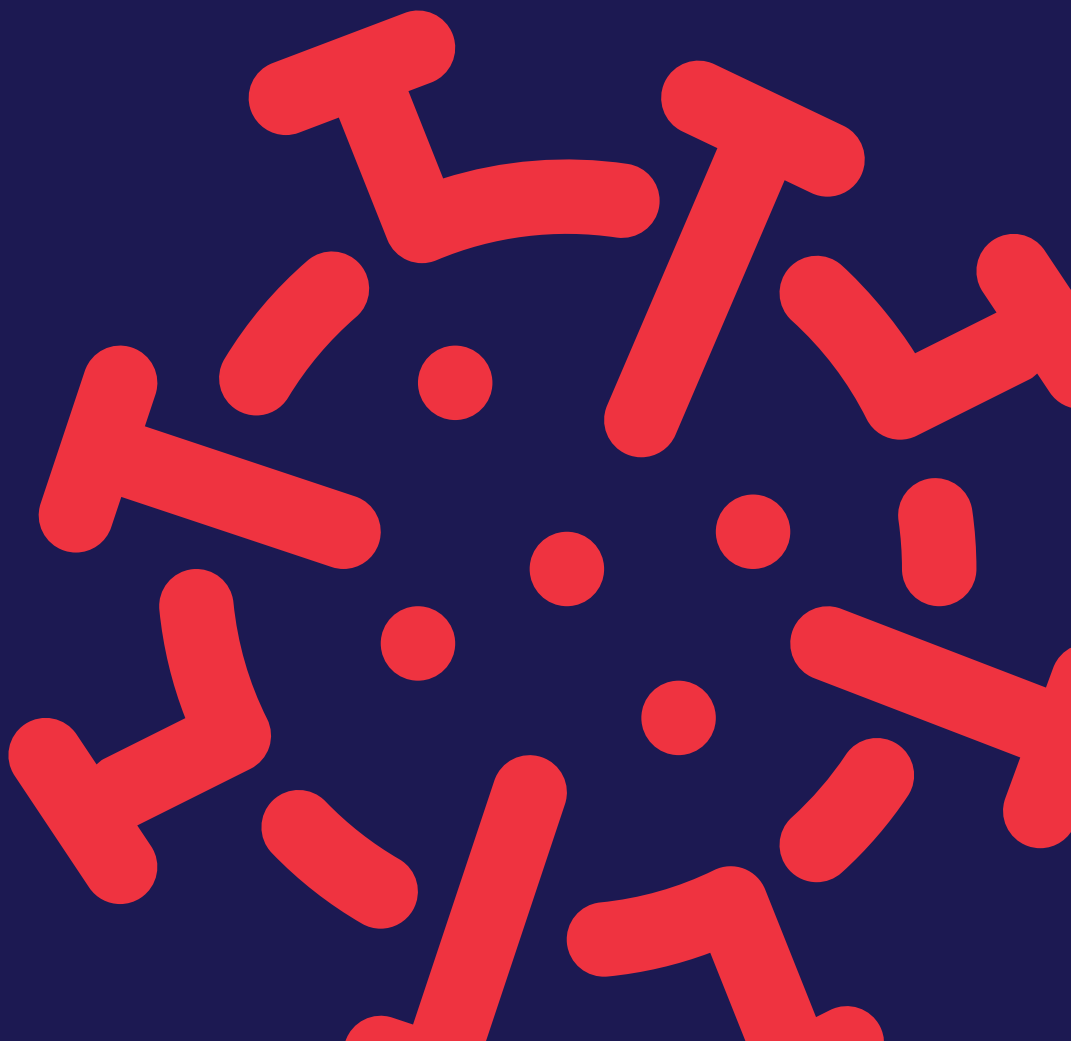
mimecast®

100 Days

of Coronavirus (COVID-19)

May 2020



The First 100 Days of Coronavirus (COVID-19)

Executive Summary

The global spread of ***COVID-19*** has created many new opportunities for threat actors since the novel ***coronavirus*** began gathering widespread attention at the end of 2019. Now, all organizations need to carefully review their multi-layered cybersecurity strategies and arm employees with knowledge of how to protect themselves against these specific attacks.

Increases in ***coronavirus***-related spam and impersonation attack campaigns are exploiting the vulnerability of users working at home, taking advantage of their desire for information about the ***coronavirus*** pandemic to entice them to click on unsafe links. Traditional fraudsters are also using spam to offer fake or non-existent goods such as protective masks or ***COVID-19*** cures.

To provide a clear picture of how malicious actors are exploiting those opportunities, the Mimecast Threat Intelligence team analyzed key trends in activity over the first 100 days.

The monthly volume of all the detection categories reviewed increased significantly – by 33% –between January and the end of March 2020.

- Spam/opportunistic detections ***(increased by 26.3%)***
- Impersonation detections ***(increased by 30.3%)***
- Malware detections ***(increased by 35.16%)***
- Blocking of URL clicks ***(increased by 55.8%)***

Employees who are working at home for the first time may not be sufficiently aware of cyber-threats. In fact, researchers found that employees from companies not using Mimecast Awareness Training were more than 5X more likely to click on malicious links than employees from companies that did utilize the training. The rise in unsafe clicks suggests that there's an urgent need to refresh awareness training for employees and help them create a secure working environment.

These new ways of working create new risks, thus email and web security best practices are paramount. Lookalike domains are easily forged, and the report documents a corresponding surge in domain-related abuse in relation to ***COVID-19*** and associated monikers. Mimecast has observed some 60,000+ ***COVID-19***-related registered spoof domains since early January 2020. The ***Retail*** industry was the hardest hit, and researchers detail the proliferation of domain spoofing of major retail brand websites – like Walmart – in attempts to steal from unsuspecting panic-buyers as they look to purchase necessities online.

IT teams need to consider which communication services they want to sanction for secure work at home. Workers should not be sharing sensitive data over WhatsApp or personal email accounts and IT teams should be able to monitor and disable usage of unsanctioned applications. Cybersecurity training needs to be regular. Our research has shown that to be most effective, training needs to short, fun and engaging to help change security culture.

Given the efforts by governments to address the ***COVID-19*** Public Health Crisis. across the globe in their attempts to contain the spread of ***COVID-19***, it is ***almost certain (≥≈ 95%)*** threat actors and criminals will continue to exploit this resulting confusion, and there will be an increase in the observed cyberattack methodologies against vulnerable targets.

Mimecast ***has therefore launched a website*** focused on helping security leaders better secure and protect their employees while enabling a mobile workforce. This site will be updated regularly to provide insights into new threats to help organizations through this challenging time.

Recommendations for Secure Remote Working:

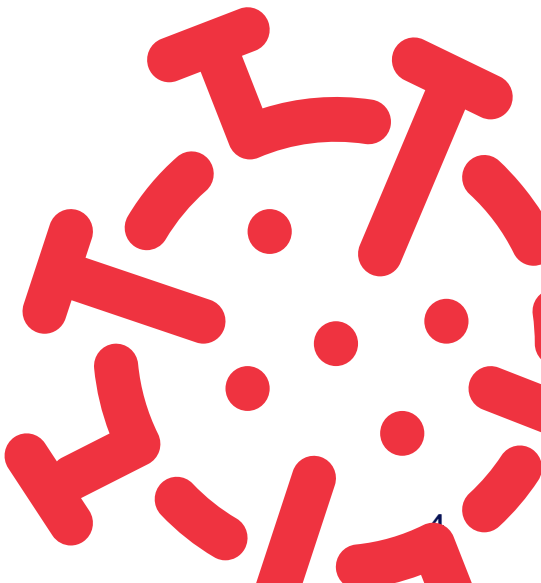
- Update home WiFi with a strong password
- Never click on ***COVID-19*** related attachments received outside your trusted perimeter
- Double-check links – if suspicious, do not click!
- Ensure the links go to the correct domain
- Update usernames and passwords on trusted sites only
- Do not use personal devices at home to access organization networks, data, or emails

Introduction

This report reviews Mimecast's detection data at various layers during the first 100-day period of ***coronavirus*** (***COVID-19***), commencing from the beginning of January 2020. Wherever possible data has been included for the entirety of the period under review. In some cases, however, additional processes have been introduced for the recording of ***COVID-19*** specific data and in these instances, data is provided for the period for which has been available. The development of the ***COVID-19*** epidemic into a global pandemic has presented a unique once-in-a-lifetime opportunity for fraud and predation which cyber threat actors, both criminal and otherwise, have been quick to exploit to the fullest.

Threat actors often use social engineering techniques (usually through pattern-of-life analysis) to increase the chances of a potential victim opening an email and clicking on a malicious link or attachment. Research has shown that over 90% of business compromises occur by email, and that over 90% of those breaches are primarily attributable to human error.

This report will break down the period into an easily digestible weekly review of detections. This activity is then reviewed, and assessments made in relation to what the data tells us in relation to threat activity during this initial period of the virus' rapid spread, and the escalating response of international bodies and national governments. At the same time recommendations are made for the efficient maintenance of cybersecurity during this exceptional, and deeply concerning, time.



Background - Key Events of the COVID-19 Pandemic

Week 1:	31 Dec 2019 – the novel ***coronavirus***, ***COVID-19***, came to global attention when China first reported a number of clustered cases of pneumonia in Wuhan, Hubei, China, to the World Health Organization (WHO).
Week 3:	16 Jan 2020 – China started "lockdown" measures.
Week 5:	30 Jan 2020 – the WHO declared a Public Health Emergency of International Concern (PHEIC). 31 Jan 2020 – the first cases of ***COVID-19*** were reported in the UK, Italy, and Spain.
Week 8:	16 – 24 Feb 2020 – the WHO-China Joint Mission, an international team of experts, investigated the outbreak in China. They issued a report which contained a range of recommendations for nations with outbreaks, including the activation of an "all of society" response to contain the virus with non-pharmaceutical public health measures. 21 Feb 2020 – There were global stock market crashes attributed to ***COVID-19***.
Week 11:	09 Mar 2020 – Italy began to impose their "lockdown" measures. 11 Mar 2020 – the WHO declared ***COVID-19*** as a pandemic. 14 Mar 2020 – Iran imposes their "lockdown" measures.
Week 12:	17 Mar 2020 – Canada and some US States began to impose "shelter-in-place" periods. 18 Mar 2020 – Spain begin their "lockdown" measures.
Week 13:	23 Mar 2020 – The UK and Australia entered indeterminate nationwide "lockdown" periods.
Week 14:	30 Mar 2020 – Russia implemented "lockdown" measures.

Sources: WHO, BBC

It is apparent that there was a considerable delay or lull in action globally during January to February 2020. The threat of a more widespread ***COVID-19*** transmission globally began to be realized from February onwards, while the WHO-China Joint Mission was taking place. Within two weeks of that Mission, Italy and Iran experienced significant clusters of the virus and Italy imposed the first European lockdown. Within the next two weeks, most of Europe and some States of the United States were in their own "lockdown" in attempts to limit the transmission of the virus.

Analysis of the limited data available shows that Nations that implemented lockdown measures approximately 60 days after initial detection of transmission. Hospital admissions then spike at their highest approximately 87 days after that initial transmission (or 27 days after lockdown) if the measures are strictly adhered to. The UK and US spike in virus-related admissions was, therefore, expected to occur in Mid-April but in both these countries, compliance with lockdown recommendations has been varied. ***Figure 1. illustrates this pattern.***

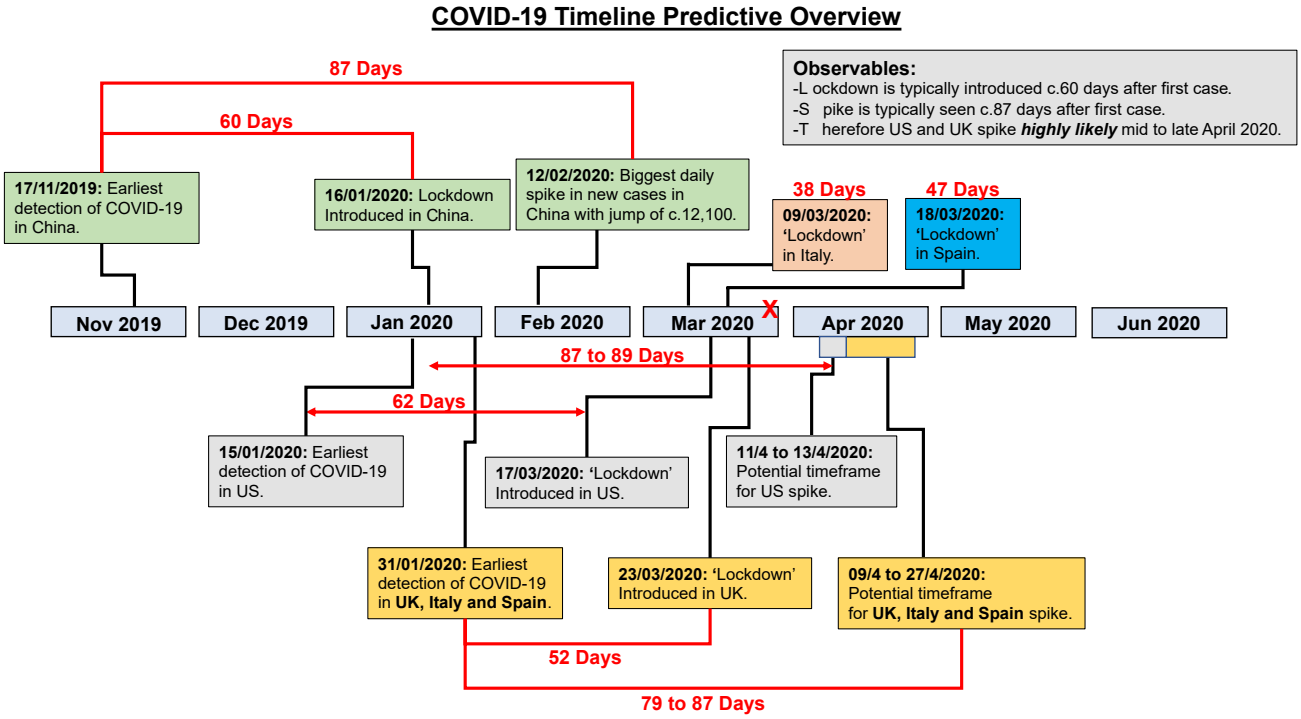


Figure 1: Timeline of Key Coronavirus (COVID-19) Pandemic Events

In cyber threat terms, there has been a step change in reputation rejections starting in late February 2020, and particularly in the UK. The biggest increased volume changes were apparent in the ***Manufacturing*** and ***Information Technology*** verticals. ***Retail*** and ***Professional Services*** also showed particularly high levels of rejections, but our data shows ***Healthcare*** rejections remaining relatively low.

The volume of all threat detections relating to spam/opportunistic, impersonation, malware, blocked clicks, and web or domain-based threats has increased significantly during the period of report. The most significant increases occurred from March 2020 onwards as threat actors had now clearly pivoted to heavily exploit the pandemic as a key theme of global concern and, therefore, representing a huge opportunity for exploitation, compromise, fraud, and theft.

The Threat Landscape

The threat landscape has evolved. Cyber threats are complex, dynamic, and network defenses often have trouble keeping up with them. Highly sophisticated and targeted attacks continue to exploit the evolution of technology and the increased drive towards mobility easing the process of the exfiltration of data from organizations. An increase in the variety and volume of attacks is inevitable given the desire of financially- and criminally-motivated actors to obtain personal and confidential information.

Countries across the world differ in terms of regulative, normative, and cognitive legitimacy to different types of attacks. Cybersecurity is an accepted part of business life and organizations invest heavily in people, resources, and budget.

As Governments around the globe seek to return societies and organizations to a phased return to former working practices, it is important to advise companies of the potential vulnerabilities such operations may have which will ***almost certainly (≥≈ 95%)*** be exploited by threat actors. Some countries have already elected to begin a phased return for some business verticals (at ICOD, Spain has lifted working restrictions for construction and ***manufacturing*** industries (and related supply chain), Italy has lifted restrictions on some retail (such as bookshops, children's clothing, etc.), whereas others (India, France, UK) have extended the period for restrictions.

Cyber threat actors and threat groups are continuously networking, researching, and testing new tactics, techniques, and procedures (TTPs). This can be seen in the significant ramping up of their response to the pandemic across all the cyber-related attack vectors reported on, particularly in March.

