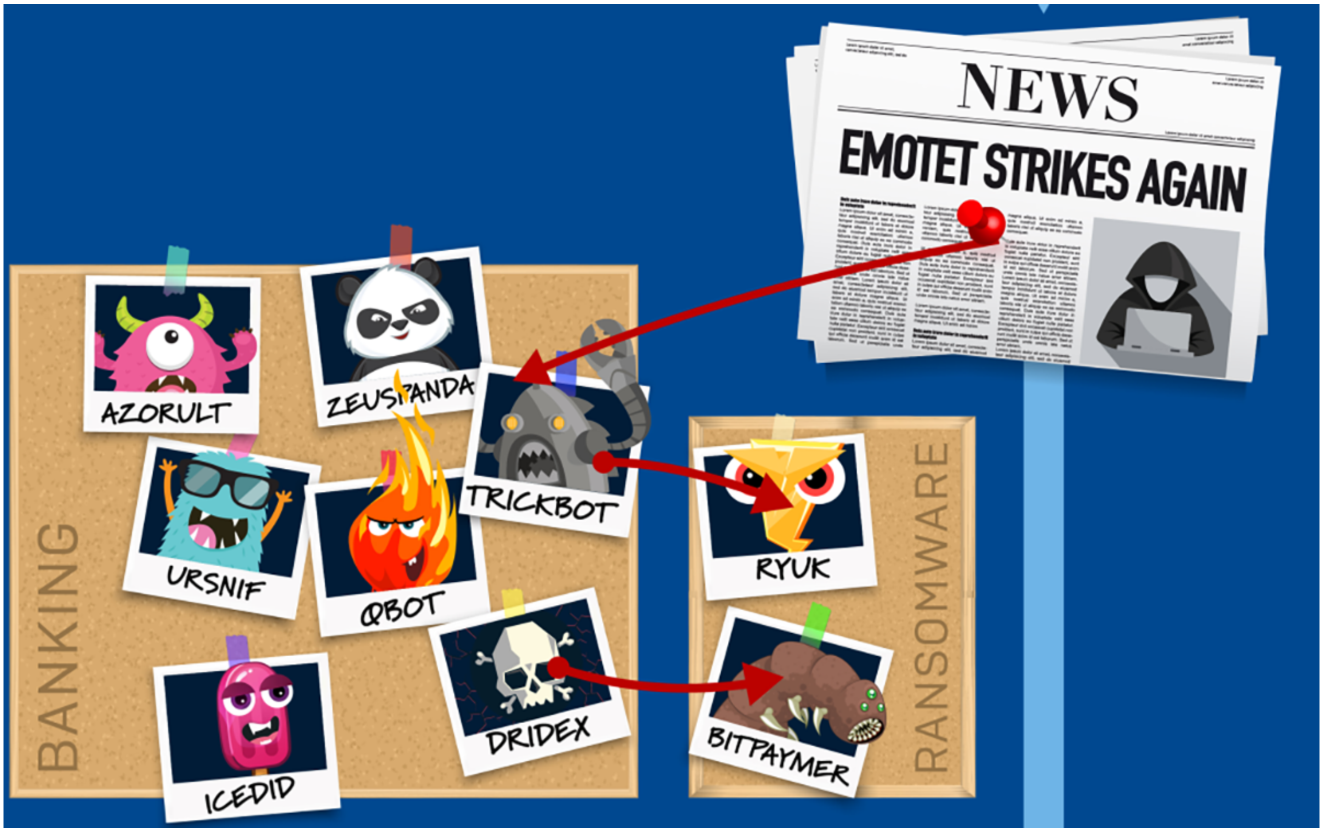
Emotet’s return is the canary in the coal mine

news.sophos.com/en-us/2020/07/28/emotets-return-is-the-canary-in-the-coal-mine/

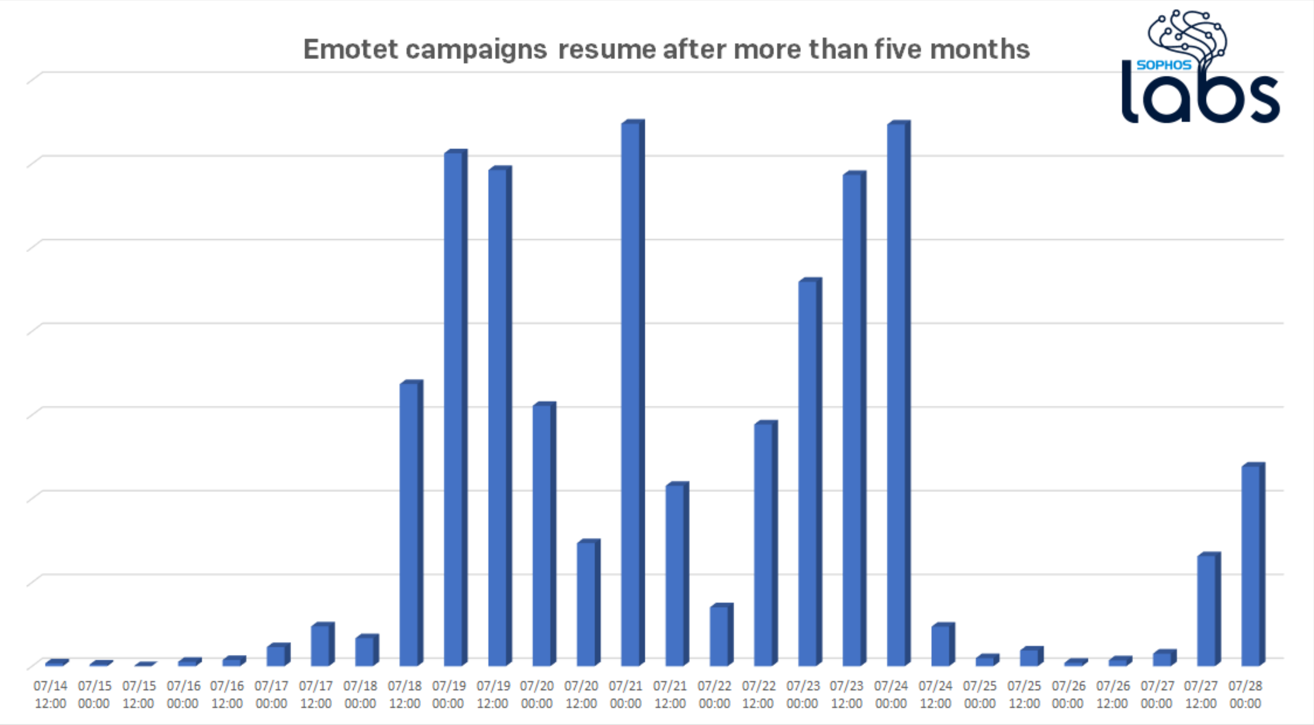
Andrew Brandt

July 28, 2020



In the past week, we’ve observed that one of the most prevalent, widely-distributed malware families in the world has reawakened after a prolonged absence. Emotet, the ubiquitous botnet that arrives in the guise of any of a thousand different bogus email messages, never really went away when it suddenly stopped appearing in our internal records and feeds of spam emails in February.

The sudden disappearance of the malware gave rise to a lot of rumors that the creators had been arrested, or contracted COVID-19, or simply had retired and planned to live the good life on the Black Sea coast. But these theories were squashed on July 17th, when we saw a new wave of Emotet attacks swing back into action.



Senior threat researcher and manager of the Abingdon, UK detection team, **Richard Cohen**, wrote this about its resurgence last week.

> We've talked a lot about Emotet in the past, including showing its malware ecosystem, and providing a series of deep-dive 101s, not forgetting showing the authors venting their frustration at Sophos. But then in February 2020, Emotet ceased production – its botnets stopped activity, and the waves of spam campaigns went silent. This isn't the first time it's vanished off the radar, only to rise again months later – and that's exactly what we saw again last Friday.

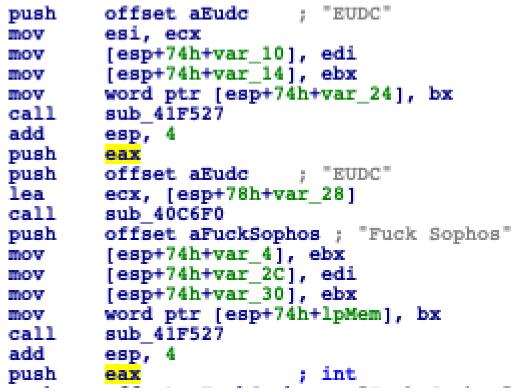
Unfortunately, Emotet is not merely a tool for thievery, but the botnet acts as a delivery mechanism for other malware, walking it through firewall over the encrypted channels it creates, bypassing network-based defenses.

As a result, we've investigated many, many cases in which a large-scale ransomware infection began as the result of this simple but effective Trojan lying undetected for a period of time, before the infected computer was used as a staging area for a larger attack against the company or organization on whose network it insinuated itself.

Richard goes on to write:

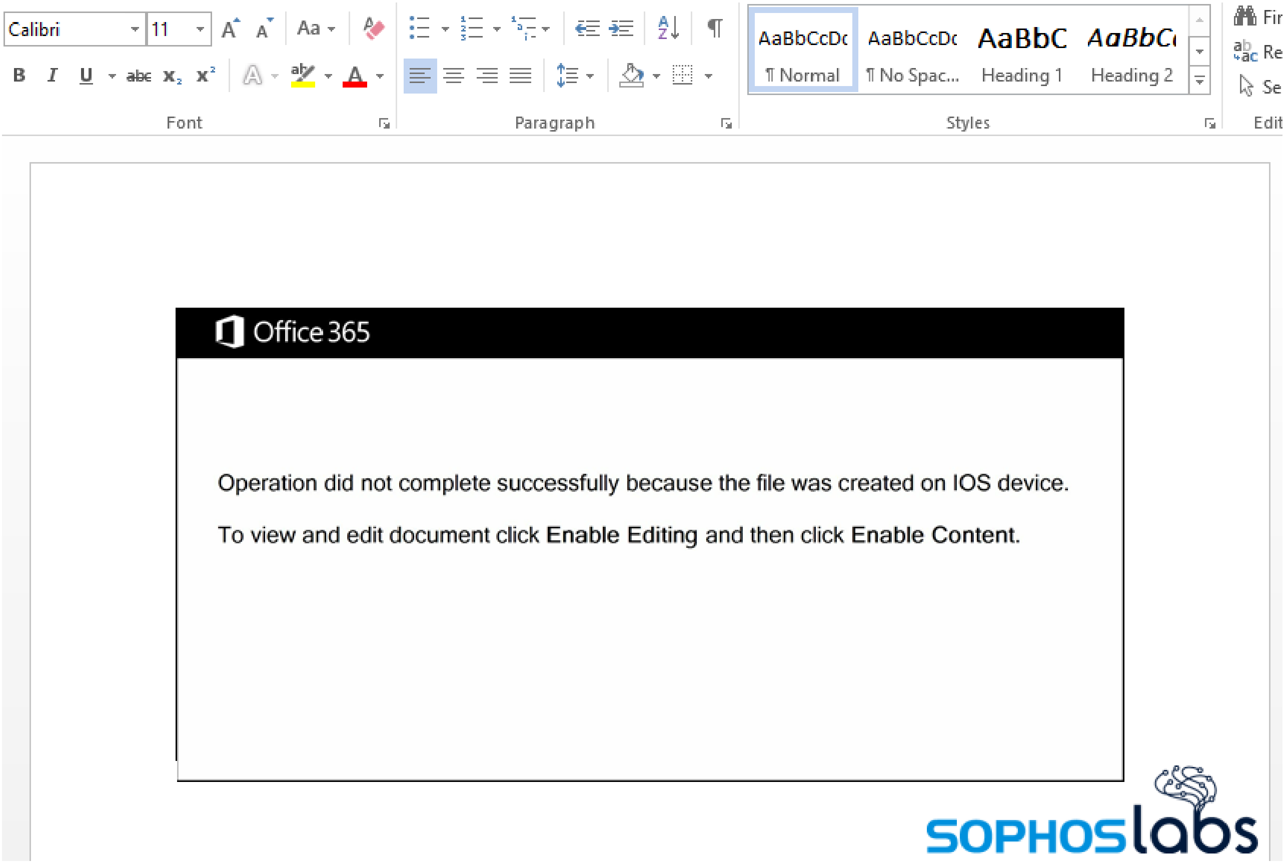
> Emotet's fundamental MO hasn't changed, as you can see from Microsoft Security Intelligence's tweets. And the protection SophosLabs has been building against different stages of these attacks remains strong.

These defenses work remarkably well. In fact, they work so well that the malware's creators added a small plaintext note to the source code letting us know just how much they appreciate Sophos' efforts at combatting their infections.



```
push    offset aEudc     ; "EUDC"
mov     esi, ecx
mov     [esp+74h+var_10], edi
mov     [esp+74h+var_14], ebx
mov     word ptr [esp+74h+var_24], bx
call    sub_41F527
add     esp, 4
push    eax
push    offset aEudc     ; "EUDC"
lea     ecx, [esp+78h+var_28]
call    sub_40C6F0
push    offset aFuckSophos ; "Fuck Sophos"
mov     [esp+74h+var_4], ebx
mov     [esp+74h+var_2C], edi
mov     [esp+74h+var_30], ebx
mov     word ptr [esp+74h+lpMem], bx
call    sub_41F527
add     esp, 4
push    eax              ; int
```

Others appear to be getting into the fight as well. For a short period of time over the past weekend, some researchers observed that payloads being accessed by Emotet had been replaced with animated GIFs on the compromised, legitimate servers the threat actor prefers to use for hosting payloads. To be sure, it was an interesting play, but ultimately futile, since the Emotet gang can read the tea leaves and see when they aren't getting the result they intended.



Operation did not complete successfully because the file was created on IOS device.

To view and edit document click Enable Editing and then click Enable Content.

The most recent versions of Emotet's malicious Office documents use Apple's iOS as an excuse to convince you to enable scripted content. **Don't do it!**

Regardless of the outcome, the Emotet gang has not changed their same, fundamental playbook they've followed for years. If you receive an email from an unknown source, or unexpectedly from a known source, with a Microsoft Office file attached, be extremely careful about opening it. In a related vein, if you receive an email that tells you to download such a file attachment in order to receive some sort of invoice or statement, be extremely suspicious.

In either case, check with the sender (if they are known to you) to ensure the file is legitimate **before** you open it. And if the document prompts you to enable advanced features like scripting, that's a huge red flag you should not ignore.

Detection

Sophos products detect Emotet or its components or payloads under a number of malware definitions:

- **Mal/DocDl-K** & **Mal/DocDl-L** on the initial document downloaders
- **AMSI/Exec-P*** on the behaviour of those downloaders
- **ML/PE-A*** from Deep Learning on the executable payloads
- **CXmal/Emotet-C** on those payloads seen in their malicious context
- **HPmal/Emotet-D** on the behaviour of those payloads
- We also have **Troj/Emotet-CJW** for Friday's wave of polymorphic payloads.

** available in Sophos Central Intercept X Advanced on Windows 10*