DEPARTMENT OF DEFENSE
FREEDOM OF INFORMATION DIVISION
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

Ref: 20-F-1335
September 10, 2020

Ms. Emily Crose
MuckRock News
DEPT MR 96352
411A Highland Ave.
Somerville, MA 02144-2516

Dear Ms. Crose:

This is the final response to your June 18, 2020 Freedom of Information Act (FOIA) request, a copy of which is enclosed for your convenience. We received your request on July 7, 2020, and assigned it case number 20-F-1335. We ask that you use this number when referring to your request.

The Defense Advanced Research Projects Agency (DARPA), a component of the Office of the Secretary of Defense (OSD), conducted a search of their records systems and provided the enclosed documents, totaling 25 pages. Mr. Mark E. Boyd, Director, Security & Intelligence Directorate, DARPA; and Ms. Tanya R. Rose, Program Manager, Office of the Assistant to the Secretary of Defense for Public Affairs, in their capacity as FOIA Initial Denial Authorities, have determined these 25 pages to be responsive to your request and appropriate for release in their entirety, without excision.

Furthermore, due to the age of the requested documents, DARPA recommends that you also submit a FOIA request to the National Archives and Records Administration (NARA). For your convenience, the contact information for NARA is provided below:

The National Archives & Records Administration
8601 Adelphi Road
College Park, MD 20740-6001

This constitutes a full grant of your request, and closes your case file in this office. There are no assessable fees associated with this response.

If you have any questions or concerns about the foregoing or about the processing of your request, please do not hesitate to contact Action Officer, Toni Wilkerson, at 571-372-0429 or antoninette.r.wilkerson.civ@mail.mil.

Additionally, if you have concerns about service received by our office, please contact a member of our Leadership Team at 571-372-0498 or Toll Free at 866-574-4970.

Our FOIA Public Liaison is also available to assist and may be reached at 571-372-0464.

Sincerely,

Stephanie L. Carr

Stephanie L. Carr
Chief

Enclosures:
As stated

MUCKROCK NEWS
DEPT MR 96352
411A HIGHLAND AVE
SOMERVILLE MA 02144-2516

000501 501 1 MB 0.439
T3 P1 *****AUTO**MIXED AADC 601
DARPA
FOIA OFFICE
1155 DEFENSE PENTAGON
WASHINGTON DC 20301-1155

June 18, 2020

To Whom It May Concern:

Pursuant to the Freedom of Information Act, I hereby request the following records:

Documents associated with the formation of the Computer Emergency Response Team (CERT/CC) in 1988. Please also include any documentation related to the Morris worm investigation.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 20 business days, as the statute requires.

Sincerely,

Emily Crose

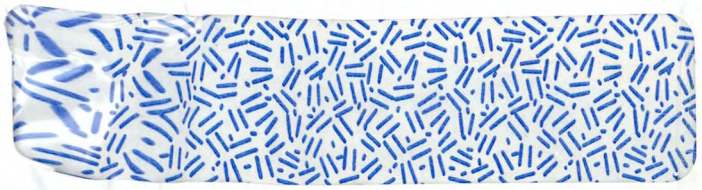
Filed via MuckRock.com
E-mail (Preferred): 96352-01691148@requests.muckrock.com

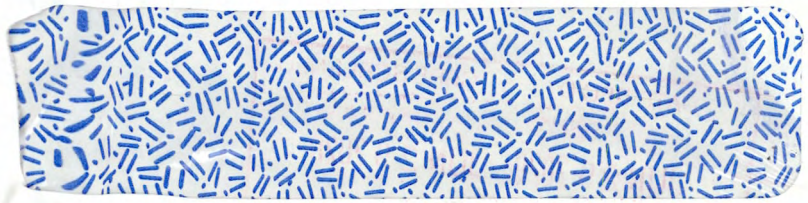
For mailed responses, please address (see note):
MuckRock News
DEPT MR 96352
411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number)

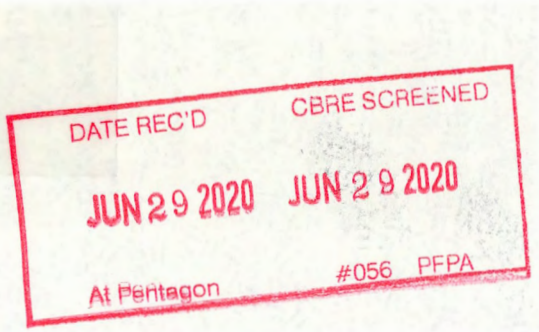
MuckRock News
DEPT MR 96352
411A Highland Ave
Somerville, MA 02144-2516
96352-01691148@requests.muckrock.com

requests might be returned as undeliverable.





PRESORTED
FIRST-CLASS MAIL
US POSTAGE
PAID
PALATINE, IL
PERMIT No. 459


DATE REC'D
JUN 29 2020
CBRE SCREENED
JUN 29 2020
At Pentagon
#056 PFPA

NEWS RELEASE

OFFICE OF ASSISTANT SECRETARY OF DEFENSE
(PUBLIC AFFAIRS)
WASHINGTON, D.C. - 20301
PLEASE NOTE DATE

No. 597-88
(202) 695-0192 (Info.)
(202) 697-3189 (Copies)
(202) 697-5737 (Public/Industry

IMMEDIATE RELEASE December 6, 1988

DARPA ESTABLISHES COMPUTER EMERGENOY RESPONSE TEAM

The Defense Advanced Research Projects Agency (DARPA) announced today that it has established a Computer Emergency Response Team (CERT) to addresss computer security concerns of research users of the Internet, which includes ARPANET. The Coordination Center for the CERT is located at the Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, Pa.

