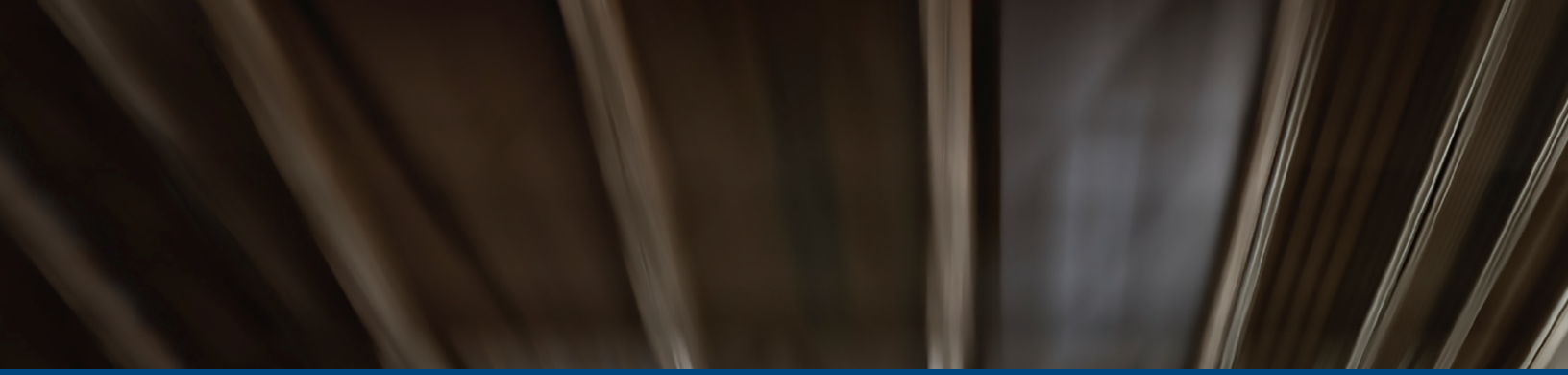


SecureWorks

Underground Hacker Markets

ANNUAL REPORT—APRIL 2016

Contents

3 Introduction: Welcome Back to the Underground

4 Price List for Hacker Goods and Services

7 Russian Hackers Expand their Working Hours and Use Guarantors to Ensure Customers' Happiness

9 Hacking Services for Hire

11 Business Dossiers for Companies in the Russian Federation
Bank Account Credentials, Tax Identification Numbers (TINS), Articles of Incorporation, Phone Numbers, Lease Agreements

12 Hacker Goods for Sale
Bank Accounts, Popular Online Payment Accounts, Airline Points Accounts, Credit Cards, Hacker Tutorials…You Name It

16 Is ATM Skimming Passé? Not on Your Life.

19 Security Measures for Protecting Against Cyber Threats

22 Conclusion

23 Glossary of Terms

Welcome Back to the Underground

For our 3rd Annual Underground Hacker Markets Report, Dell SecureWorks engaged two of our top intelligence analysts from our CISO INTEL Team. The team members spend time tracking hackers on the numerous underground hacker forums and marketplaces all over the world. While much of the cybercrime hitting organizations throughout the world is the result of cooperation by hackers working outside the confines of publicly-accessible marketplaces, these underground forums provide a small window into the world cybercriminals occupy. In this report, we concentrated on marketplaces located on the Russian Underground and on English-speaking marketplaces between Q3 2015 and Q1 2016.

Just as we did in the 2013 and 2014 Underground Hacker Reports, we wanted to see if any trends had emerged. For example, did prices for popular hacker goods such as stolen bank accounts, credit cards, and malware go up or down? What about services such as Distributed Denial of Service (DDoS) attacks or hacking company databases? Not only did we answer those questions, but we also found some intriguing new products for sale and some interesting new trends as well.

Price List for Hacker Goods and Services

Credit Cards

	Price in 2013	Price in 2014	Recent Prices
Visa and MasterCard (U.S.)	$4	$4	$7
Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data	$12	$12	$15
Visa Classic and MasterCard (Canada, Australia, and New Zealand) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$25
Visa Classic and MasterCard Standard (EU) with Track 1 and 2 Data	$28	$28	$40
Visa Classic and MasterCard Standard (U.K) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$40
Visa Classic and MasterCard Standard (Japan and Asia) with Track 1 and Track 2 Data	$28	$28	$50
Premium Visa and MasterCard (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Visa and MasterCard (EU and U.K.) with Track 1 and 2 Data		$23 (V); $35 (MC)	$50 – $60
Premium Visa and MasterCard (Canada, Australia and New Zealand) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$35 for V and MC
Premium Visa and MasterCard (Japan and Asia) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$80 for V and MC
Premium American Express Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Discover Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
VBV (U.K., Australia, Canada, EU and Asia)	$17 – $25	$28	$25

Hacking Email and Social Media Accounts

	Recent Prices
Popular U.S. Email Accounts (Gmail, Hotmail, Yahoo)	$129
Popular Russian Email Accounts (Mail.ru, Yandex.ru, and Rambler.ru)	$65 – $103
Popular Ukranian Email Accounts (Ukr.net)	$129
Popular U.S. Social Media Accounts	$129
Popular Russian Social Media Accounts (VK.ru and Ok.ru)	$194
Corporate Email Accounts	$500 per mailbox
IP address of Computer User	$90

Tools

	Price in 2013	Price in 2014	Recent Prices
Remote Access Trojans (RATs)	$50 – $250	$20 – $50	$5 – $10
Crypters	N/A	$50 – $150	$80 – $440
Angler Exploit Kit			$100 – $135

Identities, Passports, Social Security Cards and Other Documents

	Price in 2013	Price in 2014	Recent Prices
US Fullz	$25	$30	$15 – $65
Fullz (Canada, U.K.)	$30 – $40	$35 – $45	$20 (Canada) $25 (U.K.)
U.K. Passport Scan			$25
Physical Counterfeit Passports (non-U.S.)	N/A	$200 – $500	$1,200 to $3,000 (European)
Physical Counterfeit Passports (U.S.)			$3,000 to $10,000
Templates for U.S. Passports			$100 – $300
New Identity Package, including scans of Social Security Card, Driver's License and, matching utility bill		$250; matching utility bill an additional $100	$90
Physical Counterfeit Social Security Cards		$250 – $400	$140 – $250
Scans of Counterfeit Driver's License			DL Scans $14 – $20 (U.S.) $14 (U.K., CANADA)
Physical Counterfeit Driver's License (France)			$238
Physical Counterfeit Driver's License (U.S., U.K., Germany, Israel, International Driver's Permit)		$100 – $150	$173

