CTNT REPORT

Malwarebytes

CYBERCRIME TACTICS AND TECHNIQUES:

Ransomware Retrospective

August 2019

Executive summary

> Another quarter, another quarterly cybercrime report—our eleventh to date. However, unlike past CTNTs (as we affectionately call them in-house), this time we are zeroing in on a single threat and peeling back its layers to reveal how it has evolved over the last couple years, from attack methods cybercriminals use to the targets they choose to victimize. We'll look at global consumer and business detections, the families within this threat doing the most damage, regional threat analysis, the most heavily-attacked countries, and even the top US states. So, sit back, relax, and grab some popcorn as we dig into this special ransomware edition.

Oh yes, we said ransomware. This once dangerous-but-recently-dormant threat has come back to life in a big way, switching from mass consumer campaigns to highly-targeted, artisanal attacks on businesses. Cybercriminals looking for a bigger bang for their buck have been busy exploiting weak infrastructure and poorly-constructed operational security to encrypt business-critical data for larger payouts, and organizations have been largely caught with their virtual pants down. As we examine ransomware inside-out, looking at the influence of older players on the market and the trajectory of today's most influential ransomware families, we will also look to the future of this threat, considering where ransomware will go next—and how it will get there. Be on the lookout for our quarterly predictions, ransomware-style.

The statistics, graphs, and charts we created for this report were derived from our own telemetry obtained from users of our business and consumer products, reaching back as far as 2016, but largely focused on the last year—from Q2 2018 through Q2 2019. We've made some modifications to normalize the data and allow for better trend identification, utilizing more percentage increases and decreases than previous reports, as these show with more accuracy the peaks and valleys observed within our detection telemetry. Samples used for the creation of said telemetry were obtained from internal malware-hunting sources, such as honeypots and collection systems, as well as manual collection by our researchers. In addition, we've combined the observations, experience, and theories of our intelligence and research departments with collected telemetry to paint a more accurate picture of the threat landscape, and derive meaningful analysis of campaign activity and detection trends.

We hope you enjoy this special ransomware retrospective as much as we enjoyed creating it.

Key takeaways

- Over the last year, we've witnessed an almost constant increase in business detections of ransomware, rising a shocking 365 percent from Q2 2018 to Q2 2019. Meanwhile, consumer detections of ransomware have been on the decline, decreasing by 12 percent year over year and 25 percent quarter over quarter. The reason behind this shift: Cybercriminals are searching for higher returns on their investment, and they can reap serious benefits from ransoming organizations over individuals, who might yield, at best, a few personal files that could be used for extortion or identity theft. Encrypting sensitive proprietary data on any number of endpoints allows cybercriminals to put forth much larger ransom demands while gaining an exponentially higher chance of getting paid.

- Ransomware attacks featuring targeted campaigns against cities and municipalities, like those experienced in Baltimore, Florida, and Georgia, have increased in frequency, especially since the beginning of 2019. Ransomware families such as Ryuk and RobinHood are mostly to blame, though SamSam and Dharma also made appearances. Recovery from those attacks has been slow and painful, with critical infrastructure a problem. Healthcare and education, two industries also plagued with legacy infrastructure, were also targets.

- The ransomware families causing the most trouble for businesses this quarter were Ryuk and Phobos, which increased by an astonishing 88 percent and 940 percent over Q1 2019, respectively. GandCrab and Rapid business detections both increased year over year, with Rapid gaining on Q2 2018 by 319 percent. However, business detections of GandCrab slowed down by 5 percent in Q2 2019 over Q1.

- All of the top five ransomware families for consumers decreased in Q2 2019 from Q1. The family that saw the largest decrease quarter over quarter was Rapid, which fell by 57 percent in Q2, with a year over year decline of 30 percent. In fact, the only ransomware family that saw any kind of increase was Troldesh, which rose by 162 percent over the same time period in 2018, but still declined from Q1 by 55 percent.

- Looking at ransomware attacks by region—North America; Latin America; Europe, the Middle East, and Africa; and Asia Pacific—nearly half of all ransomware detections in the last year occurred in North America. Europe, the Middle East, and Africa netted 35 percent of our ransomware detections, while Latin America yielded 10 percent and Asia Pacific 7 percent. Each of the regions were plagued with high percentages of GandCrab detections, but Ryuk gave GandCrab a run for its money in North America.

- As for leading ransomware countries, the United States took home the gold with 53 percent of all detections from June 2018 through June 2019. Canada came in a distant second with 10 percent, and the United Kingdom and Brazil followed closely behind, at 9 percent and 7 percent, respectively. The remaining 21 percent was shared between Italy, France, Russia, Germany, South Africa, and Spain. Once again, GandCrab and Ryuk made the most noise in the countries we studied; however, certain families made significant impressions, such as Troldesh on Russia.

- Texas, California, and New York were the top three states infected with ransomware, ganged up on with a combination of GandCrab, Ryuk, and Rapid, which made up more than half of the detections in these states. Interestingly, the states with the most ransomware detections were not always the most populous. North Carolina and Georgia rounded out our top five ransomware states, but they are not as heavily-populated as Florida or Pennsylvania, neither of which made our list.

Ransomware shifts to businesses

In 2016, ransomware was primarily a consumer problem. With families like Cerber and Locky targeting users via drive-by exploits and the use of widespread phishing campaigns, cybercriminals held countless home systems for ransom. These threats did not single out targets; they simply blanketed the landscape with mass campaigns, and those who fell victim just happened to be in the wrong place at the wrong time.

	2017 Q4	2018 Q1	2018 Q2	2018 Q3	2018 Q4	2019 Q1	2019 Q2
Consumer	55%	-13%	-1%	22%	-16%	-34%	-16%
Business	2%	22%	-66%	23%	393%	152%	263%

Figure 1. Decline in consumer ransomware vs. increase in business ransomware

Today, consumers aren't pressured with the same relentless onslaught of ransomware attacks as they were in 2016. This is because cybercriminals have decided to pull back on targeting home computers to instead focus on endpoints plugged into larger networks of sensitive and proprietary data. To this end, from 2018 to 2019, we saw a 235 percent increase in threats aimed at organizations from enterprises to small businesses, with ransomware as a major contributor. Education, healthcare, and government are particularly at risk.

To illustrate these changes in focus by the criminals behind today's ransomware campaigns, Figure 1 shows total percentage increases and decreases of ransomware focused against consumers and larger organizations or business detections.

Starting from the first quarter of 2018, ransomware aimed at consumers started to decline, gaining significant downward momentum by the second half of the year. The initial decline was primarily due to the shift away from traditional malware in favor of pushing cryptominers, though this trend did not last long.

Figure 2 graph on page 5 expresses the overwhelming difference between consumer and business detections of ransomware as far back as June 2018. As we approached Q2 2019, consumer detections were poised to dip below business detections of ransomware for the first time, an expression of lost interest from cybercriminals

Ransomware Target Focus 12 Month View | June 2018 - June 2019

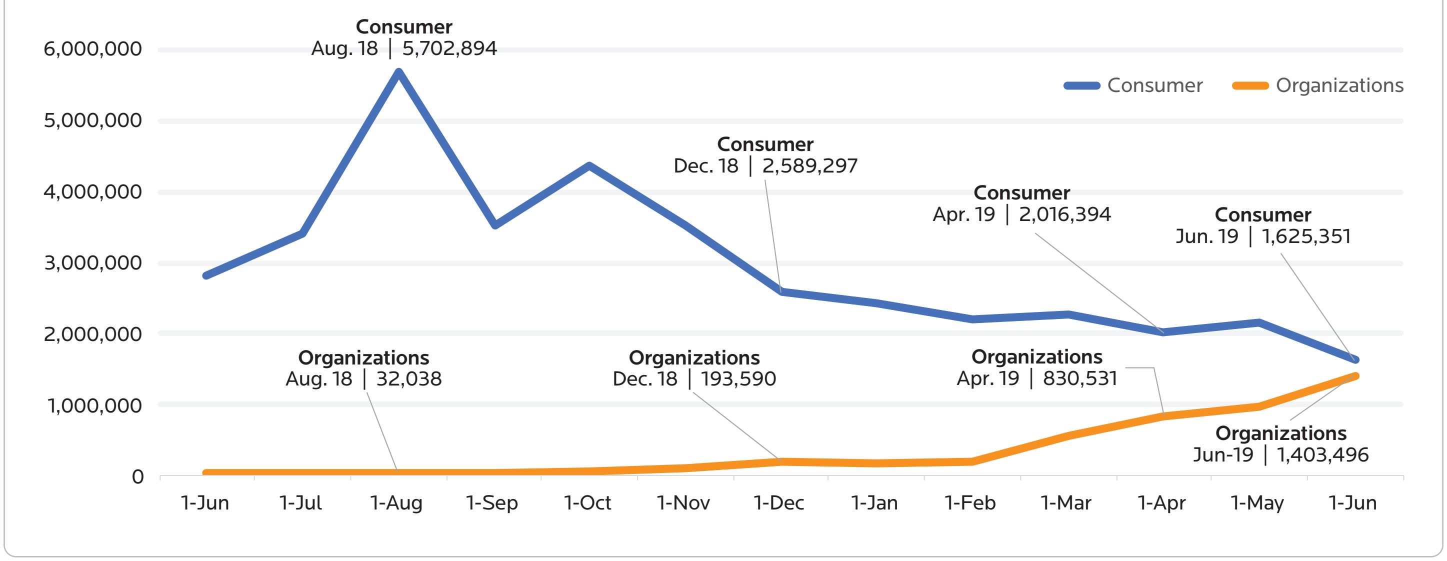


Figure 2. Ransomware target shift from June 2018 to June 2019

on individual targets. In the same vein, the rise of business detections starting around the beginning of 2019 showed the new focus of threat actors on organizations.

Never before have we observed such a similar number of ransomware detections for businesses and consumers; this is a shining example of the new ransomware reality security researchers and system admins will need to deal with in the coming quarters.

While the previous graph charted the shift in criminal focus from consumer to business by overall detection numbers, Figure 3 compares consumer and business detections by percentage quarter over quarter, demonstrating that as far back as Q4 2017, threat actors were turning their attention to organizations. As percentage changes for consumer-focused threats remained relatively negative throughout 2018 and 2019, the increase in the percentage of business-focused ransomware shot

Ransomware Detections Percentage Comparison by Quarter | Q4 2017 - Q2 2019

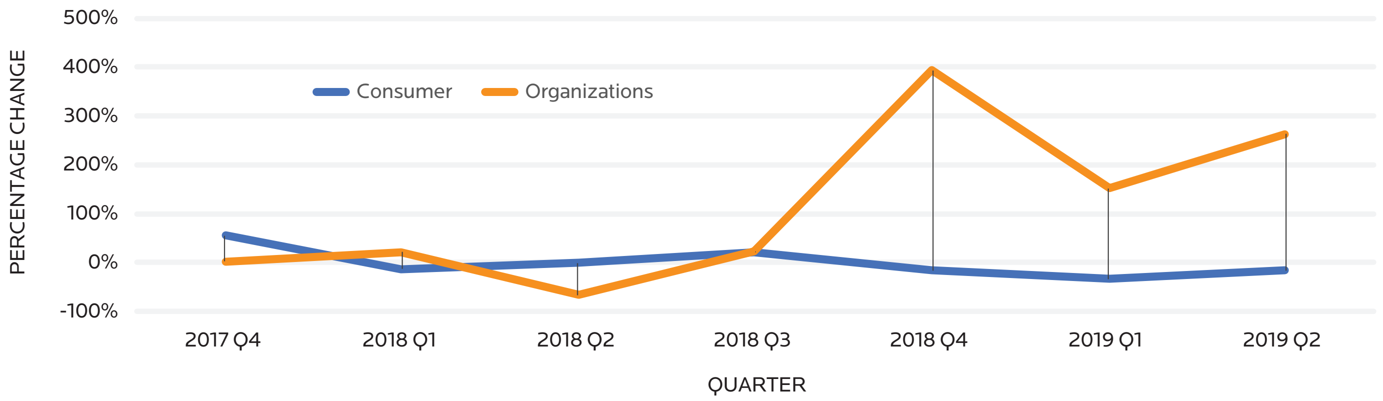


Figure 3. Consumer and business ransomware detections by percentage

through the roof during the last quarter of 2018.

There are several reasons why ransomware instigators have their eyes set on businesses. However, their main motivation boils down to one element: a higher return on investment. When ransoming a single consumer system, the ransom demand is usually low so that targets are more liable to pay up. The number of files encrypted is limited to the size of a typical hard drive, and the files themselves are considered less vital. And the impact to the user, while potentially personally traumatic, is not as devastating as, for example, identity theft, which can result in months of exhausting paperwork to restore credit, finances, and personal reputation.

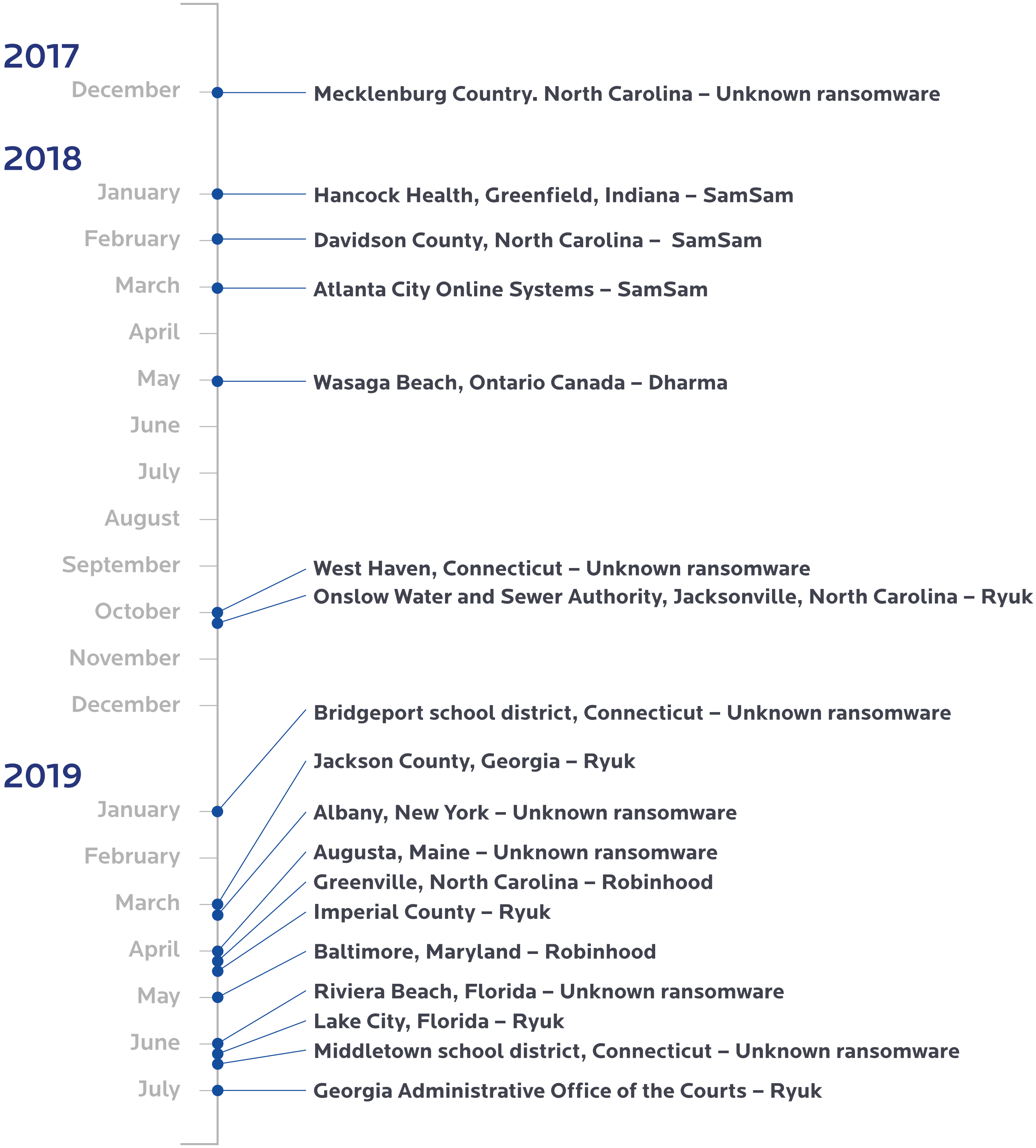
All these are reversed when cybercriminals focus on organizations, however. Encrypting business-critical files on any number of endpoints can supply huge benefits to cybercriminals, including much larger ransom demands and an exponentially higher chance of getting paid. This is because the loss of data doesn't only harm a single user, but an entire business. The fallout from ransomware can range from paying exuberant fines and losing out on high margins of productivity and profit to, for many small businesses, having to close their doors. Even worse, ransomware lodged against vital government infrastructure can bring cities to a standstill.

Ramping up on easy targets

> As the value of attacking consumers dropped due to greater availability of anti-ransomware tools and an overall low rate of return, it was no surprise that many ransomware families seemed to fall out of existence at the end of 2017, with Bitcoin miners multiplying well into 2018 instead.

During this time, however, we noted that there was an increase in the number of targeted cities, educational institutions, and healthcare organizations by ransomware, as cybercriminals wanted higher earnings than what they were seeing with miners alone. From December 2017 to present, ransomware threat actors lodged attacks against these organizations, likely because of legacy infrastructure, outdated hardware and software applications, and lack of security funding in these sectors. Unlike private organizations, who can drive their own profit margins and make unilateral decisions on funding, financial backing for local municipalities, education, and healthcare is often driven by government policy and political climate. As such, these industries must divert the majority of their limited funding to core issues, such as curriculum for education, community services for government, and research for healthcare—especially when budget cuts for these programs are on the rise.

The last year has exposed how unprepared many of these organizations are for cyberattacks, especially considering that many of the cities at the butt end of ransomware attacks this year had already experienced cybersecurity incidents in years prior. Some of the most noteworthy ransomware attacks on cities, healthcare, and education over the last year-and-a-half are as follows:



2017

December – Mecklenburg Country. North Carolina – Unknown ransomware

2018

January – Hancock Health, Greenfield, Indiana – SamSam

February – Davidson County, North Carolina – SamSam

March – Atlanta City Online Systems – SamSam

April

May – Wasaga Beach, Ontario Canada – Dharma

June

July

August

September

October – West Haven, Connecticut – Unknown ransomware

Onslow Water and Sewer Authority, Jacksonville, North Carolina – Ryuk

November

December

2019

January – Bridgeport school district, Connecticut – Unknown ransomware

February

March – Jackson County, Georgia – Ryuk

Albany, New York – Unknown ransomware

April – Augusta, Maine – Unknown ransomware

Greenville, North Carolina – Robinhood

Imperial County – Ryuk

May – Baltimore, Maryland – Robinhood

June – Riviera Beach, Florida – Unknown ransomware

Lake City, Florida – Ryuk

Middletown school district, Connecticut – Unknown ransomware

July – Georgia Administrative Office of the Courts – Ryuk

As we see more laws being pushed to increase the security and privacy around consumer data, it's likely these sectors will be required to ensure their networks are secure to maintain city services, better protect children's data in schools, and keep healthcare facilities up and running. We hope to see, in addition to many new bills proposed at the state and federal level, information security as a hot topic for political debate during the next election cycle.

Ransomware families

> To break down exactly which ransomware families are the most impactful today, we charted changes in the percentage of our overall detections between Q1 and Q2 2019, as well as from Q2 2018 to Q2 2019. We looked at the top five families of ransomware detected by our consumer and business products individually, as well as combined. We then charted the journey of each of the top five ransomware families over the last year, noting spikes and dips in consumer and business detections and aligning them with evolutions in the family's attack methods. Finally, we zeroed in on the death of two of the most popular and dangerous ransomware families, and how their departure has left room in the threat landscape for newcomers to take their place.

All Products

Ransomware Family	YoY % Change 2018-2019	QoQ % Change Q1 - Q2
All Ransomware	**16%**	**-17%**
GandCrab	-43%	-33%
Ryuk	NEW	-15%
Troldesh	265%	-53%
Rapid	-10%	-48%
Locky	-48%	-5%

Figure 4. Ransomware family detections for both consumer and business products

GandCrab has been the most active ransomware family observed over the last year. However, despite its immense spread, we saw a 43 percent drop in detections of GandCrab from the same time last year, and even a 33 percent decline from the previous quarter. At the end of May 2019, the threat actors behind GandCrab announced their retirement on a dark web forum, but researchers remain unconvinced that the group will leave behind their successful enterprise entirely.

Consumer detections of ransomware have been in decline nearly across the board. Families such as GandCrab, Ryuk, Rapid, and Locky have been on a downward consumer slope for over a year, and we don't expect this to change anytime soon. Troldesh, which was launched in a widespread campaign earlier in 2019, was the only ransomware family that increased for consumers year over year, to the tune of 162 percent. However, this ascent was short-lived, as we've already seen a decline of 55 percent between this quarter and last.

On the flip side, our business products have seen an almost constant increase in detections of ransomware families, specifically those causing the most trouble today, like Ryuk and Phobos. Ryuk detections increased by 88 percent over last quarter,

Consumer Products

Ransomware Family	YoY % Change 2018-2019	QoQ % Change Q1 - Q2
All Ransomware	**-12%**	**-25%**
GandCrab	-54%	-40%
Ryuk	NEW	-55%
Troldesh	162%	-45%
Rapid	-30%	-57%
Locky	-54%	-24%

Figure 5. Ransomware family detections, consumer products only

while Phobos—which appeared on the scene at the beginning of 2019 and is likely distributed by the same group behind Dharma/CrySis—exploded by an astonishing 940 percent from Q1 2019. Overall ransomware detections against businesses between Q2 2018 and Q2 2019 have risen by 363 percent, though if you follow the news, this shouldn't be too much of a surprise.

Each ransomware family we have observed over the last few years has gone through various evolutions in capabilities, campaigns, and target focus. To that end, we can observe exactly how these families have changed over time to try and understand where they are going next.

