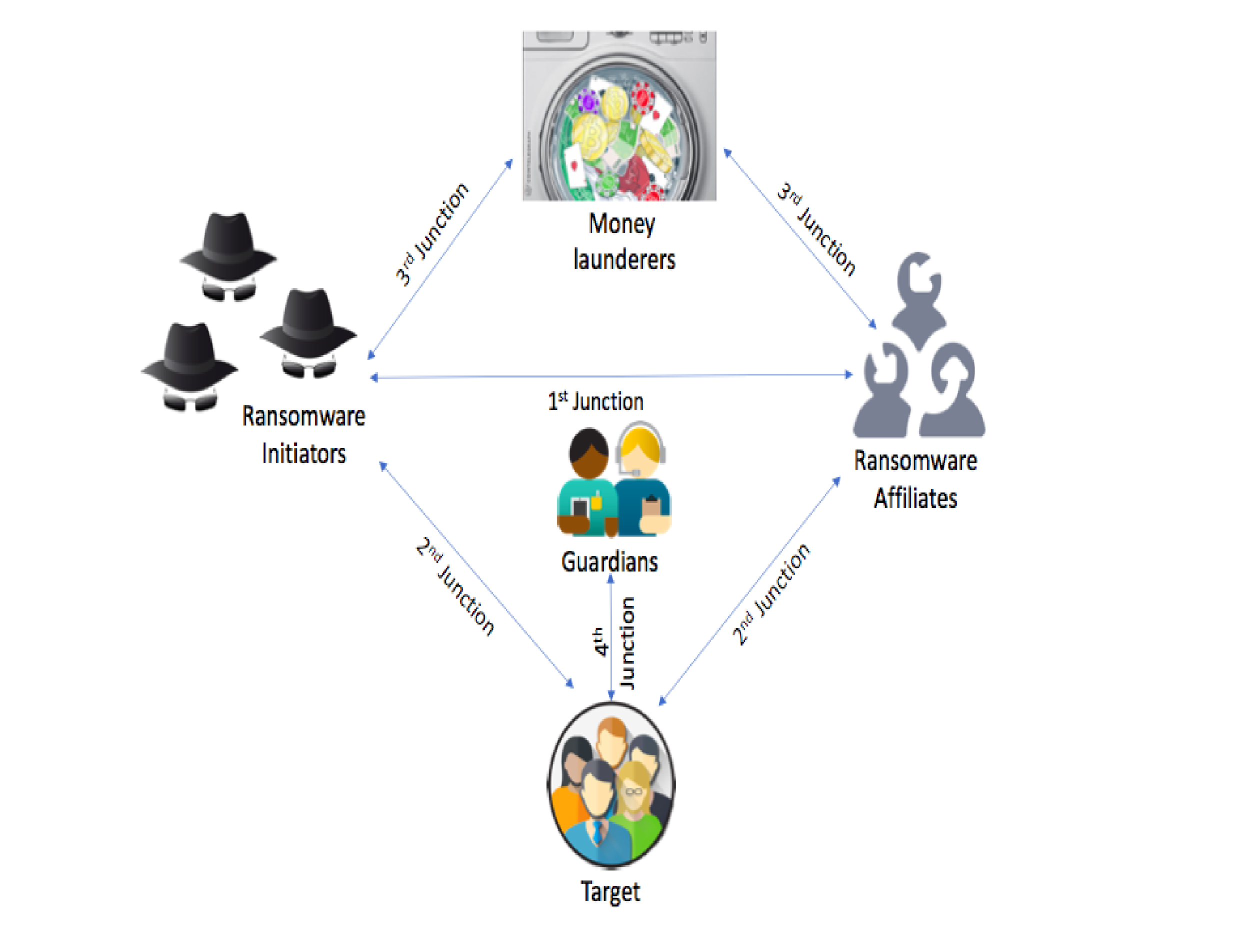
# THE RANSOMWARE ECOSYSTEM: Junctions and Disruption Points

Don Hunt, PhD[1]
David Maimon, PhD[1]
Tamar Berenblum, PhD[2]

*15 October 2018*

1. *Georgia State University, Atlanta, Georgia, USA*
2. *Hebrew University, Jerusalem, Israel*