In providing direct service to the Internet community, the CERT will focus on the special needs of the research community and serve as a prototype for similar operations in other computer communities. The National Computer Security Center and the National Institute of Standards and Technology will have a leading role in coordinating the creation of these emergency response activities.

The CERT is intended to respond to computer security threats such as the recent self-replicating computer program ("computer virus") that invaded many defense and research computers.

The CERT will assist the research network communities in responding to emergency situations. It will have the capability to rapidly establish communications with experts working to solve the problems, with the affected computer users and with government authorities as appropriate. Specific responses will be taken in accordance with DARPA policies.

It will also serve as a focal point for the research community for identification and repair of security vulnerabilities, informal assessment of existing systems in the research community, improvement to emergency response capability, and user security awareness. An important element of this function is the development of a network of key points of contact, including technical experts, site managers, government action officers, industry contacts, executive-level decision-makers and investigative agencies, where appropriate.

Because of the many network, computer, and systems architectures and their associated vulnerabilities, no single organization can be expected to maintain an in-house expertise to respond on its own to computer security threats, particularly those that arise in the research community. As with biological viruses, the solutions must come from an organized community response of experts. The role of the CERT Coordination Center at the SEI is to provide the supporting mechanisms and to coordinate the activities of experts in DARPA and associated communities.

(more)

The SEI has close ties to the Department of Defense, to defense and commercial industry, and to the research community. These ties place the SEI in a unique position to provide coordination support to the software experts in research laboratories and in industry who will be responding in emergencies and to the communities of potentially affected users.

The SEI is a federally-funded research and development center, operating under DARPA sponsorship with the Air Force Systems Command (Electronic Systems Division) serving as executive agent. Its goal is to accelerate the transition of software technology to defense systems. Computer security is primarily a software problem, and the presence of CERT at the SEI will enhance the technology transfer mission of the SEI in security-related areas.

-END-

QUESTIONS AND ANSWERS: DARPA ESTABLISHES CERT, 12/6/88

Q: Can you provide background on earlier break-ins?

A: On November 2, 1988, thousands of computers connected to unclassified DoD computer networks were attacked by a virus. Although the virus did not damage or compromise data, it did have the effect of denying service to thousands of computer users. The computer science research community associated with the Defense Advanced Research Projects Agency (DARPA), along with many other research laboratories and military sites that use these networks, quickly responded to this threat. They developed mechanisms to eliminate the infection, to block the spread of the self-replicating program, and to immunize against further attack by similar viruses. Software experts from the University of California at Berkeley, with important contributions from the Massachusetts Institute of Technology and other network sites, rapidly analyzed the virus and developed immunization techniques. These same software experts also provided important assistance in the more recent Internet intrusion of 27-28 November.

As the events unfolded, DARPA established an ad hoc operations center to help coordinate the activities of software experts working around the clock and to provide information to appropriate government officials. The operations center had three main tasks. It facilitated communications among the many groups affected, it ensured that government organizations were promptly informed of developments, and it provided initial technical analysis in DoD. Although the threat was contained quickly, a more maliciously designed virus could have done serious damage.

The recent events serve as a warning that our necessarily increasing reliance on computers and networks, while providing important new capabilities, also creates new kinds of vulnerabilities. The Department of Defense considers this an important national issue that is of major concern in both the defense and commercial sectors. The DoD is developing a technology and policy response that will help reduce risk and provide an emergency reaction response.

Q: Who will be on the CERT?

A: The CERT will be a team of over 100 experts located throughout the U.S. whose expertise and knowledge will called upon when needed. When not being called upon, they will continue their normal daily work. As noted in the release, these experts will include: technical experts, site managers, government action officers, industry contacts, executive-level decision-makers and representatives from investigative agencies.

Q: Is the CERT different from the Coordination Center that is at the SEI?

A: Yes. The Coordination Center will be made up of six or so people who will serve as the communications and nerve center for the total CERT.

Q: What kinds of actions will the CERT be able to take in response to security threats?

A: The CERT will have no authority of its own. It may make recommendations that will be acted upon by DoD authorities.

Qs AND As: CERT (cont'd)

Q: Is the CERT fully operational now?

A: We are in the very early stages of gathering people for the CERT. We are first concentrating on collecting technical experts. A staff is in place at SEI, but details are still being worked out.

Q: Will there just be one CERT?

A: The intent is that each major computer community may decide to establish its own CERT. Each CERT will therefore serve only a particular community and have a particular technical expertise. (The DARPA/SEI CERT will serve, for example, the research community and have expertise in Berkeley-derived UNIX systems and other systems as appropriate.) The National Computer Security Center and the National Institute of Standards and Technology will support the establishment of the CERTs and coordinate among them.

Q: What are the special needs of the research community that their CERT will serve?