Business Products

Ransomware Family	YoY % Change 2018-2019	QoQ % Change Q1 - Q2
All Ransomware	**363%**	**14%**
GandCrab	NEW	88%
Ryuk	24%	-5%
Troldesh	NEW	-47%
Rapid	NEW	940%
Locky	319%	19%

Figure 6. Ransomware family detections, business products only

GandCrab

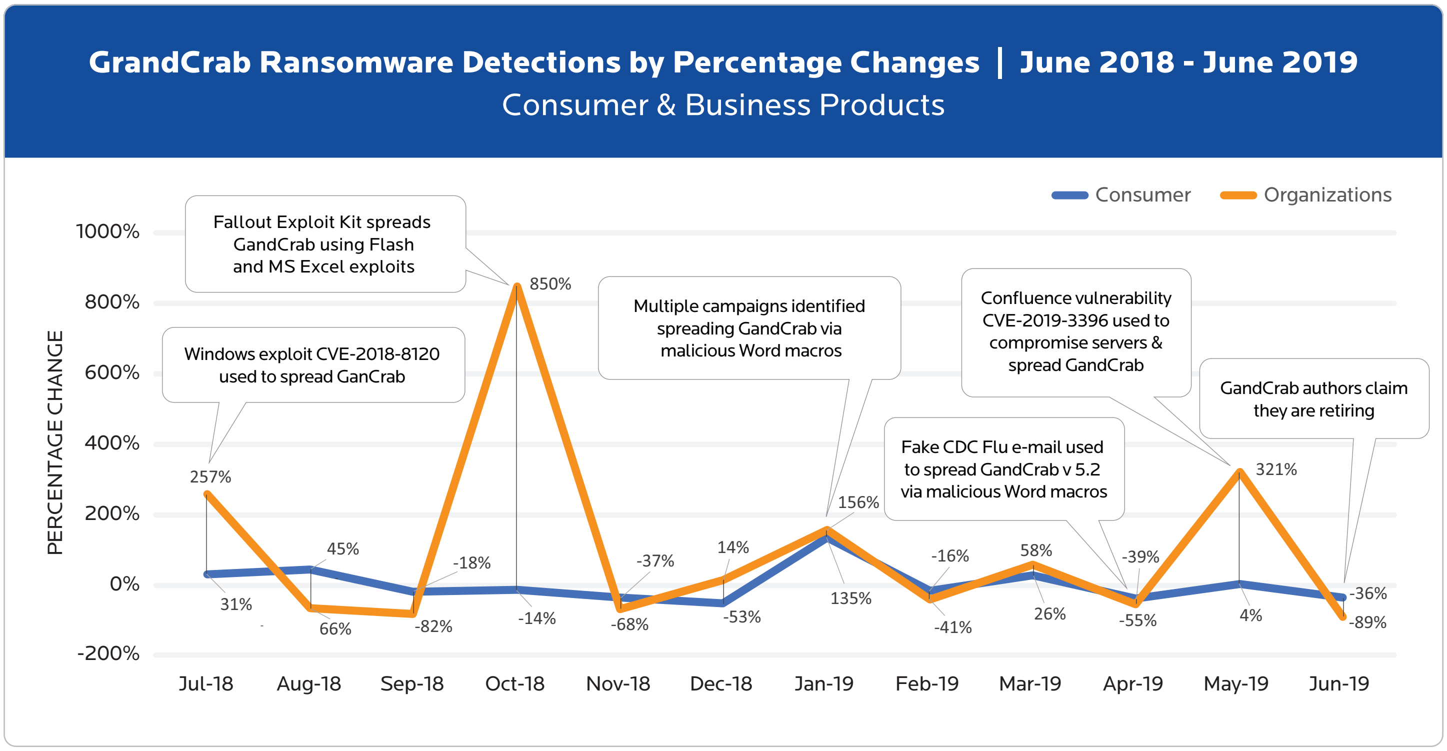


Figure 7. GandCrab evolution

GandCrab, which uses a ransomware-as-a-service (RaaS) model to sell its wares to affiliate criminal groups, was the top ransomware threat for consumers and the second-most detected threat for businesses from Q2 2018 until Q2 2019. Over the last year, GandCrab authors made multiple modifications to its campaign, including changing methods of distribution, starting with exploit kits in 2018 and moving on to malicious Word documents at the beginning of 2019. Phishing emails with fake flu alerts from the Centers for Disease Control and Prevention (CDC) ensnared victims in March 2019, and a vulnerability in Confluence, a collaboration software program, was used to compromise servers and spread GandCrab in May 2019. Finally, by the end of June, GandCrab authors appeared to be staying true to their retirement promise, slowing down operations and decreasing in detection frequency by 36 percent for consumers and 89 percent for businesses.

However, despite all appearances of closing up shop, a new threat appeared on the horizon around the same time that GandCrab announced their retreat, ramping up efforts as GandCrab slowed down. Sodinokibi ransomware, which is also a RaaS, appeared in May 2019 using similar technical components as its predecessor, and many security researchers believe it is connected with GandCrab. Time will tell if Sodinokibi picks up where GandCrab left off, or if the two ransomware families will tag team for more action in Q3.

Rapid

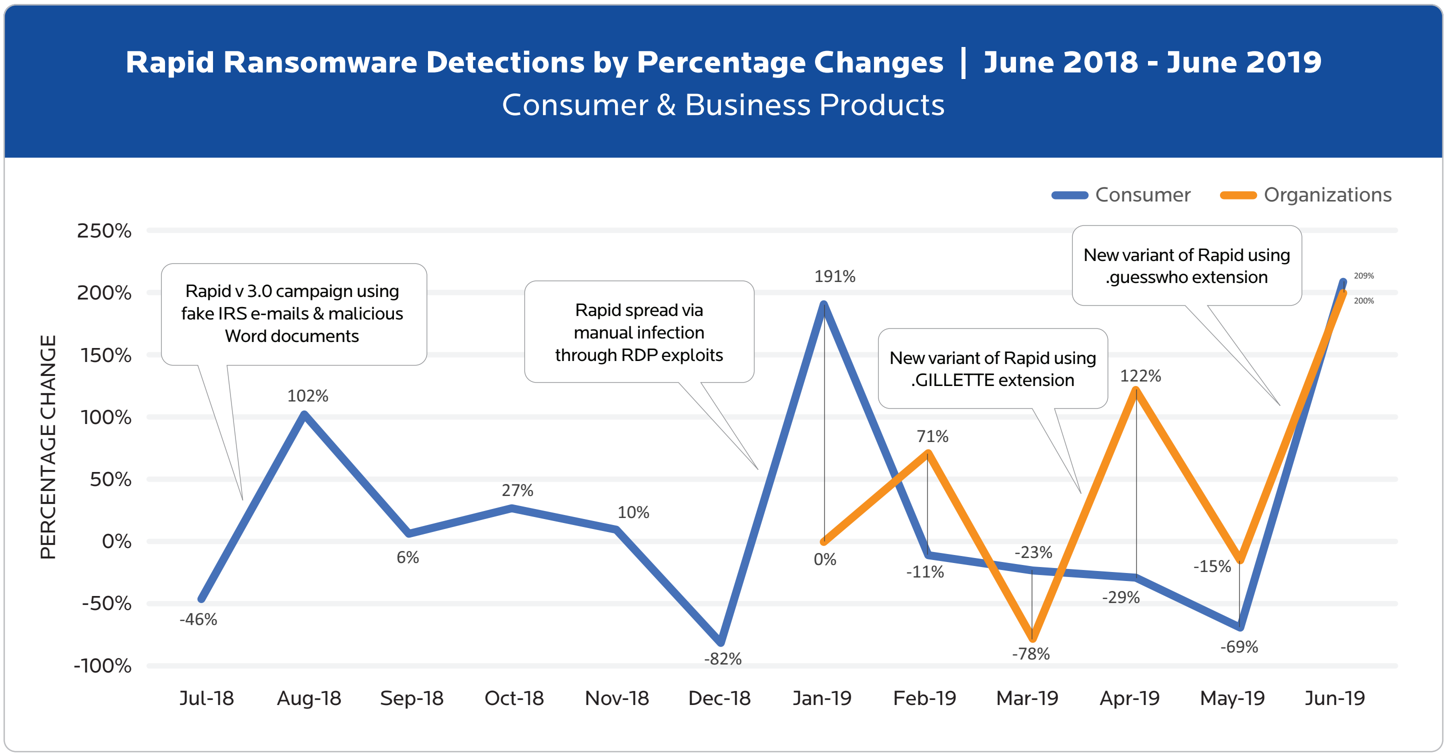


Figure 8. Rapid detections increased rapidly from May to June 2019

Rapid ransomware has not been in the headlines as much as other families; however, it's none-the-less been a thorn in the side of business and consumer users all over the world.

Rapid was already on its third version halfway through 2018, and since then, we've observed it being pushed through phishing emails that spoof the IRS and launch payloads via malicious Word documents. More recently, Rapid was spread manually through remote desktop protocol (RDP) exploits. In addition, we've seen Rapid follow in the footsteps of other ransomware families, going after business targets as it continues to evolve with new extension names. In June 2019, detections of Rapid on both consumer and business endpoints increased by more than 200 percent over the previous month.

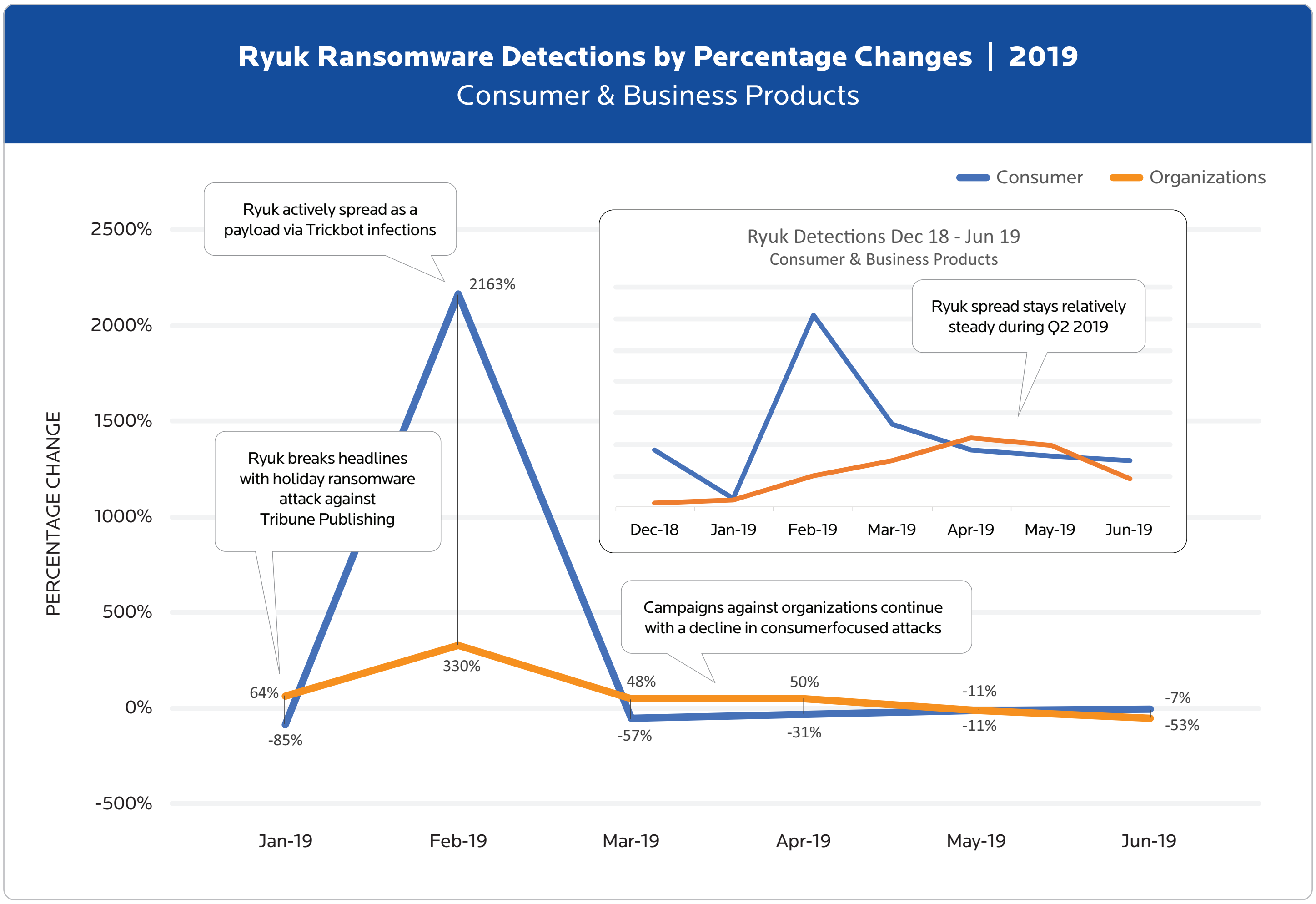


Figure 9. Ryuk ransomware detections remain steady during Q2 2019

Ryuk

Ryuk should be on the mind of every person worried about ransomware today. While it was first discovered in August 2018, Ryuk made noise over the winter holidays by encrypting data and halting operations at both Tribune Publishing and Data Resolution. The following month saw an explosion of infections—a 330 percent increase for businesses and a shocking 2,163 percent jump in detections for consumers—thanks to active "triple threat" campaigns.

The triple threat campaigns featured phishing emails that opened the door for the Emotet downloader to compromise systems. Emotet then dropped the TrickBot Trojan, which spread laterally through organizations' networks using the EternalBlue exploit. Finally, once TrickBot established a foothold on the network, it pushed Ryuk, which made itself known through multiple ransom notes demanding a higher-than-average payout.

