HOW LUCRATIVE ARE VULNERABILITIES? A CLOSER LOOK AT THE ECONOMICS OF THE EXPLOIT SUPPLY CHAIN
Summary

This report is intended for CISOs, security managers and security practitioners who are familiar with vulnerabilities and zero days and want a deeper understanding of the market dynamics driving their discovery and dissemination. It explores the vulnerability-to-exploit (V2E) cybercrime and cybersecurity supply chain, outlines the players in the different market segments and provides insights into the related economic drivers.

The Vulnerability-to-Exploit (V2E) supply chain straddles three different market segments — the white, gray and black markets — and is composed of a variety of market players, from lone wolf rogue researchers to nation states. The markets and players, while divided by their ultimate motives and objectives — defend and disclose versus attack and obfuscate — intersect and interact to create parallel, mirrored supply chains. The white market in vulnerabilities and exploits acts in the open, composed primarily of cybersecurity vendors and researchers, and making intelligence widely available. It has driven the price of zero-day exploits into astronomic six-digit figures, while also catalyzing the criminal black market to consumerize many capabilities required to conduct offensive operations, with cybercrime-as-a-service offerings available to anyone with the necessary funds. The gray market — with nation states and state-sponsored agencies and actors acquiring and developing exploits for covert intelligence operations and motivated by national security concerns — drives the market in exploits and sets the floor price for exploits. These markets are symbiotic and share an ecosystem. By the time an exploit moves from discovery of a vulnerability to ultimately being used in a breach it will have jumped across at least two and sometimes all three of these markets.
Key Insights

• Cybercrime is a far bigger business than cybersecurity. It requires roughly $11 to $12 of criminal activity to drive $1 of security spend. The money laundering activity alone, at $200 billion, is larger than the entire cybersecurity spend worldwide, which is estimated at $136 billion in 2019.

• The imbalance between the amount of resources that threat groups expend on cybercrime versus the more limited resources of defenders requires organizations to improve the efficiencies of their preventative measures. A risk based approach to vulnerability management that prioritizes those vulnerabilities most likely to be utilized in an attack (typically those that are in the most widely adopted technologies and applications) is necessary given the overwhelming number of vulnerabilities.

• The full vulnerability-to-exploit supply chain is composed of three very different market segments — the white, gray and black markets — representing a spectrum of motives between disclose and defend and obfuscate and attack.
  ◦ The white and black markets, while diverging on motives and objectives, are symbiotic. We see what we refer to as parallel and intersecting supply chains, for both legitimate and criminal buyers.
  ◦ The gray market, typified by covert nation-state actors and activities conducted in the interest of national security, has a disruptive impact on the supply chain, defining the floor for exploit value and impacting intelligence availability.

• While the cybersecurity industry’s two-pronged approach of devaluing exploits by disclosing them and driving up the price by offering bug bounties is paying dividends, the high ROI on criminal operations means these will not be sufficient by themselves to fully make zero-day exploits unaffordable.

• The exploit brokering market is dominated by a few main brokerages, almost solely operating in the gray market, with a rising demand and market value for exploits that are not publicly known. The payout ceiling has increased 500 percent in a little over two years.

• The Darknet has lost market share in the trade of exploits, with most of the activity now dominated by a small set of exploit brokerages.

• While cryptocurrencies are heavily used in the criminal business-to-consumer and business-to-business supply chain, especially in cybercrime-as-a-service and cyberattacks-as-a-service transactions, the volatility of relying on a speculative currency has caused its own set of challenges.
Introduction

The primary motivator for hacking has long shifted from tinkering and hacktivism to power, fraud and profit. Reflecting this shift, cybercrime tools and services have undergone a transition towards consumerization, with a growing and diverse supply chain ecosystem providing professionally run and commercially driven cybercrime-as-a-service (CCaaS) offerings. This “platform criminality” combined with the availability of cryptocurrencies has driven a huge growth in cybercrime, as well as democratizing offensive cybercrime capabilities. Recent estimates of the revenue of the global cybercrime market would equal the GDP of many mid-sized countries, at $1.5 trillion per year.

In contrast, cybercrime revenue dwarfs the global investment in cybersecurity, estimated at $136 billion in 2019. In fact, based on some estimates, the $200 billion in money laundering activity alone resulting from cybercrime is larger than the entire cybersecurity industry. Taken at face value, it requires roughly $11 to $12 of criminal activity to drive $1 of security spend. This is of course an oversimplification — we would also need to factor in the cost of data breaches for example — but it highlights the imbalance between what criminals are earning compared to what organizations are spending.

Although cybercrime and cybersecurity are adversarial in principle, a closer inspection of the associated supply chains and markets reveals a more symbiotic relationship, with supply chains mirroring each other and, to a considerable degree, intersecting and overlapping.

At Tenable Research, our primary focus is on managing vulnerabilities, as well as their associated cyber risk. This special report describes the vulnerability-to-exploit (V2E) cybercrime and cybersecurity supply chain, outlines the players in the different market segments and provides insights into the related economic drivers. It also demonstrates how the V2E supply chain is shared between market segments and players with opposing objectives — disclose and defend versus obfuscate and attack.
The Vulnerability-to-Exploit Supply Chain and Market Segments

The White, Gray and Black Markets for Exploits

The vulnerability-to-exploit (henceforth V2E) supply chain is really composed of market players straddling three very different markets — the white, gray and black markets.

**THE WHITE MARKET** is the visible, legitimate part of the supply chain, composed of product end users, hardware and software vendors and service providers and cybersecurity vendors on the commercial side, and open source projects, public vulnerability and exploit databases and independent researchers on the community side. The white market is typified by full and coordinated disclosure practices in general, alongside commercial product and service offerings designed to defend against cyberthreats.

**THE BLACK MARKET**, of which the Darknet is only the best known and easiest to access face, is composed of various actors catering to everything from digital economy cyber fraudsters conducting ransomware heists to more traditional criminal actors, such as drug traders selling their contraband via Darknet markets, to hacktivist activities to terrorist organizations seeking to hide their communications and funding activities from the authorities. It is composed of a mature, if chaotic and unstable, supply chain of vendors, service providers, brokers and marketplaces, with many of the capabilities required to conduct most offensive cyber operations available in the form of “-as-a-Service” and microservice offerings, creating what has been called a “platform crime” economy. Bitcoin and other cryptocurrencies are the primary payment mechanism.

**THE GRAY MARKET** is so named because the participants are primarily state-sponsored agencies and entities, such as domestic security, military and intelligence agencies and ministries of the world. The legality is in most cases in a gray zone, as actions are usually on a geopolitical scale, involving nation state versus nation state interactions. One of the paradoxes is that the gray market is actually less visible than the black market — the color designations refer to the legality, not how open they are. Threat intelligence vendors, independent researchers and the media all disseminate black market trends as their core function, whereas nation state activities are harder to attribute and less reported on.

The V2E Supply Chain Model

In this simplified supply chain model (see Fig. 1) composed of producers, suppliers, service providers and consumers, we outline associated market segments.

- Producers are involved in the discovery of vulnerabilities and the subsequent development of proof-of-concept exploit code.
- Suppliers facilitate the brokering and general availability of exploits and related knowledge to the market.
- Service providers integrate exploits into a variety of third-party products and services, from penetration testing frameworks to exploit kits.
- Consumers, for example an end user organization conducting a penetration test or a criminal gang perpetrating fraud, then use the exploits.
The table below lists the primary market players in the V2E Supply Chain Market Segments. Note how some market players are active in multiple market segments, reflecting that the entire supply chain can theoretically be delivered by a single vendor or provider. In practice, due to the sheer volume of vulnerabilities and the time, cost and effort involved in developing exploits, no major vendor or provider relies solely on in-house development.

<table>
<thead>
<tr>
<th>PRODUCER</th>
<th>PRODUCER</th>
<th>SUPPLIER</th>
<th>PRODUCT &amp; SERVICE PROVIDERS</th>
<th>CONSUMERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Discovery</td>
<td>Exploit Development</td>
<td>Exploit Brokering</td>
<td>Exploit Productization</td>
<td>Exploit Delivery</td>
</tr>
<tr>
<td>• Cybersecurity vendors and service providers</td>
<td>• Cybersecurity vendors and service providers</td>
<td>• Exploit databases</td>
<td>• Cybersecurity vendors and service providers</td>
<td></td>
</tr>
<tr>
<td>• Bug bounty programs</td>
<td>• Independent researchers</td>
<td>• Exploit brokerages</td>
<td>• Hacktivists</td>
<td></td>
</tr>
<tr>
<td>• Product vendors and manufacturers</td>
<td>• Exploit brokerages</td>
<td>• State-sponsored actors</td>
<td>• Terrorists</td>
<td></td>
</tr>
<tr>
<td>• Independent researchers</td>
<td>• State-sponsored actors</td>
<td></td>
<td>• State-sponsored actors</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. The V2E supply chain, market segments and market players.
Vulnerability Discovery

A vulnerability is a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source”. Vulnerabilities are discovered in a variety of different ways, for example through static source code analysis or dynamic application testing. Vulnerabilities are also frequently discovered indirectly, by unexpected user behavior or in the course of troubleshooting and related production incidents. Not every software or hardware flaw is a vulnerability — only those resulting in the loss of confidentiality, integrity or availability if exploited by a malicious actor. Furthermore, due to other considerations, such as access permissions and rights, software dependencies and OS and third-party security mechanisms, not every vulnerability can be exploited. Even when it can, the impact can vary between a denial of service or limited read access to full system compromise.

