expose unsecured servers. Cowhead2000 identified the World-of-Hell membership to include Rubix, e-force, vandal, n0/d, dickw33d, dawgyg, and RaFa.

(d) Cowhead2000 told the agents that RaFa was at one time a member of the group World-of-Hell, who formerly lived in Venezuela, but Cowhead2000 believed that – as of the time of the November 2001 interview – RaFa lived near Paris, France. SA Hollomon also advised me that Cowhead2000 left a voice mail message at SA Holloman's office after the interview stating that RaFa is actually Raphael Nunez ("Raphael" is agent's phonetic spelling), a U.S. citizen from South Florida.

(e) Cowhead2000 also told the DCIS SAs that he communicated with members of the World-of-Hell mainly via IRC (Internet Relay Chat) and ICQ (I Seek You).<sup>3</sup> Cowhead2000 stated that he did not trade in stolen credit cards but that some stolen credit card numbers may be located on his hard drives. In addition, Cowhead2000 indicated that he may have some child pornography on his hard drives, but only by accident if the images were included in downloads of other pornographic images.

---

<sup>3</sup> Based on my training and experience, I have learned that IRC and ICQ communication software provides users with real time, peer to peer (person to person), communication over the Internet.

11. On December 6, 2001, I provided the Defense Computer Forensics Laboratory (DCFL), Linthicum, MD with background information to be used in the analysis of the three hard drive images obtained through DCIS consensual search authorization on November 27, 2001 at the residence of Cowhead2000, as described above. I requested that the DCFL analyze Cowhead2000's hard drive images to gather evidence regarding possible illegal computer hacking activity by Cowhead2000, RaFa, and other members of the World-of-Hell. I also requested that the analysis include examining the hard drives for: IRC/ICQ logs, evidence of stolen credit card information, computer exploits, e-mails, IP addresses for the DISA Denver site, the .mil sites, the .gov sites and the web page defacements attributed to Cowhead2000, child pornography, and other evidence of hacking activity.

12. In January 2002, the DCFL provided me with ICQ log files and other evidence obtained through the forensic analysis performed on the imaged hard drives of Cowhead2000. The Cowhead2000 ICQ log files provided by the DCFL disclose extensive ICQ communications between Cowhead2000 and RaFa; and Cowhead2000 and other members of World-of-Hell from March 2001 through November 2001. The subjects of the conversations between Cowhead2000 and RaFa, in part, include: (i) web page defacements, (ii) the use of the web site alldas.de (also known as alldas.org) to post web page defacements;<sup>4</sup> (iii) the alleged use and possession of stolen credit card numbers; (iv) lists of World-of-Hell members; and (v) discussions regarding the "Feds" looking for RaFa. Narrative from the aforementioned ICQ conversations between Cowhead2000 and RaFa are provided in part in the following excerpts (spelling was taken from ICQ logs):

- a. 06-07-2001 ...(Cowhead2000) heh... are you brazilian?  
06-07-2001 (RaFa) nope Venezuelan.  
06-07-2001 (Cowhead2000) ahh... I was close, yer name sounded like brazilian or italian or something like that... what languages you know?

---

<sup>4</sup>Based on my training and experience, I know that "alldas.org" is a website that, in 2001 and at least some of 2002, posted computer hacks and web page defacement information, including the web site address; the hacker nickname claiming credit for a particular hack; and in some instances, a copy of the actual web page defacement known as a "mirror," as described further in ¶ 27.

- 06-07-2001 (RaFa) nope Venezuelan.  
 06-07-2001 (Cowhead2000) can you speak italian?or read it?  
 06-07-2001 (RaFa) yes ....
- b. 06-11-2001 (RaFa) <http://afcbt.den.disa.mil/>
- c. 06-08-2001 (RaFa) I'm buying the domain 3 woh ... where do u want world-of-hell 2 go?  
 06-08-2001 (Cowhead2000) are you paying for em or carding em?  
 06-08-2001 (RaFa) carding.. but is like paying don't worry  
 06-08-2001 (RaFa) SO, where do u want world-of-hell 2 go?  
 06-08-2001 (Cowhead2000) I know, I was gonna say you better'd card em or youll be screwd, I dunno, I think were getting rdy to be hosted by epic, so ask him if hes set anything up  
 06-08-2001 (Rafa) dude ! I'm buying just an Alias of [www.world-of-hell.com](http://www.world-of-hell.com) org. net ... just tell me The right URL u wanted redirect
- d. 06-07-2001, (RaFa): <http://www.teach.com/>... done...  
<http://defaced.alldas.de/mirror/2001/06/06/www.teach.com...>  
 06-07-2001 (Cowhead2000) ...if you can get back in, don't deface it till mornin then send it in, cause alldas wont get it at niht...  
 06-07-2001 (RaFa) ...k...there?...  
 06-07-2001 (Cowhead2000) somewhat  
 06-07-2001 (RaFa) <http://www.teach.com>  
 06-07-2001 (Cowhead2000) nice...
- e. 06-09-2001 (RaFa) ... so dude.. I.. ll put ll W0h is back.. Send Money to [money@logos4u.tv](mailto:money@logos4u.tv) ? like it ?  
 06-09-2001 (RaFa) just that?  
 06-09-2001 (Cowhead2000) yeah  
 06-09-2001 (RaFa) and kiss my ass cause I just OwnZ you ! ?  
 06-09-2001 (Cowhead2000) kiss my ass cause I just Owned yours  
 06-09-2001 (RaFa) ok ...
- f. 06-09-2001 (RaFa) =) <http://www.world-of-hell.com> ... <http://www.world-of-hell.org> ... <http://www.world-of-hell.net>  
 06-09-2001 (Cowhead2000) c000  
 06-09-2001 (Cowhead2000) now set me up a godamn shell on yer box  
 06-09-2001 (RaFa) I'll make the alias ... [cowhead2000@world-of-hell.com](mailto:cowhead2000@world-of-hell.com) ...  
 dude I can't I have NT
- g. 06-15-2001 (RaFa) ... k hey dude WoH is being famous and famous.. don u think we need to stop defacing ? for this days.. ?  
 06-15-2001 (Cowhead2000) hell no  
 06-15-2001 (RaFa) I'm a little screwed..lol  
 06-15-2001 (Cowhead2000) why?  
 06-15-2001 (RaFa) the feds, etc.. or that is shit?  
 06-15-2001 (Cowhead2000) shit  
 06-15-2001 (RaFa) ok  
 06-15-2001 (Cowhead2000) doesnt matter, yer otta jurisdiction anyway  
 06-15-2002 (RaFa) yeah but I'll live to Paris.. and is I have some work in USA..

