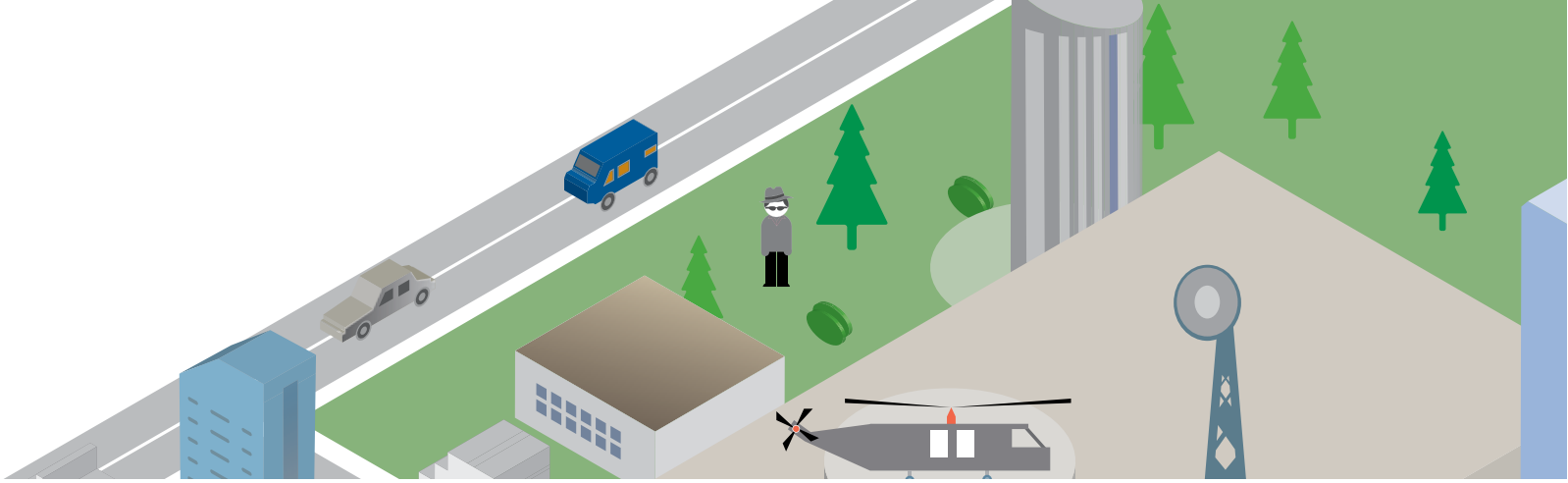
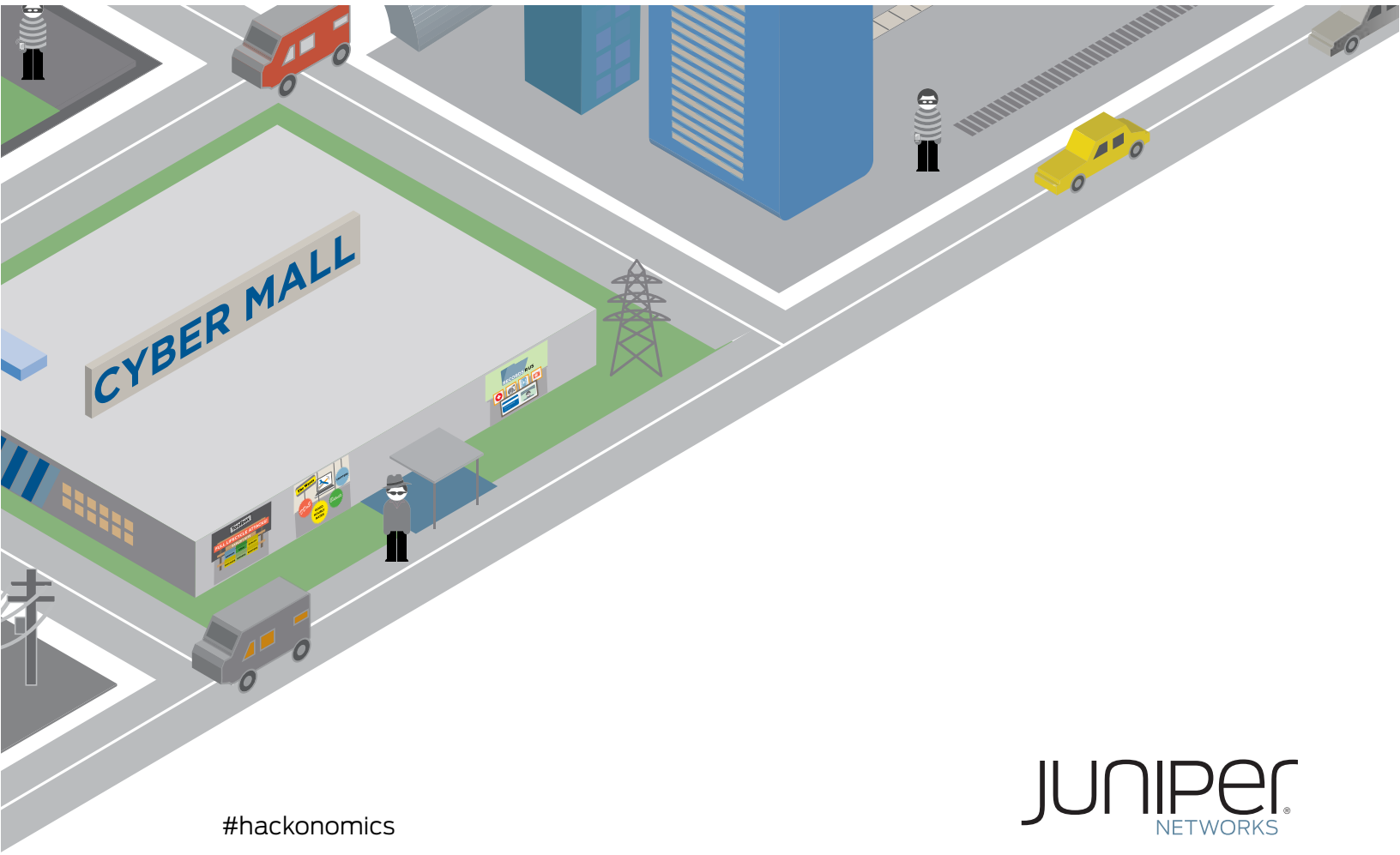


From Underground City to Thriving Metropolis

An Economic Analysis of the Cyber Black Markets

Juniper Networks Perspectives on RAND Corporation's Report



#hackonomics

JUNIPER NETWORKS

Cyber-attacks targeting our personal information are almost a daily occurrence. Why?

Juniper Networks Perspectives on RAND Corporation's Report

Attacks on our companies are putting IP and brand reputations at risk while driving up costs. Over the past decade, cybercriminals, hacking tools and black marketplaces have created an entire new economy.

The world of cybercrime is deep, complex, and has become a fully developed market economy. A new report by the RAND Corporation, sponsored by Juniper Networks, "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar" provides analysis of how these markets function, how they are composed, historical trends, and projections for the future.

While some refer to these markets as the "cyber underground," Juniper believes it would be best described as a "thriving metropolis" today.

While previous studies have attempted to quantify the impact of the hacker black markets in dollar amounts, no study has provided an analysis of its economic structure and maturity, and the implications thereof to business and government organizations worldwide.

RAND researchers conducted in-depth interviews with global experts that are currently or formally involved in the markets, including academics, security researchers, reporters, security vendors, and law enforcement. RAND's report, confirmed by Juniper's vast experience in the network security ecosystem, suggests the cyber black markets are a maturing, multi-billion-dollar economy, with robust infrastructure and social organization.

A Mature Market

RAND reports the evolution of the cyber black markets mirror that of other free markets with both innovation and growth. RAND found five key indicators of economic maturity:

1. **Sophistication:** There is greater sophistication in how the illicit markets operate and the type of tools and attacks being bought and sold. The markets change and adapt to current needs.

2. **Specialization**: There are distinct and customized products, places and participant roles within the underground and a clear hierarchy; often those at the top can make significant amounts of money.

3. **Reliability:** The people and products on the black markets are largely what they say they are, and do what they say they do – although not surprisingly, there are always those trying to rip others off or add unwanted features that give the seller an advantage. Over time, good products squeeze out bad ones, and high-quality brands can command premium prices. The report found that vendors often guarantee their product's lifespan or value and some track what a customer does with their product – a hacker's version of "digital rights management."

4. **Accessibility:** There is a low cost to entry and it is easy to get involved at some level. Forums and digital marketplaces can serve as entry points for aspiring hacker entrepreneurs. However, more transactions are increasingly being done in secret amongst trusted, vetted, and reliable partners.

5. **Resilience:** External events that seemingly would disrupt the markets don't affect it, or if they do, the markets bounce back. Despite increased and improved efforts by law enforcement to disrupt and shut down various parts of the markets-from financing to popular marketplaces – the hacker economy has proved to be quite resilient. The demand and potential profit for attackers is simply too high.

A Thriving Metropolis

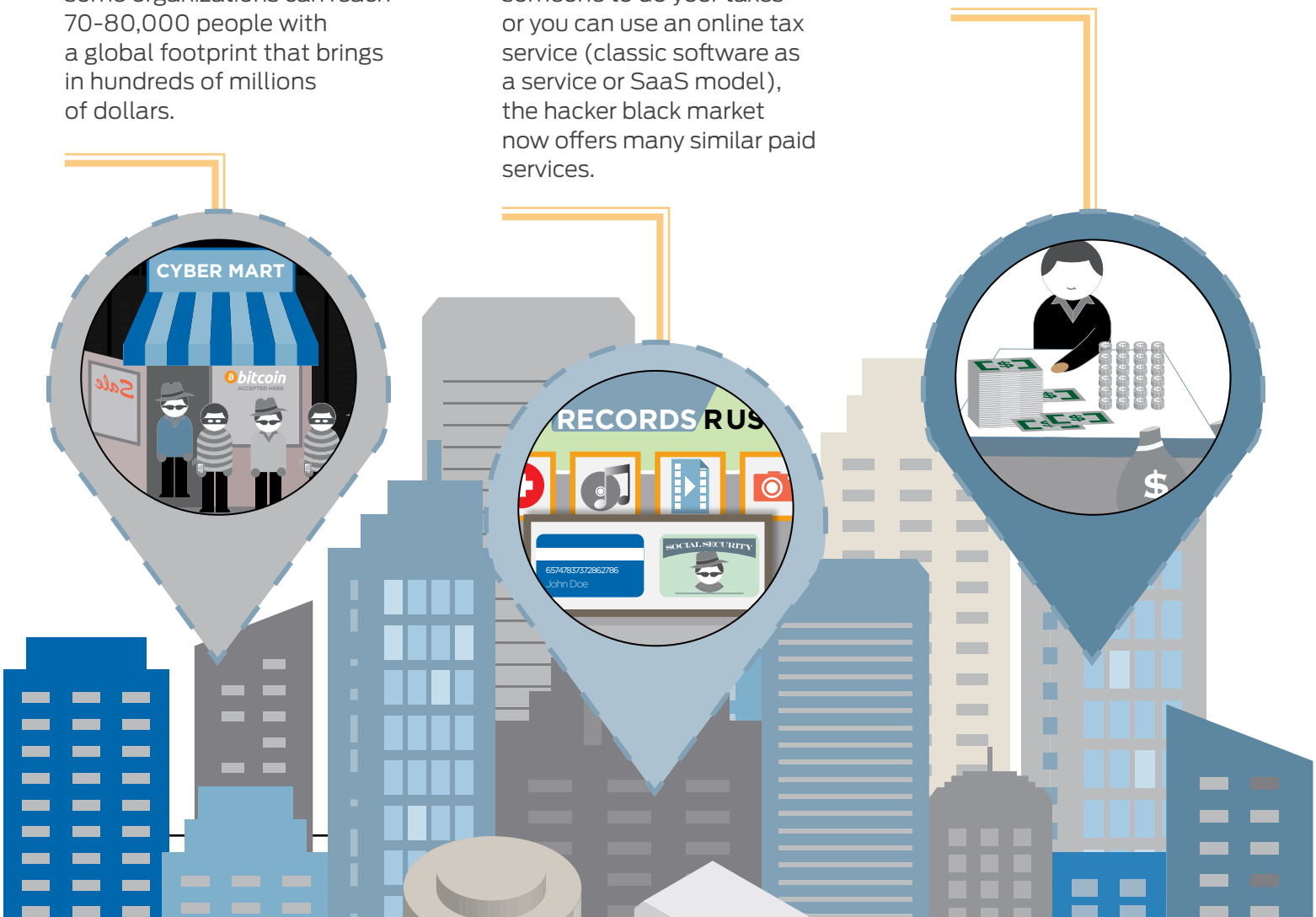
Juniper believes one way to think of the hacker economy is less as a cyber-underground and more of a thriving metropolitan city with diverse communities, industries and interactions. RAND's report asserts that the hacker market was once a varied landscape of discrete, ad hoc networks of individuals motivated by little more than ego and notoriety, but today, it has emerged as a playground of financially driven, highly organized and sophisticated groups.

Like a metropolis, the black market is a collection of (skilled and unskilled) suppliers, vendors, potential buyers, and intermediaries for goods or services surrounding digitally based crimes.

Storefronts: Like other forms of e-commerce, many data records, exploit kits and goods are bought and sold from storefronts – which can encompass everything from instant messaging chat channels, forums and bulletin boards, to sophisticated stores (not unlike an Amazon.com). RAND found some organizations can reach 70-80,000 people with a global footprint that brings in hundreds of millions of dollars.

Service Economy: Not only goods but criminal services are available from the hacker economy. The rise of botnets have made it possible for criminals to sell DDoS and spamming as a service to other criminals. In fact, exploit kits to help with attacks are often "rented" by the week or month. Just as you can pay someone to do your taxes or you can use an online tax service (classic software as a service or SaaS model), the hacker black market now offers many similar paid services.

Hierarchical Society: Much like a legitimate business, the study found it takes connections and relationships to move up the (cyber) food chain. Getting to the top requires personal connections, but those at the top are making the lion's share of the money.



A Thriving Metropolis

Currencies: Transactions in the cyber black markets are often conducted by means of digital currencies. Bitcoin, Pecunix, AlertPay, PPcoin, Litecoin, Feathercoin, and Bitcoin extensions, such as Zerocoin are a few that RAND discusses in its analysis. Although transactions can also be done by means of non-digital currency, many criminal sites are starting to accept only digital crypto currencies due to their anonymity and security characteristics.

Rule of Law: There is indeed honor among thieves. RAND found many parts of the cyber black markets are well structured, policed and have rules like a constitution. In addition, those who scam others are regularly banned or otherwise pushed off the market. And, as cybercriminals move further up the chain, there is an extensive vetting process to participate.

Criminals: Even the criminal cyber black market has criminals. Known as "rippers," these specific bad guys do not provide the goods or services they claim.

A Thriving Metropolis

Education and Training: RAND identified widely available tools and resources to teach people how to hack, including YouTube videos and Google guides on topics such as exploit kits and where to buy credit cards. This readily available instruction also helps to facilitate entry into the hacker economy. The RAND study says this access to training – coupled with a generation of digital natives – has accelerated sophistication and a broader set of roles within the economy – from administrators to subject matter experts, vendors and general members.

Diversity: While RAND found cybercriminals from China, Latin America and Eastern Europe are typically known for quantity in malware attacks, those from Russia tend to be thought of as the leader in quality. RAND also found areas of expertise and focus among cybercriminals from different countries. Many Vietnamese cybercriminals, for example, mainly focus on e-commerce hacks. Cybercriminals from Russia, Romania, Lithuania and Ukraine focus on financial institutions. Many Chinese cybercriminals specialize in intellectual property. And US-based cybercriminals primarily target US-based systems and financial systems. In addition to a diverse set of actors, RAND also found more cross-pollination between these cybercriminals than ever before.

Disrupting and Defending Against Attacks – the View from Juniper

Taken together, the growing maturity of the hacker black market is creating significant new challenges for companies and individuals. According to the report, the ability to attack will likely outpace the ability to defend. So what does this mean for those responsible for protecting companies and people's information?

Juniper believes it means we need to look at the root cause of the accelerated cybercrime market maturation – the very economics that drive its success.

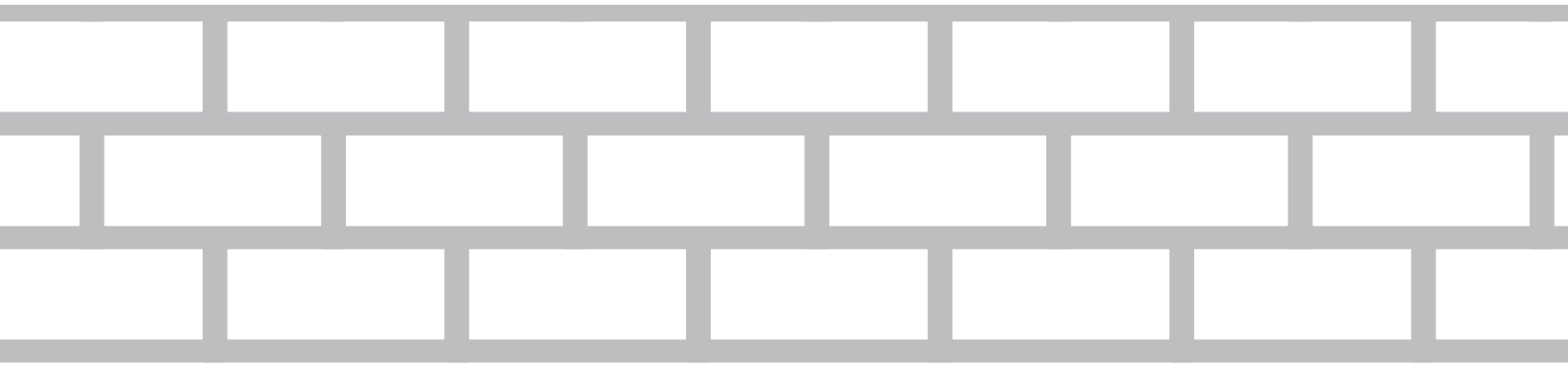
We need to change the economics of hacking and find ways to disrupt the value chains that result in successful attacks.

How do we do this? While we cannot go on the offensive and hack back – we would lose the moral high ground, not to mention the illegalities involved – we can no longer remain passive. Using forms of active defense like intrusion deception to actively identify, disrupt and frustrate attackers is a very promising approach.

For instance, if we can waste a criminal's time or make the exploit tools they purchased on the black market ineffective, we can prevent the loss of information and cut their value chain early in the attack cycle. We could also insert fake data as tar traps or hacking forums that could flood the market to breed distrust among actors. We can also create economic incentives to encourage more blackhats to become legitimate security researchers.

One thing is crystal clear, the security industry, government and legal communities must come together to establish new norms for how companies can more vigorously defend themselves in cyberspace while respecting privacy, civil liberties and the proper boundary public and private sector actions.

No matter what is ultimately done, understanding the attackers, their systems and motivations should help us, as an industry, offer better protection.



"Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," is based on in-depth interviews conducted by the RAND Corporation, between October and December 2013, with global experts who are currently or formerly involved in the market, including academics, security researchers, reporters, security vendors, and law enforcement. It is the first of a series of reports from RAND sponsored by Juniper Networks.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Copyright 2014 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.