Ransomware Recap: Dec. 19 - Dec. 31, 2016

trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-dec-19-dec-31-2016

Christmas brought an unwanted surprise to one family in 2016. On December 25, software engineer Darren Cauthon tweeted an image showing his family's LG smart TV had been infected with ransomware. The smart TV was disabled, and displayed a ransom note mimicking a notification from the FBI demanding a payment of US$500. It's worth noting that the LG TV was an older model running Google TV, a platform that was abandoned in 2014.

Cauthon asked LG to help him restore the TV to its factory settings. At first the company told him to bring it to a support center but eventually relented and gave him instructions for a factory reset. The Christmas story had an eventual happy ending—the factory reset worked and Cauthon posted a video of the process to help other smart TV owners who might encounter the same problem.

In this particular case, the ransomware that infected the smart TV was identified as the Android mobile ransomware FLocker. First discovered in May 2015, the notorious mobile ransomware has since been rewritten thousands of times to evade detection. The Cauthon incident follows the pattern of recent variants of FLocker (detected as ANDROIDOS_FLOCKER.A): the ransomware impersonates law enforcement agencies, accuses the victim of crimes they didn't commit and then demands a ransom. In June of 2016, Trend Micro already recognized that it was capable of infecting smart TVs. We also noted that it is not the first ransomware to target TVs; and with the proliferation of smart devices across the world, it won't be the last. Users should take steps to secure their smart devices and be wary about the apps they download and install.

Here are some other notable ransomware stories from the last two weeks of December:

KillDisk

KillDisk is a malware well-known for being used in cyber-espionage and sabotage operations that hit several companies in the utilities sector. The most well-known case was when it was used in the BlackEnergy attacks that victimized Ukrainian energy companies in late December 2015.

In mid-December of 2016, KillDisk was reportedly deployed in an operation hitting Ukrainian banks. According to reports, after the TeleBot backdoor Trojan was installed, KillDisk deleted, replaced, or rewrote crucial files to render computers unbootable and cover up illicit operations. The malware is believed to be developed by the TeleBots group, which created the TeleBot backdoor Trojan.

Now, KillDisk (detected as RANSOM_KILLDISK.A) has been updated with a ransomware feature that encrypts targeted files and appends them with string "do not touch crypted file." After encryption, it locks out the user and displays a simple ransom note. Other reports show that the KillDisk ransomware component asks for a huge ransom: 222 Bitcoin, which amounts to about US$210,000.

