ESET discovered an undocumented backdoor used by the infamous Stealth Falcon group

General information

UUID	5d77a165-889c-44ac-a01b-34550a000082
2019-09-10	**Date**
Owner org	No value specified.
Threat level	High (1)
Analysis	Completed (2)
Info	ESET discovered an undocumented backdoor used by the infamous Stealth Falcon group
Event date	2019-09-10 14:10:21
Published	**Yes** (2019-09-10 14:10:28)
Creator Org	Profero
# Attributes	41
Tags	osint:source-type="blog-post" tlp:white Threat Type:APT veris:actor:motive="Espionage" Actor:Stealth Falcon group misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1059" misp-galaxy:mitre-attack-pattern="Execution through API - T1106" misp-galaxy:mitre-attack-pattern="Rundll32 - T1085" misp-galaxy:mitre-attack-pattern="Scheduled Task - T1053" misp-galaxy:mitre-attack-pattern="BITS Jobs - T1197" misp-galaxy:mitre-attack-pattern="Deobfuscate/Decode Files or Information - T1140" misp-galaxy:mitre-attack-pattern="File Deletion - T1107" misp-galaxy:mitre-attack-pattern="Masquerading - T1036" misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" misp-galaxy:mitre-attack-pattern="Obfuscated Files or Information - T1027" misp-galaxy:mitre-attack-pattern="Security Software Discovery - T1063" misp-galaxy:mitre-attack-pattern="Data Staged - T1074" misp-galaxy:mitre-attack-pattern="Data from Local System - T1005" misp-galaxy:mitre-attack-pattern="Fallback Channels - T1008" misp-galaxy:mitre-attack-pattern="Remote File Copy - T1105" misp-galaxy:mitre-attack-pattern="Standard Cryptographic Protocol - T1032" misp-galaxy:mitre-attack-pattern="Automated Exfiltration - T1020" misp-galaxy:mitre-attack-pattern="Data Encrypted - T1022" misp-galaxy:mitre-attack-pattern="Exfiltration Over Command and Control Channel - T1041"

Attributes

Attribute #1

UUID	5d77a61d-d398-4528-967c-33a30a000082
Category	External analysis
Type	link
Value	https://www.welivesecurity.com/2019/09/09/backdoor-stealth-falcon-group/
Tags	osint:source-type="blog-post"

Attribute #2

UUID	5d77a6c7-c474-4228-a83c-34550a000082
Category	External analysis
Type	comment
Value	The Win32/StealthFalcon backdoor, which appears to have been created in 2015, allows the attacker to control the compromised computer remotely. We have seen a small number of targets in UAE, Saudi Arabia, Thailand, and the Netherlands; in the latter case, the target was a diplomatic mission of a Middle Eastern country. How the backdoor was distributed and executed on the target systems is beyond the scope of this investigation; our analysis focuses on its capabilities and its C&C communication.

Attribute #3

UUID	5d77a6e2-d858-4fce-a9e8-34370a000082
Category	External analysis
Type	comment
Value	In its communication with the C&C server, Win32/StealthFalcon uses the standard Windows component Background Intelligent Transfer Service (BITS), a rather unusual technique. BITS was designed to transfer large amounts of data without consuming a lot of network bandwidth, which it achieves by sending the data with throttled throughput so as not to affect the bandwidth needs of other applications. It is commonly used by updaters, messengers, and other applications designed to operate in the background. This means that BITS tasks are more likely to be permitted by host-based firewalls.

Attribute #4

UUID	5d77a7d2-440c-4467-9137-371e0a000082
Category	External analysis
Type	comment
Value	Some technical information about Stealth Falcon has already been made public – notably, in the already mentioned analysis by the Citizen Lab. Event: "OSINT - Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents"

Attribute #5

UUID	5d77a886-3f00-4b50-8917-371e0a000082
Category	External analysis
Type	link
Value	https://citizenlab.org/2016/05/stealth-falcon/

Attribute #6

UUID	5d77a8b2-ab6c-4bdc-a90f-36c70a000082
Category	External analysis
Type	comment
Value	Both Win32/StealthFalcon and the PowerShell-based backdoor described in the Citizen Lab analysis share the same C&C server: the address windowsearchcache[.]com was used as a "Stage Two C2 Server Domain" in the backdoor analyzed by the Citizen Lab, and also in one of the versions of Win32/StealthFalcon. Both backdoors display significant similarities in code – although they are written in different languages, the underlying logic is preserved. Both use hardcoded identifiers (most probably campaign ID/target ID). In both cases, all network communication from the compromised host is prefixed with these identifiers and encrypted with RC4 using a hardcoded key. For their C&C server communication, they both use HTTPS but set specific flags for the connection to ignore the server certificate.

Attribute #7

UUID	5d77a8c4-59e0-438a-9129-33a30a000082
Category	Antivirus detection
Type	text
Value	Win32/StealthFalcon

Attribute #8

UUID	5d77a8eb-fa80-4ce2-b79b-33a30a000082
Category	Payload delivery
Type	sha1
Value	31b54aebdaf5fbc73a66ac41ccb35943cc9b7f72

Attribute #9

UUID	5d77a8f3-c820-43b3-b5f5-36c70a000082
Category	Payload delivery
Type	sha1
Value	50973a3fc57d70c7911f7a952356188b9939e56b

Attribute #10

UUID	5d77a8fd-36d8-4b1e-91ad-36c70a000082
Category	Payload delivery
Type	sha1
Value	244eb62b9ac30934098ca4204447440d6fc4e259

Attribute #11

UUID	5d77a907-6610-4795-afa3-34550a000082
Category	Payload delivery
Type	sha1
Value	5c8f83cc4ff57e7c67925df4d9daabe5d0cc07e2

Attribute #12

UUID	5d77a92f-dc44-4868-96c0-389f0a000082
Category	Other
Type	comment
Value	RC4 Keys: 258A4A9D139823F55D7B9DA1825D101107FBF88634A870DE9800580DAD556BA3 2519DB0FFEC604D6C9A655CF56B98EDCE10405DE36810BC3DCF125CDE30BA5A2 3EDB6EA77CD0987668B360365D5F39FDCF6B366D0DEAC9ECE5ADC6FFD20227F6 8DFFDE77A39F3AF46D0CE0B84A189DB25A2A0FEFD71A0CD0054D8E0D60AB08DE

Attribute #13

UUID	5d77a93f-4730-44c9-a73e-34380a000082
Category	Payload delivery
Type	filename
Value	ImageIndexer.dll

Attribute #14

UUID	5d77a947-5b10-4478-a032-34380a000082
Category	Payload delivery
Type	filename
Value	WindowsBackup.dll

Attribute #15

UUID	5d77a952-7db0-422a-9fc2-389f0a000082
Category	Payload delivery
Type	filename
Value	WindowsSearchCache.dll

Attribute #16

UUID	5d77a95d-e8f8-437b-908e-389f0a000082
Category	Payload delivery
Type	filename
Value	JavaUserUpdater.dll

Attribute #17

UUID	5d77a96d-dd38-483a-aee5-339f0a000082
Category	Other
Type	comment
Value	Log file name patterns %TEMP%\dsc* %TEMP%\sld* %TEMP%\plx*

Attribute #18

UUID	5d77a9b3-ae74-45b1-a8f4-33a30a000082
Category	Persistence mechanism
Type	regkey
Value	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions

Attribute #19

UUID	5d77aa03-60f0-4d3b-9f45-37cb0a000082
Category	Other
Type	comment
Value	BITS job names: WindowsImages- WindowsBackup- WindowsSearchCache- ElectricWeb

Attribute #20

UUID	5d77aa18-6634-4779-ba52-34370a000082
Category	Network activity
Type	domain
Value	footballtimes.info

Attribute #21

UUID	5d77aa23-b024-4491-a2d6-34380a000082
Category	Network activity
Type	domain
Value	vegetableportfolio.com

Attribute #22

UUID	5d77aa2f-e240-47a4-bb0f-34380a000082
Category	Network activity
Type	domain
Value	windowsearchcache.com

Attribute #23

UUID	5d77aa3e-7c38-48b2-8509-34380a000082
Category	Network activity
Type	domain
Value	electricalweb.org

Attribute #24

UUID	5d77aa4d-572c-4159-a86d-339f0a000082
Category	Network activity
Type	domain
Value	upnpdiscover.org

Attribute #25

UUID	45587c18-aa2a-4abc-86c6-8c0bf53be206
Category	Network activity
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Type	domain
Value	dev.upnpdiscover.org

Attribute #26

UUID	b7618a5a-25e9-4b0e-8dae-9d8b1ea38724
Category	Network activity
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Type	url
Value	http://upnpdiscover.org/

Attribute #27

UUID	e70610e8-702c-4324-a18b-da0d466bdf00
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	domain
Value	ssl.electricalweb.org

Attribute #28

UUID	2edfdf7b-2b34-4170-a7c1-724fde89f2c5
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	domain

Value	forums.electricalweb.org

Attribute #29

UUID	8ed24aef-3e02-4801-b08b-df8bc3924d1d
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	domain
Value	dev.electricalweb.org

Attribute #30

UUID	eafec622-ad0d-49db-84ce-b14abcc803d8
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	domain
Value	kb.electricalweb.org

Attribute #31

UUID	a8ecfc5b-b5ba-4152-bf1a-42c72c425ab6
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	domain
Value	mobile.electricalweb.org

Attribute #32

UUID	55915b6d-ff36-46bc-bae5-d6186d8c01ea
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	url
Value	http://electricalweb.org/

Attribute #33

UUID	a2e136c3-3be8-423e-b087-f225784bdf64
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	url
Value	https://electricalweb.org/

Attribute #34

UUID	6165667a-f9bb-41ed-bc46-bf5392061dda
Category	Network activity
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	domain
Value	live.footballtimes.info

Attribute #35

UUID	bb9c2314-8076-4a7b-8808-65cc6c6b5198
Category	Network activity
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	domain
Value	ftp.footballtimes.info

Attribute #36

UUID	4fc51d42-1161-4093-8d12-d584cabb1df6
Category	Network activity
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	url
Value	http://footballtimes.info/

Attribute #37

UUID	8a4c83ca-c8f9-499b-8621-50014d2a236e
Category	Network activity

Comment	footballtimes.info: Enriched via the virustotal_public module
Type	url
Value	https://footballtimes.info/

Attribute #38

UUID	a9ce42a5-8772-45a6-8a44-4d4fd075233c
Category	Network activity
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	domain
Value	resources.vegetableportfolio.com

Attribute #39

UUID	d291a785-6b3c-414e-b018-34d4a2276903
Category	Network activity
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	domain
Value	sites.vegetableportfolio.com

Attribute #40

UUID	c97b3467-b246-4b68-9d54-0b50508a0a0a
Category	Network activity
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	url
Value	https://vegetableportfolio.com/

Attribute #41

UUID	f83190f4-2395-4f2f-80cb-4fd95a0597f5
Category	Network activity
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	url
Value	http://vegetableportfolio.com/

Objects

Object #1

UUID	076cf79b-47a4-4b31-add3-053dc0f32785
Description	Whois records information for a domain name or an IP address.
Meta Category	network
Object Name	whois
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Object date	2019-09-10 14:04:16

Attribute #1

UUID	e1c79d43-038a-421e-b366-f412afaf54dd
Category	Other
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Type	text
Value	Domain Name: UPNPDISCOVER.ORG Registry Domain ID: D189284552-LROR Registrar WHOIS Server: whois.internet.bs Registrar URL: www.internet.bs Updated Date: 2018-08-13T13:19:33Z Creation Date: 2016-07-02T18:31:16Z Registry Expiry Date: 2019-07-02T18:31:16Z Registrar: Internet Domain Service BS Corp Registrar IANA ID: 2487 Registrar Abuse Contact Email: abuse@internet.bs Registrar Abuse Contact Phone: +1.5167401179 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Domain Status: pendingDelete https://icann.org/epp#pendingDelete Domain Status: serverHold https://icann.org/epp#serverHold Domain Status: redemptionPeriod https://icann.org/epp#redemptionPeriod Registrant Country: BS Name Server: NS1.IBSPARK.COM Name Server: NS2.IBSPARK.COM DNSSEC: unsigned

Object #2

UUID	81c3ac7d-b01e-4b99-8418-093126d45d4e
Description	A domain and IP address seen as a tuple in a specific time frame.
Meta Category	network
Object Name	domain-ip
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Object date	2019-09-10 14:04:16

Attribute #1

UUID	e0a75911-f990-4473-bde3-3573aa459b32
Category	Network activity
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Type	domain
Value	upnpdiscover.org

Attribute #2

UUID	e85a27ee-53d9-4cae-9a45-3d2ad2a2a179
Category	Network activity
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Type	ip-dst
Value	103.208.86.62

Attribute #3

UUID	2d722a30-3574-4ed2-b6c3-fb76d9f18225
Category	Network activity
Comment	upnpdiscover.org: Enriched via the virustotal_public module
Type	ip-dst
Value	54.72.130.67

Object #3

UUID	87ca8fc5-3462-412b-b904-9d36502ac3a2
Description	Whois records information for a domain name or an IP address.
Meta Category	network
Object Name	whois
Comment	electricalweb.org: Enriched via the virustotal_public module
Object date	2019-09-10 14:05:11

Attribute #1

UUID	ca2daaa8-940e-4f4a-80c1-db8ea6e0588a
Category	Other
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	text
Value	Domain Name: ELECTRICALWEB.ORG Registry Domain ID: D189202461-LROR Registrar WHOIS Server: whois.publicdomainregistry.com Registrar URL: http://www.publicdomainregistry.com Updated Date: 2018-10-01T14:32:17Z Creation Date: 2016-06-21T05:59:25Z Registry Expiry Date: 2021-06-21T05:59:25Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Registrant Country: US Name Server: A8332F3A.BITCOIN-DNS.HOSTING Name Server: AD636824.BITCOIN-DNS.HOSTING Name Server: 1A7EA920.BITCOIN-DNS.HOSTING Name Server: C358EA2D.BITCOIN-DNS.HOSTING DNSSEC: unsigned Updated Date: 2016-08-21T03:03:35Z Registrar Registration Expiration Date: 2021-06-21T05:59:25Z Registrar IANA ID: 5041-DR Registry Registrant ID: Not Available From Registry Registrant Email: [REDACTED]@gdpr-masked.com Registry Admin ID: Not Available From Registry Admin Organization: GDPR Masked Admin City: GDPR Masked Admin State/Province: GDPR Masked Admin Postal Code: 00000 Admin Country: US Admin Email: [REDACTED]@gdpr-masked.com Registry Tech ID: Not Available From Registry Tech Organization: GDPR Masked Tech City: GDPR Masked Tech State/Province: GDPR Masked Tech Postal Code: 00000 Tech Country: US Tech Email: [REDACTED]@gdpr-masked.com Name Server: 1a7ea920.bitcoin-dns.hosting Name Server: a8332f3a.bitcoin-dns.hosting Name Server: ad636824.bitcoin-dns.hosting Name Server: c358ea2d.bitcoin-dns.hosting DNSSEC: Unsigned

Object #4

UUID	7bbe7aca-1e11-43a9-bdf3-c07bae3054c3
Description	A domain and IP address seen as a tuple in a specific time frame.
Meta Category	network
Object Name	domain-ip
Comment	electricalweb.org: Enriched via the virustotal_public module
Object date	2019-09-10 14:05:11

Attribute #1

UUID	a61c2d73-eb70-4e6e-a198-1a18c99e119a
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	domain
Value	electricalweb.org

Attribute #2

UUID	6b89648c-3202-4ba2-b9f6-e377233b0a34
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	ip-dst
Value	163.172.211.46

Attribute #3

UUID	09ef69f3-92ab-4b66-b394-5be3021b10cf
Category	Network activity
Comment	electricalweb.org: Enriched via the virustotal_public module
Type	ip-dst
Value	193.105.134.75

Object #5

UUID	80065337-6f14-40a6-873a-c415616da3b5
Description	Whois records information for a domain name or an IP address.
Meta Category	network
Object Name	whois
Comment	footballtimes.info: Enriched via the virustotal_public module
Object date	2019-09-10 14:05:42

Attribute #1

UUID	6a598fe8-e5fb-45ad-b75a-71737ca0686c
Category	Other
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	text
Value	Creation Date: 2016-06-01T11:36:18Z DNSSEC: unsigned Domain Name: FOOTBALLTIMES.INFO Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS-CANADA.TOPDNS.COM Name Server: NS-UK.TOPDNS.COM Name Server: NS-USA.TOPDNS.COM Registrant Country: BS Registrant Organization: 0e1b84d4e75bdded Registrant State/Province: 2ae436240819c906 Registrar IANA ID: 2487 Registrar URL: www.internet.bs Registrar: Internet Domain Service BS Corp Registry Domain ID: D503300000014464349-LRMS Registry Expiry Date: 2020-06-01T11:36:18Z Updated Date: 2018-05-31T04:29:31Z

Object #6

UUID	6bfe3437-f79a-4ec3-aaec-1db3979947d5
Description	A domain and IP address seen as a tuple in a specific time frame.
Meta Category	network
Object Name	domain-ip
Comment	footballtimes.info: Enriched via the virustotal_public module
Object date	2019-09-10 14:05:42

Attribute #1

UUID	826c1bae-b239-42a6-81af-5848e321f2c1
Category	Network activity
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	domain
Value	footballtimes.info

Attribute #2

UUID	b43408e8-a6a1-4ad5-bc72-039b64718e48
Category	Network activity
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	ip-dst
Value	178.17.170.8

Attribute #3

UUID	6ced7713-5da2-4575-8808-2dde165ee8d8
Category	Network activity
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	ip-dst
Value	185.227.82.19

Attribute #4

UUID	d705f944-8551-4a26-9baa-8cd9431cfbe0
Category	Network activity
Comment	footballtimes.info: Enriched via the virustotal_public module
Type	ip-dst
Value	37.1.202.213

Object #7

UUID	fa25884b-687e-4497-a021-0f31fbcbb143
Description	Whois records information for a domain name or an IP address.
Meta Category	network
Object Name	whois
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Object date	2019-09-10 14:08:17

Attribute #1

UUID	e11021de-18dd-4b74-87e7-7b5aa1c3dc9c
Category	Other
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	text
Value	Admin City: Nassau Admin Country: BS Admin Email: c0ccf7de3150c2cfs@customers.whoisprivacycorp.com Admin Organization: Whois Privacy Corp. Admin State/Province: New Providence Creation Date: 2016-06-30T06:39:36Z DNSSEC: unsigned Domain Name: VEGETABLEPORTFOLIO.COM Domain Status: clientTransferProhibited - http://www.icann.org/epp#clientTransferProhibited Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: DNS1.ORANGEWEBSITE.COM Name Server: DNS2.ORANGEWEBSITE.COM Name Server: dns1.orangewebsite.com Name Server: dns2.orangewebsite.com Registrant City: 0cfd40d5e4e26273 Registrant Country: BS Registrant Email: 5f3a2097f8f34960s@customers.whoisprivacycorp.com Registrant Fax Ext: 3432650ec337c945 Registrant Fax: 3432650ec337c945 Registrant Name: edeae57e15fec50a Registrant Organization: 0e1b84d4e75bdded Registrant Phone Ext: 3432650ec337c945 Registrant Phone: e49a4d0c0dd3e72f Registrant Postal Code: 3432650ec337c945 Registrant State/Province: 2ae436240819c906 Registrant Street: 8875d132245d58df Registrar Abuse Contact Email: abuse@internet.bs Registrar Abuse Contact Phone: +1.5167401179 Registrar IANA ID: 2487 Registrar Registration Expiration Date: 2020-06-30T06:39:36Z Registrar URL: http://www.internet.bs Registrar URL: http://www.internetbs.net Registrar WHOIS Server: whois.internet.bs Registrar: Internet Domain Service BS Corp Registrar: Internet Domain Service BS Corp. Registry Domain ID: 2038527430_DOMAIN_COM-VRSN Registry Expiry Date: 2020-06-30T06:39:36Z Tech City: Nassau Tech Country: BS Tech Email: d14c06a23c31bb10s@customers.whoisprivacycorp.com Tech Organization: Whois Privacy Corp. Tech State/Province: New Providence Updated Date: 2016-06-30T06:39:36Z Updated Date: 2018-06-29T04:46:06Z

Object #8

UUID	1995e94b-9860-4751-a113-f0012e445ad9
Description	A domain and IP address seen as a tuple in a specific time frame.
Meta Category	network
Object Name	domain-ip
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Object date	2019-09-10 14:08:17

Attribute #1

UUID	74fe9ae0-446d-4f58-8cc6-2bad234bcfe6
Category	Network activity
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	domain
Value	vegetableportfolio.com

Attribute #2

UUID	3e9ebfea-c972-4cc3-8032-4a4726ff4868
Category	Network activity
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	ip-dst
Value	46.183.219.85

Attribute #3

UUID	95c60f2a-ada1-49ea-92a3-3374e4344492
Category	Network activity
Comment	vegetableportfolio.com: Enriched via the virustotal_public module
Type	ip-dst
Value	82.221.128.183