

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

Date: 06/09/2014

Date UPDATED: 6/12/2014

Date UPDATED: 6/19/2014

Date UPDATED: 10/8/2014

Subject: CryptoWall Indicators

CIS has seen an increase in CryptoWall malware infections. CryptoWall is ransomware that seeks out and encrypts documents on the infected machine and any connected shares or drives. The encrypted files are held ransom for a fee. If the fee is not paid within a specific timeframe, the fee will be doubled. If it is still not paid, the encrypted files will be deleted. Decryption is only feasibly possible given the purchase of the key. However, open source intelligence suggests paying the fee does not always result in the restoration of files.

CryptoWall malware is distributed through spam emails, malicious advertisements on legitimate websites, and as fake updates for applications such as Adobe Reader, Adobe Flash, and Java.

It should be noted that once the victim is infected, the CryptoWall malware might not be downloaded immediately. It has been reported that CryptoWall has been downloaded as long as twenty-four hours following the initial infection. Because of this, it is important that infected systems be identified as quickly as possible and remediated immediately.

JUNE 19 UPDATE: CIS received information from a trusted third party that the IP range 146.185.220.0/23 is primarily owned and operated by criminal groups. We have also been informed that this range contains a high number of Ransomware domains hosted on it. We recommend entities to consider blocking traffic to/from 146.185.220.0/23 at their network perimeter.

Please note that we will issue updates to the indicators below as they become available.

OCTOBER 8 – UPDATE:

Please see the following updated domain indicators:

babyslutsnil.com

broserposter.com

craspatsp.com

crunkthatme.com

crynigermike.com

dancewithmeseniorita.com

dominicanajoker.com

dominikanabestplace.com

donotshotnigers.com

gitlerluvua.com

gretableta.com

hungarymethis.com

indeedlinkme.com

kaikialexus.com

khalisimilisi.com

likeyoudominicana.com

maskaradshowdominicana.com

milimalipali.com

newsbrontima.com

nihnihnih.com

nofbiatdominicana.com

obamawantwar.com

poroshenkogitler.com

qoweiuwea.com

slipwasher.com

suspendedwar.com

swinpintin.com

terrymerry.com

ugotkey.com

usaalwayswar.com

vivatsaultppc.com

wawamediana.com

yaroshwelcome.com

yoyosasa.com

JUNE 19 - UPDATED IP Indicators:

146.185.220.0/23

Domain Indicators:

yoyosasa.com

wawamediana.com

qoweiuwea.com

khalisimilisi.com

dominikanabestplace.com

nofbiatdominicana.com

dominicanajoker.com

likeyoudominicana.com

newsbrontima.com

yaroshwelcome.com

Domain Indicators:

- F7fc2938.pw

Primerollessando.shoe-uk.com

Statcounter.me

602ef0b0.pw

Defie-guret.com

Newsbrontima.com

Intendissequ.poolresurfacingaz.info

Niceshinesirius.pw

1044043.pw

1729c026.pw

Sample Email Indicators:

INCOMING FAX REPORT: Remote ID: <{3 digits}-{3 digits}-{3 digits}>

Fax Message at <yyyy-mm-dd hh:mi:ss EST boundary="-----{23 digits}"

UPS Exception Notification, Tracking Number <tracking number>

ex. INCOMING FAX REPORT: Remote ID: 385-567-7335

ex. Message at 2014-05-06 08:11:55 EST boundary="-----
05020600703040205040303"

ex. UPS Exception Notification, Tracking Number 1Z522A9A6892487822

Sample Email Sender Name <Sender Email Address>:

Incoming Fax

Fax Message

UPS Quantum View <auto-notify@ups.com>

Registry Indicators:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Image File
Execution Options\<random>.exe "Debugger" = 'svchost.exe'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CryptoWall
I Decrypter

HKEY_LOCAL_MACHINE\SOFTWARE\CryptoWall Decrypter

Other Registry Changes Made by CryptoWall:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings
"WarnOnHTTPSToHTTPRedirect" = '0'

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
"WarnOnHTTPSToHTTPRedirect" = '0'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
"WarnOnHTTPSToHTTPRedirect" = '0'

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore
"DisableSR" = '1'

File System Indicators:

DECRYPT_INSTRUCTION.txt

DECRYPT_INSTRUCTION.html

DECRYPT_INSTRUCTION.url

%UserProfile%\Application Data\Microsoft\[random].exe

%Documents and Settings%\All Users\Start Menu\Programs\CryptoWall Decrypter

%Documents and Settings%\All Users\Application Data\CryptoWall Decrypter

%Program Files%\CryptoWall Decrypter

Recommendations:

The following actions should be taken:

Since the emails are originating from spoofed email accounts, educate your users on checking the senders of the e-mails and verify the legitimacy of the sender

Block traffic to above domains at your network perimeter devices

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources

Remind users to be cautious when clicking on links in emails coming from trusted sources

Remind users not to download suspicious or unauthorized programs

Ensure anti-virus is installed and definitions are up to date

If infected with CryptoWall, remediate the infection via antivirus. Following the remediation, restore any encrypted files from backup or system restore points and volume shadow copies.

JUNE 19 - UPDATED RECOMMENDATIONS:

Block traffic to/from 146.185.220.0/23 at your network perimeter.

References:

<http://www.securityweek.com/rig-exploit-kit-used-deliver-cryptowall-ransomware>

<http://www.enigmasoftware.com/cryptowallransomware-removal/>

<http://www.malwareexperts.com/cryptowall-removal-guide-solved/>