Endpoint Protection

symantec.com/connect/blogs/bayrob-three-suspects-extradited-face-charges-us

Dec 16, 2016 11:31 AM

A L Johnson

Three Romanian men have been indicted in the US for allegedly operating a longstanding fraud operation known as Bayrob that conned victims out of millions of dollars. Bogdan Nicolescu (aka “Masterfraud”, aka “mf”); Danet Tiberiu (aka “Amightysa”, aka “amy”); and Radu Miclaus (aka “Minolta”, aka “min”) were arrested by police in Romania earlier this year before being extradited to the US, where they now face multiple charges relating to fraud, identity theft, money laundering, and trafficking in counterfeit goods or services.

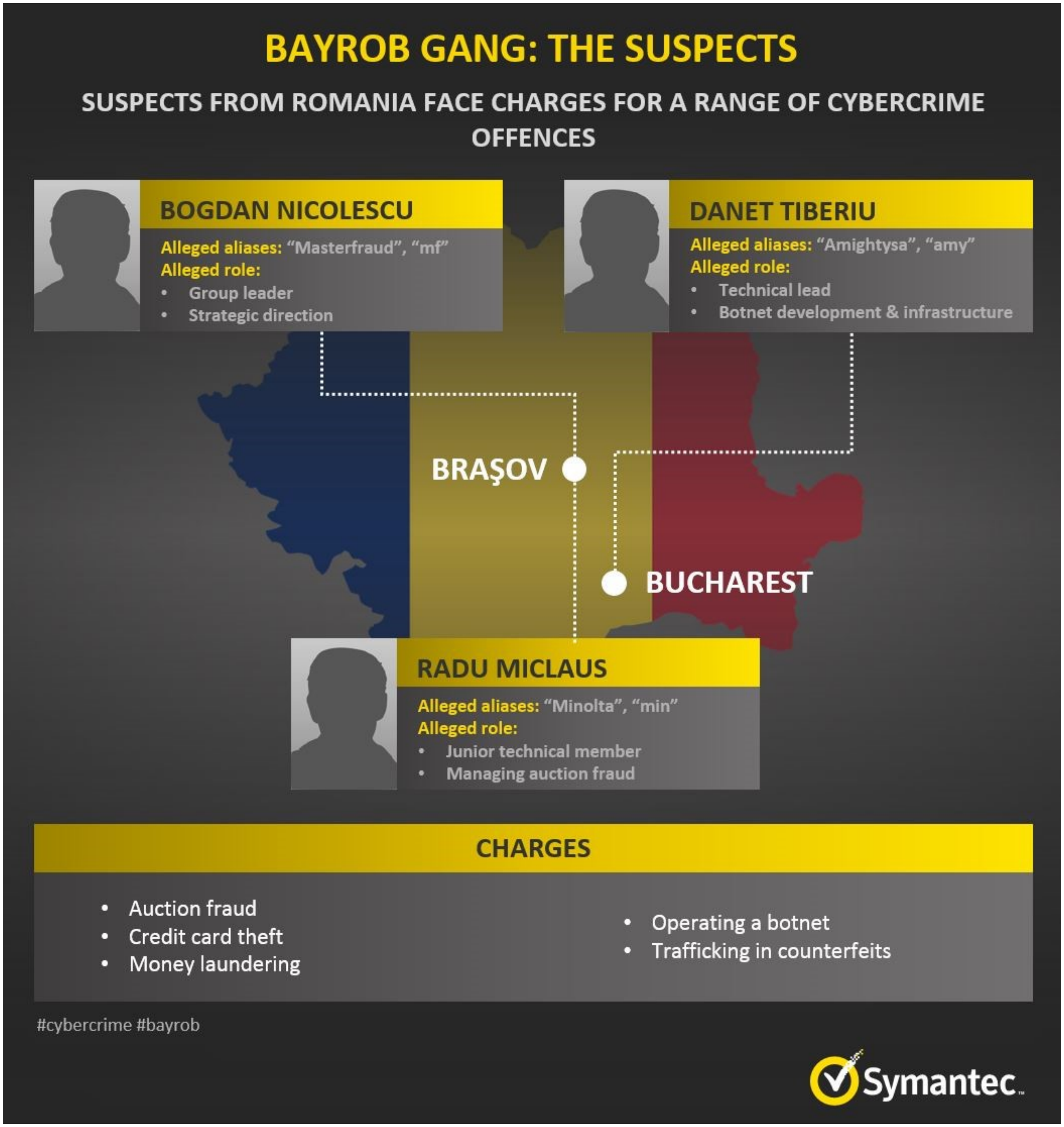
Our research shows that the Bayrob gang are career cybercriminals, earning a living from online fraud. They specialize in detailed scams and go to great lengths to craft convincing emails and create fake websites, voice messages, and even customer support chatrooms in order to dupe victims.