Due to the widespread adoption of full disclosure, and especially coordinated disclosure and bug bounty programs in the cybersecurity industry and community, vulnerability information in the form of advisories, reports and active discussions is widely and freely disseminated and available. Bug bounty programs aside, there is only a negligible market for vulnerability discovery alone.

Exploit Research and Development

Once a vulnerability has been discovered, a functional proof of concept exploit must be developed. Exploit development is a broad term, but can vary greatly in detail depending on the vulnerable application or device or the type of flaw. One example would be a typical web application flaw, such as SQL injection, where discovery is often done via brute-forcing or fuzzing and integrates active exploitation. In contrast to this, a flaw discovered in an IoT device or, to cite an extreme case,
an internet-enabled or autonomous car, requires not only specialized expertise, but also physical possession of the devices themselves and often specialized hardware and tools. Many vulnerabilities remain unexploited simply because developing an exploit is prohibitively expensive or logistically unfeasible for anyone but well-funded and well-resourced organizations.

**Exploit Brokering and Dissemination**

The dissemination of exploit code and intelligence occurs for the most part via public channels, for example via exploit databases such as ExploitDB and security conferences and papers, the latter especially being the case for new, niche or novel vulnerabilities and exploits. Commercial offerings, for example penetration testing frameworks, also make exploit code widely available. This means many exploits are free, public and readily available, with a negligent market opportunity as a result. The other consequence is that exploits that are not publicly known about have risen in demand and market value. The exploit brokering market itself has gone through major changes over the years, evolving from a large and diverse group of freelance exploit brokers scouring the Darknet for exploits and selling to the highest bidders, to being dominated by a few main brokerages. Multiple scandals rocked the small industry. Smaller brokers frequently lacked the ability to conduct targeted vulnerability discovery for in-demand target technologies and the capability to optimize and customize exploit code for different consumers. With the estimated average cost to develop a targeted exploit at $30,000, many smaller brokers have been unable to compete with the large brokerages. Independent researchers now frequently sell to the exploit brokerages directly or use freelance exploit brokers as middlemen. This trend has concentrated the zero-day and exploit market into the hands of a few big players, and, to a degree, also governments. As recently as 2017, the size of the entire gray exploit brokering market was only estimated at $10 million. Recent reports indicate that exploit brokering has all but faded on the Darknet, with only a handful of active actors, who are suspected to be working directly for the brokerages.
**Exploit Productization**

Proof-of-concept exploit code is rarely developed for productive use and requires customization, for example to include different payloads or to be adapted to different targets. Exploit code and its derivatives are frequently productized to develop active vulnerability and penetration testing self-assessment checks. Exploit intelligence is also used to develop prevention and detection signatures and correlation rules for defensive security solutions.

On the offensive, and especially the criminal side of cybersecurity, an entire ecosystem of vendors and service providers has sprung up, evolving into “platform crime” where anyone can purchase the required capabilities from cybercrime-as-a-service (CCaaS) and cyberattack-as-a-service (CAaaS) offerings on the Darknet. Exploits must ultimately be delivered to a vulnerable target, so they are for the most part integrated into malicious tools and services that aggregate several vulnerabilities for greater exploit effectiveness and broader attack surface targeting, or to facilitate multi-stage attack chains that include privilege escalation or lateral transfer.

**Exploit Delivery**

Exploits by themselves do not breach a victim. They must be delivered to vulnerable targets and be used to execute a kill chain of different attack steps to obtain an ultimate objective. The objective could be to steal credential and financial data, install a remote access Trojan (RAT) to integrate the system as a zombie into a botnet for DDoS attacks, or run a cryptominer, for example. Aside from targeted or advanced persistent attacks, which are still the exception, most criminals leverage malicious tools that are centrally and remotely managed, scalable and automate most of the kill chain, from victim identification and profiling to exploitation and payload extraction. Cyberattack-as-a-service offerings, for example offensive malicious toolkits such as exploit kits, including command-and-control infrastructure and even operator hackers-for-hire, can be purchased on the black market.
Vulnerability-to-Exploit Ecosystem

The diagram below combines the three market segments white, gray and black with the simplified supply chain capabilities and maps out the active market players.

![Diagram](image)

**Market Players**

The diversity in products and services available in the V2E supply chain, however, obfuscates the fact that in many market segments the number of active players can be quite small. Especially in the gray market, only a few active participants may be involved in the development of an exploit for a vulnerability. Information asymmetry and market value based on knowledge exclusivity are defining characteristics of the V2E market and separate the market players between those that want to publicly release knowledge about vulnerabilities and exploits to facilitate better defense and those that actively seek to keep this sort of information secret to retain its value for offensive purposes.

Below we describe the primary active players interacting and competing in the V2E supply chain.

**Independent Researchers**

Many vulnerabilities are discovered by independent researchers with a variety of motivations, ranging from idealism and curiosity to professional and peer group recognition. Independent researchers often discover the initial vulnerability, but work with technology and security vendors or organizations such as Computer Emergency Response Teams (CERTs) in most cases to publicly disclose the vulnerability.
Software and Hardware Vendors and Service Providers
Secure development lifecycle (SDLC) management and coordinated disclosure, participation in bug bounty programs and direct feedback from product users all help make software and hardware vendors and service providers amongst the most prolific publishers of vulnerability advisories and related intelligence. The majority of vulnerabilities are publicized this way and communicated to the greater community, with Microsoft’s Patch Tuesday having become a regular monthly gauntlet run for millions of businesses worldwide. Vendors and service providers must plan and coordinate the development and deployment of patches and mitigating controls and thus have a direct commercial interest in discovering vulnerabilities.

Cybersecurity Vendors and Service Providers
There are a few offensive cybersecurity vendors, for example those selling exploitation and penetration testing frameworks and services, who directly discover some vulnerabilities for the purpose of enhancing their product or service offering. In addition, some cybersecurity vendors employ their own in-house research teams to conduct investigations and issue industry reports; examples of these include Google Project Zero and Tenable’s own research team. Tenable alone has discovered 95 vulnerabilities in 2019 as of October. However, the majority of cybersecurity vendors that contribute towards vulnerability discovery do so either because of indirect inadvertent discovery — for example because they detected a new exploit in the wild — or because they conduct research in this area to enhance their defensive offering — for example adding vulnerability detection tests or intrusion protection signatures. Disclosure is usually conducted in a coordinated manner with the impacted third-party vendor, following a disclosure policy.

Cybercrime-as-a-service Providers
The black market in services to support and enable criminal cyber activities has matured into what one scholar has termed a “platform crime” ecosystem. Every conceivable capability required to successfully conduct offensive cyber operations is available in the form of “as-a-service” and microservice delivery models, with the Darknet (encompassing not just the TOR Onion network but also encrypted and onetime communication methods such as WICKR and telegram and bulletproof hosting services) the most visible and active channels.

---

**Figure 6.** Darknet advertisement for ransomware CCaaS offering.

<table>
<thead>
<tr>
<th>PACKAGE #1</th>
<th>12 MONTHS C&amp;C Dashboard (RaaS)</th>
<th>Price: 900 USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>• C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• C# Decrypter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Stub Size: 250kb (unique exe for each buyer)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Platform: Windows (both x86 and x64)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Duration: 12 Months access to Darknet C&amp;C Dashboard (to receive the AES keys from clients)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Fees: We take NO FEES from your Clients</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IP Tracking: Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Offline Encryption: Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Support: Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Real-Time Client Manager: Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (FREE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Paid Add-On (Clone): Afree FUD RANION copy with the same setup information (+90 USD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Paid Add-On (Crypter): Additional Crypter/Obluscator + unique onion address (+90 USD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Paid Add-On (Unkillable Process): Unkillable Process aka BSOD (+90 USD)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Paid Add-On: optional file types to encrypt (for all encrypted file types see (FAQ))</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Paid Add-On: optional Client’s sub-banner in your language (already present en, ru, de, fr, it, ml, fas, za)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
From exploit procurement to exploit packaging, to attack obfuscation and money laundering, CCaaS services are available to anyone with the necessary funding and motivation. Cryptocurrencies facilitate much of the day-to-day business in the CCaaS market. Some services, such as crypto tumbling and money laundering, represent a foundational pillar of the black market, as vendors themselves require these services to securely conduct their business. While there are alternative methods available, the wide proliferation and easy (compared to other approaches) access of cryptocurrency has acted as a catalyst for cybercriminal operations.

Exploit Brokerages and Brokers

Exploit brokers procure exploits and sell them to buyers. Exploit brokering is almost exclusively restricted to the gray and black market segments of the V2E supply chain, and even then is an optional component. Historically the ecosystem was composed of many independent freelance brokers, directly engaging with independent exploit developers. This composition has changed in recent years, with a few large commercial companies acting as brokerages and dealing directly with state-sponsored entities and agencies, acting as intermediaries between brokers and customers. These large brokerages offer capabilities for customizing exploit code and in some cases also develop exploits themselves. As such, we differentiate between brokers (small, independent actors) and brokerages (professional and commercial entities).

Brokering itself is frequently an optional step in the supply chain.

Bug Bounty Programs

Bug bounty programs — whether directly managed by a technology vendor or by a service provider itself, like the Google Security Reward Program, or managed by a dedicated bug bounty provider — are becoming more common and have begun contributing towards the increase in discovered and published vulnerabilities. In all cases, the actual discovery of the technical vulnerability is usually by an independent or third-party researcher and will typically result in a vendor advisory being released.
**State-sponsored Actors**

The role of state-sponsored actors in the discovery process is a hotly disputed subject, but came into sharp focus with the EternalBlue and subsequent global WannaCry and NotPetya incidents\(^\text{14}\). In general, it can be assumed that most nation states have capabilities to conduct primary and, in some cases, on-demand vulnerability discovery assessments. The success of those efforts are difficult to quantify. State-sponsored actors are prolific and visible consumers of exploits from exploit brokerages, but due to information asymmetry the proportion between what is acquired, what is developed and what is utilized is not easy to establish.

**Parallel and Intersecting Supply Chains**

One of the striking things about the vulnerability-to-exploit supply chain is how the white and black markets begin from the same source — the discovery of a vulnerability — and then diverge into parallel mirrors of one another (see Fig. 7), with the difference that the white market leverages exploit code and intelligence for defensive purposes, rather than for offensive purposes, such as exploiting adversaries or victims. The segmentation and segregation between the white, gray and black markets is not as neat and tidy, as the example of EternalBlue (see Fig. 8) showcases.

According to a May 2017 article in the *Washington Post* entitled “NSA officials worried about the day its potent hacking tool would get loose. Then it did,” EternalBlue (CVE-2017-0144) was kept a secret by the United States National Security Agency until leaked by the ShadowHackers group in 2017. From there it was released to the Metasploit Penetration Testing framework by a researcher working for another security vendor who had developed working exploit code. Threat actors quickly followed by productizing the exploit code, which led to the global WannaCry incident. What is most intriguing about this particular example is how it jumped from the gray market into the white market and from there into the black (and possibly gray again, depending on whose attribution you trust) market. All three markets, while theoretically separated by motive and intent, are in a symbiotic relationship.
While a lot of the white market supply chain is driven by community effort, there are a number of different professional career paths available to earn an honest living researching, developing and deploying exploits. Working for a cybersecurity vendor as a researcher is one common option as is working as a penetration tester for a consultancy or MSSP, or as a red-teamer in an end-user organization on the exploit consumption side.

The gray market also offers legal employment opportunities in law enforcement, domestic and foreign security, intelligence agencies and the military. Below, we look at the salary ranges for some of these types of jobs.
Penetration Tester/Red Teamer

The earnings potential for a penetration tester can vary vastly due to the fact that a penetration test can be anything from a vulnerability assessment with basic exploitation to a fully objective-based capture-the-flag style red team engagement. Specialization, such as operational technology (ICS, SCADA) or databases, can also increase salaries and daily rates. Differences based on geography (the average in the U.K. is £36,48915, or approximately $44,000 at the time of writing, versus $82,48016 in the U.S. for example) are also especially pronounced.

The limiting factor for earnings in penetration testing is how much you can charge the customer. Even assuming 90 percent billable hours (which considering scoping, training, etc. is highly aggressive), a provider would need to charge a minimum of $367 per day just to cover the base salary (not including additional costs such as pension scheme, etc.) for someone earning $90,000 per year. With competitive rates averaging $600-$80017 per day for a standard infrastructure assessment, there is a realistic ceiling on what can be earned.

Nation-state Researcher

Based on publicly available data, an entry-level NSA attack developer, described in an NSA job ad as “reverse engineering hardware and/or software to develop new exploitation capabilities,” can earn between $70,000 – $90,000 per year18. At GHCQ in the U.K., salaries for an entry-level vulnerability researcher, for example, start at $30,000 – $35,000019 (£26,091 – £29,694)

Exploit Pricing

Pricing for individual exploits varies over time, based on market demand and supply, the complexity of the exploit and the level of system compromise offered. Gray market exploit brokers publish public price lists, essentially competing against each other in a public bidding war while also driving up the monetary amount any black market brokers have to offer. This also most likely explains the reduction in exploit brokering activity on the Darknet. Few of the small freelance brokers have sufficient capital to pay millions of dollars for an exploit that may become worthless in the time it takes to sell by circumstances such as independent rediscovery.

Earnings are also potentially capped — most exploit brokers do not have unlimited capital either and ultimately also have to find buyers. Oversaturating the market will potentially reduce the exclusivity and thus the price of that particular type of exploit, and banking exploits to release over time is fraught with its own risks, such as being disclosed by a third party.

Below we provide some examples gathered from various Darknet markets and exploit brokerages.
<table>
<thead>
<tr>
<th>EXPLOIT TARGET</th>
<th>DESCRIPTION</th>
<th>GRAY MARKET (EXPLOIT BROKER) MAXIMUM PRICE</th>
<th>BLACK MARKET (DARKNET) MAXIMUM PRICE</th>
<th>WHITE MARKET (VENDOR BUG BOUNTIES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Acrobat</td>
<td>Remote code execution (typically a CVSSv3 high severity vulnerability)</td>
<td>$80,000</td>
<td>$130,000</td>
<td>-</td>
</tr>
<tr>
<td>Apache on Linux</td>
<td>Remote Code Execution, typically a CVSSv3 high severity</td>
<td>$500,000</td>
<td>$1,000,000</td>
<td>-</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Remote Code Execution with local privilege escalation</td>
<td>$100,000</td>
<td>$500,000</td>
<td>$15,000</td>
</tr>
<tr>
<td>Telegram on Android</td>
<td>Remote Code Execution and privilege escalation</td>
<td>$500,000</td>
<td>$1,000,000</td>
<td>-</td>
</tr>
<tr>
<td>Whatsapp on Android</td>
<td>Remote Code Execution and privilege escalation</td>
<td>$1,000,000</td>
<td>$1,000,000</td>
<td>-</td>
</tr>
<tr>
<td>Microsoft Office (Word/Excel)</td>
<td>Remote Code Execution, typically a CVSSv3 high severity</td>
<td>$150,000</td>
<td>$100,000</td>
<td>$15,000</td>
</tr>
<tr>
<td>Google Chrome on Windows</td>
<td>Remote Code Execution</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$200,000</td>
</tr>
<tr>
<td>Android OS</td>
<td>Remote Code Execution and privilege escalation 0-click</td>
<td>$2,500,000</td>
<td>$500,000</td>
<td>$200,000</td>
</tr>
<tr>
<td>Safari on iOS</td>
<td>Remote Code Execution and privilege escalation</td>
<td>$500,000</td>
<td>$500,000</td>
<td>$1,000,000, with $100,000 more typical</td>
</tr>
<tr>
<td>iOS</td>
<td>Remote Code Execution and privilege escalation 0-click</td>
<td>$2,000,000</td>
<td>-</td>
<td>$1,000,000, with $100,000 more typical</td>
</tr>
</tbody>
</table>

Table 2. White, gray and black market exploit price examples, October 2019."
Darknet brokers can offer up considerably more for many exploits than gray market competitors, especially in instances where the exploits are associated with current threat attack vectors, such as drive-by-exploitation and ransomware. The majority of exploits being sought focus on the client (such as web browsers and associated plugins), mobile and communication sides. The six-figure prices for secure communication applications such as telegram and WhatsApp are noticeable in both markets. Prices being offered for exploits targeting Android and iOS have rocketed in the gray market as well. Surveillance and communications espionage are driving the largest price increases in the entire market.

**Bug Bounties**

A few select researchers have joined the ranks of the wealthy by participating in bug bounty programs using dedicated bug bounty platforms, earning over $1 million\(^21\). These do seem to represent the exceptions, though, rather than the rule. Recent analysis of bug bounty data indicates that less than 1 percent of most active participants average $34,000 per year\(^22\). This may be a decent income, depending on where you live in the world, but is far below what most people can earn in a regular cybersecurity job. The income is also unpredictable, as finding valuable vulnerabilities is never guaranteed.

Participants in vendor-run bug bounty programs have fared better, with Google having paid out $60,000 for a single vulnerability for example, with total payouts since 2010 topping $15 million\(^23\). But that sum does not factor in the hundreds to thousands of participants who have invested time and effort without any success or payout.

Bug bounties generally pay far less than selling exploits in the gray or black markets, if they pay at all. The bounties do offer incentives to people who would never consider working in the shadows and do this out of fun and curiosity, with the potential for a windfall if they are fortunate. The same skills can, however, be leveraged into a more lucrative professional career for most people.

**The Impact of Bug Bounties and Similar Incentives**

Bug bounty programs, whether direct or indirect using bug bounty providers, to an extent determine and set a minimum market price. This white market price determines the floor for any gray or black market value and subsequently serves to incentivize researchers to go the coordinated disclosure path. When we look at the overall size of the cybercrime market (according to one estimate, $1.5 trillion) compared to the actual spend on cybersecurity, we can already determine an imbalance. Raising the cost of access to the means of attack, i.e. exploits in our example, only works if the sum offered is higher than the gains that can be made by the ultimate criminal act. The sum total cost of the entire attack chain, and that includes the various required exploits, must be lower than the potential win of executing it — as in any business — to derive a margin. This must also include the cost of money laundering, operational security and various other supporting capabilities.

Based on the increase in money being offered by gray market exploit brokerages, where we have seen the price for a remote-code execution exploit for Android rise to $2.5 million, at least some vendor’s efforts, such as Google, are having an impact. On the other hand, iOS exploits have decreased in price from $1.5 million to $1.0 million due to increased market supply, indicating that exploit value drives development targeting and efforts\(^24\). But overall, the earnings potential for cybercriminals and CCaaS and CAaaS providers still outweigh their costs. One additional impact of this has been that smaller actors have been priced out of the market and the ceiling for entry has risen. But it has also concentrated the market and driven a professionalization of the threat landscape.
Ecosystem and Market Trends

Parallel and Intersecting supply chains exist to cater to both legitimate and criminal buyers

As we describe in this report, what is remarkable is how the white and black markets mirror each other, and how the market segments intersect in many real-world examples of the full supply chain. The barriers between the white, gray and black markets are permeable — with tools, intelligence and knowhow easily transferable between market segments. This is especially obvious when we consider that many malicious actors leverage a similar, if not identical, toolset to the defenders for conducting many operational activities.

The Darknet has lost market share in the trade of exploits, with most of the activity now dominated by a small set of exploit brokerages

A recent report states that the amount of activity and active actors on the Darknet has dramatically decreased, with only a handful of active brokers seen in 2018, from a peak of over 30 in 2015. This decrease is based on market consolidation, with a few large commercial brokerages dominating the trade in exploits. On the one hand, this has removed exploits from the black market, at least for a while. On the other hand, it means that some exploitable vulnerabilities will remain hidden from the wider security community, thus leaving them at risk of being independently discovered by other parties who may develop a working exploit. The advantage to a nation state is dubious in the long term — offensive cyber capabilities far exceed defensive ones in effectiveness, especially when affordability and operation feasibility are concerned. Everyone can successfully attack — but not defend — so offensive advantages are offset by defensive deficits. The example of EternalBlue and WannaCry demonstrated this in the case of the private commercial sector.

While cryptocurrencies are heavily used in the criminal B2C and B2B supply chain, especially in CCaaS and CAaaS transactions, the volatility of relying on a speculative currency has caused its own set of challenges

One of the interesting consequences of relying on volatile and speculative faux currency to facilitate business transactions became apparent during our research. Due to the inherent illegal nature of most transactions, it’s a constant challenge to build and retain trust. To compensate for this lack of trust, many Darknet markets offer an escrow system. A buyer issues an order and the payment is left safely in escrow with the marketplace until the buyer confirms they have received the product and are satisfied with it before the funds are released to the vendor.

With the trading price of Bitcoin and other cryptocurrencies in recent decline, and finalizing a trade sometimes taking many days, the value of the crypto coin in escrow can drop in the intervening time. The question of who takes the financial hit, when the day-to-day price is not predictable and highly variable, has caused disagreement and dissension in some marketplaces. The fact that the marketplace holds the funds in the meantime has also led to a number of what are called “exit scams,” where the market providers abscond with the escrowed money.

The amount of revenue generated is small in comparison to the collateral damage

If we take estimates for the ransoms generated by WannaCry, $140,000, it is dwarfed by the resulting collateral damage for the victims. The cost of the IT support that the U.K. National Health Service incurred to recover data and restore systems was £73 million alone. The imbalance between what criminals can make, on the one hand, and the cost for industry and society on the other, is common across much of the data. A cynic would quip it may be more cost effective to pay criminals directly; the theory is that ransomware has operationalized, even if it more closely resembles a racket than a legitimate business. Even the FBI has recently come around to the conclusion that paying the ransom is sometimes the simplest solution.

Of course, it’s considerably more difficult to buy into the theory that paying the ransom will just encourage and embolden threat actors after you’ve just been hit by one.
Disincentivizing Cybercrime

Quickly patching those vulnerabilities that are most likely to be utilized in an attack reduces the number of targets available for cybercriminals. Such risk based prioritization works to decrease the value of a given vulnerability by reducing their overall availability for exploit.

Another approach for reducing cybercrime is to disincentivize attacks by making them so expensive to execute that they do not yield ROI.

Bug bounties, for example, disincentivize researchers from engaging with the gray and black markets by offering a legal and legitimate alternative to earn money. In theory exploit developers can earn upwards of millions of dollars — potentially becoming millionaires with a single exploit — but in reality those are the outliers and the vast majority of researchers who are involved in bug bounties and community research earn very little.

The white market has driven the cost of exploit development upwards and reduced the number of zero-day exploits available for criminal and covert operations, while reducing overall exposure and risk for enterprises and consumers everywhere. But there is a paradox here as well: Reducing market supply and increasing production cost also increases the value of exclusive zero days, thus incentivizing investment again.

Thankfully though, the greatest disincentives are the risks and ethical implications of working with the gray or black markets. Motivations for actors in all three markets can vary greatly. White market participants are frequently motivated by altruism and peer group prestige, while gray market participants, especially state-sponsored researchers and operations, have an ethical justification in national security.

Driving up the price of obtaining exploits for the black market is thus a valid approach, with the caveat that when we consider the ROI on cybercriminal operations in some cases has been estimated at 500 percent, we probably have a long way to go to be successful using this approach alone. Thankfully, though, it is just one of many policies that act together.

Historically, the black market for exploits has been around before the gray or white markets. Early black market participants often traded exploits amongst themselves for no payment other than prestige. Currently, the market for software vulnerabilities is unregulated, unstructured, decentralized and lacks transparency. Recent changes to the Wassenaar Arrangement to include intrusion software tools as dual-use goods under international law is an attempt by governments to regulate exploit markets via export controls. The very nature of vulnerabilities makes it hard to regulate, as it suffers from arrow paradox, i.e. sharing the information to establish its value also destroys its value. One can reverse engineer the exploit used against them to develop a patch, invalidating exclusivity of the knowledge of the vulnerability.

International law and governing bodies, such as NATO (Tallinn Manual in 2013) and the United Nations, have a set of guidelines for how existing laws of war can be applied to cyber conflict.

Governments can choose to exploit certain zero days when national security demands it. For any national vulnerability policy to be effective, all vulnerabilities discovered or bought by the government must be as accountable and as transparent as possible with some degree of judicial or legislative oversight to prevent abuse.
Endnotes

6. We are aware that these estimates can vary greatly depending on your assumptions and preferred data source. Readers are encouraged to use their preferred estimates for this simple calculation: total cybercrime market revenue/cybersecurity industry revenue
9. https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/
10. See https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf
18. See https://www.glassdoor.co.uk/Job/fort-meade-attack-developer-entry-mid-level-jobs-SRCH_IL.0,10_IC1165756_KO11,43.htm
20. Based on Zerodium, Vendor collateral and a review of various Darknet markets
27. https://www.theregister.co.uk/2019/10/03/fbi_softens_stance_on_ransomware/
28. https://repository.jmls.edu/cgi/viewcontent.cgi?article=1694&context=jitpl
Appendix

Literature
Below readers will find a list of the literature used to compile this report:

“In the Web of Profit”
by Dr. Michael McGuire, sponsored research by Bromium (2018)

Systematically Understanding the Cyber Attack Business: A Survey
Keman Huang, Michael Siegel, Stuart Madnick, MIT Sloan (2018)

“The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments”
Stearns Broadhead, Trilateral Research Ltd.

“Black-market ecosystem: Estimating the cost of “Pwnership””
Deloitte (2018)

“Policy Priorities for Coordinated Vulnerability Disclosure and Handling”
Cybersecurity Coalition (2019)
https://www.cybersecuritycoalition.org/policy-priorities