Deloitte.

Threat Intelligence and Analytics

Black-market ecosystem

Estimating the cost of “Pwnership”

Issue date: December 2018 | TLP: WHITE

Executive summary

Cyber-criminal black markets are a constantly evolving ecosystem that reflect broader trends and behaviors. However, they present difficulties to researchers when they attempt to study these dark and deep web businesses at the macro-economic level. Because of this, most studies take a micro-economic perspective and follow one of two similar approaches. The most common approach is to estimate the profit an actor can make for a specific criminal activity, such as ransomware. This approach requires several assumptions based on scale and is limited to a specific service or product. Similarly, security researchers have attempted to focus on the cost of individual products or services such as Distributed Denial of Service (DDoS). These approaches can only answer, with varying degrees of accuracy, the questions “How much can a cyber- criminal make?” or “How much does a tool or service cost?” These approaches fail to address the broader implications of a good or service, the actual role they serve, and the relationships a tool or service has within the cyber-criminal economy.

Deloitte Threat Intelligence and Analytics (TIA) seeks to understand the financial relationships as part of a broader criminal business. We believe that interesting observations can be drawn by looking at these cyber-criminals from the perspective of business operations. In comparison, we begin by seeking answers to “What are the most commonly used tools and services sold on underground markets?” and “What are the average estimated cost of these tools and services?” From here we can ask critical questions including “Which tools are required to operate real world criminal businesses?” and “What are the estimated operating costs of various cyber-criminal businesses?” We can then review and compare these criminal businesses to help identify which are the most affordable—both from a cost of entry and routine operations standpoint.

We began our research by looking at the most common services, enablers, and tools independently. This allowed us to gauge the average estimated cost in each of these categories. Next, we determined how these services and tools are related to one another by identifying which are necessary to perform several of the more common malicious activities.

Our investigation led us to several conclusions. To begin, the underground economy is a diverse but interrelated ecosystem where nearly every criminal business incorporates multiple related, but discrete tools and services. Such an ecosystem essentially forces threat actors to participate as both producers and consumers within the black market. Even the most basic criminal business requires several different tools or services—and all are readily purchased on the black market. Next, we observed that threat actors generally use two business models. In the first, actors offer a low cost but broadly used tool or service at a large scale. Conversely, a threat actor can pursue a more specialized service that is offered at high cost to comparatively few customers. Finally, we determined that the operational costs of an efficient criminal business can vary widely based on the skill and resource requirements which underlie the good or service. We estimate that some common criminal businesses can be operated for as little as $34 month while others may routinely require nearly $3,800 or more.

Introduction & methodology

The nature of the underground economy means that this could not be a purely empirical exercise. As such, the scope of this research will be narrowed to the most common and popular tools, services, and enablers. These can be defined as the tools, services, and enablers required to perform the majority of commonly observed malicious cyber activity. Due to the limited scope of this study, the collection of a statistically significant sample of credible information is simply not feasible. However, we have attempted to increase the accuracy of our research methodology by incorporating both qualitative and quantitative elements. We first selected the most common tools and services and identified numerous relevant examples for each. All of the pricing values are based on data observed from January 2017 or later.

However, a concerted effort was made to ensure that in the majority of cases the pricing is derived from activity observed between August and February 2018.
Sample criminal goods and services were then narrowed based on an assessment of overall popularity, a credible reputation, and the presence of a clearly defined pricing structure. For each product or service line, Deloitte TIA attempted to make a standardized estimate for the average cost so that comparison could be drawn between similar services. For the majority of these services, malware, and tools, we have attempted to estimate the cost of each on a monthly basis. Some of these, particularly source code for tools and malware, can only be bought outright. In these cases, the estimated cost is distributed over the course of a year.

Finally, we estimated the costs of these related tools and services in combination with one another. This enabled Deloitte TIA to explore these in the context of criminal businesses that have fairly standard requirements in terms of necessary services and tools. This enabled us to estimate the routine costs of monthly operations and thus, identify which one may likely require the most financial resources to operate.

Services & enablers

Bulletproof hosts

Bulletproof hosts (BPH) are a key enabler of cyber- criminal activity which provide the network infrastructure necessary to perform malicious activities. This includes all the most common attacks including: spam, scanning, brute-forcing, fraudulent/phishing pages, DDoS, and all forms of malware such as Trojans, crypto-miners, and ransomware. BPH services function in a similar manner to legitimate web hosts— more sophisticated services even model themselves after Content Delivery Networks (CDN)—but do not actively monitor clients and deliberately ignore abuse/takedown requests in response to illegal activities. BPH operators are a critical component of the cyber-criminal ecosystem and enable nearly every type of threat actor,novice, and expert. As such, the disruption of a BPH service has significant implications as a multitude of threat actors see their criminal businesses abruptly end when a BPH service shuts down.

The threat actor(s) involved in BPH often use knowledge gained while operating a quasi-legitimate hosting company to facilitate more profitable criminal businesses. Occasionally, this is reflected by the threat actors who place their BPH infrastructure on the same IP address range as their previous "legitimate" service offerings. Initially, BPH services offered web hosting located in countries with lenient policies on hosting or distribution of malicious content. However, BPH providers have evolved considerably to offer amenities such as "clean" IP addresses, Secure Sockets Layer (SSL) certificates, and domain registration. Most of these services are basic Virtual Private Server (VPS) and Virtual Dedicated Server (VDS) resellers who obtain servers in a variety of hosting locations. These range from as little as $8 to $130 per month based on server configuration. Similarly, dedicated server options are available at a premium ranging from $200 to $800 again based on configuration.

Many of the most popular BPH services offer dedicated "fast-flux" capabilities where nameservers and proxy front-end exit nodes are rapidly changed. These setups are extraordinarily resilient and may include load balancers and proxies as well. If either a nameserver or front-end is blocked or taken offline, a new one is automatically created in its place, allowing the back-end server hosting the criminal customers' content to remain online. Due to the additional resources and expertise, fast-flux capabilities are considerably more expensive. As such, they are generally used when cyber-criminals are involved in the most malicious activities such as malware distribution, command and control (C2) nodes, or illegal forums and markets. Depending on the number of domains and the type of fast-flux, this can cost between $70 to $500 per month.

BPH service	BPH A	BPH B	BPH C	BPH D	BPH E	BPH F
Virtual servers	VPS—$10/mo.	VPS—$15/mo.	VDS—$8–$125/mo.	$70–500/mo. dollars for between 1 and an "unlimited" number of domains	$350/mo. per double fast- flux domain	VDS—$75–$130/mo.
Average monthly	$10	$15	$61	N/A	N/A	$101
Dedicated servers	$200–$800/mo.	N/A	$150–300/mo.	$267	$350	$300–$430/mo.
Average monthly cost (est.)	$400	N/A	$200	$267	$350	$356

SOCKS proxy

SOCKS proxies are used to anonymize communications and mask the individuals behind a variety of criminal behaviors. By routing malicious traffic through a compromised host—via a victim machine that serves as a SOCKS server—threat actors can obfuscate the true origin of the activity. These services are commonly sold or rented on threat actor forums. One of the most common uses of SOCKS proxy services is to mask brute-forcing, scanning, or account checking activities by distributing the threat actors traffic across hundreds or thousands of compromised host IP addresses. In the case of account checking, SOCKS proxies can be tailored to imitate the specific geographies of the organizations—most commonly financial institutions—where the accounts originated. This can further reduce the likelihood that a threat actor's effort will be identified.

The cost of SOCKS proxy varies based on its reputation, actual location, and the amount of proxies purchased by the actor. Discounts are offered for bulk purchases and individual proxies can be found for well under $0.10. However, there is considerable disparity based on the provider. Deloitte TIA estimates that the cost of monthly access to 1000 SOCKS proxy addresses ranges from as little as $38 to $750. We assess with moderate confidence that this large discrepancy is based on the composition of available SOCKS proxies. For example, actor PROXY D may demand a premium for its proxy services because it is based on a mobile device botnet that is more resilient or reliable than other services based on desktop access.

