Symantec Report on the Underground Economy - Spokesperson Training

Jeff Guilfoyle (jeff_guilfoyle@symantec.com)

Principal SE, Symantec

January 21, 2009

Report on the Underground Economy Important Facts

- **What the report is:**
  - An in-depth look at the Underground Economy
  - A detailed report on Underground Economy advertisements that ***Symantec*** sees.
  - Actual transactions are conducted in private channels.
  - Based on real, ***empirical*** data collected by the Global Intelligence Network.
- **What the report is not:**
  - The Internet Security Threat Report
  - A ***survey*** of opinions.
  - Product driven ***marketing.***
  - Scientific ***certainty.***
- **Data Sources**
  - Underground Economy servers
    - Symantec observed channels on IRC server networks that were associated with the underground economy.
    - Server network sizes ranged from 5 channels to over 28,000 channels.
    - Over 44 million messages observed from the channels
  - Piracy Websites
    - Symantec observed tracker data related to pirated software shared by over 280,000 individual users.
    - Over 320,000 instances of approximately 390 software products were observed.

Underground Economy – Key Messages

- The Underground Economy is geographically diverse and shows the ability to generate millions of dollars in revenue for cybercriminals.
- It is a self-sustaining system where tools that aid in fraud and theft can be purchased and the stolen information obtained by those tools can then be sold.
- Cybercriminals range from loose collections of individuals to organized and sophisticated groups, all with a common purpose.
- Software piracy closely reflects the retail market; software categories with the highest volume of sales are also the most heavily pirated.

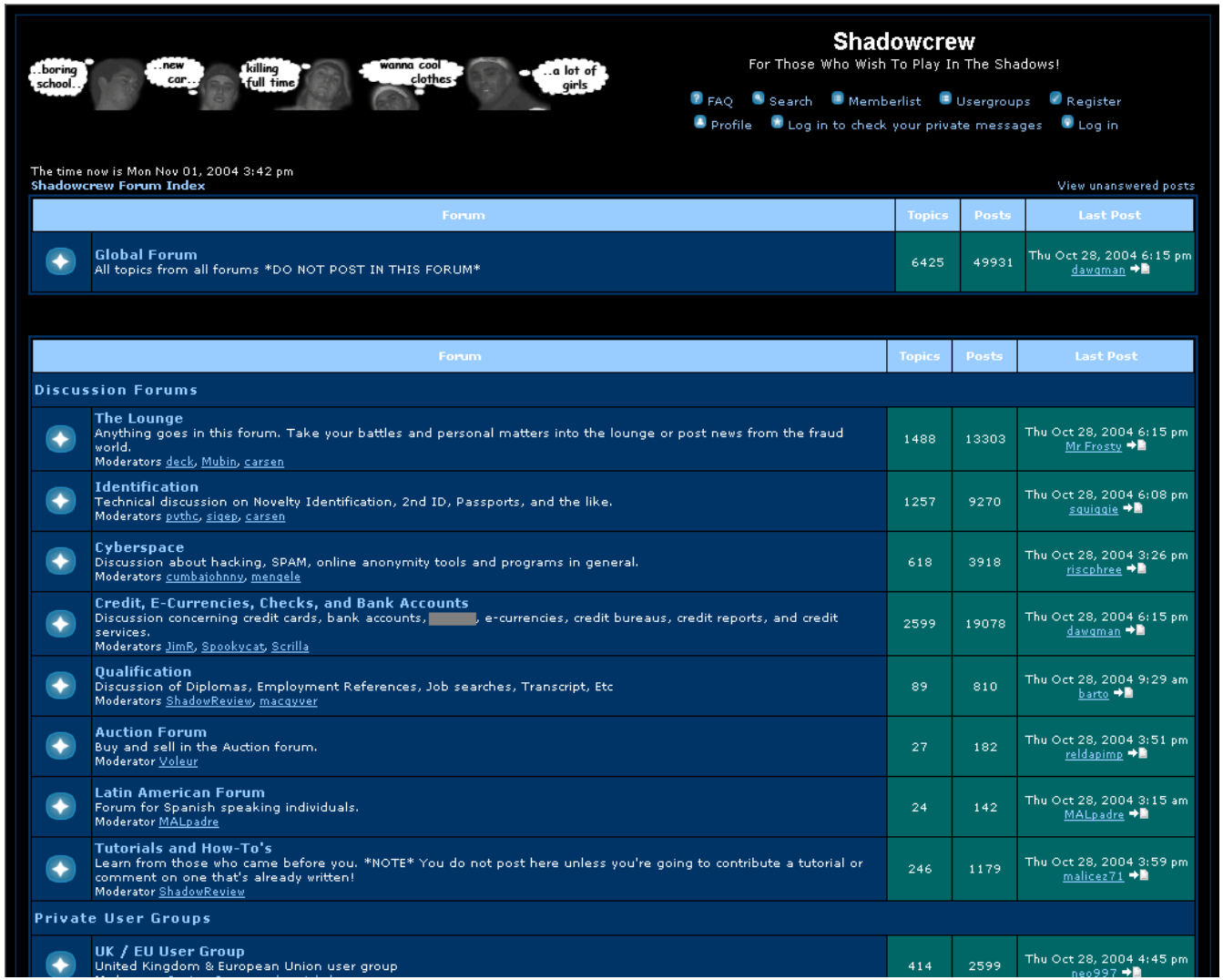
Underground Economy – Key Findings

- Symantec estimates the value of total advertised goods on underground economy servers was over $276 million for the reporting period.
- The potential worth of the top seller on the UE is $6.4 million.
- The category of credit card information accounted for 31% of all advertisements for sale.
- 45% of UE servers were located in North America.
- Desktop computer games made up 49% of software being pirated.
- In total, the approximate U.S. retail value of all tracking files observed by Symantec was $83.4 million.

Symantec Report on the Underground Economy
Key Facts and Figures

Cybercriminals range from loose collections of individuals to organized and sophisticated groups, all with a common purpose.

Groups and Organizations



Groups and Organizations

- Web forums represent some groups and organizations that have been active on the Underground Economy
- Wide range in the sophistication and capabilities of these groups and organizations
- Ample evidence exists that organized crime is involved in many cases
- Forum participants are often subject to a screening process
- Advertisements and other messages posted to the forum are readily available, even days or months afterward, making it easier to conduct business and post detailed price lists for goods or services

Groups and Organizations

- Web presence is highly visible
- May attract more attention from law enforcement
- Screening process makes it desirable to maintain a single identity
- Archived content provides a list of illegal activity
- Number of high profile stings such as Operation Firewall
- These combine to drive groups further underground to less visible and anonymous mediums such as IRC

Groups and Organizations

United States Secret Service

WWW.SECRETSERVICE.GOV

SHADOWCREW

"FOR THOSE WHO WISH TO PLAY IN THE SHADOWS....."

ACTIVITIES BY SHADOWCREW MEMBERS ARE BEING INVESTIGATED BY THE

UNITED STATES SECRET SERVICE

SEVERAL ARRESTS HAVE RECENTLY BEEN MADE...WITH MANY MORE TO FOLLOW.

Proxies, VPNs, IP Spoofing, Encryption, etc....You Are No Longer Anonymous!!

SHADOWCREW TOPICS

SHADOWCREW MEMBERS ARE FACING THE FOLLOWING CHARGES (*Charges are Not Limited to Below):

- **TITLE 18 USC 371 - CONSPIRACY**
- **TITLE 18 USC 1029 - ACCESS DEVICE FRAUD**
- **TITLE 18 USC 1028 - FRAUD W/IDENTITY DOCUMENTS, IDENTITY THEFT, ETC.**
- **TITLE 18 USC 1030 - FRAUD AND RELATED ACTIVITY IN CONNECTION WITH COMPUTERS.**

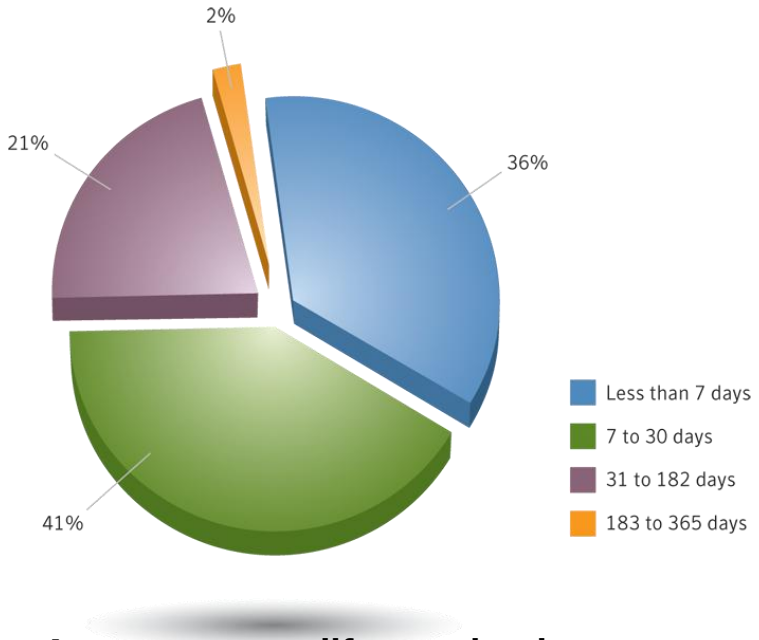
IF YOU ARE A MEMBER WHO IS CONFUSED AND/OR CONCERNED BY YOUR ACTIONS...PLEASE READ THE FOLLOWING:

RECENT NEWS REPORTS SHOULD INFORM YOU THAT THE SECRET SERVICE IS INVESTIGATING YOUR CRIMINAL ACTIVITY.

CONTACT YOUR LOCAL UNITED STATES SECRET SERVICE FIELD OFFICE....*BEFORE* WE CONTACT YOU!!

Servers and Channels
IRC Server Lifespans

- The median average observed server lifespan was 10 days
- Servers may be abandoned by participants or shut down by owners of legitimate IRC networks
- One of the largest observed IRC server networks had approximately 28,000 channels and 90,000 users



Average server lifespan by days

The Underground Economy is geographically diverse and shows the ability to generate millions of dollars in revenue for cybercriminals.

Goods and Services
Value of Advertised Goods & Services

- Symantec estimates the value of total advertised goods on underground economy servers was over $276 million for the reporting period
- The potential worth of all credit cards advertised during this reporting period would be $5.3 billion
- Using the average advertised balance of $40,000 financial accounts would potentially be worth $1.7 billion

Rank	Category	Percentage
1	Credit card information	59%
2	Identity theft information	16%
3	Server accounts	10%
4	Financial accounts	8%
5	Spam and phishing information	6%
6	Financial theft tools	<1%
7	Compromised computers	<1%
8	Malicious applications	<1%
9	Website accounts	<1%
10	Online gaming accounts	<1%

Value of advertised goods as a percentage of total, by category

Advertisers
Most Active Advertisers

- Between July 1, 2007 and June 30, 2008, Symantec observed 69,130 distinct active advertisers on underground economy servers and 44,321,095 total messages posted
- The estimated value of the total advertised goods for the top 10 most active advertisers was over $575,000
- The potential worth of the top 10 most active advertisers was $18.3 million

Rank	Advertiser	Percentage of Advertised Goods, Top 10	Percentage of Goods and Services, Top 10	Value of Goods	Potential Worth
1	Maggie	25%	27%	$144,448	$6.4 million
2	Spooki	22%	15%	$128,459	$3.3 million
3	Luna	19%	18%	$108,798	$3.2 million
4	Shadow	14%	11%	$80,309	$1.7 million
5	Expo	9%	12%	$52,599	$2.0 million
6	Ripley	8%	6%	$10,728	$0.9 million
7	Fergie	1%	3%	$5,523	Not applicable
8	Fintan	1%	3%	$5,262	$0.4 million
9	Pepper	1%	2%	$4,040	$0.3 million
10	Pranda	<1%	4%	$2,185	Not applicable

Value of total advertised goods - advertisers

Advertisers
Payment Systems

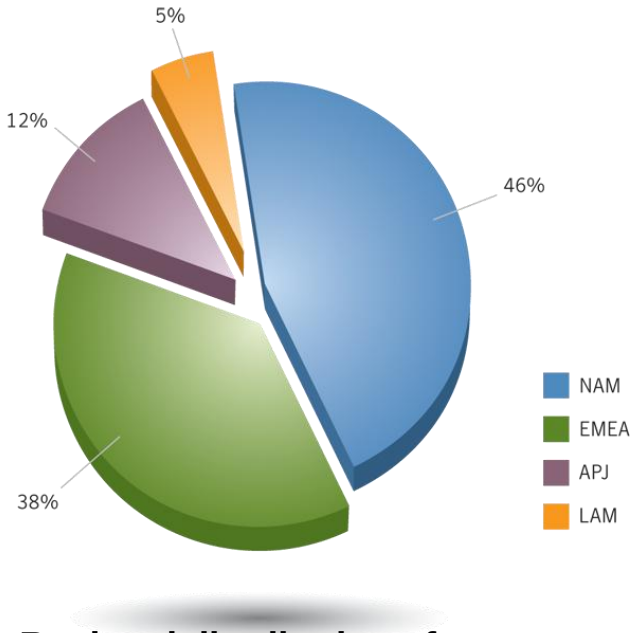
- Like traditional retailers, UE advertisers may have preferred payment methods
- Online currency accounts were the most popular method of payment, accounting for 63% of the total
- Trading is also popular because there is no middle-man or service fees
- Electronic payments can leave a trail that may be used by law enforcement

Rank	Payment System	Percentage
1	Online currency account	63%
2	Trade of goods and services	24%
3	Online payment service	9%
4	Wire transfer service	3%

Payment systems used on underground economy servers

Channels and Servers
IRC Servers by Region

- The NAM region had the largest number of underground economy servers, hosting 45% of the total
- Distribution of UE servers is similar to the regional distribution of IRC networks
- The largest contributing country by a significant margin was the United States, which hosted 41% of the total observed servers worldwide



Regional distribution of servers

The Underground Economy is a self-sustaining system where tools that aid in fraud and theft can be purchased and the stolen information obtained by those tools can then be sold.

Goods and Services Advertised by Category

- Credit card information category ranked highest between July 1, 2007 and June 30, 2008, with 31% of sale advertisements and 24% of requests
- Credit card information and Financial accounts are relatively easy to cash out, providing immediate monetary gain

Rank for Sale	Rank Requested	Category	Percentage for Sale	Percentage Requested
1	1	Credit card information	31%	24%
2	3	Financial accounts	20%	18%
3	2	Spam and phishing information	19%	21%
4	4	Withdrawal service	7%	13%
5	5	Identity theft information	7%	10%
6	7	Server accounts	5%	4%
7	6	Compromised computers	4%	4%
8	9	Website accounts	3%	2%
9	8	Malicious applications	2%	2%
10	10	Retail accounts	1%	1%

Goods and services available for sale, by category

Goods and Services Advertised by Item

- Bank account credentials were the most advertised individual item on the Underground Economy followed by credit cards with CVV2 numbers
- Requested rank and rank for sale match closely for many items indicating the market is as susceptible to supply and demand trends as legitimate markets
- Bulk pricing is available for items such as credit cards and full identities

Rank for Sale	Rank Requested	Goods and Services	Percentage for Sale	Percentage Requested	Range of Prices
1	1	Bank account credentials	18%	14%	$10–$1,000
2	2	Credit cards with CVV2 numbers	16%	13%	$0.50–$12
3	5	Credit cards	13%	8%	$0.10–$25
4	6	Email addresses	6%	7%	$0.30/MB–$40/MB
5	14	Email passwords	6%	2%	$4–$30
6	3	Full identities	5%	9%	$0.90–$25
7	4	Cash-out services	5%	8%	8%–50% of total value
8	12	Proxies	4%	3%	$0.30–$20
9	8	Scams	3%	6%	$2.50–$100/week for hosting; $5–$20 for design
10	7	Mailers	3%	6%	$1–$25

Breakdown of goods and services available for sale and requested

Goods and Services
Malicious Tools

- Malicious tools can be used to steal confidential information
- Attack kits, spam and phishing kits, malicious code, and exploits are available on the underground economy
- Exploits and attack kits had the highest average prices
- Pricing is based on supply and demand as well as the tool's capabilities

Attack Kit Type	Average Price	Price Range
Botnet	$225	$150–$300
Autorooter	$70	$40–$100
SQL injection tools	$63	$15–$150
Shopadmin exploiter	$33	$20–$45
RFI scanner	$26	$5–$100
LFI scanner	$23	$15–$30
XSS scanner	$20	$10–$30

Attack kit prices

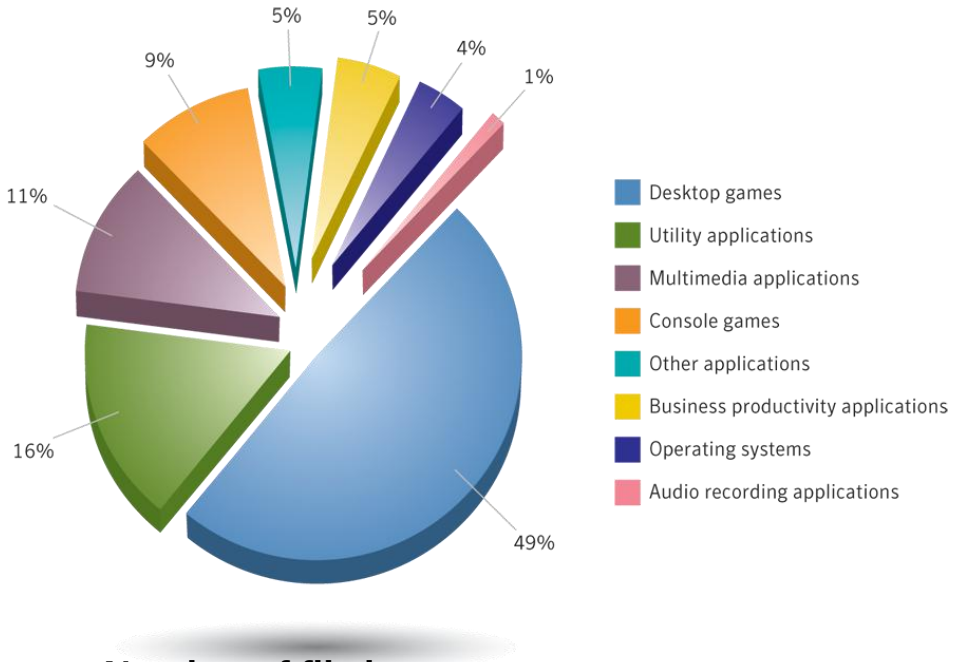
Exploit Type	Average Price	Price Range
Site-specific vulnerability (financial site)	$740	$100–$2,999
Remote file include exploit (500 links)	$200	$150–$250
Shopadmin (50 exploitable shops)	$150	$100–$200
Browser exploit	$37	$5–$60
Remote file include exploit (100 links)	$34	$20–$50
Remote file include exploit (200 links)	$70	$50–$80
Remote operating system exploit	$9	$8–$10

Exploit prices

Software piracy closely reflects the retail market; software categories with the highest volume of sales are also the most heavily pirated.

Piracy
File Instances by Category

- Desktop computer games were the most frequently seen tracking files by a significant margin, accounting for 49% of all file instances observed
- Retail sales of desktop games are among the highest of any category
- Number of tracking files for software tends to increase when a new release is available



Number of file instances per category

Piracy
Financial Effect on Business Sectors

- The total approximate value of all categorized tracking files observed by Symantec was $83.4 million
- Multimedia software accounted for approximately $53 million
- While there were more desktop game file instances the lower total value was due to a lower average price

Rank	Category	Approximate Value	Percentage of Total Value of Categories	Price Range of Software	Percentage of File Instances
1	Multimedia applications	$53,098,000	65%	$40–$8,000	11%
2	Business productivity applications	$8,671,000	11%	$400–$700	5%
3	Desktop games	$8,062,000	10%	$50	49%
4	Audio recording applications	$2,992,000	4%	$250–$700	1%
5	Utility applications	$2,573,000	3%	$20–$230	16%
6	Operating systems	$2,237,000	3%	$100–$220	4%
7	Other applications	$2,152,000	3%	$30–$600	5%
8	Console games	$1,286,000	0%	$35–$60	9%

Approximate dollar value of file instances observed

Piracy
File Instances by Country

- The top ranked country by number of file instances was the United States with 19% of the total
- The US also had the largest number of individuals sharing file instances with 19% of the total
- Some countries may have lower rankings because of the use of FTP servers or other P2P clients

Rank by Percentage	Country	Percentage	Rank by Total File Instances
1	United States	19%	1
2	United Kingdom	7%	2
3	Canada	6%	3
4	Brazil	5%	5
5	Spain	5%	4
6	Poland	5%	6
7	France	4%	7
8	Sweden	3%	8
9	Netherlands	3%	9
10	Australia	2%	10

Top 10 countries by number of users

Enterprise Mitigation

- To help prevent loss of confidential data that could be used in identity fraud, enterprises should:
  - Implement database encryption
  - Limit access to databases including use of least privilege
  - Employ secure communications channels to transfer sensitive information
  - Ensure that endpoint security measures are in place to prevent confidential information from being copied to portable media such as USB devices and compact discs

Consumer Mitigation

- To help prevent the loss of confidential information that could be used in identity fraud, consumers should:
  - Employ email filtering solutions to help block fraudulent messages such as those used in phishing attacks
  - Use defense-in-depth strategies like antivirus software, firewalls, and anti-phishing toolbars
  - Limit the amount of sensitive personal information stored on their computers
  - Utilize strong passwords and change them on a regular basis
  - Do not store online account credentials using the Web browser's "remember password" feature

Thank You!

Jeff Guilfoyle

jeff_guilfoyle@symantec.com