damn imagine when I'll entering USA.. the FEDS hey .. BANG raped =(  
06-15-2001 (Cowhead2000) nahh...  
06-15-2001 (RaFa) I hope so =)  
06-15-2001 (Cowhead2000) they don't care much any more if yer just defacein,  
unless you embaresse em  
06-15-2001 (RaFa) ok ok

- h. 06-26-2001 (RaFa) the host for WoH, done ! =)  
... Starsky (ICQ#56568977) Wrote:  
Order Summary –Annual ... LiteWeb Package (world-of-hell.com Account)  
\$299.40 ... Setup fee \$50.00 ... Subtotal \$349.40 ... Total \$349.40 ... By pre-  
paying for twelve months and receiving three months free you have a savings of  
\$74.85!...
- i. 06-27-2001 (RaFa) <http://www.world-of-hell.com/interviewRaFa.txt>
- j. 08-01-2001 (RaFa) still ... <http://www.blacknike.com/>  
08-01-2001 (Cowhead2000) heh..
- k. 08-20-2001 (RaFa) I'll away like a 1 month d00d.. I'm traveling 2morrow .. so  
gonna miss ya =( ..take care [RaFa]  
09-07-2001 (RaFa) hey cow long time no cya.. what have u been up to ?  
09-07-2001 (Cowhead2000) not much, college started, been busy, but I got more  
free time now, you?  
09-07-2001 (RaFa) reading as hell.. studying some security shit.. I left WoH like 3  
weeks ago.. now I'm in Fatelabs.com like Develover..etc :P .. Logos4u is closed...  
and chillin.. new home at France =)
- l. 10-18-2001 (RaFa) ...bored.. I don't have idea about the new WoH logo ..I made  
some shit.. but I don't like <http://world-of-hell.com/wohlogo2.jpg>  
10-18-2001 (Cowhead2000) that's cool  
10-18-2001 (RaFa) I used in [http://world-of-  
hell.com/defaced/15/10/2001/www.pyburn.com/](http://world-of-hell.com/defaced/15/10/2001/www.pyburn.com/) .. when will you update the  
page...
- m. 07-05-1990 (RaFa) ...danm I have 17000 CCs ...(credit cards)  
07-05-1990 (Cowhead)that all? Where from?  
...damn, whered you get em from?  
07-05-1990 (RaFa) <http://www.gexpress.com>  
07-05-1990 (Cowhead) cool  
07-05-1990 (RaFa) when u need one.. just tell me, and I'll give you...  
07-05-1990 (Cowhead) k, don't give em to any1 that's not in WoH ... well need  
em for stuff...  
07-05-1990 (RaFa) np.... Heh... WoH members: cowhead2000, [RaFa], Sybek,  
dawgyg, Messiah-X, FonE\_TonE...  
(Note: The date from above – 1990 – is taken from the evidence. Your affiant is  
aware that the date and time settings in a computer can be changed and  
manipulated.)
- n. 11-26-2001 (Cowhead) ... and the only ppl I know in WoH are me, you, dawgyg,  
Orl0k or whoever, and Messiah-X- vandal quit, so he doesn't get ops even if he  
says in hes woh...

- o. 09-28-2001 (RaFa) ... ahhh well.. Feds are wacko looking for me...so I just clean RaFa background..etc, heh...look this.
- p. RaFa then provided a copy of what appeared to be a conversation between RaFa and another individual named Loki. In part, Loki warned RaFa that the Feds had asked him (Loki) to setup a trap for you to aid in his (RaFa's) arrest. Loki advised RaFa to "remain low" and RaFa stated "uhmm ok".

13. On February 27, 2002, I, SA Kyle Fach, and Lt. Tina Schaber, Bartlett, TN, Police Department, re-interviewed Cowhead2000 with his parents' permission and after Cowhead2000 waived his rights. We allowed Cowhead2000 and his parents to examine evidence from the hard drives seized from his residence on November 27, 2001, which had been discovered by the Defense Computer Forensics Lab during the analysis of Cowhead2000's hard drives. This evidence included thousands of images which appeared to contain child pornography (these images appear to contain images of minors, but have not yet been submitted to a medical doctor for analysis); numerous credit card numbers in names other than those of the true name of Cowhead2000 or his family; and other data indicative of hacking activity.

