SecureWorks

Underground Hacker Markets | **DECEMBER 2014**

The Underground Hacker Markets are Booming with Counterfeit Documents, Premiere Credit Cards, Hacker Tutorials and 100% Satisfaction Guarantees

Contents

Summary Of Findings:

Underground Hacker Markets Are Booming

Dell SecureWorks' Counter Threat Unit (CTU) Director of Malware Research Joe Stewart and SecureWorks Network Security Analyst David Shear, who researched the Underground Hacker Markets last year, revisited the hacker underground to see if prices for stolen credit cards, fullz (a dossier of an individual's credentials which can be used to commit identity theft and fraud)*, bank accounts and hacker services had gone up or down in price.

Stewart and Shear found that the most significant difference between the current hacker underground markets and those of 2013, is that the markets are booming with counterfeit documents to further enable fraud, including new identity kits, passports, utility bills, social security cards and driver's licenses. Of course, these types of documents are required to commit many kinds of in-person fraud, whether it is buying high-end purchases with duplicated credit or debit cards at a retail outlet; applying for bank loans; committing check fraud; or attempting government fraud.

Other products, which were especially prominent on the underground markets this year, included Hacker Tutorials. Taking a cue from legitimate businesses, the hackers figured out that not only could they make money performing services, but they could make a little extra money teaching others.

The other notable trend was the number of hackers selling premium credit cards. With so many cyber breaches this year, reportedly involving the compromise of millions of credit and debit cards, it is not surprising to see premium credit cards so abundant in these dark markets.

The last finding of note is the focus by the underground hackers on "Excellent Customer Service." Like any market, which is crowded with multiple vendors selling many of the same products and services, reputation of the vendor becomes critical to running a successful business. It looks like more hackers on the underground have realized this and are trying to distinguish themselves by offering prompt customer service and "100% Guarantees" on the stolen data they are selling.

It is apparent that the underground hackers are monetizing every piece of data they can steal or buy and are continually adding services so other scammers can successfully carry out online and in-person fraud.

*See a complete definition of Fullz in the glossary of terms on the last page of the report.

Counterfeit Credentials for Sale:

New Identities, Passports, Driver's Licenses and Social Security Cards

One of the most notable additions to the Underground Hacker Markets is the number of fake credentials for sale. These include new identity packages, passports, drivers licenses and social security cards. These documents can enable scammers to potentially commit identity theft leading to all kinds of fraud, such as applying for bank loans, check and credit card fraud, and the list goes on.

New Identities for Sale: If you are in search of a new identity, the scammers will provide you with a scan of a working social security card , name, and address for $250. For another $100, they will throw in a utility bill for additional identity verification. These credentials, along with a matching drivers' license, would enable a person to fraudulently apply for government assistance programs, as well as commit other types of fraud.

Counterfeit Passports: Counterfeit non-US passports run between $200 to $500. For this price, you typically receive a scan of the passport, primarily because most businesses will accept a scan of a passport as proof of one's identity, and it is easier for the scammer to produce. This form of identification can be used to assist in all types of fraud: credit card fraud, check fraud, government assistance fraud, etc. Note: US passports were not widely available on the Underground Hacker Markets. We wonder if it is because US law enforcement is believed to frequent the Hacker Underground, and it is too risky for the scammers to deal in US passports?

Fake Drivers' Licenses: US-based drivers' licenses run from $100 to $150 each. Of course, if you want to purchase them in bulk the price per license goes down. A fake driver's license can be used to assist in many types of fraud, including check fraud and credit card fraud. In September of this year, US law enforcement arrested three scammers who were producing and selling fake drivers' licenses, which were reportedly used in connection with "cash out" schemes. These schemes involved stolen credit card information, usually obtained through hacking or ATM skimming operations, which was encoded on to counterfeit credit cards and then used to steal cash from victims' accounts. According to the FBI, from Dec. 30, 2013 to June 23,2014, the conspirators sold 1,514 fake driver's licenses for $232,660.

Counterfeit Social Security Cards: Counterfeit Social Security Cards run between $250 and $400 on average, and similar to the Counterfeit Passports, the scammers offer a scan of the social security cards. Fake social security cards can be used to file fraudulent tax returns, open a variety of financial accounts, etc.

Hacker Training Tutorials

Another popular product line for sale on the Cyber Underground is Hacker Training Tutorials. Not only are hackers getting paid to carry out hacking services, they are now getting paid to teach others how to hack and commit fraud.

