
mimecast®
Threat Intelligence Report
Black Hat Edition 2019

Threat Intelligence Report
Black Hat Edition 2019

Introduction

The Mimecast Threat Intelligence Report: Black Hat Edition capitalizes on research conducted by the Mimecast Threat Center alongside Mimecast engineers with the objective of enhancing our email and web security services. The aim of this report is to provide the industry with technical analysis of some emerging threats Mimecast observed during the period, as well trends observed within the evolving threat landscape. The Threat Center also uses these insights to assess future potential threats and how the landscape may change over time. This analysis enables our customers to make better risk and business decisions based on the identified threats.

This report covers the period from April to June 2019 and leverages the processing of nearly 160 billion emails. During the period Mimecast rejected more than 67 billion of those emails, and the analysis presented in this report is based on rejections classified as spam, opportunistic and targeted attacks and impersonation detections, as these rejection reasons indicate a variety of highly malicious attack techniques.

Through this analysis, two opposing themes become apparent: simplicity and complexity. Many simple opportunistic attacks observed during the quarter used well-known “lowest common denominator” threat vectors and basic social engineering techniques. These types of attacks attempt to feed off the weak – those organizations that have simplistic security controls.

However, an increasing number of more sophisticated targeted attacks are using obfuscation, layering, and bundling of malware in an effort to avoid detection. In addition, these attacks are becoming more aware of their environments, implementing multiple evasion techniques as appropriate in a further effort to avoid detection.

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Email is the number one threat vector facing organizations today, and our fully-integrated, cloud-based services protect customers across the globe from incidents that typically start with email, including advanced cyberattacks, data loss, downtime, and human error. Mimecast services protect millions of employees at over 34,000 customers across a broad set of vertical markets in over 130 countries. Integrating with enterprise email platforms including Microsoft Exchange and Office 365, as well as Google, our services process more than half a billion emails per day.

Executive Summary

Research conducted April-June 2019 reinforced a previously observed trend: malware-centric campaigns are becoming increasingly sophisticated and complex, often using different pieces and types of malware in different phases of the attack. The research shows that this trend is being driven by threat actors becoming more organized and business-like and by implementing subscription and as-a-service based business models to deliver malware to reduce their work and to improve their return-on-investment. In addition, the research also highlighted the continued use of well-known malware within attacks, which is easily identified and blocked, as well as simple social engineering tactics intended to fool victims.

Key observations during the reporting period include:

- A large number of malware campaigns were observed, including ones incorporating **Emotet**, **Adwind**, **Necurs**, and **Gandcrab** malware.
- The threat actors behind Emotet launched a campaign that saw a large increase in activity on May 22nd, 2019 with infected systems in the United States, Canada, Brazil, and Central Europe involved in spreading the malware.
- The threat actors behind Adwind updated their malware and launched attacks across a number of industry sectors, including Professional Education (largely institutions of higher learning), IT Resellers, and Biotechnology.
- Bulk email ("spam") is heavily used by threat actors as a conduit to distribute malware.
- The volume of email impersonation attacks (sometimes known as business email compromises – BEC) blocked by Mimecast increased significantly, but research uncovered no meaningful change in the tactics and techniques being used.
- Opportunistic attacks are becoming increasingly sophisticated, layering multiple types of malware and delivery mechanisms in order to avoid detection by increasingly effective scanners.
- Targeted attacks are using email attachments with obfuscated file types, which trick the victim into opening the file and infecting the system.

Looking ahead, Mimecast researchers believe that attackers will continue to refresh older malware to help avoid detection, move towards more manipulative social engineering techniques, and leverage URLs hosted on well-known, generally trusted cloud platforms to spread malware.

Emerging Attacks

This selection of emerging attacks includes tactics and techniques that are new and have not been identified previously or are targeted in a way intended to circumvent detection technology and other security controls.

1.1 Threat Actor Reconnaissance

In the following example, shown in Figure 1, an email was sent to a target containing a .zip attachment and used a common style of subject line linked to payments, credit, or invoices. This is aimed at prompting victims to engage with the email.

In this case, the email states that a payment has already been made, a slight change from the typical social engineering tactics that demand payments, with the intent of panicking the victim into thinking a financial transaction has been made and coercing them into opening the malicious attachment. Upon opening the attachment, the victim is asked to enter a password to access the encrypted file. Typically, these passwords are included in the body of the email or in the subject line. This approach is interesting as it demonstrates the interplay between the technology (obfuscating the file through encryption to avoid detection) and the social engineering of the human target to get them to play an active role in the attack. In similar attacks, threat actors have also been observed phishing for Microsoft Office 365 credentials.

The .zip attachment shown here contains a 1,656 byte file called Remittance Advice.jpg.lnk. Sandbox analysis links this attachment to domains including remit-chase[.]com[1] and remit-wellsfargo[.]com[2], both of which are known to be malicious.

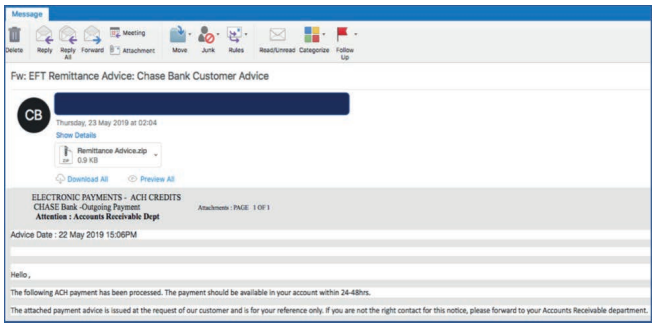


Figure 1: Sample email used for reconnaissance

We do not believe that the email seen in this example was the ultimate or final attack. Analysis suggests that the threat actor was conducting reconnaissance on the security of the targeted customer and trying to test detection response times rather than to infect the victim. We believe that the attacker will try to target this customer again within the next two quarters with a more sophisticated attack. However, while the testing and reconnaissance shows a very targeted approach by the attacker, it also implies that by catching the reconnaissance and understanding the intelligence provided, organizations can be in a better position to defend themselves.

1.2 Malicious VBScript

In this type of emerging attack an executable (.exe) file within an email-based attack is buried deep within a series of obfuscations in an effort to prevent it from being detected. In one example, an email was sent to a customer with a .tar file attachment. The .tar file type indicates that the attachment has many files and directories within this single archive file.[3] Inside the .tar is a UTF-16 VBScript. The malicious VBScript logic reconstructs the 140KB data string, then executes the resulting VBScript in order to infect the target system with malware.

1.3 Simple Impersonation Email Attacks

Research revealed a marked increase in the number of simple impersonation email attacks April-June, with no real change in the tactics used in these types of attacks, as simplicity is a great way to initiate the social engineering process. Similar to previous social engineering campaigns, the tactics used entice the user to engage with the threat actor by impersonating co-workers and superiors. CEOs, CFOs, and finance-related staff have been observed in our investigations as the most targeted candidates for impersonation, and we believe that they will continue to remain so in the future.

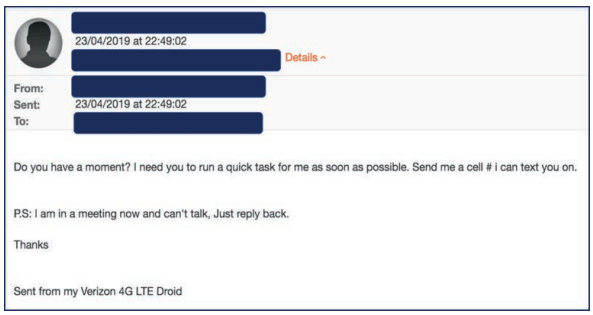


Figure 2: Example impersonation email message

Impersonation attacks are becoming more prominent as threat actors seek to target individuals for fast and easy financial gain. As noted previously threat actors are using social media sites related to work, such as LinkedIn, to target individuals in organizations. Information from these sites can help identify who is likely to work directly for executives, or who may have access to financial systems and information. In addition, the threat actors may employ similar domain names (using spellings that look correct at a quick glance) and display name spoofing (the sender's name shown by the email client) in engaging with the victim.

