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,

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.

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
- Finance
- High-tech
- Software
- *Travel
- *Education
- *Construction
- *Retail
- *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.

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

Kaitschuck James	GB	30:2e:7f:14:3a:f3:f3:98:2C
Park Travel	RU	4d:e2:87:56:98:bf:c7:74:a3

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

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

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

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

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

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

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

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

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

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\outlook2.png
cmd.exe /k "SET a01=wscr& SET a02=ipt&&call %a01%%a02% /e:jscript //b %TEMP%\errors.txt
EXIF Creation Time

C:\Users**Hass**\Desktop\Картинки\New\outlook3.png
cmd.exe /c wscript.exe //b /e:jscript %TEMP%\crashpad
EXIF Creation Time
2018:01:11 13:16:00
C:\Users**Hass**\Desktop\Картинки\New\outlook2.png
cmd.exe /c wscript.exe //b /e:jscript %TEMP%\crashpad
EXIF Creation Time
2017:10:25 07:43:00
C:\Users**oleg**\Desktop\Файлы\Картинки\New\defender.
cmd.exe /c wscript.exe //b /e:jscript %TEMP%\crashpad
EXIF Creation Time
2017:06:23 15:18:00

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@e f=fs.OpenTextFile(p,1,false);for(i=0;i^<4;i++)f.SkipLine();v >%HOMEPATH%\tt.txt@copy /y %TMP%\unlock.cmd %H
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
cmd.exe /S /D /c" echo /*@#8#@*/try{sh=new ActiveXO ActiveXObject("Scripting.FileSystemObject");p=sh.Expar

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
mshta.exe "try{jelo = 'try{w=GetObject("","Wor"+"d.App ActiveXObject("Scripting.FileSystemObject");var sh = ne
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%\t >%HOMEPATH%\ttt.txt & echo %x:@=%|cmd
EXIF Creation Time
2017:06:28 16:21:00
C:\Users**andy**\Desktop\unprotect.rtf.lnk

EXIF Creation Time
2017:05:11 12:59:00
C:\Users**user**\Documents\unprotect.lnk
C:\WINDOWS\system32\mshta.exe vbscript:Execute("Or
EXIF Creation Time
2017:04:20 16:27:00
C:\Users**testadmin.TEST**\Desktop\unprotect.lnk
C:\WINDOWS\system32\mshta.exe vbscript:Execute(&qu wprotect.ActiveDocument.Shapes(1).TextFrame.TextRang
EXIF Creation Time
2017:01:12 18:00:00
C:\Users**testadmin.TEST**\Desktop\unprotected.vbeC:\U
%WINDIR%\System32\Wscript.exe %TEMP%\WindowsUp
EXIF Creation Time

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

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"

Foothold	Run and Run Once keys	referencing .VBS and .VBA
Establish Foothold	Execution or persistence using Scheduled Tasks	New Scheduled Task referencing .CMD, .L .VBS, .VBA, .PS1 and other scripting langu extensions
Establish Foothold	Persistence using Windows Services, Startup Directory	New Windows Servic new files in Startup directories
Establish Foothold	Persistence using AppCompat Shim	New shim database f and modifications of AppCompatFlags registry keys (see FI SDB Persistence)
Maintain Presence	C2 using favored C2 ports	Outbound connectio with port-protocol mismatches on comr ports such as 53,80,443,8080

Maintain Presence	C2 using favored generic 3LDs	"sketchy" 2nd level domains with generic 3rd 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 an non-standard IP rang 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, TX and OPT record quer

Presence	with REG.RU	REG.RU
Maintain Presence	C2 domains registered with NameCheap	Newly observed domains registered v NameCheap
Maintain Presence	C2 domains registered with odd format and top-level domains	Unusually long or numerous DNS queri with the structure [a-Z]{4,5}\.[pw|us|club|info|site| (eg. “pvze[.]club”)
Maintain Presence	C2 domains registered with hyphen	Outbound connectio 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.

Filename	MD5
menu.rtf	c14eb54769ff2
	76eb6f124fba
3-ThompsonDan.rtf	4b783bd0bd7
claim.rtf	af53db730732
order.rtf	cea2989309c
order.rtf	cf4ccb3707e5
Doc2_rtf.rtf	2dc0f4bece10
doc1.doc	37759603c6c
quote.rtf	3c0bd71e91e0

[illegible].rtf	[illegible]
information.doc	5dace5ac5ba[illegible]
Doc_rest_rtf.rtf	619aa4e6c9d[illegible]
doc1.docx	67c9bfd4d6ac
Doc33.docx	6a5a42ed234[illegible]
info_.rtf	6ac5ae654674
bmg.docx	754fc509328a
Doc_0405_1.rtf	7b2315ff1f2d7
doc1.docx	99975b5ee2d[illegible]
doc0505_1.rtf	9eb71edd5ec[illegible]

rising star.rtf	c8b8420d150
inf6.docx	e494356fc0d
Claim.docx	06b9e2fdd2c
order.rtf	80eed9f87a18
Details Joseph.docx	b4d48f3e1ae3
order.doc	e2a6b351c276
	b14bc8cbc7f2
features.doc	bbd99ef280e
doc2709.rtf	01d666fcbc4c

doc1.docx	0d6619481cfd
doc1.rtf	0e0a5148905
doc0719.docx	101bdbbd99c
doc0507.docx	17fabe288d64
info_1.rtf	189c5a090d2
doc.docx	1a6c18967f4c
Mail.rtf	1a9e113b2f3c
Doc_rest_n_rtf.rtf	1f5022a02c82
doc.docx	1f98c4ff12fc2

doc_n0808.rtf	21926646a658
doc0507.rtf	22ad7c05128c
Doc2.docx	22e7d4f7401e
menu.rtf	24fab1e9831e
2-order.docx	28ad8e3a225
doc0610.docx	29a3666cee0
doc2209_1.rtf	2d36634974c8
Doc1.rtf	307a9ce257e9
doc1.rtf	325844f1b956

doc1.docx	397d45b6001
docr.rtf	3a303f02e16c
oliver_davis.docx	3b12f36a0132
doc2209.docx.docx	402c34d7d6c
Dooq.docx	41c6861313e7
info.rtf	42a2a2352f6b
james.docx	499ebef3ab31
doc1007.rtf	4b7a742d5c98
tem6.doc	4bf6918092

doc1.docx	52cf6a63da29
doc2209.rtf	560e72858ee4
doc1.docx	5a0b796c7a6(
doc0717.rtf	5d49b444734l
	5d9525b4887(
doc2.doc	5dd2e677fd1d
Dooq.docx	63e2eb258a85
doc0720.rtf	6a860285a6f7
doc0719.rtf	6adec78e8742

check.rtf	72d973ebfbc0
Doc_0405.rtf	74165408ff12c
oliver_davis.rtf	793511c86a04
doc_n0808.docx	79628a59830
Doc1.rtf	7d664485c53b
doc1.docx	82a32d98e68
document.doc	853a53419d9c
doc2806.rtf	856cec68ddd
doc1.rtf	8608b31a446f

doc1.rtf	94771bcf572d
doc1610.rtf	973377e27b5c
Doc0725.rtf	9788b3faa29b
Doc1.rtf	9b87f9f6498c
doc1.rtf	a5f75333d0c8
doc0610.rtf	a8e312d0c230
doc2_r_new.rtf	a9c50b776151
credit details.rtf	aaf42acedc38
doc2.docx_	b5cc86726ab8

doc1.rtf	c0d122bcdcb
doc2806.docx	c3f48e69bb9(
doc1.rtf	c5e94d973ed4
doc1.rtf	c6cddc475d6
doc0714.docx	caec3babdec
doc1909.rtf	d1f55491472c
doc_n0908.docx	d38fb2d95812
catering_.rtf	d5cd1dedf3bf
doc0714.rtf	dde72a54716c

doc1.rtf	e17fe2978ebe
doc2009.rtf	e184219366af
doc1610.docx	e9154e2f8038
doc1.rtf	edc4f02f265a
doc2_r_new.rtf	ee5a600ef9fc
doc1.rtf	effdaf7f61acb
info_.docx	f2ac2ec8173d
Doc0725.docx	f80a80d25b3
1.rtf	fa1c548a5d69

poisoning.rtf	faed087e820c
order.docx	fc661e1813758
SEC_Security_Policy_2017_02.doc	032fe02e54a0
SEC_Security_Policy_2017_10.doc	14334c8f93f0
VargheseJ.doc	2abad0ae32d
SEC_Security_Policy_2017_03.doc	37d323ffc33a0
2017.doc	5a88e3825c5e
SEC_Security_Policy_2017.doc	6ff3272cd9ed
EDGAR_FILLINGS_RULES_2016.doc	7bd2235f105c

SEC_Security_Policy_2017_06.doc	ccd2372bb6b
Important_Changes_to_Form10_K.doc	d04b6410ddd
SEC_Security_Policy_2017.doc	f20328b49ec
SEC_Security_Policy_2017_07.doc	f74958adcfb1
Filings_and_Forms.docx	47111e9854db
doc.doc	189c72bfd8ae
protected_instructions.doc	302ab8bd6a8
Doc2.doc	40c4c02d1e5

check.doc	5972597b729a
	6fff1d68203f8
check.doc	762eef684e01
check.doc	9b1af2d9c0c0
Doc1.doc	bb1a76702e2e
check.doc	d4088f8202e0
invoices.doc	dc8b30c5253

photos.doc	c517f48bf95a
test.doc	d7ca38e21327

Additional Malware

MD5	Malware
5f73beb23c45006ad952a71fa62c6f9f	BABYMETAL
a3754fba24f85d1d1bb7c0382e41586b	BABYMETAL
dad8ebcbb5fa6721ccad45b81874e22c	BABYMETAL
ecd8879702347966750c37247ef6c2e6	BABYMETAL
039d9e47e4474bee24785f8ec5307695	BIRDDOG
92dfd0534b080234f9536371be63e37a	BIRDDOG
188f261e5fca94bd1fc1edc1aafee8c0	CARBANAK

291a17814d5dbb5bce5b186334cde4b1	CARBANAK
4b3dac0a4f452b07d29f26b119180bd2	CARBANAK
4eda75dfd4d12eda6a6219423b5972bd	CARBANAK
6e9408c338e98a8bc166a8d4f8264019	CARBANAK
749c5085cda920e830cfed32842ba835	CARBANAK
80b022b39d91527f6ae5b4834d7c8173	CARBANAK
8ae284d547bd1b8bd6bc2431735f9142	CARBANAK
8e1e7f5ad99e48b740fd00085eab1f84	CARBANAK
9ae433cd5397af6b485f1abb06b2c5a2	CARBANAK
be1154e38df490e1dcbde3ffb2ebd05c	CARBANAK
c6b57e042ceadb60d6fab217d3523e17	CARBANAK
c6ec176592ea26c4ee27974273e592ff	CARBANAK
dd4f312c7e1c25564a8d00b0f3495e24	CARBANAK
facd37cd76989f45088ae98de8ed7aa0	CARBANAK

63241a3580cd1135170b044a84005e92	DRIFTPIN
70345aa0b970e1198a9267ae4532a11b	DRIFTPIN
de50d41d70b8879cdc73e684ad4ebe9f	DRIFTPIN
ddc9b71808be3a0e180e2befae4ff433	SIMPLECRED
90f35fd205556a04d13216c33cb0dbe3	BIRDDOG

IPs

IP Address	Malware	Attribution
107.161.159.17	CARBANAK	FIN7
107.181.160.12	CARBANAK	FIN7
107.181.160.75*	DRIFTPINHALFBAKED	FIN7
162.244.32.168	CARBANAK	FIN7
162.244.32.175	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	DRIFTPINHALFBAKED	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
95.215.46.76	CARBANAK	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

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

85.93.2.148	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

138.201.44.4	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

31.148.219.18*	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

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
bigred-tours.com	
clients12-google.com	BEACON.DNS
clients2-google.com	
p3-marketing.com	
cdn-googleapi.com	GRIFFON
cdn-googleservice.com	GRIFFON

algew.me	POWERSOURCE
aloqd.pw	POWERSOURCE
amhs.club	TEXTMATE
anselbakery.com	
apvo.club	TEXTMATE
arctic-west.com	
auyk.club	POWERSOURCE
b-bconsult.com	
bcleaningservice.com	
bigrussianbss.com	
bipismol.com	
bipovnerlvd.com	
blopsadmvdrl.com	
blopsdmvdrl.com	

bpee.pw	POWERSOURCE
bureauofinspections.com	
bvyv.club	POWERSOURCETEXTM
bwuk.club	POWERSOURCETEXTM
bwwrvada.com	
cgqy.us	POWERSOURCETEXTM
chatterbuzz-media.com	
chenstravelconsulting.com	
cihr.site	POWERSOURCETEXTM
citizentravel.biz	
cjsanandreas.com	
ckwl.pw	POWERSOURCETEXTM
cloo.com	POWERSOURCE
cnkmoh.pw	POWERSOURCE

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

doof.pw	POWERSOURCE
dosdkd.mo	POWERSOURCE
dpoo.pw	POWERSOURCE
dsud.com	POWERSOURCE
dtxf.pw	POWERSOURCE
duglas-manufacturing.com	
dvso.pw	POWERSOURCETEXTM
dyiud.com	POWERSOURCE
eady.club	POWERSOURCETEXTM
enuv.club	POWERSOURCETEXTM
eter.pw	POWERSOURCETEXTM
extmachine.biz	
facs.pw	TEXTMATE
fbjz.pw	POWERSOURCETEXTM

firsthotelgroup.com	
firstprolvdrec.com	
fkij.net	TEXTMATE
flowerprosv.com	
fredbanan.com	POWERSOURCE
futh.pw	POWERSOURCETEXTM
gcan.site	TEXTMATE
ge-stion.com	
gjcu.pw	POWERSOURCE
gjuc.pw	POWERSOURCE
glavpojdfde.com	BEACON.DNS
gnoa.pw	POWERSOURCETEXTM
gnsn.us	TEXTMATE
goldman-travel.com	

gprw.site	TEXTMATE
grand-mars.ru	
grij.us	POWERSOURCETEXTM
gsdg.site	TEXTMATE
guopksl.com	BEACON.DNS
gxhp.top	POWERSOURCETEXTM
hijrnataj.com	
hilertonv.com	BEACON.DNS
hilopser.com	BEACON.DNS
hippsjnv.com	
hldu.site	POWERSOURCE
hoplessinple.com	
hoplessinples.com	
hopsl3.com	BEACON.DNS

idjb.us	POWERSOURCETEXTM
ihrs.pw	POWERSOURCE
imyo.site	TEXTMATE
itstravel-ekb.ru	
ivcm.club	TEXTMATE
jblz.net	TEXTMATE
jersetl.com	BEACON.DNS
jimw.club	POWERSOURCETEXTM
jipdfonte.com	
jiposlve.com	BEACON.DNS
jjee.site	POWERSOURCE
johsimsoft.org	
jomp.site	POWERSOURCETEXTM
josephevinchi.com	

juste-travel.com	HALFBAKED
jxhv.site	POWERSOURCETEXTM
kalavadar.com	
kashtanspb.ru	
kbep.pw	TEXTMATE
kiposerd.com	BEACON.DNS
kiprovol.com	
kiprovolswe.com	
kjke.pw	POWERSOURCE
kjko.pw	POWERSOURCE
koldsdes.com	
kshv.site	POWERSOURCETEXTM
kuyarr.com	
kwoe.us	POWERSOURCETEXTM

lgdr.com	POWERSOURCE
lhlv.club	POWERSOURCETEXTM
lnoy.site	POWERSOURCETEXTM
luckystartwith.com	
lvrm.pw	POWERSOURCETEXTM
lvxf.pw	POWERSOURCE
manchedevs.org	
maofmdfd5.com	
meli-travel.com	HALFBAKED
melitravel.ru	
mewt.us	POWERSOURCE
mfka.pw	POWERSOURCETEXTM
michigan-construction.com	
mjet.pw	POWERSOURCE

mjut.pw	POWERSOURCE
mkwl.pw	TEXTMATE
molos-2.com	BEACON.DNS
mtgk.site	POWERSOURCE
mtxf.com	TEXTMATE
muedandubai.com	
muhh.us	POWERSOURCE
mut.pw	POWERSOURCE
mvze.pw	POWERSOURCE
mvzo.pw	POWERSOURCE
mxfg.pw	POWERSOURCE
mxtxt.net	
myspoernv.com	
navigators-travel.com	

nevaudio.com	
neverfaii.com	
nroq.pw	POWERSOURCE
ns0.site	POWERPIPE
ns0.space	POWERPIPE
ns0.website	POWERPIPE
ns1.press	POWERPIPEPOWERSOU
ns1.website	POWERPIPEPOWERSOU
ns2.press	POWERPIPEPOWERSOU
ns3.site	POWERPIPEPOWERSOU
ns3.space	POWERPIPEPOWERSOU
ns4.site	POWERPIPEPOWERSOU
ns4.space	POWERPIPEPOWERSOU
ns5.biz	POWERPIPEPOWERSOU

ns5.pw	MAL
ntlw.net	POWERSOURCE
nwrr.pw	POWERSOURCE
nxpu.site	POWERSOURCETEXTM
oaax.site	POWERSOURCETEXTM
odwf.pw	POWERSOURCE
odyr.us	POWERSOURCETEXTM
okiq.pw	POWERSOURCE
oknz.club	POWERSOURCETEXTM
olckwses.com	
olgw.my	POWERSOURCE
oloqd.pw	POWERSOURCE
oneliveforcopser.com	
onokder.com	BEACON.DNS

oof.pw	POWERSOURCE
ooyh.us	POWERSOURCETEXTM
orfn.com	POWERSOURCE
otzd.pw	POWERSOURCE
oxrp.info	POWERSOURCETEXTM
oyaw.club	POWERSOURCETEXTM
p3marketing.org	
pafk.us	POWERSOURCETEXTM
palj.us	POWERSOURCETEXTM
park-travels.com	
parktravel-mx.ru	
partnersind.biz	
pbbk.us	POWERSOURCETEXTM
pbsk.site	TEXTMATE

pdokls3.com	BEACON.DNS
pgnb.net	POWERSOURCE
pinewood-financial.com	
pjpi.com	POWERSOURCE
plusmarketingagency.com	
ppdx.pw	POWERSOURCETEXTM
prideofhume.com	
pronvowdecee.com	
proslr3.com	BEACON.DNS
prostelap3.com	BEACON.DNS
proverslokv4.com	
provnkfexxw.com	
pvze.club	POWERSOURCETEXTM
qdtn.us	TEXTMATE

qlpa.club	POWERSOURCETEXTM
qsez.club	TEXTMATE
qznm.pw	POWERSOURCE
rdnautomotiv.biz	
redtoursuk.org	
reld.info	POWERSOURCETEXTM
rescsovwe.com	BEACON.DNS
revital-travel.com	HALFBAKED
revitaltravel.com	
rmbs.club	TEXTMATE
rnkj.pw	POWERSOURCE
rtopsmve.com	BEACON.DNS
rzzc.pw	POWERSOURCE
sgvt.pw	POWERSOURCE

simpelkocsn.com	
simplewovmde.com	
soru.pw	POWERSOURCE
sprngwaterman.com	
strideindastry.biz	
strideindustrial.com	
strideindustrialusa.com	MAL
strikes-withlucky.com	
swio.pw	POWERSOURCE
tijm.pw	POWERSOURCE
tnt-media.net	
true-deals.com	BEACON.DNS
trustbankinc.com	
tsrs.pw	POWERSOURCE

twfl.us	POWERSOURCE
ueox.club	POWERSOURCETEXTM
ufyb.club	POWERSOURCETEXTM
utca.site	POWERSOURCETEXTM
uwqs.club	TEXTMATE
vdfe.site	POWERSOURCETEXTM
viebsdsccscw.com	
viebvbiiwcw.com	
vikppsod.com	BEACON.DNS
vjro.club	POWERSOURCETEXTM
vkpo.us	POWERSOURCETEXTM
voievnenibrinw.com	
vpua.pw	POWERSOURCE
vpuo.pw	POWERSOURCE

vwcq.us	POWERSOURCETEXTM
vxqt.us	POWERSOURCETEXTM
vxwy.pw	POWERSOURCE
wein.net	POWERSOURCE
wfsv.us	POWERSOURCETEXTM
whily.pw	
wider-machinery-usa.com	
widermachinery.biz	
widermachinery.com	
wnzg.us	TEXTMATE
wqiy.info	POWERSOURCETEXTM
wruj.club	TEXTMATE
wuc.pw	POWERSOURCE
wvzu.pw	POWERSOURCETEXTM

xnlz.club	TEXTMATE
xnmy.com	POWERSOURCE
yamd.pw	POWERSOURCE
ybnz.site	TEXTMATE
ydvd.net	TEXTMATE
yedq.pw	POWERSOURCE
yodq.pw	POWERSOURCE
yomd.pw	POWERSOURCE
yqox.pw	POWERSOURCE
ysxy.pw	POWERSOURCETEXTM
zcnt.pw	POWERSOURCETEXTM
zdqp.pw	POWERSOURCE
zjav.us	POWERSOURCETEXTM
zjvz.pw	POWERSOURCE

zody.pw	POWERSOURCETEXTM
zrst.com	POWERSOURCE
zugh.us	POWERSOURCETEXTM
clients14-google.com	
clients18-google.com	
clients19-google.com	
clients23-google.com	
clients31-google.com	
clients33-google.com	BEACON.DNS
clients39-google.com	
clients46-google.com	
clients47-google.com	
clients51-google.com	
clients52-google.com	

clients56-google.com	
clients57-google.com	
clients58-google.com	
clients6-google.com	HALFBAKED
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-googlesr5.com	
stats10-google.com	CARBANAK
stats25-google.com	BEACON.DNS
treasury-government.com	
usdepartmentofrevenue.com	
bols-googls.com	
moopisndvdvr.com	
dewifal.com	
essentialetimes.com	
fisrdteditionps.com	
fisrteditionps.com	

moneyma-r.com	
newuniquesolutions.com	
wedogreatpurchases.com	

Posted in Threat Intelligence—Security & Identity

Related articles

Threat Intelligence

Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military

Threat Intelligence

Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)

By Mandiant • 19-minute read

By Google Threat Intelligence Group • 10-minute read

Threat Intelligence

How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends

By Mandiant • 10-minute read

Threat Intelligence

capa Explorer Web: A Web-Based Tool for Program Capability Analysis

By Mandiant • 6-minute read