MALICIOUS

Classifications: Ransomware

Threat Names: CryptoLocker, Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**asih.exe**
ID	#10131893
MD5	a72290c3104f2ee952a5569326033580
SHA1	850484454395d8532f25aa70968928865755e253
SHA256	e03dd9097827ae4c99b9b21778b7df9bfb123c0f5986debc39fa04bd3a3d98ff
File Size	47.54 KB
Report Created	2024-03-29 07:50 (UTC+1)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (8 rules, 17 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	8	Ransomware
	• YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in memory dump data from (process #1) asih.exe. • YARA detected "CryptoLocker_set1" from ruleset "Ransomware" in memory dump data from (process #1) asih.exe. • YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in memory dump data from (process #2) asih.exe. • YARA detected "CryptoLocker_set1" from ruleset "Ransomware" in memory dump data from (process #2) asih.exe. • YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in process image data from (process #1) asih.exe. • YARA detected "CryptoLocker_set1" from ruleset "Ransomware" in process image data from (process #1) asih.exe. • YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in the sample file C:\Users\RDhJ0CNFevzX\Desktop\asih.exe. • YARA detected "CryptoLocker_set1" from ruleset "Ransomware" in the sample file C:\Users\RDhJ0CNFevzX\Desktop\asih.exe.		
4/5	Reputation	Malicious file detected via reputation	1	-
	• The sample itself is a known malicious file.			
4/5	Reputation	Malicious host or URL detected via reputation	2	-
	• Reputation analysis labels the URL "hxxps://emrlogistics[.]com/fr/to2.exe" which was contacted by (process #2) asih.exe as Mal/HTMLGen-A. • Reputation analysis labels the resolved domain "emrlogistics.com" as Mal/HTMLGen-A.			
2/5	Network Connection	Allows invalid SSL certificates	1	-
	• (Process #2) asih.exe allows network connections with an invalid SSL certificate.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) asih.exe starts (process #2) asih.exe with a hidden window.			
1/5	Obfuscation	Resolves API functions dynamically	2	-
	• (Process #1) asih.exe resolves 25 API functions by name. • (Process #2) asih.exe resolves 25 API functions by name.			
1/5	Execution	Drops PE file	1	-
	• (Process #1) asih.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe".			