14. During this February 27, 2002 interview, Cowhead2000 also advised us of the following information:

(a) He stated that he believed that RaFa still resided in Paris, France. He periodically receives ICQ messages from RaFa, but he had not corresponded with RaFa in several months.

(b) Vandal, another member of World-of-Hell, had told him (Cowhead2000) that RaFa's true name was Rafael Nunez. Cowhead2000 believed that Vandal obtained RaFa's true name from Noid, another member of World-of-Hell. Cowhead2000 also recalled receiving several photographs sent electronically from RaFa and believed RaFa to be approximately twenty-five years old.

15. On August 1, 2002, Lt. Tina Schaber, Bartlett Police Department, SA Peter Black, DCIS, and I again interviewed Cowhead2000 with the consent of his parents and his attorney. Cowhead2000 and his attorney consented to the interview as part of an agreement

between his attorney and the Shelby County (TN) District Attorney's Office. Cowhead2000 then provided the following additional information regarding RaFa:

(a) Cowhead2000 stated that he had talked with Vandal, another member of World-of-Hell, online in December 2001 or January 2002 about being previously visited by the police. Cowhead2000 stated that Vandal then told him RaFa's true name was Rafael Nunez and that he (Vandal) thought RaFa lived in Southern Florida. Cowhead2000 also stated that RaFa told the members of World-of-Hell he was quitting World-of-Hell in early or mid-December 2001.

(b) Cowhead2000 also stated that RaFa had previously told him that he (RaFa) was a fashion model for clothing. Cowhead2000 thought that RaFa may have also told other members of World-of-Hell this information.

(c) Cowhead2000 recalled that RaFa had hacked several sites, one of which was a DoD web site, but Cowhead2000 could not recall the specific initials contained in the domain name of the DoD web site. Cowhead2000 believed that RaFa had sent him the URL of the DoD web site via an electronic communication such as ICQ or IM ("instant messaging") to "show" him the hack. Cowhead2000 explained that it was common for members of World-of-Hell to send each other URLs to show the other members which web sites they had hacked. Cowhead2000 also recalled that RaFa had hacked Pfizer, the company which makes Viagra, and rolex.com as part of a mass hack in which 800 web sites hosted on the same server were hacked.

16. On August 16, 2002, Cowhead2000 pled guilty in Shelby County Juvenile Court, Memphis, TN, to 133 counts of sexual exploitation of a minor; and 176 counts of identity theft. Cowhead2000 was sentenced to the custody of the Tennessee Youth Services Bureau Juvenile Detention center for a unspecified period of incarceration.

### **Dawgyg Investigative Efforts**<sup>5</sup>

17. As part of my investigation and as described further in ¶ 30, the U.S. Attorney's Office applied for and obtained three (3) pen register/trap and trace court orders from the U.S. District Court, District of Colorado, for information pertaining to numerous e-mail accounts, to include: [dawgyg@crackdealer.com](mailto:dawgyg@crackdealer.com), [RaFa@crackdealer.com](mailto:RaFa@crackdealer.com), and [rafaelnunez.com](http://rafaelnunez.com). These court orders authorized the DCIS to receive IP<sup>6</sup> connection information, and the to/from information for the three e-mail accounts. This includes the IP address from which individuals log in to check the e-mail accounts and to perform web site maintenance. These court orders did not authorize nor did I receive the content of email communications pertaining to these accounts.

18. Information learned, in part, from the U.S. District Court issued pen registers, referenced above, indicated that an 18-year old residing near Richmond, Virginia, used the online nickname Dawgyg and was a member of the World-of-Hell hacking group.

19. On or about June 12, 2002., a Federal search warrant issued by the Eastern District of Virginia was served at Dawgyg's apartment. SA John Schoeneweis, DCIS, and I interviewed Dawgyg during the execution of the search warrant, and learned the following:

(a) Dawgyg admitted to SA Schoeneweis and me that he used the online alias Dawgyg; that he was a member of the hacking group World-of-Hell; and that he had committed numerous hacks.

(b) He knew RaFa (from online communications). They joined World-of-Hell at about the same time in approximately June of 2001. Dawgyg believed that RaFa resided in Paris, France, but stated that he thought RaFa might have recently been in Chicago, Illinois.

(c) Dawgyg also stated that RaFa had electronically sent him a picture of himself

---

<sup>5</sup>If requested by the Court, I will divulge the true identity of "Dawgyg." However, because some of the conduct referenced herein was committed while Dawgyg was a juvenile, his hacker nickname is used.

<sup>6</sup>Based on my training and experience, I know that an "IP" or Internet Protocol address is the unique numerical identifier assigned to a particular computer while it is connected to the Internet. IP addresses can be either assigned for the duration of a particular Internet connection session, and are then called a "dynamic" IP address. Alternatively, a computer that has a constant connection to the Internet can have a static IP address.

(RaFa), and it had been stored on his computer until about one week prior to the search warrant. Dawgyg stated that the photo of RaFa looked like a modeling photo, and RaFa had previously told him he was a model for clothes.

(d) Dawgyg believed that RaFa was possibly 16-17 years old, but he noted that he has never seen him in person and did not know his true name. Dawgyg advised that RaFa had given him a list of 50 or 60 stolen credit card numbers. RaFa had previously indicated to him that he wanted to hack a pornographic web site and set up a "Paypal" account to skim credit card numbers.<sup>7</sup>

(e) Dawgyg also recalled a previous contact with RaFa via Instant Messenger. Dawgyg stated that RaFa told him he sold his computer because he was afraid he would be caught by law enforcement, a fear that was increased by the author Dan Verton, who apparently told RaFa he was one of the most wanted hackers. Dawgyg also stated that RaFa has compromised a computer in the Philippines, although when he (Dawgyg) tried to use it a couple of weeks prior to the interview, Dawgyg noted it was too slow.

20. I am aware that Dan Verton is the author of *The Hacker Diaries, Confessions of Teenage Hackers*, which contains a chapter written about the hacking group World-of-Hell and its members, including Cowhead2000, dawgyg, and RaFa.

21. In or about June 2001, Special Agent Salvatore Girgente, Virginia State Police, High Technology Crimes Unit, advised me that the Virginia State Police previously investigated Dawgyg for using the Internet to make a bomb threat. SA Girgente further advised that Dawgyg was prosecuted and accepted a plea agreement in juvenile court to that offense and was sentenced in or about April 2000. Based on information provided to me by SA Girgente, I also believe that Dawgyg was on probation at the time of the search warrant.

---

<sup>7</sup>Based on my experience and training, I know that "Paypal" is an Internet based business that processes credit card and other means of payment for Internet transactions.

### **World-of-Hell Investigative Efforts**

22. At my request, on December 27, 2001, DCIS SAs Stanley Newell and John Ledden, New Jersey Resident Agency, Edison, NJ interviewed Scott Daily at his home located in Roebling, NJ. Daily was interviewed in response to Daily's name being listed as the billing contact for the World-of-Hell web site. I then read the SAs' report of that interview, and learned the following:

(a) Daily explained to the SAs that his VISA credit card account information had been stolen and fraudulently used on several occasions. Daily reported the fraudulent use of his credit card to his local police department, the Florence Township Police Department (FTPD), the U.S. Secret Service, and the credit bureaus.

(b) On his July 2001 First USA VISA credit card statement, Daily noticed several fraudulent charges. One of the fraudulent charges originated from a company named Rackshare (973) 927-5881, a web hosting company located in New Jersey.

(c) Rackshare advised Dailey that the \$33.00 charge was for the monthly fee for the domain name World-of-Hell, which was purchased from Rackshare in Daily's name. Daily requested Rackshare to remove his information from the [www.world-of-hell.com](http://www.world-of-hell.com) domain information. Rackshare advised Daily that they could not alter the [www.world-of-hell.com](http://www.world-of-hell.com) information because a company called Tucows, located in Canada owns the domain.

(d) Daily contacted Tucows and was referred to another company called webhosting.com. An attorney at webhosting.com told Daily that they would try to have his information deleted from the World-of-Hell web site.

23. In or about July 2001, subsequent to his report to the FTPD, Daily was questioned by Detective Brown of the FTPD with regard to the theft of bank account information from a bank in Southern California, allegedly committed by members of the hacker group World-of-Hell. Daily was questioned because a Southern California Sheriff's department found Daily's name to be associated with the World-of-Hell web site. Daily also stated to the DCIS Agents

that due to the World-of-Hell group allegedly hacking a “motorcycle” type web-site, an individual had traced the World-of-Hell group through the web site registration to Daily. This individual then telephoned Daily and threatened to kill Daily because of the web-site defacement. ICQ logs discovered on hard drives seized from Cowhead2000 indicated that “RaFa” allegedly set-up the [www.world-of-hell.com](http://www.world-of-hell.com) domain name registration and web hosting using a credit card stolen by another individual using the name “Starsky.”

24. As part of my investigation, I performed Internet searches, which revealed that the [www.world-of-hell.com](http://www.world-of-hell.com) web site was hosted by SBC Internet Services, Dallas, Texas.

25. Thereafter, Rhonda Compton, SBC Internet Services, advised me that the [www.world-of-hell.com](http://www.world-of-hell.com) web site was shut down because the account holder (Scott Daily) advised SBC Internet Services that he was a victim of credit card and identity theft and had not authorized anyone to use his name to register the [www.world-of-hell.com](http://www.world-of-hell.com) web site.

26. As part of my investigation, I have analyzed files regarding the [www.world-of-hell.com](http://www.world-of-hell.com) web site that I received from SBC Internet Services. The files contained information regarding the hacker group World-of-Hell, including exploits, graphic files, online interviews and news articles, and other information. A file named “littlerafa.jpg” was located. The file “littlerafa.jpg” contains a picture of a young male child sitting in front of what appears to be an older model computer. A file named [www.pyburn.com/index.html](http://www.pyburn.com/index.html) was also located. This file contains what appears to be a defaced web page. This contents state, in part “I’m back ! Owing Big HitZ ./fux0r terrorism & kiss my ass cause I just Owned yours... ..Owned by [RaFa]...” Several other files were located with the names “yo2.htm”, “yo3.htm,” and yo4.htm.” The contents of these files appear similar to other web page defacements reviewed by me and allegedly conducted by RaFa. The contents of each of these files also contain, in part, “Owned by [RaFa]”.

27. In reviewing the files from SBC Internet Services, I also located a file named “interviewRaFa.txt.” This file was also referenced in paragraph 12(i) above. The contents of

this file contain an interview conducted with RaFa by an individual using the name P1AgUe. In a part of the interview, RaFa states:

>>P1AgUe: How old are you?

>>RaFa: 17.

>>P1AgUe: So, how did you get into hacking?

>>RaFa: When a hacker group contacted me to join his crew... when they saw my personal defacements and design skills.

>>P1AgUe: What was your first hack?

>>RaFa: I think this is a kind of manifesto... for the lazy administrators who have a bad knowledge about security, and we do this for fun. My first hack was The 2nd. Venezuelan Mobile company, www.digitel.com.ve.

...

>>P1AgUe: How many groups were you in or are in now?

>>RaFa: Just 2... WoH and Box Network.

>>P1AgUe: How did you get you name RaFa?

>>RaFa: Cause of the mighty artist, Raffaello, from Italy.

>>P1AgUe: What's Your Greatest accomplishment?

>>RaFa: Hack the American Air Force Security Information of Computer System.

...

**Alldas.org (formerly known as alldas.de)**

28. Based on my experience, I am familiar with a web site known as alldas.org, formerly known as alldas.de. During a period including 2001 and some of 2002, alldas.org functioned, in part, as a "mirror" site for web page defacements. Individuals can send, via e-mail, information regarding web sites that have been hacked or defaced. Individuals associated with alldas.org then log onto these web sites and create a "mirror" of the defaced page. The "mirror" and other information regarding the defacements are then stored on the alldas.org web site. The alldas.org web site is a public domain web site.

29. I have reviewed the web site alldas.org (also known as www.alldas.de) and located a listing of approximately 451 web page defacements and "mirrors" for hacks that were allegedly conducted by members of World-of-Hell. Further, during Cowhead2000's November 27, 2001 interview with DCIS agents, Cowhead2000 advised DCIS agents that World-of-Hell members would routinely send an e-mail notification of their web page defacements to the www.alldas.de (also known as www.alldas.org) web site. Alldas.org would then attempt to go to the hacked web site and "mirror" the hacked site. The "mirror" would then be stored on the www.alldas.de web site under the appropriate "attacker."

30. I have reviewed web page “mirrors” for several web page defacements allegedly done by RaFa and documented under World-of-Hell on [www.alldas.org](http://www.alldas.org), which have revealed, in part, the following:

- a. The web site [www.blacknike.com](http://www.blacknike.com) was allegedly defaced on or about 07/30/2001. The defaced page read, in part, “[RaFa] is back ! Owning Big HitZ. & kiss my ass cause I just Owned yours... .. Owned by [RaFa]...”. The defaced page provided an e-mail address of [woh@world-of-hell.com](mailto:woh@world-of-hell.com) and listed the [www.world-of-hell.com](http://www.world-of-hell.com) web site. Your affiant also viewed the source code for the defaced page. The source code for this defacement indicated that several files were “pulled” from the World-of-Hell.com web site to be used in the defaced page. These files include “wohlogo.jpg” and “littlerafa.jpg”.
- b. The web site [www.hampton.navy.mil](http://www.hampton.navy.mil) was allegedly defaced on or about 10/22/2001. The defaced page read, in part, “#Owned ./fux0r terrorism & kiss my ass cause I just Owned yours... ..Owned by [RaFa]. The defaced page provided an e-mail address of [woh@world-of-hell.com](mailto:woh@world-of-hell.com) and listed the [www.world-of-hell.com](http://www.world-of-hell.com) web site. Your affiant also viewed the source code for the defaced page. The source code for this defacement indicated that at least one file, “wohlogo2.jpg” was “pulled” from the world-of-hell.com web site to be used in the defaced page.
- c. The web site [www.defenseshield.com](http://www.defenseshield.com) was allegedly defaced on or about 12/24/2001. The defaced page read, in part, “Owned ./fux0r terrorism – Holiday Greetings from WOH... ..Owned by [RaFa]”. The defaced page provided an e-mail address of “[RaFa@crackdealer.com](mailto:RaFa@crackdealer.com)”.
- d. The web site [www.explorer.com](http://www.explorer.com) was allegedly defaced on or about 01/09/2002. The defaced page read, in part, “...Owned by [RaFa]...”. The defaced page provided an e-mail address of “[RaFa@crackdealer.com](mailto:RaFa@crackdealer.com)”.

### **Pen Register / Trap & Trace Court Orders**

31. As part of my investigation, the U.S. Attorney’s Office has applied for and obtained numerous pen register/trap & trace court orders from the U.S. District Court, District of Colorado, for information pertaining to e-mail and web site accounts. These accounts included, in part: [RaFa@crackdealer.com](mailto:RaFa@crackdealer.com), [rafaelnunez.com](http://rafaelnunez.com), and [dawgyg@crackdealer.com](mailto:dawgyg@crackdealer.com). Based on my research, I learned that [RaFa@crackdealer.com](mailto:RaFa@crackdealer.com) and [dawgyg@crackdealer.com](mailto:dawgyg@crackdealer.com) are hosted by a company named BigMailBox.com, and [Rafaelnunez.com](http://Rafaelnunez.com) was hosted by a company named AWorldwidemall.com. These court orders authorized the DCIS to receive IP connection information and the To/From information for the e-mail accounts. This includes the IP address

from which individuals log in to check the e-mail accounts and to perform web site maintenance.

**RaFa@crackdealer.com account records**

32. I have reviewed information received from BigMailBox.com as part of the pen register/trap and trace order issued by the Court on the RaFa@crackdealer.com account, which is an e-mail address listed in numerous web page defacements allegedly conducted by RaFa. This information indicated that on or about May 9, 2002, an e-mail message was sent/received with the heading information as: “Rambo” rambo@rafaelnunez.com Thu, 9 May 2002 09:56:04 -0400...

33. Information received from BigMailBox.com as part of the Court Order on the RaFa@crackdealer.com account also indicated that on March 27, 2002 an e-mail message was sent/received with the heading information as: rafa@crackdealer.com ... “dawgyg world of hell” <nikeguy65@hotmail.com>. Additional records received during the investigation indicate that Dawgyg also uses the e-mail account nikeguy65@hotmail.com.

34. Additional information received from BigMailBox.com as part of the Court Order on the RaFa@crackdealer.com account indicated that on or about July 6, 2002, an e-mail message was sent/received with the heading information as: SUAREZ Gloria Gloria.SUAREZ@totalfinaelf.com Sat, 6 Jul 2002 19:58:36 -0400...

**www.rafaelnunez.com account records**

35. As part of my investigation, I located a web site with the domain name www.rafaelnunez.com. I have reviewed this public domain web site on several occasions, and it appears to be a web site for a model named Rafael Nunez. More specifically, I have reviewed a page on the www.rafaelnunez.com web site titled “profile,” which reads, in part,

“Hi, my name is Rafael, currently, I live in Caracas, Venezuela. I am the youngest of 6 brothers and I am proud of being a Venezuelan in The Fashion Industry. Until recently, I was going to college for Computer Science at a Catholic University Andres Bello – Caracas, but with the recent decision in my life to move to Paris, France I stopped

attending school to continue my ongoing successful modeling career in the old continent... ..I am presently being represented by LEDOM MODELS – CHICAGO, obviously in Chicago, IL USA...”.

Based on my review of the web site, I also saw that it contains numerous modeling photos purported to be of Rafael Nunez.

36. As part of my investigation, I have also reviewed account subscriber records for [www.rafaelnunez.com](http://www.rafaelnunez.com), which were received from AWorldWideMall.com. These records indicate that the [www.rafaelnunez.com](http://www.rafaelnunez.com) web site was set up with a billing name of Gloria Suarez. The account records listed an “address” of [gloria.suarez@totalfinaelf.com](mailto:gloria.suarez@totalfinaelf.com), and a city and country of “Caracas, Df, 1060 VENEZUELA”. The [gloria.suarez@totalfinaelf.com](mailto:gloria.suarez@totalfinaelf.com) e-mail address appears to be the same as referenced in paragraph 33, above, to which an e-mail was sent/received from the [RaFa@crackdealer.com](mailto:RaFa@crackdealer.com) e-mail account. The [www.rafaelnunez.com](http://www.rafaelnunez.com) account records also indicated an e-mail address of [rafaelnunez@cantv.net](mailto:rafaelnunez@cantv.net). The account was paid for with a credit card in the billing name of Gloria Suarez.

37. I have also reviewed records received from BigMailBox.com pertaining to account logins for the relevant email accounts. These records reflect the date, time, and originating IP address for logins on those accounts. Below is summary of a portion of the login records for [RaFa@crackdealer.com](mailto:RaFa@crackdealer.com), the e-mail address referenced above, which appears in numerous web page defacements allegedly done by RaFa:

<u>Account</u>	<u>Date</u>	<u>Originating IP Address</u>
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	04/14/2002	200.11.240.137
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	04/15/2002	200.11.240.137
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	04/16/2002	200.11.240.137
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	04/18/2002	200.11.240.137
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	05/10/2002	200.11.240.137
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	05/16/2002	200.11.240.137
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	06/10/2002	200.84.41.158
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	06/17/2002	200.84.41.158
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	06/29/2002	200.84.41.158
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	06/30/2002	200.84.41.158
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	07/04/2002	200.84.41.158
<a href="mailto:RaFa@crackdealer.com">RaFa@crackdealer.com</a>	07/05/2002	200.84.41.158

<u>RaFa@crackdealer.com</u>	07/10/2002	200.84.41.158
<u>RaFa@crackdealer.com</u>	07/23/2002	200.84.41.158
<u>RaFa@crackdealer.com</u>	08/04/2002	200.84.41.158

38. I have also reviewed records received from AWorldwidemall.com pertaining to account logins. These records reflect the date, time, and originating IP address for logins on those accounts. Below is summary of a portion of the login records for www.rafaelnunez.com:

<u>Account</u>	<u>Date</u>	<u>Originating IP Address</u>
<u>www.rafaelnunez.com</u>	04/14/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	04/15/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	04/18/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	04/21/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	04/28/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	05/03/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	05/05/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	05/12/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	05/16/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	05/25/2002	200.11.240.137
<u>www.rafaelnunez.com</u>	06/10/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	06/14/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	06/18/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	06/24/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	06/28/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	06/29/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	07/02/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	07/04/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	07/12/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	07/15/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	07/21/2002	200.84.41.158
<u>www.rafaelnunez.com</u>	07/24/2002	200.84.41.158

39. Based on my training and experience, I know that a WHOIS lookup is a method to locate the company to which certain IP addresses are assigned. I have performed a WHOIS lookup on the IP address 200.11.240.137, which as referenced above, was used to access both the RaFa@crackdealer.com account and the www.rafaelnunez.com account. The WHOIS lookup results indicated that the IP address 200.11.240.137 was assigned to: TRUE, The Real Unix Experts, Calle Terepaima, Zona O, Quinta El Creador, Macaracuay, Caracas, VE (DNS.TRUE.NET, DNS1.TRUE.NET, DNS.CANTV.NET).

40. I have also performed a WHOIS lookup on the IP address 200.84.41.158, which as referenced above, was also used to access both the [RaFa@crackdealer.com](mailto:RaFa@crackdealer.com) account and the [www.rafaelnunez.com](http://www.rafaelnunez.com) account. The WHOIS lookup results indicated that the IP address 200.84.41.158 was assigned to:

CANTV Servicios, C.A. Av. Fco. De Miranda, Centro Lido, Torre A, Ofc. 41-A, Caracas 1071, VE (DNS1.CANTV.NET, DNS2CANTV.NET).

41. On March 22, 2003, I was notified by SA John Schoeneweis, DCIS Richmond, that Dawgyg had spoken in an online chat with RaFa. Dawgyg then provided me with a copy of the recorded chat log, which stated in part: (Dawgyg used the nickname "Fuc|< Off):

```
[RaFa] says:
y0
[RaFa] says:
dawg
[RaFa] says:
sup
F u c | < O f f says:
y0
F u c | < O f f says:
[RaFa] says:
F u c | < O f f says:
nothin much bro
F u c | < O f f says:
you
[RaFa] says:
y0 http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0145.html
F u c | < O f f says:
wuts dat
[RaFa] says:
exploita
F u c | < O f f says:
kewl
[RaFa] says:
what's up with jew?
F u c | < O f f says:
bored as fuck
F u c | < O f f says:
wuts scientech
[RaFa] says:
a corp that i work from
F u c | < O f f says:
Kewl
```

42. I have reviewed the web site <http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0145.html>, which RaFa provided to Dawgyg in the above referenced chat. The records on this web site indicate that RaFa uses the name Rafael Nunez, and is affiliated with a business named scientech.com.ve, a portion of which reads:

[VulnWatch] iis 0day exploit  
**From:** Rafael Nuñez ([rnunez@scientech.com.ve](mailto:rnunez@scientech.com.ve))  
**Date:** Fri Mar 21 2003 - 12:36:33 CST  
• **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#)

exploit at [http://rafa.h0stile.net/iis\\_txt.c](http://rafa.h0stile.net/iis_txt.c)  
Regards

-----  
Rafael Nuñez  
Senior Research Scientist  
Latin American Security & Intelligence Operations  
Scientech de Venezuela

-----  
[w] <http://www.scientech.com.ve>  
[e] [rnunez@scientech.com.ve](mailto:rnunez@scientech.com.ve)

-----  
Tlf.:(58-212) 952.42.66  
Fax:(58-212) 951.36.35  
-----

43. I have records received in March 2003 as part of a U.S. District Court Order regarding the e-mail account [RaFa@crackdealer.com](mailto:RaFa@crackdealer.com) which indicate, in part, the following:

mail22.bigmailbox.com: "[RaFa]" <[rafa@crackdealer.com](mailto:rafa@crackdealer.com)>  
[rafa@box.sk.rnunez@scientech.com.ve](mailto:rafa@box.sk.rnunez@scientech.com.ve)  
Mon Mar 3 09:45:59 2003 200.11.241.33

mail22.bigmailbox.com: "[RaFa]" [rafa@crackdealer.com](mailto:rafa@crackdealer.com)  
[rafa@box.sk.rnunez@scientech.com.ve](mailto:rafa@box.sk.rnunez@scientech.com.ve)  
Mon Mar 3 09:47:28 2003 200.11.241.33

44. As referenced above, the records indicate that two e-mails were sent/received from the e-mail account [rafa@crackdealer.com](mailto:rafa@crackdealer.com) to [rafa@box.sk](mailto:rafa@box.sk) and [rnunez@scientech.com.ve](mailto:rnunez@scientech.com.ve). [Rnunez@scientech.com.ve](mailto:Rnunez@scientech.com.ve) appears to be an e-mail account at the Scientech.com.ve company referenced by RaFa in his online chat with Dawgyg as detailed in ¶ 40 above.