A: The special challenge of the research community is improving the level of computer security without inhibiting the innovation of computer technology. In addition, as is often DARPA's role, their CERT will serve as a prototype to explore the CERT concept so that other groups can learn and establish their own.

Q: Does the CERT Coordination Center have a press point of contact?

A: No. Their function is to serve as a nerve center for the user community.

Testimony of L. Dain Gary

Manager, CERT Coordination Center

Software Engineering Institute
Carnegie Mellon University

Before the

Subcommittee on Science

U.S. House of Representatives
Committee on Science, Space and Technology

March 22, 1994

Carnegie Mellon University
Pittsburgh, Pennsylvania 15213-3890
(412) 268-7700

CERT Coordination Center
Software Engineering Institute
(412) 268-5724
FAX: (412)-268-6989

MR. CHAIRMAN AND MEMBERS OF THE SCIENCE SUBCOMMITTEE:

Thank you for the opportunity to testify on the role of the Computer Emergency Response Team (now known as the CERT Coordination Center) in addressing Internet security concerns and on the situation related to the advisory issued by CERT on February 3, 1994.

Background

The CERT Coordination Center is located at Carnegie Mellon University's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania.

The SEI was established in 1984 as a federally funded research and development center in response to the "software crisis." Operated by Carnegie Mellon and sponsored by the Department of Defense (DoD), the SEI concentrates on technology transition to improve software engineering practice. The Advanced Research Projects Agency (ARPA) is the DoD sponsor for the CERT project within the SEI.

Following the Robert Morris Internet Worm incident in November 1988, ARPA (then called DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents like the Morris worm. Within 72 hours, the CERT Coordination Center was operational.

CERT Coordination Center

CERT was established with three members of the SEI technical staff. At that time, the Internet had approximately 80,000 hosts. Over the past five-and-a-half years, the Internet has grown to more than 2.2 million hosts, a 2,400% increase. Today, there are estimated to be as many as 20 million users in the Internet. For comparison, CERT has grown only from 3 to 14 staff members, who have responded to 2,897 computer security incidents. A figure depicting Internet dynamics is included as Appendix A. As of January 1, 1994, CERT had issued 93 computer security advisories. A CERT advisory is a communication to the Internet community alerting them of a vulnerability that is being exploited and describing corrective actions they need to take.

Many busy system administrators depend on the alerts and solutions in CERT advisories to keep them informed. We broadly disseminate these advisories: we send them to an electronic mailing list, post them on electronic bulletin boards, and place them in a public directory on our computer system, which the Internet community can reach by anonymous FTP (file transfer protocol). Also available in this directory are frequently asked questions about CERT, a security checklist, software tools, and documents on security issues.

A complete listing of the advisories issued to date is included as Appendix B. One of CERT's most recent advisories is the subject of this hearing today.

In view of current activities toward establishing new information infrastructures, we hope that our experiences are of value and benefit to others involved in complex computer network security issues.

CERT's Mission

CERT's specific mission is to give the Internet community:

- a 24-hour single point of contact for emergencies
- ease of communication among experts working to solve problems
- a central point for identifying and correcting vulnerabilities in computer systems
- an increased awareness and understanding of information security and computer security issues

The CERT plays both response and prevention roles. Like a fire department, the response efforts are most widely visible; but, also like a fire department, the prevention efforts have the greatest long-term impact.

Incident Response

In the response role, the CERT assists computer system administrators within the Internet who report security problems to us. For maximum availability, we have a 24-hour hotline. We can also be reached by electronic mail and by fax. We help the administrator of the affected site to identify and correct the problem, and we coordinate the response of other sites affected by the same problem. Our staff also works with computer vendors to identify and correct deficiencies ("vulnerabilities") in their products.

The CERT operates in an environment where intruders (often referred to as hackers and crackers) form a well-connected community and use network services, such as e-mail, netnews, and bulletin boards, to quickly distribute information on how to maliciously exploit vulnerabilities in systems. From hobbyists to serious attackers, the intruder community dedicates time to developing programs and sharing information. They have even developed their own publications, and they regularly conduct conferences that deal specifically with tools and techniques for defeating security measures in networked computer systems.

In contrast, the legitimate, often over-worked, system administrators and users on the network frequently find it difficult to take the time and energy from their normal activities to stay current with this information, much less design patches, workarounds (mediation techniques), tools, policies, and procedures to protect the computer systems for which they are responsible.

In short, the intruders are organized, they share information about system weaknesses, and they work together to defeat targeted systems. Unfortunately, legitimate system administrators work independently, trying to protect their own systems from harm as best they can.

CERT activities help to relieve the isolation and burden of the system administrators. In many cases, CERT has informed sites that they were victims of an intrusion before the sites themselves had detected the activity.

In helping the legitimate Internet community work together, we face policy and management issues that are perhaps even more difficult than the technical issues. For example, one challenge we routinely deal with concerns the dissemination of information about security vulnerabilities. CERT's experience suggests that the best way to help the legitimate Internet community improve security in their systems is to work with a small group of vendors and other experts to develop workarounds and repairs for security vulnerabilities disclosed to CERT. To this end, CERT does not publicly disclose system vulnerabilities until a repair or workaround, along with directions on how to apply it, is available and ready for distribution.

