
THE CHANGING STATE OF RANSOMWARE
F-Secure

Contents

What is Ransomware

Ransomware is a type of malicious application that steals control of the user's machine or data, then demands a payment to restore normal access to the ransomed content or system. It's nothing less than online extortion and has become increasingly popular amongst cyber criminals over the last few years.

Figure 1: Screenshots of ransom notes left by WannaCry (left) and Locky (right)

Who does Ransomware Target

Ransomware's popularity over the past two years has made it a significant threat to both individuals and companies. Ransomware campaigns have historically been opportunistic in nature, infecting anyone they can via spam emails, exploit kits and malvertising. But many cyber criminals are becoming more selective in their targets, and tailor their techniques to infect businesses or other organizations.

Targeting organizations is fairly lucrative compared to infecting individual users because ransoms are typically set per device. A 2016 F-Secure investigation of five ransomware families found that initial ransoms ranged from 150-1900 dollars (payable in bitcoin).[1] While an individual's device may only cost the equivalent of a few hundred dollars to decrypt, attackers can extort tens of thousands of dollars or more from an organization.

Furthermore, ransomware infections can often jeopardize a company's business interests, making it easier for criminals to pressure them into paying ransoms. Many organizations depend on their documents, databases, and IT systems to operate. And in some cases, they'll have legal obligations to manage and protect data provided to them by customers. These reasons increase the pressure on organizations to resolve ransomware infections quickly and quietly by paying the ransom.

Several studies have found that many organizations end up paying the ransom. According to a 2017 study from Australian telecommunications company Telstra, approximately 57 percent of businesses in the Asia-Pacific region dealt with ransomware infections by paying.[2] A similar study published in 2016 found that 70 percent of organizations paid.[3] But some estimates are more conservative, with a 2018 survey finding that only about 40 percent of companies paid the ransom (with only about half of those getting their data back).[4]

While it may be difficult to know for certain how often ransoms are paid, estimates suggest that the "ransomware industry" is now inflicting billions of dollars in damage on companies.[5] Some of the more successful ransomware families generate millions or even hundreds of millions of dollars in revenue for cyber criminals.[6] These figures confirm that ransomware's business model is a profitable method of online extortion, and help explain why ransomware has been such a prevalent threat in the last two years.

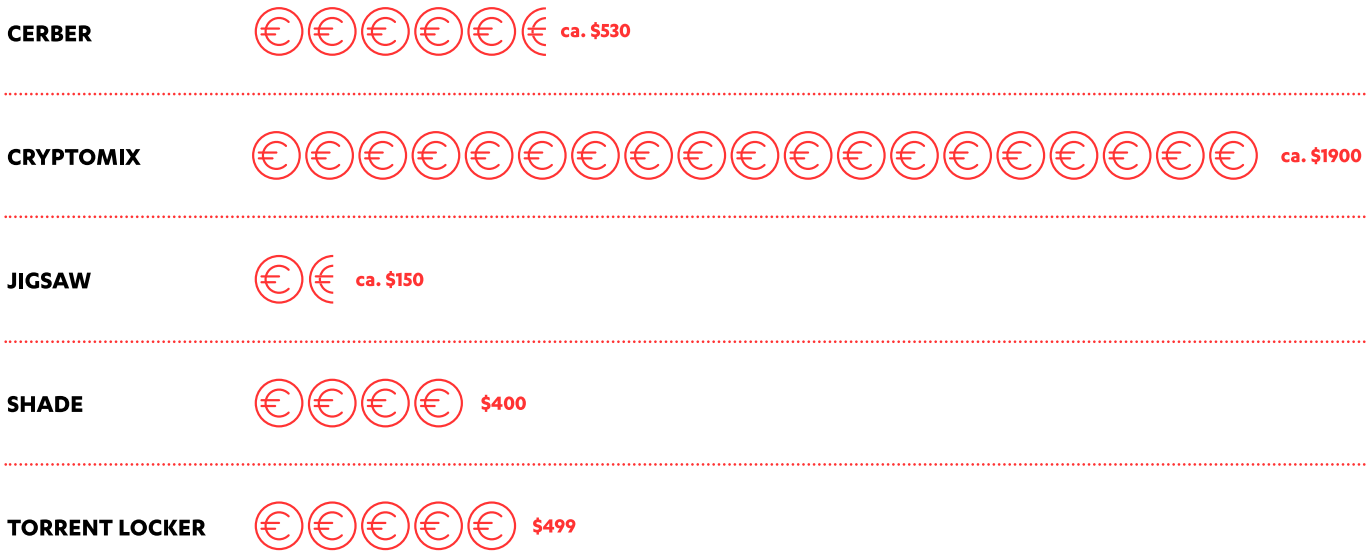

Figure 2: F-Secure researched the "customer journey" of ransomware victims in 2016 and found that initial ransoms ranged from 150-1900 (payable in bitcoin)

How the Ransomware Threat Developed

While ransomware has existed since 1989, the past few years have seen a steady increase in both the number of ransomware families used by cyber criminals and the number of attacks. There was only one ransomware family discovered in 2012. In 2016, approximately 200 new ransomware families or unique variants were discovered. 2017 saw the trend continue with the emergence of 343 new types of ransomware – a 62 percent increase over the previous year.

The number of unique variants and families is significant for defenders as different ransomware families have characteristics that can make them more or less effective. For example, many ransomware families will attempt to pressure victims into paying quickly by setting a deadline (such as Cryptomix), with some of them (such as Jigsaw and BitKangoroo) even selectively deleting files at regular intervals to instill a sense of urgency regarding the payment.

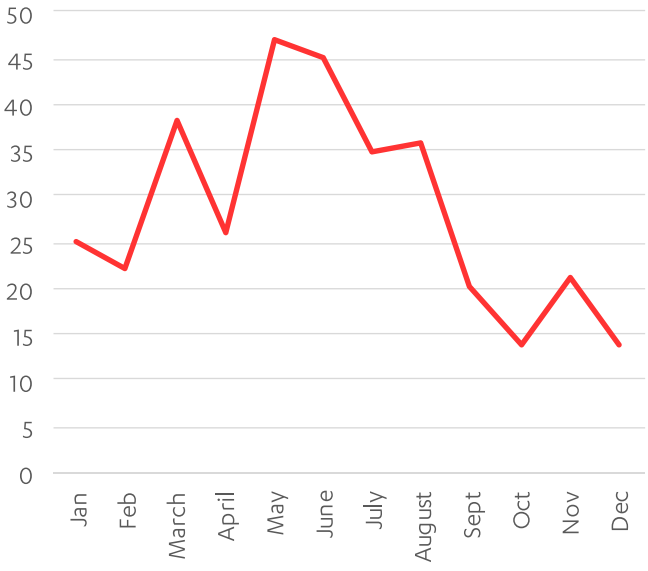

Figure 4: # of unique ransomware families/unique variants per month in 2017

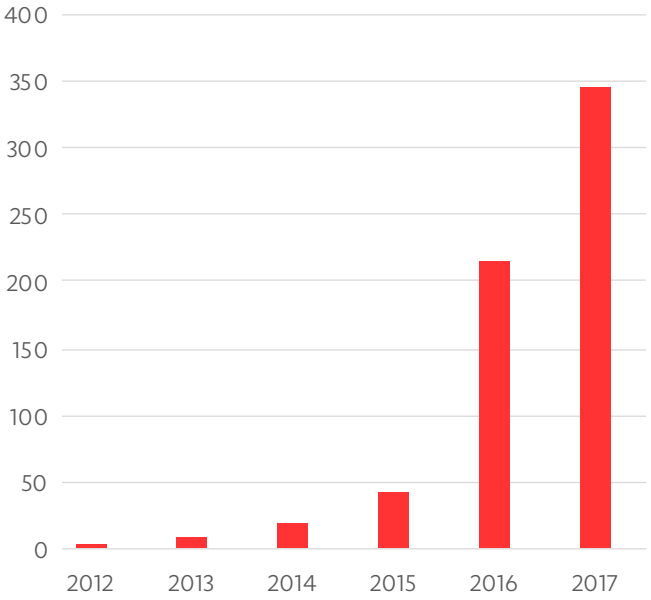

Figure 3: # of unique ransomware families/unique variants per year

One reason ransomware development has increased so dramatically (in addition to its popularity) is the degree of support it's received from cyber criminals. The availability of ransomware-as-a-service offerings (such as Cerber and Satan) and open source projects (such as HiddenTear and EDA2) make ransomware accessible to attackers that lack the skills or resources to develop their own malware from scratch. And supporting infrastructure, such as exploit kits and spam services, are readily available for rent or purchase by these adversaries.

The year-over-year trend shows a clear increase in the different families and variants of ransomware developed. But a closer look at 2017 reveals that these activities actually began to decrease toward the end of the year. It's difficult to say for certain whether this trend will continue. But in spite of the wide variety of ransomware present in the threat landscape, the majority of attacks involve only a small handful of families.

Ransomware Attacks in Numbers

According to ransomware detection reports compiled from F-Secure Labs' upstream telemetry, ransomware attacks have increased sharply since 2015. 2017 saw the number of ransomware detection reports increase by 415 percent compared with the previous year. The increase was driven by May's WannaCry outbreak, which saw the ransomware quickly spread through networks thanks to its worm-like propagation method and exploitation of a vulnerability present in nearly all versions of Windows.[7]

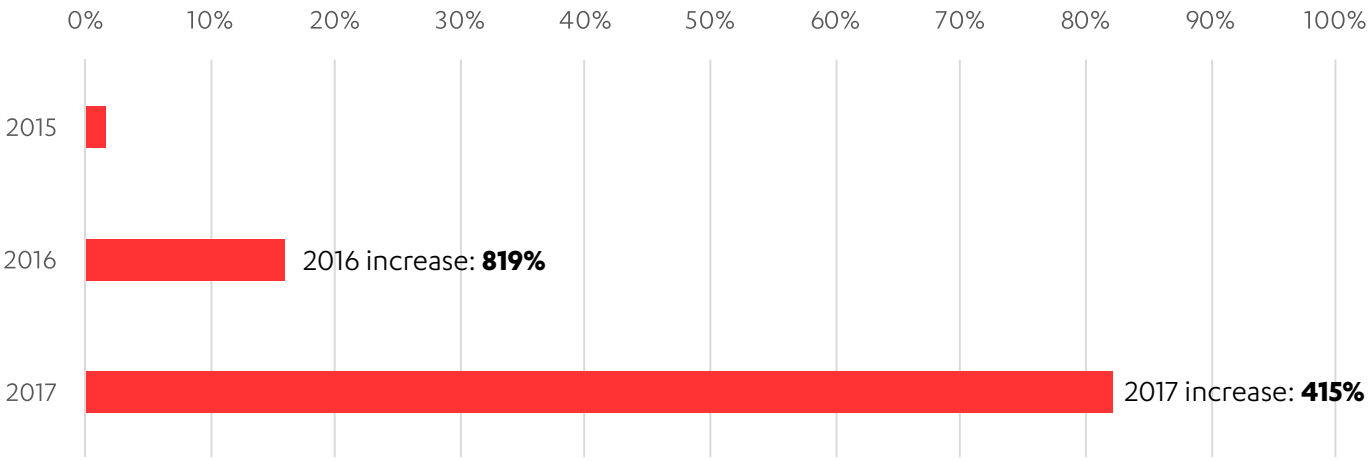

Figure 5: # of detection reports per year based on percentage of total # of ransomware detections from 2015-2017

