# EMOTET

# Descrizione e misure di contrasto

## Sommario

## Introduzione

Emotet, anche noto come Heodo, originariamente identificato come malware bancario strutturato in botnet, è un trojan modulare attivo sin dal 2014 che, negli anni, ha avuto una diffusione discontinua.

Da recenti rilevamenti, dopo un periodo di limitata attività, è emerso un incremento di attacchi finalizzati alla sua diffusione. Allo stato attuale, sia su scala globale sia in territorio italiano, rappresenta una delle famiglie malware maggiormente diffuse.

## Descrizione

La peculiarità di **Emotet** è quella di favorire la propagazione di altri malware, altrettanto pericolosi, scatenando un'infezione multipla. In questo meccanismo Emotet agisce da malware di primo stadio che si incarica, nelle fasi successive, di richiamare codice malevolo associato a trojan bancari, infostealer o ransomware. Di recente è stato osservato che le botnet Emotet rilasciano **Trickbot** per diffondere ransomware e il trojan **Qakbot** per la cattura di credenziali bancarie e altri dati. Negli ultimi mesi sono state osservate campagne di diffusione malware via posta elettronica (malspam) sul tema Covid che hanno visto la cooperazione di tre distinti impianti malware nella combinazione **Emotet** (*trojan downloader*) - **Trickbot** (*trojan bancario*) e **Ryuk** (*ransomware*).

Emotet viene solitamente distribuito con campagne di posta elettronica, tramite allegati armati di macro VBA (Visual Basic for Applications) incaricate di scaricare e installare il malware che si occuperà di estrarre le password di accesso dei vari account email configurati nei client di posta o dai gestori delle password dei principali browser web consentendo a utenti malintenzionati di carpire informazioni aggiuntive quali e-mail, elenchi di contatti o dati bancari salvati dall'utente.

Questi dati risultano utili anche per la conduzione di altri attacchi, ad esempio di spear-phishing, in cui le vittime potrebbero ricevere messaggi malevoli ma a prima vista attendibili perché associati a pregresse conversazioni o apparentemente inviati da contatti noti.

In un'infrastruttura aziendale, dopo aver infettato con successo un sistema operativo, Emotet può tentare di propagarsi all'interno della rete forzando le credenziali dell'utente per scrivere copie di sé stesso su unità condivise.

La pericolosità di Emotet, supportata dall'imponente utilizzo di questo malware da parte dei criminali, implica la necessità di attuare specifiche misure per rilevarne l'attività e interrompere la catena di infezione prima che possa arrecare ingenti danni.

Le evolute modalità di diffusione e i suoi continui sviluppi tecnologici[1] permettono di eludere i controlli di sicurezza di norma efficaci nel contrasto di malware meno avanzati.

Le tattiche associate alla diffusione di questo malware e le procedure atte a condurre l'attacco informatico vedono l'utilizzo di diverse tecniche. Tra queste, ad esempio, il tentativo di elusione basato sull'invio di allegati malevoli costituiti da archivi compressi o documenti Office protetti da password, dove il destinatario del messaggio assume un ruolo critico nel processo d'infezione e, in particolare, nell'avvio della catena di infezione.

