github.com/0xjet/ccc

Crime, Conflicts and Espionage in Cyberspace

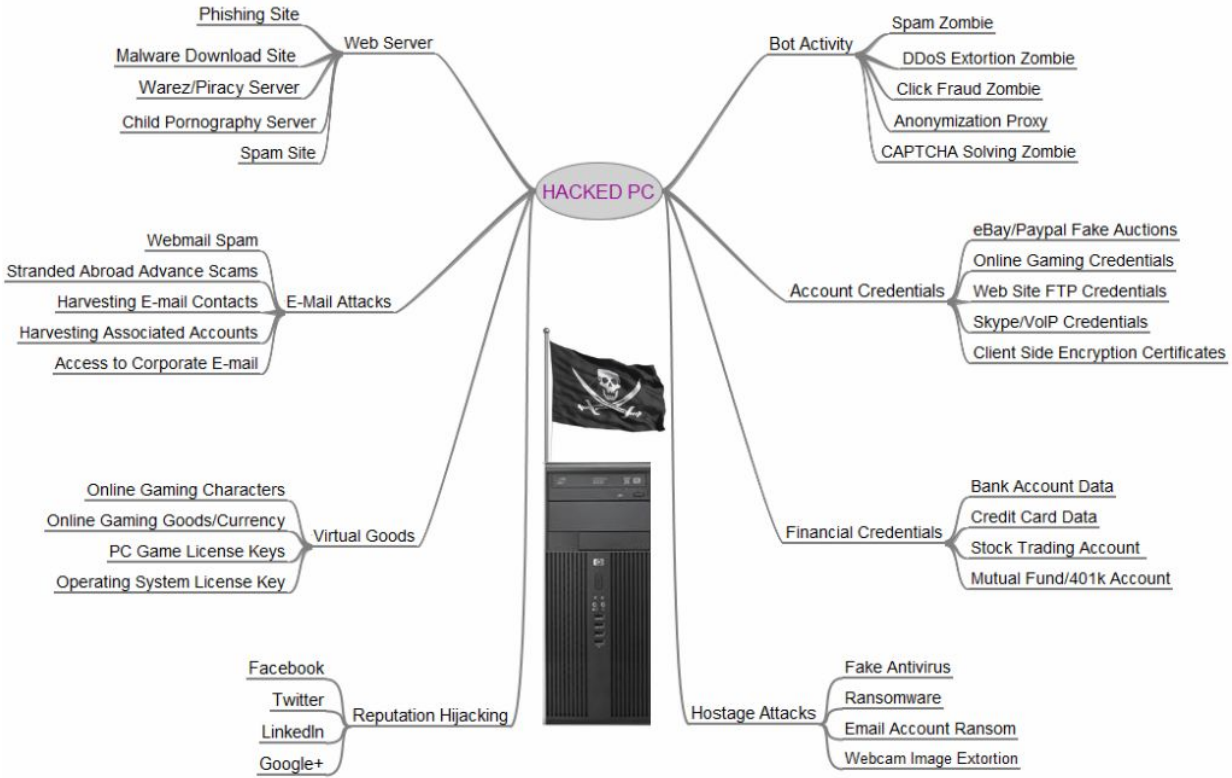
The Underground Economy of Cybercrime

Juan Tapiador (@0xjet)

uc3m

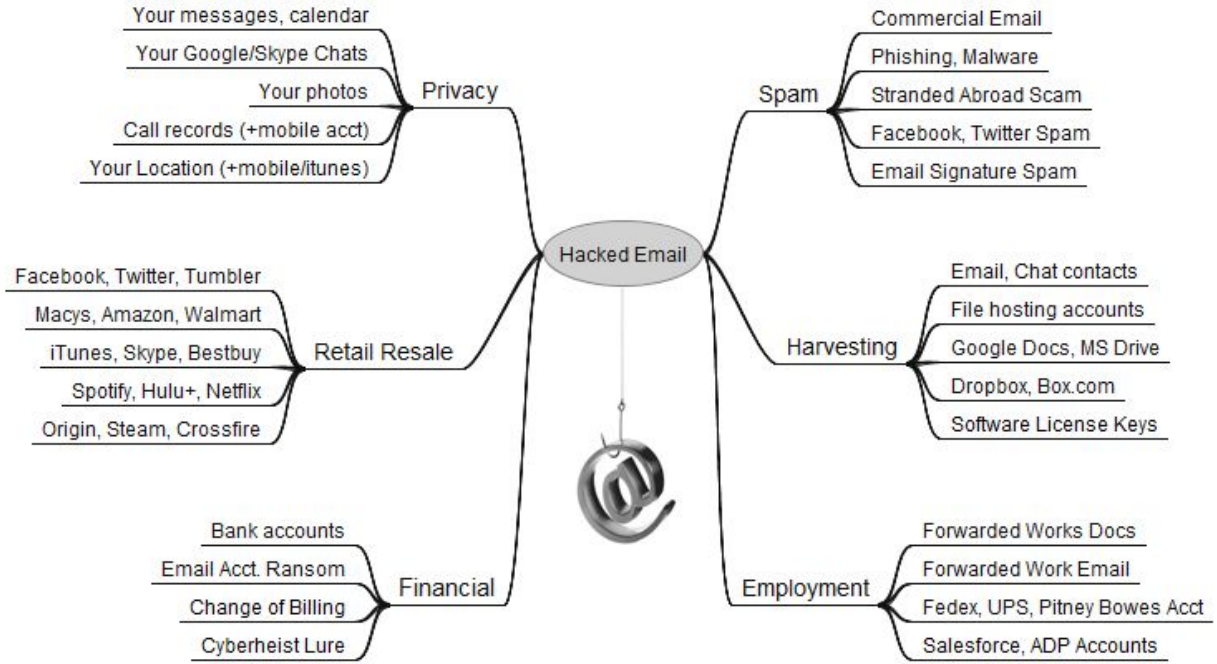
The abuse ecosystem

The value of a hacked PC



Source: [Krebs on Security]