The Training Tutorials teach beginner hackers or "newbies," as they are often called by established hackers, how to carry out almost every type of fraud imaginable. Their topics span from how to do "Basic Carding" to "Cashing Out Fullz or Credit Cards via Online Shopping" to "How to do ATM Hacks and Get Much More Money than you Withdraw" to "How to have 100% Successful Bank Transfers."

A manual containing a handful of tutorials explaining a variety of cyber activities can be purchased for $30, while individual training tutorials can run as low as $1. Tutorials on Exploit Kits, Crypters, DDoS attacks, Spam attacks, and phishing are also available. These tutorials not only explain what a Crypter, Remote Access Trojan (RAT) and exploit kit is but also how they are used, which are the most popular, and what hackers should pay for these hacker tools.

Fig. 1
Hacker Tutorials for Sale on the Hacker Underground

Premium Credit Cards for Sale:

(Platinum, Gold, Prestige, Black) Name Your Card Type & Country of Preference

The number of Hacker Markets advertising dumps of Premium Credit Cards (Platinum, Gold, Black, Prestige, etc) and Standard Credit Cards for sale (including Track I and Track II data), from different countries are numerous. Stolen credit cards from the US, Canada, the UK, Europe, Brazil, Argentina and the country of Georgia appear to be especially plentiful. One site advertised Platinum and Gold Master Cards, with Track I and II data, for $35 a piece, while standard, non-US Master Cards, with Track I and II Data, ran $17 a piece. Premium Visa cards ran $23. This same Underground site advertised that they had 14,000,000 US credit cards for sale, 294,000 Brazilian cards, 342,179 from around the world, 212,100 from Canada, 75,992 from the UK, and 26,873 from the European Union.

Another hacker offered Premium Credit credit cards in bulk (without Track I and II data) for the following prices:

10 pieces--$13 each

50 pieces--$12 each

100 pieces--$11.50 each

500 pieces--$11 each

1000 pieces--$10 each (includes a Free Tutorial for a Popular Online Payment Site)

2000 pieces--$9 each (includes a Free Tutorial for a Popular Online Payment Site)

100% Satisfaction Guarantee on Stolen Credit Cards or They Will Be Replaced

Another interesting trend Shear and Stewart found on the Underground Hacking Markets was the hackers' focus on "Excellent Customer Service." Shear and Stewart saw "Satisfaction Guarantees" from numerous sellers. In figure 2, one can see a hacker promising "100% Valid Rate," on the stolen Premium credit cards he is selling. For example, if a buyer purchases 100 credit cards, he ensures that these cards are all "live" (have not been canceled) and "valid". According to the hacker, "All dead ones will be replaced."

The same seller offered "Credit Card Guarantees" which guarantee that if a credit card doesn't pass for a $200 charge, the seller will do a check using Try2Check (a popular underground credit card verifying application), and should the card fail on a $200 charge, the card will be replaced. He also guarantees that all the credit cards he sells are Premium Cards, and if you get anything lower than a Platinum Card (like a Classic/Standard) then those cards will be replaced.

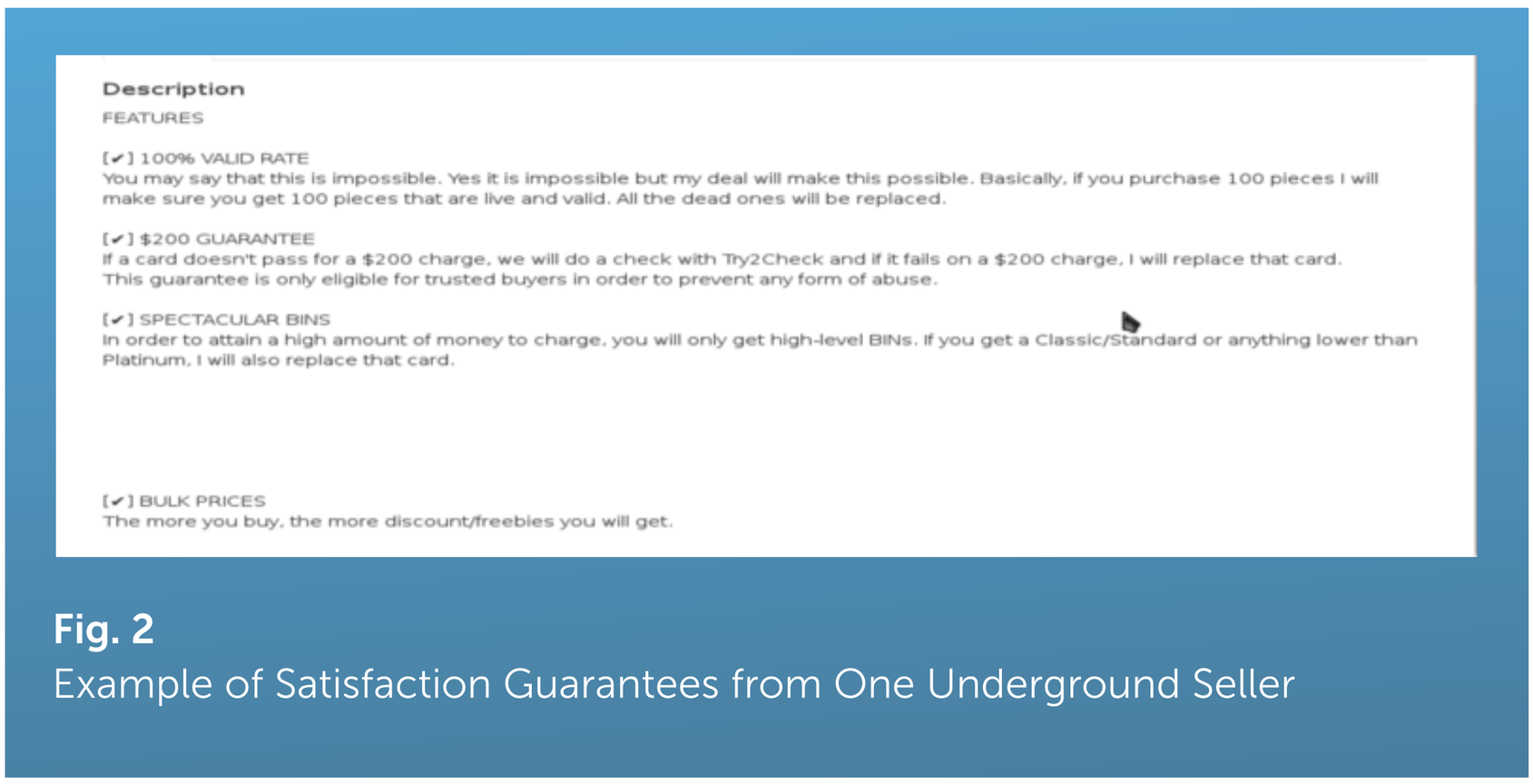

Fig. 2
Example of Satisfaction Guarantees from One Underground Seller

Malware For Sale

Remote Access Trojans (RATs) for Sale

The price for Remote Access Trojans (RATs) is considerably cheaper this year than last year. They are currently running from $20 to $50 and the most popular include:

- **darkcomet**
- ***blackshades**
- **cybergate**
- **predator pain**
- **Dark DDoser**

$50-250

Last year, RATs ranged in price from $50 to $250. Stewart and Shear suspect that the price has dropped because there are numerous RATs available on the Underground which are FREE because the source code has been cracked. Hackers are looking for a RAT that is easily available for purchase or to use for free and which they can run through a Crypter (a program which encrypts malware, making it FUD or fully undetectable to Anti-Virus and Anti-Malware programs).

Crypters for Sale

$50-150

Some of the most popular Crypters cost $50 to $150 each and include:

- **Aegis**
- **Sheikh Crypter**
- **xProtect**

The price of the Crypter depends on how well it encrypts the malware, making it FUD. According to Shear and Stewart, many seasoned hackers know how to code their own Crypters, so many of those buying Crypters are script kiddies, who do not have those skills.

Exploit Packs for Sale

The two most common exploit packs Shear and Stewart saw being talked about on the Hacker Underground were Nuclear and Sweet Orange. These Exploit Packs could be leased for:

Nuclear Exploit Pack Lease Rates

$50 --- a day

$400--- a week

$600 ---a month

$600

Sweet Orange Exploit Pack Lease Rates

$450---a week

$1,800---a month

Nuclear and Sweet Orange are similarly priced in their weekly rates but Nuclear at $600 a month is far cheaper by the month than Sweet Orange which is $1800 a month to lease.

$1800

Infected Computers for Sale

Last year, when investigating the prices for compromised computers (bots), Shear and Stewart only came across bulk pricing for bots which did not specify their location. These random bots were considerably cheaper, for example, 1,000 bots ran $20; 5,000 bots ran $90; 10,000 ran $160; etc.

However, this year they found pricing for bots located in specific countries, and these bots are considerably more expensive. The price for buying access to compromised computers does vary from country to country. The price for 5,000 individual bots located in the US runs from $600 to $1,000, while the same number of UK-based bots runs $400 to $500, a 50 to 100 percent decrease in price from the US bots.

When asked why the price for individual compromised US computers would be more expensive, Stewart and Shear theorized that US bots would potentially have access to financial sites which people in the UK don't have access to. For example, if hackers were intent on stealing Coinbase bitcoin accounts they would need access to compromised US computers since Coinbase only does business with US-based customers. Additionally, any credit card account information found on compromised bots in the UK is likely to be more secure, because the frequent use of Chip and PIN technology in the UK and Europe. Chip and PIN technology, also known as EMV (Europay, MasterCard and Visa), requires a four-digit PIN for authorization of in-person purchases. Also, all data embedded in the chip and communications are protected by cryptography, making chip and PIN cards more difficult to hack, while with many US credit cards, the card date is encoded in old-school magnetic-stripe technology and is relatively easy to steal. Also, magnetic-stripe credit cards are also much easier to counterfeit than chip and PIN varieties. Since magnetic stripe cards require no PIN, a thief can simply scrawl a bogus signature and walk away.

US (unique installs)

1,000 - $140 - $190
5,000 - $600 - $1,000
10,000 - $1,100 - $2,000

UK (unique installs)

1,000 - $100 - $120
5,000 - $400 - $500
10,000 - $700 - $1,100

Asia (unique installs)

1,000 - $4 - $12

Online Bank Accounts for Sale

Just as with stolen credit cards, there are online banking credentials for sale. Dell SecureWorks found that one can purchase the username and password for a "High Value" online bank account with a "Verified" balance between $70,000 and $150,000 for approximately 6 percent of the balance of the account. One would pay this rate only to a seller who had a reputation for providing solid credentials for premium, verified accounts. For a $70,000 account that would run approximately $4,200.

Hacker Services for Hire:

Hacking into Websites, DDoS Attacks, Doxing

Hacking into a Website

Stewart and Shear found that the current price for hacking into a website ranges between $100 to $200, whereas last year, the cost was between $100 to $300. As before, the price is determined by the reputation of the hacker. The higher the price, the more reputable the hacker.

Distributed Denial of Service (DDoS) Attacks

The current price for hiring a hacker to knock a website offline is similar to last year's costs. However, you get a break if you opt to have the DDoS attack last for a day or a week. This year's prices include:

Current DDoS Attack Prices

Attacks Per Hour = $3-$5

Attacks Per Day = $60-$90

Attacks Per Week = $350-$600

Last Year's DDoS Attack Prices

Attacks Per Hour = $3-$5

Attacks Per Day = $90-$100

Attacks Per Week = $400-$600

Doxing

Unlike last year, Shear and Stewart said they are not seeing a lot of Doxing Services for sale. Doxing is when a hacker is hired to get all the information they can about a target. This includes searching through social media sites, public information sites, manipulating the victim via social engineering and infecting them with information-stealing malware. For those hackers who are selling Doxing Services, they are charging between $25 to $100.

Organizations

Should Consider the Following Security Steps

How to Protect Your Financial Data, Personal Identifiable Information (PII), and Intellectual Property from Compromise

In order to this 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.

Dell SecureWorks advises a layered approach to security.
Organizations should consider implementing the following:

- Firewalls around your network and Web applications
- Intrusion Prevention Systems or Intrusion Detection Systems (IPS/IDS). These inspect inbound and outbound traffic for cyber threats and detect and/or block those threats
- Host Intrusion Prevention Systems (IPS)
- Advanced Malware Protection Solutions for the Endpoint and Network
- Vulnerability scanning
- 24 hours a day x7 days a week x365 days a year log monitoring,
and Web application and network scanning
- Security Intelligence around the latest threats
(people working on the latest threats in real-time, human intelligence)
- Encrypted email
- Educating your Employees on Computer Security. 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

Individuals

Should Consider the Following Security Steps

• Computer users should use a computer dedicated only to doing their 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.

• Avoid clicking on links or attachments within emails from untrusted sources. Even if you recognize the sender, you should confirm that the sender has sent the specific email to them before clicking on any links or attachments.

• Reconcile your banking and credit card statements on a regular basis with online banking and/or credit card activity to identify potential anomalous transactions that may indicate account takeover.

• Make sure your anti-virus 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 as soon as they become available you install updates for your applications and for your computer’s operating system.

• Be cautious about installing software (especially software that is too good to be true – e.g. download accelerators, spyware removal tools), and be conscience 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.

• 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.

Hacker Products and Services	Price in 2013	Price in 2014
Visa and Master Card (US)	$4	$4
American Express (US)	$7	$6
Discover Card with (US)	$8	$6
Visa and Master Card (UK, Australia and Canada)	$7 -$8	$8
American Express (UK, Australia and Canada)	$12- $13	$15(UK and Australia); $12 (CA)
Discover Card (Australia and Canada)	$12	$15(Australia); $10(CA)
Visa and Master Card (EU and Asia)	$15	$18-$20
Discover and American Express Card (EU and Asia)	$18	$18-$20
Credit Card with Track I and II Data (US)	$12	$12
Credit Card with Track I and II Data (UK, Australia and Canada)	$19-$20	$19-$20
Credit Card with Track I and II Data (EU, Asia)	$28	$28
US Fullz	$25	$30
Fullz (UK, Australia, Canada, EU, Asia)	$30-$40	$35-$45
VBV(US)	$10	$12
VBV (UK, Australia, Canada, EU, Asia)	$17-$25	$28
Premium Master Cards with Track 1 and 2 Data (Worldwide)	N/A	$35
Premium Visa Cards with Track 1 and 2 Data (Worldwide)	N/A	$23
High Quality Bank Accounts with Verified Balances of $70,000-$150,000	N/A	6% of the balance of the account
Remote Access Trojan(RAT)	$50-$250	$20-$50
Crypters	N/A	$50 -$150
Sweet Orange Exploit Kit Leasing Fees	$450 a week/$1800 a month	$450 a week/$1800 a month
Nuclear Exploit Kit Leasing Fees	N/A	$50 a day/$400 a week/$600 a month
Counterfeit Passports (Non US)	N/A	$200--$500
New Identities, plus matching utility bill	N/A	$250; matching utility bill an additional $100
Counterfeit Social Security Cards	N/A	$250-$400
Counterfeit Drivers' License	N/A	$100-$150

Hacker Products and Services	Price in 2013	Price in 2014
Hacking Tutorials	N/A	$1 each to $30 for 10 (depending on the tutorial)
Hacking Website; stealing data	$100-$300	$100 -$200
DDoS Attacks	Per Hour-$3-$5	Per Hour - $3-$5
	Per Day-$90-$100	Per Day - $60-$90
	Per Week-$400-$600	Per Week - $350-$600
Doxing	$25-$100	$25-$100
Infected Computers (US)	N/A	US (unique installs)
		1,000 - $140 - $190
		5,000 - $600 - $1000
		10,000 - $1100 - $2000
Infected Computers (UK)	N/A	UK (unique installs)
		1,000 - $100 - $120
		5,000 - $400 - $500
		10,000 - $700 - $1100
Infected Computers (Asia)	N/A	Asia (unique installs)
		1,000 - $4 - $12
		5,000/10K - N/A

Glossary of Terms

Credit Card Track I and II Data Track 1 and 2 Data is information which is contained in digital format on the magnetic stripe embedded in the backside 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 is the act of throwing so much traffic at a website, it takes it offline.

Fullz Fullz is a dossier of credentials for an individual, which also include Personal Identifiable Information (PII), which can be used to commit identity theft and fraud. Fullz usually include: Full name, address, phone numbers, email addresses (with passwords), date of birth, SSN or Employee ID Number (EIN), one or more of: bank account information (account & routing numbers, account type), online banking credentials (varying degrees of completeness), or credit card information (including full track2 data and any associated PINs).

Personal 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 is a person's full name, address, birthdate, driver's license number, telephone number, and email address.

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.

SecureWorks

Underground Hacking Markets | **DECEMBER 2014**

About Dell SecureWorks Dell SecureWorks is a market-leading provider of world-class information security services with more than 3,800 clients in 70+ countries. Organizations of all sizes rely on Dell SecureWorks to protect their assets, improve their compliance and reduce their costs. Our combination of award-winning security expertise and client support makes Dell SecureWorks the premier provider of information security services.

Dell SecureWorks uses cyber threat intelligence to provide predictive, continuous and responsive protection for thousands of organizations worldwide. Enriched by intelligence from our Counter Threat Unit research team, Dell SecureWorks' Information Security Services help organizations proactively fortify defenses, continuously detect and stop cyber attacks, and recover faster from security breaches. For more information, visit: http://www.secureworks.com.

For more information, phone 877.838.7947 to speak to a Dell SecureWorks security specialist.