Online Accounts

	Recent Prices Price based on account balance
Popular U.S. Online "Business" Payment Account Credentials	Ranges from $20 – 149
Transfer Funds from Popular Online Payment Account to Buyer's Account of Choice	$750 cost $226 $1,500 cost $377 $1,520 cost $385 $2,290 cost $573 $2,999 cost $750 $3,799 cost $950
Popular U.S. Online Payment Account Credentials	$330 cost $80 $400 cost $160 $500 cost $240 $600 cost $320 $950 cost $600

Bank Accounts; Airline and Hotel Points

	Recent Prices
Bank Account Credentials	Price based on account balance
Bank accounts — ANZ (Australia)	$18,000 cost $4,750
Bank accounts — ANZ (Australia)	$22,000 cost $2,250
Bank accounts — ANZ (Australia)	$62,567 cost $3,800
Bank accounts with no balance listed — Turkey, Sweden, Norway, Romania, Bulgaria, Croatia,	$400 (flat fee)
Bank accounts — (U.K.)	$27,003 cost $2,000
Bank account — (U.S.)	$1,000 cost $40
Bank account — (U.S.)	$2,000 cost $80
Bank account — (U.S.)	$4,000 cost $150
Bank account — (U.S.)	$7,000 cost $300
Bank account — (U.S.)	$15,000 cost $500
High Quality Bank Accounts with Verified, Large Balances of $70,000 – $150,000	6% of the balance of the account
Large U.S. Airline Points Accounts — varies based on amount	Price based on points in account 1,500,000 points cost $450 300,000 cost $90 200,000 cost $60
Large Middle East Airline Points Accounts — varies based on amount	Price based on points in account 500,000 cost $150 450,000 cost $90 250,000 cost $50
Large International Hotel Chain Points Account	Price based on points in account 1,000,000 points cost $200 400,000 cost $80 300,000 cost $60 200,000 cost $40 100,000 cost $20 50,000 cost $10

Hacking Services

	Price in 2013	Price in 2014	Recent Prices
Hacking Tutorials	N/A	$1 each to $30 for 10 (depending on the tutorial)	$20 to $40 for multiple tutorials
Hacking Website (stealing data)	$100 – $300	$100 – $200	$350
DDoS Attacks	Per Hour: $3 – $5 Per Day: $90 – $100 Per Week: $400 – $600	Per Hour: $3 – $5 Per Day: $60 – $90 Per Week: $350 – $600	Per hour: $5 – $10 Per Day: $30-$55 Per Week: $200 – $555
Doxing	$25-$100	$25-$100	$19.99

Russian Hackers Expand their Working Hours and Use Guarantors to **Ensure Customers' Happiness**

In our December 2014 report, we revealed that our security experts saw a big focus by the underground hackers on providing excellent customer service. Interestingly, that trend has not died out, but rather increased, especially on the Russian Underground forums, where we saw many of the hackers expand their working hours to include weekends and even promising to be available 24x7. For example, one hacker posted that he operates from 11:00 a.m. to 11:00 p.m. Monday through Thursday and 11:00 a.m. to 6:00 p.m. on Friday (taking an hour for lunch and an hour for dinner during these days), and is open for business on Saturday and Sunday between noon and 3:00 p.m. Another hacker seen advertising Distributed Denial of Service (DDoS) attacks states in his ad that he is: "Always online 24/7." Now that is customer service.

Another trend our security experts noticed on the Russian Underground is that the majority of the sellers they tracked are now offering customers the ability to work through "Guarantors." A guarantor for a legitimate transaction typically ensures that the exchange of data and payment takes place fairly by holding money and the product before distributing it to both parties involved in the transaction. The guarantor typically gets a small percentage of each transaction. Certainly, utilizing a "Guarantor Service" gives a prospective customer who has not done business with a seller previously more confidence that the data or

A hacker seen advertising Distributed Denial of Service (DDoS) attacks states in his ad that he is: "Always online 24/7."

Now that is customer service.

service they are purchasing will be satisfactory. In fact, one seller of email hacking services states in their ad: "Work through the Guarantor Service is welcome," and "no-prepayments, you pay only for visible results—we will present the necessary proof." The hackers' willingness to work through a "guarantor" seemed to indicate that the sellers on the Russian Underground aim to please and will do what it takes to ensure they continue to deliver the very "Best Customer Service."

Our security experts also saw lots of hacker/sellers advertising their outstanding attributes. One seller who was offering customers the service of "hacking into organizations" states in their ad:

> "Why choose us?
>
> - Professionalism. We are working only with the best technologies and developments
> - Experience. We are constantly improving our technology in this area and are adopting new advanced solutions
> - Quality. Our expertise allows us to exploit various vulnerabilities on the target servers, making our attacks the most effective.
> - Power. With the continuous improvement of our technology, we have huge abilities
> - Anonymity. You can be sure that any information regarding your order will not be shared with a third party.
> - Honesty. We provide conditions for repayment of funds, if you are not entirely satisfied.
> - Provide free-trial attacks on web servers.
> - We are Trustworthy and Professional."

Our security experts also saw several hacker/sellers advertising their outstanding attributes.

Hacking Services **for Hire**

There is no shortage of hackers offering to hack into the personal email account of your choice.

Hacking Email Accounts

On the Russian Underground, just as on other underground marketplaces, there is no shortage of hackers offering to hack into the personal email account of your choice, including Gmail accounts, Yahoo accounts, as well as accounts with popular Russian email providers such as Mail.Ru, Yandex.Ru, and Rambler.Ru. One hacker offering these services proudly lists why a buyer should choose them.

