

The Untraceable Criminal

The use of Embedded and Virtual Technologies in Cyber Crime

Tracy Lafeir

IA 325

December 2008

The Untraceable Criminal

The use of Embedded and Virtual Technologies in Cyber Crime

Note: The following is a fictional example on how readily available off the shelf embedded technologies can be used mask cyber criminal activities.

John sits in his grey sedan, laptop resting against the car's console. It is late, and most of the residents of the quiet neighborhood are asleep. Suddenly, John sees police and government cars approach from both sides of the street. A helicopter appears overhead. He quietly flicks a switch mounted in the driver's side door panel. He closes the lid of his now deactivated laptop and prepares to be arrested.

Several months later, forensics examiners continue to pour over the equipment seized from John's car. Everything seized was off the shelf hardware with a few modifications. The authorities, however, could not retrieve any data that they could use for a prosecution. In addition, the access point that was used in the crime ceased to function moments before the police arrived. It is suspected that John and his associates host one of the largest child pornography distribution sites in the country.

Within John's car, investigators discovered a treasure trove of ordinary devices, including a new Dell Inspiron laptop. Oddly enough, the laptop was missing its battery. In addition, the car also held two quad core Dell Precision Workstations, outfitted with 8 gigabytes of RAM.

Investigators had noted that the hard drives were disconnected. They also discovered that each machine now held a PCI IDE RAID card to which four 16 gigabyte Kingston Compact Flash cards were attached. Also, within the car, they discovered three 500 gigabyte Western Digital Netcenter drives, a Linksys WRT 54gl router, a 16 port gigabit Ethernet switch, a 1000 watt power inverter, as well as a Cyber Power rack mount UPS. All the equipment, save for the laptop, was concealed within the vehicle's trunk. The router antennas were replaced with high gain models and placed on the vehicle's roof.

Forensic analysis of the laptop hard disk drive revealed nothing other than a basic Windows XP installation. Save for a single encrypted executable, there was no other additional software installed, Web browsing history, or any other evidence to indicate that the laptop had ever been used. The desktop machine's hard disk was blank, but analysis of the Compact flash cards had only revealed an installation of Windows Server 2003, and a single executable, which appeared to be encrypted. The router, like the one discovered at in the home where the theft of service occurred, no longer functioned.

The Technology

Windows XP embedded – Enhanced Write Filter

Windows XP Embedded is an operating system designed with specific use devices, such as kiosks and ATMs. Windows XP embedded uses a similar kernel codebase as Windows XP Home and Professional, making its included technologies compatible with those operating systems, as well as Windows Server 2003.

Of particular interest, is an XP embedded technology, Enhanced Write Filter (EWF) driver. This driver interrupts writes to any protected drive, instead storing those writes in an overlay. This overlay can be stored on the system drive, the registry, or in memory. EWF needs only a single system driver “EWF.SYS” to function in certain modes. Changes to the overlay require the EWFMgr.exe

There are three types of EWF modes:

Disk mode – EWF stores its overlay on unpartitioned space on writable disk drive. This mode protects the configured volumes, but does not prevent data from being written to the disk. This mode requires additional features from Windows XP embedded.

RAM Mode – EWF stores its overlay in write mode, but requires that the overlay configuration be written to the host disk. This overlay configuration would be clearly visible to forensics analysis tools.

RAM Reg mode – As the only mode compatible with versions of Windows other than XP embedded, is RAM Reg mode. This mode places the EWF information into the registry, further obfuscating it from those who are unaware of the filter’s functionality.

EWF technology can be obtained from the trial version of XP Embedded, located on Microsoft’s website. The files needed are: EWFNTLDR, EWFMgr.EXE, and EWF.SYS. For added security, the EWFMgr.EXE application can be deleted, since it is only needed when modifications to the overlay configuration is made.

Several changes to the operating system need to be made to enable EWF. First, the XP bootloader (NTLDR) must be replaced with EWFNTLDR. The EWF system driver must be placed into the %SystemRoot%\System32\Drivers folder. Next, the registry key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root*, must be given full read/write permission by all users. Once that is complete, EWF enabling entries must be added to the registry.

Once the registry modifications are complete, the machine should be rebooted. EWF is enabled and all changes are discarded at power or reboot. It should be noted, that EWF is only functional while the modified operating system is running. The disk will be writable when other boot methods are used.

Embedded Devices and Linux

Numerous consumer electronic devices on the market today run Linux derived firmware. Thanks to economies of scale, these devices actually contain considerable processing power. Devices such as routers offer open source firmware replacements which add features rivaling that of enterprise class devices.

Linksys WRT-54g router

Depending on the model, The Linksys WRT router contain a CPU capable at running at speeds from 125 MHz CPU to about 240 MHz, with RAM ranging in capacity from 8 megabytes all the way to 32 megabytes. The WRT router contains flash storage ranging from 2 megabytes to about 8 megabytes.

A firmware replacement known as “DD-WRT” was developed for Linksys WRT-54g routers and clones. DD-WRT also allows the router broadcast power be increased from the standard 28mw up to 250mw. In addition, DD-WRT provides Secure Shell (SSH) access to the router. Users of a DD-WRT router can configure the router to execute shell scripts. A determined individual can install a SD card reader in the router, allowing the device to access up to 2 gigabytes of storage for programs and data.

Installing the firmware is simple. First, one must locate the appropriate firmware from DD-WRT.COM’s support matrix. Once the correct BIN is located, a user must navigate to the router’s configuration website and use the embedded upgrade tool to TFTP the BIN to the router. It is also possible to flash the device’s ROM with a firmware using a simple TFTP client.

The Western Digital Netcenter

The Western Digital Netcenter is a Network Attached Storage Device, with capacities ranging from 160 gigabytes to 500 gigabytes. This device contains 32 megabytes of RAM, as well as 16 megs of flash storage. A 10/100mb Ethernet port links the device to the LAN.

The Western Digital Netcenter firmware source was released under GPL, therefore the source code is available from the manufacturer’s website.

For the purpose of this document, gaining root access to a Western Digital Netcenter drive was attempted. Two simple changes were made. These changes involved moving the contents of /ETC/rc.start to a writable location in NVRAM. In addition, /OPT is re-linked to the device's hard disk during the boot sequence.

START SCRIPT

```
echo "root@hash value">/tmp/shadow – changes the root password (non standard)

# vsftp - Starts the embedded FTP server

vsftp &

export LD_LIBRARY_PATH=/lib:/usr/lib:/opt/lib - Relinks OPT to values to stored in NVRAM (non standard)

#/opt/usr/local/mysql/bin/mysqld --user root – Launches the MySQL server (non standard)

/opt/bin/lighttpd/bin/lighttpd -- launches a PHP compliant Webserver (Non standard)

#[C timeout haddisk activ 600 seconds

nvram set initial_disk_spin_down_setting=600

nvram commit

# Last-Power-State – Changes the onboard LED to blue

nvram unset kernel_boot_wait_gpio

nvram commit
```

As proof of concept for this modification, Light HTTPD web server and Mysql Database server were installed. The NAS now hosts a simple database driven website, as well as Telnet and FTP services. Due to the nature of the device's design, the initial modifications must be reapplied every time the device loses power. Otherwise the modifications will no longer function.

Portable Applications

Microsoft has released to its enterprise customers, an application known as AppV. AppV is an Application Virtualization program AppV is used to create applications that run in a 'virtual sandbox' thus not requiring a full installation on the host OS. During the Application Sequencing process, an application installation is analyzed. Once this analysis is complete, AppV presents a fully compiled 'portable' application, ready to run, without any modifications to the host operating system.

Unraveling the Crime

At the beginning of this paper, a hypothetical criminal had created a mobile data center using the outlined technologies. Forensics investigators were unable to locate any evidence of a crime, due to the lack of general knowledge of what can be accomplished when combining these technologies. Because of his knowledge and planning, all it took for John to evade capture was a flick of a simple switch. So John will go unpunished, free to commit his horrendous crimes, and puzzled investigators will continue to pour over.

The Equipment

In order for the crime to occur, John made several modifications to the vehicle. He installed a 1000 watt inverter, which both his laptop and the large UPS in the trunk that powered the rest of the equipment. The switch in the door was wired directly into the inverter. In the trunk, the dual serial ports on the UPS connected to both desktops. In addition, a private network connected to both desktops, ensuring high availability for the applications they ran. The three desktops, Linksys router and three Netcenter drives connected to a 16 port switch. An Ethernet cable also led to John's laptop.

John's Linksys router was running DD-WRT. The router was configured to scan for and lock onto open routers access points. The router then executed Universal Plug and Play (uPNP) commands against the target router, ensuring complete control of the device. John was able to script necessary changes against routers conforming to uPNP standards, thus shaving time off of his startup processes.

John's laptop was configured to use EWF. Removing the battery ensured that memory was cleared the moment the laptop was powered off. John's management applications all ran with AppV, thus ensuring no evidence was left on the hard disk drives. When powering up the laptop, the encrypted executable extracts an encrypted archive located on one of the three Netcenter drives. The application is written to randomly connect to any of the available drives, to ensure the loss of up to two drives do not interrupt his activities.

The desktops found in John's trunk ran Windows 2003 enterprise. EWF was configured on the compact flash drives, so that no traces were left behind for an investigator to find. The compact flash drives were arranged in a RAID 5 array, but not a lot of local storage was needed. The encrypted executable performed several tasks. First, it would immediately establish connection to the three drives. It would then extract a specific encrypted archive to the host machine, and execute several applications inside. This archive contains portable versions of Apache Web Server, as well as the static content located on the website. The Archive also

contained a portable version of TrueCrypt, configured to open several encrypted volumes on one of the NetCenter drives. Lastly, the encrypted executable runs a custom application designed to ensure an active / passive cluster between the two desktops, and monitor for specific signals on the serial port.

The Netcenter drives contained a specific firmware modification that allowed for application installation. John had installed FTP and RSYNC. RSYNC ran every several seconds, ensuring that all content was replicated across each of the three drives. The drives also contained wipe utilities that would corrupt the NVRAM when executed.

The Trapdoor

Because of the nature of John's crimes, an effective way to eliminate all evidence was needed. EWF protected changes from being written to the machines, but much more protection was needed. John had designed the entire system with this need in mind. When the inverter was powered off, the UPS would immediately signal both desktops to execute a series of commands and power off. The first command, a custom executable, was designed to telnet into the three Netcenters, and executes a shell script. The Netcenter's shell script then wiped the NVRAM, and over wrote the sectors of the hard disk which held the initial encrypted archives, as well as the File allocation Tables. The desktops then launched TFTP sessions to the router located in the car, as well as the router located in the home that he was stealing internet access from. The TFTP session then uploaded garbage data to both routers. Once the TFTP upload was complete, the routers rebooted, effectively killing them. The last step of the shutdown process was to trigger a complete power off of the UPS device. The whole process occurred in under a minute.

Conclusion and Further Reading

With the advent of inexpensive embedded devices, and the release of new software never before imagined, scenarios such as the one outlined will unfortunately become more common. It is now important than ever to stay ahead of the criminal, understanding industry trends, and understanding these new technologies before those with less honorable intentions do.

Works Cited

“Enhanced Write Filter.” MSDN: Microsoft Developer Network. 18, October 2006

<[http://msdn.microsoft.com/en-us/library/ms912906\(WinEmbedded.5\).aspx](http://msdn.microsoft.com/en-us/library/ms912906(WinEmbedded.5).aspx)>

“Installing EWF” Granturing. 3, December 2007

<<http://granturing.blogspot.com/2007/12/this-guide-is-based-off-my-original-ewf.html>>

“TrueCrypt – Free Open-Source On-The-Fly Encryption.” 1, December 2008. TrueCrypt Foundation.

2, December 2008 <<http://www.truecrypt.org>>

“Microsoft Application Virtualization” Microsoft Corporation. 23, September 2008.

2, December 2008 <http://www.microsoft.com/systemcenter/appv/default.aspx>

“DD-WRT Wiki” DD-WRT, 4, June 2007

2, December 2008 <http://www.dd-wrt.com/wiki/index.php/Main_Page>