Threat Intelligence

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

August 1, 2018

Mandiant

Written by: Nick Carr, Kimberly Goody, Steve Miller, Barry Vengerik

---

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 *Travel
- Hospitality *Education
- Casinos and Gaming *Construction
- Energy *Retail

- Finance
  *Telecommunications
- High-tech
  *Government
- Software services
  *Business

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
Korsar Travel		

TOV	UA	88:21:ac:7e:6c
Kaitschuck James	GB	30:2e:7f:14:3a
Park Travel	RU	4d:e2:87:56:9

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.

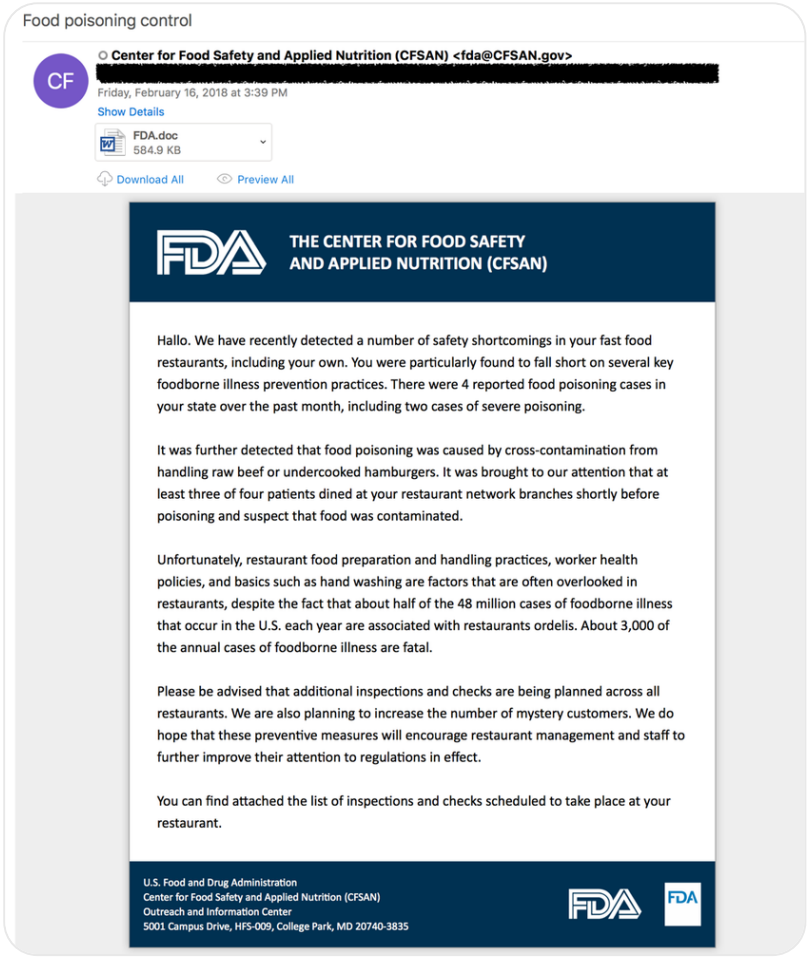

Figure 1: FDA themed spear phishing email

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.

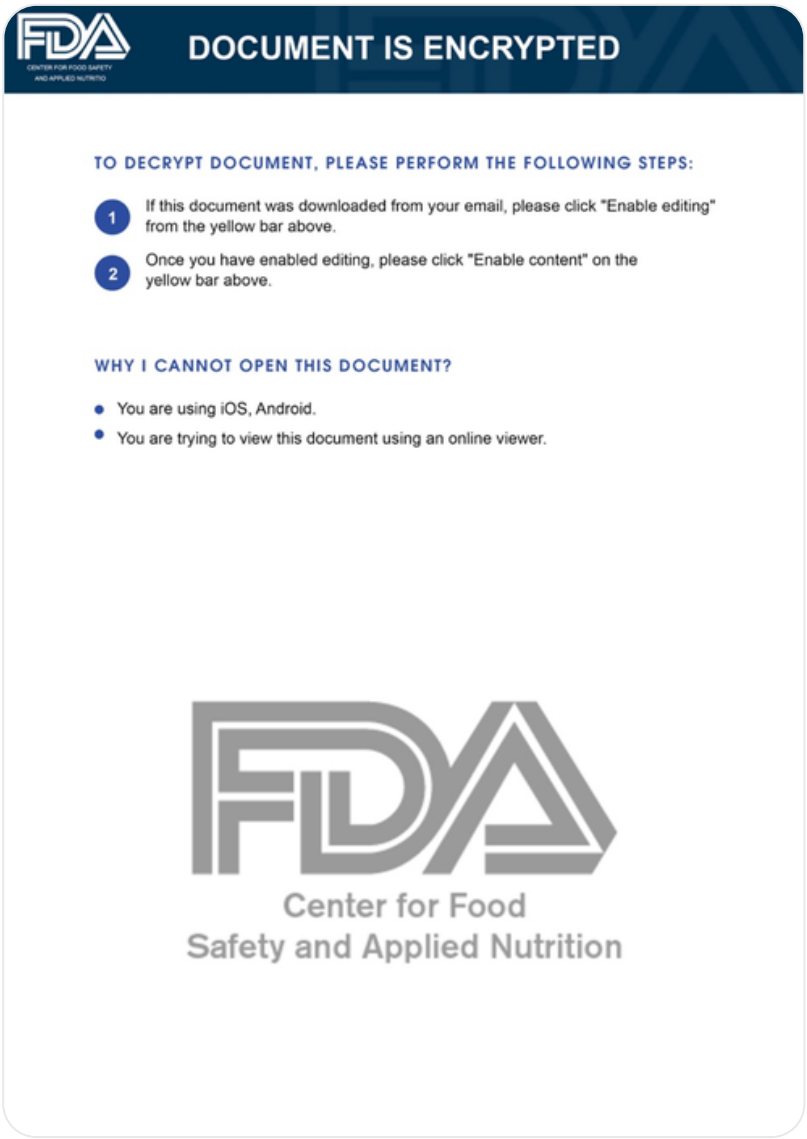

Figure 2: FDA themed spear phishing attachment

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 offensi

ve 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
2018:05:21 17:32:00
C:\Users**jimbo**\Desktop\Files\Картинки\outl
cmd.exe /k "SET a01=wscr& SET a02=ipt&& %a01%%a02% /e:jscript //b %TEMP%\errors
EXIF Creation Time

2018:01:26 15:59:00
C:\Users**Hass**\Desktop\Картинки\New\outlo
cmd.exe /c wscript.exe //b /e:jscript %TEMP%
EXIF Creation Time
2018:01:11 13:16:00
C:\Users**Hass**\Desktop\Картинки\New\outlo
cmd.exe /c wscript.exe //b /e:jscript %TEMP%
EXIF Creation Time
2017:10:25 07:43:00
C:\Users**oleg**\Desktop\Файлы\Картинки\Ne
cmd.exe /c wscript.exe //b /e:jscript %TEMP%
EXIF Creation Time
2017:06:23 15:18:00

C:\Users**Work**\Desktop\IMAGES\outlook2.pr
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 %HOMEPAT f=fs.OpenTextFile(p,1,false);for(i=0;i^<4;i++)f >%HOMEPATH%\tt.txt@copy /y %TMP%\unl
EXIF Creation Time
2017:09:27 11:56:00
C:\Users**usr**\Documents\send\270917\unloc
wmic.exe process call create "cmd start /mi
cmd.exe /S /D /c" echo /*@#8#@*/try{sh=ne ActiveXObject("Scripting.FileSystemObject"

(c);}catch(e){} >%HOMEPATH%\t.txt & wscr
EXIF Creation Time
2017:08:08 17:38:00
C:\Users**andy**\Desktop\unlock.doc.lnk
wmic.exe process call create "mshta javascr
mshta.exe "try{jelo = 'try{w=GetObject("","W ActiveXObject("Scripting.FileSystemObject"
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 %HO >%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 %HO >%HOMEPATH%\md5.txt & echo %x:@=%|cı

EXIF Creation Time
2017:05:11 12:59:00
C:\Users**user**\Documents\unprotect.lnk
C:\WINDOWS\system32\mshta.exe vbscript:I
EXIF Creation Time
2017:04:20 16:27:00
C:\Users**testadmin.TEST**\Desktop\unprotec
C:\WINDOWS\system32\mshta.exe vbscript:I wprotect.ActiveDocument.Shapes(1).TextFra
EXIF Creation Time
2017:01:12 18:00:00
C:\Users**testadmin.TEST**\Desktop\unprotec
%WINDIR%\System32\Wscript.exe %TEMP%
EXIF Creation Time
2016:08:12 11:26:00

C:\Users**test**\Documents\sploits\120816\ord
%WINDIR%\System32\Wscript.exe %TEMP%

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**	**Discove**
Initial Compromise	Spear phishing emails sent using PHP Mailer	Inbound containi such as PHPMail
Establish Foothold	Persistence using registry Run and Run	New Rur registry referenc

	Once keys	.VBA
Establish Foothold	Execution or persistence using Scheduled Tasks	New Sch referenc .VBS, .VE other sc extensio
Establish Foothold	Persistence using Windows Services, Startup Directory	New Wir new files directori
Establish Foothold	Persistence using AppCompat Shim	New shi and moc AppCom registry SDB Per
Maintain Presence	C2 using favored C2 ports	Outbour with por mismatc ports su 53,80,44
Maintain	C2 using	Outbour or DNS r "sketchy domains

Presence	favored generic 3LDs	3rd level as mail, dns, ftp "mail[.]c
Maintain Presence	C2 using VPS infrastructure with low reputation	Inbound connect non-sta especial internati Private S provider
Maintain Presence	C2 using legitimate services including Google Docs, Google Scripts and Pastebin	
Maintain Presence	C2 using DNS via A, OPT, TXT records	Unusual numerou and OPT
Maintain Presence	C2 domains registered with REG.RU	Newly ol domains REG.RU
	C2 domains	

Maintain Presence	registered with NameCheap	Newly ol domains NameCh
Maintain Presence	C2 domains registered with odd format and top-level domains	Unusual numerou with the zA-Z]{4, [pw|us|c (eg. “pv:
Maintain Presence	C2 domains registered with hyphen	Outbour to newly hyphena

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	M

menu.rtf	c1
	76
3-ThompsonDan.rtf	4b
claim.rtf	af
order.rtf	ce
order.rtf	cf
Doc2_rtf.rtf	2c
doc1.doc	37
quote.rtf	3c
Doc2_rtf.rtf	56

information.doc	5c
Doc_rest_rtf.rtf	61
doc1.docx	67
Doc33.docx	6a
info_.rtf	6a
bmg.docx	75
Doc_0405_1.rtf	7b
doc1.docx	99
doc0505_1.rtf	9e
DonovanR.docx	b5
rising star.rtf	c8

inf6.docx	e4
Claim.docx	06
order.rtf	80
Details Joseph.docx	b4
order.doc	e2
	b1
features.doc	bb
doc2709.rtf	01
doc_n0908.rtf	03
doc1.docx	0c

doc1.rtf	0e
doc0719.docx	10
doc0507.docx	17
info_1.rtf	18
doc.docx	1a
Mail.rtf	1a
Doc_rest_n_rtf.rtf	1f5
doc.docx	1f9
doc1909.docx	1fb
doc_n0808.rtf	21
doc0507.rtf	22

Doc2.docx	22
menu.rtf	24
2-order.docx	28
doc0610.docx	29
doc2209_1.rtf	2c
Doc1.rtf	30
doc1.rtf	32
doc0910.rtf	39
doc1.docx	39
docr.rtf	3a

oliver_davis.docx	3b
doc2209.docx.docx	40
Dooq.docx	41
info.rtf	42
james.docx	49
doc1007.rtf	4b
tem6.doc	4b
doc1.rtf	51
doc1.docx	52
doc2209.rtf	56
doc1.docx	5a

doc0717.rtf	5c
	5c
doc2.doc	5c
Dooq.docx	63
doc0720.rtf	6a
doc0719.rtf	6a
virus.docx	70
check.rtf	72
Doc_0405.rtf	74
oliver_davis.rtf	79

doc_n0808.docx	79
Doc1.rtf	7d
doc1.docx	82
document.doc	85
doc2806.rtf	85
doc1.rtf	86
Doc1.rtf	8b
doc1.rtf	94
doc1610.rtf	97
Doc0725.rtf	97
Doc1.rtf	9b

doc1.rtf	a5
doc0610.rtf	a8
doc2_r_new.rtf	a9
credit details.rtf	aa
doc2.docx_	b5
	b6
doc1.rtf	c0
doc2806.docx	c3
doc1.rtf	c5
doc1.rtf	c6

doc0714.docx	ca
doc1909.rtf	d1
doc_n0908.docx	d3
catering_.rtf	d5
doc0714.rtf	dc
m1.doc	e0
doc1.rtf	e1
doc2009.rtf	e1
doc1610.docx	e9
doc1.rtf	ec
doc2_r_new.rtf	ee

doc1.rtf	ef
info_.docx	f2
Doc0725.docx	f8
1.rtf	fa
	fa
poisoning.rtf	fa
order.docx	fc
SEC_Security_Policy_2017_02.doc	03
SEC_Security_Policy_2017_10.doc	14
VargheseJ.doc	2a

SEC_Security_Policy_2017_03.doc	37
2017.doc	5a
SEC_Security_Policy_2017.doc	6f
EDGAR_FILLINGS_RULES_2016.doc	7b
SEC_Security_Policy_2017_05.doc	8f
SEC_Security_Policy_2017_06.doc	cc
Important_Changes_to_Form10_K.doc	d0
SEC_Security_Policy_2017.doc	f2
SEC_Security_Policy_2017_07.doc	f7
Filings_and_Forms.docx	47

doc.doc	18
protected_instructions.doc	3C
Doc2.doc	4C
3528579_security_protocol.doc	58
check.doc	59
	6f
check.doc	76
check.doc	9b
Doc1.doc	bb

check.doc	d4
invoices.doc	dc
blah.doc	e0
photos.doc	c5
test.doc	d7

Additional Malware

MD5	M
5f73beb23c45006ad952a71fa62c6f9f	E
a3754fba24f85d1d1bb7c0382e41586b	E
dad8ebcbb5fa6721ccad45b81874e22c	E

ecd8879702347966750c37247ef6c2e6	E
039d9e47e4474bee24785f8ec5307695	E
92dfd0534b080234f9536371be63e37a	E
188f261e5fca94bd1fc1edc1aafee8c0	(
2828ea78cdda8f21187572c99ded6dc2	(
291a17814d5dbb5bce5b186334cde4b1	(
4b3dac0a4f452b07d29f26b119180bd2	(
4eda75dfd4d12eda6a6219423b5972bd	(
6e9408c338e98a8bc166a8d4f8264019	(
749c5085cda920e830cfed32842ba835	(
80b022b39d91527f6ae5b4834d7c8173	(
8ae284d547bd1b8bd6bc2431735f9142	(
8e1e7f5ad99e48b740fd00085eab1f84	(
9ae433cd5397af6b485f1abb06b2c5a2	(
be1154e38df490e1dcbde3ffb2ebd05c	(

c6b57e042ceadb60d6fab217d3523e17	(
c6ec176592ea26c4ee27974273e592ff	(
dd4f312c7e1c25564a8d00b0f3495e24	(
facd37cd76989f45088ae98de8ed7aa0	(
4dc99280459292ef60d6d01ed8ece312	[
63241a3580cd1135170b044a84005e92	[
70345aa0b970e1198a9267ae4532a11b	[
de50d41d70b8879cdc73e684ad4ebe9f	[
ddc9b71808be3a0e180e2befae4ff433	S
90f35fd205556a04d13216c33cb0dbe3	E

IPs

IP Address	Malware
107.161.159.17	CARBANAK
107.181.160.12	CARBANAK

107.181.160.75*	DRIFTPINHALFBAKED
162.244.32.168	CARBANAK
162.244.32.175	CARBANAK
179.43.140.82*	CARBANAK
179.43.140.85*	CARBANAK
179.43.160.162	CARBANAK
179.43.160.215	CARBANAK
185.104.8.173	CARBANAK
198.100.119.28	CARBANAK
204.155.30.100	CARBANAK
204.155.30.100	DRIFTPINHALFBAKED
23.249.162.161	CARBANAK
5.8.88.64	BIRDDOG
94.140.120.132	CARBANAK
95.215.45.95	CARBANAK

95.215.46.70	CARBANAK
95.215.46.76	CARBANAK
185.66.15.50	
194.165.16.113	
46.161.3.23	
85.93.2.148	
85.93.2.149	
81.177.27.41	
95.46.45.128	BATELEUR
185.17.121.200	BATELEUR
185.20.184.109*	BATELEUR

185.220.35.20	BATELEUR
185.5.248.167*	BATELEUR
194.165.16.134	BATELEUR
195.133.48.65	BATELEUR
195.133.49.73	BATELEUR
217.23.155.19	BATELEUR
31.184.234.66	BATELEUR
31.184.234.71	BATELEUR
5.188.10.102	BATELEUR
5.188.10.102	BATELEUR

5.188.10.248	BATELEUR
85.93.2.111	BATELEUR
85.93.2.148	BATELEUR
85.93.2.56	BATELEUR
85.93.2.73	BATELEUR
85.93.2.92	BATELEUR
89.223.30.99	BATELEUR
104.193.252.167	HALFBAKED
104.232.34.166	HALFBAKED
104.232.34.36	HALFBAKED
107.181.160.76*	HALFBAKED

119.81.178.100	HALFBAKED
119.81.178.101	HALFBAKED
138.201.44.3	HALFBAKED
138.201.44.4	HALFBAKED
179.43.147.71	HALFBAKED
185.180.197.20	HALFBAKED
185.180.197.34	HALFBAKED
185.86.151.175	HALFBAKED
191.101.242.162	HALFBAKED
195.54.162.237*	HALFBAKED
195.54.162.245	HALFBAKED
195.54.162.79*	HALFBAKED
198.100.119.6	HALFBAKED
198.100.119.7	HALFBAKED
204.155.31.167	HALFBAKED

204.155.31.174	HALFBAKED
217.12.208.80	HALFBAKED
31.148.219.141*	HALFBAKED
31.148.219.18*	HALFBAKED
31.148.219.44*	HALFBAKED
31.148.220.107*	HALFBAKED
31.148.220.215*	HALFBAKED
5.149.250.235	HALFBAKED
5.149.250.241	HALFBAKED
5.149.252.144	HALFBAKED
5.149.253.126	HALFBAKED
8.28.175.68*	HALFBAKED
81.17.28.118*	HALFBAKED
91.235.129.251*	HALFBAKED
94.140.120.122	HALFBAKED

94.140.120.134	HALFBAKED
95.215.46.229	HALFBAKED
95.215.47.105	HALFBAKED
5.135.73.113	BIRDDOG
5.8.88.64	BIRDDOG

*VPS that may also have legitimate traffic.

Full Qualified Domain Names (FQDNs)

Domain	Malware
bigred-tours.com	
clients12-google.com	BEACON.D
clients2-google.com	
p3-marketing.com	
cdn-googleapi.com	GRIFFON

cdn-googleservice.com	GRIFFON
acity-lawfirm.com	
algew.me	POWERSO
aloqd.pw	POWERSO
amhs.club	TEXTMATE
anselbakery.com	
apvo.club	TEXTMATE
arctic-west.com	
auyk.club	POWERSO
b-bconsult.com	
bcleaningservice.com	
bigrussianbss.com	
bipismol.com	
bipovnerlvd.com	
blopsadmvdrl.com	

blopsdmvdrl.com	
bnrnboerxce.com	
bpee.pw	POWERSO
bureauofinspections.com	
bvyv.club	POWERSO
bwuk.club	POWERSO
bwwrvada.com	
cgqy.us	POWERSO
chatterbuzz-media.com	
chenstravelconsulting.com	
cihr.site	POWERSO
citizentravel.biz	
cjsanandreas.com	
ckwl.pw	POWERSO
cloo.com	POWERSO

cnkmoh.pw	POWERSO
cnlu.net	TEXTMATE
cnmah.pw	POWERSO
coec.club	POWERSO
coffee-joy-usa.com	
cspg.pw	TEXTMATE
ctxdns.org	
ctxdns.pw	
cuuo.us	POWERSO
daskd.me	POWERSO
dbxa.pw	POWERSO
ddmd.pw	POWERSO
deliciouswingsny.com	
dlex.pw	POWERSO
dlox.pw	POWERSO

dnstxt.net	
dnstxt.org	
doof.pw	POWERSO
dosdkd.mo	POWERSO
dpoo.pw	POWERSO
dsud.com	POWERSO
dtxf.pw	POWERSO
duglas-manufacturing.com	
dvso.pw	POWERSO
dyiud.com	POWERSO
eady.club	POWERSO
enuv.club	POWERSO
eter.pw	POWERSO
extmachine.biz	
facs.pw	TEXTMATE

fbjz.pw	POWERSO
fhyi.club	POWERSO
firsthotelgroup.com	
firstprolvdrec.com	
fkij.net	TEXTMATE
flowerprosv.com	
fredbanan.com	POWERSO
futh.pw	POWERSO
gcan.site	TEXTMATE
ge-stion.com	
gjcu.pw	POWERSO
gjuc.pw	POWERSO
glavpojdfde.com	BEACON.D
gnoa.pw	POWERSO
gnsn.us	TEXTMATE

goldman-travel.com	
goproders.com	BEACON.D
gprw.site	TEXTMATE
grand-mars.ru	
grij.us	POWERSO
gsdg.site	TEXTMATE
guopksl.com	BEACON.D
gxhp.top	POWERSO
hijrnataj.com	
hilertonv.com	BEACON.D
hilopser.com	BEACON.D
hippsjnv.com	
hldu.site	POWERSO
hoplessinple.com	
hoplessinples.com	

hopsl3.com	BEACON.D
hvzr.info	POWERSO
idjb.us	POWERSO
ihrs.pw	POWERSO
imyo.site	TEXTMATE
itstravel-ekb.ru	
ivcm.club	TEXTMATE
jblz.net	TEXTMATE
jersetl.com	BEACON.D
jimw.club	POWERSO
jipdfonte.com	
jiposlve.com	BEACON.D
jjee.site	POWERSO
johsimsoft.org	
jomp.site	POWERSO

josephevinchi.com	
just-easy-travel.com	
juste-travel.com	HALFBAKE
jxhv.site	POWERSO
kalavadar.com	
kashtanspb.ru	
kbep.pw	TEXTMATE
kiposerd.com	BEACON.D
kiprovol.com	
kiprovolswe.com	
kjke.pw	POWERSO
kjko.pw	POWERSO
koldsdes.com	
kshv.site	POWERSO

kuyarr.com	
kwoe.us	POWERSO
ldzp.pw	POWERSO
lgdr.com	POWERSO
lhlv.club	POWERSO
lnoy.site	POWERSO
luckystartwith.com	
lvrm.pw	POWERSO
lvxf.pw	POWERSO
manchedevs.org	
maofmdfd5.com	
meli-travel.com	HALFBAKE
melitravel.ru	
mewt.us	POWERSO
mfka.pw	POWERSO

michigan-construction.com	
mjet.pw	POWERSO
mjot.pw	POWERSO
mjut.pw	POWERSO
mkwl.pw	TEXTMATE
molos-2.com	BEACON.D
mtgk.site	POWERSO
mtxf.com	TEXTMATE
muedandubai.com	
muhh.us	POWERSO
mut.pw	POWERSO
mvze.pw	POWERSO
mvzo.pw	POWERSO
mxfg.pw	POWERSO
mxtxt.net	

myspoernv.com	
navigators-travel.com	
neartsay.com	
nevaudio.com	
neverfaii.com	
nroq.pw	POWERSO
ns0.site	POWERPIP
ns0.space	POWERPIP
ns0.website	POWERPIP
ns1.press	POWERPIP
ns1.website	POWERPIP
ns2.press	POWERPIP
ns3.site	POWERPIP
ns3.space	POWERPIP
ns4.site	POWERPIP

ns4.space	POWERPIP
ns5.biz	POWERPIP
ns5.online	POWERPIP
ns5.pw	MAL
ntlw.net	POWERSO
nwrr.pw	POWERSO
nxpu.site	POWERSO
oaax.site	POWERSO
odwf.pw	POWERSO
odyr.us	POWERSO
okiq.pw	POWERSO
oknz.club	POWERSO
olckwses.com	
olgw.my	POWERSO
oloqd.pw	POWERSO

oneliveforcopser.com	
onokder.com	BEACON.D
ooep.pw	POWERSO
oof.pw	POWERSO
ooyh.us	POWERSO
orfn.com	POWERSO
otzd.pw	POWERSO
oxrp.info	POWERSO
oyaw.club	POWERSO
p3marketing.org	
pafk.us	POWERSO
palj.us	POWERSO
park-travels.com	
parktravel-mx.ru	

partnersind.biz	
pbbk.us	POWERSO
pbsk.site	TEXTMATE
pdoklbr.com	BEACON.D
pdokls3.com	BEACON.D
pgnb.net	POWERSO
pinewood-financial.com	
pjpi.com	POWERSO
plusmarketingagency.com	
ppdx.pw	POWERSO
prideofhume.com	
pronvowdecee.com	
proslr3.com	BEACON.D
prostelap3.com	BEACON.D
proverslokv4.com	

provnkfexxw.com	
pvze.club	POWERSO
qdtn.us	TEXTMATE
qefg.info	POWERSO
qlpa.club	POWERSO
qsez.club	TEXTMATE
qznm.pw	POWERSO
rdnautomotiv.biz	

revital-travel.com	HALFBAKE
revitaltravel.com	
rmbs.club	TEXTMATE
rnkj.pw	POWERSO

rtopsmve.com	BEACON.D
rzzc.pw	POWERSO
sgvt.pw	POWERSO
shield-checker.com	
simpelkocsn.com	
simplewovmde.com	
soru.pw	POWERSO
sprngwaterman.com	
strideindastry.biz	
strideindustrial.com	
strideindustrialusa.com	MAL
strikes-withlucky.com	
swio.pw	POWERSO
tijm.pw	POWERSO
tnt-media.net	

true-deals.com	BEACON.D
trustbankinc.com	
tsrs.pw	POWERSO
turp.pw	POWERSO
twfl.us	POWERSO
ueox.club	POWERSO
ufyb.club	POWERSO
utca.site	POWERSO
uwqs.club	TEXTMATE
vdfe.site	POWERSO
viebsdsccscw.com	
viebvbiiwcw.com	
vikppsod.com	BEACON.D
vjro.club	POWERSO
vkpo.us	POWERSO

voievnenibrinw.com	
vpua.pw	POWERSO
vpuo.pw	POWERSO
vqba.info	POWERSO
vwcq.us	POWERSO
vxqt.us	POWERSO
vxwy.pw	POWERSO
wein.net	POWERSO
wfsv.us	POWERSO
whily.pw	
wider-machinery-usa.com	
widermachinery.biz	
widermachinery.com	
wnzg.us	TEXTMATE
wqiy.info	POWERSO

wruj.club	TEXTMATE
wuc.pw	POWERSO
wvzu.pw	POWERSO
xhqd.pw	POWERSO
xnlz.club	TEXTMATE
xnmy.com	POWERSO
yamd.pw	POWERSO
ybnz.site	TEXTMATE
ydvd.net	TEXTMATE
yedq.pw	POWERSO
yodq.pw	POWERSO
yomd.pw	POWERSO
yqox.pw	POWERSO
ysxy.pw	POWERSO
zcnt.pw	POWERSO

zdqp.pw	POWERSO
zjav.us	POWERSO
zjvz.pw	POWERSO
zmyo.club	POWERSO
zody.pw	POWERSO
zrst.com	POWERSO
zugh.us	POWERSO
clients14-google.com	
clients18-google.com	
clients19-google.com	
clients23-google.com	
clients31-google.com	
clients33-google.com	BEACON.D
clients39-google.com	
clients46-google.com	

clients47-google.com	
clients51-google.com	
clients52-google.com	
clients55-google.com	
clients56-google.com	
clients57-google.com	
clients58-google.com	
clients6-google.com	HALFBAKE
clients62-google.com	
clients7-google.com	MAL
fda-gov.com	
dropbox-security.com	
google-sll1.com	
google-ssls.com	
google-stel.com	

google3-ssl.com	
google4-ssl.com	
google5-ssl.com	
ssl-googles4.com	
ssl-googlesr5.com	
stats10-google.com	CARBANAK
stats25-google.com	BEACON.D
treasury-government.com	
usdepartmentofrevenue.com	
bols-googls.com	
moopisndvdvr.com	
dewifal.com	
essentialetimes.com	
fisrdteditionps.com	

fisrteditionps.com	
micro-earth.com	
moneyma-r.com	
newuniquesolutions.com	
wedogreatpurchases.com	

Posted in Threat Intelligence—Security & Identity

Related articles