CHILDREN AND FAMILIES
EDUCATION AND THE ARTS
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INFRASTRUCTURE AND TRANSPORTATION
INTERNATIONAL AFFAIRS
LAW AND BUSINESS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
TERRORISM AND HOMELAND SECURITY

Skip all front matter: Jump to Page 1 ▼

Support RAND

For More Information

Limited Electronic Distribution Rights

This report is part of the RAND Corporation research report series. RAND reports present research findings and objective analysis that address the challenges facing the public and private sectors. All RAND reports undergo rigorous peer review to ensure high standards for research quality and objectivity.

Markets for Cybercrime Tools and Stolen Data

Hackers' Bazaar

Lillian Ablon, Martin C. Libicki, Andrea A. Golay

The research described in this report was sponsored by Juniper Networks and conducted within the Acquisition and Technology Policy Center of the RAND National Security Research Division.

RAND OFFICES
SANTA MONICA, CA • WASHINGTON, DC
PITTSBURGH, PA • NEW ORLEANS, LA • JACKSON, MS • BOSTON, MA
CAMBRIDGE, UK • BRUSSELS, BE
www.rand.org

Summary

Black and gray markets for hacking tools, hacking services, and the fruits of hacking are gaining widespread attention as more attacks and attack mechanisms are linked in one way or another to such markets. In the December 2013 breach of the retail giant Target, where data from as many as 40 million credit cards and 70 million user accounts were hijacked, such data appeared within days on black-market sites. Other examples of attacks and their links to underground markets include

- recent increases in the use of watering-hole attacks (where users visit popular, legitimate, but compromised websites) based on well-known exploit kits available for sale on the black market (see, e.g., Malwageddon, 2013)
- the growing prevalence of malware inserted into online advertisements that, when clicked, infect a victim's computer, and call back to an exploit kit to launch additional malware; data is then stolen and sold on black markets (e.g., Joostbijl, 2014)
- websites throttled by Distributed Denial of Service (DDoS) attacks implemented by rented botnets available on the black market (e.g., Schwartz, 2010).

These black markets are growing in size and complexity. The hacker market—once a varied landscape of discrete, ad hoc networks of individuals initially motivated by little more than ego and notoriety—has emerged as a playground of financially driven, highly organized, and sophisticated groups. In certain respects, the black market can be more profitable than the illegal drug trade; the links to end-users are more direct, and because worldwide distribution is accomplished electronically, the requirements are negligible.

Understanding this market in its entirety is complicated by the fact that it is geographically spread out, diverse, segmented, and usually hidden under the cloak of darknets (e.g., Tor), anonymization, and cryptographic features. What can be surmised from interviews with expert observers is that the hacker market poses a formidable challenge and an increasing threat to businesses, governments, and individuals operating in the digital world.

Increasing sophistication and specialization characterizes both how the market operates and the types of goods and services being sold. As with any other market, products and vendors tend to be reliable; but the unwary can be scammed or sold products with unwanted features. Methods for communication have gotten more innovative and secure: there is greater use of encryption and privacy mechanisms, such as off-the-record messaging and digital and cryptocurrencies. Organization of groups and forums are highly structured, and specialization of roles and responsibilities is common. Vendors often guarantee their products' lifespan or

value, and some track what a customer does with their product—a hacker's version of "digital rights management."

There has been a steady increase in the availability of goods and services offered, from stolen records and exploit kits to "stolen-to-order" goods, such as intellectual property and zero-day (more commonly, half-day) vulnerabilities. Greater availability of as-a-service models, point-and-click tools, and easy-to-find online tutorials makes it easier for technical novices to use what these markets have to offer. Despite these markets being generally illicit, they follow the same economic laws and practices as other markets: Participants communicate through various channels, place their orders, and get products. Black-market evolution mirrors the normal evolution of a free market, with both innovation and growth. Prices for credit cards, for example, are falling because the market is flooded with records, and botnets and DDoS capabilities are cheaper because so many more options are available.

Access to such markets, conversely, is getting tighter. Motivated, in part, by recent black market takedowns, more sophisticated markets are undertaking more rigorous and aggressive vetting of individuals. More transactions are taking place on virtual private networks and darknets, with anonymization and encryption capabilities enabled.

Despite increased efforts by law enforcement to disrupt and shut down various parts of the market—from its financing to popular marketplaces—the hacker economy has proved to be quite resilient. The market bounces back after a takedown or arrest. Finding comparable replacements for market leaders like the Blackhole Exploit Kit or the Silk Road may take a few iterations, but substitutes appear almost immediately as competing forums constantly vie for market share. That said, law enforcement is getting better for a number of reasons: More individuals are technologically savvy; suspects are going after bigger targets, and thus are attracting more attention; and more crimes involve a digital component, giving law enforcement more opportunities to encounter crime in cyberspace.

Adding to the complexity for defenders are the rapidly emerging and highly secretive markets for zero-day vulnerabilities, which occur in both gray (licit) and black (illicit) markets. Discussions surrounding zero-days have risen in prominence because of increased media attention and recent decisions by many software makers to pay for discoveries of such vulnerabilities. Ironically, sources of information that were once forthcoming have gone silent of late.

Noteworthy Projections and Predictions

Since the mid-2000s, the hacking community has been steadily growing and maturing, as has its market. It took more than a decade of continuous development and innovation, the introduction of new generations of digitally savvy participants, and significant trial and error to achieve today's landscape, in which experts agree on the following projections and predictions:

- There will be more activity in darknets, more checking and vetting of participants, more use of cryptocurrencies, greater anonymity capabilities in malware, and more attention to encrypting and protecting communications and transactions.
- Helped by such markets, the ability to attack will likely outpace the ability to defend.
- Hyperconnectivity will create more points of presence for attack and exploitation, so that crime will increasingly have a networked or cyber component, creating a wider range of opportunities for black markets.

- Exploitation of social networks and mobile devices will continue to grow.
- There will be more hacking for hire, as-a-service offerings, and brokers.

Experts disagree, however, on who will be most affected by the growth of the black market (e.g., small or large businesses, individuals), what products will be on the rise (e.g., fungible goods, such as data records and credit card information; nonfungible goods, such as intellectual property), or which types of attacks will be most prevalent (e.g., persistent, targeted attacks; opportunistic, mass "smash-and-grab" attacks).

For Further Research

The harmful effects of black markets on cybersecurity suggest the need for options to suppress such market activity—without which, very little is likely to change. The search for such options raises several questions. How should security technologies and law enforcement shift their approaches to thwart the rise of the markets? How might bug bounty programs or better pay and incentives from legitimate companies shift transactions and talent off the illicit markets into legitimate business operations? Would it be worthwhile to establish fake credit card shops, fake forums, and sites for counterfeit goods that would flood the market with fake items? Would more vigorous law enforcement help? Would international cooperation be required to put muscle behind today's law enforcement? Should there be mandates for encryption on point-of-sale terminals, safer and stronger storage of passwords and user credentials, implementation of "chip and PIN" (personal identification number) in the United States? If companies do not comply, would making them liable for data breaches decrease activity on the markets?

Such questions are candidates for further research.