MALICIOUS

Classifications: Ransomware

Threat Names: CryptoLocker Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**asih.exe**
ID	#10131885
MD5	00e91fb785524907ad123537290364fb
SHA1	0691ee2aff1f1d949d6313e6f9359dd23ded08bb
SHA256	d9cd8e29f72b72c8754469641d68a179a424a1e04d99228f5d0c3897c4937b17
File Size	50.23 KB
Report Created	2024-03-29 05:49 (UTC)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (7 rules, 13 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 the sample file C:\Users\OqXZRaykm\Desktop\asih.exe. • YARA detected "CryptoLocker_set1" from ruleset "Ransomware" in the sample file C:\Users\OqXZRaykm\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. • YARA detected "CryptoLocker_set1" from ruleset "Ransomware" in memory dump data from (process #4) asih.exe. • YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in memory dump data from (process #4) asih.exe.		
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Network Connection	Allows invalid SSL certificates	1	-
	• (Process #4) 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 #4) 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 #4) asih.exe resolves 25 API functions by name.			
1/5	Execution	Drops PE file	1	-
	• (Process #1) asih.exe drops file "C:\Users\OQXZRA~1\AppData\Local\Temp\asih.exe".			
1/5	Execution	Executes dropped PE file	1	-
	• Executes dropped file "C:\Users\OQXZRA~1\AppData\Local\Temp\asih.exe".			

Mitre ATT&CK Matrix

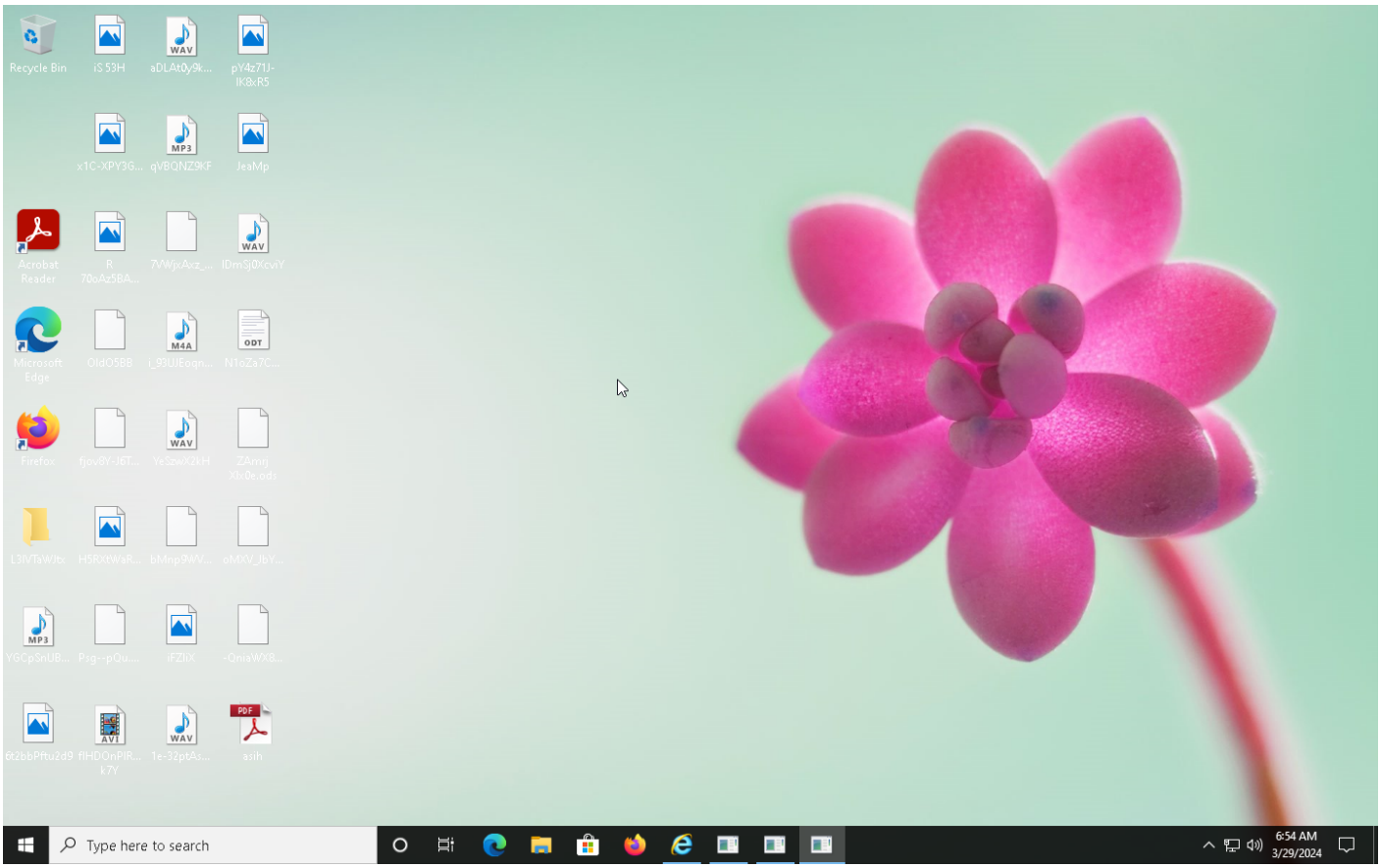
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window							
				#T1045 Software Packing							

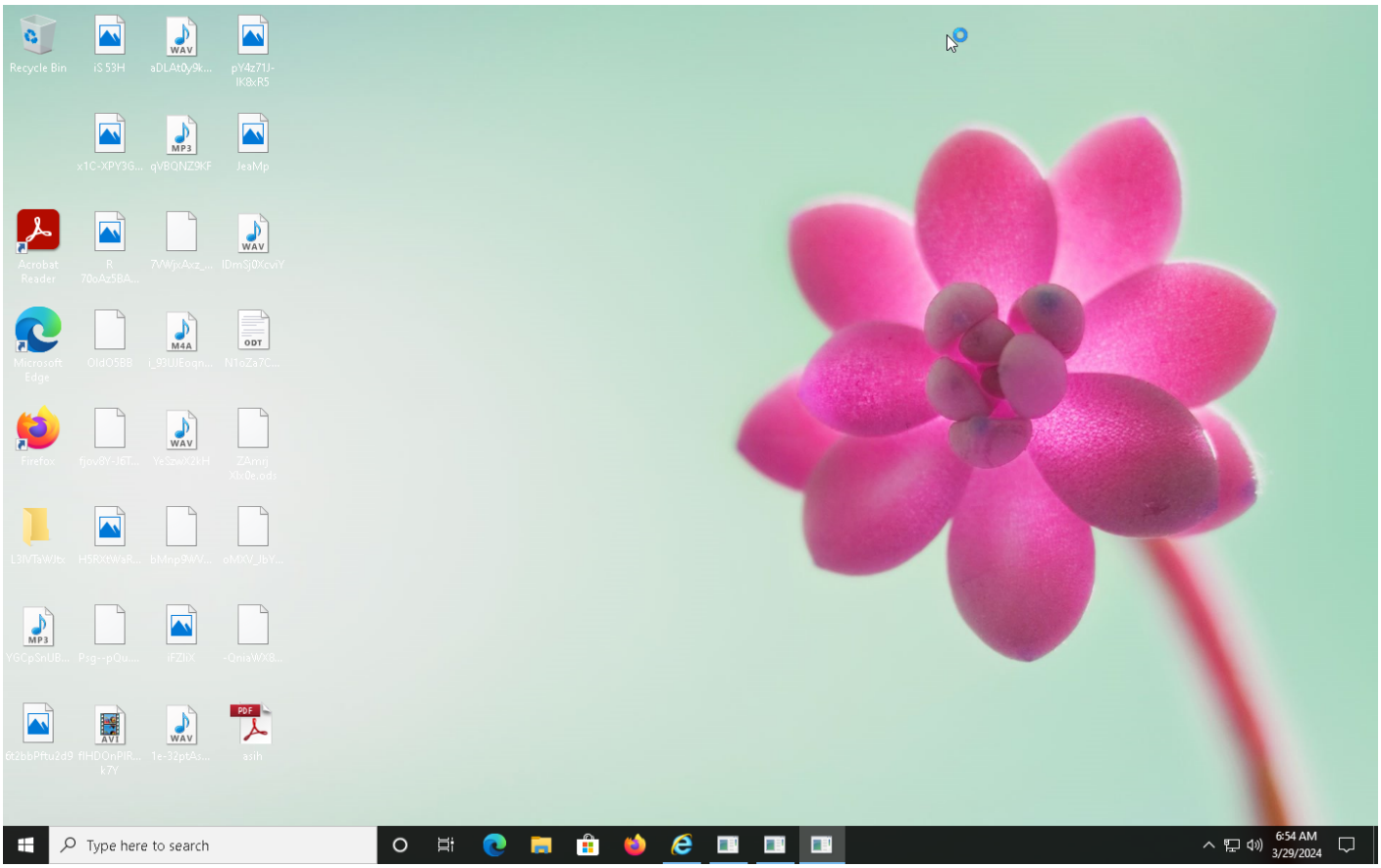
Sample Information

ID	#10131885
MD5	00e91fb785524907ad123537290364fb
SHA1	0691ee2aff1f1d949d6313e6f9359dd23ded08bb
SHA256	d9cd8e29f72b72c8754469641d68a179a424a1e04d99228f5d0c3897c4937b17
SSDeep	768:z6LsoEEeegiZPvEhHSG+gzum/kLyMro2GtOOtEvwDpj/YY1J+OT/:z6QFElP6n+gKmddpMOtEvwDpj31r
ImpHash	bd2f03255beebcd07c02192dbb770be8
File Name	asih.exe
File Size	50.23 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-03-29 05:49 (UTC)
Analysis Duration	00:02:39
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
Acrobat Reader
Microsoft Edge
Firefox
Type here to search
6:54 AM
3/29/2024


Recycle Bin
Acrobat Reader
Microsoft Edge
Firefox
Type here to search
6:54 AM
3/29/2024

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

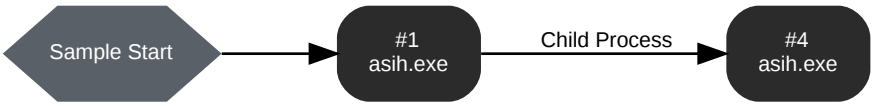
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: asih.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\asih.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\asih.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 262982, Reason: Analysis Target
Unmonitor End Time	End Time: 281234, Reason: Terminated
Monitor duration	18.25s
Return Code	0
PID	6064
Parent PID	-
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\OQXZRA~1\AppData\Local\Temp\asih.exe	50.30 KB	8d8cd2b7378b09f4887ffb43f84fa8b61ff62198b7a2e6a4bf59aa66a6cee8a6	✔

Host Behavior

Type	Count
Module	33
Window	5
File	6
Process	1

Process #4: asih.exe

ID	4
File Name	c:\users\oqxzraykm\appdata\local\temp\asih.exe
Command Line	"C:\Users\OQXZRA~1\AppData\Local\Temp\asih.exe"
Initial Working Directory	C:\Users\OQXZRA~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 279420, Reason: Child Process
Unmonitor End Time	End Time: 328108, Reason: Terminated by timeout
Monitor duration	48.69s
Return Code	Unknown
PID	5160
Parent PID	6064
Bitness	32 Bit

Host Behavior

Type	Count
Module	33
Window	5
File	253

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d9cd8e29f72b72c8754469641d68a179a424a1e04d99228f5d0c3897c4937b17	C:\Users\OqXZRaykm\Desktop\asih.exe	Sample File	50.23 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
8d8cd2b7378b09f4887ffb43f84fa8b61ff62198b7a2e6a4bf59aa66a6cee8a6	C:\Users\OQXZRA~1\AppData\Local\Temp\asih.exe	Dropped File	50.30 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
0a67be1fbf8cf9422c54a556210d26243ec68c106e187ece749af48721b4a811	-	Memory Dump	64.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
04103175626db6367b890f30c378ce55e9316b1d345ea6ab025ce14111b53fa0	-	Memory Dump	64.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
ddbc3491c1ce541a5b3aaaff1b0a53c8323d60d89d6f9e37758f48b542761a17	-	Memory Dump	64.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a0fb107971e856817cf5cb22ecbe35cfde9bf79ae571397506e83fdc32e6f274	-	Memory Dump	50.39 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
600c79e6df8b08dc26d894b54f6f4af207a29d7b5f3effc7517359820821d59a	-	Memory Dump	64.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\asih.exe	Accessed File, Sample File	Access, Read	MALICIOUS
C:\Users\OQXZRA~1\AppData\Local\Temp\asih.exe	Accessed File, Dropped File	Access, Create, Read, Write	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

Process

Process Name	Commandline	Verdict
asih.exe	"C:\Users\OqXZRaykm\Desktop\asih.exe"	MALICIOUS
asih.exe	"C:\Users\OQXZRA~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	Dropped File	C:\Users\OQXZRA~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	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_set1	CryptoLocker ransomware	Sample File	C:\Users\OqXZRaykm\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_rule2	CryptoLocker ransomware	Sample File	C:\Users\OqXZRaykm\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_set1	CryptoLocker ransomware	Dropped File	C:\Users\OQXZRA~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

ENVIRONMENT

Virtual Machine Information

Name	win10_64_20h1_en_base
Description	windows 10 (64bit 20H1 -EN-)
Architecture	x86 64-bit
Operating System	Windows 10 20H1
Kernel Version	10.0.19041.208 (dc9233f8-5819-e3d0-929a-7bde0b87f0b9)
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	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.207.19041.0
Chrome Version	Not installed
Firefox Version	108.0
Flash Version	Not installed
Java Version	8.0.3610.9

System Information

Sample Directory	C:\Users\OqXZRaykm\Desktop
Computer Name	PXTHFFRYO7
User Domain	PXTHFFRYO7
User Name	OqXZRaykm
User Profile	C:\Users\OqXZRaykm
Temp Directory	C:\Users\OQXZRA~1\AppData\Local\Temp

System Root	C:\Windows