The value of a hacked email account



Source: [Krebs on Security]

The underground economy

"A loose federation of specialists selling capabilities, services, and resources explicitly tailored to the abuse ecosystem" **[Thomas et al.]**

A significant evolution of the abuse ecosystem in the 2000s

Automatization (easy to compromise at scale)

Monetization of compromised data and systems

Natural evolution of an economy to specialize, scale up, and globalize

Framing Dependencies Introduced by Underground Commoditization

Kurt Thomas[◇] *Danny Yuxing Huang*[†] *David Wang*[◇] *Elie Bursztein*[◇] *Chris Grier*[□]
Thomas J. Holt[*] *Christopher Kruegel*[§] *Damon McCoy*[‡▽○] *Stefan Savage*[†] *Giovanni Vigna*[§]

[◇]*Google* [†]*University of California, San Diego* [§]*University of California, Santa Barbara*
[▽]*University of California, Berkeley* [○]*International Computer Science Institute*
[□]*Databricks* [‡]*George Mason University* [*]*Michigan State University*

WEIS 2015

Profit Center	Strategy	Estimated Revenue	Time Frame
Spamvertised products	Pharamcuticals [97]	$12–92 million	2007–2010
	Luxury knock-offs [152]	$68 million	2013–2014
Scareware & Ransomware	Fake anti-virus [133]	$130 million	2008–2010
	CryptoLocker [159]*	$3 million	2013–2014
Clickfraud	ZeroAccess [115]	$36 million	2013
	DNS Changer [149]*	$14 million	2007–2011
Financial Scams	Pump and dump [150]*	$120 million	2008–2013
	419 scammers [8]*	$200 million	2006
Credit Card Theft	ATM withdrawl scam [118]*	$45 million	1 day
	Zeus banking trojan [9]*	$70 million	2009–2010
	Re-selling stolen cards [35]*	$300 million	?–2013

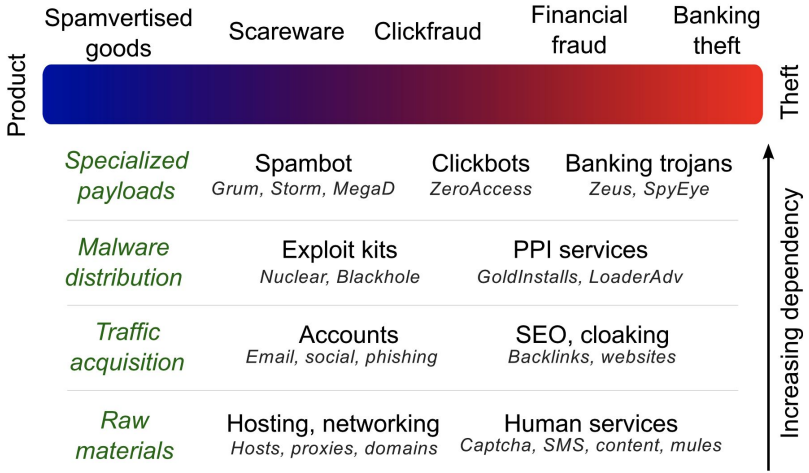


Figure 2: Taxonomy of underground actors. Profit centers supply the revenue for all abuse, while support centers provide critical resources that streamline defrauding victims.

Spamvertised products

One of the oldest forms of economically driven Internet abuse

1990s: vertically integrated operation

Now: Specialized & stratified (30%-50% commission per each sale)

From email to social networks, SEO, and newer forms of engagement

Subject to technical (blocklisting, filtering) and legal (CAN-SPAM act) countermeasures

Does it work?

- YES!
- Click rates are very high
  - **0.003%-0.006%** for email
  - **0.13%** for social networks

Scareware & ransomware

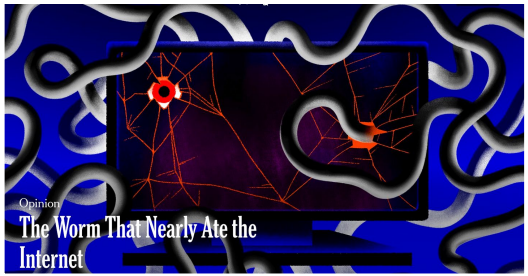
Like spam but relying on socially engineered victims under duress

Most successful example: Fake AV (2% victims bought it)

Payment through credit cards

15% of all malware detected in 2008-2011

Distribution: Conficker



Scareware stopped ~2011
- Conficker was dismantled
- LEA & banks froze transactions

Cryptolocker:
- 0.5M users, 1.3% paid => US$3M

Cost of latest ransomware attacks:
- 2015: US$325M
- 2016: US$5B
- 2017: US$8B
- 2018: US$11.5B
- 2019 up to date: **epidemic**

Trends: mobile, social media, IoT

Operation Tovar

Source: FBI

CC and banking fraud

Obtaining CC details

Name, number, CVV, exp. date

Through PoS malware and skimming

From payment sites (Sony Play Station Payment Network, 2011: 77M victims

Large-scale operations (e.g., Zeus, then Gameover Zeus for ransomware)

