

**MALICIOUS**

Classifications: Ransomware

Threat Names: CryptoLocker

Verdict Reason: -

Sample Type	Windows Exe (x86-32)
File Name	lossy.exe
ID	#10131880
MD5	01a8fe565e183f37e64f753d9a0d93bc
SHA1	a7308710a3e4418bf14400680092a80ac513c8d3
SHA256	4af3488da70ab712f3a5c13f56e575573a6dd3b6a0fc7cd48d8bf41e43298cac
File Size	39.80 KB
Report Created	2024-03-29 07:49 (UTC+1)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016)   exe

## OVERVIEW

### VMRay Threat Identifiers (8 rules, 12 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	4	Ransomware
<ul style="list-style-type: none"> <li>• YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in process image data from (process #1) lossy.exe.</li> <li>• YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in memory dump data from (process #1) lossy.exe.</li> <li>• YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in the sample file C:\Users\RDhJ0CNFevzX\Desktop\lossy.exe.</li> <li>• YARA detected "CryptoLocker_rule2" from ruleset "Ransomware" in memory dump data from (process #2) lossy.exe.</li> </ul>				
4/5	Reputation	Malicious file detected via reputation	1	-
<ul style="list-style-type: none"> <li>• The sample itself is a known malicious file.</li> </ul>				
3/5	Network Connection	All network connection attempts failed	1	-
<ul style="list-style-type: none"> <li>• Host "2ndry.com" is unavailable.</li> </ul>				
2/5	Network Connection	Allows invalid SSL certificates	1	-
<ul style="list-style-type: none"> <li>• (Process #2) lossy.exe allows network connections with an invalid SSL certificate.</li> </ul>				
1/5	Hide Tracks	Creates process with hidden window	1	-
<ul style="list-style-type: none"> <li>• (Process #1) lossy.exe starts (process #2) lossy.exe with a hidden window.</li> </ul>				
1/5	Obfuscation	Resolves API functions dynamically	2	-
<ul style="list-style-type: none"> <li>• (Process #1) lossy.exe resolves 25 API functions by name.</li> <li>• (Process #2) lossy.exe resolves 25 API functions by name.</li> </ul>				
1/5	Execution	Drops PE file	1	-
<ul style="list-style-type: none"> <li>• (Process #1) lossy.exe drops file "C:\Users\RDHJ0C~1\AppData\Local\Temp\lossy.exe".</li> </ul>				
1/5	Execution	Executes dropped PE file	1	-
<ul style="list-style-type: none"> <li>• Executes dropped file "C:\Users\RDHJ0C~1\AppData\Local\Temp\lossy.exe".</li> </ul>				

