EXAMINATION REPORT

CASE NAME / NUMBER
Bandy adv. State of Arizona
CR2005-014635

ACQUISITION

I received the Court's Protective Order on April 20, 2006. Pursuant to the Order, I had 10 days to provide the State with properly clean hard drives and CD-ROMs.

On April 20, 2006, I mailed a blank CD-ROM and a 200gb Western Digital IDE hard drive, Serial No. WCAMT1329762, forensically wiped using EnCase version 5.0, to Daniel Strange for the purpose of creating a bit for bit forensic image of the digital evidence in this case.

Pursuant to the Court's Order, the State had 10 days from the receipt of the hard drives and CD-ROMs to make "one bit by bit mirror image password protected EnCase copy of each of the hard drives and of each CD-ROM."

On or about May 24, 2006, I contacted the computer forensics expert for the State, Larry Core, regarding the status of the imaging as I had not heard anything in this regard. Mr. Core emailed me the same day and informed me that he had not yet created the images and would be unable to do so until May 30, 2006 and that I would have to pick up the evidence on May 31, 2006 as he was leaving for vacation the following day.

On May 31, 1006, I traveled from Tucson to Mr. Core's offices at 16212 North 28th Avenue to pick up the evidence. Mr. Core provided me with an envelope which contained the hard drive I had sent to Mr. Strange, confirmed by the serial number, with the forensic image of the evidence ("HDD01"). I placed the envelope into a plastic folder with the Court's Protective Order for transporting back to my lab.

Mr. Core then informed me that he had not created an image of the CD-ROM evidence. He explained that the original evidence CD was in the possession of someone else who was currently on vacation and he would not be able to obtain the CD until he returned from his own vacation. I explained to him that I had traveled from Tucson at the client's expense to pick up ALL of the evidence in this case pursuant to the Court's Order. At that time, Mr. Core offered to forward the imaged copy of the CD-ROM via Federal Express once he had completed the imaging process. I declined Mr. Core's offer due to the Court's Order and the legalities with shipping contraband. I asked Mr. Core to contact me immediately upon completion of the imaging of the CD-ROM.

I traveled directly back to my offices in Tucson and placed the plastic folder with the evidence and the Court's Protective Order into the evidence safe in my forensics lab.

TYPED EXAMINER'S NAME	ORGANIZATION	
TAMI L. LOEHRS	LAW2000, INC.	
SIGNATURE	DATE	EXHIBIT
Tami Loehrs	September 19, 2006	

EXAMINATION REPORT

CASE NAME / NUMBER
Bandy adv. State of Arizona
CR2005-014635

On June 9, 2006, I traveled from Tucson to the Maricopa County Attorney's Office and was provided with a clear CD case that contained a CD-ROM with the forensic image of the evidence, labeled "Evidence". I was provided a separate envelope with a password. I placed both items into a plastic folder with the Court's Protective Order for transporting back to my lab.

I traveled directly back to my offices in Tucson and placed the plastic folder with the evidence and the Court's Protective Order into the evidence safe in my forensics lab.

PURPOSE OF EXAM

The purpose of this exam is to locate unwanted intrusions including viruses, Trojans, malware, and evidence of hijacking and/or hacking of the system. Determine the possibility of system compromise by outside sources such as hackers.

COMPUTER FORENSIC EXAMINATION

On June 6, 2006, I removed HDD01 from the evidence safe. I connected HDD01 to a FastBloc device connected to my forensics machine, created a new EnCase case file on my local machine and added the evidence files to the case. While the Court ordered that the EnCase files be password protected, the EnCase files created by Larry Core were NOT password protected.

