

# 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



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”



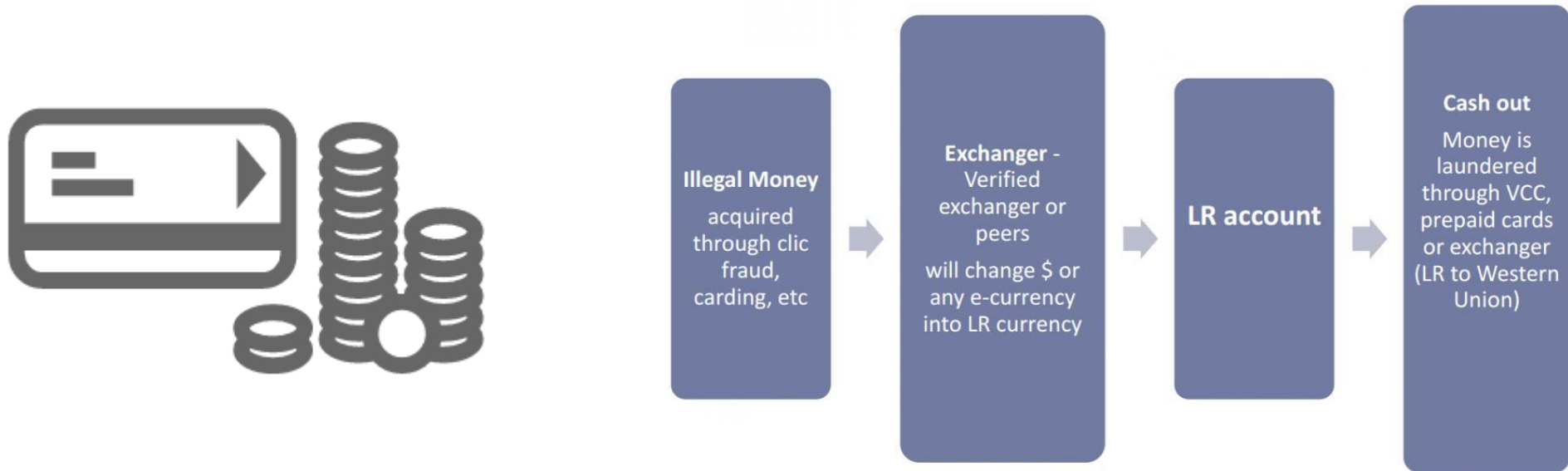
---

## 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)

---



# Dark Web Market (Platform)

---



---

Hacker



---

Online Market



---

Buyer



# DDoS ‘as a service’ (Product)



DDoS Attack

“

*“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.*

“

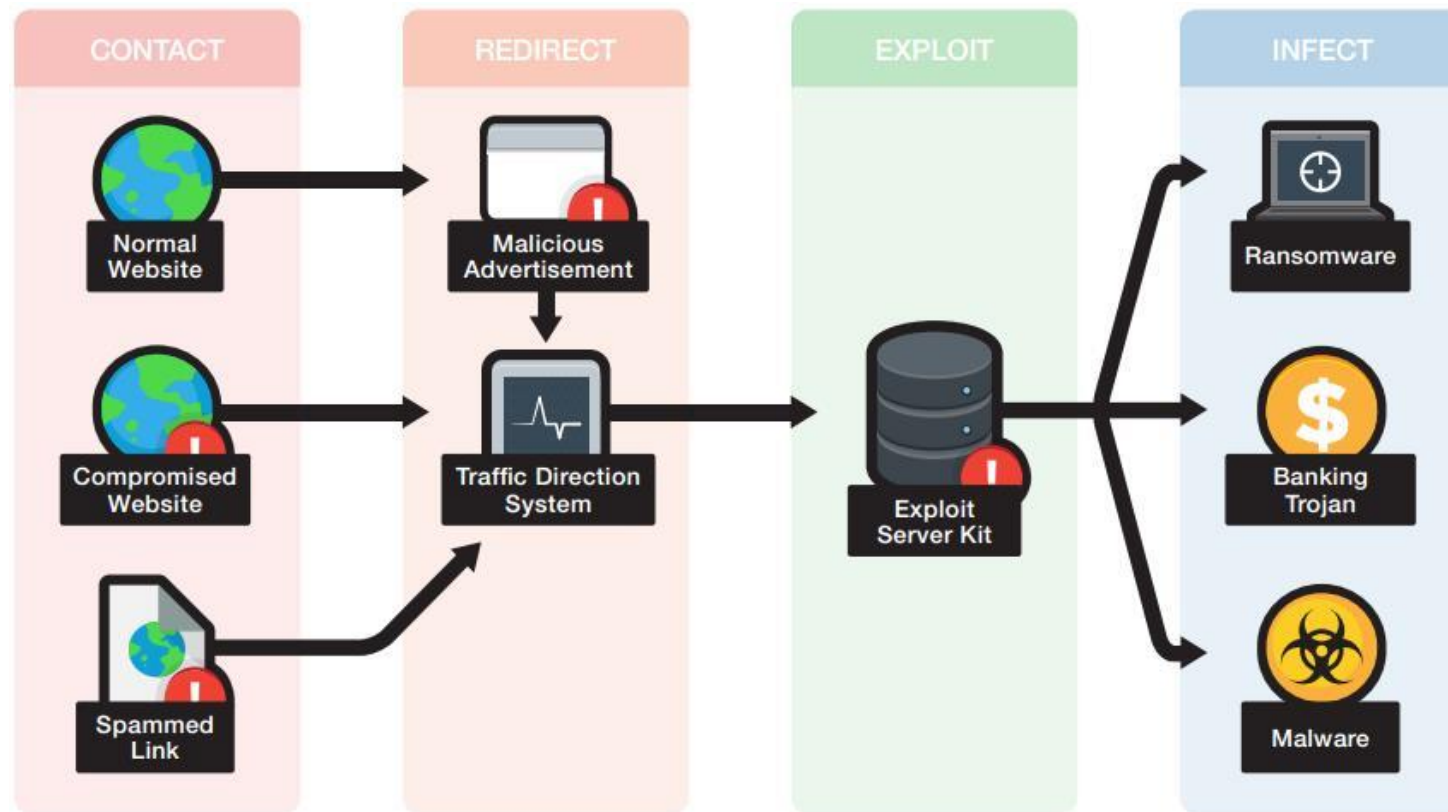
*“Given the ready availability of DDoS-as-a-service offerings and the increasing affordability of such services, organizations of all sizes and industries are at a greater risk than ever of falling victim to a DDoS attack that can cripple network availability and productivity.”*

Service Name	Service Pricing (USD)
Xakepy.cc	1 hour starts at \$5 24 hours starts at \$30 1 week starts at \$200 1 month starts at \$800
World DDoS Service	1 day starts at \$50 1 week starts at \$300 1 month starts at \$1,200
King's DDoS Service	1 hour starts at \$5 12 hours starts at \$25 24 hours starts at \$50 1 week starts at \$500 1 month starts at \$1,500
MAD DDoS Service	1 night starts at \$35 1 week starts at \$180 1 month starts at \$500
Gwapo's Professional DDoS Service	1-4 hours at \$2 per hour 5-24 hours at \$4 per hour 24-72 hours at \$5 per hour 1 month at \$1,000 fixed
PsyCho DDoS Service	1 hour for \$6 1 night for \$60 1 week for \$380 1 month for \$900
DDoS Service 911	1 night for \$50
Blaiz DDoS Service	1 day for \$70 1 week starts at \$450
Critical DDoS Service	1 day starts at \$50 1 week starts at \$300 1 month starts at \$900
No. 1* DDoS_SERVICE	1 day starts at \$50 1 week starts at \$300 1 month starts at \$1,000

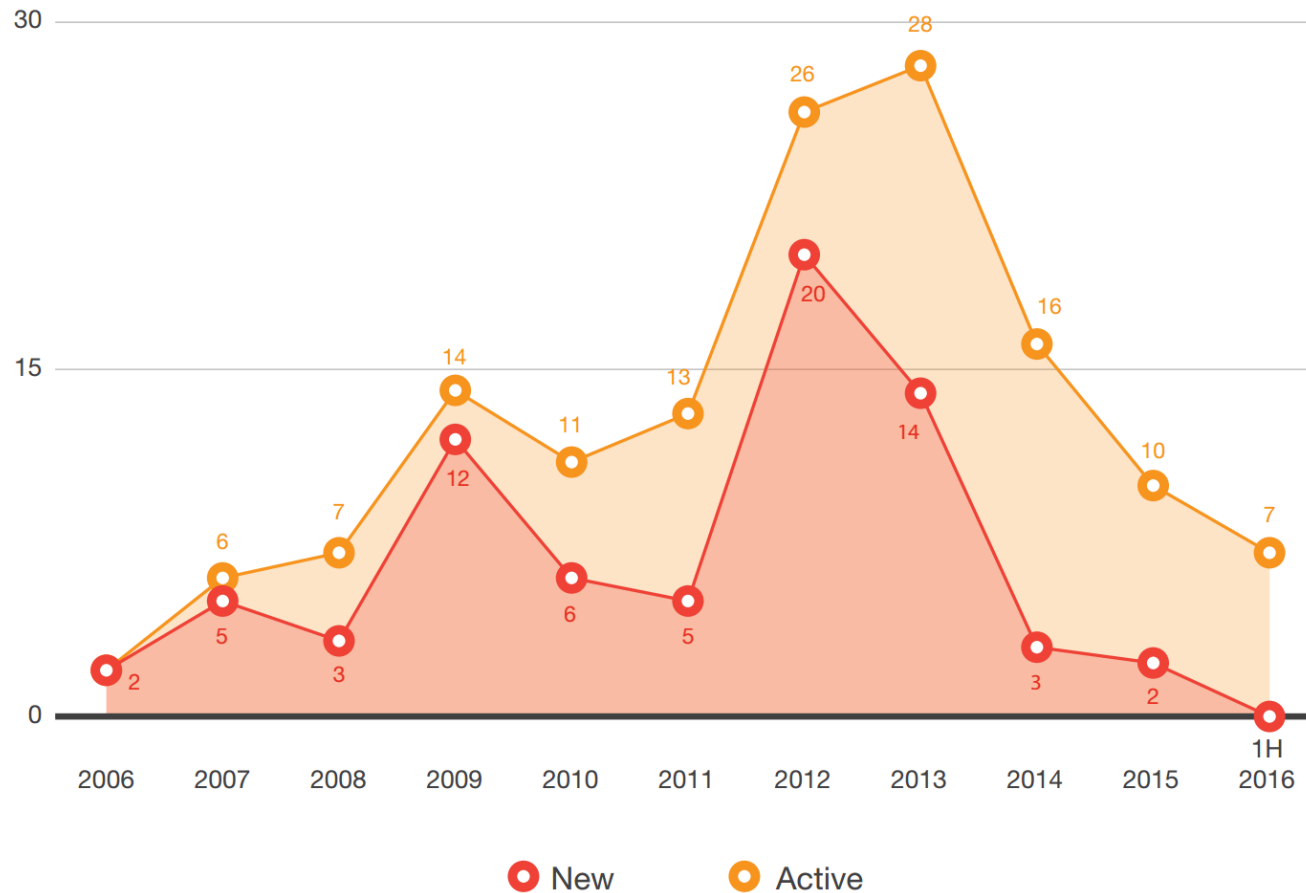
Figure 4: Price List for Select DDoS-for-Hire Services

# Exploits 'as a service' (Product)

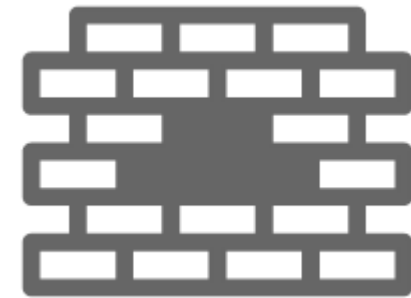
---



# Exploits Kits Trends (Product)

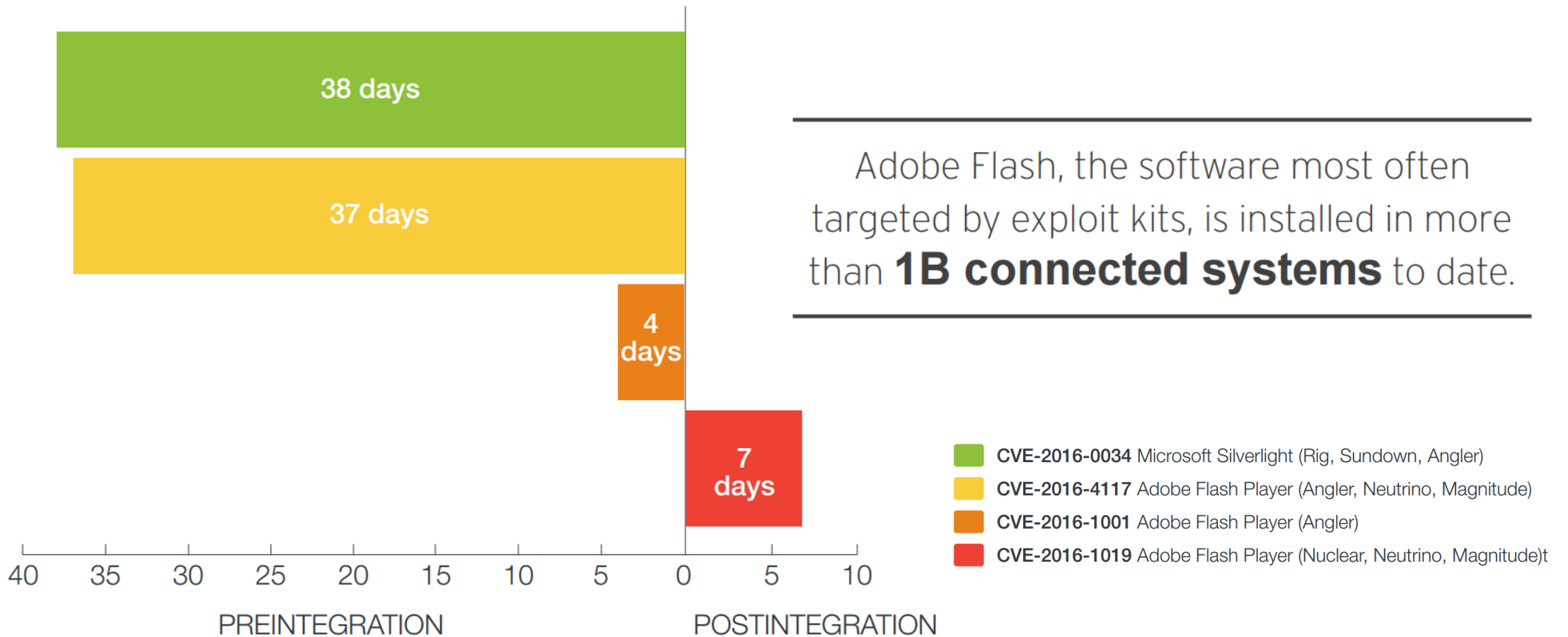


More than **100 exploits** have been integrated into 70 exploit kits in 2014.



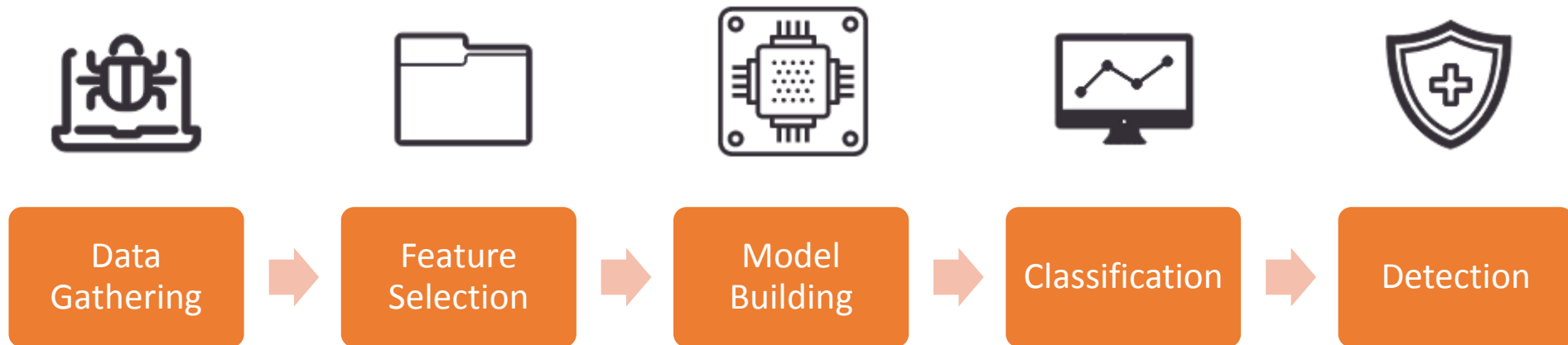
Exploit kits can be rented by the hour, day, or month. When Angler started taking a dip, Neutrino jacked up its price by 100% from **US\$3,500 to US\$7,000** per month.<sup>4</sup>

