# On the Hunt for FIN7: Pursuing an Enigmatic and Evasive Global Criminal Operation

fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html

Threat Research

Nick Carr, Kimberly Goody, Steve Miller, Barry Vengerik

Aug 01, 2018

25 mins read

Threat Research

On Aug. 1, 2018, the United States District Attorney's Office for the Western District of Washington unsealed indictments and announced the arrests of three individuals within the leadership ranks of a criminal organization that aligns with activity we have tracked since 2015 as FIN7. These malicious actors are members of one of the most prolific financial threat groups of this decade, having carefully crafted attacks targeted at more than 100 organizations. FIN7 is referred to by many vendors as "Carbanak Group," although we do not equate all usage of the CARBANAK backdoor with FIN7. This blog explores the range of FIN7's criminal ventures, the technical innovation and social engineering ingenuity that powered their success, a glimpse into their recent campaigns, their apparent use of a security company as a front for criminal operations, and what their success means for the threat landscape moving forward. With this release, FireEye is also providing technical context, historical indicators, and techniques that organizations can use to hunt for FIN7 behavior enterprise-wide.

## FIN7 Does the Crime...

The threat group is characterized by their persistent targeting and large-scale theft of payment card data from victim systems, which it has monetized at least a portion of through a prominent card shop. But FIN7's financial operations were not limited to card data theft. In some instances, when they encountered and could not obtain payment card data from point of sale (POS) systems secured with end-to-end encryption (E2EE) or point-to-point encryption (P2PE), FIN7 pivoted to target finance departments within their victim organizations.

Furthermore, in April 2017, FireEye reported that FIN7 sent spear phishing emails to personnel involved with United States Securities and Exchange Commission (SEC) filings at multiple organizations, providing further insight into FIN7's targeting. These targeted individuals would likely have access to material non-public information that FIN7 actors could use to gain a competitive advantage in stock trading.

Diversification of their monetization tactics has allowed the group to impact a wide range of industries beyond those solely associated with payment card industry. During campaigns that FireEye associates with FIN7, victims within the following sectors have been targeted within the United States and Europe:

- Restaurants
- Hospitality
- Casinos and Gaming
- Energy

- *Travel
- *Education
- *Construction
- *Retail

- Finance
- High-tech
- Software

*Telecommunications
*Government
*Business services

## FIN7's Innovation Enabled their Success

Throughout FireEye's tracking of FIN7 campaigns, the attackers have attempted to stay ahead of the game and thwart detection, using novel tactics and displaying characteristics of a well-resourced operation. For example, in April 2017, FireEye blogged about FIN7's spear phishing emails that leveraged hidden shortcut files (LNK files) to initiate the infection and VBScript functionality launched by mshta.exe to infect the victim. This was a direct departure from their established use of weaponized Office macros and highlighted the group's adaptive nature to evade detection.

FireEye also previously reported on FIN7's use of the CARBANAK backdoor as a post-exploitation tool to cement their foothold in a network and maintain access to victim environments. CARBANAK is well known for its use in highly profitable and sophisticated attacks dating back to 2013, with usage attributable to FIN7 beginning in late 2015, although how interconnected the campaigns employing the malware over this five-year span are is unclear. FIN7's use of CARBANAK is particularly notable due to their use of creative persistence mechanisms to launch the backdoor. The group leveraged an application shim database that injected a malicious in-memory patch into the Services Control Manager ("services.exe") process, and then spawned a CARBANAK backdoor process. FIN7 also used this tactic to install a payment card harvesting utility.

Another notable characteristic of FIN7 has been their heavy use of digital certificates. Unsurprisingly, malicious threat actors have sought to exploit the legitimacy afforded by these certificates. By digitally signing their phishing documents, backdoors and later stage tools, FIN7 was able to bypass many security controls that may limit execution of macros from Office documents and restrict execution of unsigned binaries on trusted systems.

| Organization | Country | Serial | Email |
|---|---|---|---|
| Korsar Travel TOV | UA | 88:21:ac:7e:6c:da:11:00:1d:b3:d3:1a:16:c1:5c:26 | korsartravel@bk.ru |
| Kaitschuck James | GB | 30:2e:7f:14:3a:f3:f3:98:20:70:42:4e:ea:52:5d:d2 | oliversoftware@hotmail.com |
| Park Travel | RU | 4d:e2:87:56:98:bf:c7:74:a3:f3:47:d6:70:7c:9b:f0 | inga@parktravel-mx.ru |

Table 1: Sample FIN7 code signing certificates

FIN7 developed evasive techniques at a rapid pace. Throughout 2017, FIN7 was observed creating novel obfuscation methods, and in some cases modifying the methods on a daily basis while launching attacks targeting multiple victims. The threat group regularly tested malicious DOC, DOCX, and RTF phishing documents against public repositories to check static detection engine coverage. Their development of a payload obfuscation style using the Windows command interpreter's (cmd.exe) native string substitution was so unique that FireEye dubbed it "FINcoding." These methods inspired deep command line obfuscation research and the release of Daniel Bohannon's Invoke-DOSfuscation. Reference Table 2 and Table 3 for a selection of samples and their associated command line obfuscation techniques.

## FIN7's Relentless Phone Calls and Bellyaching

Over the three years of responding to a multitude of compromises and proactively defending against FIN7, FireEye observed unprecedented social engineering prowess. From leveraging web forms for initial contact to targeting and engaging directly with pre-determined store managers, the operators demonstrated a range of capabilities. FIN7's reach extended beyond their targets' computer systems. FireEye has responded to incidents where FIN7 has called victims *prior* to lodging digital complaints laden with malicious documents as well as after the phishing documents have been sent, in order to check if they were received – a crude but effective FIN7 email delivery tracking technique.

As FIN7 has matured, so did the quality of their phishing lures and templates, which were most often sent from fake but thoroughly disguised individuals and businesses – and occasionally from sender addresses impersonating legitimate government entities. Their phishing has often exploited urgent, high value business matters tailored to their chosen targets. At individual stores, managers were contacted about lost items or sent a "receipt" claiming overcharging. Other FIN7 phishing emails masqueraded as detailed catering orders or requests for special menus tailored to individuals with dietary restrictions.

In early 2017, a pattern of complaints emerged and has continued for well over a year, where FIN7 has contacted stores and corporate offices to lodge food poisoning complaints with malicious attachments. Internally dubbed "FINdigestion" by FireEye, this pattern of detailed complaints eventually expanded beyond individual complaints and into litigious concerns raised on behalf of "the government", as shown in Figure 1.

Figure 1: FDA themed spear phishing email

It is noteworthy that the BATELEUR backdoor activity first identified by Proofpoint in July 2017, which FireEye tracks as a suspected FIN7 subgroup, uses highly-customized graphics for their targets, often created in Adobe Photoshop. In this same phishing campaign, FIN7's malicious attachment was graphically themed to match, as shown in Figure 2.



Figure 2: FDA themed spear phishing attachment

Throughout their operations, the professional design and continued development of phishing elements in parallel to other post-compromise tools indicated to FireEye that FIN7 was most likely a well-resourced criminal operation.

**It's Just Metadata**

FireEye has tracked several FIN7 personas throughout their operations by collecting and parsing filetypes of forensic value for juicy metadata. In a previous blog, we shared how LNK files created by FIN7 unintentionally revealed valuable information about their development environment.

LNK files can contain metadata that reveals attributes about the systems on which the LNKs were created, including original file paths, volume serial numbers, MAC addresses, and hostnames. By studying values within the LNK metadata we often identify "toolmarks," or unique values associated with distinct malware developer and operator personas.

FIN7 LNK metadata shows that the actors routinely used virtual machines with generic hostnames such as ANDY-PC or USER-PC, and default hostnames with the structure WIN-[A-Z0-9]{11} (e.g. WIN-ABCDEFGH1JK).

FireEye has tracked several hostname and path toolmarks associated with FIN7's operations, which we have used to link clusters of threat activity together. These toolmarks may be linked to FIN7 members who are involved in tool development or the broader criminal operation. Notable personas from the technical data, which are explored in more detail in the Technical Appendix section, include:

- "andy" / "andy-pc"
- "Hass"
- "jimbo"
- "Константин" (Konstantin)
- "oleg"

This analysis allowed us to understand FIN7's systems and correlate future attack activity to the different personas. Furthermore, the metadata analysis helped us monitor for files generated by the group and use the established toolmarks to establish detection for other adversary methodologies (such as direct RDP or SMB access) if the group changed TTPs.

**Video Playback of FIN7 Operations**

While responding to multiple FIN7 intrusions, FireEye recovered a custom video recording capability used by FIN7 as a part of their operations. FireEye's FLARE team reverse engineered the video protocol, which appeared to be custom-written by FIN7 as it has no external library dependencies, contained Cyrillic comments in the code, and required the use of a bespoke video player unique to FIN7. The attackers most likely leveraged this video recording capability in their arsenal to monitor operations in victim environments to inform later stages of their intrusions.

FireEye obtained a version of the criminal developers' video player from a trusted source and with the knowledge of the reverse engineered protocol, the FLARE team modified the source code to support multiple versions of FIN7's custom encoding. With the patched source code, FireEye can decode and playback FIN7's video monitoring for affected victims in possession of these files.

**Recent Shifts in FIN7 Operations**

Throughout 2018, FireEye has continued to identify multiple domains registered using patterns consistent with prior FIN7 activity, as well as campaigns using disparate TTPs that we have attributed to FIN7 with varying degrees of confidence. ZIP archives delivering the BIRDDOG backdoor were hosted on a portion of suspected FIN7 domains registered in 2018. Some evidence further characterizing the nature of this campaign suggests these malicious documents were sent to financial institution customers in Eastern Europe and Central Asia as early as September 2017. The targeting of individuals rather than organizations would mark a significant shift in their targeting, although it is also possible that the banks spoofed in these campaigns were FIN7's ultimate targets.

Additionally, we have identified similarities between FIN7 activity and BATELEUR campaigns, which began as early as mid-2017 and have been primarily aimed at U.S.-based restaurant chains. These campaigns leveraged macro-embedded Word documents directly attached to the emails as well as ones hosted on Google Drive. The documents were meticulously crafted to appear as though they came from legitimate organizations (e.g. restaurant associations and suppliers of POS hardware). This suspected FIN7 activity continued past the date of most recent arrest announced by U.S. law enforcement, although the attackers are now leveraging an updated JavaScript backdoor dubbed GRIFFON.

These recent campaigns could be representative of a decisive effort to diversify TTPs to avoid detection or could indicate the formation of FIN7 splinter groups carrying out autonomous campaigns. As a result, organizations need to remain vigilant and continue to monitor for changes in the methods employed by the FIN7 actors.

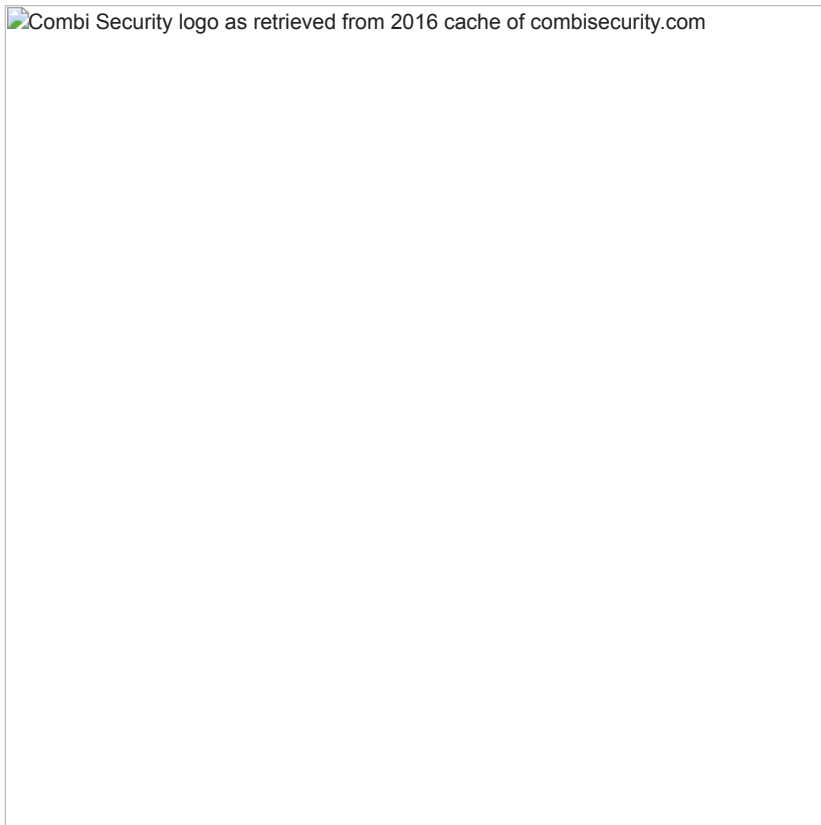**Unveiling FIN7's Front Company and Industry**

Figure 3: Combi Security logo as retrieved from 2016 cache of combisecurity.com

According to U.S. law enforcement, at least a portion of FIN7 activity was run out of a front company dubbed Combi Security. A cache of its website reveals that the company purported to be "the world leaders in the field of comprehensive protection of large information systems from modern cyber threats" with headquarters in Moscow, Haifa, and Odessa. We have identified job advertisements for Combi Security that have been posted on popular Russian, Ukrainian, and Uzbek job recruitment sites, as well as numerous individuals who most likely worked for the company. Due to the seeming legitimacy of the recruitment postings, some individuals may have been unaware of illicit nature of their work. While the recruitment of unwitting individuals as puppets has been a common component of at least some criminal schemes – for example, reshipping mules who are recruited through postings on career sites advertising attractive work-from-home jobs – FIN7's veiling of full-scale financial compromises as legitimate offensive security engagements is particularly notable. The apparent success of Combi Security in recruiting unsuspecting individuals in this manner, may lead to more of this type of technical recruitment by cyber criminals in the future.

## Splitting Up?

The criminal organization behind FIN7 is almost certainly comprised of many additional individuals beyond those already apprehended by law enforcement authorities. FireEye iSIGHT Intelligence expects that at least a portion of these malicious actors are likely to continue conducting cyber crime activity in some capacity. Although we expect activity to continue, it is extremely common for threat actors to either modify their TTPs or temporarily halt operations following significant developments such as arrests of high-level members and/or public disclosure of TTPs that they employ.

Depending on the organizational and communication structure of the group, it is also plausible that multiple subgroups could form and carry out independent operations in the future. Recent campaigns, as well as those using tactics that were atypical for historical FIN7 campaigns, such as the SEC campaigns with widespread targeting, may be representative of semi-autonomous groups pre-existing within, or cooperating with, the FIN7 criminal organization. As noted in our CARBANAK overview, certain malware families and techniques transcend strictly defined threat groups, and may be re-used by developers and operators as they transition between organizations and campaigns.

## Conclusion

These recent announcements by U.S. law enforcement highlight the positive impact that can result from synergy between private and public sector organizations in disrupting organized cyber crime operations. As demonstrated by FIN7, financially-motivated threat actors are becoming extremely advanced and are capable of inflicting significant harm on organizations through vast, but carefully orchestrated campaigns. As sophisticated threat groups continue to emerge, partnerships, such as those exhibited here, will almost certainly play a key role in combating these threats.

## Acknowledgements

Jordan Nuce, Tom Bennett, Michael Bailey, and Daniel Bohannon

## Technical Appendix

FireEye has responded to many FIN7 incidents, which has provided us extensive insight into their operations. As part of this blog post, we are also including numerous indicators that we attribute to FIN7 and an overview of their techniques to aid organizations in identifying malicious activity across their networks.

**Phishing Documents Technical Details**

In addition to LNK metadata, FIN7 phishing documents consistently contained artifacts detailing the local file system paths of component files used to construct the spear phishing documents. In the following tables, we have also included examples of the myriad of command line obfuscation techniques used by FIN7. Of particular note is the quick turnaround time between documents employing different techniques.

| EXIF Creation Time | Attribution | Malware | MD5 | Filename |
|---|---|---|---|---|
| 2018:05:21 17:32:00 | Suspected FIN7 | GRIFFON | 7e703dddcfc83cd352a910b48eaca95e | |
| C:\Users\**jimbo**\Desktop\Files\Картинки\outlook2.png | | | | |
| cmd.exe /k "SET a01=wscr& SET a02=ipt&&call %a01%%a02% /e:jscript //b %TEMP%\errors.txt | | | | |

| EXIF Creation Time | Attribution | Malware | MD5 | Filename |
|---|---|---|---|---|
| 2018:01:26 15:59:00 | Suspected FIN7 | BATELEUR | bb1a76702e2e7d0aa23385f24683d214 | Doc1.doc |
| C:\Users\**Hass**\Desktop\Картинки\New\outlook3.png | | | | |
| cmd.exe /c wscript.exe //b /e:jscript %TEMP%\crashpad.ini | | | | |

| EXIF Creation Time | Attribution | Malware | MD5 | Filename |
|---|---|---|---|---|
| 2018:01:11 13:16:00 | Suspected FIN7 | BATELEUR | 5972597b729a7d2853a3b37444e58e01 | check.doc |
| C:\Users\**Hass**\Desktop\Картинки\New\outlook2.png | | | | |
| cmd.exe /c wscript.exe //b /e:jscript %TEMP%\crashpad.ini | | | | |

| EXIF Creation Time | Attribution | Malware | MD5 | Filename |
|---|---|---|---|---|
| 2017:10:25 07:43:00 | Suspected FIN7 | BATELEUR | c4aabdcf19898d9c30c4c2edea0147f0 | document1.d |
| C:\Users\**oleg**\Desktop\Файлы\Картинки\New\defender.jpg | | | | |
| cmd.exe /c wscript.exe //b /e:jscript %TEMP%\crashpad.ini | | | | |

| EXIF Creation Time | Attribution | Malware | MD5 | Filename |
|---|---|---|---|---|
| 2017:06:23 15:18:00 | Suspected FIN7 | BATELEUR | 467062d2a5a341716c42c6d7f36ba0ed | check.doc |
| C:\Users\**Work**\Desktop\IMAGES\outlook2.png | | | | |
| wscript.exe //b /e:jscript %TEMP%\debug.txt | | | | |

Table 2: Suspected FIN7 spear phishing launch parameters and attacker local system artifacts

**EXIF Creation Time**

2017:10:06 11:21:00

C:\Users\**andy**\Desktop\unlock.cmd

cmd /c ""%TMP%\unlock.cmd" "

```
@set w=wsc@ript /b /e:js@cript %HOMEPATH%\tt.txt
@echo try{var fs=new ActiveXObject('Scripting.FileSystemObject');sh=new ActiveXObject('Wscript.Shell');p=sh.ExpandEnvironmentStrings('%%H
f=fs.OpenTextFile(p,1,false);for(i=0;i^<4;i++)f.SkipLine();var com='';while(!f.AtEndOfStream)com+=f.ReadLine().substr(1);f.Close();try{fs.DeleteFil
>%HOMEPATH%\tt.txt
@copy /y %TMP%\unlock.cmd %HOMEPATH%\pp.txt
@echo %w:@=%|cmd
```

**EXIF Creation Time**

2017:09:27 11:56:00

C:\Users\**usr**\Documents\send\270917\unlock.doc.lnk

wmic.exe process call create "cmd start /min cmd /c for /f \"usebackq delims=\" %x in (`FindStr /R /C:\"@#[0-9]#@\" \"%TEMP%\unlock.doc.lnk\"`)

```
cmd.exe /S /D /c" echo /*@#8#@*/try{sh=new ActiveXObject("Wscript.Shell");fs=new
ActiveXObject("Scripting.FileSystemObject");p=sh.ExpandEnvironmentStrings("%TM"+"P%");f=fs.GetFile(p+"//unlock.doc.lnk");s=f.OpenAsTextSt
(c);}catch(e){} >%HOMEPATH%\t.txt  & wscript //b /e:jscript %HOMEPATH%\t.txt  >nul 2>&1 &"
```

**EXIF Creation Time**

2017:08:08 17:38:00

C:\Users\**andy**\Desktop\unlock.doc.lnk

wmic.exe process call create "mshta javascript:eval(\"try{eval('wall=GetObject(\\'\\'"+String.fromCharCode(44)+'\\'Word.Application\\')');eval(wall.Ac

```
mshta.exe "try{jelo = 'try{w=GetObject("","Wor"+"d.Application");this[String.fromCharCode(101)+\\'va\\'+\\'l\\'](w.ActiveDocument.Shapes(1).TextFr
ActiveXObject("Scripting.FileSystemObject");var sh = new ActiveXObject("Wscript.Shell");var p = sh.ExpandEnvironmentStrings("%HOMEPATH%
```

**EXIF Creation Time**

2017:07:27 15:51:00

C:\Users\**jinvr-3-1**\Desktop\unlock.doc.lnk

```
cmd.exe /C set x=wsc@ript /e:js@cript %HOMEPATH%\ttt.txt & echo try{w=GetObject("","Wor"+"d.Application");this[String.fromCharCode(101)+'
>%HOMEPATH%\ttt.txt & echo %x:@=%|cmd
```

**EXIF Creation Time**

2017:06:28 16:21:00

C:\Users\**andy**\Desktop\unprotect.rtf.lnk

```
cmd.exe /C set x=wsc@ript /e:js@cript %HOMEPATH%\md5.txt & echo try{w=GetObject("","Wor"+"d.Application");this[String.fromCharCode(101
>%HOMEPATH%\md5.txt & echo %x:@=%|cmd
```

**EXIF Creation Time**

| | |
|---|---|
| 2017:05:11 12:59:00 | |

C:\Users\**user**\Documents\unprotect.lnk

C:\WINDOWS\system32\mshta.exe vbscript:Execute("On Error Resume Next:set yjdsqjtrn=GetObject(,""Word.Application""):execute yjdsqjtrn.Ac

**EXIF Creation Time**

2017:04:20 16:27:00

C:\Users\**testadmin.TEST**\Desktop\unprotect.lnk

C:\WINDOWS\system32\mshta.exe vbscript:Execute(&quot;On Error Resume Next:set wprotect=GetObject(,&quot;&quot;Word.Application&quot; wprotect.ActiveDocument.Shapes(1).TextFrame.TextRange.Text:close&quot;)

**EXIF Creation Time**

2017:01:12 18:00:00

C:\Users\**testadmin.TEST**\Desktop\unprotected.vbe
C:\Users\**tst01**\Desktop\unprotected.vbs

%WINDIR%\System32\Wscript.exe %TEMP%\WindowsUpdate_X24532\beginer.vbs

**EXIF Creation Time**

2016:08:12 11:26:00

C:\Users\**test**\Documents\sploits\120816\order.vbe

%WINDIR%\System32\Wscript.exe %TEMP%\AdobeUpdateManagementTool.vbs

Table 3: FIN7 spear phishing launch parameters and attacker local system artifacts

**FIN7 Tactics, Techniques & Procedures (TTPs)**

FireEye is providing insight into FIN7's notable methodologies across multiple stages of the attack lifecycle and tips for identifying evidence of this activity and similarly suspicious activity in your environment.

| Attack Lifecycle Stage | Adversary Methodology | Discovery Tips |
|---|---|---|
| **Initial Compromise** | Spear phishing emails sent using PHP Mailer | Inbound emails containing metadata such as "X-Mailer: PHPMailer" |
| **Establish Foothold** | Persistence using registry Run and Run Once keys | New Run and RunOnce registry entries referencing .VBS and .VBA |
| **Establish Foothold** | Execution or persistence using Scheduled Tasks | New Scheduled Tasks referencing .CMD, .LNK, .VBS, .VBA, .PS1 and other scripting language extensions |
| **Establish Foothold** | Persistence using Windows Services, Startup Directory | New Windows Services, new files in Startup directories |

| | | |
|---|---|---|
| **Establish Foothold** | Persistence using AppCompat Shim | New shim database files and modifications of AppCompatFlags registry keys (see [FIN7 SDB Persistence](#)) |
| **Maintain Presence** | C2 using favored C2 ports | Outbound connections with port-protocol mismatches on common ports such as 53,80,443,8080 |
| **Maintain Presence** | C2 using favored generic 3LDs | Outbound connections or DNS resolutions to "sketchy" 2$^{nd}$ level domains with generic 3$^{rd}$ level domains such as mail, www1, www2, dns, ftp (eg. "mail[.]qefg[.]info") |
| **Maintain Presence** | C2 using VPS infrastructure with low reputation | Inbound and outbound connections from and to non-standard IP ranges, especially from international Virtual Private Server (VPS) providers |
| **Maintain Presence** | C2 using legitimate services including Google Docs, Google Scripts and Pastebin | |
| **Maintain Presence** | C2 using DNS via A, OPT, TXT records | Unusually long or numerous DNS A, TXT and OPT record queries |
| **Maintain Presence** | C2 domains registered with REG.RU | Newly observed domains registered via REG.RU |
| **Maintain Presence** | C2 domains registered with NameCheap | Newly observed domains registered via NameCheap |
| **Maintain Presence** | C2 domains registered with odd format and top-level domains | Unusually long or numerous DNS queries with the structure [a-zA-Z]{4,5}\.[pw\|us\|club\|info\|site\|top] (eg. "pvze[.]club") |
| **Maintain Presence** | C2 domains registered with hyphen | Outbound connections to newly registered, hyphenated domains |

Table 4: FIN7 TTPs

**FIN7 Indicators**

FireEye is providing these granular technical indicators so that interested parties can better understand the threat actor and search for their historical activity across enterprise networks.

Phishing Documents Droppers

| Filename | MD5 | Attribution | Malware |
|---|---|---|---|
| menu.rtf | c14eb54769ff208a2562e4ef47958d9e | FIN7 | |
| | 76eb6f124fba6599a54e92b829c55b63 | FIN7 | BEACON |
| 3-ThompsonDan.rtf | 4b783bd0bd7fcf880ca75359d9fc4da6 | FIN7 | BEACON BELLHOP HALFBAKED |
| claim.rtf | af53db730732aa7db5fdd45ebba34b94 | FIN7 | BEACON BELLHOP HALFBAKED |
| order.rtf | cea2989309ccd5128f437335622978f1 | FIN7 | BEACON BELLHOP HALFBAKED |
| order.rtf | cf4ccb3707e5597969738b4754782e4d | FIN7 | BEACON BELLHOP HALFBAKED |

| | | | |
|---|---|---|---|
| Doc2_rtf.rtf | 2dc0f4bece10759307026d90f585e006 | FIN7 | BEACON HALFBAKED |
| doc1.doc | 37759603c6cd91ebc8a1ea9ac0f2d580 | FIN7 | BEACON HALFBAKED |
| quote.rtf | 3c0bd71e91e0f18621ba43de4419f901 | FIN7 | BEACON HALFBAKED |
| Doc2_rtf.rtf | 562a64f1c09306d385962cf8084b6827 | FIN7 | BEACON HALFBAKED |
| information.doc | 5dace5ac5ba89c9bba4479264f75b2b6 | FIN7 | BEACON HALFBAKED |
| Doc_rest_rtf.rtf | 619aa4e6c9db275381ab0e7fc7078f5f | FIN7 | BEACON HALFBAKED |
| doc1.docx | 67c9bfd4d6ac397fb0cd7da2441a6fe2 | FIN7 | BEACON HALFBAKED |
| Doc33.docx | 6a5a42ed234910121dbb7d1994ab5a5e | FIN7 | BEACON HALFBAKED |
| info_.rtf | 6ac5ae6546746e3a9502cc489b71146e | FIN7 | BEACON HALFBAKED |
| bmg.docx | 754fc509328af413d93131e65fc46d31 | FIN7 | BEACON HALFBAKED |
| Doc_0405_1.rtf | 7b2315ff1f2d763857aa70ad34b75449 | FIN7 | BEACON HALFBAKED |
| doc1.docx | 99975b5ee2ddd31e89c9bdda7a3871d9 | FIN7 | BEACON HALFBAKED |
| doc0505_1.rtf | 9eb71edd5ec99294a1c341efa780b1b1 | FIN7 | BEACON HALFBAKED |
| DonovanR.docx | b5829caad7c448c558cb1dab2d9f4320 | FIN7 | BEACON HALFBAKED |
| rising star.rtf | c8b8420d1503ae48ff35362f5d29eeb3 | FIN7 | BEACON HALFBAKED |
| inf6.docx | e494356fc0db7ef6009d29e5ae869717 | FIN7 | BEACON HALFBAKED |
| Claim.docx | 06b9e2fdd2c0eeb78b851c93ca66f25f | FIN7 | BELLHOP |
| order.rtf | 80eed9f87a18b0093eb3f16fa495b6f7 | FIN7 | BELLHOP |
| Details Joseph.docx | b4d48f3e1ae339f2fcb94b7abceecfff | FIN7 | BELLHOP |
| order.doc | e2a6b351c276d02d71e18cd0677e8236 | FIN7 | BELLHOP HALFBAKED |
| | b14bc8cbc7f2d36179ebff96ade6d867 | FIN7 | CARBANAK |

| | | | |
|---|---|---|---|
| features.doc | bbd99ef280efebe9066c0aef91bf02cd | FIN7 | DRIFTPIN HALFBAKED |
| doc2709.rtf | 01d666fcbc4cdcedbfe7963f498e7858 | FIN7 | HALFBAKED |
| doc_n0908.rtf | 03e85ad4217775906e6b5ceae8dc27af | FIN7 | HALFBAKED |
| doc1.docx | 0d6619481cfd29791a51ebb42ace5c03 | FIN7 | HALFBAKED |
| doc1.rtf | 0e0a51489054529a9dcb177d39f08b81 | FIN7 | HALFBAKED |
| doc0719.docx | 101bdbbd99cfd74aa5724842404642f2 | FIN7 | HALFBAKED |
| doc0507.docx | 17fabe288d640476a70154c59d5a1ba1 | FIN7 | HALFBAKED |
| info_1.rtf | 189c5a090d2b3b87ab65a8b156cd971e | FIN7 | HALFBAKED |
| doc.docx | 1a6c18967f4ce1c91c77098af4957e6e | FIN7 | HALFBAKED |
| Mail.rtf | 1a9e113b2f3caa7a141a94c8bc187ea7 | FIN7 | HALFBAKED |
| Doc_rest_n_rtf.rtf | 1f5022a02c82fbe414dc91bf3f1b5180 | FIN7 | HALFBAKED |
| doc.docx | 1f98c4ff12fc2c6fbf8247a5b2e4e7f4 | FIN7 | HALFBAKED |
| doc1909.docx | 1fbe77a3b5771ce4f95e02a49c5b7f30 | FIN7 | HALFBAKED |
| doc_n0808.rtf | 21926646a658bdf39cf28cdfbb1aced7 | FIN7 | HALFBAKED |
| doc0507.rtf | 22ad7c05128ca7b48b0a2a4507803b16 | FIN7 | HALFBAKED |
| Doc2.docx | 22e7d4f7401ef34b3b6d17c15291c497 | FIN7 | HALFBAKED |
| menu.rtf | 24fab1e9831e57307d17981abaabf960 | FIN7 | HALFBAKED |
| 2-order.docx | 28ad8e3a225400a1d00f6023f8e6c9c8 | FIN7 | HALFBAKED |
| doc0610.docx | 29a3666cee0762fcd731fa663ebc0011 | FIN7 | HALFBAKED |
| doc2209_1.rtf | 2d36634974c85eff393698b39edc561c | FIN7 | HALFBAKED |
| Doc1.rtf | 307a9ce257e97189e046fa91d3c27dab | FIN7 | HALFBAKED |
| doc1.rtf | 325844f1b956c52fc220932bc717f224 | FIN7 | HALFBAKED |
| doc0910.rtf | 3917028799d2aa3a43ec5bad067e99a5 | FIN7 | HALFBAKED |
| doc1.docx | 397d45b6001919b04739e26379c84dd9 | FIN7 | HALFBAKED |
| docr.rtf | 3a303f02e16d7d27fa78c3f48a55d992 | FIN7 | HALFBAKED |
| oliver_davis.docx | 3b12f36a01326ec649e4def08b860339 | FIN7 | HALFBAKED |
| doc2209.docx.docx | 402c34d7d6ce92bf5a048023bd2fde4a | FIN7 | HALFBAKED |

| | | | |
|---|---|---|---|
| Dooq.docx | 41c6861313e731bd3f84dd70360573ce | FIN7 | HALFBAKED |
| info.rtf | 42a2a2352f6b1f5818f3b695f240fc3a | FIN7 | HALFBAKED |
| james.docx | 499ebef3ab31a2f98fc8a358bd085b0f | FIN7 | HALFBAKED |
| doc1007.rtf | 4b7a742d5c98fc62f0f67445032e7bc6 | FIN7 | HALFBAKED |
| tem6.doc | 4bf691809224d17e49cebb071d22a867 | FIN7 | HALFBAKED |
| doc1.rtf | 511af2b4c62fa4c2bb91f3be1ca96094 | FIN7 | HALFBAKED |
| doc1.docx | 52cf6a63da29331d805a5a9b5015580f | FIN7 | HALFBAKED |
| doc2209.rtf | 560e72858ee413d7a6f72fff5ab7577b | FIN7 | HALFBAKED |
| doc1.docx | 5a0b796c7a6040e02c822cac4475f11a | FIN7 | HALFBAKED |
| doc0717.rtf | 5d49b444734b003b6917b81f0a779b3e | FIN7 | HALFBAKED |
| | 5d9525b48870dc438130bd96fb8c5b66 | FIN7 | HALFBAKED |
| doc2.doc | 5dd2e677fd1d65f051b7f54e7402721f | FIN7 | HALFBAKED |
| Dooq.docx | 63e2eb258a85ed4e72f951cdbff2a58e | FIN7 | HALFBAKED |
| doc0720.rtf | 6a860285a6f7521995151a2a0cb6e316 | FIN7 | HALFBAKED |
| doc0719.rtf | 6adec78e874232722c3758bbbcb95829 | FIN7 | HALFBAKED |
| virus.docx | 70f0f8db551dd6b084682188c3923e26 | FIN7 | HALFBAKED |
| check.rtf | 72d973ebfbc00d26170bfafdfbbd0179 | FIN7 | HALFBAKED |
| Doc_0405.rtf | 74165408ff12d195fb9d68afe0a6011e | FIN7 | HALFBAKED |
| oliver_davis.rtf | 793511c86a0469d579ff8cc99a7311e3 | FIN7 | HALFBAKED |
| doc_n0808.docx | 79628a598303692238cc4aeb19da6fed | FIN7 | HALFBAKED |
| Doc1.rtf | 7d664485c53b98180e6f3c69e9dfa81e | FIN7 | HALFBAKED |
| doc1.docx | 82a32d98e68891625b6de67a9d0b61c6 | FIN7 | HALFBAKED |
| document.doc | 853a53419d9dbc606d2392b99e60c173 | FIN7 | HALFBAKED |
| doc2806.rtf | 856cec68ddd28367c0d0f0a6f566187a | FIN7 | HALFBAKED |
| doc1.rtf | 8608b31a446f42a7f36807bd6c16d2c0 | FIN7 | HALFBAKED |
| Doc1.rtf | 8bd798e89d075827cc757b9586f15ce2 | FIN7 | HALFBAKED |
| doc1.rtf | 94771bcf572d5c0b834f73d577f06cc8 | FIN7 | HALFBAKED |

| | | | |
|---|---|---|---|
| doc1610.rtf | 973377e27b5dffa289f84e62a6833ebc | FIN7 | HALFBAKED |
| Doc0725.rtf | 9788b3faa29ba9eb4cae46f3c249937e | FIN7 | HALFBAKED |
| Doc1.rtf | 9b87f9f6498c241f50208f9906907195 | FIN7 | HALFBAKED |
| doc1.rtf | a5f75333d0c81387a5a9c7696b967a20 | FIN7 | HALFBAKED |
| doc0610.rtf | a8e312d0c230e226e97e7a441fadbd85 | FIN7 | HALFBAKED |
| doc2_r_new.rtf | a9c50b7761519fb684cdee2d59f99f91 | FIN7 | HALFBAKED |
| credit details.rtf | aaf42acedc38565f4c33cfdbb09733b9 | FIN7 | HALFBAKED |
| doc2.docx_ | b5cc86726ab8f1fb3c281ab8f935260f | FIN7 | HALFBAKED |
| | b6f005236a37367a147f9060c708ccca | FIN7 | HALFBAKED |
| doc1.rtf | c0d122bcdcb6ede7fc7f1182e4d0e599 | FIN7 | HALFBAKED |
| doc2806.docx | c3f48e69bb90be828ba2835b76fb2080 | FIN7 | HALFBAKED |
| doc1.rtf | c5e94d973ed4f963ddc09ab88def3b5f | FIN7 | HALFBAKED |
| doc1.rtf | c6cddc475d62503a17a34419918e7fc0 | FIN7 | HALFBAKED |
| doc0714.docx | caec3babdec3cf267cc846fd084c4626 | FIN7 | HALFBAKED |
| doc1909.rtf | d1f55491472ca747561509106b71eab8 | FIN7 | HALFBAKED |
| doc_n0908.docx | d38fb2d95812ffa1014e52ef3079e5da | FIN7 | HALFBAKED |
| catering_.rtf | d5cd1dedf3bf5c943e348a8b84e37b2a | FIN7 | HALFBAKED |
| doc0714.rtf | dde72a54716deb88c1ffef2a63faab6b | FIN7 | HALFBAKED |
| m1.doc | e0ca85c0d264b84d977df0c48fd383cc | FIN7 | HALFBAKED |
| doc1.rtf | e17fe2978ebe1b0a6923acd2ffeda3c2 | FIN7 | HALFBAKED |
| doc2009.rtf | e184219366afb2e6bd0b9502beab1156 | FIN7 | HALFBAKED |
| doc1610.docx | e9154e2f80389b853ab4cf2fe98f1ed2 | FIN7 | HALFBAKED |
| doc1.rtf | edc4f02f265a4aaa552435f293409f01 | FIN7 | HALFBAKED |
| doc2_r_new.rtf | ee5a600ef9fd1defe07ea097095d1beb | FIN7 | HALFBAKED |
| doc1.rtf | effdaf7f61acb277ac44ee4d9bc8900a | FIN7 | HALFBAKED |
| info_.docx | f2ac2ec8173db4963dc2089ac90b8807 | FIN7 | HALFBAKED |
| Doc0725.docx | f80a80d25b3393825baa1e84e76ddf6c | FIN7 | HALFBAKED |

| | | | |
|---|---|---|---|
| 1.rtf | fa1c548a5d691ac9ce7bfd929f204261 | FIN7 | HALFBAKED |
| | fa93c93a02fe2dee8a3b3d1cd82f293f | FIN7 | HALFBAKED |
| poisoning.rtf | faed087e820cad3c023be1db8d4ba70a | FIN7 | HALFBAKED |
| order.docx | fc661e18137583dc140e201338582a99 | FIN7 | HALFBAKED |
| SEC_Security_Policy_2017_02.doc | 032fe02e54a010d21fd71e97596f4101 | FIN7 | POWERSOURCE |
| SEC_Security_Policy_2017_10.doc | 14334c8f93f049659212773ecee477a2 | FIN7 | POWERSOURCE |
| VargheseJ.doc | 2abad0ae32dd72bac5da0af1e580a2eb | FIN7 | POWERSOURCE |
| SEC_Security_Policy_2017_03.doc | 37d323ffc33a0e1c6cd20234589a965d | FIN7 | POWERSOURCE |
| 2017.doc | 5a88e3825c5e89b07fa9050b6b6eca7c | FIN7 | POWERSOURCE |
| SEC_Security_Policy_2017.doc | 6ff3272cd9edf115230bad6a55cb3ca8 | FIN7 | POWERSOURCE |
| EDGAR_FILLINGS_RULES_2016.doc | 7bd2235f105dee20825b4395a04892bf | FIN7 | POWERSOURCE |
| SEC_Security_Policy_2017_05.doc | 8fa8d4c30429c099dc7e565e57db55c0 | FIN7 | POWERSOURCE |
| SEC_Security_Policy_2017_06.doc | ccd2372bb6b07f1b5a125e597005688d | FIN7 | POWERSOURCE |
| Important_Changes_to_Form10_K.doc | d04b6410dddee19adec75f597c52e386 | FIN7 | POWERSOURCE |
| SEC_Security_Policy_2017.doc | f20328b49ec605fd425ed101ff31f14b | FIN7 | POWERSOURCE |
| SEC_Security_Policy_2017_07.doc | f74958adcfb11abcb37e043013f6a90f | FIN7 | POWERSOURCE |
| Filings_and_Forms.docx | 47111e9854db533c328ddbe6e962602a | FIN7 | POWERSOURCE (Downloader) |
| doc.doc | 189c72bfd8ae31abcff5e7da691a7d30 | Suspected FIN7 | BATELEUR |
| protected_instructions.doc | 302ab8bd6a8effa58a675165aa9600a2 | Suspected FIN7 | BATELEUR |
| Doc2.doc | 40c4c02d1e506a5ffc2939ec0ee8e105 | Suspected FIN7 | BATELEUR |
| 3528579_security_protocol.doc | 58fbf6f9405327d8d158a1eeac19b81a | Suspected FIN7 | BATELEUR |
| check.doc | 5972597b729a7d2853a3b37444e58e01 | Suspected FIN7 | BATELEUR |
| | 6fff1d68203f8d23ccd23507ba00b9df | Suspected FIN7 | BATELEUR |
| check.doc | 762eef684e01831aa2f96031eff378bf | Suspected FIN7 | BATELEUR |
| check.doc | 9b1af2d9c0c0687c70466385800b6847 | Suspected FIN7 | BATELEUR |
| Doc1.doc | bb1a76702e2e7d0aa23385f24683d214 | Suspected FIN7 | BATELEUR |
| check.doc | d4088f8202e0eb27f90e692f988f0780 | Suspected FIN7 | BATELEUR |

| | | | |
|---|---|---|---|
| invoices.doc | dc8b30c5253f02a790a31f2853fe41f8 | Suspected FIN7 | BATELEUR |
| blah.doc | e020668055eb1d22710aa07f72860075 | Suspected FIN7 | BATELEUR |
| photos.doc | c517f48bf95a4f3ecba2046d12e62c88 | Suspected FIN7 | GRIFFON |
| test.doc | d7ca38e21327541787ab84bde83d7f81 | Suspected FIN7 | GRIFFON |

Additional Malware

| MD5 | Malware | Attribution |
|---|---|---|
| 5f73beb23c45006ad952a71fa62c6f9f | BABYMETAL | FIN7 |
| a3754fba24f85d1d1bb7c0382e41586b | BABYMETAL | FIN7 |
| dad8ebcbb5fa6721ccad45b81874e22c | BABYMETAL | FIN7 |
| ecd8879702347966750c37247ef6c2e6 | BABYMETAL | FIN7 |
| 039d9e47e4474bee24785f8ec5307695 | BIRDDOG | FIN7 |
| 92dfd0534b080234f9536371be63e37a | BIRDDOG | FIN7 |
| 188f261e5fca94bd1fc1edc1aafee8c0 | CARBANAK | FIN7 |
| 2828ea78cdda8f21187572c99ded6dc2 | CARBANAK | FIN7 |
| 291a17814d5dbb5bce5b186334cde4b1 | CARBANAK | FIN7 |
| 4b3dac0a4f452b07d29f26b119180bd2 | CARBANAK | FIN7 |
| 4eda75dfd4d12eda6a6219423b5972bd | CARBANAK | FIN7 |
| 6e9408c338e98a8bc166a8d4f8264019 | CARBANAK | FIN7 |
| 749c5085cda920e830cfed32842ba835 | CARBANAK | FIN7 |
| 80b022b39d91527f6ae5b4834d7c8173 | CARBANAK | FIN7 |
| 8ae284d547bd1b8bd6bc2431735f9142 | CARBANAK | FIN7 |
| 8e1e7f5ad99e48b740fd00085eab1f84 | CARBANAK | FIN7 |
| 9ae433cd5397af6b485f1abb06b2c5a2 | CARBANAK | FIN7 |
| be1154e38df490e1dcbde3ffb2ebd05c | CARBANAK | FIN7 |
| c6b57e042ceadb60d6fab217d3523e17 | CARBANAK | FIN7 |
| c6ec176592ea26c4ee27974273e592ff | CARBANAK | FIN7 |
| dd4f312c7e1c25564a8d00b0f3495e24 | CARBANAK | FIN7 |

| | | |
|---|---|---|
| facd37cd76989f45088ae98de8ed7aa0 | CARBANAK | FIN7 |
| 4dc99280459292ef60d6d01ed8ece312 | DRIFTPIN | FIN7 |
| 63241a3580cd1135170b044a84005e92 | DRIFTPIN | FIN7 |
| 70345aa0b970e1198a9267ae4532a11b | DRIFTPIN | FIN7 |
| de50d41d70b8879cdc73e684ad4ebe9f | DRIFTPIN | FIN7 |
| ddc9b71808be3a0e180e2befae4ff433 | SIMPLECRED | FIN7 |
| 90f35fd205556a04d13216c33cb0dbe3 | BIRDDOG | Suspect FIN7 |

IPs

| IP Address | Malware | Attribution |
|---|---|---|
| 107.161.159.17 | CARBANAK | FIN7 |
| 107.181.160.12 | CARBANAK | FIN7 |
| 107.181.160.75* | DRIFTPIN HALFBAKED | FIN7 |
| 162.244.32.168 | CARBANAK | FIN7 |
| 162.244.32.175 | CARBANAK | FIN7 |
| 179.43.140.82* | CARBANAK | FIN7 |
| 179.43.140.85* | CARBANAK | FIN7 |
| 179.43.160.162 | CARBANAK | FIN7 |
| 179.43.160.215 | CARBANAK | FIN7 |
| 185.104.8.173 | CARBANAK | FIN7 |
| 198.100.119.28 | CARBANAK | FIN7 |
| 204.155.30.100 | CARBANAK | FIN7 |
| 204.155.30.100 | DRIFTPIN HALFBAKED | FIN7 |
| 23.249.162.161 | CARBANAK | FIN7 |
| 5.8.88.64 | BIRDDOG | FIN7 |
| 94.140.120.132 | CARBANAK | FIN7 |
| 95.215.45.95 | CARBANAK | FIN7 |
| 95.215.46.70 | CARBANAK | FIN7 |

| IP | Malware | Attribution |
|---|---|---|
| 95.215.46.76 | CARBANAK | FIN7 |
| 185.66.15.50 | | Suspected FIN7 |
| 194.165.16.113 | | Suspected FIN7 |
| 46.161.3.23 | | Suspected FIN7 |
| 85.93.2.148 | | Suspected FIN7 |
| 85.93.2.149 | | Suspected FIN7 |
| 81.177.27.41 | | Suspected FIN7 |
| 95.46.45.128 | BATELEUR | Suspected FIN7 |
| 185.17.121.200 | BATELEUR | Suspected FIN7 |
| 185.20.184.109* | BATELEUR | Suspected FIN7 |
| 185.220.35.20 | BATELEUR | Suspected FIN7 |
| 185.5.248.167* | BATELEUR | Suspected FIN7 |
| 194.165.16.134 | BATELEUR | Suspected FIN7 |
| 195.133.48.65 | BATELEUR | Suspected FIN7 |
| 195.133.49.73 | BATELEUR | Suspected FIN7 |
| 217.23.155.19 | BATELEUR | Suspected FIN7 |
| 31.184.234.66 | BATELEUR | Suspected FIN7 |
| 31.184.234.71 | BATELEUR | Suspected FIN7 |
| 5.188.10.102 | BATELEUR | Suspected FIN7 |
| 5.188.10.102 | BATELEUR | Suspected FIN7 |
| 5.188.10.248 | BATELEUR | Suspected FIN7 |
| 85.93.2.111 | BATELEUR | Suspected FIN7 |
| 85.93.2.148 | BATELEUR | Suspected FIN7 |
| 85.93.2.56 | BATELEUR | Suspected FIN7 |
| 85.93.2.73 | BATELEUR | Suspected FIN7 |
| 85.93.2.92 | BATELEUR | Suspected FIN7 |
| 89.223.30.99 | BATELEUR | Suspected FIN7 |

| | | |
|---|---|---|
| 104.193.252.167 | HALFBAKED | FIN7 |
| 104.232.34.166 | HALFBAKED | FIN7 |
| 104.232.34.36 | HALFBAKED | FIN7 |
| 107.181.160.76* | HALFBAKED | FIN7 |
| 119.81.178.100 | HALFBAKED | FIN7 |
| 119.81.178.101 | HALFBAKED | FIN7 |
| 138.201.44.3 | HALFBAKED | FIN7 |
| 138.201.44.4 | HALFBAKED | FIN7 |
| 179.43.147.71 | HALFBAKED | FIN7 |
| 185.180.197.20 | HALFBAKED | FIN7 |
| 185.180.197.34 | HALFBAKED | FIN7 |
| 185.86.151.175 | HALFBAKED | FIN7 |
| 191.101.242.162 | HALFBAKED | FIN7 |
| 195.54.162.237* | HALFBAKED | FIN7 |
| 195.54.162.245 | HALFBAKED | FIN7 |
| 195.54.162.79* | HALFBAKED | FIN7 |
| 198.100.119.6 | HALFBAKED | FIN7 |
| 198.100.119.7 | HALFBAKED | FIN7 |
| 204.155.31.167 | HALFBAKED | FIN7 |
| 204.155.31.174 | HALFBAKED | FIN7 |
| 217.12.208.80 | HALFBAKED | FIN7 |
| 31.148.219.141* | HALFBAKED | FIN7 |
| 31.148.219.18* | HALFBAKED | FIN7 |
| 31.148.219.44* | HALFBAKED | FIN7 |
| 31.148.220.107* | HALFBAKED | FIN7 |
| 31.148.220.215* | HALFBAKED | FIN7 |
| 5.149.250.235 | HALFBAKED | FIN7 |

| | | |
|---|---|---|
| 5.149.250.241 | HALFBAKED | FIN7 |
| 5.149.252.144 | HALFBAKED | FIN7 |
| 5.149.253.126 | HALFBAKED | FIN7 |
| 8.28.175.68* | HALFBAKED | FIN7 |
| 81.17.28.118* | HALFBAKED | FIN7 |
| 91.235.129.251* | HALFBAKED | FIN7 |
| 94.140.120.122 | HALFBAKED | FIN7 |
| 94.140.120.134 | HALFBAKED | FIN7 |
| 95.215.46.229 | HALFBAKED | FIN7 |
| 95.215.47.105 | HALFBAKED | FIN7 |
| 5.135.73.113 | BIRDDOG | Suspect FIN7 |
| 5.8.88.64 | BIRDDOG | FIN7 |

*VPS that may also have legitimate traffic.

Full Qualified Domain Names (FQDNs)

| Domain | Malware | Attribution |
|---|---|---|
| bigred-tours.com | | FIN7 |
| clients12-google.com | BEACON.DNS | FIN7 |
| clients2-google.com | | FIN7 |
| p3-marketing.com | | FIN7 |
| cdn-googleapi.com | GRIFFON | Suspect FIN7 |
| cdn-googleservice.com | GRIFFON | Suspect FIN7 |
| acity-lawfirm.com | | FIN7 |
| algew.me | POWERSOURCE | FIN7 |
| aloqd.pw | POWERSOURCE | FIN7 |
| amhs.club | TEXTMATE | FIN7 |
| anselbakery.com | | FIN7 |
| apvo.club | TEXTMATE | FIN7 |
| arctic-west.com | | FIN7 |

| | | |
|---|---|---|
| auyk.club | POWERSOURCE | FIN7 |
| b-bconsult.com | | FIN7 |
| bcleaningservice.com | | FIN7 |
| bigrussianbss.com | | FIN7 |
| bipismol.com | | FIN7 |
| bipovnerlvd.com | | FIN7 |
| blopsadmvdrl.com | | FIN7 |
| blopsdmvdrl.com | | FIN7 |
| bnrnboerxce.com | | FIN7 |
| bpee.pw | POWERSOURCE | FIN7 |
| bureauofinspections.com | | FIN7 |
| bvyv.club | POWERSOURCE TEXTMATE | FIN7 |
| bwuk.club | POWERSOURCE TEXTMATE | FIN7 |
| bwwrvada.com | | FIN7 |
| cgqy.us | POWERSOURCE TEXTMATE | FIN7 |
| chatterbuzz-media.com | | FIN7 |
| chenstravelconsulting.com | | FIN7 |
| cihr.site | POWERSOURCE TEXTMATE | FIN7 |
| citizentravel.biz | | FIN7 |
| cjsanandreas.com | | FIN7 |
| ckwl.pw | POWERSOURCE TEXTMATE | FIN7 |
| cloo.com | POWERSOURCE | FIN7 |
| cnkmoh.pw | POWERSOURCE | FIN7 |
| cnlu.net | TEXTMATE | FIN7 |
| cnmah.pw | POWERSOURCE | FIN7 |

| | | |
|---|---|---|
| coec.club | POWERSOURCE TEXTMATE | FIN7 |
| coffee-joy-usa.com | | FIN7 |
| cspg.pw | TEXTMATE | FIN7 |
| ctxdns.org | | FIN7 |
| ctxdns.pw | | FIN7 |
| cuuo.us | POWERSOURCE TEXTMATE | FIN7 |
| daskd.me | POWERSOURCE | FIN7 |
| dbxa.pw | POWERSOURCE TEXTMATE | FIN7 |
| ddmd.pw | POWERSOURCE | FIN7 |
| deliciouswingsny.com | | FIN7 |
| dlex.pw | POWERSOURCE | FIN7 |
| dlox.pw | POWERSOURCE | FIN7 |
| dnstxt.net | | FIN7 |
| dnstxt.org | | FIN7 |
| doof.pw | POWERSOURCE | FIN7 |
| dosdkd.mo | POWERSOURCE | FIN7 |
| dpoo.pw | POWERSOURCE | FIN7 |
| dsud.com | POWERSOURCE | FIN7 |
| dtxf.pw | POWERSOURCE | FIN7 |
| duglas-manufacturing.com | | FIN7 |
| dvso.pw | POWERSOURCE TEXTMATE | FIN7 |
| dyiud.com | POWERSOURCE | FIN7 |
| eady.club | POWERSOURCE TEXTMATE | FIN7 |
| enuv.club | POWERSOURCE TEXTMATE | FIN7 |
| eter.pw | POWERSOURCE TEXTMATE | FIN7 |

| | | |
|---|---|---|
| extmachine.biz | | FIN7 |
| facs.pw | TEXTMATE | FIN7 |
| fbjz.pw | POWERSOURCE TEXTMATE | FIN7 |
| fhyi.club | POWERSOURCE TEXTMATE | FIN7 |
| firsthotelgroup.com | | FIN7 |
| firstprolvdrec.com | | FIN7 |
| fkij.net | TEXTMATE | FIN7 |
| flowerprosv.com | | FIN7 |
| fredbanan.com | POWERSOURCE | FIN7 |
| futh.pw | POWERSOURCE TEXTMATE | FIN7 |
| gcan.site | TEXTMATE | FIN7 |
| ge-stion.com | | FIN7 |
| gjcu.pw | POWERSOURCE | FIN7 |
| gjuc.pw | POWERSOURCE | FIN7 |
| glavpojdfde.com | BEACON.DNS | FIN7 |
| gnoa.pw | POWERSOURCE TEXTMATE | FIN7 |
| gnsn.us | TEXTMATE | FIN7 |
| goldman-travel.com | | FIN7 |
| goproders.com | BEACON.DNS | FIN7 |
| gprw.site | TEXTMATE | FIN7 |
| grand-mars.ru | | FIN7 |
| grij.us | POWERSOURCE TEXTMATE | FIN7 |
| gsdg.site | TEXTMATE | FIN7 |
| guopksl.com | BEACON.DNS | FIN7 |
| gxhp.top | POWERSOURCE TEXTMATE | FIN7 |

| | | |
|---|---|---|
| hijrnataj.com | | FIN7 |
| hilertonv.com | BEACON.DNS | FIN7 |
| hilopser.com | BEACON.DNS | FIN7 |
| hippsjnv.com | | FIN7 |
| hldu.site | POWERSOURCE | FIN7 |
| hoplessinple.com | | FIN7 |
| hoplessinples.com | | FIN7 |
| hopsl3.com | BEACON.DNS | FIN7 |
| hvzr.info | POWERSOURCE TEXTMATE | FIN7 |
| idjb.us | POWERSOURCE TEXTMATE | FIN7 |
| ihrs.pw | POWERSOURCE | FIN7 |
| imyo.site | TEXTMATE | FIN7 |
| itstravel-ekb.ru | | FIN7 |
| ivcm.club | TEXTMATE | FIN7 |
| jblz.net | TEXTMATE | FIN7 |
| jersetl.com | BEACON.DNS | FIN7 |
| jimw.club | POWERSOURCE TEXTMATE | FIN7 |
| jipdfonte.com | | FIN7 |
| jiposlve.com | BEACON.DNS | FIN7 |
| jjee.site | POWERSOURCE | FIN7 |
| johsimsoft.org | | FIN7 |
| jomp.site | POWERSOURCE TEXTMATE | FIN7 |
| josephevinchi.com | | FIN7 |
| just-easy-travel.com | | FIN7 |
| juste-travel.com | HALFBAKED | FIN7 |

| | | |
|---|---|---|
| jxhv.site | POWERSOURCE TEXTMATE | FIN7 |
| kalavadar.com | | FIN7 |
| kashtanspb.ru | | FIN7 |
| kbep.pw | TEXTMATE | FIN7 |
| kiposerd.com | BEACON.DNS | FIN7 |
| kiprovol.com | | FIN7 |
| kiprovolswe.com | | FIN7 |
| kjke.pw | POWERSOURCE | FIN7 |
| kjko.pw | POWERSOURCE | FIN7 |
| koldsdes.com | | FIN7 |
| kshv.site | POWERSOURCE TEXTMATE | FIN7 |
| kuyarr.com | | FIN7 |
| kwoe.us | POWERSOURCE TEXTMATE | FIN7 |
| ldzp.pw | POWERSOURCE | FIN7 |
| lgdr.com | POWERSOURCE | FIN7 |
| lhlv.club | POWERSOURCE TEXTMATE | FIN7 |
| lnoy.site | POWERSOURCE TEXTMATE | FIN7 |
| luckystartwith.com | | FIN7 |
| lvrm.pw | POWERSOURCE TEXTMATE | FIN7 |
| lvxf.pw | POWERSOURCE | FIN7 |
| manchedevs.org | | FIN7 |
| maofmdfd5.com | | FIN7 |
| meli-travel.com | HALFBAKED | FIN7 |
| melitravel.ru | | FIN7 |
| mewt.us | POWERSOURCE | FIN7 |

| | | |
|---|---|---|
| mfka.pw | POWERSOURCE TEXTMATE | FIN7 |
| michigan-construction.com | | FIN7 |
| mjet.pw | POWERSOURCE | FIN7 |
| mjot.pw | POWERSOURCE | FIN7 |
| mjut.pw | POWERSOURCE | FIN7 |
| mkwl.pw | TEXTMATE | FIN7 |
| molos-2.com | BEACON.DNS | FIN7 |
| mtgk.site | POWERSOURCE | FIN7 |
| mtxf.com | TEXTMATE | FIN7 |
| muedandubai.com | | FIN7 |
| muhh.us | POWERSOURCE | FIN7 |
| mut.pw | POWERSOURCE | FIN7 |
| mvze.pw | POWERSOURCE | FIN7 |
| mvzo.pw | POWERSOURCE | FIN7 |
| mxfg.pw | POWERSOURCE | FIN7 |
| mxtxt.net | | FIN7 |
| myspoernv.com | | FIN7 |
| navigators-travel.com | | FIN7 |
| neartsay.com | | FIN7 |
| nevaudio.com | | FIN7 |
| neverfaii.com | | FIN7 |
| nroq.pw | POWERSOURCE | FIN7 |
| ns0.site | POWERPIPE | FIN7 |
| ns0.space | POWERPIPE | FIN7 |
| ns0.website | POWERPIPE | FIN7 |
| ns1.press | POWERPIPE POWERSOURCE.V2 | FIN7 |

| | | |
|---|---|---|
| ns1.website | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns2.press | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns3.site | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns3.space | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns4.site | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns4.space | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns5.biz | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns5.online | POWERPIPE POWERSOURCE.V2 | FIN7 |
| ns5.pw | MAL | FIN7 |
| ntlw.net | POWERSOURCE | FIN7 |
| nwrr.pw | POWERSOURCE | FIN7 |
| nxpu.site | POWERSOURCE TEXTMATE | FIN7 |
| oaax.site | POWERSOURCE TEXTMATE | FIN7 |
| odwf.pw | POWERSOURCE | FIN7 |
| odyr.us | POWERSOURCE TEXTMATE | FIN7 |
| okiq.pw | POWERSOURCE | FIN7 |
| oknz.club | POWERSOURCE TEXTMATE | FIN7 |
| olckwses.com | | FIN7 |
| olgw.my | POWERSOURCE | FIN7 |
| oloqd.pw | POWERSOURCE | FIN7 |
| oneliveforcopser.com | | FIN7 |
| onokder.com | BEACON.DNS | FIN7 |
| ooep.pw | POWERSOURCE TEXTMATE | FIN7 |

| | | |
|---|---|---|
| oof.pw | POWERSOURCE | FIN7 |
| ooyh.us | POWERSOURCE TEXTMATE | FIN7 |
| orfn.com | POWERSOURCE | FIN7 |
| otzd.pw | POWERSOURCE | FIN7 |
| oxrp.info | POWERSOURCE TEXTMATE | FIN7 |
| oyaw.club | POWERSOURCE TEXTMATE | FIN7 |
| p3marketing.org | | FIN7 |
| pafk.us | POWERSOURCE TEXTMATE | FIN7 |
| palj.us | POWERSOURCE TEXTMATE | FIN7 |
| park-travels.com | | FIN7 |
| parktravel-mx.ru | | FIN7 |
| partnersind.biz | | FIN7 |
| pbbk.us | POWERSOURCE TEXTMATE | FIN7 |
| pbsk.site | TEXTMATE | FIN7 |
| pdoklbr.com | BEACON.DNS | FIN7 |
| pdokls3.com | BEACON.DNS | FIN7 |
| pgnb.net | POWERSOURCE | FIN7 |
| pinewood-financial.com | | FIN7 |
| pjpi.com | POWERSOURCE | FIN7 |
| plusmarketingagency.com | | FIN7 |
| ppdx.pw | POWERSOURCE TEXTMATE | FIN7 |
| prideofhume.com | | FIN7 |
| pronvowdecee.com | | FIN7 |
| proslr3.com | BEACON.DNS | FIN7 |
| prostelap3.com | BEACON.DNS | FIN7 |

| | | |
|---|---|---|
| proverslokv4.com | | FIN7 |
| provnkfexxw.com | | FIN7 |
| pvze.club | POWERSOURCE TEXTMATE | FIN7 |
| qdtn.us | TEXTMATE | FIN7 |
| qefg.info | POWERSOURCE TEXTMATE | FIN7 |
| qlpa.club | POWERSOURCE TEXTMATE | FIN7 |
| qsez.club | TEXTMATE | FIN7 |
| qznm.pw | POWERSOURCE | FIN7 |
| rdnautomotiv.biz | | FIN7 |
| redtoursuk.org | | FIN7 |
| reld.info | POWERSOURCE TEXTMATE | FIN7 |
| rescsovwe.com | BEACON.DNS | FIN7 |
| revital-travel.com | HALFBAKED | FIN7 |
| revitaltravel.com | | FIN7 |
| rmbs.club | TEXTMATE | FIN7 |
| rnkj.pw | POWERSOURCE | FIN7 |
| rtopsmve.com | BEACON.DNS | FIN7 |
| rzzc.pw | POWERSOURCE | FIN7 |
| sgvt.pw | POWERSOURCE | FIN7 |
| shield-checker.com | | FIN7 |
| simpelkocsn.com | | FIN7 |
| simplewovmde.com | | FIN7 |
| soru.pw | POWERSOURCE | FIN7 |
| sprngwaterman.com | | FIN7 |
| strideindastry.biz | | FIN7 |

| | | |
|---|---|---|
| strideindustrial.com | | FIN7 |
| strideindustrialusa.com | MAL | FIN7 |
| strikes-withlucky.com | | FIN7 |
| swio.pw | POWERSOURCE | FIN7 |
| tijm.pw | POWERSOURCE | FIN7 |
| tnt-media.net | | FIN7 |
| true-deals.com | BEACON.DNS | FIN7 |
| trustbankinc.com | | FIN7 |
| tsrs.pw | POWERSOURCE | FIN7 |
| turp.pw | POWERSOURCE | FIN7 |
| twfl.us | POWERSOURCE | FIN7 |
| ueox.club | POWERSOURCE TEXTMATE | FIN7 |
| ufyb.club | POWERSOURCE TEXTMATE | FIN7 |
| utca.site | POWERSOURCE TEXTMATE | FIN7 |
| uwqs.club | TEXTMATE | FIN7 |
| vdfe.site | POWERSOURCE TEXTMATE | FIN7 |
| viebsdsccscw.com | | FIN7 |
| viebvbiiwcw.com | | FIN7 |
| vikppsod.com | BEACON.DNS | FIN7 |
| vjro.club | POWERSOURCE TEXTMATE | FIN7 |
| vkpo.us | POWERSOURCE TEXTMATE | FIN7 |
| voievnenibrinw.com | | FIN7 |
| vpua.pw | POWERSOURCE | FIN7 |
| vpuo.pw | POWERSOURCE | FIN7 |
| vqba.info | POWERSOURCE TEXTMATE | FIN7 |

| | | |
|---|---|---|
| vwcq.us | POWERSOURCE TEXTMATE | FIN7 |
| vxqt.us | POWERSOURCE TEXTMATE | FIN7 |
| vxwy.pw | POWERSOURCE | FIN7 |
| wein.net | POWERSOURCE | FIN7 |
| wfsv.us | POWERSOURCE TEXTMATE | FIN7 |
| whily.pw | | FIN7 |
| wider-machinery-usa.com | | FIN7 |
| widermachinery.biz | | FIN7 |
| widermachinery.com | | FIN7 |
| wnzg.us | TEXTMATE | FIN7 |
| wqiy.info | POWERSOURCE TEXTMATE | FIN7 |
| wruj.club | TEXTMATE | FIN7 |
| wuc.pw | POWERSOURCE | FIN7 |
| wvzu.pw | POWERSOURCE TEXTMATE | FIN7 |
| xhqd.pw | POWERSOURCE | FIN7 |
| xnlz.club | TEXTMATE | FIN7 |
| xnmy.com | POWERSOURCE | FIN7 |
| yamd.pw | POWERSOURCE | FIN7 |
| ybnz.site | TEXTMATE | FIN7 |
| ydvd.net | TEXTMATE | FIN7 |
| yedq.pw | POWERSOURCE | FIN7 |
| yodq.pw | POWERSOURCE | FIN7 |
| yomd.pw | POWERSOURCE | FIN7 |
| yqox.pw | POWERSOURCE | FIN7 |
| ysxy.pw | POWERSOURCE TEXTMATE | FIN7 |

| | | |
|---|---|---|
| zcnt.pw | POWERSOURCE TEXTMATE | FIN7 |
| zdqp.pw | POWERSOURCE | FIN7 |
| zjav.us | POWERSOURCE TEXTMATE | FIN7 |
| zjvz.pw | POWERSOURCE | FIN7 |
| zmyo.club | POWERSOURCE TEXTMATE | FIN7 |
| zody.pw | POWERSOURCE TEXTMATE | FIN7 |
| zrst.com | POWERSOURCE | FIN7 |
| zugh.us | POWERSOURCE TEXTMATE | FIN7 |
| clients14-google.com | | FIN7 |
| clients18-google.com | | FIN7 |
| clients19-google.com | | FIN7 |
| clients23-google.com | | FIN7 |
| clients31-google.com | | FIN7 |
| clients33-google.com | BEACON.DNS | FIN7 |
| clients39-google.com | | FIN7 |
| clients46-google.com | | FIN7 |
| clients47-google.com | | FIN7 |
| clients51-google.com | | FIN7 |
| clients52-google.com | | FIN7 |
| clients55-google.com | | FIN7 |
| clients56-google.com | | FIN7 |
| clients57-google.com | | FIN7 |
| clients58-google.com | | FIN7 |
| clients6-google.com | HALFBAKED | FIN7 |
| clients62-google.com | | FIN7 |

| | | |
|---|---|---|
| clients7-google.com | MAL | FIN7 |
| fda-gov.com | | FIN7 |
| dropbox-security.com | | FIN7 |
| google-sll1.com | | FIN7 |
| google-ssls.com | | FIN7 |
| google-stel.com | | FIN7 |
| google3-ssl.com | | FIN7 |
| google4-ssl.com | | FIN7 |
| google5-ssl.com | | FIN7 |
| ssl-googles4.com | | FIN7 |
| ssl-googlesr5.com | | FIN7 |
| stats10-google.com | CARBANAK | FIN7 |
| stats25-google.com | BEACON.DNS | FIN7 |
| treasury-government.com | | FIN7 |
| usdepartmentofrevenue.com | | FIN7 |
| bols-googls.com | | FIN7 |
| moopisndvdvr.com | | FIN7 |
| dewifal.com | | Suspect FIN7 |
| essentialetimes.com | | Suspect FIN7 |
| fisrdteditionps.com | | Suspect FIN7 |
| fisrteditionps.com | | Suspect FIN7 |
| micro-earth.com | | Suspect FIN7 |
| moneyma-r.com | | Suspect FIN7 |
| newuniquesolutions.com | | Suspect FIN7 |
| wedogreatpurchases.com | | Suspect FIN7 |