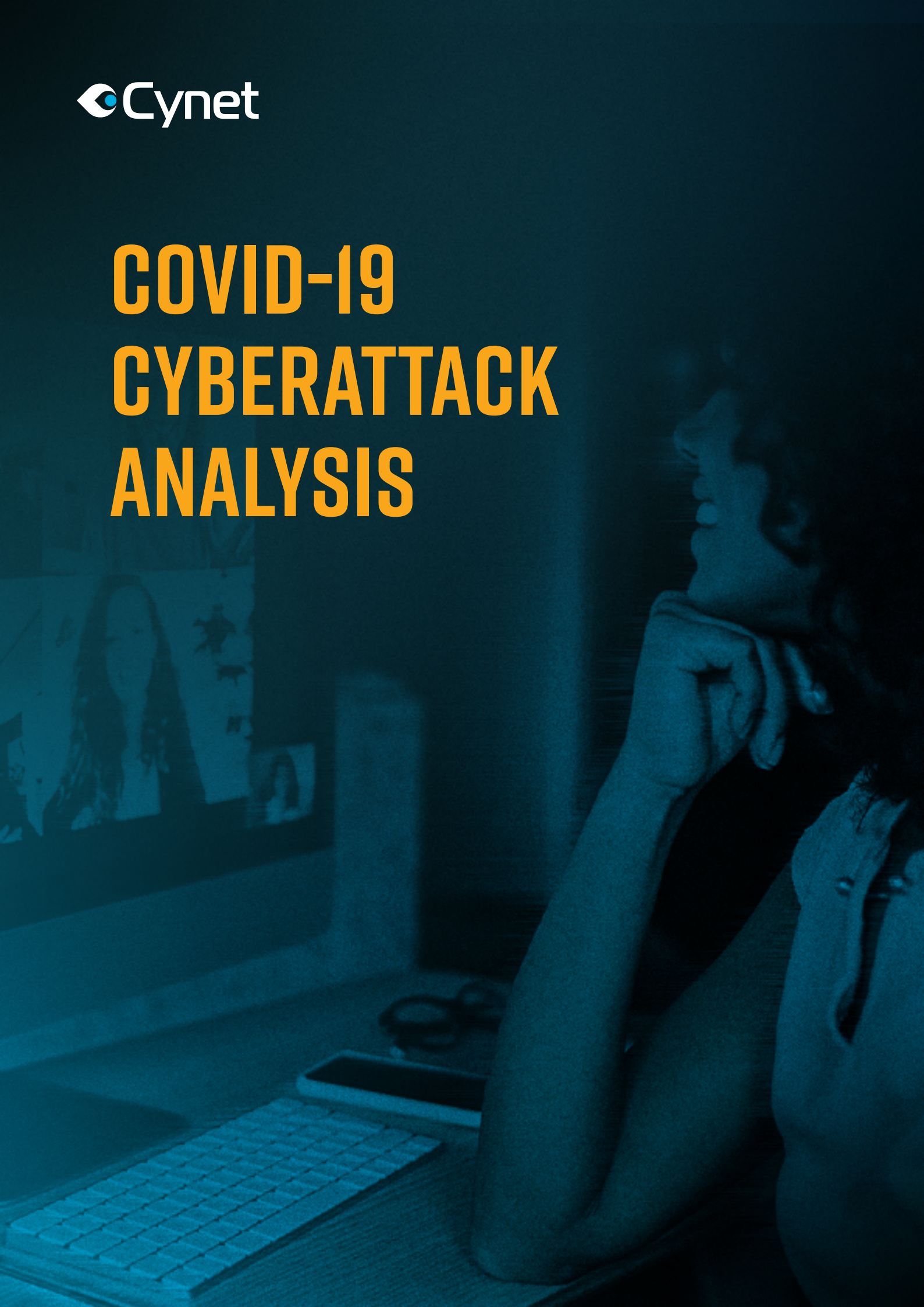
Cynet

COVID-19 CYBERATTACK ANALYSIS



FOREWORD

Since the beginning of the Covid-19 pandemic, Cynet has witnessed a sharp increase in new, highly sophisticated cyber-threats across its global customer base. These new threats are clearly designed to take advantage of the circumstances created by the pandemic:

Mass transit of employees to working from home.

