MOVING TARGET DEFENSE BLOG

CYBERSECURITY TRENDS, EXPLORING MOVING TARGET DEFENSE AND PUTTING ENDPOINT THREAT PREVENTION FIRST

FIN7 TAKES ANOTHER BITE AT THE RESTAURANT INDUSTRY

Posted by **MICHAEL GORELIK** on June 9, 2017

Find me on:

Tweet Share Like 0 Share

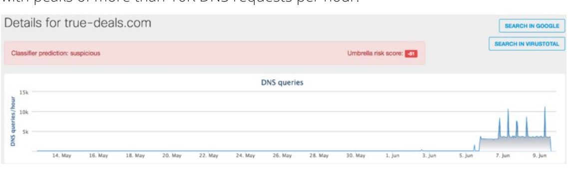
INTRODUCTION

On June 7, 2017, Morphisec Lab identified a new, highly sophisticated fileless attack targeting restaurants across the US. The ongoing campaign allows hackers to seize system control and install a backdoor to steal financial information at will. It incorporates some never before seen evasive techniques that allow it to bypass most security solutions – signature and behavior based.

Aside from these updated techniques, Morphisec's investigation revealed an almost perfect match to FIN7 attack methods. Past highly successful and damaging attacks on banks, SEC personnel, large restaurant chains and hospitality organizations have all been attributed to the financially-motivated FIN7 group. FIN7, which is also associated with the Carbanak gang, must be seen as one of the leading threat actor groups operating today.

Like past attacks, the initial infection vector is a malicious Word document attached to a phishing email that is well-tailored to the targeted business and its day-to-day operations. The Word document executes a fileless attack that uses DNS queries to deliver the next shellcode stage (Meterpreter). However, in this new variant, all the DNS activity is initiated and executed solely from memory – unlike previous attacks which used PowerShell commands.

OpenDNS investigate data, shared in coordination with the Cisco Advanced Threat Research & Efficacy Team, shows that this is a large-scale, currently active attack with peaks of more than 10K DNS requests per hour.



Alarmingly, the detection score on VirusTotal for all of the documents continues to be 0/56 from the time the first documents were uploaded (1.6.2017) up until the date of this publication. This means the attackers successfully bypass static analysis by most of the security solutions.

By contrast, Morphisec's Moving Target Defense-based technology prevents the attack in its early stages, before any channel to the attacker is opened.

virustotal

SHA256:	2781526f6b302da00661b9a6a625a5a6ecf4ffccafa61202e9b0e9b61b657867
File name:	menu.rtf
Detection ratio:	0 / 56
Analysis date:	2017-06-06 13:42:25 UTC (1 day, 19 hours ago)

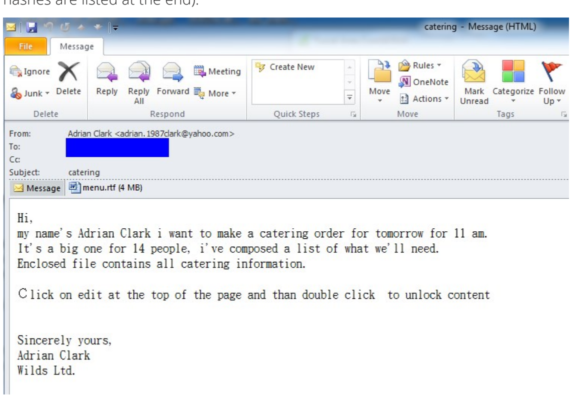
1 0

TECHNICAL ANALYSIS

Below we describe the full technical details, beginning with the initial email through the final Meterpreter session used to hijack the computer.

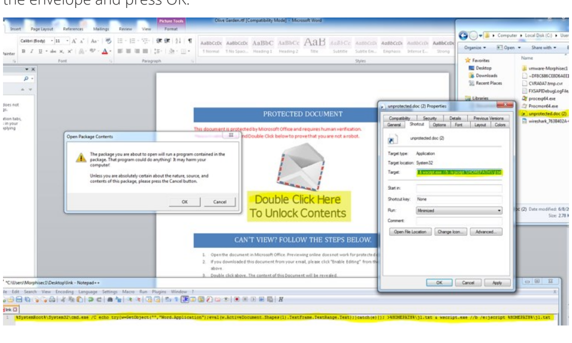
PHISHING EMAIL:

As seen in the email below, FIN7's attack campaign targets restaurants. The content of the email is well crafted to avoid suspicion. Some of the email attachments are called menu.rtf, others Olive Garden.rtf or Chick Fil A Order.rtf (all the identified hashes are listed at the end).

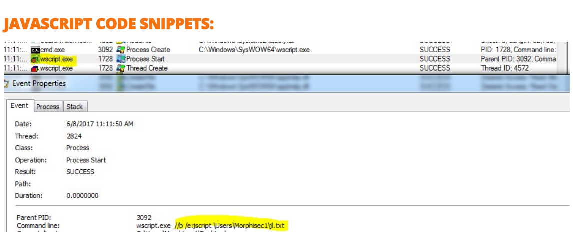


WORD DELIVERY:

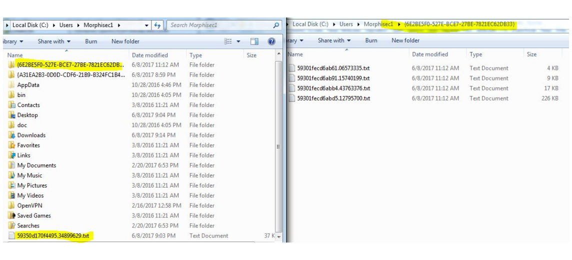
The attached .rtf file uses OLE and has many similarities to previous FIN7 attacks. But this attack, instead of activating hta files (mshta.exe) from within the link, executes obfuscated JavaScript code. All the victim needs to do is double click on the envelope and press OK.



JAVASCRIPT CODE SNIPPETS:



The first stage JavaScript copies additional JavaScript code snippets in txt format from the RTF document into a random directory "C:\Users\<User Name>\<Random guid>\". The same code snippets are combined into a second stage JavaScript in "C:\Users\<User Name>\". Additionally, the first stage JavaScript creates a scheduled task that executes the second stage code within a minute – this delayed execution helps to bypass behavior analysis since the second stage is not directly executed by the first stage.

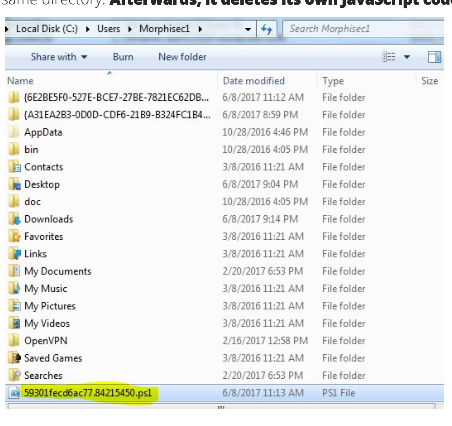


PERSISTENCY:

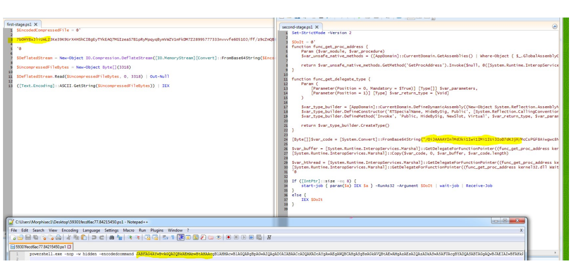
In some cases, an additional scheduled task "AdobeFlashSync" is created for persistency. This task is executed every 25 minutes and will repeat the actions described above – recreating the JavaScript code which later will create and execute a PowerShell script (described below).

SECOND STAGE JAVASCRIPT INTO POWERSHELL:

The second stage JavaScript creates a PowerShell file with the same name in the same directory. **Afterwards, it deletes its own JavaScript code traces**.



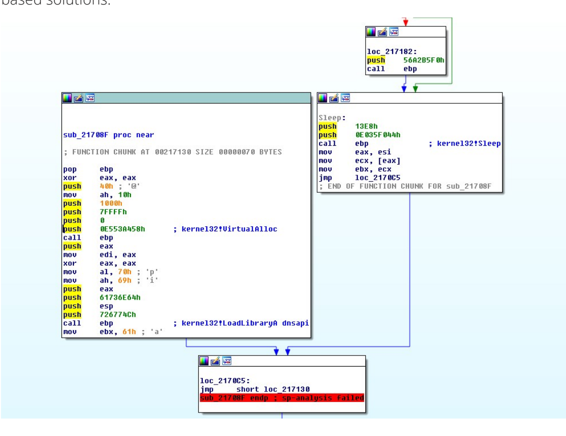
The PowerShell script executes a compressed first stage PowerShell child process, which then performs a second stage PowerShell process. The latter PowerShell injects a shellcode into its own process using well-known CreateThread and VirtualAlloc techniques:



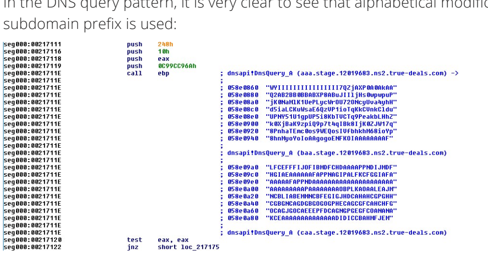
SHELLCODE:

The shellcode phase of this attack is unique and demonstrates the constantly advancing abilities of attackers. The shellcode is the primary differentiating technique between this campaign and past attacks by FIN7 and other threat actors.

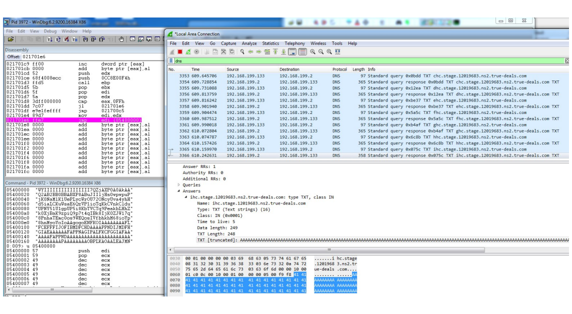
This shellcode iterates over process environment block and looks immediately for dnsapi.dll name (xor 13) and its DnsQueryA function. Basically, FIN7 implemented a shellcode that gets the next stage shellcode using the DNS messaging technique directly from memory. This way they can successfully evade many of the behavior based solutions.



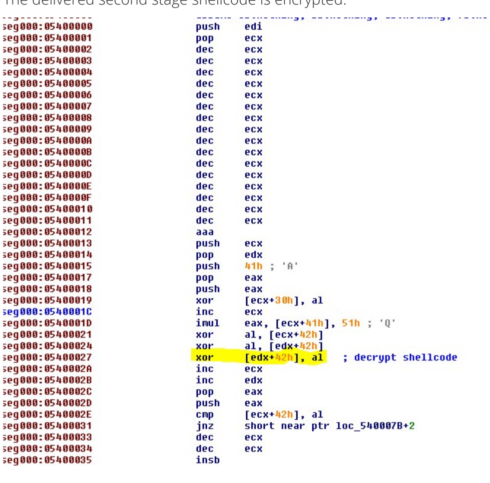
In the DNS query pattern, it is very clear to see that alphabetical modification of the subdomain prefix is used:



Each such DNS query results in an additional snippet of shellcode being appended to a reallocated buffer. When, finally, the first stage shellcode receives a special "FF" signal, it then executes the delivered shellcode. (It takes a few minutes for the DNS queries to finish. The last query is to the subdomain ihc[.]stage[.]12019683[.]ns2[.]true-deals[.]com):



The delivered second stage shellcode is encrypted:



METERPRETER:

After decryption of the second stage shellcode, the shellcode **deletes** the 'MZ' prefix from within a very important part of the shellcode. This prefix indicates it may be a dll, and its deletion helps the attack **to evade memory scanning solutions**.

Just before this step executed, we extracted the dll from memory and uploaded it to VirusTotal. If this dll was saved on disk, many security solutions would immediately identify it as a CobaltStrike Meterpreter, which is used by many attackers and pen testers. Having a Meterpreter session on a compromised computer allows for full control of the computer and exfiltration of any data, and in some cases lateral movement inside the organization.

SHA256:	55dc09574c4569d72314aa0beb3c02ff9b31379f4cb916fd108cff659ca27013
File name:	injected_dns.dll
Detection ratio:	30 / 58
Analysis date:	2017-06-08 16:21:34 UTC (0 minutes ago)

0 0

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Ad-Aware	Gen:Variant.Application.HackTool.CobaltStrike.1	20170608
AhnLab-V3	HackTool/Win32.Cobalt.R197271	20170608
Antiy-AVL	HackTool/Win32.Cobalt	20170608
Arcabit	Trojan.Application.HackTool.CobaltStrike.1	20170608
BitDefender	Gen:Variant.Application.HackTool.CobaltStrike.1	20170608
CAT-QuickHeal	Trojan.Skeeyah	20170607
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20170420
DrWeb	BackDoor.Meterpreter.4	20170608
Emsisoft	Gen:Variant.Application.HackTool.CobaltStrike.1 (B)	20170608
Endgame	malicious (high confidence)	20170515
ESET-NOD32	a variant of Win32/RiskWare.CobaltStrike.Beacon.A	20170608
F-Secure	Gen:Variant.Application.HackTool	20170608
GData	Gen:Variant.Application.HackTool.CobaltStrike.1	20170608
Ikarus	Trojan.Win32.Conbea	20170608
Invincea	heuristic	20170607
K7AntiVirus	Unwanted-Program (004c3a6f1)	20170608

CONCLUSIONS:

FIN7 constantly upgrades their attacks and evasion techniques, thus becoming even more dangerous and unpredictable. The analysis of this attack shows, how easy it is for them to bypass static, dynamic and behavior based solutions. These attacks pose a severe risk to enterprises.

Fileless attacks are on the rise – Carbon Black reports that researchers found a 33% rise in severe non-malware attacks in Q4 2016 compared to Q1. Defenders will see more attacks on their businesses by hacker groups utilizing memory for evasion while keeping executable artifacts far away from disk.

In this continuously evolving threat landscape, enterprises need to look for new defenses that are resilient to such changes and are able to prevent fileless attacks. Morphisec Endpoint Threat Prevention specializes in preventing in-memory attacks, using Moving Target Defense to make the target itself unpredictable.

ARTIFACTS:

Documents:

2781526f6b302da00661b9a6a625a5a6ecf4ffccafa61202e9b0e9b61b657867

c357396ca82fdcd6b6f46b748f2b6941051dbc81be5326cf9548e6e95507af7c

ffebcc4d2e851baecd89bf11103e3c9de86f428fdeaf0f8b33d9ea6f5ef56685

Domains:

- true-deals[.]com; strikes-withlucky[.]com
- Email account in registration is: isvarawski@yahoo.com
- Attacker email account: adrian.1987clark@yahoo.com

SUBSCRIBE TO OUR BLOG

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

FIRST NAME
LAST NAME
EMAIL
COMPANY
SUBSCRIBE

SEARCH OUR SITE

Keyword...

RECENT POSTS

Parallax: The New RAT on the Block
Remote Employees Offer Different Security Challenges
Why Client-Grade Technology Doesn't Cut It for Cloud Workload Protection
Trickbot Delivery Method Gets a New Upgrade Focusing on Windows 10
Introducing the Morphisec Unified Threat Prevention Platform -- Version 4
Endpoint Security Is Harder than Ever
Trickbot Trojan Leveraging a New Windows 10 UAC Bypass
Morphisec Protects Customers Against Internet Explorer Scripting
Endpoint Detection and Response Is Not the Next Step
Are Guests Safe From a Hotel Data Breach?

POSTS BY TAG

Cyber Security (94)
Endpoint Security (74)
Attack Analysis (45)
Cyber Attacks (45)
Company News (38)
See all