The gang began its career running elaborate cons where it created fake vehicle auctions to defraud victims out of tens of thousands of dollars. It later expanded and diversified with a number of different fraud and malware operations, ranging from credit card theft to cryptocurrency mining using infected computers.

The FBI believes that the Bayrob group has stolen at least US$4 million from victims over the past eight years, though the actual total may be up to $35 million. It also established that the group infected between 60,000 and 160,000 computers and sent out 11 million malicious emails.

The arrests are the culmination of an eight-year law enforcement investigation which was assisted by Symantec. During this time, Symantec discovered multiple versions of Bayrob malware, collected helpful intelligence data, and witnessed Bayrob as it morphed from online fraud to a 300,000+ botnet for cryptocurrency mining.

Symantec succeeded in exposing the gang’s operations, gaining insight into its key players, tactics, malware, and the potential impact and criminal activity undertaken.



BAYROB GANG: THE SUSPECTS

SUSPECTS FROM ROMANIA FACE CHARGES FOR A RANGE OF CYBERCRIME OFFENCES

BOGDAN NICOLESCU
Alleged aliases: “Masterfraud”, “mf”
Alleged role:
- Group leader
- Strategic direction

DANET TIBERIU
Alleged aliases: “Amightysa”, “amy”
Alleged role:
- Technical lead
- Botnet development & infrastructure

BRAŞOV

BUCHAREST

RADU MICLAUS
Alleged aliases: “Minolta”, “min”
Alleged role:
- Junior technical member
- Managing auction fraud

CHARGES
- Auction fraud
- Credit card theft
- Money laundering
- Operating a botnet
- Trafficking in counterfeits

#cybercrime #bayrob

Symantec

Elaborate car auction scams

Bayrob first came to our attention in 2007, when it was discovered operating a scam that conned victims into believing they were buying a vehicle on eBay. Victims’ computers were infected with custom designed malware (Trojan.Bayrob) which displayed fake eBay web pages and misled users into thinking they were conducting a legitimate purchase on the auction site.

The gang identified potential victims by listing vehicles for sale on a number of websites, including eBay and classified advertising websites. It noted anyone who displayed an interest in the sale, such as those who asked questions or put a bid on the vehicle. The gang would then pretend that the sale had concluded but later email potential victims, informing them that the sale had fallen through and asking if they were still interested.

Attached to these emails was a slideshow file, containing pictures of the vehicle supposedly on sale. This file was infected with Trojan.Bayrob. If the victim opened it, the malware was installed on their computer.

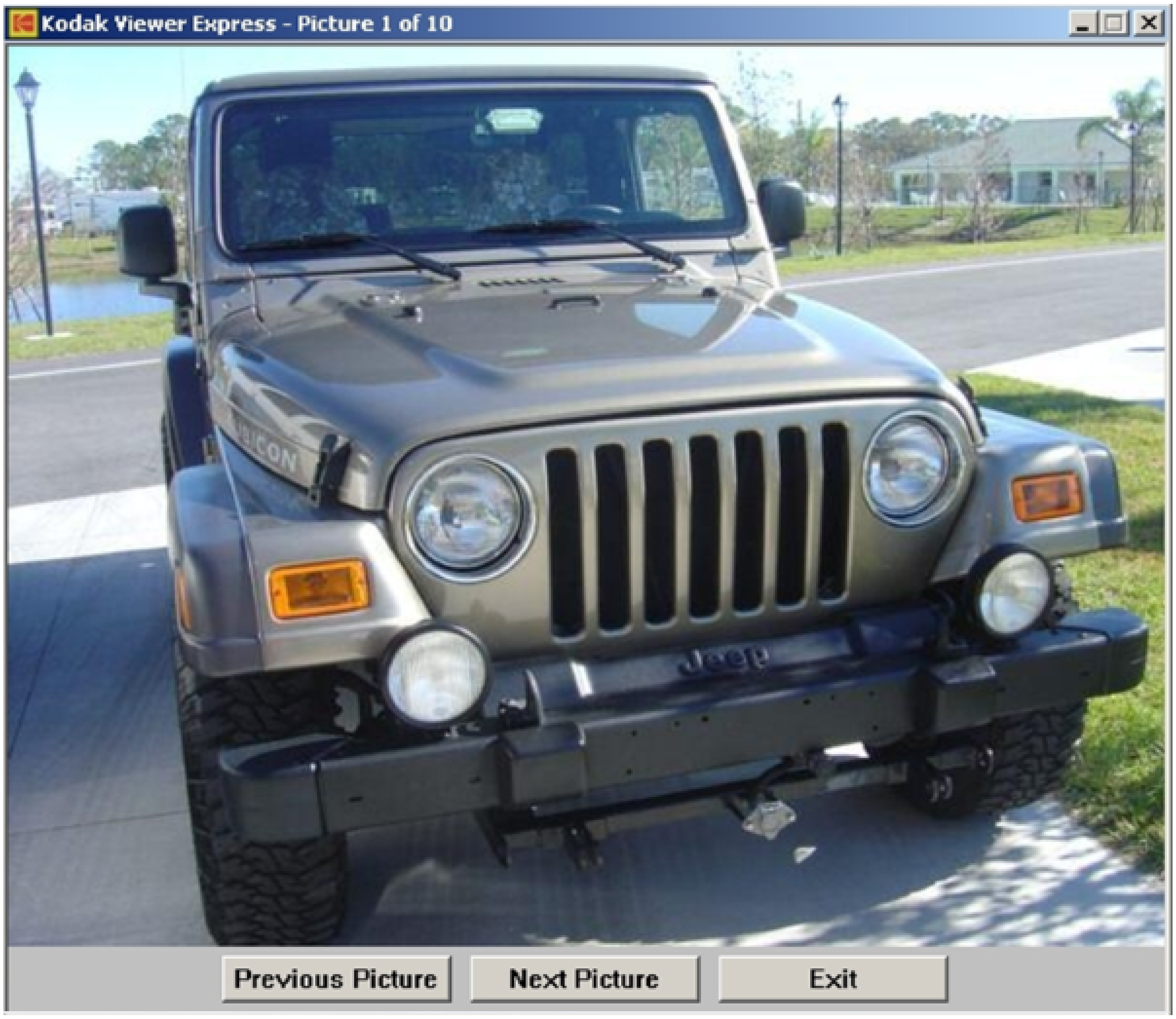


Figure 1. Slideshow files with pictures of the vehicle supposedly on sale were infected with the Bayrob Trojan

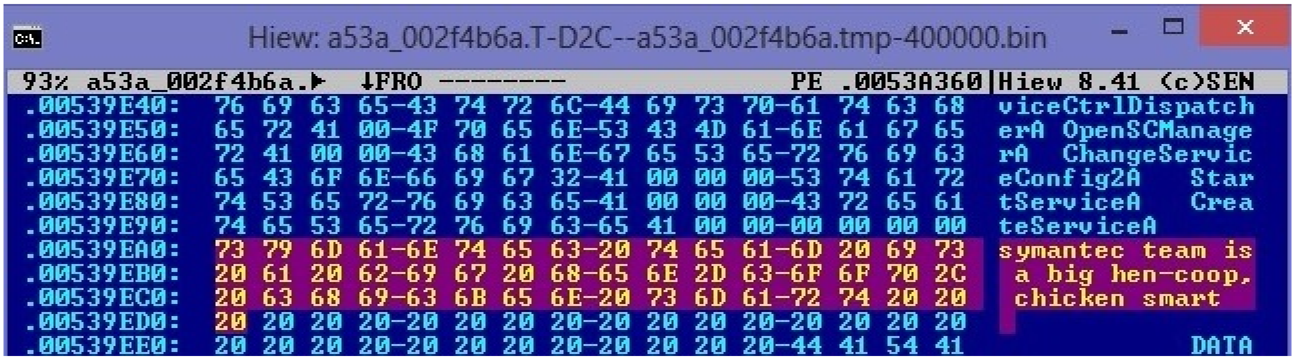
Once the attackers verified that the Bayrob Trojan was running on a victim's computer, they moved on to the next stage of the scam by sending an email with what they claimed was a link to a new auction for the vehicle. It was at this point that the Trojan came into play. If the victim clicked on the link, it would redirect them to a fake eBay page. If they decided to buy the vehicle, they were asked to pay by way of a bank transfer, which was routed to an account that belonged to a money mule, who would in turn transfer the proceeds of the fraud to the gang.

From the victim’s standpoint it appeared they were visiting a real eBay auction. However, if the link was followed from an uninfected computer, there would be no such auction. The gang went to great lengths to make the scam appear realistic. Its emails were composed in fluent English and every iteration of the Bayrob Trojan was customized for its intended victim. The fake eBay web pages even included fictitious feedback about the seller. The Trojan was also capable of generating fake vehicle history reports, along with fake pages from escrow and delivery services.

The fraud had a major impact on its victims, who often transferred thousands of dollars thinking they were paying for a new car and ended up with nothing.

Exposure and expansion

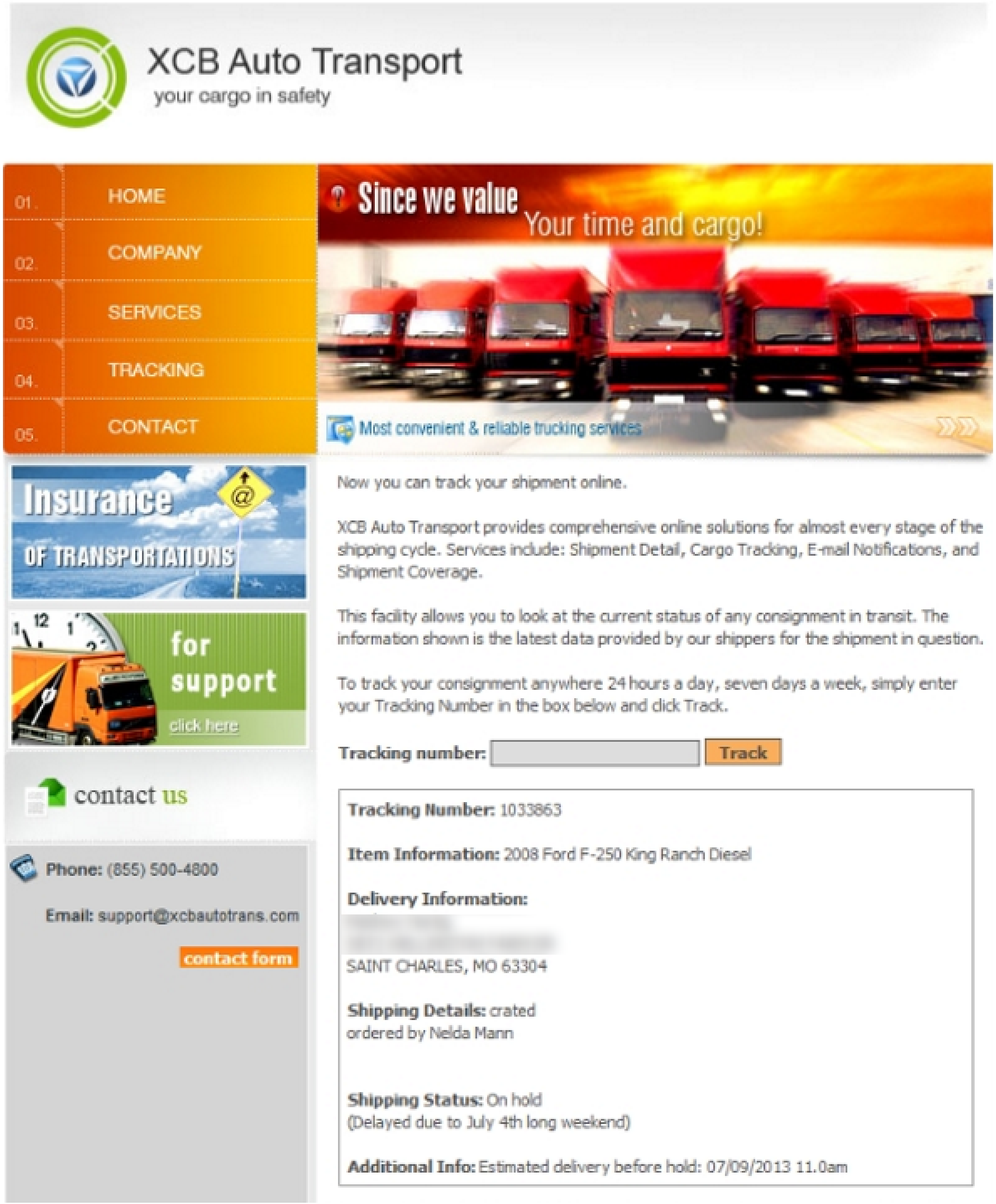
Bayrob’s activities were initially exposed by Symantec in 2007, when we published a series of blogs highlighting the eBay scam, and several media outlets reported on their activities. The gang reacted angrily and, for a while, registered command and control (C&C) domain names that contained abusive references to our researchers and made disparaging references to Symantec in its code.



```
 93% a53a_002f4b6a.▶  ↓FRO ---------             PE .0053A360|Hiew 8.41 (c)SEN
 .00539E40:  76 69 63 65-43 74 72 6C-44 69 73 70-61 74 63 68  viceCtrlDispatch
 .00539E50:  65 72 41 00-4F 70 65 6E-53 43 4D 61-6E 61 67 65  erA OpenSCManage
 .00539E60:  72 41 00 00-43 68 61 6E-67 65 53 65-72 76 69 63  rA  ChangeServic
 .00539E70:  65 43 6F 6E-66 69 67 32-41 00 00 00-53 74 61 72  eConfig2A   Star
 .00539E80:  74 53 65 72-76 69 63 65-41 00 00 00-43 72 65 61  tServiceA   Crea
 .00539E90:  74 65 53 65-72 76 69 63-65 41 00 00-00 00 00 00  teServiceA
 .00539EA0:  73 79 6D 61-6E 74 65 63-20 74 65 61-6D 20 69 73  symantec team is
 .00539EB0:  20 61 20 62-69 67 20 68-65 6E 2D 63-6F 6F 70 2C   a big hen-coop,
 .00539EC0:  20 63 68 69-63 6B 65 6E-20 73 6D 61-72 74 20 20   chicken smart
 .00539ED0:  20 20 20 20-20 20 20 20-20 20 20 20-20 20 20 20
 .00539EE0:  20 20 20 20-20 20 20 20-20 20 20 20-44 41 54 41              DATA
```

Figure 2. One of the more polite references to Symantec made by the gang in its code

However, public attention didn’t deter the gang from further expanding and refining its operations. For example, they created a fake trucking company, which was used to supposedly transport purchased vehicles to their victims. The trucking company would first inform the victim their vehicle was on the way and then later email them informing them of delays. It even operated a phone line and fake voicemail service to appear more convincing. The whole purpose of the fake trucking company was to string the victim along for as long as possible in order to make sure the gang received the money before the victim realized they’d been conned.



Now you can track your shipment online.

XCB Auto Transport provides comprehensive online solutions for almost every stage of the shipping cycle. Services include: Shipment Detail, Cargo Tracking, E-mail Notifications, and Shipment Coverage.

This facility allows you to look at the current status of any consignment in transit. The information shown is the latest data provided by our shippers for the shipment in question.

To track your consignment anywhere 24 hours a day, seven days a week, simply enter your Tracking Number in the box below and click Track.

Tracking number:

Phone: (855) 500-4800

Email: support@xcbautotrans.com

Tracking Number: 1033863

Item Information: 2008 Ford F-250 King Ranch Diesel

Delivery Information:
[redacted]
SAINT CHARLES, MO 63304

Shipping Details: crated
ordered by Nelda Mann

Shipping Status: On hold
(Delayed due to July 4th long weekend)

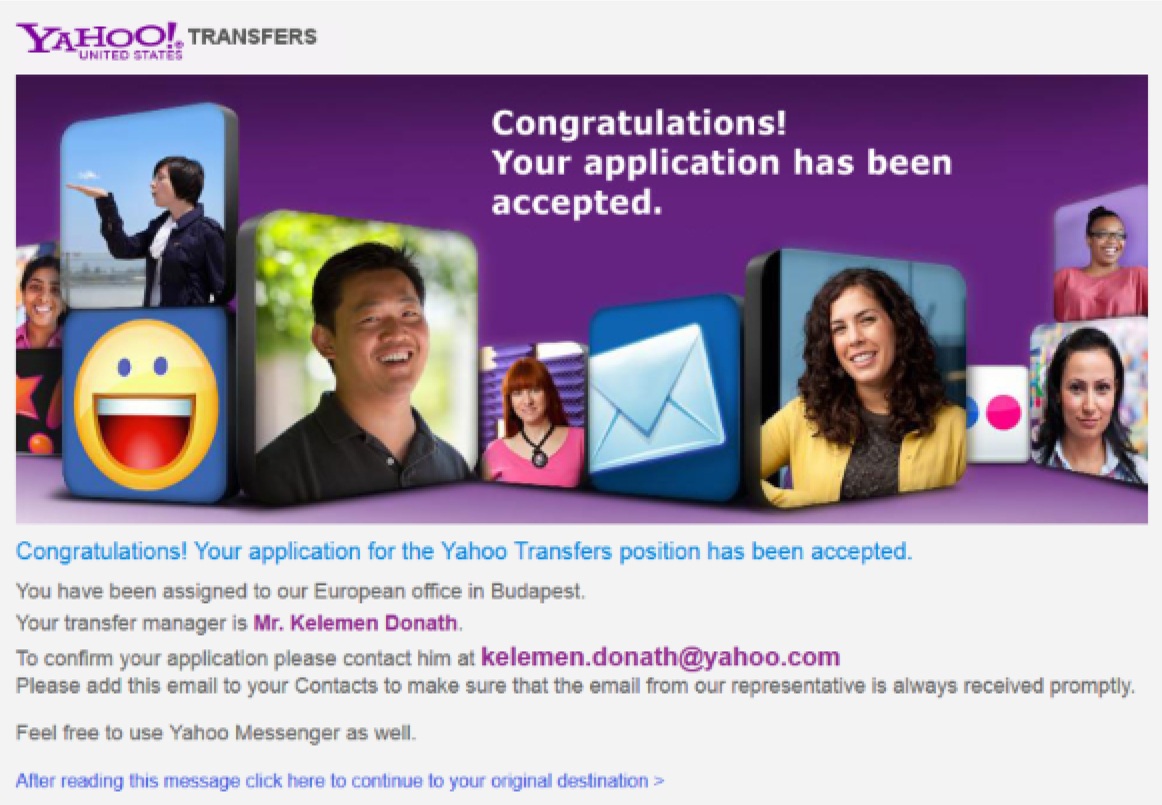
Additional Info: Estimated delivery before hold: 07/09/2013 11.0am

Figure 3. The gang set up fake trucking companies to string the victim along for longer and make them believe their vehicle had been shipped

Network of money mules

In order to move the proceeds of its scams back to Romania, the gang recruited a wide network of money mules. It found potential mules by spamming classified advertising websites with fake job ads. Rather than the usual cybercriminal tactic of using “work from home” ads, the Bayrob gang often copied legitimate job ads in order appear more convincing. Those who responded were told that the job had been filled but were then offered an alternative, work from home job.

As with its other operations, money mule recruitment was professionally executed and backed up by a series of fake websites and convincing looking emails, such as one purporting to offer the recipient a job with a technology company. Some victims were even told they’d gotten a job with a fake Yahoo subsidiary called Yahoo Transfers.



Congratulations!
Your application has been accepted.

Congratulations! Your application for the Yahoo Transfers position has been accepted.

You have been assigned to our European office in Budapest.

Your transfer manager is **Mr. Kelemen Donath**.

To confirm your application please contact him at **kelemen.donath@yahoo.com**
Please add this email to your Contacts to make sure that the email from our representative is always received promptly.

Feel free to use Yahoo Messenger as well.

After reading this message click here to continue to your original destination >

Figure 4. Some money mules were told they’d gotten a job with a fake Yahoo subsidiary

Given that they would be handling the gang’s stolen money, mules were thoroughly vetted during recruitment, using Google searches, instant messaging, and VoIP calls. The group recruited mules on both sides of the Atlantic. Victims in the US were instructed to route payments to a bank account controlled by a mule in the US. These in turn were asked to transfer the money to another mule, usually in an Eastern European country. They would then presumably transfer the money on to gang members.

Mules in the US were often vulnerable people in difficult circumstances. They appeared to be unwitting pawns of the gang, unaware of what they’d become involved with. Less is known about the money mules used in Europe, but most appeared to collect transferred funds using fake identities, indicating they may have been more complicit in the gang’s activities.

Mules in the US were given two options for payment. They could keep six percent of the funds they transferred or they could send the entire amount and later receive a check for 10 percent of the total. The latter option was a scam and nobody who opted for it received any payment from the gang. Despite putting these money mules at risk of arrest and prosecution, the gang had no qualms about double crossing them and stealing from them too.

Diversification of operations

Over time, the Bayrob gang expanded beyond its original auction fraud and into other areas of cybercrime. The group began stealing credit card information from the users of infected computers, using the stolen cards to finance the purchase of online infrastructure and services that allowed it to grow its operations.

In recent years, the gang has concentrated on rapidly growing the number of infected computers in order to build a botnet. When it was exclusively involved in auction fraud, the number of infected computers was around 1,000 at any one time. However, by 2014 it had jumped to approximately 50,000 and by mid-2016 it had grown to over 300,000 and continued to grow.

One of the main purposes of this botnet appeared to be cryptocurrency mining. A large number of infected computers provided the gang with the necessary processing power to profit significantly from mining.

Breakthrough in the investigation

Since 2011, Symantec has managed to progressively uncover the gang’s network, gaining a broad picture of its operations. The information generated by our investigation not only helped us to improve our protections against the group’s malware, but also allowed us to prevent future attacks and warn potential victims. What we learned assisted the FBI in its investigation and we opted not to publish what we discovered in recent years until the FBI investigation was concluded.

Bayrob employed a high degree of internal security. Their online communications involved extensive use of encryption, with email encrypted using PGP and instant messaging encrypted with the Off-The-Record (OTR) messaging protocol.

In order to cover its tracks, the gang hid behind a double layer of proxies, connecting first to proxies in Romania and then to more proxies in the US. One of our most significant breakthroughs came when we discovered a weak point in their use of these proxies. Due to this weakness, the gang's malicious activities were exposed, allowing us to passively observe its activities on computers Symantec was protecting.

Our investigation required time and patience. In one case, we observed the gang’s malicious activities for a year and a half before it made an error that exposed one of its

suspected members. Over time we came to understand the group’s infrastructure which helped us to get see more of the gang’s operations.
Symantec’s pursuit of Bayrob is one of many long standing investigations we currently have underway, all of which are motivated by a desire to protect our customers. Today’s arrests illustrate the value of effective co-operation between security companies and law enforcement and sends a clear signal to international cybercrime gangs that they are not beyond the reach of the justice system.

Protection

Symantec products use multiple layers over protection against Bayrob’s malware. Protection has been continuously updated since 2007 to block against each new iteration of the group’s malware.

Symantec and Norton products block Bayrob malware with the following detections:

Antivirus

Intrusion prevention system

In addition to this, a range of Symantec generic detections also successfully block Bayrob malware. The addition of generic detections to our defense layer makes it more difficult for attackers to identify which detections are designed to specifically block their malware, making it hard to test against them.

Further information

Symantec has gathered full technical details and indicators of compromise for all Bayrob malware variants discovered since 2007. This can be supplied to any member of the information security community upon request.