The accolades he/she lists, include:

- Operational performance of my work; can hack into the most complex of systems
- No prepayments, you pay only for visible results — we will present the necessary proof.
- We provide results from 1 hour to 7 days
- Complete Confidentiality—the victim will not even notice that their email account has been hacked
- Burglary of the email account will be carried out without changing the password, the victim, will access their email account noticing no suspicious activity
- Regular customer discounts
- Working through a guarantor service is welcome!
- Provide the email address you want to hack and within a few hours or just a few days (for severe cases), we will give you the results and evidence of our service's smooth operation.

The hacker goes on to state that, "Buyers have, at their disposal, access to all of the following items after he/she has hacked the email account of the victim":

- Access to all the websites registered by the owner of the email account
- Personal correspondence and confidential data of the victim
- Exact details regarding the date/time of the email account hack
- Ability to make changes to the victim's mailbox—including changing the username and password, ability to change the design of the email account and even remove the email account permanently

Rates the hacker charges for hacking an email or social media account are listed in Table 1. The seller accepts payment via WebMoney and Yandex.Money.

DDoS Attacks; Free 5-10 Minute DDoS Tests Offered

Providing DDoS Attacks remains a popular service offered by hackers on the underground hacker markets, including the Russian markets. One of the hackers selling their DDoS skills states in a forum that he is happy to "offer their services so as to address the websites and forums of your competitors using DDoS Attacks, and that they will take on virtually any projects ranging from servers, which have weak protection to servers with high protection!" They go on to state that "their service is a quick solution to your problems with competitors and enemies."

Still another hacker selling DDoS services offers "an attack on any computer port that you specify with complete anonymity." The hacker also promises that "long time, regular customers and wholesale customers receive big discounts," and that he is online 24X7. He offers the "best value for the money," and if you have any problems, "a money back guarantee." He then goes on to state that the "services does not violate the law," which our security experts found quite amusing.

The security experts did find that most of the Russian hackers they observed who were offering DDoS Attack services were willing to perform a free 5- to 10-minute DDoS test for customers.

They discovered that DDoS Attack services on several of the Russian Underground markets cost the following:

- $5 per hour
- $50 per day
- $200 to $350 per week (the higher price is charged if the target website has anti-DDoS protection installed)
- $1,000 per month

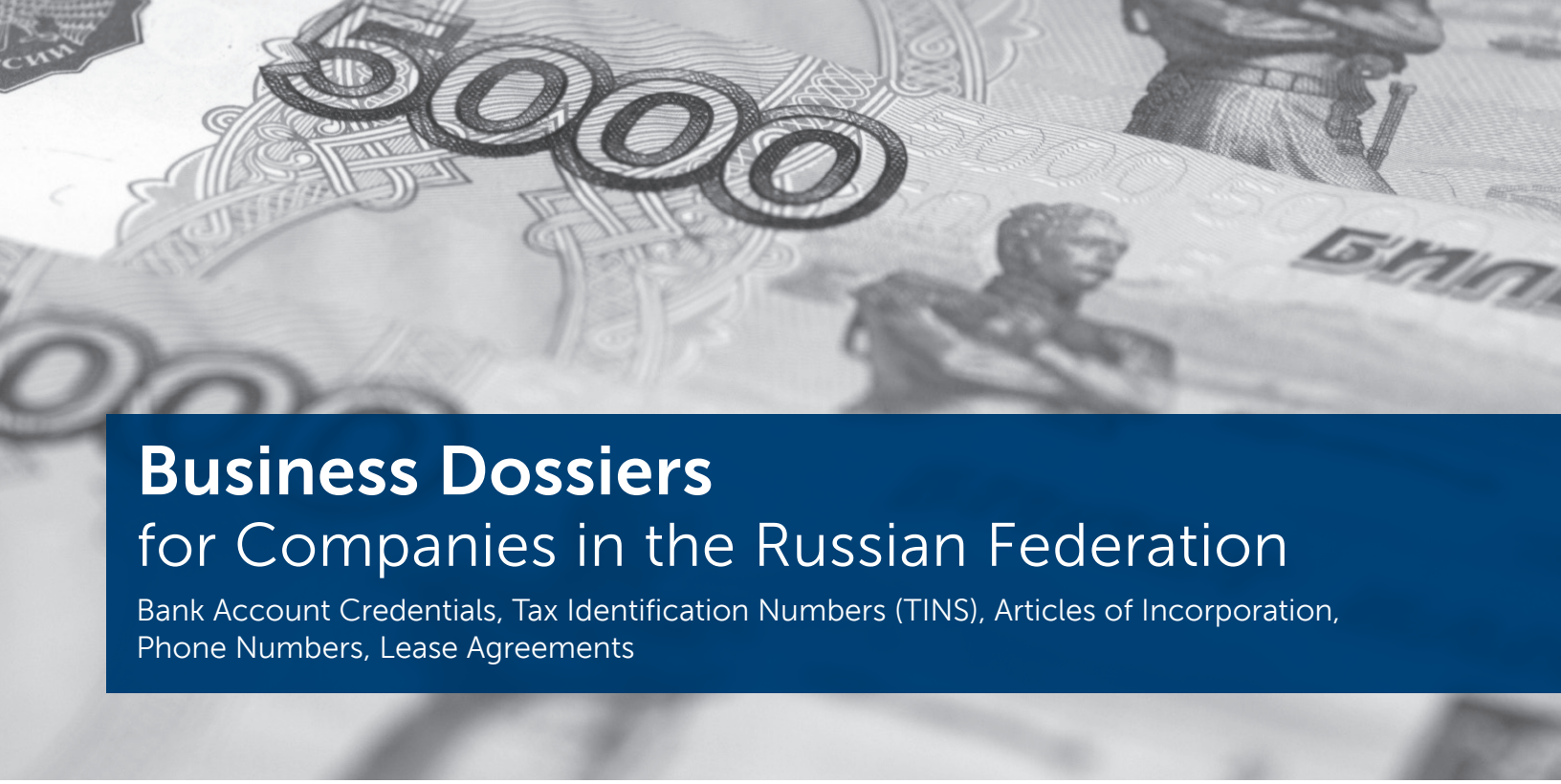
Plus, most of the hackers offer a variety of DDoS attacks including:

- UDP Flood
- TCP Flood
- HTTP/HTTPS Flood
- SYN Flood

The hackers accept WebMoney and Yandex.Money, and some accept Bitcoin.

