WHITE PAPER

The Underground Hacker Marketplace

Executive Summary

While many businesses around the world continue to struggle financially, the Underground Hacker Market is thriving. Observing market changes year over year, Dell SecureWorks' researchers have seen a growing selection of stolen information and tools for hacker enablement.

In this white paper we will look at the evolving level of sophistication of the hacker marketplace and why it is critical to remain aware of threat activity occurring in the dark market in order to put the best security measures in place to protect against the latest threats.

What You Will Learn

- The common stolen goods that enable hackers to defraud, deceive and cheat victims out of money.
- Tools, trainings and additional services available for "off-the-shelf" cybercrime.
- The going rates for stolen goods, tools, trainings and additional services and how they change year over year and regionally.

Who Should Read This White Paper

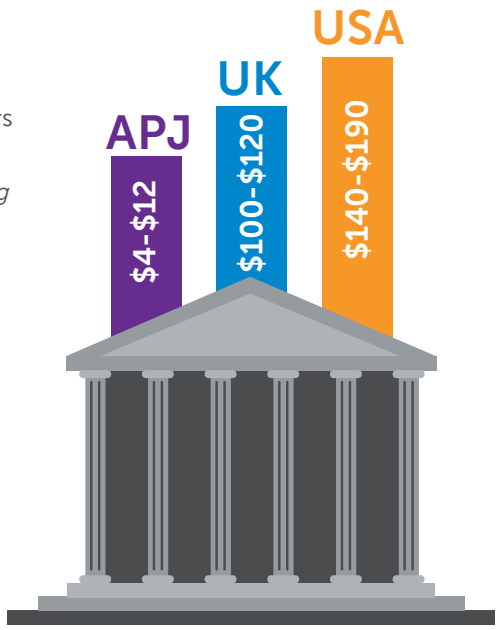
- Board of Directors
- C-Suite
- CISO/CSOs
- Directors of Security

"As long as there is valuable data available to steal, the Underground Hacker Marketplace will continue to boom."

The Underground Hacker Marketplace

Imagine walking through a marketplace with vendors lining both sides of the street. As you look at all the displays, you notice a wide range of products and services, from high-end to low-end offerings, with something for everyone. Many vendors you walk by provide discounts for bulk purchases and promise money-back guarantees if you are not happy with the product. As you examine the products you become inspired and ask yourself, *"Why can't I learn to make these products myself and use them?"* Just as this thought bubble dissipates from your brow, you turn the corner and find a row of vendors offering classes on how to build and use these products in the comfort of your own home. *Truly a one-stop-shop! Why can't more businesses have such a forward thinking strategy?*

Underground marketplace rate for bots by region in 2014.



Welcome to the underground hacker marketplace.

The imagery described above is an accurate depiction of today's marketplace for cybercriminals: a world of commerce with goods, tools and training to enable hackers to breach unsuspecting individuals, groups, and companies. Dell SecureWorks', Director of Malware Research Joe Stewart and Network Security Analyst David Shear visited this dark market during November 2014 to see how the underground market was evolving. They found a larger selection of stolen goods and tools for hacker enablement, along with a new level of business strategy and sophistication.

Stolen Goods for Hacker Enablement

The underground hacker marketplace is a haven for purchasing stolen personal data, credit cards and bank accounts. Shopping is easy in this dark market. Shoppers can obtain these illicit goods with a simple click of a button, in the comfort of their home. All the dirty work of obtaining the stolen credentials and accessing accounts has already been done.

One of the most notable additions in the market is an increase in the number of fake credentials for sale. These fake credentials include new identity packages, passports, driver's licenses and social security cards. These documents can enable criminals to defraud, deceive and cheat victims out of money via false bank loan applications, counterfeit checks and fake credit cards. According to one US Law Department, three scammers were producing and selling fake driver's licenses and using them for "cash out" schemes. These schemes involved stolen credit card information, usually obtained through hacking or ATM skimming operations, which are encoded onto counterfeit credit cards and then used to steal cash from victims' accounts. According to the FBI, from December 30, 2013 to June 23, 2014, the conspirators sold 1,514 fake driver's licenses for $232,660. This is just one example of how cybercriminals commit fraud.

For the more tech-savvy criminal shopper, online banking credentials are for sale. These electronic stolen goods provide the username and password for a "High Value" online bank account with a "verified" balance between $70,000 and $150,000 for approximately six percent of the account balance. Smart criminals 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 payoff would run approximately $4,200.

The hacker marketplace carries a wide array of products at different price points. New types of bundled illicit goods are continually being adding to upsell and cross-sell, resulting in increased profitability for cybercriminals. Below is the typical going rate for stolen credentials, credit cards and bank accounts.

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

Source: Dell SecureWorks, Underground Hacker Markets Report December 2014

Tools and Training for Beginner Hackers

An easy way to begin a career in cybercrime and commit other acts of fraud is by simply purchasing the goods necessary to perform the fraudulent act. For hackers who have higher aspirations and are ready to take a deeper plunge, there are readily available training and tools for sale. In this section of the underground market, both malware and infected computers can be quickly and easily purchased for "off-the-shelf" cybercrime. Hacker Tutorials train eager-to-learn beginners, and hacker services are easily obtained for more advanced cybercrime.

Malware in this section of the market ranges anywhere from $20 for basic Remote Access Trojans (RATs) to $1,800 a month for more advanced exploit kits. Many common RATs for purchase include: Darkcomet, *Blackshades, Cybergate, Predator Pain and Dark DDoser. RAT prices have dropped during the past 12 months, likely due to the fact that there are numerous RATS available which are free because the source code has been leaked. Hackers like a RAT that is easily available for purchase or for free because they can run it through a Crypter which makes it undetectable to anti-virus and anti-malware programs. A popular Crypter such as Aegis, Sheikh Crypter or xProtect cost a criminal shopper somewhere between $50 and $150, depending on how well it encrypts the malware and makes it fully undetectable. Advanced hackers know how to code their own Crypters, so many of those buying Crypters are unskilled "script kiddies" looking to make a quick hit. The two most common types of exploit kits for sale are Nuclear and Sweet Orange which can be leased by day, week or month. The cost in the underground market for a month of Nuclear runs around $600, and Sweet Orange runs approximately $1,800 a month.

> "According to the FBI, from December 30, 2013 to June 23, 2014, the conspirators sold 1,514 fake driver's licenses for $232,660."

A new feature in the hacker marketplace is geographically focused products and services. Compromised computers or bots for sale, are now located in specific countries so that they can access region-specific financial sites. This improvement has increased the price of bots substantially. Bots located in the US are priced higher than many other regions. It is theorized that US bots would potentially have access to financial sites that people in other countries don't have access to. For example, if the hackers' intention is to steal Coinbase bitcoin accounts, they would need access to compromised US computers because Coinbase only does business with US-based customers. Likewise, European-issued credit cards are more secure due to the use of chip and pin technology mandated by EMV, a technical standard for smart payment cards and payment terminals. They are more difficult to hack, resulting in a lower price for European bots. In the underground market, the going rate for a thousand US bots is $140-$190 but only $100-$120 for a thousand UK bots, and a nominal$4-$12 for Asia bots.

For novice hackers or "newbies," as they are often called by established hackers, the underground marketplace is a great avenue to learn from experienced hackers who sell Hacker Training Tutorials. The 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 that you Withdraw" to "How to have 100% Successful Bank Transfers." Manuals containing handfuls of tutorials explain a variety of cybercriminal activities can be purchased for a mere $30, while individual training tutorials can run as low as one dollar. 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 are but also how their used, popularity and typical purchase price.

For hackers who don't want to do the dirty work themselves, hacker services are available for hire. Some common services include: hacking into a website, Distributed Denial or Service (DDoS) Attacks and Doxing. The purchase price for website hacking varies depending on the reputation of the hacker. The higher the price, the more reputable the hacker. It is common to see prices range $100 -$300. The cost of a hacking service that knocks a website offline has remained stable. Pricing is established by number of attacks for a specified period of time. For example, a DDoS attack will run $3- $5 per hour, $90- $100 per day, and $400 - $600 per week. Lastly, Doxing is available and used when someone is seeking intel on a target. A hired hacker will get all the information on the target by searching through social media sites, public information sites, social engineering manipulation and information-stealing malware. Doxing Services are priced $25 - $100.

> "These virtual storefronts of illegal commerce are well-oiled machines offering 100% Satisfaction Guarantees and bundled deals on numerous offerings."

Conclusion

Continuous Improvement to Products and Services

The underground marketplace continually evolves. These virtual storefronts of illegal commerce are well-oiled machines offering 100% Satisfaction Guarantees and bundled deals on numerous offerings. It's important to remain aware of the sophistication of this changing marketplace to make better decisions about the best security measures to protect against known and evolving threats. This short visit to the illegal underground hacker bazaar, has provided you a brief snapshot of the thriving cybercriminal world of commerce. As long as there is valuable data available to steal, the Underground Hacker Marketplace will continue to boom. This underscores the importance of a layered security approach.

.

For more information, call (877) 838-7947 to speak to a Dell SecureWorks security specialist.
www.secureworks.com