I ran the "initialize case" feature of EnCase to determine the system specifications and the forensics imaging performed by Larry Core, reported as follows:

Name:	**120 GB HD**
ActualDate:	**06/06/05 10:49:25AM**
TargetDate:	**06/06/05 10:49:44AM**
FilePath:	**E:\120 GB HD.E01**
Case Number:	**04-42357269**
Evidence Number:	**501**
Examiner Name:	**Detective Larry K. Core #140**
Notes:	**Seagate HD #3JT1CK22 HP Pavilion**
Drive Type:	**DRIVEFIXED**
File Integrity:	**Completely Verified, 0 Errors**
Acquisition Hash:	**CEDFE153E90EB6F972759DE7389E47AB**
Verify Hash:	**CEDFE153E90EB6F972759DE7389E47AB**
EnCase Version:	**3.22g**
System Version:	**Windows 2000**
Fastblocked:	**Yes**
Is Physical:	**Yes**
Compression:	**None**
Total Sectors:	**234441648**

TYPED EXAMINER'S NAME	ORGANIZATION	
TAMI L. LOEHRS	LAW2000, INC.	
SIGNATURE	DATE	EXHIBIT
	September 19, 2006	

EXAMINATION REPORT

CASE NAME / NUMBER
Bandy adv. State of Arizona
CR2005-014635

C

Volume

File System:	FAT32	Drive Type:	Fixed
Sectors per cluster:	8	Bytes per sector:	512
Total Sectors:	9,313,857	Total Capacity:	4,759,379,968 bytes (4.4GB)
Total Clusters:	1,161,958	Unallocated:	722,849,792 bytes (689.4MB)
Free Clusters:	176,477	Allocated:	4,036,530,176 bytes (3.8GB)
Volume Name:		Volume Offset:	63
OEM Version:	RECOVERY	Serial Number:	2ED6-1123
Heads: 240	Sectors Per Track:	63	
Unused Sectors:	63	Number of FATs:	2
Sectors Per FAT:	9,078	Boot Sectors:	32

Unable to open registry on volume C

D

Volume

File System:	NTFS	Drive Type:	Fixed
Sectors per cluster:	8	Bytes per sector:	512
Total Sectors:	225,106,560	Total Capacity:	115,254,554,624 bytes (107.3GB)
Total Clusters:	28,138,319	Unallocated:	106,293,133,312 bytes (99GB)
Free Clusters:	25,950,472	Allocated:	8,961,421,312 bytes (8.3GB)
Volume Name:	HP_PAVILION	Volume Offset:	9,313,920
Driver Information:	NTFS 3.1 Chkdsk 0		

OS Info

Product Name:	Microsoft Windows XP
Current Version:	5.1
Registered Owner:	
Registered Organization:	
System Root:	C:\WINDOWS
Current Build Number:	2600
Path Name:	C:\WINDOWS
Product ID:	55277-OEM-0011903-00106
Last Service Pack:	Service Pack 1

I reviewed the user login accounts and noted the only accounts are the Windows XP default accounts. It appears that all users were accessing the computer using the default account "Owner. User account information is reported as follows:

Account Info

User name: Administrator

Full Name:	
Type of User:	Local User
Account Description:	Built-in account for administering the computer/domain
Primary Group Number:	513
Security Identifier:	S-1-5-21-1142254380-2972230178-3110824138-500
User belongs to group:	Administrators
Logon Script:	

TYPED EXAMINER'S NAME	ORGANIZATION	
TAMI L. LOEHRS	LAW2000, INC.	
SIGNATURE	DATE	EXHIBIT
	September 19, 2006	

EXAMINATION REPORT

CASE NAME / NUMBER
Bandy adv. State of Arizona
CR2005-014635

Profile Path:
Last Logon:
Last Password Change:
Last Incorrect Password Logon:

User name: Guest
Full Name:
Type of User: Local User
Account Description: Built-in account for guest access to the computer/domain
Primary Group Number: 513
Security Identifier: S-1-0-0-0-0-0-0
User belongs to group: Guests
Logon Script:
Profile Path:
Last Logon:
Last Password Change:
Last Incorrect Password Logon:

User name: HelpAssistant
Full Name: Remote Desktop Help Assistant Account
Type of User: Local User
Account Description: Account for Providing Remote Assistance
Primary Group Number: 513
Security Identifier: S-1-5-21-1142254380-2972230178-3110824138-1005
Logon Script:
Profile Path:
Last Logon:
Last Password Change: 12/04/04 06:37:52PM
Last Incorrect Password Logon:

User name: Owner
Full Name:
Type of User: Local User
Account Description:
Primary Group Number: 513
Security Identifier: S-1-5-21-1142254380-2972230178-3110824138-1003
User belongs to group: Debugger Users
Administrators
Logon Script:
Profile Path: D:\Documents and Settings\Owner
Last Logon: 12/13/04 09:27:08PM
Last Password Change: 04/09/03 04:19:24PM
Last Incorrect Password Logon:

I reviewed HDD01 for malicious software infections and located over 200 infected files which is detailed in the attached report. One or more of the infections identified on the system renamed a significant number of computer files making it impossible to detect or track all of the activity. While I could not positively identify all of the intrusions found on the system, the following are some of the more serious infections identified:

TYPED EXAMINER'S NAME	ORGANIZATION	
TAMI L. LOEHRS	LAW2000, INC.	
SIGNATURE	DATE	EXHIBIT
	September 19, 2006	

EXAMINATION REPORT

CASE NAME / NUMBER
Bandy adv. State of Arizona
CR2005-014635

Process Name: Backdoor.W32.Rbot
Description: bb.exe is a process registered as a backdoor vulnerability which may be installed for malicious purposes by an attacker allowing access to your computer from remote locations, stealing passwords, Internet banking and personal data. This process is a security risk and should be removed from your system.

Process Name: Backdoor.Rbot.gen
Description: RBot represents the large family of backdoors - hacker's remote access tools. These tools allow access to control the victims' computer remotely by sending specific commands via IRC channels. Also these backdoors can steal data, manipulate data, spread to local networks and to other computers vulnerable to exploits.

Process Name: TrojanProxy.Win32.Bobax.c
Description: This worm is known to exploit Windows LSASS vulnerability, which is a buffer overrun that allows remote code execution and enables an attacker to gain full control of an affected system. It also exploits the Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability present on Windows NT, 2000, and XP Systems.

Process Name: Win32.Winshow.G
Description: This is a trojan that redirects a user's Internet Explorer start page and search URLs. Its main intention is to get more visits to web pages owned by the trojan authors. The trojan executable has been distributed in variable sizes and UPX packed. The trojan consists of a number of different components that are downloaded from various locations during its installation process.

Process Name: divx.exe
Description: If the divx.exe process is on your computer, your computer could be infected with a trojan that goes by the name of Irc.aladinz.g. dr.divx.exe is considered to be a security risk, not only because antivirus programs flag *irc.aladinz.g trojan* as a trojan, but also because other sites consider it a Trojan as well. **irc.aladinz.g trojan** is likely a Trojan and as such, presents a serious vulnerability which should be fixed immediately! Delaying the removal of dr.divx.exe may cause serious harm to your system and will likely cause a number of problems, loss of data, loss of control or leaking private information.

Process Name: instsrv.exe
Description: Finding a program by the name of instsrv.exe running on your pc is usually a sign that your system has potentially been infected with a variant of the remadmin worm. instsrv.exe is considered to be a security risk, not only because antivirus programs flag *remadmin worm* as a virus, but also because a number of users have complained about its performance. Remadmin worm is likely a virus and as such, presents a serious vulnerability which should be fixed immediately! Delaying the removal of instsrv.exe may cause serious harm to your system and will likely cause a number of problems, such as slow performance, loss of data or leaking private information to websites.

In addition, I noted a significant number of suspicious executable files that began running on or about 11/6/2004 and continued through 12/3/2004. All files had similar naming conventions (ie: A0004696.exe, A0009921.exe, A0007346.exe, etc.) I was unable to determine the purpose of these files, however, they appear to be related to one or more of the backdoor Trojans identified on the system.

TYPED EXAMINER'S NAME	ORGANIZATION	
TAMI L. LOEHRS	LAW2000, INC.	
SIGNATURE	DATE	EXHIBIT
	September 19, 2006	

EXAMINATION REPORT

CASE NAME / NUMBER
Bandy adv. State of Arizona
CR2005-014635

The backdoor Trojans are the most significant problems inasmuch as they allow hackers to utilize your computer as a tool for malicious activity which may include downloading or uploading child pornography. Bypassing the normal authentication procedures, hackers gain full access to your computer virtually undetected. In addition, a computer equipped with a high-speed Internet connection through a DSL or cable modem is at greater risk for compromise inasmuch as the computer is "always on" and is more vulnerable to being cracked and exploited. Protection from this type of activity includes various hardware devices and software applications including firewalls, virus protection and intrusion detection systems.

In this case, we know that the computer was connected to the Internet using a high-speed cable modem through Cox Communications.

A firewall is a hardware device or software application that filters information coming through the Internet connection into your computer or network. If an incoming packet of information is flagged by the filters, it is not allowed through. I reviewed the evidence sheets and photographs of the scene and found no evidence of any hardware security devices such as a firewall. I reviewed all installed applications on the system and did not locate any firewall software installed.

Anti-virus software is used to detect and remove viruses, Trojans and worms. The anti-virus software should be running at all times and must be updated with current definition files to maintain effective protection. In addition, scans may be run at any time to detect and remove intrusions. I located the Norton AntiVirus software installed on HDD01. The Version.dat file identified the software as version 10.0.10. In addition, I located virus definition files with the last date of December 14, 2004.

Spyware detection software is similar to anti-virus software except that it detects spyware. Spyware is a generic term for malicious software that is used to gather information about you and the data on your computer. Information typically includes websites visited and personal information that may be used for identity theft. Like the anti-virus software, the spyware software must be updated with current definition files for effective protection. I located SpySweeper installed on HDD01 and located the application in the Startup folder. The readme.txt file identified the software as Version 2. According to the SpysweeperLog.txt file, the software was last run on December 12, 2004. I was unable to determine conclusively the date of the latest definition files.

An intrusion detection system (IDS) inspects all inbound and outbound activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break

TYPED EXAMINER'S NAME	ORGANIZATION	
TAMI L. LOEHRS	LAW2000, INC.	
SIGNATURE	DATE	EXHIBIT
	September 19, 2006	

EXAMINATION REPORT

CASE NAME / NUMBER
Bandy adv. State of Arizona
CR2005-014635

into or compromise a system. I did not locate any intrusion detection software installed on the system.

CONCLUSION

Based on my examination and analysis of the digital evidence in this case (ie: HDD01) I found the system extensively infected with malicious software. While I did note current anti-virus software installed, I can only conclude that it was not functioning properly or had been disabled due to the significant number of viruses, Trojans and worms infecting the system. Of considerable concern are the backdoor Trojans found on the system. With no firewall protection in place, the system was extremely vulnerable to compromise by outside sources such as hackers. Conversely, with no IDS system in place, it would be virtually impossible to determine if, when or by whom the system was compromised. In this regard, it would be impossible to state with certainty which activities were conducted by users within the household and which activities were a result of one of the many malicious software applications and/or outside sources such as hackers.

Further, all activity on this computer was conducted under the default user account "Owner". Computer activity is often associated with a user based on the personal account with which they log on to the computer. With no personal user accounts identified, it is impossible to state with any certainty which user was responsible for which activity.

TYPED EXAMINER'S NAME	ORGANIZATION	
TAMI L. LOEHRS	LAW2000, INC.	
SIGNATURE	DATE	EXHIBIT
	September 19, 2006	