*Email malevole*

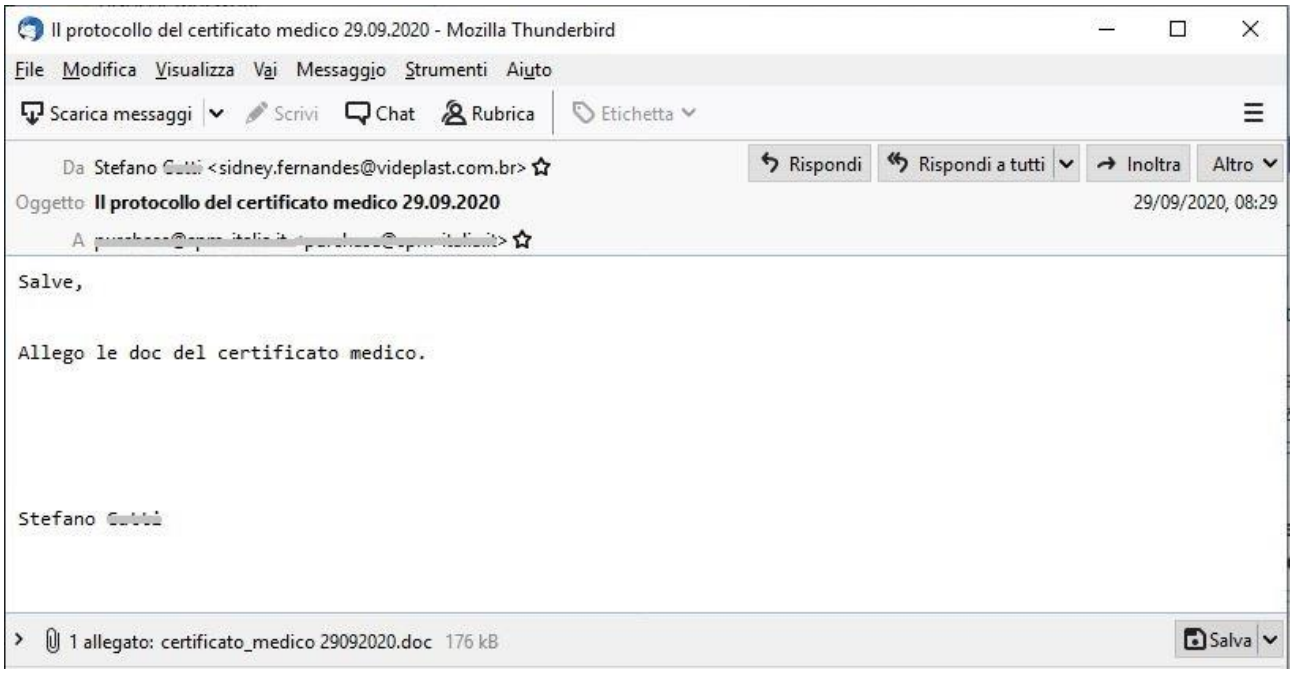


*Figura 1 – Email malevola*

[1] Il malware utilizza, infatti, librerie di collegamento dinamico modulari per aggiornare le sue capacità

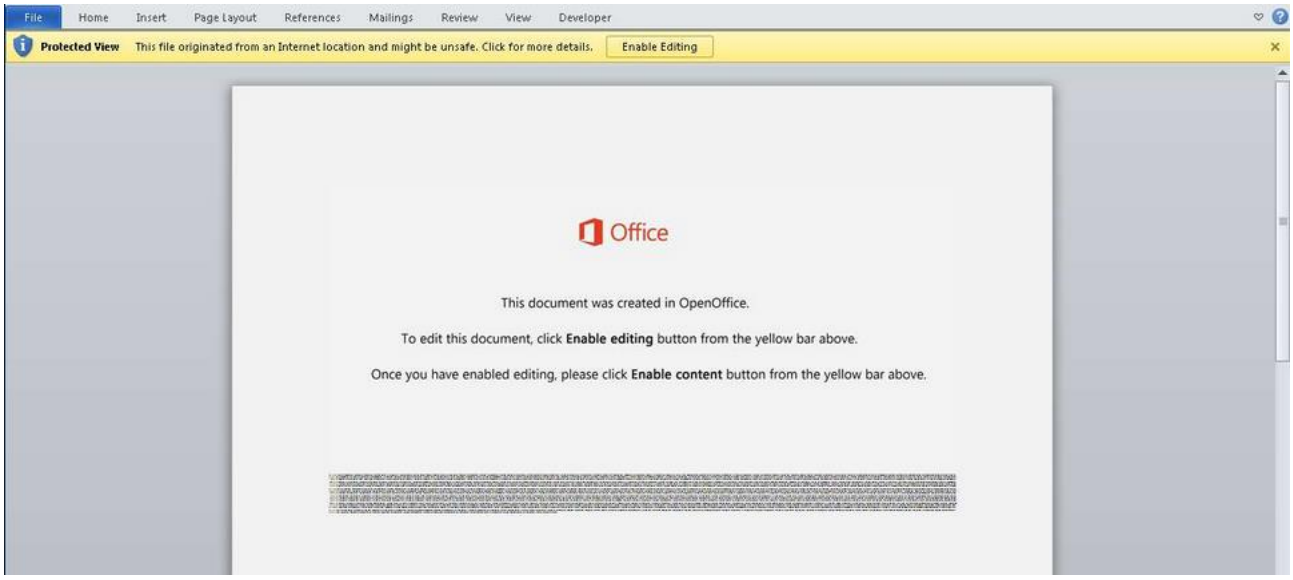


*Figura 2 - Esempio richiesta attivazione macro tramite documento allegato*

## Tattiche e tecniche in riferimento ad Emotet

Per avere una visione generale dei comportamenti degli aggressori, quindi delle tattiche e tecniche associate ad Emotet, si riportano di seguito quelle più rilevanti, basate su osservazioni del mondo reale, riferite al catalogo noto come ATT&CK (*Adversarial Tactics, Techniques & Common Knowledge*) predisposto e manutenuto dal MITRE:

| **Tecniche ATT&CK utilizzate** | **Uso da parte di Emotet** | **Mitigazioni ATT&CK consigliate** |
|---|---|---|
| [T1003.001] OS Credential Dumping: LSASS Memory | Rilascio di moduli per l'acquisizione di password, incluso Mimikatz. | [M1026] Privileged Account Management<br>[M1027] Password Policies<br>[M1043] Credential Access Protection<br>[M1017] User Training<br>[M1015] Active Directory Configuration<br>[M1025] Privileged Process Integrity<br>[M1028] Operating System Configuration<br>[M1041] Encrypt Sensitive Information |
| [T1021.002] Remote Services: SMB/Windows Admin Shares | Uso della condivisione di cartelle Admin per movimenti laterali, una volta ottenuta la password dell'amministratore locale. | [M1032] Multi-factor Authentication<br>[M1018] User Account Management |

| | | |
|---|---|---|
| [T1027] Obfuscated Files or Information | Inserimento di macro offuscate all'interno di documenti dannosi per nascondere gli URL malevoli. | [M1049] Antivirus/Antimalware |
| [T1027.002] Obfuscated Files or Information: Software Packing | Uso di packer personalizzati per proteggere i propri payload. | |
| [T1040] Network Sniffing | Uso delle API di rete finalizzato al monitoraggio del traffico di rete. | [M1032] Multi-factor Authentication<br>[M1041] Encrypt Sensitive Information |
| [T1041] Exfiltration Over C2 Channel | Cattura delle informazioni di sistema memorizzate nei cookie e successivo invio via HTTP GET ai server di comando e controllo (C2). | [M1031] Network Intrusion Prevention |
| [T1047] Windows Management Instrumentation | Uso di WMI per eseguire "*powershell.exe*". | [M1026] Privileged Account Management<br>[M1018] User Account Management |
| [T1055.001] Process Injection: Dynamic-link Library Injection | Aggiunta di processi in Explorer.exe. | [M1040] Behavior Prevention on Endpoint<br>[M1026] Privileged Account Management |
| [T1057] Process Discovery | Enumerazione dei processi locali. | [T1057] Process Discovery Mitigation |
| [T1059.001] Command and Scripting Interpreter: PowerShell | Utilizzo di Powershell per recuperare il payload dannoso e scaricare risorse aggiuntive come Mimikatz. | [M1038] Execution Prevention<br>[M1045] Code Signing<br>[M1026] Privileged Account Management<br>[M1042] Disable or Remove Feature or Program<br>[M1049] Antivirus/Antimalware<br>[M1021] Restrict Web-Based Content |
| [T1059.003] Command and Scripting Interpreter: Windows Command Shell | Uso di cmd.exe per eseguire script PowerShell. | |
| [T1059.005] Command and Scripting Interpreter: Visual Basic | Uso di documenti di Microsoft Word con macro incorporate al fine di richiamare script per scaricare payload aggiuntivi. | |
| [T1078.003] Valid Accounts: Local Accounts | Acquisizione, tramite attacco brute-force, di password di amministratore locale, successivamente usata per movimenti laterali. | [M1026] Privileged Account Management<br>[M1027] Password Policies<br>[M1013] Application Developer Guidance |
| [T1087.003] Account Discovery: Email Account | Acquisizione di indirizzi e-mail da Outlook. | [M1028] Operating System Configuration |
| [T1110.001] Brute Force: Password Guessing | Uso di elenchi interni di password per attività di brute-force. | [M1027] Password Policies<br>[M1032] Multi-factor Authentication<br>[M1036] Account Use Policies |

| | | |
|---|---|---|
| | | [M1018] User Account Management |
| [T1114.001] Email Collection: Local Email Collection | Analisi di dati della posta elettronica da Outlook. | [M1032] Multi-factor Authentication<br>[M1041] Encrypt Sensitive Information<br>[M1047] Audit |
| [T1204.001] User Execution: Malicious Link | Uso di un collegamento web dannoso fornito tramite messaggi di spear phishing. | [M1017] User Training<br>[M1021] Restrict Web-Based Content<br>[M1038] Execution Prevention<br>[M1031] Network Intrusion Prevention |
| [T1204.002] User Execution: Malicious File | Uso di un allegato malevolo consegnato tramite messaggi di spear phishing. | |
| [T1210] Exploitation of Remote Services | Uso del protocollo SMB tramite un exploit di vulnerabilità come ETERNALBLUE (MS17-010) per movimenti laterali e per la propagazione nella rete. | [M1016] Vulnerability Scanning<br>[M1051] Update Software<br>[M1019] Threat Intelligence Program<br>[M1026] Privileged Account Management<br>[M1030] Network Segmentation<br>[M1050] Exploit Protection<br>[M1042] Disable or Remove Feature or Program<br>[M1048] Application Isolation and Sandboxing |
| [T1543.003] Create or Modify System Process: Windows Service | Creazione di nuovi servizi al fine di mantenere la persistenza sul sistema colpito. | [M1018] User Account Management<br>[M1047] Audit<br>[M1033] Limit Software Installation<br>[M1022] Restrict File and Directory Permissions |
| [T1547.001] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | Mantenimento della persistenza attraverso associazione del payload scaricato alla chiave *HKEY_CURRENT_USER* \ *Software* \ *Microsoft* \ *Windows* \ *CurrentVersion* \ *Run* | [T1547] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder Mitigation |
| [T1053.005] Scheduled Task/Job: Scheduled Task | Mantenimento della persistenza attraverso la definizione di un'attività pianificata. | [M1026] Privileged Account Management<br>[M1028] Operating System Configuration<br>[M1047] Audit<br>[M1018] User Account Management |

| | | |
|---|---|---|
| [T1552.001] Unsecured Credentials: Credentials In Files | Utilizzo, nel contesto della sessione dell'utente, di un modulo di recupero delle password memorizzate sul un sistema. | [M1047] Audit<br>[M1015] Active Directory Configuration<br>[M1022] Restrict File and Directory Permissions<br>[M1017] User Training<br>[M1037] Filter Network Traffic<br>[M1026] Privileged Account Management<br>[M1027] Password Policies<br>[M1028] Operating System Configuration<br>[M1041] Encrypt Sensitive Information<br>[M1051] Update Software |
| [T1555.003] Credentials from Password Stores: Credentials from Web Browsers | Rilascio di moduli di cattura delle password salvate nel browser. | [M1027] Password Policies |
| [T1560] Archive Collected Data | Cifratura dei dati raccolti prima dell'invio al server C2. | [M1047] Audit |
| [T1566.001] Phishing: Spearphishing Attachment | Diffusione tramite allegati consegnati via e-mail di phishing. | [M1049] Antivirus/Antimalware<br>[M1031] Network Intrusion Prevention<br>[M1021] Restrict Web-Based Content<br>[M1017] User Training |
| [T1566.002] Phishing: Spearphishing Link | Diffusione tramite l'attivazione di collegamenti in e-mail di phishing. | |
| [T1571] Non-Standard Port | Instaurazione di connessioni via protocollo HTTP utilizzando porte non standard come: 20, 22, 7080 e 50000. | [M1030] Network Segmentation<br>[M1031] Network Intrusion Prevention |
| [T1573.002] Encrypted Channel: Asymmetric Cryptography | Uso di chiavi RSA per cifratura del traffico C2. | [M1020] SSL/TLS Inspection<br>[M1031] Network Intrusion Prevention |

*Tabella 1 - Emotet: tattiche e tecniche, mitigazioni*

Tale elenco offre una rappresentazione delle attività associate al malware in oggetto, offrendo spunto utile per predisporre gli opportuni controlli e per attivare meccanismi difensivi.

## Individuazione

L'individuazione di Emotet, oltre che tramite l'uso di firme antivirus, può realizzarsi tramite l'analisi del traffico di rete. Generalmente questa attività è demandata a

strumenti noti come NIDS (*Network Intrusion Detection System*) e apposite firme idonee all'identificazione comportamentale del malware.

Si riportano di seguito le firme per Snort, software libero per l'analisi dei pacchetti all'interno di una rete, sviluppate per rilevare connessioni di rete associate all'attività di Emotet.

Firma Snort sviluppata da *Center for Internet Security* (MS-ISAC):

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"[CIS] Emotet C2 Traffic Using Form Data to Send Passwords"; content:"POST"; http_method; content:"Content-Type|3a 20|multipart/form-data|3b 20|boundary="; http_header; fast_pattern; content:"Content-Disposition|3a 20|form-data|3b 20|name=|22|"; http_client_body; content:!"------WebKitFormBoundary"; http_client_body; content:!"Cookie|3a|"; pcre:"/:?(chrome|firefox|safari|opera|ie|edge) passwords/i"; reference:url,cofense.com/flash-bulletin-emotet-epoch-1-changes-c2-communication/; sid:1; rev:2;)
```

Firme Snort sviluppate da Cybersecurity and Infrastructure Security Agency (CISA):

```
alert tcp any any -> any $HTTP_PORTS (msg:"EMOTET:HTTP URI GET contains '/wp-content/###/'"; sid:00000000; rev:1; flow:established,to_server; content:"/wp-content/"; http_uri; content:"/"; http_uri; distance:0; within:4; content:"GET"; nocase; http_method; urilen:<17; classtype:http-uri; content:"Connection|3a 20|Keep-Alive|0d 0a|"; http_header; metadata:service http;)
```

```
alert tcp any any -> any $HTTP_PORTS (msg:"EMOTET:HTTP URI GET contains '/wp-admin/###/'"; sid:00000000; rev:1; flow:established,to_server; content:"/wp-admin/"; http_uri; content:"/"; http_uri; distance:0; within:4; content:"GET"; nocase; http_method; urilen:<15; content:"Connection|3a 20|Keep-Alive|0d 0a|"; http_header; classtype:http-uri; metadata:service http;)
```

## Mitigazioni

Esistono diverse soluzioni e misure restrittive per individuare Emotet e bloccarne la diffusione. Di seguito le più comuni suddivise per ambito di riferimento:

### Contesto domestico

Si consiglia di:

- prestare attenzione all'apertura degli allegati di posta elettronica. Anche qualora l'allegato sia atteso e il mittente sembri essere noto è bene prevedere una scansione antivirus dell'allegato;
- non fare clic sul pulsante "Abilita contenuto" e non attivare macro da documenti che arrivano via e-mail anche se provengono da una fonte attendibile o conversazioni e-mail familiari;
- aggiornare regolarmente il software antivirus con le definizioni utili per il riconoscimento del malware;
- assicurarsi di applicare patch a software e sistemi operativi.

## Contesto aziendale

Per quanto attiene alle attività di formazione del personale, si suggerisce di:

- informare ed istruire il personale sui casi di phishing, con particolare riferimento al riconoscimento dei messaggi sospetti (ad esempio, messaggi in cui le informazioni del mittente sono state alterate);
- sensibilizzare l'utenza circa i pericoli connessi l'apertura di determinati allegati e-mail come i file contenenti macro di Office (.doc, .docx, .xls, .xlsx) particolarmente popolari per consegnare Emotet e malware.

Gli amministratori di sistema, dopo aver valutato le possibili ripercussioni e gli impatti indesiderati sull'erogazione dei servizi, possono valutare di:

- bloccare gli allegati di posta elettronica comunemente associati a malware (ad es. .dll ed .exe);
- bloccare gli allegati e-mail che non possono essere scansionati da software antivirus (ad esempio file .zip o documenti provvisti di password);
- implementare criteri di gruppo restrittivi e regole specifiche sul firewall locale;
- ove possibile, disabilitare PowerShell 2.0 o limitare l'esecuzione sulle workstation degli utenti, impostando i criteri di esecuzione di PowerShell per consentire solo gli script firmati o prediligere l'uso nella modalità "Constrained Language" attivando restrizioni che limitano l'esecuzione di codice;
- impedire l'esecuzione di macro nei prodotti Office consentendolo solo agli utenti che ne hanno comprovata necessità, in alternativa impedire l'esecuzione delle macro Office non firmate;
- installare un software antivirus dotandolo di un processo di gestione automatizzata delle definizioni;
- implementare filtri nel gateway di posta elettronica;
- incrementare la sicurezza perimetrale al fine di bloccare C&C e, in generale, gli indirizzi IP contrassegnati come malevoli;
- utilizzare, ove possibile, il principio del privilegio minimo per l'utente;
- autorizzare l'accesso, sia livello di rete sia di sistema, alle risorse in modo puntuale evitando che tutti gli utenti possano liberamente accedere a risorse aziendali non necessarie;
- implementare un sistema di autenticazione, reporting e conformità dei messaggi di posta basato su dominio (SPF/DMARC/DKIM) per verificare il mittente;
- segmentare e separare le reti e le funzioni;
- limitare le comunicazioni tra sistemi interni della rete impedendo e monitorando quelle non necessarie;

- quando non necessari disabilitare i servizi di condivisione di file e stampanti e in ogni caso prediligere l'utilizzo di password complesse o l'autenticazione di Active Directory;
- ove possibile, prediligere l'autenticazione a più fattori;
- abilitare un firewall sui sistemi garantendo solo il traffico verso i servizi e sistemi necessari (negando le richieste di connessione non esplicitamente necessarie);
- disattivare i servizi non necessari sia nelle workstation sia sui server;
- scansionare gli allegati di posta elettronica al fine di rimuovere quelli sospetti come quelli la cui estensione non corrisponde all'intestazione del file;
- monitorare le abitudini di navigazione web degli utenti;
- limitare l'accesso a siti sospetti o rischiosi;
- limitare o attivare controlli per supporti rimovibili ad es. chiavette USB, unità esterne, CD;
- scansionare ogni software scaricato da Internet prima della sua esecuzione;
- mantenere un elevato grado di consapevolezza sulla situazione delle minacce in modo da rispondere con specifiche misure alla diffusione e all'evoluzione del malware;
- visitare le pagine MITRE ATT&CK Techniques riportate nella Tabella 1 sopra indicata per valutare ulteriori e personalizzate strategie finalizzate alla mitigazione e al rilevamento.

## Riferimenti


- https://us-cert.cisa.gov/ncas/alerts/aa20-280a
- https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode/
- https://attack.mitre.org/