MALICIOUS

Classifications: Spyware

Threat Names: RedLine.E, RedLine.F, Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Debut.exe**
ID	#10398287
MD5	89dd9b90e6df2ebe2a3bd8071a3f22b2
SHA1	05c5199b9e0865bbb36822f3ea3470d41aaf5531
SHA256	6fea47929205ee6ccaf014456c2ce24b6fcd330722cf3bffba2b3085cd2d1594
File Size	168.59 KB
Report Created	2024-05-09 16:11 (UTC+2)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (7 rules, 10 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	RedLine configuration was extracted	1	Spyware
	• A configuration for RedLine was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	4	Spyware
	• YARA detected "RedLine_E" from ruleset "Malware" in the sample file C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe. • YARA detected "RedLine_F" from ruleset "Malware" in the sample file C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe. • YARA detected "RedLine_E" from ruleset "Malware" in memory dump data from (process #1) debut.exe. • YARA detected "RedLine_F" from ruleset "Malware" in memory dump data from (process #1) debut.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	1	-
	• Reputation analysis labels the contacted IP address 217.196.96.101 as Mal/HTMLGen-A.			
3/5	Network Connection	All network connection attempts failed	1	-
	• Host "217.196.96.101" is unavailable.			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #1) debut.exe opens an outgoing TCP connection to host "217.196.96.101:4132".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #1) debut.exe tries to connect to TCP port 4132 at 217.196.96.101.			

Malware Configuration: RedLine

Metadata	Key	Extracted Value
Version	Value	1
Mission ID	Value	mihan
Encryption Key	Key Algorithm	SG9zdGVsbGVy xor
Socket	Address Port Network Protocol C2 Listen	217.196.96.101 4132 tcp ✔ ✖

Mitre ATT&CK Matrix

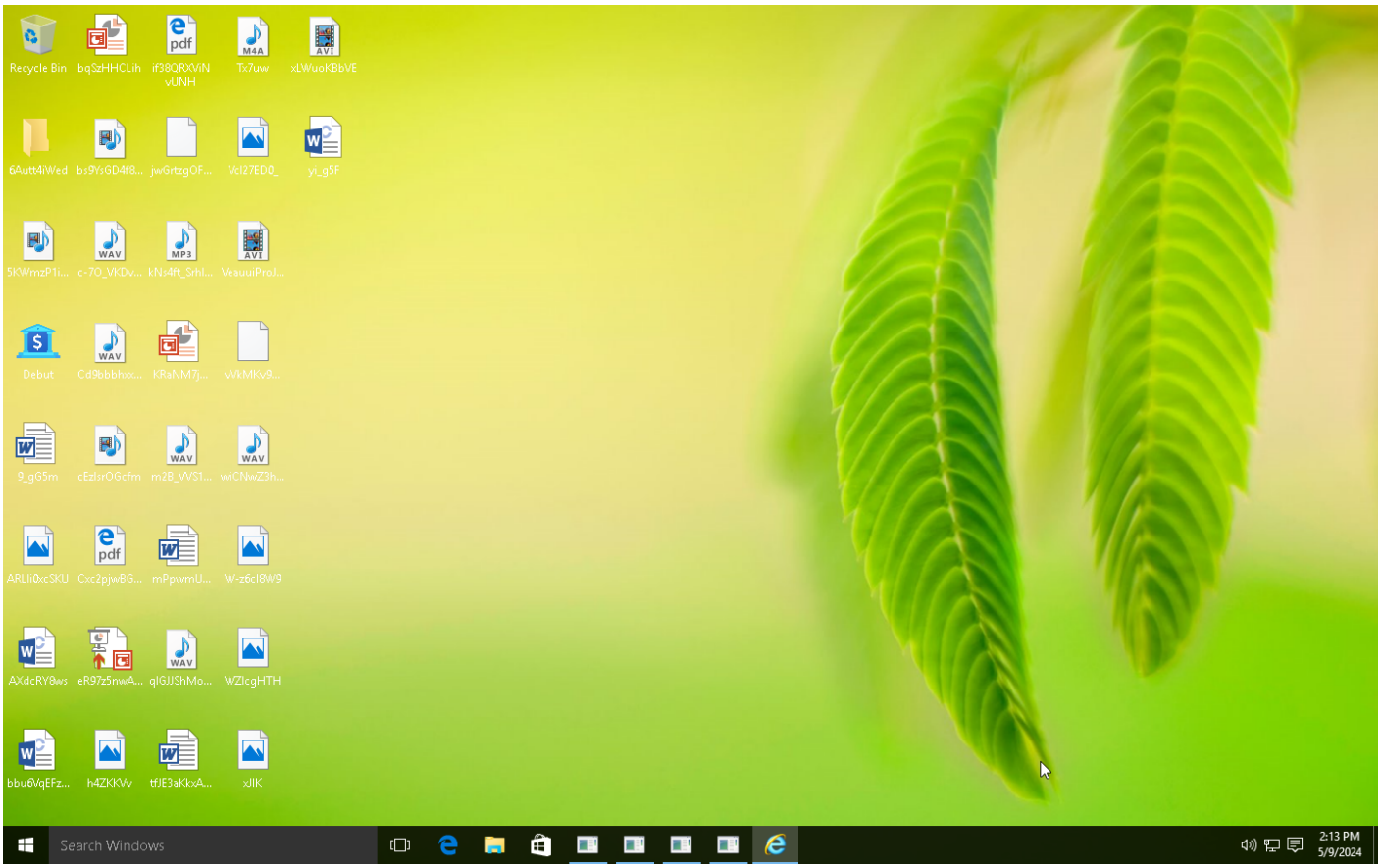
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
									#T1065 Uncommonly Used Port		

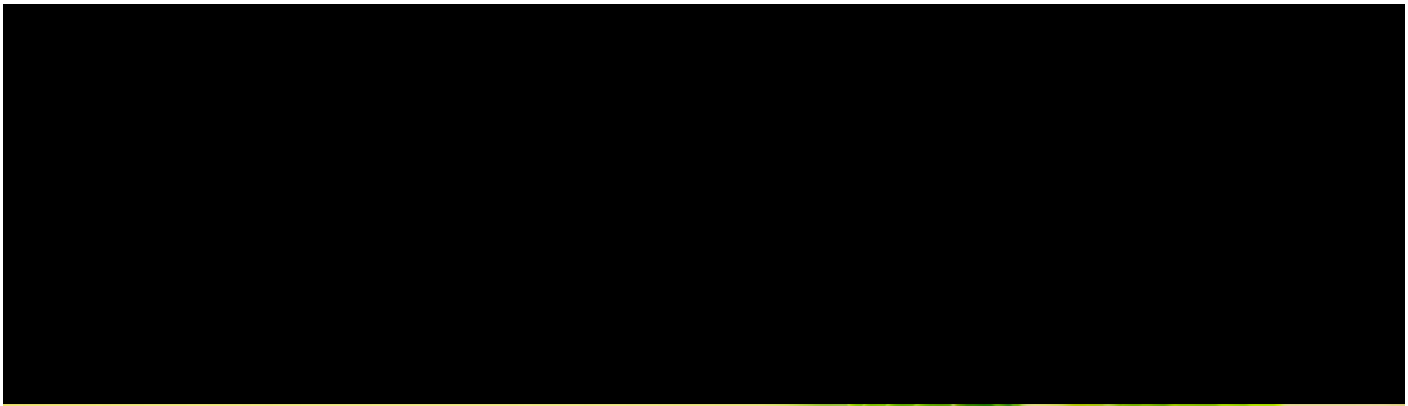
Sample Information

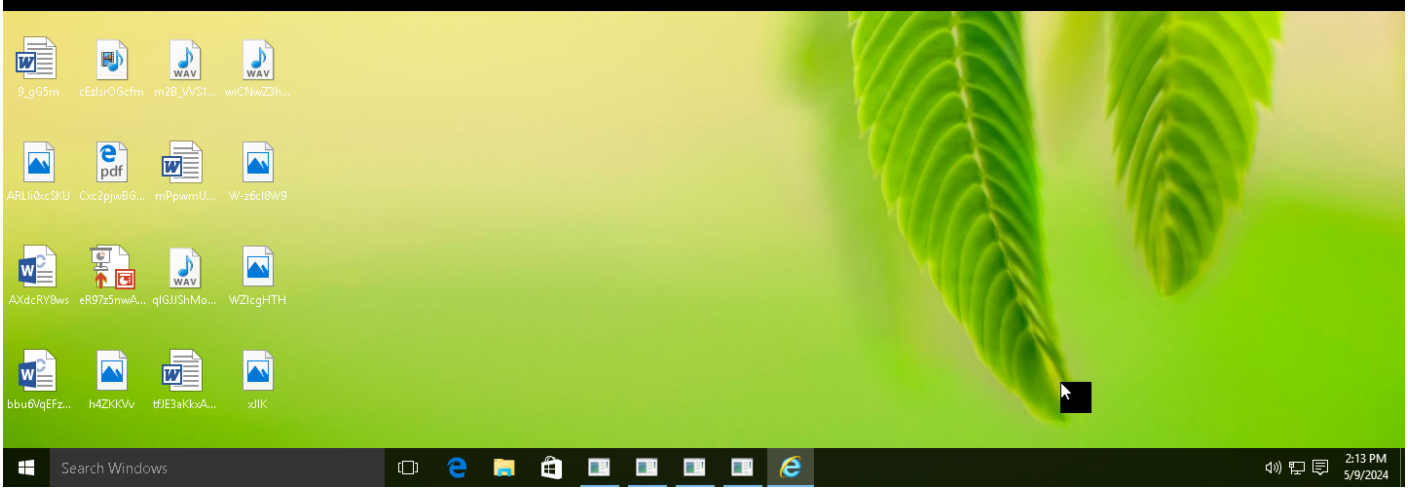
ID	#10398287
MD5	89dd9b90e6df2ebe2a3bd8071a3f22b2
SHA1	05c5199b9e0865bbb36822f3ea3470d41aaf5531
SHA256	6fea47929205ee6ccaf014456c2ce24b6fcd330722cf3bffba2b3085cd2d1594
SSDeep	1536:wPCNTP3mqlVZRGW6sRrrmMn8JlwVJWHGTGqVQbuwgSFOuZS67d83wYkS8e8hd:wPCZeX2tD+qVgzF/ZS67dA8e8hd
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	Debut.exe
File Size	168.59 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

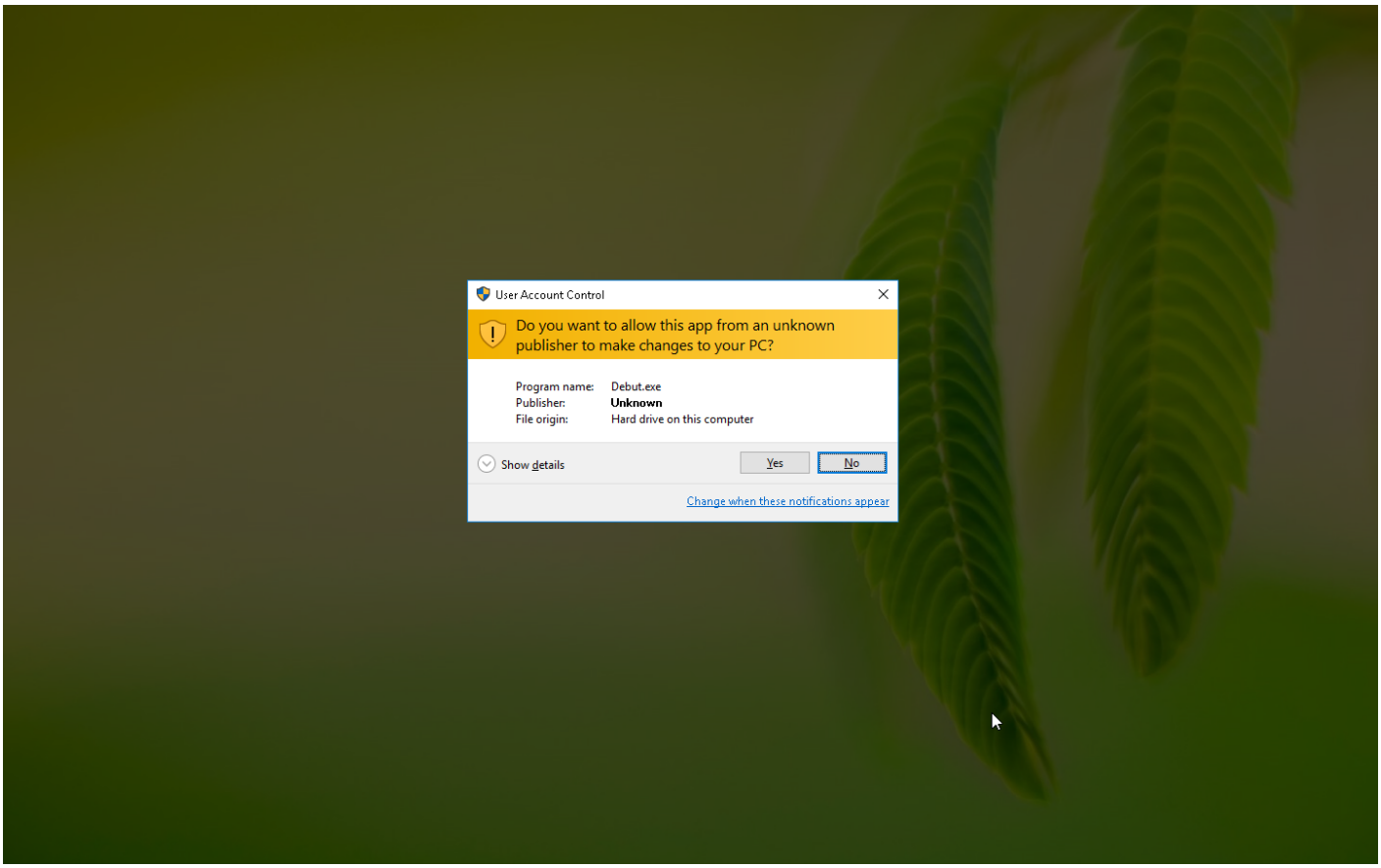
Analysis Information

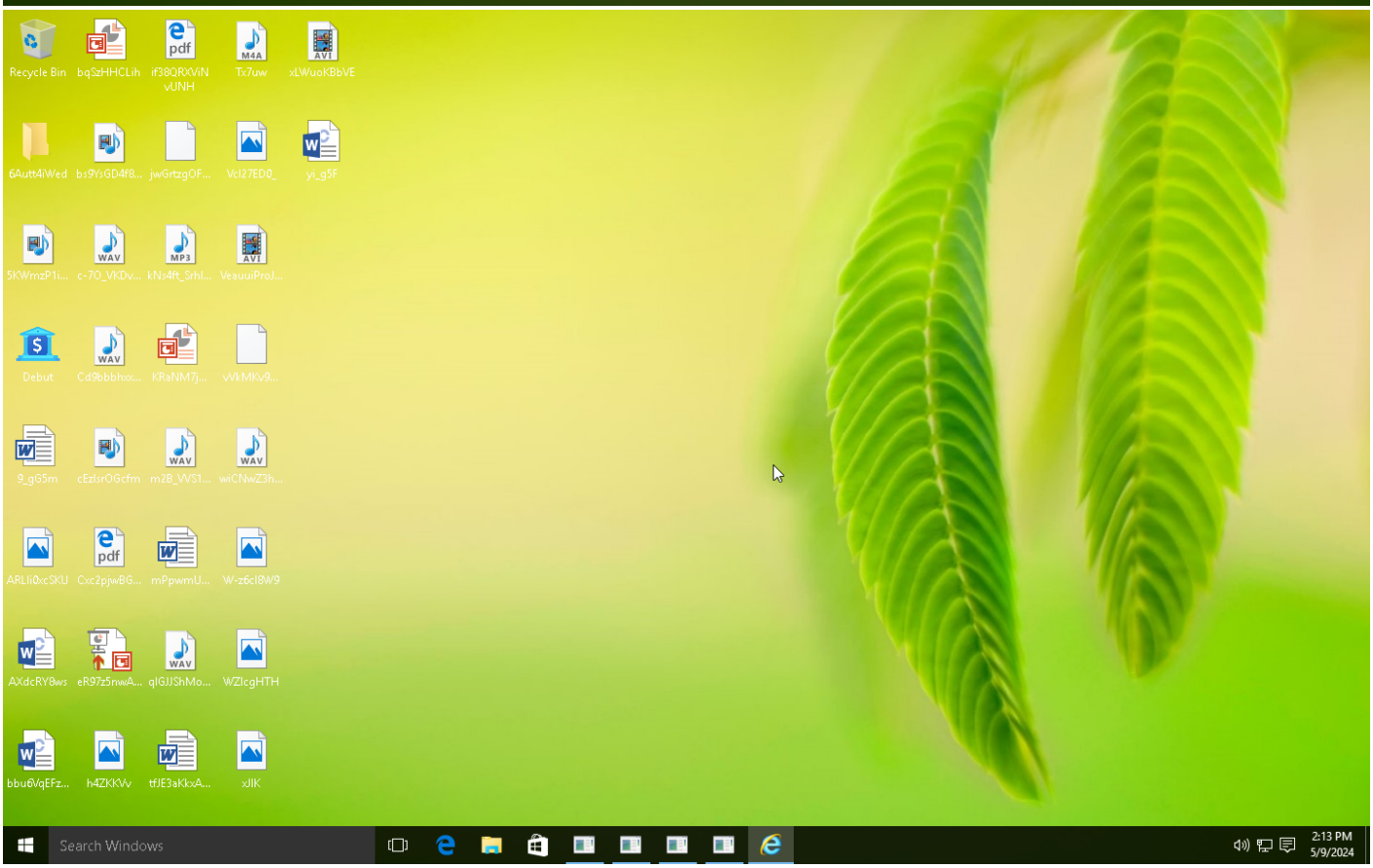
Creation Time	2024-05-09 16:11 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	1
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✖
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, 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	4


Recycle Bin
Search Windows
2:13 PM
5/9/2024




Search Windows
2:13 PM
5/9/2024


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


Recycle Bin
Debut
Search Windows
2:13 PM
5/9/2024

NETWORK

General

152 bytes total sent

0 bytes total received

1 ports 4132

1 contacted IP addresses

0 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

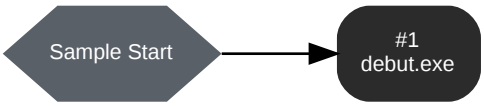
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: debut.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\debut.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 101578, Reason: Analysis Target
Unmonitor End Time	End Time: 341586, Reason: Terminated by timeout
Monitor duration	240.01s
Return Code	Unknown
PID	2788
Parent PID	-
Bitness	32 Bit

Host Behavior

Type	Count
Module	14
Environment	1
Registry	15
File	18

Network Behavior

Type	Count
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
6fea47929205ee6ccaf014456c2ce24b6fcd330722cf3bffba2b3085cd2d1594	C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe	Sample File	168.59 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
d19104950c2b25ed0c4f27a0775ab55d292a6e226cc6597610eacc47c0dd5c14	-	Memory Dump	192.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe	Sample File	-	MALICIOUS
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe.config	Accessed File	Access	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
217.196.96.101	-	Russia	TCP	MALICIOUS

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Net Framework Setup\NDP\v4\Client	access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Net Framework Setup\NDP\v4\Client\InstallPath	read, access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	debut.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\.NETFramework\XML	access	debut.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\XML	access	debut.exe	CLEAN

Process

Process Name	Commandline	Verdict
debut.exe	"C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe"	MALICIOUS

YARA / AV

YARA (4)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	RedLine_E	RedLine Stealer, RedLine.E variant	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe	Spyware	5/5
Malware	RedLine_F	RedLine Stealer, RedLine.F variant	Memory Dump	-	Spyware	5/5
Malware	RedLine_E	RedLine Stealer, RedLine.E variant	Memory Dump	-	Spyware	5/5
Malware	RedLine_F	RedLine Stealer, RedLine.F variant	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\Debut.exe	Spyware	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	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.27 / 2024-05-02 14:06:04
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.27 / 2024-05-02 14:06:04
YARA Built-in Ruleset Version	2024.2.1.24

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