MALICIOUS

Classifications: Downloader | Injector

Threat Names: Mal/HTMLGen-A | Gen:Variant.Bulz.604474

Verdict Reason: -

Sample Type	**Excel Document**
File Name	**3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls**
ID	#967595
MD5	b4b3a2223765ac84c9b1b05dbf7c6503
SHA1	57bc35cb0c7a9ac6e7fcb5dea5c211fe5eda5fe0
SHA256	3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36
File Size	126.00 KB
Report Created	2021-09-27 23:15 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (28 rules, 60 matches)

Score	Category	Operation	Count	Classification
4/5	Discovery	Queries OS version via WMI	1	-
	• (Process #3) explorer.exe queries OS version via WMI.			
4/5	Discovery	Executes WMI query	9	-
	• (Process #3) explorer.exe executes WMI query: SELECT * FROM Win32_OperatingSystem. • (Process #3) explorer.exe executes WMI query: SELECT * FROM AntiVirusProduct. • (Process #3) explorer.exe executes WMI query: SELECT * FROM Win32_Processor. • (Process #3) explorer.exe executes WMI query: select * from Win32_ComputerSystem. • (Process #3) explorer.exe executes WMI query: select * from Win32_Bios. • (Process #3) explorer.exe executes WMI query: select * from Win32_DiskDrive. • (Process #3) explorer.exe executes WMI query: select * from Win32_PhysicalMemory. • (Process #3) explorer.exe executes WMI query: select Caption,Description,Vendor,Version,InstallDate,InstallSource,PackageName from Win32_Product. • (Process #3) explorer.exe executes WMI query: select Caption,Description,DeviceID,Manufacturer,Name,PNPDeviceID,Service,Status from Win32_PnPEntity.		
4/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #3) explorer.exe tries to detect antivirus software via WMI query: "SELECT * FROM AntiVirusProduct".			
4/5	Discovery	Collects hardware properties	1	-
	• (Process #3) explorer.exe queries hardware properties via WMI.			
4/5	Discovery	Collects BIOS properties	1	-
	• (Process #3) explorer.exe queries BIOS properties via WMI.			
4/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #2) regsvr32.exe creates a new explorer.exe process.			
4/5	Injection	Writes into the memory of another process	3	Injector
	• (Process #2) regsvr32.exe modifies memory of (process #3) explorer.exe. • (Process #4) regsvr32.exe modifies memory of (process #5) explorer.exe. • (Process #6) regsvr32.exe modifies memory of (process #7) explorer.exe.			
4/5	Reputation	Contacts known malicious URL	2	-
	• Reputation analysis labels the URL "https://71.74.12.34/t4" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A". • Reputation analysis labels the URL "https://120.150.218.241/t4" which was contacted by (process #3) explorer.exe as "Mal/HTMLGen-A".			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 120.150.218.241 as "Mal/HTMLGen-A".			
4/5	Network Connection	Downloads executable	3	Downloader
	• Downloads executable via http from http://190.14.37.178/44466.8866396991.dat. • Downloads executable via http from http://185.183.96.67/44466.8866396991.dat. • Downloads executable via http from http://185.250.148.213/44466.8866396991.dat.			

Score	Category	Operation	Count	Classification
4/5	Network Connection	Attempts to connect through HTTPS	2	-
	• (Process #3) explorer.exe connects to "71.74.12.34/t4". • (Process #3) explorer.exe connects to "120.150.218.241/t4".			
4/5	Network Connection	Tries to connect using an uncommon port	2	-
	• (Process #3) explorer.exe tries to connect to TCP port 995 at 120.150.218.241. • Tries to connect to TCP port 995 at 120.150.218.241.			
4/5	Heuristics	Document tries to trick users into running macros	1	-
	• Extracted text from an image embedded in C:\Users\RDhJ0CNFevzX\Desktop\3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls suggests enabling macros.			
4/5	Execution	Document tries to create process	3	-
	• Document creates (process #4) regsvr32.exe. • Document creates (process #2) regsvr32.exe. • Document creates (process #6) regsvr32.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	1	-
	• Built-in AV detected a memory dump of (process #2) regsvr32.exe as "Gen:Variant.Bulz.604474".			
3/5	Discovery	Enumerates running processes	4	-
	• (Process #2) regsvr32.exe enumerates running processes. • (Process #4) regsvr32.exe enumerates running processes. • (Process #6) regsvr32.exe enumerates running processes. • (Process #3) explorer.exe enumerates running processes.			
3/5	Anti Analysis	Delays execution	1	-
	• (Process #3) explorer.exe has a thread which sleeps more than 5 minutes.			
3/5	Obfuscation	Contains obfuscated URL	3	-
	• C:\Users\RDhJ0CNFevzX\Desktop\3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls contains an obfuscated URL "http://185.183.96.67/". • C:\Users\RDhJ0CNFevzX\Desktop\3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls contains an obfuscated URL "http://185.250.148.213/". • C:\Users\RDhJ0CNFevzX\Desktop\3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls contains an obfuscated URL "http://190.14.37.178/".			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #17) ipconfig.exe reads the network adapters' addresses by API.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #3) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Execution	Office macro uses an execute function	1	-
	• Office macro uses the run function.			
2/5	Execution	Office macro uses a file I/O function	1	-
	• Office macro uses the close function.			
2/5	Execution	Executes macro on specific event	4	-

