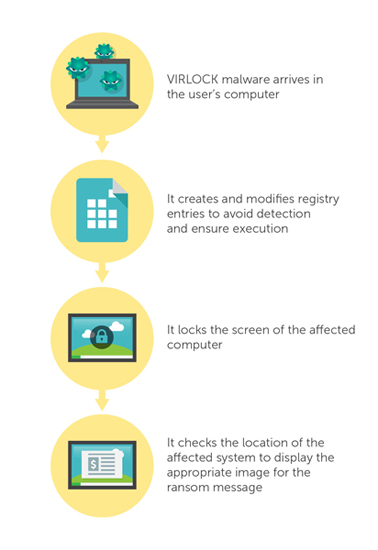
**Polymorphic viruses** are complex file infectors that can create modified versions of itself to avoid detection yet retain the same basic routines after every infection. To vary their physical file makeup during each infection, polymorphic viruses encrypt their codes and use different encryption keys every time.  
  
Polymorphic viruses rely on mutation engines to alter their decryption routines every time they infect a machine. This way, traditional security solutions may not easily catch them because they do not use a static, unchanging code. The use of complex mutation engines that generate billions of decryption routines make them even more difficult to detect.  
  
Polymorphic viruses are usually distributed via spam, infected sites, or through the use of other malware. URSNIF, VIRLOCK, VOBFUS, and BAGLE or UPolyX are some of the most notorious polymorphic viruses in existence. When combined with other malicious routines, polymorphic viruses pose even greater risk to its victims. In March 2015, researchers found that [VIRLOCK](http://blog.trendmicro.com/trendlabs-security-intelligence/virlock-combines-file-infection-and-ransomware/) evolved to include ransomware routines, making it a challenge to detect and remove.

Ransomware has become one of the biggest problems for end users are as of late. In the past months alone, we have reported on several variants of both ransomware and crypto-ransomware, each with their own “unique” routines. We recently came across one malware family, detected as PE\_VIRLOCK, as that not only locks the computer screen but also infects files—a first for ransomware.

**Ransomware Routine**

VIRLOCK variants may arrive bundled with other malware in infected computers. We have even seen [one VIRLOCK variant](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/PE_VIRLOCK.F-O) in the [CARBANAK/ANUNAK targeted attack campaign](http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/3142/carbanak-targeted-attack-campaign-hits-banks-and-financial-institutions).

  
*Figure 1. VIRLOCK infection diagram*

Once inside the computer, VIRLOCK creates and modifies registry entries to avoid detection and ensure execution. It then locks the screen of the affected computer, disabling explorer.exe and preventing the use of taskmgr.exe. Meanwhile, it also checks the location of the affected system to display the appropriate image for the ransom message.

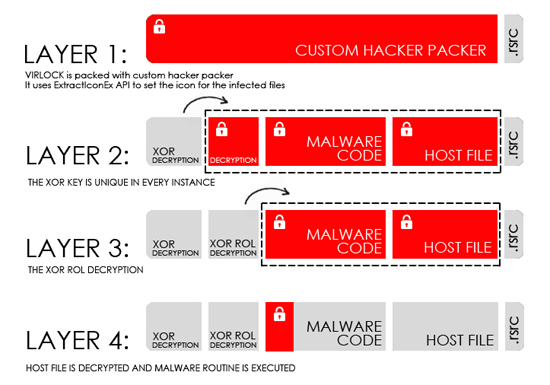
  
*Figure 2. Sample ransom message*

**Infection Routine**

As mentioned, VIRLOCK also has file-infecting routines. Once in the computer, PE\_VIRLOCK checks for specific file types, including the following:

* Executable files (\*.exe)
* Common Document files (\*.doc, \*.xls, \*.pdf, \*.ppt, \*.mdb)
* Archive files (\*.zip, \*.rar)
* Audio/Video files (\*.mp3, \*.mpg, \*.wma)
* Image files (\*.png, \*.gif, \*.bmp, \*.jpg, \*.jpeg, \*.psd)
* Certificate files (\*.p12, \*.cer, \*.crt, \*.p7b, \*.pfx, \*.pem)

Once the malware finds its targeted files, it then encrypts the host file and embeds it in the malware body. It will also add a .RSRC section to the infected file. The .RSRC section includes the resources used by the executable that are not considered part of the executable, such as icons, images, menus, and strings. VIRLOCK uses that section to store the resources of the host file. When the infected host file contains an icon similar to the original icon of the host file, it can trick unsuspecting users into executing the infected files.

  
*Figure 3. A detailed representation of the levels of encryption found in infected files*

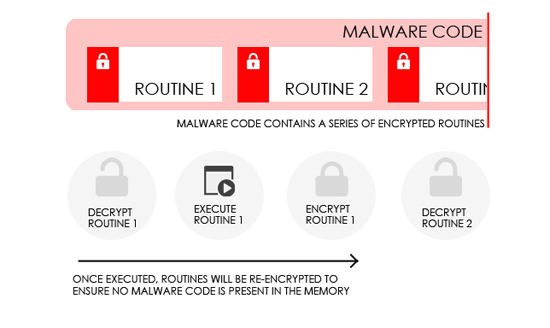
Upon execution, the infected file will drop a decrypted host file on the same directory where it was executed. The malware will then execute the decrypted host file, to make the user think that no suspicious activity is happening even if the malware is running silently in the background.

The malware author programmed the mother file just like the logic of infected files. It uses a dummy file (garbage) for it to drop and execute like the infected file’s routine. The author may have used a dummy file for two reasons: 1) code recycling, and 2) polymorphism—since every instance is unique.