# Impact on Enterprise

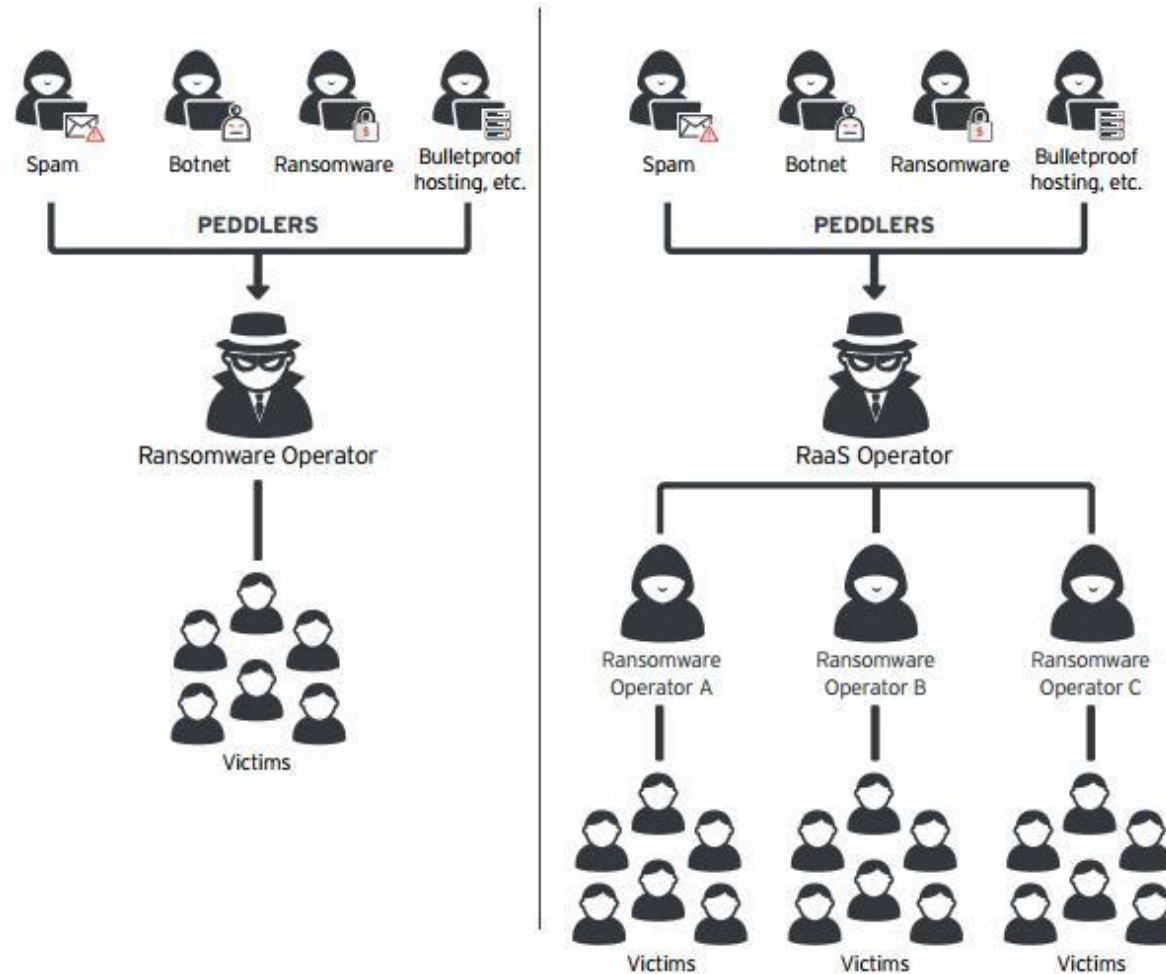


# What Enterprise Can do

---

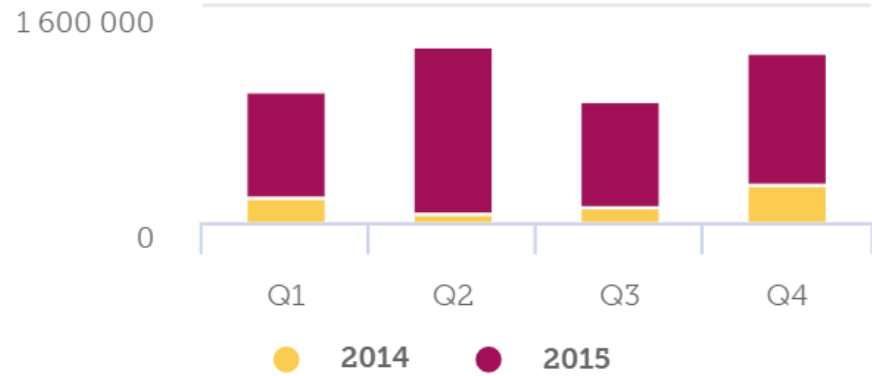


# Ransomware 'as a service'

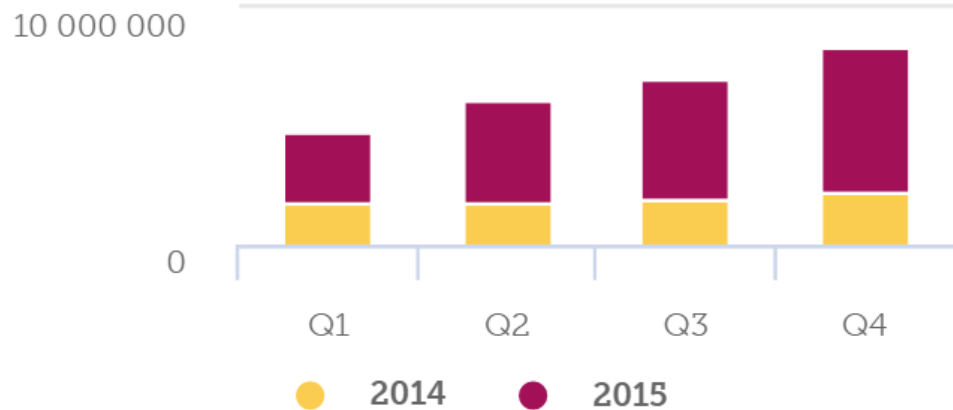


# Ransomware Trends

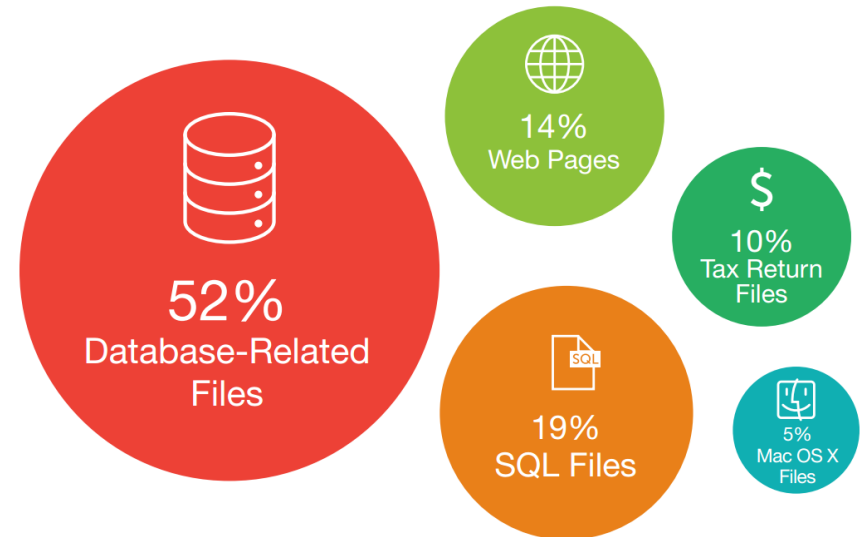
## New Ransomware



## Total Ransomware



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



# Why Criminals Love Ransomware



**WANTED  
BY THE FBI**

**EVGENIY MIKHAILOVICH  
BOGACHEV**

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud



**\$ 3,000,000** Reward

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

McAfee





# Catch me if you CAN

---



---

Principality of Sealand



THANK

YOU

# Q & A

---

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**

# Q & A

---

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

# Q & A

---

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

---

<https://www.symantec.com/content/dam/symantec/docs/reports/2016-norton-cyber-security-insights-report.pdf>

<http://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396>

<http://documents.trendmicro.com/assets/guides/executive-brief-exploits-as-a-service.pdf>

<https://www.technologyreview.com/s/520501/the-secrets-of-online-money-laundering/>

<https://securityintelligence.com/cybercrime-as-a-service-poses-a-growing-challenge/>

<https://www.mcafee.com/uk/resources/reports/rp-quarterly-threats-mar-2016.pdf>

<http://documents.trendmicro.com/assets/resources/ransomware-as-a-service.pdf>

<https://www.forbes.com/special-report/2012/126-billion-forbes-cover.html?v=3>

<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://en.wikipedia.org/wiki/Principality_of_Sealand)

[https://www.wikiwand.com/en/The\\_Pirate\\_Bay](https://www.wikiwand.com/en/The_Pirate_Bay)

<http://securityaffairs.co/wordpress/33916>