**[How CISOs Should Prepare for Coronavirus Related Cybersecurity Threats](https://thehackernews.com/2020/03/coronavirus-cybersecurity-ciso.html)**

March 18, 2020[The Hacker News](https://thehackernews.com/p/authors.html)

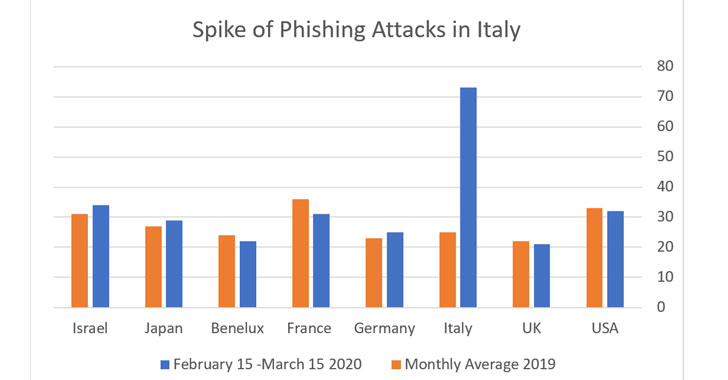
[](https://1.bp.blogspot.com/-eJz4TzZiKl8/XnI31FIGoDI/AAAAAAAAARw/_t6uHsjLahsDpNcJeoqMSZdUAkZxUuQxQCLcBGAsYHQ/s728-e100/Coronavirus-cyber-attacks.jpg)

The [Coronavirus](https://www.who.int/health-topics/coronavirus) is hitting hard on the world's economy, creating a high volume of uncertainty within organizations.  
  
Cybersecurity firm Cynet today revealed new data, showing that the Coronavirus now has a significant [impact on information security](https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html) and that the crisis is actively exploited by threat actors.  
  
In light of these insights, Cynet has also shared a few ways to best prepare for the Coronavirus derived threat landscape and provides a solution ([learn more here](https://www.cynet.com/corona-cyber-effect/?utm_source=thn)) to protect employees that are working from home with their personal computers because of the Coronavirus.  
  
The researchers identify two main trends – attacks that aim to steal remote user credentials and weaponized email attacks:

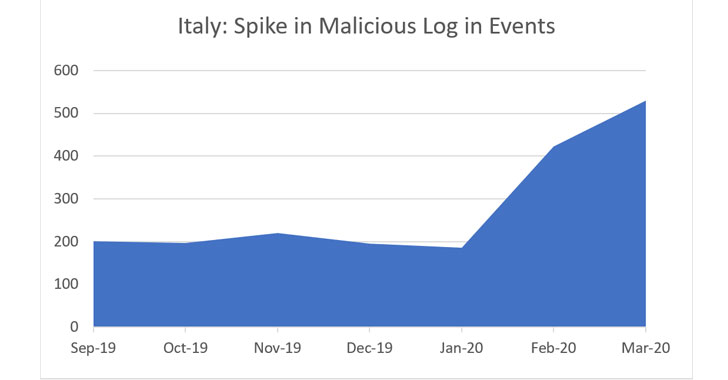
**Remote User Credential Theft**

The direct impact of the Coronavirus is a comprehensive quarantine policy that compels multiple organizations to allow their workforce to work from home to maintain business continuity.  
  
This inevitably entails shifting a significant portion of the workload to be carried out remotely, introducing an exploitable opportunity for attackers.

The opportunity attackers see the mass use of remote login credentials to organizational resources that far exceed the norm. As a result, remote connections are established by employees and devices that have never done so before, meaning that an attacker could easily conceal a malicious login without being detected by the target organization's security team.  
  
Cynet's global threat telemetry from the recent three weeks reveals that Italy features a sharp spike in phishing attacks in comparison to other territories, indicating that attackers are hunting in full force for user credentials.

[](https://1.bp.blogspot.com/-vqcrPcAq-no/XnI5R4H8eXI/AAAAAAAAAR8/UjyB9FhMn5gF9Tut1b_8ItwTN6h2aYClQCLcBGAsYHQ/s728-e100/Coronavirus-Italy.jpg)

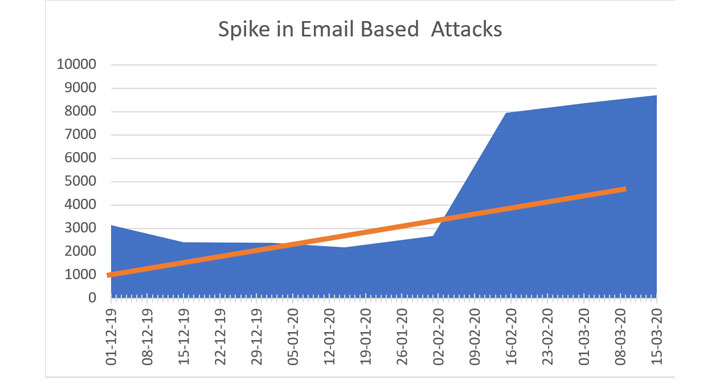
In addition, the researchers also detect a respective spike both in detected anomalous logins to its customers' environments, as well as in customers actively reaching out to CyOps (Cynet MDR) to investigate suspicious logins to critical resources.

[](https://1.bp.blogspot.com/-_wL83H9wjg0/XnI5tLreMoI/AAAAAAAAASE/oVcmCvnuwnAk0S5hz4WiZ9hb3OerAUXQACLcBGAsYHQ/s728-e100/coronavirus-in-italy.jpg)

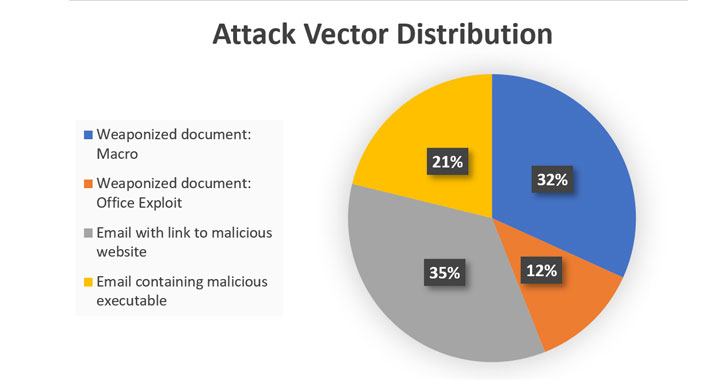
Correlating the two spikes validates that attackers are actively exploiting the Coronavirus derived havoc.

**Weaponized Email Attacks**

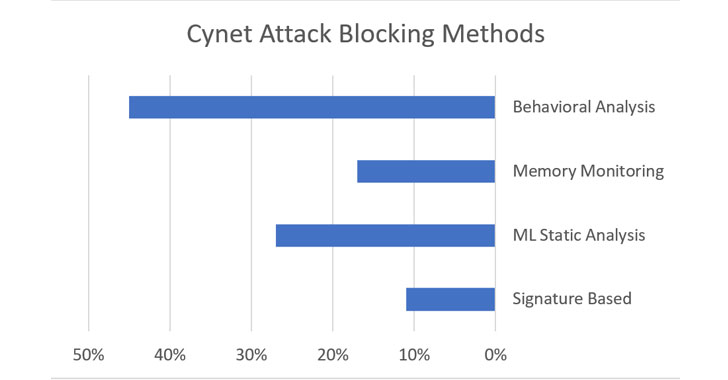
Employees that work from home often would do so from their personal computers, which are significantly less secure than the organizational ones, making them more vulnerable to malware attacks.  
  
Besides, Cynet released today's figures that support the above claim. Here is the double spike Cynet sees within its customers from Italy of email-based attacks:

[](https://1.bp.blogspot.com/-q2ptPMiKqDQ/XnI5-qQK7jI/AAAAAAAAASM/i34sQXEQNcMBmTb7mZ9wDfORyQCzTJL_QCLcBGAsYHQ/s728-e100/email-cyberattack.jpg)

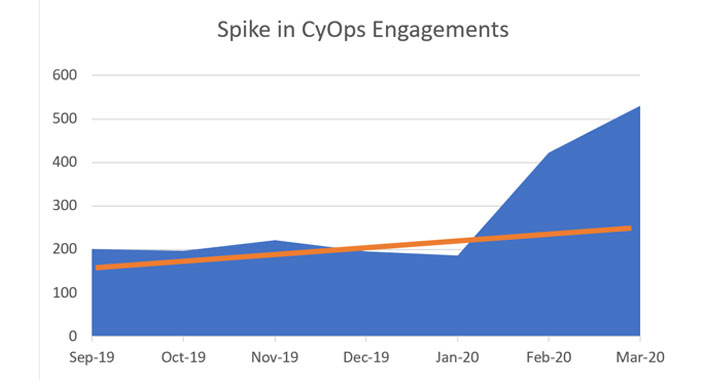
A closer look at the attacks reveals that they possess a considerable threat to organizations that do not have advanced protection in place:

[](https://1.bp.blogspot.com/-FpmBxU2uc8E/XnI6SJjNrZI/AAAAAAAAASU/CJiroRie6IQVjUz6JDDEnzquwD1tXqXOgCLcBGAsYHQ/s728-e100/email-malware.jpg)

While 21% of these emails featured simplistic attacks with a link to download a malicious executable embedded in the email body, the vast majority included more advanced capabilities such as malicious Macros and exploits or redirection to malicious websites – a challenge that surpasses the capabilities of most AV and email protection solutions.  
  
Taking a closer look at how these attacks were blocked verifies that they should be regarded as a severe risk potential:

[](https://1.bp.blogspot.com/-m6XuwjtVYKA/XnI6nefXHeI/AAAAAAAAASc/uuOqNnBIDNMynTXB088DSBf5kGBcH_K3gCLcBGAsYHQ/s728-e100/cyber-attack-protection.jpg)

'The fact that only about 10% of the malware in these attacks was identified by its signature, indicates that the attackers behind these campaigns are using advanced attacking tools to take advantage of the situation', says Eyal Gruner, CEO, and Co-Founder of Cynet.  
  
Moreover, there is another aspect to the Coronavirus impact. In many cases, the functioning of the security team itself is impaired due to missing team members in quarantine, making the detection of malicious activity even harder.  
  
From conversations with these companies, it turns out that the operations of many security teams are significantly disturbed due to quarantined team members, causing them to use Cynet's MDR service more often to compensate for the lack of staff.

[](https://1.bp.blogspot.com/-VKOu6aETLvU/XnI65LJGXmI/AAAAAAAAASk/r8r9Hty40gcCQ078kDEC5UztPHHAKj4OgCLcBGAsYHQ/s728-e100/cyberattacks.jpg)

'We have reached out to our customers in Italy ', says Gruner, 'and they have confirmed that a significant part of their workforce works from home these days.'  
  
To sum up the situation in Italy, employees working from home, security teams that are not fully operational and general atmosphere of uncertainty, create ideal conditions for attackers that seek to monetize the new situation through phishing, social engineering, and weaponized emails.  
  
The data from Cynet's Italian install base should serve as an illustrative example of the cyber effect in a territory where Coronavirus has a high prevalence. While this is not yet the case for other countries, the rapid Coronavirus spread implies that the cyber threat landscape in Italy would soon be duplicated in other geolocations as well.  
  
In order to efficiently confront these threats, CISOs should evaluate the defenses they have in place and see whether they provide protection against phishing and malicious logins.  
  
As a breach protection platform, Cynet introduces a dedicated offering tailored to the new Coronavirus related cyber risks.  
  
For both existing and new customers, Cynet will allow, free of charge (for 6 months), the deployment of its product, Cynet 360, on personal computers used by employees working from home.  
  
Cynet massively adds staff to CyOps, its MDR services team, to be able to cover for companies with reduced security staff because of the Coronavirus.