Once those conditions have been met, CERT issues an advisory to the entire Internet community, explaining the problem and detailing the corrective action to be taken. To announce a system vulnerability before developing a correction is clearly not in the best interest of the majority of the Internet community; it gives intruders information that can be exploited without giving system administrators a way to prevent intrusion.

Technology Developers

CERT has developed a close rapport with 33 computer system vendors, who view CERT as a neutral and trustworthy source of advice. CERT works closely with this community to inform them of security deficiencies in their products, and to facilitate and track their response to these problems. CERT members work to influence the vendors to improve the basic, as shipped, security within their products and to add security topics in their standard customer training courses. CERT sponsors an annual Vendor Workshop to bring that community together to discuss issues specific to product security, vulnerability analysis, and incident response activities/responsibilities.

CERT members, whenever possible, visit the vendor's site in an effort to meet the developers face-to-face and to improve working relationships within the community. A complete listing of the vendors with whom CERT has established a working relationship is shown below.

Amdahl	Data General	Motorola
Appollo	DEC	NeXT
Apple Computer	Encore	Novell
AT&T	GE Medical Systems	Pyramid
BSD	Harris	Sequent
Cayman Systems	Hewlett Packard	SGI
Cisco Systems	IBM	Solbourne
Cray	Intergraph	Starden/Stellix
Commodore	ISC	Sun
Computer Vision	MIPS	Tennon
Convex	Mt. Xinu	UNISYS

Law Enforcement and Investigative Agencies

CERT has also developed a close rapport with the international community of law enforcement and investigative agencies. These organizations have unique requirements for understanding the security mechanisms within modern computer systems and CERT is a trusted source of accurate, technical information. Listed below are the agencies with whom CERT has established an exchange of technical information.

Federal Bureau of Investigation	United States Secret Service
Royal Canadian Mounted Police	New Scotland Yard
Australian Federal Police	French DST
Interpol	USAF Office of Special Investigation
Dutch National Criminal Intelligence Service	

In November 1992, CERT conducted a special one-day security seminar for several of these agencies.

Incident Prevention

Our investment of time and attention to address the growing problems of incident response allows us to explore the relationship between computer security incidents, system design, system administration and law enforcement issues. These reactive and knowledge gathering activities are of little value without a concerted effort toward devising proactive approaches for resolving critical issues and working with the community to prevent problems before they occur. Since its inception, CERT has labored to balance its increasing incident response load with a prevention program focused on contributing to improvements in information security technology and information security practice.

CERT's association with ARPA, the SEI, and Carnegie Mellon University afforded us an opportunity to reach a broad audience. This position also gave us a foundation for building the credibility we have earned among Internet users and administrators and developing our reputation as a center of experts who can be trusted with sensitive information and who respond with objectivity. Because CERT is not connected with industry, we have no bias toward particular products. Because we are not part of the government, we have no regulatory or enforcement powers. Our role is that of objective advisor.

Research

CERT has established a research effort designed to help us better understand the genesis of security related computer and network security problems. A near term objective of this effort is to narrow the gap between computer security emergencies and the human and technological resources available to deal with them.

As part of our prevention program, we disseminate guidance and information bulletins from time to time, focusing on specific technical management and site administration practices that can improve security or reduce vulnerability to threats known to the CERT. CERT has published and made available the following technical documents:

- **Configuration of Anonymous FTP Areas**

  Anonymous FTP areas can provide valuable services; however, if misconfigured, a site can be vulnerable to several known attacks. Based on observed activity during the past few years, CERT has developed guidelines a site can use to configure their anonymous FTP directory in a more secure manner. A sample directory set-up is provided.

- **Packet-filtering Guidelines**

  The Packet-filtering document was developed as a result of the vulnerabilities discovered in several TCP/IP services, and an increase in the observed exploitation of these vulnerabilities. This document suggests specific services that should either be disabled or filtered at a site's network gateway.

- **Router Configurations**

  Router configurations can be used to either permit or deny access privileges to external or internal hosts. In effect, the router can be used to implement a site's packet-filtering policy. This document provides a sample Cisco configuration file, complete with descriptive notes, that

site administrators may want to review when configuring their own router access privileges.

- **Generic Security Information**

  Useful information collected from CERT incident handling data has been used to create a document discussing UNIX and VMS vulnerabilities exploited by intruders to attack sites. The security document provides information about tools that can be used by system administrators to help make their systems more secure. It is designed to:

  - assist sites that may have experienced a break-in,
  - provide techniques sites can use to assess the security of their systems and to determine if they have been compromised.

In addition, CERT staff members participate in multiple conferences and workshops, and are members of various information security task forces and working groups.

CERT has also developed two security seminars, one targeted specifically at system administrators within the Internet and the other designed to help computer and network managers better understand Internet security issues. CERT staff members, drawing on their incident response experience, developed these seminars to address the recurring problems encountered by sites on the Internet.

For example, we have found that in most cases, site managers can avoid a large number of incidents by taking a number of simple actions. One key action is to establish more rigorous authentication policies for user access. This usually involves giving guidance to users about how to choose passwords; in many cases, it is also useful to install password filter programs to help users avoid passwords that can be easily guessed. Another key action is to develop more rigorous configuration management policies and procedures. These procedures are important not only to ensure that security-related fixes are installed, but also to facilitate the location of unauthorized alterations to systems programs. Many intrusions exploit failures to apply published fixes to well-known vulnerabilities. In many cases, once the intrusion is detected and the obvious holes are closed on a given host, system administrators later discover that the system programs were previously altered by the intruders to allow them to get back into the system.

CERT is an active member of the Federal Information Systems Security Educators Association (FISSEA) and as such, is contributing to the security education efforts of the federal government. An analysis of CERT's tutorial

materials by the FISSEA revealed that CERT's seminars compliment rather than compete with the more traditional courses available from other federal agencies. CERT will continue to work within FISSEA to improve educational offerings within the government.

Our proactive activities continue to grow. Currently, CERT is developing techniques to conduct qualitative and quantitative site security audits, or profiles. Once completed, this capability will serve as the foundation for the development of comprehensive, site specific, computer security improvement programs.

FIRST

From the beginning, ARPA realized that the scale of emerging networks, and the diversity of user communities, would make it impractical for a single CERT organization to provide universal computer security response support. The CERT model, therefore, presumed the creation of multiple incident response organizations, together with mechanisms for coordinating among them. The challenge was to develop prevention and response capabilities that are sensitive to the cultural differences among communities, that account for the nature of the vulnerabilities usually encountered, and that depend on the potential impact of those vulnerabilities.

The CERT Coordination Center worked closely with a number of other organizations and agencies to help them create their own incident response teams. The early model involving multiple response teams was known as the CERT-System. ARPA collaborated with the National Institute of Standards and Technology (NIST) to create a facility for interaction between these incident response organizations. That initiative resulted in the Forum of Incident Response and Security Teams (FIRST).

Within the FIRST, the individual response teams focus on specific user constituencies. A constituency is a group of users, who, while probably geographically dispersed, are bound together by a particular network or a set of common needs and policies. Listed below are the constituencies currently represented within FIRST.

USAF	Motorola	U.S. Sprint
DoD	DDN	Sun
DEC	NASA Ames	NASA NSI
DOW USA	USN	TRW
DoE	Penn State	CCTA (UK)
Purdue	DFN (Germany)	SERT (Australia)
Unisys	Westinghouse	Micro-Bit Virus Center (Germany)
SURFnet (NL)	Renater (France)	General Electric
JAnet (UK)	Apple CORE	NIST

The FIRST members are from government, from academe, and from private industry, and reflect the international distribution of the Internet. There are now seven response teams overseas, six within the European continent, and one on the Pacific Rim. Each response team builds trust within its constituent community by establishing contacts and working relationships with members of that community. These relationships enable response teams to be sensitive to the distinct needs, technologies, and policies of that community. FIRST members collaborate and pool resources when necessary. Contacting their response team is all that is required for a site to gain access to the appropriate resources. The FIRST members work together to avoid overlap of coverage and to cover areas not in their primary portfolios.

Observed Intruder Activities

The initial activities of the intruder community, regardless of the intent or target of an attack, are well understood. Generally the intruders gain access to the Internet through the telephone system - they use dial-up terminal servers or dial directly to a system connected to the Internet - or they have physical access to a system on the Internet. Once established on the initial system, intruders have full access to the Internet and they connect to one or more compromised accounts at other sites before finding a host from which to base their activities. From such a host, they run programs that literally scan hundreds of other computer systems attached to the network to identify which network services those computer systems offer. If the intruders learn that a host computer is offering services that are known to be vulnerable, they then probe that system to determine if those services are indeed vulnerable to attack. If the site manager or system administrator has not configured the system correctly and has not applied published fixes for known security vulnerabilities, the intruders gain access to the system and then attempt to

gain privileged status by exploiting other security weaknesses. This activity, devastating as it may be, often goes undetected by the system administrator.

Activity such as that just described is not infrequent. During 1993, CERT responded to 1,334 computer security incidents, an average of 111 per month. Although the initial steps taken to compromise a networked computer system are well understood, subsequent actions vary from browsing, to collecting sensitive or proprietary information, to inflicting malicious damage.

In July 1993, one of the incidents reported to CERT involved a situation in which it appeared that intruders had installed a network monitoring program and were monitoring network traffic passing through the compromised computer system.

The attack was fairly standard. The intruders looked for, and found, systems with uncorrected vulnerabilities. Once the intruders were into the system, they quickly gained privileged access and did the following:

1) installed and started their network monitoring program.

2) installed a back door (a secret way into the computer) to the system to allow them to come and go at will. In this case, the intruders re-entered the system to collect the results of their monitoring activity.

3) installed modified systems utilities in an effort to conceal their activities and the presence of the network monitor.

Total elapsed time for this activity, from initial access by the intruder to having the network monitor installed, can be as little as 45 seconds.

One of the 157 incidents reported to CERT in September involved monitoring activity similar to that observed in July.

In October, a computer operated by an Internet access service provider was found to be compromised, and a monitoring program had been installed. An analysis of the computer log files from the site revealed that connections to 369 other computer systems had been made while the monitor was active. With reference to the FIRST model, many of the 369 "downstream" computers were in other constituent communities. CERT contacted the response teams within those communities and gave them information specific to sites in their domains. CERT contacted the remaining administrators to ensure they were aware that sensitive log-in data for accounts on their systems may have been captured at the compromised service provider's site.

