Emotet Botnet Takedown

hornetsecurity.com/en/threat-research/emotet-botnet-takedown/

Security Lab January 28, 2021

Summary

On 2021-01-27 it was announced by Europol that an international worldwide coordinated law enforcement and judicial action has disrupted the Emotet botnet and investigators have taken control of Emotet's infrastructure. If successful this could mean the end of Emotet, its botnet, malspam, and malware loader operation. While the situation is still developing, we can confirm that the Emotet botnet infrastructure is disrupted. Victims will be notified by responsible country CERTs and should take appropriate actions to clean their Emotet malware and secondary malware infections to prevent still active malware that was downloaded by Emotet to deploy ransomware.

Background

Emotet (also known as Heodo) was first observed in 2014. It was a banking trojan stealing banking details and banking login credentials from victims. But it pivoted to a malware-as-a-service (MaaS) operation providing malware distribution services to other cybercriminals. Today, Emotet is probably the most prolific malware distribution operation. To this end, it

steals the emails of its victims and replies to the victim's previous conversations. This is known as email conversation thread hijacking[5]. Hornetsecurity has written numerous blogposts about Emotet[2,3,4,5].

What happened?

An international worldwide law enforcement and judicial effort, coordinated by Europol and Eurojust, has disrupted the Emotet botnet. The following authorities took part in this operation:

- Netherlands: National Police (Politie), National Public Prosecution Office (Landelijk Parket)
- Germany: Federal Criminal Police (Bundeskriminalamt), General Public Prosecutor's Office Frankfurt/Main (Generalstaatsanwaltschaft)
- France: National Police (Police Nationale), Judicial Court of Paris (Tribunal Judiciaire de Paris)
- Lithuania: Lithuanian Criminal Police Bureau (Lietuvos kriminalinės policijos biuras), Prosecutor's General's Office of Lithuania
- Canada: Royal Canadian Mounted Police
- United States: Federal Bureau of Investigation, U.S. Department of Justice, US Attorney's Office for the Middle District of North Carolina
- United Kingdom: National Crime Agency, Crown Prosecution Service
- Ukraine: National Police of Ukraine (Національна поліція України), of the Prosecutor General's Office (Офіс Генерального прокурора).

The investigators obtained control over the infrastructure from one suspect located in Ukraine. Emotet's C2 communication has been sinkholed and information of connecting victims has been given to the responsible country CERTs, which will notify the victims so they can clean up the infection.

The Dutch National Police has also obtained a database containing e-mail addresses, usernames and passwords stolen by Emotet over the years. They provide a website to check whether an email address has been compromised at http://www.politie.nl/emocheck.

Emotet "uninstaller"

Additionally, German Federal Criminal Police (Bundeskriminalamt (BKA)) is distributing a Emotet remover program **from within the Emotet botnet** that will uninstall Emotet on 2021-04-25 at 12:00.

The program will create a timestamp for 2021-04-25 12:00 (note `tm_month` goes from 0 to 11, while `tm_day` goes from 1 to 31).

```
local_8 = DAT_1004c068 ^ (uint)&stack0xfffffffc;
emotet_uninstall_time.tm_year = 121;
emotet_uninstall_time.tm_mon = 3;
emotet_uninstall_time.tm_mday = 25;
emotet_uninstall_time.tm_hour = 12;
emotet_uninstall_time.tm_min = 0;
FID_conflict:__time64((__time64_t *)&stack0xffffffec);
_Time2 = __mktime64(&emotet_uninstall_time);
dVar3 = __difftime64(in_stack_ffffffec,_Time2);
if (dVar3 <= 0.0) {
  hObject = CreateThread(NULL,0,emotet_uninstall_thread,NULL,0,NULL);
  uVar4 = SUB81(dVar3,0);
  uVar2 = extraout_DL;
  if (hObject != (HANDLE)0xffffffff) {
    CloseHandle(hObject);
    uVar2 = extraout_DL_00;
  }
  FUN_100071b9(local_8 ^ (uint)&stack0xfffffffc,uVar2,uVar4);
  return;
}
emotet_uninstall();
pcVar1 = (code *)swi(3);
(*pcVar1)();
return;
}
```

2021-04-25

The program will spawn a thread that in a loop will sleep for 1000 minutes (16.6 hours) until the time to uninstall Emotet is reached.

```
void emotet_uninstall_thread(void)

{
  code *pcVar1;
  __time64_t uninstall_time;
  undefined auStack36 [4];
  double time_difference;
  undefined4 now;
  undefined4 local_14;
  uint local_c;

  local_c = DAT_1004c068 ^ (uint)auStack36;
  do {
    Sleep(60000);
    FID_conflict:__time64((__time64_t *)&now);
    uninstall_time = __mktime64(&emotet_uninstall_time);
    time_difference = __difftime64(CONCAT44(local_14,now),uninstall_time);
  } while (time_difference <= 0.0);
  emotet_uninstall();
  pcVar1 = (code *)swi(3);
  (*pcVar1)();
  return;
}
```

Once the time to uninstall Emotet is reached Emotet's registry key and its service are removed. The Emotet binary is moved to a temporary file path presumably to quarantine it for possible DFIR investigations on the infected system.

```
hSCManager = OpenSCManagerW(NULL,NULL,0xf003f);
if (hSCManager == NULL) {
  LVar4 =
  RegCreateKeyExW((HKEY)0x80000001,L"SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run",0,NULL,0,
  2,NULL,(PHKEY)&local_238,NULL);
  if (LVar4 == 0) {                                   Remove Emotet registry key
    emotet_tmp_path(shadowed) = FUN_10002e90(&local_234);
    RegDeleteValueW(local_238,(LPCWSTR)emotet_tmp_path(shadowed));
    hSCManager = (SC_HANDLE)local_238;
    goto LAB_10005e47;
  }
}
else {
  emotet_tmp_path(shadowed) = &local_234;
  if (7 < local_220) {
    emotet_tmp_path(shadowed) = local_234;
  }
  hService = OpenServiceW(hSCManager,(LPCWSTR)emotet_tmp_path(shadowed),0x10000);
  if (hService != NULL) {
    DeleteService(hService);                          Remove Emotet service
    CloseHandle(hService);
  }
LAB_10005e47:
  CloseHandle(hSCManager);
}
emotet_tmp_path(shadowed) = (undefined4 *)emotet_get_tmp_path((undefined2 *)local_268);
local_8 = CONCAT31(local_8._1_3_,1);
emotet_binary_path = (undefined4 *)emotet_get_emotet_path((undefined2 *)local_250);
emotet_tmp_path(shadowed) = FUN_10002e90(emotet_tmp_path(shadowed));
emotet_binary_path = FUN_10002e90(emotet_binary_path);
MoveFileW((LPCWSTR)emotet_binary_path,(LPCWSTR)emotet_tmp_path(shadowed));
FUN_10002ea0(local_250);
FUN_10002ea0(local_268);      Move Emotet to temporary folder
```

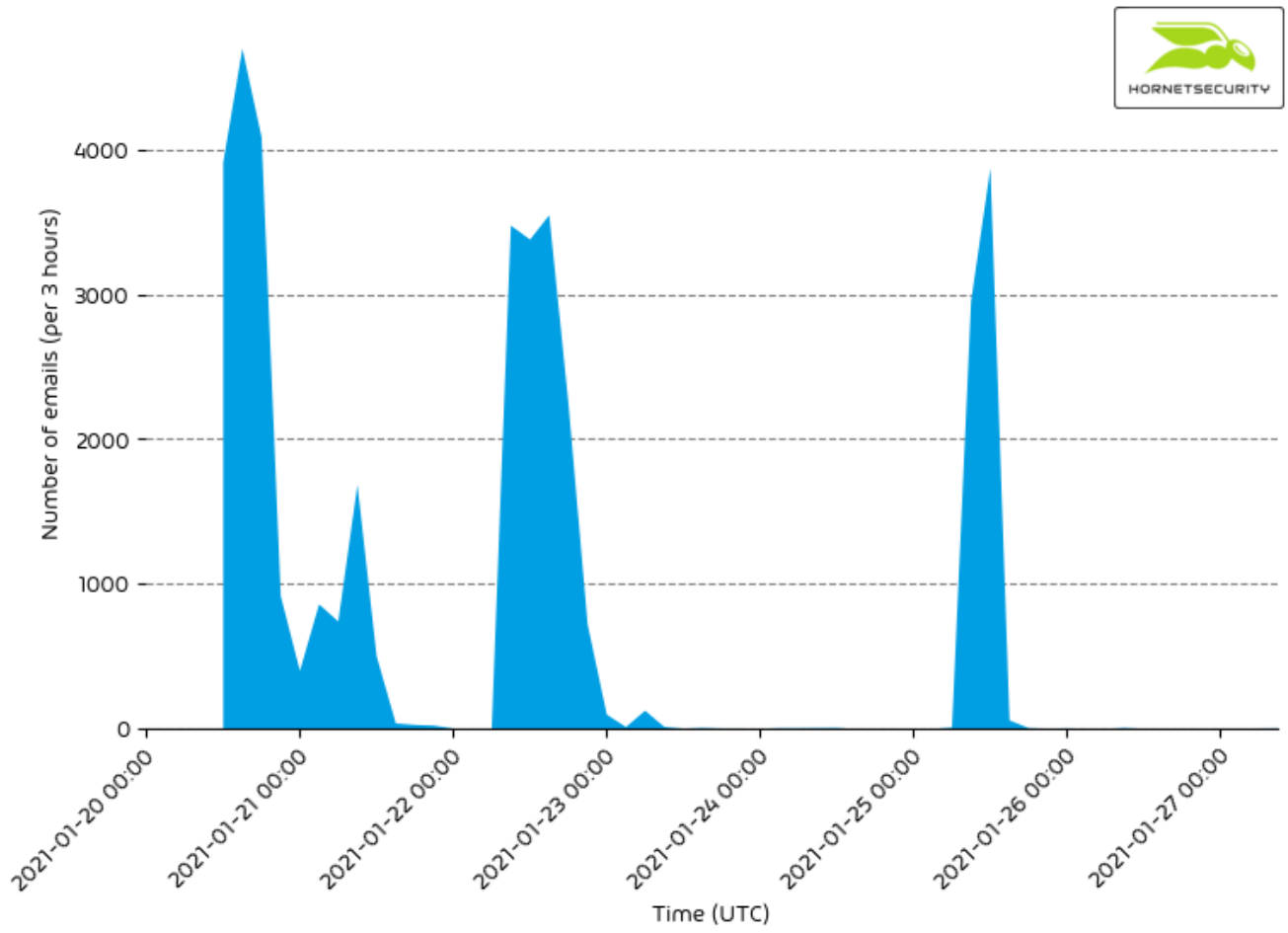
The likely reason why Emotet isn't removed immediately is to allow affected parties to run DFIR investigations to discover potentially secondary malware that was deployed via Emotet.

From our understanding the sinkholing and "uninstallation" actions are performed under the auspices of the German Federal Criminal Police (Bundeskriminalamt (BKA)), hence, the sinkhole IP addresses are owned by German ISP Deutsche Telekom.

What will happen next?

While our mail filters are still detecting sporadic emails containing malicious Emotet documents, these are likely emails that had still been lurking in queues either of the Emotet spambots or email systems and are just now being delivered even though the Emotet botnet

infrastructure has been disrupted.



We expect that these last drips of Emotet malspam dripping out of the dying Emotet botnet to dry out over the next days and weeks and if the takedown is successful stop entirely.

While there is always a chance that a botnet can regroup after a disruption (see TrickBot), this, however, seems unlikely in this case as not just the Tier 1 C2 proxy servers have been disrupted (as was the case with the disruption of the TrickBot botnet), but – from our information – also the Tier 2 C2 server, i.e., the real C2 server, to which the Tier 1 C2 proxy servers only relayed the traffic to, have been disruption as well.

Who will fill the void?

Emotet constituted around 20% of the malicious email traffic processed by Hornetsecurity. It distributed malware by other threat actors. While a successful takedown will mean no more Emotet malspam, it likely won't mean a decrease in malspam, as other threat actors will try to fill the void and take over the existing customer base of Emotet's malware-as-a-service (MaaS) operation.

One strong contender to fill the void generated by Emotet's disruption is QakBot[10]. Last year QakBot added email conversation thread hijacking[5] to its arsenal, i.e., like Emotet it steals emails from victims and crafts no tailored malspam by replying to existing email conversation threads. QakBot has also been observed loading other malware, such as ZLoader.[8] In addition to that, QakBot's XLM macro based malicious documents[7] often have a lower detection rate then Emotet's VBA macro base malicious documents. Thus, fulfilling all requirements a criminal would have towards an Emotet replacement.

Conclusion and Countermeasures

We congratulate all participating parties and hope for a successful longterm takedown of Emotet.

While Emotet itself may be inoperable, other threats Emotet has previously loaded such as TrickBot[6], QakBot[7], or Zloader[8] remain active and could still deploy ransomware such as Ryuk and Egregor. If the authorities inform you of an Emotet infection you must also clean up these possible secondary infects to mitigate the complete threat.

In case the Emotet botnet can recover, Hornetsecurity's Spam Filter Service and Malware Protection, with the highest detection rates on the market, will again, as before the disruption, detect and quarantine malicious Emotet documents.

References

- [1] https://www.hornetsecurity.com/en/security-information/email-conversation-thread-hijacking/
- [2] https://www.hornetsecurity.com/en/security-information/awaiting-the-inevitable-return-of-emotet/
- [3] https://www.hornetsecurity.com/en/security-information/emotet-is-back/
- [4] https://www.hornetsecurity.com/en/security-information/webshells-powering-emotet/
- [5] https://www.hornetsecurity.com/en/security-information/emotet-update-increases-downloads/
- [6] https://www.hornetsecurity.com/en/security-information/trickbot-malspam-leveraging-black-lives-matter-as-lure/
- [7] https://www.hornetsecurity.com/en/security-information/qakbot-malspam-leading-to-prolock/
- [8] https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader
- [9] https://www.hornetsecurity.com/en/threat-research/qakbot-distributed-by-xlsb-files/
- [10] https://www.hornetsecurity.com/en/threat-research/qakbot-reducing-its-on-disk-artifacts/
- [11] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

Indicators of Compromise (IOCs)

IPs

These are the IPs used by the German Federal Criminal Police (Bundeskriminalamt (BKA)) to sinkhole Emotet.

- `80.158.3.161:443`
- `80.158.51.209:8080`
- `80.158.35.51:80`
- `80.158.63.78:443`
- `80.158.53.167:80`
- `80.158.62.194:443`
- `80.158.59.174.8080`
- `80.158.43.136:80`

Hashes

This is the hash of the program distributed by the German Federal Criminal Police (Bundeskriminalamt (BKA)) to remove Emotet on 2021-04-25 at 12:00.

MD5	Description
`9a062ead5b2d55af0a5a4b39c5b5eadc`	Emotet “uninstaller”