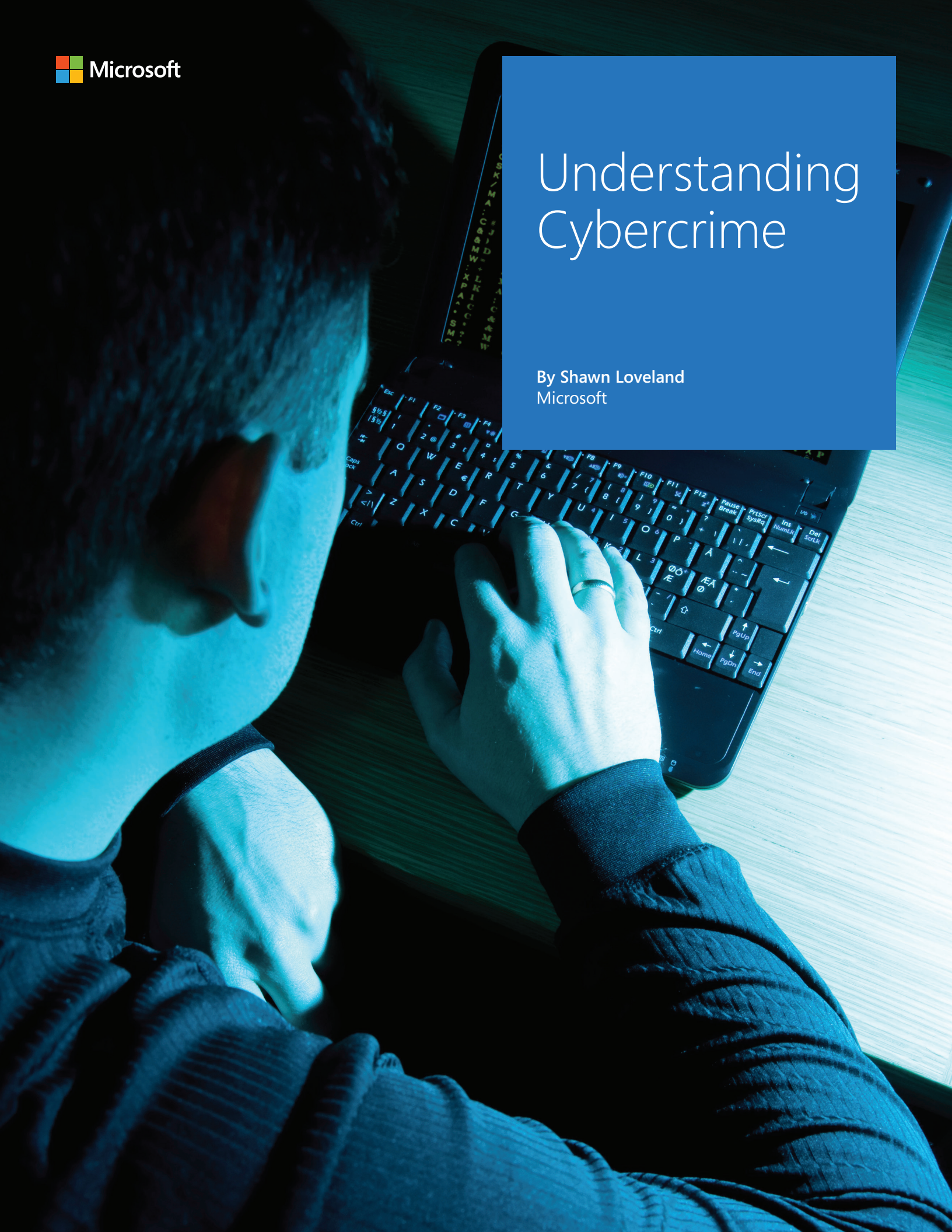


Microsoft

Understanding Cybercrime

By Shawn Loveland
Microsoft

Blackhat cybercrime is a form of malicious online behavior motivated by money. Ignoring this, for example, by treating Blackhat cybercrime as a purely technological problem, makes mitigation difficult and costly. Understanding Blackhat criminal techniques, motivations, culture, and ecosystem are critical to defending against current attacks and deterring future ones.

This paper describes key elements of the Blackhat cybercrime ecosystem -- an ecosystem that is harming nearly every company and user on the Internet.

Just as the PC/computer/ mobile device ecosystem has grown over the decades, so has the cybercrime industry, which today is more organized and motivated than at any time in history.

Defining the Blackhat Cybercriminal

There are various types of bad actors on the Internet. Regional, cultural, and economic, considerations influence their motivations and choices of targets. Their tools and techniques differ as well.

There are two broad categories of cybercriminals:

- **Non-professional cybercriminals** exhibit little or no business or technical expertise using "off-the-shelf" malware kits[1], crimeware kits[2], and cybercrime services[3]. They often communicate in open forums that do little to no vetting of their members. Even though these cybercriminals are not sophisticated, they should not be taken lightly -- several of the most significant cybercrime events over the last few years, which caused hundreds of millions of dollars in losses to their victims, were conducted by this category of cybercriminals.

- **Blackhat cybercriminals** are equipped with business and technical expertise. These are the people who create the crimeware kits and services used by other Blackhat cybercriminals, non-professional cybercriminals, and some state-sponsored abusers. In most regions, they communicate in closed forums that vet their members, working in small, specialized groups, cooperating and splitting the proceeds of their activities.

There are other categories of bad actors, whose tools, techniques, or motivations differ so much from cybercriminals that they must be defended against separately. These include:

- **Hactivists** who attack to gain attention for their cause. They are not motivated by profit, but their actions can cause great damage to victims' reputations and lead to significant expense.

- **Grayhats** offer online services that can be valuable to legitimate companies as well as to cybercriminals. They are bad actors to the extent they allow cybercriminals to use their services. Example include:

    - Search Engine Optimization (SEO) that promotes criminal or fraudulent search results

    - High volume e-mail marketing (spam) that promotes counterfeit goods or malicious payloads (phishing URLs, malware attachments, etc.)

- **State-sponsored groups** are motivated by national interests. Their attacks are normally covert and focused on gaining access to a specific asset such as product designs, proprietary information, or an e-mail account being used in sensitive negotiations. State-sponsored attacks also can be used to send political messages. For example, gaining embarrassing information on protestors, and leaking it to the press.

---

1. Malware kits are software packages designed to gain unauthorized access to victims' computers. Examples include: exploit kits, banking Trojans, Remote Access Trojans (RATs), etc.
2. Crimeware kits are software packages that aid in internet based attacks. Examples include: Bot management consoles, compromised account checkers, abuse account creators (aka spam accounts).
3. Crimeware services offer malware kits and crimeware kits for sale or subscription (Cybercrime as a Service (CaaS)). It is analogous to legitimate companies having the option of buying software licenses or subscribing to services.

Abuser Personas

Tools, techniques, motivations (TTM) vary by abuser

BLACK-HATS

- Run as a business
- Business and technical expertise
- Often works in a closed group of other professional cybercriminals
- Criminal reputation is everything

NON-PROFESSIONAL CYBERCRIMINALS

- Use crime kits to make spending money
- Little to no business or technical expertise

GRAY-HATS

- They believe they are offering legitimate services. However, their customers can be both "legitimate" or criminal
- Ran as a business

HACTIVISTS

- Individuals or groups who hack for a social cause, without economic motivation
- Has both technical people and followers

STATE SPONSORED

- National security and/or economic motivation
- Technical expertise
- Work in a closed group of other professionals
- Often uses Black-Hat resources and/or techniques to mask their identity

Defining the Blackhat Cybercriminal Ecosystem

Internet abuse used to be carried out by lone hackers motivated by the thrill of discovery. Now it is predominately carried out by professional businesses motivated by money. It is a multibillion-dollar underground economy, with Cybercrime-as-a-Service (CaaS) and thousands of Blackhat Cybercriminals trading millions of compromised computers, billions of compromised credentials, and untold terabytes of stolen information.

Bad actors on the Internet are not a monolithic group, and neither are the cybercrime ecosystems they've created. There are regional and cultural differences, including social norms concerning acceptable monetization strategies. However, with the globalization of cybercrime in recent years, the cultural differences are more evident when a tool, technique, or monetization strategy is new.

The Blackhat Cybercrime Supply Chain

In the early days of cybercrime, a cybercriminal would have to develop all the components of their attacks. This limited their techniques and flexibility, making them easier to defend against. But the cybercrime ecosystem has evolved in the criminals' favor. Now there is an industry of tool writers who are paid well to create crimeware kits and keep them one step ahead of the defenders, using cheap labor in developing countries to keep costs low.

Examples of services Blackhats have access to:

- **Exploit markets** where software vulnerabilities – capable of silently infecting PCs, tablets, and smartphones with malware – are bought and sold. The price of exploits depend on the prevalence of the software being targeted, how exclusive the seller is, and the intended victim. It is not uncommon for exploits to be sold to buyers for as little as $100 to more than $350,000.

- **Anti-AV** services that allow cybercriminals to distribute malware to their victim's PC without fear of being detected by anti-virus products. There also are services that will notify the Blackhat when different AV products begin to detect their malicious software, so that updated malware can be pushed to the victim PCs ahead of AV signature updates. Two examples of anti-AV services:

    - Monitoring AV products to alert the bad actor when a piece of malware begins to be detected by various AV products. This type of service can cost the bad actor less than $0.01 per scan, to a monthly subscription of $10.00, or more.

    - File encryptors, packers, and other techniques to change the signature of malware. This type of service can cost the bad actor less than $50.00 to over $500.00 per update.

- **Breaching services** available to Blackhats for breaching websites and other company systems. Some services do breaches on speculation with the expectation that a buyer for the compromised systems can be found, and some services do breaching for hire against a designated website or company.

- **Criminal proxy networks** allow criminals to route their Internet traffic to defeat security services based on IP reputation or the geolocation of the user logging in. These services give the attacker the ability to route traffic to within a couple of miles of any physical address. The price of this type of service varies a lot based on geolocation of the proxy and how fresh it is into the proxy's lifecycle. The need of many bad actors can met by proxy services that cost as little as $20.00 per month for unlimited proxies. Some bad actors are willing to pay $30.00 or more per proxy for fresh proxy in a desirable geolocation,

- **Account Take Over Services (ATOS)**, also referred to as spear-phishing services, charge the attacker anywhere from $15.00 to $500.00 to take over a specific victim's account. The techniques often used by these services:

    - Conduct a socially-engineered attack against the victim (e.g. phishing or targeted malware attack) so the user provides their credentials to the attacker.

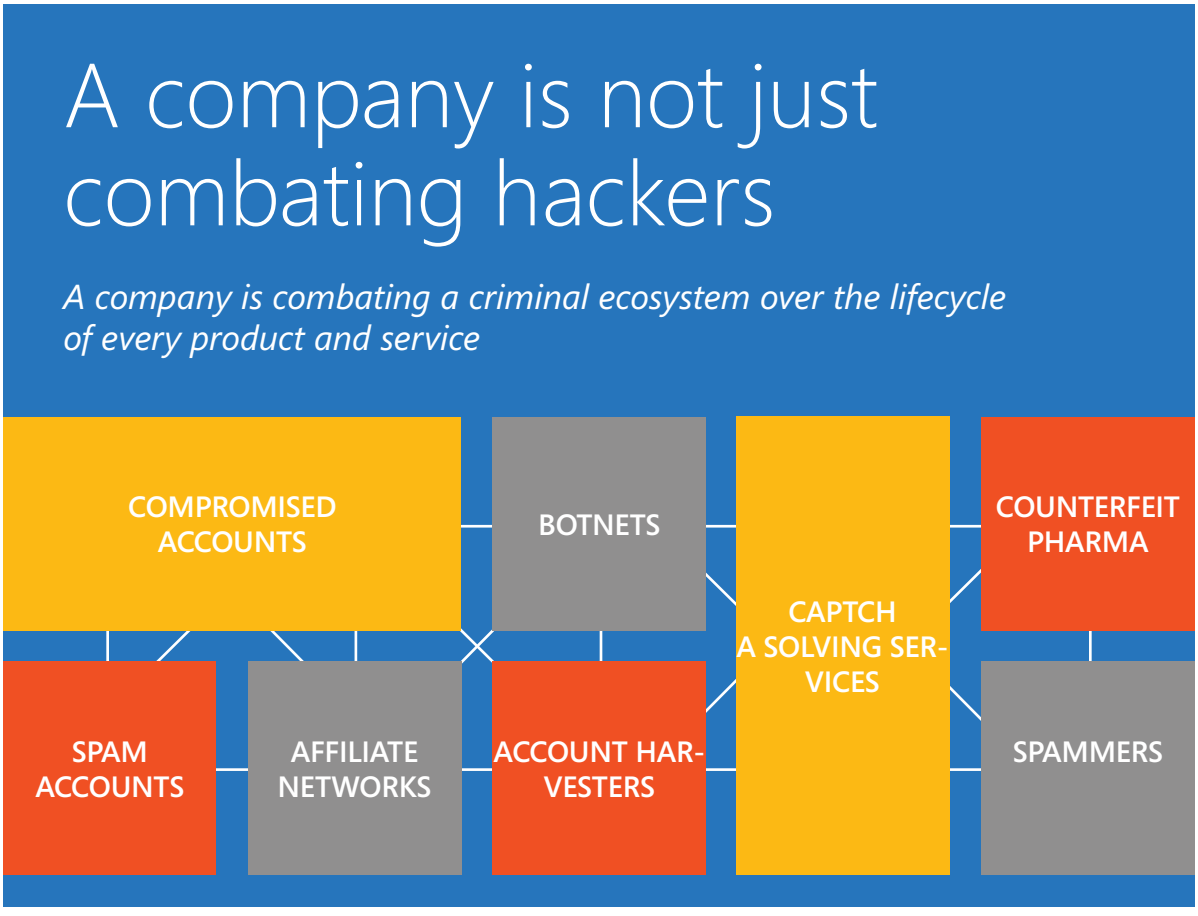
    - Exploit a technical or business process vulnerability in the Internet service or corporate infrastructure to gain access to user credentials.

    - Access data from historical breaches with the user's name and password, or enough information to conduct a "password recovery" of the user's account.

- **Remote Access Trojan (RATs)** allow cybercriminals to install software to gain remote access to a victim's PC, server or phone, which can then be used to gain control over the devices as well as access connected systems. There are many RAT cybercrime kits available to cybercriminals. Prices vary from free, to more advance kits that have a subscription price of over $650 per year.

- **Compromised accounts** in the form of compromised credentials. Depending on several factors, the cost of compromised accounts runs from $0.03 to $25.00 or more per 1,000 accounts when bought in bulk. There are even services that will sell a complete dossier on a victim, including name, address, credit card information, bank account information, credit reports, business reports, real-time and historic geographic location data, medical information, and more.

- **Other common markets** include ones where Blackhats can sell any of the assets they steal, accounts, credit cards, banking information, compromised PCs, intellectual property stolen from companies, and more. They no longer need to put together end-to-end attacks, they can now specialize on small parts of the value chain.



Considerations for Combating Blackhats

To quote Sun Tzu in the "Art of War," "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.... If you know neither the enemy nor yourself, you will succumb in every battle." The same rule can be applied to defending against cybercrime. To be successful in cyber-defense, one needs to know his/her adversaries and what motivates them.

Here are examples of questions a company should answer to understand their adversary:

- **Who are you combating?** Not only the individual, but the persona, national or cultural identity, and the ethics and norms that influence their goals and behavior.

- **What are their tools, techniques, and motivations?**

- **What is their history of abuse, both by a particular group and with a particular product?**

- **What do you have that is valuable to an attacker?** For example:

    - Items that can be directly monetized:
        - Credit cards, bank credentials, and stored value instruments
        - The ability to purchase physical and digital goods
        - Data that can be held for ransom

    - Items that are indirectly monetizable:
        - Intellectual property of your employees, company, and customers
        - Personal information, credentials, and data of your users, customers, and employees
        - Company infrastructure data such as IP addresses, network bandwidth, or storage capacity
        - Infrastructure that can be used as a stepping stone into a third-party's systems

Here are examples of questions a company should answer to understand its defenses:

- **What forms of abuse can your company measure?**
  Are there baselines and ranges for normal behavior? Are there alerts for abnormal behavior?

- **Are your metrics and analysis real-time or offline?**
  How quickly can your systems detect and alert on abuse or attacks? Do you measure the impact of cyberattacks to your systems, users, customers, brand, etc.?

- **What actions can your company take?**
  What is your company's ability from both technical and business process perspectives to quickly take action(s) when an attack is detected? Is the process fast enough to mitigate the threat?

- **Does the adversary have access to your systems to test your defenses?** For example:
  - Can you detect these test accounts?
  - Do attackers have accounts on your e-mail system to find a way through your spam filters?
  - Do attackers have service accounts that allow them to monitor the company's website user interface and perform transactions to test anti-fraud detection?
- **Do you belong to an industry group to share threat intelligence?** Examples of such groups include the Anti-Phishing working Group (APWG), the Messaging, Malware, and Mobile Anti-Abuse Working Group (M3AAWG), various regional and industry Computer Emergency Readiness Teams (CERTS), and industry specific Information Sharing and Analysis Center (ISACs).
- **Has your company deployed the appropriate operational alerts?** For example, HoneyTraps or trip wires inside and outside your network to detect suspicious activity that was otherwise undetected.

Techniques and Tools Available to Companies to aid in Disrupting the Cybercrime Business Model

In combating abuse, nothing is static or durable

Effective defenses against cybercriminals are neither static nor durable because cybercrime is essentially a crime of opportunity. A Blackhat cybercriminal's success relies on his/her ability to evade existing defenses, perform actions that generate a high ROI[4], and do so in a cost effective manner. Therefore by definition, what may be an adequate defense strategy today will become less effective over time. Simply put, if attackers believe there is an adequate ROI, they will continue to invest time and money to probe and adjust their attacks until they are successful.

That said, the profit motive behind cybercriminals can also be used as an advantage to the defender. We know that in general, a Blackhat cybercriminal is just like any other businessperson whose goal is to maximize the ROI. Therefore the "crime of opportunity" is usually an attack that uses as much commoditized tooling as possible, and produces large volumes of compromised computers, stolen credentials, and other data that can be easily generate revenue in one or more of the underground markets. Therefore, if the defender can increase the level of effort required to breach a system or network, and also to reduce or eliminate the ROI to the attacker of a potential breach, the result may be a decreased level of interest in those systems or networks as potential targets for cybercrime.

4. ROI= Return on Investment

Once cybercrime is thought of as a business problem, strategies can be applied to target the criminal's economics and undermine their business model. A strategic view includes the evolution of security risk to include a notion of, "Abuse Risk" that considers not just the tools and techniques of the attacker, but their motivations as well as the particular roles they play within the cybercrime ecosystem. Abuse risks need to be evaluated, just as security risks are, during a product or service's Software Development Life Cycle (SDLC) process. This ensures the product or service being developed is in a position to detect abuse and adjust defenses quickly over its lifecycle. Particularly before attackers are able to validate their business model of abusing your products, services, and/or users.

Future papers in this series cover existing and new techniques disrupting abuse threats.
Topics will include:

- Abuse threat modeling as an extension to the SDL

Some of the existing information Microsoft makes available to companies, include:

- Software Development Lifecycle (SDL)
- Attack Surface Analyzer 1.0: Understand your attack surface before & after new apps are deployed
- Microsoft Threat Modeling Tool 2014: A tool to help engineers find and address system security issues
- MiniFuzz basic file fuzzing tool: A simple fuzzer designed to ease adoption of fuzz testing
- Regular expression file fuzzing tool: A tool to test for potential denial of service vulnerabilities

www.Microsoft.com