Pakistan Telecom Authority Headquarters, Islamabad

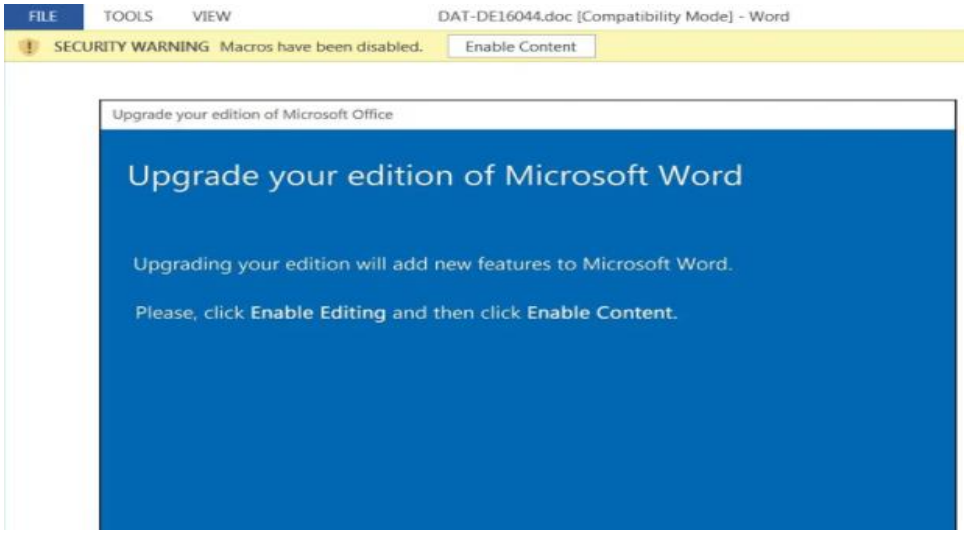
PTA Cyber Security Advisory No.:110 **28-10-2020**

Name: EMOTET malware now pretending to be a feature of Microsoft Office

Threat Classification: Malware

Summary:

Emotet malware, which **spreads through emails containing Word documents with malicious macros**, has now switched to a new template pretending to be a Microsoft Office message stating that Microsoft Word needs to be updated to add a new feature. Upon its installation, Emotet use the computer to install other malwares that **could lead to sensitive data breach** (passwords, banking information) and even a **Ransomware attack on the victim's network**.



New upgrade Microsoft Word EMOTET attachment

For more details on Emotet malware, please visit: https://us-cert.cisa.gov/ncas/alerts/aa20-280a

Recommendations:

a. For Detection:

- Following **SNORT signature** has been reported for the detection of Emotet activity:

```
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;)
```

b. For Mitigation:

- **Disable macros execution by default**, only enable when required and limit the permissions to allow macros execution.
- Implement filters at Email gateway to **filter out emails with known malware spamming indicators**. Also block the suspicious IP addresses at perimeter firewall.
- Use Group Policy Object to set Firewall rules for **restricting inbound SMB** communication between the client systems.
- Implement Software Restriction Policies (SRP) to **block unsigned binaries running from %APPDATA% and %TEMP%** locations.
- **Block email attachments commonly associated with malware like .dll and .exe**, also block outbound network connections originating from **WinWord.exe, Powershell.exe, Powershell_ise.exe, Mshta.exe** and block inbound connections if remote access of system is not required.
- Ensure the **principle of least privilege** and **disable unnecessary services**/ ports as malware often exploit such services.
- **Regularly maintain data backups** and also ensure that backups are stored offline at a secure site.
- **Regularly update all software** including Operating System, Microsoft Office and other.
- Use **licensed antivirus software with heuristics and reputation ratings system** to identify and prevent malicious attachments, and also regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Regularly **provide Cyber security awareness trainings** to the employees.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.