During the period between October and January, although CERT handled 397 computer security incidents, only one other incident involving a network monitoring attack was reported.

During this entire period, the intruders employed well-known and time-proven techniques for breaking into networked computer systems, and their network monitoring activities were isolated and sporadic at best. From CERT's perspective, there was no evidence of unusually threatening behavior.

CERT Advisory 94:01 - Ongoing Network Monitoring Attacks

During the last week of January, CERT received seven reports of network monitoring activity. This dramatic increase was especially significant for several reasons.

1) In analyzing the systems at sites reporting problems, CERT discovered subtle differences in the techniques being employed by the intruders. This was an indication that the technique being used to attack and compromise these systems had been distributed within the intruder community. Now it looked as though a number of different intruders had copied the original technique and had begun to enhance it. At least one intruder had begun using encryption techniques to protect the surveillance data.

2) Two of the sites reporting incidents were network service providers. It was at these sites that the exposure was the most significant. Log files from one compromised computer at a service provider's site contained 20,000 entries.

3) The intruders had gained access to systems critical to the network. Although we had not yet observed any malicious behavior, the potential for widespread damage was tremendous.

CERT released its Network Monitoring Advisory on February 3, 1994. We believed the potential for damage was so great that, in addition to the standard Internet announcement, we issued a press release to ensure the message reached as many system users as possible.

Since then, 27 sites, using the information in the CERT advisory, have found network monitoring programs surreptitiously installed on their computer systems, and at least 12 others suspect the activity but have been unable to confirm the presence of a monitoring program.

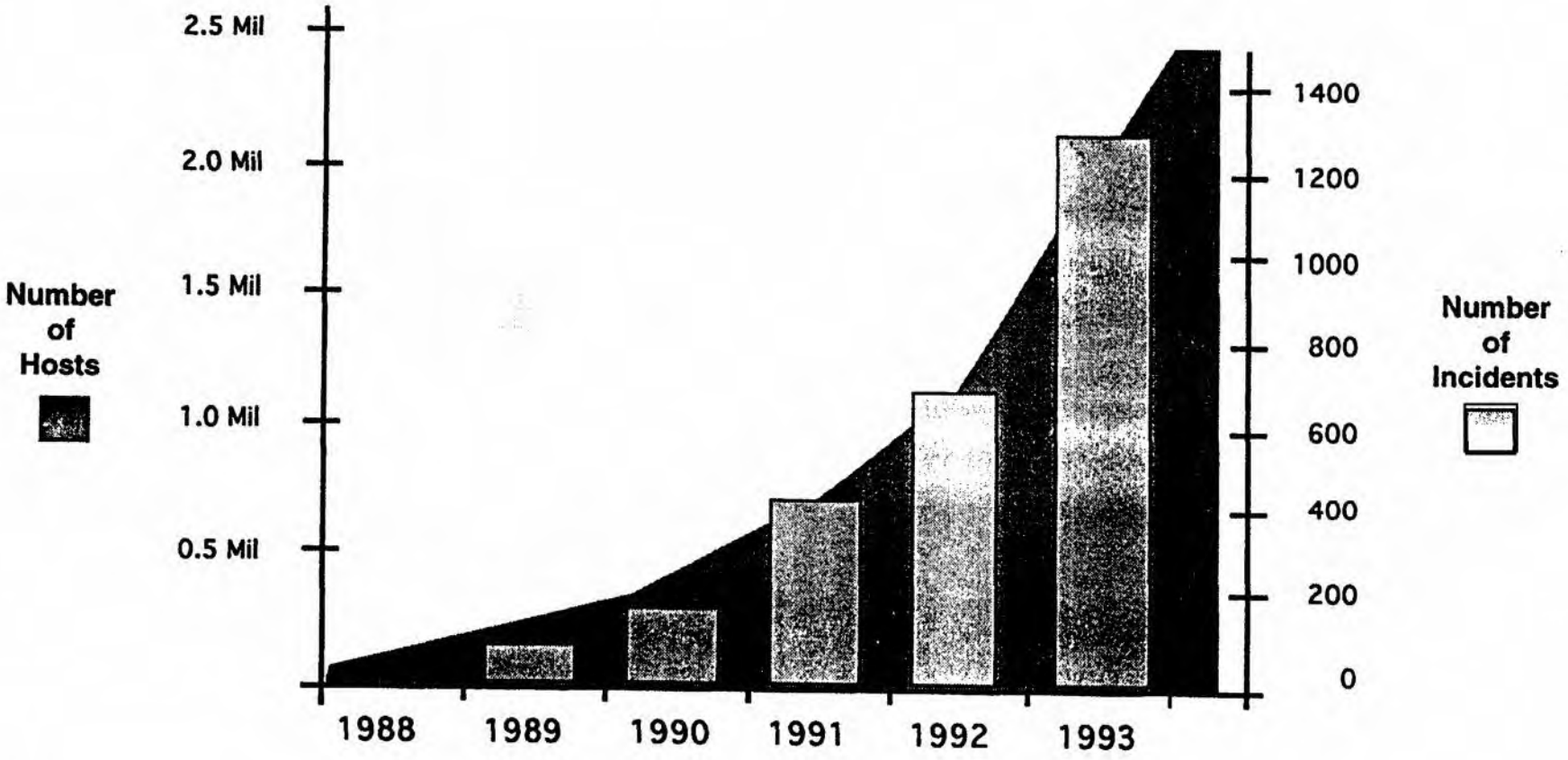
Next Steps

CERT, with ARPA's support, will continue to provide incident response and computer security services to the Internet community and looks forward to providing those services to the next generation of information infrastructure we see emerging. CERT will continue to champion better security in network products "as shipped" from the vendor's site, and we will continue work on the development of tools and technologies to aid the system and security administrators in securing their systems.

ARPA will continue investing in programs that extend our knowledge of computer security, network security, and network management technology.

Thank you for the opportunity to discuss the CERT Coordination Center and its role in the Internet. I would be pleased to answer any questions you may have.

Internet Dynamics



Sponsored by the Advanced Research Projects Agency

Appendix B

CERT Advisories

Number	Title
CA-88:01	ftpd Vulnerability
CA-89:01	Passwd Hole
CA-89:02	Sun Restore Hole
CA-89:03	Telnet Break-in Warning
CA-89:04	"Wank" Worm on SPAN Network
CA-89:05	DEC/Ultrix 3.0 Systems
CA-89:06	DEC/Ultrix 3.0 Systems Update
CA-89:07	Sun RCP Vulnerability
CA-90:01	Sun Sendmail Vulnerability
CA-90:02	Internet Intruder Warning
CA-90:03	Unisys U5000 /etc/passwd Problem
CA-90:04	Apollo Domain/OS suid_exec Problem
CA-90:05	SunView selection_svc Vulnerability
CA-90:06	NeXT's System Software
CA-90:06a	NeXT's System Software
CA-90:07	VMS ANALYZE/PROCESS_DUMP
CA-90:08	IRIX 3.3 & 3.31 /usr/sbin/Mail
CA-90:09	VAX/VMS Break-ins
CA-90:10	Rumor of Alleged Attack

CA-90:11	Security probes from Italy
CA-90:12	SunOS TIOCCONS Vulnerability
CA-91:01a	REVISED SunOS /bin/mail Vulnerability
CA-91:02a	SunOS in.telnetd Vulnerability
CA-91:03	Unauthorized Password Change Requests Via Mail Messages
CA-91:04	Social Engineering
CA-91:05	DEC Ultrix Vulnerability
CA-91:06	NeXT rexd, /private/etc, Username me Vulnerabilities
CA-91:07	SunOS Source Tape Installation Vulnerability
CA-91:08	AT&T System V Release 4 /bin/login Vulnerability
CA-91:09	Patch for SunOS /usr/etc/rpc.mountd
CA-91:10	SunOS lpd Vulnerability
CA-91:10a	REVISION NOTICE: New Patch for SunOS /usr/lib/lpd
CA-91:11	Ultrix LAT/Telnet Gateway Vulnerability
CA-91:12	Trusted Hosts Configuration Vulnerability
CA-91:13	DEC Ultrix /usr/bin/mail Vulnerability
CA-91:14	SGI "IRIX" /usr/sbin/fmt Vulnerability
CA-91:15	Mac/PC NCSA Telnet Vulnerability
CA-91:16	SunOS SPARC Integer Division Vulnerability
CA-91:17	DECnet-Internet Gateway Vulnerability
CA-91:18	Active Internet tftp Attacks
CA-91:19	AIX TFTP Daemon Vulnerability
CA-91:20	/usr/ucb/rdist Vulnerability

CA-91:21	SunOS NFS Jumbo and fsirand Patches
CA-19:22	SunOS OpenWindows V3.0 Patch
CA-91:23	Hewlett Packard/Apollo Domain/OS crp Vulnerability
CA-92:01	NeXTstep Configuration Vulnerability
CA-92:02	Michelangelo PC Virus Warning
CA-92:03	Internet Intruder Activity
CA-92:04	AT&T /usr/etc/rexecd Vulnerability
CA-92:05	AIX REXD Daemon Vulnerability
CA-92:06	AIX uucp Vulnerability
CA-92:07	AIX /bin/passwd Vulnerability
CA-92:08	Silicon Graphics Computer Systems "IRIX" lp Vulnerability
CA-92:09	AIX Anonymous FTP Vulnerability
CA-92: 10	AIX crontab Vulnerability
CA-92:11	SunOS Environment Variables and setuid/setgid Vulnerability
CA-92: 12	Revised Patch for SunOS /usr/etc/rpc.mountd Vulnerability
CA-92: 13	SunOS NIS Vulnerability
CA-92: 14	Altered System Binaries Incident
CA-92: 15	Multiple SunOS Vulnerabilities Patched
CA-92: 16	VMS Monitor Vulnerability
CA-92: 17	Hewlett-Packard NIS ypbind Vulnerability
CA-92:18	Revised VMS Monitor Vulnerability
CA-92: 19	Keystroke Logging Banner
CA-92:20	Cisco Access List Vulnerability

