International Police Cooperation in Cyberspace

TIMOTHY B. ATKINS

Supervisor Agente Especial de la F.B.I. EEUU

Good Morning. My name is Tim Atkins and I am a Supervisory Special Agent with the FBI. I am with the Computer Investigations Unit of the Computer Infrastructure and Threat Assessment Center (CITAC) at FBI Headquarters in Washington, DC. My responsibilities include the oversight of FBI Computer Investigations in the Western part of the United States. I will begin this morning by discussing the investigative authority of the FBI in the area of computer investigations and then I will give an overview of the FBI's CITAC including some of the cases which we have investigated and are currently investigating.

The FBI possesses broad investigative authority in the area of computer investigations, both in the National Security and Criminal realm. The sources of authority for National Security Investigations include Executive Order 12333 which establishes the FBI's authority to conduct Counterintelligence Investigations. Additionally, Presidential Decision Directive 39 directs the FBI to serve as the lead agency for all incidents of terrorism in the US.

In the Criminal realm, the FBI is the lead investigative agency for violations of several federal criminal statutes which criminalize cyber related activities. Title 18 USC Section 1030 is the primary statute authorizing the FBI to investigate computer intrusions.

Title 18 USC 1030 serves as the backbone for the FBI's authority to investigate computer intrusions. This authority is quite broad in scope. For instance, it criminalizes acts as isolated as a disgruntled employee who maliciously destroys his company's Web page, as well as a foreign terrorist group that penetrates the computer systems of our nation's critical infrastructures and wreaks havoc nationwide. It protects any US government or financial institution computer and also any computer used in interstate or foreign commerce, which includes any computer used for Internet access. It protects against the unauthorized access by both insiders and outsiders of a company. It protects against both intentional and unintentional damage (as long as the intrusion was intentional), as well as the unauthorized obtaining of National Security Information or any information valued in excess of $5,000 from a protected computer. So, whether a cyber threat or attack is Domestic or Foreign, Isolated or Multifaceted, the FBI has jurisdictional authority to respond.

Attacks may originate from a multitude of various sources, both inside and outside of the US. And when a cyber attack is first discovered, there is often no way to initially identify the source of the attack. One of the greatest challenges to computer intrusion investigations is that the intruder can instantaneously cross national and international jurisdictions with the click of a mouse.

Additionally, if terrorists launch a large scale cyber attack against the US, they may not limit their attack to the cyber realm. They may concurrently launch more traditional types of terrorist acts as well, such as the World Trade Center or Oklahoma City Federal Building bombing. Therefore, the most efficient response to such a multifaceted attack is facilitated and coordinated by the one law enforcement entity equipped with the authority and resources to investigate them. In the US, that entity is the FBI.

CITAC is part of the FBI's Office of Computer Investigations and Infrastructure Protection (OCIIP). CITAC is composed of five Units, the Critical Infrastructure Protection Unit, the Computer Investigations Unit, the Special Technologies Applications Unit, the Strategic Planning Analysis Unit, and the Watch and Threat Analysis Unit. Also part of OCIIP is the Infrastructure Protection Task Force which is responsible for the recent report to the Presidential Commission on Infrastructure Protection in the United States.

The CIPU focuses on eight critical infrastructures, Telecommunications, Electric Power Systems, Storage & Transportation of Gas & Oil, Banking & Finance, Transportation, Water Supply Systems, Emergency Services, &

Continuity of Government Services. The CIPU utilizes the resources in Industry, Government, the Military, and Law Enforcement to IDENTIFY, ASSESS AND WARN about threats and unlawful acts that target these infrastructures. These threats include both traditional and nontraditional threats - both physical and cyber - particularly terrorist threats.

CITAC's Watch and Threat Analysis Unit's mission is to gather and disseminate information about cyber intrusions, computer facilitated crimes, and emerging intrusion trends and techniques. This mission is accomplished through CITAC WATCH, a Watch Center located at FBIHQ. CITAC WATCH has been established to be the first point of contact in the FBI for victims of cyber intrusions.

