Endpoint Protection

symantec.com/connect/blogs/trojanbayrob-strikes-again-1

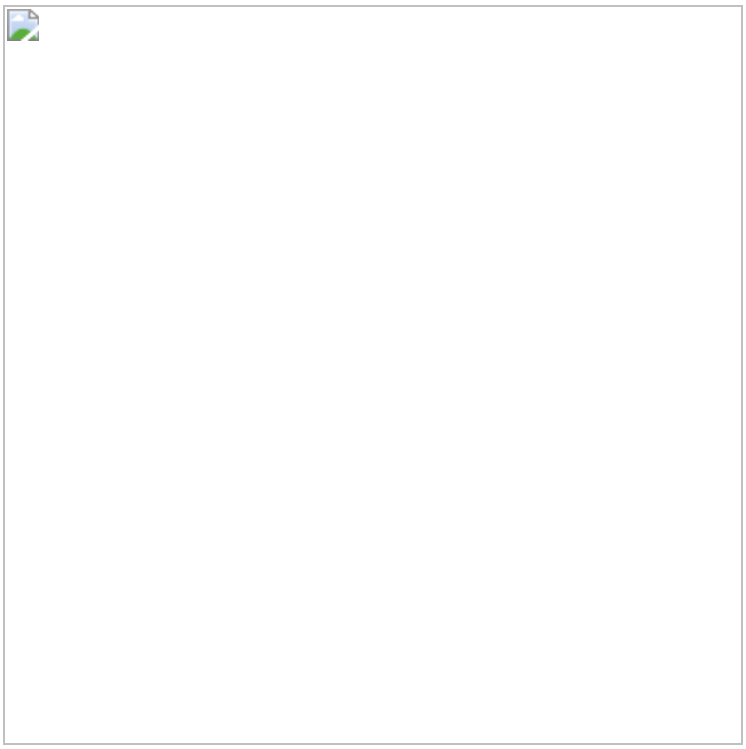
Migration User

Recent reports have shown thatTrojan.Bayrob is scamming people again. The latest victim lost over€5,000 to the scam but luckily was able to track down where the moneyhad been sent. Unfortunately the final destination for the money was aWestern Union outlet in Greece, after having been first sent through amoney mule in the US.

Once Trojan.Bayrob is executed on a user's system it can interceptall traffic to eBay. It can then show the infected user any contentthat it chooses instead of the real pages and it can also alterinformation that is shown to the user from the real pages.Trojan.Bayrob is used to scam people who are trying to buy cars oneBay.

The attack is a targeted attack and as such it is difficult toestablish the exact methods that are used to distribute the Trojan;however, from evidence gathered thus far the attack works in a mannersimilar to the following:
• The attacker posts an auction on eBay.
• This auction is used to gain information about potential buyers/victims.
• Anyone who asks a question about the auction may become a target.
• If a user asks a question about the item the attacker will reply,sending the Trojan disguised as further pictures of the car for sale.In the past we have seen the file name DisplayPics.exe used.
• The email may also give a plausible explanation as to why the car isa great offer. The email also states that the car has been re-listed oneBay since it did not sell during the previous auction.
• When the user opens "Displaypics.exe" the Trojan shows a slide showof the car for sale, using "Kodak Viewer Express" however it also dropsanother file silently in the background and executes it as well.

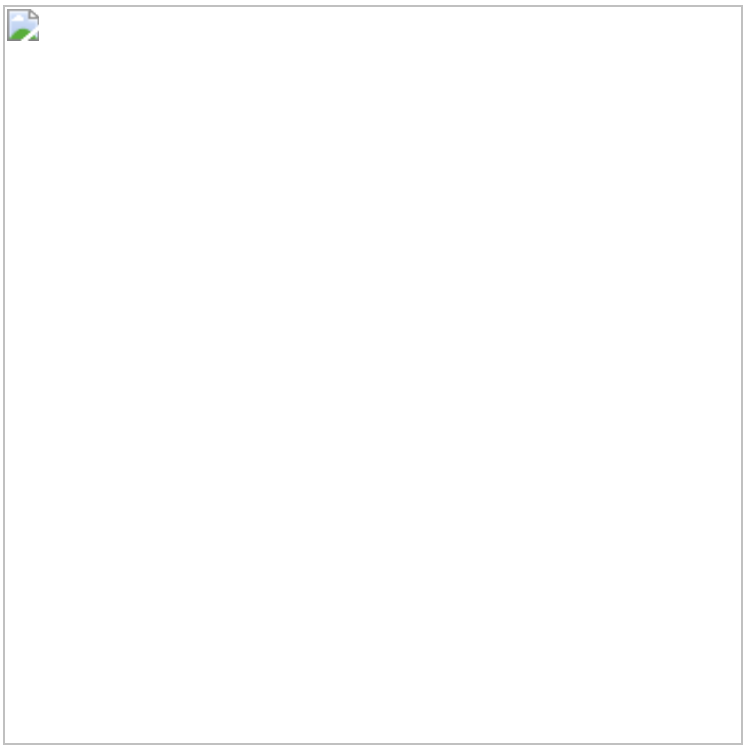
The images that were used in this case were for a Jeep:



Click for larger image

At this point the Trojan is running in the background. All trafficdestined for eBay.com is now silently intercepted by the Trojan. Then adecision is made as to whether the infected user should be shown thereal eBay pages or if fake eBay pages should be displayed instead.Anytime the infected user tries to view pages that are related to thecar they are interested in buying, the Trojan will make the decision toshow fake pages instead of the real eBay pages. These fake pages canshow a variety of fake information, including inflated ratings for theseller and fake positive feedback for the seller.

The Trojan is specifically designed to make sure that the user does notnotice any difference between the real content and the altered contentthat the Trojan returns. This all leads the infected user to trust thatthe car auction and seller are trustworthy and to proceed to buy thecar. While the auction looks completely legitimate on the infecteduser's machine, if the same auction is viewed from a non-infectedmachine the difference can be seen immediately.
For example, here is a screen shot taken from an infected user's machine:



Click for larger image

In this shot the Trojan has silently altered the page returned fromeBay, it shows that the seller has a feedback rating of 13, howeverwhen viewed from a non-infected machine the seller had a feedback ofjust 1.

Since it was first discovered in March the Trojan has been underfurther development. The Trojan can now intercept and alter trafficdestined for sites other than eBay! The ability to intercept trafficfor the following sites has been added to the new version of the Trojan:

- www.carfax.com
- www.autocheck.com
- wwwapps.ups.com
- escrow.com
- my.escrow.com
- ecart.escrow.com
- www.escrow.com

This is very worrying as it shows the lengths that the Bayrob gangwill go to in order to convince infected users that what they areseeing is real. Now even if a (infected) shopper is very cautious anddecides to check the car out at sites outside of eBay (in this casecarfax.com or autocheck.com) they will receive fake results also.

It is also very interesting to see that traffic for ups.com is alsointercepted; can the Trojan also show fake information about apackages' delivery status? We have not been able to confirm this as yetbut it would fit with the pattern of this Trojan.

The site escrow.com has also fallen into the crosshairs of thisTrojan. It appears that even if the user wished to pay via the escrowsite so as to protect their money, the gang behind Trojan.Bayrob willbe able to detect this and intercept or alter that traffic also.

Of course the Trojan can still intercept traffic destined for the following eBay sites also just as it could before:

- my.ebay.com
- cgi.ebay.com
- offer.ebay.com
- feedback.ebay.com
- motors.search.ebay.com
- search.ebay.com
- us.ebayobjects.com
- pages.ebay.com
- pages.motors.ebay.com
- motors.listings.ebay.com
- cgi1.ebay.com

From analysis of the sample involved in this case it is clear thatthis was a targeted attack against a single user. This can be seen dueto the fact that there are specific details related to the victimembedded in the executable. This means that every time the gang want toscam a new victim they create a new, slightly different, Trojan thatcontains the specific details of the new victim. This shows that thegang behind this Trojan are very involved in each particular scam thatis perpetrated.

The most recent case of the fraud sheds more light on how the scamworks and what happens to the money after the auction has ended. Moneymules in the US are recruited before the scam takes place so that thevictim will not be suspicious about the destination of the money forthe auction. Most people would be sceptical of sending money to Greecefor a car on sale in the US for example. By using money mules in the USthe scammers avoid raising suspicions about the auction until the moneyhas already been delivered to the attackers via the mules. I suspectthat the attackers did not collect the money in Greece themselves butrecruited other people to collect these payments also.
Money mules normally receive funds to their own bona fide USaccounts then withdraw it in cash and send it to the operators of thescam via Western Union (in this case) taking a percentage of the amountfor their part. The mules are often recruited in work-from-home typescams – much has already been written on that subject elsewhere.

In the latest disclosed case the victim realized they had beeninfected by the Trojan when the user posted to the eBay forum stating ascam had occurred. When other eBay users checked the details of the bidthey informed the user that they were seeing different information ontheir computers than what was being shown on the infected machine.

When the user viewed the bidding history on the infected machine, afake eBay page was returned by the Trojan and this fake page showedthat the user had bid on a Jeep and had won the auction. However, whenthe same page was viewed from an uninfected machine there was no recordof the user's purchase of the Jeep.

The gang behind this Trojan have shown themselves to be veryorganized and skilled and they possess many different abilities; theyare able to code in php, write Trojans, recruit money mules, andorganize money drops. This is a sophisticated operation that has becomemore advanced since it was first discovered in March with the additionof other sites, such as carfax.com, ups.com, and escrow.com.

The Trojan is currently known to use the following servers:

- wmwbc.com
- vam-ars.com
- cameradealsusa.com
- michelleorea.com

Other servers are also being investigated as being part of the scam. Afirewall should be used to deny access to the above addresses. EBayusers that have been affected by Trojan.Bayrob are encouraged tocontact eBay and local law enforcement to report the scam.