2015	2016	2017
Browlock	Locky	WannaCry
Cryptowall	TeslaCrypt	Locky
Crowti	Cerber	Mole

Figure 6: Top Ransomware Families per Year

While many people may have had only a passing familiarity with ransomware before WannaCry, it's a threat that's been trending upward for years. The Locky ransomware family first appeared in early 2016[8] and contributed significantly to ransomware's growing prevalence. Locky was a prominent threat for much of 2016 and 2017 thanks to its regular use in large spam campaigns.[9] Its activity seemed to peak in a July 2016 with spam campaigns that triggered over 120,000 hits per hour — over 200 percent more than what's seen on a normal day. [10]

Locky accounted for nearly 60 percent of all ransomware attacks reported in F-Secure Labs' telemetry in 2016. And while it remained prevalent throughout much of 2017, it was quickly overshadowed by WannaCry after the latter's May 2017 attack.

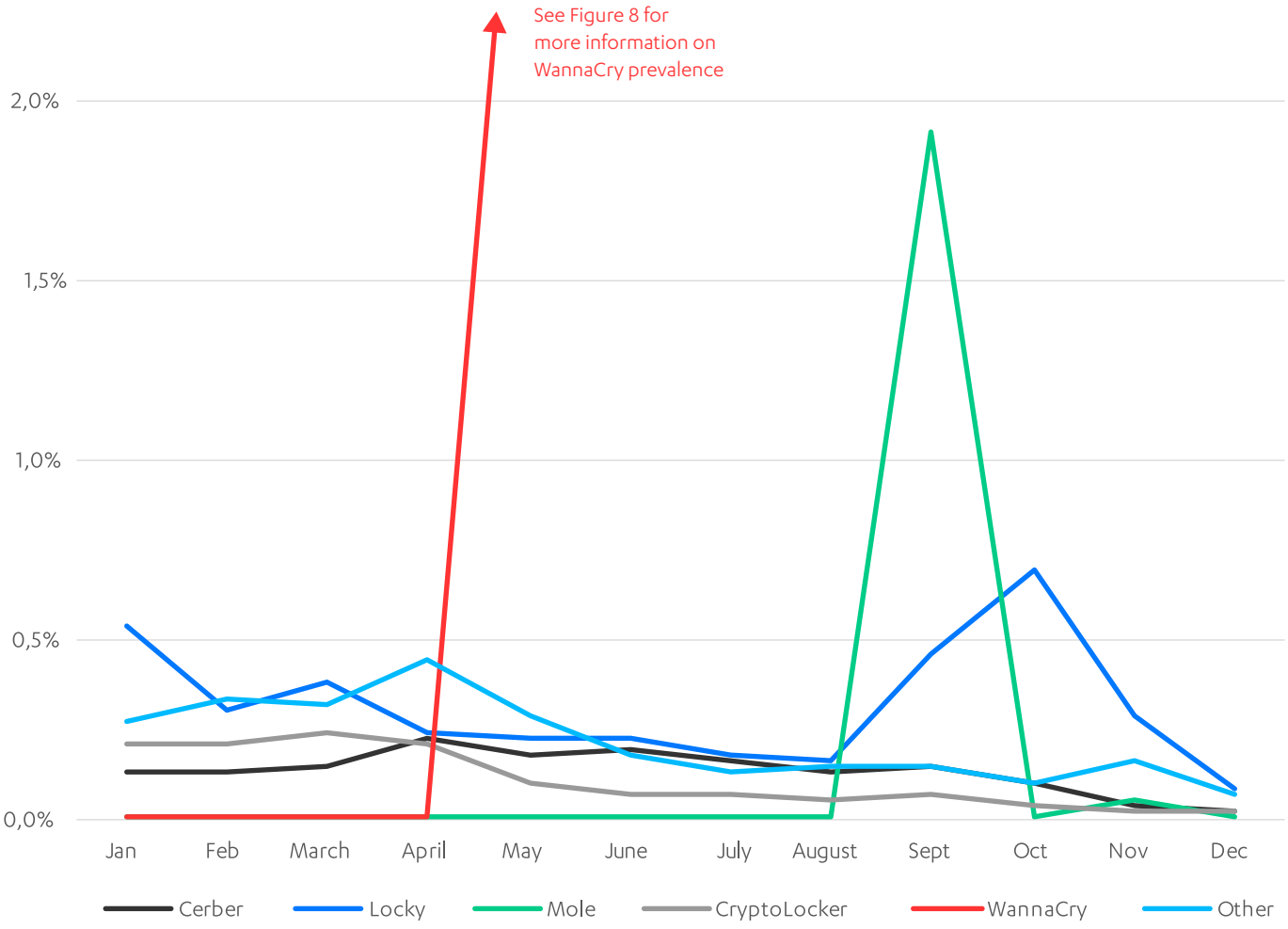

Figure 7: # of detection reports for specific ransomware families/unique variants based on percentage of total # of ransomware detections in 2017

While well-known ransomware families like Locky, Cerber, and Cryptolocker were prevalent in 2017, their use seemed to decline as the year progressed. Notable Locky and Mole campaigns were detected in Fall 2017, but those, as well as the ongoing prevalence of WannaCry thanks to its worm-like qualities, were exceptions to a general reduction in the volume of ransomware attacks seen as the year progressed.

Several factors are playing a role in this trend. The most significant is the price of bitcoin. Bitcoin's value increased considerably in 2017[11] , fueling speculation in other cryptocurrencies. Cyber criminals are responding to this trend by gravitating toward crypto mining as a way to make money, including by spreading crypto mining malware that covertly steals CPU cycles in order to process cryptocurrencies.[12] This scheme draws considerably less attention than ransomware, and can prove lucrative if cryptocurrencies increase in value.

Other factors influencing the trend include the continuing decline of exploit kits as an attack vector, massive fluctuations in the value of bitcoin creating logistical difficulties in setting and collecting ransoms, and industry initiatives such as The No More Ransom Project[13] increasing awareness about the threat and making decryption tools accessible to victims.

However, there are already signs that ransomware attacks are migrating to more targeted methods, which would make ransomware less prominent in the overall threat landscape while still a significant concern for companies. While WannaCry was incredibly prevalent, its spread via SMB ports ensured that the threat was focused on organizations. Ransomware spreading via exposed, compromised RDP ports is no longer uncommon, and is an attack vector that allows criminals to focus on the quality rather than quantity of targets in the hopes of getting a better payday.

WannaCry's the new Downadup

WannaCry is the family behind May 2017's global ransomware pandemic, which is now recognized as the largest ransomware outbreak in history.[14] While the initial wave of infections was quickly rendered inert with the discovery of an apparent "kill switch",[15] it did not actually stop the malware from spreading.

Historically, prevalent ransomware threats have spread via spam campaigns, exploit kits, or malvertising. These attack vectors spread ransomware opportunistically and affect any user unfortunate enough to click the wrong link or open a malicious email attachment. But WannaCry spread like a computer worm via vulnerable SMB ports – it would infect one device, and then automatically spread itself through networks to infect more. The more hosts it infects, the faster it spreads. This helps explain why it was able to infect so many organizations so quickly last May.

Worms are notoriously difficult to eradicate, and a small number of machines hosting the malware result in repeated infection attempts in the surrounding network(s), creating significant IT problems for organizations. That's why threats like the Downadup/Conficker worm – which was first encountered nearly ten years ago – still attempts to infect millions of devices per year.[16]

As seen below, WannaCry's prevalence in F-Secure's upstream telemetry shows it dominating all other ransomware families. By the end of the year, 9 out of every 10 ransomware detection reports received was WannaCry.

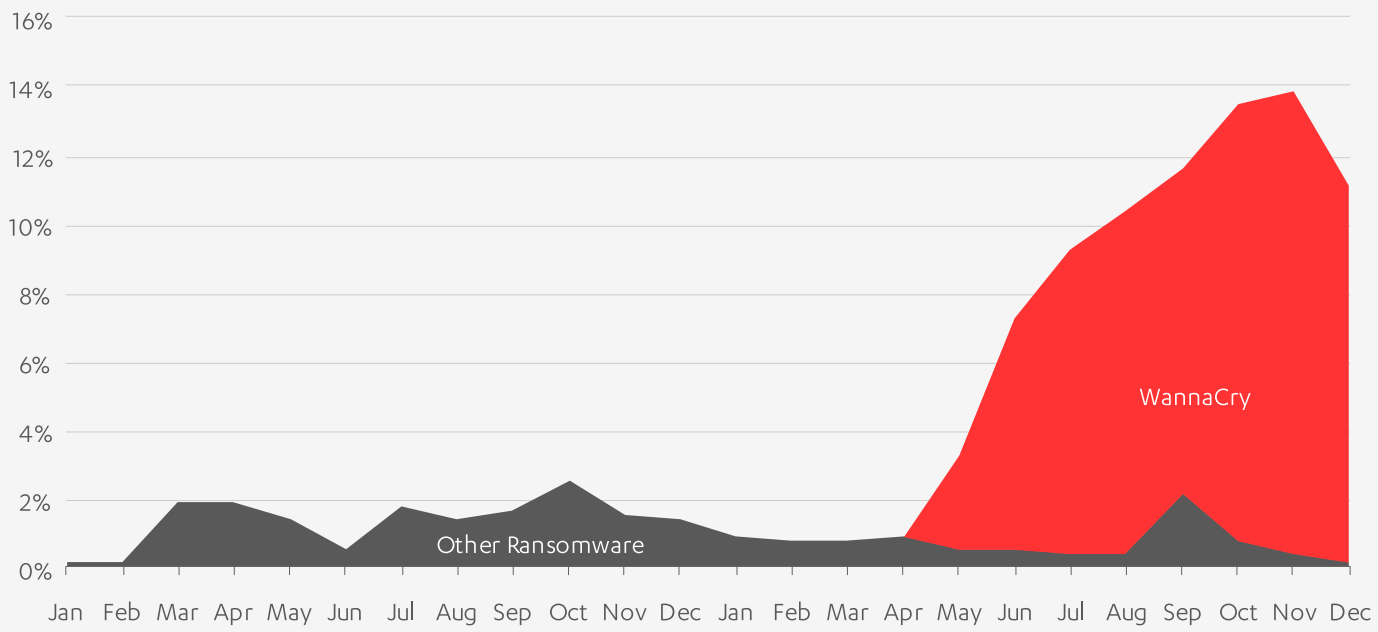

Figure 8: comparison between # of detection reports for WannaCry vs. other ransomware based on percentage of total # of ransomware detections in 2016-2017

While WannaCry's ongoing prevalence may surprise some, it's important to note that the months following May's outbreak saw numerous variations of the malware begin to circulate. Some variants retained WannaCry's propagation method without actually encrypting the files,[17] making the impact less noticeable for victims. But these variants still inflict damage in the way of downtime and service outages due to the worm's bandwidth consumption.

The vast majority of the WannaCry detection reports in 2017 came from countries in Asia. But reports of recent WannaCry infections in the US states of Connecticut[18] and North Carolina[19] confirm that it is alive and well in other parts of the world.

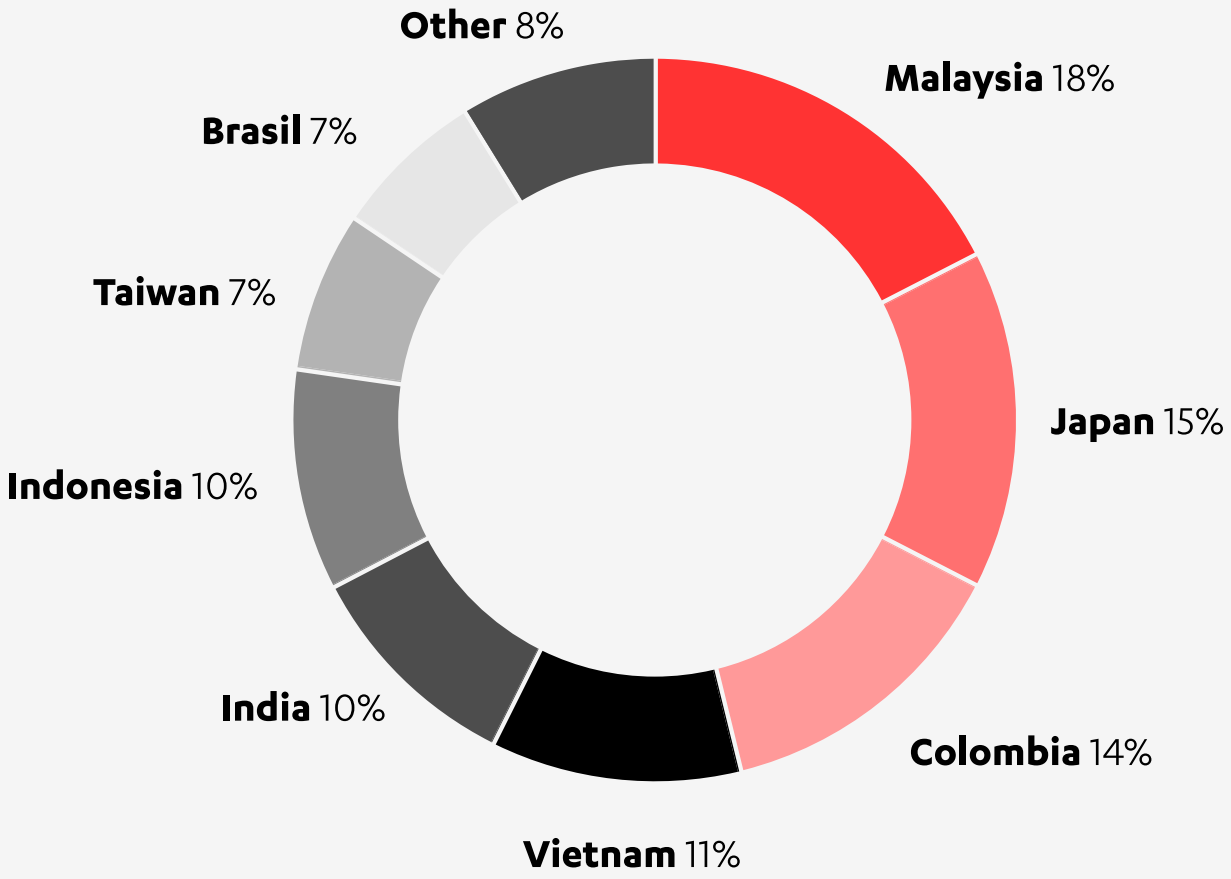

Figure 9: WannaCry detections per country

Getting rid of a worm is difficult but organizations can combat the threat by configuring their firewalls to limit the spread. In the case of WannaCry, this means preventing workstations from accepting inbound traffic through ports 135, 137, 138, and 445 (unless required for a specific service), and blocking all outbound traffic coming from servers.

Patching oudated software is another key preventative measure. But WannaCry's continued prominence in detection reports shows that there's no shortage of unpatched machines vulnerable to attacks leveraging the same SMB vulnerability as 2017's WannaCry and NotPetya outbreaks.

Beyond the Trends

There's no question that 2017 was a milestone year for ransomware. The raw number of attacks spiked thanks to notorious incidents such as the WannaCry, NotPetya,[20] and Bad Rabbit[21] outbreaks. A statement from the US White House went as far as calling the NotPetya outbreak "the most destructive and costly cyber-attack in history."[22] And as discussed earlier, many cyber criminals attempted to cash in on the trend with new families and variants of ransomware. These are just a few of the reasons why ransomware's reputation as a severe threat to people, organizations, and the general public is well earned.

But some of ransomware's most notable developments aren't reflected in these trends. Cyber crime in general is often most "successful" when it achieves something seen as an exception to a rule. So while threats like WannaCry and Locky dominate prevalence statistics, they are arguably not ransomware's biggest "success" stories. For example, in June 2017 a South Korean web hosting company paid a one million dollar ransom to cyber criminals after falling victim to a Linux variant of the Erebus ransomware[23] – a rarity given that the vast majority of ransomware targets Windows.[24] That approach seems far more lucrative than WannaCry, which earned about $140,000 US for its attackers in spite of it's vast reach and notoriety.[25]

In fact, WannaCry and NotPetya's legacies focus more on the disruptive nature of these threats rather than their fiscal achievements. Its completely possible that these incidents could discourage others from conducting ransomware attacks in the long term: in both cases paying the ransom was unnecessary for victims (WannaCry's encryption process was killed and payment did not result in decryption for NotPetya). So if WannaCry and NotPetya publicized that victims don't necessarily get their data back by paying, why would future victims bother? And if these crimes don't pay, why would criminals continue to commit them?

There are many different ways people and companies can protect themselves from ransomware. The good news is that there are many ways to combat ransomware.[26] The bad news is that someone will always be vulnerable to ransomware attacks and pay to get their data back. Until this changes, everyone should continue to back up their files and practice restoring them to avoid playing into the hands of online extortionists.

References

1 https://fsecureconsumer.files.wordpress.com/2016/07/customer_journey_of_crypto-ransomware_f-secure.pdf
2 https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf
3 https://www.infosecurity-magazine.com/news/70-of-businesses-pay-up-to/
4 https://www.bleepingcomputer.com/news/security/only-half-of-those-who-paid-a-ransomware-were-able-to-recover-their-data/
5 https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
6 https://www.theregister.co.uk/2016/01/13/ransomware_for_next_tech_unicorn_firm/
7 https://labsblog.f-secure.com/2017/05/15/wannacry-party-like-its-2003/
8 https://labsblog.f-secure.com/2016/02/22/locky-clearly-bad-behavior/
9 https://labsblog.f-secure.com/2017/11/23/necurs-business-is-booming-in-a-new-partnership-with-scarab-ransomware/
10 https://labsblog.f-secure.com/2016/07/13/a-new-high-for-locky/
11 http://nordic.businessinsider.com/bitcoin-price-in-2017-review-2017-12
12 https://www.youtube.com/watch?v=TP3gA6NRtN4
13 https://www.nomoreransom.org/en/index.html
14 https://safeandsavvy.f-secure.com/2017/05/12/wannacry-may-be-the-biggest-cyber-outbreak-since-conficker/
15 https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
16 https://www.cyberscoop.com/conficker-trend-micro-2017/
17 https://safeandsavvy.f-secure.com/2017/05/18/wannacry-now-hitting-asia/
18 https://www.scmagazine.com/wannacry-hits-12-connecticut-state-agencies/article/746764/
19 http://www.healthcareitnews.com/news/new-wannacry-variant-takes-down-north-carolina-provider
20 https://labsblog.f-secure.com/2017/06/29/petya-i-want-to-believe/
21 https://labsblog.f-secure.com/2017/10/26/following-the-bad-rabbit/
22 https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/
23 https://www.bleepingcomputer.com/news/security/south-korean-web-hosting-provider-pays-1-million-in-ransomware-demand/
24 https://www.techrepublic.com/article/report-99-of-ransomware-targets-microsoft-products/
25 https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/
26 https://www.f-secure.com/documents/996508/1030745/Ransomware_how_to_ppdr.pdf