# THE RANSOMWARE ECOSYSTEM



# The Ransomware Initiators – Ransomware Affiliates Junction

Ransomware Initiators: *The online offenders who write and propagate the malicious software*

Ransomware Affiliates: *The online offenders who are mainly involved in the distribution of that software*

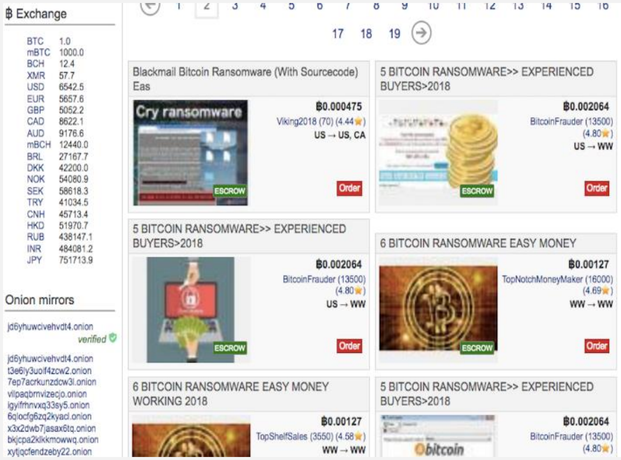
Few studies focus on the underground business model of cybercrime markets but they can be divided into two groups: Cybercrime-as-a-Service (CaaS) and crimeware products (An & Kim 2018; Sood & Enbody 2013).

CaaS: "Do-it-for-me" model. Less sophisticated actors can purchase services or ransomware attacks

Crimeware business model. Offenders purchase ransomware software to launch an attack themselves.

Several online underground markets exist where ransomware initiators actively post "for sale" advertisements of both ransomware as a service and ransomware as a product. While the volume of these posts and the amount of effort invested by initiators in finding affiliates is still unclear, Kharraz and colleagues' (2015) found that few ransomware services and products have sophisticated destructive capabilities and are available on darknet markets.

Little knowledge about the number of ransomware affiliates actively seeking opportunities to become part of a ransomware campaign, their skill levels, or their commitments to launching a ransomware infection event.



฿ Exchange

| | |
|---|---|
| BTC | 1.0 |
| mBTC | 1000.0 |
| BCH | 12.4 |
| XMR | 57.7 |
| USD | 6542.5 |
| EUR | 5657.6 |
| GBP | 5052.2 |
| CAD | 8622.1 |
| AUD | 9176.6 |
| mBCH | 12440.0 |
| BRL | 27167.7 |
| DKK | 42200.0 |
| NOK | 54080.9 |
| SEK | 58618.3 |
| TRY | 41034.5 |
| CNH | 45713.4 |
| HKD | 51970.7 |
| RUB | 438147.1 |
| INR | 484081.2 |
| JPY | 751713.9 |

Onion mirrors

jd6yhuwcivehvdt4.onion
verified

jd6yhuwcivehvdt4.onion
t3e6ly3uolf4zcw2.onion
7ep7acrkunzdcw3l.onion
vilpaqbmvizecjo.onion
igyifmnvxq33sy5.onion
6qlocfg6zq2kyacl.onion
x3x2dwb7jasax6tq.onion
bkjcpa2klkkmowwq.onion
xytjqcfendzeby22.onion

Blackmail Bitcoin Ransomware (With Sourcecode) Eas
฿0.000475
Viking2018 (70) (4.44★)
US → US, CA

5 BITCOIN RANSOMWARE>> EXPERIENCED BUYERS>2018
฿0.002064
BitcoinFrauder (13500) (4.80★)
US → WW

5 BITCOIN RANSOMWARE>> EXPERIENCED BUYERS>2018
฿0.002064
BitcoinFrauder (13500) (4.80★)
US → WW

6 BITCOIN RANSOMWARE EASY MONEY
฿0.00127
TopNotchMoneyMaker (16000) (4.69★)
WW → WW

6 BITCOIN RANSOMWARE EASY MONEY WORKING 2018
฿0.00127
TopShelfSales (3550) (4.58★)
WW → WW

5 BITCOIN RANSOMWARE>> EXPERIENCED BUYERS>2018
฿0.002064
BitcoinFrauder (13500) (4.80★)

# The Online Offenders - Targets Junction

US victimization statistics suggest that ransomware victimization was one of the most reported online crimes by individuals in the USA between 2015 and 2017. While the number of ransomware victims slightly decreased from 2,673 victims in 2016 to 1,783 victims in 2017, the overall financial costs to victims was consistent, ranging between $2.3 and $2.4 million in each of these years (IC3 2015, 2016, 2017).

Estimates of the overall ransomware yield range considerably between sources.

The FBI estimated that ransomware generated $209 million in the first three months of 2016.

Academic assessments lower profits of only $13 million slightly higher (Huang et al 2018; Liao et al 2016).

Regardless, research indicates that offenders follow a low cost/low risk business model (Huang et al 2018).

Ransomware offenders target large or affluent countries such as the USA, Japan, the UK, and Germany (Savage, Coogan, and Lau 2015),

The market is highly skewed and that only few ransomware families (i.e. Locky, CryptXXX, DMALocker3, SamSam and CryptoLocker) are responsible for the majority of payments. (Gazet, 2010)

Take the path of least resistance - most common vectors of attacks are either email (either as a link or an attachment) or website and web applications (Richardson and North 2017).

Open to negotiation: Victims' communicating with ransomware offenders may result in up to a 25% discount on the original ransom amount demand (Masi et al 2016; FTC, 2016).

But we still know little about both individual and organizational ransomware victims.

*Which gender, racial, ethnic, and age groups are more susceptible to these attacks?*
*Do some online routines expose targets to becoming the victims of ransomware attacks?*
*Which organizational features expose an organization and result in a ransomware victimization?*
*What is the rate of ransom payment per ransomware infection?*
*Is there a relationship between ransomware offenders' success and the size of the criminal group?*
*How effective is media attention in preventing a ransomware campaign?*

# The Online Offenders – Money Launderers Junction

The least studied junction within the ransomware ecosystem.

In general, most ransomware transactions are performed using Bitcoin (Paquet-Clauston et al 2018).

Mainly due to a combination of victims' access to Bitcoin services (which in turn leads to an increase in the number of victims that eventually pay the ransom) and the relative ease with which the ransomware offenders can launder the money and cover their tracks.

Commonly use BitMixer and Bitcoin Fog to break the link between the ransomware senders and receivers, and that e BTC-e*, CoinOne, and LocalBitcoins (Huang et al., 2018)

Payment voucher systems.

Offenders use online betting services that accept voucher codes as a method to collect the ransom payment, then transfer those payments to prepaid debit cards and "money mules" that are used to withdraw cash (Savage, Coogan, and Lau 2015).

Research efforts should be invested in exploring the different purposes the ransom money supports once cashed out by offenders.

Empirical research is also needed regarding the effectiveness of police crackdowns on both Bitcoin mixers and exchange services in preventing the development and progression of ransomware campaigns.

* Recently seized and shut down by law enforcement authorities

# The Guardians – Target Junction

**IT Managers to End Point Users**

The problem of securing a corporation's data is the idea that the security they meticulously put in place can be unraveled in a matter of minutes, if an end-point user, for example, violates policy and clicks on a malicious email, … (Luo & Liao 2007; Whitman 2003).

Awareness training considered by users to be "sub-optimal, unengaging, and inconvenient" (Thomas, 2018)

Unfortunately, we have no rigorous empirical evidence regarding the effectiveness of these policies and tools in preventing ransomware infection in organizations.

**Law Enforcement to End Point Users**

In contrast to the frequent interactions between IT managers and potential ransomware targets, interaction between law enforcement agencies and ransomware targets is rare, and occurs only once the target becomes a victim.

Over the past two decades, federal law enforcement officials in the U.S. have forged relationships with local and international agencies to address cyber security in general and, more recently, the prevalence of ransomware.

Electronic Crimes Task Force (ECTF) formed in 2001.

Mission: To work alongside the corporate sector and academia to respond to cyber threats to these nations' financial systems and critical infrastructures.

35 ECTF offices, partnered with 4,000 private sector entities, over 2,000 law enforcement agencies globally, and nearly 400 academic institutions (Subcommittee on Cybersecurity 2014).

Local law enforcement agencies to contend with financial constraints and a lack of technical skills among their limited resources, forcing cyber investigations to lag behind the normal investigative course (Holt, Burruss, & Bossler 2015).

# Suggested Interventions

**The initiators–affiliates junction: disrupt markets**

Online police crackdowns on hackers' forums and online black-market websites (Décary-Hétu & Gimmoni 2017) may prove effective in reducing the rewards from cyber-dependent crimes.

> We suggest that the deployment of ransomware honeypots, as well as infiltration into ransomware campaigns as legitimate affiliates, may be effective in preventing the development and progression of ransomware attacks.

Ransomware affiliates are looking for opportunities to engage in ransomware campaigns and spread malware for financial gain (Savage et al 2015). Moreover, some affiliates are even willing to pay entrance fees in hopes of getting monetary profit from their work in distributing ransomware.

> We suspect that deploying fake ransomware and flooding the market with it will 1) allow us to identify ransomware affiliates, 2) prevent the distribution of real ransomware, and 3) introduce confusion among ransomware affiliates and possibly reduce their likelihood to engage in ransomware spreading.
>
> Posing as an interested ransomware affiliate and initiating business relationships with ransomware initiators could reveal some of the communication patterns and financial relationships between ransomware initiators and affiliates, assist in identifying ransomware initiators' intentions, and allow the development of preventive efforts against such campaigns.

# Suggested Interventions

**The online offenders–targets junction: deflect offenders, deny benefits, and extend guardianship**

Deflecting offenders away from vulnerable places and potential targets is a crime prevention strategy that is designed to increase the amount of effort required from offenders to engage in crime.

> The storage, processing, and sharing of data across multiple geographical locations, as well as through hosting valuable data on a "cloud."
>
> Deployment of production honeypots, which are designed to protect organizations by mitigating the risk of cyberattacks, can be used to distract offenders from more valuable machines (Mokube and Adams 2007; Zhang, Zhou, Qin, and Liu 2003)

Denying offenders' gratifications and benefits from initiating crime reduces the probability that a criminal event will develop and progress.

> Encrypting digital data in such a way that the data can only be read by individuals who have the correct decryption key, would prevent offenders from gaining profit and joy from cyber-dependent crime and reduce the probability of these crimes from progressing (Coles-Kemp and Theoharidou 2007; Beebe and Rao 2005).

Increasing informal monitoring and surveillance efforts by ordinary citizens increases offenders' risk of detection, and in turn reduces the likelihood that offenders will initiate a criminal event.

> Hartel and associates (2011) propose that reporting spam emails and suspicious activities on users' computers to the relevant parties (either email service providers or system administrators) may reduce the probability of cyber-dependent crimes progressing.

# Suggested Interventions

**The online offenders–money launderers junction: reduce anonymity**

Increasing the risk of offenders' detection by restricting individuals' opportunities to remain anonymous

Capitalizing on the availability of "blacklists" of deviant IP addresses, email accounts, or URLs may prevent the occurrence of cyber-dependent crimes (Sinha, Bailey, & Jahanian 2008).

One key intervention that could be tailored to this junction and reduce ransomware offenders' anonymity is the implementation of fake Bitcoin mixers and CoinJoin services.

Bitcoin transactions are publicly visible on the blockchain (Bitcoin's distributed data structure that is held at each Bitcoin node) and the transaction flows between Bitcoin addresses can be easily tracked.

Similarly, monitoring Bitcoin exchange markets may also yield crime prevention outcomes in this junction.

Few businesses are willing to accept direct payment in Bitcoins. It is therefore most  likely that ransomware distributers will need to convert their payments back to more conventional forms of currency to collect their rewards. Most established exchanges that allow Bitcoins to be traded for "regular" government-issued currency are subject to regulation, which typically includes a requirement to "Know Your Customer" (KYC).

We propose monitoring unregulated exchanges and payments markets that ransomware offenders employ for collecting and distributing both Bitcoins (through the bitcoin transaction graph) and other conventional forms of currency (typically handled through wire transfers).

# Suggested Interventions

**The guardians–target juncture: target hardening, formal surveillance, and assisting compliance**

Target hardening: Installing antivirus scanners (Brookson et al 2007) in addition to updating and patching operating systems, applications, and other network software to remove vulnerabilities as soon as fixes are available (Hinduja and Kooi 2013; Beebe and Rao 2005).

Formal surveillance: Keeping and maintaining audit log trails used to collect operational data from the network, which has the potential to deter cybercriminals from initiating cyber-dependent crimes (Newman and Clarke 2013). Similarly, monitoring employees' computers and logging events using designated software and tools can serve as a deterrent to cyber-dependent crimes (Schneier 2000).

Assisting Complaince: User compliance with approved procedures may be the most critical aspect of the guardian process. Creating an environment in which people are encouraged to comply with normative standards of behavior reduces the probability that a situation conducive to crime will emerge, and in turn reduces the probability of criminal events. Both Willison and Siphonen (2009) and Morris (2004) suggest that educating staff and employees regarding organizational security practices assists with compliance and may reduce the risk of cyber-dependent crimes.

Increasing awareness about the hazards of ransomware, among potential targets in both private companies and governmental organizations, is the first step in developing cybersecurity programs. By educating users of these networks to be cautious about their online behaviors, organizations can use their computer users as an additional tool to better protect themselves once a ransomware campaign begins. However, many users remain uneducated regarding the hazards of ransomware and other malicious software. The government should take upon itself the role of identifying potential populations that may not be exposed to cyber-related education programs, reach out to those populations, and educate them about these issues.

While there remains some contention about the effectiveness of end-user partnerships and training (see Albrechtsen, 2007), when IT managers build a culture of awareness concerning the deleterious effects of these incidents and demonstrate the importance of a collective partnership, users' ability to detect, avoid, and better counter the initial phishing and social engineering phase of the typical attack is enhanced (Komatsu, Takagi, and Takemura 2013; Sun and Lee 2016; Thomas 2018). Most subject matter experts agree that awareness training is crucial not only to compliance with procedures, but also in empowering users to counter suspicious activity, as unfamiliarity with phishing and ransomware can put them at higher odds of being susceptible to these attempted intrusions (Thomas 2018). Unfortunately, Thomas (2018) noted that end-point users in previous qualitative studies often stated the training they received was "sub-optimal, infrequent, or unengaging" (p. 16).

Employees should be specifically made aware that attackers are not only deploying these types of technological intrusions, but have begun to couple them with initial social engineering techniques to aid in the intrusion. In fact, the majority of successful attacks combine these two techniques (Verizon 2016). Because file encryption methods, powered by social engineering, are reaching the limits of modern-day cryptography (Luo and Liao 2007), it is important to demonstrate to users how successful attacks using the combination of these two methods can be disastrous to system security. Therefore, an all-inclusive awareness training program should be a priority for any company housing sensitive information.

# Conclusions

Although the volume of ransomware attacks on target computers seems to have slightly declined between 2016 and 2017, some evidence suggests that these campaigns are now more targeted and more destructive than ever before.

There is a pressing need for the development of comprehensive understandings of the problem, and for the deployment of effective interventions

One way to accomplish this goal is to study ransomware within the ecosystem in which it exists.

Understanding the different actors and junctions that are part of this ecology is crucial for embedding successful interventions which aim to disrupt the progression of successful ransomware campaigns. Still, upon implementation of these proposed interventions, there is a need to assess their effectives while adopting an evidence-based cybersecurity approach.

Future research should employ more quasi-experimental and experimental research designs, to obtain more valid and reliable empirical findings on the actual incidence and predictors of the development and progression of successful ransomware campaigns. The implementation of such research designs would allow for a better understanding of the causal mechanisms underlying ransomware offending and victimization, by reducing or eliminating the effects of confounding factors in these empirical relationships. Moreover, by using an experimental approach with innovative technology such as real-time user and system intrusion tracking on devices, researchers will be better able to collect, manage, and analyze empirical data on ransomware infections, and to assess it in the context of our proposed policies once they are adopted.

Similarly, scholars across disciplines should collectively develop universal matrices that could be used for assessing the success of our proposed interventions in disrupting the development of ransomware campaigns, to guide future empirical analyses, to ensure consistency, and to facilitate more interdisciplinary research collaborations. This coordinated research effort would enhance the accurate and rigorous study of behaviors and processes in the ransomware ecosystem, which would maximize the scholarly consensus about key concepts and their operationalization.

## Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1650862.