Proxy service	PROXY A	PROXY B	PROXY C	PROXY D	PROXY E
Pricing	$3 for 60 proxies $5 for 120 proxies $10 for 300 proxies $20 for 720 proxies	$249/3000 proxies/mo. $74 for 150 proxies/mo.	$0.30—per proxy for 24 hours $0.90—per proxy (permanent) $0.15 surcharge for proxies (added in last 24 hours)	120 proxies for $100/mo. 1200 proxies $300/mo. 3500 proxies $700/mo. 6000 proxies $1000/mo.	WorldMIX—5,000 proxies EU, US. Asia, L. America $50/wk. US—4500 IP $ 110/wk GB—1,000 IP $180/wk IT—3,000 IP $180/wk RU—3,500 IP $50/wk
Average monthly cost (est.)	$27	$288	$375	$360	$230

*note - monthly costs for proxies estimated based on average service price per 1k proxies

Virtual Private Networks (VPN)

VPNs are ubiquitous on the criminal underground and are essential services for maintaining anonymity and security. A VPN allows a remote user to access the internet from a different host. By routing traffic through an intermediary, in this case a VPN server, the actual IP address associated with a criminal is effectively masked. In addition to increased anonymity, VPN protocols also support strong encryption algorithms which ensures that traffic—even successfully captured — is indecipherable.

When threat actors interact with criminal infrastructure or perform any criminally related activity such as accessing forums, they will likely most often use a VPN or a series of VPNs to disassociate themselves from any incriminating activity. As such, all reputable underground VPN providers claim that no logs are stored while providing numerous global traffic exit points - including TOR nodes.

The necessity of VPN use in cyber-criminal activity means they are some of the more affordable tools ranging from under $10 to around $60 for most services. Several providers also chain together multiple VPN servers into "double," "triple," or "quadruple" VPNs— however, the additional anonymity or security provided by such configurations is debatable. This additional service can also raise the cost of monthly VPN service from $29 to $60. BPH providers also offer preconfigured VPN servers. These are some of the more affordable options at around $10 a month. It is important to note that, based on our observations of forum activity, many commercial providers including NordVPN, Private Tunnel, and IPVanish are also popular among criminals, particularly among entry level cyber-criminals.

VPN service	VPN A	VPN B	VPN C	VPN C	VPN E
Pricing	Light Single VPN $2/day $20/mo. $154/yr. Extra Double VPN $3/day $40/mo. Quad VPN $4/day $60/mo.	$10/mo. Any country	Vpnlab[.]net Single VPN 3.99/3 days 19.90/mo. 69.90/yr. Double VPN 7.99/3 days 29.90/mo. 129.00/yr.	DoubleVPN[.]com Single VPN $25/mo. Double VPN $36/mo. Triple $42/mo.	$9.5/mo.
Average monthly cost (est.)	$40	$10	$25	$34	$9.5

Traffic Direction Services (TDS)

TDS vendors support click fraud and also serve as a distribution channel for malware. Underground TDS vendors purchase advertising space from legitimate ad networks. When a user clicks the advertisement, traffic is re-routed to a destination pre-determined by the criminal customer. TDS services are closely aligned with exploit kit (EK) activity as they can easily funnel the traffic to the malicious landing pages to deliver a payload. Deloitte TIA has observed an apparent downturn in the popularity of TDS vendors over the last two years, which in turn closely correlates to the decreasing popularity of EK activity. However, it is unclear whether the lack of quality TDS options impacted EK market negatively or TDS vendors simply moved on as EK popularity declined and their efforts were no longer as profitable.

While not the dominant market force they once were, TDS vendors remain relevant to the black-market ecosystem. Pricing for TDS services is based on several business models with an estimated monthly cost of between $100 and $583 per month. The most common of these is a “pay-per-load” model, as demonstrated by TDS A, where costs are derived from a set number of malware loads based on the number of times a TDS redirects traffic. These can be further refined based on geography to infect users from specific countries or regions. This capability is reflected in pricing models as traffic from certain geographies is considerably easier to obtain. Another model is the licensed service where a TDS developer grants criminals access to their TDS software or sells the source code outright. Finally, there is the pay-per-target model which charges based on the number of redirects regardless of whether they result in successful loads.

Service	TDS A	TDS B	TDS C	TDS D
Pricing	Per 1k loads varies from $10 Turkey $10 Thailand $150 UK $200 France $300 USA $350 Canada	License $300 Source code 1 BTC (~$7000 USD)	$6/1 day $45/10 days $105/mo. $240/3 mos.	$10/per thousand targets
Average monthly cost	$170	$304	$105	$100

*note - monthly costs for TDS B distributed over 12-month period and TDS D based on 10% hit rate.

Account checkers

An account checker is a custom-built software program or web-based service that automates the checking of customer account credentials from financial institutions, online payment services, online retail stores, customer rewards programs, cryptocurrency wallets, cloud-based storage, device management portals, and various other account types.

Account checkers are commonly developed in-house or rented out by threat actors that manage and sell compromised account credentials. The most affordable option is the purchase of configurations ($10-15) for the easily acquired Sentry MBA account checking tool. Threat actors that manage their own online markets of compromised account credentials often utilize custom-built account checkers to replenish inventory. It is also common for vendors on dark web markets to rent account checkers from other threat actors offering the tool as a service. Deloitte TIA analysts have observed multiple threat actors selling GUI account-checking tools as a service on Russian-language dark web forums.

They are available for individual purchase for between $25 and $100 depending on the targeted organization. However, an industrious threat actor would need to build an arsenal of these types of account checkers to ensure they can cycle through dumps as availability fluctuates from various sources. Conversely, they could use a web-based service like HDC3CK which charges based on the number of valid accounts identified.

These tools are used in "credential stuffing" attacks where account-checking tools often leverage credentials leaked in past breaches. A stuffing attack is possible because the account checker attack exploits user password reuse. Credential reuse drastically increases the probability of a user being compromised in account checking attacks. Account checker scripts iterate through a list of proxies and leverage proxy/VPN services to host the account checker to evade network blacklists. In addition, account checker scripts often randomize the User-Agent string to further obfuscate the scripts from valid web traffic.

Service	Actor A	Actor B	Actor C	Actor D	Actor E
Pricing	$60 for several US banks	$50 for multiple US and EU-based financial institutions	Price: $50–$70 for multiple US and EU technology firms and financial institutions	Web based checking tool: 100 credits = $1.75 Sentry MBA configuration $10–$15	Rental $25–$35/wk. $100/mo.
Average monthly cost (est.)	$60	$50	$60	$53	$100

*note-monthly costs for HDCH3CK based on cost of 1000 valid accounts retried at 3 credits each.

File encryption/"Crypting" services

Crypter services serve a critical role in the cyber-criminal ecosystem by enabling threat actors to reuse malware without time consuming alterations to the malware's original code. Malware authors submit their software to crypting vendors, which then run custom encryption to obfuscate the underlying code. This invalidates any previous signatures associated with the malware developed by anti-virus vendors, making the malware "fully undetectable" or "FUD."

These services are a necessity for any malware-based business and many options are available. They typically range from as little as $12 a month to $100 for a "lifetime" license (unlimited license is often called lifetime by threat actors). Generally, there are no restrictions on the number of crypted payloads that can be created and the vast majority of these crypting services focus on WIN32 Portable Executables. However, specialized services such as CryptoShell cater to the burgeoning mobile malware market by offering mobile program crypting. This niche market allows Actor D to charge a premium—it can run up to $900 per month—while also limiting the number of packages which can be generated.