**Mitre ATT&CK Matrix**

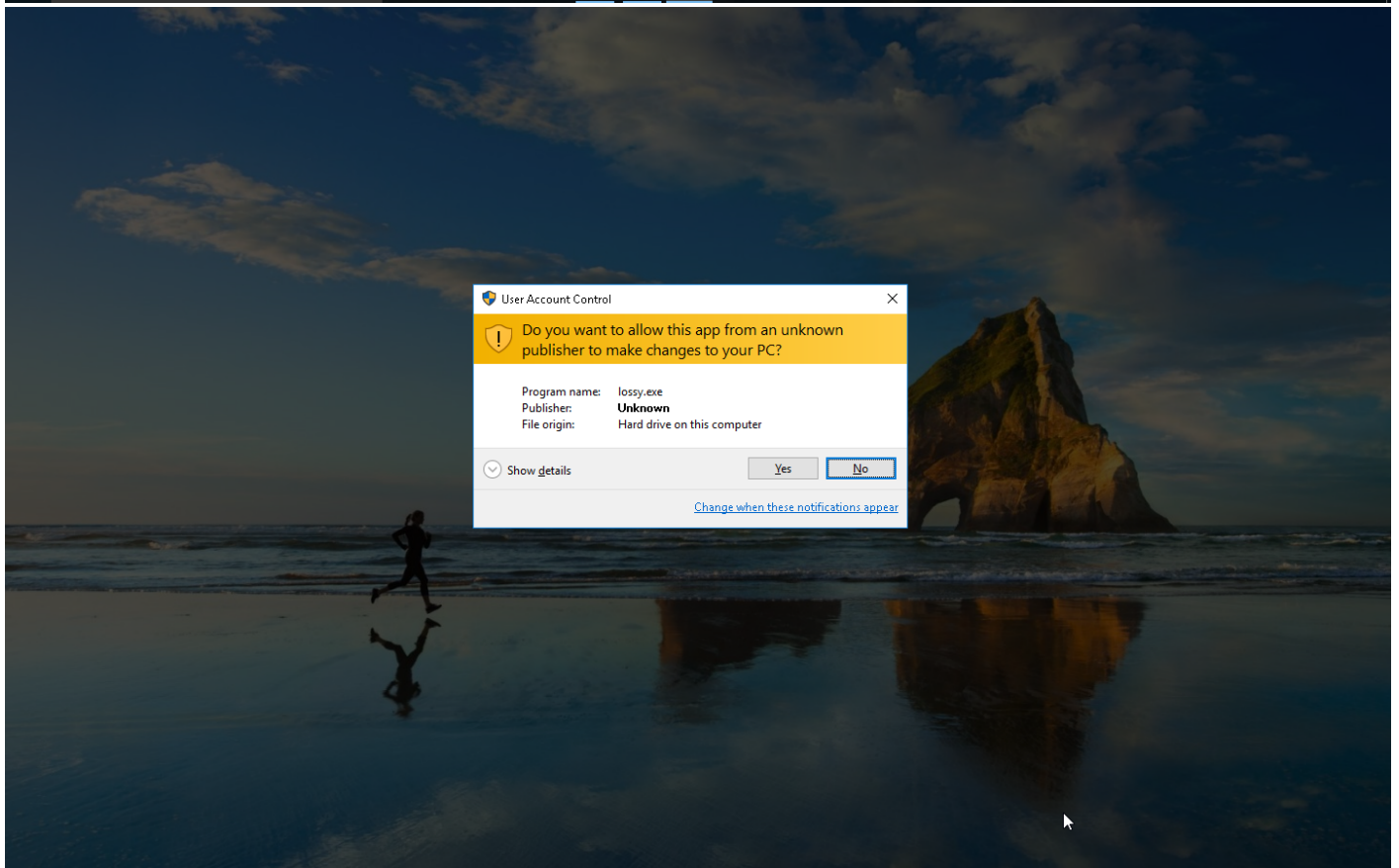
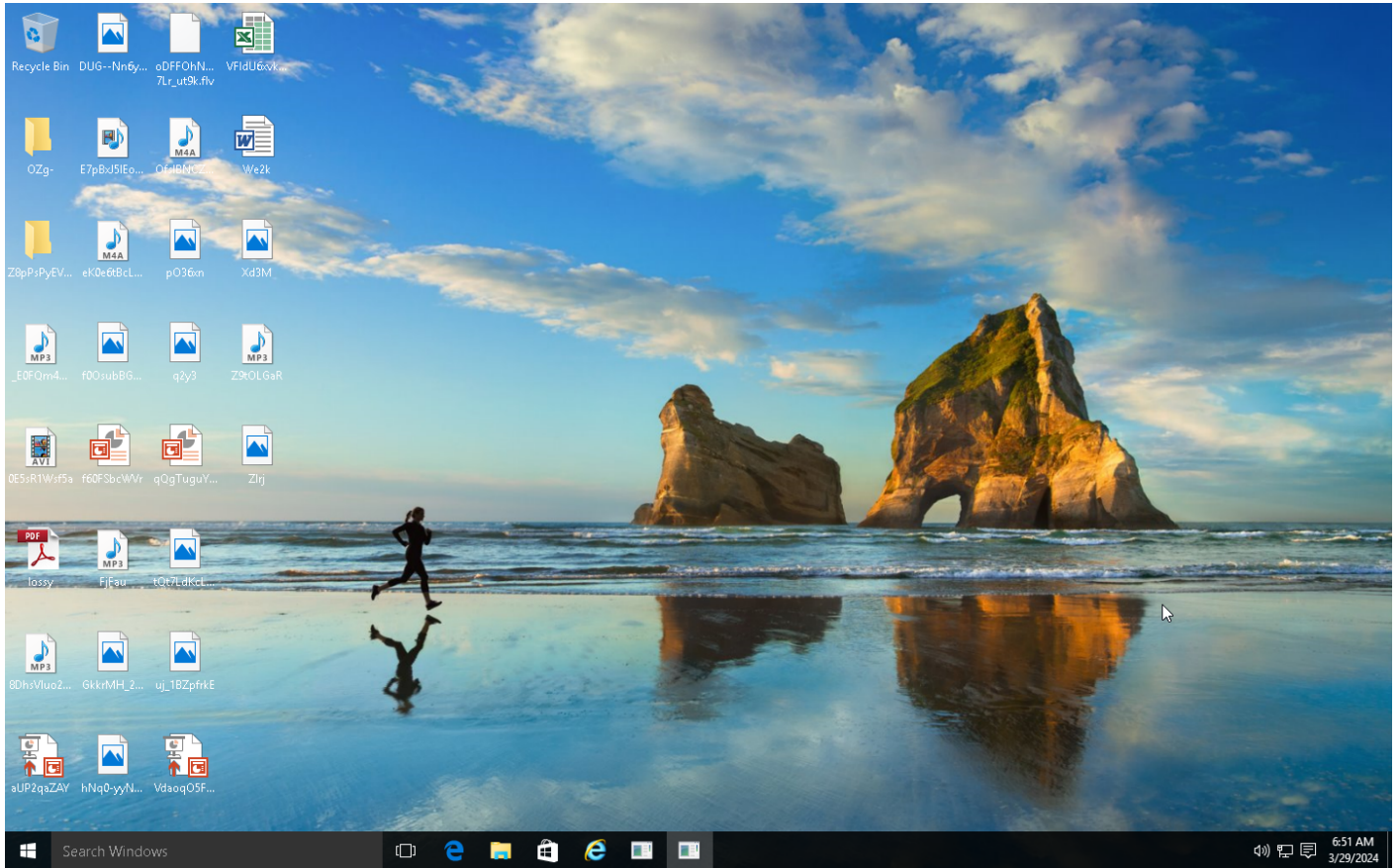
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window							
				#T1045 Software Packing							

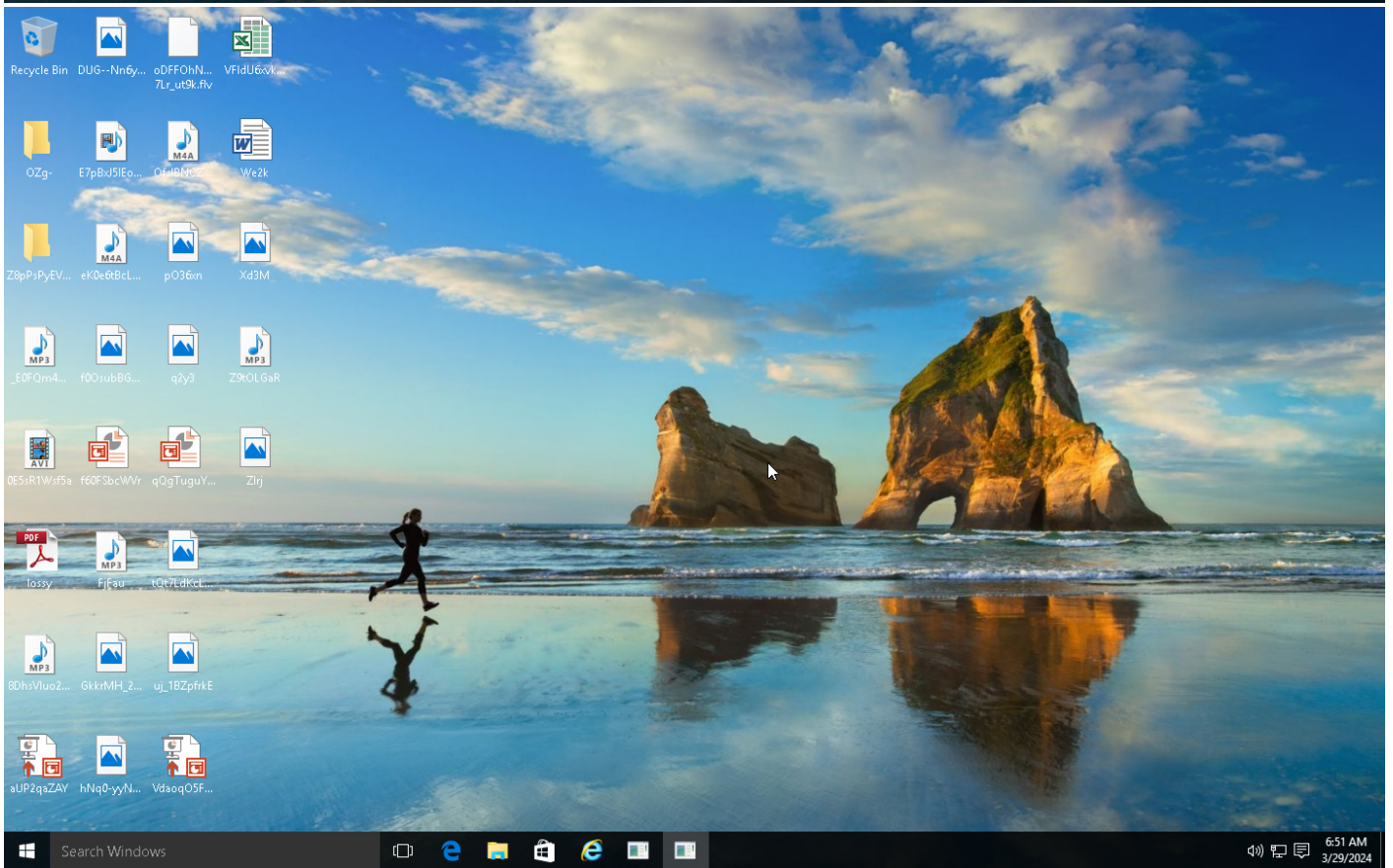
**Sample Information**

ID	#10131880
MD5	01a8fe565e183f37e64f753d9a0d93bc
SHA1	a7308710a3e4418bf14400680092a80ac513c8d3
SHA256	4af3488da70ab7f2f3a5c13f56e575573a6dd3b6a0fc7cd48d8bf41e43298cac
SSDeep	768:blDOW9UiaCHfjnE0Sf88AvvP1oghYvm9/6Dy8Pc:blDOW9a0Dwo3P1ojvUSDhU
ImpHash	0bcae7989ef60f5550a7f5735f53a2aa
File Name	lossy.exe
File Size	39.80 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✓

**Analysis Information**

Creation Time	2024-03-29 07:49 (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	6





Screenshots truncated

## NETWORK

### General

55 bytes total sent

128 bytes total received

1 ports 53

1 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

### DNS

1 DNS requests for 1 domains

1 nameservers contacted

1 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	hxtps://2ndry[.]com/gold/a3mor.exe	-	-	-	0 bytes	CLEAN

### DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	2ndry[.]com	NX_DOMAIN	-	-	SUSPICIOUS

## BEHAVIOR

### Process Graph

---





**Process #1: lossy.exe**

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\lossy.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\lossy.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 110661, Reason: Analysis Target
Unmonitor End Time	End Time: 118987, Reason: Terminated
Monitor duration	8.33s
Return Code	0
PID	3484
Parent PID	-
Bitness	32 Bit