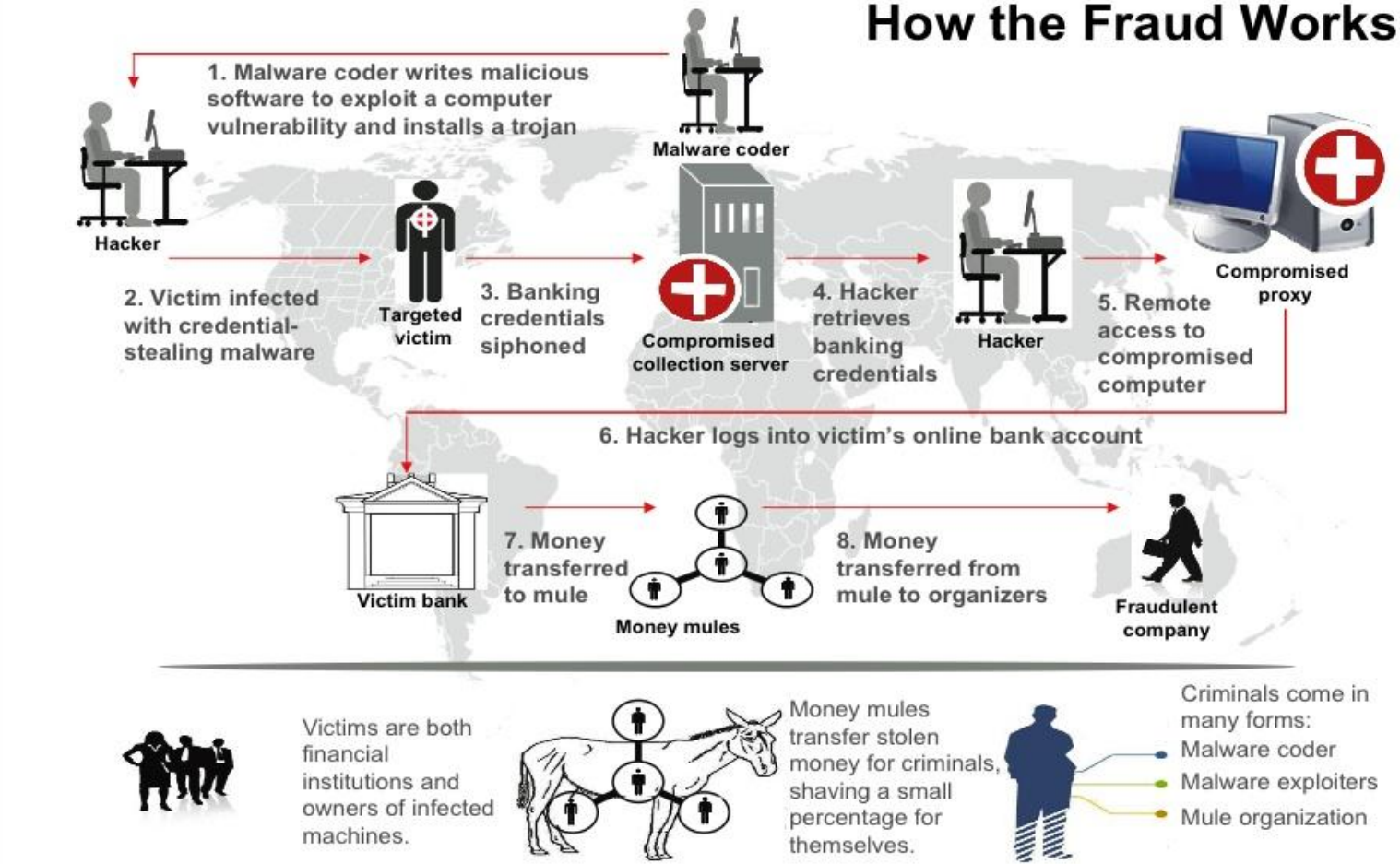
Cashing out

Money mules (NY, 2014: US$45M in hours)

Physical goods (online retail) or electronic goods (e.g., gaming, in-app purchases) later resold

PSD2 made life just a bit harder for fraudsters

Source: FBI: The Zeus Fraud Scheme



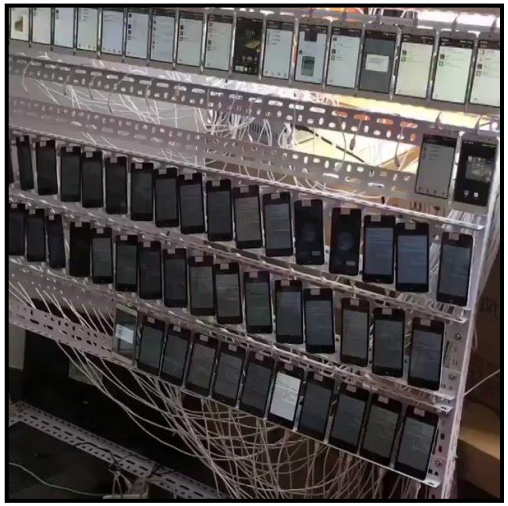
Click fraud

Online advertisement is a multi-billion dollar market
Online social media engagement has enormous value (“**influence**”)

Fraudster becomes publisher of ads (ad network), runs website and drive hijacked traffic to ads in order to receive payment from advertisers (PPC)

Bots or manual workers clicking on URLs

Specific malware (ClickBot.A, 7cy, Fiesta, ZeroAccess, DNSChanger, ...) to use residential IPs and circumvent detection




FIELD_
OF_
VISION
LIKE


making hundreds of dollars with smartphones


抖音
抖音号:Bailun304335634

Supporting infrastructure

Human Services

E.g., CAPTCHA solving services
KOLOTIBABLO
E.g., Phone verification (SMS)

DNS & hosting

Must be cheap because of continuous renewal due to blocking

Accounts

Automatically generated fraudulent accounts
Compromised accounts hijacked from victims

