

OSINT - New Malware with Ties to SunOrcal Discovered

General information

UUID	5a0a9aa9-23a4-4607-b6df-41a9950d210f
Date	2017-11-10
Owner org	None
Threat level	3
Analysis	2
Info	OSINT - New Malware with Ties to SunOrcal Discovered
Event date	2017-11-17 12:40:35
Published	Yes (2018-02-12 17:11:34)
Creator Org	CIRCL
# Attributes	75
Tags	<code>type:OSINT</code> <code>tlp:white</code> <code>circl:incident-classification="malware"</code> <code>osint:source-type="blog-post"</code>

Attributes

Attribute #0

UUID	5a0a9ade-3b60-4fbb-87d2-4628950d210f
Category	External analysis
Type	link
Value	https://researchcenter.paloaltonetworks.com/2017/11/unit42-new-malware-with-ties-to-sunorcal-discovered/
Tags	osint:source-type="blog-post"

Attribute #1

UUID	5a0a9af4-0d1c-4ae0-8903-45c4950d210f
Category	External analysis
Type	comment
Value	Unit 42 has discovered a new malware family we've named "Reaver" with ties to attackers who use SunOrcal malware. SunOrcal activity has been documented to at least 2013, and based on metadata surrounding some of the C2s, may have been active as early as 2010. The new family appears to have been in the wild since late 2016 and to date we have only identified 10 unique samples, indicating it may be sparingly used. Reaver is also somewhat unique in the fact that its final payload is in the form of a Control panel item, or CPL file. To date, only 0.006% of all malware seen by Palo Alto Networks employs this technique, indicating that it is in fact fairly rare.
Tags	osint:source-type="blog-post"

Attribute #2

UUID	5a0a9d47-1c7c-4353-8523-440b950d210f
Category	Persistence mechanism
Type	regkey
Value	%COMMONPROGRAMFILES%\services\
Tags	No tags

Attribute #3

UUID	5a0a9d47-808c-4833-b739-43bf950d210f
Category	Persistence mechanism
Type	regkey
Value	%APPDATA%\microsoft\mmc\
Tags	No tags

Attribute #4

UUID	5a0a9d47-91e0-4fea-8a8d-48ce950d210f
Category	Persistence mechanism
Type	regkey

Value	HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Common Startup
Tags	No tags

Attribute #5

UUID	5a0a9d47-0d2c-4f98-9913-4ea3950d210f
Category	Persistence mechanism
Type	regkey
Value	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup
Tags	No tags

Attribute #6

UUID	5a0a9d47-a0a4-4f6b-bd53-42b4950d210f
Category	Payload delivery
Type	filename
Value	'%TEMP%\~WUpdate.Ink
Tags	No tags

Attribute #7

UUID	5a0a9d96-48d4-4538-b643-4c26950d210f
Category	Payload delivery
Type	filename
Value	%TEMP%\~Update.Ink
Tags	No tags

Attribute #8

UUID	5a0a9d96-d87c-4b6f-b3a6-4eea950d210f
Category	Persistence mechanism
Type	regkey
Value	%APPDATA%\microsoft\credentials\
Tags	No tags

Attribute #9

UUID	5a0a9d96-83dc-4a40-90fe-46d9950d210f
Category	Payload delivery
Type	filename
Value	%TEMP%\winhelp.dat
Tags	No tags

Attribute #10

UUID	5a0a9d96-cc18-491c-b16b-4ffe950d210f
------	--------------------------------------

Category	Payload delivery
Type	filename
Value	[path_previously_identified]\winhelp.cpl
Tags	No tags

Attribute #11

UUID	5a0a9e4c-1c14-49c0-bee2-4f7d950d210f
Category	Network activity
Comment	C2
Type	hostname
Value	www.fyoutside.com
Tags	No tags

Attribute #12

UUID	5a0a9e4c-ab08-47f8-991f-471c950d210f
Category	Network activity
Comment	C2
Type	hostname
Value	www.tashdqdxp.com
Tags	No tags

Attribute #13

UUID	5a0a9e4c-8ba4-43d7-a8e3-4b52950d210f
Category	Network activity
Comment	C2
Type	hostname
Value	www.weryhstui.com
Tags	No tags