Lack of security team members presence, due to lockdowns and quarantine.

Extensive use of remote connection to organizational resources through VPN.

Conspiracy theories which were fueled on account of the virus.

Extensive use of private computers to access work emails.

Cybercriminals are leveraging the widespread confusion surrounding Covid-19 by using pandemic-related topics to disguise many of their email-based attacks. They are increasing both the volume of attacks and the use of new malware while security teams are distracted by supporting the growing remote work environment. More details on these findings uncovered by Cynet's research team follow.

NEW MALWARE ON THE RISE

Cynet deploys multiple types of detection sensors to discover different kinds of attacks in customer environments. Our historical data shows that cybercriminals use existing malware in roughly 80% of attacks and new malware in roughly 20% of attacks on a worldwide basis. Existing malware can generally be detected using static, signature-based techniques whereas new attack techniques, which include modifying existing malware to bypass static detection techniques, can only be effectively detected using behavioral and heuristic analysis. When analyzing the threats aimed at Cynet's customer base over the past eight months, we can clearly see a shift in this equilibrium since the advent of the Covid-19 pandemic.

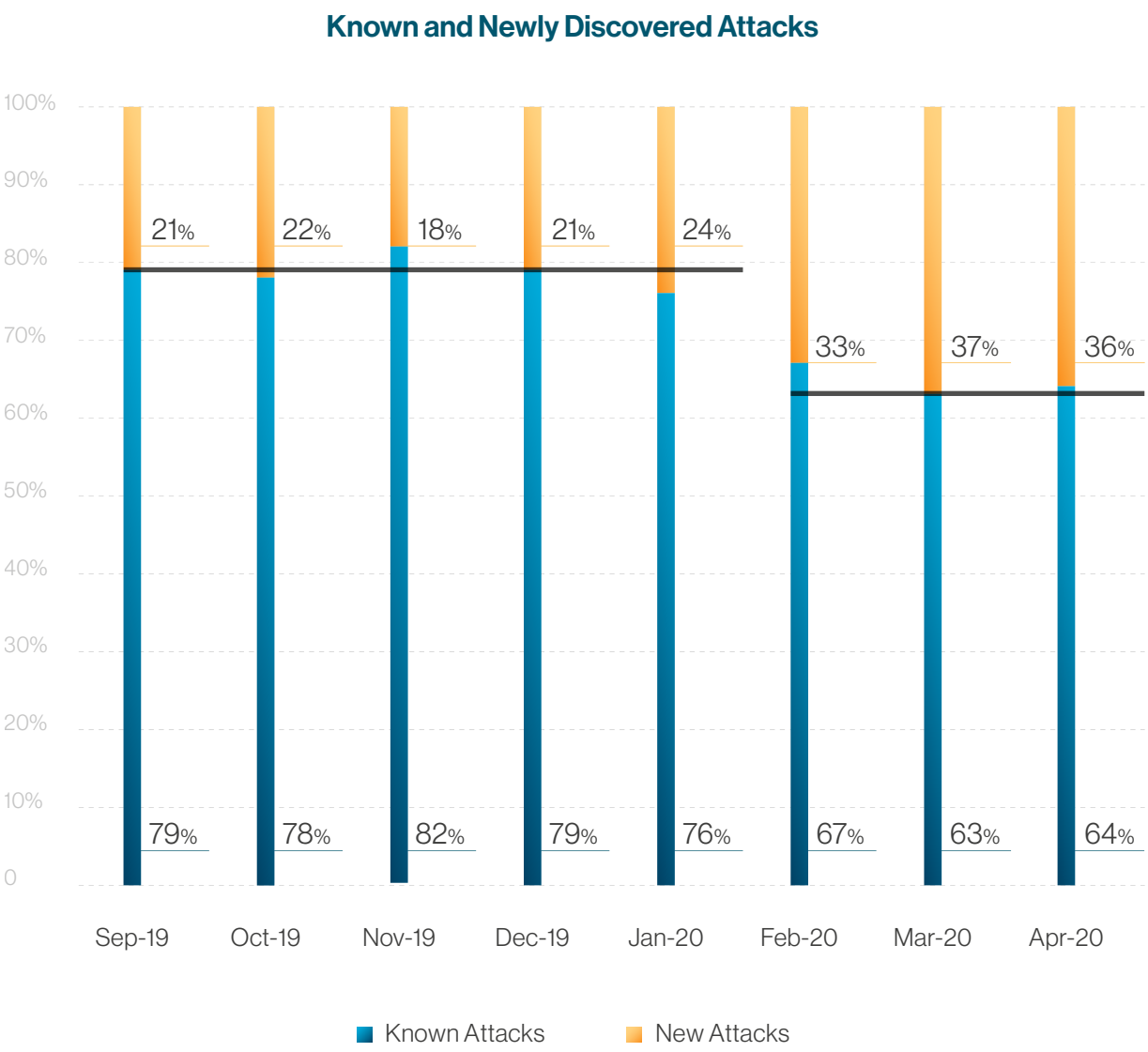


Figure 1 Ratio of attacks using well-known malware versus new malware

Figure 1 shows the expected ratio of known threats versus new threats at about 80% to 20% through the end of 2019. However, as the Covid-19 pandemic peaked, we observed an increase in the amount of new phishing attempts, new malware variants and even new malware. This increase has changed the ratio to about 65% of known attacks to 35% new attacks, **representing a 75% increase in the use of new attack methods**. This trend can also be observed when segmenting the results by geographic region, as shown in Figure 2.

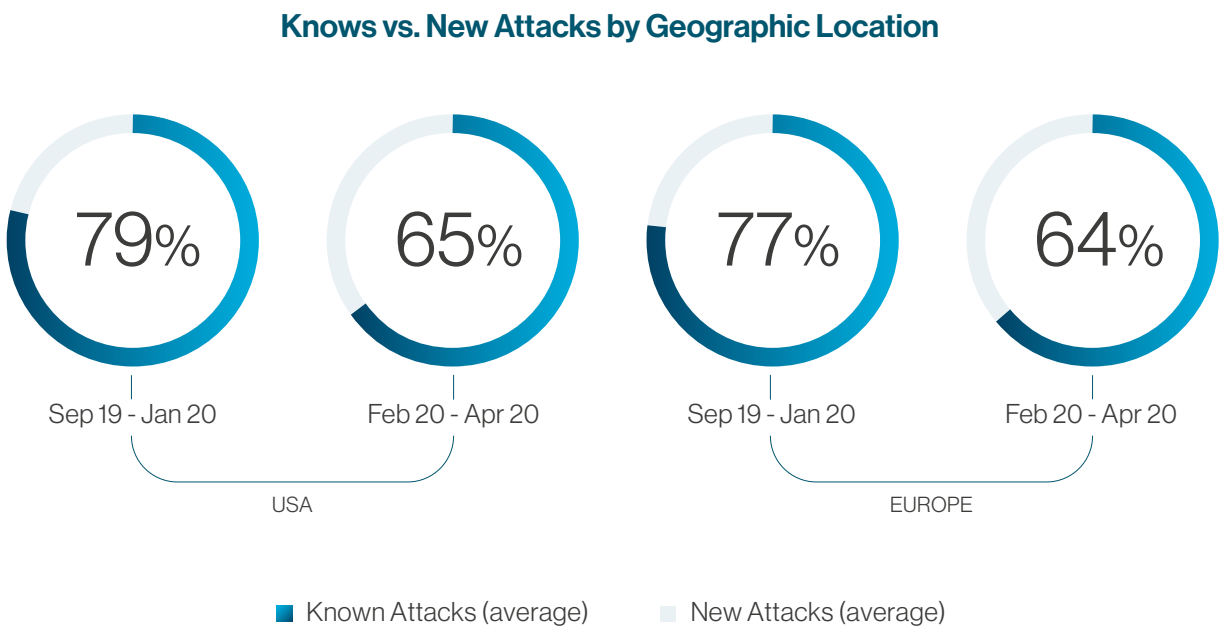


Figure 2 Comparison of Spear-Phishing attacks between peak coronavirus period (February, March 2020) and monthly average of 2019

New attack variants can only be detected using behavioral detection sensors, especially since some of these attacks utilize file-less techniques. New attack techniques cannot be detected and mitigated using Anti-Virus software alone.