While percentage increases and decreases have stabilized since March 2019, this is because Ryuk is being pushed at a steady rate by its controllers, something that should be concerning to anyone protecting a network.

Troldesh

Troldesh Ransomware Detections by Percentage Changes | June 2018 - June 2019

Consumer & Business Products

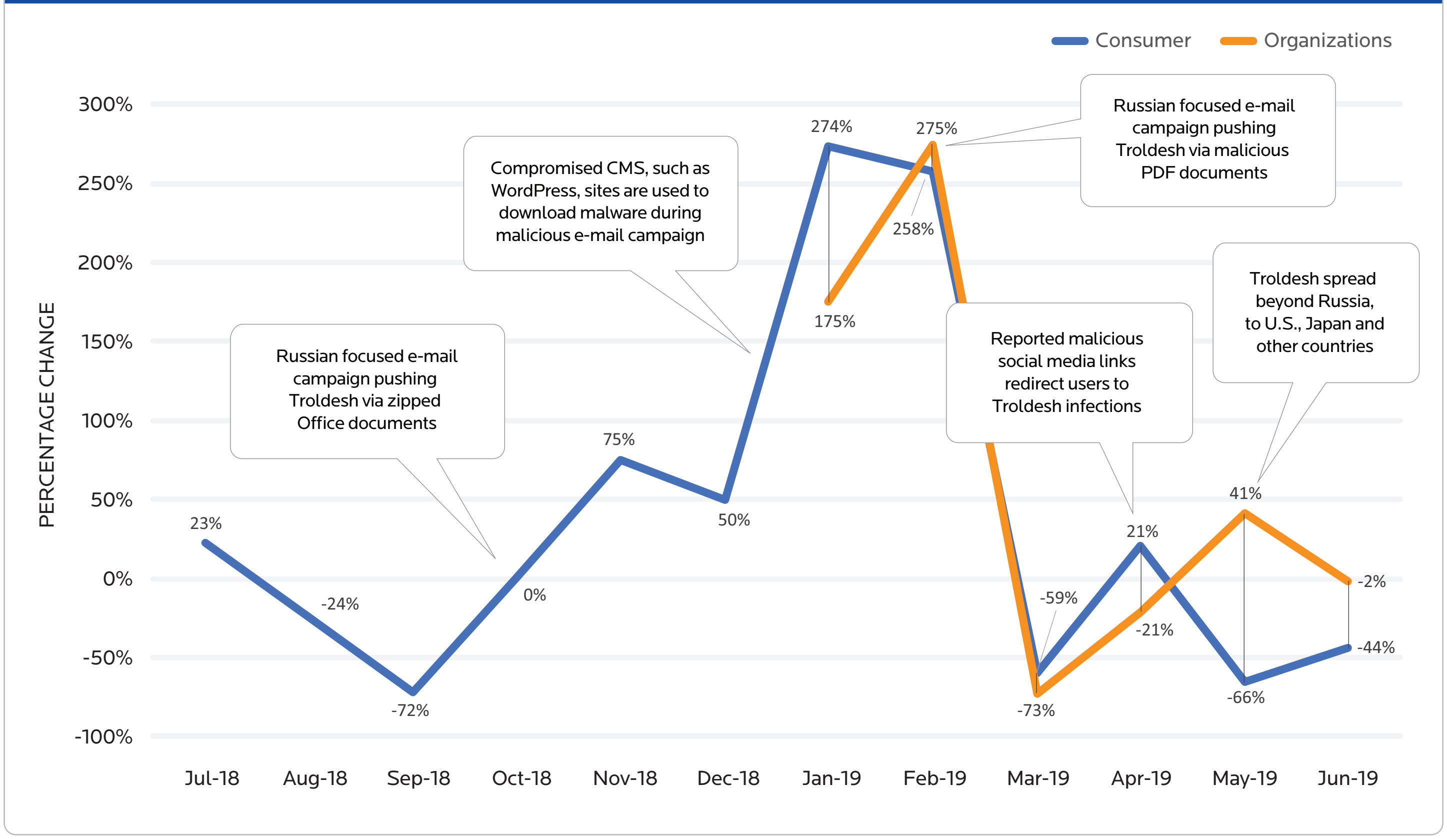


Figure 10. Troldesh percentage changes from July 2018 to June 2019

Troldesh, aka Shade, is an older ransomware—it's been around for many years, periodically returning in different forms. We observed a sharp incline in consumer detections of Troldesh from September to December 2018, and then a dramatic drop off between February and March 2019. And while consumer detections never recovered to their 2018 heyday, business detections outpaced them for all of Q2 2019.

Over the last year, we've observed a large campaign pushing Troldesh via malspam with PDF attachments. In addition, compromised content management systems (CMSes), such as WordPress or Joomla, have been used to host Troldesh executables, waiting to be downloaded by malicious scripts found within the email attachments.

There are reports that social media has also been used to spread malicious Troldesh links. Unlike many of our other top ransomware families, Troldesh has primarily been focused on attacking Russia, singling out systems using the Russian language. Only in the last six to eight months have we seen more activity in the West.

Phobos

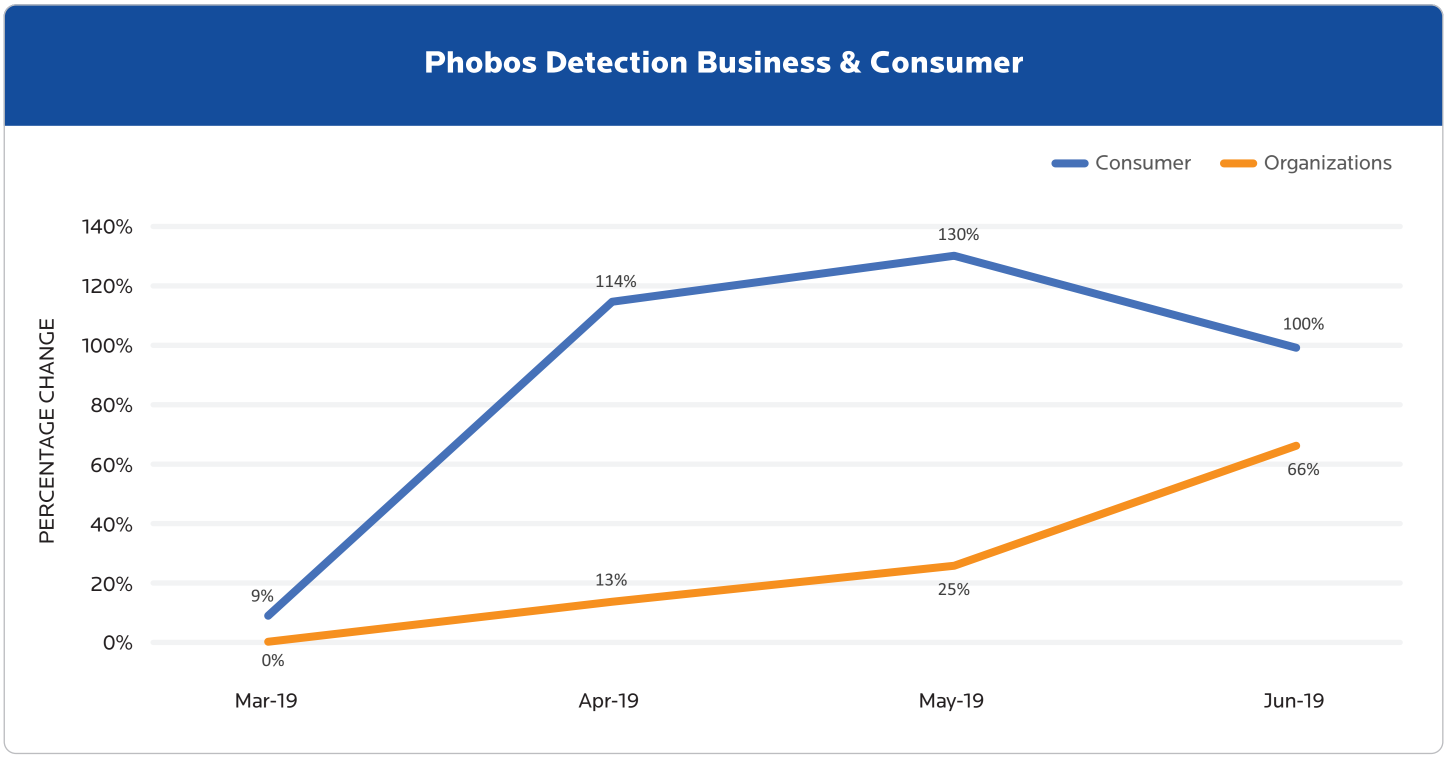


Figure 11. Phobos consumer and business detections

Hot on the heels of a revival of the 2016 ransomware family known as Dharma or CrySIS, which saw an uptick of activity in Q1 2019, entered Phobos. An initial spike in consumer detections of Phobos in April gave way to a steady increase in business detections, which then shot up in May and June 2019. By the end of June, business detections had increased by 164 percent over the previous month, while consumer detections decreased by 23 percent. We expect this trend to continue over the coming quarters, as analysis of Phobos' attack vector, behavior, and encryption process indicate it was developed for business targets.

Phobos targets endpoints by exploiting open or poorly-secured RDP ports, a trend we see continuing, as hacked RDP servers are a cheap commodity on the underground market, and make for an attractive and cost-efficient dissemination vector for threat groups. Once Phobos gains entry, it attacks and encrypts all local files and network shares. It also uses several persistence mechanisms, installing itself in %APPDATA% and in a Startup folder, and adding the registry keys to autostart its process when the system is restarted.

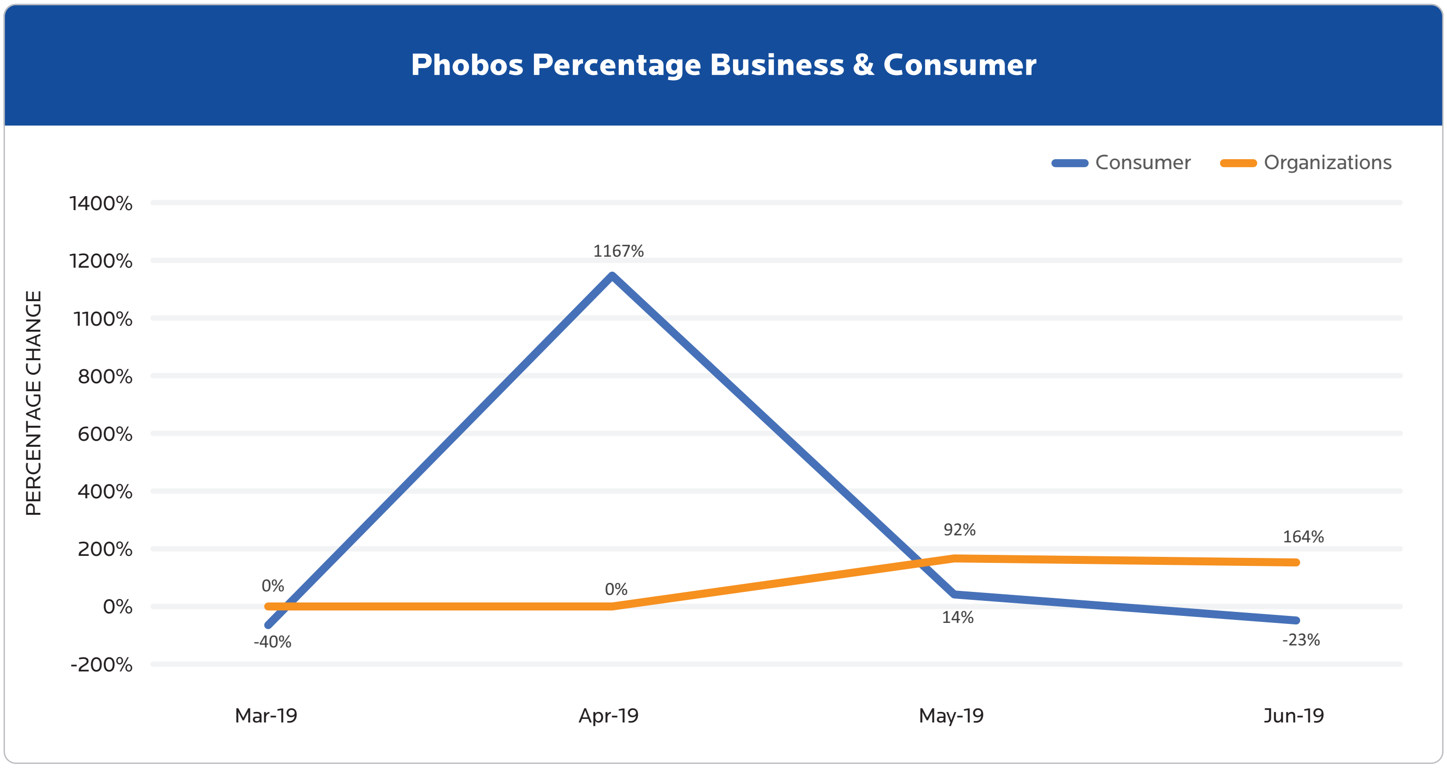


Figure 12. Percentage of business and consumer Phobos detections

Security researchers quickly noted similarities between Phobos and Dharma, which both target organizations via hacked RDP connections and use the exact same ransom note text and typeface, only rebranded with a Phobos logo. In fact, there are also parallels in the code base of Dharma and Phobos, which indicates that the two variants were developed by the same threat actors. So why the second ransomware family? Most likely, the cybercriminals behind Dharma wanted an insurance policy, in case their highly successful and visible efforts were thwarted with decryption keys or security solves. Their secondary efforts proved valuable, as detections of Phobos far outpaced Dharma on Malwarebytes endpoints in 2019.

Old families die hard

> As we continue our exploration of ransomware activity over the last few years, we are going to see certain families show up that have been considered long dead. Two of these are Cerber and Locky, both dangerous families that used to dominate the threat landscape in ransomware's 2016 golden era.

Cerber

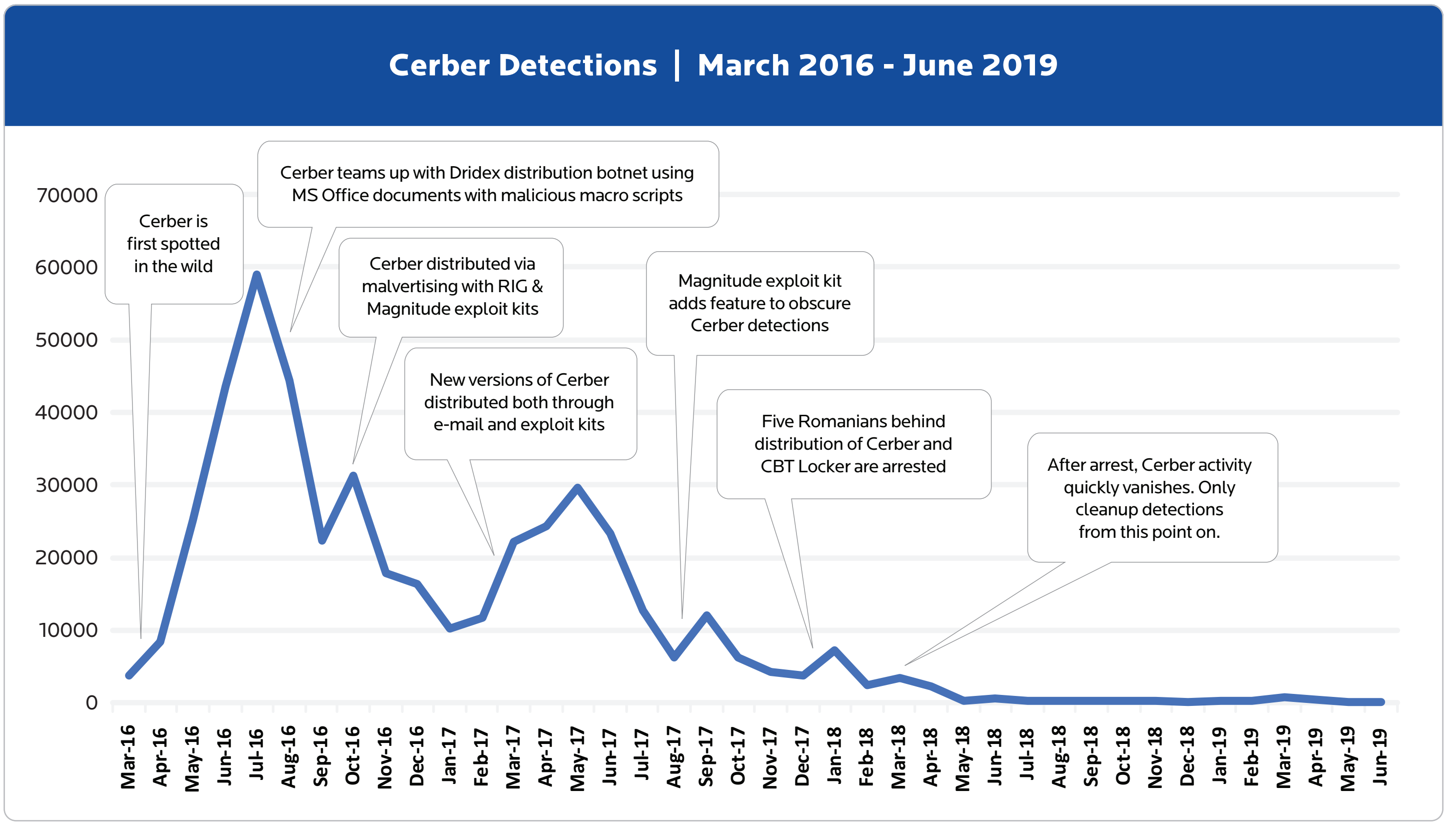


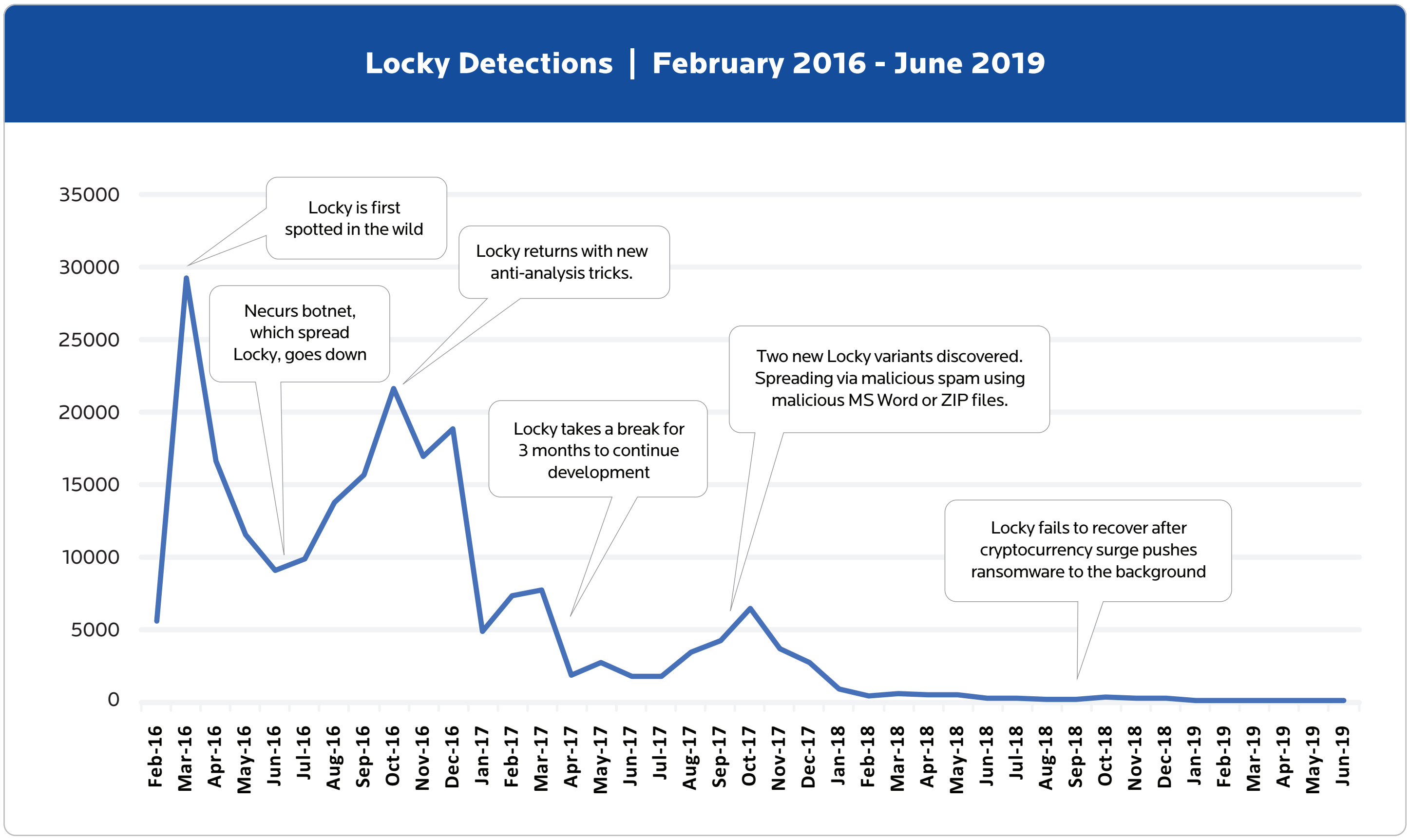
Figure 13. Cerber detections

Cerber was first discovered in March 2016 and quickly made itself one of the most frequently distributed ransomware families ever seen. Cerber was the first to act as a RaaS, which is becoming the norm for many modern malware families, but was a novel idea when Cerber first adopted it.

By allowing "affiliates" to spread the ransomware, the creators of Cerber were able to take a percentage of the ransom from far more infections than they could have gained on their own. Affiliates then spread Cerber through a wide variety of attack vectors, including exploit kits, malicious email campaigns, and malvertising attacks.

In December 2017, it was announced that five Romanian nationals were arrested for their role in distributing Cerber. Since then, Cerber hasn't had the same ransom market share, and many have deemed the family dead since early 2018. Despite its apparent deceased status, "zombie" Cerber infections continue to be identified, either as leftover artifacts from earlier campaigns or feeble attempts to utilize the ransomware again by script kiddies. As Malwarebytes is a leading remediation product, it's not surprising to see this family in our stats.

Locky


Locky Detections | February 2016 - June 2019

Locky is first spotted in the wild

Necurs botnet, which spread Locky, goes down

Locky returns with new anti-analysis tricks.

Locky takes a break for 3 months to continue development

Two new Locky variants discovered. Spreading via malicious spam using malicious MS Word or ZIP files.

Locky fails to recover after cryptocurrency surge pushes ransomware to the background

Figure 14. Locky detections

Locky is another family that has been considered offline since early 2018, though theories about its disappearance are not as interesting as Cerber. After the rise of cryptomining from late 2017 through early 2018 due to the increase in value of Bitcoin, Locky fell silent, likely because its authors adapted to the shift and changed course.

Locky first appeared in February 2016, a month before Cerber, and for a time, it was the second-most common ransomware family detected. Unlike Cerber, which had multiple affiliates spreading the malware, Locky was suspected to be under the control of a single group that frequently pushed out campaigns in spurts.

The months leading up to Locky's death showed increased efforts by its creators to add new features to hide the malware from security tools, as well as to increase its capacity for demanding ransom. Perhaps this was a last-ditch effort to keep the once-great ransomware from disappearing into obscurity, but the constant attention paid to this family by security researchers ensured that any new capabilities would be quickly made obsolete.

Ransomware by region, country, and state

> Not every part of the world deals with the same type of ransomware. In many cases, we have observed certain families, like Troldesh, focus specifically on one country or region over another. Therefore, to identify which threats are focused on which countries—and who has the most ransomware detections—we sliced and diced our telemetry by region, country, and even by US state.

Regional ransomware

Our first look is at overall ransomware infections per region—a combination of our global business and consumer detections. The obvious target is North America (NORAM), taking up nearly half of all ransomware reported. Next up is Europe, the Middle East, and Africa (EMEA) at 35 percent, with the Latin American (LATAM) and Asia Pacific (APAC) regions raking in 10 percent and 7 percent, respectively.

Digging a little deeper, each region is targeted by different ransomware families—or so we thought. Surprisingly, all four regions share the same top four ransomware families in the same order: GandCrab, Ryuk, Troldesh, and Rapid. Only North America

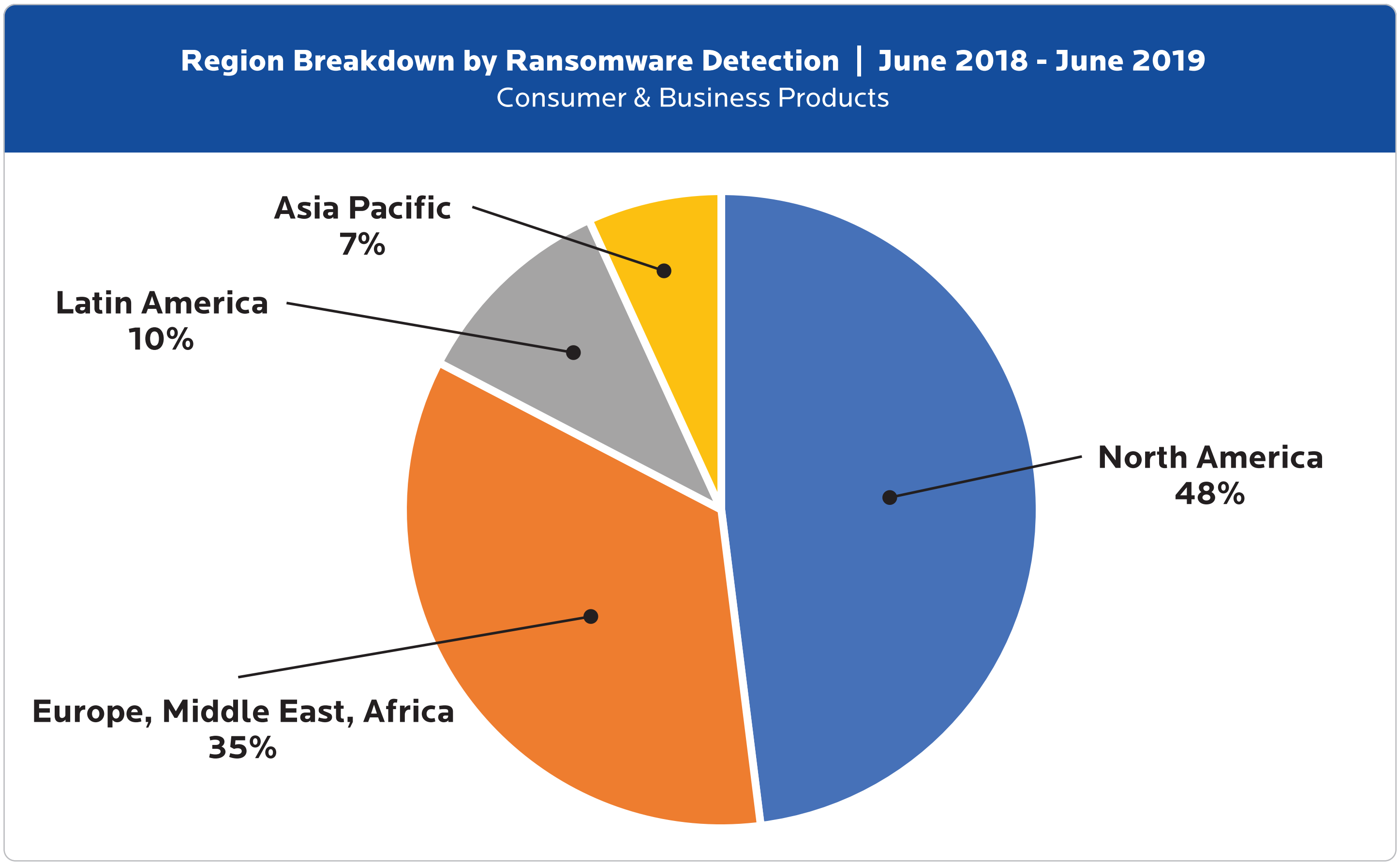
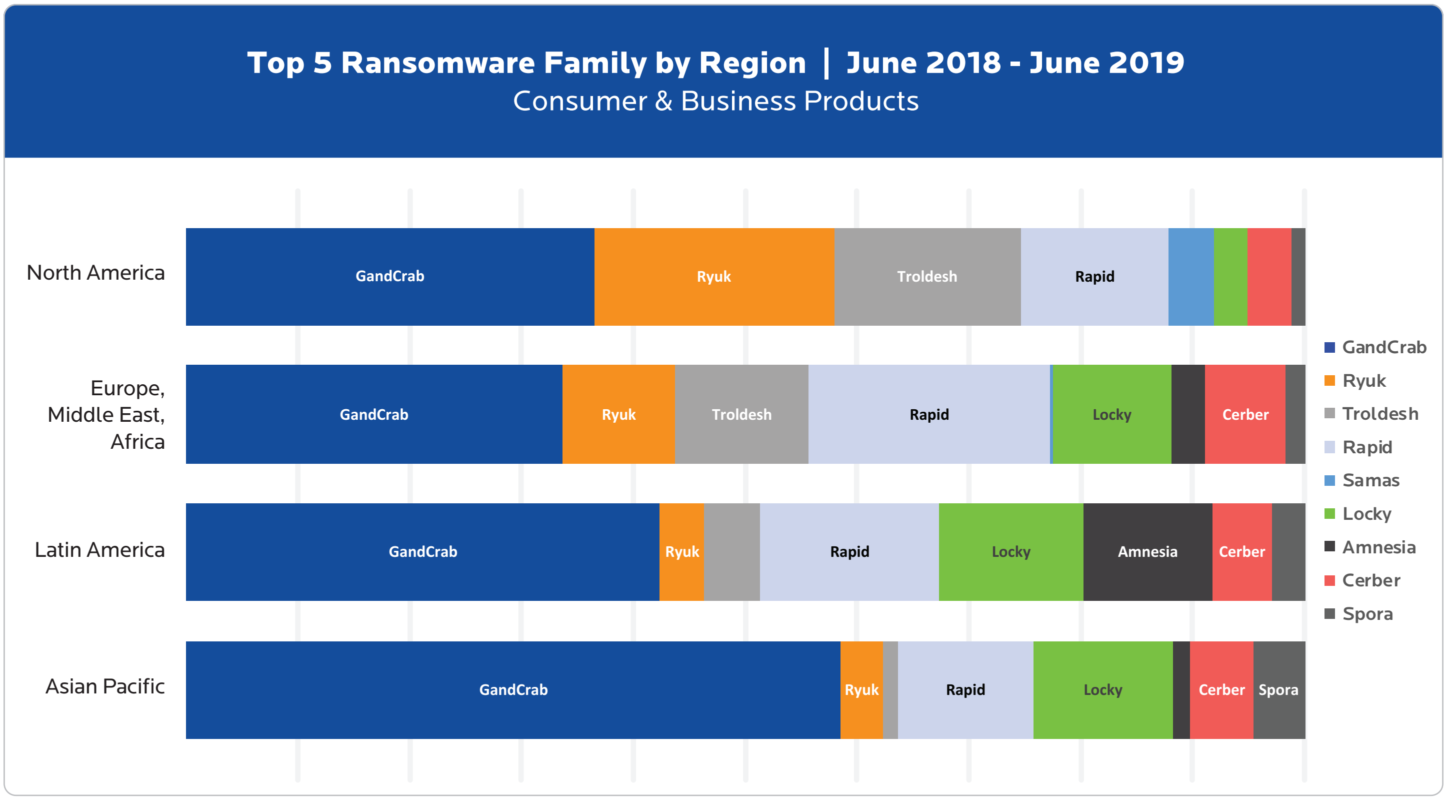


Figure 15. Global ransomware infections by region


Top 5 Ransomware Family by Region | June 2018 - June 2019

Consumer & Business Products

Figure 16. Top ransomware families per region

differed on its fifth-highest ransomware family—Samas—which was instead replaced with Locky in the other three regions. Locky came in sixth place for North America. When we dig into individual countries and states, however, there are fewer similarities.

Clearly, GandCrab took the biggest piece of the pie, or rather, globe. But, the percentage of its penetration actually declined in the most competitive ransomware regions. For example, while NORAM was the top region for ransomware and GandCrab was its top family, GandCrab only represented about one-third of North America's total ransomware. By contrast, APAC was targeted the least by ransomware actors, but when they did decide to attack Asia Pacific, they turned to GandCrab more than half the time.

Ransomware by country

A regional breakdown of ransomware helps us understand which geographic (and economic) areas on which threat actors focus their attention. However, that doesn't mean every country in the region is equally affected. For example, Mexico is the second-largest country in North America by population, but it doesn't even make our list of top 10 ransomware countries.

So which countries were most affected? The United States tops the list with 53 percent of our business and consumer detections. Canada came in a distant second at 10 percent, with the United Kingdom close behind at 9 percent, confirming theories that most ransomware targets English-speaking countries.

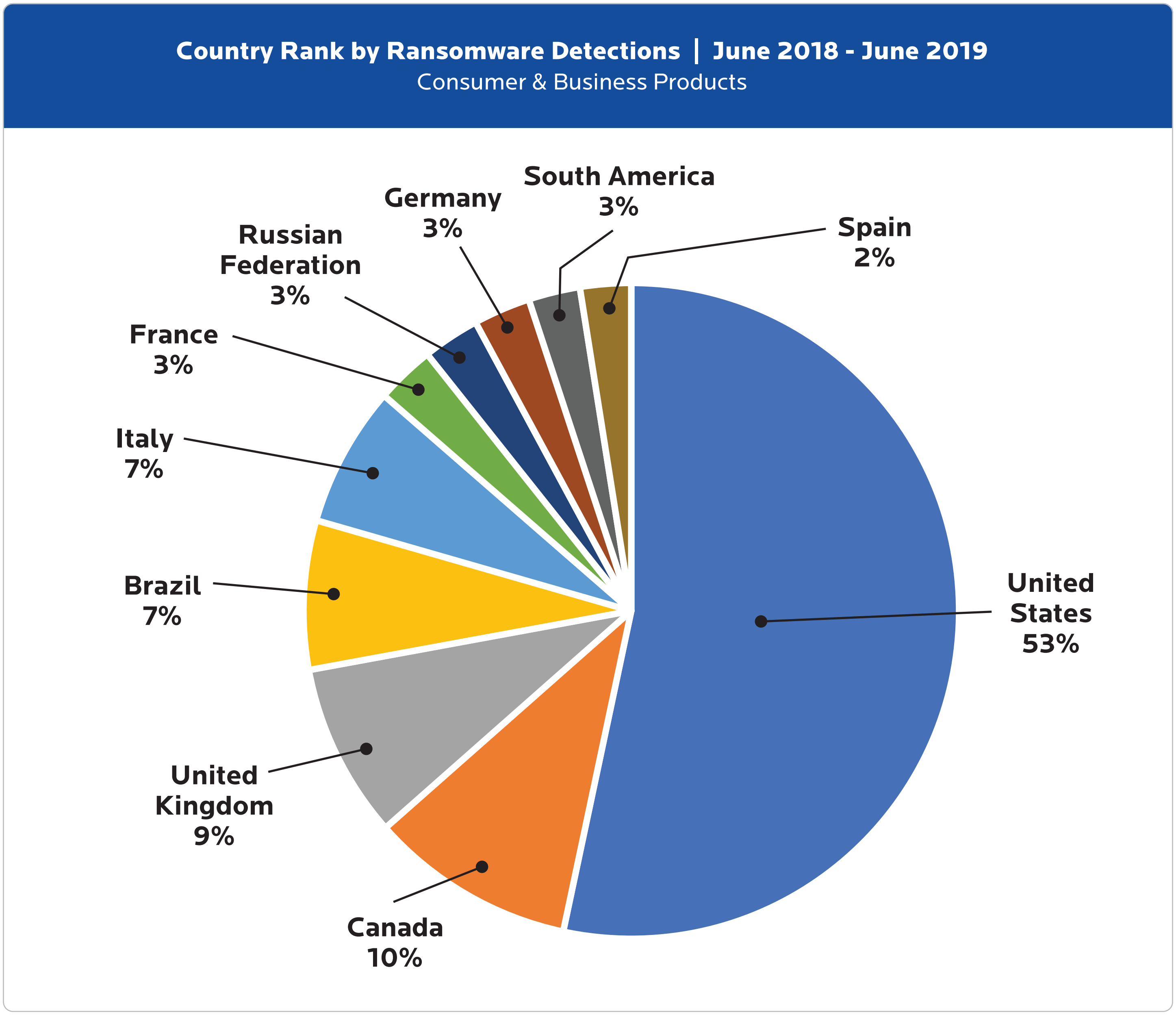
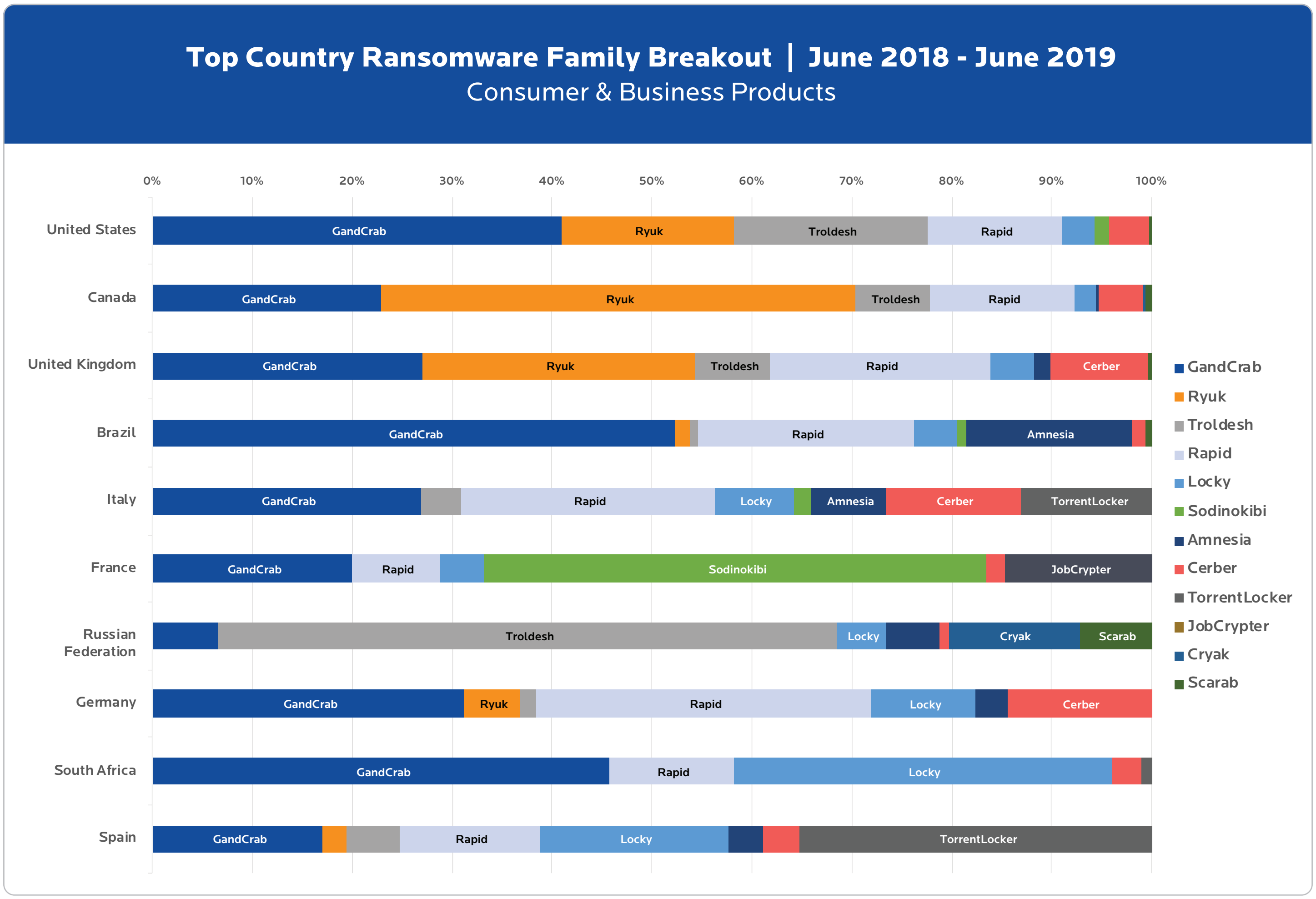


Figure 17. Top 10 countries for ransomware



Top Country Ransomware Family Breakout | June 2018 - June 2019

Consumer & Business Products

Figure 18. Top ransomware families per country

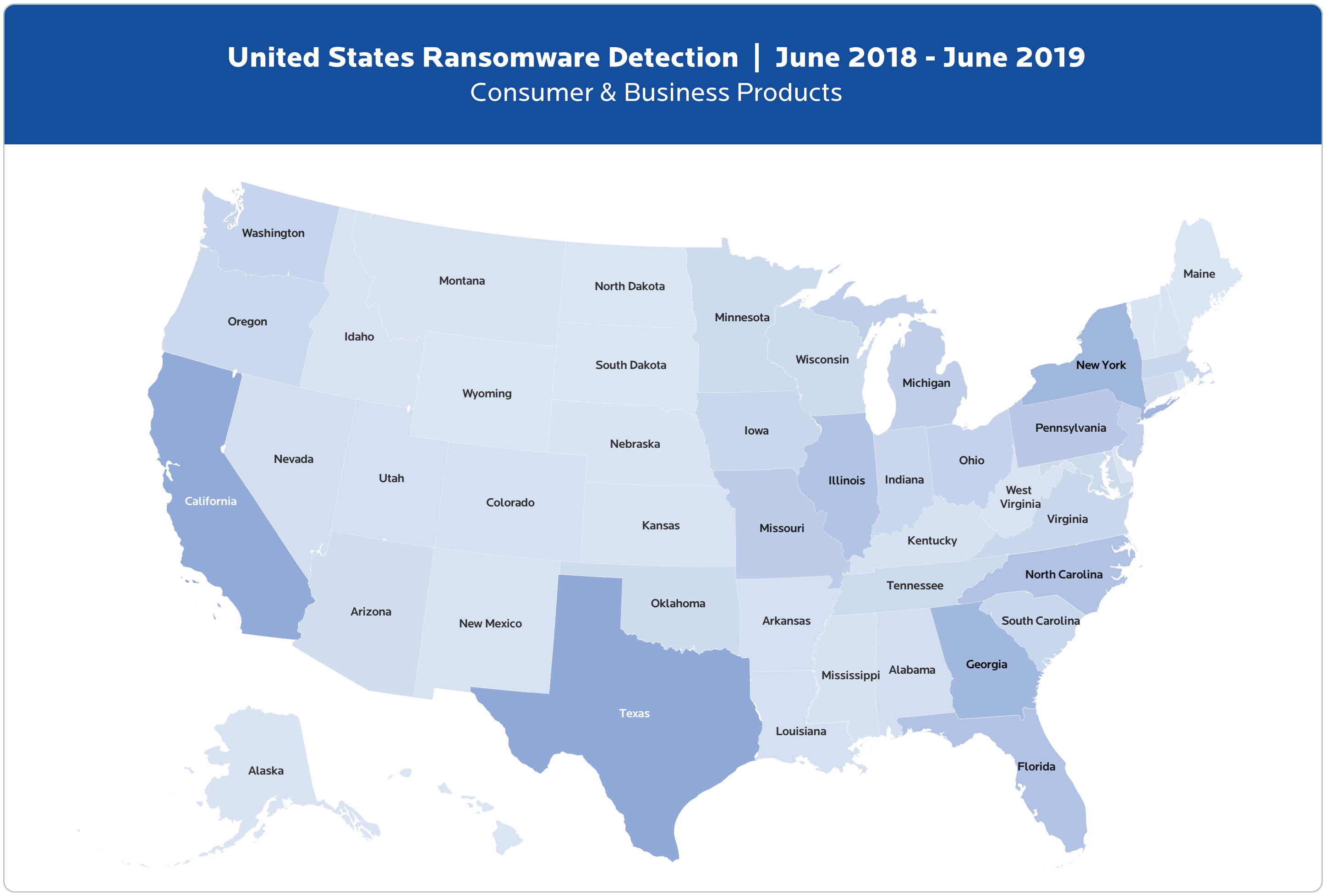
A further breakdown of these countries by ransomware family reveals, once again, many common families. However, certain countries—including Russia, Spain, and France—are attacked at higher rates by threats not typically seen in other countries. Russia is dominated by Troldesh, but also grapples with little-known families Scarab and Cryak. Sodinokibi ransomware, which is slowly gaining steam in other regions, represents a huge chunk of France's ransomware problem, but it is joined by the cryptic JobCrypter. About 35 percent of Spain's ransomware infections are from TorrentLocker, which only shows up in small amounts in South Africa and Italy.

US states affected by ransomware

While many US cities received attention for ransomware attacks that crippled their infrastructure, we noted earlier this year that ransomware is not just a big city problem—we've also noted heavy detections in less-populated areas, which supports our theory that organizations needn't be located in cities known as ransomware targets to become one.

To that end, we decided to zoom out and look at the top five US states affected by ransomware instead, including which families were detected in each state.

As the largest market for most malware in the world, the United States has once again found itself grappling with a rising tide of ransomware threats. However, while consumer-facing ransomware detections made the most populous states the most at-risk for ransomware, the shift in focus to business targets yielded an interesting mix of populous and industrious regions. Therefore, the top five states for ransomware from June 2018 through June 2019 were not necessarily the most populated. Texas had the most detections, for example, even though it has about 10 million fewer people than California. In addition, Georgia and North Carolina made the top five states for ransomware, though they are the eighth- and ninth-most populous US states.



United States Ransomware Detection | June 2018 - June 2019

Consumer & Business Products

Figure 19. Ransomware detections among the 50 US states; The darker the blue, the more ransomware we detected.

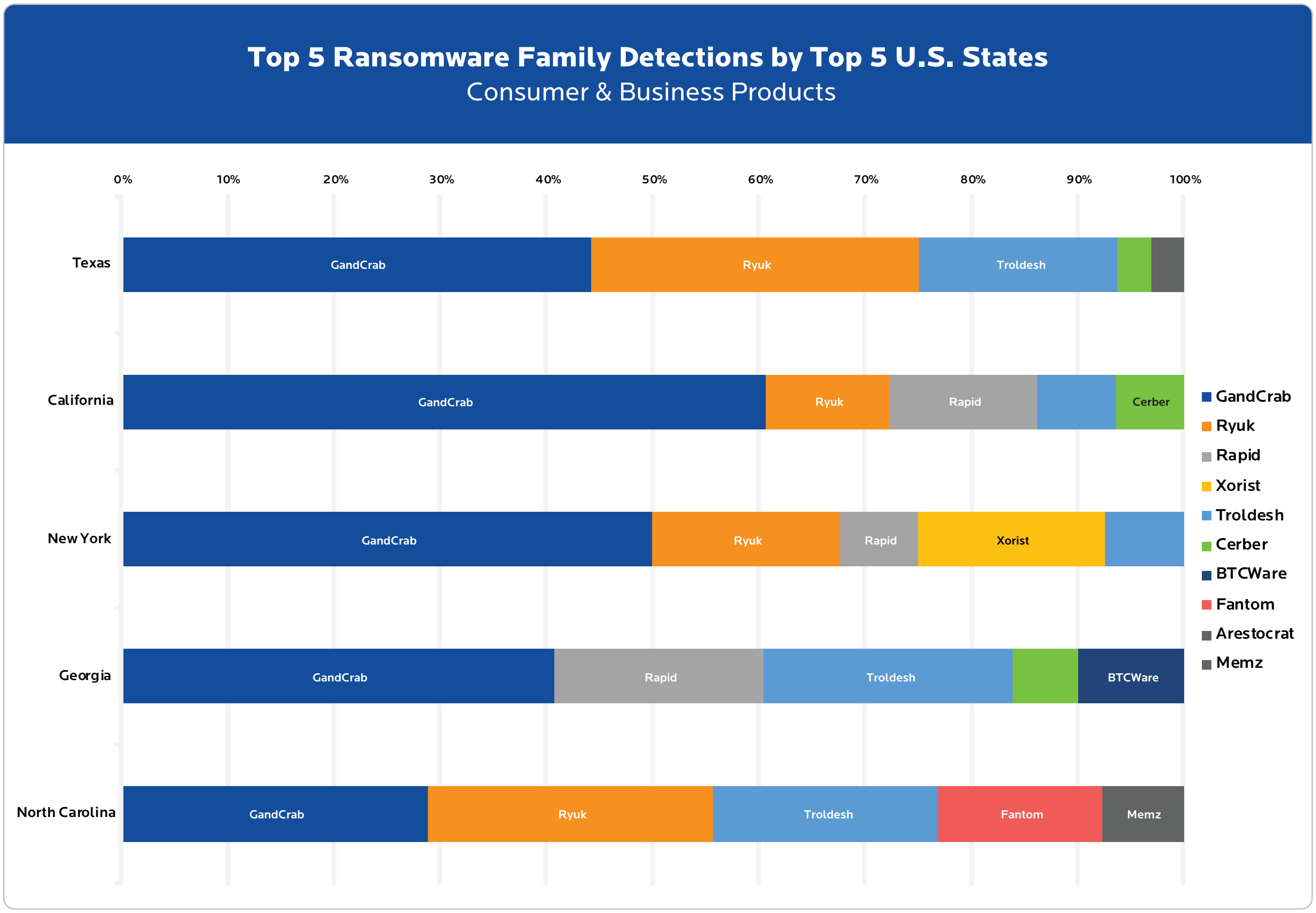


Figure 20. Top five US states for ransomware and the families that target them

When we look at the families that target the top states, once again, GandCrab is all over the place. However, the states with the highest percentage of GandCrab detections—California, New York, and Texas—are also the most populous. This indicates that consumer-focused ransomware such as GandCrab ensnared a larger percentage of victims in highly-populated areas. Whereas the higher percentage of Ryuk in Texas and North Carolina suggests that a greater number of organizational networks were targets in this region.

New ransomware tactics

> When focusing on a new target, the same old tools won't cut it anymore. Cybercriminals know they must evolve their tactics in order to stay ahead of security researchers and penetrate more sophisticated defenses paid for with bigger budgets. We've watched ransomware progress its attack strategy over the last few years, working with new infection vectors, threat partners, tools, and encryption techniques.

The latest ransomware variants observed in Q2 2019, including Ryuk and RobinHood, have adopted specific, customized focuses for their targets. Some are deployed only when the time is right, rather than waiting for a user to take the bait. Others are launched as a second or third payload of another Trojan attack. In some cases, ransomware is executed manually, making its identification and removal difficult for those protecting the network.

With renewed focus and novel technologies at their disposal, cybercriminals are using a mix of old and new tactics to launch ransomware against their victims in 2019. Manual break-ins take advantage of unsecured remote desktop protocol (RDP) connections to breach company networks, while targeted spear phishing attacks—inspired by similar state-sponsored campaigns—fool employees into doing the dirty work for threat actors. Once inside, additional payloads are dropped within the web of systems and then spread laterally, expanding adversary control of the target network.

To understand how cybercriminals have evolved their tactics to better target organizations, we've highlighted three infection vectors that have allowed threat actors to pull off successful attacks at scale.

Exploits

WannaCry and NotPetya were two of the first ransomware families to have exploit code as part of their primary functions. These exploits, which target SMB vulnerabilities, were allegedly leaked from the US National Security Agency (NSA) and posted online a few months prior to WannaCry's first appearance in May 2017.

The SMB-targeting exploits, including EternalBlue and EternalRomance, allow their payloads to spread laterally through connected systems in a worm-like infection, bringing cybercriminals multiplying returns for little effort.

Since the introduction of these exploits in 2017, we've seen EternalBlue and EternalRomance used in other ransomware families and, more commonly, in various forms of Trojan, empowering them to breach entire networks in one swoop.

Blended attacks

Ransomware infections of the past usually ran solo, either through widespread phishing campaigns or drive-by exploits. However, the business-oriented ransomware attacks that began in late 2018 have relied upon extra help from some popular and dangerous Trojan families.

Ryuk ransomware, for example, is after endpoints that are already infected with Emotet and TrickBot. Emotet starts the infection chain, attempts to spread itself via spamming module, and then drops additional malware. One of the common drops we've observed over the last eight months is TrickBot.

TrickBot is capable of brute-forcing credentials, using the EternalBlue exploit to move laterally through the network, as well as other modular components that gain persistence, propagate, harvest emails, and even steal Bitcoin wallets.

Likely once all meaningful data has been stolen, these families achieve full network infection. At this point, TrickBot then downloads and executes Ryuk on all affected systems, causing a mass and instant ransoming of hundreds of thousands of files, adding insult to injury.

Manual infection

In 2018 and 2019, we saw a trend opposite of what we regularly see with ransomware: the manual execution of ransomware on a network endpoint. This method requires an already-breached network, which is achieved in any number of ways. Once on the network, the attackers can prepare the environment for a ransomware attack by disabling security software. Families such as SamSam and Robinhood primarily use this attack method.

Manual infection is a step above a "regular" Trojan or ransomware attack, in that the cybercriminal's ability to ransom, steal, and disrupt organizational operations are far more effective, which in turn yields greater returns. Of course, by manually attacking a network, threat actors put themselves at risk of discovery if they don't do enough to hide their source location and activity.

The ransomware of tomorrow

> We have looked at the past and present of ransomware in this report from as far back as 2016 to the end of Q2 2019, observing the rise and fall of ransomware families that many believed would kick the dust but didn't or were replaced by newcomers with tighter attack strategies. Locky, Cerber, and GandCrab were expected to fully die down, but still have a decent foothold from old infections caused by massive campaigns. However, newer ransomware families like Ryuk and Phobos have rendered the big players of yesteryear nearly obsolete, crushing organizations with techniques developed for mass destruction—at least for now.

Ransomware predictions

So, what are we going to see next? The ransomware of tomorrow is going to look even more alien compared to the ransomware of 2013–2016. You can expect that the following features will be built into most new families of ransomware in the coming quarters and years:

- Manual infections will increase, allowing for attackers to disable security tools and launch ransomware on their own. However, manual interaction with the target network will leave cybercriminals at higher risk of being discovered by law enforcement. The US government was able to indict two Iranian individuals for their part in attacking networks with the SamSam ransomware last year.
- There will be more blended attacks on the horizon. Rather than relying on downloaded threats from a command and control (C&C) server, ransomware will include worm-like functionality that allows it to spread, as well as Trojan elements that allow it to go unnoticed on organizational networks and encrypt files offline.

- Ransomware will continue partnering with other malware families for even more “triple threat” action. While Ryuk has maintained domination over the last couple quarters thanks to its Emotet-initiated, TrickBot-delivered distribution mechanism, other actors who control similar or new malware families will begin to utilize this approach for different phases of their attacks. One threat might identify the target while another exploits it and a third drops the intended payload.

- Infection vectors are always going to change, yet always stay the same. We will see further development of email attacks that take advantage of not just technical vulnerabilities but human ones as well. In addition, more ransomware is expected to be pushed through the remaining exploit kit world; however it may not be in the regions we expect.

- Ransom attacks against consumers will all but disappear, as most families will focus on the biggest target rather than the easiest. Attackers will increasingly target critical infrastructure, recognizing that disrupting publicly-controlled, essential networks will likely result in a higher chance of payment. Ransom against consumers will be replaced with a flood of adware and other malware designed to hijack attention and processing power.

Finally, are we ever going to see the end of ransomware? No way. For too many years, there have been hugely-successful ransomware attacks that have resulted in criminals making off with thousands, even millions of dollars from a single infection. If that isn’t motivation to double down on this attack type, we don’t know what is.

Conclusion

> As we wrap up this ransomware report, we want to provide a reminder to our readers to continue taking this threat seriously. We've seen an increase of over 300 percent in ransomware detections on businesses, and many new, dangerous families are gaining market share as the "top dogs" of the ransom game. Yet, despite the success of these new threats, which are using advanced technology and sophisticated attack vectors, we still see remnants of long-dead families, such as Cerber and Locky, which could continue causing damage—or at least mark users as future targets—if not removed.

We were able to identify that Western countries, especially the United States, are targeted for ransomware infections more than other parts of the world. Whether this is the result of a strong economy, lackadaisical security practices, lagging infrastructure updates, or all of the above, we can't be sure. Either way, ransomware is still a major concern for many other regions of the world, including Latin America, many parts of Europe, and Asia. Those regions, countries, and states that aren't currently at the top of the list shouldn't discount the ransomware threat. As we've shown, a simple shift in the wind can bring about massive climate change.

We can now say that back in 2017 when ransomware began to decline in favor of miners, we thought it was the end of ransomware—and in many ways, it was. The ransomware landscape of today has been completely reshaped. Threat actors have new, more challenging yet more enticing targets, and they deliver their ransomware in different ways than we've seen in the past. The encryption algorithms of the new generation of ransomware, as well as their techniques for avoiding detection, will only become even more difficult for traditional security measures to defeat.

Yet the ransomware epidemic we experienced between 2013 to 2017 gave us clues about the future of ransomware. First, ransom was used to fool users, but they learned how to recognize it. Then it froze them out of their systems and encrypted their files, but decryption keys, anti-ransomware technology, and prevention techniques helped users beat it. Today's ransomware doubles down on previous ransomware techniques by circumventing earlier protections that were developed in 2017 to stop them in their tracks. Modern ransomware finds new ways onto the network, spreads instantly, sneaks past the programs of many cybersecurity vendors, and achieves persistence.

This does not mean that ransomware is unbeatable. Rather, it speaks to a realization that we need to expand our methods of prevention, detection, remediation, and recovery from these attacks beyond what we did in the past. This means organizations cannot become complacent with the practices developed to thwart ransomware just a couple years ago. They must look not just at the ransomware itself or even the entire attack chain, but also focus on every aspect of reconnaissance, delivery, infection, encryption, and threat behavior to determine how best to stop ransomware and all threats associated with it. In addition, businesses cannot assume that preventative action, including implementing security best practices and automatically backing up files, will save them from ransomware attacks. An incident response and recovery plan is necessary in today's ransomware world. Hope for the best, but plan for the worst. And as always, stay safe out there.

Contributors

Adam Kujawa
Director of Malwarebytes Labs

Wendy Zamora
Director of Content, Malwarebytes Labs

Jovi Umawing
Senior Content Writer, Malwarebytes Labs

Jérôme Segura
Director of Threat Intelligence

William Tsing
Head of Operations, Threat Intelligence

Marcelo Rivero
Threat Intelligence Analyst

Hasherezade
Threat Intelligence Analyst

Chris Boyd
Senior Threat Intelligence Analyst

Pieter Arntz
Threat Intelligence Analyst

David Ruiz
Content Writer, Malwarebytes Labs

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.