NIPC ADVISORY 99-031

"Year 2000 Y2K"

December 28, 1999

Introduction

Large-scale U.S. infrastructure disruptions are not expected from "Y2K failures" during the Y2K transition period. However we are prepared for a possible increase in real or reported criminal cyber activity (such as hacking and spreading computer viruses), considering the heightened awareness of and media focus on malicious activity during the Y2K period.

Any increased criminal activity during the Y2K period could raise the level of problems in infrastructure systems, adding to genuine Y2K-generated issues and the normal level of infrastructure concerns. We anticipate encountering both known and new viruses and hacking exploits. We could see the dissemination of several new and possibly destructive viruses, and the successful exploitation of both corporate and government information systems. But even these possibilities reflect only a larger assembly of the same kinds of malicious activity seen and addressed every day.

Finally, known and possible extremist or apocalyptic terrorist activity in the United States by individuals or groups suggests the possibility of threats to domestic infrastructures. For example, the media have reported arrests of certain individuals allegedly planning violent actions against electric power and oil and gas facilities. These indications of possible threats to our infrastructures warrant an increased vigilance to protect against both cyber and physical threats to our nation's critical infrastructures.

Summary

The Y2K Transition might be seen by potential malefactors as an unprecedented opportunity for malicious code release and associated publicity, where a new and significant exploit can achieve a widespread notoriety in the information security and hacker world. Viruses and exploits like Melissa and its variants, ExploreZip, Back Orifice, mobile code, etc. reflect increasing sophistication in the use of e-mail and attachments, increasing variation on prior exploits, and remote access and control of malicious code. Additional virus activity can be expected during the Y2K period, following the recent examples of W32.mypics, ICQ Greeting and Babylonia.

Distributed denial of service tools have recently been discovered on various computer systems, creating large networks of hosts capable of launching significant coordinated packet flooding denial of service attacks. These tools target high bandwidth sites and connections, use readily accessible technical vulnerabilities for installation, and reflect suspicious installation and tool development activity. Possible motives for this deployment could include exploit demonstration, network systems reconnaissance, or even preparation for major denial of service attacks. Such attacks could take place during the Y2K period.

Back Orifice 2000 remains a significant open-source tool easily customized for malicious purpose; we expect that its malicious use and adaptation will continue to increase in the future, and could be applied during the Y2K period.

The installation of malicious code under cover of Y2K-remediation remains a possibility, considering the numbers and scale of systems remediated for Y2K, the significant access granted throughout computer systems and networks for this work, and the clear, predictable window of opportunity to conduct this action. Such code could be activated during the transition period or long thereafter, to allow future access to the network or to deny service.

A number of long-known computer viruses continue to impact systems because of inconsistent and incomplete security implementation and oversight. The rising attention to computer virus activity during the Y2K transition period will likely include "discovery" and publicity of old virus problems like Marker and Melissa.

Harassing and malicious actions against Internet sites (such as those seen by U.S. Government and military web sites, the WTO, commercial sites like eBay and eToys, etc.) continues as an element of network systems activity; these actions are increasingly common and could well be a part of the Y2K transition and associated press coverage.

Finally, security measures taken in preparation for Y2K or as a result of initial Y2K problems may cause unintended consequences. Systems may be shut down to avert problems, only to cause a more serious operational impact than remaining connected. For example, the closure of network connections could generate a significant e-mail backlog that might generate more problems when reconnected than if connectivity were maintained throughout. Information systems owners and operators must remain deliberate and logical in their situational assessment, actions and management recommendations. Y2K is primarily a higher volume, higher attention version of the types of problems seen in normal network operations.

Virus Summary

At this point there are four viruses that are of particular concern during the Y2K transition. The first three of the viruses are Microsoft Word macro viruses. These three viruses, in their current variants are not very destructive; however, because macro viruses are so easily modified, there may possibly be new variants with "trigger" dates during the Y2K transition that may have destructive payloads. The last virus, PC CIH, is an older, more common virus, but still very prevalent and has a very destructive payload and could cause very severe damage to infected machines.

W97M/Marker is a macro virus that is spreading very rapidly and has a disruptive payload. All variants of Marker steal some type of information from infected machines and then covertly FTP the information to a specified IP address.

W97M/Class is a macro virus that infects documents and templates created in Microsoft Word. Class is polymorphic, which means it is capable of mutating its signature, thus making detection and removal more difficult. Class also exhibits stealth characteristics, which further complicates detection and removal. The Class virus has several "trigger" dates for execution of the payload, the 31st or 14th of the month, depending on the variant. In current versions the payload is not destructive.

W97M/Melissa is a relatively old virus, but is still a threat due to the number of variants and the potential to cause a denial of service on mail servers. Melissa spreads as an e-mail message with an infected Microsoft Word document as an attachment. Despite the age of the original Melissa virus, the numerous variants of Melissa and their ability to spread constitute a continued threat.