Mitre ATT&CK Matrix

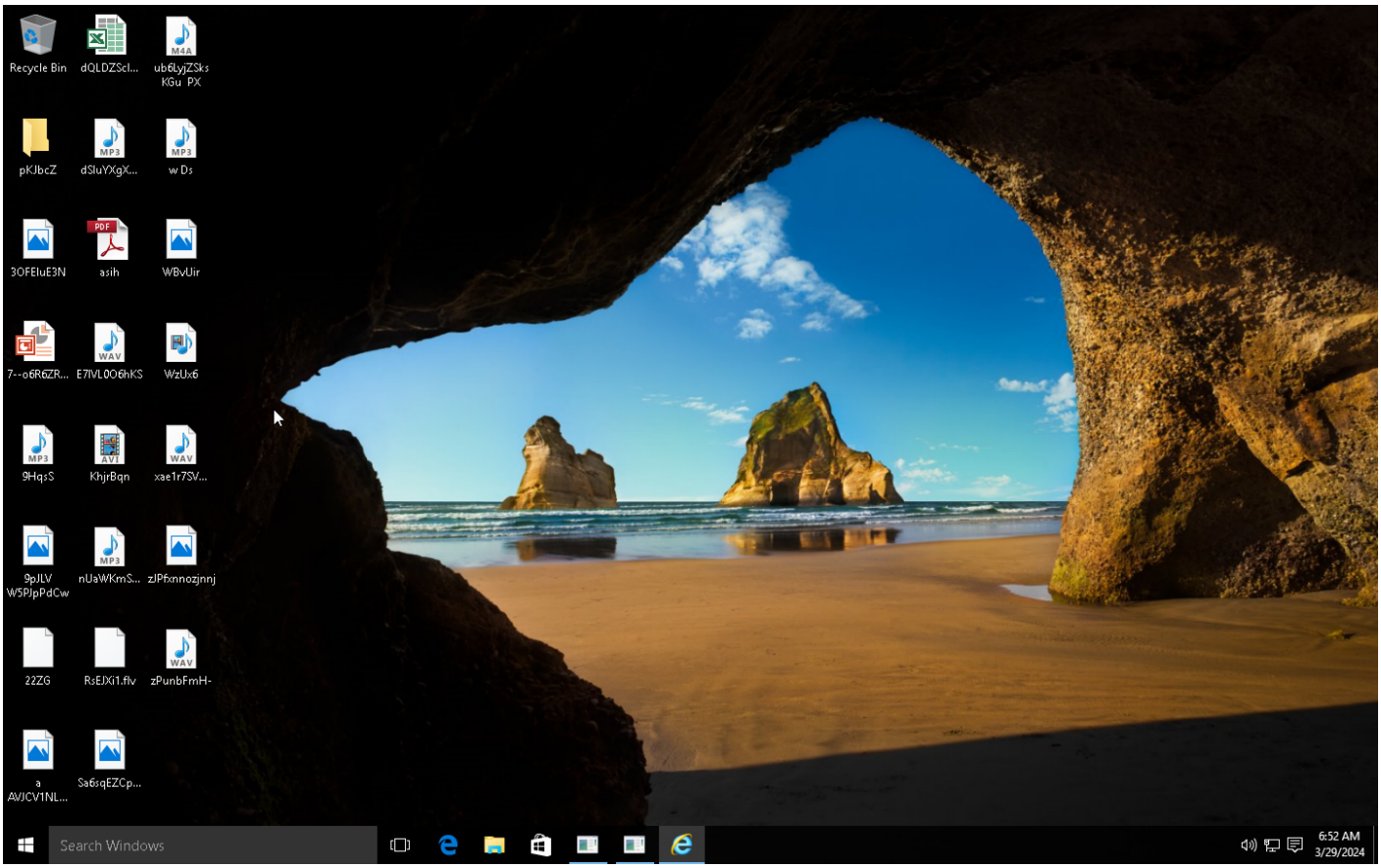
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window							
				#T1045 Software Packing							

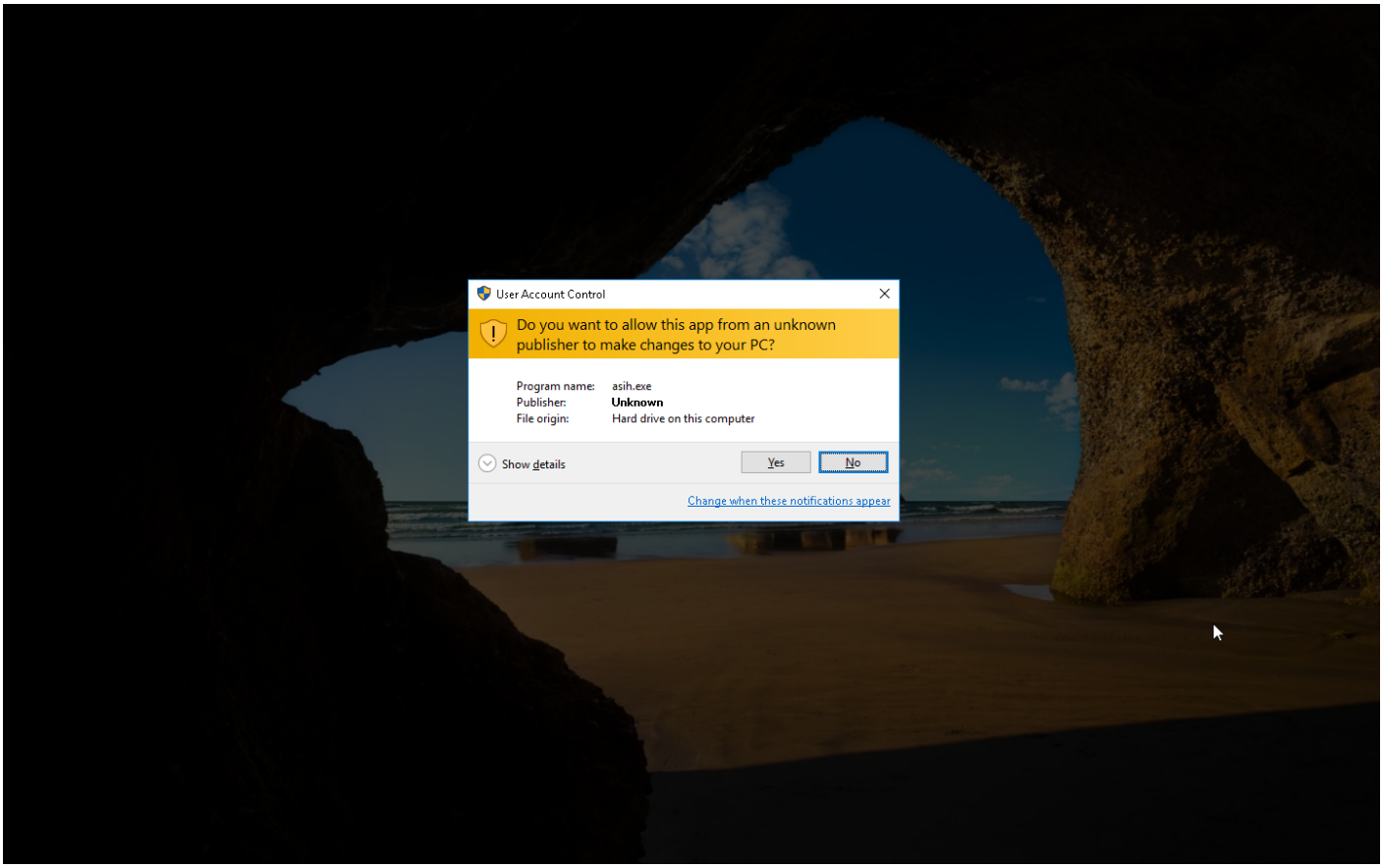
Sample Information

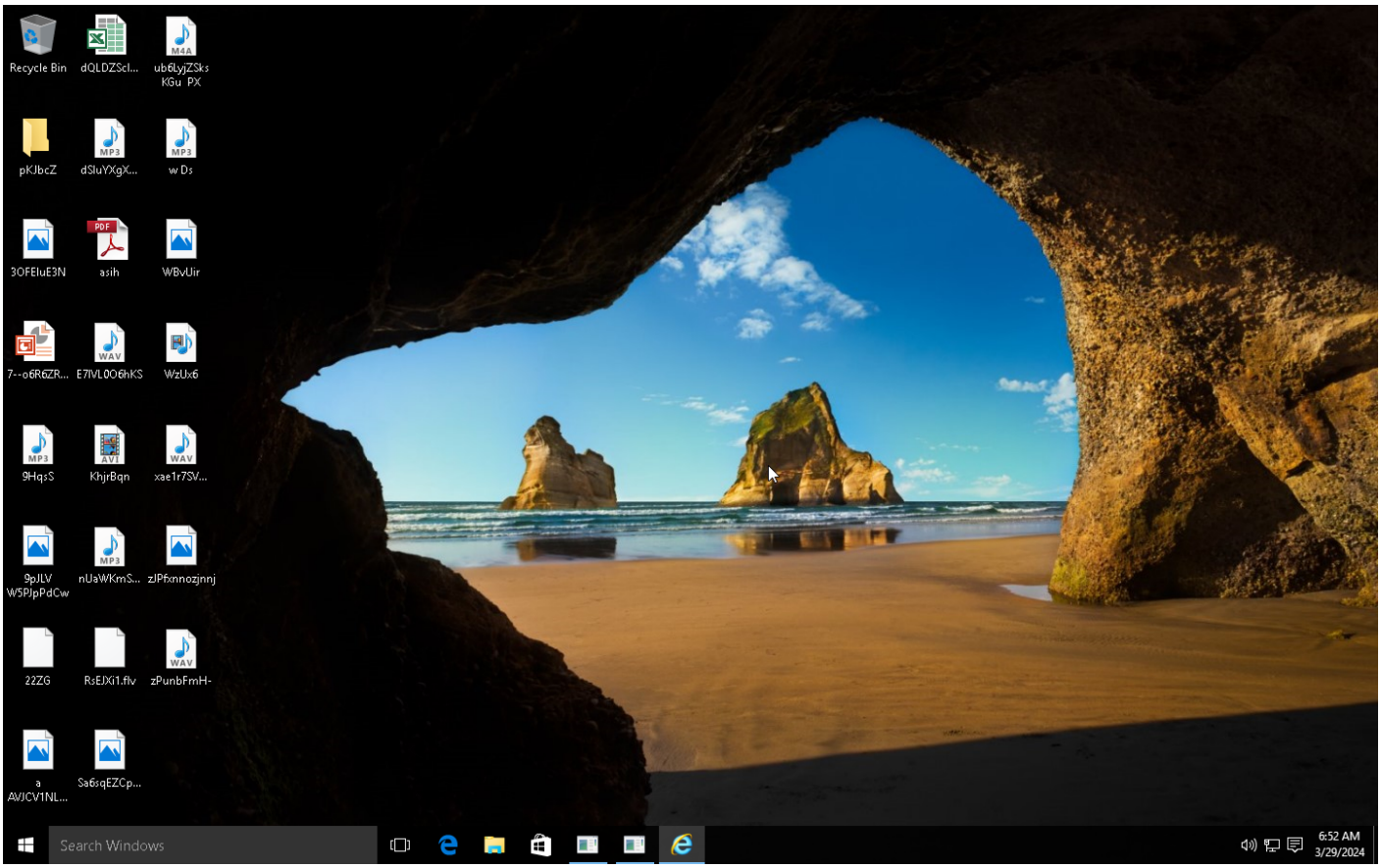
ID	#10131893
MD5	a72290c3104f2ee952a5569326033580
SHA1	850484454395d8532f25aa70968928865755e253
SHA256	e03dd9097827ae4c99b9b21778b7df9bfb123c0f5986debc39fa04bd3a3d98ff
SSDeep	768:X6LsoEEeegiZPvEhHSG+gp/BtOOtEvwDpjBVaD3E09vdXe:X6QFElP6n+gJBMOtEvwDpjBtEdXe
ImpHash	7ba3aa8366ce167c7a77ebd6e6fea8e5
File Name	asih.exe
File Size	47.54 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-03-29 07:50 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✖
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	16


