Emotet Activity Identified

esentire.com/security-advisories/emotet-activity-identified

THE THREAT

As of November 15th, 2021, multiple sources [1] [2] have observed activity associated with the Emotet malware. This activity includes malware delivery through email and existing infections.

Successful Emotet payload execution has not been observed across customers at this time. The Threat Intelligence team assesses with medium confidence current campaigns are focused on re-establishing botnet infrastructure following law enforcement's action to take down the botnet in January 2021[3]. Email delivery techniques and payload execution remain consistent or similar to past Emotet infections. The eSentire Threat Intelligence team assesses, with medium confidence, Emotet's email campaigns will continue.

What we're doing about it

- eSentire MDR for Network and Endpoint have rules in place to detect Emotet.
- IP addresses associated with Emotet have been blocked via MDR for Network.
- Threat hunting has been performed for all eSentire MDR for Endpoint customers.
- eSentire security teams are tracking this threat for additional detection and prevention opportunities.

What you should do about it

Employ email filtering and protection measures

- Block or quarantine email attachments such as EXEs, Password Protected Zip archives, JavaScript, Visual Basic scripts.
- Implement anti-spoofing measures such as DMARC and SPF.
- Employ an MFA solution to reduce impact of compromised credentials.
- Train users to identify and report suspicious emails, including from trusted contacts.

Protect endpoints against malware

- Ensure antivirus signatures are up-to-date.
- Use a Next-Gen AV (NGAV) or Endpoint Detection and Response (EDR) product to detect and contain threats.
- Limit or disable macros across the organization. See UK's National Cyber Centre guidance on Macro Security

Additional information

Emotet is an information stealer malware that is also used for initial access by multiple threats such as Qakbot and Trickbot. Emotet has been previously observed leading to Ryuk, Conti, ProLock, and Egregor ransomware threats.

As of this writing, follow-on malware has not been observed in these latest campaigns. Emotet activity halted in early 2021, after law-enforcement acted against the Emotet threat and seized malicious infrastructure. Recent activity is believed to be focused on re-establishing botnet hosts.

Overview of November 15th to 17th 2021 Emotet Activity

Distribution

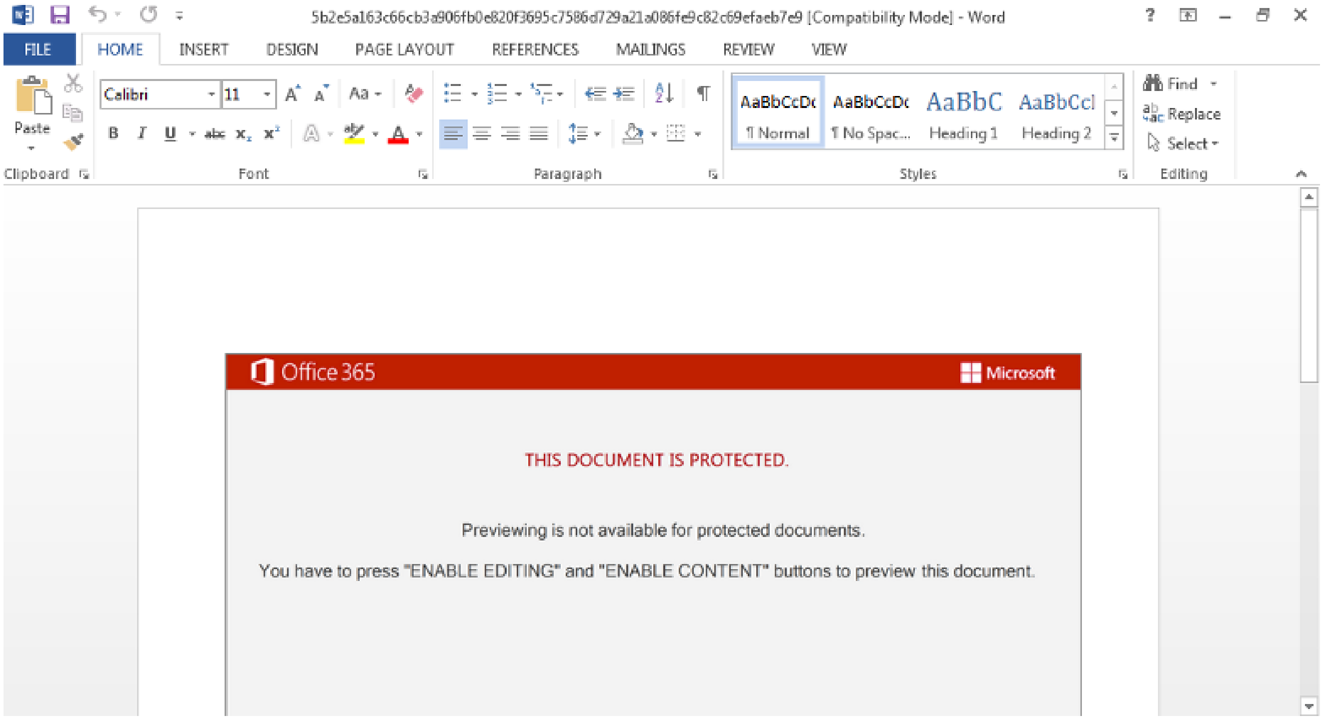
- Existing Trickbot Infections.
- Mass email delivery.

Emotet Email Content

- Spoofed replies to stolen email threads (email thread hijacking).
- Excel (.xlsm) attachments.
- Word (.docm) attachments.
- Password protected Zip archives containing malicious office documents.
- Links to malicious office documents.

Malicious Office Documents

- Use of standard lures to entice recipients to enable macros (see images below).
- Successful macros execution results in PowerShell commands to retrieve and execute payloads via rundll32.exe.
- No secondary payloads have been observed as of time of writing.

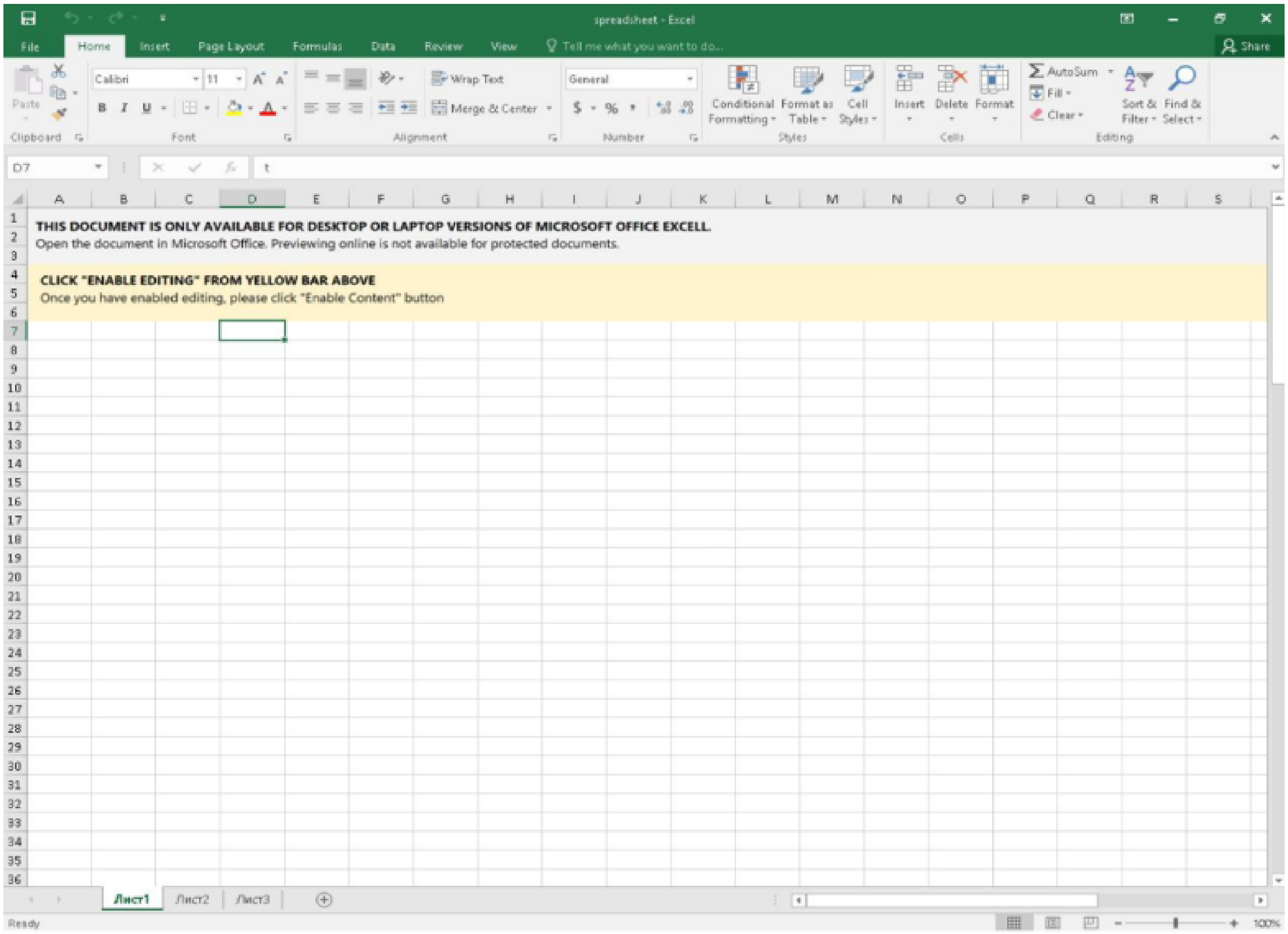


THIS DOCUMENT IS PROTECTED.

Previewing is not available for protected documents.

You have to press "ENABLE EDITING" and "ENABLE CONTENT" buttons to preview this document.

Figure 1: Malicious Word Document



THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCELL.

Open the document in Microsoft Office. Previewing online is not available for protected documents.

CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE

Once you have enabled editing, please click "Enable Content" button

Figure 2: Malicious Excel Document

A detailed breakdown of current infection scheme can be found here: https://isc.sans.edu/forums/diary/Emotet+Returns/28044/

References:

[1] https://isc.sans.edu/forums/diary/Emotet+Returns/28044/
[2] https://twitter.com/Cryptolaemus1/status/1460302706954981385
[3] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action