Cisco Umbrella

E-BOOK

Economics of cybercrime.

The evolving cybercriminal business model

Introduction

It was almost 5 pm on a Friday, but he wanted to finish a few more things before he shut down for the weekend. He had only started this new gig a month ago, but he was already feeling really good about his decision to come on board. The organization he worked for had really good credibility and a stellar reputation in the market. He had been specifically tasked with working on product innovation. Some of their products were not as successful as they had been when they first emerged into the market, but through a few simple changes he had figured out a way to make the product faster, more efficient, and more impactful. During beta testing, they had a 38% success rate. He was looking forward to his big paycheck later this month. His portion would definitely be enough to pay for that luxury trip to Italy he was planning for late spring.

He closed his laptop and smiled. If it wasn't illegal, he was sure the cybercrime organization he worked for would make the Forbes best places to work list. The hours were great and the money was absolutely unbeatable.

Cybercrime has become a low risk, high reward business that looks very similar to a place you might work. Employees have the evenings and weekends off, product innovation is key, and credibility and reputation are paramount. It doesn't require a lot of capital, expensive tools, or experience to get started.

How did this happen?
What factors are perpetuating this type of business model? Where will it go from here?

As an MSP, it is important to be able to explain the cybercrime business model to your customers. This isn't about the fear of threats, but the facts behind the proliferation of attacks. One of the best security tools is knowledge. Knowing how cybercriminals operate is key to knowing how to protect yourself – and your customers.

It's time to arm yourself with knowledge.

This isn't about the fear of threats, but the facts behind the proliferation of attacks.

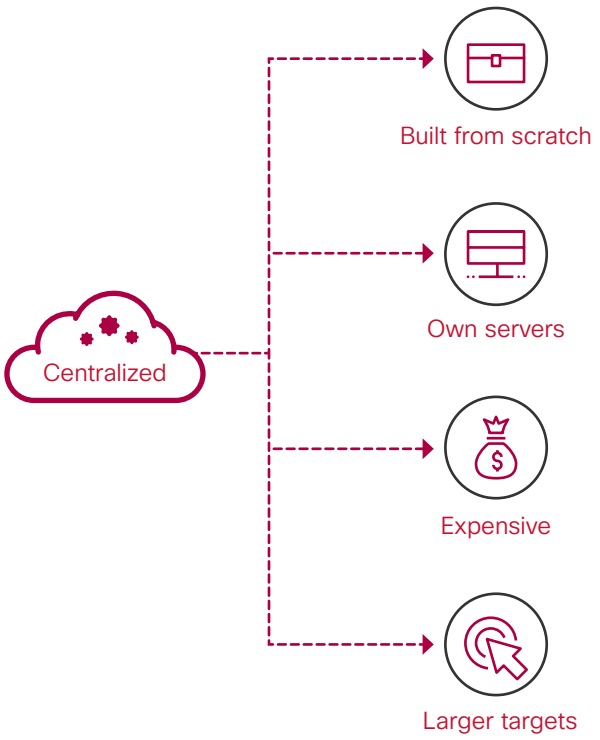
Once upon a time there was a cybercriminal...

Cybercrime continues to become cheaper to operate and more profitable to execute. Cybercrime is currently at a 20:1 profit to effort ratio.[1] Through market and technology shifts, cybercriminals have been able to find more efficient (and cheaper) ways to deploy and execute malware. It has become more targeted and more effective with higher success rates.

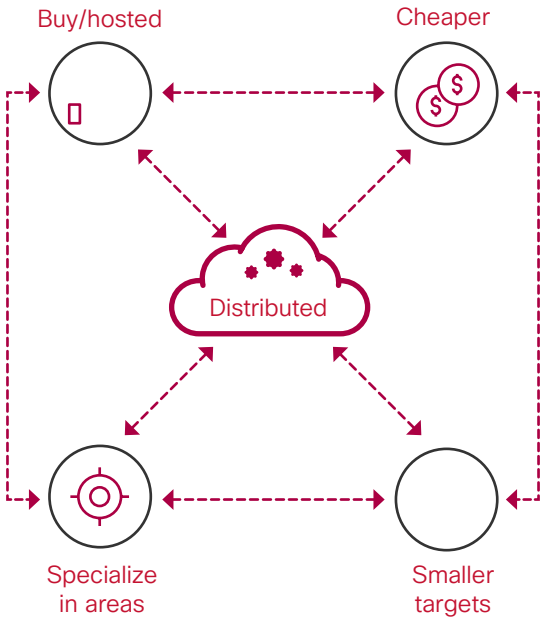
The infrastructure of cybercrime has evolved significantly. Historically, there were higher barriers to entry. Cybercriminals owned their own servers and built malware from scratch. It was expensive to operate and incredibly time consuming. As shown in the image below, the business model has changed on all fronts. It used to be centralized, with cybercriminals using their own servers. Since it was very time consuming and expensive to build malware, large organizations were often targeted in order to achieve profits. Over the years, it has become an ecosystem with a distributed system and specialization areas. It costs much less to create malware, and for those that are not interested in creating their own malware, they can simply purchase it as a service. Volume has become key, with smaller targets becoming more of interest.

Evolution of cybercrime

Hacker organization

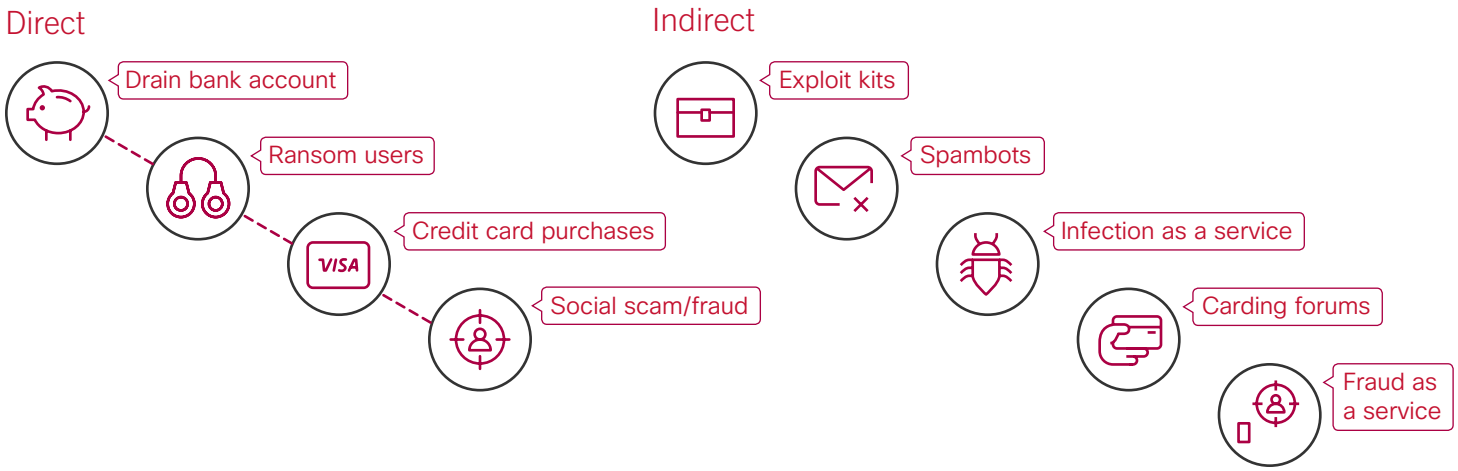


Criminal ecosystem



Monetizing cybercrime

What is the driver behind cybercrime? As Nelly said, "it must be the money." There has been a profound shift from the earlier days of cybercrime, with a focus on notoriety to the current focus on profit. There are both direct and indirect ways to make money off of cybercrime. The direct method is when money is taken directly from the victim. Examples include draining the victim's bank account, requiring a ransom, using the victim's credit card to make purchases, and social fraud such as emails mimicking a CEO. The other method is indirect, and involves obtaining information from the victim that is valuable to sell into an ecosystem or directly selling malware. Examples of the indirect method include exploit kits, spambots, infection as a service, carding forums, and fraud as a service.



Cybercrime is a thriving marketplace. Credit card numbers have been a popular item to steal, and stolen credit cards are often found for sale on the black market. These markets are known as card shops or "carding sites" that are not searchable on traditional search engines but are accessible on the darknet.[2] Credit cards that are fresh on the market and have balances tend to fetch a higher price since these variables make it more likely the card has not been deactivated.

The proliferation of threats comes down to profitability, and it continues to be a very profitable business. This year, ransomware has dominated the threat market. Ransomware is a type of malware that encrypts information on your computer, so it can't be accessed until a ransom is paid. An average of $300 is usually charged, and victims often end up purchasing the decryption key so they can regain access to their own data.[3] In 2016, the cybercriminals have started to charge higher ransoms for businesses with mission critical data. For example, hospitals that have fallen victim to ransomware have felt forced to pay the ransom because they needed access to crucial patient data. For example, Hollywood Presbyterian recently paid a $17,000 ransom to get their systems back.[4]

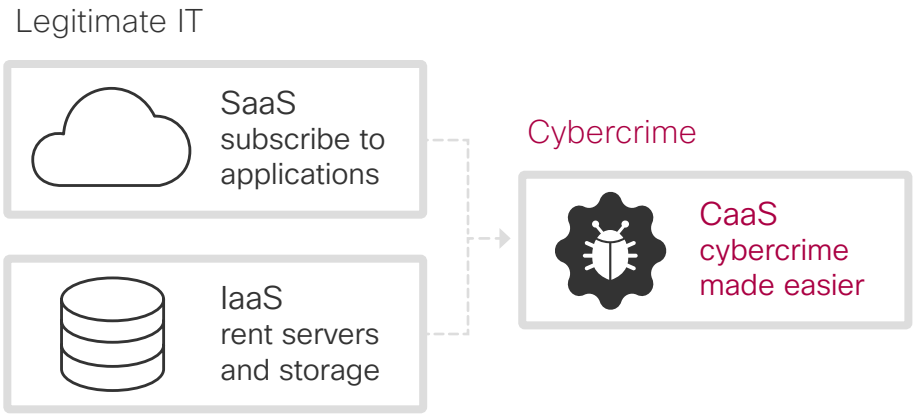
The numbers tell it all. In 2015, 430 million new malware threats made their appearance on the threat landscape.[5] This is a significant increase from the 30 million new malware threats that were made in 2013.[6] As long as there is a profit to be made, there will continue to be an abundant supply of cybercrime.

Evolution of attacks

Because cybercrime is such a lucrative business, once an attack method becomes ineffective, cybercriminals evolve their methods of attack until they are successful. An example of this is ransomware, which first made an appearance in 1989 as an AIDS trojan.[7] Ransomware has evolved from misleading applications to fake antivirus and lockers to the current form of crypto-ransomware.

Technology has played a significant role in propelling cybercrime. One example is the creation and distribution of malware. The Software as a Service (SaaS) model allows legitimate organizations to more easily sign up for more applications since they do not need to build out infrastructure and are able to dynamically change applications. Infrastructure as a Service (IaaS) is another model that enables businesses to rent servers and storage, accelerating the IT within an organization. A new breed has emerged that applies SaaS and IaaS to the cybercriminal world — Cybercrime as a Service. This is a spin on SaaS and IaaS, which was originally built to help businesses provide varying consumption models and make it faster, cheaper, and easier to deploy applications. But, as we have learned, what helps businesses work faster and cheaper also helps cybercriminals.

Changes in technology



Another way technology has helped propel cybercrime is in the collection of funds. Cryptocurrency is a type of digital money that utilizes a decentralized peer-to-peer payment network.[8] The nature of cryptocurrency — decentralized, anonymous — makes it difficult to discover criminal activity.[9] These forms of payment are most often used for legitimate transactions, but also allow cybercriminals to anonymously collect funds as they engage in illegal activity. Bitcoin has been used globally while Webmoney remains utilized in Russia and Eastern Europe.[10]

Early stages of attack

There are various methods of attack. Different styles are employed in the hopes of making victims susceptible to cybercrime. Let's explore a few.

Spam/phishing:

Spam/phishing incorporates an email as part of the cybercrime chain. The goal in this maneuver is to get the end user to click on the link or open an attachment. This method has been around for a while, but a few key aspects have changed.

These emails are starting to look very professional and leverage logos of vendors and other small businesses. Elements of interest are utilized, such as resumes, to encourage recipients to click. Through some social engineering, an email and resume can be crafted that targets the recipient – highlighting commonalities such as the same alma mater and participation in similar organizations. If a cybercriminal does not want to exert the effort to craft their own spam/phishing, they can utilize mass mailer services to execute the cybercrime.

Malvertising:

Malvertising is malicious advertising. An ad is run and it either redirects users to a malicious site or is a dynamic ad that runs javascript code once the ad is loaded. These ads are also looking more and more professional, are located on legitimate websites, and in many instances are copies of real ads. A user goes to a legitimate website and sees a legitimate looking ad – it is not hard to imagine the number of users that end up becoming victims.

These ads are also looking more and more professional, are located on legitimate websites, and in many instances are copies of real ads.

Tools of attack

Exploit kit:

Exploit kits are software kits that are designed to identify software vulnerabilities on computers connecting to a web server, and then run malicious code designed to exploit vulnerabilities on those computers. Exploit kits are plug and play modules that cybercriminals can buy or subscribe to. Subscription is often a preferred choice since these continue to be on the pricey side. One of the biggest values of an exploit kit is the ease of use; non-technical cybercriminals can leverage the exploit kit to engage in cybercrime. By simply copying and pasting a snippet into a website, one can begin their cybercrime. The code will try different sorts of tactics to break through the browser, such as drive by download, web clicks, and email. These kits have business analytic dashboards in order to monitor and improve efficacy rates. There is a breakdown in terms of which exploits are working and in-app purchases are available to increase effectiveness.

Droppers:

Droppers are another attack tool that is gaining popularity. Droppers are malware that establish a foothold in a system. Once installed, the dropper phones home to the server and notifies the cybercriminal that it has been installed on the user's computer while asking for directions on what to install next. The cybercriminal can either install their own malware or sell infection rights to the user's machine.

Droppers enable high efficacy because they provide critical information back to the cybercriminal prior to final infection. The droppers deliver details on the computers infected, including language, country, whether it is a server or desktop, network performance, and the type of antivirus that is being run. This provides the necessary details to choose a more impactful, effective, and profitable piece of malware for each computer.

Antivirus: The protection that doesn't fully protect

A question that often comes up is "why isn't my antivirus protecting me?" The answer is that your antivirus is protecting you against some threats. It helps block certain threats and protects against commoditized malware. An antivirus looks for either a signature or heuristic and tries to understand elements such as where data is stored and how memory is used. The antivirus then maintains the malicious signatures that should be blocked. It is an important element of an overall security solution, but it is only a piece. If a malware is tweaked (which it often is), then the antivirus will not recognize the signature. In today's threat landscape, an antivirus is not enough. With attackers using a number of methods to attack, organizations need to utilize a layered approach to protect.

You need to have your antivirus. But, you also need other layers of protection as well.

How to become more secure

Deploying a tool to protect before connections to malicious destinations are even established is a key component of any security solution. By stopping threats from hitting the network and endpoints, the number of security alerts is reduced since there are fewer attacks that hit the infrastructure. Reducing the volume of alerts is key to alleviating the pressure for MSPs that often deal with a significant number of alerts. Most customers have not thought about protecting at the DNS layer, but there is a significant benefit to deploying protection at a level that is used by every device on the network.

Cisco Umbrella for MSPs is a core layer of an overall security solution. As discussed, the continuously evolving threat landscape makes it imperative to have layers of defense to protect your employees and customers from cybercrime.

Cisco Umbrella for MSPs works the way the internet works, offering a consistent layer of security through recursive DNS. It protects before a connection is even made. Simply point all DNS traffic to Umbrella for consistent domain-level visibility. Cisco Umbrella for MSPs provides:

First line of defense against threats. Umbrella is built into the foundation of the internet and blocks requests to malicious and unwanted destinations before a connection is even established – without adding any latency.

Visibility and protection everywhere. With Umbrella you have the visibility needed to protect internet access across all devices on your customer's network, all office locations, and roaming users. You can secure your customers' networks and endpoints, providing malware and phishing protection.

MSP-wide deployment in minutes. Umbrella is easy to deploy in just minutes, enabling you to provide fast security for your customers.

Centralized settings and reporting. The centralized settings and reporting features in Umbrella for MSPs were built with MSPs in mind. It provides a simple and powerful way for you to create and manage settings as well as reporting that are shared among multiple customers and can be automatically applied from day one.

Umbrella for MSPs also comes with the Partner Enablement Pack. As discussed in this whitepaper, one of the best ways to protect is with knowledge. The Partner Enablement Pack is a collection of assets that helps MSPs educate their customers on the overall threat landscape and threats specific to SMBs.

Key benefits of Cisco Umbrella for MSPs:

- A key layer of defense, the first line of defense
- It's easy to use without any need for specialized training
- Save time with standardization and automation
- Manage your customers with complete control and flexibility

The compelling economics of cybercrime make it clear that cybercrime is here to stay. Staying up to date on the evolving business model and utilizing a layered approach to protection is one of the best ways to stay protected in this environment.

(1) https://business.kaspersky.com/cybercrime-inc-how-profitable-is-the-business/2930/
(2) http://www.vocativ.com/311187/dark-net-credit-card/
(3) http://www.infoworld.com/article/3043197/security/4-reasons-not-to-pay-up-in-a-ransomware-attack.html
(4) http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
(5) http://www.infosecurity-magazine.com/news-features/techniques-of-cybercriminal/
(6) http://www.pcworld.com/article/2109210/report-average-of-82-000-new-malware-threats-per-day-in-2013.html
(7) https://blog.knowbe4.com/a-short-history-evolution-of-ransomware
(8) https://bitcoin.org/en/faq#what-is-bitcoin
(9) http://www.makeuseof.com/tag/cybercrime-goes-offline-role-bitcoins-ransom-extortion/
(10) http://krebsonsecurity.com/tag/webmoney/