CITAC WATCH will analyze incidents, facilitate the opening of appropriate investigations (criminal or Foreign Counter Intelligence), and support investigations. With CITAC WATCH as the central repository for information about cyber intrusions, CITAC will assess the information, analyze it to determine any similarities to other cyber attacks, and disseminate the information to the appropriate FBI field offices. We are in the process of increasing the staffing level of CITAC WATCH and we will soon be going to 16 hours a day 7 days a week. Sometime in 1998 we will be 24 hours a day 7 days a week.

The following example is given to demonstrate how CITAC WATCH works. A few weeks ago, NSA, USAF, Army & NASA independently reported attacks on their systems that originated from an ISP in the LA division. A case was opened and the case agent obtained the assistance of the ISP and set up a trap & trace. A CITAC WATCH alert was sent to advise all participating government agencies of the attacks and a request was made for any attacks from that ISP be reported immediately to CITAC WATCH and the case agent. We have since received notifications from other government agencies of additional attacks and we have been able to do real time monitoring of attacks to be better able to trace the attacks to their source. CITAC WATCH, the Computer Investigations Unit, and FBI LA are continuing to work together to identify and apprehend the intruder.

The responsibilities of the Computer Investigations Unit include managing computer investigations nationwide. We also provide education, awareness and outreach to both the public and private sectors. For instance, we have a Supervisory Special Agent from the CIU that regularly meets with America Online to discuss policy issues relating to computer investigations and to cultivate

a relationship so that we can have an established point of contact for crisis situations such as when a kidnapper is utilizing America OnLine to send his ransom notes. Additionally, we coordinate computer investigation training for FBI Special Agents and support personnel; we provide equipment and technical expertise in support of investigations; and we establish cooperation with domestic and foreign law enforcement and computer incident response teams.

Training is a high priority in the area of FBI computer investigations. We have developed a basic entry level training package for Special Agents who conduct computer investigations. They include Introduction to UNIX for Investigations; Internet & Network Investigations; Hacker Tools, Exploits, and Techniques; and Introduction to Telecommunications. Additionally we will provide advanced training in specialized areas.

No one is an expert in every technical area. Even the hackers admit that and cooperate among themselves to solve problems when they are illegally hacking into systems. Our first goal in training computer illiterate agents is to equip them with enough knowledge and hands-on experience so that they will not feel intimidated when they conduct interviews of technically advanced system administrators who speak "techno-babble". We want them to be able to ask the right questions and work with the system administrators to get them to use their skills and resources to help us identify the source of the intrusions. We have to get them to explain things in elementary terms - after all, that's how we have to present it to a jury if we ever hope to get any convictions in a case.

With our advanced training, we want to develop a diverse pool of resources so that when we encounter specific technical issues, we can call upon those resources within the FBI. However, with the continuing explosion in technology, we will never have all the required expertise within the FBI to address every investigative situation that we encounter. That is why we are continuing to develop relationships with experts in industry, education, and government.

The following is an example of how these relationships help us to investigate cases:

An ISP in California was the victim of repeated attacks by an intruder. Just to give you an idea about the mentality of the hacker community, an employee of the ISP was a former hacker and it was believed that one of his former hacker associates who was jealous of him was responsible for the attacks. The ISP employee was at a hacker conference, DEFCON, where he met an author who

seemed more interested in talking to him than his old friend who was still hacking. Out of jealousy, this hacker repeatedly hacked into the ISP; gained root access; replaced the message of the day with child pornography and profanity about the ISP employee; launched numerous denial of service attacks; and erased their logs. The ISP had to shut down and as a result lost many customers. The attack was reported to CITAC and FBI LA went to the ISP that evening. FBI LA contacted CITAC requesting technical assistance. We contacted a technical expert in Chicago and arranged a conference call with CITAC, FBI LA, the ISP, and the expert.. During this two hour conference call, the expert was able to provide the ISP with procedures to secure their system and remotely log activity from the router to a second UNIX box which would go undetected by the intruder. The ISP sent their log files to the expert for analysis. Additionally, another ISP in Detroit reported similar attacks and the logs from that ISP were sent to the expert as well.

The incidents of computer related crimes continues to grow astronomically. Unfortunately, our resources and expertise have not grown at quite the same pace, but we're getting there. And as we continue to successfully investigate cases, develop liaison, increase our number of agents, and grow our technical expertise, we will continue to see improved results such as we have in the past few years.

During fiscal year 1997, we have worked over 700 cases and we now have approximately 500 cases pending. And our statistical accomplishments continue to grow as well. Arrests are up 950%, indictments are up 110%, and convictions are up 88%. These are the statistics relating only to Title 18 USC 1030 violations, such as computer intrusions. In addition to these cases we also have the more traditional types of crimes that are facilitated by computers. These include crimes facilitated by the Internet such as extortion and child exploitation as well as crimes relating to computer hardware and software theft. Particularly troublesome has been Computer Component Thefts especially prevalent in California's Silicon Valley. Armed robberies are occurring there where computer chips are stolen, sold to SE Asian companies, placed in computers and sold back to the United States. At CITAC, we also support these types of cases with technical, informational, and investigative assistance.

So we're obviously quite busy. Fortunately we reap rewards as a result of our efforts, such as the next case illustrates:

On March 28, 1997, an ISP in San Diego discovered that their servers had been compromised by an intruder. Investigation revealed that a "packet sniffer" was installed on the system which was used to capture user IDs and passwords of authorized users. A cooperating witness (CW) who was using the ISP when the intruder was active engaged the intruder in an Internet Relay Chat conversation. The intruder bragged about how easy it was to compromise the server and advised that he had removed all of the credit card numbers from one of the sites on the server. The intruder offered to sell the credit card numbers to the CW. The FBI enlisted the services of the CW to identify and apprehend the intruder.

Negotiations between the CW and the intruder culminated with the agreement to meet at the San Francisco airport on May 21, 1997 at 11:15 AM to exchange a large number of stolen credit card numbers for approximately $260,000. The meeting took place and the intruder provided the credit card numbers to the CW on an encrypted CD ROM. The intruder gave the CW the book, "The Last Don" and said that the pass phrase to decode the encrypted CD ROM was the first character of every line on page 128 of the book. The subject was then arrested and identified as CARLOS FELIPE SALGADO.

The aggregate credit line on all of the credit carts totaled $1,036,000,000. Based upon projections from the credit cart companies, this translates into a $160,540,000 potential economic loss that was prevented. On August 25, 1997, SALGADO pleaded guilty to two counts of 18 USC Section 1030 and two counts of 18 USC Section 1029. Sentencing is scheduled for November 25, 1997.

As we continue to improve, we will increase our knowledge, innovation, and speed in response which translates into the increased ability for law enforcement to prevent, respond, and conduct high tech investigations across international and organizational boundaries.

La Cooperación Internacional Policial en el Ciberespacio

TIMOTHY B. ATKINS *

Supervisor Agente Especial de la F.B.I. EEUU

Buenos días. Mi nombre es Tim Atkins y soy agente especial Supervisor del FBI. Estoy asignado a la Unidad de Investigaciones de Computadora de la Computer Infrastructure and Thrat Assesment Center (CITAC) de la Jefatura FBI en Washington, DC. Mis responsabilidades incluyen la vigilancia de Investigaciones de Computadora FBI en la parte Occidental de los Estados Unidos. Comenzaré esta mañana por discutir la autoridad investigadora del FBI en el área de investigaciones de computadora y daré una descripción del FBI CITAC incluyendo algunas de las causas que nosotros hemos investigado y actualmente investiga.

El FBI posee gran autoridad investigadora en el área de investigaciones de computadora, ambas en la Seguridad Nacional y en el mundo Criminal. Las fuentes de autoridad para las Investigaciones Nacionales de Seguridad incluyen la Orden Ejecutiva 12333 que establece la autoridad de que el FBI conduzca las Investigaciones. Por lo demás, la Directiva Presidencial de Decisión 39, administra al FBI a servir como la agencia principal para todos los incidentes de terrorismo en US.

En el mundo Criminal, el FBI es la agencia investigadora principal para violaciones de las leyes penales federales relacionadas con actividades

* Traducción del artículo anterior, realizado mediante el programa Power Translator Profesional

cybercriminales. EL título 18 USC de Sección 1030 es el estatuto primario que autoriza a que el FBI investigue intrusiones de computadora.

La denominación 18 USC 1030 permite autoridad al FBI para investigar intrusiones de computadora. Esta autoridad es bastante amplia. Por ejemplo, los actos criminales de un empleado contrariado que destruye malintencionadamente la página WEB de su compañía, así como también un grupo extranjero terrorista que penetre los sistemas de computadora de infraestructuras críticas de nuestra nación y haga estragos en todo el país. Protege cualquier computadora de institución financiera o GOBIERNO DE LOS ESTADOS UNIDOS y también cualquier computadora usada en interestadual o comercio exterior, y que incluye cualquier computadora que usó Internet para el acceso. Protege contra el acceso no autorizado para personas empleadas y forasteros de una compañía. Protege daños intencionados (mientras la intrusión sea intencional), así como también la no autorizada obteniendo de la Información Nacional de Seguridad un informe que valoró en la demasía de $5,000 para una computadora protegida. Tanto si la cyberamenaza o el ataque es Nacional o Extranjero, Aislado o Multifacético, el FBI tiene autoridad jurisdiccional para responder.

Los ataques pueden originarse desde una multitud de diversas fuentes, ambos dentro y fuera de US. Y cuando un cyberataque es descubierto, no hay inicialmente ninguna manera de identificar la fuente del ataque. Una de las más grandes recusaciones a las investigaciones de intrusión de computadora es que el intruso puede cruzar instantaneamente jurisdicciones nacionales e internacionales con el click de un ratón.

Por lo demás, si los terroristas lanzan una escala extensa de cyberataques contra el US, ellos no pueden limitar su ataque al mundo cyber. Ellos pueden lanzar concurrentemente tipos más tradicionales de actos terroristas también, tal como el Centro Mundial de Comercio o bombardear en Oklahoma el Edificio Federal Municipal. Por lo tanto, la respuesta más eficiente a tal ataque multifacetico es facilitada y coordinada por la una entidad de ejecución que la ley equipó con la autoridad y dió recursos para los investigar. En la US, esa entidad es el FBI.

CITAC es parte de la Oficina del FBI de Computers Investigations and Infrastructure Protection (OCIIP). CITAC se compone de cinco Unidades, Unidad de Protección de Infraestructura Crítica, la Unidad de Investigaciones de Computadora, la Especial Unidad de Aplicaciones de Tecnologías, la Unidad Estratégica de Análisis Planificador, y Unidad de Inspección y Análisis de

Amenazas. También parte de OCIIP es el Task Infrastructure Force Protection que responsabiliza con el informe reciente de la Comisión Presidencial sobre la Protección de Infraestructuras en los Estados Unidos.

El CIPU enfoca ocho infraestructuras críticas, Telecomunicaciones, Sistemas Eléctricos de Autoridad, Almacenaje & Transporte de Gas & el Petróleo, Depósito & Finanza, Transporte, Sistemas de abastecimiento de agua, Servicios de Emergencia, & Continuidad de Servicios de Gobierno. El CIPU utiliza los recursos en la Industria, Gobierno, Militar, y la Aplicación de Derecho para IDENTIFICAR, TASAR Y ADVERTIR sobre amenazas y actos ilegales. Estas amenazas incluyen ambos las tradicionales y no tradicionales - tanto físicas y cyber - particularmente amenazas terroristas.

CITAC'S Unidad de Inspección y análisis de amenazas tiene la misión de reunir y diseminar informes sobre cyber intrusiones, la computadora facilita los crímenes, y emerge técnicas y tendencias de intrusión. Esta misión se realiza mediante CITAC WATCH, un Centro de Inspección ubicado en FBIHQ. CITAC WATCH se ha establecido para ser el primer contacto en el FBI en víctimas de cyber intrusiones.

CITAC WATCH analizará los incidentes, facilita la apertura de investigaciones aptas (Inteligencia Contraria criminal o Extranjera), y apoyará las investigaciones. CITAC WATCH es como el depósito central para el informe sobre cyberintrusiones, CITAC tasará el informe, analiza y determina cualquier similitud a otro cyberataque, y diseminará el informe a las oficinas exteriores aptas de FBI. Estamos en proceso para aumentar el nivel de contratación de CITAC WATCH.

El ejemplo siguiente se da para demostrar como trabaja CITAC WATCH. Hace unas semanas, NSA, FUERZA AEREA DE LOS EE.UU., el Ejército & NASA independientemente informó de ataques sobre sus sistemas que originaron desde un ISP en la división LA. Se abrió un proceso y el agente asignado obtuvo la asistencia del ISP y estableció una trampa & rastro. Una alerta CITAC WATCH fue enviada para aconsejar a todas las agencias participantes de gobierno de los ataques y se hizo una llamada para cualquier ataque desde ese ISP e informar inmediatamente a CITAC WATCH y el agente asignado. Nosotros tenemos notificaciones recibidas desde otras agencias de gobierno de ataques adicionales y hemos podido ser en tiempo real el que controla los ataques para obtener la mejor fuente de ataques. CITAC WATCH, la Unidad de Investigaciones de

Computadora, y el FBI LA continúan juntos para trabajar e para identificar y comprender al intruso.

Las responsabilidades de la Unidad de Investigaciones de Computadora incluye administrar las investigaciones de computadora en todo el país. Nosotros también abarcamos educación y otros sectores tanto a nivel público como sectores privados. Por ejemplo, nosotros tenemos un agente especial Supervisor desde el CIU que regularmente se encuentra conectado con América para discutir emisiones políticas relacionado con investigaciones de computadora y cultivar una relación para que nosotros podamos tener una cuestión establecida de contacto para situaciones de crisis tal y como cuando un secuestrador utiliza la conexión en América para enviar sus notas de rescate. Por lo lo demás, coordinamos la investigación con agentes especiales de FBI a nivel personal; nosotros proveemos de equipamiento y pericia técnica como apoyo a las investigaciones; y establecemos cooperación con la ejecución de la ley y computadora a nivel nacional y extranjera mediante equipos de respuesta de incidente.

La Capacitación es una gran prioridad en el área de investigaciones de computadora del FBI. Nosotros hemos desarrollado un nivel básico de entrada basado en el paquete para agentes especiales en investigaciones de computadora de conducción. Ellos incluyen Introducción al UNIX para Investigaciones; Internet & Investigaciones de Red; Las Herramientas Hacker, Explotación, y Técnicas; e Introducción a las Telecomunicaciones. Por demás nosotros proveeremos formación avanzada en áreas especializadas.

Nadie es un perito en cada área técnica. Igual que los hackers hay que admitir y colaborar entre sí para resolver los problemas cuando sabotean ilegalmente en sistemas. Nuestra meta primera es entrenar a los agentes analfabetos de computadora y equiparlos con el conocimiento suficiente - experiencia para que ellos no se sientan intimidados en las entrevistas de administradores de sistemas técnicamente avanzados-. Nosotros queremos que ellos sean adecuados para este trabajo y que las preguntas sean correctas con los administradores de sistemas y consigan el uso de sus habilidades y los recursos a ayudar e identificar la fuente de las intrusiones. Nosotros tenemos que explicar casos en plazos elementales, que es como nosotros tenemos que presentarnos y convencer a un jurado.

Con nuestra formación avanzada, queremos desarrollar una combinación diversa de recursos para que cuando encontremos emisiones técnicas específicas, podamos llamar a esos recursos dentro del FBI. Sin embargo, con la explosión

continua en la tecnología, nosotros nunca tendremos toda la pericia requerida dentro del FBI y que dirija cada situación investigadora que nosotros encontramos. Que es por lo que nosotros continuamos para desarrollar relaciones con peritos en la industria, la educación, y el gobierno.

El siguiente es un ejemplo de como estas relaciones nos ayudan para investigar causas:

Un ISP en California era la víctima de ataques repetidos por un intruso. Justo para darles a ustedes una idea sobre la mentalidad de un hacker, un empleado del ISP que fue un hacker creia que uno de sus antiguos compañeros hackers era el responsable de los ataques a su empresa. El trabajador del ISP estuvo a una conferecia de hackers, DEFCON, y encontró un ponente a quien le pareció más interesado hablarle a él que con su antiguo amigo que todavía era hacker. Este hacker repetidamente saboteó en el ISP; consiguió llegar a la raíz de acceso; reemplazado el mensaje del día con la irreverencia y pornografía infantil sobre el empleado del ISP; los sucesivos ataques fueron revocados; y borrados sus registros. El ISP tuvo que parar y como resultado perdió muchos clientes. El ataque se informó a CITAC y al FBI. El FBI pidió asistencia técnica a CITAC. Nosotros llamamos a un perito técnico en Chicago y contactamos con CITAC, el FBI, el ISP, y el perito. Durante esta dos visitas de consulta, el perito fue apto para proveer al ISP con procedimientos para asegurar su sistema y controlar la actividad de registro desde el router a una segunda caja de UNIX que no sería detectado por el intruso. El ISP envió su registro al perito para el análisis. Por lo demás, otro ISP en Detroit con ataques similares reportados y los registros desde ese ISP se enviaron al perito también.

