

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

<b>UNITED STATES OF AMERICA</b>	:	<b>CRIMINAL NO.</b> _____
<b>v.</b>	:	<b>DATE FILED: November 19, 2009</b>
<b>CHRISTOPHER ALLEN LEWIS,</b> a/k/a "EBK,"	:	<b>VIOLATION:</b>
<b>JAMES ROBERT BLACK, JR.,</b> a/k/a "Defiant,"	:	<b>18 U.S.C. § 371 (conspiracy to</b>
<b>MICHAEL PAUL NEBEL,</b> a/k/a "Slacker"	:	<b>intentionally damage protected computer</b>
	:	<b>system – 1 count)</b>
	:	

**INDICTMENT**

**COUNT ONE**

**THE GRAND JURY CHARGES THAT:**

1. At all times material to this indictment, Comcast Corporation ("Comcast"), was an Internet service provider headquartered in Philadelphia, Pennsylvania. Comcast provided the portal internet website www.comcast.net for subscribers to access their e-mail, voice mail, and other services. The portal website at www.comcast.net is operated and maintained by a protected computer system which is used in interstate and foreign commerce and communication. In May, 2008, approximately 5 million different users visited www.comcast.net each day.

2. From on or about May 26, 2008 to on or about May 29, 2008, in the Eastern District of Pennsylvania, and elsewhere, defendants

**CHRISTOPHER ALLEN LEWIS,**  
a/k/a "EBK,"  
**JAMES ROBERT BLACK, Jr.,**  
a/k/a "Defiant," and

A TRUE COPY CERTIFIED TO FROM THE RECORD  
DATED: 11/19/09  
ATTEST: \_\_\_\_\_  
DEPUTY CLERK, UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF PENNSYLVANIA

**MICHAEL PAUL NEBEL,  
a/k/a "Slacker,"**

conspired and agreed to commit an offense against the United States, that is, to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to a protected computer, and thereby disrupt the availability of the computer network operating the website www.comcast.net, causing more than \$5,000 in loss within a one-year period, in violation of Title 18, United States Code, Section 1030(a)(5)(A)(i).

**MANNER AND MEANS**

It was part of the conspiracy that:

3. Defendants CHRISTOPHER ALLEN LEWIS, JAMES ROBERT BLACK, JR., and MICHAEL PAUL NEBEL, who were associated with the hacker group Kryogeniks, planned and executed an attack on www.comcast.net to disable subscriber access to this Comcast website by redirecting Comcast customers trying to connect to www.comcast.net to other websites of the defendants' choosing and creation, and thereby prevented Comcast customers from accessing e-mail, digital voicemail, and other services at www.comcast.net.

4. Defendants CHRISTOPHER ALLEN LEWIS, JAMES ROBERT BLACK, JR., and MICHAEL PAUL NEBEL redirected Comcast customers away from www.comcast.net by gaining unauthorized access to, and then altering, Comcast's Domain Name System ("DNS") records which were maintained by a domain registrar company.

5. Defendants CHRISTOPHER ALLEN LEWIS, JAMES ROBERT BLACK, JR., and MICHAEL PAUL NEBEL continued to alter Comcast's DNS records after Comcast employees in Philadelphia, Pennsylvania, made efforts to correct the altered DNS

records for www.comcast.net.

6. Defendants CHRISTOPHER ALLEN LEWIS, JAMES ROBERT BLACK, JR., and MICHAEL PAUL NEBEL posted a message on the webpage to which the Comcast subscribers were directed after the defendants had altered DNS records for www.comcast.net, and the message on that webpage attributed the attack to their group.

7. Defendants CHRISTOPHER ALLEN LEWIS, JAMES ROBERT BLACK, JR., and MICHAEL PAUL NEBEL changed the listed contact information available to the public for the www.comcast.net account to a false mailing address and a false e-mail address.

8. These actions caused a loss to Comcast in Philadelphia, Pennsylvania, of approximately \$128,578.

#### **OVERT ACTS**

In furtherance of the conspiracy, defendants committed the following overt acts in the Eastern District of Pennsylvania, and elsewhere:

1. On or about May 26, 2008, defendants CHRISTOPHER ALLEN LEWIS, in the state of Delaware, and JAMES ROBERT BLACK, in the state of Tennessee, and another person known to the grand jury, participated in a telephone conference call in which the defendants discussed a website called fearnet.com, owned by Comcast, and discussed taking control of the comcast.net domain.

2. On or about May 27, 2008, defendant CHRISTOPHER ALLEN LEWIS, in the state of Delaware, anonymously called Comcast employee No. 1, an employee listed as being associated with the www.comcast.net website, at his home telephone in the Eastern District of Pennsylvania, and asked the employee if he would answer questions concerning Comcast's fearnet.com domain.

3. On or about May 27, 2008, defendant CHRISTOPHER ALLEN LEWIS, in the state of Delaware, twice made telephone calls through which he obtained information which he and his coconspirators later used in gaining unauthorized access to Comcast's DNS server information.

4. On or about May 28, 2008, defendants CHRISTOPHER ALLEN LEWIS, in the state of Delaware, JAMES ROBERT BLACK, JR., in the state of Tennessee, and MICHAEL PAUL NEBEL, in the state of Michigan, created substitute websites to which Comcast subscribers would be directed when they tried to reach www.comcast.net. These substitute websites showed the message "KRYOGENIKS Defiant and EBK RoXed COMCAST sHouTz to VIRUS Warlock elul21 coll1er seven," on their opening webpage, a message created by these defendants.

5. On or about May 28, 2008, defendant CHRISTOPHER ALLEN LEWIS, in the state of Delaware, directed defendant MICHAEL PAUL NEBEL, in the state of Michigan, to log onto a specific Comcast e-mail account.

6. On or about May 28, 2008, defendant MICHAEL PAUL NEBEL, in the state of Michigan, while on a telephone conference call with defendants CHRISTOPHER ALLEN LEWIS, in the state of Delaware, and JAMES ROBERT BLACK, JR., in the state of Tennessee, and in collaboration with those defendants, logged onto a specific Comcast e-mail account and used that account to communicate with the entity which maintained Comcast's DNS server information.

7. On or about May 28, 2008, CHRISTOPHER ALLEN LEWIS, in the state of Delaware, JAMES ROBERT BLACK, JR., in the state of Tennessee, and MICHAEL PAUL NEBEL, in the state of Michigan, signed onto Comcast's account at the entity which maintained

Comcast's DNS records and changed the DNS record for www.comcast.net to point to one of the substitute websites which they had created. As a result of this change, the content, data, programs, and information on www.comcast.net was no longer available to Comcast customers trying to connect to their Comcast e-mail, voicemail, and other services through www.comcast.net.

8. On or about May 28, 2008, CHRISTOPHER ALLEN LEWIS, JAMES ROBERT BLACK, JR., and MICHAEL PAUL NEBEL changed the publicly-available contact information for www.comcast.net, to "69 dick tard lane, dildo room, Philadelphia, PA 19103" and an e-mail address of kryogeniksdefiant@gmail.com.


9. On or about May 28, 2008, defendants CHRISTOPHER ALLEN LEWIS, JAMES ROBERT BLACK, JR., and MICHAEL PAUL NEBEL retained access to this specific e-mail account and continued their attack after Comcast employees, some of whom were based in Philadelphia, Pennsylvania, attempted to regain control of this specific e-mail account.

10. On or about May 28, 2008, defendant CHRISTOPHER ALLEN LEWIS anonymously called Comcast employee No. 1, an employee listed as being associated with the Comcast.net website, at his home telephone number in the Eastern District of Pennsylvania, and asked the employee if Comcast's domains were working properly.

All in violation of Title 18, United States Code, Section 371.

**A TRUE BILL:**

  
\_\_\_\_\_  
**GRAND JURY FOREPERSON**

  
\_\_\_\_\_  
**MICHAEL L. LEVY**  
**UNITED STATES ATTORNEY**