Emotet strikes Quebec's Department of Justice: An ESET Analysis

By Gabrielle Ladouceur Despins

Archived: 2026-04-05 19:19:34 UTC

Cybercrime

The cyberattack, which affected 14 inboxes belonging to the Department of Justice, was confirmed by ESET researchers

16 Sep 2020 • , 6 min. read

ESET's team of malware researchers in Montreal, in collaboration with journalist Hugo Joncas, helped shed light on a cyberattack that affected the Quebec Department of Justice.

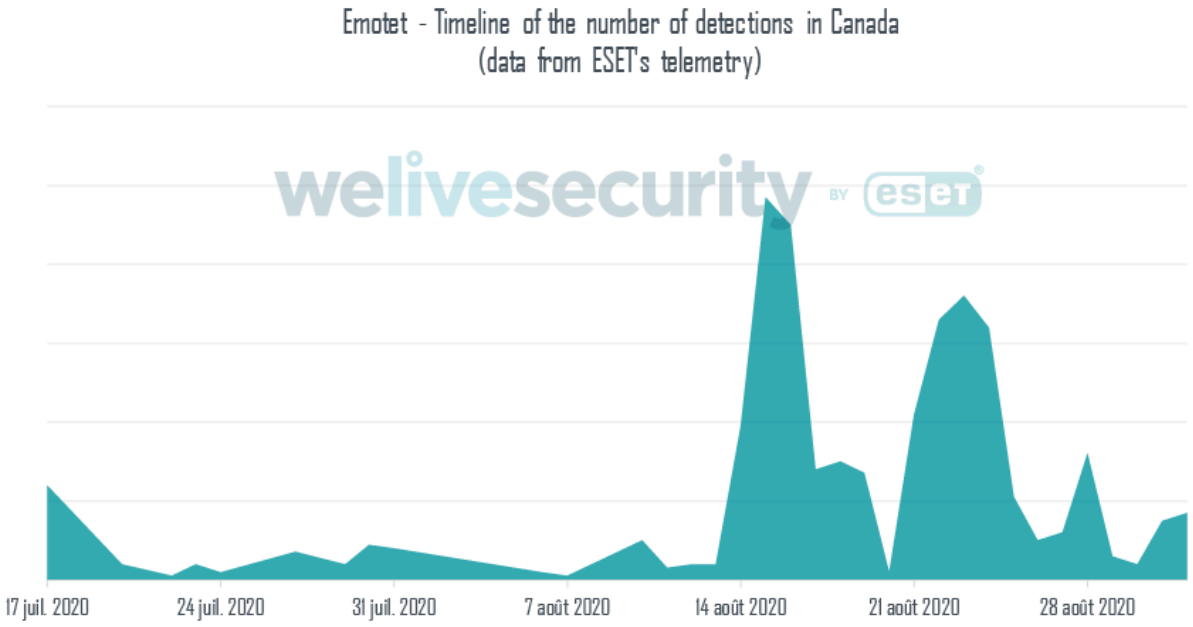
Indeed, on August 11 and 12, the Department of Justice suffered a cyberattack in which threat actors used malicious software to compromise 14 inboxes under the Department's jurisdiction. The attackers were thus able to access the emails addressed to these mailboxes. Alexis Dorais-Joncas (no relation), director of ESET's R&D office

in Montreal, reported that the hackers used a version of the Emotet malware, whose malicious campaigns have been running for several years.

In the case of this latest attack, the hackers used the stolen information to spread their malware in a particularly insidious manner. Cybercriminals sent seemingly legitimate messages to those who contacted the afflicted mailboxes, apparently originating from the Department, and included malicious attachments. "We have to assume that all messages sent to these accounts were stolen," says Dorais-Joncas.

In addition to the data of citizens who contacted the department, the union Syndicat de professionnelles et professionnels du gouvernement du Québec points out that "the hackers allegedly stole the personal information of approximately 300 active and inactive employees (retired or now working elsewhere). "

ESET telemetry shows a significant peak in Emotet detections in Canada during the month of August.



This corresponds to the period when the Department of Justice was targeted. Given the modus operandi of Emotet's campaigns, it is likely that other companies and organizations were also targeted.

A strategy in case of security incidents, an asset for your organization

This is a good time, as always, to develop or review your organization's strategy in the event of a security incident. Whatever the type of emergency, planning is your ally. Just like your fire plan, your security incident strategy will ensure a more effective and coordinated response when needed. And unlike your fire escape plan, when it comes to cyberattacks, the question is not whether you will use your plan, but when you will.

You may not think your organization would be a potential target for bad actors but think again. If you have electronic data, it has value to cybercriminals, regardless of your organization's size, industry or revenue.

According to Dorais-Joncas: "The incident at the Department of Justice is a reminder to all organizations dealing with personal data. An information leak is not always the result of a targeted and sophisticated attack. Indeed, the

simple act of opening a malicious attachment can lead to the theft of the entire contents of the email inbox. A prepared organization can quickly circumscribe the breach, identify the extent of the damage and go into notification mode to warn people whose personal data has been compromised. "

RELATED READING: ***Now is the best time to craft your breach response***

Your security breach strategy should contain several important elements. Here are some key elements to include:

- The first step in your action plan should be to assess the extent of the attack. Don't just rely on intuition - or worse, magical thinking! - when it comes to determining this. There is no substitute for an analysis of the problem. Points to check include

- Which systems were affected and how?
- Were any data stolen? What types of data? Does it affect clients, staff, partners?

- Is the incident limited to certain devices only, or does it also affect sub-networks?
- Determine which key teams and individuals within the organization will be involved in this analysis.

- Then you will want to do business continuity planning. This is where transparent communication becomes essential. It's never easy to communicate with customers and employees to notify them of a data breach that threatens their data. Creating a response template now can help you focus your team's efforts on providing timely and accurate information. Your plan should include contacting potential victims regularly to keep them informed of the situation, rather than waiting until the survey is complete.
- If the cyber-attack is still ongoing, you will then need to develop an infestation contingency plan. This begins by isolating the material that you know has been compromised, following the first step in your strategy. Isolate the subnets, devices and systems that have been affected by the cyber-incident to prevent the problem from spreading throughout the organization. You will then be able to eradicate the attack, and make sure to remove the vulnerability(ies) that made the cyberattack possible. Also include passwords update or any access information that attackers might have had access to in your plan.
- After a data breach, companies often offer their customers enhanced security measures to help mitigate any damage that may have been caused. In the case of credit monitoring, it makes sense to offer it only after an attack. Plan for the steps your organization can take, both upstream and downstream, to protect the security and privacy of customers in the event of an attack.

- Test your plan regularly and prepare your analysis and response feedback. For example, in the case of Emotet's campaigns, this usually involves employees opening a message containing malicious content. Once the malware has been completely removed from the organization's systems, more in-depth cybersecurity training for all staff can prevent further compromise.

What if my personal information have been breached?

There is always concern if you suspect that you may have been the victim of a data breach like this. However, users who have contacted the Department by email do not have to wait to receive notification from the Department if one is forthcoming. Simple security measures, and increased attention, are your best allies.

Alexis Dorais-Joncas explains: "If you have exchanged emails with the Registries and Certification Branch of the Department of Justice in the past, you need to be even more vigilant than usual. If you receive an email that appears to be from the Department and contains an attachment, do not open it. Instead, contact the Department by telephone to confirm whether or not the communication is legitimate." These tips echo the Department's press release, which invites the public to contact their Client Contact Centre at 1-866-536-5140 (option 4) for any inquiries regarding this incident.

RELATED READING: Would you get hooked by a phishing scam? Test yourself

If you are concerned that your personal information may have been stolen as part of this Emotet campaign, or as a result of another security incident, here are some tips to follow.

- Spam campaigns such as Emotet's are transmitted through malicious attachments. Never open an attachment or hyperlink from a source you do not know. Even if the message seems urgent or a priori legitimate, pay attention to details such as the source address, mistakes, or quick action notices.
- Visit Have I Been Pwned. This service allows users to check if an email address has been stolen and is on an email and password list available online. This database is regularly updated and includes emails and passwords that have been stolen recently. Keep in mind, however, that the absence of your address or passwords does not imply that your data has not been affected. They could indeed appear on a list that is not registered by the site.
- Speaking of passwords, be sure to use secure and separate passwords - or passphrases - for each of your accounts. Also change any passwords that have been potentially compromised. If you are concerned that you may have opened a malicious attachment, change the password associated with your email.
- Pay attention to any suspicious situation, on all of your accounts. Also pay special attention to transactions made on your behalf. Following a major security breach, many organizations will offer you a credit verification service. And actually, this is what the Department decided, as they committed to offering this service to the victims of this breach.

Source: https://www.welivesecurity.com/2020/09/16/emotet-quebec-department-justice-eset/