mimecast®

# Threat Intelligence Report

*RSA Conference Edition 2020*

# Threat Intelligence Report

*RSA Conference Edition 2020*

## Table of Contents

**DISCLAIMER:** This Threat Intelligence Research Report is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. Mimecast Services Limited and its affiliates (collectively, "Mimecast") have exercised reasonable care in the collecting, processing, and reporting of this information but have not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. Mimecast shall not be responsible for any errors or omissions contained on this Threat Intelligence Research Report, and reserves the right to make changes anytime without notice. Mention of non-Mimecast products or services is provided for informational purposes only and constitutes neither an endorsement nor a recommendation by Mimecast. All Mimecast and third-party information provided in this Blog is provided on an "as is" basis. MIMECAST DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, WITH REGARD TO ANY INFORMATION (INCLUDING ANY SOFTWARE, PRODUCTS, OR SERVICES) PROVIDED IN THIS RESEARCH PAPER, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. In no event shall Mimecast be liable for any damages whatsoever, and in particular Mimecast shall not be liable for direct, special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue or loss of use, cost of replacement goods, loss or damage to data arising out of the use or inability to use any Mimecast website, any Mimecast solution. This includes damages arising from use of or in reliance on the documents or information present on this Blog, even if Mimecast has been advised of the possibility of such damages.

# Introduction

In the Mimecast Threat Intelligence Report: RSA Conference Edition, Mimecast Threat Center analyzed global attack activity from October 2019 through December 2019 and discovered a mixture of simple, low effort, and low-cost attacks targeting certain Mimecast customers. At the same time, the data highlights complex, targeted campaigns leveraging a variety of vectors and lasting several days. These sophisticated and coordinated attacks were ***likely*** carried out by organized and determined threat actors, employing obfuscation, layering, exploits, and encryption to evade detection. The key threat identified during this period has been the resurgence and substantial increase in the use of **Emotet** malware activity following its relative inactivity between May and September 2019.

This research will explore these themes through the lens of the four main categories of attack types discovered in the quarter: spam, impersonation, opportunistic, and targeted. This report considers major campaigns carried out by threat actors and identified from Mimecast's detection data over an entire quarter – October through December 2019 – inclusive of **202 billion emails, of which 92 billion** were rejected by Mimecast as illegitimate in this period. The report identifies the trends that emerge from attacks, and assesses the ***likely*** future trends and activity given threat actors' current behaviors, events, and technology. Taken together, these factors will ***likely*** impact the cybersecurity landscape going into 2020.

This report utilizes research conducted by the Mimecast Threat Center; its aim is to provide in-depth information about the nature of attack campaigns, to observe and anticipate the evolving nature of these threats, and to provide a set of recommendations to help guide organizations' security decisions accordingly.

# Research Methodology

The Mimecast Threat Center Team conducted round-table discussions to produce this Report. Analysts utilize an uncertainty yardstick matrix which would be readily recognizable to any intelligence professional and which seeks to assign a probability percentage to any key assessments made and the likelihood of any predicted future outcomes being realized. Please see **Figure A** for the matrix utilized by the Mimecast Threat Center researchers, and the corresponding probabilities assigned to each assessment statement made throughout this report.

The team has the capability to research and study specific issues using the wealth of detection data collected by Mimecast but are also trained to utilize open source (OSINT) and research techniques to provide an in-depth analysis of an issue or attack, giving context to the range of threats and activity various threat actors take against customers. Working with a wide range of partner organizations including the security industry, academics, and law enforcement, the team aims to provide threat trends and insights to broadly increase cyber resilience for global enterprises and governments.

| Qualitative Term | Probability Range |
|---|---|
| ***Remote chance*** | ≤≈5% |
| ***Highly unlikely*** | ≈10% - ≈20% |
| ***Unlikely*** | ≈25 – ≈35% |
| ***Realistic probability*** | ≈40% – <50% |
| ***Probable*** or ***Likely*** | ≈55% – 75% |
| ***Highly likely*** | ≈80% – ≈90% |
| ***Almost certain*** | ≥≈ 95% |

***Figure A: The Mimecast Threat Center's Uncertainty Yardstick***

# Key Takeaways: 3 Minute Read

From October to December 2019, the Mimecast Threat Center analyzed more than 202 billion emails and rejected 92 billion. Overall, efforts to modify threats to evade detection within sandboxing continued, and some older forms of malware are being modified as extensively as newer forms of attack to evade detection. Alongside this malicious software, threat actors' impersonation efforts have reduced since last quarter, although they remain significantly heightened from those seen since **June-August 2019**.

Malware-centric campaigns are continuing quarter-over-quarter. As observed in previous threat research, these campaigns are increasingly sophisticated, using a diverse range of malware during the different phases of an attack.

The most striking observation of this quarter's research has been the widespread deployment of the **Emotet** "dropper" malware on a scale not seen before, across all regions. This subscription-based Malware-as-a-Service (MaaS) model increases the availability of simple attack methods to a wider audience, simultaneously keeping older, well-known malware in circulation. The use of fileless malware is also increasing, and criminals continue to put efforts into the use of impersonation attacks against businesses.

**Researchers detected and analyzed the following campaign insights:**

- There were **61 significant campaigns** against various business sectors during this quarter, marking a **145% increase** over last quarter.
- The attacks from October-December incorporated ***AgentTesla*, *Azorult*, *Barys*, Emotet, *Lokibot*, *Nanocore*, *Racoonstealer*, *Remcos*, and *Strictor*,** and involved a combination of mass generic Trojan delivery with complex, simultaneous threats preceding their deployment, at the same time or in subsequent days. During this quarter, however, **Emotet** has returned with significant detections noted throughout all sectors of every region on specific days. This discovery demonstrates a level of sophistication that goes beyond an opportunistic cybercriminal. In addition, due to the variety of businesses attacked, it's ***highly likely*** the attacks are carried out by highly organized criminal groups for monetary gain.
- **Emotet** activity became a significant component in every hybridized campaign identified. It had returned to greater activity in the previous quarter, on September 16, 2019, after four months of relative inactivity, initially utilizing a link-based attack vector before resuming its email attachment-related vector. This quarter, **Emotet** has been utilized far more extensively, and has been seen in widespread campaigns against all sectors of the global economy.
- Bulk emailing, or spam, remained a significant, high volume means to distribute malware, and it relied on human error for success. This vector is ***likely*** to continue as a powerful threat vector given it can be deployed in huge volumes, increasing the possibility of success for cybercriminals.
- While the volume of impersonation attacks decreased by 5% since last quarter, this attack vector is still a prominent threat. Along the same lines, because of the overall rise in impersonation attacks, voice phishing continues to be an advanced threat.

The campaigns observed in this quarter range from relatively simple phishing campaigns to complex, multi-vector campaigns that alternate file types, attack vector, types of malware and vulnerabilities. Compared to previous quarters, Mimecast researchers noted a marked difference in the significant attacks conducted: from October to December 2019, the attacks targeted a wider range of companies across various sectors and for shorter periods of time than in previous quarters. The holiday season drove attack campaigns in the Retail sector, for example, and continued their attacks over the course of just one or two days.

Specific campaigns have primarily been conducted in only one- or two-day periods, as opposed to the multi-day campaigns spotted last quarter, although the continued development of the hybridized (simple and complex attacks) threat noted in the last quarter has now evolved to include a significant **Emotet** component in almost all of its determined attacks, paired with additional forms of malware. Notably, the 61 attack campaigns in this report showed a significant uptick in the use of short-lived, high volume, targeted and hybridized attacks against all sectors of the global economy, as opposed to days-long attacks. This massive increase in activity is ***highly likely*** to be an indication of threat actors refocusing their efforts from impersonation to exploiting the current effectiveness of ransomware. The large number of significant campaigns that had ransomware components and malware delivery via **Emotet** is indicative of threat actors' efforts to maximize the utility of ransomware now, before organizations undertake significant cyber resilience measures.

# Analysis & Commentary on the Global Threat Landscape *Oct - Dec 2019*

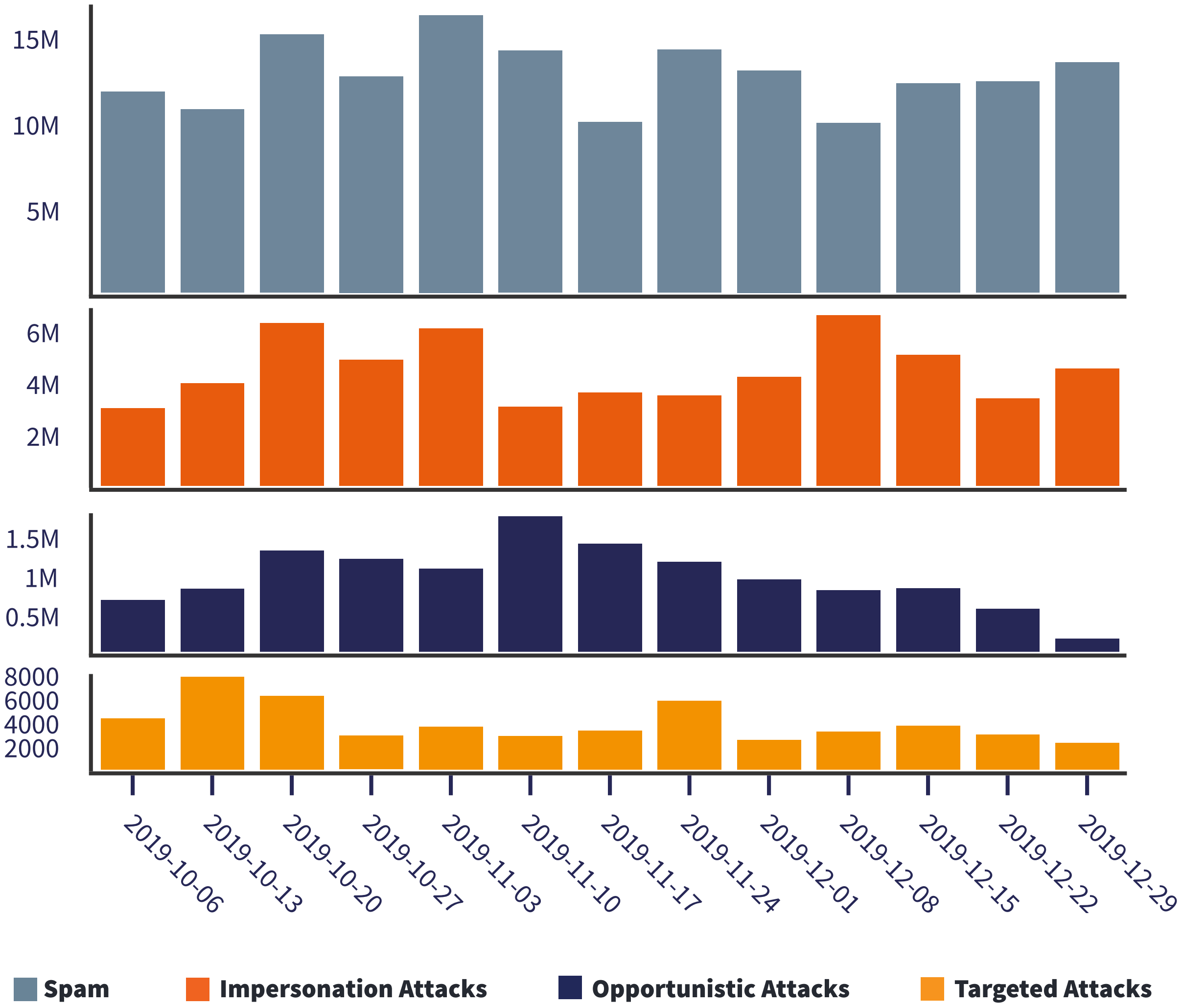
**The four primary threat categories analyzed in this report are spam, impersonation attacks, opportunistic attacks, and targeted attacks.**

Research shows these threats were distributed across all industry sectors and global regions due to the holiday shopping season.

Figure B below illustrates the volume of threats blocked across these four primary categories, showing peak volume on October 17, 2019 with 5,130,000 combined threats detected on that day alone.

In addition to the four primary threat categories, the Mimecast Threat Center analyzed the landscape for targeted attacks and malware.

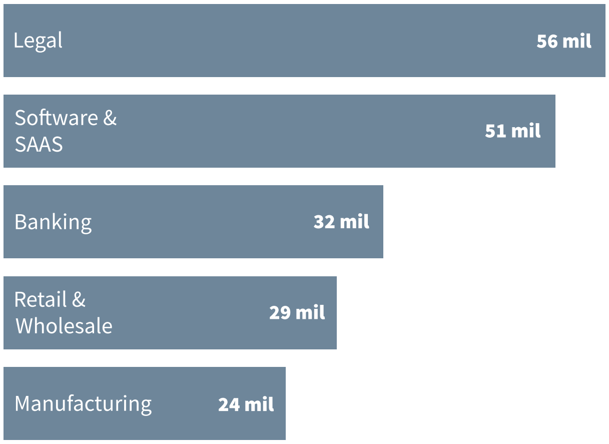
***Figure B: Volume of Threats Blocked Across Four Primary Categories***



## Spam Campaigns

**In the spam attack category, researchers found bulk email campaigns continued to be used to spread malware, targeting industry sectors including Legal Services, Software and SaaS, and Banking, as shown in Figure C.**

***Figure C: Top Sectors - Spam***



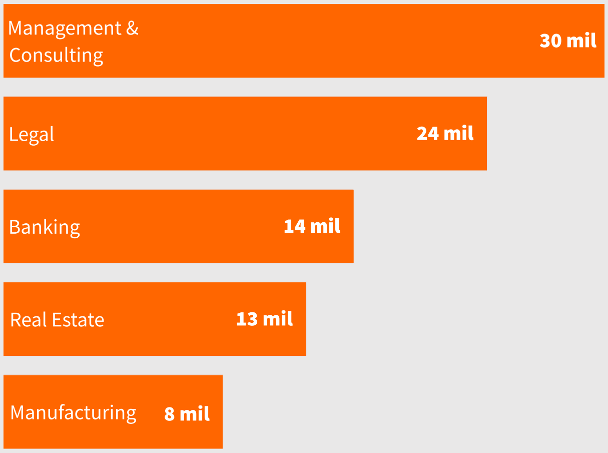
These are the same sectors as targeted in the last quarter, because they are key to criminal groups' monetary objectives. It is also noteworthy that their share of spam as a percentage of the overall figure has remained relatively stable and comparable to the previous quarter, despite higher total combined threats overall. Campaign volume was at its highest during the week ending November 3, 2019, with more than 24 million threats blocked in that week alone.

The increased spam activity in November coincides with significant increased **Emotet** activity, primarily its regular behavior in bulk emailing attachment spam. The spam module uses the botnet to send phishing emails containing malicious URLs or attachments. Other significant campaigns have coincided with more targeted attacks against the range of business sectors identified within this report, and this vector denotes the most common, en masse form of attack still taking place. This form of cheap, low sophistication, high volume attack vector remains the predominant method to spread malware. December 12, 2019 saw peak spam use for a single day during this quarter, with more than 116,000 detections on that day alone.

## Impersonation Attacks

**Social engineering - most commonly done through impersonation tactics - remains an effective tactic for threat actors and has shown a sustained increase throughout 2019, until this quarter.**

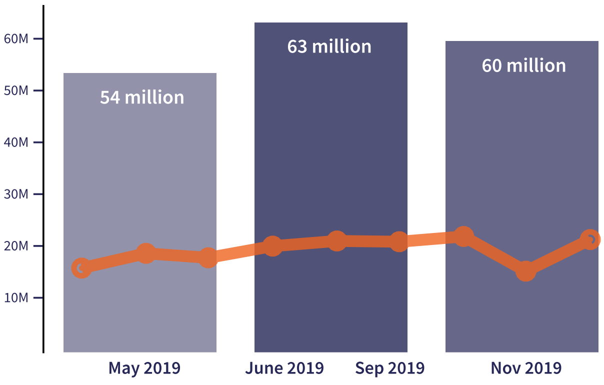
***Figure D: Top Sectors - Impersonation***



Attackers impersonate domains, subdomains, landing pages, websites, mobile apps, and social media profiles, many times in combination, to trick the target organization and/or its employees into surrendering credentials and other personal information, initiating fraudulent wire transfers, or installing malware. This increase in impersonation attacks that rely on social engineering, instead of tactics detectable through email scans, suggests an improvement in the industry's email scan efficacy – this is a continuation of what was reported last quarter, indicating a larger trend at play. There was significant reporting of ransomware attacks during 2019, including during the period October to December 2019, and it is ***highly likely*** that threat actors rebalanced their efforts during this quarter towards the delivery of ransomware through the bulk use of **Emotet** once it became operational again.

Management and Consulting again remains the primary target of impersonation attacks, continuing its nine-month streak; this industry accounts for 14% of threat volume as shown in Figure D. The Legal sector has also remained a significant target for this type of attack since the previous report, accounting for 11% of the attack volume. Due to the heavily interpersonal, social nature of these industries, Management and Consulting and Legal industries are suffering approximately twice as many impersonation attacks as other sectors.

***Figure D2: Blocked Impersonation Attacks***



Additionally, due to the monetary reward, the Banking industry has also remained a significant target and continues to suffer 7% of these attacks. Individuals at the C-suite level in Banking and those in positions with the ability to escalate privileges or access funds, such as finance, HR, and IT, have been heavily targeted and are at an increased risk of attack via impersonation. As with spam, the percentage of the overall volume targeting these specific sectors is consistent with last quarter.

Last quarter, researchers highlighted the evolution of impersonation into voicemail phishing messages; this form of attack has continued, and it is ***almost certain*** this form of attack will be used again in the coming year. Data shows impersonation attacks made up 26% of total detections from July-September, and the volume of these attacks grew by 18% in that time period. During this period, however, threat actors have re-focused on malware delivery via **Emotet** during this quarter, which may have led to a drop in voice phishing this quarter. Impersonation remains a significant focus for threat actors and if the current efforts they are expending on **Emotet** and ransomware delivery prove unsuccessful, impersonation tactics are ***highly likely*** to rise again.

The business email compromise (BEC)/impersonation figures for the period of the last three Mimecast Threat Intelligence Reports was 53.5 million between April and June 2019, 63 million between July to September 2019 (an increase of 18%), and 59.62 million during the period of this report (a reduction of 5.3%), remaining above the April-June 2019 figure (Figure D2).

## Opportunistic Attacks

**Opportunistic attacks are a fixture in the security industry; they utilize well-known malware and are expected to proliferate given they have shown sustained levels throughout 2019 and are relatively low effort for attackers.**

***Figure E: Top Sectors - Opportunistic Attacks***

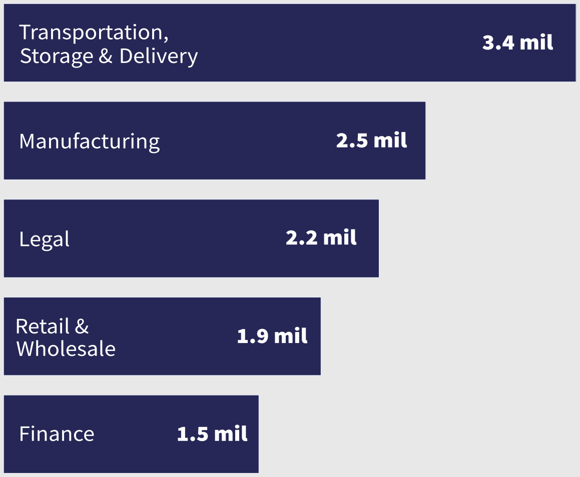


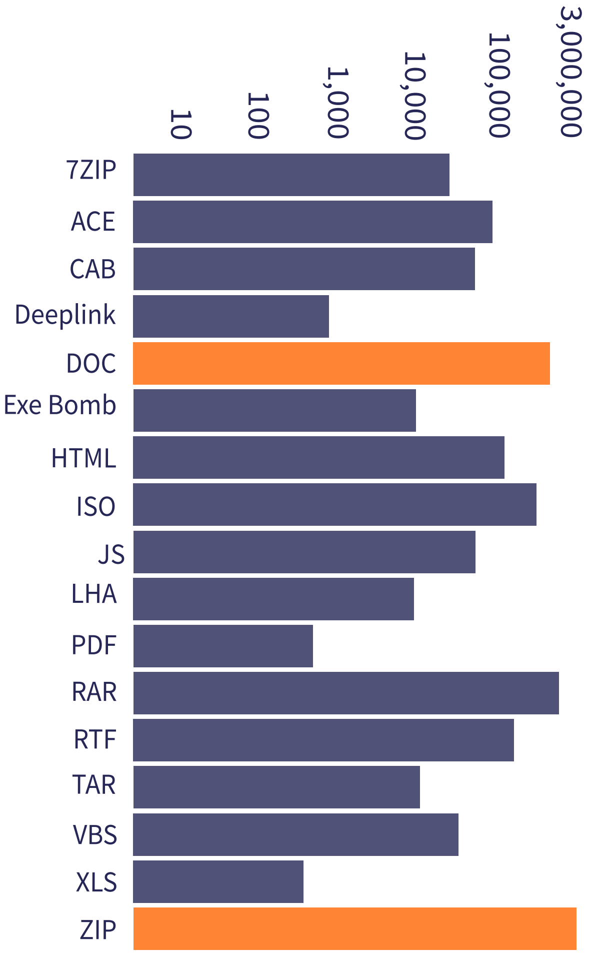
Figure E shows the Transportation, Storage and Delivery sector was subject to 9% of the opportunistic attack threat volume this quarter. Several significant and targeted attacks explored later on in this report have also sought to compromise this sector more determinedly, which is a new development since last quarter and can ***almost certainly*** be attributed to the continuing efforts of various APT actors, including state-sponsored advanced persistent threats (APTs), to target the logistics and supply chains of their rivals.

Manufacturing and the Legal sector suffered a significant 7% and 6% of the attack volume respectively. However, when compared to last quarter, these numbers are not as disproportionate.

# ZIPs & Tricks
## *Abstracts from Mimecast Global*

**The trend data in this section of the Threat Intelligence Report is based on Mimecast signature detections and does not include data from the other detection layers or applications available.**

***Figure E2: Mimecast Signature Detections***



**After analyzing data from all regions October-December 2019, the following patterns emerged:**

- **File compression continues to be an attack format of choice, but Emotet activity via DOC and DOCX formats has substantially increased.** Compressed files allow for a more complex, potentially multi-malware payload, but also serve as a very basic means to hide the true file name of any items held within the container. The ZIP format of file compression dominated detections – approximately 3 million throughout the quarter. Any available form of file compression format will remain the most attractive to threat actors.

- **Threat actors' concentration of effort into Emotet *highly likely* constitutes a significant refocusing of their efforts onto the attempted delivery of ransomware. Emotet** is an effective dropper of other malware as it is modular in nature and can deliver a variety of payloads. A number of significant campaigns utilizing **Emotet** have included ransomware detections, and it is ***highly likely*** that threat actors are focusing on the delivery of ransomware. In fact, Strictor and Teslacrypt were present in 25% of all detections - notable given ransomware tends to be a secondary infection post-malware compromise. Official advisories from the US, UK, and Canadian cyber centers since June 2019 have also stressed the particular threat **Emotet** poses in the targeted delivery of ransomware.

- **Specific sectors are repeatedly targeted, but growth in campaign activity due to the holiday season. The top sectors for attack globally are Transportation, Storage and Delivery, Financial: Banking, and the Professional Services: Legal sectors.** These three sectors have remained subject to high levels of attack throughout 2019, although the Transportation, Storage and Delivery as well as the Retail and Wholesale sectors were disproportionately attacked this quarter, accounting for almost a third of the most significant global campaign activity. However, given the holiday gift-giving season, much of this increase is to be expected.

- **Although the number of impersonation attacks is slightly fewer, they remain a key attack vector. Impersonation attacks now include a range of voice messaging and a generally less coercive form of communication, which presents as a more nuanced and persuasive threat.** It is ***highly likely*** impersonation reduced as a result of threat actors' focus towards the delivery of malware to exploit the monetary successes of ransomware attacks in 2019.

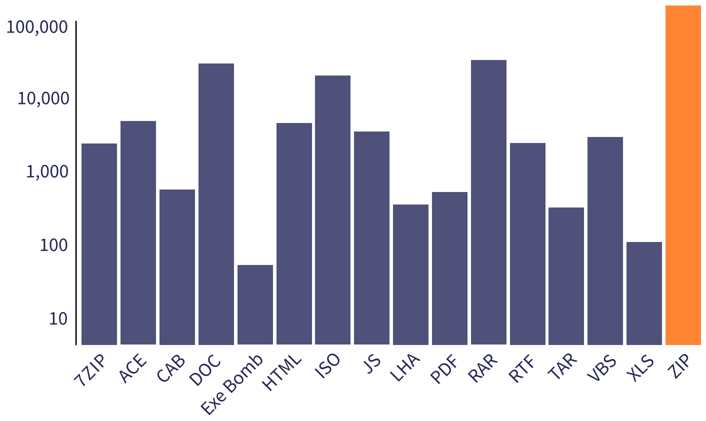
- **The overwhelming majority of attacks are again less sophisticated, high volume forms of attack, although more complex attacks are present and can take place over a period of several days.** This is ***almost certainly*** a reflection of the increasing ease of access to online tools and kits for any individual to launch a cyberattack, particularly the return of **Emotet** as a paid-for service. The trend also reflects the challenges of human error - even the simplest attacks can be successful. As attacks progress, they alter exploits and include more potent forms of malware and ransomware.

# Regional Trends

The regional data that follows is compiled from Mimecast's own detection signatures and identifies the specific file type or attack vector employed and detected. Across the entire region there are significant reductions in detections visible every Saturday and Sunday, indicating threat actors' tendency to take the weekends off.

## Trend Summary: Australia

***Figure F: Trend Summary Australia***



Australia, similar to all other regions this quarter, was subjected to more concentrated campaigns which heavily utilized **Emotet** in their attacks. ***Strictor*** ransomware was also present, and **Emotet** activity was also identified as a key threat during this quarter by the Australian Cyber Security Centre (ACSC) on October 24, 2019[1]. While the Education sector continues to be a significant target on a weekly basis, researchers also uncovered, for the first time, a significant campaign against the region's Transportation, Storage and Delivery sector.

Compared to the previous quarter, the Australian region suffered a significant increase in cyberattacks utilizing large volumes of **Emotet** malware, sometimes exclusively, to attack a wide range of sectors. In particular, the Education sector suffered sustained attacks. The volume and regularity of attacks appears to have increased, particularly with the attempted delivery of significant volumes of **Emotet** malware. Given the repeated nature of the threats and the resource and effort behind them, it is ***almost certain*** the threat actors involved represent an organized and determined criminal or state-sponsored threat. Targeting remains ***likely*** to be intended to impact or steal research and intellectual property, but may also be intended to monitor student activities or behavior, especially since Australia is becoming a key investment area for Chinese businesses over the USA, making it ***highly likely*** the future threat landscape will be negatively impacted in terms of the volume and complexity of threats and attacks. The region is also strategically key to US and Chinese interests and is ***likely*** to suffer increased targeting as a consequence of this importance.

Australia has experienced eight notable campaigns of significant volume against several sectors; this activity was significantly higher than in previous quarters and targeted a wide range of organizations and sectors of the economy.

## Technical Attack Campaign Detail:

1. On **October 3-4**, the Education sector was attacked primarily with large volumes of **Emotet** malware on the first day, followed by the inclusion of Windows 97 document exploits with **Emotet** on day 2. While the volume decreased on day 2, detection data remained higher than normal daily activity. **Emotet** accounted for the overwhelming majority of detections for malware against this sector on October 3, comprising more than 9,600 detections. Exploit **CVE-2017-0199** was also attacked.

2. **October 10-11** brought another attack against the Education sector; while this attack utilized **Emotet**, the volume was less significant as in the first campaign. Generic malware including Sagent and Zmutzy was also present. As in the previous attack, the second day introduced a large volume of Windows 97 document exploits in concert with **Emotet**, and in both attacks, Windows 97 document exploits accounted for nearly 50% of the detections. Because the makeup of both attacks was virtually identical, Mimecast researchers assess it is ***highly likely*** the same attacker was involved in both campaigns. Exploit **CVE-2017-11882** was attacked in this campaign.

[1] *https://www.cyber.gov.au/news/widespread-exploitation-vulnerable-systems-emotet-malware*

3. On **October 15**, the Education sector was again attacked, this time almost exclusively by a significant volume of **Emotet** malware, comprising more than 3,600 detections.

4. On **October 17-18**, there was again an attack against Education made up of more than 12,500 detections of **Emotet** malware, marking the highest volume of all attacks against this sector during this period. On day 2, another version of **Emotet** was utilized with more than 3,000 detections.

5. Between **October 22-25**, an even higher volume of **Emotet** malware was used to attack the Education sector, peaking more than 27,000 detections on the first day, 5,500 on day 2 with low-volume addition of ***Strictor*** malware, and more than 4,500 detections of **Emotet** on days 3 and 4 before the attack ceased.

6. The Government and public administration sector was also attacked between **October 22-25, 2019**. This campaign overwhelmingly utilized **Emotet** (7,796 detections on day 1). More than 4,500 **Emotet** detections were made on day 1, 2,900 on day 2, and reduced to 2,300 and 2,100 in the remaining two days of the campaign. This campaign, like the ones against the region's Education sector, overwhelmingly leveraged DOC attachments containing **Emotet** in huge volume attacks.

7. From **October 22-25, 2019**, the Transport, Storage and Delivery sector was also targeted over four days of activity, again, primarily utilizing masses of **Emotet** malware to attack the sector. On day 1 over 2,200 detections of **Emotet** alone were made, day 2 more than 1,500, day 3 over 1,900 and day 4, an apparent last push of 2,900 detections. The exploits **CVE-2017-0199**, **CVE-2017-8570** and **CVE-2017-11882** were also attacked during this campaign.

8. In the final major campaign against the region, the Manufacturing sector suffered an attack from **October 22-25** that exclusively used masses of **Emotet** malware. Over the course of four days, the sector had in excess of 6,700 detections related to **Emotet**. As with the attack on the Transport sector, peak activity was detected on the first and last days of the campaign.

Although these campaigns represent the most significant during this quarter, research found that peaking activity against all sectors of the Australian regional economy occurred on specific days of heightened **Emotet** activity. This was found to be a significant component in almost all of these attacks and periods of heightened **Emotet** activity was noted in all of the other regions monitored, except for Continental Europe.

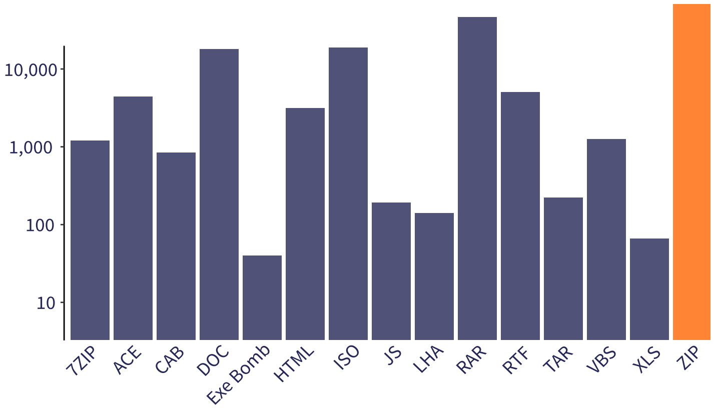
**Targeting remains likely to be intended to impact or steal research and intellectual property, but may also be intended to monitor student activities or behavior.**

*Trend Summary Australia*

# Trend Summary: Continental Europe

In Continental Europe, unlike other regions, the Transportation, Storage and Delivery sector suffered all of the identified, most significant campaigns for the region during this quarter. However, much like other regions, **Emotet** was detected in nearly all campaigns, along with additional significant threats ***AgentTesla***, ***Lokibot***, Nanobot, ***Racoonstealer*** and ***Remcos***. It is also noteworthy that ***AgentTesla*** and ***Strictor*** ransomware were detected during these attacks. The use of ransomware has exploded this quarter, and given its rapid rise since last quarter, it should be considered an increasing threat during 2020.

***Figure G: Trend Summary Continental Europe***



Given the consistency of the attack vector during these campaigns, it is ***highly likely*** the criminal group targeting this sector is the same for each of these attacks. The repeated targeting of this sector will proliferate as threat actors seek to compromise the logistics infrastructure of the organizations targeted and potentially use any compromise as a means to launch additional third-party attacks against any organizations linked to their targets.

The four cyberattack campaigns in this region highlight a move towards more significant targeted activity, for example, the Transportation, Supply and Delivery sector saw repeated, sustained targeting.

## Technical Attack Campaign Detail:

1. On **October 3, 2019** the Transportation, Supply and Delivery sector was targeted. The attack primarily utilized **Emotet** malware in DOC and DOCX formats and the version used utilized Macros, obfuscation and anti-analysis capabilities; also, the title of attachments concentrated on the words “Payment” and “DOC.” Complementing this were RAR and ZIP files containing the generic Trojans Agensla, Bladabindi, Crypt, Eldorado, Kryptik, Kryjetor, Mokes, Noon, Spygate and Zmutzy. The more significant threat detected, besides **Emotet**, was ***Lokibot***.

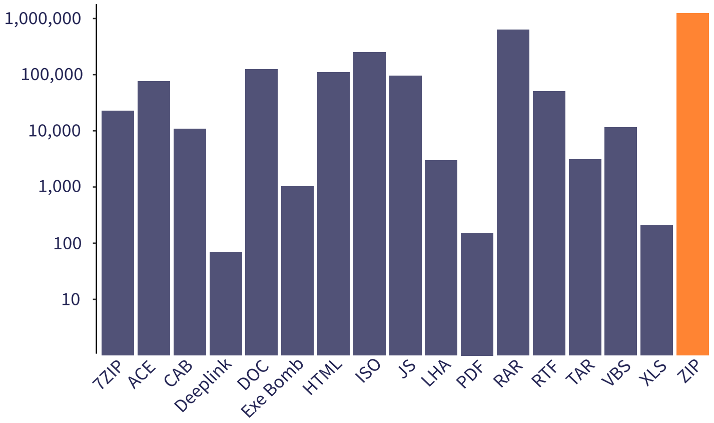
2. The sector was targeted again from **October 25-29, 2019**, again, primarily by **Emotet**.

3. Between **December 9-10, 2019**, Transportation was targeted by **Emotet** in DOC format. This version employed macros and obfuscation capabilities, and it was complemented by a significant number of RAR files containing generic Trojans including Andromeda, Eldorado, Krypt, Kryptik, Razy. ***AgentTesla***, ***Racoonstealer*** and ***Remcos*** were also detected. ZIP files containing Floxif, Kryptik, Dothetuk and Zmutzy were also present. A prominent courier brand featured during the campaign, and files primarily referenced POs (purchase orders), Invoice or INV.

4. Lastly, from **December 12-13, 2019**, a high volume **Emotet** campaign was used against the Transportation sector. This time, the version was more simplistic, without obfuscation or anti-analysis. Complementing this were RAR files containing generic Trojans Eldorado, Predator, ***Racoonstealer***, ***Strictor*** and Sonbokli. ZIP files containing further generic Trojans included Andromeda, Eldorado, Delphiless, Dothetuk, Kryjetor, Predator, and Zmutzy.

# Trend Summary: United Kingdom

*Figure H: Trend Summary United Kingdom*



The UK region suffered cyberattacks across a range of its sectors; this quarter illustrates the diversity of the threat posed to the UK's various organizations and sectors. The Transportation, Delivery and Supply sector has consistently been in the top three targeted sectors throughout 2019 and this quarter; the UK Legal and Finance sectors have also been persistently targeted. Similar to Australia, the Retail sector suffered repeated attacks, which can be attributed to the holiday shopping season.

The key threats detected in the UK region were ***Azorult***, ***Barys***, **Emotet**, ***Lokibot***, ***Strictor*** and Trickbot; the increase in ***Barys*** malware is related to Dropbox implementation, and is indicative of the increasing trend towards fileless malware. Most of the significant campaigns witnessed in the UK during this quarter involved a combination of **Emotet** and other mass generic Trojans combined with more complex threats at the same time and/or in subsequent days. This shows a level of sophistication beyond that of an opportunistic attacker, making it ***highly likely*** most of the identified attacks were carried out by organized criminal groups for monetary gain, particularly given the disparate sectors of the economy attacked.

Notably, research found that peaking activity against all sectors of the UK regional economy occurred on specific days of heightened **Emotet** activity – this finding is consistent with all other regions except Continental Europe.

Seven campaigns emerged this quarter due to their complexity, the threats detected and their significant volume.

## Technical Attack Campaign Detail:

1. On **October 15, 2019**, the Professional Services: Legal sector was attacked. ZIP, RAR and ISO image formats featured prominently in these attacks. Detections included a range of generic Trojans, although more than 40% of detections were related to **Emotet**. A courier delivery brand also featured significantly as an attack vector, as did the use of image files and "/temp/eml_attach_for_scan/" due to their ability to evade scanners. Additionally, the attackers attempted to exploit the vulnerabilities **CVE-2017-3077** and **CVE-2017-11882.** The most attacked vulnerability was **CVE-2017-11882.**

2. From **November 7-8**, a campaign against the Retail/Wholesale sector occurred, using generic Trojans such as Agensla, Kryptik, and Ursu in concert with the more potent threat of **Emotet**, which was macro-based and hid application usage. Notably, there was no apparent attempt to target specific vulnerabilities during this two-day campaign, suggesting a broad-strokes approach to the attack in advance of the holiday season.

3. The UK also saw a campaign against the Finance: Banking sector from **November 7-8**, primarily comprising DOC files delivering **Emotet** and supplemented by RAR and ZIP files containing purportedly scanned or copied documents. Generic Trojans Agensla and Nymeria were also present, along with ***Barys***, Pantera, Razy, Sylkagent, and ***Azorult***. Notably, ***Barys*** was detected in more volume than has been seen in any previous quarter's research, and given it implements Dropbox researchers believe it will become more commonly used in future attacks.

4. From **November 12-15**, the Professional Services: Legal sector was attacked via ZIP and RAR formats, but the use of ISO and other image files was significantly lowered from those seen on the October 15 campaign. The attack primarily utilized a range of generic Trojans and phishing emails with attachments; the more significant threats included significant use of **Emotet** with the addition of ***Lokibot***. "/temp/eml_attach_for_scan/" featured as a key delivery focus of the attachments; the **CVE-2017-11882** exploit was also again attacked.

5. On **November 18**, Retail/Wholesale was attacked via **Emotet** DOCs comprising more than 3,000 detections against the sector on that day, although the version utilized did not contain significant obfuscation or anti-analysis measures. The complementing malware utilized was in an array of file types including ACE, ZIP, RAR, and ISO files which contained Bladabindi, Crypt, Kryptik, Midie, Noon, and Razy Trojans. The file extension temp/eml_attach_for_scan/ again featured in this campaign as did a well-known courier brand. Exploits **CVE-2017-8759** and **CVE-2017-11882** were also attacked.

6. On **December 9-10**, the Finance sector was subjected to a malware campaign utilizing RAR files almost exclusively, rising in volume from more than 10,000 detections on the 9th to more than 30,000 on the 10th. Considerably lesser supporting complements of ACE and ISO files containing generic malware and Trickbot were also detected as were DOC attachments containing **Emotet**. Again, the version utilized did not have significant obfuscation or anti-analysis capabilities. Exploit **CVE-2017-11882** was again attacked.

7. On **December 20**, Retail/Wholesale was attacked for the last time in 2019. As on **November 18**, attackers used a large quantity of **Emotet** DOCs, accounting for more than 4,000 detections which again did not contain significant obfuscation or anti analysis measures; this was complemented by a diverse array of files including ZIP, RAR, ACE, and ISO formats containing Agensla, Kryptik, Nanobot, and Zmutzy. **CVE-2017-11882** was again also attacked. The term “module” and “/temp/eml_attach_for_scan/” were features of the attachment titles

The UK regional Retail/Wholesale sector suffered high levels of detections throughout December 2019 when compared to its usual detection activity. In fact, the dates reported cover only those noted as the most significant volume campaigns; the month of December saw many days where activity against this particular sector fell just short of significant detection thresholds included in this report and, therefore, indicates the tremendous targeting of this sector during peak holiday sales season.

**...most of the identified attacks were carried out by organized criminal groups for monetary gain.**

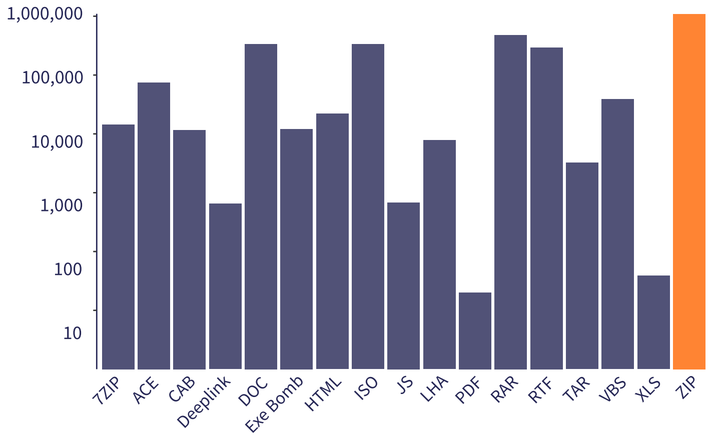
*Trend Summary United Kingdom*

# Trend Summary: USA

Due to the higher volume of businesses headquartered in the U.S., threat detections tend to be higher overall; in fact, the U.S. suffered both the highest number of campaigns and the highest levels of detection volume during the quarter against nearly every sector of its economy. As with all other regions, high usage of **Emotet** was apparent, and compressed file formats remained a common attack vector, behaving as a complement to **Emotet** during this quarter.

Retail/Wholesale was repeatedly attacked this quarter due to the holiday shopping season, as criminals attempted to gain from consumers' increased spending this period.

***Figure I: Trend Summary USA***



The key malware detected against the U.S. region this quarter included ***Barys***, Cottonmouth, Hawkeye, Nanobot, Netwire, ***Remcos*** and ***Strictor*** and Teslacrypt ransomware, while every campaign utilized a mixture of generic Trojans with more significant threats. On their own, this diverse range of threats against networks is capable of inserting ransomware, implementing Dropbox, and compromising USB devices, Windows, and Mac devices. It is ***almost certain*** that the current heightened campaign activity utilizing the key threat of **Emotet** is also driven by the intent to deliver ransomware, as in all other regions. In nearly all campaigns, the exploit **CVE-2017-11882** was attacked, as well as the /temp/eml_attach_for_scan/ string, indicating attackers' attempt to evade detection from scanners through image files.

Although the campaigns detailed represent the most significant during this quarter, research found that peaking activity against all sectors of the U.S.' regional economy occurred on specific days of heightened **Emotet** activity.

The majority of attacks in the U.S. are concentrated, single-day campaigns, and a few days stand out for their huge volumes of multi-sector **Emotet** campaigns on October 2, October 14, and December 16-17. Targeted campaign activity in the U.S. increased this quarter; 27 significant, standout campaigns were identified for this report, whereas just 6 were of note in the previous report.

## Technical Attack Campaign Detail:

### October 2, 2019:

1. The Construction sector experienced a significant volume of **Emotet** detections in DOC format, comprising more than 4,000 detections. Interestingly, this campaign utilized a mixture of **Emotet** and VBA-based variants and these versions had either anti-analysis capability or anti-analysis, obfuscation and VBA hidden processes.

2. On the same day, a campaign against the Health and Social Care: Hospitals and Clinics sector experienced more than 7,000 detections of overwhelmingly **Emotet** in DOC format, and was complemented by other generic obfuscated VB droppers in DOCX format.

3. A campaign against the IT sector comprised more than 1,000 **Emotet** detections and also utilized anti-analysis and VBA hidden process capabilities, complemented by obfuscated VBA droppers utilizing obfuscation and a significant volume of ZIP, RAR, ISO and 7ZIP files containing Andromeda, Agensla, Bobik, Cryxos, Hawkeye, Kryjetor, Kryptik, ***Lokibot***, Noon, ***Remcos***, and Zmutzy Trojan malware.

4. A campaign took place against the Retail/Wholesale sector. A core **Emotet** component was again used but in two separate versions, both DOC- and DOCX-based; the former utilized only VBA hidden processes while the latter was obfuscated. The attack on this sector was complemented by large numbers of VB-based Trojans and ZIP, RAR, ISO and ACE files containing malware. A high volume of more basic phishing emails was also detected.

### October 4, 2019:

1. A further campaign took place against the Health and Social Care: Hospitals and Clinics sector, again utilizing exclusively **Emotet**, with more than 4,500 detections. This version of the malware utilized anti-analysis and VBA hidden processes.

### October 14, 2019:

1. The last campaign against the Health and Social Care: Hospitals and Clinic sector took place with a significant increase to approximately 22,000 **Emotet** detections, although this version of the

malware again utilized anti-analysis and VBA hidden processes. Low numbers of ZIP and RAR files were also utilized containing other Trojan malware including Agensla and Kryjetor.

2. A campaign was launched against the Transport, Supply and Delivery sector, with more than 8,000 **Emotet** DOC detections in a version with anti-analysis and VBA hidden process capabilities. This was complemented by an array of other file types including ZIP, 7ZIP, RAR, RTF, ISO, and ACE.

3. The Finance: Banking sector experienced a campaign utilizing **Emotet** in DOCs with more than 5,000 detections. Like the October 2 campaigns, the version utilized on this occasion had anti-analysis capabilities and hidden VBA processes, and this core component was supplemented by attacks via ZIP, RAR, and ISO formats containing the generic Trojans Agensla, Hawkeye, Kryjetor, and ***Strictor*** ransomware. Exploit **CVE-2017-11882** was also attacked.

4. The Insurance sector experienced a significant campaign primarily made up of **Emotet**, with more than 6,000 detections and had anti-analysis and VBA hidden processes, supplemented by ZIP, 7ZIP, RAR, ACE and ISO files containing Kryptik, Zmutzy and ***Strictor*** ransomware. This campaign appeared to essentially be structured the same as the campaign on the same day against the Banking sector.

5. A campaign against the Manufacturing: Electronics sector utilized a core component of **Emotet** amounting to more than 3,000 detections, supported by a complex array of files including ZIP, RAR, ACE, ISO, RTF and encrypted files. These utilized Fareit, Kryjetor, Noon, Occamy, Ursu, and Zmutzy, malware. ***Lokibot*** was also detected. In addition, the MyDoom worm was also detected in high volumes as complementing malware in a later attack against this sector.

6. A campaign against the Mining and Extraction sector included a significant **Emotet** component comprising more than 3,000 detections and supplemented by a significant number of phishing emails and a complex mix of file types, as seen with other campaigns against other sectors on the same date.

7. The Construction sector experienced another campaign, again using bulk **Emotet** malware in DOC format with over 8,000 detections containing a mix of anti-analysis and VBA hidden processes. Complementing this were ZIP, 7ZIP, RAR, ACE, RTF, and ISO files including Sagent and Nanobot malware.

8. The IT sector endured a campaign with more than 4,000 detections of **Emotet**, again with anti-analysis and VBA hidden process capabilities supported by a complex range of other malware in ZIP, RAR, RTF, and ISO image formats, including Agensla, Andromeda, Kryjetor, Kryptik, Razy, Ursu, and Zmutzy Trojan malware. Nanobot was also detected.

9. A campaign against the Mining and Extraction sector included a significant **Emotet** component comprising more than 3,000 detections and supplemented by a significant number of phishing emails and a complex mix of file types, as seen with other campaigns against other sectors on the same date.

10. A campaign against the Professional Services: Legal sector took place; the core component of more than 6,000 **Emotet** detections was supported by a number of other file types, and the version utilized has anti-analysis and VBA hidden process capabilities. The malware complementing this campaign was present in an array of formats including ZIP, RAR, ISO, and 7ZIP. The generic Trojans detected were Fareit and Zmutzy. The campaign also featured a significant number of more basic phishing attempts.

11. The Retail sector experienced a significant **Emotet**-based campaign, featuring more than 16,000 **Emotet** detections. This was supplemented by a diverse and complex range of other threats contained in significant numbers of ZIP, RAR, ACE, 7ZIP, and ISO files.

### October 17, 2019:

1. A complex hybridized campaign took place against the IT sector, this time without any significant **Emotet** component. Instead, the attack primarily utilized ZIP and RAR files supported by ISO and ACE formats and containing Agensla, Crypt, Eldorado, Fareit, Perseus, and Ponystealer Trojans.

### October 25, 2019:

1. In the Banking sector, researchers saw a further campaign with over 600 **Emotet** detections at its core. This version of **Emotet** utilized VBA hidden processes with no significant obfuscation or anti-analysis capabilities, complemented by ZIP, XLS, and ISO files containing the generic Trojans Kryptik and Pantera. Coin miners were also detected.

### November 5, 2019:

1. The Construction sector experienced another campaign, for the last time in 2019. It a comprised a core component of more than 3,000 **Emotet** detections accompanied by a significant wave of over 4,000 phishing emails. The version of **Emotet** used utilized VBA hidden processes with no significant obfuscation or anti-analysis capabilities. These were complemented by ZIP, RAR, ACE, and ISO files containing Cottonmouth, Ponystealer, ***Lokibot*** and Netwired Trojan malware.

2. A further attack took place against the Manufacturing: Electronics sector, this time utilizing a higher volume of phishing emails (over 3,000) and an accompanying **Emotet** component. This version utilized VBA hidden processes but no significant obfuscation or anti-analysis capabilities.

3. The Retail sector's campaign featured significant numbers of **Emotet** (over 4,000) supported by a complex array of malware contained in ZIP, RAR, ISO, and ACE files. The **Emotet** version utilized had only VBA hidden process capabilities, and Trojan malware was detected along with the more significant ***Barys***, Nanobot, Netwire and ***Strictor***, and Teslacrypt ransomware threats. A significant number of phishing emails also accompanied them.

### November 9, 2019:

1. In the IT sector, Mimecast researchers discovered a huge volume of solely phishing email-based campaign, comprising over 15,000 detections.

### November 11, 2019:

1. A final campaign against the IT Sector again comprised predominantly phishing emails, again with over 15,000 detections. This time, however, the phishing emails were supplemented by significant numbers of ZIP files in combination with 7ZIP, RAR, and ISO files. Trojans detected included Kryjetor, Noon, Ponystealer, Razy, and Zmutzy; ***Barys*** was also detected.

2. A further campaign against the Professional Services: Legal sector concentrated on the overwhelming delivery of thousands of ZIP- and RAR-based files containing malware and attempted JS script injection. The Trojans Oroles, Sagent, and ***Remcos*** were detected.

3. A final campaign took place against the Manufacturing: Electronics sector - this time activity was focused on a complex mix of file types with significantly less **Emotet** detections, with no noteworthy characteristics. There was however also a significant increase in basic phishing emails to complement the malware. ZIP, 7ZIP, RAR, ACE, ISO, and encrypted files were detected in these emails.

4. The Retail sector experienced a diverse campaign of files, and a lesser **Emotet** component with no advanced capabilities. DOC, ZIP, RAR, ISO, ACE, RTF, and 7ZIP files were all utilized in significant numbers, many including encryption. This was also complemented by significant numbers of phishing emails, and as with attacks against the Manufacturing sector, the MyDoom worm was also detected. The subsequent days increased the volume of **Emotet** mixed with volume phishing but reduced each day until the 14th when activity finally ceased.

### December 17, 2019:

1. A final campaign against the Banking sector took place with over 5,000 XLS documents and a high volume of DOC files which included an **Emotet** component of over 790 detections although unlike most other campaigns, the version utilized had no significant obfuscation or anti-analysis capabilities. The additional malware detected was contained in a complex array of ZIP, RAR, DOC, ACE, PDF, RTF, and XLS formats. Attempted use of LOLBins was also detected and Trojans including Kryptik, Pantera, Sagent, and Sylkagent were also detected.

2. The Transport, Supply, and Delivery sector experienced its last attack over the course of two days, from December 16-17. On the 16th there were over 5,000 DOC **Emotet** detections that used two versions, one of which was obfuscated and the other with no significant additional capabilities. On the 17th the campaign altered in much the same way as that against the retail sector, with the addition of a lesser ZIP, RAR, and ISO format component.

3. A further campaign took place against the Retail sector from December 16-17. On the 16th, attackers commenced utilizing a core component of two different version of **Emotet**: one version was obfuscated and the other had no significant capabilities, and both versions made up over 5,000 detections. The threat actors again attempted to exploit LOLbins, and a complementary component of ZIP, RAR, and ISO files was also used. On December 17, the campaign included new formats and malware, while the **Emotet** component was maintained at the same level with two mixed versions.

Given the predominance of **Emotet**, single-day attacks, bulk threats, file-less malware and additional significant threats, it is ***highly likely*** that all the campaigns in the U.S. were carried out by organized criminal groups for monetary gain. As in the other regions there is evidence of ransomware detection alongside **Emotet** and it is ***highly likely*** that criminal efforts in this region, as well as globally, are targeting a wide range of verticals for the insertion of ransomware.

Given the similarity of detections across sectors on specific days. It is highly likely the detections were undertaken by the same threat actor group. However, it is ***unlikely*** that a single group undertook all of this activity due to the level of resources this would require. In any case, each of the groups should be considered as well-resourced and capable, if not state-sponsored or affiliated.

**The majority of attacks in the U.S. are concentrated, single-day campaigns.**

*Trend Summary USA*

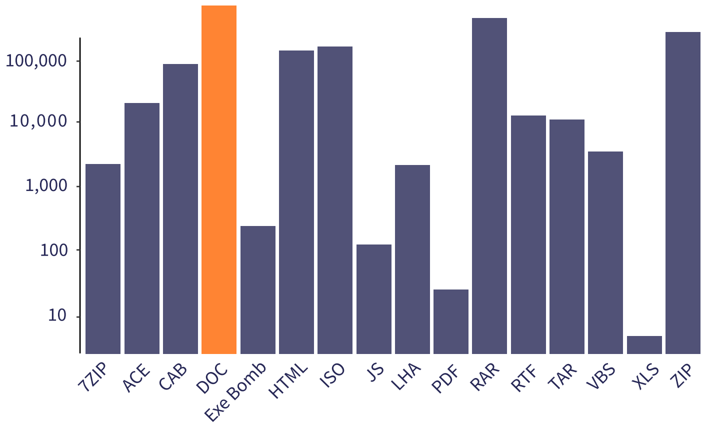
# Trend Summary: South Africa

The South African region suffered 14 major attacks this quarter; threat actors targeted a wide range of sectors on specific dates in November and December, which is similar activity in all other regions except Continental Europe. In addition, the attacks that had besieged the financial sector in the last quarter gave way to a more widespread targeting of multiple organizations, and are now heavily utilizing **Emotet** and image files for malware and ransomware delivery.

As in other regions, **Emotet** activity was present as a key malware component in every significant campaign identified in the region during this period. Far more diverse activity has taken place during this period, with a number of significant campaigns against a wide range of sectors. The diversified attack activity remains high volume but less concentrated; in particular, key campaigns mainly took place alongside notably increased **Emotet** activity. As in the U.S., most campaigns expressed versions of **Emotet** with no obfuscation or anti-analysis capabilities. The file extension temp/eml_attach_for_scan/ was commonly featured in campaigns, as well as the exploit **CVE-2017-11882.**

Similar to other regions during this quarter, **Emotet**, Nanobot, ***Lokibot***, ***Remcos***, and ***Strictor*** ransomware were the most significant threats deployed against this region, utilized in concert with a range of generic Trojans.

***Figure J: Trend Summary South Africa***



## Technical Attack Campaign Detail:

### November 11, 2019:

1. A campaign against the IT sector took place, utilizing a core component of over 500 detections of **Emotet** malware supported by other generic trojans including ZIP files containing Agensla, Hesv, Kryptik, Noon, and Zmutzy. ***Strictor*** ransomware was also detected and ***Barys*** was detected in TAR files. RAR files were also utilized to attempt delivery of Kryjetor, Ponystealer, Predator, and Nanobot. Sagent malware also accompanied the **Emotet** DOC delivery. IMG and ISO files also featured as an additional means of malware delivery.

2. The Transport, Storage and Delivery sector was attacked with over 1,000 **Emotet** detections. Much like other campaigns in this region and in the U.S., two versions of **Emotet** were used which activated via macro and contained no significant attempt at obfuscation or anti-analysis capabilities.

3. The Retail/Wholesale sector was attacked; **Emotet** delivered in DOC format was again utilized, absent significant obfuscation and anti-analysis capabilities. It was hybridized with ZIP documents containing Agensla, Kryptik, ***Strictor***, and ***Remcos***, and RAR files containing Agensla and Nanobot.

4. The Finance: Insurance sector was subjected to a significant campaign; an **Emotet** component comprising over 600 detections was core to a campaign supported by Sagent DOC files, ZIP files containing Zmutzy, RAR files containing Eldorado and ISO images containing Noon malware.

5. The Manufacturing sector was subject to attack; like other campaigns in this region, the first attack on the 11th utilized a core **Emotet** component of over 600 detections. This was supplemented by DOCs containing Sagent, ZIP files containing the generic Trojans Agent W, Crypt, and Graftor, and RAR files containing ***Remcos***. The **Emotet** version used remained unobfuscated.

6. The Finance: Banking sector was also subjected to a significant campaign between November 11-14. On the 11th a significant **Emotet** component comprising over 1,400 detections was core to a campaign again supported by Sagent DOC files, ZIP files containing Kryjetor, Noon, Zmutzy, and ***Remcos***; RAR files containing Kryptik, Noon, and Nanobot, and over 400 ISO images containing malware. Ponystealer was also detected.

### November 14, 2019:

1. In the Finance: Banking sector, on the 14th, unlike other attacks, cybercriminals increased the **Emotet** component and only slightly increased the image-based malware component via ISO to over 600 detections. Cottonmouth and ***Strictor*** ransomware were also detected, and interestingly, multiple detections of Cottonmouth denote that individuals are ***almost certain***ly attempting to com-

promise banking networks in the region utilizing malware intrinsic to a compromised USB cable or device.

2. The IT sector experienced its second campaign, which was quite similar to the November 11 attack; it again utilized a core component of more than 500 **Emotet** detections, supported by generic Trojans including ZIP files containing Crypt, Kryptik, Perseus, and Zmutzy. ***Remcos*** was also present. RAR files were also detected containing Kryptik and Noon. IMG and ISO files featured as a significant means of malware delivery with other 1,500 detections.

3. The Transport sector was again attacked, relying on a blend of more than 600 **Emotet** detections. This attack was unique in that it utilized far more images in ISO format, and it was supplemented by ZIP files containing Kryptik and Zmutzy.

4. The Finance: Insurance sector experienced a continuation of the November 11 attack; the cybercriminals reduced the **Emotet** component to just over 300 detections and significantly increased the image-based malware component via ISO to over 1,500 detections.

5. The Manufacturing sector experienced a continuation of the November 11 attack. Nearly identical to other sectors, the campaign reduced its reliance on **Emotet** and relied more heavily on ISO or image related files which comprised over 1,000 detections. ZIP files containing Ulize and RAR files containing Agensla, Eldorado, Noon, ***Lokibot***, and ***Remcos*** also supplemented this.

6. As with the other campaigns noted, a second day of activity against the Retail sector took place with a core **Emotet** component, comprising more than 500 detections and supplemented by ZIP files containing Eldorado and Hawkeye, and RAR files containing Andromeda. Valyria was also detected.

**December 5, 2019**

1. The Transport, Storage, and Delivery sector was subject to its third attack. The campaign utilized a significant volume of **Emotet** in over 2,000 detections, but this time, there were significant levels of obfuscation. This was complemented by the volume use of ZIP, RAR, XLS, and ISO files containing Agensla, Fareit, Kryjetor, ***Remcos***, and Ulise malware. The word “Order” and the attachment string /temp/eml_attach_for_scan/ again featured, indicating the appearance of social engineering tactics.

2. The Mining and Extraction sector was subject to attack; the core component on this occasion was a large volume of ISO image files with over 1,700 detections containing Kryjetor and ***Strictor*** ransomware, supplemented by an **Emotet** component of over 700 detections which was now obfuscated in this campaign. ZIP and RAR files also supplemented these attacks containing the trojans Kryjetor, Kryptik, Ponystealer, and ***Remcos***.

**December 10, 2019:**

1. In the last significant campaign in the region, the Finance: Banking sector was targeted. This campaign switched to utilizing a core component of almost 4,000 phishing emails supported by a significant **Emotet** component of over 800 detections and a mix of ZIP, RAR, TXT, and ISO files containing Trojans Agensla, Cryxos, Kryptik, Nanobot, and Symmi. The version of **Emotet** utilized did not contain significant obfuscation or anti-analysis capabilities. A prominent courier company again featured, as did the attachment string /temp/eml_attach_for_scan/ and the words INV and Invoice, highlighting attackers’ ongoing commitment to monetary gain via phishing in this sector.

Unique to the region, the attacks against the South African region occurred within a short time frame during which a range of organizations across sectors were repeatedly targeted. Given the similarity in attack vectors and the make-up of the attacks it is ***highly likely*** the threat actors are the same for each and all of the periods of activity noted against the various sectors attacked on both November 11th and 14th. The resources required to target several sectors of the economy and multiple organizations would be considerable.

**The attacks that besieged the banking sector last quarter gave way to widespread targeting of multiple organizations across sectors.**

*Trend Summary South Africa*

# What Can You Do?

**This research demonstrates attackers' attempts to utilize phishing or malware to defeat detection methods through the exploitation of human error. At the same time, it demonstrates their ability to adapt to email scan efficacy; they were creative in the deployment of hybridized campaigns with a broad target-based approach to different industries.**

**Despite these challenges, a proactive approach to cybersecurity involves monitoring the external environment for cyber threats to detect system breaches when they happen, adopting tools such as network penetration testing, strict controls governing access to internal systems, vulnerability scanning tools, data encryption, timely security updates, and network monitoring.**

**Given the increased determination in relation to the delivery of specific volume malware, particularly Emotet, which criminal adversaries have shown during this quarter, the Mimecast Threat Center recommends:**

## 1 Emphasize the importance of security controls and resilience.

As **Emotet** and related threats of ransomware delivery have significantly increased, now is the time for organizations to seriously consider their ability to recover from a successful attack when it happens to them and consider in detail how the organization might continue business as usual under circumstances where there is a potential recovery time of six months and the **loss of crucial data**. Only fallback capabilities in relation to cloud and web-based email and **data archiving** can provide this kind of business continuity.

## 2 Make patching to remain up-to-date a business priority and reduce shadow IT.

Clearly articulate the enhanced level of threat faced by older, unsupported or obsolete technologies when they are still used to do business; regional detection data indicates cybercriminals continue to exploit CVEs that should be patched to avoid this. In addition, organizations should be alert to the threat of shadow IT, and particularly the potential for malware exploit delivery via outdated or aging machines and browsers. If these operate using unsupported operating systems which are no longer being patched or updated, then this risk should be considered severe.

## 3 Increase Security Awareness Training.

Keep users informed on current, prevalent threats; this should be a priority to avoid the risk posed by simple human error.

Indeed, this is of paramount importance now, given the mounting risk around impersonation attacks and voicemail phishing attacks.

## 4 Enforce a strict password regime for users and admins.

Given the particular capabilities of **Emotet**, which seeks to brute force commonly used passwords on infection, avoid the use of weak passwords. To prevent initial infection, users should NOT routinely enable macros within any electronic documents received. Allied to this, organizations should review their administrative passwords and ensure they have modified any default administrative passwords in the same way. These passwords are key to breaching a network and strong password discipline should be the default for them.

## 5 Implement two-factor authentication whenever possible.

This should be utilized on any application or log-in available.

Security for any organization going forward will require a comprehensive, layered approach which ensures the integrated consideration of human error, malicious intent, and technical failure to ensure maximum target hardening against attack.

# Conclusion

Mimecast's last **Threat Intelligence Report: Risk and Resilience Insights**, released in November 2019, highlighted a blend of simple and complex attacks. Many of the attacks detected and analyzed spanned multiple days, and included a hybridized threat as the means of attack. These themes are again apparent this quarter: attackers are continuing to use high-volume, commodity malware or simple social engineering techniques as a blanket strategy, incorporating a number of attack vectors in sustained attempts to compromise their targets. At the same time, however, other cybercriminals invest effort into a targeted industry attack, leveraging unique malware and smart attack techniques. If that fails, the sheer volume of threats seek to take advantage of the potential for human error in the face of the onslaught.

The "simple" tactics are also continuing to develop in complexity, with older file types and malware being recycled and modified, and levels of obfuscation and anti-analysis capability being added to attempt to evade detection. Threat actors are continuing the use of evasion techniques in efforts to avoid detection at the gateway, as they use multiple layers of obfuscation to avoid detection at the endpoint. The use of multiple forms of malware in a layered attack has now become commonplace for any determined attacker, and reconnaissance efforts by threat actors are continuing as well, as they try to evade detection and understand how to slip past increasingly sophisticated controls. Simple social engineering techniques also continue to evolve as they attempt to stay ahead of user awareness and seek to take advantage of human error – which is responsible for the overwhelming majority of breaches.

**Stay up to date with the latest in Threat Intelligence**

Check Mimecast's new Threat Intelligence Hub

**MIMECAST.COM/THREATHUB**

# Glossary

### Targeted Attacks

Throughout the quarter, Mimecast discovered 61 significant campaigns threat actors carried out which demonstrate their capability to conduct complex, varying campaigns spanning several days of activity, leveraging a variety of attack methods. For example, this includes the use of bulk and attachment-based malware, fileless malware, URLs, exploits and a variety of complex malware which includes significant obfuscation.

### Malware Observed

Across the Mimecast regions, researchers detected a complex range of malware, some of which has been around for many years and other more recent threats. Many threats are increasingly automated, which is apparent within the daily detections data over periods of time as there is little change in detection numbers from one day to the next in relation to many of the specific file types used in particular attacks. The following identified threats are described in order of the identified frequency of their individual use within the significant attacks detailed over this quarter and included in Section 3 of this report:

***Azorult*** is a commonly bought and sold information stealer or keylogger used to attack Windows computers. ***Azorult*** first appeared in 2016 and has been repeatedly modified. ***Azorult*** has been seen in to use the ISO file format and VBS.

***Barys*** The ***Barys*** Trojan is primarily utilised as a dropper for other malware but can also implement Drop Box online file storage. Normally delivered via malspam campaigns.

**Cottonmouth** This malware relates to compromised USB wires or Flashdrives. This malware's presence may therefore denote physical, as-well as purely online, cyberattacks against a network.

**Hawkeye** is yet another remote access Trojan (RAT) which is offered as-a-service. Hawkeye has been available since 2013.

**Loki or *Lokibot*** is an information stealing, keylogger banking Trojan used against Windows computers. ***Lokibot*** has been available since 2017 and is primarily delivered by MSOffice documents containing macros.

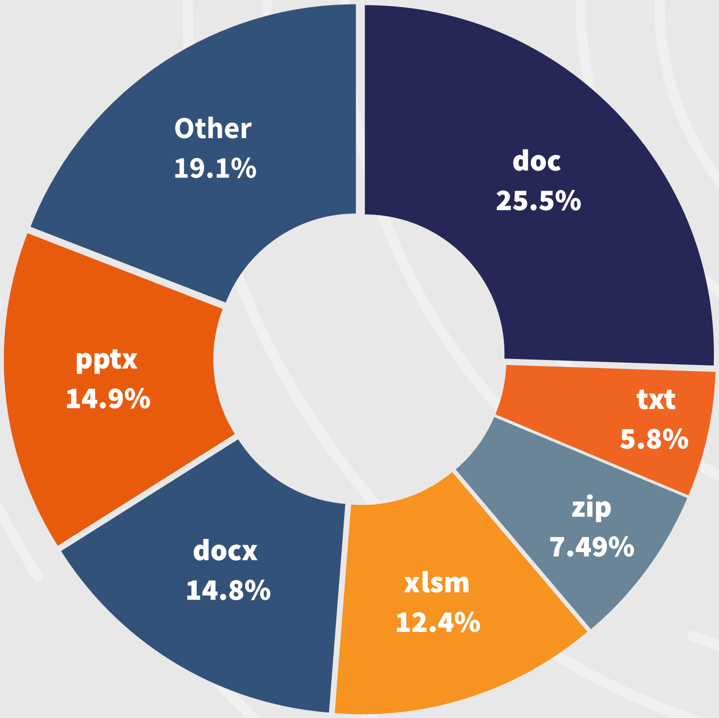
***Nanocore* or Nanobot** is a remote access tool (RAT) used to take over control of Windows computers. ***Nanocore*** has been available since 2013 and is sold for legitimate purposes online. It has been re-purposed by criminals and primarily infects targets via a ZIP archived executable or MSOffice documents containing macros.

***Remcos*RAT** ***Remcos*** is a remote access tool (RAT) used to take control of Windows computers. ***Remcos*** appeared as a threat in 2016. It is spread through malspam campaigns and normally infects through attachments such as MSOffice documents.

***Strictor*** An open source form of ransomware first noted in 2016 and originating from the "Hidden Tear" project

### The figure identifies the file types detected as threats throughout this quarter by Attachment Protect.

This data varies from detection data at the other layers between October to December 2019. All the detected threats within this dataset are categorized by the method of file type delivery utilized to deliver their malicious payload. The dominating file type used has varied considerably within the 3 month period and it is apparent that DOC and DOCX file types, most notably utilized to deliver **Emotet** malware, are returning to usage in high volume in attempts by threat actors to gain a foothold in networks through sheer volume and the potential for human error. Additional measures which remain in use which are widespread and commonly employed are basic obfuscation via file compression, file renaming, double extensions and the increasing use of encryption and complex obfuscation. Versions of **Emotet** have been detected utilizing obfuscation and anti-analysis capabilities. The general trend away from file attachments to URL links is apparent in the increasing deployment of ***Barys*** malware, which implements Dropbox, so this is developing further to being hosted within the cloud, as criminals focus efforts to evade detection by any means possible. MSOffice documents are now the primary attack vector, whether hidden in archived containers such as ZIP and RAR files or attached as is. This is clearly as a result of the numerous exploitable vulnerabilities present within its various iterations, as our campaign analysis shows repeatedly, and particularly those versions which are older and no longer supported. .ACE and .LHA files remain in sporadic use across all regions. These threats are also detected and blocked by Mimecast before they reach Attachment Protect.


Other
doc
txt
zip
xlsm
docx
pptx