Quantitative Cyber-Security

Colorado State University

Yashwant K Malaiya

CS559

L24

CSU Cybersecurity Center
Computer Science Dept

Presentations/Final Report

Slides: Post 24 hours in advance. Use the format given with title, name, abstract, slides and one reference link.

Th Nov 19, 2020

1. Al Amin, Md. **Quantitative Modeling of Economics of Ransomware**
2. Neumann, Don. **Quantitative Modeling of Economics of Ransomware**
3. Haynes, Katherine, **Combining Adversarial Synthesized Data and DeepNeural Networks to Improve Phishing Detection**
4. Houlton, Sarah, **Cyber Crime and Criminals: Their Methods and Motivations**
5. Jepsen, Waylon, **Motivation and Methods of North Korea's Cyber Criminals**
6. Rodriguez, Luis, **A Quantitative Examination of Phishing**

- Peer reviews will be needed.

Colorado State University

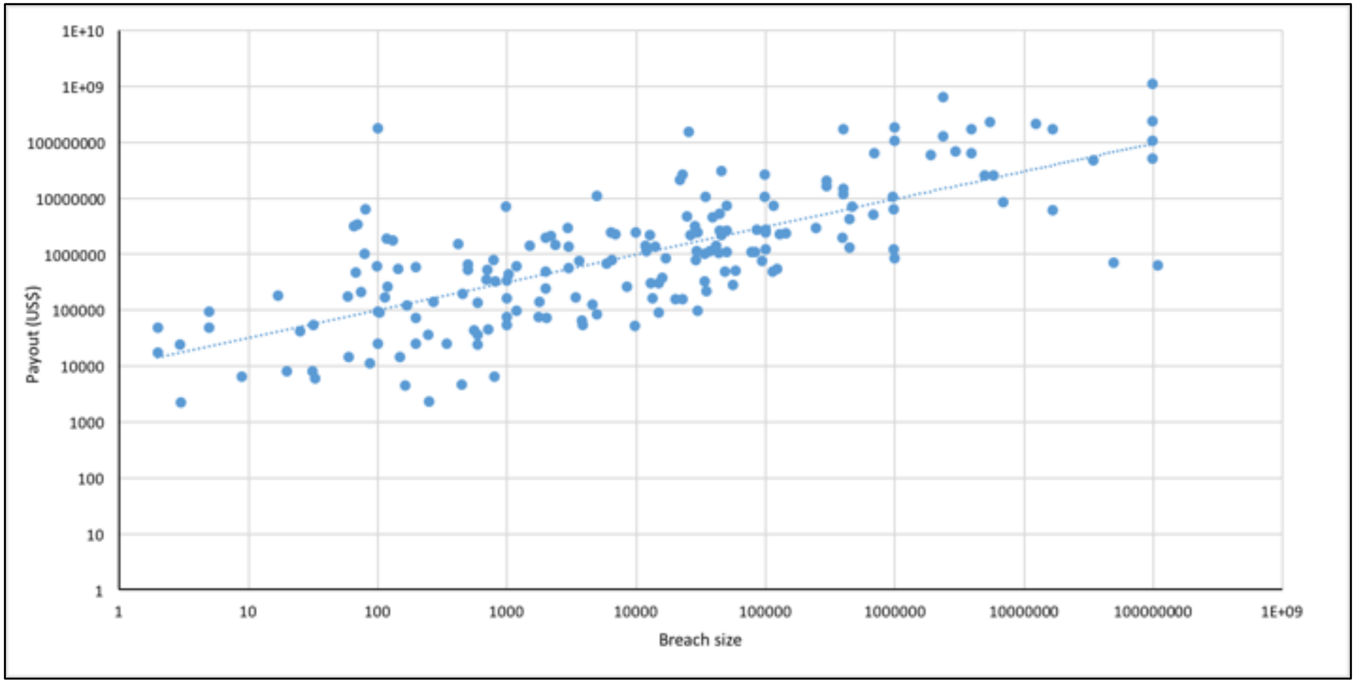
Presentations

- Each presentation is limited to 10 minutes and two minutes are allowed for discussions. I suggest using no more than 20 slides. You should practice and time your presentation.
- These sessions will be live using MS Teams. Everyone is required to participate, ask questions and take notes. Distance students who are working full time need to provide a video with link sent to cs559@cs.colostate.edu at least **24 hours** before the presentation (to allow us to ensure it works properly).
- Students with closely related presentations should coordinate among themselves to minimize overlap.

Topics

- Review
  - Breach cost
  - Impact of a breach on the stock price
- Vulnerability markets
  - Vulnerability Rewards Programs
  - Black and gray markets

The breach cost vs. breach size



Verizon 2015 data, the claim amount vs. breach size. Note log-log axes.

Our proposed model

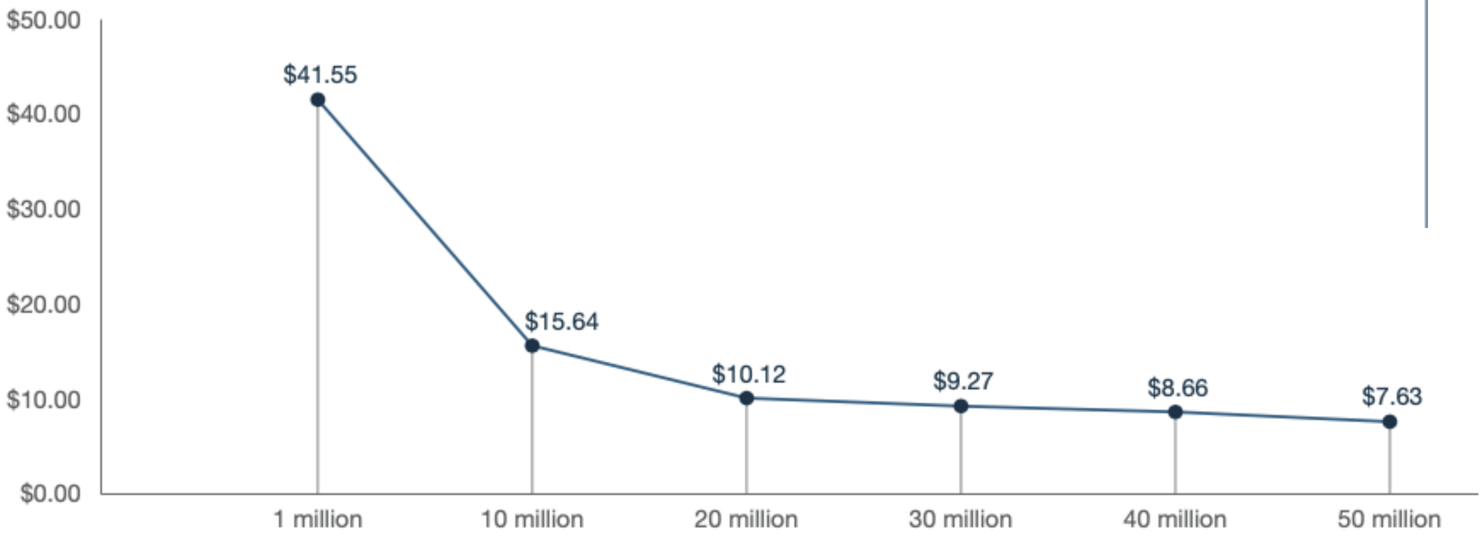
$$\boldsymbol{Total\ breach\ cost} = a * size \wedge b$$

for breach sizes bigger than or equal to 1000 records

Nonlinearity caused by ***economy of scale;*** *thus b should be < 1.*

Colorado State University

Per capita cost of a mega breach



- At 50 million records, we estimate a per capita cost of $7.63. Per capita cost flattens out beyond 50 million records.
- From 2018 Cost of a Data Breach Study: Global Overview, IBM/Ponemon

Partial Costs: average breach

		Cost in $million in category					
Category	**Percent**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**
Lost business	39.4	1.57	1.63	1.51	1.45	1.42	1.52
Ex-post response	28.8	1.07	1.1	0.93	1.02	1.07	0.99
Notification	6.2	0.17	0.18	0.19	0.16	0.21	0.24
Detection and escalation	25.6	0.98	1.09	0.99	1.23	1.22	1.11

Detection and escalation: Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion and to report the breach of protected information to appropriate personnel within a specified time period.

Notification: Activities that enable the company to notify individuals who had data compromised in the breach (data subjects) as regulatory activities and communications.

Post data breach response: Processes set up to help individuals affected by the breach to communicate with the company, as well as costs associated with redress activities and reparation with data subjects and regulators.

Lost business: Activities associated with cost of lost business including customer churn, business disruption, and system downtime. Also included in this category are the costs of acquiring new customers and costs related to revenue loss.

Total cost: sum of the four partial costs.

Chang, Gao, Lee 2020 **Hypotheses**

- **Hypothesize 1 (H1).** *The announcement of a data breach has a negative effect on the short-term market value of the breached company.*
- **Hypothesize 2 (H2).** *The announcement of data breach has a negative effect on the long-term market value of the breached company.*
- **Hypothesize 3.1 (H3.1).** *The size of the data breach is positively associated with a higher negative return on the short-term market value of the breached company.*
- **Hypothesize 3.2 (H3.2).** *The size of the data breach is positively associated with a higher negative return on the long-term market value of the breached company.*

All of them were found to hold.

The Effect of Data Theft on a Firm's Short-Term and Long-Term Market Value **2020**

Quantitative Security

Colorado State University

Yashwant K Malaiya

Summer 2019

Vulnerability markets

CSU CyberCenter
***Course Funding Program* – 2019**

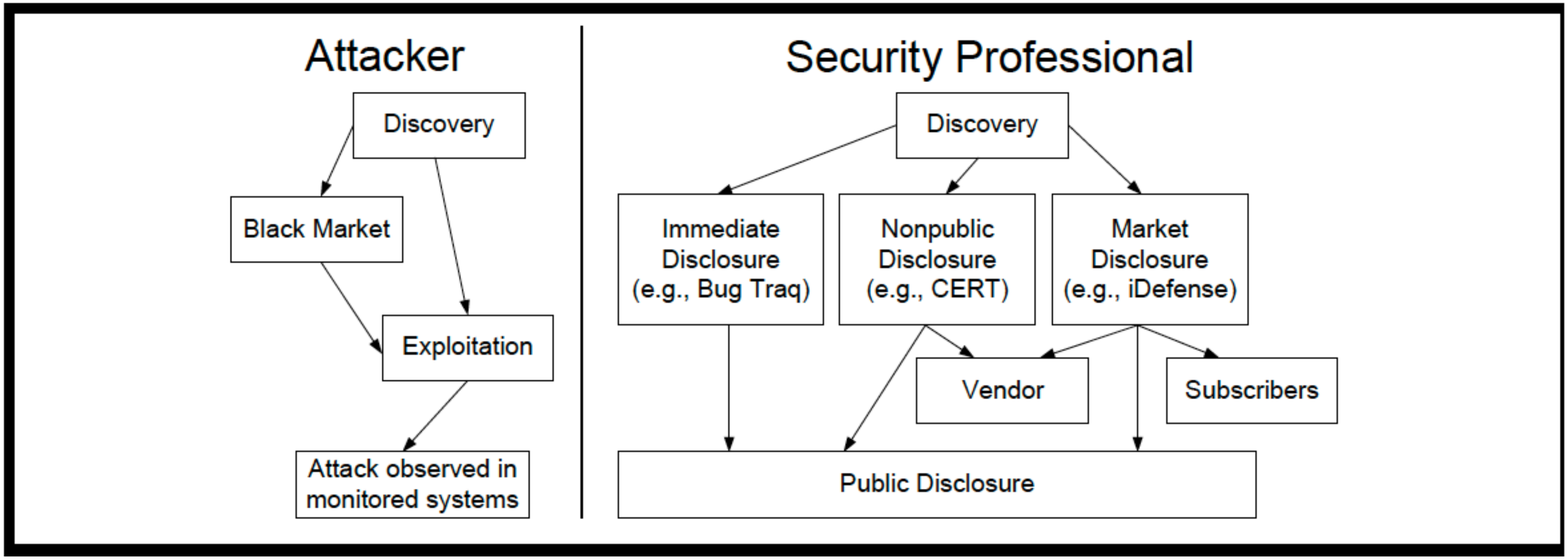
Vulnerability markets

- Vulnerability flow through the markets
- Vulnerability reward programs (VRP or bugs bounty)
- Middle Organizations
- Markets for Cybercrime Tools and Stolen Data

This topic needs further work to

- Organize available information
- Dig out numbers and trends
- Understand and model market mechanisms

Vulnerabilities & Money



Attacker

Discovery

Black Market

Exploitation

Attack observed in monitored systems

Security Professional

Discovery

Immediate Disclosure (e.g., Bug Traq)

Nonpublic Disclosure (e.g., CERT)

Market Disclosure (e.g., iDefense)

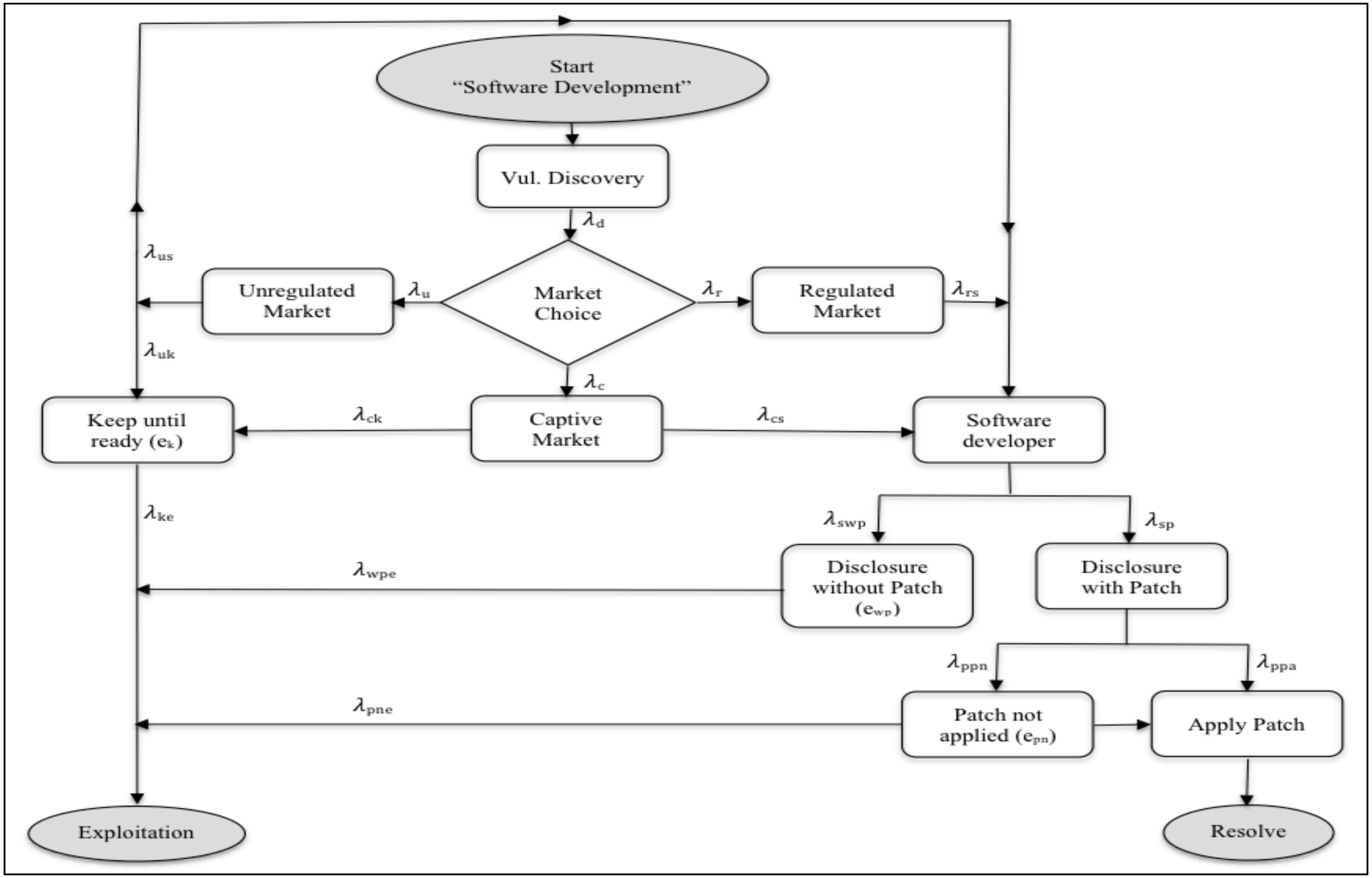
Vendor

Subscribers

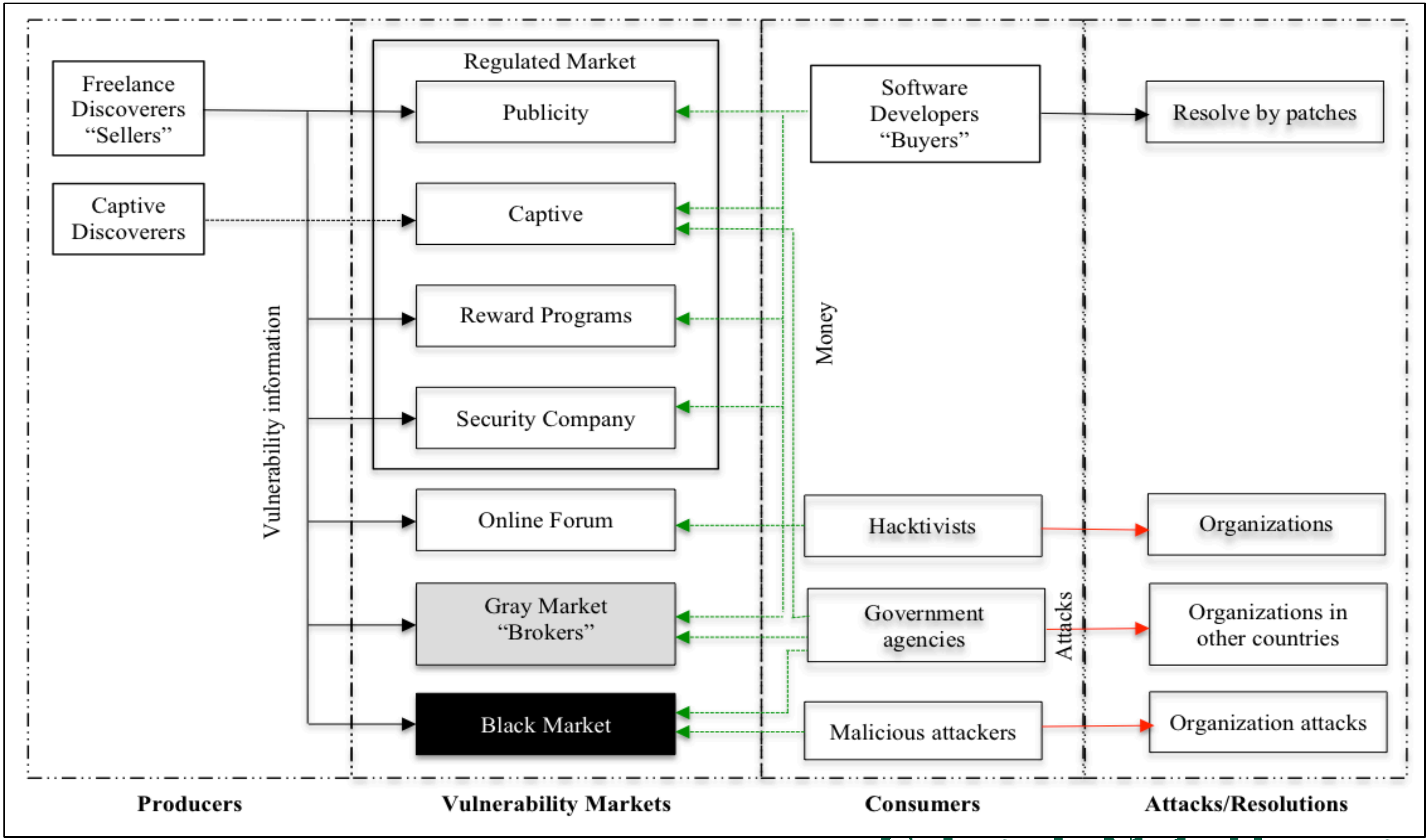
Public Disclosure

Algarni and Y. Malaiya. Software vulnerability markets: Discoverers and buyers.
Int. J. of Computer, Information Sci. and Eng., 8(3):71–81, 2014.

Vulnerability flow through markets

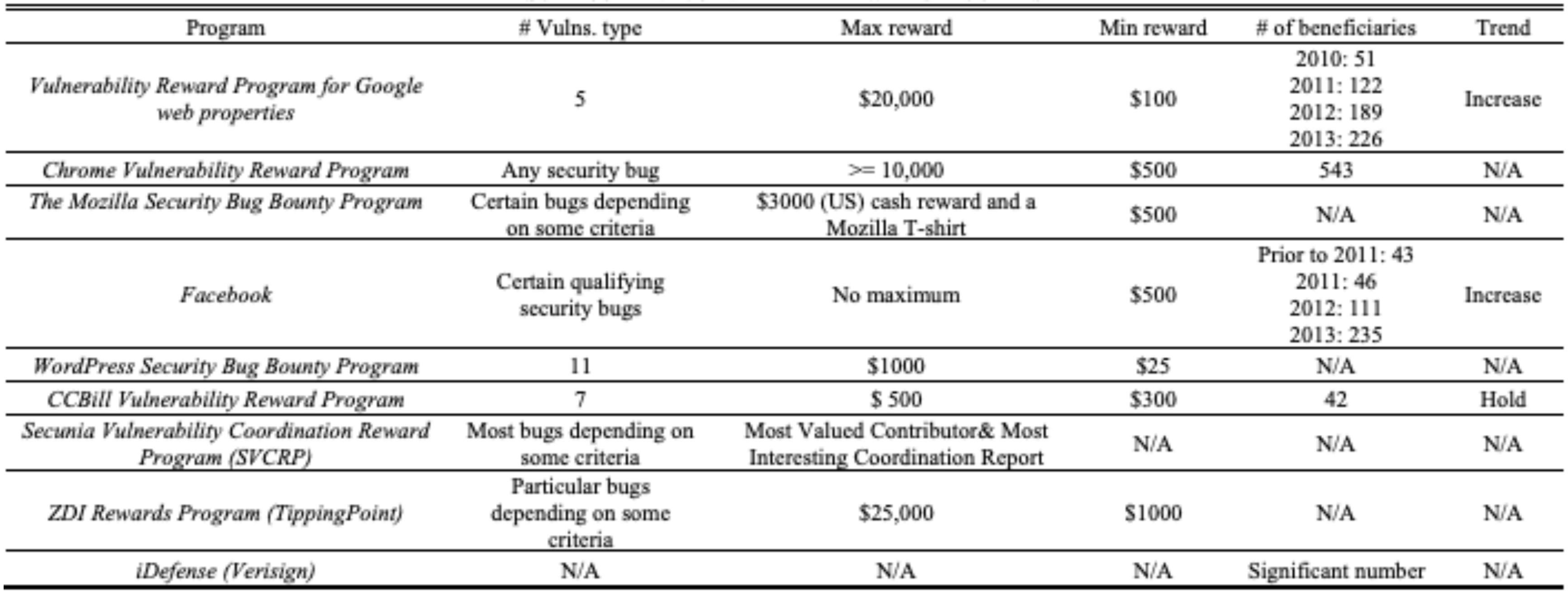


Types of Vulnerability Markets



Colorado State University

SOME CURRENT VULNERABILITY REWARDS PROGRAMS

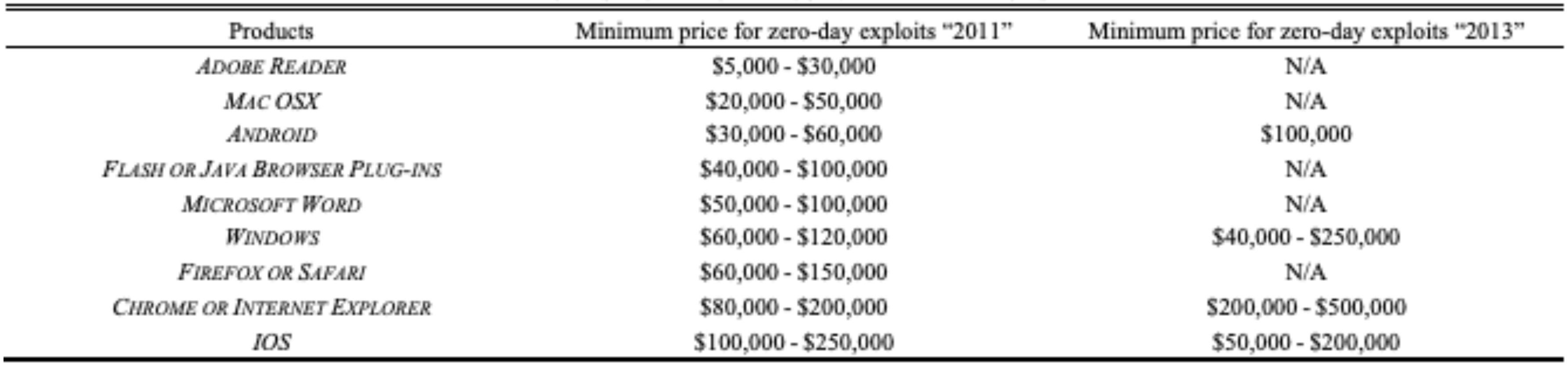


Program	# Vulns. type	Max reward	Min reward	# of beneficiaries	Trend
Vulnerability Reward Program for Google web properties	5	$20,000	$100	2010: 51 2011: 122 2012: 189 2013: 226	Increase
Chrome Vulnerability Reward Program	Any security bug	>= 10,000	$500	543	N/A
The Mozilla Security Bug Bounty Program	Certain bugs depending on some criteria	$3000 (US) cash reward and a Mozilla T-shirt	$500	N/A	N/A
Facebook	Certain qualifying security bugs	No maximum	$500	Prior to 2011: 43 2011: 46 2012: 111 2013: 235	Increase
WordPress Security Bug Bounty Program	11	$1000	$25	N/A	N/A
CCBill Vulnerability Reward Program	7	$ 500	$300	42	Hold
Secunia Vulnerability Coordination Reward Program (SVCRP)	Most bugs depending on some criteria	Most Valued Contributor& Most Interesting Coordination Report	N/A	N/A	N/A
ZDI Rewards Program (TippingPoint)	Particular bugs depending on some criteria	$25,000	$1000	N/A	N/A
iDefense (Verisign)	N/A	N/A	N/A	Significant number	N/A

Algarni and Y. Malaiya. Software vulnerability markets: Discoverers and buyers.
Int. J. of Computer, Information Sci. and Eng., 8(3):71–81, 2014.

[Needs update]

PRICE LIST FOR ZERO-DAY VULNERABILITY EXPLOITS



Products	Minimum price for zero-day exploits "2011"	Minimum price for zero-day exploits "2013"
Adobe Reader	$5,000 - $30,000	N/A
Mac OSX	$20,000 - $50,000	N/A
Android	$30,000 - $60,000	$100,000
Flash or Java Browser Plug-ins	$40,000 - $100,000	N/A
Microsoft Word	$50,000 - $100,000	N/A
Windows	$60,000 - $120,000	$40,000 - $250,000
Firefox or Safari	$60,000 - $150,000	N/A
Chrome or Internet Explorer	$80,000 - $200,000	$200,000 - $500,000
IOS	$100,000 - $250,000	$50,000 - $200,000

[Needs update]

Bounty programs

Votipka, R. Stevens, E. Redmiles, J. Hu and M. Mazurek, "Hackers vs. testers: A comparison of software vulnerability discovery processes", *2018 IEEE Symposium on Security and Privacy*, pp. 134-151, 2018.

Bounty Programs: sources of information

- Finifter et al. studied the Firefox and Chrome bug bounty programs.
  - Chromium and Firefox public bug trackers provide the email addresses of anyone who has submitted a bug report
- Maillart et al. studied 35 public HackerOne bounty programs,
  - finding that hackers tend to focus on new bounty programs and that a significant portion of vulnerabilities are found shortly after the program starts.
- HackerOne , maintains profile pages for each of its members which commonly include the hacker’s contact information.
- To identify individuals who successfully submitted vulnerabilities, they followed the process given by Finifter et. al. by searching for specific security-relevant labels

Demographics

Their profile of subjects was similar to HackerOne and BugCrowd.

Age: Their hacker population studied was 60% under 30 and 90% under 40 years old.

- 90% of HackerOne’s 70,000 users were younger than 34;
- 60% of BugCrowd’s 38,000 users are 18-29 and 34% are 30-44 years old.

Education: 93% of their hackers have attended college and 33% have a graduate degree.

- 84% of BugCrowd hackers have attended college and
- 21% have a graduate degree

Heuristics for finding vulnerabilities

Where are the vulnerabilities are likely

- Code segments that they expect were not heavily tested previously
  - where developers are “not paying attention to it [security] as much.”
- Parts of the code where multiple bugs were previously reported
  - “There were issues with those areas anyway. . . so I figured that that was probably where there was most likely to be security issues...bugs cluster.”
- When code is new (e.g., rushed to release to fix a major feature issue), or when they do not think the developers understand the underlying systems they are using (e.g., they noticed an odd implementation of a standard feature).
- Additionally, some hackers also looked at old code (e.g., developed prior to the company performing stringent security checks) and features that are rarely used.

Where attacks are more rewarding

- Testers determine value by estimating the negative effect to the company if exploited or if the program fails a mandated audit (e.g., HIPAA, FERPA)
- They tend to focus on features that are most commonly used by their user base and areas of the code that handle sensitive data (e.g., passwords, financial data).
    - An informant said he considers “usage of the site, [that is] how many people are going to be on a certain page or certain area of the site, [and] what’s on the page itself, [such as] forms” to determine where a successful attack would have the most impact.

How to maximize VRP payouts?

- Hackers are more likely to participate in a program whenever the bounties are higher and bounty prices increase with vulnerability severity.
- Two strategies when deciding how to best maximize their collective payouts.
  - The first strategy seeks out programs where the hacker has a competitive advantage based on specialized knowledge or experience that makes it unlikely that others will find other similar vulnerabilities. Hackers following this strategy participate in bug bounties even if they are unlikely to receive immediate payouts, because they can gain experience that will help them later find higher-payout vulnerabilities.
  - The other strategy is to primarily look for simple vulnerabilities in programs that have only recently started a bug bounty program.
    - In this strategy, the hackers race to find as many low-payout vulnerabilities as possible as soon as a program is made public. Hackers dedicate little time to each program to avoid the risk of report collisions and switch to new projects quickly.
    - The informant said that he switches projects frequently, just looking for "low-hanging fruit," because "somebody else could get there before you, while you are still hitting your head on the wall on this old client."

An empirical study of bug bounty programs

Walshe, T. and Simpson, A. An empirical study of bug bounty programs. In 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF), pages 35– 44.

Examples of bugs bounty programs:

- Swiss government launched a program offering e132,000 for hackers to find vulnerabilities in an e- voting system. Rewards of up to e44,000 were made available to hackers who discovered undetectable ways of manipulating votes.
- US Department of Defense (DoD) launched the ‘Hack the Pentagon’ pilot program in April 2016, with the aim of assessing the benefit of opening up vulnerability discovery to hackers. Within six hours 138 vulnerabilities were found and reported.
- HackerOne platform: As of January 2019, the top 25 companies using have used it to obtain reports for
  - over 19,000 vulnerabilities,
  - at an average of 0.71 vulnerabilities reported for each day the program is run
  - resulting in $11.9 million being paid out to hackers for successfully finding vulnerabilities.
- Assumption in this paper: an average value of $65,133 will be used to represent the cost of hiring an additional software engineer (based on UK salary).

An empirical study of bug bounty programs

- The daily cost to operate each program is reported as $485 for Google and $658 for Mozilla; over the course of a year, the total cost is $177,025 ($485 × 365 days) and $240,170 ($658 × 365 days).
- This is broadly comparable to the salary of three or four additional software engineers, with the current average salary of a software engineer being $65,133. The
- Wooyun served as the predominant platform in China from 2010 until being shut down in 2016 [31].

- **An Empirical Study of Web Vulnerability Discovery Ecosystems**

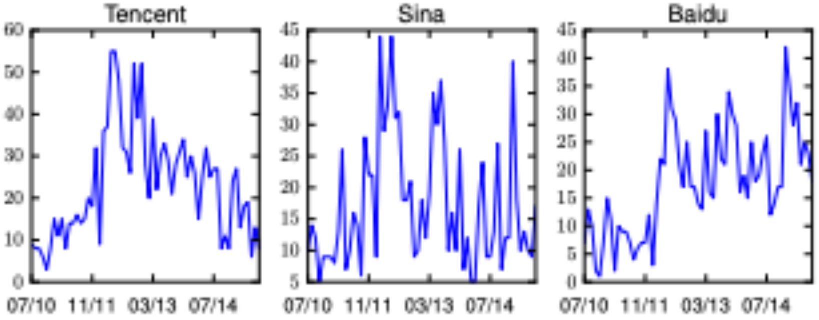


Figure 14: Trend of vulnerability report count for three organizations on Wooyun.

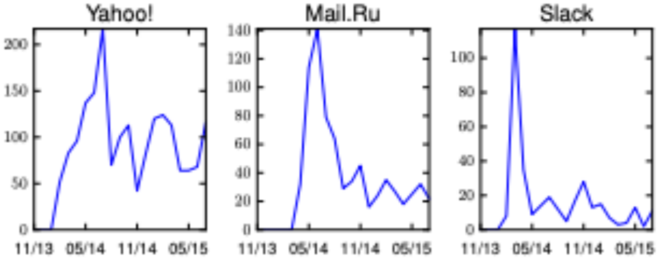
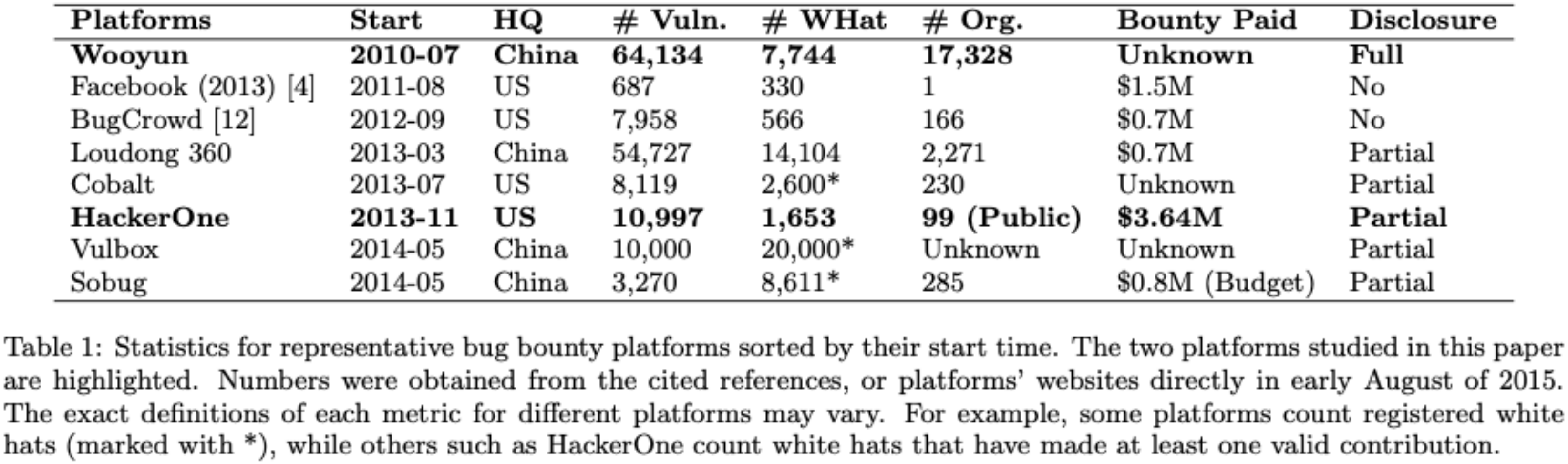


Figure 15: Trend of vulnerability report count for three organizations on HackerOne.

An empirical study of bug bounty programs

An Empirical Study of Web Vulnerability Discovery Ecosystems



Platforms	Start	HQ	# Vuln.	# WHat	# Org.	Bounty Paid	Disclosure
Wooyun	**2010-07**	**China**	**64,134**	**7,744**	**17,328**	**Unknown**	**Full**
Facebook (2013) [4]	2011-08	US	687	330	1	$1.5M	No
BugCrowd [12]	2012-09	US	7,958	566	166	$0.7M	No
Loudong 360	2013-03	China	54,727	14,104	2,271	$0.7M	Partial
Cobalt	2013-07	US	8,119	2,600*	230	Unknown	Partial
HackerOne	**2013-11**	**US**	**10,997**	**1,653**	**99 (Public)**	**$3.64M**	**Partial**
Vulbox	2014-05	China	10,000	20,000*	Unknown	Unknown	Partial
Sobug	2014-05	China	3,270	8,611*	285	$0.8M (Budget)	Partial

Table 1: Statistics for representative bug bounty platforms sorted by their start time. The two platforms studied in this paper are highlighted. Numbers were obtained from the cited references, or platforms' websites directly in early August of 2015. The exact definitions of each metric for different platforms may vary. For example, some platforms count registered white hats (marked with *), while others such as HackerOne count white hats that have made at least one valid contribution.

Markets for Cybercrime Tools and Stolen Data

Markets for Cybercrime Tools and Stolen Data - Hackers' Bazaar, L. Ablon, M. C. Libicki and A. A. Golay, RAND Corporation, 2014 source for next several slides

Comments

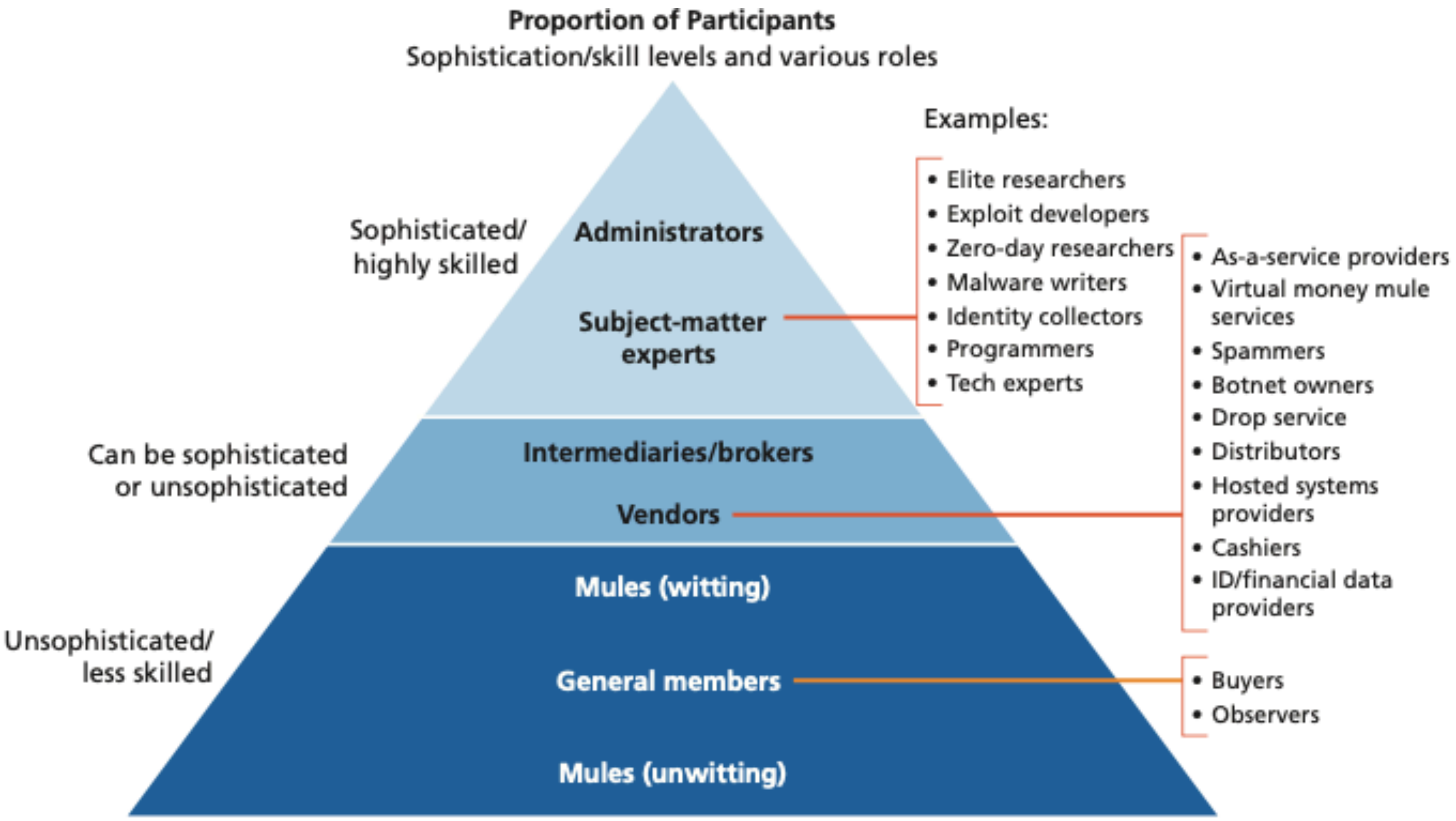
- The RAND Corporation is a research organization that develops solutions to public policy challenges throughout the world.
- The situation has advanced significantly since then. Numbers and relative magnitudes may have changed.
- Some activity may have shifted to legitimate markets because of reward programs (VRPs).
- Crime can only be defined within a legal system
  - Laws within a country
  - International law as defined by treaties and protocols.
  - Nation against nation – cyber warfare or economic intelligence gathering may be consider legitimate by some/many/all actors. Some countries may tolerate crime as long as it is against their rivals.
- Governments may be the major players in the vulnerability markets.

Markets for Cybercrime Tools and Stolen Data

Markets for Cybercrime Tools and Stolen Data - Hackers' Bazaar, L. Ablon, M. C. Libicki and A. A. Golay, RAND Corporation, 2014

- The black market is not so much a market as it is a collection of activities that range from simple to extremely sophisticated and operate all over the world, from New Jersey to Nigeria to China and Southeast Asia.
- When we say *market(s)*, we mean the collection of (skilled and unskilled) suppliers, vendors, potential buyers, and intermediaries for goods or services surrounding digitally based crimes.
- A marketplace is the location in which a market operates—in our case, it is typically virtual or digital.
- Some underground organizations can reportedly reach 70,000–80,000 people, with a global footprint that brings in hundreds of millions of dollars
  - e.g., carder.su, a now-defunct forum that was dedicated to all aspects of credit card fraud.
- One expert estimates that in the mid-2000s, approximately 80% of black-market participants were freelance (the rest being part of criminal groups), but has declined and is closer to 20&% today. [Update needed]

Different Levels of Participants in the Underground Market



Market(s): (skilled and unskilled) suppliers, vendors, potential buyers, and intermediaries for goods or services surrounding digitally based crimes.

Markets for Cybercrime Tools and Stolen Data

Markets for Cybercrime Tools and Stolen Data - Hackers' Bazaar, L. Ablon, M. C. Libicki and A. A. Golay, RAND Corporation, 2014

- Zero-day prices range from a few thousand dollars to $200,000–$300,000, depending on the severity of the vulnerability, complexity of the exploit, how long the vulnerability remains undisclosed, the vendor product involved, and the buyer.
- Some estimates even go up to $1 million but are often thought to be exaggerated.
- Third parties: VUPEN, Endgame, Netragard, ReVuln [Update needed]
- Google's bounty program usually pays $3,000 to $5,000, with some non-Chrome exploits fetching up to $20,000 and up to $150,000 for Chrome exploits. [Update needed]

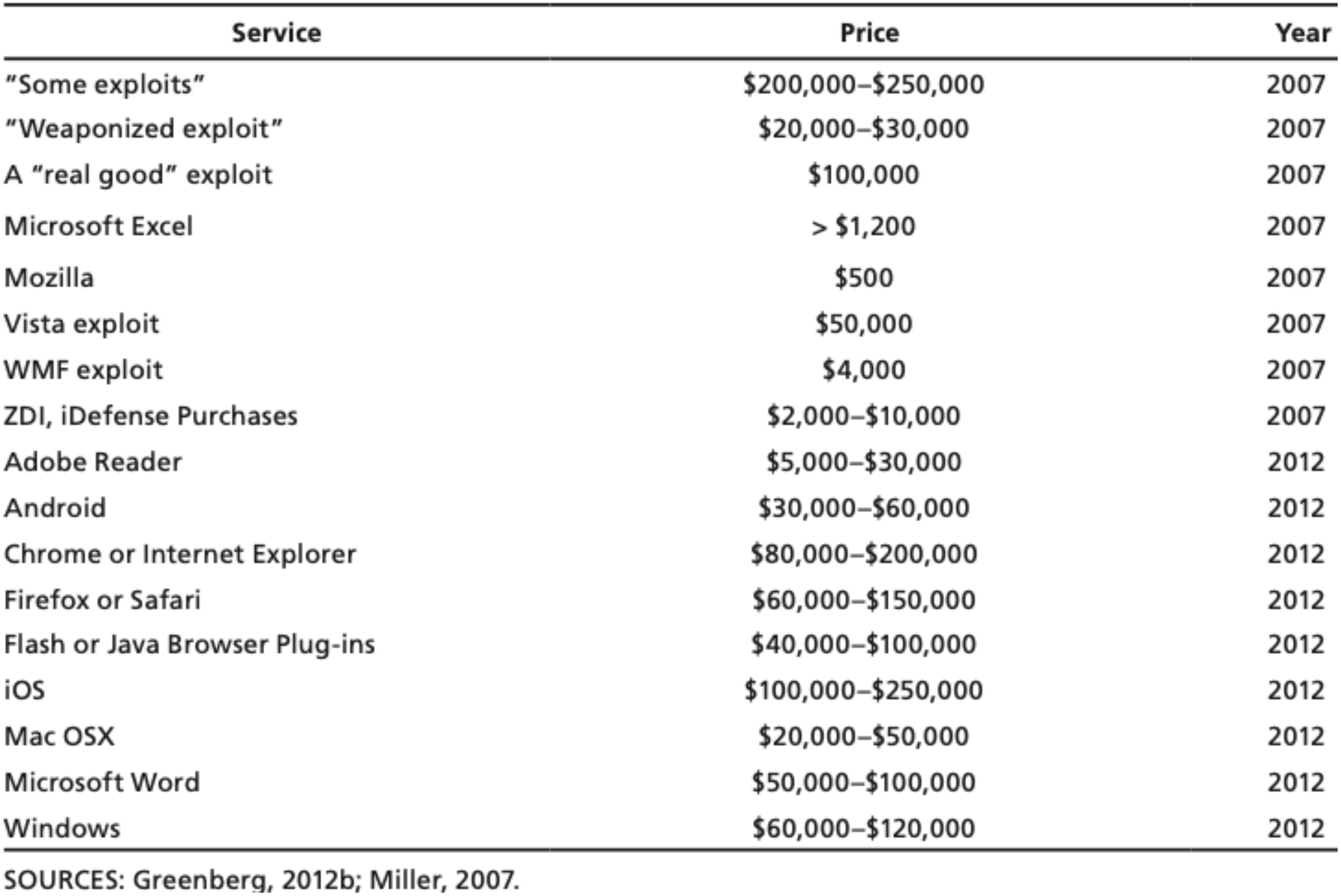
- Prices on both the black and gray markets run much higher than the bounties that companies pay to have bugs in their own systems disclosed.
- Some sources say a researcher could earn 10–100 times what a software vendor with a bug bounty would pay; for example. [Update needed]
- HP’s Zero Day Initiative and Verisign’s iDefense Vulnerability Contributor Program only pay up to $10,000 for exploits. [Update needed]
- As a result, some of those who offer bug bounties, such as Google, have started to increase their rewards.
- Some experts say the price for zero-days is decreasing significantly, and others say they are getting more expensive (along with advanced delivery mechanisms). A price drop may indicate higher volume (i.e., higher supply), or less demand (i.e., less wanted, something else has become more valuable). [Update needed]

Market Breakdown

An estimate breaks down the market thusly: [Update needed]

- 70 percent individuals or small groups
- 20 percent criminal organizations
- 5 percent cyberterrorists
- 4 percent state-sponsored players
- 1 percent hacktivists (“pseudo cyberarmies,” not Anonymous)

Zero-Day Prices Over Time



Service	Price	Year
"Some exploits"	$200,000–$250,000	2007
"Weaponized exploit"	$20,000–$30,000	2007
A "real good" exploit	$100,000	2007
Microsoft Excel	> $1,200	2007
Mozilla	$500	2007
Vista exploit	$50,000	2007
WMF exploit	$4,000	2007
ZDI, iDefense Purchases	$2,000–$10,000	2007
Adobe Reader	$5,000–$30,000	2012
Android	$30,000–$60,000	2012
Chrome or Internet Explorer	$80,000–$200,000	2012
Firefox or Safari	$60,000–$150,000	2012
Flash or Java Browser Plug-ins	$40,000–$100,000	2012
iOS	$100,000–$250,000	2012
Mac OSX	$20,000–$50,000	2012
Microsoft Word	$50,000–$100,000	2012
Windows	$60,000–$120,000	2012

SOURCES: Greenberg, 2012b; Miller, 2007.

[Update needed]

Black markets participants

- Russia leads in terms of quality. Different groups operate in distinct spaces. [Update needed]
- For example, there are Vietnamese groups that mainly focus on eCommerce,
- A majority of Russians, Romanians, Lithuanians, Ukrainians, and other Eastern Europeans mainly focus on attacking financial institutions.
- Chinese hackers are believed to focus more on IP.
- There has been a migration toward U.S.-based actors becoming more involved; many U.S. participants are thought to be involved in financial crime.

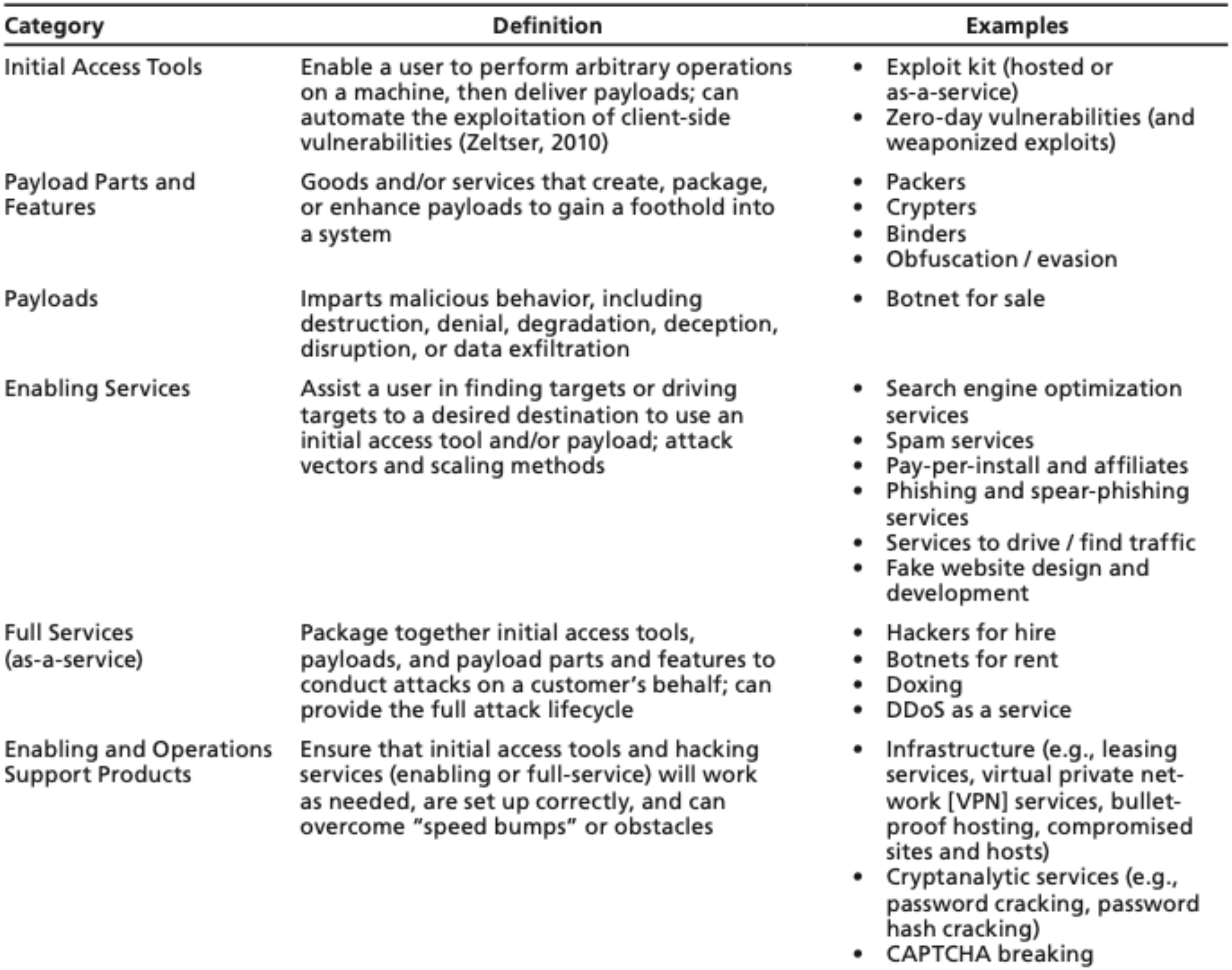
I am taking this from the RAND report. This is a difficult slide, considering we are an international class.

As some of you know, some of the IRS call scams and fake Windows support claims originate from India, and money transfer scams may originate from Nigeria. The bank account verification scams in India originate from the Jamtara village in Jharkhand.

Business channels & Goods

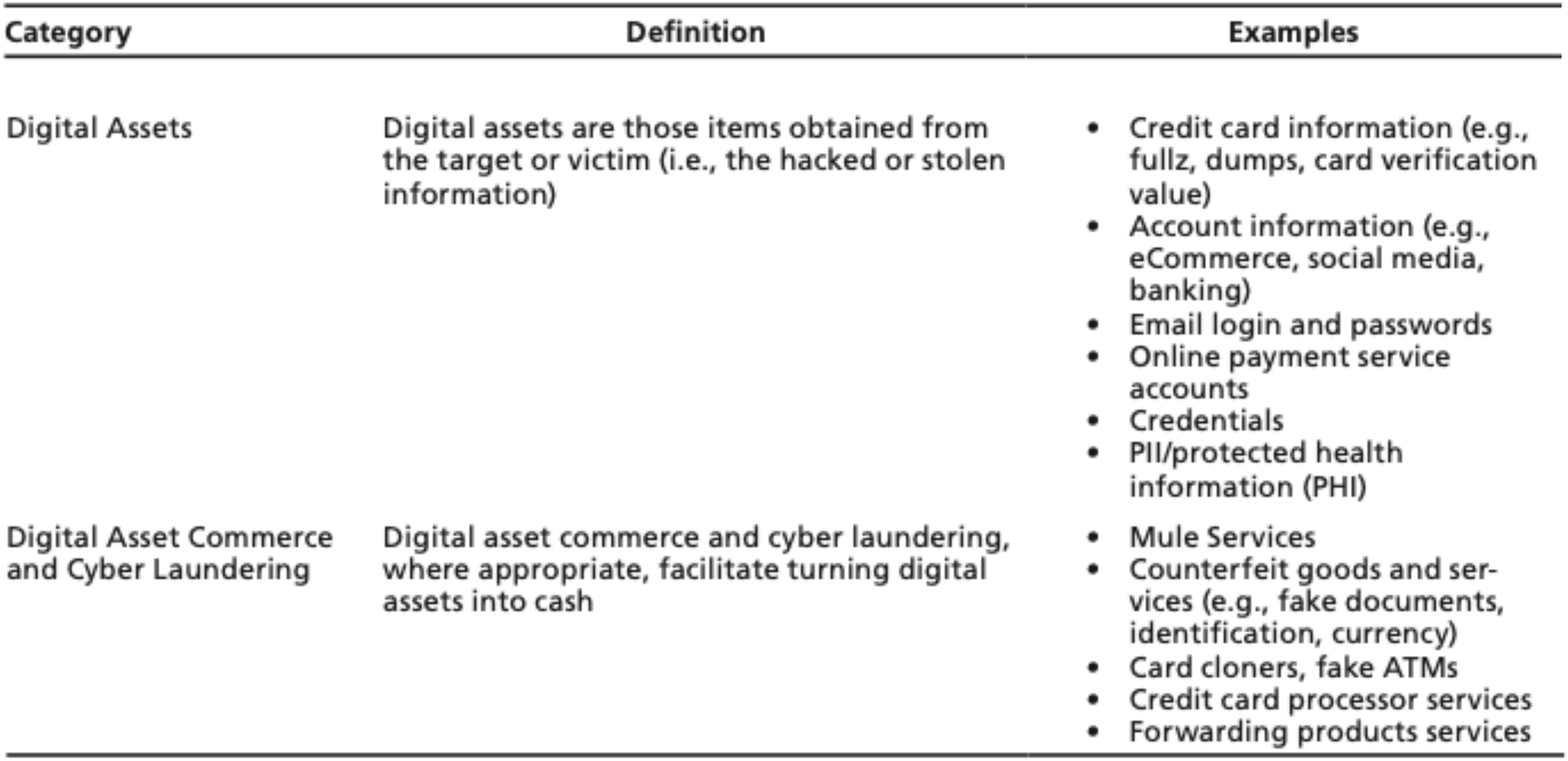
- Channels initially were largely a combination of bulletin-board-style web forums, email, and instant-messaging platforms that support both private messaging or open chat rooms (e.g., IRC Protocol, ICQ, Jabber, and QQ), and email.
- Today's participants also commonly frequent online stores where buyers can choose their desired product, pay with digital currency, like the legitimate eCommerce storefronts.
- They may use off-the-record messaging, the encryption scheme GNU Privacy Guard (GPG), private Twitter accounts, and anonymizing networks such as Tor, Invisible Internet Project (I2P), and Freenet.
- Products include both goods (hacking tools, digital assets) and services (as-a-service hacking, digital asset handling).
  - Hacking goods consist of tools that help gain initial access on a target, parts and features to package within a payload, and payloads to have an intended effect on a target.
  - Hacking services consist of enabling services to help scale or deliver a payload, and full-service capabilities that can provide a full-attack lifecycle

Goods and Services on the Black Market



Category	Definition	Examples
Initial Access Tools	Enable a user to perform arbitrary operations on a machine, then deliver payloads; can automate the exploitation of client-side vulnerabilities (Zeltser, 2010)	• Exploit kit (hosted or as-a-service) • Zero-day vulnerabilities (and weaponized exploits)
Payload Parts and Features	Goods and/or services that create, package, or enhance payloads to gain a foothold into a system	• Packers • Crypters • Binders • Obfuscation / evasion
Payloads	Imparts malicious behavior, including destruction, denial, degradation, deception, disruption, or data exfiltration	• Botnet for sale
Enabling Services	Assist a user in finding targets or driving targets to a desired destination to use an initial access tool and/or payload; attack vectors and scaling methods	• Search engine optimization services • Spam services • Pay-per-install and affiliates • Phishing and spear-phishing services • Services to drive / find traffic • Fake website design and development
Full Services (as-a-service)	Package together initial access tools, payloads, and payload parts and features to conduct attacks on a customer's behalf; can provide the full attack lifecycle	• Hackers for hire • Botnets for rent • Doxing • DDoS as a service
Enabling and Operations Support Products	Ensure that initial access tools and hacking services (enabling or full-service) will work as needed, are set up correctly, and can overcome "speed bumps" or obstacles	• Infrastructure (e.g., leasing services, virtual private network [VPN] services, bulletproof hosting, compromised sites and hosts) • Cryptanalytic services (e.g., password cracking, password hash cracking) • CAPTCHA breaking

Goods and Services on the Black Market

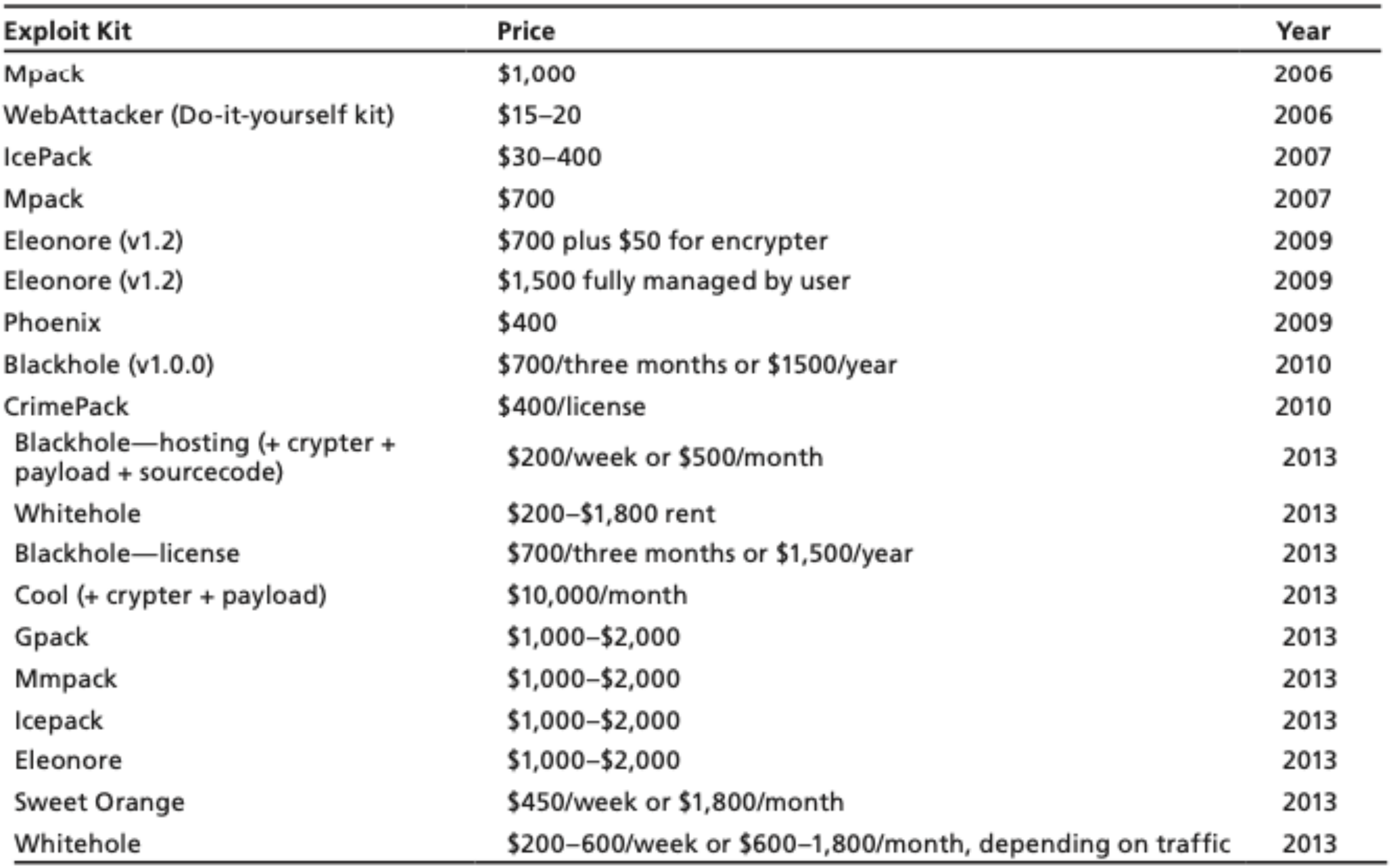


Category	Definition	Examples
Digital Assets	Digital assets are those items obtained from the target or victim (i.e., the hacked or stolen information)	• Credit card information (e.g., fullz, dumps, card verification value) • Account information (e.g., eCommerce, social media, banking) • Email login and passwords • Online payment service accounts • Credentials • PII/protected health information (PHI)
Digital Asset Commerce and Cyber Laundering	Digital asset commerce and cyber laundering, where appropriate, facilitate turning digital assets into cash	• Mule Services • Counterfeit goods and services (e.g., fake documents, identification, currency) • Card cloners, fake ATMs • Credit card processor services • Forwarding products services

Pricing

- The black market can be more profitable than the illegal drug trade
  - Links to end-users are more direct, and because worldwide distribution is accomplished electronically, the requirements are negligible.
  - This is because a majority of players, goods, and services are online-based and can be accessed, harnessed, or controlled remotely, instantaneously.
  - "Shipping" digital goods may only require an email or download, or a username and password to a locked site. This enables greater profitability.
- According to experts, black markets operate the same ways traditional markets do.
  - Easily exchanged goods, such as PII or account data, are prey to the normal microeconomic fluctuations of supply and demand.
  - By contrast, stolen-to-order, nonfungible goods—such as new technology designs, details on R&D activities, mergers and acquisitions—can command a very high price, provided that the right buyer exists.
  - A Twitter account costs more to purchase than a stolen credit card because the former's account credentials potentially have a greater yield.
    - [2020] A 17-year-old stole twitter accounts of Elon Musk, Bill Gates, Kanye West, Joseph R. Biden Jr., Barack Obama and sold them for $180,000 in Bitcoins.

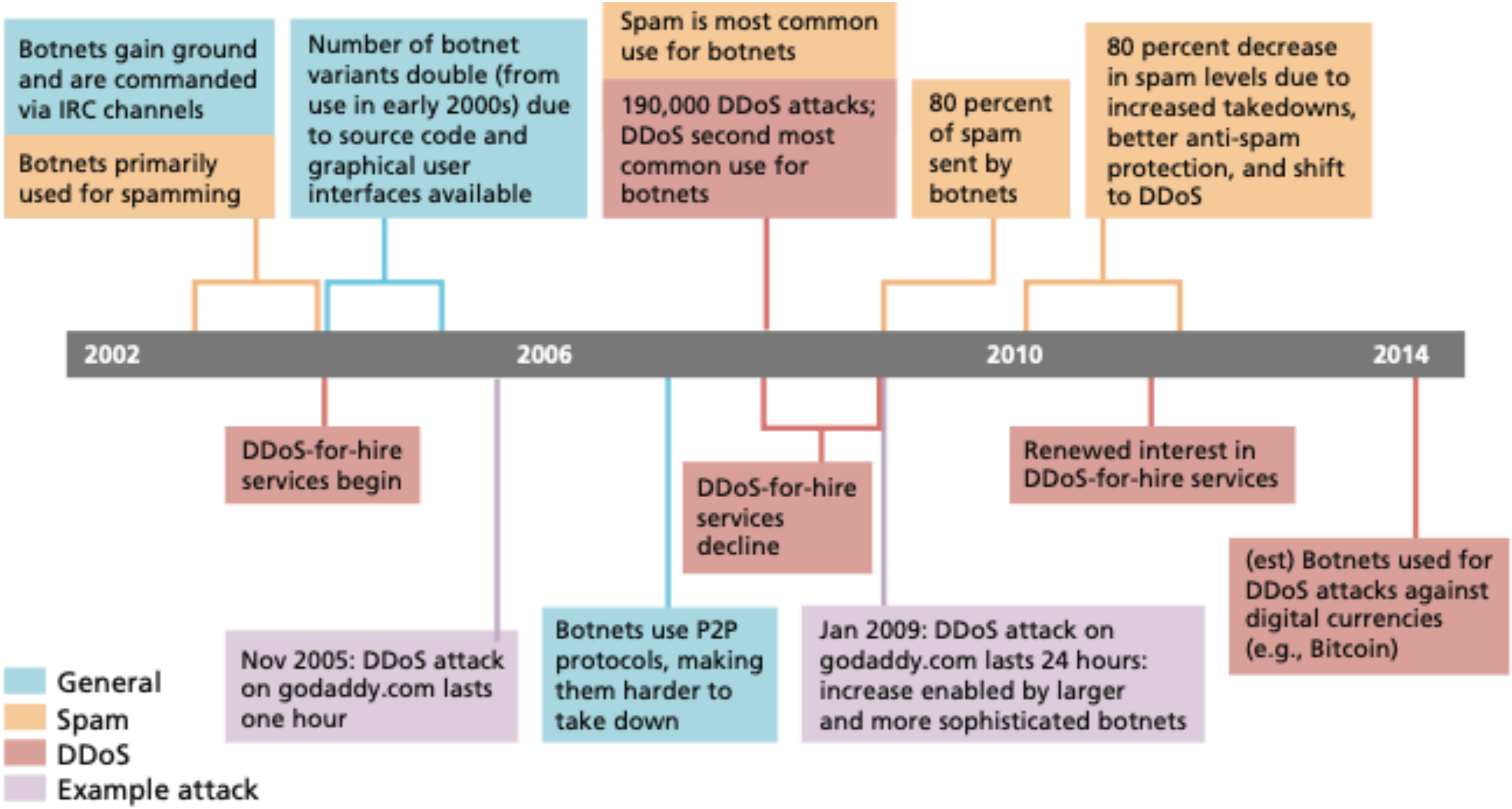
Exploit Kit Prices Over Time



Exploit Kit	Price	Year
Mpack	$1,000	2006
WebAttacker (Do-it-yourself kit)	$15–20	2006
IcePack	$30–400	2007
Mpack	$700	2007
Eleonore (v1.2)	$700 plus $50 for encrypter	2009
Eleonore (v1.2)	$1,500 fully managed by user	2009
Phoenix	$400	2009
Blackhole (v1.0.0)	$700/three months or $1500/year	2010
CrimePack	$400/license	2010
Blackhole—hosting (+ crypter + payload + sourcecode)	$200/week or $500/month	2013
Whitehole	$200–$1,800 rent	2013
Blackhole—license	$700/three months or $1,500/year	2013
Cool (+ crypter + payload)	$10,000/month	2013
Gpack	$1,000–$2,000	2013
Mmpack	$1,000–$2,000	2013
Icepack	$1,000–$2,000	2013
Eleonore	$1,000–$2,000	2013
Sweet Orange	$450/week or $1,800/month	2013
Whitehole	$200–600/week or $600–1,800/month, depending on traffic	2013

- Partial table

Botnet Timeline



2002 2006 2010 2014

Botnets gain ground and are commanded via IRC channels

Botnets primarily used for spamming

Number of botnet variants double (from use in early 2000s) due to source code and graphical user interfaces available

Spam is most common use for botnets

190,000 DDoS attacks; DDoS second most common use for botnets

80 percent of spam sent by botnets

80 percent decrease in spam levels due to increased takedowns, better anti-spam protection, and shift to DDoS

DDoS-for-hire services begin

Nov 2005: DDoS attack on godaddy.com lasts one hour

Botnets use P2P protocols, making them harder to take down

DDoS-for-hire services decline

Jan 2009: DDoS attack on godaddy.com lasts 24 hours: increase enabled by larger and more sophisticated botnets

Renewed interest in DDoS-for-hire services

(est) Botnets used for DDoS attacks against digital currencies (e.g., Bitcoin)

🟦 General
🟧 Spam
🟥 DDoS
🟪 Example attack

This and preceding slides - material from Markets for Cybercrime Tools and Stolen Data - Hackers' Bazaar, L. Ablon, M. C. Libicki and A. A. Golay, RAND Corporation, 2014