MALICIOUS

Classifications: Ransomware

Threat Names: CryptoLocker Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**asih.exe**
ID	#10131907
MD5	99c930a9101ee6e24b3a979e13e6358c
SHA1	5322c3fdf93409bd5d8b9faa8f6d33cf1ce980fa
SHA256	d2aebe923c85cc32a23b73751d306c46379e70a65bf4291489b29893d38a223c
File Size	46.46 KB
Report Created	2024-03-29 07:51 (UTC+1)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (8 rules, 15 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	6	Ransomware
	• 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 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. • 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 #1) 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

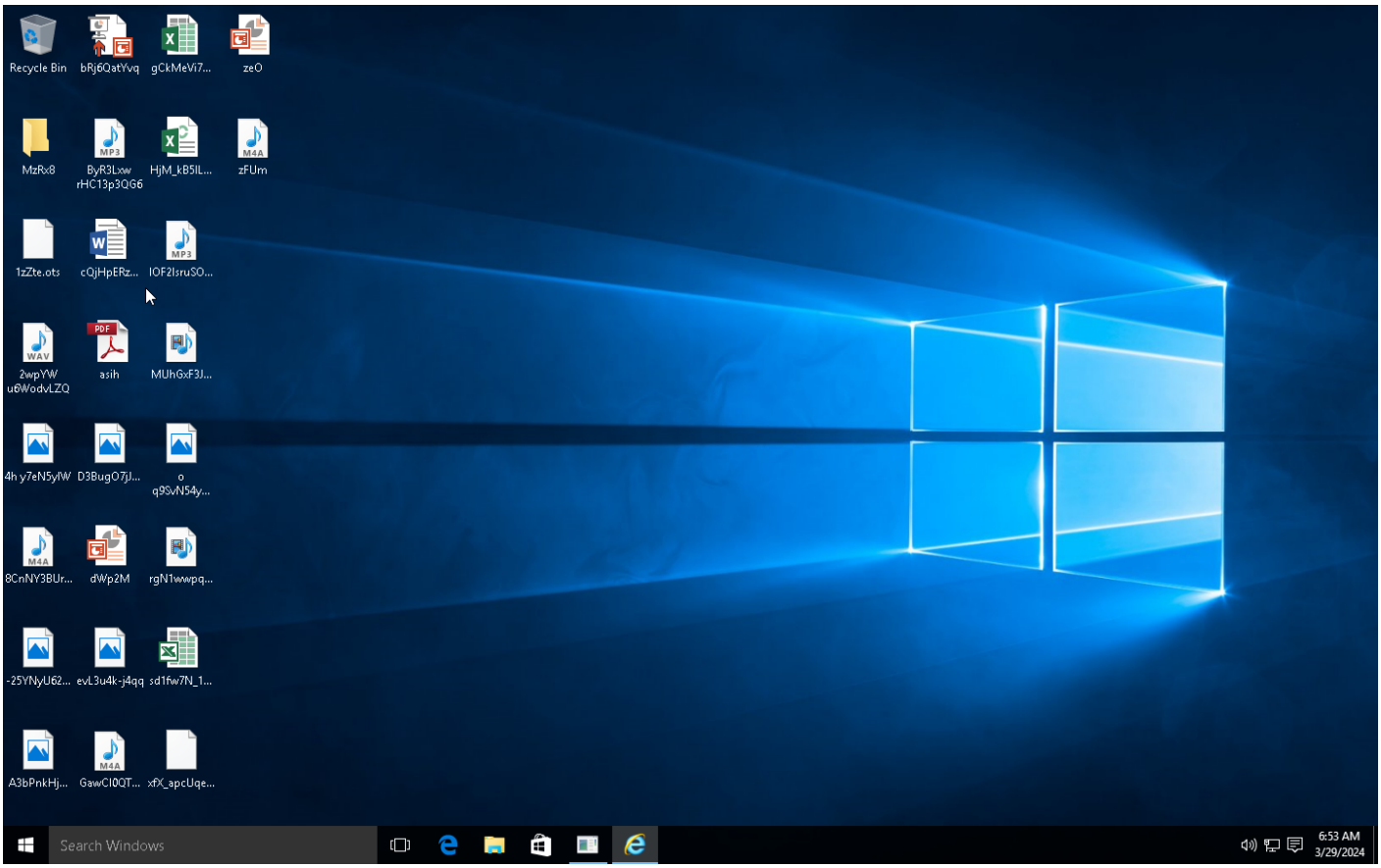
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window							
				#T1045 Software Packing							

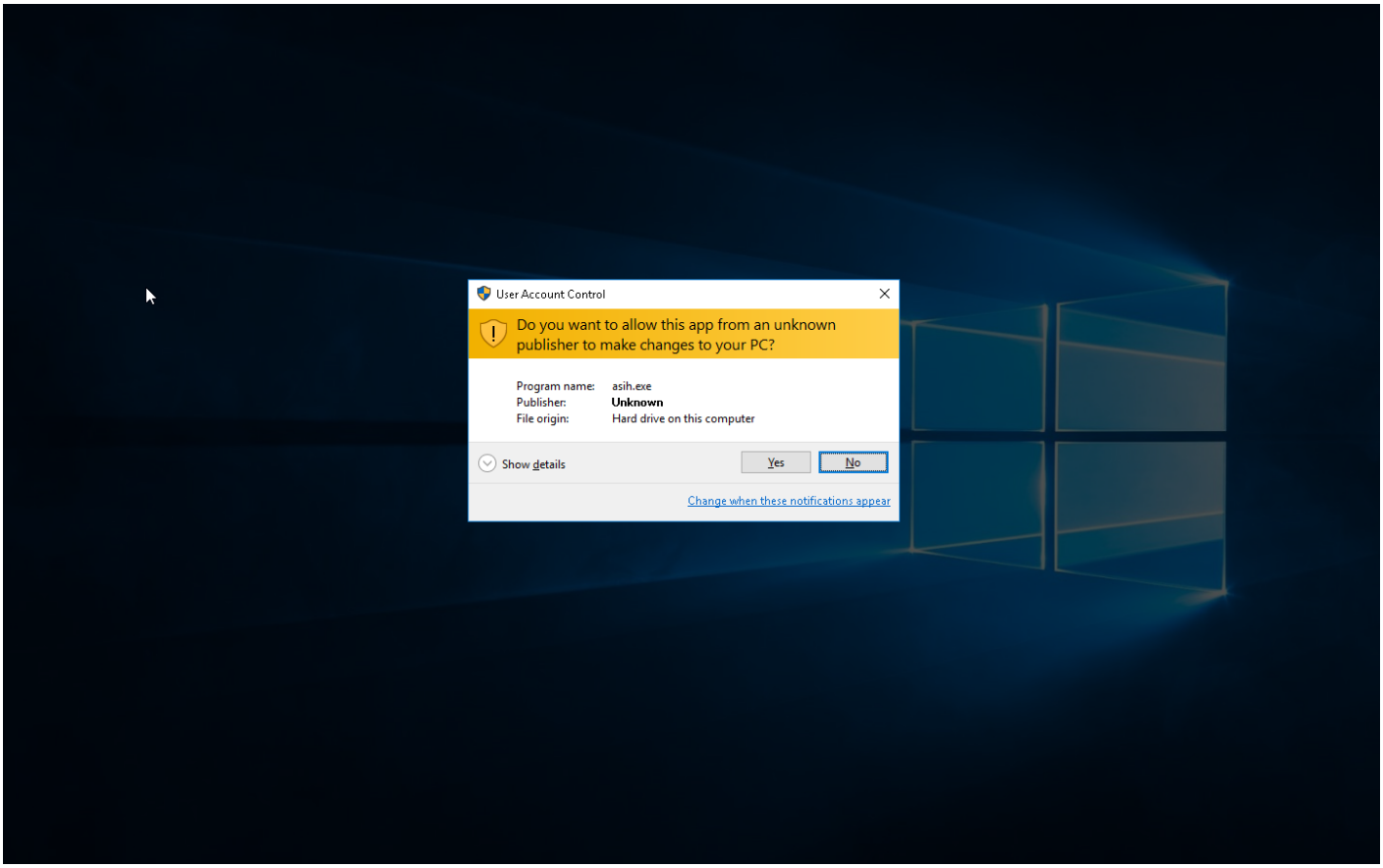
Sample Information

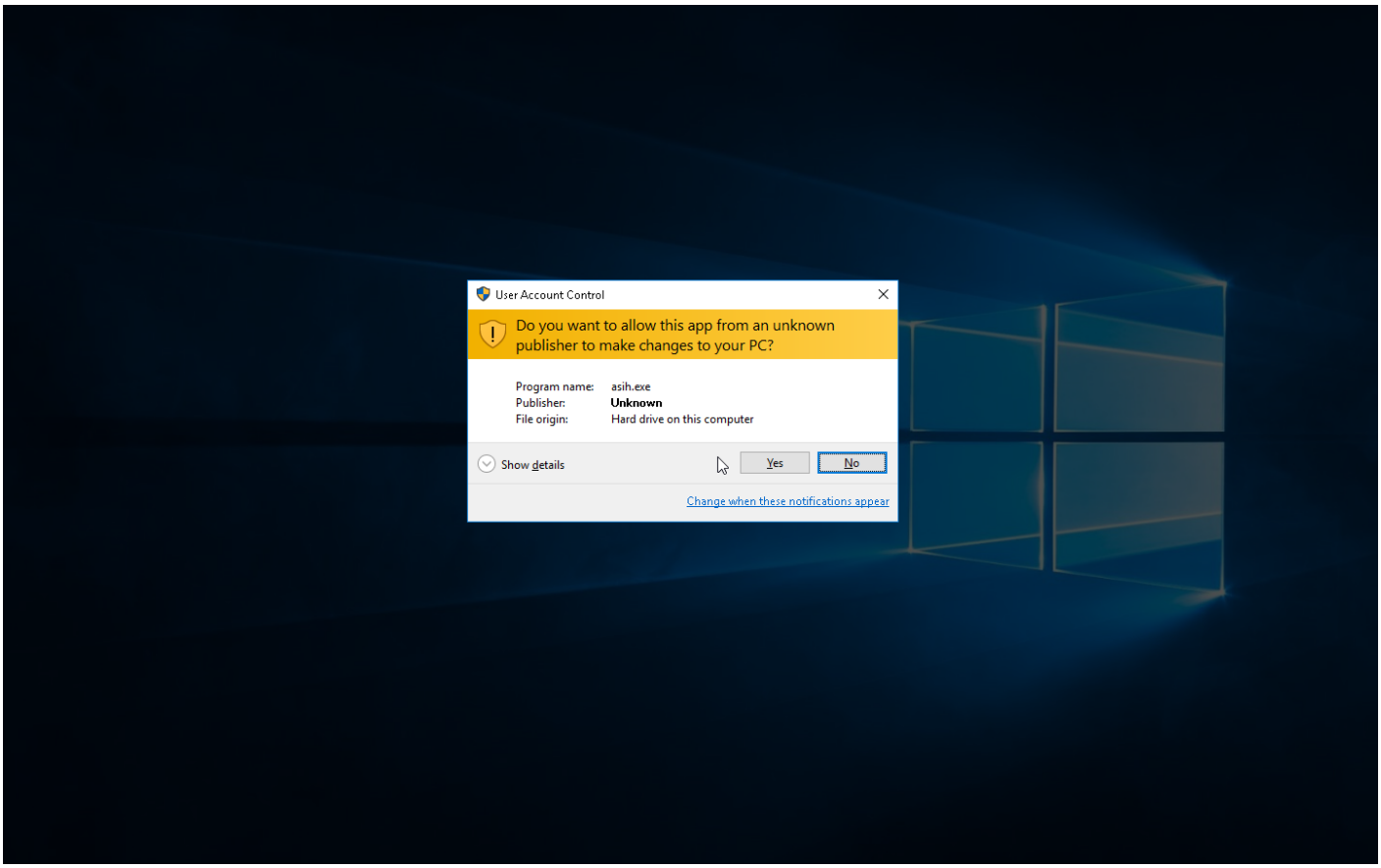
ID	#10131907
MD5	99c930a9101ee6e24b3a979e13e6358c
SHA1	5322c3fdf93409bd5d8b9faa8f6d33cf1ce980fa
SHA256	d2aebe923c85cc32a23b73751d306c46379e70a65bf4291489b29893d38a223c
SSDeep	768:wHGGaSawqnwjRQ6ESlmFOsPoOdQtOOtEvwDpjm6j4AYsqSh+DETkedmhXSV7:YGzl5wjRQBBOsP1QMOtEvwDpjl39+D+f
ImpHash	a0c275da44db88d1f2fc3943daf6948b
File Name	asih.exe
File Size	46.46 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

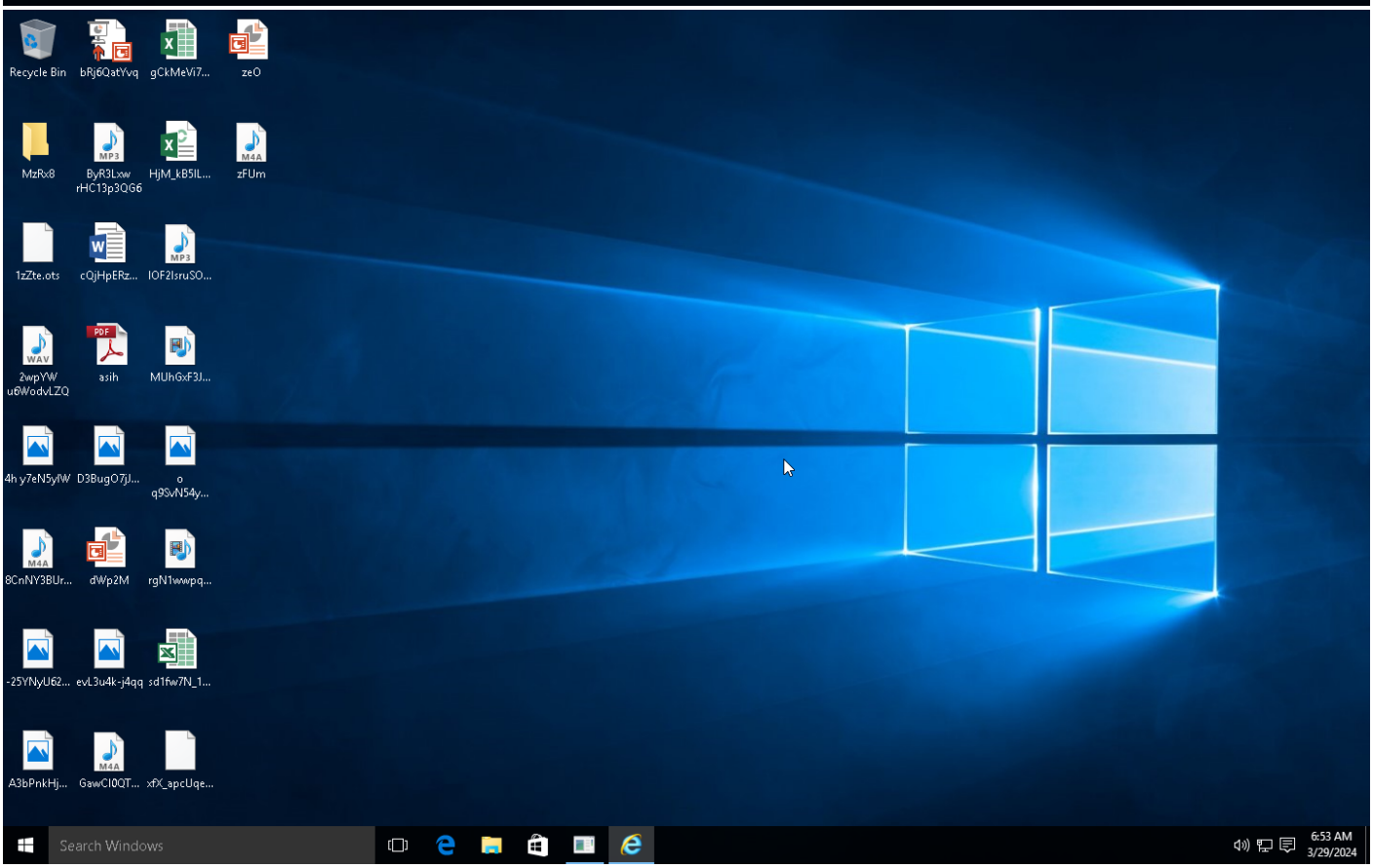
Analysis Information

Creation Time	2024-03-29 07:51 (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	14


Recycle Bin
bRj6QatYvq
gCkMeVi7...
zeO
MzRx8
ByR3Lxw rHC13p3QG6
HjM_kB5IL...
zFUm
1zZte.ots
cQjHpERz...
IOF2IsruSO...
2wpYW u6WodvLZQ
asih
MUhGxF3J...
4h y7eN5yfW
D3BugO7jI...
o q9SvN54y...
8CnNY3BUr...
dWp2M
rgN1wwpq...
-25YNyU62...
evL3u4k-j4qq
sd1fw7N_1...
A3bPnkHj...
GawCI0QT...
xfX_apcUqe...
Search Windows
6:53 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





Screenshots truncated

NETWORK

General

1.98 KB total sent

774 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

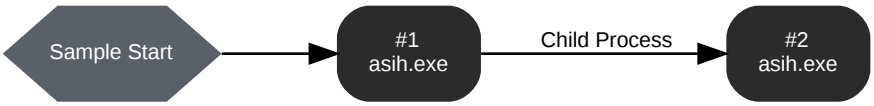
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://emrlogistics[.]com/fr/to2.exe	-	-	-	0 bytes	MALICIOUS

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	3.94.41.167, 52.86.6.113	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: 115527, Reason: Analysis Target
Unmonitor End Time	End Time: 124497, Reason: Terminated
Monitor duration	8.97s
Return Code	0
PID	4368
Parent PID	-
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe	46.54 KB	89f9d308b17f1b92fa9a0f6191b585ae525f22d19c475016de661c3bc1840079	✔

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: 121961, Reason: Child Process
Unmonitor End Time	End Time: 355580, Reason: Terminated by timeout
Monitor duration	233.62s
Return Code	Unknown
PID	4420
Parent PID	4368
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
d2aebe923c85cc32a23b73751d306c46379e70a65bf4291489b29893d38a223c	C:\Users\RDhJ0CNFevzX\Desktop\asih.exe	Sample File	46.46 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
89f9d308b17f1b92fa9a0f6191b585ae525f22d19c475016de661c3bc1840079	C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe	Dropped File	46.54 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
57084e58e61bebdeb831e0aa7bd002cdd0c3493d4c429ab7de2257beeb03de91	-	Memory Dump	44.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c2c759792c39ec0b88e41b67c8bec5c9276d7b0cdfc16060e1b983ed676019f7	-	Memory Dump	44.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a9dd5c8faf27c52ac0b3b9b96dfce68da6ad9dc4fdf6dc6dcfc686bca28096ba	-	Memory Dump	44.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
874cc90e9c1c1f8a82a36b36aaee313a1051e79494f2057deecb45d8714b5492	-	Memory Dump	46.63 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c749e9f7fea4753e57441ebd7bd33aa56042331fa0d190e941eeecde095016e8	-	Memory Dump	44.00 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:\Users\jbayuelo\AppData\Local\Temp\Rar$EX00.060\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

IP Address	Domains	Country	Protocols	Verdict
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\RDhJ0CNFevzX\Desktop\asih.exe"	MALICIOUS
asih.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\asih.exe"	MALICIOUS

YARA / AV

YARA (14)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
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_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\asih.exe	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	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_rule2	CryptoLocker ransomware	Memory Dump	-	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	Dropped File	C:\Users\RDHJ0C~1\AppData\Local\Temp\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