Email Attack Vectors

Email, as the key communication mechanism for many organizations, means it is a highly attractive attack vector to a wide range of threat actors, whether for unskilled and opportunistic attacks by lone individuals, or organized and extensive campaigns by organized criminal, or states-sponsored, groups. Analysis of the malicious cyber activity utilizing Mimecast's detection data and the significant campaigns identified has been broken down to give a weekly overview of this period covering the first 100 days of activity since the end of December 2019.

The information assessed here includes that from the spam/opportunistic, impersonation protect, malware detection, and blocked URL click layers of the Mimecast suite. The following detail in relation to analysis of this data gives a weekly account of the levels, and types, of activity detected by Mimecast and the evolution of the threats detected throughout the initial weeks of 2020, which saw the escalation of the ***COVID-19*** epidemic to a global pandemic, and its related crises. For the meaningful comparison of weekly data, the period of analysis commenced from 30 Dec 2019 to the intelligence cut-off date (ICOD) of 12 Apr 2020.

Week 1: 30 Dec 2019 - 05 Jan 2020

The year 2020 started with a noticeable lull in threat actor activity, following the December 2019 holiday season. This being the first week that the novel ***coronavirus*** (***COVID-19)***, first came to wider global attention.

The week 1 baseline was established at:

- 110.6 million spam/opportunistic detections
- 3.8 million impersonation detections
- 1.24 million AV/malware detections
- 902,000 blocked URL clicks

- 20.6% of Malware threats were contained in ***RAR*** files primarily focused on the Continental Europe and UK regions.
- 11.4% were contained in ***ZIP*** files primarily against the North America & the Caribbean, and UK regions.
- 7% were VBA droppers, almost exclusively against the America & the Caribbean region.
- 6.7% was phishing, primarily against the North America & the Caribbean, and UK regions.
- 5.9% was ***ISO***/image based and primarily against the North America & the Caribbean region.

The Finance: Banking vertical was the most attacked during this period, followed by the ***Professional Services*** sector.

Week 2: - 06 Jan - 12 Jan 2020

In contrast to the first week of 2020, this second week saw threat actor activity increase at a significant rate following the initial lull. This week saw significant detections at all layers and a notable increase in users interacting with unsafe clicks.

There was a significant increase in observed detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 16.7%
- Impersonation increased by 53.8%
- Malware increased by 239%
- Blocked URL clicks increased by 19.87%

The extent of the initial post-holiday lull of the week before is indicated by the substantial percentage increases across all detection data, particularly in relation to AV/Malware, and Impersonation detections.

- 16.7% of Malware threats were contained in ***JS***-based phishing emails, almost entirely against the Australasia and Sub-Saharan Africa regions.
- 11.4% were generic Trojans primarily against the North America & the Caribbean, and UK regions.

- 9.65% were ***RAR*** file based and primarily targeting the Australasia, Continental Europe, and UK regions.
- 8.55% were ***ISO***/image-based files primarily targeting the North America & the Caribbean, and UK regions.
- 6.2% specifically attacked the ***CVE-2017-11882*** vulnerability and primarily targeted the UK region.
- 5.48% were ***ZIP*** file based and primarily targeted the UK region.

The ***Retail/Wholesale*** vertical was the most attacked during this period, followed by ***Manufacturing***.

Week 3: 13 - 19 Jan 2020

This week, significant volume campaigns were again apparent in detections data, with campaigns being conducted by threat actors in the multiple regions. There was a sustained increase in the volume of all threats detected, with a continued surge in Malware. Despite the continued substantial increase in threats, cyber hygiene (in relation to unsafe clicks) appeared to have improved.

There was an observed increase in most detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 30%
- Impersonation increased by 19%
- Malware increased by 181.7%
- Blocked URL clicks reduced by 13.7%

The volume of threats continued to increase significantly, particularly in terms of Malware. This represented a period (similar to Week 2) where threat activity and detections returned to a more normalized level following the significant lull seen in Week 1.

- 19.6% of Malware threats were detected as a variety of ***Microsoft Office*** based files, including ***Emotet***, and heavily focused on the North America & the Caribbean, and UK regions.
- 12.95% were detected as VBA based, including ***Emotet***, marking the return of significant volume activity for the botnet. This activity was apparent across all regions but 58% of this total was focused on North America & the Caribbean region.
- 9.6% were ***ZIP*** file based and apparent across all regions.
- 7.8% were ***RAR*** file based and apparent across all regions.
- 6.8% were ***ISO***/image based and primarily focused on the UK region.

The ***Retail/Wholesale*** vertical remained the most attacked during this period, again followed by ***Manufacturing***.

Week 4: 20 - 26 Jan 2020

There were reductions in all detection categories during this week. However, the reductions were

not as significant as the two preceding week's more substantial cumulative increases and detections, therefore, remained significantly high across all categories. Cyber hygiene, in relation to unsafe clicks, continued to improve and this week was to be its lowest and best performance for the entire reporting period.

There was a noteworthy decrease in observed detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic decreased by 13.50%
- Impersonation decreased by 24.20%
- Malware decreased by 16.90%
- Blocked URL clicks reduced by 4.1%

- 33.9% of Malware detections were VBA and ***Emotet*** related detection, surpassing 100,000 globally on the 22 Feb 2020 as part of a three-(3)-day campaign that had started on 20 Feb 2020. This activity significantly impacted detections in the Australia, Continental Europe, MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- 10.2% of detections were ***RAR*** file related. This activity significantly impacted the Central Asia & Indian sub-continent, MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- 9.8% of detections related to ***ZIP*** file detections, primarily focused on the Central Asia & Indian sub-continent, Continental Europe, MENA, and UK regions.
- 6.19% of detections related to ***ISO***/image based files, primarily targeting the MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.

The ***Manufacturing*** and ***Retail/Wholesale*** verticals here targeted to almost exactly the same extent (detections varied by less than 400 between the two categories during this week), ***Manufacturing*** taking over as the top targeted vertical.

Week 5: 27 Jan - 02 Feb 2020

The reductions in Impersonation and Malware detections appeared to be sustained, but all detections remained above those seen during the first 2 weeks of the reporting period (except for Impersonation attacks). Cyber hygiene deteriorated significantly during this week with a substantial increase in unsafe clicks – significantly exceeding any of the gains observed during the two (2) preceding weeks.

There continued an observed decrease in most areas of detections and threat actor campaigns across all data analyzed:

- Spam-opportunistic decreased by 4.9%
- Impersonation decreased by 16.88%
- Malware decreased by 35.10%
- Blocked URL clicks increased by 11.18%

- 16.89% of all detections were ***Emotet***. A large-scale ***Emotet*** campaign again took place (this time over four (4) days commencing 29 Jan 2020) and exceeded 120,000 detections. This activity was primarily focused towards the Australasia, Continental Europe, MENA, North America & Caribbean,

Sub-Saharan Africa, and UK regions.

- 9.5% of detections were ***ZIP*** file related and focused on the MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- 9.1% of detections were ***RAR*** file related and focused on the MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- 8.8% of detections were VBA related on 28 – 29 Jan 2020 and primarily focused on the
- Australasia and North America & the Caribbean regions.
- 7.97% of detections were ***ISO***/Image based.

The ***Manufacturing*** and ***Retail/wholesale*** verticals remained the top targeted globally, but ***Manufacturing*** was being increasingly targeted. Activity against the ***Transportation, Storage and Delivery*** vertical was also notably increasing to place it third.

Week 6: 03 - 09 Feb 2020

All detections, again, increased significantly, surpassing any reductions in the preceding two (2) weeks in all categories except for Impersonation, which remained at a reduced level. Cyber hygiene deteriorated at its highest rate since the start of the reporting period. This deterioration was the most significant for the entire period of reporting, not to be followed by a comparably significant deterioration until Weeks 13 and 14 (at the end of March).

This week was notable as it immediately followed the first reports of ***COVID-19*** infections in the UK, Italy, and Spain. It is ***almost certain (≥≈ 95%)*** that the virus' spread saw an increasing uncertainty, spurring the incidence of human error to increase as significant numbers of individuals sought information in relation to the outbreak.

There was an observed increase in all areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 9%
- Impersonation increased by 24.8%
- Malware increased by 47.1%
- Blocked URL clicks increased by 31.5%

- 15.27% of all Malware detections were ***Emotet*** related. A large-scale campaign of over 100,000 detections took place over 03-04 Feb 2020. This activity was primarily focused on the Australasia, Continental Europe, MENA, North America & the Caribbean, and UK regions.
- 14.6% of detections were detected as a variety of ***MSOffice*** based files, including ***Emotet***, and between 04 – 07 Feb 2020 heavily focused on the Continental Europe, North America & the Caribbean, and UK regions.
- 10.4% were ***RAR*** file based and observed in the Continental Europe, MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- 9.98% were ***ZIP*** file based and observed in the Continental Europe, MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.

- 5.5% were ***ISO***/image based and primarily targeted the North America & Caribbean, Sub-Saharan Africa, and UK regions.

Retail/Wholesale became the top targeted vertical once more, followed closely by ***Manufacturing***. The increased activity against the ***Transportation, Storage and Delivery*** vertical appeared to be sustained.

Week 7: 10 - 16 Feb 2020

This week saw further substantial increases to all detections, and in particular, a huge increase in the use of Malware, which would peak at its highest volume for the entirety of the reporting period. Cyber hygiene, as indicated by unsafe clicks, deteriorated further, to a level at which it would remain relatively stable for the next five (5) weeks.

There continued an observed increase in all areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 7.6%
- Impersonation increased by 20.5%
- Malware increased by 64.1%
- Blocked URL clicks increased by 10.5%

- 18.3% of Malware detections were ***RAR*** file based and were utilized in significant numbers across all regions during that week.
- 8.58% of detections were ***ZIP*** file based and again, impacting across all regions.
- 8.2% of detections were ***ISO***/image based and primarily against the Australasia, Continental Europe, MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- 7.57% of all detections specifically attacked the ***CVE-2017-11882*** vulnerability and impacted all regions.
- 6% of detections comprised generic Trojans focused on the Continental Europe, MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- Australasia also suffered a significant five (5) day ***VBS*** based campaign (commencing 10 Feb 2020, and comprising over 45% of all the region's detections over this week.

The ***Manufacturing*** and ***Retail/wholesale*** remained the top targeted verticals globally, but ***Manufacturing*** was again subject to increased targeting. The detections against the ***Transportation, Storage and Delivery*** sector declined and activity against the ***Professional Services*** sector increased to place it third.

Week 8: 17 - 23 Feb 2020

Fluctuations in all detection data highlighted an increased focus by threat actors on Impersonation during this week; it being the only detection category to increase again. The increased focus and significant volume increases to Impersonation attacks was sustained from Week 6 onwards. This would then increase inexorably throughout the remaining period of the report. Overall detections remained at a high level. Cyber hygiene was assessed as having generally improved.

There was an observed decrease in most areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic decreased by 13.50%
- Impersonation increased by 10.4%
- Malware decreased by 16.90%
- Blocked URL clicks decreased by 7.54%

- 15.3% of Malware detections were ***RAR*** file observed in all regions but most significantly impacting the North America & the Caribbean, and UK regions in terms of volume.
- 8.3% were Malware phishing-based and again most significantly impacting the North America & the Caribbean, and UK regions in terms of volume.
- 7.6% were ***ZIP*** file based impacted all regions but with more significant detection volume in the UK.
- 7.2% were ***ISO***/image based primarily impacting Australasia, Continental Europe, MENA, North
- America & the Caribbean, and UK regions.
- 6.5% continued to exclusively target the ***CVE-2017-11882*** vulnerability and most significantly in the MENA, North America & the Caribbean, and UK regions most.

The ***Manufacturing*** and ***Retail/wholesale*** verticals again remained the top targeted globally, but ***Manufacturing*** remained subject to increased targeting. The detections against the ***Transportation, Storage and Delivery*** sector remained stable and activity against the ***Professional Services*** sector remained significant enough to place it third.

Week 9: 24 Feb - 01 Mar 2020

Following the previous week's reductions all detection categories saw substantial increases to beyond the levels preceding week 8. Impersonation volume reached what would be its second highest level throughout the period, spam it's third. These figures would be not be surpassed until Week 14. Cyber-hygiene fluctuated to a deterioration.

There was an observed increase in all areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 25.17%
- Impersonation increased by 17.7%
- Malware increased by 27.58%
- Blocked URL clicks increased by 7.6%

- 16.5% of Malware was in ***RAR*** file format which significantly impacted all regions.
- 10.6% was in ***ISO***/image file format significantly impacted all regions but with the most volume of detections across the North America & the Caribbean, Sub-Saharan Africa, and UK regions.
- 6.9% was in ***ZIP*** file format which impacted all regions.
- 4.8% again continued to exclusively target the ***CVE-2017-11882*** vulnerability which also impacted every region, but most significantly in the MENA, North America & the Caribbean, and UK regions.
- On 28 Feb 2020 a high-volume campaign using ***Zmutzy*** malware targeted the Australia region.

The ***Retail/Wholesale*** and ***Manufacturing*** sectors remained the top targeted verticals but significant increased detections against ***Retail*** put it in front. The ***Professional Services*** and ***Transportation, Storage and Delivery*** verticals remained subject to sustained volumes of attack.

Week 10: 02 - 08 Mar 2020

Threat actors continued to exploit Impersonation attack methodologies this week; it being the only detection category to continue increasing. Overall detections remained at a high level. Cyber hygiene (evidenced through user clicks) showed an improvement (comparable to Week 8).

There was an observed decrease in most areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic decreased by 10%
- Impersonation increased by 10.4%
- Malware decreased by 24.50%
- Blocked URL clicks reduced by 7%

- 16.2% of Malware was in ***RAR*** file format and impacted all regions, but with disproportionate detection increased volumes observed in the MENA, North America & Caribbean, Sub-Saharan Africa, and UK regions.
- 8.85% was in ***ISO***/image file format significantly impacted all regions but with the most significant volume of detection in the North America & the Caribbean, and UK regions.
- 5.57% was in ***ZIP*** file format which again impacted all regions.
- 4.9% was in HTML format which impacted all regions but mostly affecting the North America & the Caribbean region.
- 4.58% once again continued to exclusively target the ***CVE-2017-11882*** vulnerability which now significantly impacted every region.

The ***Manufacturing*** and ***Retail/wholesale*** verticals again remained the top targeted globally, separated by less than 300 detections, but ***Manufacturing*** remained subject to increased targeting.

The detections against the ***Transportation, Storage and Delivery*** sector declined significantly but activity against the ***Professional Services*** sector remained significant and rising enough to place it third. The Finance: Insurance sector now also experienced a significantly increased volume of detections to a level comparable to Professional Services.

Week 11: 09 - 15 Mar 2020

Once more, following widespread reductions in detections, significant increases took threat activity to significant peaks for the period of report. Spam/opportunistic had now increased to the highest volume to be observed during the period of report at over 21.8 million detections. Malware reached its third highest volume, higher than every other week excluding Weeks 7 and 14, at over 1.2 million detections. By overall volume, this week saw the most significant activity of the entire period reported on, at over 32.5 million detections. Given the significant increase to detections, cyber hygiene (as measured via unsafe clicks) appeared to remain constant.

There was an observed increase in all areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 31.7%
- Impersonation increased by 65.9%
- Malware increased by 47%
- Blocked URL clicks increased by 7.5%

- 12.7% of Malware was in ***RAR*** file format and impacted across every region.
- 8.27% was in ***ZIP*** file format and impacted every region.
- 7.5% of detections exclusively targeted the ***CVE-2017-11882*** vulnerability which impacted every region.
- 7% were generic Trojans related to phishing and primarily impacted the North America & the Caribbean, Sub-Saharan Africa, and UK regions.
- 6.4% was Chatres malware which was VB-based and delivered over 12 – 13 Mar 2020. This almost exclusively targeted the North America & the Caribbean region.
- 5.6% were ***XLS*** file macro-related malware. These primarily targeted Australasia on 13 Mar 2020.

The ***Manufacturing*** and ***Retail/wholesale*** verticals again remained the top targeted globally. The detections against the ***Transportation, Storage and Delivery*** sector declined significantly as did activity against the Finance: Insurance sector. Whilst the volume of detections against the ***Professional Services*** sector declined overall it remained at a significant enough level to continue to place it third.

Week 12: 16 - 22 Mar 2020

After the significant volume increases across all types of detections in Week 11, activity reduced in observed detection volumes this week. There was also an observed improvement in cyber hygiene (via fewer interactions with unsafe URLs).

There was an observed decrease in all areas of detections and threat actor campaigns across all data analysed:

- Spam/opportunistic decreased by 22.60%
- Impersonation decreased by 31%
- Malware decreased by 9.51%
- Blocked URL clicks reduced by 5.83%

- 15.59% of Malware was in ***RAR*** file format and significantly impacted across every region.
- 14.48% was in ***ZIP*** file format and significantly impacted every region.
- 6.3% was in ***ISO***/image format and also impacted every region.
- 6.25% once again continued to exclusively target the ***CVE-2017-11882*** vulnerability which again significantly impacted every region.
- 4.48% were ***XLS*** file macro-related malware. targeting the Australasia region on 17 Mar 2020, and the North America & the Caribbean region over that entire week.
- 4.4% comprised exclusively ***JS*** format ***Cryxos*** malware detections. These were detected in every region but this campaign disproportionately targeted the MENA and UK regions between 17 – 22 Mar 2020.

The ***Retail/wholesale*** and ***Manufacturing*** verticals again remained the top targeted globally. The detections against the ***Transportation, Storage and Delivery*** sector showed a significant increase again, as did activity against the ***Professional Services*** sector, placing it third most impacted.

Week 13: 23 - 29 Mar 2020

Detections for Spam/opportunistic and Malware saw significant reductions, but impersonation again saw a huge increase. This week saw a significant deterioration in cyber-hygiene via blocked clicks and this week marked the end of the relatively stable fluctuations in this measure.

There was no clear increase / decrease in the areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic decreased by 12.40%
- Impersonation increased by 40.7%
- Malware decreased by 41.12%
- Blocked URL clicks increased by 29.9%

- 18.9% of Malware was in ***RAR*** file format and continued to significantly impact across every region. The Sub-Saharan Africa region suffered a significantly increased level of these detections during this week.
- 10.79% was in ***ZIP*** file format which impacted every region.
- 8.7% comprised exclusively ***JS*** format ***Cryxos*** malware detections. These were now almost exclusively targeted at the North America & the Caribbean region.
- 7.1% was phishing-related and although detected across all regions, most significantly targeted the Sub-Saharan Africa region.
- 5.26% was in ***ISO***/image format and impacted every region.
- 4.7% were ***XLS*** file macro-related malware. These were now detected in all regions but primarily targeted Australasia and the North America & the Caribbean regions over the course of the week.
- 3.8% exclusively targeted the ***CVE-2017-11882*** vulnerability, most significantly impacting the Australasia, Continental Europe, North America & the Caribbean, and UK regions.

The ***Retail/wholesale*** and ***Manufacturing*** verticals again remained the top targeted globally. The detections against the ***Transportation, Storage and Delivery*** sector and ***Professional Services*** sectors maintained their increased levels, continuing to place the latter third by volume.

Week 14: 30 Mar - 05 Apr 2020

There were significant increases in all detection categories during this week. Impersonation peaked in volume during this week. The volume of user interactions with unsafe click increased.

There was an observed increase in all areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 30.3%
- Impersonation increased by 23.7%
- Malware increased by 53.7%
- Blocked URL clicks increased by 25%

- 27.17% of Malware was in ***RAR*** file format which impacted across every region, but most significantly by volume in the MENA, North America & the Caribbean, and UK regions.
- 17.1% was the observed use of ***Cryxos*** malware in ***JS*** format, which impacted every region, but which most significantly hit the North America & the Caribbean region on 31 Mar 2020, with over
- 30,000 detections on that day alone, and the Sub-Saharan Africa region daily over the course of the week.
- 7% was in ***ZIP*** file format and which impacted every region.
- 6.4% was in ***ISO***/image format and also impacted every region.
- 5.5% was in ***VBS*** format and which primarily impacted the Australasia and North America & the Caribbean regions.
- 3% was observed to exclusively target the ***CVE-2017-11882*** vulnerability which impacted all regions.
- 4.5% was from ***XLS*** file macro-related malware. These primarily targeted the Australasia, North America & the Caribbean, and UK regions between 30 Mar – 01 Apr 2020.

The ***Manufacturing*** and then ***Retail/wholesale*** verticals again remained the top targeted verticals globally. The volume of detections against the ***Professional Services*** sector increased significantly due to the ***Cryxos*** campaign against accounting in the North America & the Caribbean region on 31 Mar 2020, placing it third.

Week 15: 06 - 12 Apr 2020

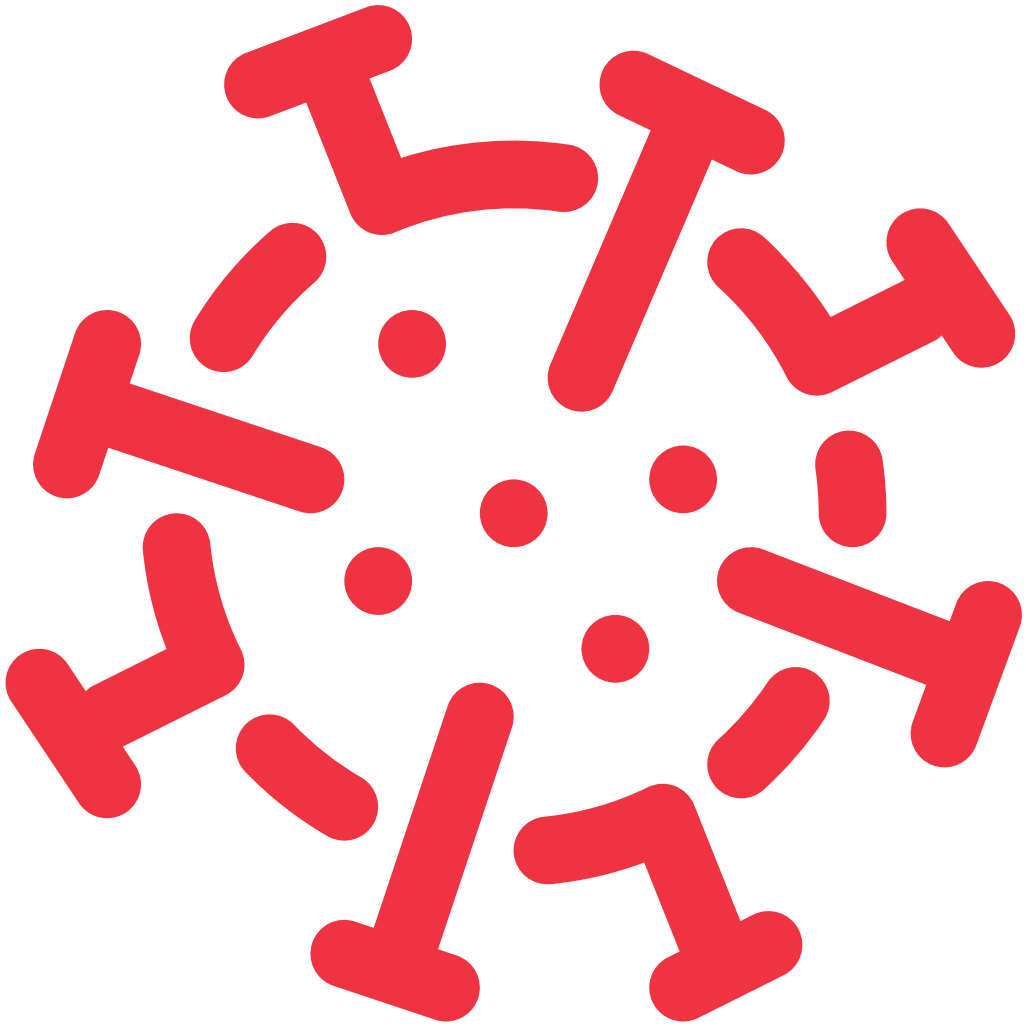
There were significant increases to Spam/opportunistic and Malware detections. The reduction to Impersonation was slight considering previous significant volume increases. This was still high enough in volume to be its 3rd highest for the entire period of report, at over 82.5 million. Blocked clicks improved slightly but remained at a concerningly elevated level.

There was no clear increase / decrease in the areas of detections and threat actor campaigns across all data analyzed:

- Spam/opportunistic increased by 8.37%
- Impersonation reduced by 14.6%
- Malware increased by 23.88%
- Blocked URL clicks decreased by 12%

- 23.76% of Malware was in ***RAR*** file format and impacted across every region, although significantly more heavily by volume in the UK region.
- 17% was phishing related and impacted the Sub-Saharan Africa and UK regions.
- 12.18% was from the observed use of ***Cryxos*** malware which almost exclusively targeted the North America & the Caribbean region.
- 8% was in ***ZIP*** file format and impacted every region.
- 5% was in ***ISO***/image format and impacted every region.
- 4.66% targeted the ***CVE-2017-11882*** vulnerability which impacted all regions.

The ***Manufacturing*** and then ***Retail/wholesale*** verticals remained the top targeted verticals globally, with little volume separating them (less than 300 detections). The volume of detections against the ***Professional Services*** sector continued to place it third.



What Does it Mean?

This section reviews the findings of the various weekly detection outputs and gives a broad summary of the activity seen over the period of analysis. Where identified, recommendations will be detailed to aid the mitigation of the threats identified and these are summarized in a later section of this report with the addition of other recommendations considered of importance given the current situation and the ongoing pandemic.

Throughout this assessment additional consideration is given to the recent transformation of daily business forced upon organizations by the various national and regional lockdowns in force, and the significantly increased numbers of employees working from home, and likely to be so for varied and indeterminate periods, potentially on a repeated or prolonged basis differing significantly by national jurisdiction.

The period under analysis and subject to this report began with an apparent short period of lull after the December holiday season. This was very quickly followed by significant volume increases in all threat actor activity. In the following weeks all detections experienced significant increases, partly anticipated as detection levels returned to previous levels. However, detection levels resumed their previous scale very rapidly in January, only to continue to increase substantially throughout the rest of the period of this report. This is abnormal behavior considering the apparent significant volume escalation of all detections during this period.

Ordinarily, moderate increases and a regular weekly fluctuation in detections with a discernible but gradual increase over time would be considered normal. During the first three months of 2020 alone, the volume of these detections increased from 103.7 million in January to more than 118.7 million by the end of March, a 27.85% increase in detections.

Overall, the total volume of activity January to February was similar to previous periods, with most of the additional increase taking place in March, and apparent through repeatedly significant increases in detection volume during that month. Spam and Impersonation detections both experienced three weeks of their peak volume during March, Malware its second highest peak, and blocked URL clicks deteriorated significantly and experienced two weeks of peaking volume at the end of March.

Weeks 3 through to 6 (ending on 07 Feb 2020) experienced significant ***Emotet*** campaigns in an anticipated continuation of similar campaign activity between October and December 2019, as reported in ***Mimecast's Threat Intelligence Report, RSA Conference Edition***. However, this activity then appears to give way to a step change where increasingly the focus and attention was on enhanced volumes of Spam and Impersonation.

Malware fluctuated significantly throughout the period of report, but as with all other detections increased. Each detection measured increased by between 26% to 35%. Blocked URL clicks saw two distinct periods of deterioration, an initial significant deterioration over Weeks 5 to 7 (between 27 Jan 2020 and 16 Feb 2020), followed by several weeks of relative stability before a significant and sustained deterioration from Week 13 (from 23 Mar 2020). The overall increase to detections is shown in ***Figure 2***:

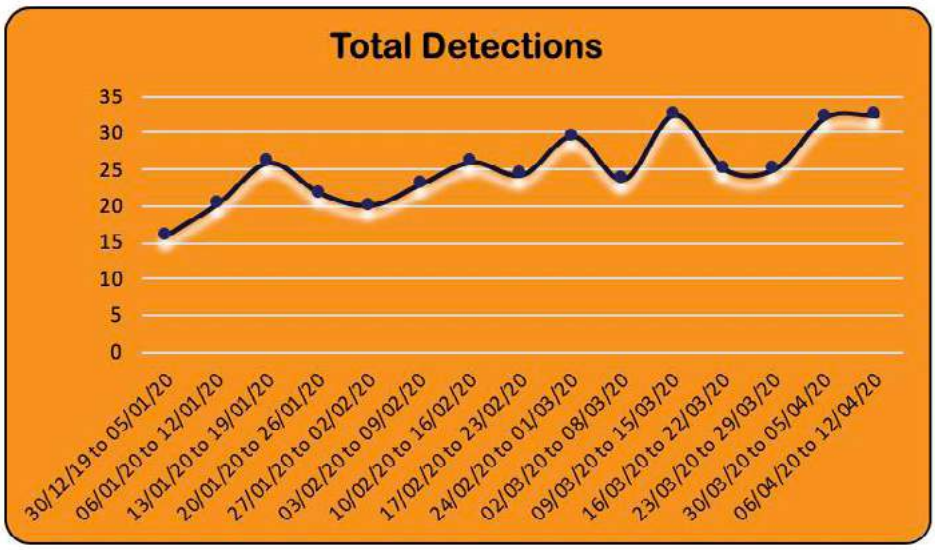


Figure 2: Total Detections Trend

Towards the end of February, as WHO experts completed their Joint Mission with China, threat actors appeared to engage in a refocusing of effort which then gained significant pace in the following weeks and throughout March. It appears clear that they quickly recognized the opportunity the spread of ***COVID-19*** represented and made significant efforts to pivot to higher volume and, in some cases, less nuanced and sophisticated means to capitalize on the increased vulnerability of employees working from home in those nations under "lockdown".

The observed significant deterioration in the volume of blocked clicks, most noticeably in the last weeks of March, is cause for significant concern, and may evidence a widespread deterioration in cyber hygiene over any prolonged period of working from home under uncertain and stressful "lockdown" conditions. This is likely further exacerbated by the significant numbers of employees working from home for the first time because of current circumstance and having potentially not been adequately prepared for that eventuality at short notice.

A wide-range of email samples from the period that relates to ***COVID-19*** themes are included in a later section of this report in date order and show the gradual increase and evolution in complexity as threat actors shifted their focus to concentrate their efforts into sustained volume Spam/opportunistic and Impersonation campaigns.

An awareness of current threats is of increased importance when lines of communication and accountability are stretched.

An awareness of current threats is of increased importance when lines of communication and accountability are stretched.

Spam/opportunistic Detections

Spam detections witnessed an exponential 26.3% increase during the period of analysis. Peak volumes, in order of volume, were experienced in Weeks 11, 15, and 14. These increases are illustrated in ***Figure 3***:

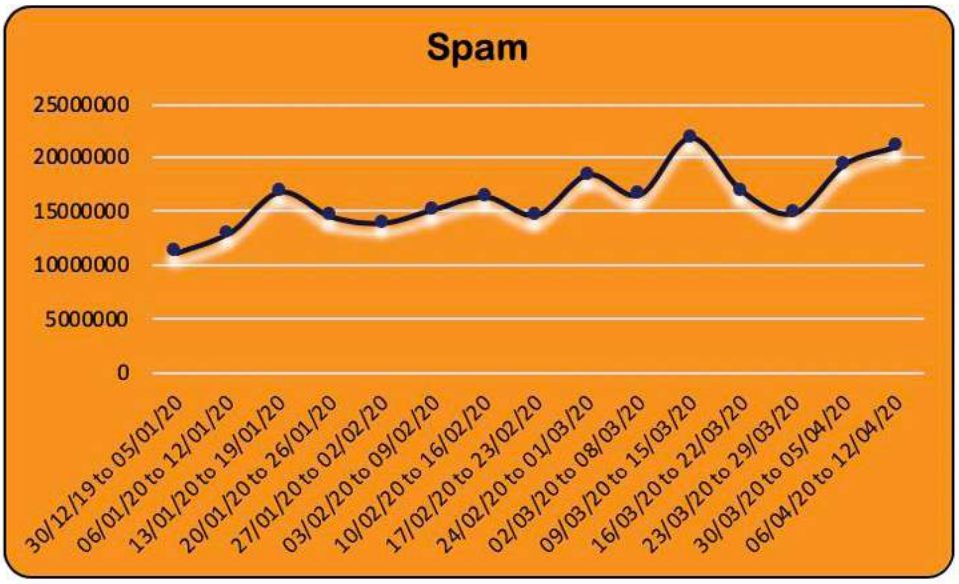


Figure 3: Spam Volume Trend

Mimecast blocked the delivery of over 83 million ***COVID-19*** related emails at the Spam/opportunistic layer in the last four (4) weeks; this includes 10 million rejections and over 73 million quarantined emails. To indicate the overwhelming prevalence of the virus as a subject at the Spam/opportunistic layer the last week of reporting's word cloud for that layer has been included below at ***Figure 4***. In addition, ***Figure 5***, illustrates the current and greater focus of this volume Spam/opportunistic delivery for the Continental Europe and the North America and the Caribbean regions.

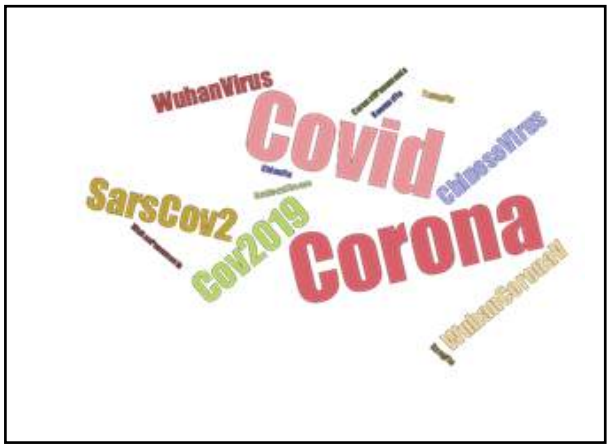


Figure 4: Spam Word Cloud – Week 14

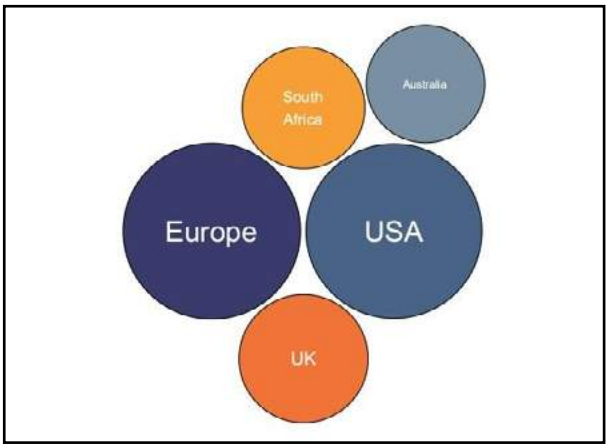


Figure 5: Rejected Spam Volume per User

Impersonation Detections

Impersonation detections increased by 30.3% during the period of analysis. Peak volumes, in order of volume, were seen in Weeks 14, 9, and 15. These increases are illustrated in ***Figure 6:***

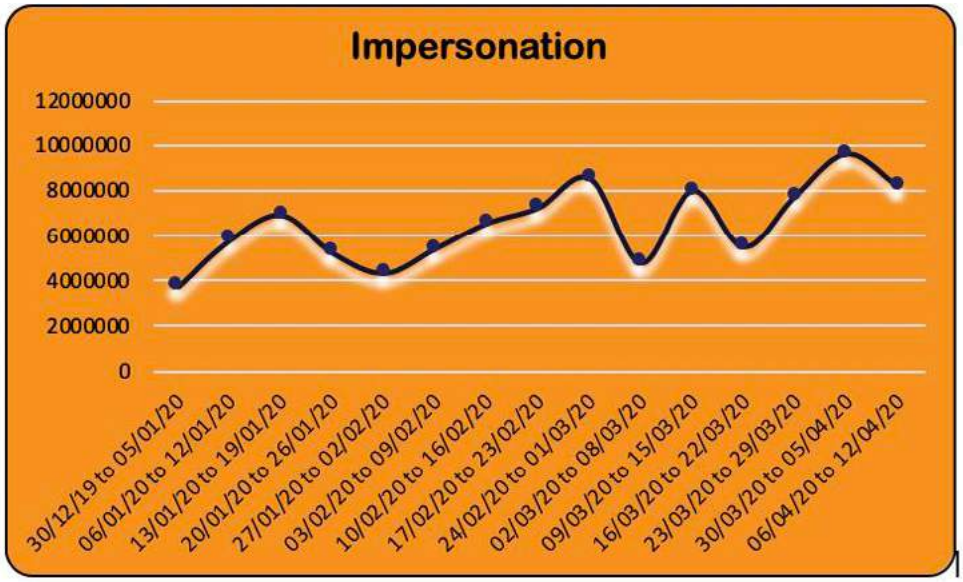


Figure 6: Impersonation Volume Trend

Impersonation detections were the only category to continue to significantly increase during many later weeks when other categories experienced significant reductions. This is ***likely (≈55% – 75%)*** indicative of the increased focus on this type of social engineering or Impersonation behavior by threat actors. Business email compromise (BEC) and social engineering are ***likely (≈55% – 75%)*** to be attractive as an attack while significant numbers of individuals are potentially working from home or isolated from their peers and other support.

Impersonation had increased significantly between July and September 2019 and the declaration of the pandemic has given the shift to this attack vector a renewed impetus and importance given the unique opportunities which the current situation presents.

In the reporting period, more than 1,000 ***COVID-19*** themed emails were blocked by Targeted Threat Protection IP alone, including a single significant campaign of more than 500 emails delivered in ***XLS*** format on 06 Apr 2020 to the North America & the Caribbean region. These contained the ***Stratos*** malware dropper, an Office macro based trojan.

Malware Detections

Malware detections increased by 35.16% during the period of analysis. Peak volumes, in order of volume, were seen in Weeks 7, 15, and 11. These increases are illustrated in ***Figure 7***:

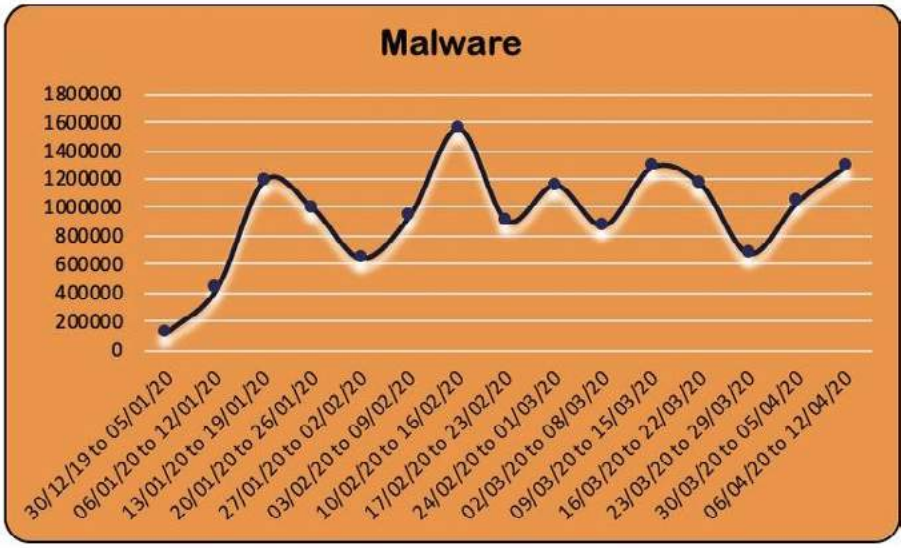


Figure 7: Malware Detections Trend

The most significant volume Malware campaigns were delivered in ***RAR, ZIP, ISO/image***, and ***VBA*** files. To a lesser extent other campaigns featured ***DOC, HTML***, and ***JS***, as well as generic trojans and phishing. ***CVE-2017-11882*** was targeted on its own as a sole vulnerability to an extent previously unseen in bulk campaign volume to attempt compromise. In addition, ***XLS*** files were also observed in notable volume hitherto not seen, and this activity was observed in significant volume campaigns from Week 11 onwards (from 13 Mar 2020).

Chartres, Cryxos, and Zmutzy Malware were observed in significant volume campaigns during the period of report and these should be considered significant key threats in the weeks ahead.

Separate additional research into the Australasian region for this same period also suggests that these three Malware threats are ***likely (≈55% – 75%)*** to see increased use, and all were detected in varying volumes in a range of campaigns within that region during the same period.

The same research detected ransomware present in 60% of the ten (10) identified campaigns against the Australian ***Education*** vertical during the same period. It is ***almost certain (≥≈ 95%)*** that threat actors are exploiting this period of increased disruption and uncertainty to attempt ransomware insertion to any vertical possible through the increased use of all potential attack vectors.

Blocked URL Click Detections

Significant increases were observed in Weeks 13, 14, and 15. This had deteriorated by 55.8% at the end of March. This detection data gives cause for concern. This represents the detection data concerning the clicking of unsafe URL links by users or employees, linking to websites that are considered malicious or unsafe. The increases are illustrated in ***Figure 8***:

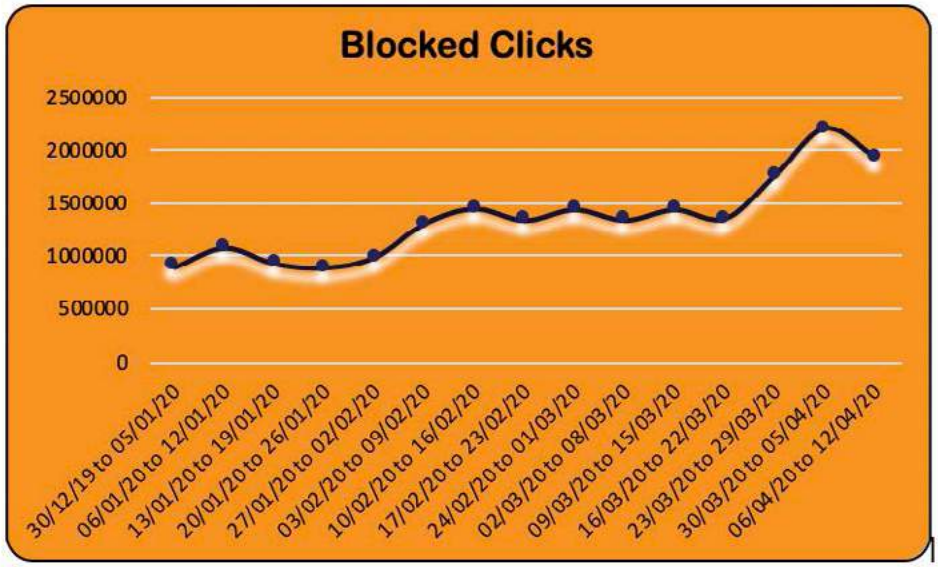


Figure 8: Blocked URL Click Trend

Blocked URL click detections showed an initial increase in Week 6 (ending 09 Feb 2020), to a relatively stable level which was maintained, although fluctuating weekly, for a period of approximately seven (7) weeks. In the last three (3) weeks (from Week 13, ending 29 Mar 2020), this volume increased, with an overall increase of 55.8% by the conclusion of the period of analysis.

The data relating to the period up to mid-February evidenced the successful maintenance of cyber hygiene up to the close of Week 7 (ending 16 Feb 2020). The fluctuations here (and over the following weeks to the week ending 22 Mar 2020) are indicative of an apparent seven (7) week long period of relative stability in the total volume of unsafe clicks (maintained at a slightly increased level than normal from the week beginning 03 Feb 2020). During this period there was repeated weekly fluctuation in the headline total for unsafe clicks, but between two relatively stable upper and lower figures.

Since Week 13 there has, however, been a significant increase in the volume of unsafe clicks detected. There has also been a significantly increased volume of threats detected during this same period, but this current trend is considered ***highly likely (≈80% – ≈90***%) indicative of increasing human error and a deteriorating situation in relation to individual's cyber hygiene generally, as huge sections of workforces globally have now been working from home for many weeks. This is ***almost certainly (>95%)*** being exacerbated by the addition of large sectors of workforces ordinarily unaccustomed to working from home being introduced to unfamiliar practices and procedures outside of the supervision and constraints ordinarily supported, encouraged or imposed by the workplace environment.

Additional factors to consider, which may also be significantly impacting this figure, are the extent of lockdowns regionally and globally at present and the onset of boredom, a desire for up-to-date information and news, and the significantly enhanced potential for misuse by persons other than an employee through the poor physical security of work-related devices. ***Figure 9*** illustrates the significant concentration of effort on ***COVID-19*** themed domains and websites, becoming a key issue from the beginning of March, with over 8,400 clicks related to this subject alone since then.

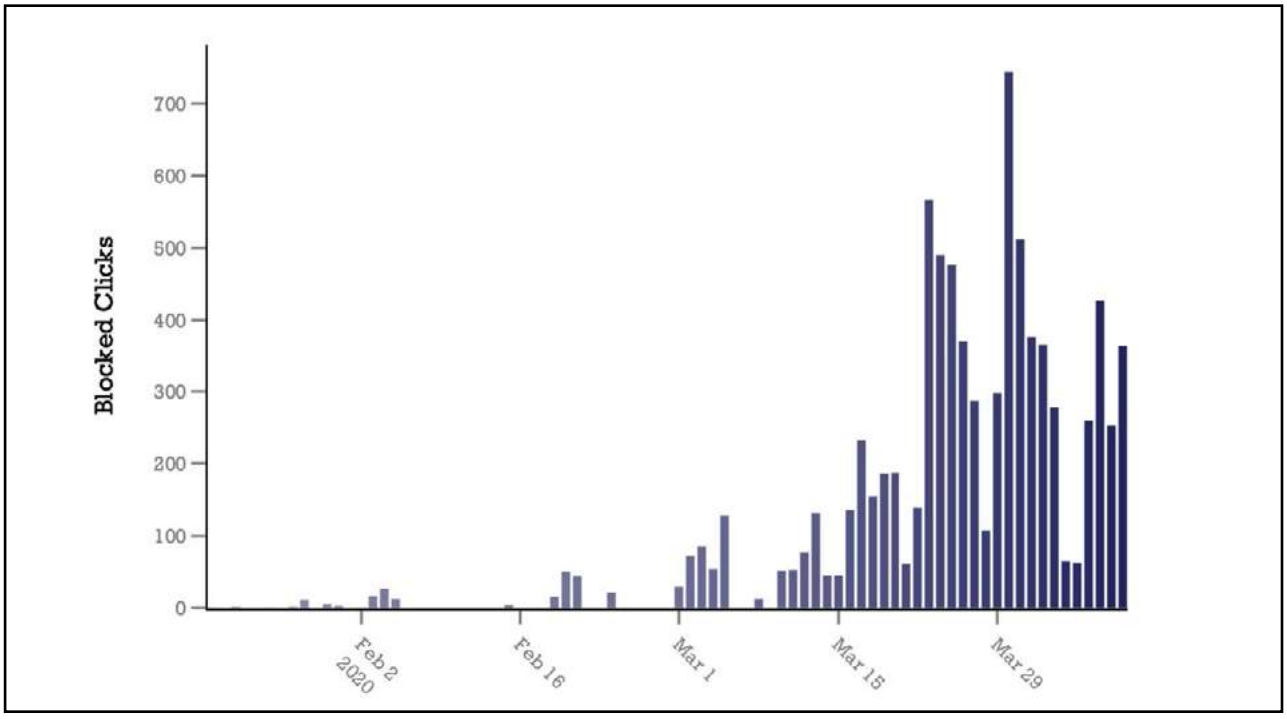


Figure 9: Blocked COVID-19 URL Clicks

Malicious Emails - Examples

This section of the analysis contains examples of email samples subject to investigation. These demonstrate the range of ***COVID-19*** related campaigns undertaken by threat actors during the period of reporting. These campaigns have been seen in volume by Mimecast and samples of the email messages are included.

It is evident that there is a diverse mix of campaigns being undertaken, which includes the recycling of tried and tested methods by threat actors. Given the evolution of threats illustrated here, it is assessed that the range of threats encountered is ***likely (≈55% – 75%)*** to continue to both increase in volume and become more sophisticated the longer the pandemic remains a subject of significant concern to the global community.

As with the "Email Attack Vectors" section of this report (above) the samples are noted in week and date order to illustrate the nature and increasing diversity of the threat, and to allow easy cross-referencing to the other sections of this report.

Figure 10 is an example of a potentially malicious email used by threat actors as a vector for delivery of malicious content. As is typical in such campaigns, it requires the victim to click on a link, in this case a ***.pdf*** document, to download malicious code, or be redirected to a malicious URL. The body of the email acknowledges this by making repeated requests to shape the recipient's action, by suggesting that the link be clicked.

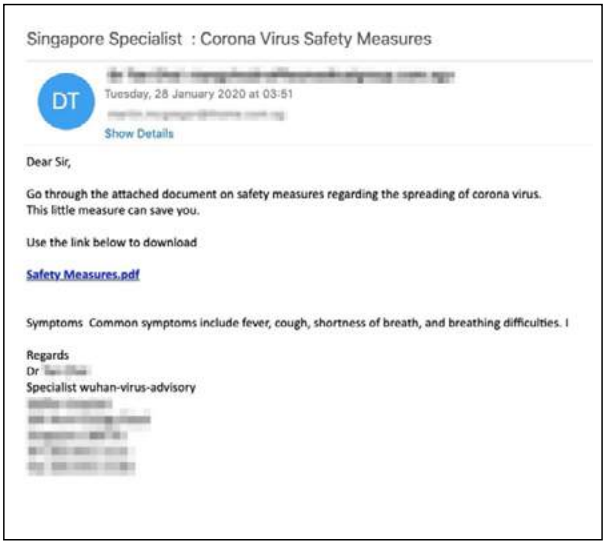


Figure 10: Example of potential email vector for malware delivery

Threat actors aim to play on the target's genuine fear of the impact on them by such global incidents, to increase the likelihood of victims clicking on an attachment or link delivered in a malicious communication. Ultimately this will cause infection of a single machine, system, or network, or can be made for monetary gain. Research has shown that over 90% of compromises occur by email, and that over 90% of those breaches are primarily attributable to user error.

Researchers at Mimecast uncovered several different campaigns – including emails targeting healthcare professionals regarding a staff seminar on the virus (where they are encouraged to enter their credentials in an Outlook application) or emails containing a link that directs recipients to a fake website bearing an HMRC logo offering a tax refund (where they are encouraged to enter bank account details):

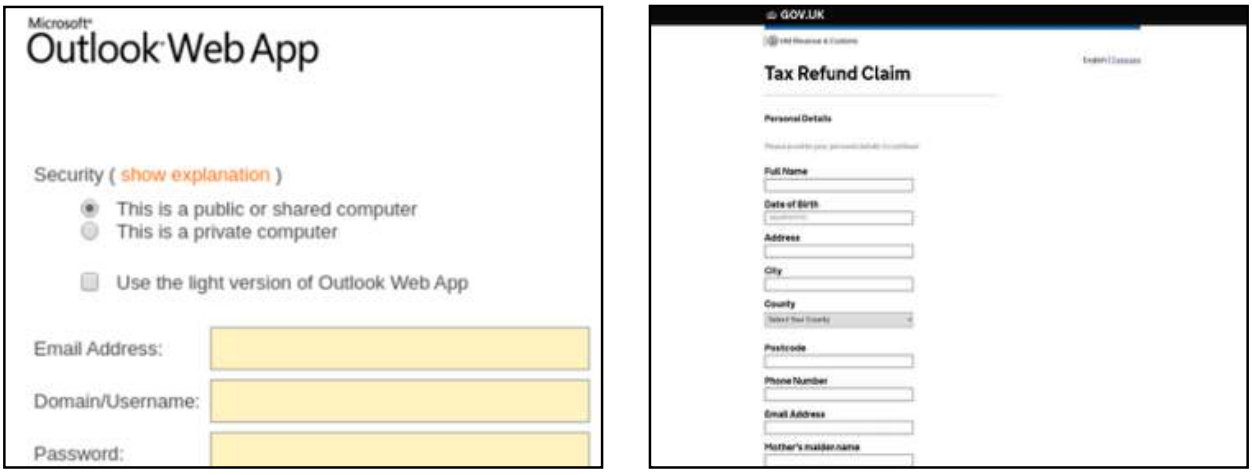


Fig 11: Screenshots of Coronavirus Campaigns – Healthcare Professionals (left) and HMRC (right)

Numerous example emails follow to illustrate the diverse and changing nature of the campaigns undertaken during this period of analysis. Each is in date order and is also noted by the week of the report they were sent in. They are primarily Spam/opportunistic and phishing samples which sought to steal credentials and/or personal details.

Week 5: 31 Jan 2020 - Spoofed CDC Email

This sample, sent to a US recipient, attempted to lure clicks by spoofing the CDC and purporting to provide information on local virus cases for personal safety purposes:

Figure 12: Spoofed CDC Email

Week 11: 09 Mar 2020 - Trump Sexting Disinformation Email

This sample, sent to a US recipient, attempted to lure clicks by spoofing a media outlet with an apparently salacious but false story about the US President:

Figure 13: Spoofed News Outlet Email

Week 11: 11 Mar 2020 - Fraudulent Treatment Email

This sample, sent to a US recipient, attempted to lure clicks and online sales of "the best protection against ***Coronavirus***" by purporting to originate from a senior clinician in South East Asia:

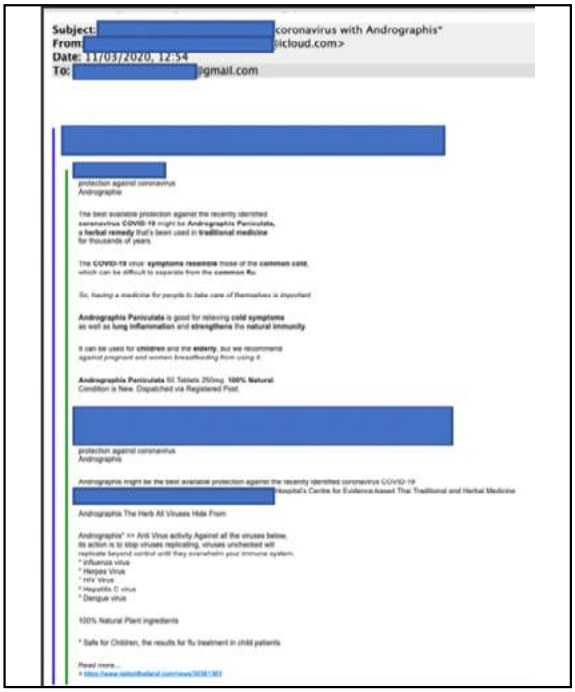


Figure 14: Fraudulent Treatment Email

Week 11: 13 Mar 2020 - "Health HelpDesk" COVID-19 update Email

This sample, sent to a US recipient, attempted to lure clicks through purporting to offer helpful ***COVID-19*** related information including from the CDC:

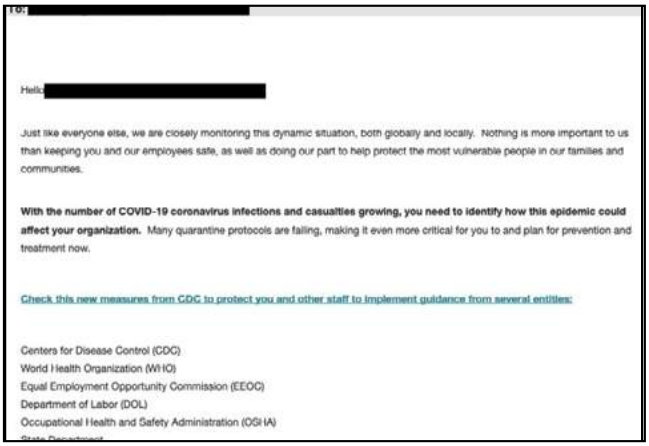


Figure 15: "Health HelpDesk" update

Week 12: 16 Mar 2020 - Spoofed WHO Health Alert - COVID-19 - spread up 25% Email

This sample, sent to a US recipient, attempted to lure clicks through an alarming headline in relation to the ***COVID-19***'s spread:

Figure 16: Spoofed WHO Health Alert

Week 12: 16 Mar 2020 - "All Staffs" Mandatory COVID-19 Update Email

This sample, sent to a US recipient, attempted to steal credentials by linking to a ***OneDrive*** login page, presenting as an essential safety related policy change. Given the extent to which workforces are working from home, perhaps even for the first time, this would be a plausible and effective lure:

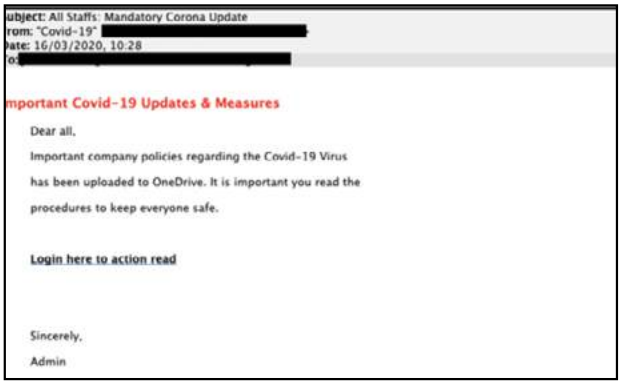


Figure 17: "All Staffs" COVID-19 Update Email

Figure 18: Landing page

Week 12: 20 Mar 2020 -

Action Required - Work Remotely Enrollment Email

This sample attempted to steal personal data and credentials by utilizing a fraudulent "remote work enrolment process" in an attempt to present as an essential employment related process. Again, given the extent to which workforces are working from home this would also potentially be an entirely plausible lure:

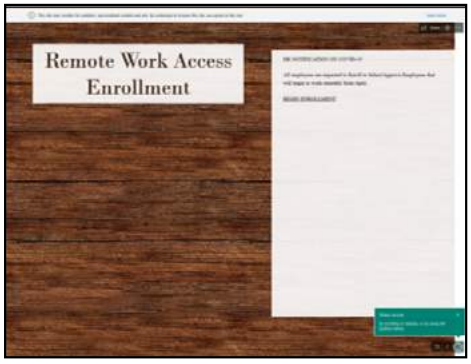


Figure 20: Landing page

Figure 19: "Action Required" Email

Figure 21: Credential Stealing "Log in" Page

Week 12: 24 Mar 2020 -

Spoofed WHO "Safety COVID-19" Awareness Email

This sample obviously had increased effort put into it by the threat actors, spoofing the WHO plausibly and appearing far more professional than previous or similar WHO related emails. This kind of login, requesting a phone number, might well lead to telephone contact to effectively avoid security measures, and given the increased vulnerability of isolating employees away from the workplace:

Figure 22: WHO Awareness Email

Figure 23: WHO Landing Page

Week 13: 25 Mar 2020 - Coronavirus Safety Measures - Urgent Care Spoof

This sample purports to be from medical providers in relation to ***COVID-19*** safety measures to solicit opening of the attached malicious document:

Figure 24: COVID-19 Safety Measures Email

Week 13: 27 Mar 20 - COVID-19 Loan Offer

This sample is an interesting example of cyber-enabled fraud, given the variety of contact means provided it is ***likely (≈55% – 75%)*** that personal contact would be used to evade security measures and to gain credentials or bank details from the target. Given the difficulties some will experience during any period of furlough, or loss of earnings, this is clearly targeting those who are already worse off or struggling:

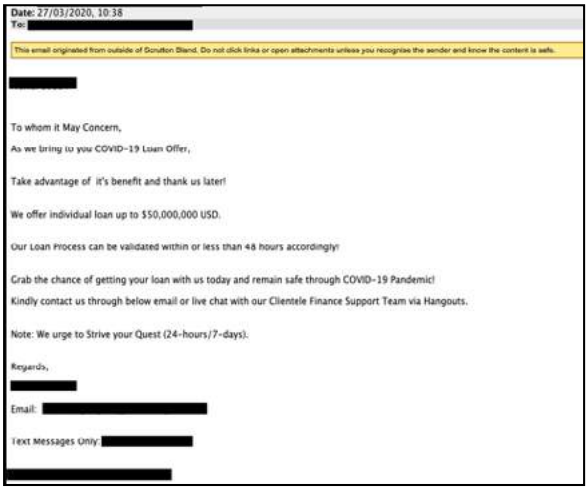


Figure 25: COVID-19 Loan Offer Email

Week 14: 31 Mar 2020 - COVID-19 Deceased Estate Transfer Email

This sample is a variation on a typical scam that has been seen before, with reference to effectively splitting the proceeds of a deceased individual's estate with the recipient, simply seeking to capitalize on the potential for the appetite to initiate an ***exchange*** and credential or monetary theft.

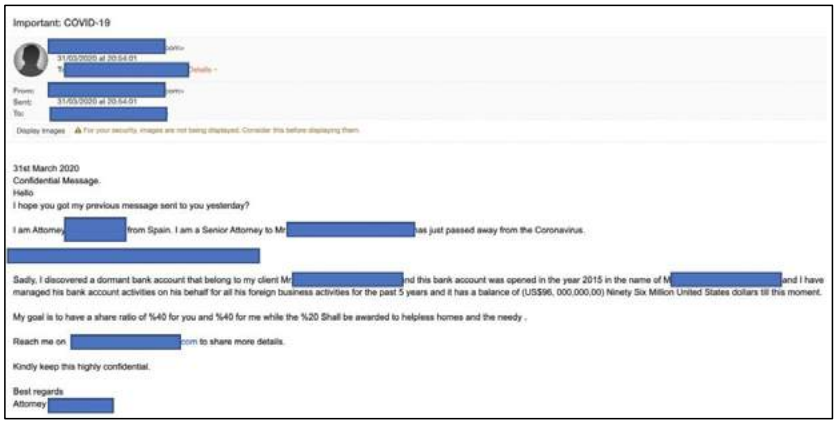


Figure 26: Deceased Estate Email

Week 14: 02 Apr 2020 -

New Pandemic Instruction allegedly from the White House Email

This sample attempts to appear to originate from the White House and to provide key instructions related to the pandemic to elicit clicks on the link:

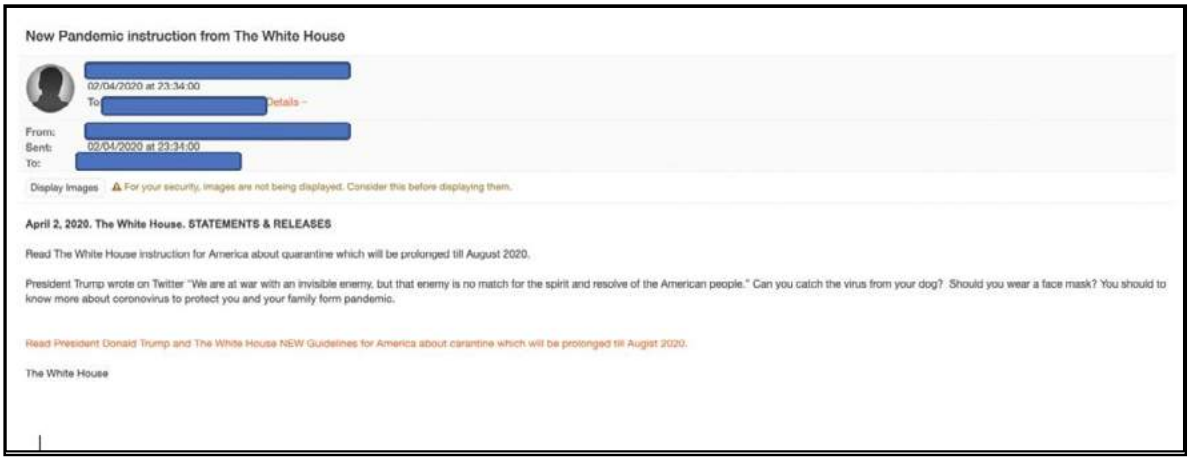


Figure 27: Pandemic Instruction – White House Email

Week 14: 02 Apr 2020 -

COVID-19 Tax Cut Document Email

This sample is part of wider and more general targeting globally in relation to any fund seeking to support employees during the current crisis. This threat actor has utilized ***SharePoint*** to attempt to evade detection. As with other examples, given the difficulties some will experience during any period of furlough, or loss of earnings, this is clearly targeting those who may well already be worse off or struggling:

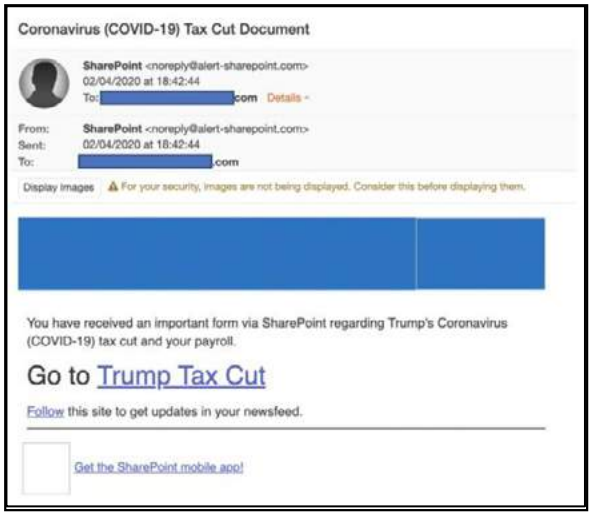


Figure 28: Tax Cut Email

Week 15: 27 Mar 2020 -

Airline Flight Refund Email

This sample is an interesting flight refund example which has only recently surfaced, attempting to exploit individuals who may well now be seeking genuine recompense for holidays booked. The landing page requests personal details including payment details:

Figure 29: Flight Refund Email Figure

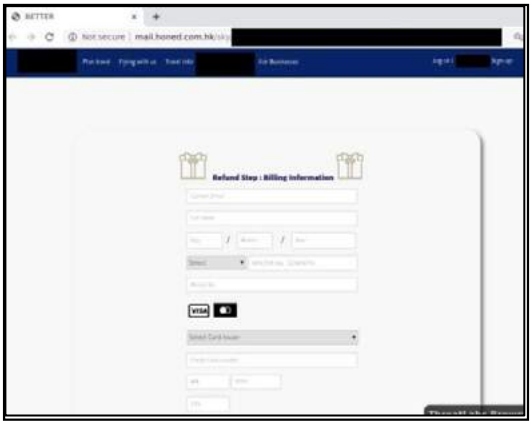


Figure 30: Landing Page

Week 15: 06 Apr 2020 -

COVID-19 Dropbox File Share Email

This sample is another example of the Dropbox scam, claiming someone whose name appears in the title has shared documents with you. This is of course unlikely to be successful unless in stress and error, or where an employee with that name is known to the recipient:

Figure 31: Dropbox Email

Week 15: 06 Apr 2020 -

GOV UK Tax Refund Email

This sample is essentially a variant of the Week 14 US Tax example, seeking to gain clicks and then credentials in relation to a promised tax refund. With many employees furloughed or working from home this may be enticing if individuals are struggling:

Figure 32: GOV UK Tax Refund

Week 15: 08 Apr 2020 -

Breaking News Disinformation Email

This sample is an interesting example of crossover into disinformation through exploiting well-known political division and tensions, albeit to lure clicks and to cause compromise to anyone who is curious enough to click:

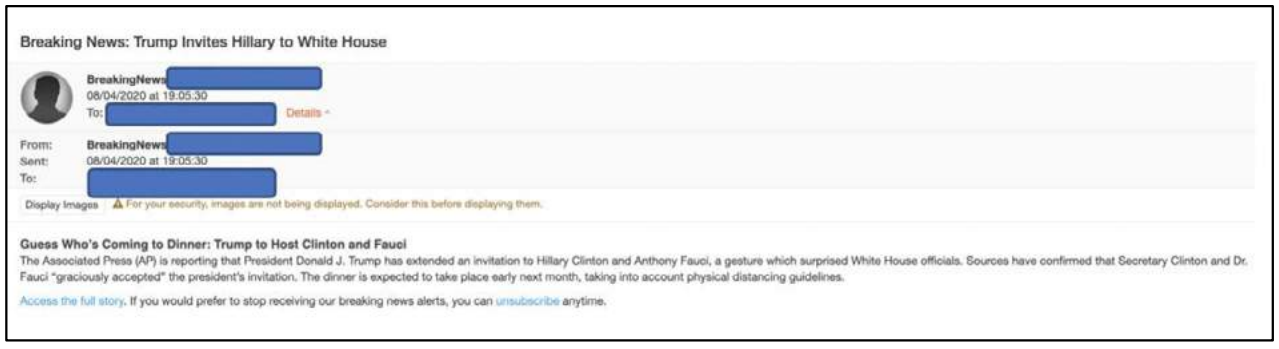


Figure 33: Breaking News Email

Week 15: 08 Apr 2020 -

COVID-19 Economic Trend & *Manufacturing* Report Email

This sample was seen in volume from this initial date and clearly attempts to spoof a well-known publication with a potentially interesting article, again to lure clicks:

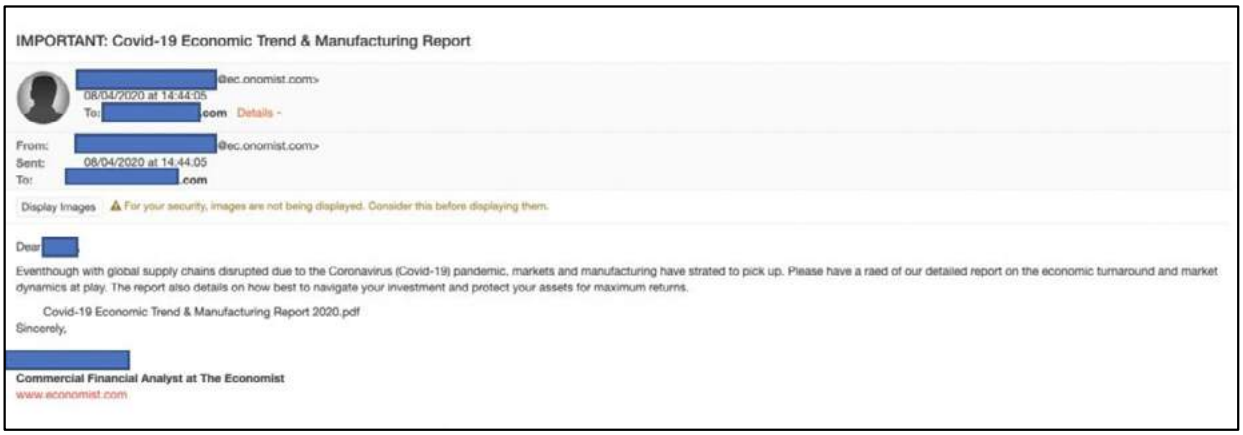


Figure 34: Economic Trend Report Email

Week 15: 09 Apr 2020 -

Stranded Email

This sample is perhaps one of the most potentially distressing for victims of all, and essentially presents an almost apocalyptic scenario to tug at individuals' heartstrings and engage in communication, almost certainly to initiate fraud and social engineering. It's interesting because of the increasing intersection of traditional fraud, which is now being cyber-enabled, and what is considered a cyberattack. The line is increasingly blurred:

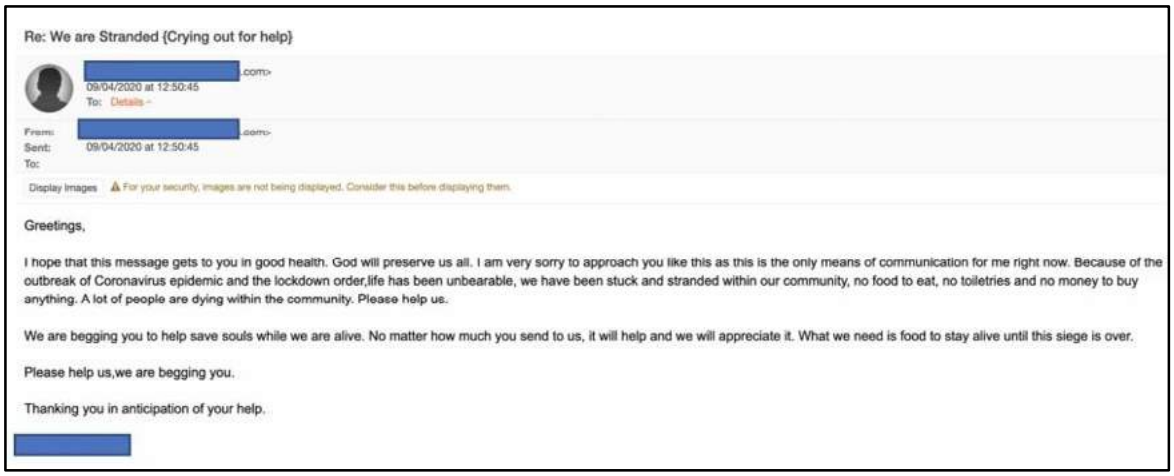


Figure 36: Stranded Email

Week 15: 09 Apr 2020 -

COVID-19 *Healthcare* Welcome Email

This sample is also a message that was apparent in volume from this date and purported to represent a virus specific healthcare scheme in an attempt to lure clicks and credential theft. The group and policy ID's were the same in all noted cases:

Figure 37: Healthcare Welcome Email

Week 15: 09 Apr 2020 -

Kills COVID-19 for 28 days Email

This is another example of the cross-over between cyber-enabled criminal activity and pure cyberattacks. Using the brand of an existing company, it presents a tempting, albeit fantastic, solution to the virus to lure social engineering and attempt fraud:

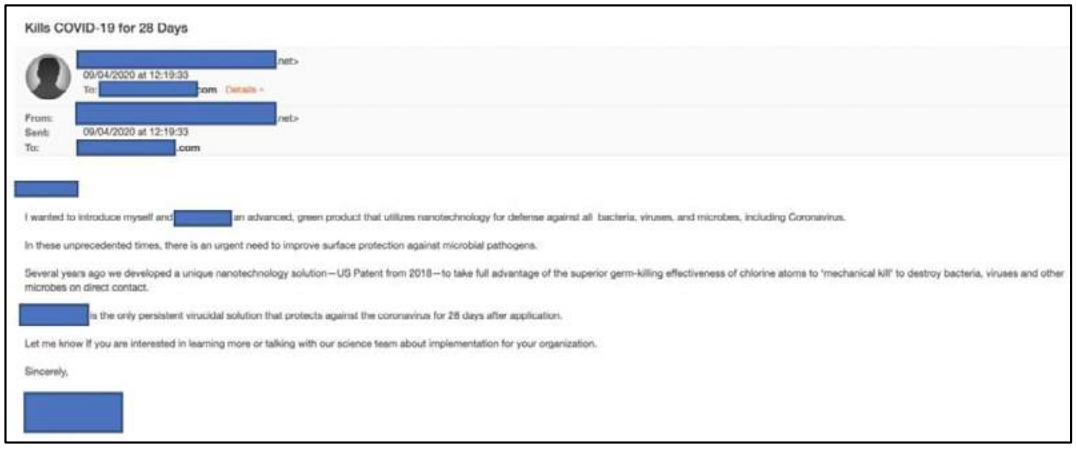


Figure 38: Kills COVID for 28 days Email

Web Campaigns

During this reporting period, a surge in domain-related abuse became apparent in relation to COVID-19 and associated monikers. ***Figure 39*** illustrates the volume of suspicious domains seen to be registered in relation to the virus. ***Figure 40*** illustrates Mimecast's blocking activity, having now blocked over 115,000 of these domains during the period analyzed.

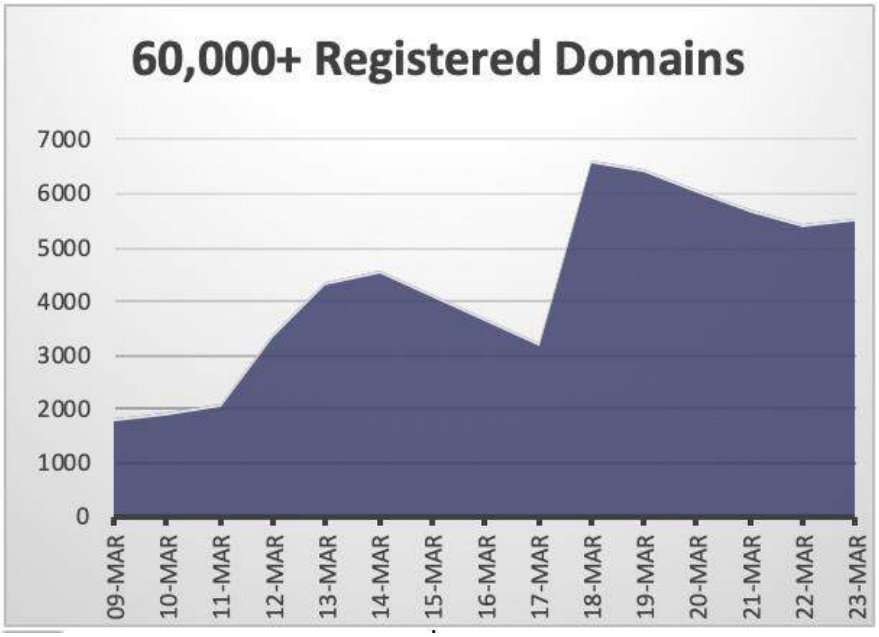


Figure 39: Virus related Domains Registered

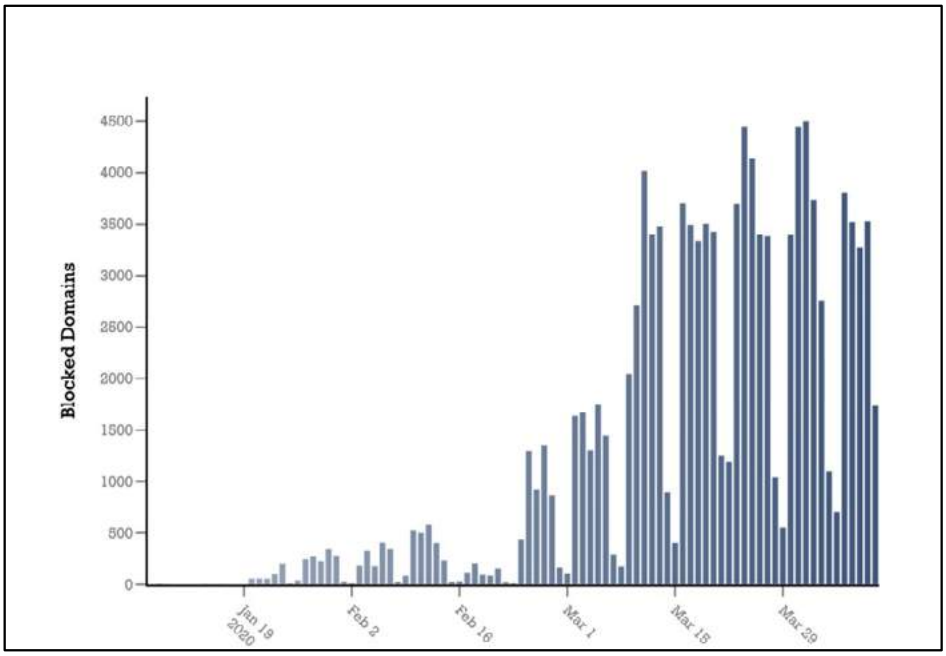


Figure 40: Virus related Domains Blocked

There is some activity in January 2020 but gathers pace significantly throughout February 2020 before huge increases to approaching 4,500 blocked domains each day on several days from mid-March. This activity clearly shows the effort of threat actors focused on domain attack methodologies, ***likely (≈55% – 75%)*** to enable a varied fraud and cyber-enabled criminal activity of all kinds in relation to the virus.

At the same time, the heavily targeted ***Retail*** vertical has seen spoofing of major retail brand domains to steal from unsuspecting consumers attempting to use their online sites. ***Figures 41 and 42*** illustrate examples of this activity seen - "Walmartone.fyi", an anonymized registration in Panama on 31 Jan 2020.

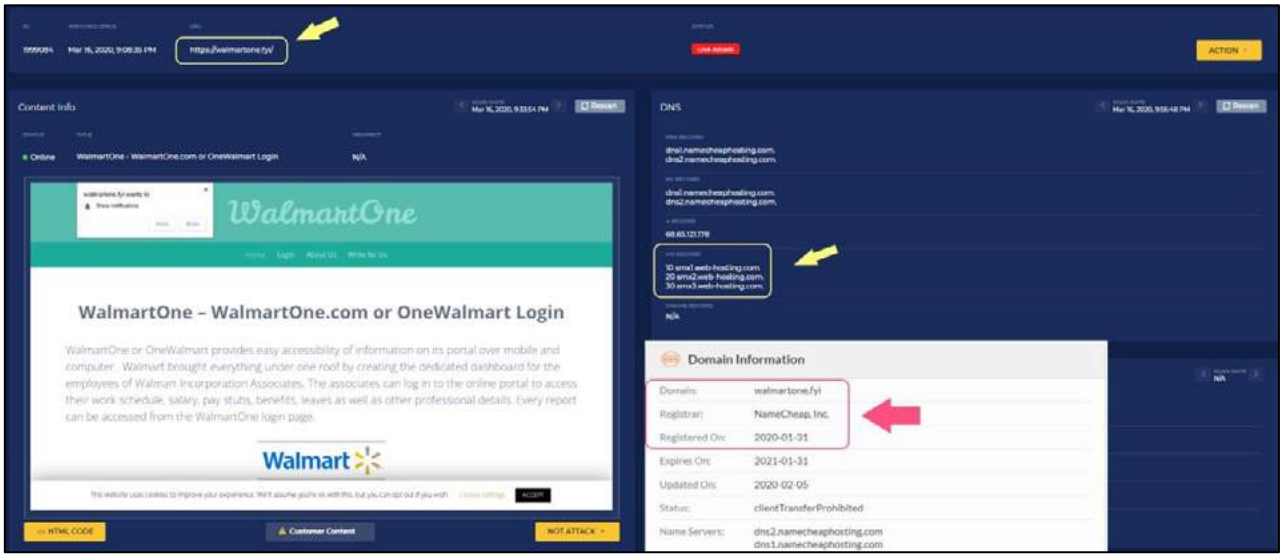


Figure 41: Walmart - Spoofed Website

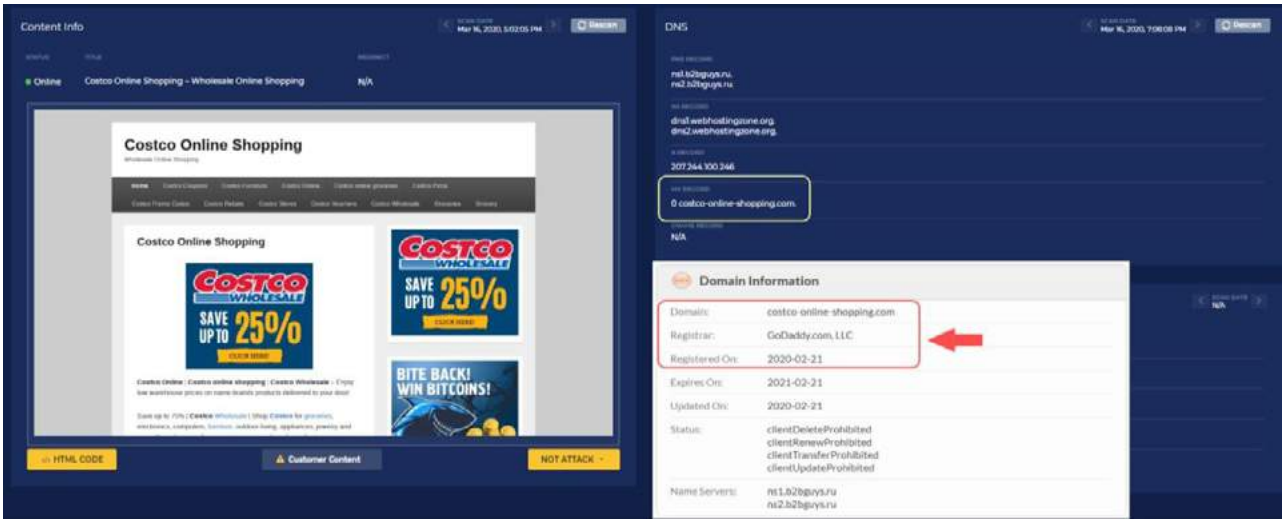


Figure 42: Costco – Spoofed Website

Additional web security research has indicated that prominent charities related to the current crisis and affiliated with major media outlets, particularly at least one major US publication, have been subject to domain/website spoofing over recent weeks and these are clearly criminal efforts seeking to divert much needed funds away from legitimate causes. This should indicate that threat actors will exploit different avenues to advance fraud and compromise objectives at this time, given the wide- ranging opportunities presented by the current situation across much of the world, at this time including multiple "lockdown" conditions across many nations.

The volume of ***COVID-19*** related blocked pages significantly increased from 25 Feb 2020, increasing from 537 on the Monday to 1,537 on the Tuesday. They have stayed high since. This coincides with the period soon after the US stock Market crash on Monday 21 Feb 2020, the WHO-China Joint

Mission and the later declaration of a pandemic and the ensuing national "lockdowns". The figure below illustrates this trend

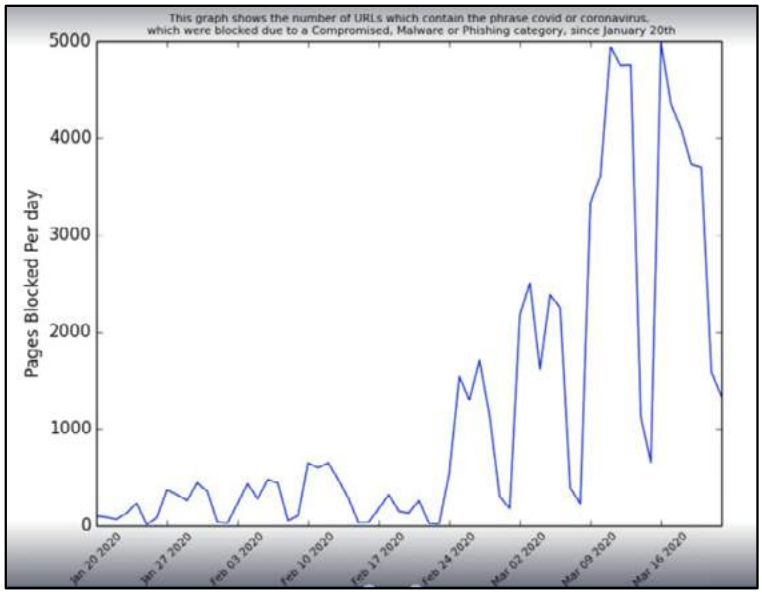


Figure 43: Pages Blocked per day - 20 Jan 2020 onwards

Analysis & Comment

Common Vulnerabilities

As demonstrated in the section above, the efforts to exploit the crises in relation to the pandemic use previously-identified (via reporting) vulnerabilities and behaviors. Such vulnerabilities and behaviors have common themes and processes:

Assets

Most organizations lack a complete view of their internet-facing assets. These assets comprise a large and complex attack surface that needs to be understood and ***actively managed*** to reduce the 'low-hanging fruit' available for cybercriminals to exploit. There are two potential contributors to this lack of visibility: shadow IT and vulnerabilities potentially resulting from mergers & acquisitions.

Some of the key shadow IT asset types include: hosts, domains, websites, certificates, third-party applications, and third-party components. Often over-looked and unmanaged, over time these assets will not be habitually patched, or security tested, and the operating systems, frameworks, and third-party applications of which they comprise can quickly age and become vulnerable to common hacking tools and techniques.

Mergers and acquisitions often bring with them their own shadow IT issues that can further exacerbate the problem. While some of these assets will have mitigating controls to prevent the identified vulnerabilities and exposures from being exploited, many will not.

Apart from their own assets, organizations should also be aware of activities impersonating or affiliating assets created to target their customers and third-party stakeholders. Phishing tactics continue to be increasingly sophisticated, often leveraging multiple cyber activities and process.

Malware / Ransomware

As discussed in the "Threat Landscape" section above, emails often appear legitimate and may have an attachment, such as a ***pdf, document, zip*** file, video, or spreadsheet. Often, when the target clicks on the attachment to open it, malware is downloaded onto the target network.

Global ransomware attacks have increased significantly in number over previous years and have caused millions of dollars of data recovery costs, brand damage recovery costs, operational costs, insurance costs, and other expenses to organizations.

Managerial and Policy Implications

If there is not a clear cyber resilience / mitigation culture within an organization (or clear process for sub-contracting / out-sourcing to a third-party organization), vulnerabilities may develop which could be exploited. Again, such vulnerabilities could be discovered from social engineering or phishing campaigns.

Weak governance compounds the problem of defending against cyberattack and makes it difficult for organizations to cooperate with each other in defending against such attacks. Even unsophisticated attacks can succeed in this environment and evidences the importance of sharing techniques to enhance one's partners' abilities to identify, detect, or respond to threats.

The inability to create a governance structure for information-sharing among organizations and with the government, for example, means that many attacks are not identified, prevented, or remedied.

Additionally, as discussed above, mergers & acquisitions may also bring challenges to managerial and policy implementation as the new infrastructure is onboarded. This could be exploited by experienced threat actors who would have carried out social engineering processes or "pattern- of-life" analysis of their target to launch their attack / campaign during this period.

Machine / Human Interface

In examining each of the common vulnerabilities highlighted above, there is a common factor that runs throughout them all, that is human interaction. Whether it is following a link, not patching hardware / software, not creating a robust framework, humans are involved. It is assessed that human error and social engineering account for 90% of all breaches. By implementing a robust training process the presence of the 'human firewall' will greatly add to a layered security strategy.

Which Technologies Are of Most Concern?

From the "Threat Landscape" section above, an important part of assessing the potential for systemic risk from a cyberattack is understanding the mechanisms and pathways that could propagate the effects of an attack.

As organizations become more dependent on technology as a business enabler, the security and reliability of their connectivity is inevitability of increasing importance. Such businesses are reliant on the Internet and networks to function. However, this evolution of technology and the increased drive towards mobility has facilitated threats from cyberattack who use this same enabler to gain access to organizational networks, exfiltrate Personally Identifiable Information (PII) and take advantage of any potential vulnerabilities.

Zero-Day Attacks

'Zero-day attacks' exploit previously unknown vulnerabilities for which defenders are unprepared. Zero-day attacks are readily available and let attackers use new and undetectable software tools to siphon off cash, IP, PII, or disrupt networks.

There continues to be a thriving global market for zero-day attacks, with researchers in many countries offering their discoveries of unknown vulnerabilities for sale to cyberattack, governments, or sometimes even the company that produced the software.

5G

Fifth-generation mobile technology is opening us to a period of increased vulnerability of disruption. 5G will also present an increased exposure platform for attacks, offering more potential entry points for attackers to utilize.

5G topology will be increasingly based on software, and the associated risk and security flaws resultant from poor software development processes by suppliers will gain in importance.

Insufficient processes could make it easier for threat actors to insert backdoors into products and make malicious code harder to detect.

Internet of Things (IoT) and Industrial Internet of Things (IIoT)

State-sponsored, hacktivist-driven, and other adversary-driven attacks on IIoT systems are increasing in the utilities, energy (oil, LNG, and natural gas), and ***manufacturing*** industries. Adversaries are taking advantage of the fact that the ONG industry is slowly moving to digitize its IIoT systems.

Geopolitical Outlook

With the ***COVID-19*** pandemic global infection continuing to rise there is an increasing impact on medical facilities (and the associated supply chain industries) and domestic retail suppliers. Prior to the outbreak, it is estimated that supermarkets accounted for approximately 60% of food sales. With the closing of restaurants, cafes, and bars to contain transmission, supermarkets were propelled instantaneously to the sole provider of food. This coupled with unprecedented 'panic buying', left many communities short of the most basic provisions that stores would take time to recover from.

As the virus has spread, international borders, travel, social interactions, and relationships have become more strained. With organizations from all sectors having to rapidly adapt to a remote working posture, and now embracing not only cyber, but personal, operational, and political resilience, a period of uncertainty is upon us.

It is hoped lessons are learned from this phase of 'experimental remote working' and regularly tested in moving forward. With the global spread of the ***COVID-19*** virus continuing apace, accompanied by an increasing number of cyberattack campaigns, many organizations are mandating their employees 'work from home' where able.

Despite being a physical and geographical issue comparisons can be clearly drawn with cyber targeting methodology where times of confusion or global events are exploited to conduct campaigns. These actors are often opportunistic and inventive, and will seek to exploit the public's, governments', and organizations' fears, in order to perpetrate malicious activity.

Governments will be under pressure to provide financial assistance to organizations, individuals, and other nation states. There is a ***high likelihood (≈80% – ≈90%)*** that as organizations seek financial assistance, malicious campaigns will seek to exploit this in the very near future.

Furthermore, with a number of global events having to have been cancelled or postponed, such as the 2020 Olympics, there is considered a ***high likelihood (≈80% – ≈90%)*** that future cyber campaigns may focus on using the lure of reclaiming expenses to elicit interaction with malicious content.

Organizational response to the concerns over the transmission of the ***COVID-19*** virus included many organizations opting to have their staff work from home, thereby maintaining organizational resilience. This upsurge in the adoption of remote working can be considered as revolutionary, and even only a few years ago, would have been thought of as implausible. But with the advancement in technology facilitating collaborative team environments, chat applications, video conferencing, and VPNs, this way of working is proving to be a more cost effective and a business and employee sustainability option.

For remote working to be effective, staff must be trusted to be productive off-site, and managers and organizations must adapt accordingly. This should not consist of a 'big-brother' mentality utilizing key loggers, camera / microphone access, or time and motion studies, but be based on trust. This allows for a better work / home life balance and any issues with this now tried and tested methodology can be seen as with management, rather than the employees.

Assessment (So What?):

The ongoing situation and continued transmission of the ***COVID-19*** virus is threatening to cause long-term effects globally. This will be felt across a range of industries from ***manufacturing*** / ***production***, ***logistics / transportation***, ***hospitality / catering*** through to ***finance***.

It is assessed there will ***almost certainly (>95%)*** be an increase in cyberattacks following on from any significant disruptive event that exploits perceived human vulnerabilities such as benevolence and fear. The motive for these attacks being to identify vulnerabilities in infrastructure and defenses, which can be exploited and used to improve future attack methodologies.

Recommendations

The Mimecast Threat Intelligence team assesses there will be an increase in the observed cyberattack methodologies against vulnerable targets during this time of significant uncertainty and instability. There are several significant but simple steps you can take to minimize risk and increase cyber awareness, such as following safe cyber hygiene practices, for example, strong password usage and never enabling macros in any attachments if you do open them. The necessity and prevalence of working from home and the potential impact of vast numbers of employees working from home includes a significant increase to the size of any organization's attack surface and, therefore, there is more opportunity for attackers to exploit, particularly if employees let cyber hygiene slip or are distracted at home by the competing priorities of work and home. Threat actors and criminals will ***almost certainly (>95%)*** seek to exploit the increased numbers of employees working from home and see them as an enhanced opportunity to compromise secure workplace networks. We recommend the following be considered now:

1. In anticipation of the further, additional and expected increase in cyberattacks, and because business email compromise (BEC) is a prominent attack vector, we strongly advise companies to review their policies and practices on cybersecurity – including increasing awareness training on the most common attack campaigns and encouraging IT/SOC teams to enforce unique password policies and to enable two-factor authentication wherever possible.

   This also includes training employees to maintain a level of discipline in relation to screen-locking devices when away from them and being careful not to let children, family members or other unauthorized users to use work devices due to the risk of unintentional or inadvertent compromise via human error. This will also help reduce the risk and limit the impact of any successful phishing scam. Finally, do not click on any links or attachments related to ***COVID-19*** that are received via email or messaging apps.

2. Be wary of any electronic communications received and be vigilant to the potential for significantly increased social engineering or pattern-of-life analysis attacks that working from home presents. It is ***highly likely (≈80% – ≈90***%) that attempts will be made by threat actors to move interaction with staff to other means of communication outside of the protected network as soon as possible, particularly by telephone. In this way they will try to draw personnel into what might be considered more traditional scams or fraudulent behavior. This is already evident in some samples already observed.

3. In anticipation of a resumption of ***Emotet*** activity at any time, it is noteworthy that it is being tailored to take advantage of current events in much the same way as phishing does. User awareness of current campaigns will ***likely (≈55% – 75%)*** aid any organization in resisting compromise by ***Emotet***. Any significant event or tragedy is ***almost certain (≥≈ 95%)*** to become subject to specific campaigns by threat actors to entice users to click links or open attachments. Current and recent examples of this activity seen by Mimecast relate to charitable donations for the Australian Bushfires and a wide range of varied campaigns in relation to the ***COVID-19*** pandemic.

4. On infection ***Emotet*** uses a compendium of weak or commonly used passwords to brute force its way into a system. A network can, therefore, be hardened against this specific threat by adherence to a strong user password regime and verification that all default administrative or supervisory passwords to applications and systems have been changed from their defaults. Threat actors in recent ransomware attacks have made specific comments in relation to the particularly poor or lax password regimes, and security, maintained by organizations they have successfully breached.

5. Given the prevalence of ransomware, apparent in 60% of the most recent campaigns against one regions ***Education*** vertical, likely representative of wider use generally, and the potential for ***Emotet*** campaigns being primarily intended to insert this threat, it should be considered an unacceptable risk at this time for any organization to use ***Internet Explorer*** (***IE***) as an Internet browser. The

same should be considered for ***Flash Plugin*** software. Ransomware threat actors are making increased use of Exploit kits at this time as an additional means to compromise networks and both ***IE*** and ***Flash*** are vulnerable to exploitation via this means and are ***highly likely (≈80% – ≈90***%) to be compromised if used to visit an infected or threat actor-controlled website. A review of cyber resiliency to mitigate this threat should ensure that non-networked backups are undertaken and that the organization has the facility to use fallback email and file archiving capabilities.

6. Consistently high levels of activity against, and now targeting of, the ***Retail/Wholesale*** and ***Manufacturing*** sectors globally is assessed as related to their primary importance at this time given the limited opportunities other sectors may present during any "lockdown" periods. These particular organizations, much like ***Transportation, Storage and Delivery*** which has previously been similarly targeted, represent key 3rd party risk to any organization and all should be vigilant to any potential compromise of their 3rd party supply chain. A review of service level agreements in relation to minimum levels of cybersecurity and data security may need to be considered.

7. Consideration should be given to ensuring active blocking of all image-based file types at this time. Mimecast's detections have evidenced that threat actors are increasingly exploiting image- based formats to attempt to evade detection in relation to specific attacks, including sextortion and phishing, and that this has included the use of special characters and foreign language text within images, accompanied by encryption. QR codes have also increasingly featured. This is ***likely (≈55% – 75%)*** to continue to increase as a means of attack given that some vendors have difficulty with the processing of image-based malware.

8. Ensuring that vulnerabilities are patched at the earliest opportunity is key to maintaining network security and a range of specific vulnerabilities which have been repeatedly attacked by threat actors are identified in this report from advisories or specifically ***CVE-2017-1182*** detections in volume. As a minimum, steps should be taken to ensure that all of these vulnerabilities are eliminated, if applicable. All organizations should also be aware that ***Microsoft*** recently ended support for ***Windows 2007*** and so this operating system (OS) is significantly vulnerable to increased attack if it remains in use. Consideration should be given to decommissioning any assets that use this or any older OS. A range of significant vulnerabilities have also been identified in ***Microsoft*** products recently which require patching as a matter of urgency.

9. A range of key and significant vulnerabilities in software related to VPNs and other products have been disclosed in the last quarter. There is evidence that some of them are being exploited by threat actors and so the following advisories should be noted, and appropriate action taken to update the products detailed if used by the organization: ***Apache Tomcat/ Ghostcat***[2], ***Pulse VPN*** servers[3]; ***Citrix*** Servers[4], ***Internet Explorer***[5]; Telerik UI[6] and Windows[7]. Additionally, research indicates over 80% of internet-facing ***Exchange*** servers vulnerable to ***CVE-2020-0688*** exploitation.[8]

10. Attention should be given to the security of individuals working remotely given the likely increased and significant targeting of these individuals at this time. Threat actors are ***likely (≈55%– 75%)*** to target home networks for compromise to "piggy back" into business networks and users should be wary of using any non-encrypted email or applications from home, particularly whilst using work assets. Home routers should have their default passwords changed, encryption and any firewall enabled. Any application or sign-in that can use multi-factor or two- factor (MFA/2FA) authentication should be enabled to do so. A Virtual Private Network (VPN) should also be used whenever possible.

2 ***https://nvd.nist.gov/vuln/detail/CVE-2020-1938***
3 ***https://www.us-cert.gov/ncas/alerts/aa20-010a***
4 ***https://www.us-cert.gov/ncas/alerts/aa20-020a***
5 ***https://www.us-cert.gov/ncas/current-activity/2020/01/17/microsoft-releases-security-advisory-internet-explorer***
6 ***https://www.cyber.gov.au/threats/advisory-2020-004-telerik***
7 ***https://www.us-cert.gov/ncas/alerts/aa20-014a***
8 ***https://nvd.nist.gov/vuln/detail/CVE-2020-0688***

Summary

Analysis of the first 100 days of ***COVID-19*** clearly indicates a step change in threat actor activity (particularly from the last week of February 2020) coinciding with the WHO-China Joint Mission and the US stock market crash, and across the entire spectrum of detections covered in this report.

There have been significant increases to the volume of all threats, particularly those already high in volume such as spam and impersonation. The determination of threat actors to take advantage of the unique circumstances and, therefore, opportunities the current pandemic and its attendant fear and uncertainty present should not be underestimated. Threat actors and ***likely (≈55% – 75%)*** those criminals who have hitherto committed other offences are ***almost certainly (≥≈ 95%)*** focused on taking maximum advantage of the once-in-a-lifetime opportunity to exploit and defraud individuals and organizations that the current situation of varying national "lockdowns" and supply demand presents.

Threat actors will always seek opportunities for exploiting chaos, confusion, and uncertainty to their advantage. Through utilizing deception, feigns, and guile they seek to deliver malicious effects. It is considered ***almost certain (≥≈ 95%)*** that threat actors will exploit the uncertainty with the application of mitigating measures to target those who are most vulnerable, and who are increasingly likely to be isolated at home and, therefore, more difficult to support organizationally.

The current situation of uncertainty and fear will ***almost certainly (≥≈ 95%)*** lend itself to increased incidents of human error due to stress and the difficulties of working in an environment that may be further deteriorated by a lack of workspace or additional caring issues if any household has vulnerable co-residents or children present with schools closed. This will inevitably increase stress and tiredness and, therefore, the likelihood of human error playing a part in any compromise These are ***likely (≈55%– 75%)*** to increase further over time as self-isolation measures are extended.

During the current environment of uncertainty, with the ***realistic probability (≈40% – <50%)*** of significant disruption continuing for many months, successive waves of the virus, and the potential for further geographical or national "lockdown" periods, cyber resiliency will be key to exiting this current crisis intact.

Cybersecurity should be considered a multi-layer, multi-discipline, and collaborative environment. Organizations and sectors should be encouraged to share information and adopt a proactive, rather than reactive, approach to securing networks, information, finances, and PII. At the same time, your employees are increasingly working alone or in isolation and the greater burden of judgment may we ll fall on them in the coming days and weeks as threat actors continue to attempt every means possible to compromise organizational networks.

Any compromise during a "lockdown" may prove exceptionally problematic given the travel and distancing regulations in many jurisdictions, and in many cases outright replacement of assets may be the only realistically feasible option for remediating any compromise of machines isolated at individual's homes. Cyber hygiene and user awareness are more critical to cybersecurity than they have ever been before.

In the coming weeks much of the uncertainty will gradually be replaced by a clearer picture of the steps necessary to return to (as close to) normality as reasonably possible as it can be, prior to a treatment being widely available. This may include further periods of "lockdown" and so it will be critical to keep the developing situation under continuous review and for organizations to be prepared to sustain remote working and refresh user awareness skills over a prolonged people whilst doing so.

And finally…, if you're under "lockdown", or restrictions on distancing apply in your jurisdiction at present, please remember to stay at home and save lives. We wish you all to stay safe at home and work during these unprecedented times and look forward to seeing you on the other side of this global tragedy.

Contact:

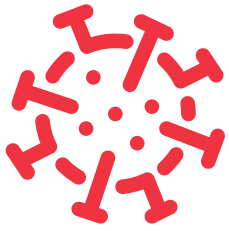
For further details, please contact:
customer.advocacy.gb@mimecast.com

Acknowledgements

This research was produced by Mimecast Threat Intelligence team members **Carl Wearn**, **Francis Gaffney**, **Kiri Addison** and **Jonathan Miles**.

How Mimecast Mitigates the Threat:

- Multiple anti-virus engines and continually updated global signature database stop known malware.
- Multi-layered attachment scanning including static file analysis, sandboxing and safe file conversion blocks unknown malware.
- URL re-writing with time-of-click analysis protects against links leading to malicious sites and content.
- Internal and outbound threat protection monitors, detects, and remediates security threats that originate internally as a result of compromise, careless or malicious action.
- Web security prevents access to malicious sites and analyses suspicious file downloads.
- Data recovery restores lost or corrupted email content to a known good state.
- Awareness training improves employee security knowledge and vigilance to improve the human firewall.



Appendix: Advisories[9]

CISA – Potential for Iranian Cyber Response to US Military Strike in Baghdad

6 Jan 2020 - The Cybersecurity and Infrastructure Security Agency (CISA) is sharing the following information with the cybersecurity community as a primer for assisting in the protection critical infrastructure considering the current tensions between the Islamic Republic of Iran and the United States, and Iran's historic use of cyber offensive activities to retaliate against perceived harm. ***Source URL***

NCSC – Alert: Actors exploiting Citrix products vulnerability

14 Jan 2020 - The NCSC is investigating exploitations of a critical vulnerability in the ***Citrix*** Application Delivery Controller (ADC) and ***Citrix*** Gateway that could allow an unauthenticated attacker to perform arbitrary code execution on a network. The vulnerability is CVE-2019-19781 and its exploitation has been widely reported online in early January. ***Source URL***

CISA – Alert AA20-014A: Critical Vulnerabilities in Microsoft Windows Operating Systems

14 Jan 2020 - ***Microsoft*** released software fixes to address 49 vulnerabilities as part of their monthly Patch Tuesday announcement. Among the vulnerabilities patched were critical weaknesses in ***Windows CryptoAPI, Windows Remote Desktop Gateway (RD Gateway),*** and ***Windows Remote Desktop Client***. An attacker could remotely exploit these vulnerabilities to decrypt, modify, or inject data on user connections. ***Source URL***

CCCS – AL20-004 Active Exploitation of Internet Explorer Vulnerability

17 Jan 2020 - ***Microsoft*** released a security bulletin detailing a critical, remotely-exploitable vulnerability in ***Internet Explorer 9, 10 and 11***. The vulnerability may allow an actor to execute arbitrary code in the context of the current user. ***Microsoft*** has assigned ***CVE-2020-0674*** to this vulnerability and stated they are working on a fix to be released as part of their February 2020 patch cycle. ***Microsoft*** has stated this unpatched vulnerability is actively being abused to compromise exposed systems. ***Source URL***

CISA – Alert AA20-020A: Revised Critical Vulnerability in Citrix Application Delivery Controller, Gateway, and SD-WAN WANOP

27 Jan 2020 - This Alert is an updated version of the Alert published on 14 Jan 2020. It provides updated information on another product (***SD-WAN WANOP***) also affected by the vulnerability, newly released fixes and creation of an IoC scanning tool to detect exploitation. The second source URL below relates to UK NCSC information regarding the same issue.
Source URL ***Source URL***

NCSC – Summary of NCSC's security analysis for the UK Telecoms sector

28 Jan 2020 - The NCSC has performed an extensive and detailed analysis of the security of the UK telecommunications (telecoms) sector. The outcomes of that analysis are now being provided through a ***blog by N C SC' s Technical Director, formal advice on the use of High Risk Vendors (HRVs)***, and through this document, a summary of NCSC's security analysis for the UK telecoms sector. ***Source URL***

ACSC – Advisory 2020-003: Mailto Ransomware Incidents- 5 January

5 Jan 2020 - The Australian Signals Directorate's Australian Cybersecurity Centre (ACSC) is aware of recent ransomware incidents involving a ransomware tool known as '***Mailto***' or '***Kazakavkovkiz***'. ***Mailto*** belongs to the ***KoKo*** ransomware family. Currently, the ACSC is unaware whether these incidents are indicative of a broader campaign. ***Source URL***

FBI – 2019 Internet Crime Report Released

11 Feb 2020 - Internet-enabled crimes and scams show no sign of letting up, according to data released by the FBI's Internet Crime Complaint Center (IC3) in its 2019 Internet Crime Report. The last calendar year saw both the highest number of complaints and the highest dollar losses reported since the center was established in May 2000. ***Source URL***

CISA – Alert (AA20-049A) Ransomware Impacting Pipeline Operations

18 Feb 2020 - CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility. A cyber threat actor used a ***Spearphishing*** Link to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network. The emergency response plan gave no consideration to the potential for cyberattack. ***Source URL***

NCSC – Foreign Secretary condemns Russia's GRU after NCSC assessment of Georgian cyber attacks

20 Feb 2020 - The decision to attribute the attack was made after the NCSC assessed that the Russian military intelligence service was almost certainly responsible for defacing websites, cyber- attacks and interruption to TV channels in Georgia in October 2019. ***Source URL***

ACSC – DDoS Threats being made against Australian Organizations

25 Feb 2020 - The threats in question are delivered via email and threaten the recipient with a sustained DoS attack unless a sum of the ***Monero*** cryptocurrency is paid. The actors behind these threats claim to be the ***'Silence Hacking Crew'***, however the ACSC is unable to verify this claim. The ACSC cannot positively verify the legitimacy of any threats made by the actor. However, the ACSC has received no reports of the threats materializing in DoS and is aware of a number of DoS threats made in the past against Australian organizations that did not eventuate.
Source URL

ACSC – Joint Agency public statement on Independent review of CSCP and IRAP

2 Mar 2020 - An independent review of the Cloud Services Certification Program (CSCP) and Information Security Registered Assessors Program (IRAP) has recommended the closure of the CSCP and the expansion of IRAP. ***Source URL***

ACSC – Advisory 2020-004: Targeting of Telerik CVE-2019-18935

3 Mar 2020 - Sophisticated actors have been scanning for and attempting exploitation against unpatched versions of ***Telerik UI*** for ***ASP.NET AJAX*** using publicly available exploits. Successful exploitation could allow an attacker to execute arbitrary code on the vulnerable server.
Source URL

NCSC – Consumers urged to secure internet connected cameras

3 Mar 2020 - Owners of smart cameras and baby monitors in the home are being urged to take three steps to protect their devices from cyberattack. With the continuing growth in popularity of these smart devices, the ***National Cybersecurity Centre (NCSC) has produced security guidance*** for users of this technology to help ensure it is used safely. ***Source URL***

CCCS – Let's Encrypt Certificate Advisory

4 Mar 2020 - The Cyber Centre recommends that all users of ***Let's Encrypt TLS/SSL*** certificates renew their certificates as soon as possible, whether ***Let's Encrypt*** has advised them of an issue with their individual certificate. ***Source URL***

ACSC – Cybersecurity is essential when preparing for COVID19

13 Mar 2020 - A reminder to incorporate cybersecurity into your contingency planning. As more staff may work from home, and the use of remote access technology increases, ***adversaries may attempt to take advantage.*** The Australian Cybersecurity Centre (ACSC) encourages Australians to remain vigilant and ensure sound cybersecurity practices. Ensuring good cybersecurity measures now is the best way to address the cyber threat. ***Source URL***

CISA – Alert AA20-073A Enterprise VPN Security

13 Mar 2020 - As organizations prepare for the impact of ***Coronavirus Disease 2019 (COVID-19)***, many may consider alternate workplace options for their employees. Remote work options—or telework—require an enterprise virtual private network (VPN) solution to connect employees to an organization's information technology (IT) network. ***Source URL***

NCSC - NCSC issues guidance as home working increases in response to COVID-19

17 Mar 2020 – Advice to help organizations manage the cybersecurity challenges of increased home working. Organizations are being urged to follow cybersecurity best practice guidance to help prepare for an increase in home and remote working in the wake of the ***coronavirus*** (***COVID-19***) outbreak. ***Source URL***

CCCS- Cyber threats to Canadian health organizations

20 Mar 2020 – The pandemic presents an elevated level of risk to the cybersecurity of health organizations involved in the national response. It is recommended that these organizations remain vigilant and take the time to ensure that they are engaged in cyber defense best practices, including increased monitoring of network logs, reminding employees to practice phishing awareness and ensuring that servers and critical systems are patched for all known security vulnerabilities. ***Source URL***

FBI- Alert I-032020-PSA: Rise in Coronavirus related fraud

20 Mar 2020 - Criminals are leveraging the pandemic to steal money, personal information, or both. Do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up personal information to receive money or other benefits. ***Source URL***

CCCS – Considerations when using video-teleconference products and services

3 Apr 2020 - As organizations adapt to health policy measures associated with the ***COVID-19*** pandemic, many are increasingly using video-teleconferencing (VTC) software products to facilitate business continuity. Care should be taken in the implementation and use of these to ensure that expected levels of integrity and confidentiality are maintained. ***Source URL***

FBI – Protect yourself from pandemic scammers

6 Apr 2020 - The head of the FBI's Financial Crimes Section discusses scams and crimes related to the ***COVID-19*** pandemic and offers tips on how to protect yourself. ***Source URL***

ACSC- Protecting small business against cyberattacks during COVID-19

7 Apr 2020 - Advice published on how small businesses can better protect themselves from cyberattacks and disruptions during ***COVID-19***. The Head of the ACSC, Ms. Abigail Bradshaw CSC, said since early March 2020, there has been a significant increase in ***COVID-19*** themed malicious cyber activity across Australia and small businesses are far from immune. ***Source URL***

CISA-DHS-NCSC- Advisory: COVID-19 exploited by malicious cyber actors

8 Apr 2020 - This is a joint advisory from the United Kingdom's National Cybersecurity Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). This advisory provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current ***coronavirus*** disease 2019 (***COVID-19***) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice. ***Source URL***

NCSC – Cloud back-up options for mitigating the threat of ransomware

8 Apr 2020 – The increase in cyberattacks related to ***COVID-19*** (and the number of people now home working) means it is more important than ever to ensure your information is backed up securely. ***Source URL***

9 *Advisories selected from include the ACSC, CCCS, CISA, DHS, FBI, NCSC, and the NSA websites