CA-92:21 ConvexOS and ConvexOS/Secure Vulnerabilities

CA-93:01 Revised Hewlett-Packard NIS ypbind Vulnerability

CA-93:02a REVISION NOTICE: New Patch for NeXT NetInfo "_writers" Vulnerabilities

CA-93:03 SunOS File/Directory Permissions

CA-93:04a REVISION NOTICE: Commodore Amiga UNIX finger Vulnerability

CA-93:05 OpenVMS and OpenVMS AXP Vulnerability

CA-93:06 wuarchive ftpd Vulnerability

CA-93:07 Cisco Router Packet Handling Vulnerability

CA-93:08 SCO /bin/passwd Vulnerability

CA-93:09 SunOS/Solaris /usr/bil/expreserve Vulnerability

CA-93:09a REVISION NOTICE: SunOS/Solaris /usr/lib/expreserve Vulnerability

CA-93:10 Anonymous FTP Activity

CA-93:11 UMN UNIX gopher and gopher+ Vulnerability

CA-93:12 Novell LOGIN.EXE Vulnerability

CA-93:13 SCO Home Directory Vulnerability

CA-93:14 Internet Security Scanner (ISS)

CA-93:15 /usr/lib/sendmail, /bin/tar, and /dev/audio Vulnerability

CA-93:16 Sendmail Vulnerability

CA-93:16a Sendmail Vulnerability **Supplementary advisory containing vendor patch information**

CA-93:17 xterm Logging Vulnerability

CA-93:18 SunOS/Solbourne loadmodule and modload Vulnerability

CA-94:01 Ongoing Network Monitoring Attacks

CA-94:02 Revised Patch for SunOS /usr/etc/rpc.mountd Vulnerability

CA-94:03 IBM AIX Performance Tools Vulnerability

CA-94:04 SunOS /usr/ucb/rdist Vulnerability

CA-94:05 MD5 Checksums

L. DAIN GARY

Dain has been working in the area of computer and information security for over 16 years. Currently he is the manager of the CERT Coordination Center, located at Carnegie Mellon University's Software Engineering Institute. Dain joined the CERT team from Mellon Bank Corporation where he served as the Director of Corporate Data Security. While at Mellon, he was named to the ANSI X9F Committee developing Financial Information Security Standards, and was appointed to the Information Systems Security Committee of the American Bankers Association. Dain spent four years at the National Computer Security Center where he directed the Commercial Product Evaluations program.

Dain is a Certified Information Systems Security Professional (CISSP), and is currently the Vice President of the Information Systems Security Association (ISSA).

Carnegie Mellon University

Software Engineering Institute

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the Department of Defense through the Advanced Research Projects Agency (ARPA). The SEI contract was competitively awarded to Carnegie Mellon University in December 1984. It is staffed by approximately 250 technical and support people from industry, academia, and government.

➤Mission

Because software has become an increasingly critical component of U.S. defense systems and because the demand for quality software produced on schedule and within budget exceeds its supply, the U.S. Department of Defense established the Software Engineering Institute with a charter to advance the practice of software engineering.

The SEI mission is to provide leadership in advancing the state of the practice of software engineering to improve the quality of systems that depend on software.

The SEI expects to accomplish this mission by promoting the evolution of software engineering from an ad hoc, labor-intensive activity to a discipline that is well managed and supported by technology.

➤Focus Areas

The SEI carries out its mission through four areas of focus:

- *Software Process*: making lasting improvements in the software engineering practice to enable production of high-quality software within budget and schedule constraints.
- *Software Risk Management*: developing and institutionalizing a systematic approach for identifying and managing the uncertainty in developing software-intensive systems.
- *Real-Time Distributed Systems*: ensuring that developers of all major real-time distributed software systems in the DoD routinely employ quantitative methods to evaluate software engineering designs, upgrades, and tradeoffs.
- *Software Engineering Techniques*: codifying an accepted best practice to engineer software, and standards supporting the practice.

To increase the number of highly qualified software engineers, the SEI also seeks to improve software engineering education within academia, government, and industry.

In response to computer security threats, ARPA established the Computer Emergency Response Team (CERT) Coordination Center at the SEI to support Internet users. The members of the CERT Coordination Center work with the Internet user community and technology producers to address and prevent computer emergencies.

To accelerate the dissemination of new technologies and methods, the SEI offers U.S. organizations from industry, academia, and government several methods of interacting with the institute. For information on the subscriber program, technical reports, continuing education courses, and symposia, write or call:

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: (412) 268-5800
FAX: (412) 268-5758

St. Johns

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

SUBCOMMITTEE ON SCIENCE

HEARING ON INTERNET SECURITY

March 22, 1994

9:30 a.m. - 2318 Rayburn House Office Building

WITNESS LIST

Mr. L. Dain Gary, Manager
Computer Emergency Response Team Operations
Carnegie Mellon University
Pittsburgh, Pennsylvania
(CERT is one of the response teams that form the
Forum of Incident Response and Security Teams (FIRST))

Mr. Thomas T. Kubic, Chief
Financial Crimes Section
Federal Bureau of Investigation
Washington, DC

Dr. Vinton G. Cerf, President
Internet Society
Reston, Virginia
(Senior Vice President of Data Architecture, MCI)

Mr. Lynn McNulty
Associate Director for Computer Security
Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, Maryland
(NIST is the secretariat for FIRST)

Dr. Stephen D. Crocker, Vice President
Trusted Information Systems
Glenwood, Maryland
(Area Director for Security, Internet Engineering Task Force)