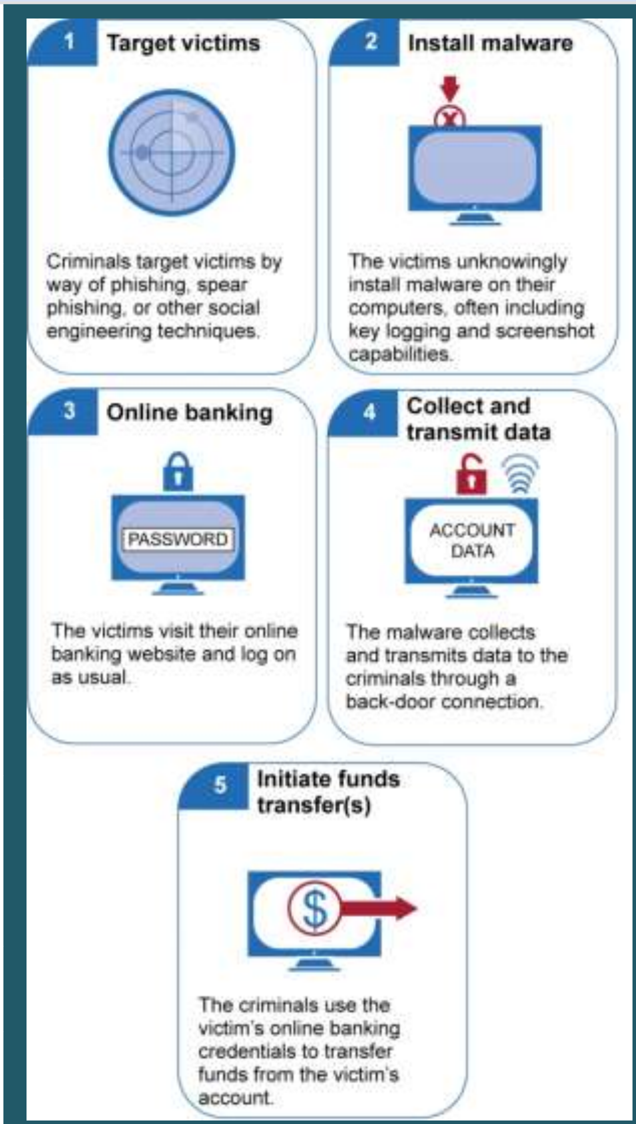
2015

Cybercrime Black Market



1 Target victims

Criminals target victims by way of phishing, spear phishing, or other social engineering techniques.

2 Install malware

The victims unknowingly install malware on their computers, often including key logging and screenshot capabilities.

3 Online banking

The victims visit their online banking website and log on as usual.

4 Collect and transmit data

The malware collects and transmits data to the criminals through a back-door connection.

5 Initiate funds transfer(s)

The criminals use the victim's online banking credentials to transfer funds from the victim's account.

(**Source:** U.S. Congress GAO July 2015)

Homeland Security Research Corp.

Cybercrime Black Market – 2015

August 2015

Homeland Security Research Corp. (HSRC) *is an international market and technology research firm specializing in the Homeland Security (HLS) & Public Safety (PS) Industry. HSRC provides premium market reports on present and emerging technologies and industry expertise, enabling global clients to gain time-critical insight into business opportunities. HSRC's clients include U.S. Congress, DHS, U.S. Army, U.S. Navy, NATO, DOD, DOT, GAO, and EU, among others; as well as HLS & PS government agencies in Japan, Korea, Taiwan, Israel, Canada, UK, Germany, Australia, Sweden, Finland, Singapore. With over 750 private sector clients (72% repeat customers), including major defense and security contractors, and Fortune 500 companies. HSRC earned the reputation as the industry's Gold Standard for HLS & PS market reports.*

Washington D.C. 20004, 601 Pennsylvania Ave., NW Suite 900,
Tel: 202-455-0966, info@hsrc.biz, www.homelandsecurityresearch.com

Table of Contents

List of Figures

1 The Cybercrime Underground Market

The dispersed character of the cyberspace facilitates a textbook cyber-attack market. Hackers and traders use the open market advantages to trade cyber-attack tools and services to anyone who likes to trade them for an agreed upon price.

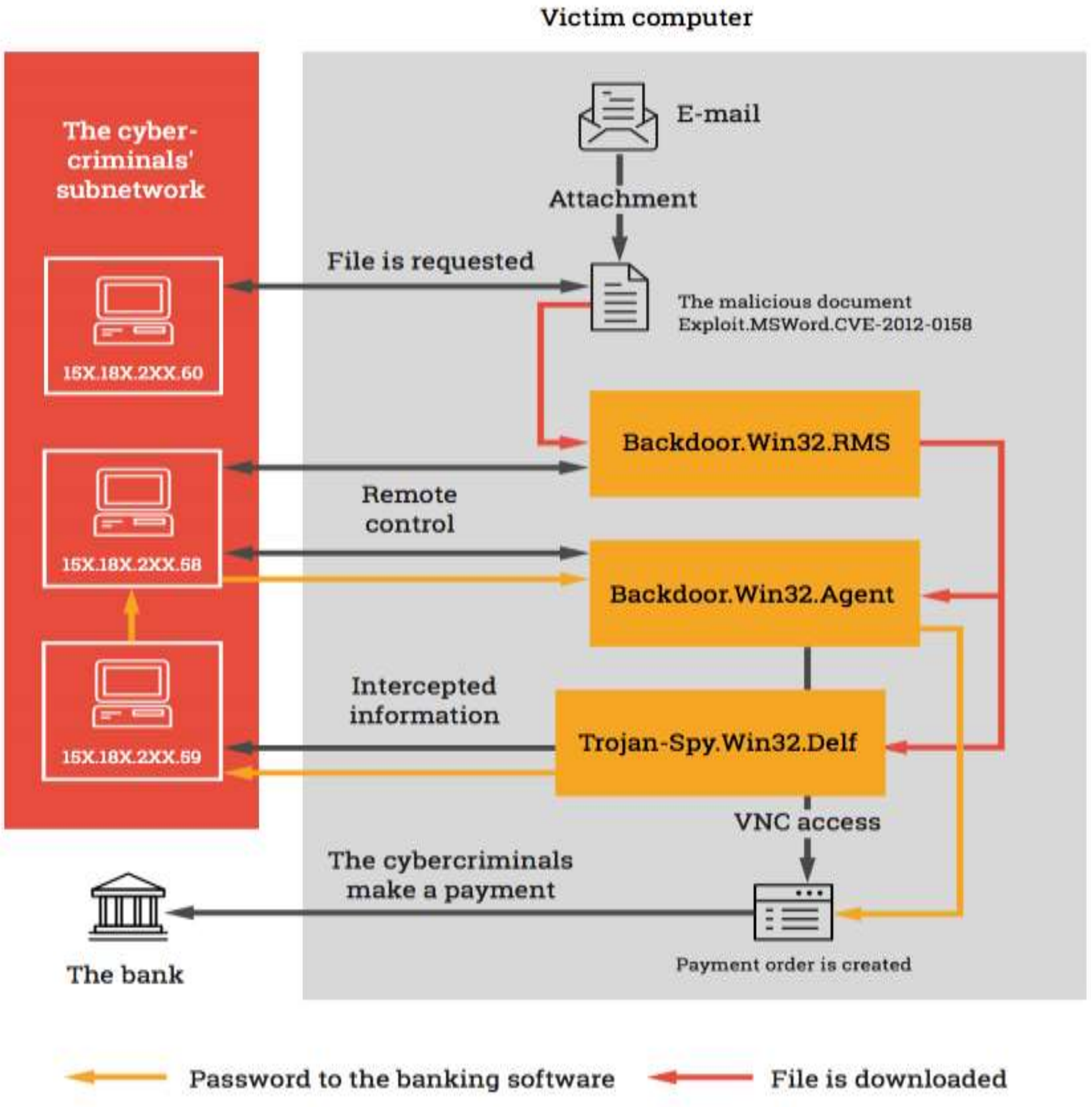
A varied and sophisticated market in cyber products trading for a variety of purposes has thus emerged, with a range of prices varying from a few dollars for a simple one-time denial of service attack to thousands of dollars for the use of unfamiliar vulnerabilities and the capabilities to enable a cybercriminal to maneuver his way into the most protected IT system.

Thanks to cyberspace, this market is growing by using the infrastructure of social networks and forums that allow anonymous communications between traders and buyers. In an interesting phenomenon, seen only recently, these traders are leaving the web underground and stepping out into the light. They can be found on the most popular social networks e.g. Facebook.

A new black market business sector is the sale of customized turnkey systems. Traders offer a complete service, including design, installation of command and control servers, training and the option of selective purchase of individual attack elements. Discounts and bargains are a daily reality in this market.

- ❑ The cyber black market has evolved from a varied landscape of discrete, ad hoc individuals into a network of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells) and nation-states.
- ❑ The cyber black market does not differ much from a traditional market or other typical criminal enterprises; participants communicate through various channels, place their orders, and get products.
- ❑ Its evolution mirrors the normal evolution of markets with both innovation and growth.
- ❑ For many, the cyber black market can be more profitable than the illegal drug trade.
- ❑ Attackers of all skill levels can enter the arena of financial fraud, as the underground marketplace is a service industry that provides an abundance of resources. Those who lack expertise can simply purchase what they need. The Trojans and services available to attackers vary depending on the experience and financial resources available. Entry-level attackers have a limited selection of financial Trojans, while more experienced or trusted attackers will have access to private Trojans. Experienced attackers may even decide to develop their own custom Trojan.

Figure 1 - Diagram of the Cybercriminal Attack



(**Source**: M. Prokhorenko)

- ❑ Forks of Zeus began to emerge, including the enhanced kits Ice IX and Citadel, which competed for market share. Cybercriminal gangs also built custom versions of Zeus for personal use, such as the notorious "Gameover," which appeared in July 2011. One month after Zeus' source code leaked, an individual who goes by the moniker of Xylibox cracked the builder protection for Spyeye. It suffered from a similar price crash to Zeus. Currently, neither Trojan is being actively developed by their original authors in the public domain. Many modern financial Trojans have copied the techniques and architecture of Spyeye and Zeus

- ❑ For as little as $100, an attacker can avail of a leaked Zeus or Spyeye equipped with Web-injects. These bots are unintelligent and require configuration updates.
- ❑ A state-of-the-art Zeus fork, like Citadel, costs around $3,000 to an outsider and includes regular updates.
- ❑ Custom Web-injects can be purchased for between $30 and $100. Third-party spam services, location-aware exploit kits and traffic direction services can then be used to deliver the payload. Those services may come with explanatory videos or even free chat support during installation.
- ❑ Some programming services are more expensive than others, according to published ads, a software programmer a banking Trojan can charge $1,300, while fake programs only cost approximately $15.
- ❑ One particularly interesting tendency is that bulletproof server hosting pricing is dropping in the underground. One can purchase a dedicated server service for anywhere from 50 cents to $1 per month, for example, and a bulletproof hosting service for $15- to $250 per month.
- ❑ DDoS and botnet services are relatively inexpensive: one day of DDoS' a victim prices between $30 up to a one-month subscription goes for approximately $1,200.
- ❑ Botnet rental is actually rare in the underground market because it's not as lucrative as other services. Hackers normally operate their own botnets because selling them is less profitable.
- ❑ But bots go for approximately $200 for 2,000 infected machines. A DDoS botnet can cost $700 and $100 per DDoS botnet update.
- ❑ The cost of hosting is being driven down. What's surprising is that it's so inexpensive, but if one look at what's happening in legitimate business, one shouldn't be that surprised: the hosting business has low margins.
- ❑ The most popular services after customized software services and software sales are:
  - Hacking services
  - Dedicated server sales and bulletproof-hosting services
  - Spam and flooding services download sales
  - DDoS services
  - Traffic sales
  - File encryption services
  - Trojan sales
- ❑ The bottom line is that cybercrime support industry is a large business.
- ❑ Key factors in determining the success of an attack are:

  - Trojan selection – Reliable, stable, low detection rate
  - Web-inject configuration – Intelligent, up to date
  - Distribution – The target user must be a customer of financial institutions specified in the Trojan's configuration data
  - Money laundering – Reliable source of money mule bank accounts

- ❑ The cybercrime underground is now a vast, sophisticated, high-volume market. There are at least 20 different types of services offered in forums for just anyone who wants to make a profit off of cybercrime, everything from crime-friendly VPN and security software-checking services to plain old off-the-shelf exploits.

"The effect of the internet is to lower financial transaction costs. Everything else is just advertising"

- ❑ Many of the services identified are well-known, but it's the breadth and relatively inexpensive pricing for the banking & financial services fraud services. This shows the fully fledged commercial nature of it. It's very much crime-as-a-service, it's a mature market.
- ❑ Programming services basically malware-software and software sales are the most popular cybercrime services and activities, according to the report, which provides a glimpse into the underground activity in forums and cybercriminal circles. The sale of off-the-shelf malware programs like Trojans, spammers, DDoS bots, Zeus, and SpyEye are also among the hottest markets.
- ❑ The basic spamming or botnet businesses are inexpensive first steps into the business, but the more sophisticated – and lucrative – services are zero-day development and other heavy coding services. If a criminal wants to find out how to break into cybercrime, he/she can rent a botnet, buy a BlackHole exploit kit, and infect the targeted organization with his own custom Trojan from this other vendors.

More information can be found at:
U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020