Evolution of Emotet: From Banking Trojan to Malware Distributor

By The Hacker News

Published: 2020-11-19 · Archived: 2026-04-05 18:46:20 UTC

Emotet is one of the most dangerous and widespread malware threats active today.

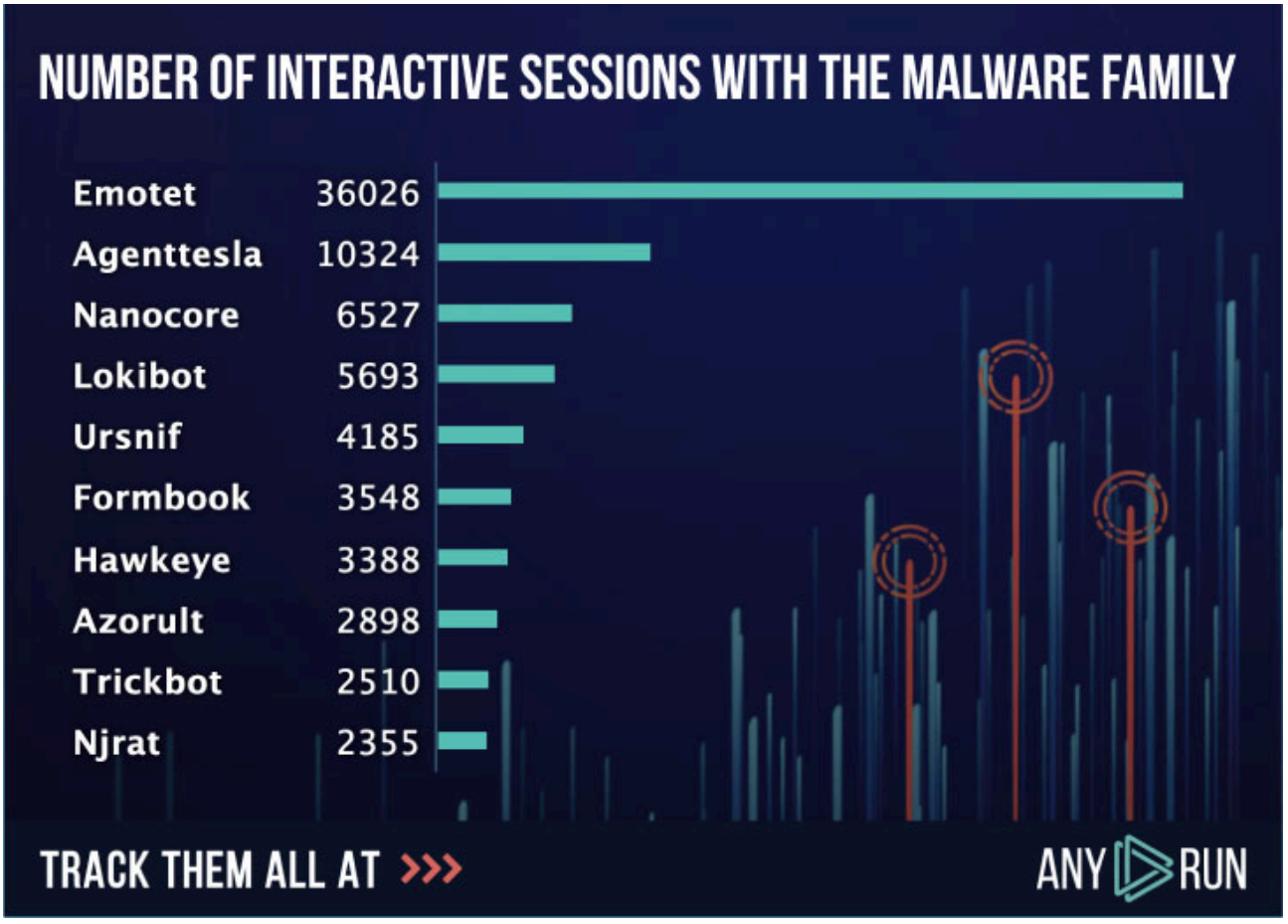
Ever since its discovery in 2014—when Emotet was a standard credential stealer and banking Trojan, the malware has evolved into a modular, polymorphic platform for distributing other kinds of computer viruses.

Being constantly under development, Emotet updates itself regularly to improve stealthiness, persistence, and add new spying capabilities.

This notorious Trojan is one of the most frequently malicious programs found in the wild. Usually, it is a part of a phishing attack, email spam that infects PCs with malware and spreads among other computers in the network.

If you'd like to find out more about the malware, collect IOCs, and get fresh samples, check the following article in the Malware trends tracker, the service with dynamic articles.

Emotet is the most uploaded malware throughout the past few years. Here below is the rating of uploads to ANY.RUN service in 2019, where users ran over 36000 interactive sessions of Emotet malware analysis online.



The malware has changed a lot over time, and with every new version, it gets more and more threatening for victims. Let's have a closer look at how it evolved.

When it was just like any other standard banking Trojan, the malware's main goal was to steal small companies' credentials, mainly in Germany and Austria. By faking invoices or other financial documents, it made users click on the links and let the malware in.

Later that year, it acquired a diverse modular architecture, whose primary focuses were downloading a malware payload, spreading onto as many machines as possible, and sending malicious emails to infect other organizations.

In early 2015 after a little break, Emotet showed up again. The public RSA key, new address lists, RC4 encryption were among the new features of Trojan. From this point, the victims' range started to increase — Swiss banks joined it. And overall, evasion techniques were improved a lot.

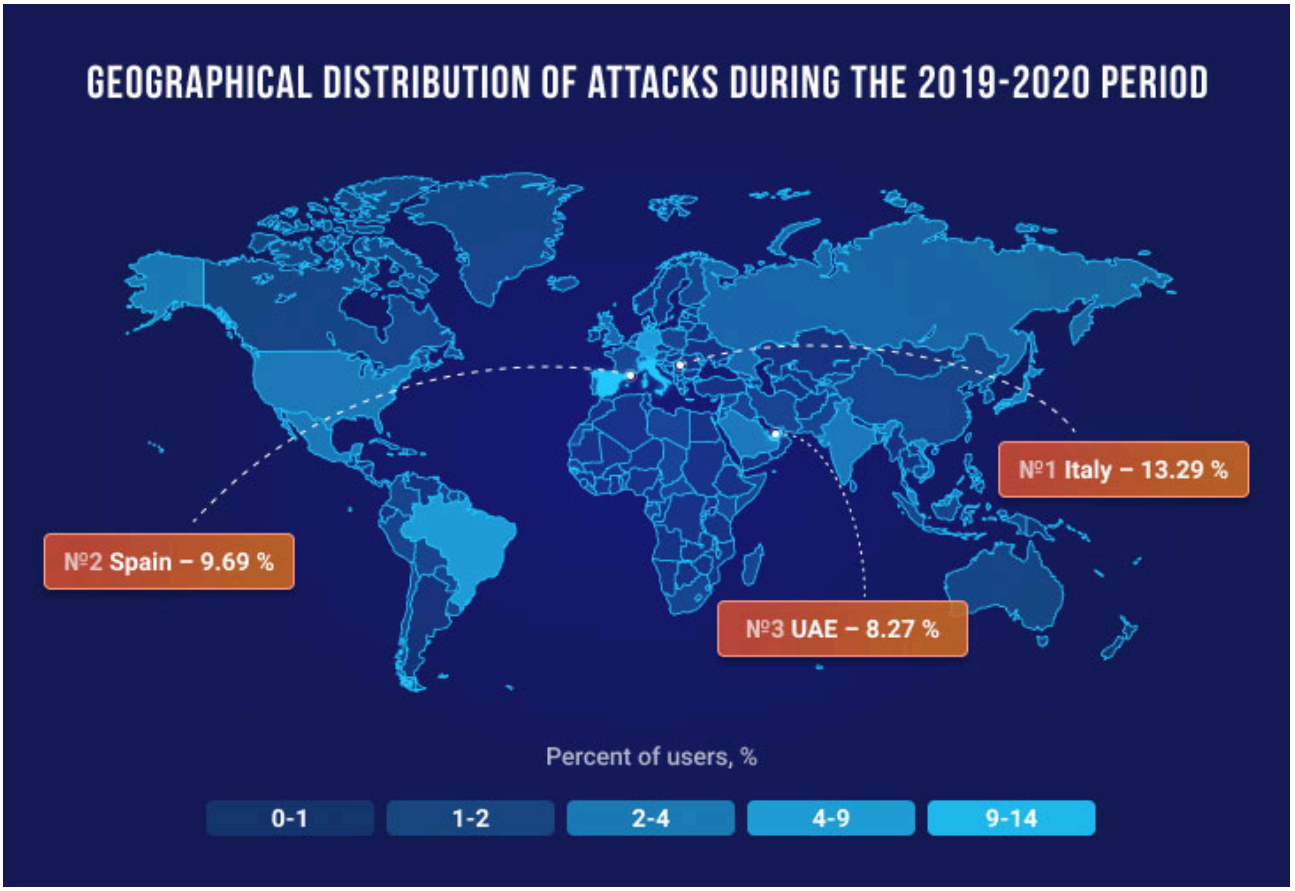
In recent versions, a significant change in the strategy has happened. Emotet has turned into polymorphic malware, downloading other malicious programs to the infected computer and the whole network as well. It steals data, adapts to various detection systems, rents the infected hosts to other cybercriminals as a Malware-as-a-Service model.

Since Emotet uses stolen emails to gain victims' trust, spam has consistently remained the primary delivery method for Emotet—making it convincing, highly successful, and dangerous.

For example, in 2018, the government system suffered an Emotet infection in Allentown, a city in eastern Pennsylvania, which cost them $1 million for recovery.

The whole city of Frankfurt had to shut down the network because of Emotet in 2019. Different kinds of organizations, from the government to small businesses, all public services were forced to stop their work via IT.

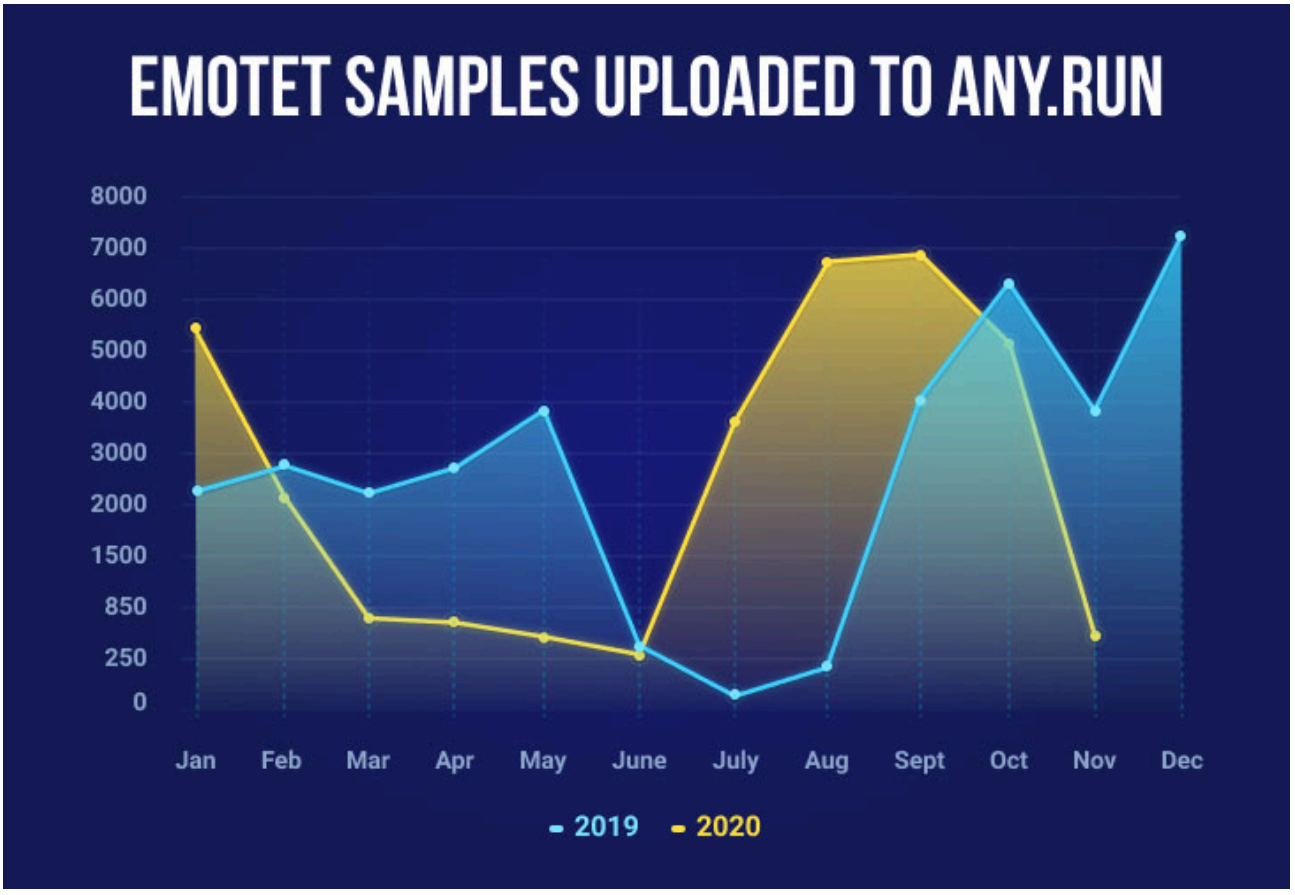
According to the latest research, Emotet is a worldwide threat that affects all kinds of spheres. Just look at the following map, Italy, Spain, and the United Arab Emirates are the top countries with the most attacked users.



Recently France, Japan, and New Zealand's cybersecurity companies have announced a rise in Emotet attacks targeting their countries.

Emotet then and now

According to a graph of the Emotet samples uploaded to ANY.RUN service, you can see the behavior of the malware in 2019 and 2020.



We can notice some similarities in its activity. For example, in June, Emotet tends to be on the decline. However, it seems to show an increasing trend from August till October. In 2019 the end of the year was very active for this kind of attack, so we can expect it to be on the rise this year as well.

Emotet has remained a threat for years as it changes permanently. Early versions differ from the current one, even by its intentions — Emotet has developed from the banking Trojan to the loader. When it comes to execution evolution and document templates, we will describe only versions that come after 2018. There were changes even over these two years, but the only thing that remains unchanged is delivery.

For distribution and user execution, Emotet is using malicious spam and documents with VBA macros. After a target downloads the attached malicious documents from an email and opens it, the Office document tricks the user into enabling the macro. After that, the embedded macro starts its execution, and subsequent scenarios may vary. The most common variant over the past years is that macros start a Base64 encoded Powershell script that later downloads an executable. But at this point, Emotet brings a lot of different executions.

Many variants come to its life when we talk about the initial steps after a maldoc was opened. VBA macro in Office documents can start cmd, Powershell, WScript, and, lately, for the first time, Certutil was used by the Emotet's execution chain.

Other changes in the execution process happened in the chain between malicious documents and dropped/downloaded executable files.

Not only has the execution chain transformed over time, but also the Emotet's executable file itself — registry keys, files, and child processes in the file system. For example, in the 2018-2019 years, Emotet dropped its executable at the folder under a particular path and generated a filename and the name of a folder using a particular algorithm.

It changed the file name generation algorithm, process tree, and path generation algorithm for C2 communication.

Another big part that characterizes this malware family is the maldocs' templates it uses. They are continually changing, and most of the time, Emotet uses its own ones. But between them can also be found templates that previously were used to distribute other malware families such as Valak and Icedid.

Emotet from the ANY.RUN's perspective

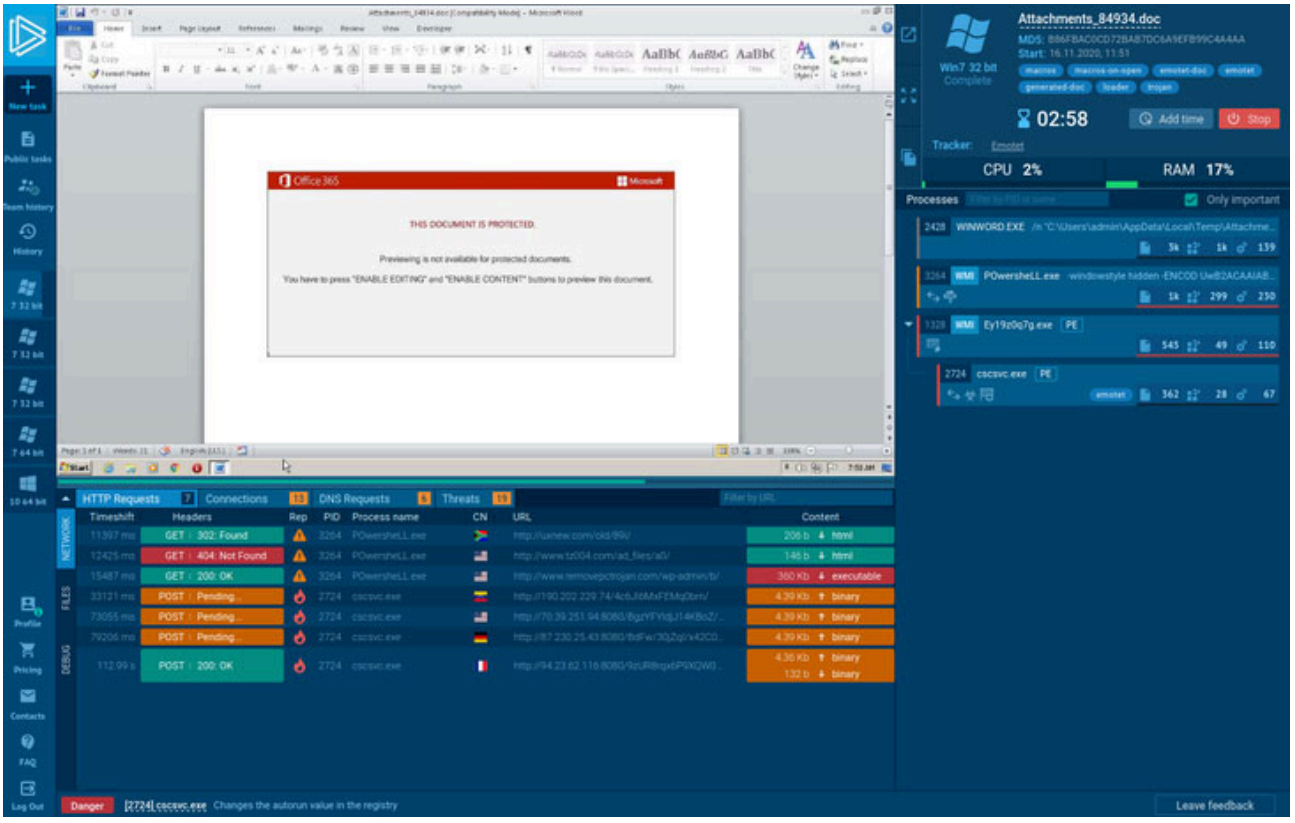
Of course, the main challenge with Emotet is to find a way to identify it and understand its behavior, so after that, you could improve the weak points in security.

There is a tool that can give you a hand with that. ANY.RUN is an interactive online sandbox that detects, analyzes, and monitors cybersecurity threats, necessary if you deal with Emotet.

Moreover, ANY.RUN has a special tool — the research of public submissions. It's a vast database where users share their investigations. And quite often, Emotet becomes the "hero" of the day: it has a leading position of the most downloaded samples into ANY.RUN. That's why ANY.RUN's experience with the malware is interesting.

The first step of protecting your infrastructure from Emotet infection is — detecting the malware. ANY.RUN sandbox has outstanding tools for Emotet detection and analysis.

The online service deals with Emotet regularly. So, let's try the interactive approach for Emotet detection and investigate one of the samples together:



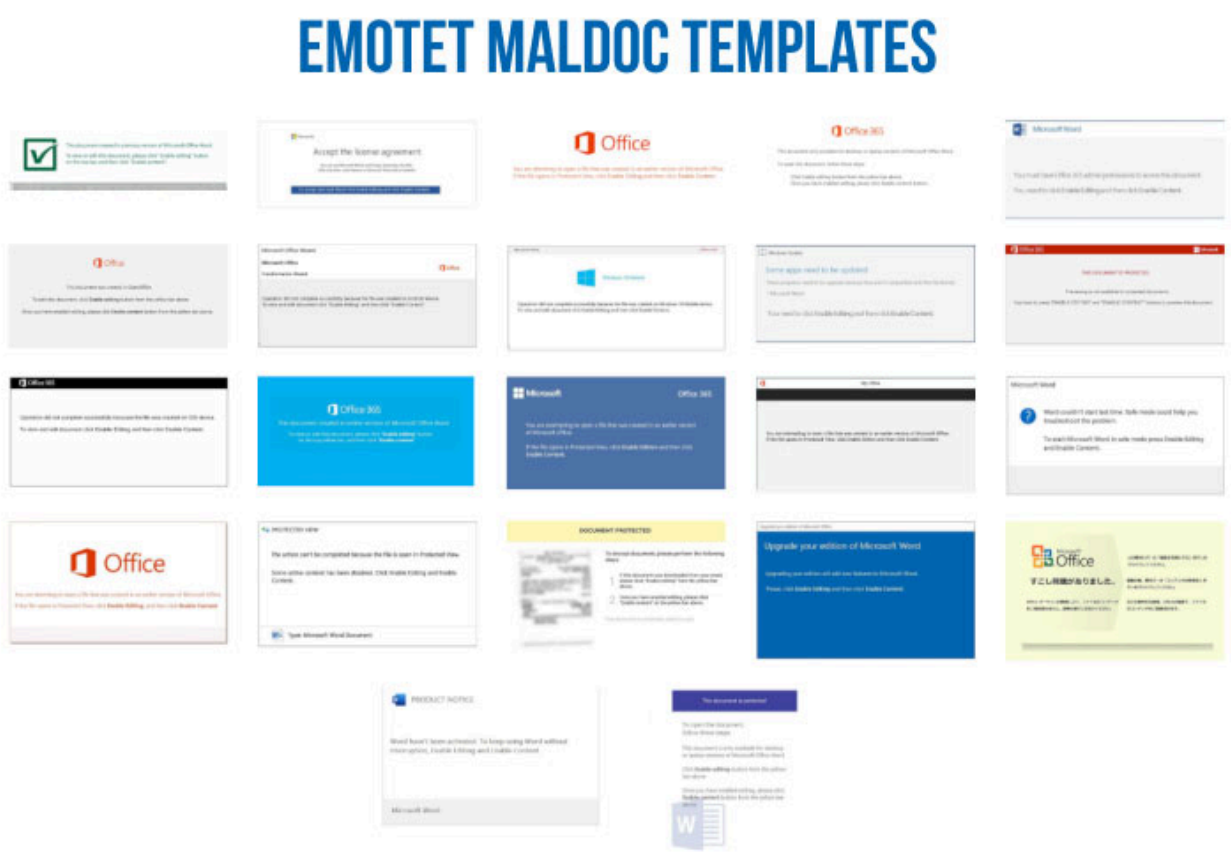
Here is a malicious attachment from the phishing email that we uploaded to ANY.RUN and immediately get the first results. The process tree on the right reflects all operations that were made.

As shown, the first process starts to create new files in the user directory. Then POwersheLL.exe connects to the network and downloads executable files from the Internet. The last one, winhttp.exe changes the autorun value in the registry and connects to the command-and-control server, both to retrieve instructions for subsequent malicious activities and exfiltrate stolen data.

And finally, Emotet was detected by network activity. Fresh Suricata rulesets from premium providers such as Proofpoint (Emerging Threats) and Positive Technologies are a big part of the detection process.

In addition, ANY.RUN offers a useful Fake Net feature. When turned on, it returns a 404 error that forces malware to reveal its C2 links that help collect Emotet's IOCs more efficiently. That helps malware analysts optimize their time as there is no need to deobfuscate it manually.

Interestingly, a set of malicious documents with the same template can have embedded VBA macro, leading to creating different execution chains. All of them have the main goal to trick a user who opened this maldoc to enable VBA macro.



If you'd like to take a look at all of those templates, just search by tag "emotet-doc" in ANY. RUN's public submissions — these maldocs are clustered by content similarity.

Conclusion

This kind of tendency proves that Emotet isn't going to give up or lose the ground. Its evolution showed that the malware develops very quickly and adapts to everything.

If your enterprise is connected to the Internet, the risks may be broader and deeper than you realize. That's why it's true that combating sophisticated threats like Emotet requires a concerted effort from both individuals and organizations.

Moreover, the goal of services like ANY.RUN is to be aware of such potential threats and help companies recognize malware early and avoid infections at any cost.

Analysis and detection with ANY.RUN is easy, and anyone can analyze a bunch of fresh samples every day.

What's more, the service is free to use and for downloading samples, and there is no doubt you can make use of ANY.RUN — just give it a try!

Found this article interesting? This article is a contributed piece from one of our valued partners. Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2020/11/anyrun-emotet-malware-analysis.html