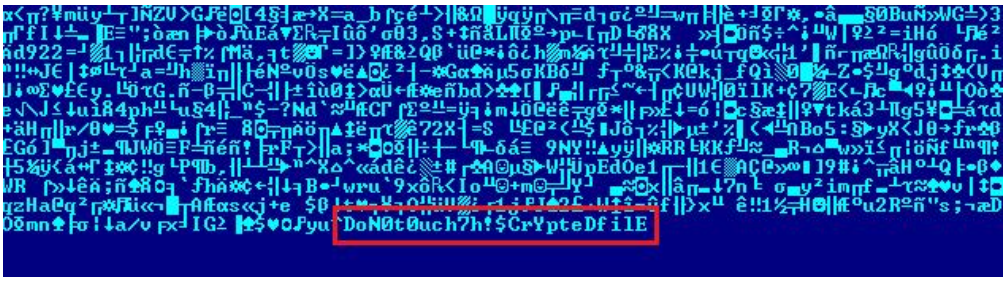

Figure 1.KillDisk sample encrypted file

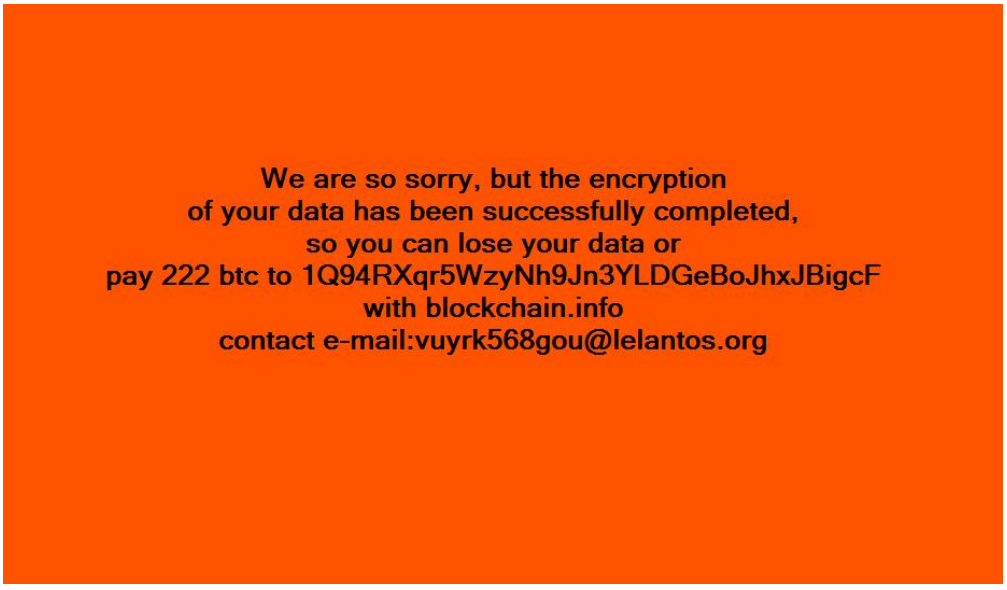

Figure 2. KillDisk ransom note

We have identified that KillDisk fulfills a certain purpose for cybercriminals, the ‘clean up’ after a Trojan installation to hide traces of the infection. This new ransomware update adds another layer to that—if the victim is preoccupied by the ransomware, he or she might not

look for another type of malware infection.**Koovla**

Koovla (detected as RANSOM_EDA2RUNSOME.B) is a new and unusual ransomware variant. It calls itself a Jigsaw "twin", but doesn't follow the behavior of the older ransomware. After it encrypting targeted files, Koovla offers a free decryption key if the victim reads two security articles, one about safe browsing and the other about the Jigsaw ransomware. The motive behind this tactic is unclear, but if the aim of the ransomware operators is to raise awareness then they follow the footsteps of other "educational" families such as EduCrypt and Shinolocker.

In their ransom note, the ransomware operators say that if the victim is too "lazy" to read the articles, their files will be deleted. It doesn't seem ready for distribution though, as the sample obtained will actually terminate if the button of its message window is clicked.

The complete text of the ransom note reads:

"Hello, I'm nice Jigsaw or more commonly known as Jigsaws twin.

Unfortunately all of your personal files (pictures, documents, etc...) have beenencrypted by me, an evil computer virus know as 'Ransomeware'.

Now now, not to worry I'm going to let you restore them but only if you agree to stop downloading\unsafe applications off the internet.

If you continue to do so may end up with a virus way worse than me! You might even end up meetingmy infamous brother Jigsaw :(

While you're at it, you can also read the small article below by Google's security team on how to stay safe online.

Oh yeah I almost forgot! In order for me to decrypt your files you must read the two articles below, once you have click the \"Get My Decryption Key\" button.

Then enter in your decryption key and click the \"Decrypt My Files\" button. Eventually all of your files will be decrypted :)
If the timer reaches zero then all of your personal files will be deleted because you were too lazy to read two articles."

Adam Locker

Adam Locker (detected as RANSOM_ADAMLOCK.A) encrypts targeted files on a victim's system but offers them a free decryption key which can be accessed through Adf.ly, a URL shortening and advertising service. Victims just need to click on the "Open" button on the ransom note and they are led to adf[.]ly/1h2U8c. The shortened link redirects them to http://adamlocker[.]000webhostapp[.]com/key.html, a page that shows the decryption key.

This ransomware veers away from traditional extortion techniques: instead of demanding ransom from victims directly, it uses them to earn money through Adf.ly's payment scheme. The company promises that people can "earn money just by posting links". Adf.ly typically shows ads before leading users to their intended link, and the link posters get paid for driving traffic to the ads.

The company compensates each poster every time their link is clicked —the more views, the more money earned. The ransomware operators are simply driving up their page views and making money by abusing this legitimate service.

Figure 3.The AdamLocker ransom note

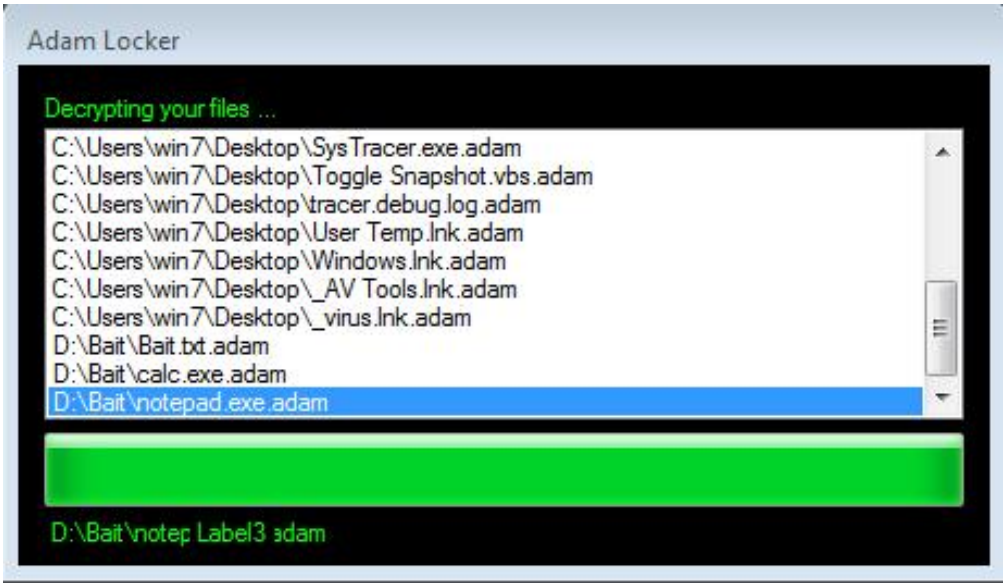

Figure 4.Adam Locker's decryption screen

DeriaLock

Another ransomware family that was spotted during the Christmas holidays was DeriaLock. First seen on Christmas Eve and updated only a few days after, this particular family asks victims to contact a Skype account for the ransom payment.

The first variant (detected as RANSOM_DERIALOCK.A) was only a screenlocker. The second variant (detected as RANSOM_DERIALOCK.B) was updated with an encryption routine and appends .deria to the names of files that it encrypts.

Even after the update, victims are still asked to contact a Skype account for payment purposes. The amount demanded is actually US $10 less than the first variant. The updated version also has a progress bar showing the time allotted for paying the ransom: 1 day. If payment is not made by that time, it claims that it will delete all private files.

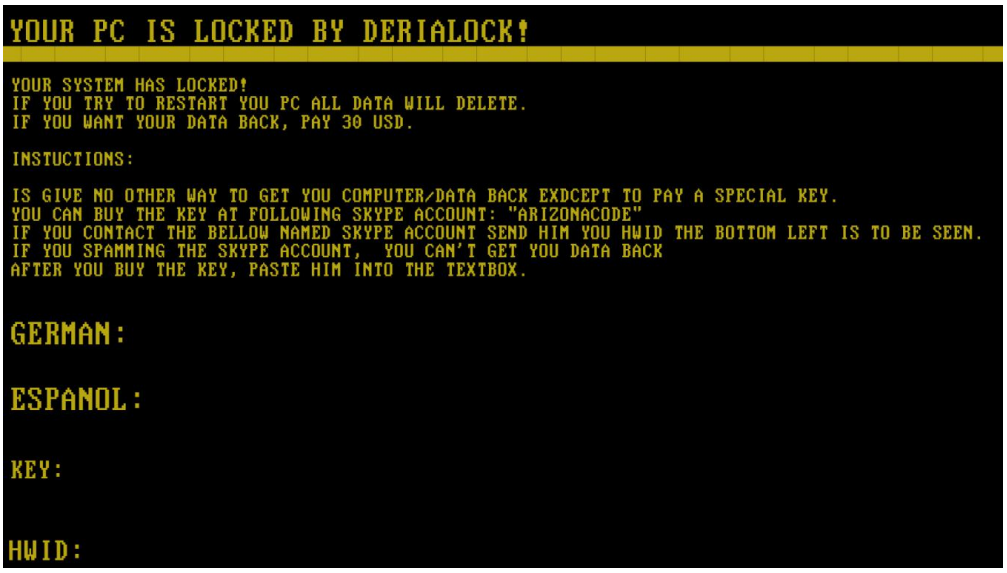

Figure 5. DeriaLock's first variant was a simple screenlocker

Figure 6. DeriaLock is updated with an encryption routine and new visuals

Hidden Tear variants

Two new Hidden Tear-based variants were spotted in late December 2016. The first is KoKoKrypt (detected as RANSOM_HIDDENTEARKOKO.A), which is a very straightforward ransomware. It encrypts files and adds the extension .kokolocker. Victims are served a ransom note demanding .1 Bitcoin, or US$90.

The second is the Guster ransomware (detected as RANSOM_HIDDENTEARGUSTER.A). It uses the extension .locked. This particular ransomware has an animated screenlocker with a voice-over and a 48:00:00 countdown. The ransom is set at .4 Bitcoin, or roughly $365.

The continuing emergence of Hidden Tear variants shows just how dangerous open source ransomware is. Opportunistic malware developers will abuse any available resource.

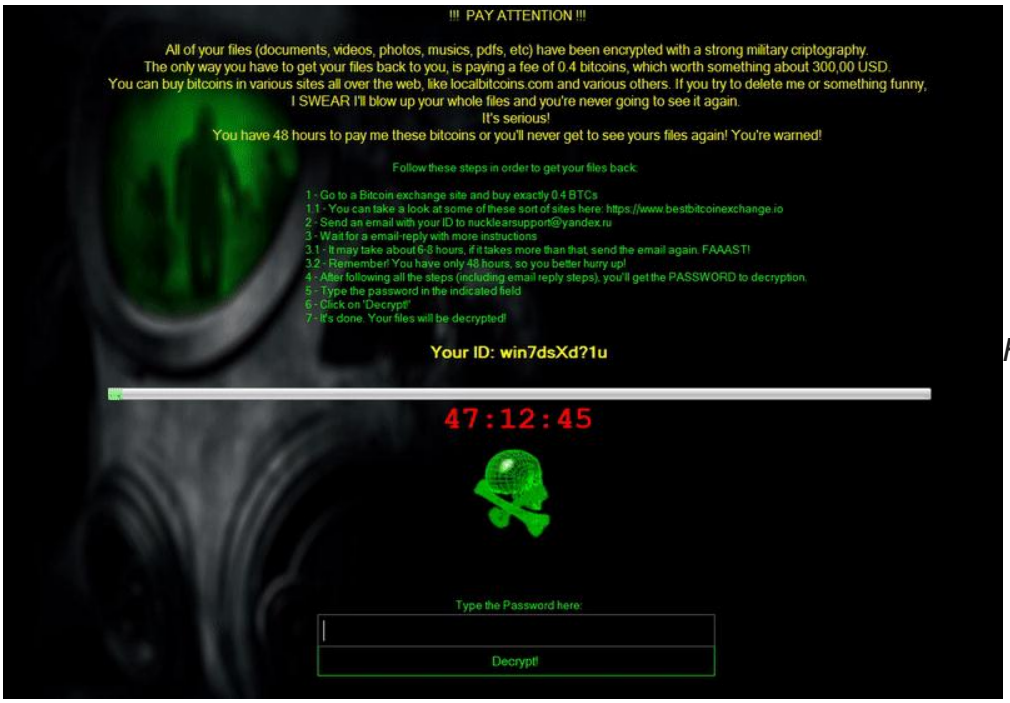

Figure 7.The ransom note for Guster

Ransomware solutions:

Trend Micro offers different solutions to protect enterprises, small businesses, and home users to help minimize the risk of getting infected by ransomware:

Enterprises can benefit from a multi-layered, step-by-step approach in order to best mitigate the risks brought by these threats. Email and web gateway solutions such as Trend Micro™ Deep Discovery™ Email Inspector and InterScan™ Web Security prevents ransomware from ever reaching end users. At the endpoint level, Trend Micro Smart Protection Suites deliver several capabilities like high-fidelity machine learning, behavior monitoring and application control, and vulnerability shielding that minimizes the impact of this threat. Trend Micro Deep Discovery Inspector detects and blocks ransomware on networks, while Trend Micro Deep Security™ stops ransomware from reaching enterprise servers–whether physical, virtual or in the cloud.

For small businesses, Trend Micro Worry-Free Services Advanced offers cloud-based email gateway security through Hosted Email Security. Its endpoint protection also delivers several capabilities such as behavior monitoring and real-time web reputation in order detect and block ransomware.

For home users, Trend Micro Security 10 provides strong protection against ransomware by blocking malicious websites, emails, and files associated with this threat.

Users can likewise take advantage of our free tools such as the Trend Micro Lock Screen Ransomware Tool, which is designed to detect and remove screen-locker ransomware; as well as Trend Micro Crypto-Ransomware File Decryptor Tool, which can decrypt certain variants of crypto-ransomware without paying the ransom or the use of the decryption key.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Ransomware