Cyber security groups are challenged to keep pace with the increase in attacks during the Covid-19 pandemic and simply do not have the time to needed to utilize behavioral detection mechanisms to analyze and remediate a sharp rise in new cyberthreats. Figure 3 illustrates the number of Cynet Detection and Response Team (CyOps) engagements for September 2019 – April 2020, showing a sharp spike during the Coronavirus period (February 2020 – April 2020).

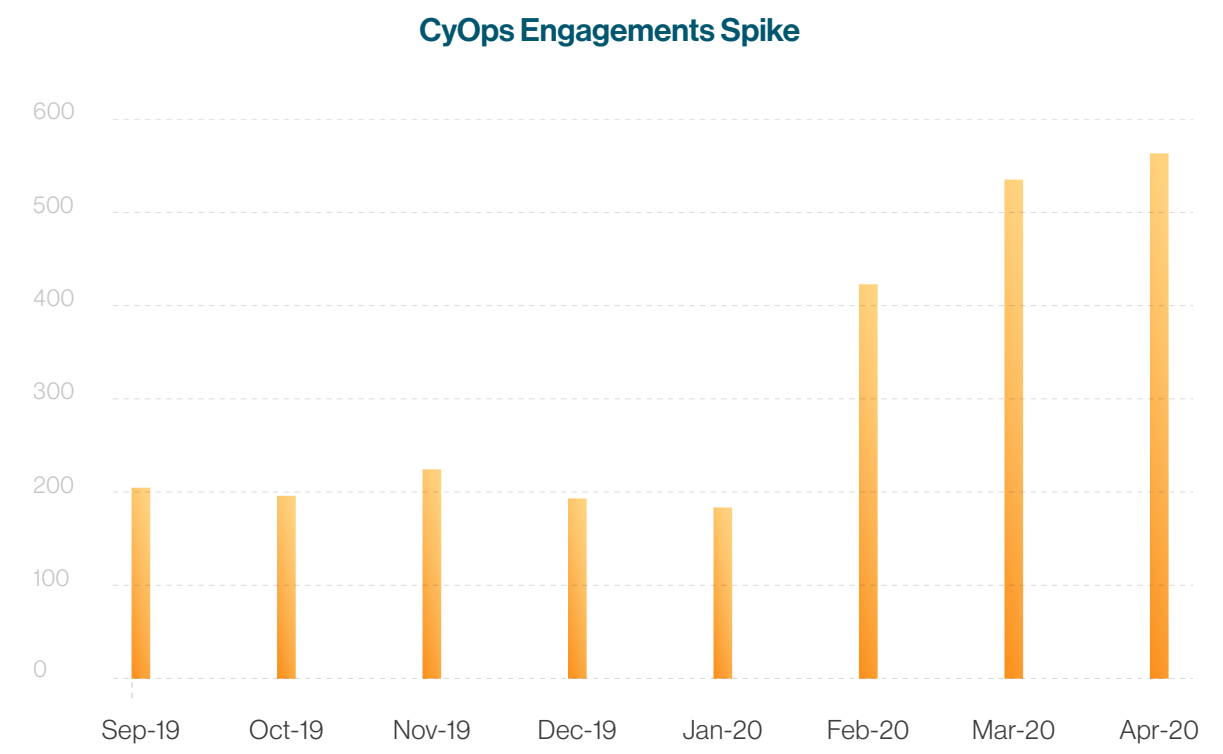


Figure 3 CyOps engagements during September 2019 to April 2020, showing a sharp spike in CyOps engagements during the Coronavirus period (February 2020 – April 2020)

Based on our experience, mitigating new threat vectors require a combination of advance Extended Detection and Response (XDR) and deep cybersecurity skills. Virtually all clients have increased their engagement with the CyOps 24/7 service team for their high level of expertise during the Covid-19 pandemic. CyOps oversight and advice is included in the Cynet offering.

CYBER ATTACK TRENDS ACROSS INDUSTRY SECTORS

Throughout the Coronavirus pandemic period, our analysts witnessed an increase in cyberattacks on most of our customers. In Figure 6, compares the number of attacks during the Covid-19 outbreak to the prior three months for several industry sectors. Most markets exhibited an increase in attacks, with three sectors exhibiting and increase of over a 20%.

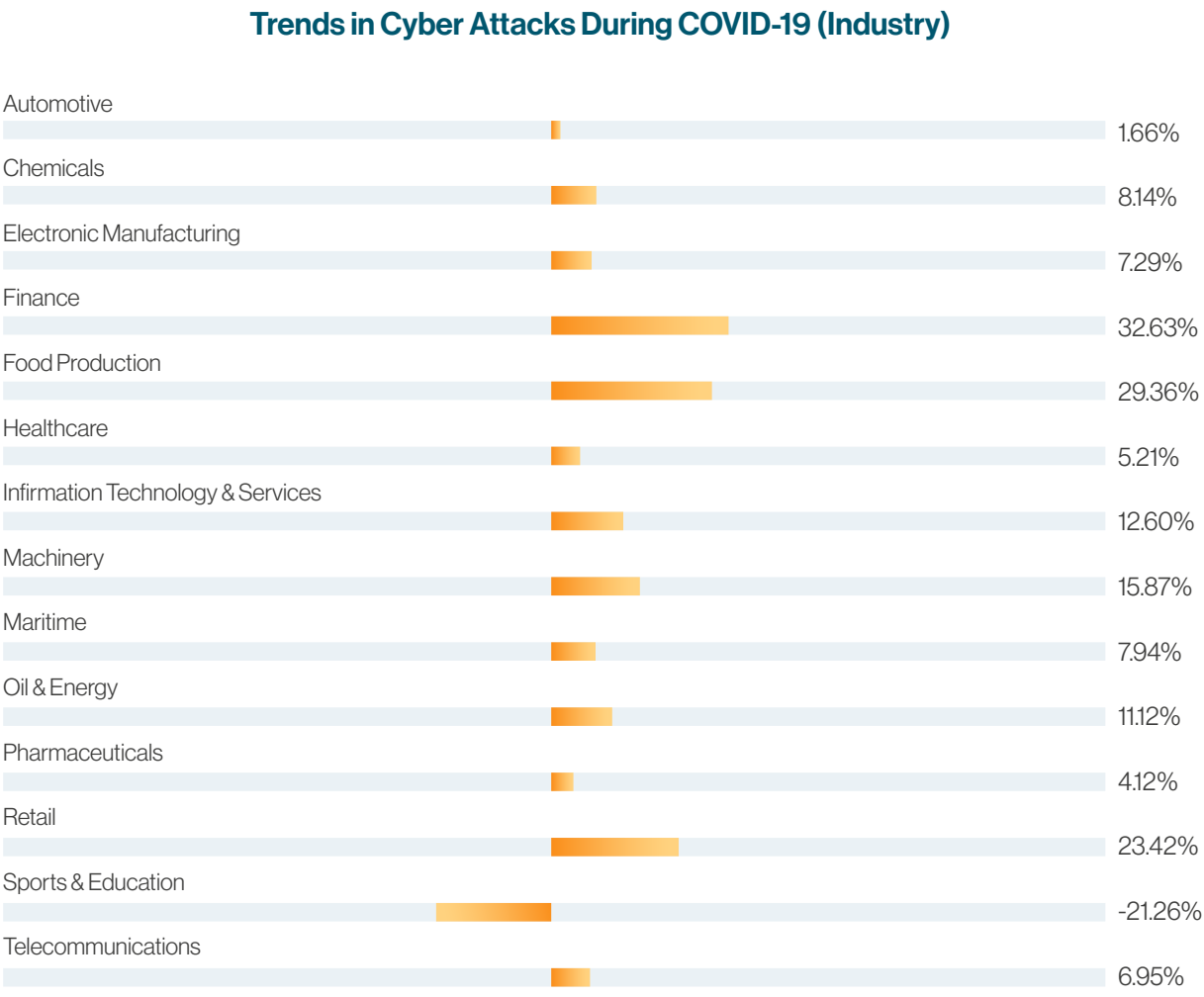


Figure 6 Trends in amount of cyber attacks during Covid-19 for different industrial sectors

INITIAL ACCESS VECTOR – SPEAR PHISHING

One of the areas our CyOps team found interesting was the increased use of spear phishing during the Covid-19 pandemic. Spear phishing is commonly used as an initial access vector for malware distribution. This attack involves an email sent to the client, masquerading as an innocent email from a seemingly trusted source. These emails often contain malicious attachments in several different forms, such as:

- Weaponized office document containing a Macro script which can execute a script on the victim's host machine.
- Weaponized office document containing an exploit which utilizes a known or 0-day vulnerability in order to execute code on the victim's host.
- Containing a malicious executable as an attachment.
- Containing a link to a malware distribution site which can infect the victim's host machine.

Figure 4 shows the breakdown of the spear phishing attacks Cynet detected across our client base over the past year.

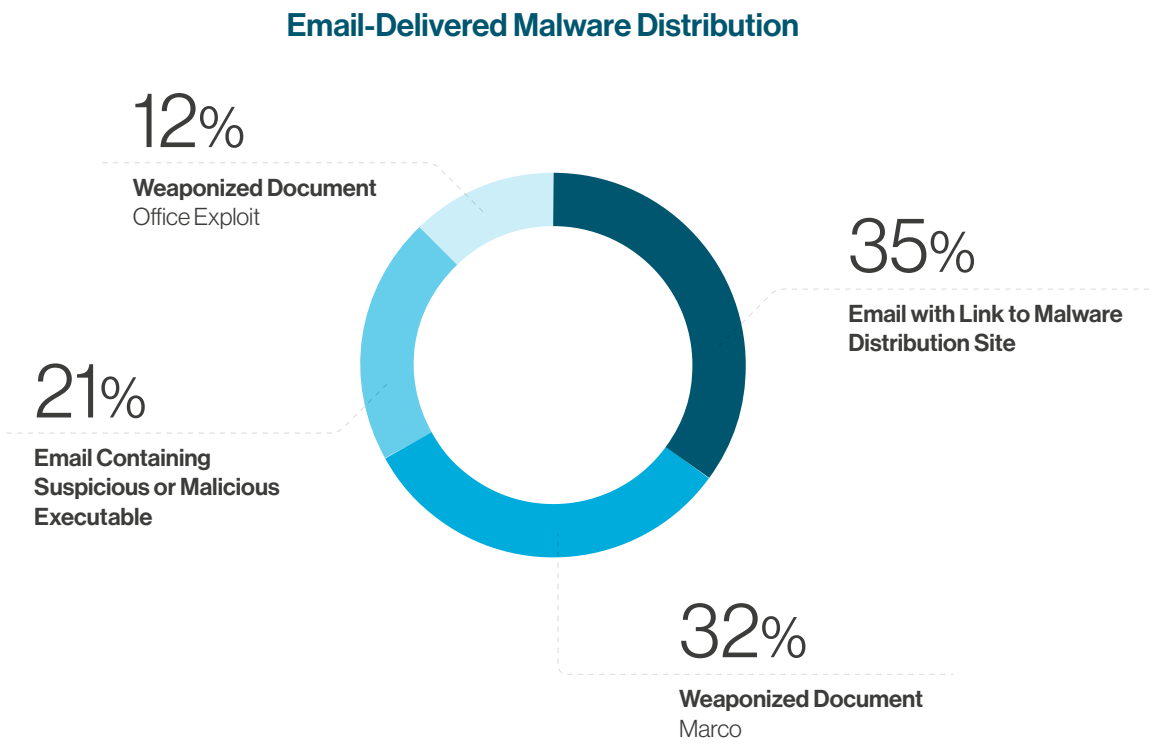


Figure 4 Spearfishing techniques used to achieve initial access to customer's network

An example of a spear phishing email containing a link that was sent to a Cynet customers is shown in Figure 5.

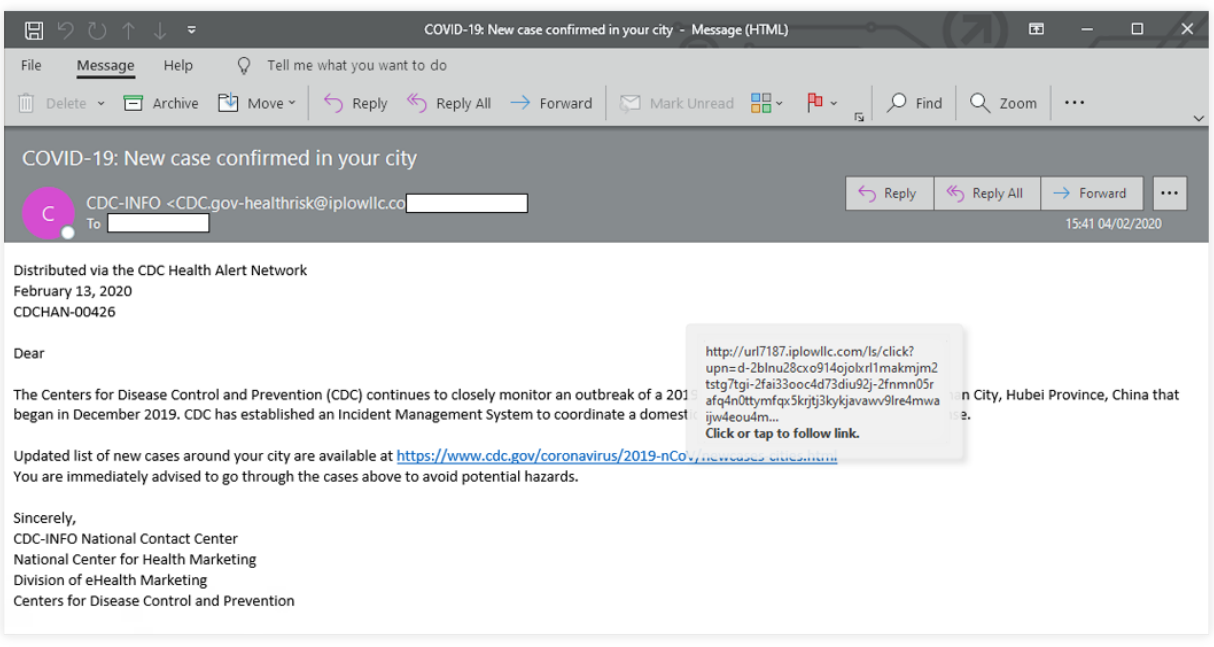


Figure 5 Spear Phishing email containing an archived file which contains a link to a malware distribution site

The suspicious email contains a link to a malware distribution site masquerading as an innocent link to the Center for Disease Control (CDC) website. Cynet has found a sharp increase in spear-phishing attacks relating to COVID-19 discussion topics. Based on our experience, once a spear-phishing attack is successful, a continuous attack effort is observed, such as escalation of privileges, data collection or lateral movement between hosts in the infected network. The most effective way to deal with this kind of attack is a combination of advance detection and prevention capabilities along with automated response and remediation. The volume of attacks along with the complexity of compromise requires a strong and instantaneous response that can fully uncover and mitigate all aspects of an advanced attack.

CONCLUSION

Cyber-criminals are leveraging the distraction of the Covid-19 global health pandemic to push new malware and increase spear phishing attacks across North America and Europe. An increase in attacks was observed across most industries, particularly Finance, Food Production, Retail and Machinery. New malware cannot be effectively prevented and detected using traditional antivirus and EDR solutions. Detecting and mitigating new threat vectors requires a combination of more advanced XDR solutions and deep cybersecurity expertise. Leveraging the Cynet XDR platform, along with CyOps (24/7 MDR service) allows Cynet clients to more effectively protect their environments during the Covid-19 era.

ABOUT CYNET

Cynet 360 is the world's first Autonomous Breach Protection platform that natively integrates XDR attack prevention and detection capabilities with automated investigation and remediation, via a single lightweight agent with zero operational effort. Cynet 360 technology is complemented by a 24/7 MDR service, placing end to end breach protection within reach for any organization regardless of its security team size and skill.