Recycle Bin
dQLDZScl...
ub6LyjZSks KGu PX
pKJbcZ
dSluYXgX...
w Ds
3OFEIuE3N
asih
WBvUir
7--o6R6ZR...
E7lVL0O6hKS
WzUx6
9HqsS
KhjrBqn
xae1r7SV...
9pJLV W5PJpPdCw
nUaWKmS...
zJPfxnnozjnnj
22ZG
RsEJXi1.flv
zPunbFmH-
a AVJCV1NL...
Sa6sqEZCp...
Search Windows
6:52 AM
3/29/2024


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: asih.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
dQLDZScl...
ub6LyjZSks
KGu PX
pKJbcZ
dSluYXgX...
w Ds
3OFEluE3N
asih
WBvUir
7--o6R6ZR...
E7lVL0O6hKS
WzUx6
9HqsS
KhjrBqn
xae1r7SV...
9pJLV
W5PJpPdCw
nUaWKmS...
zJPfxnnozjnnj
22ZG
RsEJXi1.flv
zPunbFmH-
a
AVJCV1NL...
Sa6sqEZCp...
Search Windows
6:52 AM
3/29/2024

NETWORK

General

2.02 KB total sent

780 bytes total received

2 ports 443, 53

3 contacted IP addresses

1 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

4 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

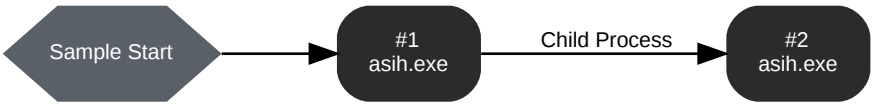
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://emrlogistics[.]com/fr/to2.exe	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	emrlogistics[.]com, traff-4[.]hugedomains[.]com, hdr-nlb8-39c51fa8696874ee[.]elb[.]us-east-1[.]amazonaws[.]com	NO_ERROR	52.86.6.113, 3.94.41.167	traff-4[.]hugedomains[.]com, hdr-nlb8-39c51fa8696874ee[.]elb[.]us-east-1[.]amazonaws[.]com	MALICIOUS

BEHAVIOR

Process Graph



Process #1: asih.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\asih.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\asih.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 120906, Reason: Analysis Target
Unmonitor End Time	End Time: 128840, Reason: Terminated
Monitor duration	7.93s
Return Code	0
PID	4892
Parent PID	-
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe	47.61 KB	68988f23aeab59ac0611042f0651b681e5e4f3d3687d76dab86b1b5be7fd204f	✔

Host Behavior

Type	Count
Module	33
Window	4
File	6
Process	1

Process #2: asih.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\asih.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 126382, Reason: Child Process
Unmonitor End Time	End Time: 360928, Reason: Terminated by timeout
Monitor duration	234.55s
Return Code	Unknown
PID	5084
Parent PID	4892
Bitness	32 Bit

Host Behavior

Type	Count
Module	33
Window	4
File	253

Network Behavior

Type	Count
HTTPS	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e03dd9097827ae4c99b9b21778b7df9bfb123c0f5986debc39fa04bd3a3d98ff	C:\Users\RDhJ0CNFevzX\Desktop\asih.exe	Sample File	47.54 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
68988f23aeab59ac0611042f0651b681e5e4f3d3687d76dab86b1b5be7fd204f	C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe	Dropped File	47.61 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
bf2b3b93882d67b0758c5ce5fea2889b7f2290341f7bb9bd2499f6ef2e6c488e	-	Memory Dump	40.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
024b7092970f12c1e130918dc3a6877789b051fb9878c23cfd96b5e63660d660	-	Memory Dump	1408.00 KB	application/octet-stream	-	MALICIOUS
1dafb02b2ad1ab6f183bd596708fc24f7140412ba7817ec7b8f382052cb50d75	-	Memory Dump	40.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
6a12afa224374ba5dbb7f9483224a33edb8cd3d37bdb47e0c51f1055dd52010c	-	Memory Dump	40.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
06fe79b5dc0fb8876cd1b7ada129f29291042a5a1ddde84bd398a09ccce5cc77	-	Memory Dump	47.71 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8c0338b2a201160eaacabff51abc94b95075db5bbd7e92cf131006fb295d2009	-	Memory Dump	40.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\asih.exe	Accessed File, Sample File	Access, Read	MALICIOUS
C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
last.inf	Accessed File	Access	CLEAN
C:\DOCUME~1\SUPERV~1\LOCALS~1\Temp\Temporary Directory 1 for Invoice_OCT-02-2013.zip\Invoice_OCT-02-2013.exe	Accessed File	Access, Delete	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://emrlogistics[.]com/fr/to2.exe	Extracted	52.86.6.113, 3.94.41.167	United States	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
emrlogistics[.]com	52.86.6.113, 3.94.41.167	United States	DNS, TCP	MALICIOUS
traff-4[.]hugedomains[.]com	52.86.6.113, 3.94.41.167	United States	DNS, TCP	CLEAN
hdr-nlb8-39c51fa8696874ee[.]elb[.]us-east-1[.]amazonaws[.]com	52.86.6.113, 3.94.41.167	United States	DNS, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
52.86.6.113	hdr-nlb8-39c51fa8696874ee[.]elb[.]us-east-1[.]amazonaws[.]com, emrlogistics[.]com, traff-4[.]hugedomains[.]com	United States	DNS, TCP	CLEAN
3.94.41.167	hdr-nlb8-39c51fa8696874ee[.]elb[.]us-east-1[.]amazonaws[.]com, emrlogistics[.]com, traff-4[.]hugedomains[.]com	United States	DNS, TCP	CLEAN

Process

Process Name	Commandline	Verdict
asih.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe"	MALICIOUS
asih.exe	"C:\Users\RDhJ0CNFevzX\Desktop\asih.exe"	MALICIOUS

YARA / AV

YARA (16)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Dropped File	C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Dropped File	C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\asih.exe	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\asih.exe	Ransomware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.9 / 2024-03-26 09:11:11
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.5 / 2024-03-22 20:39:30
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.12 / 2024-03-28 09:41:51
YARA Built-in Ruleset Version	2024.2.1.11

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows