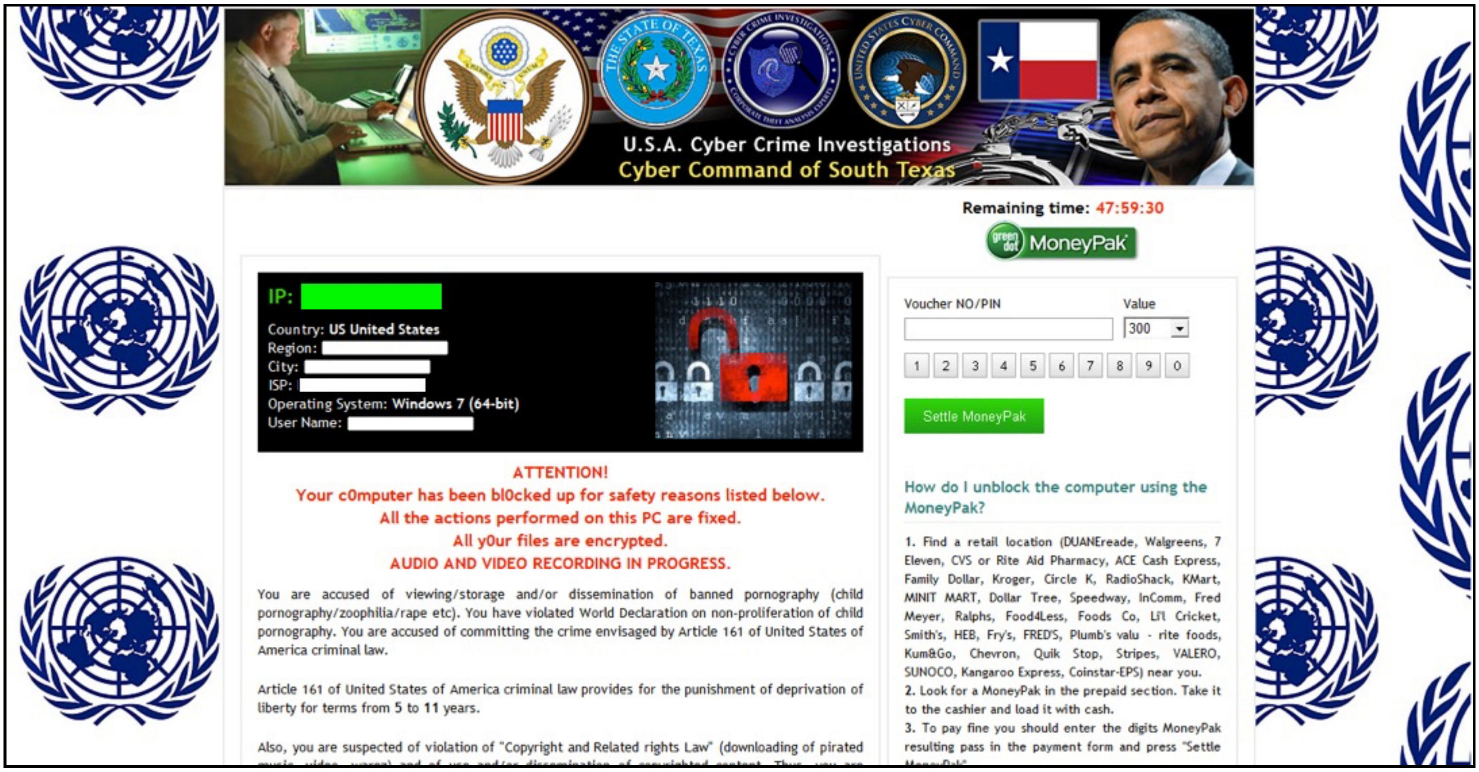
2014-12-12 - RANSOMWARE INFECTION AFTER NUCLEAR EK FROM 128.199.52.211 - YQUESRERMAN.GA

ASSOCIATED FILES:

- ZIP of the pcap: 2014-12-12-Nuclear-EK-traffic.pcap.zip
- ZIP of the malware: 2014-12-12-Nuclear-EK-malware.zip

NOTES:

- I'm finding more Nuclear EK, now that it's been updated and the traffic patterns have changed.
- See my 2014-12-10 blog entry for details on Nuclear EK's new traffic patterns (payload being XOR-ed, etc).
- Unlike the 2014-12-10 blog entry on Nuclear EK, this one was not caused by Operation Windigo, so it has a different payload.
- The malware didn't do anything when I infected the VM earlier in the day.
- I ran the malware on another VM later that evening and got ransomware (see the image below).


U.S.A. Cyber Crime Investigations
Cyber Command of South Texas

Remaining time: 47:59:30

MoneyPak

IP: [redacted]

Country: US United States
Region: [redacted]
City: [redacted]
ISP: [redacted]
Operating System: Windows 7 (64-bit)
User Name: [redacted]

ATTENTION!
Your c0mputer has been bl0cked up for safety reasons listed below.
All the actions performed on this PC are fixed.
All y0ur files are encrypted.
AUDIO AND VIDEO RECORDING IN PROGRESS.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, warez) and of use and/or dissemination of copyrighted content. Thus, you are

Voucher NO/PIN:
Value: 300

1 2 3 4 5 6 7 8 9 0

Settle MoneyPak

How do I unblock the computer using the MoneyPak?

1. Find a retail location (DUANEreade, Walgreens, 7 Eleven, CVS or Rite Aid Pharmacy, ACE Cash Express, Family Dollar, Kroger, Circle K, RadioShack, KMart, MINIT MART, Dollar Tree, Speedway, InComm, Fred Meyer, Ralphs, Food4Less, Foods Co, Li'l Cricket, Smith's, HEB, Fry's, FRED'S, Plumb's valu - rite foods, Kum&Go, Chevron, Quik Stop, Stripes, VALERO, SUNOCO, Kangaroo Express, Coinstar-EPS) near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash.
3. To pay fine you should enter the digits MoneyPak resulting pass in the payment form and press "Settle MoneyPak".

CHAIN OF EVENTS

ASSOCIATED DOMAINS:

- 128.199.52.211 - **yquesrerman.ga** - Nuclear EK
- 176.9.245.80 - **bloghersked.com** - post-infection traffic

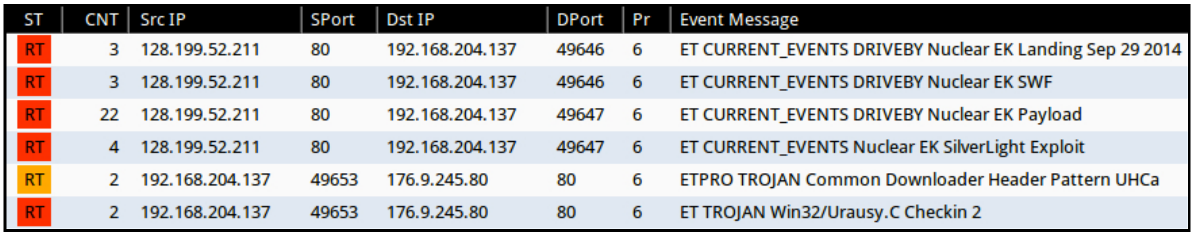
Nuclear EK:

- 2014-12-12 21:43:07 UTC - yquesrerman.ga - GET /AkNVHkgGT0Q.html
- 2014-12-12 21:43:09 UTC - yquesrerman.ga - GET /AwoVG1ADAw4OUhlVDlRTBQoHRUJTXVYOUVYaAwtGXFRVVFxXVwBOVRtA
- 2014-12-12 21:43:11 UTC - yquesrerman.ga - GET /ABsJAkhWAkcLGlEaQRlWAAMLQ0BWUF5CGVMFHAJPQ0hXVkBLVQQGT0IOIhMIIw4ffQ
- 2014-12-12 21:43:15 UTC - yquesrerman.ga - GET /ABsJAkhWAkcLGlEaQRlWAAMLQ0BWUF5CGVMFHAJPQ0hXVkBLVQQGT0IOCB0uGQEzYlVPRQ
- 2014-12-12 21:43:16 UTC - yquesrerman.ga - GET /AwoVG1ADAw4OUhlVDlRTBQoHRUJTXVYOUVYaAwtGXFRVVFxXVwBOQB4eEAAU
- 2014-12-12 21:43:17 UTC - yquesrerman.ga - GET /ABsJAkhWAkcLGlEaQRlWAAMLQ0BWUF5CGVMFHAJPQ0hXVkBLVQQGT0AOIhMIIw4ffQ
- 2014-12-12 21:43:21 UTC - yquesrerman.ga - GET /ABsJAkhWAkcLGlEaQRlWAAMLQ0BWUF5CGVMFHAJPQ0hXVkBLVQQGT0AOCB0uGQEzYlVPRQ
- 2014-12-12 21:43:22 UTC - yquesrerman.ga - GET /ABsJAkhWAkcLGlEaQRlWAAMLQ0BWUF5CGVMFHAJPQ0hXVkBLVQQGT08OIhMIIw4ffQ
- 2014-12-12 21:43:25 UTC - yquesrerman.ga - GET /ABsJAkhWAkcLGlEaQRlWAAMLQ0BWUF5CGVMFHAJPQ0hXVkBLVQQGT08OCB0uGQEzYlVPRQ

POST-INFECTION TRAFFIC:

- 2014-12-12 21:44:23 UTC - bloghersked.com - GET /mf_llksxjSOQYxu5lzLdigricqvz2vcvt_jzifnsuoYbufEqAvPhOEip2ntpo3tzjz_yxhr_yhwg_zkbHgSqGyz1QBzxPWCvDZppsmufIfatBFvshc1QvAsVZ.html
- 2014-12-12 21:44:36 UTC - bloghersked.com - GET /vz_VCvt2jz0iFnSuoYbufVeLulGCbPatHjw9prneWHtwzl7SAsqvcdm9HOin6pcJWwq1gn0lj4lmoe-avDANNtavvas2yxsc_jnzx_bhdhrqzu9gfcb6hYIeHoypfx.html

SNORT EVENTS



ST	CNT	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	3	128.199.52.211	80	192.168.204.137	49646	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Landing Sep 29 2014
RT	3	128.199.52.211	80	192.168.204.137	49646	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK SWF
RT	22	128.199.52.211	80	192.168.204.137	49647	6	ET CURRENT_EVENTS DRIVEBY Nuclear EK Payload
RT	4	128.199.52.211	80	192.168.204.137	49647	6	ET CURRENT_EVENTS Nuclear EK SilverLight Exploit
RT	2	192.168.204.137	49653	176.9.245.80	80	6	ETPRO TROJAN Common Downloader Header Pattern UHCa
RT	2	192.168.204.137	49653	176.9.245.80	80	6	ET TROJAN Win32/Urausy.C Checkin 2

Emerging Threats and ETPRO rulesets from Sguil on Security Onion using Suricata (without ET POLICY or ET INFO events):

- 128.199.52.211:80 - 192.168.204.137:49646 - ET CURRENT_EVENTS DRIVEBY Nuclear EK Landing Sep 29 2014 (sid:2019315)
- 128.199.52.211:80 - 192.168.204.137:49646 - ET CURRENT_EVENTS DRIVEBY Nuclear EK SWF (sid:2019845)
- 128.199.52.211:80 - 192.168.204.137:49647 - ET CURRENT_EVENTS Nuclear EK SilverLight Exploit (sid:2019917)
- 128.199.52.211:80 - 192.168.204.137:49647 - ET CURRENT_EVENTS DRIVEBY Nuclear EK Payload (sid:2019873)
- 92.168.204.137:49653 - 176.9.245.80:80 - ETPRO TROJAN Common Downloader Header Pattern UHCa (sid:2803270)
- 92.168.204.137:49653 - 176.9.245.80:80 - ET TROJAN Win32/Urausy.C Checkin 2 (sid:2016567)

Sourcefire VRT ruleset from Snort 2.9.7.0 on Debian 7.6:

- 128.199.52.211:80 - 192.168.204.137:49646 - [1:32359:1] FILE-FLASH Adobe Flash Player worker shared object user-after-free attempt

PRELIMINARY MALWARE ANALYSIS

FLASH EXPLOIT:

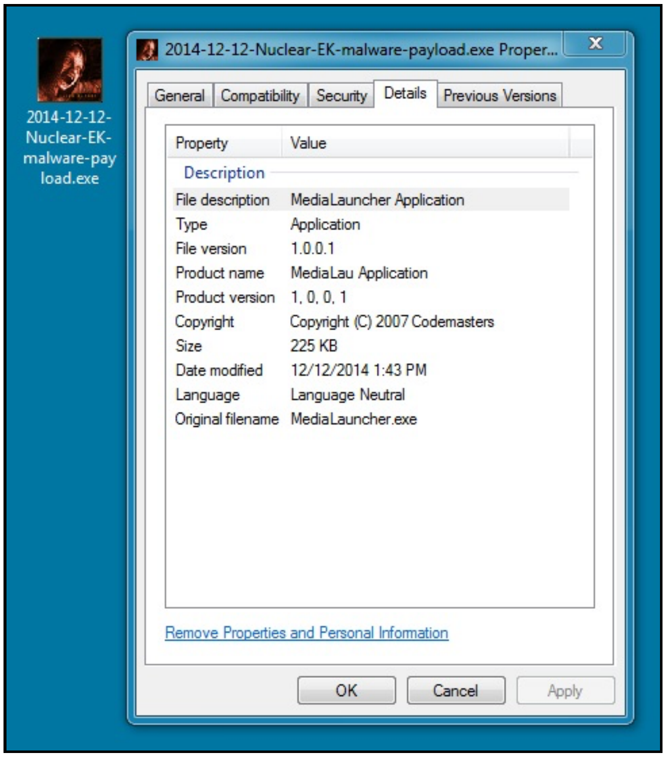
File name: **2014-12-12-Nuclear-EK-flash-exploit.swf**
File size: 21.8 KB (22361 bytes)
MD5 hash: 9b3ad66a2a61e8760602d98b537b7734
Detection ratio: 0 / 56
First submission: 2014-12-13 01:24:10 UTC
VirusTotal link: https://www.virustotal.com/en/file/00730977f6a6c1e8a7221a11785e525cdc2a39638b869d77da9b828e4643f839/analysis/

SILVERLIGHT EXPLOIT:

File name: **2014-12-12-Nuclear-EK-silverlight-exploit.xap** (same as the one from 2014-12-10)
File size: 6.8 KB (6924 bytes)
MD5 hash: 87d140b1b68cbe2b46a4a355fbd87a09
Detection ratio: 10 / 55
First submission: 2014-12-10 18:31:15 UTC
VirusTotal link: https://www.virustotal.com/en/file/a0b5876419025568915bfea24d22163169f4b3634935edafd998c26d57900055/analysis/

MALWARE PAYLOAD:

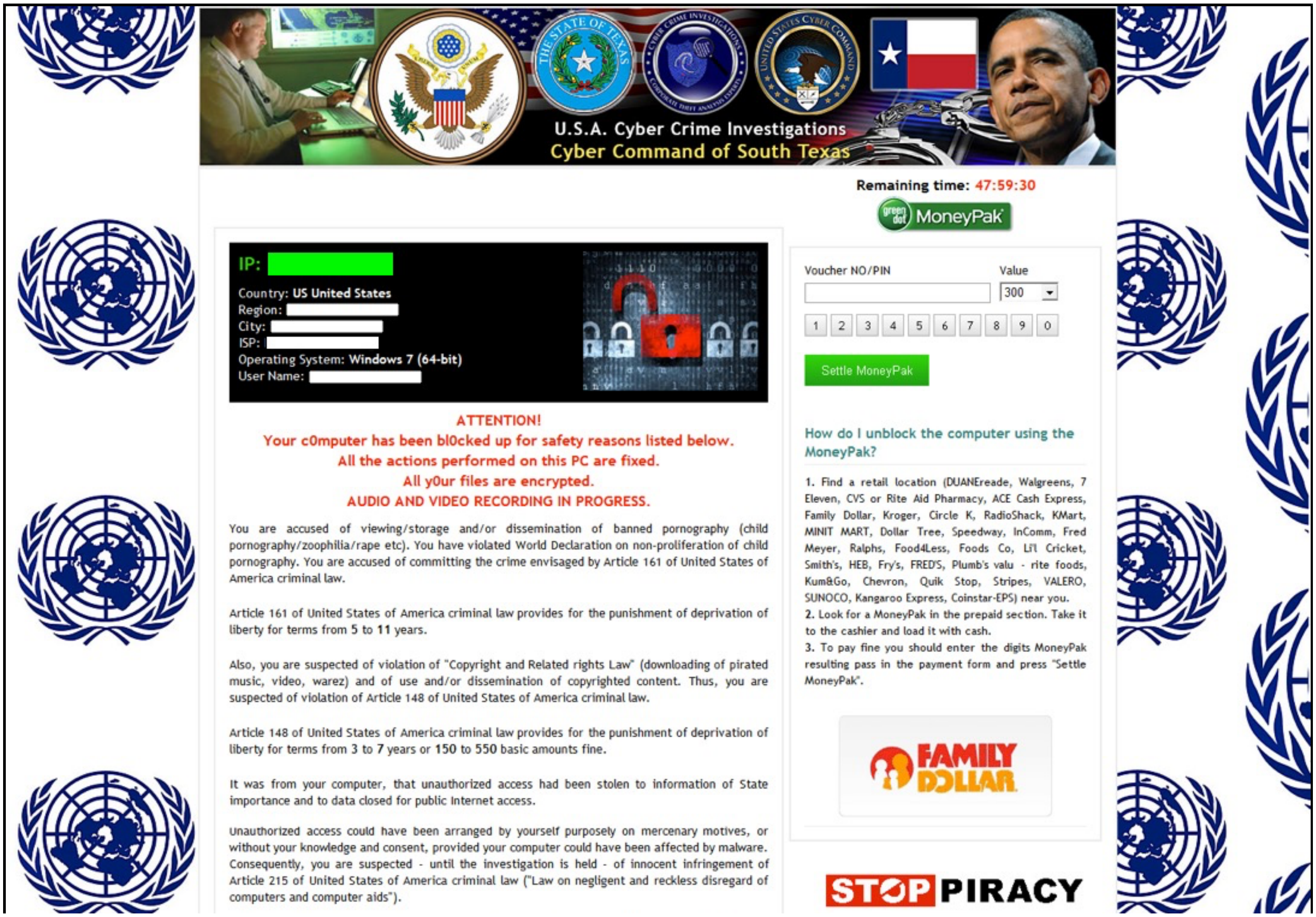
File name: **2014-12-12-Nuclear-EK-malware-payload.exe**
File size: 225.0 KB (230400 bytes)
MD5 hash: bf230af91ac92924a745f42021abbba0
Detection ratio: 7 / 53
First submission: 2014-12-13 01:24:44 UTC
VirusTotal link: https://www.virustotal.com/en/file/18cb84c0d9c87fa5ed74da826270bd416aa039795b731fc91e700b03b7738610/analysis/
Malwr link: https://malwr.com/analysis/M2QxMWFiZTc5YjNkNGI0MjkwY2RhMGViMjNkOTdmOTA/


2014-12-12-Nuclear-EK-malware-payload.exe
2014-12-12-Nuclear-EK-malware-payload.exe Proper...
General
Compatibility
Security
Details
Previous Versions
Remove Properties and Personal Information
OK
Cancel
Apply

Property	Value
Description	
File description	MediaLauncher Application
Type	Application
File version	1.0.0.1
Product name	MediaLau Application
Product version	1, 0, 0, 1
Copyright	Copyright (C) 2007 Codemasters
Size	225 KB
Date modified	12/12/2014 1:43 PM
Language	Language Neutral
Original filename	MediaLauncher.exe

SCREENSHOTS

Full view of the ransomware screen from the infected VM:



U.S.A. Cyber Crime Investigations
Cyber Command of South Texas

Remaining time: 47:59:30

IP: [redacted]

Country: US United States
Region: [redacted]
City: [redacted]
ISP: [redacted]
Operating System: Windows 7 (64-bit)
User Name: [redacted]

ATTENTION!
Your c0mputer has been bl0cked up for safety reasons listed below.
All the actions performed on this PC are fixed.
All y0ur files are encrypted.
AUDIO AND VIDEO RECORDING IN PROGRESS.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/rape etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of United States of America criminal law.

Article 161 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, warez) and of use and/or dissemination of copyrighted content. Thus, you are suspected of violation of Article 148 of United States of America criminal law.

Article 148 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to 550 basic amounts fine.

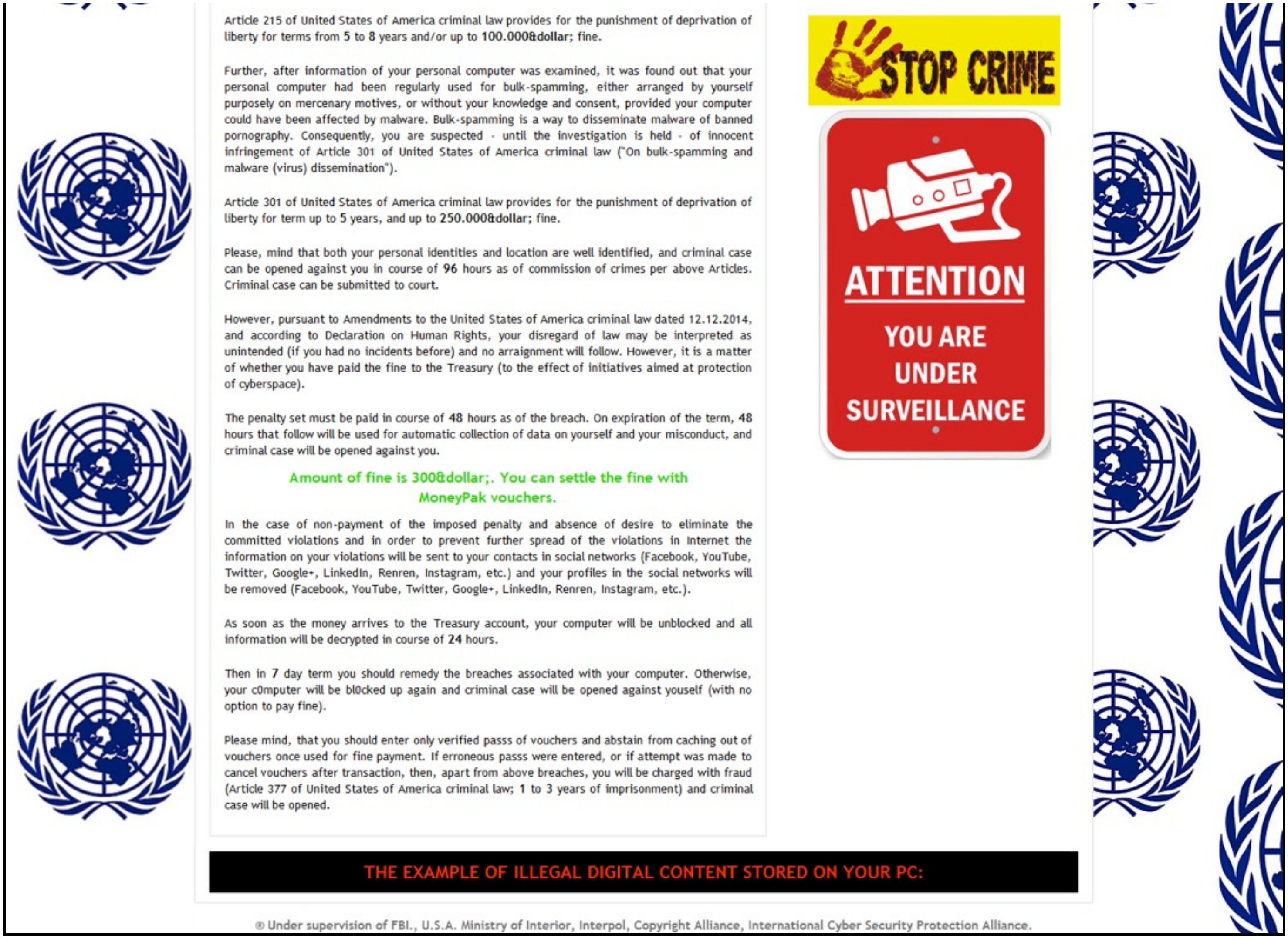
It was from your computer, that unauthorized access had been stolen to information of State importance and to data closed for public Internet access.

Unauthorized access could have been arranged by yourself purposely on mercenary motives, or without your knowledge and consent, provided your computer could have been affected by malware. Consequently, you are suspected - until the investigation is held - of innocent infringement of Article 215 of United States of America criminal law ("Law on negligent and reckless disregard of computers and computer aids").

Voucher NO/PIN | Value: 300

How do I unblock the computer using the MoneyPak?

1. Find a retail location (DUANEreade, Walgreens, 7 Eleven, CVS or Rite Aid Pharmacy, ACE Cash Express, Family Dollar, Kroger, Circle K, RadioShack, KMart, MINIT MART, Dollar Tree, Speedway, InComm, Fred Meyer, Ralphs, Food4Less, Foods Co, Li'l Cricket, Smith's, HEB, Fry's, FRED'S, Plumb's valu - rite foods, Kum&Go, Chevron, Quik Stop, Stripes, VALERO, SUNOCO, Kangaroo Express, Coinstar-EPS) near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash.
3. To pay fine you should enter the digits MoneyPak resulting pass in the payment form and press "Settle MoneyPak".



Article 215 of United States of America criminal law provides for the punishment of deprivation of liberty for terms from **5** to **8** years and/or up to **100.000&dollar;** fine.

Further, after information of your personal computer was examined, it was found out that your personal computer had been regularly used for bulk-spamming, either arranged by yourself purposely on mercenary motives, or without your knowledge and consent, provided your computer could have been affected by malware. Bulk-spamming is a way to disseminate malware of banned pornography. Consequently, you are suspected - until the investigation is held - of innocent infringement of Article 301 of United States of America criminal law ("On bulk-spamming and malware (virus) dissemination").

Article 301 of United States of America criminal law provides for the punishment of deprivation of liberty for term up to **5** years, and up to **250.000&dollar;** fine.

Please, mind that both your personal identities and location are well identified, and criminal case can be opened against you in course of **96** hours as of commission of crimes per above Articles. Criminal case can be submitted to court.

However, pursuant to Amendments to the United States of America criminal law dated 12.12.2014, and according to Declaration on Human Rights, your disregard of law may be interpreted as unintended (if you had no incidents before) and no arraignment will follow. However, it is a matter of whether you have paid the fine to the Treasury (to the effect of initiatives aimed at protection of cyberspace).

The penalty set must be paid in course of **48** hours as of the breach. On expiration of the term, **48** hours that follow will be used for automatic collection of data on yourself and your misconduct, and criminal case will be opened against you.

Amount of fine is 300&dollar;. You can settle the fine with MoneyPak vouchers.

In the case of non-payment of the imposed penalty and absence of desire to eliminate the committed violations and in order to prevent further spread of the violations in Internet the information on your violations will be sent to your contacts in social networks (Facebook, YouTube, Twitter, Google+, LinkedIn, Renren, Instagram, etc.) and your profiles in the social networks will be removed (Facebook, YouTube, Twitter, Google+, LinkedIn, Renren, Instagram, etc.).

As soon as the money arrives to the Treasury account, your computer will be unblocked and all information will be decrypted in course of **24** hours.

Then in **7** day term you should remedy the breaches associated with your computer. Otherwise, your c0mputer will be bl0cked up again and criminal case will be opened against youself (with no option to pay fine).

Please mind, that you should enter only verified passs of vouchers and abstain from caching out of vouchers once used for fine payment. If erroneous passs were entered, or if attempt was made to cancel vouchers after transaction, then, apart from above breaches, you will be charged with fraud (Article 377 of United States of America criminal law; **1** to **3** years of imprisonment) and criminal case will be opened.

THE EXAMPLE OF ILLEGAL DIGITAL CONTENT STORED ON YOUR PC:

® Under supervision of FBI., U.S.A. Ministry of Interior, Interpol, Copyright Alliance, International Cyber Security Protection Alliance.

FINAL NOTES

Once again, here are the associated files:

- ZIP of the pcap: 2014-12-12-Nuclear-EK-traffic.pcap.zip
- ZIP of the malware: 2014-12-12-Nuclear-EK-malware.zip

ZIP files are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

Click here to return to the main page.