Trend Micro Incorporated
Research Paper
2012

Police Ransomware Update

By: David Sancho

CONTENTS

Background Information

A ransomware is a kind of malware that withholds some digital assets from victims and asks for payment for the assets' release. Ransomware attacks were first seen in Russia in 2005–2006 and have since changed tactics and targets.

The most recent wave of ransomware attacks targeted users in a very specific way—tracking their geographic locations and scaring them with a scam that fakes their respective countries' police forces while holding their entire systems captive. These attacks have come to be known as the "Police Trojan" attacks. The social networking plot in this case is posing as their local police force and telling the victim that the computer is suspected of illegal operations and they need to pay a fine in order to be able to use it again.

A mix of well-tuned social engineering tactics as well as an advanced and very dynamic networking model shows that the Police Trojan's creators are well-organized, apart from being persistent and creative.

Although technically, the Trojan is not very advanced, it has interesting features. Most importantly, it has been designed to be difficult to clean. Some variants cannot be easily uninstalled even by safe booting the computer.[1]

Fake Antivirus Redux?

The diversity of police ransomware attacks is increasing in the latest number of months and we have observed that there have been many new cybercriminal groups developing their own new versions of the police ransomware. Therefore, it is not straightforward to do a thorough categorization of each and every group that can be found currently in the wild. This seems to be an aftereffect of the malware's success in extracting money from its victims. It seems to be so good at extracting money from victims that more and more new variants coming from different new groups are joining the malware landscape. Our guess is that police ransomware is taking the place of fake antivirus software, whose effectiveness seems to have eroded over time. This observation is purely empirical from the detection side and we cannot contrast it with the real dollar figures that both strategies are yielding from scammed victims. Even in the detection side, figures are misleading because a higher infection count of one does not immediately translate into a higher dollar amount for cybercriminals employing that particular strategy.

As is the case with the fake antivirus phenomenon, police ransomware come mainly from Russia and use affiliate marketing campaigns for their distribution. These campaigns are managed individually by the affiliates of the program, which get a percentage of each scam that is fully realized. Each affiliate uses their own method of spreading the Trojan ranging from hacked sites drive-by-download to botnet victim uploading. We have noticed a tendency of the infection vectors of these Trojans to be related to pornographic web sites. This makes sense within the logic of the whole scam because when the ransom is being claimed on the victim's screen, the Trojan always mentions as part of its social engineering routine that the infected computer has been used to access pornographic contents as well as other illegal actions. This claim, of course, has a much higher impact if it is true so the victim is more likely to end up paying the ransom.

[1] NOTE: The findings in this research paper were presented in "VB2012" in Dallas, Texas by fellow Trend Micro senior threat researcher Loucif Kharouni.

Different Groups, Same Beast

Over the course of our investigations, we have been able to locate at least two suspect affiliate programs of police ransomware but even those change names and URLs quite often and are restricted so we have not been able to sign up and obtain a consistent influx of samples.

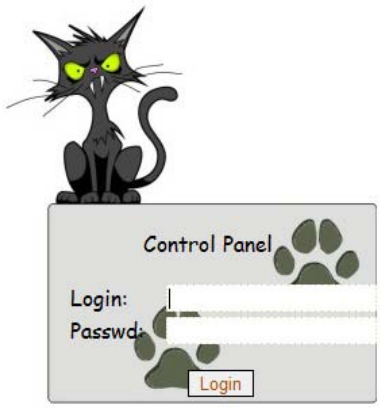

Figure 1: Login panel for the affiliate program

Figure 2: Control panel

Group A

The server side of this group contains all the images and a script that identifies what country the victim is coming from. This script serves the right image to the infected client, which includes the police threat written in the local language plus the logo of the local police force. This is an open directory we found on one of their servers:

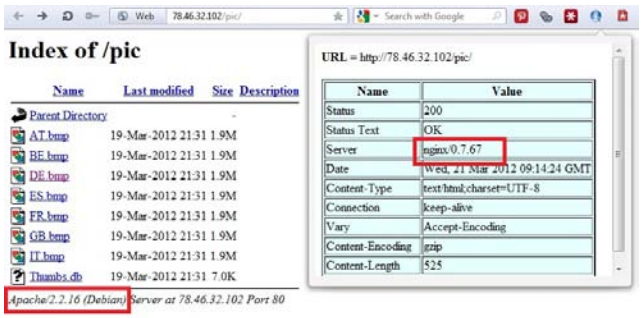

Figure 3: Open directory 1

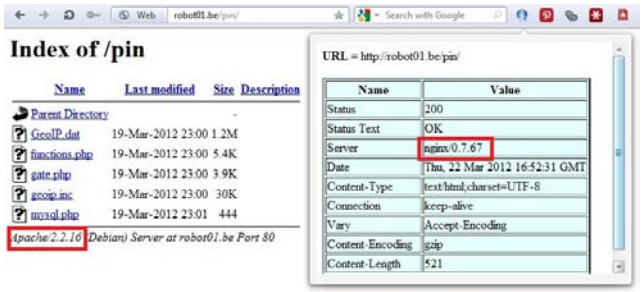

Figure 4: Open directory 2

This group is one of the earliest ones and their strategy is one of the most straightforward. Some other groups are complicating this.

Group B

This is another of the more recognizable ones, also from the earlier batches, from the second half of 2011. This group embeds the images right into the PHP scripts so that they are never downloaded separately. This is a screenshot of the main PHP script that generates the fake threat posing as the Canadian Police:

Figure 5: Embedded images

Note how the image is directly inside the PHP code, encoded in base64. The final page, when shown to the victim displays as the recomposed image pictured below:

Figure 6: Sample image served to victims in Canada

In both cases and in a whole lot of other variants, the threats are very similar. Here are a couple of examples showing the British and German attacks.

Figure 7: British-targeted example

Figure 8: German-targeted example

Another reason why we think there is a relationship between fake antivirus and police ransomware is that the latter have also used fake security tool notifications when the country the victim was coming from could not be determined. These notifications are very similar to standard fake antivirus attacks. This overlap of attacking techniques makes us think that the same developers are behind the attacks and they are just switching attacking tactics as fake antivirus become less able to con computer users.

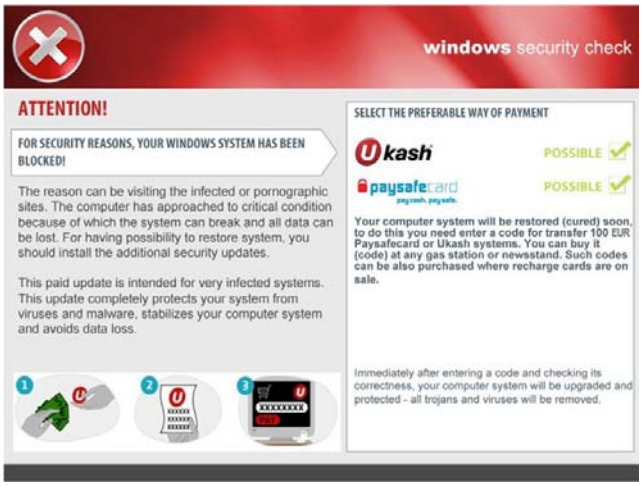

Figure 9: Image served when the country the victim is in can't be determined

Following the Money Trail

The payment method these attackers utilize is not random. It is carefully planned to make the money trail as faint as possible. Instead of accepting credit card payments as was the case with fake antivirus, these fake "fines" only accept two kinds of vouchers that can be used to buy goods and service online. These vouchers are PaySafeCard and UKash, which are commonly bought in newsagents, petrol stations, chemists or kiosks through Europe. There are minor differences between the two kinds of vouchers but the general idea is the same. Some of these differences are: PaySafeCard can be purchased in the US and Canada. UKash purchases may require a valid means of identification; they might not be completely anonymous.

The main problem in following the money trail in PaySafeCard/UKash transactions is that there is no record that the voucher changed hands until it is finally spent. Imagine that a victim is scammed for $100. They went to a shop, bought a voucher and gave the voucher code to the ransomware cybercriminals. These scammers can sell the voucher and it will keep changing hands until it is sold to an end customer, who will spend it. By then, since there is no record, it is difficult to discern where that voucher came from.

In order to monetize PaySafeCard/UKash vouchers, there are underground voucher exchange sites that buy them from the cybercriminals paying somewhere between 40 and 50 percent of the nominal value of the voucher. These web sites then resell them to regular users who want to buy discounted vouchers for about 90% of the nominal value. Often times this buying and selling PaySafeCard and UKash vouchers also commonly takes place in underground forums or through shadier media, such as ICQ and other untraceable communication methods.

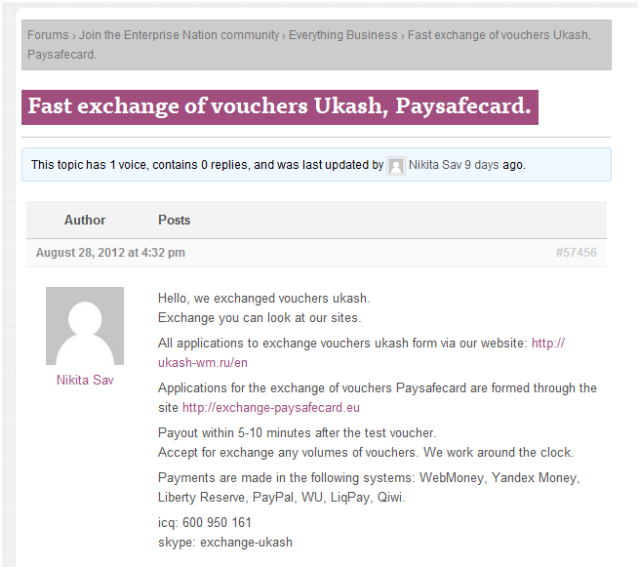

Figure 10: uKash voucher exchange in an underground forum

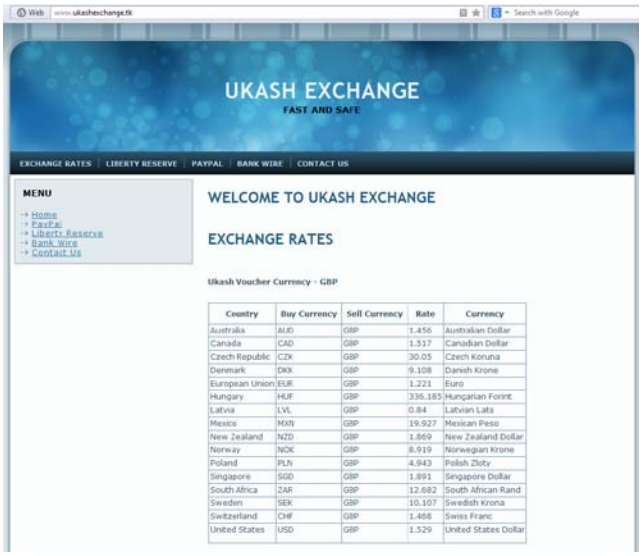

Figure 11: Sample uKash exchange rates

CONCLUSION

The way these companies are tackling this problem is the following:

1. Reporting and taking down public exchange web sites. This forces cybercriminals to use one-to-one communication methods so it slows down monetization and it ups their costs decreasing the long-term feasibility of this business model.

2. Identifying these vouchers by the behavior of the exchanges. Repeated balance checking and other observed patterns make this heuristically feasible. Once one of these vouchers has been identified, the company voids them.

This phenomenon is becoming a threat landscape change rather than a single isolated malware incident. As the business model of ransomware improves and that of fake antivirus worsens, more criminal groups jump on board. We are seeing a diversification of developments that means that we are just at that stage. Once the victim pool has become too aware of this tactic, the cybercriminals will probably switch to a different one, as usual. In this process, though, the criminals have learned that online vouchers such as those offered by UKash and PaySafeCard are perfect for their needs: practically untraceable. The bad guys will keep using them as long as there is an underground economy of voucher exchanges.

TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014
U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud