Israeli IRS themed ransomware attack

General information

UUID	5d8129c9-8fb8-4aff-8cfa-72b60a000082
2019-09-17	Date
Owner org	No value specified.
Threat level	No threat level specified.
Analysis	Initial (0)
Info	Israeli IRS themed ransomware attack
Event date	2019-09-17 21:05:13
Published	No
Creator Org	Profero
# Attributes	15
Tags	Ransomware tlp:white misp-galaxy:mitre-attack-pattern="Spearphishing Link - T1192" misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1059" misp-galaxy:mitre-attack-pattern="Execution through API - T1106" misp-galaxy:mitre-attack-pattern="Windows Management Instrumentation - T1047" misp-galaxy:mitre-attack-pattern="Hidden Files and Directories - T1158" misp-galaxy:mitre-attack-pattern="New Service - T1050" misp-galaxy:mitre-attack-pattern="Registry Run Keys / Startup Folder - T1060" misp-galaxy:mitre-attack-pattern="File Deletion - T1107" misp-galaxy:mitre-attack-pattern="Modify Registry - T1112" misp-galaxy:mitre-attack-pattern="Query Registry - T1012"

Attributes

Attribute #1

UUID	5d812ad9-bde4-4b00-abdb-73a30a000082
Category	External analysis
Type	link
Value	https://www.eset.co.il/eset-blog/law-enforcement-and-collection-ransomware

Attribute #2

UUID	5d812b20-4b60-4db0-950c-7c3f0a000082
Category	External analysis
Type	link
Value	https://app.any.run/tasks/ca6e6576-07a4-4ebc-b5b4-b59b39d4d8e7/

Attribute #3

UUID	5d812b3f-2674-448d-b427-7c320a000082
Category	External analysis
Type	link
Value	https://www.virustotal.com/gui/file/71327d7ca505fe4fae8fb285b634c9150c3a3253188879fcea2e3bf68196a766/detection?fbclid=IwAR3OFOe0O7zOiAnft8leT_XetK4AdnTYyjxpkNOGIl9TqYpyzhECAf-MtCk

Attribute #4

UUID	5d812b97-a230-4439-81f5-7c320a000082
Category	Payload delivery
Type	sha256
Value	71327d7ca505fe4fae8fb285b634c9150c3a3253188879fcea2e3bf68196a766

Attribute #5

UUID	5d812bc7-40d4-4591-b7d9-72b60a000082
Category	Network activity
Type	domain
Value	aurmus.is

Attribute #6

UUID	5d812bf5-7774-46a6-b31d-7c330a000082
Category	Other
Type	comment
Value	Ransom emails: BhatMaker@protonmail.com,BhatMaker@tutanota.com

Attribute #7

UUID	5d812c12-e870-4a6a-a2d9-72b40a000082
Category	Network activity
Type	url
Value	http://iplogger.ru/1OnzW.jpg

Attribute #8

UUID	5d812c69-472c-4163-8244-72b50a000082
Category	Artifacts dropped
Type	sha256
Value	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7

Attribute #9

UUID	5d812c80-e2b4-4df4-bc9f-73a30a000082
Category	External analysis
Type	link
Value	https://analyze.intezer.com/#/files/029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7

Attribute #10

UUID	5d814a57-5440-4252-8ff9-01911c6c3325
Category	Network activity
Comment	aurmus.is: Enriched via the dns module

Type	ip-src
Value	82.221.136.4

Attribute #11

UUID	567aabdf-607c-4015-87eb-e500c5c4e9f3
Category	Payload delivery
Comment	aurmus.is: Enriched via the virustotal_public module
Type	sha256
Value	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7

Attribute #12

UUID	4a2dcaa7-4ca9-42cb-a788-ee40190590af
Category	Network activity
Comment	aurmus.is: Enriched via the virustotal_public module
Type	domain
Value	www.aurmus.is

Attribute #13

UUID	481e5349-796f-47f0-bca1-032d6fa0a9e8
Category	Network activity
Comment	aurmus.is: Enriched via the virustotal_public module
Type	domain
Value	mail.aurmus.is

Attribute #14

UUID	efa50fef-5147-4c29-bf0c-66f75689979a
Category	Network activity
Comment	aurmus.is: Enriched via the virustotal_public module
Type	domain
Value	divineyoniverse.aurmus.is

Attribute #15

UUID	7f8e6111-799b-4610-a5a9-57cb0a1ce4bb
Category	Network activity
Comment	aurmus.is: Enriched via the virustotal_public module
Type	url
Value	https://aurmus.is/wp-includes/css/BjdZ7xa.exe

Objects

Object #1

UUID	b843aea8-74f6-467c-b239-edea7e38617f
Description	File object describing a file with meta-information
Meta Category	file
Object Name	file
Comment	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7: Enriched via the virustotal_public module
Object date	2019-09-17 21:03:42

Attribute #1

UUID	1e45b03a-2e1c-42bc-8445-5cdad0551608
Category	Payload delivery
Comment	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7: Enriched via the virustotal_public module
Type	md5
Value	1b9a1b9afbba387ea8193e9b056488c5

Attribute #2

UUID	9b161e69-4c16-4ce9-a7e4-2d651ca41ca4
Category	Payload delivery
Comment	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7: Enriched via the virustotal_public module
Type	sha1
Value	fd838fd7bb131093c6910f771aa7020a07e10b25

Attribute #3

UUID	f2a202c3-0607-4249-9ec7-a0be2b2a2b52
Category	Payload delivery
Comment	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7: Enriched via the virustotal_public module
Type	sha256
Value	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7

Object #2

UUID	241cc6ed-d0d7-4aca-926c-72b8673d3520
Description	VirusTotal report
Meta Category	misc
Object Name	virustotal-report
Comment	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7: Enriched via the virustotal_public module
Object date	2019-09-17 21:03:42

Attribute #1

UUID	d71ba20e-eb12-4f8a-b1f2-b883c33717da
Category	External analysis
Comment	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7: Enriched via the virustotal_public module
Type	link
Value	https://www.virustotal.com/file/029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7/analysis/1568697601/

Attribute #2

UUID	a924fa19-2ada-4ee6-a2fb-b64d6628b141
Category	Other
Comment	029678e8e36b7d51328953d67326b2e0e8adb8c9dcd3d8975006e5a9500ba9a7: Enriched via the virustotal_public module
Type	text
Value	45/69

Object #3

UUID	cd51c480-f30d-4ff7-bdbd-6a874353f809
Description	Whois records information for a domain name or an IP address.
Meta Category	network
Object Name	whois
Comment	aurmus.is: Enriched via the virustotal_public module
Object date	2019-09-17 21:05:13

Attribute #1

UUID	8097ed47-2017-446f-afa9-6b0a06c8a69c
Category	Other
Comment	aurmus.is: Enriched via the virustotal_public module
Type	text
Value	created: August 27 2019 created: March 17 2016 dnssec: unsigned delegation domain: aurmus.is e-mail: c215fc66323f439as@orangewebsite.com expires: August 27 2020 nic-hdl: IL65-IS nserver: ns3.orangewebsite.com nserver: ns4.orangewebsite.com registrant: 9d307828061771ff source: ISNIC

Object #4

UUID	cec043d3-6939-46d8-8587-bcfec9a3cc2b
Description	A domain and IP address seen as a tuple in a specific time frame.
Meta Category	network
Object Name	domain-ip
Comment	aurmus.is: Enriched via the virustotal_public module
Object date	2019-09-17 21:05:13

Attribute #1

UUID	8e0c30ea-fd9c-45ef-aac8-32808a6bc40c
Category	Network activity
Comment	aurmus.is: Enriched via the virustotal_public module
Type	domain
Value	aurmus.is

Attribute #2

UUID	2f9bb025-6ead-4dfa-84fa-a6fb1b5ce434
Category	Network activity
Comment	aurmus.is: Enriched via the virustotal_public module
Type	ip-dst
Value	82.221.136.4