Table 1: Rates for hacking social media and email accounts

Mail.ru	5,000 rubles (approximately $65)
Yandex.ru	7,000 rubles (approximately $90)
Rambler. Ru	8.000 rubles (approximately $103)
Ukr.net	10,000 rubles (approximately $129)
Gmail.com, Yahoo.com, Hotmail.com	10,000 rubles (approximately $129)
Facebook.com	10,000 rubles (approximately $129). Please note: the victim's password stays the same.
IP address of computer user	7,000 rubles (approximately $90)
Corporate email account	$500 per mailbox
VKontakte (VK) social media account	15,000 rubles (approximately $194)
Odnoklassniki (OK.ru) social media account	15,000 rubles (approximately $194)



Business Dossiers
for Companies in the Russian Federation

Bank Account Credentials, Tax Identification Numbers (TINS), Articles of Incorporation, Phone Numbers, Lease Agreements

One of the most interesting items we found for sale on the Russian Underground were full business dossiers on companies located within the Russian Federation. The hackers are selling information and documents from Russian organizations, including all of the credentials associated with a company's various bank accounts (account numbers, logins, passwords, tokens). They are also providing the company's original articles of incorporation, lease agreements, and the company's Tax Identification Number (TIN), also known as an Employer Identification Number. TIN is a number used to identify entities for tax-related purposes such as filing tax returns, or other actions such as opening a bank account.

With this full dossier, they are also providing the passport for the company officer affiliated with the bank accounts, and the business phone number associated with the bank accounts. Our security experts had never seen a full business dossier being sold for any companies, much less for Russian organizations. What could one do with this type information besides potentially siphon off all the money in the company's bank accounts? Well, the possibilities are extensive. If the company has good credit, there is certainly the potential for those possessing this data to apply for hefty bank loans, high-limit credit cards, car loans and other lines of credit.

It is not that surprising to see Russian organizations' bank account credentials and sensitive company data being sold on the Russian Underground. In November 2015, Dell SecureWorks discovered that one of the most popular Banking Trojans, Tinba, is being used by hackers to target customers of some of the top banks and financial firms in Russia. It would not be a big stretch for these same hackers to also target valuable corporate data, in addition to a company's bank credentials.

According to one hacker/seller of such data, buyers get two full days to review the company documents, and the seller is also willing to work through a "Guarantor Service." The hacker/seller states that they accept payment through QIWI or Yandex.Money. The price for the Russian company dossiers ranges between 40,000 ($547) and 60,000 rubles ($822)*.

The price for the Russian company dossiers ranges between 40,000($547) and 60,000 rubles ($822).

*Please note: all prices listed in this report are in U.S. dollars unless otherwise indicated.

Hacker Goods for Sale

Bank Accounts, Popular Online Payment Accounts, Airline Points Accounts, Credit Cards, Hacker Tutorials...You Name It

The smaller the balance in the account, the higher the seller's fee. For example, one U.S.-based account with a balance of $1,000 was selling for $40, while another U.S.-based account with a $50,000 balance was selling for $587.

Internet Bank Account Credentials

Just as there is no lack of credit cards for sale on the underground markets, there is no lack of bank account credentials for sale. Our security experts saw stolen bank credentials for accounts located in the U.S, U.K., Denmark, Sweden, Croatia, Turkey and Australia. The hackers were selling the credentials for anywhere from 1 percent up to 5 percent of the account balance. The smaller the balance in the account, the higher the seller's fee. For example, one U.S.-based account with a balance of $1,000 was selling for $40, while another U.S.-based account with a $50,000 balance was selling for $587. However, our security experts did come across credentials for accounts based in the U.K. and Europe that were selling for a flat $400. In that case, the seller did not list the balance in the account publicly. One wonders if bank account credentials, like credit cards in the U.K. and Europe, are more expensive because they are harder to come by due to there being fewer breaches involving this type of data.

Online Payment Accounts Sell for a Hefty Fee

Just as one's bank account credentials reap hefty prices on the underground, so do account credentials for popular online payment accounts because in many ways they are very similar to a bank

account. However, many online payment accounts do not have the same level of fraud alerts that larger banks employ. We found hackers selling the credentials for "personal" and "business" online payment accounts. In fact, these credentials, depending on the balance in the account, often sell for more than bank account credentials, in regards to the percentage of the balance charged. Cashing out these types of accounts, especially if the account owners do not implement the two-factor authentication option, can be very simple for the criminal. Our security experts found numerous Hacker Tutorials outlining how one can easily cash out these accounts, especially when there is actual cash sitting in the accounts. Our security experts found hackers willing to transfer the balances of online payment accounts to the account of your choice, whether it be a bank account, an online payment account, and so on. This is not cheap of course, since they are taking the risk. For example, one hacker was willing to transfer $750 for $226, while the same hacker was charging $377 to transfer $1,500 from an online payment account.

Need a Cheap Vacation Anyone? Airline and Hotel Points Accounts on the Auction Block.

If you think you are the only one interested in your frequent flyer points and hotel points, think again. As we have previously pointed out, hackers have a way of monetizing almost any piece of data, and this includes your frequent flyer accounts and your hotel points accounts. Our security experts found hackers on English-speaking sites selling frequent flyer account credentials for a variety of large U.S.- and Middle East-based airlines. The prices were for the following: an account with 1,500,000 points cost $450, while another frequent flyer account with 300,000 points cost $90. The hackers were also selling credentials for hotel accounts, associated with many of top hotel chains. For example, a brand-name hotel account with 100,000 points sells for $20, and an account with 50,000 points runs $10. Clearly, the airline points accounts are deemed more valuable by the sellers than the hotel points, though $10 here and $20 there can add up.

One is probably asking why would a scammer want to purchase someone's frequent flyer or hotel points account number? Well, the answer is simple. There are legitimate websites where one can trade their airline and hotel points for gift cards. For example, on the site https://www.points.com/#/, 6,412 reward points for a major U.S. airline could be exchanged for a $25 gift card to a number of popular chain restaurants, while 12,294 points was enough for a $50 gift card to a high-end retail store.

Scammers also have the potential of cashing out airline points for cash via online businesses called mileage brokers. Although that activity is deemed a no-no with the airlines, scammers are clearly not worried about breaking any of their rules since they are purchasing stolen points in the first place. One such site offering cash for points is called http://flipmymiles.com/. On their FAQ, they state:

> **Q: How much will I get paid?**
>
> This depends on the type of points or miles sold but we pay at the most competitive industry rates ranging upwards of a penny to the point. To give you an idea, we pay anywhere from $1,000 to $1,500 for a 100,000 points. Compared to the $500 to $1,000 your credit card company would pay you, that's quite the difference.

Credit Cards for Sale

As in prior years, the market for stolen credit and debit cards is bustling and knows no geographic bounds. Throughout the dark web, interested buyers can find credit card information from countries all over the world, from the U.S. to Japan to Australia. And while the damage a stolen credit card can potentially do is significant, the cards themselves are relatively cheap – a stolen U.S. MasterCard or Visa card (without Track 1 or Track 2 data) could be purchased for just $7, a slight increase from 2014 and 2013 when those cards sold for $4.

Not surprisingly, cards with Track 1 and Track 2 data were more expensive, and in some cases rose significantly in price compared to previous years. For example, while our security experts found prices for such cards from the U.S. selling for as little as $12 in 2014, recently, cybercriminals were spotted selling U.S. Master Card and Visa cards with Track 1 and Track 2 data for $15. While cards with Track 1 and Track 2 data from the UK sold for $19–$20 in 2014, Dell SecureWorks has observed Master Card and Visa cards from the UK with that data selling for $40. In Japan meanwhile, Visa and Master Cards with Track 1 and Track 2 data sold for $50.

Premium cards from each of the major brands were the most expensive, reaching $30 for

MasterCard and Visa cards from the U.S. with Track 1 and Track 2 data. Those same cards from the U.K. sold for as much as $60, while in Japan the price was $80.

As an additional boost to fraudsters, underground marketplaces make VBV (Verified by Visa) data available as well. A security measure meant to protect cardholders, VBV is another password or piece of data assigned to Visa cardholders to defend against fraud. VBV data for cardholders in the U.K., Asia, Canada and Australia dipped slightly in value compared to 2014, dropping from $28 to $25.

Stolen Identities, Passports, Social Security Cards and Other Documents

Identity theft is the stock and trade of many criminal hacker groups, and for good reason. A scammer who can impersonate an unsuspecting victim can open the door to all kinds of crimes, such as bank fraud and insurance fraud. For that reason, documents that can be used to impersonate another individual, especially those with impeccable credit, are worth their weight in gold.

Often, this type of information is sold in packages. The prices for these packages — as well as the items individually — vary from market to market. In one instance, our security experts discovered a package that included a social security number, driver's license and a matching utility bill being offered for $90.

Relatively cheap packages of data known as Fullz are also bought and sold on the criminal underground. Fullz — what hackers call a dossier of credentials for an individual that can be used to commit fraud — typically include data such as names, addresses, and social security numbers in combination with one or more of the following: bank account information, online banking credentials, or credit card numbers. Recently, our security experts saw Fullz selling for $15 for a U.S. victim.

There was a difference in pricing between when cybercriminals offered physical counterfeit social security cards or scans of cards, versus when they offered just the social security numbers. The cost of physical counterfeit social security cards spotted by Dell SecureWorks ranged from $140 to $250, a significant drop off from 2014, when those items were sold for between $250 and $400 each. A physical counterfeit Canadian Social Identification Number card — which is similar to a social security number in the U.S. — was observed being sold by cybercriminals out of China for approximately $173.

The price of driver's licenses varied, too. A physical counterfeit French driver's license was spotted being sold by one vendor for approximately $238, while German, U.S., Israeli, U.K. and international driver's permit sold for about $173.

Currently, the price for an actual U.S. passport ranges from $3,000 to as high as $10,000. The higher the quality, the higher price. Templates for U.S. passports sold anywhere from $100 to $300, and the buyer must find their own printer. Passports for European countries have been seen going for between $1,200 to $3,000. Beyond financial scams, the trafficking of these kinds of items can have other potential implications as well. For example, an ABC report in December 2015 noted that authorities in the U.S. suspected that the terrorist group ISIS had the ability to print legitimate-looking Syrian passports so that their members could travel undetected.

These are not the only documents worth their weight in gold to criminals trafficking in stolen identities. Utility bills are also offered in many deals as part of the package – for the price of the $90 mentioned above for example, one seller offered a scan of a social security card, a driver's license (for California, Nevada, Connecticut, or Florida) and a matching utility bill. According to our experts, the price for such packages depends on the number of documents involved, and in some cases could go up if the seller is providing additional help creating

Table 2: Rates for premium credit cards with Track 1 and Track 2 data

Credit Card	Recent Prices*
American Express (U.S.)	$30
Discover Card (U.S.)	$30
MasterCard and Visa (Australia)	$35
MasterCard and Visa (U.K.)	$50 to $60
MasterCard and Visa (Japan)	$80

*All prices are in USD

the identity and guiding the buyer through the process.

Shopping Mall for Malware

Malware is still an effective weapon in the holster of hackers targeting end-users. Remote access Trojans (RATs) are malware programs that have a backdoor that hackers use to gain administrative control of a compromised machine. Some of the cheaper and more accessible RATs on the forums our security experts examined included: BlackShades, AlienSpy, and DroidJack. Some RATs were spotted being sold for between $5 to $10, compared to $20 to $50 in 2014. Typically, the longer a RAT has been accessible on the underground, the cheaper it is. Hackers often look for free or cheap RATs to run through programs called crypters that encrypt the malware and make it more difficult for security programs to detect. Crypters were sold for prices ranging from $80 to $440. Among the most popular ones were Aegis, Inferno Worm, Beef and Spoof and Pandora rat. It is not clear what caused the spike in the Crypter prices that our security experts saw.