PC CIH was first seen in the summer of 1998, but is still spreading very rapidly. PC CIH has a very destructive payload which will delete the first megabyte of data on all hard drives available to the infected machine and overwrite flash BIOS memory. The payload is triggered on different dates depending on the variant which infected the machine. Typical trigger dates are the 26th of any month.

Other viruses in the high-medium threat range, based on an NIPC evaluation, are:

Name of Virus	Variants	Type	Risk
PE PADANIA (Padania)	joke, ne 230, 3932,a,b	Macro	High

W97 PRILISSA.A (Prilissa)		Macro	High-Medium

Viruses in the medium to low threat range:

Name of Virus	Variants	Type	Risk
W32.MyPics (MyPics)		Worm	Medium
Count2K (Y2Kcount)		Trojan	Medium
W97M TRISTATE (TRISTATE)	O97M, P97M, W97M	Macro	Medium - Low
W97.MELISSA.AD (Melissa AD)		Macro	Medium - Low
Troj ICQGreeting (ICQ Greeting)		Trojan	Medium - Low
W97M/MMKV.A (MMKV)		Macro	Medium - Low
W32/Fix (FIX) or (Trojan Fix2001)		Win32	Medium - Low

Viruses in the low to medium threat range:

Name of Virus	Variants	Type	Status	Risk
Millennium v2.0 (Millennium2)		Trojan		Low to Medium
W97M/ETHAN (Ethan)	a, at, b, c, q, frome, mod, mrx	Macro		Low
PE Babylonia (Babylonia)		Trojan		Low to Medium
W32/ska (Happy New Year)		Win 32		Low
W97M/Chantal (Chantal)		Macro		Low
W97M/CLSTNT.B (CLSTNT.B))		Macro		Low
X97M/PIXLY (Pixly))		Macro		Low
ATOMIC-1A (ATOMIC-1A)		Virus		Low
ATOMIC-1B (ATOMIC-1B)		Virus		Low
ARCV-718 (ARCV)		Virus		Low
CPW.1527 (CPW)		Virus		Low
DIOGENES (DIOGENES)		Virus		Low

MINOSSE (MINOSSE)		Virus		Low
NULL (Null)		Virus		Low
PE KRIZ (PE Kris)		Virus	Old	Low
PRIME (Prime)		Virus	Old	Low
TOPO (TOPO)		Virus	Old	Low
VBS Chrystal.C (Chrystal)		Virus	Old	Low
W97M A OPEY (OPEY)		Virus	Old	Low
W97M CALIGULA (CALIGULA)		Virus	Old	Low

Disclaimer

The above lists are not comprehensive due to the sheer number of known viruses. The virus evaluations are based on all information available to the NIPC at the time of advisory preparation and are subject to change as new information becomes available concerning new viruses and variants. In particular, judgments made concerning risk are subjective and supersede previously disseminated NIPC virus listings.

Recommendations

1. Get and stay informed about potential threats and possible solutions; keep up to date by regularly reviewing Y2K breaking news from various sources. Expect a certain degree of initial confusion and conflicting reports.
2. Get yourself a good anti-virus package, easy to use and update, and able to screen incoming messages for the fast-multiplying e-mail viruses.
3. After installation, keep the signature files and scanning engine updated. Hundreds of new viruses emerge each month, and the January 1st transition may see a boom in new activity. Virus writers are constantly inventing new ways of designing and distributing viruses, so your only secure source of protection is to make sure that you update your signature files regularly. In times of high threat, you may want to set your anti-virus programs to automatically download new pattern files every day.
4. Getting and maintaining a good anti-virus package solves only some of your security issues; viruses may still enter through your browser or macro files. Configure your browser security to a higher level by disabling ActiveX and Java controls in Internet Explorer and Netscape, and enable macro protection in Excel and Word. If you find something suspected as a virus and it has not been stopped by anti-virus software, report it and get it checked immediately.
5. During the holiday season, you may also find your system clogged by spam and electronic holiday cards. The added overhead in delivering and filtering these messages may also strain your e-mail servers and system RAM and storage resources.
6. Make sure that the rest of your systems, servers and firewalls are secure. Download the latest security patches and install them correctly. As with the anti-virus protection, regularly check to make sure you have the latest protection.
7. Understand your system's normal baseline operating parameters, so differences are quickly spotted and investigated.

8. Prepare and implement (if necessary) realistic contingency plans.
9. Recipients are asked to report significant or suspected criminal activity to their local FBI office or the NIPC Watch and Warning Unit, and computer emergency response support and other law enforcement agencies, as appropriate. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206, or nipc.watch@fbi.gov.