45. Additionally, in or about March 2003, I received records provided under a U.S. District Court order regarding the modeling web site and associated e-mail accounts of [www.rafaelnunez.com](http://www.rafaelnunez.com). The records, in part, indicate that the [www.rafaelnunez.com](http://www.rafaelnunez.com) account appears to have been accessed from an IP address affiliated with [scientech.com.ve](http://scientech.com.ve), as follows:

2003-02-19 14:15:39 18lcV3-0003Bm-00 <= [info@rafaelnunez.com](mailto:info@rafaelnunez.com)  
H=(servidor1) [200.11.241.33] P=smtp S=1001  
[id=003c01c2d863\\$f6258090\\$631ba30a@scientech.com.ve](mailto:id=003c01c2d863$f6258090$631ba30a@scientech.com.ve)

2003-02-13 09:51:58 18jNWf-0005kH-00 <= [info@rafaelnunez.com](mailto:info@rafaelnunez.com) H=(user13)  
[200.11.241.33] P=smtp S=1274  
[id=006301c2d388\\$97e27950\\$681ba30a@scientech.com.ve](mailto:id=006301c2d388$97e27950$681ba30a@scientech.com.ve)

46. On March 27, 2003, I reviewed a web site called [www.securityfocus.com](http://www.securityfocus.com). This is a computer security oriented web site that includes an affiliated mailing list called "BugTraq" whereby individuals can post and read information regarding computer security vulnerabilities. I reviewed a posting purported by the "BugTraq" mailing listing to have been posted by Rafael Nunez, which read as follows:

[ Message Index ] [ Thread Index ]  
[ Reply ]  
[ prev Msg in Thread ]  
[ next Msg in Thread ]

To: BugTraq  
Subject: WebDav Exploit ffs  
Date: Mar 24 2003 6:57PM  
Author: Rafael Nuñez <[rnunez@scientech.com.ve](mailto:rnunez@scientech.com.ve)>  
Message-ID: 021601c2f237\$2f3a05d0\$1500000a@scientech.com.ve>

I've been receiving a bunch of emails concerning if the exploit that I sent to the list (iis\_txt.c) was focus on WebDav Vuln.. Of course Not (was a totally different one, based on the old \*.asp like iistart.asp). If David Litchfield read the 1st one he proolly cried.

Regarding this I'm sending the WebDav exploit tested 100% by me

Best Regards

Note: don't ask for the binary one.. Please compile yourself.

-----  
Rafael Nuñez  
Senior Research Scientist  
Latin American Security & Intelligence Operations

Sciencetech de Venezuela

-----  
[w] <http://www.sciencetech.com.ve>

[e] [rnunez@sciencetech.com.ve](mailto:rnunez@sciencetech.com.ve)  
-----

Tlf: (58-212) 952.42.66

Fax: (58-212) 951.36.35  
-----

[ attachment: (application/octet-stream) ]

47. In March 2003, I also reviewed the attachment listed in the above referenced posting to the “BugTraq” mailing list. The attachment appears to be the source code for a computer vulnerability exploit. According to text listed in the mailing list attachment, the exploit was created by an individual who uses the nickname “kralor”. Additional text in the introduction to the source code in the attachment states that the exploit was tested by Rafael [RaFa] Nunez of [sciencetech.com.ve](http://sciencetech.com.ve). The attachment, in part, states:

[Crpt] ntdll.dll exploit trough WebDAV by kralor [Crpt]  
this is the exploit for ntdll.dll through WebDAV.

...

Tested by Rafael [RaFa] Nunez [rnunez@sciencetech.com.ve](mailto:rnunez@sciencetech.com.ve)

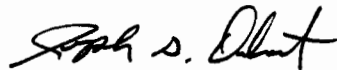
48. The text provided as listed in the “BugTraq” attachment as referenced above indicates that Rafael [RaFa] Nunez tested the exploit. The spelling and characters of [RaFa] in this posting appear exactly as referenced in ¶ 5, above. Paragraph 5 described the DISA computer intrusion and web page defacement. As referenced in Paragraph 5, the hacked DISA web page read, in part, “woh is Back...and kiss my ass cause I just Owned yours! – America’s Air Force Department of Defense computer system Own3d by [RaFa] – [woh@world-of-hell.com](mailto:woh@world-of-hell.com) – <http://www.world-of-hell.com>”.

49. On March 26, 2003, I reviewed an online news article located on the web site <http://zdnet.com>, an online news and technology magazine, and I located an article titled “Program targets Windows 2000 Flaw” written by Robert Lemos. The online news article is a report about a Venezuelan security consultant named Rafael Nunez, whom the article states, released the source code for a small program designed to compromise Microsoft Internet

Information Service servers which have not had a specific security patch installed. The article states in part, "I released (the code) to enlighten the public and to promote system security for administrators with these exploits," said Rafael Nunez, information security consultant for Scientech de Venezuela and a former hacker who used the handle 'RaFa.' "

50. Based on the foregoing, probable cause exists to believe that, on or about June 11, 2001, JOHN DOE, aka "Rafael Nunez" aka "RaFa" violated 18 U.S.C. § 1030(a)(5)(A)(i) by intentionally causing the transmission of a program, information, code or command, and as a result of such conduct, intentional intentionally causing damage, without authorization, to a protected computer, namely the Department of Defense computer located at the Defense Information Systems Agency in Denver, CO. Accordingly, I respectfully request that an arrest warrant be issued for JOHN DOE, aka "Rafael Nunez" aka "RaFa."

I declare under penalty of perjury that the foregoing is true to the best of my information and belief.



\_\_\_\_\_  
Joseph Diebert  
Special Agent  
Defense Criminal Investigative Service

Subscribed and sworn to before me this 12<sup>th</sup> day of May, 2003, in Denver, CO.



\_\_\_\_\_  
United States Magistrate Judge