
mimecast
Threat Intelligence Report
Black Hat USA Edition 2020

Threat Intelligence Report

Black Hat USA Edition 2020

Table of Contents

Key Takeaways - 5 Minute Read

From January to June 2020, the Mimecast Threat Center analyzed more than 195 billion emails in the U.S. and Caribbean region alone, rejecting 92 billion (or 47%). While this report explores how the U.S. threat landscape stacks up against a global backdrop, Mimecast researchers also consistently track threat detections in the four primary threat categories across the globe: spam, impersonation attacks, opportunistic attacks, and targeted attacks.

Malware-centric campaigns are a fixture of 2020, becoming increasingly sophisticated and employing a diverse range of malware during the different phases of an attack. This ongoing trend is clearly pronounced in the most persistent, days-long attacks.

One of the most significant observations of this research is that threat actors are launching opportunistic and malware-based campaigns across multiple verticals at volumes never seen before, yet simultaneously, **Emotet** activity came to a halt in early February after a meteoric rise in the last few months of 2019. It's likely this trend will continue, since the subscription-based **Malware-as-a-Service** (MaaS) model provides simple attack methods to a wider audience while keeping older, well-known malware in circulation.

The use of fileless malware continues to increase, and despite the halt in **Emotet** activity there has been a notable increase in the broad use of VB-based droppers in many more campaigns.

Alongside this malicious software, threat actors have increased their sender impersonation efforts, seeking to take advantage of the circumstances of the ongoing pandemic with business email compromise containing multiple forms of social engineering. In fact, according to the Mimecast report **100 Days of COVID**, researchers found impersonation detections had increased by 30% from January to April 2020. The ongoing pandemic has increased the attractiveness of BEC attacks, so that criminals can take advantage of the circumstances prevailing during the periods of stay-at-home orders across many U.S. states.

195 bil

Emails analyzed in U.S. and Caribbean

92 bil

Emails Rejected in U.S. and Caribbean

Mimecast researchers' analysis of the data resulted in the following key takeaways:

Significant attacks came from organized criminal groups for primarily monetary gain, instead of focusing on intellectual property theft.

The attacks from January-June incorporated a vast array of threats, such as **Azorult** and **Emotet**, and which are included in the Technical Attack Detail in the appendix of this report. These threats involved a combination of mass generic **Trojan** delivery with phishing campaigns and other more complex, simultaneous threats preceding their deployment, at the same time or in subsequent days.

01

Attackers chose file compression as their main attack delivery format despite Emotet's halt in activity.

Compressed files allow for a more complex and potentially multi-malware payload, but they also serve as a basic means of hiding the underlying files within the container. The **ZIP** and **RAR** formats of file compression dominated detections – approximately three million throughout the period – and they are the most commonly detected formats for attack.

02

Verticals with "essential" status during the pandemic were repeatedly targeted.

The top verticals for attack in the U.S. and Caribbean region were Manufacturing, Retail/Wholesale and Finance: Insurance. Because this is unusual activity for these American verticals, researchers believe it is ***highly likely*** they were subject to the most significant attack as a consequence of threat actors targeting the industries that remained operable during stay at home periods, and which are key to any nation's recovery from the current pandemic. What's more, the Media and Publishing sector suffered high volumes of impersonation attacks, potentially as a vehicle for cybercriminals to spread disinformation across the United States.

03

The majority of attacks were hybridized.

Cybercriminals used both simple and complex forms of attack. This is ***almost certainly*** a reflection of the ease of access to online tools and kits for any individual to launch a cyberattack. The trend also reflects the ongoing challenge of human error – even the simplest attacks can be successful. As attacks progress, they alter exploits and include more potent forms of malware and ransomware.

04

Ransomware is on the rise, placing businesses at greater risk of ransomware attack.

Threat actors are focusing on delivering ransomware more than ever, particularly since multiple sources of reporting during this period have noted growth, both in the forms of ransomware deployed, and the number of threat actors engaging in this activity.

05

Impersonation attacks continue to accelerate as threat actors sought to sow confusion during stay-at-home orders.

Impersonation attacks increased by 24% from January to June, and since October 2019, this attack vector has been a prominent and increasing threat. Along the same lines, voice phishing (vishing) also continues to be an advancing threat with the addition of SMS-borne threats.

06

There were 42 significant and often wide-ranging campaigns against various business verticals during this quarter targeting the Mimecast customer base in the region. Given the activity increasingly evident across multiple verticals, researchers conducted deeper analysis of 92 particular attacks. Some campaigns were primarily conducted in only one- or two-day periods, as opposed to the multi-day campaigns seen in 2019, although hybridized (simple and complex attacks) threats evolved to include a phishing component in almost all attacks, paired with additional forms of malware.

Notably, the 42 attack campaigns in this report showed a significant uptick in the use of short-lived, high volume, targeted and hybridized attacks against all all verticals of the U.S. economy, as opposed to days-long attacks. This massive increase in activity is ***highly likely*** to be indicative of threat actors' efforts to capitalize on the COVID-19 pandemic, as well as attempts to exploit the necessity for employees to work from home in greater numbers by initiating high volume and determined **Cryxos** campaigns – in other words, threat actors know security practices tend to be less stringent when employees work from home.

In many ways, the circumstances of the pandemic render organizations more vulnerable to ransomware, so it remains a significant threat going into the second half of 2020.

Threat actors know security practices tend to be less stringent when employees work from home.

How They Did It

In the Mimecast Threat Intelligence Report: Black Hat USA Edition, the Mimecast Threat Center analyzed attack activity targeting Mimecast customers in the U.S. and Caribbean from January 2020 through June 2020.

The attack activity highlighted a mixture of simple, low effort and low-cost attacks, and also showed sophisticated, targeted campaigns leveraging a variety of vectors and lasting several days. These sophisticated attacks were likely carried out by organized and determined threat actors, employing obfuscation, layering, exploits, and encryption to evade detection.

Unsurprisingly, the key threat identified in the first half of this year was the multitude of ways cybercriminals sought to exploit the circumstances of the global COVID-19 pandemic. Researchers found significant, opportunistic, mixed threat campaigns in huge volumes across multiple verticals, and the mass utilization of specific malware, to sow confusion and reap the benefits.

This research explores these themes through the lens of the four main categories of attack types analyzed in the quarter: spam, impersonation, opportunistic, and targeted. This report considers major campaigns carried out by threat actors and identified from Mimecast's detection data over the first six months of 2020, inclusive of 290 million detections, more than 195 billion emails processed, and 92 billion emails rejected in the U.S. and Caribbean region. Globally, Mimecast processed over 378 billion emails and made 671 million detections during this same period.

The report identifies the trends that emerge from attacks, and assesses likely future activity given threat actors' current behaviors, events, and technology. Taken together, these factors will impact the cybersecurity landscape going into the latter part of 2020; businesses must be more vigilant than ever about the nature of attack campaigns and should follow the set of recommendations in this report to help guide security decisions accordingly.

