## Today's Ransomware

Jul. 18, 2016

1. I've received a ransomware today.

## - jsshim\_DF391.zip =>account\_report b1a.wsf - Locky(zepto)

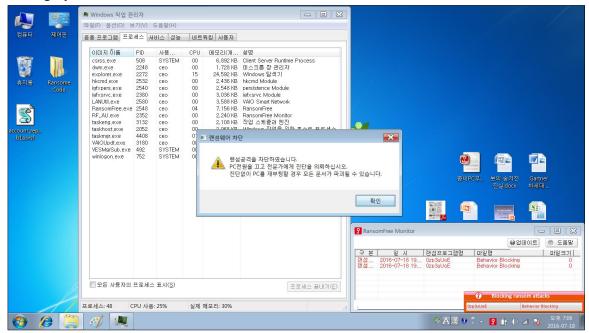
보낸 사람:	Lakisha Goodman [Goodman,10555@airtelbroadband,in]	보낸 날짜:	2016-07-18 (뭘)	오후 <del>6</del> :05
받는 사람:	jsshim@truecut.co.kr			
참조:				
제목:	bank account report			
⊠ 메시지	i jsshim_DF391.zip (8 KB)			
				-
How are	e things?			
Thank you very much for responding my email in a very short time. Attached is the bank account				
report. I	Please look at it again and see if you have any disapproval.			
				=
Yours f	faithfully,			
	a Goodman			
	h Youth Council			
Phone:	+1 (609) 903-30-23, Fax: +1 (609) 903-30-26			•

## 2. Victim under attack

## - Process : C:\U00f8 login account\U00f8 AppDataU02alU0E.exe

<pre>!!! IMPORTANT INFORMATION !!!! !!! IMPORTANT INFORMATION !!!! !!! IMPORTANT INFORMATION !!!! !!! IMPORTANT INFORMATION !!!! !!!! IMPORTANT INFORMATION !!!! !!!! IMPORTANT INFORMATION !!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!</pre>	аня жа андар		
More Grifformation about the RSA and AES can be found here: If the view wikipedia org/wiki/RSA_(cryptosystem) in the view org/org/org/org/org/org/org/org/org/org/	III IMPORTANT INFORMATION III		
<pre>interplate in the address bar: mphtadhci5mrdlju.onion/0E0E220E3BA07937 if plow the instructions on the site. if your personal identification ID: 0E0E220E3BA07937 if your personal identification ID: 0E0E20E3BA07937 if your personal identification ID: 0E0E20E3BA07937 if your personal identific</pre>	All of your files, are encrypted with RSA-2048 and AES-128 ciphers. Moreomformation about the RSA and AES can be found here:		
De vour prive key follow one of the links: 1			
<ul> <li>1. p://tadSmrdlju.tor2web.org/0E0E220E3BA07937</li> <li>1. p://tadSmrdlju.onion.to/0E0E220E3BA07937</li> <li>1. Jownload and install Tor Browser: https://www.torproject.org/download/download-easy.html</li> <li>2. After a successful installation, run the browser and wait for initialization.</li> <li>3. Type in the address bar: mphtadhci5mrdlju.onion/0E0E220E3BA07937</li> <li>4. Follow the instructions on the site.</li> <li>11. Your personal identification ID: 0E0E220E3BA07937 !!!</li> </ul>	De a weight and generalized of your files is only possible with the private key and decrypt program, wi	hich is on our secret ser	/er.
<ol> <li>Download and install Tor Browser: https://www.torproject.org/download/download-easy.html</li> <li>After a successful installation, run the browser and wait for initialization.</li> <li>Type in the address bar: mphtadhci5mrdlju.onion/0E0E220E3BA07937</li> <li>Follow the instructions on the site.</li> <li>Your personal identification ID: 0E0E220E3BA07937 !!!</li> <li>**+-=++~=.*_~\$+=</li> </ol>	🕗 1. p:// 🔤 tac 5mrdlju.tor2web.org/0E0E220E3BA07937		
**+-=`++~=.*_~\$+=	<ol> <li>Download and install Tor Browser: https://www.torproject.org/download/download/2. After a successful installation, run the browser and wait for initialization.</li> <li>Type in the address bar: mphtadhci5mrdlju.onion/0E0E220E3BA07937</li> </ol>	oad-easy.html	
🚱 🔏 🚆 🦪			
	📀 🧭 🗒 🛷	参A漢 ♥ ݨ ▲ 許 心 副 №	오후 7:11 2016-07-1

3. Blocking by RansomFree<sup>®</sup>



RansomFree<sup>®</sup> is blocking in real-time until the unknown ransomware.