**Evasion Tactics**

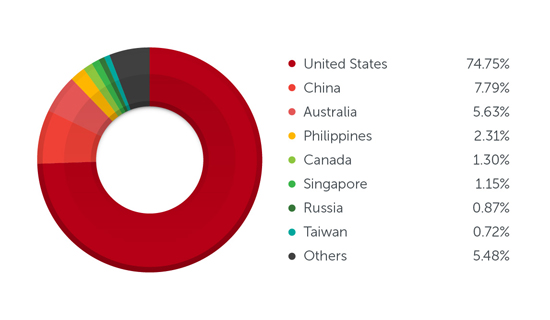
Our analysis shows that VIRLOCK is polymorphic. The malware was packed with custom hacker packer that uses randomized API calls. This malware continuously changes the hacker packer that it uses to avoid detection. This makes it harder to for security researchers and products to detect as the code changes each times it runs.

VIRLOCK encrypts the host file to make it more difficult for security solutions to clean and restore the infected files. Based on our analysis, VIRLOCK uses custom encryption, with two layers of encryption. First is a combination of XOR and ROL (rotate on left) encryption and the second layer is an [XOR encryption](http://en.wikipedia.org/wiki/XOR_cipher).

  
*Figure 4. Representation of malware code execution*

***Affected Countries***

Based on feedback from the Smart Protection Network, the top affected country is the United States, followed by China and Australia.

  
*Figure 5. Top affected countries, based on data from January 2015 to present*

**Ransomware, Worms, and File Infectors: a Potent Combination**

As mentioned earlier, this is the first ransomware that includes file infection in its routine. Ransomware often arrives via two methods: 1) botnets, and 2) social engineering. However, these methods aren’t necessarily foolproof. Social engineering can be thwarted by a well-informed user. Botnets are only successful if they are undetected, which only usually happens when they are new or highly complex.

VIRLOCK does not use any of those methods to infect systems. Instead, its very nature is more damaging: a polymorphic worm with file infecting capabilities. It bears stressing that file infectors and worms are two malware types that can effectively and efficiently spread malware—and VIRLOCK can be considered both.

If the infected system is not properly cleaned, even the presence of a single infected file will trigger the infection chain all over again. Once VIRLOCK gets into a system network, it will be all over the place; it can infect a whole network system without notice.

There is also a high chance of executing VIRLOCK on removable drives by mistake since the icons are the same as what you’d expect for certain files on a flash drive. The infected files on the affected removable drive can infect computers with ease.

Since the motivation of the malware is to earn money through ransom fees, infecting files could help the malware to spread to other systems, increasing the chance of getting more money.

**The Future of VIRLOCK**

In our analysis, we also found traces of incomplete modules or illogical codes in VIRLOCK. It’s highly possible that the modules/codes are proof that VIRLOCK is still in the development stage; it won’t be a surprise if we see a more sophisticated VIRLOCK variant in the coming months. One possible development we might see with VIRLOCK is in its arrival vectors. We might see VIRLOCK use a mass-mailing malware to help them to propagate, similar to those used by the [ransomware family CRYPCTB](http://blog.trendmicro.com/trendlabs-security-intelligence/?s=CTB+Locker).

**Countermeasures**

The first line of defense in staying protected against all types of ransomware is being erring on the side of caution. For example, it’s best to avoid opening emails and links sent by unknown or unverified sources/contacts. Some emails may look legitimate in nature, it’s always best to check the sender’s address, subject line, and of course email contents for anything that appears suspicious. Try to visit sites that have been verified as safe. Users can also use the [Trend Micro Site Safety Center](http://global.sitesafety.trendmicro.com/) to check if unfamiliar sites are safe. Never download anything unless they come from official or trusted sources.

As VIRLOCK has propagating capabilities, we highly encourage users to limit connecting their removable drives to computers that are trusted or with security software installed. The same goes for computers: avoid connecting flash drives that cannot be vouched by other people.

Users should always have a security solution installed in their devices. [Trend Micro Security](http://www.trendmicro.com/us/home/products/software/index.html#what-it-does) products leverage the [Smart Protection Network™](http://cloudsecurity.trendmicro.com/us/technology-innovation/our-technology/smart-protection-network/index.html), which rapidly and accurately identifies new threats and delivers global threat intelligence.

Hashes of related files:

* 87cfc5f73a9086ef2f5b0cf08d2c72f4d77b3414
* fef99e8df0bdb9b01406d84061f93d65577b5786
* dc9cf071130ba09f453b7b5613fe36ab84f3c1d4
* 835ae9ae9f3b8936c248a3db26b0ab5e44fe873d
* 4aa26d213ef2424ca3172b7525093fbec6a911f8
* 9a0991919eab723382cb6b5faa0ef8702fb73d01
* 8645176aa24d61ac78b0af67f9bdf50c89b24f78
* abba1e34ec66bff12af2dc59be71fd0edd6bc63e
* a777bbcc78c32df8b1a4d4745c9b6858fd7baaa6
* 77c7551f10777886b1050eea563c3456ce60b1ce
* 514a53baa309b4e1db68d6145e489ff65d283a61
* 4aa26d213ef2424ca3172b7525093fbec6a911f8
* a578bf637d3cb10da62167f5aba3109c1e40e266
* 10ee0549f8f387c55827c48cdd526aac03f3d0c9
* 769c5b0bec033f6651e05122fc31ebdef3c5d8e7
* 52db9a788f1131c43140d0af9781258b8ef2eaf6
* 1b56b6333f46bb3dc4c77d795228a25aefb7a216
* 2a9b4134978bbed27144fd01397da42526250cc3
* 6789c9b1514587055529af821056456f85447d8c