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

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

Fig. A: The Mimecast Threat Center's Uncertainty Yardstick

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

How the U.S. Stacks Up Against the Global Threat Landscape: January - June 2020

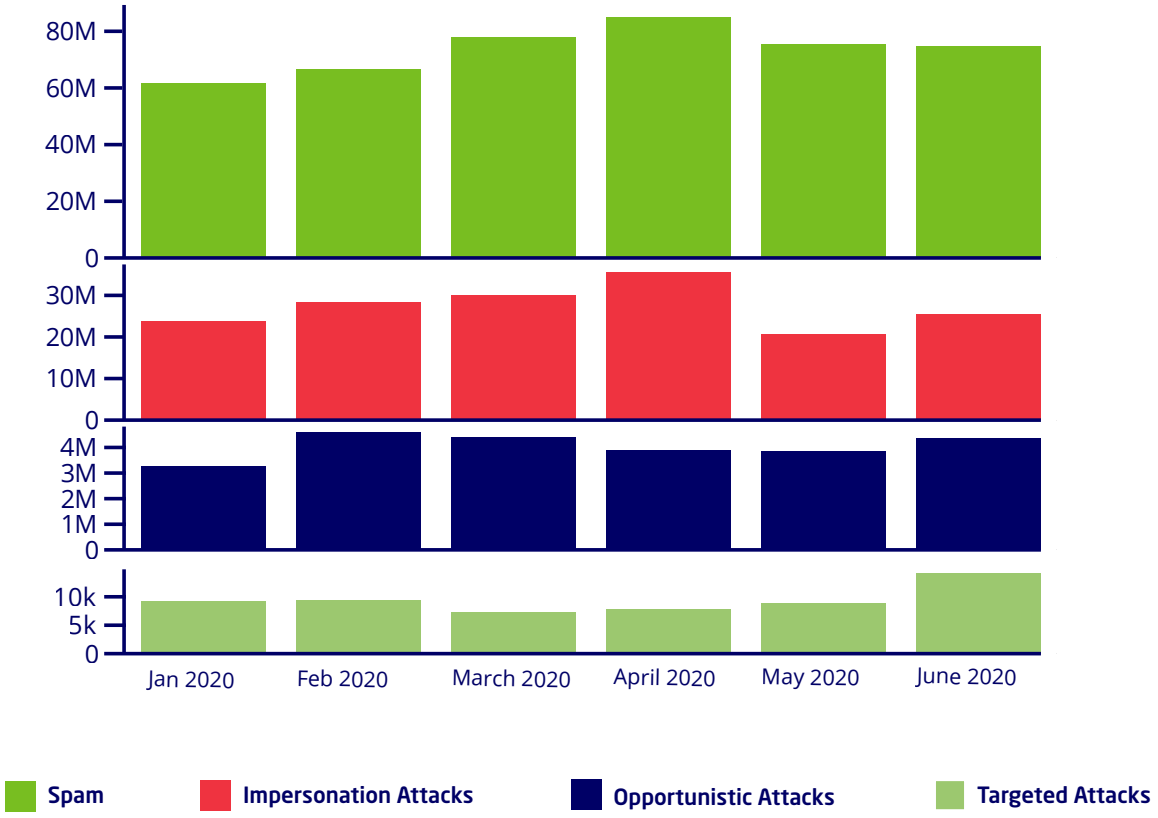
Mimecast consistently tracks threat detections in the four primary threat categories across the globe: spam, impersonation attacks, opportunistic attacks, and targeted attacks.

Figure B illustrates the volume of threats blocked across these four primary categories, showing peak volume globally on February 11, with more than 7.1 million threats detected. In the US and Caribbean regionally, the peak occurred on April 21, with 3.9 million combined threats being detected.

Peak volumet Feb 11, threats detected:

7.1mil

Fig. B: Threats by Category



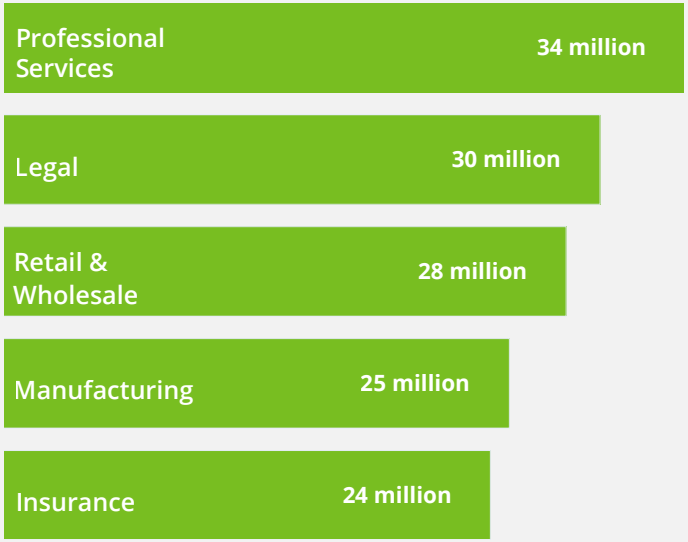
Spam Campaigns

In the spam attack category, researchers found bulk email campaigns were used to spread malware, targeting industries including Legal Services, Software and SaaS, Retail/Wholesale and Manufacturing, as shown in Figure C. These are, in the case of Legal Services and SaaS, the same verticals as targeted in the previous quarters, because they are key to criminal groups' monetary objectives. The data also reflects threat actors' concentration on Retail/Wholesale and Manufacturing over recent months. The share of spam as a percentage of the overall figure has remained relatively comparable to the previous quarter, despite higher total combined threats overall, including a significantly higher volume of detections at the spam layer.

Campaign volume globally was at its highest during the week ending March 15, 2020, with more than 32.58 million threats blocked, a 36% percent increase over the 24 million threats blocked on the day of peak activity in the last quarter of 2019. In the U.S. and Caribbean region, the week ending April 19 saw peak threat volume, with 16.77 million threats detected on that day alone.

The increased spam activity starting in March coincided with the pandemic and stay-at-home orders in the U.S., ***almost certainly*** reflecting an acceleration in basic attack-related behavior due to the opportunity the pandemic presented to threat actors. Other significant campaigns have coincided with more targeted attacks against the range of business verticals identified within this report, and this vector denotes the most common, en-masse form of attack still taking place. This cheap, unsophisticated, high volume attack vector remains the predominant method to spread malware.

Fig. C: Top Verticals - Spam



Week ending March 15, threats blocked:

32.58mil

Increase of

36%

Impersonation Attacks

Social engineering - most commonly done through impersonation tactics – gained steam so far in 2020. Attackers impersonate domains, subdomains, landing pages, websites, mobile apps, and social media profiles, many times in combination, to trick the target organization and/or its employees into surrendering credentials and other personal information, initiating fraudulent wire transfers, or installing malware. Threat actors tend to rely on social engineering instead of tactics more easily detectable through traditional email such as the direct embedding of malware.

Ransomware was very active in 2019; it is ***highly likely*** that threat actors continued their efforts in 2020 towards ransomware delivery through enhanced opportunistic targeting of multiple verticals in high volumes.

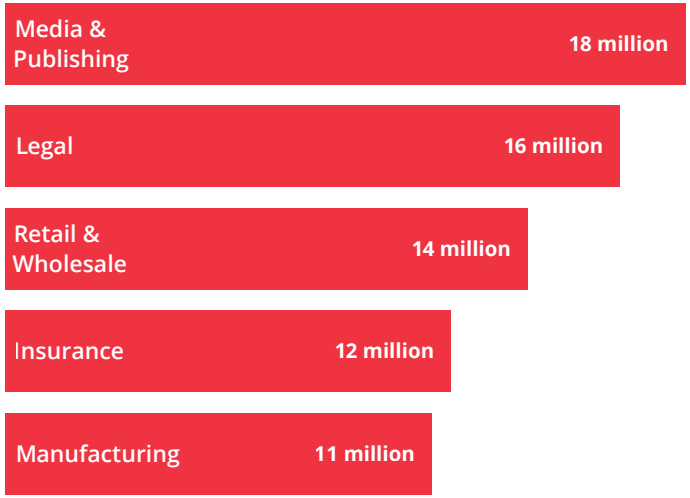
There were some significant changes to the verticals targeted by impersonation, ***almost certainly*** driven by pandemic-related circumstance in addition to the heavily social and interpersonal nature of these industries:

Media and Publishing suffered 48.4 million detections, or 13% percent, of the overall volume as shown in Figure D. In the previous year, the Management and Consulting sector had been the primary target of impersonation attacks. The shift towards targeting Media and Publishing is both notable and unusual; it's likely indicative of the prevalence of disinformation, and attempts to gain access to information during a period of uncertainty, fear, and chaos.

The Legal Industry remained a top impersonation target, accounting for 10% of detections, having been 11% of the attack volume in the last quarter of 2019.

Manufacturing supplanted Banking during this period, suffering 26.8 million attacks, or 7% percent of the volume. This is ***almost certainly*** due to the continued operation of many manufacturing capabilities in response to the pandemic, and the key role they play in any recovery.

Fig. D: Top Verticals - Impersonation Attacks



Media and publishing was the primary target of impersonation attacks. Detections blocked:

48.4mil

The evolution of impersonation into voicemail phishing messages has grown; it is ***almost certain*** this form of attack will be used continuously and will evolve again in the coming year. Impersonation attacks made up 24% percent of total detections from January-June. The actual volume of these attacks grew by 37% percent in that same time period.

As show in Figure D2, the **business email compromise** (BEC)/impersonation figures for the period of the last four reports was 54 million between April and June 2019, 63 million between July to September 2019 (an increase of 18%), and 60 million between October and December 2019 (a reduction of 5%), remaining above the April-June 2019 figure. Between January and March 2020 that increased to 82 million and between April and June 2020 dropped slightly from that peak to 81.7 million.