1. *https://www.virustotal.com/#/url/1c7fa4a9bfb4f35006b0d3b1cf17fcbdc3123d5187cf385c9363e4748ac90a7d/detection*
2. *https://www.virustotal.com/#/url/b1497a478ff9c8744e88a91324ab045a123689e3323238cbe88a5b2969526d60/detection*
3. *https://en.wikipedia.org/wiki/Tar_(computing)*

The sample message shown in Figure 2 focuses on getting the targeted victim to engage in a conversation with the threat actor. Note the attempted shift from email to texting – from communicating over a potentially secure channel to one that isn't secured. These types of attack can ultimately result in victims handing over confidential or financial information willingly to the threat actor without realizing it is an impersonation attack.

Most Active Campaigns

In these campaigns, threat actors are using well-known malware components, distributing them through Microsoft Office documents, Java applications, and attachments to brand fraud email messages. The attackers are evolving and adapting the capabilities of these components to help avoid detection as scanner efficiency increases.

2.1 Emotet

First witnessed in the wild in 2014, Emotet was originally built as a banking trojan that primarily targeted the financial sector across Europe. Its initial method of self-propagation was reported as brute force attacks against passwords by numerous security vendors. The most notable targeted threat campaign April-June, identified as the "latest Emotet" campaign, can be seen in Figure 3 below, with a clear peak in activity on May 22nd, 2019. Analysis of this particular attack found it spread through a known Emotet attack vector: a Microsoft Word document that automatically enables the malicious macros that start the infection process. The threat actors may have chosen to launch an opportunistic attack using a known attack vector to impact organizations with lax security controls – that is, those that have not yet properly cleaned, patched, and prepared their network for previously discovered attacks.

Investigation showed that this campaign was associated with malicious URLs on domains including aspectivesolutions[.]com, bettyazari[.]com, and fitnescook[.]com. Additional analysis4 indicated that these sites all use the PHP framework and WordPress content management system.

During the research period, this campaign reached multiple business sectors, but the Retail & Wholesale, Legal, Manufacturing, Financial, Transport, and Insurance sectors were the most frequently targeted when normalized on a per user basis. Analysis of the campaign found that attack origination sources related to the campaign appeared to be mostly originating in the United States and Canada, Brazil, and Central Europe (including Germany and Poland), as illustrated in Figure 4. The highest concentration was in the United States, with more than three times as many detections as Germany and Brazil, and more than four times as many as Canada and Poland.

Research found a significant increase in Emotet activity in 2019, having seen a large number of individual campaigns that use it, but which appear to download a secondary malware package instead of acting as a banking trojan and stealing credentials for itself. This may be because the threat actors behind Emotet have adapted it into a packing and delivery service for other threat actors – essentially using it as a downloader-as-a-service for other malware.

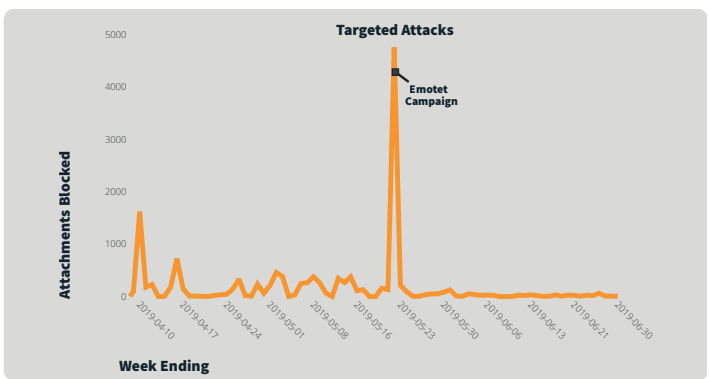


Figure 3: .doc file type blocked threat volume, April-June 2019

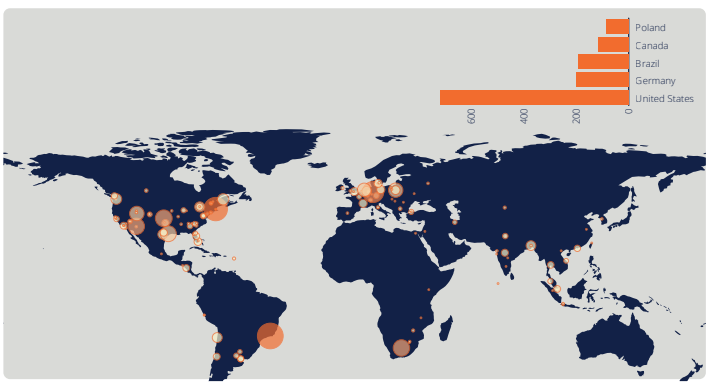


Figure 4: Location of infected systems involved in Emotet campaigns

4. *https://builtwith.com/detailed/aspectivesolutions.com, https://builtwith.com/detailed/bettyazari.com, https://builtwith.com/detailed/fitnescook.com*

2.2 Adwind

Adwind is classified as a Remote Access Trojan (RAT), and has evolved significantly since its genesis in 2012, with many different versions released over the years. The release of the Adwind RAT source code to public forums allowed other threat actors to customize it for their own purposes. It is possible the original creator is behind the recently observed attacks, but research suggests that there are a range of different malicious actors now using the underlying code for their own campaigns.

The current version of the malware includes a number of new capabilities, including collecting keystrokes, stealing passwords and data from web forms, taking screenshots and video from webcams, transferring files to a remote server controlled by the threat actors behind the malware, stealing from cryptocurrency wallets, and exploiting VPN certificates.[5]

Adwind targets Java applications and uses malicious JAR files to infect its victims, distributing the files by attaching them to spam emails. Java's massive install base means that the potential attack surface essentially spans all major operating systems and platforms. The latest variant uses the VBScript-based worm "Houdini" to infect target systems. As detection tools and other security vendors block these attacks, research suggests that the threat actors will update the malware and add new features over the coming months. In addition, research indicates that attackers will move from using malicious attachments to spread Adwind to using embedding URLs on compromised systems within emails that take the victim to a landing page where Adwind can be downloaded, or where a different payload is used to initially infect the victim, as a precursor to an Adwind infection.

2.3 Brand Fraud

With the shift to SaaS-based services for both business and personal activities, users have become accustomed to receiving emails with status updates, requests for additional information, and the like. This has created an opportunity for threat actors to both harvest credentials for future attacks and deliver malware through emails that fraudulently appear to come from a well-known, trusted brand.

During the three month research period, hundreds of brand fraud attacks appearing to come from a well-known package delivery service were identified, often discovered during unrelated research and investigations. The emails sent to victims are often very convincing, tricking users into clicking on malicious attachments and links within the messages. In these cases, the victims were targeted with payment-related fraud.

Analysis of the related messages indicated that the content is actually an image, pasted into the email, and not text that can be manipulated or searched. For instance, the email contains an invoice file with a ".ace" extension, which is a compressed archive file format that was popular in 1999-2016. Analysis indicates two executable files (winrar. exe and ace32loader.exe) are contained within it, both of which install malware, including Trojans and downloaders, when executed.

This type of brand fraud that heavily relies on images versus text is an evolving trend, as threat actors look to update older attacks and frauds, and renew the techniques being used in an effort to circumvent increasingly effective detection tools and security controls.

THREAT LANDSCAPE OVERVIEW: April-June 2019

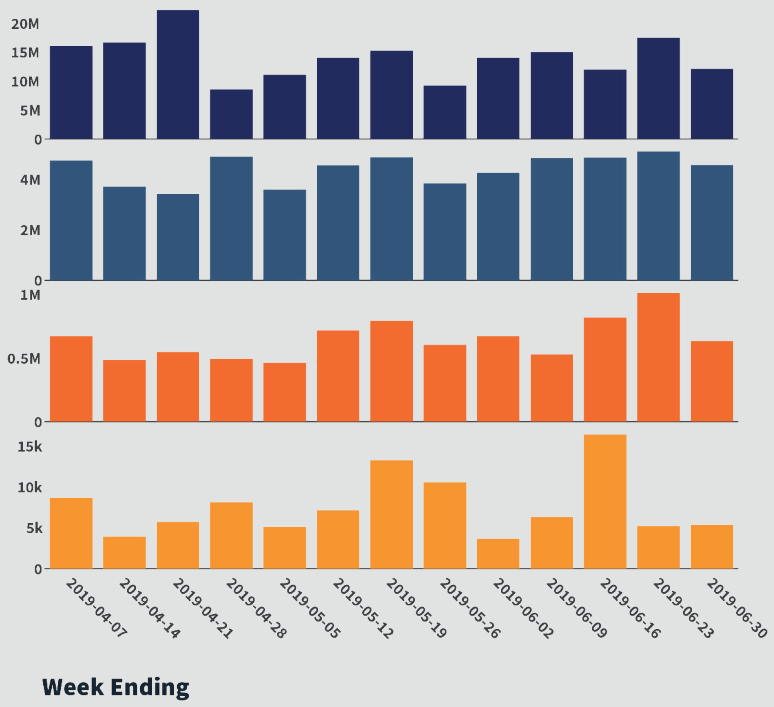
The four primary threat categories analyzed within this report are Spam, Impersonation Attacks, Opportunistic Attacks, and Targeted Attacks. Our research shows that these threats are persistent and widespread across a broad set of industry sectors.

Threat activity during the April-June 2019 period observed across the Mimecast Global Grid (global datacenters that support the delivery of Mimecast cloud-based services) has increased over the previous year, with Figure 5 illustrating the number of threats blocked across the four primary categories. Peak threat volume was seen during the week ending April 21, 2019 with more than 25 million threats detected and blocked during the associated seven-day period. The volume of spam-related threats was significantly higher than the other categories throughout the three-month research period. Peak targeted attack threat volume during the week ending June 15, 2019 was associated with a HawkEye malware campaign. HawkEye is a trojan distributed through Microsoft Word documents that monitors and exfiltrates data from infected systems.[7]

The percentages in the 'by sector' figures below are based on normalized "attacks per user" data sets to eliminate the impact of over-represented sectors.

5. *https://cyware.com/news/adwind-rat-resurfaces-again-relies-on-another-malware-for-infection-4910082a*
6. *https://en.wikipedia.org/wiki/ACE_(compressed_file_format)*
7. *https://www.cyber.nj.gov/threat-profiles/trojan-variants/hawkeye*

Threats Blocked Across the Four Primary Categories



- **Spam**
  Bulk email used as a conduit to distribute malware.
- **Impersonation Attacks**
  Communications attributed to trusted senders in an attempt to maliciously fool users.
- **Opportunistic Attacks**
  Leverage well-known threats including malware samples detected primarily with signatures.
- **Targeted Attacks**
  Uses vulnerabilities that are actively exploited and are not known, specifically designed to get past commodity malware scanners.

Figure 5: Blocked threat type and volume, April-June 2019

3.1 Spam Campaigns

During the research period, threat actors used bulk email campaigns to propagate malware, targeting industry sectors including Professional Education, Software & SaaS, and IT Resellers, as shown in Figure 6. The figure also illustrates the long tail of spam targets, as the top five most targeted sectors accounted for less than half of the observed. Campaign volume was at its most active during the week ending April 21, 2019 with more than nine million threats blocked in a single day early that week, more than two to three times higher than any other daily peak April-June, as seen in Figure 7. The figure also shows a noticeable drop in blocked threat volume during the Memorial Day holiday weekend in the U.S.

One of the most prolific campaigns observed during the quarter was generated by Emotet, which uses its spam module to spread the Emotet botnet (known to be a huge botnet split into two separately operating subsets). The spam module uses the botnet to send emails containing malicious URLs within the main body of the message or malicious attachments that lead to the victim to unknowingly download Emotet. Keeping up with the growth of the botnet, along with the continuing evolution of Emotet's capabilities, presents significant challenges for the industry. Further details on Emotet can be found in Section 2.1 above.

Other significant spam campaigns observed during the reporting period were generated by Adwind, a malware-as-a-service platform. This research found that Adwind has recently been used in renewed efforts to target victims with multiple malware payloads, including crypto miners. This new version incorporates H-worm, a Visual Basic Script (VBScript)-based Remote Access Trojan (RAT) that often incorporates multiple layers of obfuscation, including standard and custom Base64 encoding and character substitutions.[8] This obfuscation demonstrates determination on the part of the attacker to avoid detection by scanning and analysis tools. Further details on Adwind are detailed in Section 2.2.

8. *https://en.wikipedia.org/wiki/ACE_(compressed_file_format*

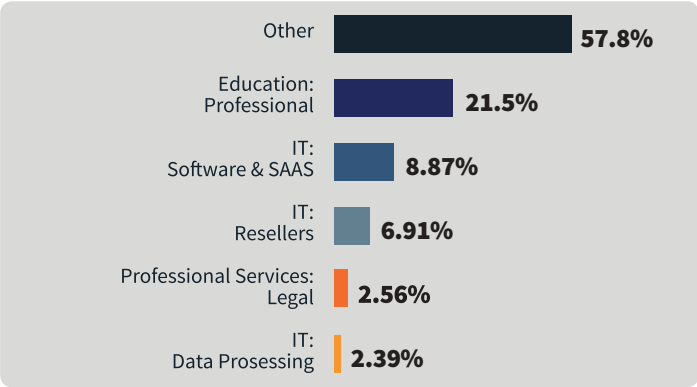


Figure 6: Spam distribution by sector (attacks per user)

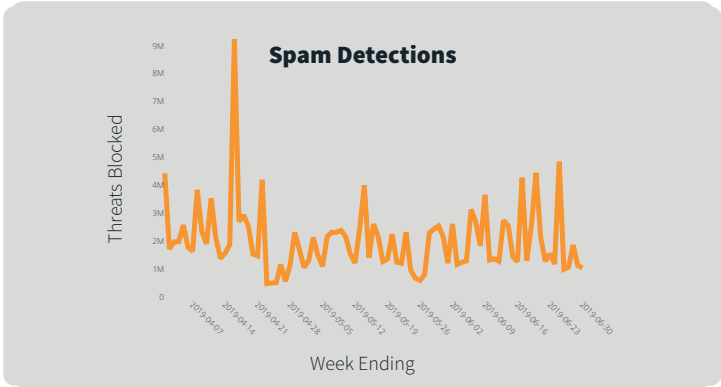


Figure 7: Spam campaign blocked threat volume, April-June 2019

3.2 Impersonation Attacks

Threat Center research also uncovered a large number of impersonation attacks that were detected and blocked throughout the April-June period. Management & Consulting and Biotechnology were the two most heavily targeted sectors, accounting for nearly 30% of threat volume even when normalized on a per user basis, as shown in Figure 8. These industries may have been heavily targeted because they represent a rich store of intellectual property, both organically and related to the companies that they work with, and as such are a ripe target for data exfiltration. Similar to spam, impersonation attacks also target a long tail of sectors, with the top five most targeted sectors comprising slightly less than half of the observed threat volume during the three month research period. Figure 9 highlights impersonation attack activity across the quarter. It is interesting to note that like spam, attack activity appears to have dropped around the Memorial Day holiday weekend (May 25-27) in the United States, which suggests that the attackers responsible for these threats may be located in the U.S. or are professionally aligned with U.S. holidays.

Individuals at the senior and C-suite level are frequently impersonated, with threat actors targeting those they believe are closely associated with the impersonated individual, such as a personal assistant. These relationships are often easily discoverable using social media platforms,[9] as this information makes it easy to identify reporting hierarchies within an organization. Analysis of a selection of these emails found that they are successfully employing relatively unsophisticated methodologies, such as coercing the victim into doing something they shouldn't, like using socially engineered content within the main body of the email, instead of including malicious URLs or attachments. More information on these attacks can be found in Section 3.3 below.

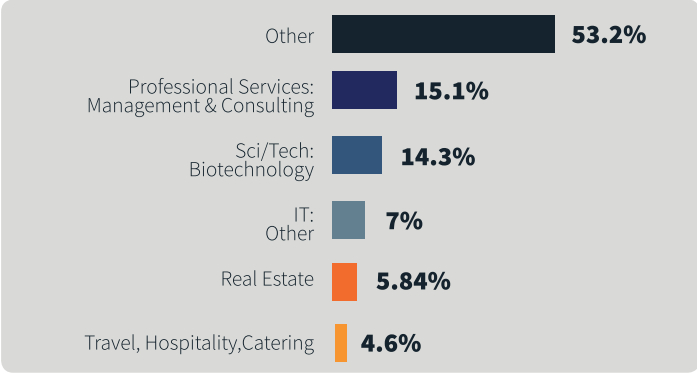


Figure 8: Impersonation Attacks distribution by sector (attacks per user)

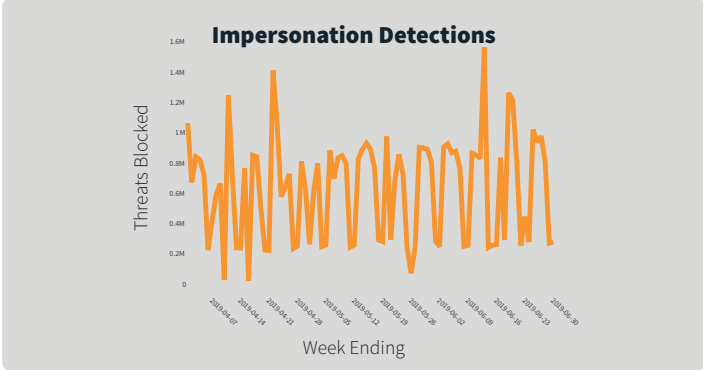


Figure 9: Impersonation Attack blocked threat volume, April-June 2019

3.3 Opportunistic Attacks

Opportunistic attacks make use of malware that has been previously identified through analysis of previously detected attacks by Mimecast, our technology partners, or the broader security vendor marketplace. Mimecast researchers and engineers anticipate their evolution and future use and implement specialized analytics to detect and block them. Figure 10 shows that the Data Processing industry sector was targeted by just over 25% of the normalized

9. *https://mashable.com/article/linkedin-is-full-of-spies/*

Opportunistic Attack threat volume during the April-June period, with other sectors seeing no more than four percent of this activity. Threat activity was most significant during mid-June 2019, as Figure 11 demonstrates, with a peak volume nearly two times higher than those measured earlier in the research period.

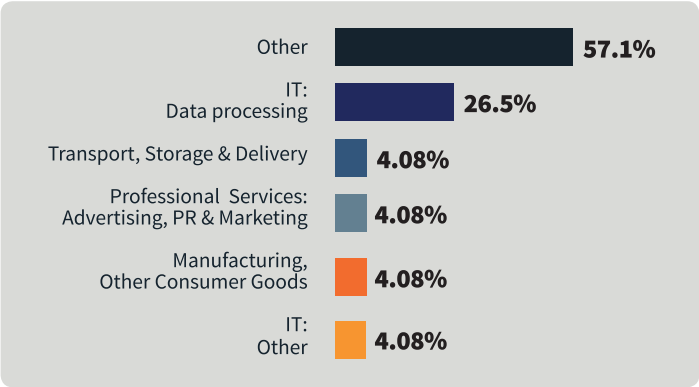


Figure 10: Opportunistic Attack threat distribution by sector (attacks per user)

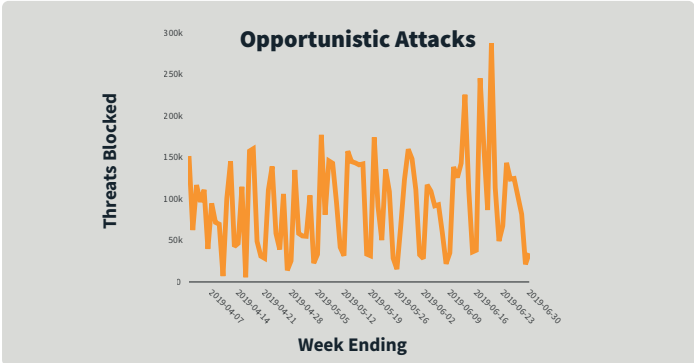


Figure 11: Opportunistic Attack blocked threat volume, April-June 2019

During April-June 2019, more than two million opportunistic attacks were blocked by Mimecast. Figure 13 details the top opportunistic attack categories blocked during the reporting period, and the top three categories are reviewed in more detail below.

Top Opportunistic Attack Malware Categories

Trojans

Research showed that the large number of Trojans blocked during the quarter is due to its use as a delivery mechanism for more dangerous malware payloads. The most common threats delivered via Trojans included:

- A significant Emotet campaign at the end of May (see Section 2.1 for further information).
- A significant volume of Adwind activity targeting a number of sectors (see Section 2.2 for further information).
- Malware related to coin/crypto mining activity.

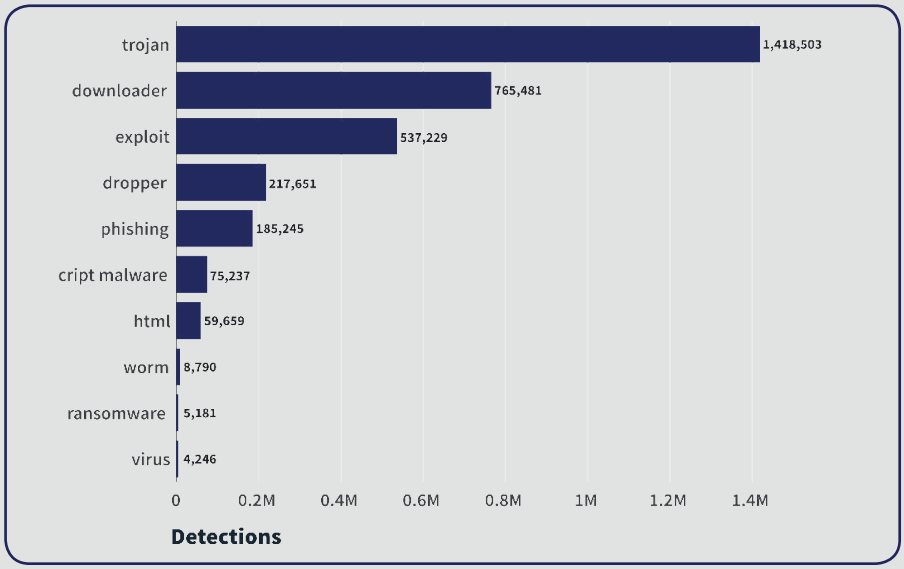


Figure 12: Top Opportunistic Attack malware categories, April-June 2019

Downloaders

Downloaders were the second most frequently blocked type of opportunistic attack malware over the three month research period. The most potent downloader at present is Emotet. However, recent attacks have increasingly found Trickbot infections to be combined with Emotet infections, with the potential for an extension to RYUK ransomware attacks if these infections are not remediated early.[10] sLoad downloader activity was also detected throughout April and May, as shown in Figure 14, targeting multiple customers across multiple regions. sLoad is a PowerShell downloader used to download additional specific malware types based on the host information that the downloader reports back to its Command and Control server.[11]

Analysis indicated that the spikes on the graph represent the points at which the attacker switched file types for attachments, moving from Microsoft Excel to Microsoft Word to text.

10. https://www.ncsc.gov.uk/news/ryuk-advisory
11. https://success.alienvault.com/s/question/0D50Z000094ELPe/alien-labs-threat-intelligence-update-for-usm-anywhere-march-24-march-30-2019

Mimecast Threat Center believes that this indicates that the attacker is attempting to take advantage of the lag inherent in signature-based security control systems; by the time one technique is identified, the attacker is on to the next one. To that end, the threat actor community has tools that they use to validate whether their technique is still viable, or if it has been detected by commercial industry toolsets.

Exploits

During the research period, multiple threats were detected attempting to exploit the CVE-2017-11882 vulnerability, a 19-year-old flaw in Microsoft Office.[12] This vulnerability lets attackers execute remote code on a vulnerable machine, even without user interaction, after a malicious document is opened, and threat actors exploit the vulnerability to steal information and credentials. Detected attempts to exploit this flaw were most active in early April and mid-June, as seen in Figure 15 below. Before deploying Microsoft Office-based exploits, attackers often test their malware and approaches against their own instances of the productivity suite.

Opportunistic Attack Assessment

The data shows that there is a growing trend of campaigns becoming increasingly sophisticated as they are often no longer based upon a single type of malware. Attacks are instead combining different types of malware and delivery mechanisms, as can be seen by the large number of Trojans observed April-June 2019. This approach reaches more victims and capitalizes on the work of other cyber criminals by leveraging existing botnets or spam systems.

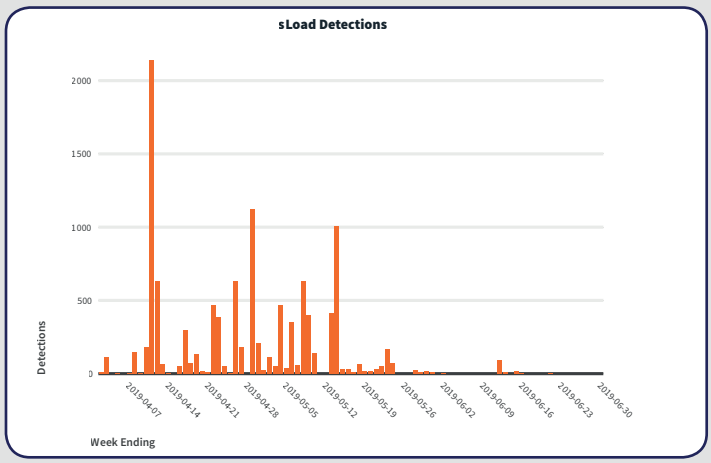


Figure 13: sLoad downloader detection, April-June 2019

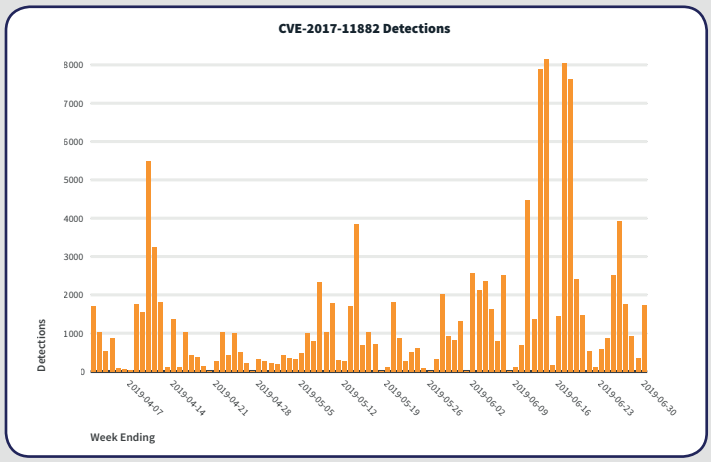


Figure 14: Detected CVE-2017-11882 exploit activity, April-June 2019

3.4 Targeted Attacks

Targeted attacks are specifically designed to get past commodity malware scanners by using newly detected or updated malware not detectable with file signatures. During the three month research period, tens of thousands of targeted attack threats were detected and blocked by Mimecast. It is worth highlighting that the volume of targeted attacks is significantly lower than that of other threat categories, which saw hundreds of thousands to tens of millions of threats blocked during the period. This discrepancy is due to the expertise and innovation required to create, customize, and deploy new malware.

Figure 15 illustrates that targeted attack threats do not appear to be heavily targeting any particular industry sector, with only one ("IT: Other") receiving more than 10% of the threat volume. A peak in threat activity was observed on June 13, as shown in Figure 16 – further analysis associated this spike with a HawkEye malware campaign. This campaign was active between June 3-13, 2019 and delivered malware via files that contained malicious macros which downloaded more malware from an Iranian IP address.

12. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/17-year-old-ms-office-flaw-cve-2017-11882-actively-exploited-in-the-wild

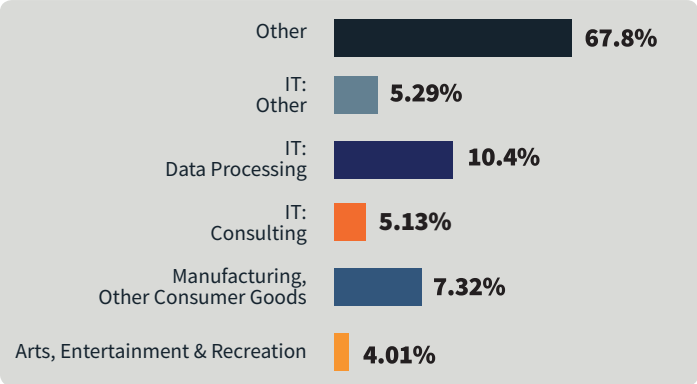


Figure 15: Targeted Attack threat distribution by sector (attacks per user)

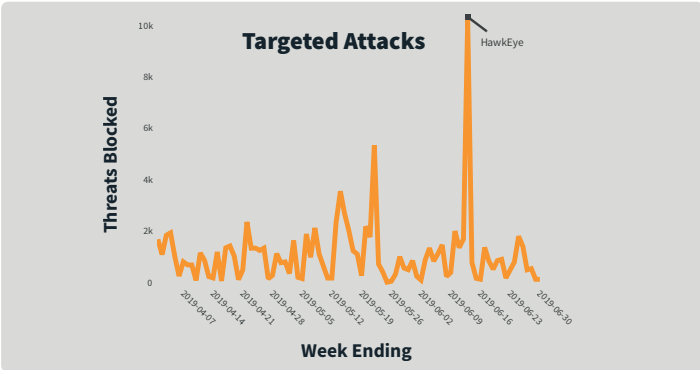


Figure 16: Targeted Attack blocked threat volume, April-June 2019

Targeted Attack Assessment

Unfortunately, Email remains a reliable way to deliver malware[13] and is the most commonly used attack initiation vector. However, as users become more aware of the risk of clicking on files with certain file extensions and opening unexpected emails from email addresses not known to the user, as well as becoming more skilled at identifying fraud and other social engineering techniques, threat actors have had to update their tactics and techniques. This includes using attachments with a variety of sometimes obscure, or older, file types to distribute malware. One example is the use of .ace files, a compression format that peaked in popularity nearly 20 years ago, as discussed in Section 2.3 above.

Figure 17 illustrates the file extensions that were commonly associated with targeted attacks detected during the three-month research period. Microsoft Office is clearly popular, with more than 40% of detected threats using files associated with Microsoft Excel solutions, while file types associated with Microsoft Word technology were seen in nearly 15% of threats. This highlights the recognition by threat actors that nearly everyone in the business world uses Microsoft Office tools, making wholesale blocking of attachments containing Office files an unacceptable solution, since so many legitimate emails contain such attachments. Additionally, this research demonstrates that the majority of Microsoft Office-based files used in attacks tend to be older formats, as they now lack support to patch vulnerabilities. As such, attackers use these file types to exploit and circumvent weak security controls.

More than 10% of threats attempted to bundle malware in archive formats, such as .zip. Section 2 highlights several campaigns that attempted to use archive formats as a means of evading detection. Another key technique observed during this report period includes using attachments that obfuscated the extension of the attachment. This technique is designed to trick the victim into opening the file,

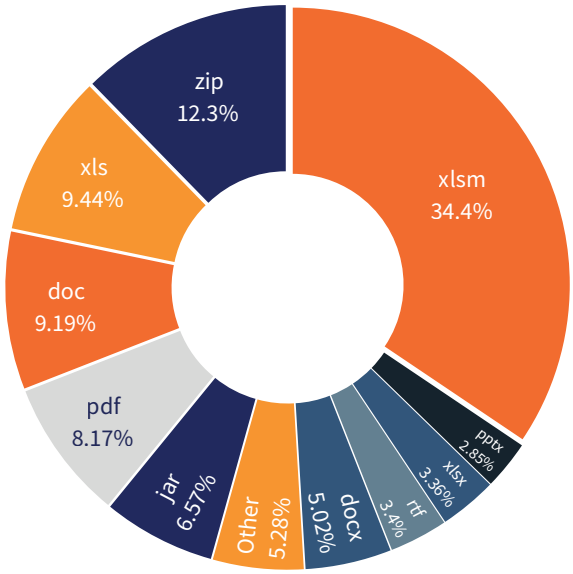


Figure 17: Targeted attack file extension distribution

causing the system to become infected. Such behavior by attackers indicates a move towards more sophisticated attacks as they try to circumvent detection tools and other traditional security controls.

In general, the rapid detection of targeted attacks at a cloud-based gateway is critical to protecting organizations that often only have antivirus or signature-based techniques in their downstream security infrastructures.

13. https://www.mimecast.com/content/malware/

TOP TARGETED SECTORS

In addition to analyzing the top threat categories, Threat Center researchers also examined the top industry sectors targeted during April-June 2019. Figure 18 highlights the top sectors targeted by both opportunistic and targeted attacks, based on attacks per user. Across all tracked sectors, there were 29 attacks per user, on average. The Professional Education sector is a clear outlier, with users there seeing nearly 9x as many attacks as compared to the average.

4.1 Professional Education

The Professional Education sector, which includes private educational companies, colleges, institutes, and training providers, was targeted by a significant campaign between May 6-9, 2019. Analysis revealed that the campaign included Adwind malware, also known as jRAT, that has circulated since December 20, 2014, and which recently updated its attack methodology. Refer to Section 2.2 above for a detailed analysis of Adwind. Research suggests that the sector's attack rate was significantly higher than others due to constantly changing student populations that are unlikely to have high security awareness, and the potential for attackers to get access to personal data. Attackers may also recognize that such educational institutions are harder to defend because of the apparent conflict between their inherent openness for academic reasons and the need to protect high-value research conducted for government and industry partners.

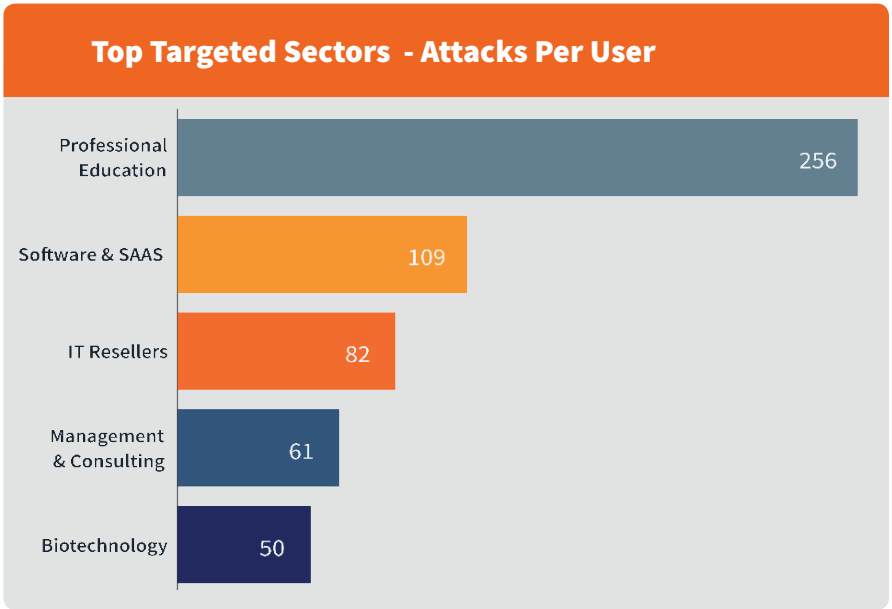


Figure 18: Top targeted sectors, April-June 2019

The most unusual activity seen during the research period targeting this sector was a massive increase in blocked spam threats on April 16, 2019 jumping to a peak more than eight times higher than the normal daily volume, as shown in Figure 19. A similar spike was observed on May 20, 2019 for Targeted Attack threats, but even at the peak, volume was significantly lower than the other threat types. Research revealed that this spike was related to .zip files that contained malicious Microsoft Office (Excel or Word) files that downloaded a trojan linked to the **TA505 threat actor group**.[15] This campaign was part of a larger cross-sector campaign focused on companies in the U.S. and U.K., and research suggests that it had a financial motivation.

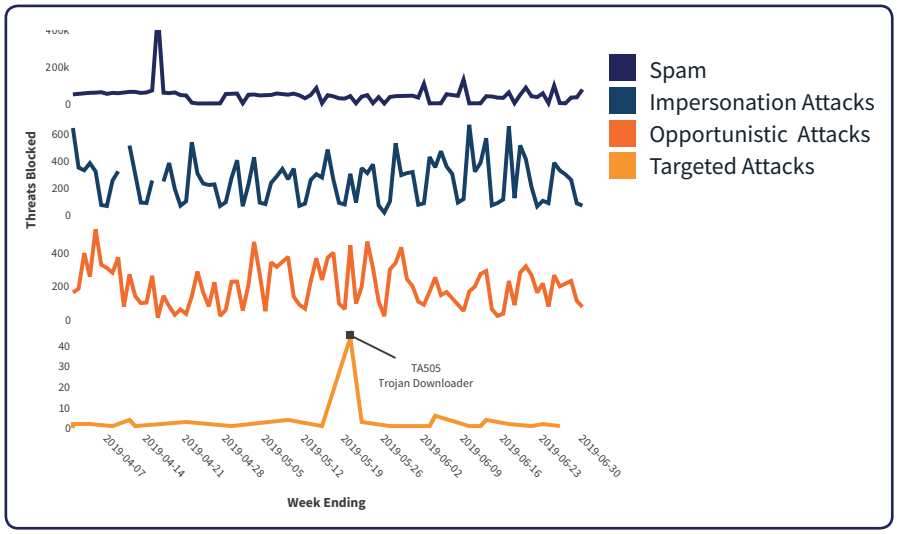


Figure 19: Threat Activity observed across the Professional Education sector, April-June 2019

14. https://www.kaspersky.co.uk/resource-center/threats/adwind
15. https://blog.yoroi.company/research/ta505-is-expanding-its-operations/

4.2 Software and SaaS

The Software and SaaS sector was hit by a number of significant attacks during the research period, using Adwind and QRat. Similar to Adwind, QRat is a Trojan that targets Java-based platforms and uses JAR attachments in the malicious emails. It is, however, distinct from Adwind although sometimes mistaken for it. A key reason that these trojans keep using Java is that its code can be very heavily obfuscated – the trojans are created in such a way that make it very hard to detect all of them using regular scanning mechanisms, including pattern matching and static analysis. Single significant spikes were observed across the Spam, Impersonation Attacks, and Opportunistic Attacks.

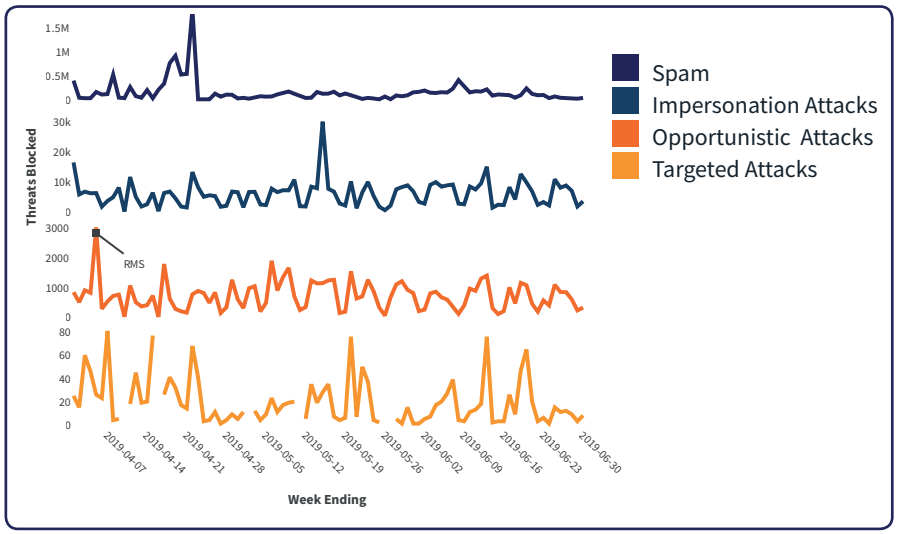


Figure 20: Threat Activity observed across the Software and SaaS sector, April-June 2019

Single significant spikes were observed across the Spam, Impersonation Attacks, and Opportunistic Attack threat types April-June, while Targeted Attack threat activity had more spikes, albeit with much lower activity volume. These latter spikes are likely related to a number of short-lived campaigns, including Emotet on May 22, 2019 and Qrat at the end of June 2019. Other activity shown in the graph may be related to campaigns sustained at a lower level throughout the research period, including Adwind and HawkEye.

The Opportunistic Attack spike on April 5, 2019 labelled "RMS" in Figure 20 is related to a campaign using emails with archive files that included malicious content attached to the messages. This malicious content ultimately leads to the installation of the Remote Manipulator System (RMS) client, a remote access tool which gives the attacker full control of the victim's machine.[16]

4.3 IT Resellers

This sector was hit by a significant volume of Adwind attacks throughout the reporting period, as well as a mixture of other Trojan downloaders. Refer to Section 2.2 above for a detailed analysis of Adwind.

Figure 21 shows that there were spikes in activity observed across both Opportunistic and Targeted Attack threat categories on June 13. The Targeted Attack peak was associated with the Hawkeye malware campaign, which impacted the Management and Consulting sector as well. Further research determined that the Opportunistic Attack peak was due to a combination of Mimecast generic trojan signature detections and a Microsoft Word macro trojan which made up 46% and 23% of detections on that day, respectively. In addition, it is interesting to note that Spam threat activity dropped to near zero for several days following the spikes in activity observed on April 1 and April 22, 2019.

Figure 21: Threat Activity observed across the IT Resellers sector, April-June 2019

Just as Adwind targeted the Software and SAAS sector, research showed that the threat actors behind it were targeting a large number of IT-related companies, including the IT resellers sector.

16. *https://securityaffairs.co/wordpress/86274/cyber-crime/ta505-expands-operations.html*

4.4 Management and Consulting

Research indicated that Management and Consulting companies were targeted by several Microsoft Office exploits during the three-month research period including ones linked to **CVE-2017-8570** and **CVE-2017-11882**[17] vulnerabilities in Microsoft Word. Further investigation indicates that the URLs linked to this exploit are hosting coin mining malware. Attacks using older exploits, such as these from 2017, indicate that attackers are hunting for organizations and systems that are not up-to-date with their patching. Adwind also targeted this sector during the quarter. Adwind also targeted this sector in the April-June period. Refer to Section 2.2 above for a detailed analysis of Adwind.

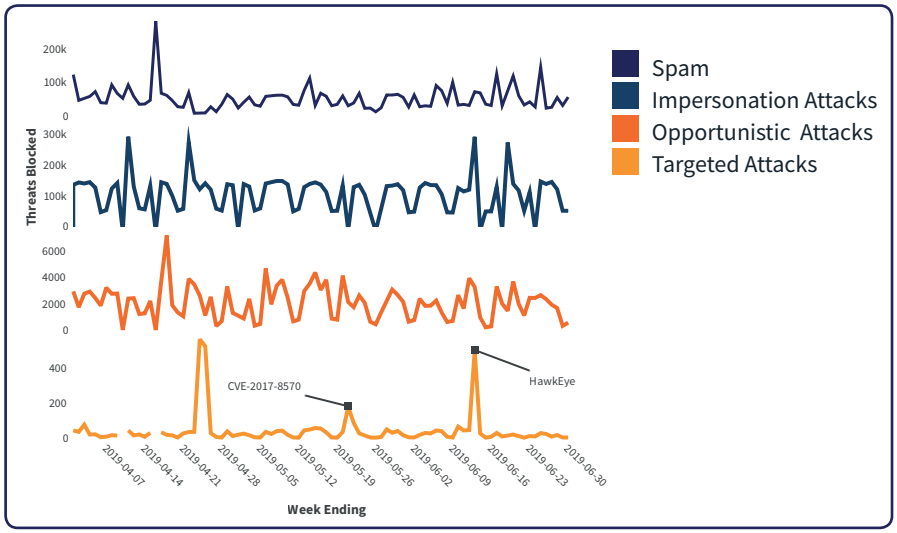


Figure 22: Threat Activity observed across the Management and Consulting sector, April-June 2019

The exploit targeting **CVE-2017-8570** is visible as a nominal peak on May 21, 2019 in the Opportunistic Attack graph in Figure 22, although the volume is lower than the peaks observed on April 24, 2019 and June 13. Further analysis of the data found that the June 13, 2019 was related to the HawkEye malware campaign.[18] (The IT Resellers and Software and SaaS sectors also saw Opportunistic Attack threat activity peaks on June 13, as part of the HawkEye malware campaign, in line with the observations in Section 3.4 above.)

This sector may have been targeted by so-called cryptojackers as a means of bridging into other sectors, with a goal of targeting the third parties that the management and consulting companies work with to increase the amount of processing power available for their crypto mining activity. However, cryptojacking also tends to take place in concert with the delivery of other forms of malware through the effective use of a dropper to install multiple payloads, which means that the threat is multi-headed.

4.5 Biotechnology

The biotechnology sector was hit by a range of attacks April-June, including a number of Adwind campaigns throughout April and May 2019, Emotet atthe end of May and QRat during the first week of June 2019. Refer to Section 2 above for a detailed analysis of these attack vectors.

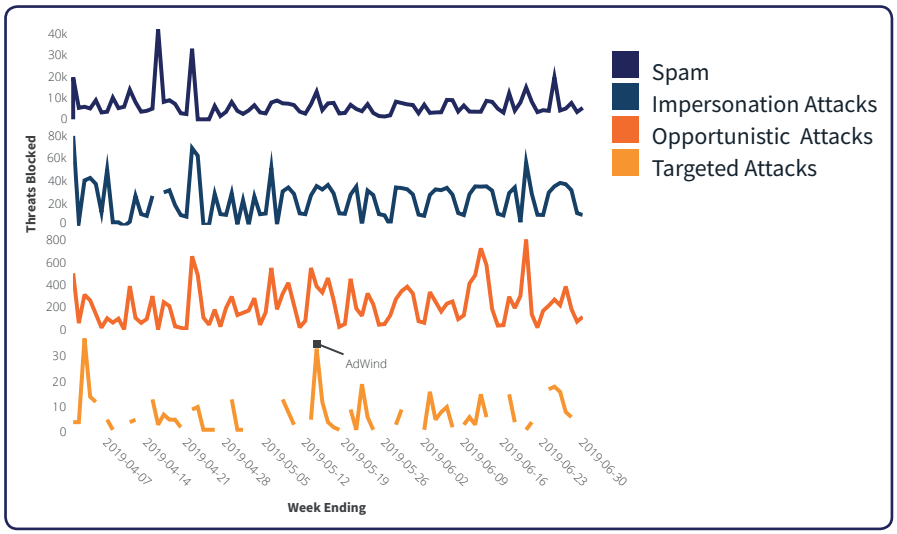


Figure 23: Threat Activity observed across the Biotechnology sector, April-June 2019

Significant spikes in Spam threat activity are evident in Figure 23 on April 16 and 22, 2019. These spikes align with peaks in Spam threat activity seen in the Professional Education and Management and Consulting sectors on April 16, and in the IT Resellers and Software and SaaS sectors on April 22. Peaks in Impersonation Attacks and Opportunistic Attack threats were also observed in the Biotechnology sector on April 22. The Opportunistic Attack spike was due to Emotet and Fareit trojan campaigns. It is interesting to note that the April 22, 2019 spikes align with the start of the International Summit on Biotechnology & Healthcare, which took place in Dubai.

17. https://www.bleepingcomputer.com/news/security/new-technique-recycles-exploit-chain-to-keep-antivirus-silent/
18. https://www.securityweek.com/new-variant-hawkeye-stealer-emerges

Looking ahead

Updating Old Tricks

Mimecast is observing an increase in unsophisticated attacks and simple impersonation attacks, along with threat actors turning their attention to updating older malware with new modules and code to get around detection tools. The research suggests that this trend will accelerate through the end of 2019 as tool efficiency continues to increase, forcing threat actors to use different techniques to reach their intended victims. It is also likely that we will see a shift towards more manipulative social engineering techniques, aiming to entice a range of targets across all sectors into giving up information, including financial data. These techniques are likely to succeed, as human error is frequently implicated in successful cyber-attacks.[19]

New Tactics and Techniques

Threat Center research suggests that there will likely be a rapid shift over the next six months to the use of new tactics and techniques to circumvent security controls and detections. Mimecast has detected an evolution of malware threats where threat actors link to documents or landing pages on well-known cloud platforms using URLs that otherwise would appear to be legitimate. These documents or landing pages then link or redirect users to other malicious sites or documents that download malware onto a victim's system. Additionally, research indicates the use of fileless techniques to continue to increase. Most observed malware currently incorporates at least one such technique, and additional ones will likely be integrated in an effort to avoid detection at the endpoint.

The coming months will also see increased usage of sandbox evasion techniques, as these capabilities continue to become more readily available as checkbox items in black market malware creation/bundling tools. Observed evasion techniques include malware checking for the presence of a printer, analyzing system configuration (resolution, cores, RAM) and uptime, and counting running processes and recently accessed files. By identifying whether the code is running within a sandbox or on an end-user system, the malware will act benign or malicious accordingly. A third of analyzed malware samples have been observed to layer as many as six evasion techniques, and research indicates that this percentage will grow rapidly. When sandboxing is used as part of a detection workflow, sandbox environments should be customized to resemble actual user environments and not freshly instantiated VMs.

Encryption technology is also starting to be widely used by enterprises and threat actors are starting to consider how this technology will impact their ability to access sensitive information being sent via methods other than email. In addition, threat actors will make increasing use of file encryption to further evade scanner detections.

19. *Mimecast - The State of E-mail Security Report 2019 (https://www.mimecast.com/the-state-of-email-security-2019/*

Conclusion

Opposing attack themes of simplicity and complexity are apparent throughout this report. While some attackers choose to blast out commodity malware or employ simple social engineering techniques hoping they randomly find victims, others invest effort in targeting their attacks towards specific industry verticals, using unique malware and targeted attack techniques. As threat actors evolve their operations to be more business-like, the approach they choose will depend on their ultimate goal, as they aim to only consume the amount of resources necessary to achieve that goal.

However, even the simple is becoming more complex - this is certainly the case for attack vectors and needs to be the case for an organization's security controls as well.

Threat actors now implement multiple sandbox evasion techniques in an effort to avoid detection at the gateway and use multiple layers of obfuscation to avoid detection at the endpoint. The use of multiple forms of malware in a layered attack is also becoming typical, as attackers move beyond reliance on a single vector. Simple social engineering techniques will continue to evolve, attempting to stay ahead of improved user awareness. Reconnaissance efforts by threat actors will continue to increase as well, as they try to understand how to get past increasingly sophisticated detection tools and security controls.

Given this, organizations need to adopt more sophisticated security and resilience strategies as they can't afford simplistic security controls as attack sophistication increases. Similarly, they can't afford to become lax at handling simple attack techniques, such as threat actors exploiting old vulnerabilities. At the very least organizations must recognize that patching is not optional. Organizational security controls need to have broad coverage of commodity malware as well as analytic techniques that can detect new malware based on its structure or behavior, not simply based on it having been seen before.

Since the cat-and-mouse game with attackers will continue for the foreseeable future, organizations can gain the upper hand using services that provide next generation static analysis, sandboxing, and dynamic analysis, operated and managed by expert threat researchers. In addition, training users on the threat landscape and their role in protecting the organization is critical as well, as it is an effective way to further reduce the potential attack surface. Having a comprehensive security strategy is critical, otherwise organizations risk compromise by both simple and complex attacks.