MALICIOUS

Classifications: -

Threat Names: CryptOne

Verdict Reason: -

Sample Type	**Windows DLL (x86-32)**
File Name	**2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a.dll**
ID	#967524
MD5	803768a34f7e59b8a9a2f3969624c47e
SHA1	09a38940ef023929897fdc9c996de0b0f39116e2
SHA256	2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a
File Size	506.98 KB
Report Created	2021-09-27 22:05 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (2 rules, 2 matches)

Score	Category	Operation	Count	Classification
5/5	YARA	Malicious content matched by YARA rules	1	-
	• Rule "CryptOne_Packer" from ruleset "Generic" has matched on a memory dump for (process #1) pyzajnlcl.exe.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) pyzajnlcl.exe resolves 192 API functions by name.			

Mitre ATT&CK Matrix

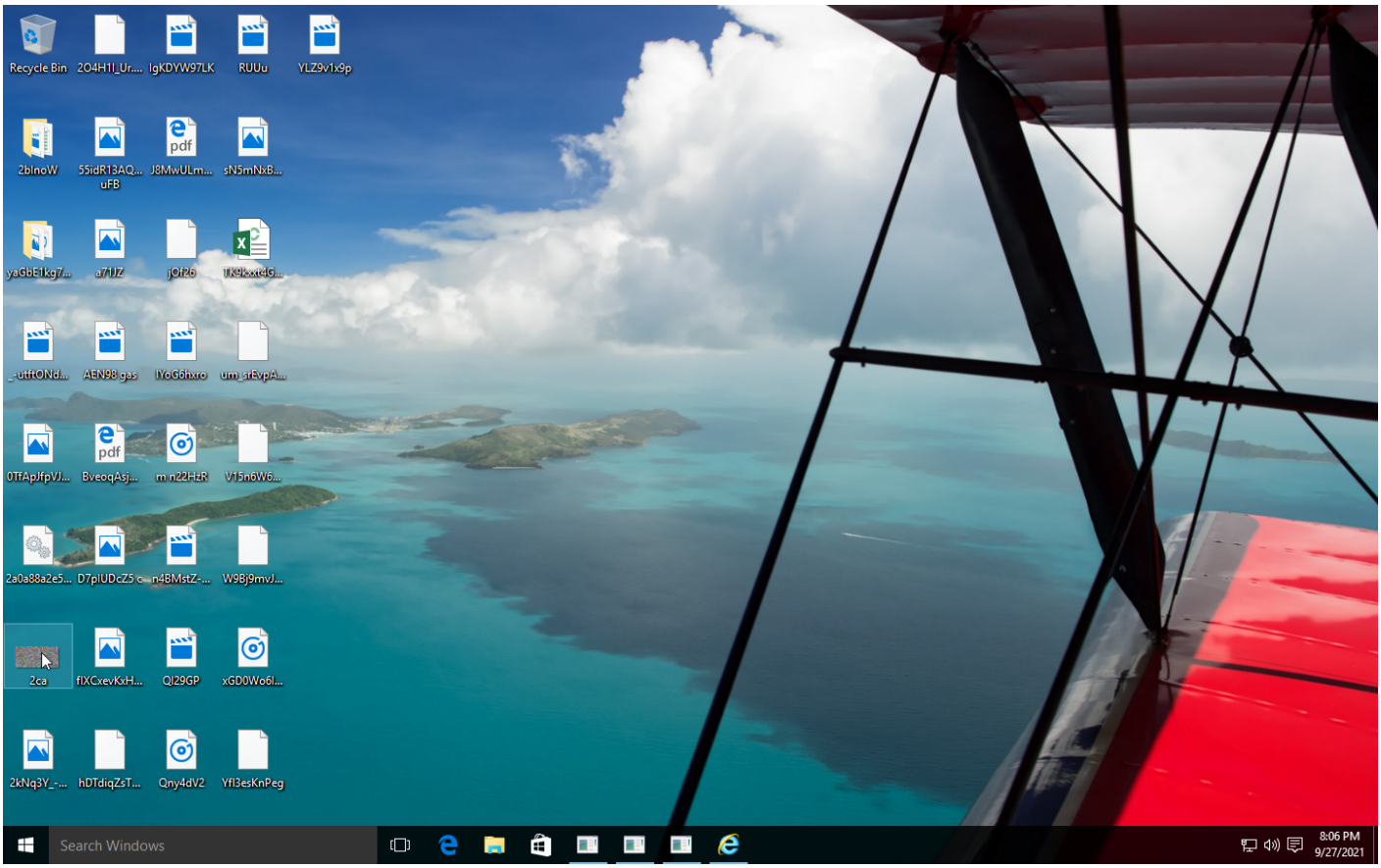
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing							

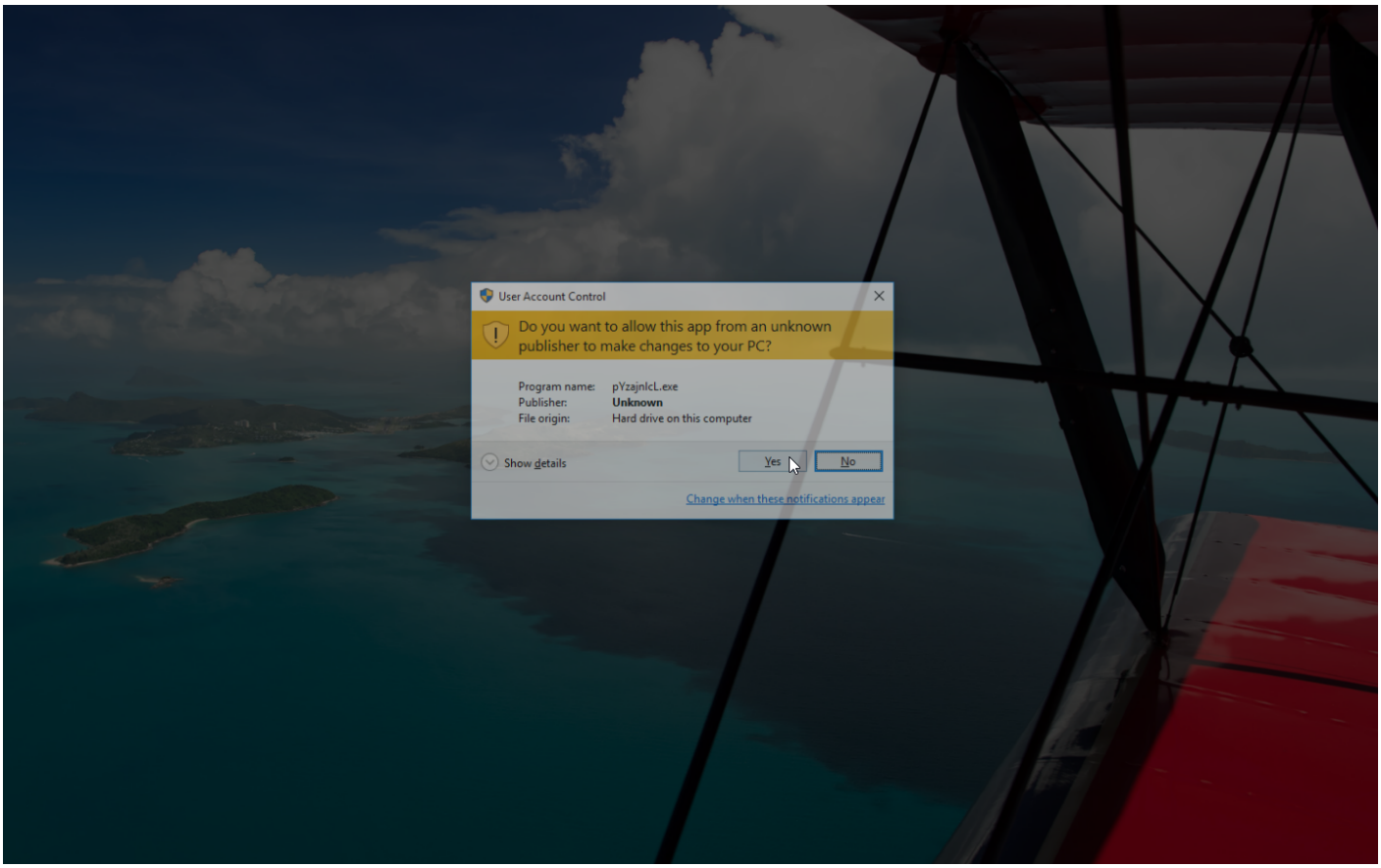
Sample Information

ID	#967524
MD5	803768a34f7e59b8a9a2f3969624c47e
SHA1	09a38940ef023929897fdc9c996de0b0f39116e2
SHA256	2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a
SSDeep	12288:+xyHC8LAE/azElTT4c7Bo+526Tb/jXiQle601:eb8LxazE9X7C96Tz7iA/C
ImpHash	5097c68ca7573db2997ab353ba37473b
File Name	2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a.dll
File Size	506.98 KB
Sample Type	Windows DLL (x86-32)
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 22:05 (UTC+2)
Analysis Duration	00:01:50
Termination Reason	All processes terminated
Number of Monitored Processes	1
Execution Successful	False
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	2


Recycle Bin
2O4H1I_Ur....
lgKDYW97LK
RUUu
YLZ9v1x9p
2blnoW
55idR13AQ... uFB
J8MwULm...
sN5mNxB...
yaGbE1kg7...
a7IJZ
jOf26
TfX9xxt4G...
_-utftONd...
AEN98.gas
lYoG6hxro
um_stEvpA...
0TfApJfpVJ...
BveoqAsj...
m n22HzR
V15h6W6...
2a0a88a2e5...
D7plUDcZ5 c...
n4BMstZ-...
W9Bj9mvJ...
2ca
fIXCxevKsH...
Ql29GP
xGD0Wo6l...
2kNq3Y_-...
hDTdiqZsT...
Qny4dV2
Yfl3esKnPeg
Search Windows
8:06 PM
9/27/2021


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

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

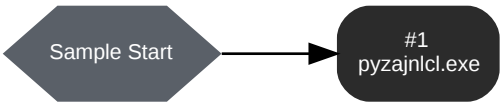
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: pyzajnlcl.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\pyzajnlcl.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\pYzajnlcL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a.dll"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 63374, Reason: Analysis Target
Unmonitor End Time	End Time: 163998, Reason: Terminated
Monitor duration	100.62s
Return Code	0
PID	4988
Parent PID	1636
Bitness	32 Bit

Host Behavior

Type	Count
Module	372
File	3
System	6
Environment	1
Keyboard	3
Registry	3
-	3
Window	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a	C:\Users\RDhJ0CNFevzX\Desktop\2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a.dll	Sample File	506.98 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\pYzajnlcL.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\Desktop\2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a.dll	Sample File	Access	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Borland\Locales	access	pyzajnlcl.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Borland\Locales	access	pyzajnlcl.exe	CLEAN
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales	access	pyzajnlcl.exe	CLEAN

Process

Process Name	Commandline	Verdict
pyzajnlcl.exe	"C:\Users\RDhJ0CNFevzX\Desktop\pYzajnlcL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2a0a88a2e5f9cafa10a48d63bdfcdf965b72c25978ab46cf28e795dbedc9624a.dll"	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	CryptOne_Packer	Shellcode used by the CryptOne packer	Memory Dump	-	-	5/5
Generic	CryptOne_Packer	Shellcode used by the CryptOne packer	Memory Dump	-	-	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
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	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-27 16:34:30+00:00
Built-in AV Database Records	10473840

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
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	Not installed

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