Fig. D2: Blocked Impersonation Attacks

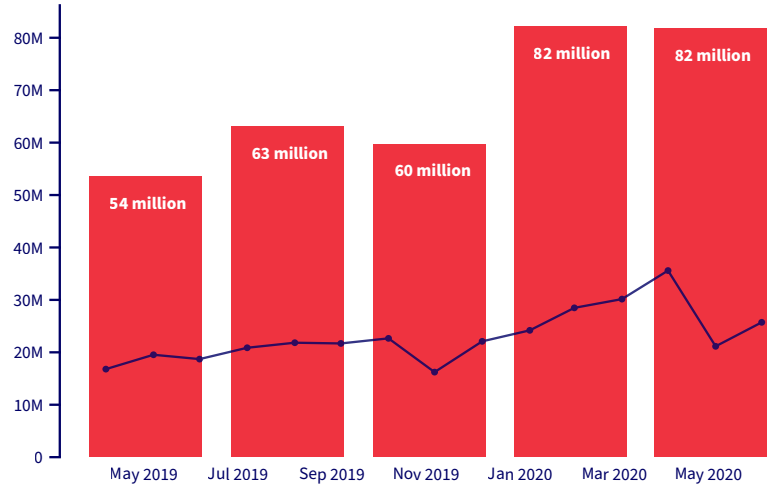
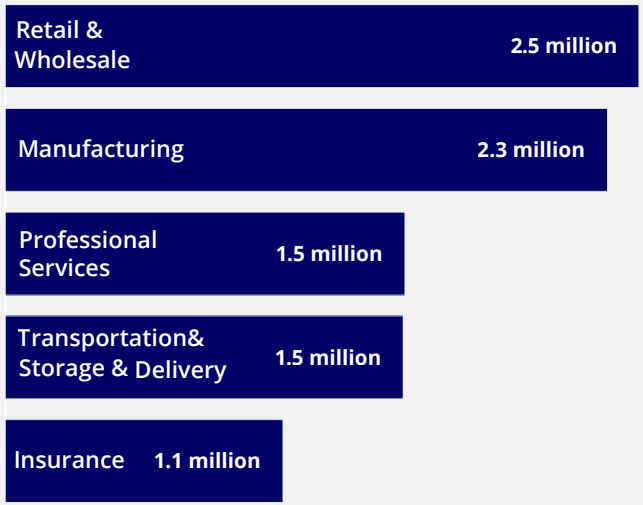


Fig. E: Top Verticals - Opportunistic Attacks



Opportunistic Attacks

Opportunistic attacks are a continuing fixture in the security industry since they are relatively low effort for attackers, and they use well-known malware. Figure E shows the Retail/Wholesale and Manufacturing verticals experiencing the highest volume of these threats, with 10% and 9% of threats hitting each of them respectively.

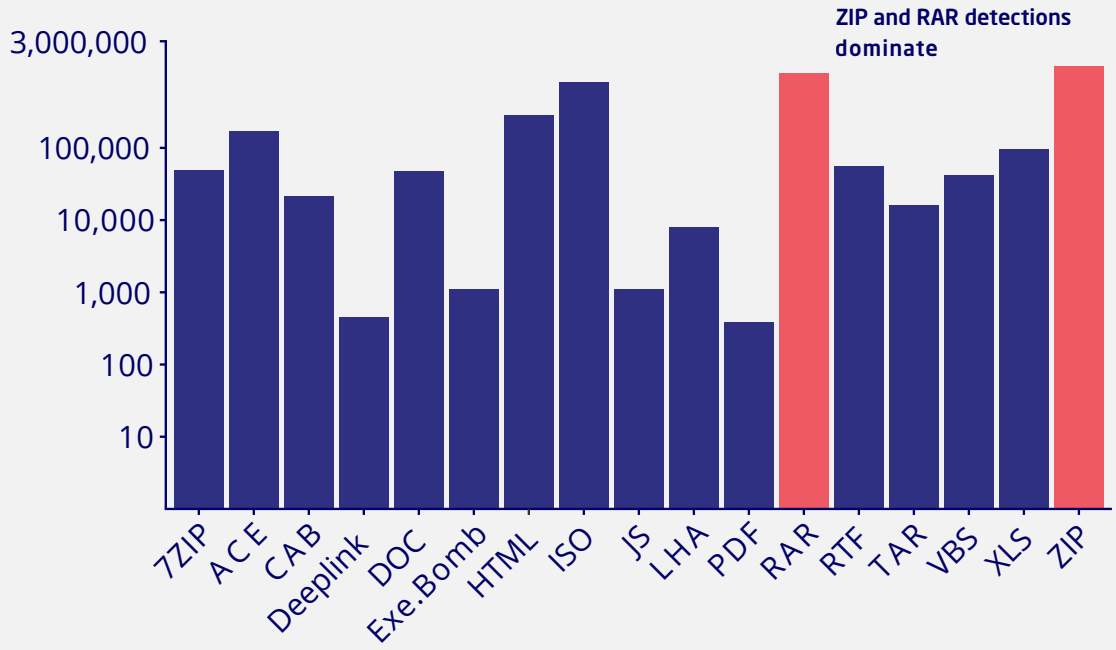
This shift in targeting has displaced the Transportation, Storage and Delivery sector, which has repeatedly been subject to the highest volumes of opportunistic attack. Several significant and targeted attacks (explored in Appendix) have also sought to compromise these verticals more determinedly, which is a new development and can ***almost certainly*** be attributed to various advanced persistent threat (APT) actors, including state-sponsored APTs, to take advantage of increases to ecommerce and the vulnerability of retail and manufacturing during the pandemic.

Targeted Attacks

Throughout the quarter, Mimecast uncovered 42 significant campaigns threat actors carried out which demonstrate their capability to conduct sophisticated, varying campaigns spanning several days of activity, leveraging a variety of attack methods. For example, this includes the use of bulk and attachment-based malware, fileless malware, URLs, exploits and a variety of complex malware which includes significant obfuscation.

Mimecast Signature Detections

Beyond these four categories of attack, file compression continues to be an attack format of choice, because compressed files allow for a more complex and potentially multi-malware payload, but also serve as a basic means of hiding the true file content held within the container. The **ZIP** and **RAR** formats of file compression dominated detections – approximately three million throughout the period – and they are the most commonly detected formats for attack. Continued use of any available form of file compression format remains the most attractive to threat actors unless merely exploiting human error at a large scale.



Attack Campaign Overview: USA

Each quarter, threat detections in the United States tend to be higher and more concentrated due to the sheer volume of businesses headquartered in the U.S. In fact, similar to the previous research period (October-December 2019) the U.S. suffered both the highest number of campaigns and the highest levels of detection volume against nearly every sector of its economy.

Emotet was apparent and central to almost all campaigns until it ceased activity in early February, and compressed file formats remained a common attack vector, behaving as a complement to **Emotet**, before becoming the key component of many of the subsequent hybridized campaigns.

The Manufacturing and Retail/Wholesale verticals were repeatedly attacked during this period due to their key importance in responding to the pandemic. This was a shift from the usual opportunistic and vertical targeting activity from March onwards, which has begun to return to normal patterns as economic activity and industry began to resume.

The key malware detected in the first half of the year included **Azorult**, **Barys**, **Cryxos**, **Emotet**, Hawkeye, **Lokibot**, **Nanocore**, **Nemucod**, **Netwired**, **Remcos**,**Trickbot**, **Zloader** and **Strictor** ransomware, while almost every campaign utilized a mixture of generic Trojans and phishing with more significant threats. These represent diverse range of threats against networks in the region with the capability to implement Dropbox, compromise USB devices, Windows and MAC devices and the potential to insert ransomware. It is ***almost certain*** that the current heightened campaign activity remains driven by the intent to deliver ransomware, as in other regions.

CVE-2017-11882, also known as Microsoft Office Memory Corruption Vulnerability, was more heavily attacked in volume than has been previously seen, sometimes hundreds or thousands of times in a single day across all verticals. Because this vulnerability has been so heavily attacked since its discovery years ago, it's even more imperative that organizations implement the patch and avoid risk of exploit.

Although the campaigns detailed in the Appendix are the most significant during this period, research found that peaking activity against all verticals of the U.S. and Caribbean regional economy occurred on specific days of heightened threat activity, many campaigns opportunistically targeting a widespread range of verticals for compromise. In addition, in May and June 2020, cybercriminals increased the level of general daily threat activity against many verticals to significantly higher volumes of general opportunistic attacks.

The Manufacturing and Retail/Wholesale verticals were repeatedly attacked during this period due to their key importance in responding to the pandemic.

The majority of attacks in the U.S. are concentrated, single-day campaigns. Targeted volume campaign activity in the U.S. increased during this period to the extent that 42 significant, standout campaigns were identified for this report, with many now impacting a wider range of multiple verticals on the same day, or over a more prolonged period of several days.

It is ***highly likely*** that the majority of the campaigns in the U.S. and Caribbean region were carried out by organized criminal groups for monetary gain, as well as to spread disinformation during a time of chaos in the United States.

Given the similarity of detections across verticals on various days and the persistent use of significantly hybridized threats across multiple verticals on specific days, it is ***highly likely*** that many of the campaigns are related or coordinated, although it cannot be established that the threat actors are the same, as each campaign differs in profile. However, it is ***unlikely*** that a single group undertook the majority of this activity due to the level of resources this would require, ***almost certainly*** requiring state organization. In any case, each of the groups should be considered as well-resourced and capable, if not state-sponsored or affiliated.

To gain insight into the technical attack detail, visit the Appendix of this report.

It is highly likely that the majority of the campaigns in the U.S. and Caribbean region were carried out by organized criminal groups for monetary gain, as well as to spread disinformation during a time of chaos in the United States.

Recommendations: What Can You Do?

Attackers are able to adapt to circumstances and defeat detection methods by exploiting human error, or seeking to take users away from their corporate IT security solutions.

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

The Mimecast Threat Center recommends:

01

Emphasize the importance of security controls and resilience.

As significant opportunistic, hybridized campaign activity has grown, targeting a wide range of verticals at any one time, and the growing threat of ransomware delivery, now is the time for organizations to seriously consider their ability to recover from a successful attack when it happens to them and consider in detail how the organization might continue business as usual – or as much as is possible when a pandemic has upended the U.S. economy. Only fallback capabilities in relation to cloud and web-based email and data archiving can provide necessary business continuity. Organizations may find it more problematic to recover from a ransomware attack or compromise given the constraints of pandemic-related lockdowns, the stress to the overall economy, and the likelihood of more of these challenges to follow.

02 Increase security awareness training.

Keep users informed on current, prevalent threats; this should be a priority to avoid the risk posed by simple human error. This is even more critical now as lengthy stay-at-home orders or lockdown periods have shown a 55% increase to unsafe clicks. Mimecast's data during the first months of 2020 also shows that organizations that maintain frequent awareness training are five times less likely to see significant increases to unsafe behavior.

03 Enforce a strict password regime for users and admins.

Given the particular capabilities of **Emotet**, which seeks to brute force commonly used passwords on infection, avoid weak passwords. To prevent initial infection, users should never routinely enable macros within any electronic documents received. Related to this, organizations should use multi-factor authentication, and review their administrative passwords to ensure they have modified any default administrative passwords in the same way. **Emotet** will almost certainly resume activity in the short to medium-term and organizations need to be prepared for this to increase the already significant levels of attack volume further

04 Keep third-party supplier details up-to-date and under constant review.

Threat actors will seek to take advantage of any weaknesses in the supply chain, including exploiting businesses that may have ceased trading as a result of the current economic landscape.

05 Take the opportunity to properly review and update remote-working practices as the world enters a second wave of the pandemic.

Reviews should aim to streamline and cement processes so that employees can maintain secure levels of remote working; related to this, employers must reiterate basic cyber hygiene principles to avoid the potential for users to be compromised while using insecure home networks.

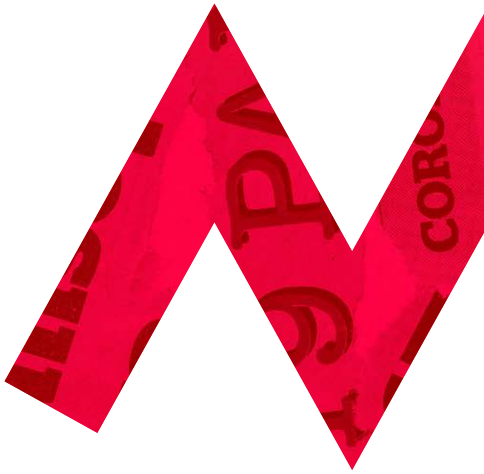
The Bottom Line

Mimecast's previous Threat Intelligence Report, released in February 2020, highlighted a blend of simple and sophisticated attacks, heavily dominated by **Emotet** driven campaigns against an increasingly diverse range of verticals. Many of the attacks detected and analyzed were brief and included an increasingly complex and hybridized threat as the means of attack.

These themes are again apparent in the period of this analysis: attackers used high volumes of commodity malware or simple social engineering techniques as a blanket strategy, incorporating an increasing array of attack vectors in sustained attempts to compromise their targets. At the same time, however, other cybercriminals invested effort into a targeted industry attack, leveraging unique malware and smart attack techniques. If that failed, the sheer volume of threats took advantage of the potential for human error in the face of the onslaught.

Threat actors continued the development of obfuscation and encryption techniques in efforts to avoid detection at the email gateway, as they use multiple layers of obfuscation to avoid detection at the endpoint. The use of multiple forms of malware in a layered attack gained steam and became commonplace for any determined attacker; reconnaissance efforts by threat actors are continuing, as they continue to try to evade detection. Simple social engineering techniques also evolved as attackers attempted to stay ahead of user awareness and take advantage of the increased potential for human error during the pandemic – a driving factor in the overwhelming majority of breaches.

Attackers used high volumes of commodity malware or simple social engineering techniques as a blanket strategy, incorporating an increasing array of attack vectors in sustained attempts to compromise their targets.



Glossary

Malware Observed

Across the Mimecast regions, researchers detected a complex range of malware, some of which has been around for many years and other more recent threats.

Many threats are increasingly automated, which is apparent within the daily detections data over periods of time as there is little change in detection numbers from one day to the next in relation to many of the specific file types used in particular attacks. The following identified threats are described in order of the identified frequency of their individual use within the significant attacks detailed over this quarter and included in Section 3 of this report:

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

Barys This malware implements Dropbox.

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

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

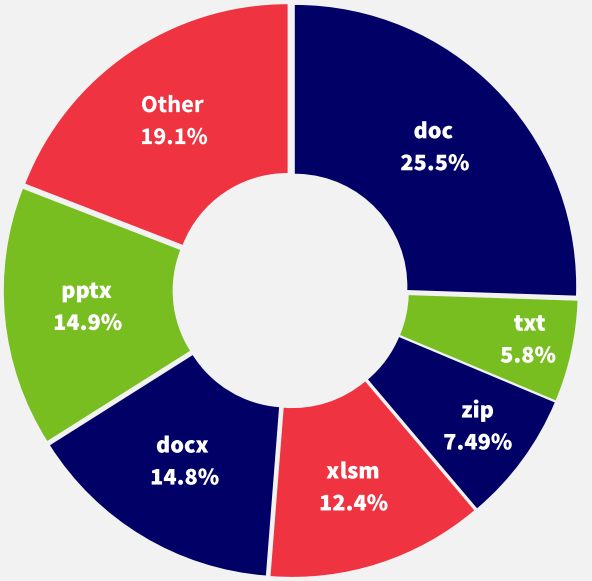
Nanocore or Nanobot is a remote access tool (RAT) used to take over control of Windows computers. **Nanocore** has been available since 2013 and is sold for legitimate purposes online. It has been re-purposed by criminals and primarily infects targets via a **ZIP** archived executable or MSOffice documents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

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

Strictor is an open source form of ransomware first noted in 2016 and originating from the “Hidden Tear” project.

1.7 File Types

Figure K identifies the file types detected as threats throughout this period by Mimecast's Attachment Protect. This data varies from detection data at the other layers between January to June 2020. All of the detected threats within this dataset are categorized by the method of file type delivery utilized to deliver their malicious payload. The dominating file type used has varied considerably within the 6 month period and it is apparent that Excel documents in XLSM, XLS, XLSX and XLSB file types have been subject to significant increased use by threat actors during the period analyzed. This activity was apparent as an increased and more significant component than previously seen, present in some campaigns after February. File compression through the **ZIP** remains a key format utilized in high volume in attempts by threat actors to gain a foothold in networks through sheer volume and the potential for human error. Additional measures which remain in use which are widespread and commonly employed are basic obfuscation via file compression, file renaming, double extensions and the increasing use of encryption and complex obfuscation. MSOffice documents remain the primary attack vector, whether hidden in archived containers such as **ZIP** and **RAR** files or attached as is. This is as a result of the numerous exploitable vulnerabilities present within its various iterations, as our campaign analysis shows repeatedly, and particularly those versions which are older and no longer supported, which now includes Windows 2007. .ACE files remain in use across all regions as does the continued volume use of ISO/image files in campaigns. These threats are also detected and blocked by Mimecast before they reach Attachment Protect.



Appendix

1. January 13, 2020

The Government verticals, both Public administration and the state local government sector, experienced a two-day campaign ending on January 14. The first day saw over 4,000 **Emotet** detections in an obfuscated DOC format, followed by a further 3,000 similar variant detections of **Emotet** the following day.

The Construction sector experienced a significant volume of **Emotet** detections in DOC format, comprising over 6,000 detections. Interestingly, this campaign utilized a mixture of obfuscated **Emotet**, **Trickbot** (83 detections) and VBA-based malware variants including **Nemucod**. Hundreds of phishing emails complemented this core component and the trojans Graftor and **Nanocore** were contained in ISO/image files. Exploit **CVE-2017-11882** was attacked in volume.

On the same day, a campaign against the Finance: Banking sector experienced more than 3,000 detections of overwhelmingly **Emotet**, obfuscated and in DOC format. This was complemented by other generic obfuscated VB droppers, phishing emails, **ZIP**, **RAR**, ISO/image files and XLS files containing **Lokibot** the Ursu trojan were also detected. The **Emotet** detections heavily utilized the text INV or Invoice in the subject field.

2. January 13-17, 2020

A campaign against the Retail/Wholesale sector also took place over five days, ending on January 17. The campaign commenced on 13 January with detections of over 2,500 obfuscated variants of **Emotet** in DOC format. This was complemented by the use of phishing emails, and VBS, **ZIP**, **RAR**, ACE, RTF and ISO/image files containing Agensla, Andromeda, Graftor, Kryptik, **Nemucod**, Noon, Razy, **Remcos,** Valyria, and Wacatac malware. The subject fields notably featured the words INVOICES, waybill and newest payment. The exploits CVE-2012-0158 and **CVE-2017-11882** were also subject to repeated attack.

On January 14 the campaign continued with a similar core obfuscated **Emotet** component of over 2,000 detections. In addition to the threats detected on day one of the campaign, AgentTesla, AveMaria, Dothetuk, Fareit, Kpavtoit, **Lokibot**, **Netwired**, **Nanocore** and Ponystealer were also detected.

This pattern of attack activity against this sector continued with the same proportional threat profile apparent for the following 3 days, gradually reducing by 1,000 to 2,000 detections per day until the campaign ceased on January 17.

3. January 20-22, 2020

A further significant volume obfuscated **Emotet** driven campaign took place over a three-day period against an increasingly widening range of verticals, primarily impacting:

a. The Construction sector was attacked from the January 20, commencing on this day with a core component of over 300 obfuscated **Emotet** variants, complemented by other VB droppers, ACE, **RAR** and **ZIP** files using **Azorult**, Fareit and Ponystealer malware. **Cryxos** was also detected in JS format. Exploit **CVE-2017-11882** was once again attacked in volume.

On January 21 the obfuscated **Emotet** core increased to over 2,500 detections, continuing to be complemented by the malware and phishing activity detected in the previous day.

On January 22 the obfuscated **Emotet** core again increasing, this time to over 5,500 detections. Again, complemented by similar but increased activity to the previous days.

a. The Finance: Insurance sector experienced the same campaign activity as the Construction sector over the same dates. The core obfuscated **Emotet** component against this sector comprising over 300, 1,500 and 3,000 detections on consecutive days.

b. Finance: Banking experienced the same campaign as the other verticals, incurring lower volume detections of over 200, 1,000 and 1,400 obfuscated **Emotet** detections.

c. Attacks also took place against Mining and Extraction, appearing identical in nature and make up in term of threats to the other attacks over January 20 - 22. The core obfuscated **Emotet** component against this sector comprised over 500, 1,300 and 2,200 detections on consecutive days.

d. The Professional Services: Legal sector also experienced the same campaign activity, with an increased proportion of ISO/image file format detections than the other verticals had experienced. The obfuscated **Emotet** component comprised over 250, 1,400 and 2,500 detections on consecutive days.

e. Lastly, over the same period, the Retail/Wholesale sector was also attacked, experiencing the same campaign activity as each of the other verticals identified. This vertical experienced the highest attack volume of all the verticals attacked and across all of the same formats and threats previously identified over these dates, including obfuscated **Emotet** components of over 700, 3,800 and 7,500 detections.

4. January 22, 2020

An additional attack also occurred against the Higher Education sector, which experienced a separate campaign appearing very different to the other attacks identified over the same dates. It utilized over 1,900 generic trojans

supported by small numbers of **ZIP**, **RAR** and ISO/image files, and a small component of over 150 obfuscated **Emotet** detections was also made.

5. January 27, 2020

A further **Emotet** campaign impacted a wider range of verticals utilizing a different variant:

a. A campaign took place against the Construction sector, utilizing over 4,500 detections of an obfuscated **Emotet** component in DOCX format. This was complemented by volume phishing emails and documents, ACE, ISO/image, **RAR** and **ZIP** format detections. These included detections of Noon malware. CVE-2017-0199 and **CVE-2017-11882** were also attacked in volume.

b. The same activity was seen against the Finance: Banking sector, with over 1,200 detections of the same obfuscated **Emotet** variant and the same supporting activity as seen against the Construction sector that same day, including phishing emails and volume attack against **CVE-2017-11882**.

c. The same campaign affected the Finance: Insurance sector, with over 2,000 detections of the same obfuscated **Emotet** variant. A more significant phishing component was seen against this particular sector, of over 2,000 detections, otherwise the activity was the same as that seen against the other verticals, again including volume attack against **CVE-2017-11882**.

d. The same campaign also affected the Government sector, both the administrative, and state and local verticals, comprising almost exclusively over 1,800 and 700 of the same obfuscated **Emotet** variant in DOCX format.

e. The campaign also affected the Health and Social Care: Hospitals and Clinics sector, with the core obfuscated **Emotet** variant component detected over 1,800 times.

f. The campaign also impacted the IT sector, including software and SaaS, which also experienced the same campaign, with over 1,900 detections of the same **Emotet** variant.

g. The campaign also impacted the Manufacturing: Electronics sector, with over 1,200 detections of the same **Emotet** variant.

h. Mining and Extraction was also impacted, also experiencing over 1,200 detections of the same **Emotet** variant, and the same overall detection activity as the other verticals.

i. Media and Publishing was also impacted, but with less **Emotet**, of over 500 detections, but with significantly increased ACE, ISO/image, **ZIP** and **RAR** format components. The Parazit trojan was also detected in ISO format. **CVE-2017-11882** alone was attacked over 500 times.

j. The Professional services sector as a whole was also impacted across all of its verticals, with over 5,500 detections of the same **Emotet** variant across the sector.

k. The campaign also impacted the Real Estate sector, with over 1,500 detections of the same **Emotet** variant.

l. The Retail and Wholesale sector was the most heavily impacted, with over 8,500 detections of the same obfuscated **Emotet** variant. There was also significantly higher detection activity of all the other components as previously detailed against the construction sector on the same date and the addition of VBS format detections. **Barys** and Zmutzy malware were also detected, as was **Strictor** ransomware, in addition to the previously noted threats.

6. January 31, 2020

A wide range of verticals were impacted by a significant **Emotet** campaign utilizing a further variant to the previous campaigns. This campaign utilized **Emotet** almost exclusively alone:

a. In the Construction sector an attack utilized almost exclusively in excess of 6,000 detections of an obfuscated **Emotet** variant in DOCX format.

b. In the Finance: Banking sector the same campaign again utilized almost exclusively over 1,600 of the same **Emotet** variant in DOCX format.

c. Finance: Insurance also suffered the same campaign, again utilized almost exclusively over 3,000 of the same **Emotet** variant in DOCX format.

d. Health and Social Care: Hospitals and Clinics sector also suffered the same campaign, attacked almost exclusively by over 2,000 of the same **Emotet** variant in DOCX format.

e. The Manufacturing sector was hit widely, with over 6,000 detections of the same **Emotet** variant as the other verticals.

f. The Mining and Extraction sector experienced over 1,400 detections of the same **Emotet** variant.

g. The Professional services sector was also impacted with over 8,000 detections of the same **Emotet** variant across the entire sector.

h. Retail and Wholesale was also again attacked, with over 6,000 detections of the same **Emotet** variant utilized against the sector.

7. February 4, 2020

A further **Emotet** campaign, using a DOC based variant, again impacted a wide range of verticals:

a. The Construction sector experienced another campaign. This utilized over 5,000 obfuscated **Emotet** detections in multiple variants. This was complemented by volume phishing, ACE, DOC, ISO/Image, JS, **RAR**, RTF, VB and **ZIP** detections. Andromeda, **Cryxos**, Noon, Vebzenpak and Zmutzy malware was detected. The exploits CVE-2017-8570 and **CVE-2017-11882** were also attacked repeatedly.

b. The Finance: Insurance sector experienced over 3,000 detections of **Emotet**. The supporting campaign detections once again closely mirrored those seen in the activity against the construction sector on that same day, but with a significantly increased component of ISO/image-based files.

c. A further attack took place against the Manufacturing sector which was impacted by over 9,000 obfuscated **Emotet** detections across the sector. The supporting activity mirrored that seen in the activity against the construction sector on that same day.

d. A further Professional Services sector campaign featured over 9,300 obfuscated **Emotet** related detections across the sector. The supporting campaign detections again also mirrored that seen in the activity against the construction sector on that same day, but in greater volume, with the additional detection of Hawkeye, Jaik, Kpavtoit, Kryptik, **Nanocore**, Noon and Vebzenpak malware, and **Strictor** ransomware.

e. Real Estate suffered over 2,400 **Emotet** detections. The supporting campaign detections again mirrored that seen in the activity against the construction sector on that same day, with the addition of Boxter and Lazarus malware detections.

f. Retail and Wholesale over 6,000 **Emotet** detections. The supporting campaign detections again mirrored that seen in the activity against the construction sector on that same day, with the addition of Agensla malware and **Strictor** ransomware detections. A prominent courier brand also featured in detections.

g. Transport, storage and Delivery over 3,000 **Emotet** detections. The supporting campaign detections again mirrored that seen in the activity against the construction sector on that same day, with additional detections of **Nanocore** and Noon malware.

8. February 6, 2020

The last identified, major wide-ranging **Emotet** campaign took place for the period under review:

a. In the Construction sector, Mimecast researchers discovered a volume VB-based campaign, comprising over 6,000 obfuscated **Emotet** detections. JS, **RAR**, ISO/image and **ZIP** formats supported the campaign in low volume. **Cryxos** and Jacard malware were also detected. **CVE-2017-11882** remained under significant attack.

b. The Finance: Insurance sector experienced over 4,000 detections of **Emotet**. The supporting campaign detections once again closely mirrored those seen in the activity against the construction sector on that same day, but with a significantly increased component of ISO/image-based files.

c. A further attack took place against the Manufacturing sector, which was impacted by over 8,000 **Emotet** detections across the sector. The supporting campaign detections once again mirrored those seen in the

activity against the construction sector on that same day but in greater volume, with the additional detection of Agensla, Burkina, Hawkeye, Noon, Vebzenpak and Ursu malware.

d. The Professional Services sector suffered a widespread attack of over 10,000 **Emotet** detections across the sector. The supporting campaign detections once again mirrored those seen in the activity against the construction sector on that same day, with **CVE-2017-11882** attacked over 2,000 times alone.

e. Real Estate over 2,000 **Emotet** detections with complementing activity as the construction sector on this same day, but with the addition of Jacard and Lazarus malware.

f. Retail and Wholesale over 6,000 **Emotet** detections. The supporting campaign detections again mirrored that seen in the activity against the construction sector on that same day, with additional detections of Agensla and Predator malware.

g. Lastly, Transportation, Storage and Delivery suffered over 3,800 **Emotet** detections. The supporting campaign detections once again mirrored those seen in the activity against the construction sector on that same day, with the additional detection of Zmutzy malware.

9. February 11, 2020

a. A further campaign against the Manufacturing Sector again, with over 15,000 detections. This utilized volume phishing emails and malware contained in thousands of ACE, CAB, DOC, ISO/Image, JS, **RAR**, RTF, VBA, **ZIP** and 7ZIP formats. Agensla, Babar, Boxter, Crypt, **Cryxos**, Hawkeye, Mydoom, Noon, Nymeria, Ponystealer, and Vebzenpak malware were detected. **Strictor** ransomware was also detected. A well-known courier brand featured in the malware campaign. The exploit **CVE-2017-11882** was attacked hundreds of times.

b. The same campaign also further impacted against the Professional Services sector with over 7,000 detections. With the same threats profiled and utilized in volume phishing emails, and malware contained in thousands of ACE, CAB, DOC, ISO/Image, JS, **RAR**, RTF, VBA, XML, **ZIP** and 7ZIP formats. Agensla, Andromeda, Boxter, **Cryxos**, Kryptik, **Lokibot**, Noon, Nymeria, Ponystealer, and Zmutzy malware were detected. A well-known courier brand was noted in the malware campaign. The vulnerability **CVE-2017-11882** was also attacked hundreds of times against this sector.

c. The same campaign, structured the same way, also took place against the Retail and Wholesale sector with other 11,000 mixed detections. As with other verticals attacked on the same day, it was structured with the same formats containing threats, and supported by a high volume of phishing emails. Agensla, Boxter, **Cryxos**, Noon, Oroles, Ponystealer, **Remcos,** Ulise, VBCryptor, Vebzenpak, Zbot and Zmutzy malware were detected. **Strictor** ransomware was also detected. A well-known courier brand featured in the malware campaign. The words order and scan appeared prominent in subject titles. As with the other verticals targeted, the vulnerability **CVE-2017-11882** was also attacked hundreds of times.

d. The Transport, Storage and Delivery sector was also hit by this same campaign. This utilized the same mixed structure the other verticals were attacked and over 9,000 detections were made. The phishing component against this sector was larger than that experienced by other verticals on the same day, numbering over 3,000. Agensla, Andromeda, **Cryxos**, Fareit, **Nanocore**, Nymeria, VBCryptor and Zmutzy malware were detected. A well-known courier brand featured in the malware campaign. The exploit **CVE-2017-11882** was again attacked hundreds of times.

10. February 17, 2020

a. A campaign against the Manufacturing sector took place with over 32,000 mixed format detections. This campaign was structured as the campaign the sector had experienced on February 11, but was proportionally more significant, with a far larger volume of over 10,000 phishing emails deployed against the sector on this day.

b. Professional Services was also again subject to the same campaign, suffering over 19,000 mixed format detections. This was also structured strikingly similar to the one the sector had experienced on February 11, but was also proportionally more significant, with a larger overall

volume of threats and over 1,500 phishing emails deployed against the sector. Teslacrypt ransomware was also detected.

c. The campaign, again, also took place against the Retail and Wholesale sector, which experienced over 14,000 mixed detections. This campaign was also structured as the one the sector experienced on February 11, but was also more significant, with over 2,000 phishing emails deployed against the sector. **Lokibot** and Pantera malware were also detected in addition to the previously noted threats.

d. The Transport, Supply, and Delivery sector also experienced the same campaign, but to a lesser extent than the other verticals noted, with over 6,000 threats detected. This sector, contrary to the others however, saw significantly less activity than that seen against it on February 11, but still experiencing over 2,000 phishing emails.

Threat actor activity significantly altered in March, with some significant volume campaigns utilizing masses of the same types of malware, in the case of **Cryxos** this included several variants of the same threat, on some dates up-to six variants of this malware was being detected. The complex, heavily mixed format of threats also continued to be deployed in other campaigns. **Cryxos** was heavily used opportunistically against multiple verticals throughout March.

11. March 3, 2020

The Finance: Insurance sector saw a campaign of over 13,000 detections, utilizing a mass of over 11,000 threats in HTML format and over 400 XLS documents.

12. March 3 - 4, 2020

Three particular verticals were impacted by a mixed campaign that was seen to impact across each of these verticals. Threat activity proportionally altered significantly on the second day of this campaign, but was the same across all of these verticals and all of these same verticals were impacted by this activity on each day:

a. Construction. This sector was hit by over 2,000 detections on March 3, increasing to over 2,400 the next day. This campaign utilized volume phishing emails and malware contained in ACE, CAB, DOC, HTML, ISO/Image, JS, **RAR**, RTF, VBS, over 400 XLS, **ZIP** and 7ZIP formats. Agensla, **Cryxos**, Noon, Ponystealer, and Vebzenpak malware were detected. The vulnerability **CVE-2017-11882** was attacked again, but not as significantly as in previous campaigns.

b. The Manufacturing sector was impacted by over 7,000 detections on 3 March, and over 9,000 detections on the following day. Phishing emails and ACE, CAB, DOC, HTML, ISO/Image, JS, **RAR**, RTF, VBS, XLS, **ZIP** and 7ZIP formats containing malware. Bsymem, **Cryxos**, Krypt, Nanobot, Noon, Pantera, Perseus, Ursu, Vebzenpak and Zmutzy malware was detected. **Strictor** ransomware was also detected. **CVE-2017-11882** was attacked over 200 times.

March 4 saw in increase to the ISO and XLS format components, and the addition of obfuscated VBA downloaders and TAR format threats. Andromeda, and over 500 detections of two variants of **Cryxos** malware were detected. The subject lines included the term Order prominently and a well-known courier brand featured.
CVE-2017-11882 was attacked over 600 times.

c. The Retail/Wholesale sector was also impacted by over 6,000 detections on the first day and then over 8,000 on 4 March. This campaign utilized over 900 phishing emails and malware contained in ACE, DOC, 700+ ISO/Image, JS, 900+ **RAR**, RTF, VBS, XLS and **ZIP** formats. The malware Agensla, Andromeda, Crypt, **Cryxos**, Fareit, **Nanocore**, Noon, Pantera, Perseus, Razy and Vebzenpak were detected. The vulnerabilty **CVE-2017-11882** was attacked again, over 300 times on this occasion.

On March 4 there was a similarly structured hybridized attack utilizing the same threats but in an increased volume, and including over 400 XLS detections again. A more significant component volume of generic trojans and the addition of a volume obfuscated VBA downloader format were detected. ACE, CAB, TAR and 7ZIP format usage was also added at volume, or increased. Bsyemen, Graftor and Ursu malware were also detected. The vulnerability **CVE-2017-11882** was again attacked over 300 times.

13. March 6, 2020

The Professional Services: Legal sector experienced a campaign of over 2,800 detections, including over 1,900 detections of **Cryxos** malware in multiple variants, supported by a smaller number of generic trojans, phishing emails and malicious ISO/Image files.

14. March 16 - 17, 2020

Retail/Wholesale was again impacted by a campaign of over 6,000 detections on each day. These were again heavily mixed/hybridized detections. Activity was virtually identical on each day, with the only difference being a variation in the volume of generic trojan use on the March 17. Threats in ACE, HTML, ISO/image, JS, **RAR**, RTF, Obfuscated VBA downloader, VBS, XLS, **ZIP** and 7ZIP formats were detected, including Agensla, Chartres, **Cryxos**, Eldorado, Hawkeye, Kryptik, Mydoom, **Nanocore**, Noon and Valyria malware. Scan featured in the subject line and **CVE-2017-11882** continued to be attacked.

15. March 17, 2020

The Professional Services: Legal sector again experienced a campaign, this time of over 5,000 detections, including over 3,500 detections of malicious XLS files. Supported by a smaller number of generic trojans in ACE, DOC, HTML, ISO/image, **RAR**, VB, **ZIP**, and 7ZIP formats and phishing emails. Chartres malware was detected and **CVE-2017-11882** was attacked.

16. March 28, 2020

Manufacturing: Electronics was subjected to a campaign utilising exclusively a single variant of **Cryxos** malware in JS format. This was detected in over 5,000 instances. This same **Cryxos** variant was also seen impacting every vertical across the US region, but in significantly smaller numbers, on the same day.

17.March 31, 2020

The Professional Services: Accounting sector suffered almost exclusively over 30,000 detections of a single **Cryxos** variant, supported by a small number of over 100 malicious XLS file detections.

18. April 3-4, 2020 (2 Days)

A two-day campaign utilizing a large volume of over 17,000 VBS files as its core component was noted as taking place across the Construction, Professional services, Real Estate, and Transport, Storage and Delivery verticals. It also impacted the Finance: Insurance, and Manufacturing: Food and Beverage verticals, but not to a significant level of detections. The attack volume petered out considerably in day two, more than halving against all of these verticals, and then ceased. This was supported by ACE, DOC, HTML, ISO/image, JS, **RAR** and **ZIP** format threats. **Cryxos**, Mydoom and Zmutzy malware where detected and **CVE-2017-11882** continued to be attacked across these verticals.

19. April 6, 2020

Retail/Wholesale experienced a significant campaign, with over 7,000 mixed detections, including over 2,000 detections of Boxter malware. **Cryxos**, Valyria

20. April 8-9, 2020 (2 Days)

A phishing campaign of over 20,000 detections impacted every vertical of the US region over these two days. This was accompanied across every vertical by a **Cryxos** variant which was detected over 12,000 times.

21. April 19, 2020

The Finance: Insurance sector experienced a campaign using exclusively over 21,000 malicious JS format detections.

22. April 21, 2020

A wide-ranging hybridized campaign of mixed threat formats impacted every vertical in the region, but most significantly the following:

a. Construction over 6,000 detections

b. IT: Software and SaaS over 6,000 detections

c. Manufacturing sector over 45,000 detections, including over 3,000 **Cryxos**.

d. Professional Services: Legal over 12,000 detections including over 4,000 XLS format threats.

e. Retail and Wholesale with over 20,000 detections.

f. Transportation, Storage and Delivery over 6,000 detections.

Each of these attacks were similar in content, driven by thousands of Phishing emails, and ACE, HTML, ISO/image, **RAR**, RTF, VBA, VBS, XLS and **ZIP** format threats. Agensla, AgentTesla, three **Cryxos** variants, Krytpik, Morpheus, Ponystealer, **Remcos,** and Ursu malware were detected. **Strictor** ransomware was also detected.

CVE-2017-11882 was attacked over 11,000 times across these verticals. A well-known courier brand featured, as did the word scan in the subject line.

23. April 30, 2020

Another wide-ranging hybridized campaign of mixed threats again impacted every vertical in the region, but the most significantly impacted on this occasion were again:

a. Manufacturing, with over 15,000 detections.

b. Retail/Wholesale with over 10,000 detections.

Thousands of Phishing emails were supported by malware threats contained in ACE, DOC, HTML, ISO/image, JS, **RAR**, TAR, XLM and **ZIP** format. Abracadabra, two variants of **Cryxos**, Kryptik, **Lokibot**, Nanobot, Povertel and Vebzenpak malware were detected. **Strictor** ransomware was again detected. Scan again featured in the subject line. CVE-2017-0199 and **CVE-2017-11882** were attacked thousands of times.

In May threat activity altered again, this time to a generally high level of daily detections and general threat activity in relation to every vertical in the US region, and using a mixed threat throughout the month against a wide range of industries. This pattern of activity was sustained into June.

24. May 5, 2020

The Finance: Insurance sector experienced a campaign of over 7,000 detections. Phishing emails supported threats contained in DOC, HTML, ISO, PDF, **RAR**, VBA, VBS, XLS and **ZIP** formats. **Nemucod** and Pantera malware were detected and CVE-2016-7262 and **CVE-2017-11882** were attacked.

25. May 12 -15, 2020

The Retail/Wholesale sector was attacked by an XLS-borne **Zloader** campaign, comprising over 1,000, 600 and then 400 detections on successive days. Additional threats contained in phishing emails were supported by ACE, DOC, HTML, ISO, JS, **RAR**, RTF, XLS and **ZIP** format threats. Agensla, two variants of **Cryxos**, Fareit, Kryptik, Noon, Nymeria, Ponystealer, **Remcos,**, Vebzenpak and Zmutzy malware were also detected. CVE-2017-0199 and **CVE-2017-11882** were attacked and the words scan and order featured in subject lines.

26. May 12 - 13, 2020

The Finance: Banking sector experienced the **Zloader** campaign as Retail/ Wholesale, with over 500 **Zloader** detections. This was supported by a DOC, HTML and JS format component including over 400 **Cryxos** detections.

The following day Finance: Banking experienced over 4,000 detections, with more than 300 **ZLoader** detections complemented by over 2,000 HTML threats. Phishing emails also supported further threats contained in DOC, **RAR**, RTF, VB, XLS and **ZIP** format. Andromeda, Nanobot, **Nemucod**, Pantera and Sylkagent malware were detected. CVE-2010-3333, CVE-2014-1761, CVE-2016-7262 and **CVE-2017-11882** were also now attacked.

27. May 18, 2020

A campaign took place against the Real Estate sector, with over 5,000 detections. Over 3,000 phishing emails supplemented small numbers of HTML, ISO, JS, **RAR** and **ZIP** formats. **Cryxos** malware was again detected.

28. May 17 – 21, 2020

A further hybridized campaign against Retail/Wholesale took place over five days of over 4,000, 6,000, 6,000, 6,000 and 4,000 detections, respectively. Thousands of Phishing emails were supported by threats in ACE, DOC, HTML, ISO/image, **RAR**, RTF, VBA, VBS, XLS, **ZIP** and 7ZIP format. Agensla, AveMaria, Bsymem, three variants of **Cryxos**, Dothetuk, Graftor, Krytpik, **Lokibot**, **Nanocore**, Noon, **Remcos,** Ursu and Vebzenpak malware were all detected. **CVE-2017-11882** was attacked over 1,400 times in these five days. Scan and PO featured in subject lines and two prominent courier companies featured.

29. May 19 – 20, 2020

Manufacturing experienced over 10,000 and then over 18,000 detections, heavily comprised of DOC format threats, over 2,000 and then over 14,000 on the second day. ACE, ISO/image, **RAR** and **ZIP** formats threats were also present and included detections of Agensla, Krytpik, **Nanocore**, Noon, **Remcos,**, and Vebzenpak. **Strictor** ransomware was also detected again. **CVE-2017-11882** was attacked over 600 times in these two days. Scan again featured in subject lines.

30. May 26 – 27, 2020

The Finance: Banking sector experienced a campaign of over 10,000 detections, followed by over 6,000 the following day. VB droppers formed the core component of the attack. Other threats included DOC, HTML, VBA, XLS and **ZIP** formats containing **Nemucod** and Pantera malware. CVE-2016-7262 and **CVE-2017-11882** were also attacked.

31. May 26 – 28, 2020

Retail/Wholesale suffered a further campaign, this time over three days and including over 6,000, 7,000 and a further 7,000 detections over successive days. Each day included over 2,000 Phishing emails and ACE, HTML, ISO/image, JS, **RAR** and **ZIP** format threats. Agensla, Crypt, Crysan, two variants of **Cryxos**, Kryptik, **Nanocore**, Noon, Ponystealer, Razy, Ursu, Vebzenpak and Zmutzy malware were detected as was a bitcoinminer. **CVE-2017-11882** was attacked over 500 times in these three days. Scan and order featured prominently in subject lines.

32. June 1 – 5, 2020

A further campaign against Manufacturing took place over five days, with over 7,000, 6,000, 13,000, 12,000 and 14,000 detections respectively. Volume phishing emails were supported by ACE, DOC, HTML, ISO/image, JS, **RAR**, RTF and **ZIP** formats. These contained malware including Agensla, AgentTesla, **Barys**, Grenam, Kryptik, **Nanocore**, Noon, Razy, **Remcos,**, Stelega, Vebzenpak and Zmutzy. CVE-2017-1182 was attacked over 1,400 times. Variations to the threat occurred on June 3, with three variants of **Cryxos** detected over 3,000 times, and on June 5 **Cryxos** alone was detected over 11,000 times. Scan featured in subject lines.

At the same time, a similar hybridized and mixed threat was once again also impacting the Retail/Wholesale sector, with over 5,000, 4,000, 5,000, 5,000 and 3,000 detections on consecutive days. This appeared to be a **Zloader** campaign of over 400 detections. Phishing emails, ACE, DOC, HTML, ISO/image, JS, **RAR**, RTF, VBA, XLS, XLSM and **ZIP** format threats were detected. This included Agensla, **Azorult**, Dothetuk, Kryptik, **Nanocore**, Noon, Razy, TOA-3 and Zusy malware. Over 3,500 detections of **Cryxos** were made in the last two days.

Scan again featured in the subject line for many emails.

33. June 8, 2020

The Retail/Wholesale sector experienced a further **Zloader** campaign of over 11,000 detections, including over 700 of **Zloader**. Over 3,000 phishing emails and ACE, DOC, HTML, ISO/image, JS, **RAR**, RTF, XLSM and **ZIP** formats were all detected. Malware detections included Agensla, Andromeda, **Barys**, over 1,000 of two **Cryxos** variants, Krytpik, Razy, Ursu, Vebzenpak and Zusy. Scan again featured prominently in subject lines.

34. June 8 – 11, 2020

Manufacturing suffered a new four-day campaign, which included **Zloader** in the first day, and over 18,000, 11,000, 7,000 and 7,000 detections. Over 6,000 phishing emails were detected in the first two days, with additional threats then contained in DOC, HTML, ISO/image, JS, **RAR**, RTF, XLS and XLSM format. Agensla, Crysan, two variants of **Cryxos** numbering over 2,000 detections, **Nanocore**, Razy, Toa-3, Ursu, Vebzenpa and Zusy malware were detected.

CVE-2017-11882 was attacked and PO and scan featured in subject lines. A well-known courier company again featured.

35. June 8 – 10, 2020

Finance: Banking suffered a significant three-day **Zloader** campaign of over 6,000, 4,000 and 5,000 overall detections on consecutive days. Volume phishing emails and small numbers of DOC, HTML, JS, **RAR**, RTF, VBA and **ZIP** borne threats supplemented the over 2,000k, 1,000k and 2,000 **ZLoader** detections during the three days. Three variants of **Cryxos** were also detected and **CVE-2017-11882** was again attacked.

36. June 14 – 15, 2020

A huge two-day campaign impacted the Finance: Insurance sector, with over 162,000 generic trojan detections in the first day and 170,000 on day 2.

37. June 15 – 17, 2020

Manufacturing again suffered a multi-day hybridized campaign, of over 14,000, 10,000 and 6,000 detections. The core component on this occasion was **Cryxos**, with over 9,000, 5,000 and, 3,000 detections on consecutive days. This activity was supplemented by phishing emails, DOC, HTML, ISO/image JS, **RAR**, RTF and **ZIP** format threats. This included Andromeda, Agensla, Bitstealer, Chisburg, two variants of **Cryxos**, Graftor, Injuke, Kryptik, Perseus, Razy, Ursu, Zenpak and Zmutzy malware.**CVE-2017-11882** was again attacked, scan featured in subject lines and a well-known courier company again featured.

38.June 17, 2020

Finance: Insurance was impacted again by similar threat activity as that seen over June 14-15, with 27,000 generic trojans detected on this occasion.

39. June 21, 2020

Finance: Banking was subjected to a further campaign of over 10,000 detections. Including DOC, HTML, PDF, RTF, **ZIP**, and over 5,000 VB dropper and 1,000 XLS format threats. **Nemucod** and Pantera malware were detected and CVE-2016-7262, CVE-2017-0199 and CVE-2018-8414 were attacked on this occasion.

40. June 23, 2020

The Professional Services: Legal sector experienced over 5,000 detections, including over 2,400 phishing emails and DOC, HTML, ISO, **RAR**, VBA and **ZIP** format threats. Agensla, Bladabindi, two variants of **Cryxos**, Kryptik, Morpheus, Razy and Zmutzy malware were detected. The subject line again featured scan in the text, and a well-known courier company featured.

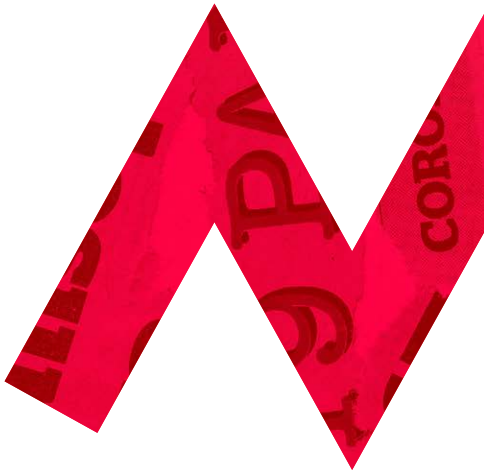
41. June 25, 2020

Manufacturing once again suffered a campaign, this time of over 8,000 detections. This included over 1,800 Phishing emails, ACE, DOC, HTML, ISO/image, JS, **RAR**, XLS and **ZIP** format threats. Agensla, **Cryxos**, Kryptik, Noon, Razy, Ursu and Zmutzy malware were detected. Scan again featured prominently in email subject lines and a well-known courier brand continued to feature.

Retail/Wholesale suffered the same campaign, of over 7,000 detections. For Retail this included over 3,000 Phishing emails, ACE, DOC, HTML, ISO/image, JS, **RAR**, VBA, XLS and **ZIP** Formats. Agensla, **Cryxos**, Eldorado, Morpheus, Noon, Razy, Zmutzy and Zusy malware were detected. **CVE-2017-11882** continued to be attacked and scan again featured prominently in email subject lines.

42. June 29-30, 2020

The final campaign of the report period, a two-day campaign against the Manufacturing vertical, numbered over 10,000 detections and over 8,000 the following day. Over 2,000 phishing emails were detected on each day, supported by ACE, DOC, JS, **RAR**, XLS and **ZIP** formats. Agensla, Andromeda, **Cryxos**, Eldorado, Fareit, Injexa, Noon, Razy, Ursu, Zenpak, Zmutzy and Zusy malware were also detected. **CVE-2017-11882** remained under sustained attack and scan again featured prominently in email subject lines.



mimecast™

Relentless protection. Resilient world.™

Visit the Mimecast Threat Intelligence Hub to learn more.

Learn more

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first and tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure.