Cyber-crime as a Service

CaaS analysis report

Y. Zheng A. Chaudhry
What is Cyber-cime?

- Crimes that target computer networks or devices
- Crimes that use computer networks to advance other criminal activities
Within the last year, 689 MILLION PEOPLE in 21 countries experienced cybercrime. In the 17 countries surveyed in both 2015 and 2016, we've seen a 10 percent increase since last year.

Since 2015, cybercrime victims spent $126 BILLION globally and spent 19.7 hours dealing with cybercrime.
THE $126 BILLION PHOTOGRAPH

Total Net Worth
$126 BILLION

Photograph by Michael Prince for Forbes
What is Cyber-crime as a Service (CaaS)?

- Software-as-a-service (SaaS)
- Platform-as-a-service (PaaS)

“THE provision of services to others to facilitate their commission of cyber-crimes”
Types of Cyber-Crime-as-a-Service

- Online Money Laundering
- Dark Web Market
- DDoS ‘as a service’
- Exploits ‘as a service’
- Ransomware ‘as a service’
Online Money Laundering (Currency)

Illegal Money acquired through click fraud, carding, etc.

Exchanger - Verified exchanger or peers will change $ or any e-currency into LR currency

LR account

Cash out
Money is laundered through VCC, prepaid cards or exchanger (LR to Western Union)
Dark Web Market
(Platform)

Hacker
Online Market
Buyer
DDoS ‘as a service’
(Product)

“Since their inception in 2010, DDoS-for-hire capabilities have advanced in success, services and popularity, but what’s most unnerving is booters have been remarkably skilled at working under the radar,” according to the Verisign’s Distributed Denial of Service Trends report.

“Given the ready availability of DDoS-as-a-service offerings and the increasing affordability of such services, organizations of all sizes and industries are at a greater risk than ever of falling victim to a DDoS attack that can cripple network availability and productivity.”

Figure 4: Price List for Select DDoS-for-Hire Services
Exploits ‘as a service’ (Product)
Exploits Kits Trends
(Product)

More than 100 exploits have been integrated into 70 exploit kits in 2014.

Exploit kits can be rented by the hour, day, or month. When Angler started taking a dip, Neutrino jacked up its price by 100% from US$3,500 to US$7,000 per month.⁴
Impact on Enterprise

Adobe Flash, the software most often targeted by exploit kits, is installed in more than 1B connected systems to date.
What Enterprise Can do

Data Gathering → Feature Selection → Model Building → Classification → Detection
Ransomware ‘as a service’
Ransomware Trends

Hollywood Presbyterian paid US$17,000 to decrypt files encrypted by Locky.

52% Database-Related Files
14% Web Pages
10% Tax Return Files
19% SQL Files
9% Mac OS X Files
Why Criminals Love Ransomware

$3,000,000 Reward

"They're financially lucrative with little chance of arrest."

McAfee
Catch me if you CAN

Principality of Sealand
Q1. Which one of the following is/are considered to be the possible CaaS provider?

A. 16-year-old pimply kid in his mom’s basement hacking between World of Warcraft and Call of duty.
B. Traditional organized crime group with multinational background hackers
C. Data centered committed to protect privacy
D. All of the above
Q2. Which one of the following is not considered as ransomware’s behavior?

A. overwrites the Master Boot Record, causing BSoD
B. **Grab the IP packets and modify protocol**
C. Lock up your computer and ask for payment to unlock
D. exploit vulnerable Web servers
Q3. Why is it difficult to catch cyber criminals?

A. The difficulties of tracking them through the internet
B. It is usually too late when people realize and report the situation
C. One internet, many laws
D. All of the above
Reference

http://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396
https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/
https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/
http://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf
http://www.pcquest.com/cybercrime-service-a-very-modern-business/
https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev
https://www.techopedia.com-definition/2387/cybercrime
https://en.wikipedia.org/wiki/Principality_of_Sealand
https://www.wikiwand.com/en/The_Pirate_Bay
http://securityaffairs.co/wordpress/33916