Exploit kits are also a common item on the digital shelves of the underground market. Exploit kits seek to identify and exploit software vulnerabilities on targeted computers. They are typically designed to be modular and are often updated to add newer exploits to replace older ones. One of the most popular exploit kits continues to be Angler, which first appeared in 2013, and in 2015 was linked to the use of several zero-day vulnerabilities in the Adobe Flash Player. The Angler exploit kit was observed selling for between $100 and $135.

How-to for Hackers

Hackers are not just interested in selling malware and stolen information. They also sell tutorials to help other budding criminals launch their own operations. In 2014, the cost for the tutorials ran from $1 each to $30 for 10, depending on the tutorial. Recently, buyers could expect to purchase multiple tutorials for between $20 and $40. The tutorials cover a number of subjects, such as Denial of Service (DoS) Attacks, cracking Wi-Fi, Crypters and phishing. In some cases, these tutorials explain for example what a Crypter, a RAT and an exploit kit is, how are they used and how much hackers should pay for these hacker tools. Taken in combination with the easy-to-use tools, the tutorials certainly help to lower the barrier to entry for new hackers wanting to break into cybercrime.

The price for an actual U.S. passport ranges from $3,000 to as high as $10,000. Templates for U.S. passports sell anywhere from $100 to $300, and the buyer must find their own printer.

Is ATM Skimming Passé? **Not on Your Life.**

Although Automated Teller Machine (ATM) skimming was first reported in the news as far back as 2002, anyone who thinks this type of fraud is passé needs to think again.

According to a *Wall Street Journal* article from spring 2015, "Criminals are stealing card data from U.S. automated teller machines at the highest rate in two decades, preying on ATMs while merchants crack down on fraud at the checkout counter."

The story was based on statistics released by FICO, a credit-scoring and analytics firm. FICO found that debit-card compromises at ATMs located on bank property had jumped 174% from January 1 to April 9, 2015, compared with the same period in 2014, while successful attacks at nonbank machines soared by 317%. Most of this activity can be directly attributed to the use of ATM skimming technology.

ATM skimming is a method used to capture data from the magnetic stripe on the back of a debit card or credit card. Capturing the account data is done via a device called a skimmer. Many of the skimmers are smaller than a deck of cards and are typically fastened over the top of the ATM's factory-installed card reader, so it grabs your card details when you slip your debit or credit card into the card slot. Just as organizations look for advanced technology to improve their operations, so do criminal enterprises. In July 2014, the European ATM Security Team discovered criminals using several mini-skimmers that were so small and slim that they fit entirely into the ATM's card reader slot undetected. On top of that, the skimmer runs on a $3 lithium coin battery.

Skimming thieves not only have to capture the data on your card, but they must also capture your card's four-digit PIN number. This is typically achieved by rigging up a pin-hole camera overhead to capture your PIN number as you enter it or by positioning a keylogging device over the keypad itself that records your secret PIN as you enter it.

Making ATM Skimming a Not So "Risky Business"

Rigging up a skimmer and a pin-hole camera or keylogging device to an ATM can be risky. One has to wonder why criminals would take that chance when there are plenty of retailers and other businesses sitting on thousands of customer credit card and debit card credentials within their IT networks, and the potential for successfully hacking into some of these caches is pretty high. However, for those criminals who are "not so savvy at computer hacking," two technical advancements have played in their favor. One is the addition of Bluetooth functionality to skimmers and ATM PIN pad keyloggers. Until a couple of years ago, thieves had to return to the ATMs they had rigged and retrieve their skimmers and accompanying memory chips, as well as their pin-point cameras. However, most modern skimmers have the option of adding Bluetooth capability, allowing thieves to position themselves 30 to 40 feet away and pick up the stolen data wirelessly.

The second advancement is the increasing availability of reasonably priced, high-quality 3D printing services. These offer low-tier criminals the opportunity to compete with more professional criminal organizations while lowering their risk and their costs.

The ATM skimming devices our security experts observed for sale on the English-speaking hacker marketplaces ran between $400 and $1,775 per skimmer, depending on the make and model of the ATM it worked with. All of the sellers gave buyers the option of adding Bluetooth functionality to the skimmers they sold, typically for an additional $500. Interestingly, a Bluetooth device purchased from a legitimate electronics outlet tends to run $50 to $60. So it appears the scammers, selling their Bluetooth devices for an additional $500, certainly stand to make a nice profit.

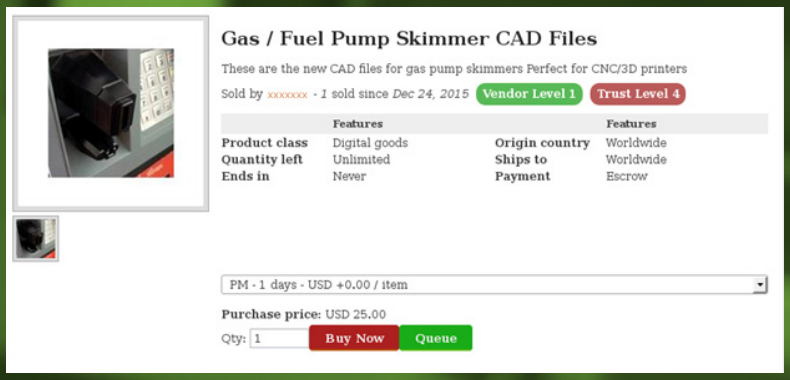
If a buyer also wants to add a micro-camera to their skimmer, that costs an extra $275. Micro-audio hardware runs $300, while GSM functionality runs a whopping extra $800. GSM functionality means the device includes a SIM card and GSM radio and uses commercial cellular data networks to wirelessly connect the skimming device to the Internet. This allows them to stream the stolen card data in real-time directly from the compromised ATM to the criminal's servers located anywhere in the world. If a criminal elects to use a PIN pad keylogger to capture the cardholders' PIN numbers, they can purchase the computer design files and software for one keylogger device for $125. The seller also advertises that they can "hook up" a buyer with a production facility that can produce the keylogging device.