Los incidentes de computadora relacionaron crímenes continuos que crecían astronómicamente. Desafortunadamente, nuestros recursos y la pericia no ha crecido a la misma marcha, pero nosotros conseguimos estar allí. Y como continuamos exitosamente a investigar causas, desarrollar enlaces, aumentar nuestro número de agentes, y crecer nuestra pericia técnica, continuaremos para ver resultados mejorados.

Durante el ejercicio económico 1997, hemos trabajado sobre 700 causas y ahora tenemos aproximadamente 500 causas pendientes. Y nuestras estadísticas continúan creciendo también. Los arrestos están por encima del 950%, las acusaciones están por encima del 110%, y las convicciones están por encima del 88%. Estas son las estadísticas que relacionaron la Denominación 18 USC con 1030 violaciones, tales como intrusiones de computadora. Además de estas causas

nosotros también tenemos los tipos más tradicionales de crímenes que son facilitados por computadoras. Estos incluyen crímenes facilitado por Internet tal como extorsión así como también explotación infantil que relacionan al software y hackers de computadora con el hurto. Particularmente penoso han sido los hurtos de Computadora especialmente frecuentes en el Valle de Silicio de California. Los robos armados ocurren allí donde se roban los chips de computadora, vendidas a las compañías Asiáticas SE, puestos en computadoras y vendidos en los Estados Unidos. Nosotros también apoyamos a CITAC en estos tipos de causas con la asistencia técnica, informativa, e investigadora.

Obviamente estamos bastantes ocupados. Afortunadamente cosechamos gratificaciones como resultado de nuestros esfuerzos, tal como la próxima causa ilustra:

Sobre el 28 de Marzo de 1997, un empleado del ISP en San Diego descubrió que sus servidores había sido saboteados por un intruso. La investigación dada a conocer como "el olfateador de cajetilla" se instaló sobre el sistema y se usó para capturar los identificativos de usuarios IDs y las contraseñas de usuarios autorizados. Un testigo colaborante (CW) que usaba el ISP cuando el intruso estaba activo comprometió al intruso en una Charla por Internet. El intruso fanfarroneado sobre lo fácil que estuvo saboteando el servidor y aconsejó que él había quitado toda la numeración de tarjetas de crédito desde uno de los puestos sobre el servidor. El intruso ofreció para vender los números de tarjeta de crédito al CW. El FBI alistó los servicios del CW para identificar y comprender al intruso.

Las negociaciones entre el CW y el intruso culminó con el convenio de encontrarse en el aeropuerto de San Francisco el 21 de Mayo de 1997 a las 11:15 y cambiar un número largo de tarjeta de crédito hurtada y numerada para aproximadamente $260,000. La reunión tuvo lugar y el intruso proveyó que la tarjeta de crédito al CW sobre un DISCO COMPACTO ROM encriptado. El intruso dio al CW el libro "El Ultimo Don" y dijo que es la frase para descifrar el DISCO COMPACTO ROM encriptado y era el carácter primero de cada linea sobre la página 128 del libro. El súbdito se fue identificado como CARLOS FELIPE SALGADO.

La línea de crédito agregada sumaba $1,036,000,000. Basada sobre proyecciones desde las compañías crédito, esto se traduce en unos $160,540,000 como pérdida económica potencial. Sobre el 25 de Agosto de 1997, SALGADO se

declaró culpable de dos cargos de 18 USC Sección 1030 y de dos cargos sobre 18 USC Sección 1029. Fue condenando el 25 de Noviembre de 1997.

Como nosotros continuamos para mejorar, aumentaremos nuestro conocimiento, y la innovación, y aumentamos la capacidad para que la ejecución de la ley pueda impedir, responder, y conducir investigaciones de alta tecnología a través de campos internacionales y orgánicos.