Carbon Black.

OCTOBER 2017

The Ransomware Economy

How and Why the Dark Web Marketplace for Ransomware Is Growing at a Rate of More Than 2,500% Per Year

Executive Summary

CryptoLocker. GoldenEye. Locky. WannaCry. It's no secret that 2017 is shaping up to be the most notorious year on record for ransomware. Even a casual news consumer can identify several, if not all, of the menacing ransomware attacks that have cost worldwide businesses an estimated $1 billion this year.

With ransomware illuminated in the cybersecurity spotlight, **Carbon Black's Threat Analysis Unit (TAU)** leveraged its own intelligence network to investigate the deepest, darkest portions on the web, where ransomware is currently being created, bought, and sold in burgeoning underground economies.

Our research found that, from 2016 to 2017, ***there has been a 2,502% increase in the sale of ransomware*** on the dark web. This increase is largely due to a simple economic principle - supply and demand. Cybercriminals are increasingly seeing opportunities to enter the market and looking to make a quick buck via one of the many ransomware offerings available via illicit economies. In addition, a basic appeal of ransomware is simple: it's turnkey. Unlike many other forms of cyberattacks, ransomware can be quickly and brainlessly deployed with a high probability of profit.

As our research found, these dark web economies are empowering even the most novice criminals to launch ransomware attacks via do-it-yourself (DIY) kits and providing successful ransomware authors with annual incomes into six figures.

KEY FINDINGS

1. There are currently **6,300+** estimated dark web marketplaces selling ransomware, with **45,000** product listings.

2. The prices for do-it-yourself (DIY) kits range from **$0.50 to $3K**. The median price is **$10.50**.

3. Comparing 2016 vs. 2017 YTD, the ransomware marketplace on the dark web has grown from **$249,287.05 to $6,237,248.90**, a growth rate of **2,502%**. This economy extorts, according to the FBI, ransom payments that totaled about **$1B** in 2016, up from **$24M** in 2015.[1]

4. Some sellers of ransomware are making **more than $100,000** per year simply retailing ransomware. (This compares to $69,000 for a legitimate software developer, according to figures from PayScale.com.)

5. The most notable innovations contributing to the proliferation and success of the dark web ransomware economy have been the emergence of **Bitcoin** for ransom payment, and the anonymity network, **Tor**, to mask illicit activities. Bitcoin allows money to be transferred in a way that makes it nearly impossible for law enforcement to "follow the money." Bank transfers and credit card transactions traditionally aid in the quick take-down of scams. Bitcoin means there's no bank to identify the account holder.

6. Ransomware sellers are increasingly specializing in one specific area of the supply chain, further contributing to **ransomware's boom and economy development**.

[1]http://www.ciodive.com/news/symantec-size-of-ransomware-demands-jumped-266-in-2016/441365/

Analysis

During August and September 2017, Carbon Black researchers monitored 21 of the largest dark web marketplaces for new, virtual offerings related to ransomware. The description of the offering and the sales price were recorded.

To represent the complete dark web economy, the sample of findings from 21 of the largest marketplaces was extrapolated to a population-wide value based on an assumption that approximately 25% of the total dark web website population is composed of similar marketplaces. (NOTE: All prices and values are reported in USD. In instances where prices were offered in Bitcoin, conversion to USD was made for the day the offer was identified.)

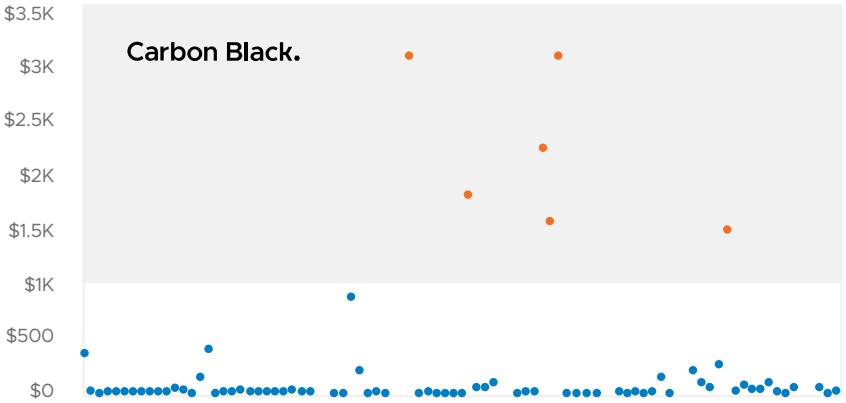
Based on our research, ransomware has become its own economy based on a turnkey system. As of this writing, there are currently more than ***6,300*** estimated dark web marketplaces selling ransomware, ***with more than 45,000 current listings.***

The offerings on these marketplaces are vast, ranging from lockscreen ransomware targeting Android devices (for $1.00) to custom ransomware including source code (for $1,000+.) The chart below reflects a sampling of listings and USD prices for underground ransomware offerings during a portion of September 2017.

RANSOMWARE	PRICE (USD)
Custom Stealer Ransomware BTC	**$199**
Code Source Bitcoin Thief & Ransomware BTC	**$99**
Intelligent Bitcoin Theif Copy/Paste Source Code/Ransomware Modified 2017 More Agressive	**$50**
Android Locker Ransomware	**$250**
Ransomware - Custom Made	**$1470**
Ransomware Pigsaw Source Code Modified 2017	**$30**
Personal Custom Stealer & Ransomware BTC	**$75**
Source Code Bitcoin Thief & Ransomware BTC HQ	**$50**
Intelligent Bitcoin Theif Copy/Paste Source Code/Ransomware Modified 2017 More Agressive	**$25**
?Code Source Bitcoin Thief & Ransomware BTC???	**$99**
6 Bitcoin Ransomware Easy Money System	**$5**
Philadelphia Ransomware and Other Make Top $$$(Clone)	**$1**
Custom Stealer & Ransomware	**$50**

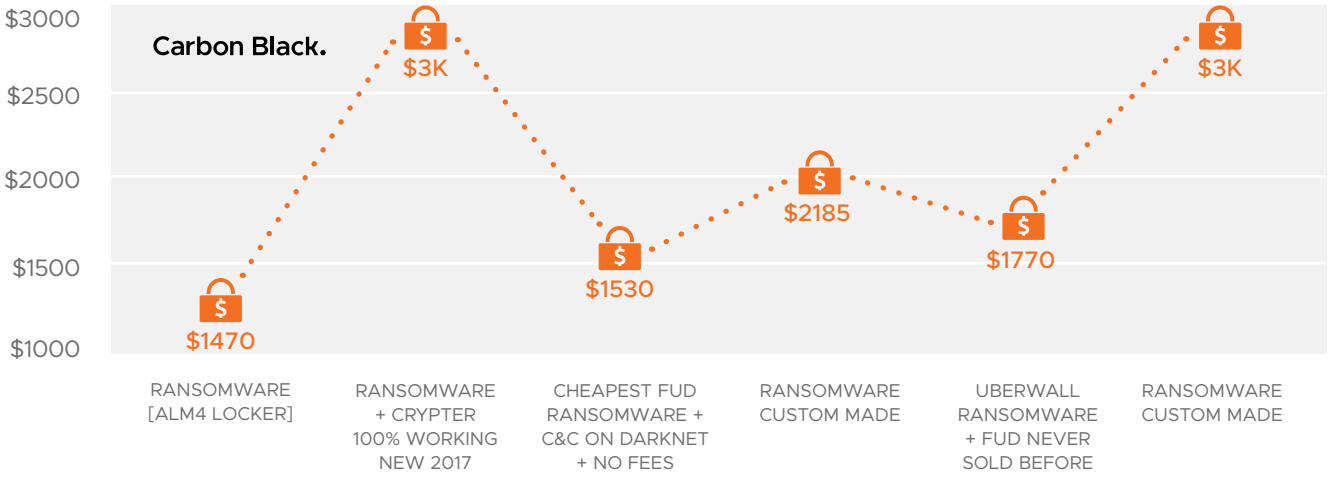
In aggregating all of the data from August and September, we found the ***median cost of a ransomware offering to be $10.50***

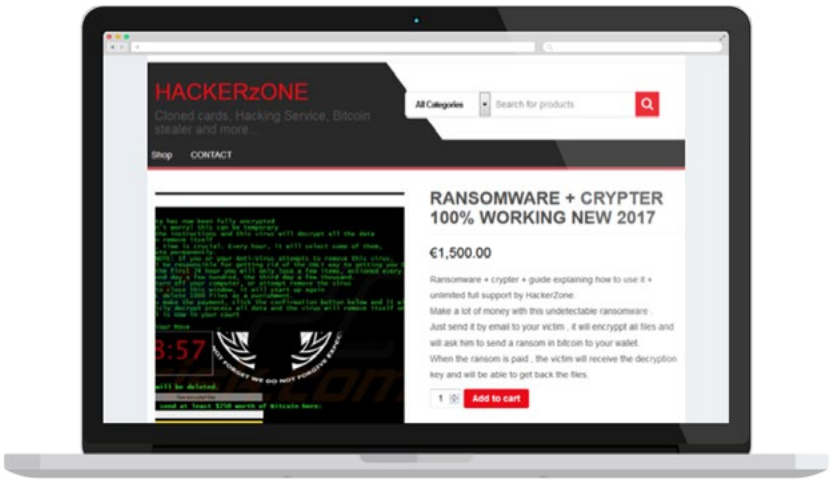
To the left are examples of a marketplace selling ransomware on the dark web



We found six listings with prices greater than $1,000. These listings are either custom-developed, unique code or have been seldom-deployed in the wild.

See below for ransomware offerings by price in USD





The higher asking prices suggest the sellers expect a high level of success for these specific products.

To the left is an example of a dark web marketplace selling a higher-end kit.

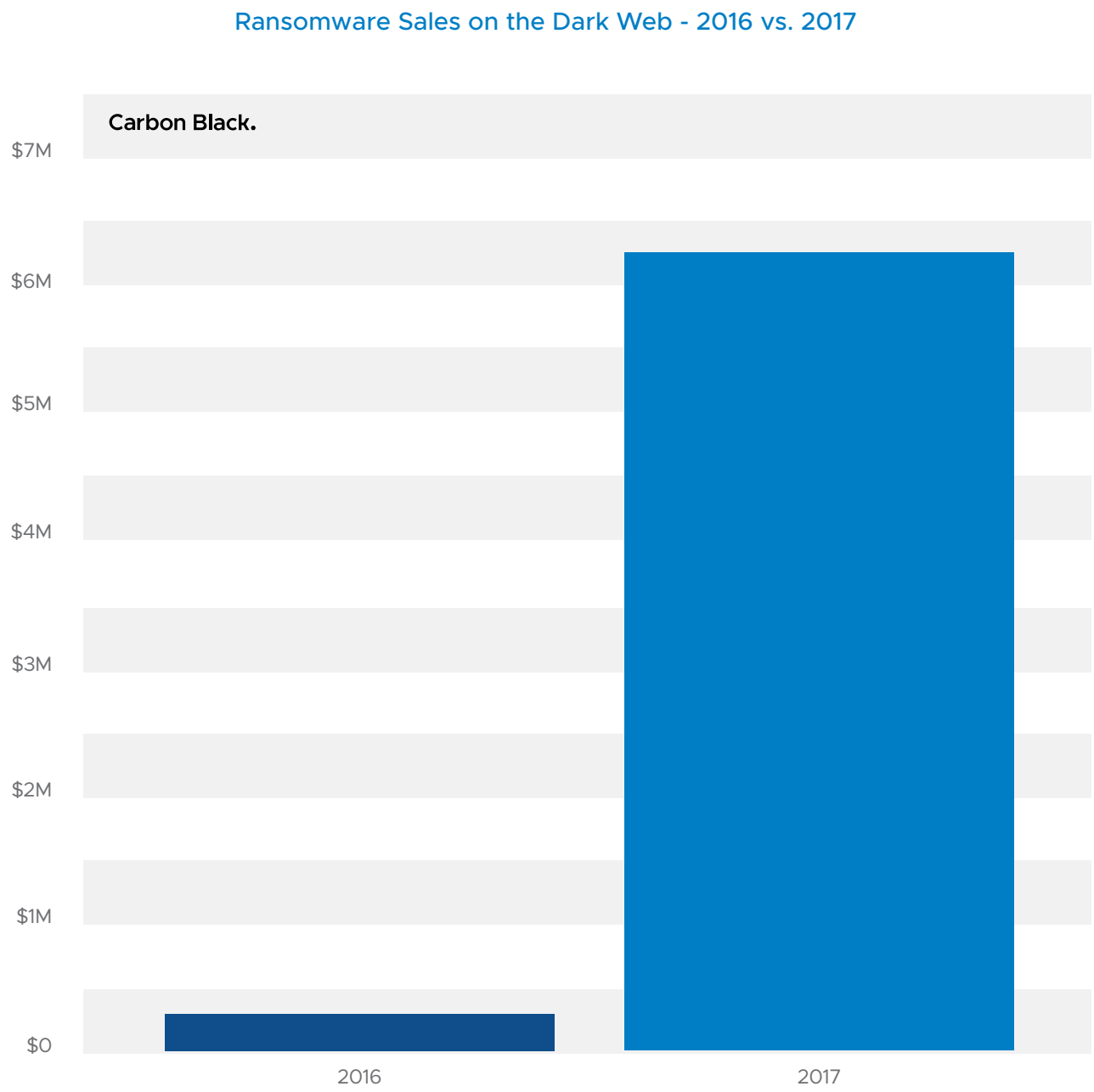
For ransomware authors, successful creation and selling of ransomware offerings appears to be fruitful. Based on our research, ***some ransomware sellers are making more than $100,000 per year simply retailing ransomware***. In some instances, this is double the salary for legitimate software developers, who pull in an average of $69,000 a year, according to PayScale.com. (In Eastern Europe developer salaries are a bit lower, hovering around $45,000.)

Ransomware developer salary vs legal software development by country is shown below[2]

[2]http://swexperts.com/news/software-engineer-salaries-by-country/

With the ability for ransomware authors to make more than $100,000 per year (and probably tax free), it comes as very little surprise that dark web underground economies are flourishing. Through a historical analysis of dark web database dumps, we were able to determine that ***the underground economy for ransomware has grown 2,502% in 2017 when compared to 2016.***

Shown below is a comparison of ransonware sales on the dark web in 2016 vs. 2017.



Underground Ransomware Market: Emergence and Innovation

The 2,502% growth in the dark web ransomware economy has been aided by:

1. Bitcoin and Tor, which allow for pseudo-anonymous activities.
2. Proliferation of service providers, which allow anyone to get in the business of ransomware.
3. A lack of fundamental security controls such as backups, testing, restoration, patching, visibility, and out-of-date prevention strategies.

While ransomware has existed for some time, the proliferation of Bitcoin and Tor have lowered the risk and driven down the barrier to entry for ransomware perpetrators. You no longer need to know how to anonymize your traffic or make and receive payments. These services already exist and can be purchased.

The availability of these services has allowed underground ransomware to hide effectively, making attribution and takedowns by law enforcement extremely difficult. If takedowns do happen, they happen over months or years of hard work.

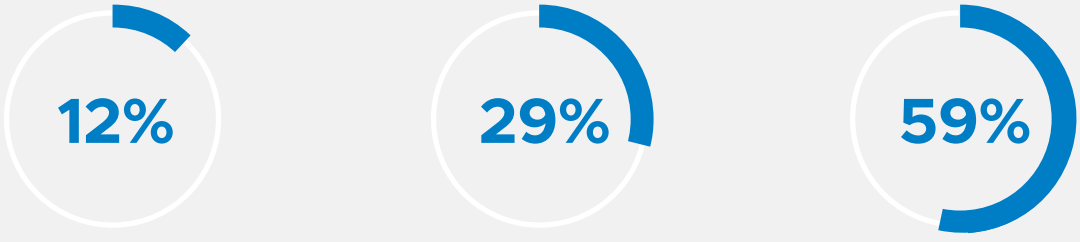
Not only have the dark web marketplaces evolved to better support high-risk, low-trust transactions through escrow systems, but the requirement for ransoms to be paid over the Tor network has ensured there's no centralized endpoint to investigate with traditional geo-based law enforcement approaches.

As a result of the maturity with these innovations, the underground ransomware economy is now an industry that resembles commercial software — complete with development, support, distribution, quality assurance and even help desks.

We should also consider consumers' willingness to pay ransoms. In a recent Carbon Black survey, we asked participants if they would personally be willing to pay ransom money if their personal computer and files were encrypted by ransomware. 52% said "yes."

Carbon Black.

How much money would you be willing to pay if your personal computer and files were encrypted by ransomware?



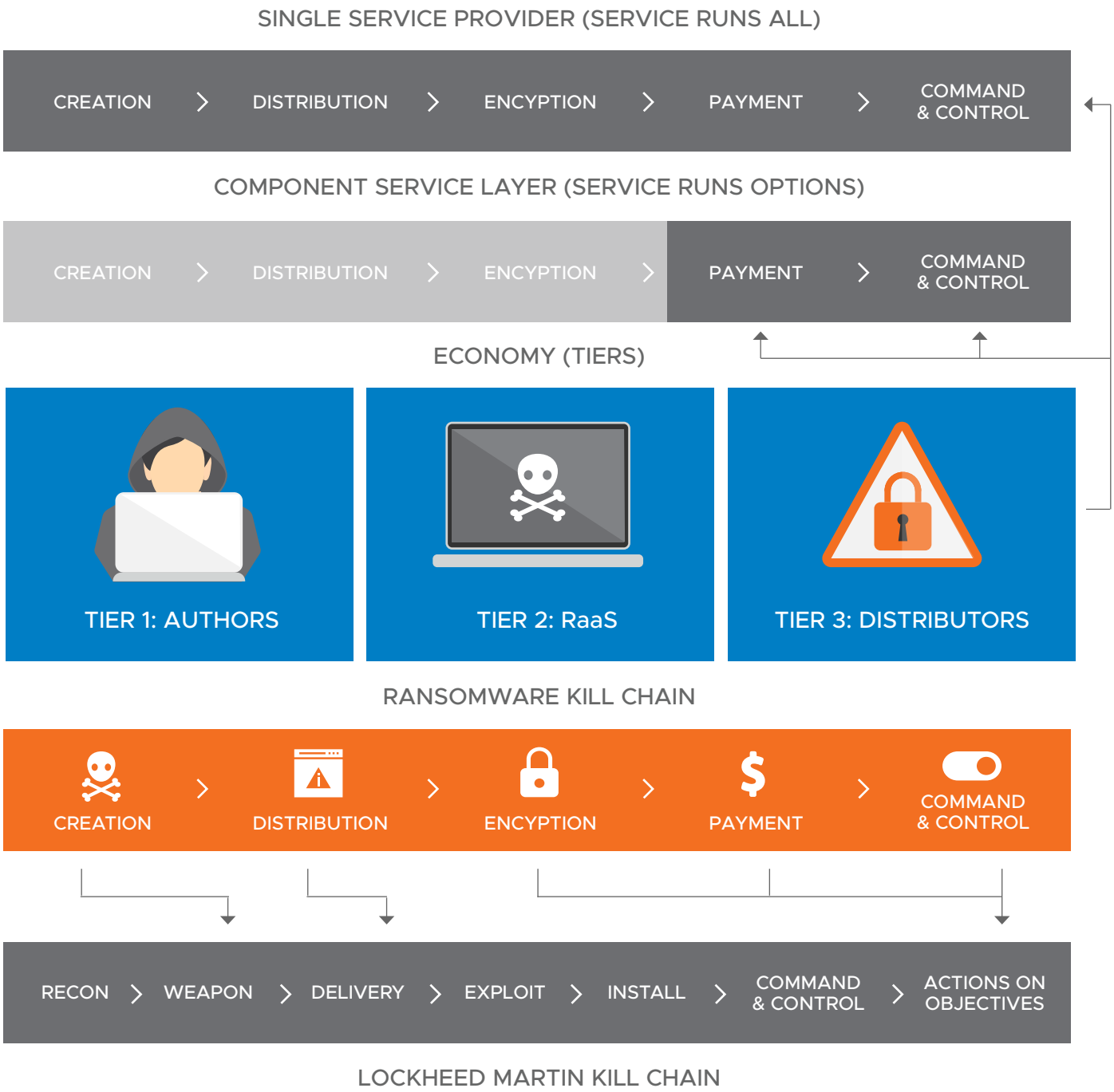
WOULD PAY $500 OR MORE TO GET THEIR DATA BACK

WOULD PAY $100-$500 TO GET THEIR DATA BACK

WOULD PAY LESS THAN $100 TO GET THEIR DATA BACK

The Underground Ransomware Economy and Supply Chain

Based on our research, the dark web ransomware market currently consists of the following tiers and players:



Carbon Black.

TIER 1: AUTHORS

Authors are responsible for:

1 – Creation of new ransomware for sale
2 – Advanced coding skills
3 – Training and support

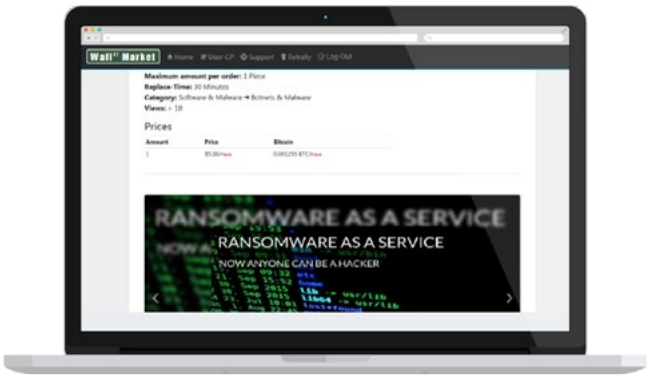
Think of authors as the "weapons makers." They never use what they create. They only sell their code. They also sell support or changes to the code.

Authors make money (sometimes $100,000+ per year, according to our research) by: selling the ransomware code itself; selling a platform to author code (for others who don't actually have coding skills); and / or teaching others to code.

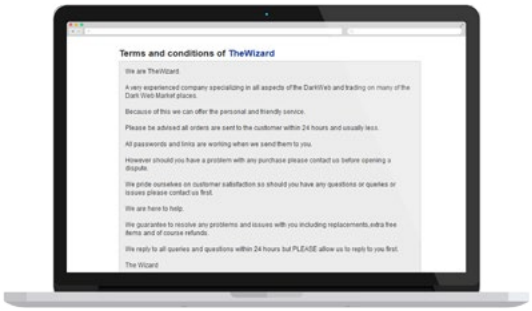
Authors can sell the specialized components of ransomware in the supply chain (creation, distribution, encryption, payment, C2) or they can sell an entire kit to a buyer. These kits contain everything you need to build and customize your ransomware.

TIER 2: RANSOMWARE-AS-A-SERVICE (RaaS)

In some cases, ransomware authors will stand up ransomware-as-a-service (RaaS) platforms. In others, buyers will purchase the platform from an author and stand up their own service.



In this area, a ransomware author might decide to begin an "affiliate" program to earn money while minimizing risk.



An "affiliate" will look to utilize existing infrastructure to achieve speed to market, minimize and share risk amongst affiliates, and provide target lists.

Here's how the process generally works:

1 – Distributors buy "shares" in a ransomware campaign. The revenue split is usually agreed upon at the beginning.

2 – The service owner embeds the split in their distribution servers. The distribution servers are then used to track the campaign (metrics, etc). In most cases, the revenue share favors the distributors because they do the distribution. The distributor takes on the most risk because they have to make changes to make the code less detectable and preventable.

3 – RaaS providers perform campaign tracking as a service, Bitcoin transaction monitoring and Bitcoin distribution.

Metrics from campaigns are used to make the next campaign more successful/profitable than the last one. (i.e. What country should we target based on pay rates?)

The service owners provide the necessary platforms and infrastructure to distributors.

There are two types of programs that exist. The "trusted-and-verified" distributor model, where someone knows you as a criminal and vouches for you. Think of this as the premium model.

The standard model is for anyone with a target list. (NOTE: Due to the success of ransomware-as-a-service, the third tier below is starting to collapse.)

TIER 3: DISTRIBUTORS

There is high profit but also high risk at this tier. Distributors are responsible for:

1 – Distributing ransomware themselves via spam campaigns, social engineering, targeted hacks or exploit kits.

2 – Leveraging ransomware-as-a-service. RaaS makes ransomware available to even novice criminals.

Carbon Black.

The Ransomware Supply Chain

The underground ransomware economy fosters some very profitable business models. To curb the proliferation of the economy, we must first understand the economics behind the model.

Most people think about ransomware monetization at only one point - where the criminal actually receives payment from a victim. This may be the one of the headlines, but it's actually at the tail end of the economy.

Here's what the "Ransomware Supply Chain" looks like:

RANSOMWARE CREATION

Ransomware is software. Someone has to create it, maintain it, test it. Sometimes, ransomware is created for the mass market and sometimes it is authored for targeted campaigns. The cost is based on how customized the code is for a particular target.

It's important to understand that the entire supply chain could be provided by one group or one person but it may also be piecemealed together. The trend continues toward DIY kits and specialization within the underground economy is further contributing to ransomware's boom.

RANSOMWARE DISTRIBUTION (SOCIAL ENGINEERING, SPAN, TARGETED HACKS, EXPLOIT KITS)

This is where most people encounter ransomware for the first time. This is generally done in a "spray-and-pray" fashion where attackers send the same malicious email to a giant list hoping a small percentage will click. Moving into 2018, ransomware will increasingly target businesses, as we saw with the WannaCry attacks in 2017. Perhaps more alarming is how WannaCry leveraged NSA tools to spread the attack across the globe.

ENCRYPTION / DECRYPTION

This is the module responsible for the activity on a system that actually encrypts the data. We've all seen the big, red splash screens commonly used in ransomware attacks. Ostensibly, once payment is rendered, the data is decrypted. For attackers, encryption and decryption tools can be purchased on their own, or as part of a DIY kit.

PAYMENT

This module facilitates, tracks and communicates payments, typically via Bitcoin. Service providers and distributors use this information to make future campaigns more successful.

COMMAND AND CONTROL

This module is responsible for the end-to-end operations of ransomware and is used to control infected hosts throughout the ransomware life cycle. These are becoming fairly standardized.

DEFENDERS' INHERENT ADVANTAGE

The silver lining when it comes to breaking the ransomware supply chain is that defenders have an inherent advantage. If defenders can break or interrupt even one link of the chain, the entire attack falls apart.

Taking down distributors and operators is chasing the tail of the problem. To begin to put a dent in the underground ransomware economy, efforts should be enacted to disrupt the supply chain upstream and change the incentive for malware authors. By decreasing the ROI for attackers, defenders can decrease the financial incentive for the crime.

Additionally, we need to STOP paying ransoms. The system only works if victims choose to pay. Until people decide not to pay, this problem will only continue to grow. Additionally, as it stands right now, law enforcement cannot scale to the problem. Companies are largely on their own when it comes to stopping ransomware attacks.

SPECIALIZATION IS DRIVING UNDERGROUND ECONOMIC GROWTH

The growth in the underground ransomware economy highlights a few unsettling trends. Namely, as an industry, we are often getting the fundamentals of security wrong. In too many instances, we are failing to do the basic blocking and tackling of security such as: backing up files and systems; testing restorations; patching; having adequate, enterprise-wide visibility; and implementing outdated prevention measures, such as legacy antivirus.

Attackers will continue to go where the money is. Right now, with ransomware, there is money to be made hand over fist. To begin to shift the economic tide, organizations should take careful inventory of their security best practices and look to implement user education programs in order to close any gaps that may exist.

In conjunction with user education, these organizations should turn to security software that can provide full visibility across the enterprise and prevent ransomware attacks before they cause any damage.

Specialization in the various components of ransomware has contributed to the 2,502% growth we've seen in the underground ransomware market over the past year.

For ransomware to be profitable, you no longer have to be "good" at the entire supply chain, just know where to purchase the individual components.

The economy itself has become so much more robust because of the now-existing service layers. These services drive down the barrier to entry and attackers no longer have to have multiple specializations. In fact you don't have to have any. You just need some Bitcoin. This enables anyone who is inclined to launch attacks.

Ransomware can no longer be perceived as small groups of criminals performing stick ups and kidnappings; instead think of ransomware more like the consumer of cloud service. You simply need to know how to put the pieces together. Startup CEOs no longer hire tons of IT staff or invest heavily in infrastructure. They achieve speed to market by utilizing existing services. So do cyber criminals. The criminals are jumping right to the point of profit.

Because of this specialization, ransomware attacks are more likely to succeed. The frequency and severity of the attacks will also increase. The power to attack is no longer in the hands of a few experts, but in the hands of anyone looking to make illicit money.

To begin to shift the economic tide, organizations should take careful inventory of their security best practices and look to implement user education programs in order to close any gaps that may exist.

Projections

As improvements in prevention models continue to hit the market, we expect threats to converge resulting in the underground market increasing the profit-sharing model and a consolidation and centralization of threats. This consolidation means ransomware strains may become fewer but more effective.

Some additional projections regarding ransomware as we move toward 2018:

1 – Based on the direction ransomware is trending, we believe ransomware will increasingly target Linux systems in an effort to further extort more money per infection. For example, attackers will increasingly look to conduct SQL injections to infect servers and charge a higher ransom price. We have already observed attacks hitting MongoDB earlier this year which provide excellent foreshadowing.

2 – Ransomware will become more targeted by looking for certain file types and targeting specific companies such as legal, healthcare, and tax preparers rather than "spray-and-pray" attacks we largely see now. There is already ransomware that targets databases, preying on businesses, and small tweaks to their code can target critical, proprietary files such as AutoCAD designs. A focused targeting of extensions can allow many ransomware samples to hide under the radar of many defenders.

3 – While most ransomware samples we analyzed in recent research simply encrypt files in place and transmit encryption keys for the purpose of decryption, there will be ransomware samples that will take the extra step of exfiltrating data prior to encryption. Not only would such an evolution put stress on companies to restore their data but also incorporate the loss of proprietary data that could be sold on the black market.

4 – Ransomware will increasingly be used as a smokescreen. For example, in the past, Zeus botnet operators hit victims with DDoS attacks after an infection to take investigators off the trail. A similar trend is emerging with ransomware attacks where the encryption of files could take place after more damning actions are taken by adversaries. Using already existing techniques of deleting Volume Shadow Copies, which deletes potential file backups, and the deletion of Windows event logs, adversaries can thwart many incident response efforts by forcing responders to focus on decrypting files instead of investigating data and credentials exfiltrated.

5 – Ransomware will emerge as a secondary method when initial forms of attack fail. Adversaries that rely upon more crafted and targeted attacks may use ransomware as an attack of last resort. Failing to entrench in an environment with a Remote Access Tool (RAT) or exfiltrate data, adversaries can push a ransomware across the environment to ensure at least a minimum return for their effort invested.

6 – Ransomware will be used more commonly as a false flag, as seen with NotPetya. Solely from dynamic analysis it was perceived to be Petya, when more detailed analysis showed it wasn't. Such quick analysis also insinuated it to be obvious ransomware, but a greater depth of disassembly showed that data was not held at ransom; it was simply destroyed.

7 – Ransomware will increasingly leverage social media to spread either intentionally or unintentionally. Similar to malware such as Koobface, maliciously shared content on sites such as Facebook could lead victims to click enticing links. Intentionally shared ransomware, seen in prior concepts, such as Popcorn Time where victims could share to reduce or eliminate their ransom, could see larger-scale use.

8 – Ransomware will start to morph to gain persistence on systems to re-encrypt them for more money some period of time later.

METHODOLOGY

During the months of August and September 2017, researchers monitored 21 of the largest dark web marketplaces for new virtual offerings related to ransomware. The description of the offering and sales price was recorded for each offering. To represent the complete dark web marketplace economy the sample of findings from 21 of the largest marketplaces was extrapolated to a population-wide value based on an assumption that approximately 25% (Wired, 2014) of the total darkweb website population (per Tor unique .onion observations/day reported at on the Tor Metrics site (https://metrics.torproject.org/hidserv-dir-onions-seen.html) is comprised of similar marketplaces. All prices and values are reported in USD. In instances where prices were offered in BTC (Bitcoin) conversion to USD was made for the day the offer was identified.

Historical information about the dark web marketplace activity for 2016 was developed through analysis of dark web database dumps. The sample size of sites analyzed for this historical perspective is approximately 10,000 .onion sites (20% of the dark web) as of February 2017.

The basic statistical model for generating point estimates based on samples collected. The number of observations in a period of time is multiplied by the total population and that product is divided by sample size (the population observed).

ABOUT CARBON BLACK

Carbon Black is the leading provider of next-generation endpoint security. Carbon Black's Next-Generation Antivirus (NGAV) solution, Cb Defense, leverages breakthrough prevention technology, "Streaming Prevention," to instantly see and stop cyberattacks before they execute. Cb Defense uniquely combines breakthrough prevention with market-leading detection and response into a single, lightweight agent delivered through the cloud. With more than 13 million endpoints under management, Carbon Black has more than 3,000 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks.

Carbon Black.

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com