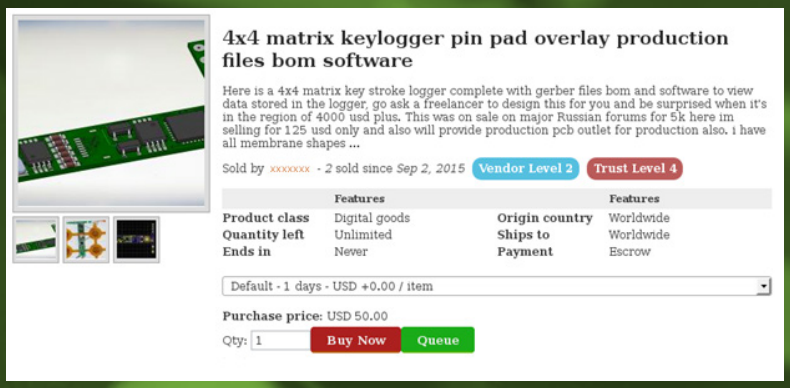
So if a scammer installs a skimmer and a keylogger PIN pad device onto an ATM and hooks up Bluetooth to both devices, then how does the scammer get the card data? Easy. He or she merely needs to use a matching Bluetooth communication module that plugs into a laptop to remotely retrieve the card data and corresponding PIN numbers. The criminal can literally be 30 to 40 feet away, sitting comfortably in their car or in a cushy lobby chair, stealing all of your ATM account credentials. If they purchased the GSM option mentioned above, they can pull the data from anywhere on the planet with a cell tower signal.

The criminal can literally be 30 to 40 feet away, sitting comfortably in their car or in a cushy lobby chair, stealing all of your ATM account credentials. If they purchased the GSM option mentioned above, they can pull the data from anywhere on the planet with a cell tower signal.

The criminal has an array of ways to cash out on this valuable data, too. They can opt to transfer the data onto blank cards and then use them at ATMs to make withdrawals, often emptying the victim's bank account. Or, they can purchase high-end, popular items from online retailers, or in-person with your debit or credit card number. They can then turnaround and sell these expensive goods for below retail price. Or, they can simply sell the credentials to other criminals shopping on the underground marketplaces.

You might be asking yourself: What about the new chip technology that is being embedded into credit and debit cards, making it harder for criminals to counterfeit cards? Well, although financial institutions in the





Criminals are taking advantage of recent improvements in the speed and quality of 3D printing technology.

U.S. are working to update debit and credit cards with this technology, there are still a good number of ATMs that still are not equipped to take the chip-enabled cards, which makes those ATMs more vulnerable to skimming and counterfeit cards.

3D Printing of ATM Skimmers

Our security experts found a wide array of 3D printed card skimmers (including most of the popular ATM makes and models) for sale on the English-speaking and Russian hacker marketplaces. For several years now, there have been card thieves who have used 3D printers to manufacture card skimmers that fit snugly over the card slots on ATMs, gas pumps and in-store point-of-sale (PoS) devices. However, 3D printing has often been slow and expensive, producing less-than-convincing replica parts.

That said, it is apparent with the increase of 3D printed skimmers on the underground markets that the criminals are taking advantage of recent improvements in the speed and quality of 3D printing technology. In fact, one seller states in his online ad that promotes skimmers for 13 of the most popular ATMs, "All my skimmers are 3D printed in house at 25 micron, using our own methods, and all models are gloss finished to perfection...." Now, we do not know if his claims of "perfection" are true; however, we did find that he was charging $275 less than one of his competitors who sells the same style of skimmer but that had been conventionally manufactured. And we even found one scammer selling a package of 3D design files of skimmer fronts for some of the most popular ATMs — new and old models.

He also promises to connect buyers to a 3D printing factory, stating, "Don't worry as the factory is cheap and discreet, and all the pieces are custom made and tested in the real world, every piece have been designed to fit perfect, this is no bull...."

Security Measures for **Protecting Against Cyber Threats**

In order to protect your valuable information from this type criminal activity, it is essential that organizations, as well as individuals, stay aware of the threat and implement protective measures to ward against the loss of financial data, PII and intellectual property. Dell SecureWorks has outlined a set of key security steps for both organizations and individuals and advises a layered approach to security.

Steps for Organizations

Implement Secure Practices

- Educate your employees on how to spot computer security threats, especially spear phishing attempts.
  - A key protective measure is to educate your employees to never click on links or attachments in emails, even if they know the sender. Employees should check with the sender prior to clicking on the email links or attachments. Email and surfing the web are the two major infection vectors.
- Mandate the use of two-factor authentication for all remote access solutions and for all company employees and business partners (anyone authorized to access your corporate network). This provides a second layer of security to prevent intrusions in the event credentials are compromised.

Mandate the use of two-factor authentication for all remote access solutions and for all company employees and business partners

- Remove Local Administrator rights for users. Attackers often take advantage of users that have of elevated privileges
- Back up all data (not just critical data), and document and rehearse contingency plans
- Audit privilege domain account usage, including administrator and service accounts
- Segment sensitive data on the network and closely monitor choke points

Build Strong Technology Defenses

- Install firewalls around your network and web applications
- Deploy Intrusion Prevention Systems or Intrusion Detection Systems (IPS/IDS), which inspect inbound and outbound traffic for cyber threats and detect and/or block those threats
- Host Intrusion Prevention Systems (IPS)
- Use Advanced Malware Protection solutions for the endpoint and network
- Employ vulnerability scanning
- Institute 24x7 log monitoring, and web application and network scanning
- Take advantage of security intelligence around the latest threats (people working on the latest threats in real time, human intelligence)
- Use encrypted email

We also advise organizations with valuable data to implement an endpoint security solution across their environment which is focused on threat actor behavior and determining if an activity within one's network is malicious or not. The solution should be able to:

- Assess the host for known and unknown threats
- Monitor for threats attempting to maintain persistence
- Monitor process creations and associated files
- Examine thread injection events looking for adversaries moving between processes
- Examine network connection data at the host level to identify suspicious communications being sent to and from the host
- Monitor DNS activity at the host level

Steps for Individuals

For Safe Banking and Online Bill Pay

- Use a computer dedicated only to doing online banking and bill pay. That computer or virtualized desktop should not be used to send and receive emails or surf the web, since web exploits and malicious email are two of the key malware infection vectors.
- Be extra cautious when withdrawing money from an ATM:
  - Cover the keypad with your other hand when entering a PIN
  - Try to avoid nonbank locations where the ATM is in a hidden location that thieves could easily access without being detected
  - Check your bank and credit card statements regularly for fraudulent activity
- Consider subscribing to a 3 in 1 credit monitoring service to alert you when new credit or bank accounts are applied for, credit balances go over the norm, etc.

Using Your Computer Safely

- Avoid clicking on links or attachments within emails from untrusted sources. Even if you recognize the sender, you should confirm that the sender sent that email, before clicking on any links or attachments.
- Make sure your anti-virus software is current and can protect against the latest exploits. Also, make sure that your anti-virus vendor has signatures for detecting the latest Trojans and that you have the most up-to-date anti-virus protections installed.
- Do not use "trial versions" of anti-virus products as your source of protection. Trial versions of anti-virus products are good for testing products, but do not continue to use the trial version as your protection for your home or work PC. The danger is that the trial version does not receive any updates, so any new Trojan or virus that is introduced after the trial version was released will have total access to your PC.
- Make sure you have your security protections in place. Software patch management is key. It is critical that you install updates for your applications and for your computer's operating system as soon as they become available.
- Be cautious about installing software (especially software that is too good to be true — e.g., download accelerators, spyware removal tools), and be conscientious about pop-ups from websites asking users to download/execute/or run otherwise privileged operations. Often this free software and these pop-ups have malware embedded.

It is critical that you install updates for your applications and for your computer's operating system as soon as they become available.

Conclusion

Like any other market in a capitalist system, the business of cybercrime is guided by the supply and demand for various goods and services waxes and wanes. Unfortunately for the law abiding public, both sides of that equation remain strong, with everything from credit cards to hacker-for-hire services being sold online. ATM skimming jumped during the year, and the skimmers necessary to perform that kind of scam were of particular interest to many cybercriminals and were seen selling for as much as $1,775. Meanwhile, malware was much cheaper, and continues to offer a low barrier to entry for cybercriminals looking to steal information such as bank account credentials and other data that can be turned into money. This also includes items like airline rewards points that can be exchanged online for gift cards to restaurants, retailers and others. Another hot commodity is information that can be used to commit identity fraud, such as social security cards, utility bills, and driver's licenses.

But prices and goods are not the only way sellers are distinguishing themselves. There also continues to be a focus on salesmanship. Compared to the report last year, our security experts noted this time around that many hackers were expanding their working hours to include weekends and even promising to be available 24 hours a day.

While law enforcement remains vigilant, business appears to be booming, and underground forums continue to thrive.

Glossary of Terms

Credit Card Track 1 and 2 Data — Track 1 and 2 data is information that is contained in digital format on the magnetic stripe embedded in the back of the credit card. Some payment cards store data in chips embedded on the front side. The magnetic stripe or chip holds information such as the primary account number, expiration date, card holder name, plus other sensitive data for authentication and authorization.

Distributed Denial of Service (DDoS) Attacks — DDoS Attacks are the act of throwing so much traffic at a website, it takes it offline.

Fullz — Fullz is a dossier of credentials for an individual, including Personally Identifiable Information (PII), that can be used to commit identity theft and fraud. Fullz usually include: full name, address, phone numbers, email addresses (with passwords), date of birth, social security number (SSN) or Employee ID Number (EIN), and one or more of the following: bank account information (account and routing numbers, account type), online banking credentials (varying degrees of completeness), or credit card information (including full Track 2 data and any associated PINs).

Odnoklassniki — This is a social network service for classmates and old friends. It is popular in Russia and former Soviet Union.

Personally Identifiable Information (PII) — This is information that can be used on its own or with other information to identify, contact or locate a single person, or to identify an individual in context. Some examples of PII are a person's full name, address, birthdate, driver's license number, telephone number and email address.

Qiwi — This is a publicly traded Russian payment service provider headquartered in Nicosia (Cyprus), that operates electronic online payment systems primarily in Russia, Kazakhstan, Moldova, Belarus, Romania, the U.S and the United Arab Emirates.

VBV (Verified by Visa) — VBV works to confirm an online shopper's identity in real time by requiring an additional password or other data to help ensure that no one but the cardholder can use their Visa card online.

VKontakte — This is Europe's largest social networking website, with more than 100 million users. It is most popular in Russia, Ukraine, Kazakhstan, Moldova and Belarus. Similar to Facebook, VKontakte allows users to message their friends privately or publicly, create groups and public pages, share and tag images and videos, and play games.

WebMoney Transfer (WMT) — This is a global bank settlement system and environment for online business activities, established in 1998. WMT originally targeted clients in Russia and the former Soviet Union, however, it is now used worldwide. The system enables internet users to conduct safe transactions in real time using WebMoney units (WM-units). No bank account or credit card is required to open or operate a WebMoney account. According to WebMoney, thousands of online shops and services accept WebMoney payments. WMT also provides online financial services, P2P payment solutions, internet based trading platforms, merchant services and online billing systems.

Yandex.Money — This is an online payment service. It is especially popular in Russia and describes itself as enabling users to pay anytime and anywhere for mobile services, internet, Skype, games, tickets, home utilities, and many other goods and services. Users can deposit money at bank branches, mobile retailers, payment kiosks, and other points, with most methods being omission free. Yandex Payment Solution is a universal tool for accepting payments online. Merchants can implement this Payment Solution to start accepting payments to a bank account by credit card and other popular methods.

SecureWorks

SecureWorks provides an early warning system for evolving cyber threats, enabling organizations to prevent, detect, rapidly respond to and predict cyber attacks. Combining unparalleled visibility into the global threat landscape and powered by the Counter Threat Platform — our advanced data analytics and insights engine — SecureWorks minimizes risk and delivers actionable, intelligence-driven security solutions for clients around the world.