Attribute #14

UUID	5a0a9e4c-bcf8-42ac-86dc-48b0950d210f
Category	Network activity
Type	ip-dst
Value	98.126.156.210
Tags	No tags

Attribute #15

UUID	5a0a9e4c-9440-40fa-ac80-4320950d210f
Category	Network activity
Comment	C2
Type	hostname

Value	www.olinaodi.com
Tags	No tags

Attribute #16

UUID	5a0a9eae-a23c-4b65-b46b-4683950d210f
Category	Payload delivery
Comment	Reaver.v1
Type	sha256
Value	d560f44188fb56d3abb11d9508e1167329470de19b811163eb1167534722e666
Tags	No tags

Attribute #17

UUID	5a0a9eae-5e1c-411a-b1ba-49ac950d210f
Category	Payload delivery
Comment	Reaver.v2
Type	sha256
Value	98eb5465c6330b9b49df2e7c9ad0b1164aa5b35423d9e80495a178eb510cdc1c
Tags	No tags

Attribute #18

UUID	5a0a9eae-ccf0-4390-bcde-43bd950d210f
Category	Payload delivery
Comment	Reaver.v2
Type	sha256
Value	05ddb0506ec95fb460b3994e5b21cdb0418ba4aa406374ca1b91249349b7640
Tags	No tags

Attribute #19

UUID	5a0a9eae-3ef4-42d5-baca-44c4950d210f
Category	Payload delivery
Comment	Reaver.v3
Type	sha256
Value	18ac3b14300ecfeed4b64a844c16dcc06b0e3513d0954d6c6182f2ea14e4c92
Tags	No tags

Attribute #20

UUID	5a0a9eae-8cc8-4bbd-aded-4e38950d210f
Category	Payload delivery
Comment	Reaver.v3

Type	sha256
Value	c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d
Tags	No tags

Attribute #21

UUID	5a0a9eae-486c-4820-b2b3-4bf0950d210f
Category	Payload delivery
Comment	Reaver.v3
Type	sha256
Value	9213f70bce491991c4cbbbd7dc3e67d3a3d535b965d7064973b35c50f265e59b
Tags	No tags

Attribute #22

UUID	5a0a9eae-bef4-4696-a1ab-4c83950d210f
Category	Payload delivery
Comment	Reaver.v3
Type	sha256
Value	26c234c73e2c3448589c7d4a0cf17f615ad3666541a4e611e2d8b77637205bcf
Tags	No tags

Attribute #23

UUID	5a0a9eae-7560-4794-90d1-4f4d950d210f
Category	Payload delivery
Comment	Reaver.v3
Type	sha256
Value	ae9f158e4886cfdbfb4f1b3b25707d05f6fd873d0be9d8e7334a2c28741228ee
Tags	No tags

Attribute #24

UUID	5a0a9eae-d3c4-4809-aea5-435c950d210f
Category	Payload delivery
Comment	Reaver.v3
Type	sha256
Value	1fcda755e8fa23d27329e4bc0443a82e1c1e9a6c1691639db256a187365e4db1
Tags	No tags

Attribute #25

UUID	5a0a9eae-a5dc-43ab-9158-451c950d210f
------	--------------------------------------

Category	Payload delivery
Comment	Reaver.v3
Type	sha256
Value	c906250e0a4c457663e37119ebe1efa1e4b97eef1d975f383ac3243f9f09908c
Tags	No tags

Attribute #26

UUID	5a0a9eae-1d70-4f14-b316-4ce4950d210f
Category	Payload delivery
Comment	Reaver.v3
Type	sha256
Value	1813f10bcf74beb582c824c64fff63cb150d178bef93af81d875ca84214307a1
Tags	No tags

Attribute #27

UUID	5a0a9eae-7674-4a3f-a595-4006950d210f
Category	Payload delivery
Comment	SunOrcal
Type	sha256
Value	799139b5278dc2ac24279cc6c3db44f4ef0ea78ee7b721b0ace38fd8018c51ac
Tags	No tags

Attribute #28

UUID	5a0a9eae-4a58-4535-9998-49b7950d210f
Category	Payload delivery
Comment	SunOrcal
Type	sha256
Value	81d887fefdbb0219647991c2b7bddf45c2fede4dc6fc18408f1706e0279615b2
Tags	No tags

Attribute #29

UUID	5a0a9eae-6ae4-41a1-8402-4328950d210f
Category	Payload delivery
Comment	SunOrcal
Type	sha256
Value	58312fb742ce881e040e1b5b8555f00a402b8dd4fc886acaae2f862040b3bfc5
Tags	No tags

Attribute #30

UUID	5a0a9eae-6edc-4177-afd5-4c93950d210f
Category	Payload delivery
Comment	SunOrcal
Type	sha256
Value	38ea33dab0ba2edd16ecd98cba161c550d1036b253c8666c4110d198948329fb
Tags	No tags

Attribute #31

UUID	5a0a9eae-8388-4e7f-ab5b-4e95950d210f
Category	Payload delivery
Comment	SunOrcal
Type	sha256
Value	cb7c0cf1750baaa11783e93369230ee666b9f3da7298e4d1bb9a07af6a439f2f
Tags	No tags

Attribute #32

UUID	5a0a9efc-6604-4cd9-acbb-4632950d210f
Category	Network activity
Comment	C2
Type	ip-dst
Value	104.148.70.217
Tags	No tags

Attribute #33

UUID	5a0ed8bb-5df0-47a8-9785-44a702de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: cb7c0cf1750baaa11783e93369230ee666b9f3da7298e4d1bb9a07af6a439f2f
Type	sha1
Value	da7a5e54d1d45462bda65807c1ef03ee34b7e777
Tags	No tags

Attribute #34

UUID	5a0ed8bb-f580-4b51-a866-482602de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: cb7c0cf1750baaa11783e93369230ee666b9f3da7298e4d1bb9a07af6a439f2f
Type	md5
Value	7dcf79a66192e88b92ccc12810e61329
Tags	No tags

Attribute #35

UUID	5a0ed8bb-8a94-47be-9f1e-463f02de0b81
Category	External analysis
Comment	SunOrcal - Xchecked via VT: cb7c0cf1750baaa11783e93369230ee666b9f3da7298e4d1bb9a07af6a439f2f
Type	link
Value	https://www.virustotal.com/file/cb7c0cf1750baaa11783e93369230ee666b9f3da7298e4d1bb9a07af6a439f2f/analysis/1510574305/
Tags	No tags

Attribute #36

UUID	5a0ed8bb-3f4c-411b-9507-4d1602de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 38ea33dab0ba2edd16ecd98cba161c550d1036b253c8666c4110d198948329fb
Type	sha1
Value	704886d56ded5817e39d7442b0203c2f76207f92
Tags	No tags

Attribute #37

UUID	5a0ed8bb-6f34-4e76-ba5b-45ae02de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 38ea33dab0ba2edd16ecd98cba161c550d1036b253c8666c4110d198948329fb
Type	md5
Value	af6a25fc28e0560860c01d74854a2cba
Tags	No tags

Attribute #38

UUID	5a0ed8bb-5b24-48ce-82c4-4e2b02de0b81
Category	External analysis
Comment	SunOrcal - Xchecked via VT: 38ea33dab0ba2edd16ecd98cba161c550d1036b253c8666c4110d198948329fb
Type	link
Value	https://www.virustotal.com/file/38ea33dab0ba2edd16ecd98cba161c550d1036b253c8666c4110d198948329fb/analysis/1510574322/
Tags	No tags

Attribute #39

UUID	5a0ed8bb-830c-472b-9d19-481002de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 58312fb742ce881e040e1b5b8555f00a402b8dd4fc886acaae2f862040b3bfc5
Type	sha1

Value	9adbe92835ee2cc93e0d99b9d4536eb7727acf47
Tags	No tags

Attribute #40

UUID	5a0ed8bb-b94c-4e75-a47d-488002de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 58312fb742ce881e040e1b5b8555f00a402b8dd4fc886acaae2f862040b3bfc5
Type	md5
Value	47cc3592bbf8c3b516ae74c95efb3344
Tags	No tags

Attribute #41

UUID	5a0ed8bb-8d8c-4b7a-a223-498e02de0b81
Category	External analysis
Comment	SunOrcal - Xchecked via VT: 58312fb742ce881e040e1b5b8555f00a402b8dd4fc886acaae2f862040b3bfc5
Type	link
Value	https://www.virustotal.com/file/58312fb742ce881e040e1b5b8555f00a402b8dd4fc886acaae2f862040b3bfc5/analysis/1510574347/
Tags	No tags

Attribute #42

UUID	5a0ed8bb-b9b0-40ac-a84f-4b6002de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 81d887fefdbb0219647991c2b7bddf45c2fede4dc6fc18408f1706e0279615b2
Type	sha1
Value	7fa8bfc051b98698e6b95cbc7163e4aa41880279
Tags	No tags

Attribute #43

UUID	5a0ed8bb-65e8-471f-9a66-4e3102de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 81d887fefdbb0219647991c2b7bddf45c2fede4dc6fc18408f1706e0279615b2
Type	md5
Value	5eb3a846092cae378fcd45bdf5453536
Tags	No tags

Attribute #44

UUID	5a0ed8bb-d7c0-4ed1-9bdc-497002de0b81
Category	External analysis

Comment	SunOrcal - Xchecked via VT: 81d887fefdbb0219647991c2b7bddf45c2fede4dc6fc18408f1706e0279615b2
Type	link
Value	https://www.virustotal.com/file/81d887fefdbb0219647991c2b7bddf45c2fede4dc6fc18408f1706e0279615b2/analysis/1510574318/
Tags	No tags

Attribute #45

UUID	5a0ed8bb-a260-4d97-b3c8-43eb02de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 799139b5278dc2ac24279cc6c3db44f4ef0ea78ee7b721b0ace38fd8018c51ac
Type	sha1
Value	a6e538a01c366580e90e49249251b66dfe39c72f
Tags	No tags

Attribute #46

UUID	5a0ed8bb-61ec-48e1-8327-492b02de0b81
Category	Payload delivery
Comment	SunOrcal - Xchecked via VT: 799139b5278dc2ac24279cc6c3db44f4ef0ea78ee7b721b0ace38fd8018c51ac
Type	md5
Value	11a5b1901243396984670af7acc6cf72
Tags	No tags

Attribute #47

UUID	5a0ed8bb-4f20-46d8-b762-4cf702de0b81
Category	External analysis
Comment	SunOrcal - Xchecked via VT: 799139b5278dc2ac24279cc6c3db44f4ef0ea78ee7b721b0ace38fd8018c51ac
Type	link
Value	https://www.virustotal.com/file/799139b5278dc2ac24279cc6c3db44f4ef0ea78ee7b721b0ace38fd8018c51ac/analysis/1510574343/
Tags	No tags

Attribute #48

UUID	5a0ed8bb-b6ec-4b31-8078-4c9b02de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 1813f10bcf74beb582c824c64fff63cb150d178bef93af81d875ca84214307a1
Type	sha1
Value	03bc4181fb54af3151cab60406a01a44158e5277
Tags	No tags

Attribute #49

UUID	5a0ed8bb-67e0-45e3-86d3-4a9d02de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 1813f10bcf74beb582c824c64fff63cb150d178bef93af81d875ca84214307a1
Type	md5
Value	17587683361d8458aebd9b8fdd07137a
Tags	No tags

Attribute #50

UUID	5a0ed8bb-cfec-48d4-9919-49ab02de0b81
Category	External analysis
Comment	Reaver.v3 - Xchecked via VT: 1813f10bcf74beb582c824c64fff63cb150d178bef93af81d875ca84214307a1
Type	link
Value	https://www.virustotal.com/file/1813f10bcf74beb582c824c64fff63cb150d178bef93af81d875ca84214307a1/analysis/1510849386/
Tags	No tags

Attribute #51

UUID	5a0ed8bb-cb84-4739-a17e-456b02de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: c906250e0a4c457663e37119ebe1efa1e4b97eef1d975f383ac3243f9f09908c
Type	sha1
Value	b31160953ff19e6abf12fc8319420ab2e1c88e77
Tags	No tags

Attribute #52

UUID	5a0ed8bb-8bd8-4a20-a99e-498b02de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: c906250e0a4c457663e37119ebe1efa1e4b97eef1d975f383ac3243f9f09908c
Type	md5
Value	2d563bf83bddca1f24e8a0ffb951a7e9
Tags	No tags

Attribute #53

UUID	5a0ed8bb-c264-45c1-acf8-4ece02de0b81
Category	External analysis
Comment	Reaver.v3 - Xchecked via VT: c906250e0a4c457663e37119ebe1efa1e4b97eef1d975f383ac3243f9f09908c
Type	link
Value	https://www.virustotal.com/file/c906250e0a4c457663e37119ebe1efa1e4b97eef1d975f383ac3243f9f09908c/analysis/1510574300/
Tags	No tags

Attribute #54

UUID	5a0ed8bb-bc04-47cf-8f7b-49cb02de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 1fcda755e8fa23d27329e4bc0443a82e1c1e9a6c1691639db256a187365e4db1
Type	sha1
Value	172b4578cb50985b08c227360d9c9df2cf32117a
Tags	No tags

Attribute #55

UUID	5a0ed8bb-9340-4443-b23e-4e1902de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 1fcda755e8fa23d27329e4bc0443a82e1c1e9a6c1691639db256a187365e4db1
Type	md5
Value	aab319d9715d38a37a10d82e87478dfc
Tags	No tags

Attribute #56

UUID	5a0ed8bb-b9c8-43aa-8797-462302de0b81
Category	External analysis
Comment	Reaver.v3 - Xchecked via VT: 1fcda755e8fa23d27329e4bc0443a82e1c1e9a6c1691639db256a187365e4db1
Type	link
Value	https://www.virustotal.com/file/1fcda755e8fa23d27329e4bc0443a82e1c1e9a6c1691639db256a187365e4db1/analysis/1510574331/
Tags	No tags

Attribute #57

UUID	5a0ed8bb-8a68-4f7a-adcb-46c302de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: ae9f158e4886cfdbfb4f1b3b25707d05f6fd873d0be9d8e7334a2c28741228ee
Type	sha1
Value	d62f1f039d0be1d7b2a8ed122d97ee917dbc9ce8
Tags	No tags

Attribute #58

UUID	5a0ed8bb-dcf8-4fe9-bdee-484502de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: ae9f158e4886cfdbfb4f1b3b25707d05f6fd873d0be9d8e7334a2c28741228ee
Type	md5
Value	892350b2a44efd9fa1e7c88aec013818

Tags	No tags
------	---------

Attribute #59

UUID	5a0ed8bb-23d8-4bbe-b367-4fae02de0b81
Category	External analysis
Comment	Reaver.v3 - Xchecked via VT: ae9f158e4886cfdbfb4f1b3b25707d05f6fd873d0be9d8e7334a2c28741228ee
Type	link
Value	https://www.virustotal.com/file/ae9f158e4886cfdbfb4f1b3b25707d05f6fd873d0be9d8e7334a2c28741228ee/analysis/1510574327/
Tags	No tags

Attribute #60

UUID	5a0ed8bb-d850-43f6-aa30-4f5702de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 9213f70bce491991c4cbbbd7dc3e67d3a3d535b965d7064973b35c50f265e59b
Type	sha1
Value	e96be5b542d100913a5bca0f02fb094d6f3ad85b
Tags	No tags

Attribute #61

UUID	5a0ed8bb-3ae4-4f3e-b592-474002de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 9213f70bce491991c4cbbbd7dc3e67d3a3d535b965d7064973b35c50f265e59b
Type	md5
Value	dd7edadd019bc120978a4dad284fbae6
Tags	No tags

Attribute #62

UUID	5a0ed8bb-c9a4-4669-a3ba-47e002de0b81
Category	External analysis
Comment	Reaver.v3 - Xchecked via VT: 9213f70bce491991c4cbbbd7dc3e67d3a3d535b965d7064973b35c50f265e59b
Type	link
Value	https://www.virustotal.com/file/9213f70bce491991c4cbbbd7dc3e67d3a3d535b965d7064973b35c50f265e59b/analysis/1510574335/
Tags	No tags

Attribute #63

UUID	5a0ed8bb-e764-4ad4-8cdb-438902de0b81
Category	Payload delivery

Comment	Reaver.v3 - Xchecked via VT: c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d
Type	sha1
Value	cbde40a234bff8870f8746eca969c364da7f4aec
Tags	No tags

Attribute #64

UUID	5a0ed8bb-02e0-4eb5-9e34-41e602de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d
Type	md5
Value	ae185e9c43bb1498a3c653a0886896e3
Tags	No tags

Attribute #65

UUID	5a0ed8bb-586c-4a4d-aa3b-4f7c02de0b81
Category	External analysis
Comment	Reaver.v3 - Xchecked via VT: c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d
Type	link
Value	https://www.virustotal.com/file/c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d/analysis/1510921773/
Tags	No tags

Attribute #66

UUID	5a0ed8bc-ba8c-4160-8374-4dba02de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 18ac3b14300ecfeed4b64a844c16dccb06b0e3513d0954d6c6182f2ea14e4c92
Type	sha1
Value	5c6b231111239c0625dc9ff4359d1b8553159ecc
Tags	No tags

Attribute #67

UUID	5a0ed8bc-eff4-4d36-947a-424c02de0b81
Category	Payload delivery
Comment	Reaver.v3 - Xchecked via VT: 18ac3b14300ecfeed4b64a844c16dccb06b0e3513d0954d6c6182f2ea14e4c92
Type	md5
Value	c629f8f3206e5a6de83b4c996a2bacfb
Tags	No tags

Attribute #68

UUID	5a0ed8bc-60d8-4f2e-aa79-4d6f02de0b81
Category	External analysis
Comment	Reaver.v3 - Xchecked via VT: 18ac3b14300ecfeed4b64a844c16dcc0b0e3513d0954d6c6182f2ea14e4c92
Type	link
Value	https://www.virustotal.com/file/18ac3b14300ecfeed4b64a844c16dcc0b0e3513d0954d6c6182f2ea14e4c92/analysis/1510610402/
Tags	No tags

Attribute #69

UUID	5a0ed8bc-0124-4bd3-9049-4e6b02de0b81
Category	Payload delivery
Comment	Reaver.v2 - Xchecked via VT: 98eb5465c6330b9b49df2e7c9ad0b1164aa5b35423d9e80495a178eb510cdc1c
Type	sha1
Value	c05d15fc94d096a821f2c689a29dff7679ce087a
Tags	No tags

Attribute #70

UUID	5a0ed8bc-c04c-49c4-9d39-464802de0b81
Category	Payload delivery
Comment	Reaver.v2 - Xchecked via VT: 98eb5465c6330b9b49df2e7c9ad0b1164aa5b35423d9e80495a178eb510cdc1c
Type	md5
Value	dadf3d3dd411bc02d7c05ee3a18259ea
Tags	No tags

Attribute #71

UUID	5a0ed8bc-37cc-47c1-bdcd-454e02de0b81
Category	External analysis
Comment	Reaver.v2 - Xchecked via VT: 98eb5465c6330b9b49df2e7c9ad0b1164aa5b35423d9e80495a178eb510cdc1c
Type	link
Value	https://www.virustotal.com/file/98eb5465c6330b9b49df2e7c9ad0b1164aa5b35423d9e80495a178eb510cdc1c/analysis/1510823791/
Tags	No tags

Attribute #72

UUID	5a0ed8bc-4014-447e-8efc-450702de0b81
Category	Payload delivery
Comment	Reaver.v1 - Xchecked via VT: d560f44188fb56d3abb11d9508e1167329470de19b811163eb1167534722e666
Type	sha1
Value	0cea48067ddbc9227363168013142f6f3a5dea9f
Tags	No tags

Attribute #73

UUID	5a0ed8bc-5768-4c26-85a2-47b902de0b81
Category	Payload delivery
Comment	Reaver.v1 - Xchecked via VT: d560f44188fb56d3abb11d9508e1167329470de19b811163eb1167534722e666
Type	md5
Value	9f289cce6f95949450e3f4c96a187f5d
Tags	No tags

Attribute #74

UUID	5a0ed8bc-a7a0-499f-bd08-48bb02de0b81
Category	External analysis
Comment	Reaver.v1 - Xchecked via VT: d560f44188fb56d3abb11d9508e1167329470de19b811163eb1167534722e666
Type	link
Value	https://www.virustotal.com/file/d560f44188fb56d3abb11d9508e1167329470de19b811163eb1167534722e666/analysis/1510823685/
Tags	No tags