Proxy & anonymization

Residential
Mobile

A REPORTER AT LARGE AUGUST 3 & 10, 2020 ISSUE

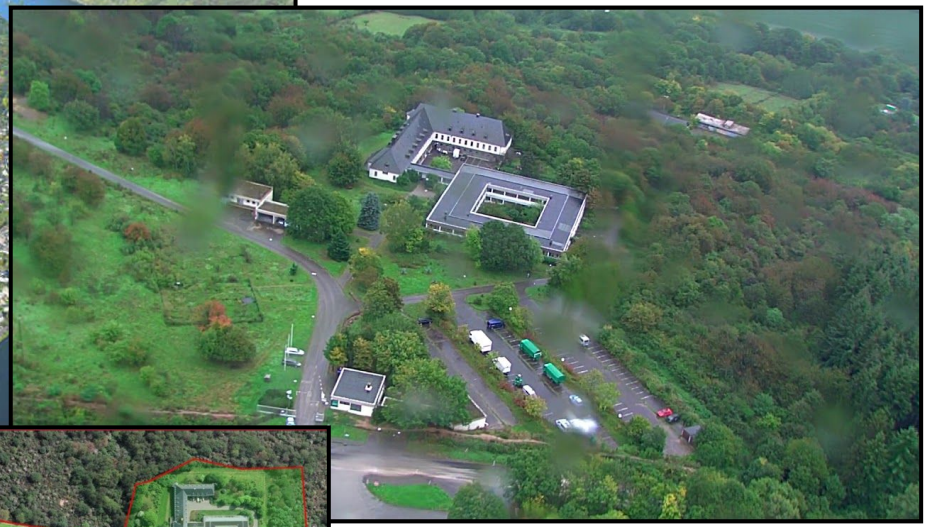
THE COLD WAR BUNKER THAT BECAME HOME TO A DARK-WEB EMPIRE

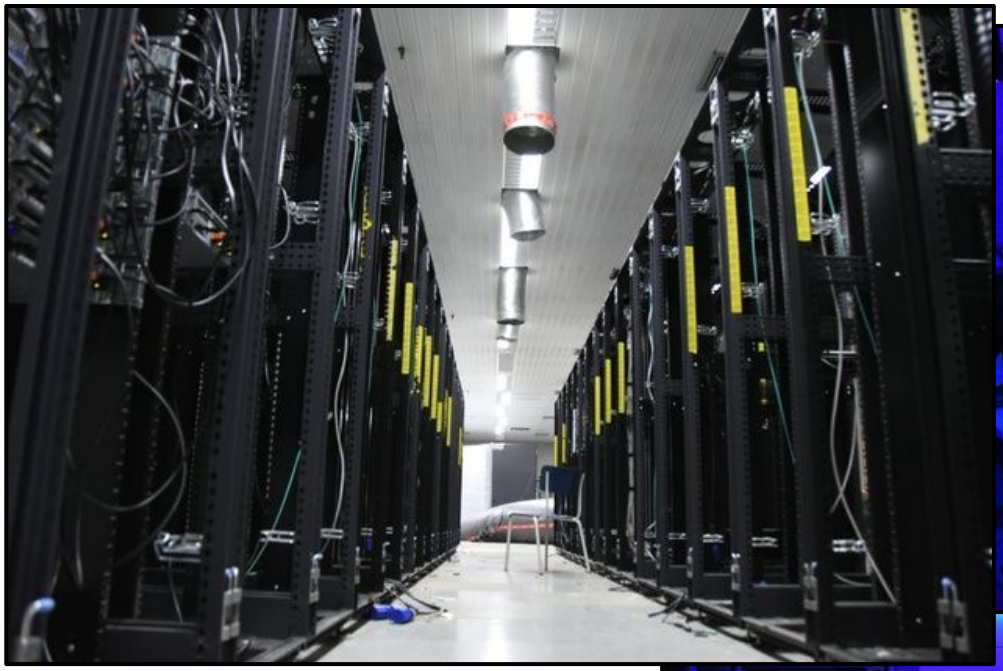
An eccentric Dutchman began living in a giant underground facility built by the German military—and ran a server farm beloved by cybercriminals.

By Ed Caesar

July 27, 2020


Standort Ex-Bundeswehrbunker





The Hacker Infrastructure and Underground Hosting: Services Used by Criminals

Vladimir Kropotov, Robert McArdle, and Fyodor Yarochkin

TREND MICRO | research

Commodified Cybercrime Infrastructure

Exploring the Underground Services Market for Cybercriminals

The provision of services, as well as the way criminals operate in the underground, have gone through many changes over the years to cater to the market's different infrastructure demands.

Learning services

Cybercriminal Degree

The Cybercriminal degree covers advanced topics introducing you to Operational Security (OPSec), Wi-Fi hacking, updated Man-In-The-Middle (MiTM) attacks, creating malicious Word Documents, and how to be successful in hacking an individual or business for profit or pirating. This degree will prepare you for operating as an efficient and effective hacker, as well as providing all the information required for you to to start your career into cybercrime.

* The topics discussed, tools, techniques, and resources within this degree are up to date as of 2021.

Cybercriminal Courses Offered:

- ACT 0 - OPSec - Click for description

Build a strong foundation in Operational Security (OPSec) by learning through theoretical lessons reinforced with practical exercises, covering topics like er
email, how to use cryptocurrency anonymously, hacker history, and enabling you to operate online anonymously. Also known as avoiding jail.

- ACT I - Wi-Fi Hacking - Click for description

You will learn how to hack Wi-Fi networks so you can stop using your own Wi-Fi network when doing devious things and instead use other people's Interne

- ACT II - Network and MiTM attacks - Click for description

Learn up to date MiTM attacks to sharpen your claws and attack others on the same Wi-Fi network as you.

- ACT III - Wordup - Click for description

Deliver malicious Word Documents to people in order to infect them with a RAT, ransomware, keylogger, etc.

- ACT IV - Online Scams and Tor Hidden Services - Click for description

Design and launch online scams and setup a Tor hidden service to spread your propoganda to the masses.

- ACT V - Phishfood - Click for description

Design and launch phishing attacks against people to gain access to their online accounts (Facebook, Twitter, email accounts, etc.). Includes updated tools to

- ACT VI - Ride the Snake - Click for description

This course will teach you step by step how to compromise an individual or business with any malware (RAT, ransomware, password stealer, etc.) from a ha

Carding

This diploma will teach you everything there is to know about committing credit card. Afte
the resources to commit credit card fraud should you choose to do so.

This course is is meant for people who wish to learn credit card fraud with real information
be. This course is original content with pictures and screenshots to help your learning.

Who the fuck I am? I was a successful cybercriminal who retired many years ago with cash
DAT cryptocurrency boom! I've been floating around in life for quite some time and having
I've always enjoyed writing I've designed these courses around my experience as a cybercri
techniques, and procedures to experience financial freedom for yourself. I can't sell my boo

This course is good for:

- Carders
- Fraudsters
- All the information surrounding credit card fraud your mind can handle

You'll learn from real world examples and from other carders history.

This course isn't for everyone and is not designed to hold your hand all the way through. It does include resources, articles, and links that you should read, understand, and be able to apply the knowledge learned in order to be successful and to maximize the knowledge taught here.

* The topics discussed, tools, techniques, and resources are up to date as of 2021.

The **HackTown** course curriculum is designed around my expertise and experience when I was operating as a cybercriminal. I was a successful cybercriminal who retired many years ago with cashing out the profits I made through cybercrime and enjoying DAT cryptocurrency boom along with it. I've been floating around in life for quite some time and having too much time on your hands is never a good thing. Since I've always enjoyed writing I've designed these courses around my experience as a cybercriminal giving you the opportunity to duplicate my tactics, techniques, and procedures to experience financial freedom for yourself.

We offer a degree or diploma in specific areas of cybercrime that cater to individuals with little to no programming experience. However, all levels of cybercriminals, hackers, and fraudsters out there will enjoy what this place has to offer!

Programs of Study

Carding Diploma - Click here for description

This diploma will teach you everything you need to know about credit card fraud and is designed around real world experiences.

After finishing this diploma you'll have the knowledge, skills, and the resources to commit credit card fraud.

Cybercriminal Degree - Click here for degree course list

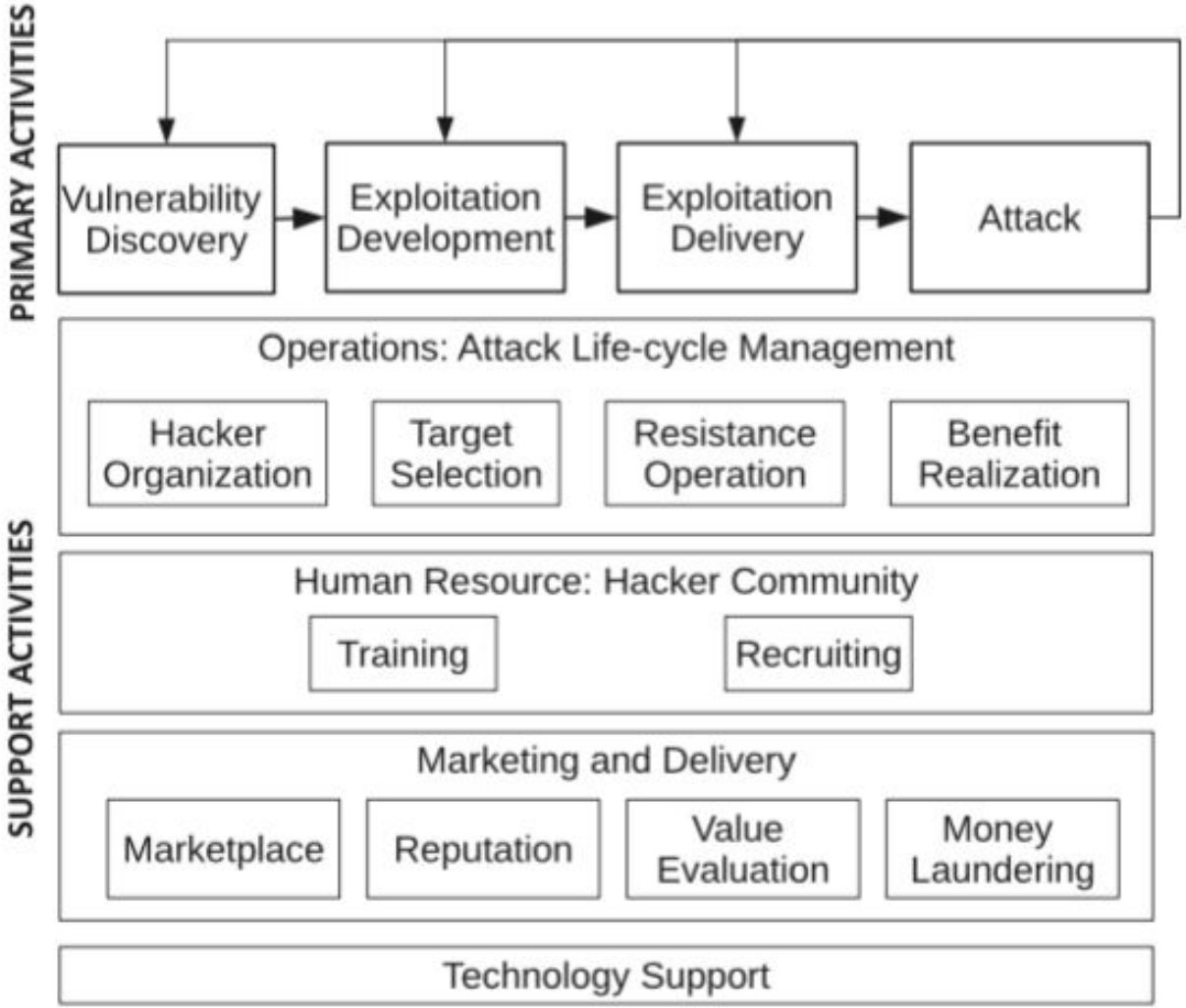
The Cybercriminal degree covers advanced topics introducing you to Operational Security (OPSec), Wi-Fi hacking, Man-In-The-Middle (MiTM) attacks, creating malicious Word Documents, online scams, phishing, and includes how to hack an individual or business for profit or pirating.

This degree will prepare you for your career in cybercrime as an efficient and effective hacker.

Future Courses - Click here for future courses yet to be released

These future courses will enhance your cybercriminal skills giving you more of advantage as an attacker.

The supply chain

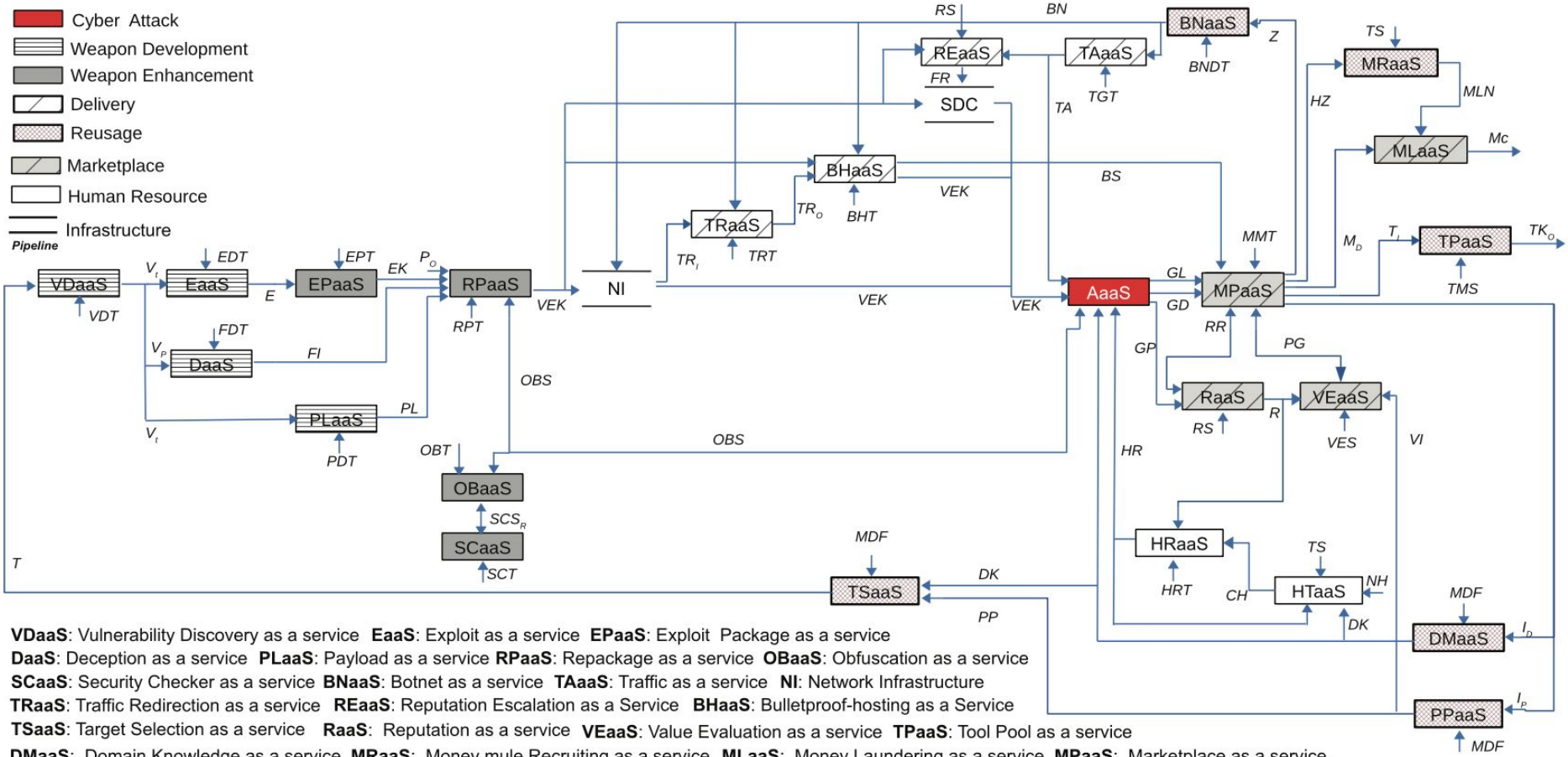


The value chain

Huang et al. (2018)

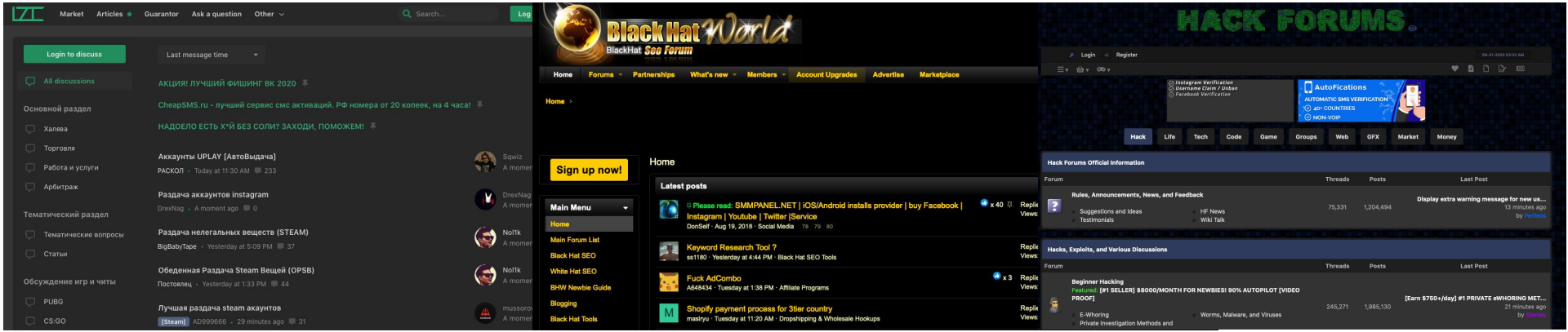
The cyberattack business supply chain

Huang et al. (2018)



VDaaS: Vulnerability Discovery as a service **EaaS**: Exploit as a service **EPaaS**: Exploit Package as a service
DaaS: Deception as a service **PLaaS**: Payload as a service **RPaaS**: Repackage as a service **OBaaS**: Obfuscation as a service
SCaaS: Security Checker as a service **BNaaS**: Botnet as a service **TAaaS**: Traffic as a service **NI**: Network Infrastructure
TRaaS: Traffic Redirection as a service **REaaS**: Reputation Escalation as a Service **BHaaS**: Bulletproof-hosting as a Service
TSaaS: Target Selection as a service **RaaS**: Reputation as a service **VEaaS**: Value Evaluation as a service **TPaaS**: Tool Pool as a service
DMaaS: Domain Knowledge as a service **MRaaS**: Money mule Recruiting as a service **MLaaS**: Money Laundering as a service **MPaaS**: Marketplace as a service
SDC: Software Distribution Channel **PPaaS**: Personal Profile as a service **HRaaS**: Hacker Recruiting as a service **HTaaS**: Hacker Training as a service **AaaS**: Multi-step attack as a service

Marketplaces



Forums / Web storefronts / IRC / Discord / …

Mostly English, Russian, Chinese

Password-based registration + user levels (e.g., VIP) + reputation mechanisms

Open vs invite-only / clearnet vs dark web (e.g., onionland)

100s of marketplaces

Some flourish, some disappear
TrendMicro's The Cybercriminal Underground

Forum	Primary Lang.	Focus	Comments
Blackhat World	English	SEO	Started in Oct'05. Changed over the past decade
Darkode	English	Cyber tools	Taken down in '15 by a joint multinational effort
Hack Forums	English	Cyber and Non-cybercrime topics	–
Hell	English	Credit card fraud and data breaches	Tor hidden service. Shut down in Jul'15. Re-launched in Jan'16
Nulled	English	Leaks and tools for data breach	Hacked in May'16 and full DB was leaked

Forum	Primary Lang.	Focus
antichat.ru, xeka.ru, exploit.in, InAttack, XaKePoK.su, XakNet.ru, zloy, HAckForke.ru	Russian	Non-specialized, multiple cyber tools
fe-ccshop.su, Rescator, gocvv.cc, carding-cc.com	Russian	Carding and associated info
xdedic.biz	Russian	credentials (amazon, ebay, paypal, gaming, HBO, Netflix, ...)
ordaproject.com	Russian	passports and ID cards
ssndob.cc	Russian	personal info (SS numbers, full details ,etc)

The darkness online

Cryptopolitik and the Darknet

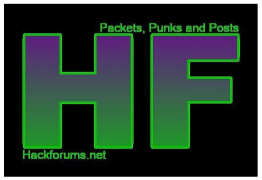
Daniel Moore & Thomas Rid

Pages 7-38 | Published online: 01 Feb 2016

Category	Details
Arms	Trading of firearms and weapons
Drugs	Trade or manufacture of illegal drugs, including illegally obtained prescription medicine
Extremism	Content espousing extremist ideologies, including ideological texts, expressions of support for terrorist violence, militant how-to guides and extremist community forums
Finance	Money laundering, counterfeit bills, trade in stolen credit cards or accounts
Hacking	Hackers for hire, trade or distribution of malware or DDoS[45] capabilities
Illegitimate pornography	Pornographic material involving children, violence, animals or materials obtained without participants' consent
Nexus	Websites primarily focused on linking to other illicit websites and resources within the darknet
Other illicit	Materials that did not easily fit into the other categories but remain problematic, such as trade of other illegal goods and fake passports or IDs
Social	Online communities for sharing illicit material in the form of forums, social networks and other message boards
Violence	Hitmen for hire, and instructional material on conducting violent attacks
Other	Non-illicit content, such as ideological or political content, secure drop sites, information repositories, legitimate services
None	Websites which were either completely inaccessible or otherwise had no visible content, including websites which hosted only placeholder text, indicating that their operator had yet to generate indicative content

Category	Websites
None	2,482
Other	1,021
Drugs	423
Finance	327
Other illicit	198
Unknown	155
Extremism	140
Illegitimate pornography	122
Nexus	118
Hacking	96
Social	64
Arms	42
Violence	17
Total	5,205
Total active	2,723
Total illicit	1,547

Walkthroughs



Prices and pricing models

Pricing models and typical values for various cybercrime services

Huang et al. (2018)

Service	Status	Pricing Model	Example Case	Estimated Price
EaaS	Existing	License	Exploit Trading [71]	up to more than $250,000
		Subscription	Up-to-date Zero-day Exploits [151]	$150,000 per month
PLaaS	Existing	Pay-per-install Commission	Payload Renting [10, 16]	$0.02–0.10 per install 40%
DaaS	Existing	Subscription	Phishing Service [145]	$85–$115 per month 40%
		Commission	Fake Anti-virus [97]	
OBaaS	Existing	Subscription	Obfuscation Platform [50]	$50–150 per month
SCaaS	Existing	Subscription	Scan4you [72]	$25 per month
TRaaS	Existing	Pay-per-click	Traffic Redirection [50]	$7–$15 per 1,000 visitors
BNaaS	Existing	Subscription	Botnet Shops [145]	$40 per month
BHaaS	Existing	Subscription	Cloud Bulletproof Servers [100]	$300 per month
TAaaS	Existing	Subscription	DDoS Attack Service [134]	$999 per month
REaaS	Existing	Pay-per-record	Reputation Escalation Markets [170]	$0.4–0.7 per record
MPaaS	Existing	License	Market Framework [35]	$4,500 per licence
		Commission	Marketplace [34]	2%–10%
MRaaS	Existing	License	Money Laundering Recruitment Package [99]	$1,700 per licence
MLaaS	Existing	Commission	Money Laundering Service [127]	2%–30%
HTaaS	Existing	License	Hacker Training Courses [138]	$250–$800 per person
PPaaS	Evolving	License	Personal Profile Investigator [59]	$4–$20 per record
TPaaS	Evolving	Subscription	"One-stop-shop" Platform [2, 73]	$4,000 per month
RaaS	Evolving	Subscription	Smart Contract [79]	/
HRaaS	Evolving	Subscription	Online Hacker Recruiting Market [105]	/
VDaaS	Emerging	Subscription	Bug Bounty Program [132]	$542.04–$1810.31 per vulnerability
TSaaS	Emerging	Subscription	Targets Ranking based on Value [101]	/
EPaaS,RPaaS	Emerging	Subscription	Repackaging Platform [143, 151]	$4,000 per month
DMaaS	Emerging	Subscription	"How-to" Knowledge Systems [27]	/
VEaaS	Emerging	Subscription	Comparison "Shopping" Service [57]	/

PRIVACY Affairs

Dark Web Price Index

2020 2021

Estimated average costs

Thomas et al. (2015)

Support Center	Resource	Estimated Cost	Volume or Period
Compromised Hosts	Blackhole exploit kit [27]	$1,500	1 year
	Nuclear exploit kit [27]	$1,500	1 year
	Neutrino exploit kit [27]	$450	1 month
	Phoenix exploit kit [27]	$1,000–1,500	1 month
	Pay-per-install: US/UK [15]	$100–180	1,000
	Pay-per-install: Europe [15]	$20–160	1,000
	Pay-per-install: Other [15]	<$10	1,000
Human Services	CAPTCHAs [106]	$1–2	1,000
	SMS challenge [143]	$200	1,000
	Mobile SIMs [143]	$140–420	1,000
	English blog content [107]	$2–4	1
	Chinese blog content [156]	$0.25	1
Networking & Hosting	Proxy: 150 IPs	$25	1 month
	Proxy: 15,000–30,000 IPs	$250	1 month
	DDoS: 800 Mbps [70]	$10	1 month
	DDoS: 100 Gbps [30]	$200	1 day
Accounts & Engagement	Hotmail account [145]	$4–30	1,000
	Yahoo account [145]	$6–15	1,000
	Twitter account [145]	$1–20	1,000
	Facebook PVA [145]	$80–400	1,000
	Google PVA [145]	$80–500	1,000
	Twitter followers [136]	$4–20	1,000
	Twitter retweets [136]	$79–550	1,000
	Facebook likes [36]	$15–70	1,000

Intervention

Intervening the underground economy

Experience from traditional illicit economies (drug markets, prostitution, stolen goods) suggests that cannot be disrupted by law enforcement intervention alone.

Strategies?

Technical measures to protect users & systems

Challenging and so far with limited success

Wrong incentives

Wrong business models

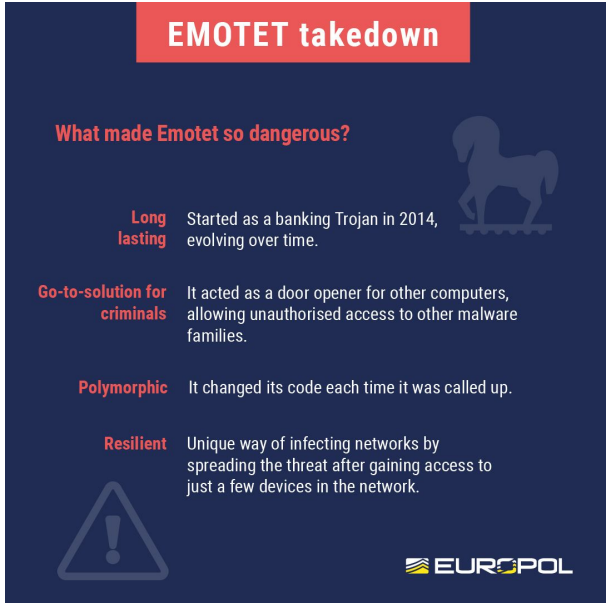
Exhausting resources (i.e., attacking the attacker)

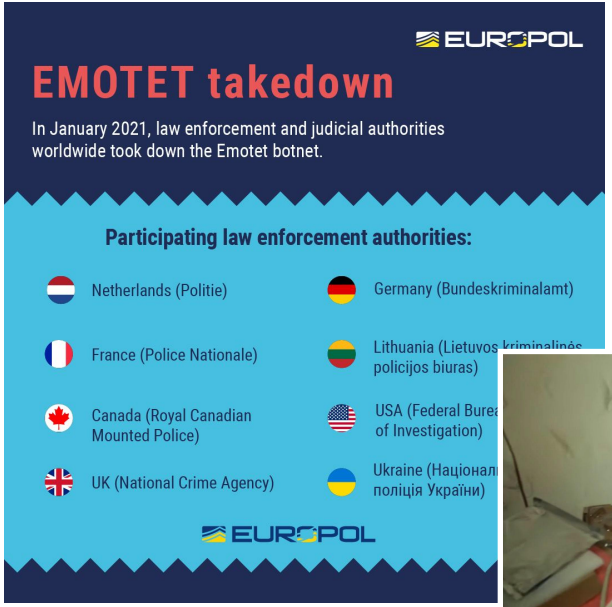
Limited success in botnet/market take down operations

Many recover after just 1 month

Costly international public-private coordination

At the time, the world's largest cybercrime operation (EUROPOL)





Disrupting payment (no payment = no business)

Many early digital currencies (LibertyReserve, e-Gold)

dismantled because of money laundering

But bitcoin?

Targeting actors

“A spokesman for the German federal cybercrime unit that led the international investigation into Wall Street Market told me frankly that the war against dark-Web bazaars was unwinnable. Just as Wall Street Market had flourished after the Silk Road’s demise, new markets would grow in the place of Wall Street Market. People would continue to have illicit desires, and the Internet would find ways to satisfy them.”

The Cold War Bunker That Became Home to a Dark-Web Empire
Ed Caesar
THE NEW YORKER - July 27, 2020