EXAMPLE OF A VIRUS & MALWARE CLEANUP FOR A "WINDOWS" COMPUTER: "FBI PC LOCK" RANSOMWARE

SUMMARY:
Here is an another example of the successful use of Harry Elver's malware cleanup procedure on October 3, 2012.

MALWARE INFECTION

A computer running "Windows Vista Home Premium" with "Service Pack 2" was infected with "FBI PC Lock" ransomware. Whenever the computer was connected to the Internet, a screen that purportedly was from the FBI demanded payment of $200 in return for the computer user's purported online computer crimes:
ATTENTION!

IP: United States
Location: GTS Central Europe

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated – first time) may be considered as conditional in case you pay the fine to the State.

Fines may only be paid within 72 hours after the infringement. As soon as 72 hours elapse, the possibility to pay the fine expires, and a criminal case is initiated against you automatically within the next 72 hours.

To unblock the computer, you must pay the fine through MoneyPak of 100$.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to $4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

When you pay the fine, your PC will get unlocked in 1 to 48 hours after the money is put into the State’s account.

In case an error occurs, you’ll have to send the code by email fine@fbi.gov (Do not forget to specify IP address)
ADDITIONAL INFORMATION

The infected computer had a current copy of "Norton Internet Security" that was provided by Comcast but "Norton Internet Security" was unable to detect, block, and/or expunge the "FBI PC Lock" ransomware.

See
http://www.zimbio.com/Latest+Computer+Threats/articles/SHo2GTw2Iys/FBI+Moneypak+Ransomware+Virus+Sampsonics+Computer
and
http://www.im-infected.com/ransomware/winlocker.html
PHOTOS OF THE INFECTED COMPUTER

ATTENTION!

IP: 98.225.77.226
Location: United States, Tucson
IP6: Comcast Cable

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoophilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to $100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated – first time) may be considered as conditional in case you pay the fine to the State.
hs specified below.

Video, Music, Software) and illegally
Article 1, Section 8, Clause 8, also
States of America.

for a fine of two to five hundred
years.

ic content (Child Porno/Zoophilia and
ed States of America. Article 202 of
our to twelve years.

t knowledge or consent, your PC may
 neglectful Use of Personal Computer.
$100,000 and/or a deprivation of
States of America of May 28, 2011,
be considered as conditional in case

Where I can buy MoneyPak?

*
May 28, 2011, conditional in case 4 hours elapse, the 5 automatically

MoneyPak

Pay MoneyPak

Where I can buy MoneyPak?

7 [Image] CVS/pharmacy
RITE [Image]
AID PHARMACY

Walmart [Image]

K [Image] kmart

Walgreens

FRAUD ALERT: Use your MoneyPak number only with businesses listed at MoneyPak and United States Department of Justice. If anyone else asks for your MoneyPak number, it's probably a scam. If a criminal gets your money, Green Dot is not responsible to pay you back.

*
Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011, this law infringement (if it is not repeated – first time) may be considered as conditional in case you pay the fine to the State.

Fines may only be paid within 72 hours after the infringement. As soon as 72 hours elapse, the possibility to pay the fine expires, and a criminal case is initiated against you automatically within the next 72 hours!

To unblock the computer, you must pay the fine through MoneyPak of 200$.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of up to $4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak.

When you pay the fine, your PC will get unlocked in 1 to 48 hours after the money is put into the State’s account.

In case an error occurs, you’ll have to send the code by email fine@fbi.gov (Do not forget to specify IP address)

FBI.gov is an official site of the U.S. Federal Government, U.S. Department
We meticulously followed Harry Elver’s cleanup procedure that is described at 
http://aztcs.org/meeting_notes/winhardsig/malwarcleanup/malwarecleanup.htm
and the computer was returned to full functionality.

The actual procedure that expunged the malware was as follows:

Step 1:
Download the free version of "MalwareBytes", using another computer.

Step 2: Burn the installation file for "MalwareBytes" onto a CD-R disc.

Step 3:
Boot up the infected computer in "Safe Mode".

Step 4:
Insert the CD-R disc.

Step 5:
Double-click on the installation file for "MalwareBytes".

Step 6:
Remove the CD-R disc.

Step 7:
Run "MalwareBytes" to perform a "Full Scan" of the computer. "MalwareBytes" found 12 items of malware inside the infected computer.
Step 8:
When the scan is complete, have "MalwareBytes" delete all detected malware.

Step 9:
Reboot the computer.