Coronavirus update: not the type of CV you're looking for

By gmcdouga

Published: 2020-06-04 · Archived: 2026-04-10 02:05:36 UTC

- Criminals are using malicious CV and medical leave forms to spread banking Trojans and infostealers
- Overall cyber-attacks up 16% compared to March and April, as businesses start to re-open
- Covid-19 related cyber-attacks during May decline 7% compared to April

At the end of May, CNN reported that more than 40 million Americans have filed for first-time unemployment benefits since the coronavirus pandemic put the US economy on hold in March. In fact, 1 in 4 Americans have filed for unemployment during the pandemic – the highest the country has had in its history, surpassing even the era of the Great Depression in the 1930s.

We previously reported that because of high unemployment rates, people became vulnerable to scams and phishing attacks involving relief package payments. We found that in May, 250 new domains containing the word "employment" were registered. 7% of these domains were malicious and another 9% suspicious.

Under the guise of CVs and Medical Leave forms

We have seen an increase in CV-themed campaigns in the US, and their ratio – out of all malicious files identified – doubled in the last two months with 1 out of every 450 malicious files being a CV-related scam.

Recently, we discovered a malicious campaign using the Zloader malware to steal victims' credentials and other private information. Zloader malware is a banking Trojan and a variant of the infamous Zeus malware that specifically targets customers of financial institutions.

Malicious .xls files with file names indicating they are individuals' CVs were sent via email with subjects such as "applying for a job" or "regarding job". When opening the attached file, victims were asked to "enable content" (see image below) and when they did, a malicious macro started running, downloading the final payload. Once a device was infected, threat actors could use the malware to carry out financial transactions on the device.

In the United Kingdom and Romania, some companies received an email that looked like this:

The emails came with the subject "CV from China" and contained an ISO file (CV.iso) that dropped a malicious EXE file (CV.exe) that would run an Info-stealing malware on the user's machine.

Campaigns that use CVs as an attack vector aren't the only ones taking place. We also discovered a campaign using Medical Leave forms that delivered the Icedid malware, a banking Trojan that steals users' financial data.

Malicious documents with names such as "COVID -19 FLMA CENTER.doc" were sent via emails with subjects like "The following is a new Employee Request Form for leave within the Family and Medical Leave Act (FMLA)". The emails were sent from different sender domains like "medical-center.space" to lure victims into opening the malicious attachments.

A similar campaign delivered Trickbot, a dominant banking Trojan constantly being updated with new capabilities, features and distribution vectors, allowing it to be a flexible and customizable enough to be distributed as part of multipurpose campaign. In this campaign, the same FMLA theme is adopted, with the emails being sent from domains such as "covid-agency.space".

Malware attacks increase as organizations get back to business

We previously reported that while there was an increase in the number of coronavirus-related attacks, overall, there was a decrease in the total number of cyberattacks. In March, when the pandemic was at its peak, we saw a 30% decrease in malware attacks compared to January 2020. This was because many countries went into quarantine and most businesses and other organizations were shut as a result, greatly reducing the potential number of targets for attackers.

Now that the world is seeing some relief from the pandemic as a result of the quarantine measures, things have started to open up and businesses are running again and – guess what? – Cyber criminals are also ramping up their malicious activities. In May, we saw a 16% increase in cyber attacks when compared to the period between March and April, when coronavirus was at its peak. This was largely due to the increase in malware attacks.

Coronavirus-related attacks continue

In May, we witnessed an average of more than 158,000 coronavirus-related attacks each week. When compared to April, this is a 7% decrease.

New Coronavirus registered domains:

Over the past 4 weeks, 10,704 new coronavirus-related domains were registered. 2.5% of them were malicious (256) and another 16% (1,744) suspicious.

The graph represents data detected by Check Point's Threat Prevention technologies across networks, endpoints and mobile devices, stored and analyzed in ThreatCloud, the world's most powerful threat intelligence database.

Staying protected

To stay protected against these opportunistic attacks, remember these golden rules:

1. Beware of lookalike domains, spelling errors in emails or websites, and unfamiliar email senders.
2. Be cautious with files received via email from unknown senders, especially if they prompt for a certain action you would not usually do.
3. Ensure you are ordering goods from an authentic source. One way to do this is NOT to click on promotional links in emails, and instead, Google your desired retailer and click the link from the Google results page.
4. Beware of "special" offers. "An exclusive cure for coronavirus for $150" is usually not a reliable or trustworthy purchase opportunity. At this point of time there is no cure for the coronavirus and even if there was, it definitely would not be offered to you via an email.
5. Make sure you do not reuse passwords between different applications and accounts.

Also, organizations should prevent zero-day attacks with end to end cyber architecture, to block deceptive phishing sites and provide alerts on password reuse in real time. Check Point Infinity is effective because it combines two key ingredients: full convergence across all attack surfaces and all attack vectors, and advanced prevention that can tackle the most sophisticated zero-day phishing and account takeover attacks.
