Emotet Changes TTPs and Arrives in United States

Published: 2017-04-28 · Archived: 2026-04-05 23:21:46 UTC

The MS-ISAC recently observed a malicious email campaign delivering the Emotet banking Trojan via a malicious PDF in the United States. This appears to be the first time Emotet has targeted the United States and used a PDF file attachment. The campaign targeted federal, state, local, tribal, and territorial (FSLTT) government employees, among others, with fake invoices and documents from national branded businesses and organizations. Emotet is a variant of the Feodo Trojan family, which is a family of banking Trojans that include Emotet, Bugat, and Dridex.

Geographic History

Emotet was first reported by the cybersecurity community in June 2014. Its first two versions targeted German and Austrian banking clients from June 2014 until it went silent in December 2014. At the end of January 2015, reporting indicated that a third version emerged with upgraded evasion techniques. This version expanded outside of Germany and Austria to target Swiss banks. No significant campaigns were publicly documented during the rest of 2015 or all of 2016. Feodo Tracker, a site that tracks the Feodo Trojan family, showed the botnet infrastructure to be almost completely offline in 2016 and completely offline as of April 27, 2017.

However, around mid-April 2017, Forcepoint analyzed samples from a large-scale UK spam campaign and noted that it used Geodo malware. Only instead of the new Dridex derivative, the campaign used the older Emotet variant.

The April campaign used a fake invoice as the attachment and focused on the .uk country code domain (ccTLD). According to Forcepoint, the campaign peaked on April 18, 2017.

On April 24, 2017, the MS-ISAC observed a spam campaign against FSLTT government employees in the United States, that has expanded to include targeting of the financial sector. We confirmed the malicious PDF attachments as directing recipients to URLs that downloaded the Emotet malware.

Current Delivery Methodology

The U.S. campaign displays many similarities with the UK campaign from mid-April, although there are some notable differences.

Emotet, like most malware, has continuously evolved its delivery method. Proofpoint documented the mid-April 2017 UK campaign as using an attachment with fake phone bills and then switching to embedding links to malicious files within the emails. In the U.S. variant, the MS-ISAC has noted malicious PDF file attachments containing a link to javascript (JS), which the recipient is directed to download. The subject line of the emails varied between fake billing notifications to reports needing to be read.

Subject: Invoice from info@
Importance: High

Please find attached your Invoice dated - 25 Apr 17 any queries please ring the following:-

91095 990382
The following are attached to this email:
KZSY284404.PDF

Document 239543604

Voice & Video Services <emilie.[redacted]@[redacted]fr>
Monday, April 24, 2017 at 1:55 PM
To: [redacted]
: Document_11861097_NI_NSO__11861097.pdf (4.3 KB) Preview

This message is high priority.

Your report is attached in PDF format.

Attachments: Document_11861097_NI_NSO___11861097.pdf

Thanks for your business!
VOICE & VIDEO SERVICES

Inside the PDF, there is an overt reference to the link's target being a JS file. The MS-ISAC believes this is done to inform the recipient about the unusual invoice format.

```
You have received an invoice from <> for $3,492.84. To view, print or
download a JS copy of your invoice, click the link below:

http://[redacted]/invoice-80633-Apr-24-2017-US-665952/name=<>
(Your report is attached in JS format)

Best regards, <>
```

This link returns a .JS file, which is heavily obfuscated and laced with large amounts of ‘junk’ data. The de-obfuscated data shows around 2000 lines of junk data, with only one of the function lines being used.

The .JS file is meant to show the victim an error message (shown below) when run.

```
}
getData(function (data, error) {
        if (!error) {
                saveToTemp(data, function (path, error) {
                        if (!error) {
                                try {
                                        var wsh = new ActiveXObject("WScript.Shell");
                                        wsh.Run(path);
                                        WshShell = WScript.CreateObject("WScript.Shell");
                                        Text = "There was an error opening this document. The file is damaged and could not be repaired (for example, it was
sent as an email attachment and wasn't correctly decoded).";
                                        Title = "Not Supported File Format";
                                        Res = WshShell.Popup(Text, 0, Title, 0 + 64);
                                } catch (error) {}
```

Once the .JS file is run, it makes HTTP GET requests over port 8080 to the command and control (C2) IP with what the MS-ISAC believes is identification data encrypted within an encoded cookie string.

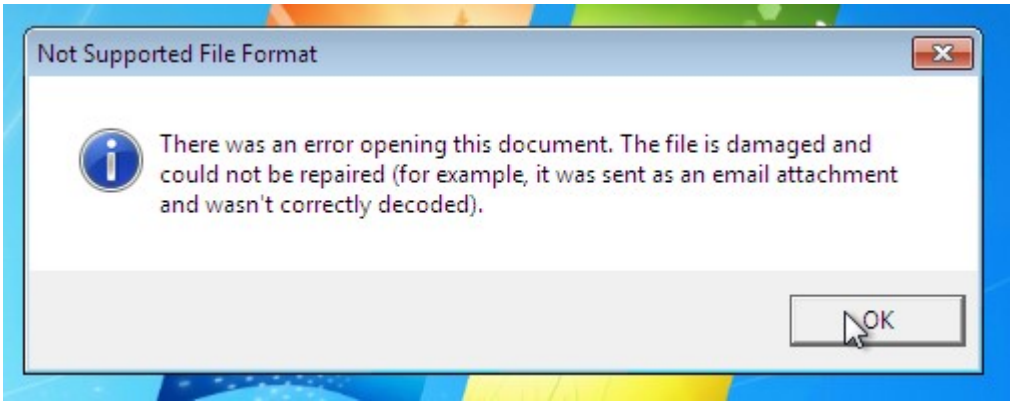
When the malware was successfully run, the remote IP address responded with a 404 error header and encrypted data. The MS-ISAC observed that using the same cookie string in the requests, when resent, would garner differing content length in the server’s responses, showing that the reply could vary in response despite static cookie values being reused in testing.

Association Between U.S. and UK Spam Campaign

Though there are some notable differences, the U.S. campaign displays many similarities with the mid-April UK campaign observed by Forcepoint. The UK emails took the form of fake billing notifications and around half of the MS-ISAC observed emails used fake billing as the lure.

Though the TTPs for delivery of the .JS file changed between campaigns, with the U.S. campaign using a malicious link inside of a malicious attachment and the UK campaign using a malicious link inside the email body, the .JS files from both campaigns were similar. Both the MS-ISAC and Forcepoint noted that the .JS file downloaded from the malicious link was heavily obfuscated and contained a large amount of junk data.

When the .JS runs, Forcepoint observed an error message that matched the error message found within the MS-ISAC .JS verbatim. Both are shown below:




```
}
getData(function (data, error) {
	if (!error) {
		saveToTemp(data, function (path, error) {
			if (!error) {
				try {
					var wsh = new ActiveXObject("WScript.Shell");
					wsh.Run(path);
					WshShell = WScript.CreateObject("WScript.Shell");
					Text = "There was an error opening this document. The file is damaged and could not be repaired (for example, it was
sent as an email attachment and wasn't correctly decoded).";
					Title = "Not Supported File Format";
					Res = WshShell.Popup(Text, 0, Title, 0 + 64);
				} catch (error) {}
```

The MS-ISAC also observed differences between the C2 servers involved in previous Emotet versions and in the latest interation of the malware. The communication request was an HTTP GET request with an encoded cookie string. The C2 server responded to the request with a “404 Not Found” message containing an encrypted response.

Indicators of Compromise (IOC)

Attachments

- Document attachments with names similar to “Document_11861097_NI_NSO__11861097.pdf” or “11861097_11861097.pdf” The same number is repeated twice with either a “_” or “_NI_NSO__” between them.
- A PDF with no other indicators, such as “KZSY284404.PDF.” It is 7 or 9 characters long using only letters and numbers, mostly follows the format of “LLLNNNNNN.pdf.”
- The invoice PDF variant, “Invoice.PDF.”

As of June 23, 2025, the MS-ISAC has introduced a fee-based membership. Any potential reference to no-cost MS-ISAC services no longer applies.

Source: https://www.cisecurity.org/blog/emotet-changes-ttp-and-arrives-in-united-states/