**Dropped Files (1)**

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\lossy.exe	39.88 KB	9e2f075d09137dd116f942e930ecd3fae2e6e355589c90682cd62f8bf00467e5	✓

**Host Behavior**

Type	Count
Module	33
Window	4
File	6
Process	1

**Process #2: lossy.exe**

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\local\temp\lossy.exe
Command Line	"C:\Users\RDHJ0C~1\AppData\Local\Temp\lossy.exe"
Initial Working Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp\
Monitor Start Time	Start Time: 116459, Reason: Child Process
Unmonitor End Time	End Time: 350663, Reason: Terminated by timeout
Monitor duration	234.20s
Return Code	Unknown
PID	4356
Parent PID	3484
Bitness	32 Bit

**Host Behavior**

Type	Count
Module	33
Window	4
File	253

**Network Behavior**

Type	Count
HTTPS	1
TCP	1

## ARTIFACTS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
4af3488da70ab7f2f3a5c13f56e575573a6dd3b6a0fc7cd48d8bf41e43298cac	C:\Users\RDHJ0CNFevzX\Desktop\lossy.exe	Sample File	39.80 KB	application/vnd.microsoft.portable-executable	Access, Read	<b>MALICIOUS</b>
9e2f075d09137dd116f942e930ecd3fae2e6e355589c90682cd62f8bf00467e5	C:\Users\RDHJ0C~1\AppData\Local\Temp\lossy.exe	Dropped File	39.88 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	<b>MALICIOUS</b>
2951823ccb7575517efa7d147c0a865ba6f773468e154df228c5252209c5408	-	Memory Dump	36.00 KB	application/vnd.microsoft.portable-executable	-	<b>MALICIOUS</b>
7566583ce2b3a607a6bd59b9ba7bcee2ffa41eae5d2f01b1b80f67c04948c	-	Memory Dump	36.00 KB	application/vnd.microsoft.portable-executable	-	<b>MALICIOUS</b>
624f41f909b01fba89423facc49428fd871a21f56dd1062eca4e75e2f81b3840	-	Memory Dump	640.00 KB	application/octet-stream	-	<b>MALICIOUS</b>
5dc6319635a4be7b71cd9d5ebc98364c32e59813505bd83e1a22d3c1517bac6e	-	Memory Dump	36.00 KB	application/vnd.microsoft.portable-executable	-	<b>MALICIOUS</b>

Filename	Category	Operations	Verdict
C:\Users\RDHJ0CNFevzX\Desktop\lossy.exe	Accessed File, Sample File	Access, Read	<b>MALICIOUS</b>
C:\Users\RDHJ0C~1\AppData\Local\Temp\lossy.exe	Accessed File, Dropped File	Access, Create, Read, Write	<b>CLEAN</b>
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	<b>CLEAN</b>
prev.inf	Accessed File	Access	<b>CLEAN</b>
C:\Users\BMONIK~1.NSP\AppData\Local\Temp\Rar\$EX00.290\Reference_03102013.exe	Accessed File	Access, Delete	<b>CLEAN</b>

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxps://2ndry[.]com/gold/a3mor.exe	Extracted	-	-	-	<b>CLEAN</b>

Domain	IP Address	Country	Protocols	Verdict
2ndry[.]com	-	-	-	<b>SUSPICIOUS</b>

Process Name	Commandline	Verdict
lossy.exe	"C:\Users\RDHJ0CNFevzX\Desktop\lossy.exe"	<b>MALICIOUS</b>
lossy.exe	"C:\Users\RDHJ0C~1\AppData\Local\Temp\lossy.exe"	<b>MALICIOUS</b>

## YARA / AV

### YARA (6)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Sample File	C:\Users\RDhJ0CNFevz\IDesktop\lossy.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	Dropped File	C:\Users\RDhJ0C-1\AppData\Local\Temp\lossy.exe	Ransomware	5/5
Ransomware	CryptoLocker_rule2	CryptoLocker ransomware	Memory Dump	-	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

---