Service	Actor A	Actor B	Actor C	Actor D	Actor E	Actor F
Pricing	$15/mo. $35/3 mos. $60/6 mos. $75/lifetime	Price 1 mo.–$12 3 mos.—$25 Lifetime—$75	1) Bronze 30 days $13 2) Silver 90 days $25 3) Gold 180 days $35	Android Package Kit (APK) 5 crypted APK—$50 Rental options $280/mo. for 5 pkgs./day $900/mo. for 50 pkgs./day	$35–45 days $60–90 days $110.50–180 days $250–Lifetime	$30/1 mo. $45/3 mos. $70/6 mos. $100/lifetime
Average monthly cost (est.)	$15	$12	$13	$100	$24	$30

Malware loads or Pay-Per-Install (PPI) services

Malware "loads" services specialize in large-scale malware distribution and support. Deloitte TIA assesses that many of the malware campaigns we observe are facilitated by these distribution channels. In this model, the "affiliate" distributor will typically partner with a malware developer or license holder who does not have the resources to disseminate a payload at scale. These loads service operators are compensated based on the number of malware installs they can provide. Because of this, they are also known referred to as "Pay-per-install" (PPI) services by security researchers. Under the most common pricing model, a distributor receives a set value per-1k installs. It is worth noting that affiliates can also be paid on commission or negotiate a portion of profits under a revenue sharing model as well. The cost of a load service varies based on the geographic location of the desired victims. This appears to range between $70 and $400. North America and Western Europe and are the most expensive loads as they are also the most lucrative. Compared to standalone spam or a TDS service, which also distribute malware, a malware loads service operator has a considerably broader focus and a variety of tools at their disposal. In addition to spam or malvertising, a malware loads service may simultaneously engage in seeding file-sharing networks with tainted programs, placing payloads on legitimate websites as part of watering hole attacks, or conducting brute-force attacks to install malware on compromised machines. Similarly, they may engage in massive scanning operations to exploit vulnerabilities, which would allow them to remotely load the malware on a victim. As the profit is dictated by the number of installs, the operators of these services are incentivized to construct massive botnets that facilitate secondary and even tertiary infections by retrieving multiple payloads.

Service	Actor A	Actor B	Actor C	Actor D	Actor E
Pricing	World mix—$60 1k USA—$400 1k EU mix—$ 250 1k Germany—$350 1k UK—$300 1k CA—$300 1k RU—$150 1k UA—$70 1k AU—$350 1k MX—$200 1k NE—$300 1k IT—$250 k BR—$ 80 1k FR—$250 1k	Installs (Price for 1,000) World mix—$90 Loads (Price for 1k) World mix—$100 Mix EU—$250 Mix Asia—$150 All other country (USA/CAN/FR/DE/CN/KR, etc.) contact for details Discount starts @ +5,000 loads	$85/1k loads World mix	$90/1k installs World mix	$70 per 1k mixed installs $70 per 1k US installs
Average cost per month (est.)	$236	$148	$85	$90	$70

*note - monthly costs based on estimate for average of services charges of 1k installs

Distributed Denial-of-Service (DDoS) attack services

There is a thriving ecosystem for DDoS attack services which primarily support harassment and hacktivism. Many of these sites cater to users who want to perform revenge attacks due to perceived wrongs. DDoS attack services are commonly affiliated with the online gaming community and lower level cyber-criminal forums. Lower skill and predominantly younger actors regularly harass one another because it is relatively simple to obtain identifying information on real-life targets (such as name and IP) for DDoS attack. However, the tools are target agnostic and Deloitte TIA assesses with high confidence that the DDoS services and recon tools which facilitate such attacks, are regularly used to target organizations across multiple industry sectors and regions.

DDoS attack services allow relatively unsophisticated threat actors to quickly gain access to capable tools at a low cost. The price of these services is dependent on the type of DDoS attack, the velocity of the attack, and the duration. For most of these services, the price averages between $36 to $62 per hour. It is worth noting that more skilled actors may use DDoS activity to distract network security personnel during complex, multi-phase attack scenarios. In these instances, a DDoS attack draws the attention of an organization and overwhelms its logging capabilities while the actual attack—such as a system vulnerability exploit—is used to gain persistence on a network.

Service	Actor A	Actor B	Actor C	Actor D
Pricing	$10/hr.—regular website $25/hr.—protected website $150/hr.—govt/military/bank website	360 seconds $10 600 seconds $15 900 seconds $20 1200 seconds $25 VIP 1 1200 second long attack — $30 VIP MAX 1600 seconds $40 Ultra 1 3600 seconds $60 Maxed 7200 seconds $120	15-20 Gbps per attack SILVER—$15/mo. 1200 seconds boot time NOVA—$30/mo. 2700 seconds boot time MASTER—$50/mo. 3600 seconds boot time	30 GBP attack Trial account ($2 USD) 130 seconds $5/800 seconds $15/1500 seconds $25/2500 seconds
Average cost per hour (est.)	$62	$60	$50	$36

Spamming services

Spam email is the primary vector or distribution method used by threat actors to spread all forms of malware from Trojans to ransomware. Threat actors have several options for email-based distribution. The simplest option is the use of SMTP servers which could be purchased on the black market for $8 to $10. These servers—which may be hijacked or a pre-configured VPS—can then be scripted to disseminate large volumes of spam. However, this will likely result in the blacklisting of the server in relatively short period of time.

To compensate for this, more specialized spam services offer to distribute messages and attachments based on volume. For example, Actor A will distribute a million emails for an average of $14 based on geography. There are also sophisticated and notorious spam services, such as Necurs or Send-Safe, which reflect a botnet infrastructure that uses compromised machines as mail servers. This allows spam botnets to perform multiple, often concurrent, spam campaigns that deliver several different malware payloads to millions of emails in various regions throughout the globe. While the cost of the previously mentioned services is not known, the Actor D service is likely relevant for cost comparison purposes. Actor D, which costs an estimated $1200 per month, is purportedly botnet-based and is more expensive than other observed spam distribution channels.

Service	Actor A	Actor B	Actor C	Actor D	Actor E
Pricing	$200/20 million US only $150/25 million—DE, FR, IT, UK and US $75/5 million—RU	SMTP servers $8-10	Sends html page emails Sends attachments Sends spoofed email address from any address Email lists provided $25	Standard: 100 bots $1000/mo. Pro Package: 500 bots $1400/mo. Additional bots: 100—$330 500—$750 1000—$1000	Price: • minimum order $40 for 50k sent • $70 per 100k • more than 100k is considered individually
Average monthly cost	$14	$9	$25	$1200	$500

*note - monthly costs for Actor A based on per million emails

Compromised servers/"Dedic" marketplaces

Hacked servers or "dedic" services offer access to an inventory of compromised victim machines. These criminal businesses are primarily focused on selling remote access via Remote Desktop (RDP), Secure Shell (SSH), or Virtual Network Computing (VNC) protocols. "Dedics" such as Actor A and Actor D are often sold on the same markets where carding "dumps," account credentials, and Personal Identifiable Information (PII) are traded. Compromised servers are affordable and can be obtained for just over $1. However, the cost can easily increase to upwards of $60 based on the victim machines organization, configuration, data types, location, and other factors.

The potential malicious uses for compromised "dedic" servers vary and are limited only by the imagination and capabilities of the attacker. Actors can exfiltrate data (Point of Sale (POS), PII, Protected Health Information (PHI) etc., implant Trojans or ransomware, or use the compromised server as a staging point to launch further attacks. This means individuals and organizations are not only potential victims of data theft, but potential enablers of future attacks. The primary drawback of these "dedics" is the duration for which remote access can be expected. They are typically obtained via brute-forcing, exploits, or stolen credentials. As such,there is considerable variation in the access periods and the attacker may have remote control of system that can vary from a few hours to several weeks or longer. Without additional persistence mechanisms, access to the victim machine will be lost immediately after the admin changes the password or the compromised system is updated.

Service	Actor A	Actor B	Actor C	Actor D
Pricing	RDP $5-35 SSH $3.40-60 Web Shell $10-12	SSH tunnels <50 $4 each 50+ $3each	SSH tunnel $1.55 each RDP $4-6.00 each	RDP servers and SSH tunnels $3.15-$8.30 based on location and server config
Average cost per machine	$26	$3.50	$4	$6

Personally Identifiable Information (PII) & Protected Health Information (PHI)

The sale of sensitive personal information, including PII and PHI, has been a mainstay of cyber-criminals for several decades. While such records can enable several different malicious activities, they are most often leveraged in support of fraudulent purchases and identity theft. Actors will most often take the information in these records and use them to gain access to financial accounts or establish new accounts under the assumed identity of a victim.

"Fullz" is slang term commonly used on underground forums for a full set of personally identifying information (full name, date of birth, Social Security number, address, etc.) that is used for identity theft and other insuring fraudulent purposes. Fullz typically range from $10 to $50 depending on the location and the type of financial information contained within the record. The value of PII or PHI database records is typically reflected by the amount of detail each contains and the relative "freshness" of the data. The basic PII, such as name and credit card information, is sold in bulk and for $0.10 or less, older "stale" data may be freely given or traded when its value has diminished considerably.

In general, PHI data is more detailed and thus more costly than basic PII at $5 per record. The rich pool of data found in insurance and healthcare records is exceptionally valuable for a threat actor seeking to commit identity theft. This is because PHI records contain data Social Security Number (SSN), Date of Birth (DOB), address, email, phone, dependent family members, etc.) which is less perishable and can be reused to create multiple fraudulent accounts over time. The trafficking of stolen healthcare data is a trend that is likely to be exacerbated by the continued transition from paper records to electronic health records (EHR).

Similarly, some PII records—particularly those related to taxes or loan and job applications—are remarkably detailed as well. They may include very specific information including the victim's driver's license information, all financial holdings and institutions, household income data, and credit score. Such records can potentially allow threat actors to perform identity theft and fraud for years and thus demand $50 to $150 per record.

Actor	Actor A	Actor B	Actor C	Actor D	Actor E
Pricing	Database of Americans with a credit score of 700 and above. Data: SSNs, DOB, marital status, dependents; 1040, 1120S tax forms up to 2015; credit statements, driver's license, passports, affidavits which can substitute a for background report. US $50 to US $150 per profile	PII of US citizens intended to bypass credit background check questions Data: Name, SSN, DOB, driver's license, military service, loan amount, residence type, address phone, contact time, email, ip_addr, pay frequency, net income, employment status, employer name, job title, bank names, account type, direct deposit, routing_no, references $50	Selling PII of US nationals accompanied by selfie photos 1,000 records for $200 USD 500 records for $100 USA kit—$70 USD	Database of Healthcare records	Scanned copies of documents from orthopedic clinic $0.12 per scan
Average cost per record	$75	$50	$70	$5	$0.12

Malware and tools

Phishing kits

Phishing kits are fraudulent “scam” pages that harvest credentials and other sensitive personal information by imitating a legitimate service, vendor, program, or organization. Unsuspecting users input valuable data into pre-determined fields which is then captured and retrieved by threat actors. Phishing kits vary considerably in price based on the sophistication of the page. Low cost but designed phishing kits often fail to render properly on different browsers and or may not even target a specific organization. In comparison, others are purpose built and may even target specific users. A high-quality phishing kit imitates very specific pages and behaviors similar to web injects for banking Trojans. This may include capabilities such as input validation, credit card recognition based on BIN, CAPTCHA, and two-factor authentication.

These variations in sophistication are reflected in the disparate prices observed by Deloitte TIA. A basic phishing kit for a commonly targeted financial institution or email provider can be obtained for as little as $10. In comparison, a custom build that incorporates special credit card related features may sell for up to $350.

Actor	Actor A	Actor B	Actor C	Actor D	Actor E
Pricing	Payment system or bank themed US $300	US banks or other financial institutions Price: $10	Payment themed phish kit Email/pass, address, CC, CVV, payment card photo $200	UK/US/CA Banks US/UK/CA/ AU Fullz: Retail and Technology themed public pages $125 VBV/ID upload option available $250 custom/private pages $350	US Banks $30 Bank of America Chase Bank Wells Fargo USAA Bank CIBC Canadian Bank Santander Bank UK Barclays Bank UK HSBC Bank UK Other scam pages are also available for social media and retail sites
Average cost per kit (est.)	$300	$10	$200	$242	$30

Loaders & “maldocs”

A downloader is a small program designed to retrieve, install, or drop another malware (ransomware, RAT, etc.) on a target system. Downloaders are a critical component of the malware infection chain as well as the malware distribution ecosystem. They range from simplistic email attachments that immediately retrieve other payloads, to modular malware that is capable of keylogging, credential theft, and other activities. While downloaders are used indiscriminately in spam campaigns, they are often employed during highly targeted spear-phishing attacks as well. For example, advanced state-sponsored groups and cyber criminals have both used macro-enabled Excel spreadsheets as downloaders in notorious campaigns.

These types of malicious document or “maldoc” attacks, previously reserved for spear-phishing activities and sophisticated actors, have become ubiquitous as downloaders with these capabilities are increasingly affordable and available. Deloitte TIA has observed a sharp reduction in the cost of maldoc downloaders over the last year. Previously niche capabilities, such as Actor F, demanded between $3 to $4,000. Maldocs are now abundant and versions with recently disclosed exploits—such as Actor’s D Silent Office exploit—can be purchased for as little as $100. More expensive options remain but include unique features. For example, Actor G allows a threat actor to generate customized macros with randomized junk code and string values for $500 a month.

Actor	Dodoaska Genryu Loader	Heisenberg	Quant Loader	Elm0d's Silent Office Exploit	Microsoft Word Penetration Tool	Microsoft Word Intruder	Rubella Office Crafter
Pricing	Loader Build $2,000 Rebuilds free	Macros source code with built-in EXE file $5,000	175-275 per build Rebuild $17.50	$100 -$200 per build depending on program (Word, Excel, PPT)	$200/wk. subscription model includes updates to macro builds and web panel	Builder $4,000 Stripped-down $3,000	$500/mo. (including 10 rebuilds)
Average monthly cost (est.)	$166	$416	$260	$150	$800	$292	$500

*note-monthly costs for Genryu and Quant loader based on build and 2x monthly rebuild distributed over 12-month period

Remote Access Trojans (RAT)

A Remote Access Trojan often referred to as a "backdoor," is a malicious program which is used to observe or control victim machine. The ability to identify and retrieve sensitive data, when coupled with the potential for direct interaction by a threat actor on a compromised host, allows a threat actor using a RAT to remotely perform a multitude of malicious activities from data theft, manipulation, espionage, and sabotage.

RATs are pervasive and vary considerably in terms of their sophistication and capabilities. They are multi- featured and, in addition to remote access, often contain many of the capabilities that are seen in standalone downloaders or infostealers. RATs are often multi-platform and impact all operating systems. They range from custom tools used by nation-state actors, to commercial/ quasi-legitimate software offered for public sale. These affordable (often derivative) programs are sold by professional criminals on underground forums and are typically used to facilitate data theft and fraud. Many of the more common RATs, such as Nanocore, njRAT, and Adwind (aka JBifrost) have been cracked and variants of each are regularly distributed publicly. These often serve as the basis of the most affordable customized RATs— such as the RAT C, which is based on Safeloader, and available for only $100. More advanced security controls are increasingly adept at developing static and behavioral signatures for these older derivative malwares. As such, RATs with a custom VNC module like RAT D warrant an exponentially higher price of $1000. Additionally, many of these RATs are modular in nature and can include ransomware, DDoS, cryptomining, wiper, and other components.

Service	RAT A	RAT B	RAT C	RAT D	RAT E
Pricing	Builder for a selection of remote control programs for "any budget" Starts at $100 USD $1,500 lifetime license	• a software license (with free updates) for US $750 • changing IP addresses hardcoded into the build for free two first times; then US $25 each • hardcoding three or more IP addresses/ domain names for US $10 each address • creating a unique build for US $100 extra; rebind a build US $50 • code cleaning: US $100	Based on Safeloader Includes: 1. Admin panel. 2. Clean script. 3. An obfuscated script. (FUD) Price: $100	Includes admin panel $1,000 per build $150 per re-build	LITE Version All features w/o ROOT $80 PREMIUM All features w/ROOT $120
Average monthly cost	$75	$75	$8	$96	$8

*note - monthly costs based on lifetime license or initial build plus rebuild distributed over 12-month period

Banking Trojans

Banking Trojans are most commonly delivered via socially engineered spam though a small but significant portion is distributed via malvertising and exploit kit. Regardless of the infection vector, once a banking Trojan infects the victim's machine it connects to a C2 server to receive the instructions and configurations that allow it to perform man-in-the-middle browser manipulation through web injects. To accomplish this, the malware downloads additional plugins responsible for exfiltrating information from the machine such as file transfer protocol passwords, email addresses, and bank accounts.

The financial focus of banking Trojans means the data they retrieve can be quickly and easily monetized. However, developing of a banking Trojan also requires comparatively sophisticated threat actors as the institutions they target often leverage more advanced security controls. The authors of banking Trojans can charge a premium as they are some of the most expensive malware payloads on the underground. Deloitte TIA estimates that the most affordable banking Trojans are licensed for over $1000. Acquiring the source code is much more expensive at between $8 to $15,000. Even when estimates are adjusted to distribute the cost purchasing the source code over the period of a year, a banking Trojan will still likely demand from $140 to over $1333 a month depending on the developer or service.

The developers of the banking Trojan payload are not necessarily those responsible for the pages which are necessary to perform the browser-based attacks. Therefore, the banking Trojan ecosystem is supported by developers of customized web-injects which are designed to mirror the look and function of payment portals. While these are still offered as discrete services, throughout 2017 Deloitte TIA observed a shift where most major players in the banking Trojan arena package web-injects with their malware. An example of this is Actor A, an increasingly popular mobile-device based banker, which also illustrates the notable shift into the mobile arena such malware has undergone over the course of 2016 to 2017.

Service	Red Alert	XBOT	GozNym	Dellette	robert.gd	Demetra
Pricing	Android Trojan $200 USD weekly $600 USD month *includes web inject updates and BPH hosting	Private banking bot HVNC Malware + web-panel, US $1,500 per build $8,000 for a source [code] in C	Full Kit (Admin Panel + Build for unlimited number of domains) $1200 Rebuild $250 Custom functionality $250	"Private" banking Trojan test the bot for $50 USD per day. The price is $2K USD for the bot with VNC module	Empire (atmos-based Trojan) Builder: $10000 for a full set of features. Monthly fee: $500 technical support	4k monthly rental fee Source Code $15K Optional VNC module
Average monthly cost	$600	$666	$141	$166	$1,333	$1,250

*note - monthly costs based on lifetime license or initial build plus rebuild(s) distributed over 12-month period

Keyloggers & infostealers

Threat actors often use keyloggers to capture victim's keystrokes and credentials before exfiltrating the information to a remote server or via email. Infostealer malware often encompasses a wide range of tools used to exfiltrate sensitive information from the victim's machine, including passwords and credit card information stored in web browsers, system information, instant message history, and files. Many information stealers are inherently built with keylogging capabilities. Some of the objectives threat actors hope to accomplish when deploying infostealers and keyloggers include password collection that can be used for privilege escalation, lateral movement, or for use in later stages of an attack campaign. Additionally, threat actors can use these tools to log keystrokes, capture system screenshots, and target specific file types.

Keyloggers and infostealers are distributed broadly across lower-level and highly-vetted cyber-criminal forums. These tools can be leveraged in both targeted attacks by adept adversaries and broad opportunistic attacks. Keyloggers and information stealing malware can be used to accomplish multiple objectives in cybercrime and corporate espionage campaigns. Readily available infostealers (from criminal forums) can be purchased anywhere from $28 to $400 and provide a simple but effective mechanism for accomplishing this task on both a broad and narrow scale. Basic keyloggers can be purchased for $4-$10, which provides threat actors with an effective tool at a low-overhead cost.

Actor	Keyloggers			Infostealers		
	Acotr A	Acotr B	Acotr C	Acotr D	Acotr E	Acotr F
Pricing	Agent Tesla 1 mo. $10 3 mo. $25 6 mo. $35 1 yr. $45	Viotto Keylogger Viotto Keylogger private version: $40 License includes lifetime free program updates.	Compact Keylogger v2 1 mo. license $4.99 All updates Full PM and Skype support Lifetime license $9.99 All updates Full PM and Skype support	Formbook $28/wk. $59/mo. $99/3 mo. $250–$299/Pro	Azorult Price: $100 Rebuild: $30	Snatch license and the first build: $400 USD Re-build: (up to two domains): $20 USD New version update: $60 USD
Average monthly cost	$10	$3	$5	$59	$8	$33

Ransomware-as-a-service

Ransomware is a malicious code designed to prevent access on a compromised system until a financial demand is met. Over the last several years, Ransomware has rapidly grown in popularity while evolving to leverage public key infrastructure (PKI), autonomous offline encryption, and self-propagation. Ransomware's ability to block access to critical business operations data makes it an attractive and lucrative option for threat actors at all levels of sophistication. New ransomware variants continue to multiply at a prodigious rate. Deloitte TIA analysis has shown that the average ransomware license costs between $250 and $650.

In an effort to increase market share, ransomware developers have modified their software to offer complementary capabilities. This enables them to provide a malicious "suite" of services in conjunction with ransomware, known as Ransomware as a Service (RaaS). Threat actors are also experimenting with alternative distribution methods and business models while simplifying ransomware interfaces. The Shark, Atom, and Satan RaaS are all publicly accessible at no initial cost to a potential malware distributor who instead shares a portion the profits with the developer(s). This business model is referred to as "freemium" or "no-cost profit sharing" and has become a more common practice within the last year. Under this model, a threat actor can select the targeted file extensions/directories, set a ransom price, convert currency to a target country, and input a Bitcoin address for payment within a simple Graphical User Interface (GUI) that completely eliminates the need for any coding or command line skills. Other affiliate RaaS models, such as GandCrab, Spora, and Rapid require their affiliates to apply to their programs and adhere to strict terms and conditions after acceptance. These terms and requirements typically pertain to the affiliate's delivery methods, install rates, and regional targeting limitations.

As with any malware, the detection rates for ransomware correspond directly to the price a threat actor can demand for their product. For example, the Stampado ransomware quickly became detectable after going to market resulting in a steep reduction of price to only $39. However, the Stampado developers retooled and updated the ransomware. This modified version was then published as the Philadelphia ransomware which sold for a premium price of $389—nearly 10 times the cost of the previous, more detectable Stampado version. To expand the lifetime of a malware payload, the developers often ask their clients to refrain from uploading samples to VirusTotal and other automated detection engines, because these companies often distribute the files to each one of the AV companies that they are partnered with.

Model	Affiliate programs				Builds and source code		
Actor	**GandCrab**	**Spora**	**Shark Atom Satan**	**Rapid**	**Philadelphia**	**Trojans**	**InTheMood Cryptolocker**
Pricing	60/40 profit share. Major partners get an opportunity to increase their share up to 70 percent.	Fixed rate 70/30	Percentage of ransom (20-30%)	75/25 profit share	Lifetime license + free updates and full support! Introductory price: $389 Discounted price of US $320 Stampado Ransomware—Cheapest - only $39 lifetime license	Price: US $650 per copy	Price: $1,500 USD
Average license cost (est.)	N/A—Restricted Affiliate Program with profit sharing model	N/A—Restricted Affiliate Program with profit sharing model	N/A—Open Affiliate program with profit sharing model	N/A—Restricted Affiliate Program with profit sharing model	$21	$54	$125

*note - monthly costs for ransomware builds distributed over 12-month

"Zero-day" exploits

Zero-day exploits arise from the discovery of previously undisclosed software vulnerabilities. Such vulnerabilities are found by software vendors, users, security companies, security researchers, and occasionally, threat actors. If the exploit is first discovered by a threat actor, particularly nation states or cyber-criminals, the threat actor will often weaponize the zero-day vulnerability for a targeted attack. The unique ability to circumvent all publicly known security controls to access data makes a working zero-day exploit an incredibly valuable commodity.

The prices of zero-day exploits are often extremely difficult to uncover because of the tradecraft secrecy needed to keep the exploit private. Once a zero-day becomes publicly known, its market value is likely to drop drastically as affected parties scramble to develop patches for the vulnerable software, which would render the attack impractical or impossible. Exploit prices must also take into account how widely used the target software is and the level of difficulty for a successful attack. Notably, Adobe Reader exploits are often priced lowest and the highest price point is often for mobile devices.

Deloitte TIA regularly observes zero-day exploits advertised on criminal forums. However, we assess that many of these claims—perhaps half or more—are not actually credible. Actors who can reasonably be assumed to have discovered genuine zero-days typically avoid specifying a price publicly. Moreover, it is generally unclear when the exploit was sold, to whom, and for what value. The limited examples which are reputable would indicate that, at a minimum, a working zero-day exploit can cost several thousand dollars. However, the cost can easily be priced at hundreds of thousands of dollars depending on the potential number of victims, victim type, and expected lifetime of the exploit.

Actor	Actor A	Actor B	Actor C
Pricing	PDF zero-day vulnerability without sandbox escape to one buyer $300,000.	Zero-day exploits targeting Intuit QuickBooks, price: US $75,000 Oracle Sybase SQL Anywhere price: US $90,000	0-day vulnerability in CMS for e-commerce Starting bid: (US) $2,000 Increment: (US) $200 Take now: (US) $5,000
Estimated cost	$300,000	$82,500	$3,500

Brute-forcing

As noted above, dedicated services offering remote administration access such as RDP, SSH, or VNC are a key enabler for criminal activity. Additionally, multiple vendors were observed selling brute force tools for other services, such as SMTP and cPanels. Brute force compromise is the most popular technique used to obtain access to machines. These tools typically include features to conduct port scanning, check for running services, and carry out brute force attacks. After successfully compromising these services, threat actors may use the access to deploy malware or monetize their access by selling the access as a dedicated service.

Deloitte TIA found that these brute forcing tools could be obtained for as little as $50. They are also available on a licensed basis, which can include unlimited installs for distributed brute forcing attacks on a large scale. In comparison, these larger scale brute-forcing tools cost upwards of $500.

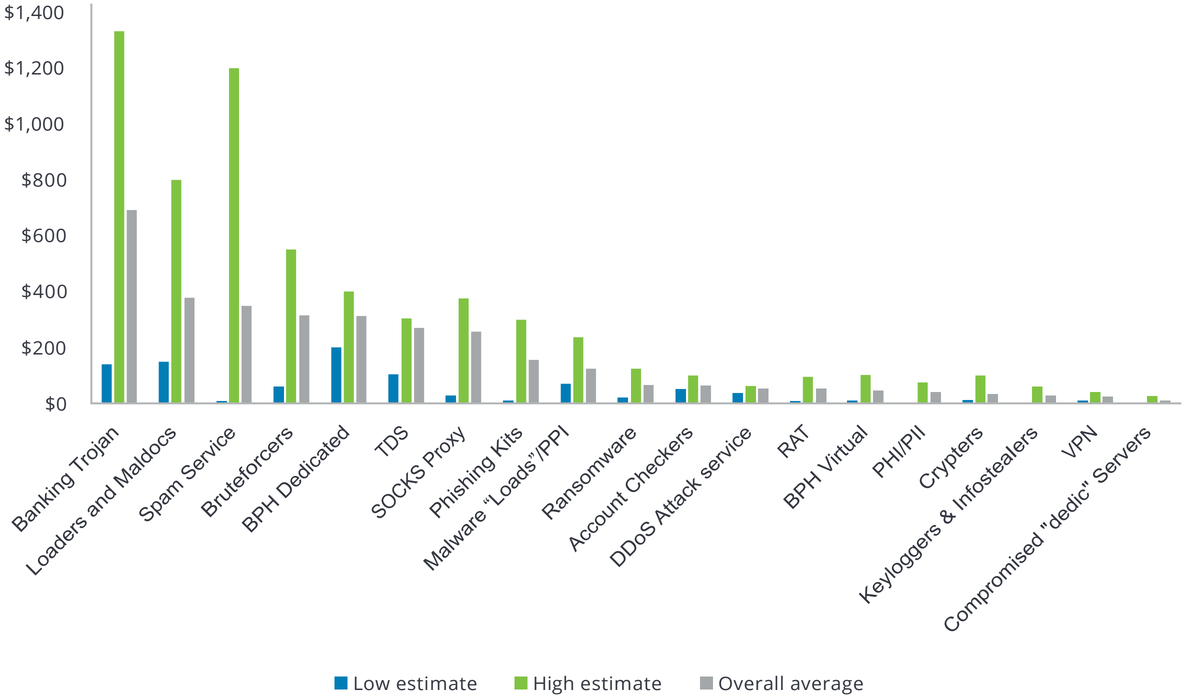
Actor	Actor A	Actor B	Actor C	Actor D
Pricing	SMTP scanner+ bruteforcer $50 VNC scanner+bruteforcer $50 Cpanel's scanner +bruteforcer $80	RDP PlatinumBrute $350 license $200 rebuild Single—a single license to be run on one server RDPPlatinumBrute $900 license $200 rebuild. Multi—a multi-license to be run on several servers for distributed brute forcing attacks	Price: $500	$50–$250 for RDP scan + brute
Average cost per tool	$60	$550	$500	$150

Comparison of tools & services

While many of these tools and services are conceptually similar and perform nearly identical tasks and functions, there is considerable variation in terms of overall sophistication and capability. For every category of criminals, a product almost certainly exists which caters to their needs. This holds true whether the criminal is a novice looking for entry level products, to practitioners capable of modifying and customizing their tools, to the seasoned experts who often offer skills developing custom products. However, the cost of these products does not necessarily correlate to the skill level of the threat actors who purchase them. As an example, a lower level threat actor may be willing to pay a premium for ease of use while a more skilled professional may prefer a cheaper—but more technically demanding—product.

For the reasons stated above, Deloitte TIA calculated a low estimate, high estimate, and overall average cost for each tool and service. These estimates are based on a combination of the individual services, malware, and tools discussed in the previous sections of this study and are displayed for the sake of comparison in the chart below.

Tools and services



Several interesting conclusions can be drawn from a comparison of the estimated costs of the individual goods and services. Unsurprisingly, highly capable malware developers such as those behind banking Trojans, loaders, and maldocs demand a premium and constitute some of the most expensive tools available. Similarly, spam vendors and brute forcers can also demand a high premium for their products. These are followed by resource and infrastructure intensive activities such as dedicated fast-flux BPH hosting or sophisticated proxy services. However, some tools and services display a marked disparity between the lowest cost options and most expensive options. This is most apparent when looking at spam, bruteforcers, and phishing kits where the difference between an entry level service and its most expensive counterpart can be several hundred dollars.

Estimated monthly costs of operation

Overview

In the following sections Deloitte TIA will provide several examples of the estimated monthly operating costs for a criminal business. The examples explored in the following sections represent common scenarios. Deloitte TIA understands that exceptions to each of these scenarios exist—the ingenuity of cyber-criminals practically guarantees such an occurrence. They are meant to provide a reasonable case study that can be used for the sake of comparison. For this reason, some components of malicious activity (such as VPNs), which relate to virtually any criminal business, are omitted.

Phishkit data harvesting

Average estimated operational cost: $494
High estimated operational cost: $1601
Low estimated operational cost: $28
Components: Phishkit + BPH (generic VPS)/dedicated + distribution method (spam/TDS)

Phishkit based credential harvesting is one of the simplest criminal enterprises, and the necessary tools and services are fairly limited. A threat actor only requires the phishing kit itself, a host, and a method for ensuring that victims are directed to the phishing page. The hosting can most likely be accomplished via low cost BPH VPS server or a compromised "dedic" (dedicated) server. The latter, however, would be less stable and may require 5 or more dedicated servers over the course of the month. Finally, a threat actor would need a method enticing users to the phishkit itself. This would most likely leverage a spam campaign and social engineering but may also make use of a TDS and malvertising.

Brute-forcing

Average estimated operational cost: $618
High estimated operational cost: $1026
Low estimated operational cost: $97
Components: Bruteforcer + SOCKS proxy + BPH VPS

Brute-forcing is another relatively straightforward criminal enterprise when examined individually. It requires only a brute-forcing tool, and servers from which to host and operate the tool. However, most criminals would likely choose to use at least a virtual BPH server (possibly dedicated) and incorporate SOCKS proxy service. This ensures that their scanning and brute attempts are both masked by proxies and their backend servers are not subject to abuse or takedown requests.

Infostealer/Keylogger campaign

Average estimated operational cost: $723
High estimated operational cost: $2,260
Low estimated operational cost: $183
Components: InfoStealer Payload + crypter + downloader + file host + distribution method (spam/TDS/Malware "Loads" Service) + C2 node

The most popular methods for infostealer-based data harvesting campaigns require a level of user interaction. To deliver the infostealer and possibly aid in the likelihood of infection via social engineering, the payload will most likely be paired with a downloader or "maldoc." Given the common code base and signatures for infostealers, it will require crypting services to render the malware undetectable. Finally, the actor must choose a distribution method of which they have several options. While spam is the primary vector for malware distribution, they could also leverage a TDS for malvertising, or malware "loads" PPI service. Finally, the actor will most likely require a server to act as a C2 node to coordinate malicious activity and retrieve stolen data. This would also most likely come in the form of a virtual BPH server.

Ransomware campaign

Average estimated operational cost: $1044
High estimated operational cost: $2625
Low estimated operational cost: $391
Components: Ransomware Payload + downloader + crypter + fast-flux BPH+ distribution method (spam/TDS/Malware "loads" service/BruteForce)

Ransomware payloads are the initial requirement but, like other malware, they will most likely require the use of a downloader to ensure it is retrieved and executed. Similarly, a threat actor engaged in a ransomware campaign will almost certainly leverage a crypting service on a regular basis to ensure that the ransomware campaigns can persist undetected. Given the overtly malicious nature of ransomware, a dedicated fast-flux BPH is probably preferred for file hosting and (if necessary) C2 communications. Ransomware distribution is most commonly accomplished with spam or exploit kit-based infections via a TDS or as part of a malware "loads" service. However, bruteforced remote access—either performed by the actor or purchased seperatelyon a "dedic" market—has emerged as a popular method for implanting ransomware as well.

Banking Trojan campaign

Average estimated operational cost: $1,389
High estimated operational cost: $3,534
Low estimated operational cost: $321
Components: Trojan Payload + downloader + crypter + FF BPH + distribution method (spam/EK/loads service/TDS)

The most popular methods for banking Trojan campaigns generally requires low levels of user interaction. Given the common code base and signatures for banking Trojans, it may also require crypting services to render the malware undetectable. Banking Trojans are typically delivered via exploit kits, loaders, or spam distribution with malicious documents. Banking Trojans rely on C2 infrastructure to receive commands and to exfiltrate data. The C2 infrastructure will most likely leverage a FastFlux BPH. Finally, the actor must choose a distribution method of which they have several options. Depending on the quality of the spam distribution service, spam may be cheapest or the most expensive option.

RAT campaign

Average estimated operational cost: $1,116
High estimated operational cost: $ 2,596
Low estimated operational cost: $182
Components: Trojan Payload + downloader + crypter + FF BPH/dedicated/SOCKS + distribution method (spam/EK/loads service/TDS)

RAT campaigns typically require higher levels of interaction than other malware because the threat actor can issue direct commands from the C2 console. This heightened level of interaction will require added layers of security through fast-flux BPH, dedicated servers, or multiple layers of SOCKS proxies. Given the common code base and signatures for RATs, it may also require crypting services to render the malware undetectable. RATs are typically delivered via exploit kits, loaders, or spam distribution with malicious documents.

Multiple payload

Average estimated operational cost: $1,691
High estimated operational cost: $3,796
Low estimated operational cost: $544
Components: Infostealer+ Downloader + crypter + Banking Trojan/Ransomware + FF BPH distribution method (spam/malware "loads" service/TDS)

Many of the more notorious campaigns incorporate several types of malware to include a downloader, infostealer, and final payload that is either a banking Trojan or ransomware. In this scenario, multiple executables will potentially require crypting. Given the resources of attackers who have access to several forms of malware, they would most likely leverage dedicated fast-flux BPH infrastructure for payload hosting and C2. The actor may choose to use a standalone spam service, malware "loads" service, or TDS most likely associated with malvertising and exploit kits.

Account shop

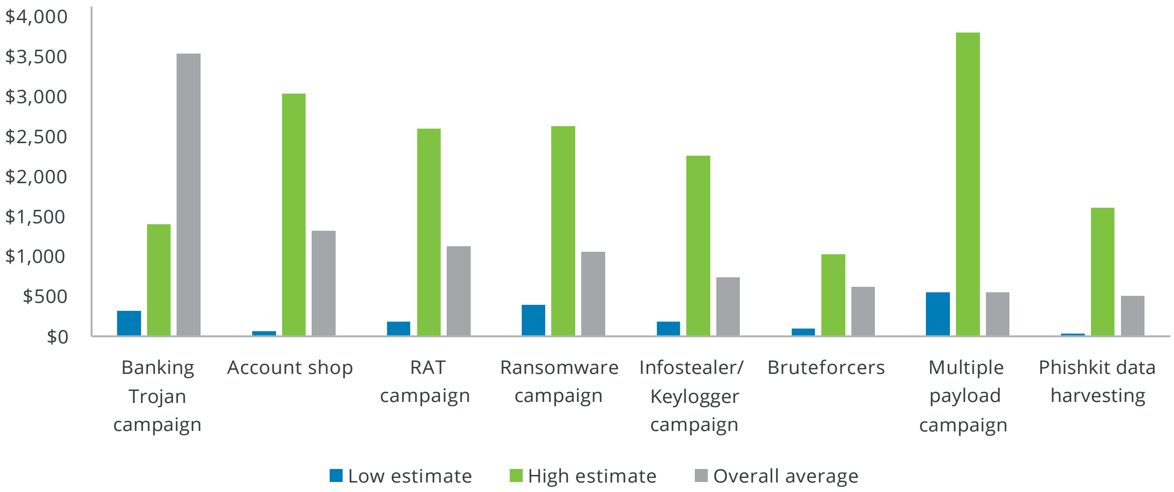
Average estimated operational cost: $3025
High estimated operational cost: $1311
Low estimated operational cost: $68
Components: Phishkit + BPH (generic VPS)/dedic + distro method (spam/TDS) + Account Checker + Proxy service + combo lists AND/OR InfoStealer Payload + crypter + downloader

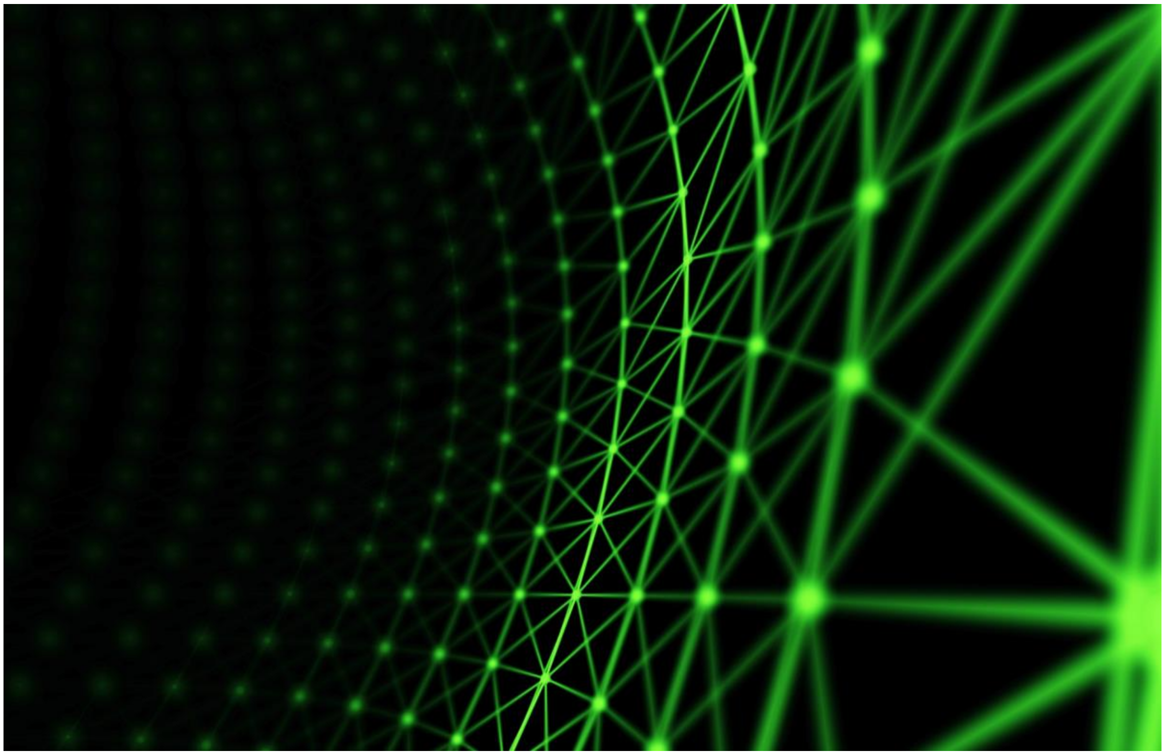
Account shops are commonly advertised across criminal markets and forums. These shops typically specialize in the sale of compromised account credentials harvested via account checkers, info stealing malware, or phishing campaigns. Often, account shops also offer Fullz in addition to their credential offerings. A standalone or web-hosted account checker can be fed with combo lists obtained on the underground. The account checker will typically be paired with a proxy service to hide its origin and to avoid blacklists. Alternatively, data obtained information stealing malware botnets and credential harvesting campaigns that make use of phishing kits are also frequently used to refresh account shop inventories.

Estimated criminal enterprise operations comparison

A comparison of the low end, high end, and average estimates for the previously explored criminal businesses yields additional insights. Phishing kits continue to be the overall most affordable approach both in terms of low estimate and average cost. While banking Trojans remain the most costly on average, a multiple payload campaign, unsurprisingly, is potentially the most expensive criminal business we modeled. These campaigns are followed closely by account shops which are also—surprisingly— one of the most affordable businesses as well. This is largely explained by the several optional factors we incorporated into our analysis. Lastly, it is worth noting the close correlation between ransomware, keylogger, and RAT campaigns in terms of all three estimated values.

Criminal enterprise operation cost





Conclusion

The underground economy is a diverse but interrelated ecosystem where nearly all criminal enterprises incorporate a mixed assortment of tools and services. As demonstrated by Deloitte TIA's analysis of the approximate monthly operational costs, even the most simplified criminal enterprise—such as phishkit based credential harvesting—is dependent on the incorporation of multiple tools and services. This diversification of illicit market offerings is not accidental—it almost certainly reflects a very efficient underground economy where threat actors specialize in a product or service, instead of trying to diversify their proficiency in several disparate and highly technical disciplines. This same concept is reflected in legitimate markets where businesses and economies focus their effort on the production of a limited scope of products or services to achieve productive efficiencies, increase quality, and reduce costs. Unfortunately, in the criminal sphere, this means that threat actors who may otherwise be incapable of performing diversified tasks can instead purchase or partner to acquire the necessary capabilities to launch an attack.

The prices observed by Deloitte TIA appear to indicate one of three approaches. In the first approach, threat actors offer low costs for broadly used products (such as VPN or proxy services) at a large scale. This allows the developers of these products or services to go to market as quickly. However, they run the risk of operating in a densely populated market and must continuously innovate to compete with other low-price offerings. In the second, a threat actor can pursue a more specialized service line that is offered at high price to a limited—perhaps intentionally—select group of users. This is often the case with higher-profile criminal offerings and well-established threat actors and is likely done for operational security purposes. Finally, in the third model an innovative and specialized services with few—if any—viable alternatives are designed to operate at scale. These products and services serve a large customer base but can simultaneously demand highest prices by "cornering" the market niche which they have developed. It is not a coincidence that highly tailored skills, such as malware payload development and fast-flux BPH, demand the most exorbitant prices within the criminal ecosystem.

Trends and shifts in malware distribution and other TTPs can be directly correlated to the implications of this delicate economic system. Due the interdependencies within the criminal ecosystem, the removal or disruption of one product or service can have a profound impact on the black-market ecosystem. This is particularly true for those that could be deemed "lynchpin" services and products.

This collateral effect was seen in 2017 with the fall of the Kelihos spam botnet and the resulting surge of Necurs spam. This trend indicates that a large portion of Kelihos patrons transitioned to the Necurs spam botnet to ensure the resiliency of their operations. Similarly, the disappearance of EK market leaders in combination with a brief hiatus from the Necurs spam botnet in 2016 lead to the exploration of a low-cost malware distribution alternatives. As a result, Deloitte TIA observed a large uptick in the use of RDP brute force for malware distribution.

Changes and innovations seen in the underground economy directly impact organizations' security operations. A common fallacy is that security operations are the focus in tactical indicators of compromise such as domains, IP addresses, and malware hash values. These IP addresses, file hashes, and domains are readily ingested into security appliances despite their short-lived utility. These tactical implementations are often the most trivial defenses to evade. Low-level indicators are dynamic variables that can be changed by threat actors with little effort and are often thwarted entirely with the use of a BPH or proxy service. Similarly, file hashes are trivial to modify—any change to a file, even the flip of a bit will result in a unique file hash. The use of crypting and rebuilding services provide threat actors with a cheap and effective offering to continue their operations with limited to no down-time. Deloitte's observations of market redundancies and the underground market's ability to yield innovative resilience would likely prove that even an elimination of a market-leading crypting or proxy service would likely have little to no impact on cyber-criminal operations and continuous flow of IOCs would persist.

This knowledge of the underground economy illustrates the need to develop, maintain, and mature robust monitoring solutions that focus on the tactics, techniques, and procedures leveraged in threat actor campaigns. For example, use cases that can be used to detect pass-the-hash, PowerShell abuse, and data exfiltration would almost certainly be more impactful and longer lasting impacts than IOC watch lists. Monitoring with well-developed and well-defined use cases driven by priority-based threat intelligence can allow an organization to better detect and prevent malicious activity within the enterprise environment. Monitoring and tuning security controls based on TTPs derived from threat intelligence—rather than atomic indicators—can have a direct impact on the underground market by forcing threat actors to reinvent their operations from scratch, which can take significant amount of time, effort, and money.

Deloitte.