Score	Category	Operation	Count	Classification
	• Executes macro automatically on target "document" and event "open". • Executes macro automatically on target "workbook" and event "open". • Executes macro on target "document" and event "close". • Executes macro on target "workbook" and event "activate".			
2/5	Execution	Drops PE file	1	-
	• (Process #3) explorer.exe drops file "C:\Users\RDhJ0CNFevzX\Drezd.red".			
2/5	Obfuscation	Document contains obfuscated macros	1	-
	• C:\Users\RDhJ0CNFevzX\Desktop\3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls contains an obfuscated macro.			
1/5	Mutex	Creates mutex	8	-
	• (Process #3) explorer.exe creates mutex with name "Global\{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #3) explorer.exe creates mutex with name "{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #3) explorer.exe creates mutex with name "{61969771-19E3-435D-AE55-CFB18F1249EF}". • (Process #5) explorer.exe creates mutex with name "Global\{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #5) explorer.exe creates mutex with name "{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #7) explorer.exe creates mutex with name "Global\{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #7) explorer.exe creates mutex with name "{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}". • (Process #3) explorer.exe creates mutex with name "eahrqgzlvtqtlrmoknrvvoqdzbad".			
1/5	Discovery	Queries Office version	1	-
	• Queries office version via application COM object.			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			
-	Trusted	Known clean file	2	-
	• File "c:\users\rdhj0cnfevzx\appdata\local\temp\~df29dbd0834f02d2ce.tmp" is a known clean file. • File "c:\users\rdhj0cnfevzx\appdata\local\temp\~dfad4a9cdf69cebb65.tmp" is a known clean file.			

Mitre ATT&CK Matrix

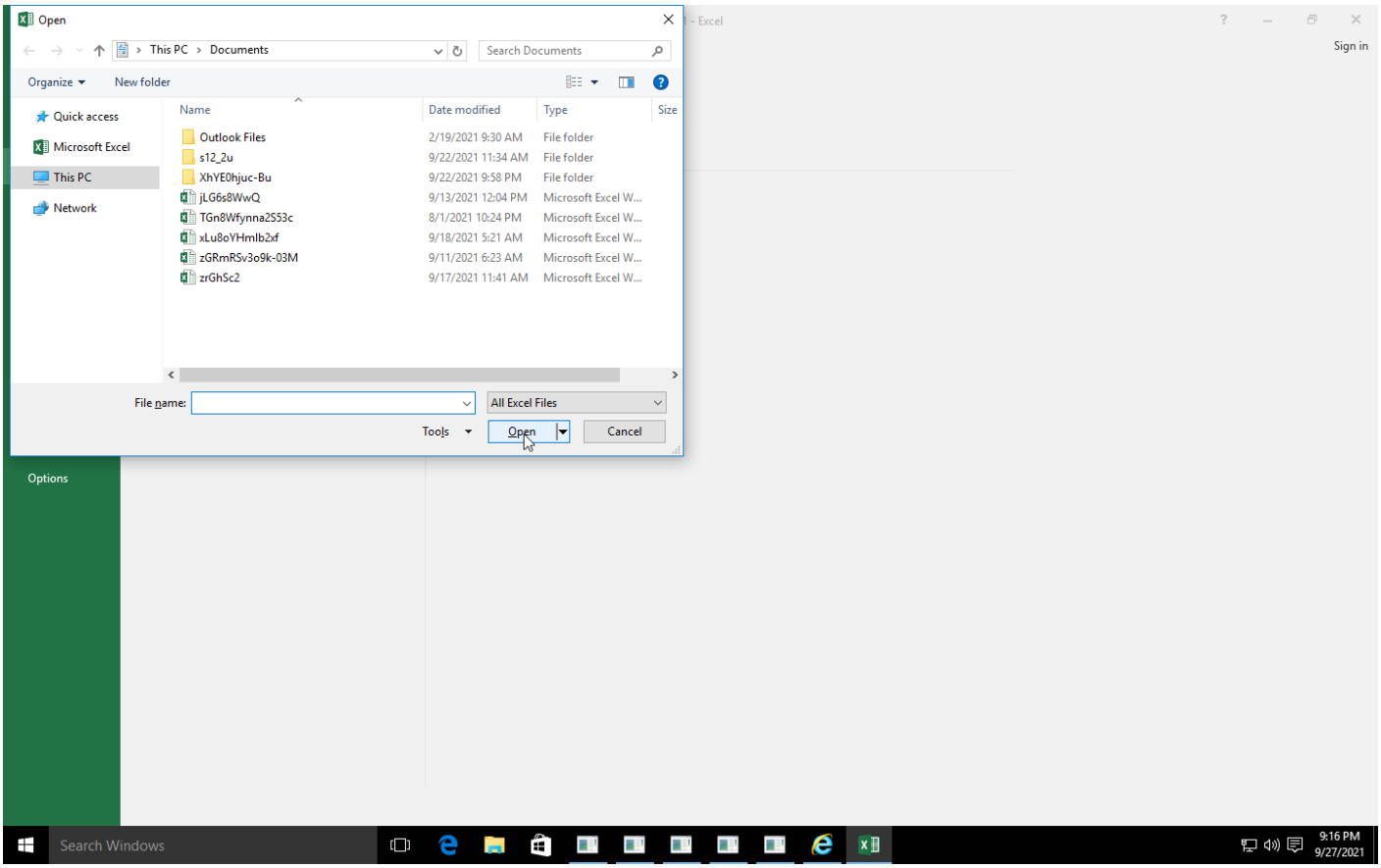
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1064 Scripting	#T1081 Credentials in Files	#T1057 Process Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
	#T1064 Scripting			#T1027 Obfuscated Files or Information		#T1082 System Information Discovery		#T1005 Data from Local System	#T1105 Remote File Copy		
						#T1063 Security Software Discovery			#T1032 Standard Cryptographic Protocol		
						#T1016 System Network Configuration Discovery			#T1065 Uncommonly Used Port		
						#T1083 File and Directory Discovery					

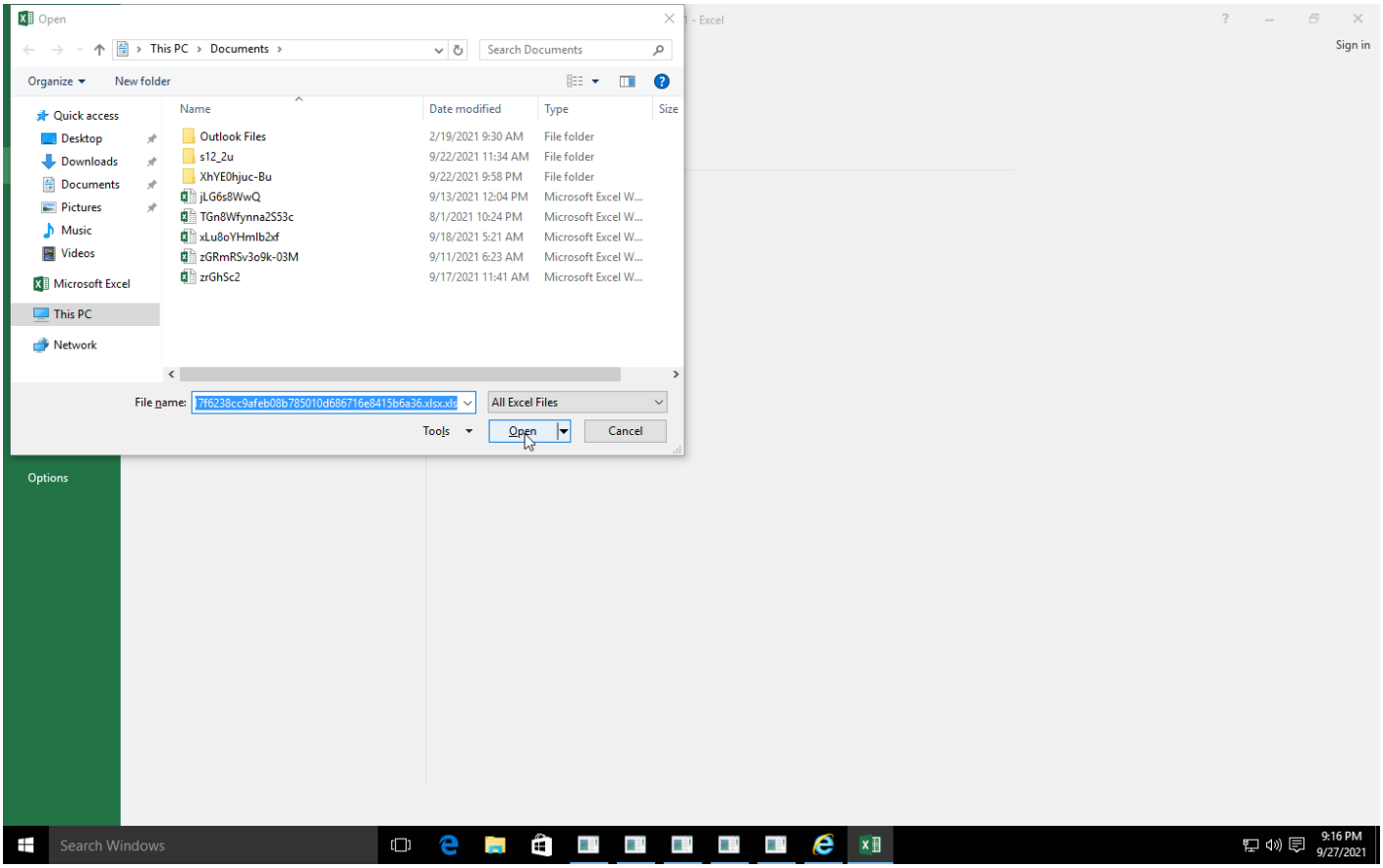
Sample Information

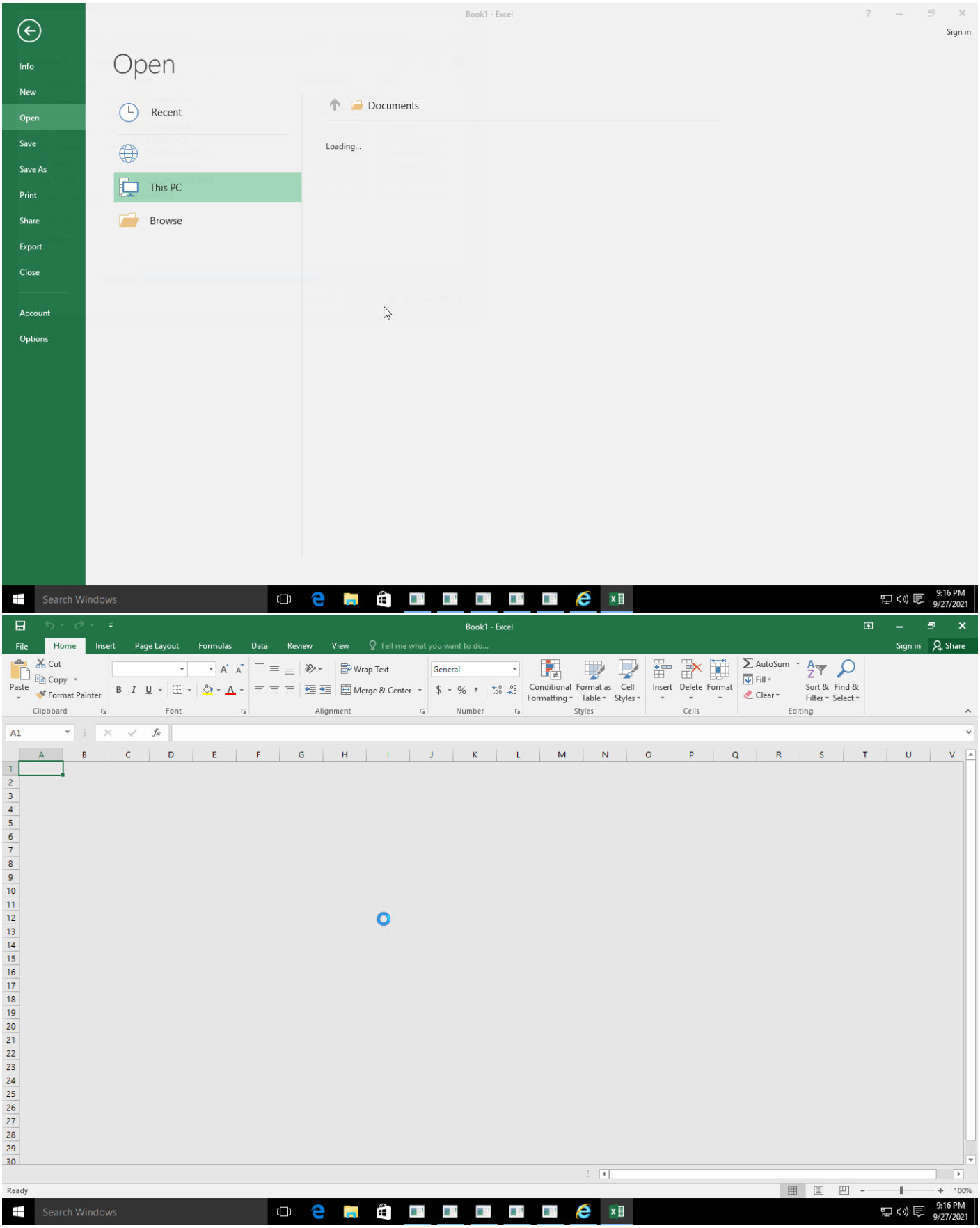
ID	#967595
MD5	b4b3a2223765ac84c9b1b05dbf7c6503
SHA1	57bc35cb0c7a9ac6e7fcb5dea5c211fe5eda5fe0
SHA256	3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36
SSDeep	3072:Cik3hOdsylKlgxopeiBNhZFGzE+cL2kdAnc6YehWfG+tUHKGDbpmsiilBti2JtqV:vk3hOdsylKlgxopeiBNhZF+E+W2kdAnE
File Name	3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls
File Size	126.00 KB
Sample Type	Excel Document
Has Macros	✓

Analysis Information

Creation Time	2021-09-27 23:15 (UTC+2)
Analysis Duration	00:04:07
Termination Reason	Timeout
Number of Monitored Processes	22
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	1
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Open
This PC › Documents
Search Documents
Organize
New folder
Quick access
Microsoft Excel
This PC
Network
Name
Date modified
Type
Size
Outlook Files 2/19/2021 9:30 AM File folder
s12_2u 9/22/2021 11:34 AM File folder
XhYE0hjuc-Bu 9/22/2021 9:58 PM File folder
jLG6s8WwQ 9/13/2021 12:04 PM Microsoft Excel W...
TGn8Wfynna2S53c 8/1/2021 10:24 PM Microsoft Excel W...
xLu8oYHmlb2xf 9/18/2021 5:21 AM Microsoft Excel W...
zGRmRSv3o9k-03M 9/11/2021 6:23 AM Microsoft Excel W...
zrGhSc2 9/17/2021 11:41 AM Microsoft Excel W...
File name:
All Excel Files
Tools
Open
Cancel
Options
Sign in
Search Windows
9:16 PM
9/27/2021


Open
This PC › Documents ›
Search Documents
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
Microsoft Excel
This PC
Network
Name
Date modified
Type
Size
Outlook Files 2/19/2021 9:30 AM File folder
s12_2u 9/22/2021 11:34 AM File folder
XhYE0hjuc-Bu 9/22/2021 9:58 PM File folder
jLG6s8WwQ 9/13/2021 12:04 PM Microsoft Excel W...
TGn8Wfynna2S53c 8/1/2021 10:24 PM Microsoft Excel W...
xLu8oYHmlb2xf 9/18/2021 5:21 AM Microsoft Excel W...
zGRmRSv3o9k-03M 9/11/2021 6:23 AM Microsoft Excel W...
zrGhSc2 9/17/2021 11:41 AM Microsoft Excel W...
File name:
7f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls
All Excel Files
Tools
Open
Cancel
Options
Sign in
Search Windows
9:16 PM
9/27/2021



Screenshots truncated

NETWORK

General

132.28 KB total sent

1229.91 KB total received

4 ports 80, 443, 53, 995

6 contacted IP addresses

3 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

5 URLs contacted, 5 servers

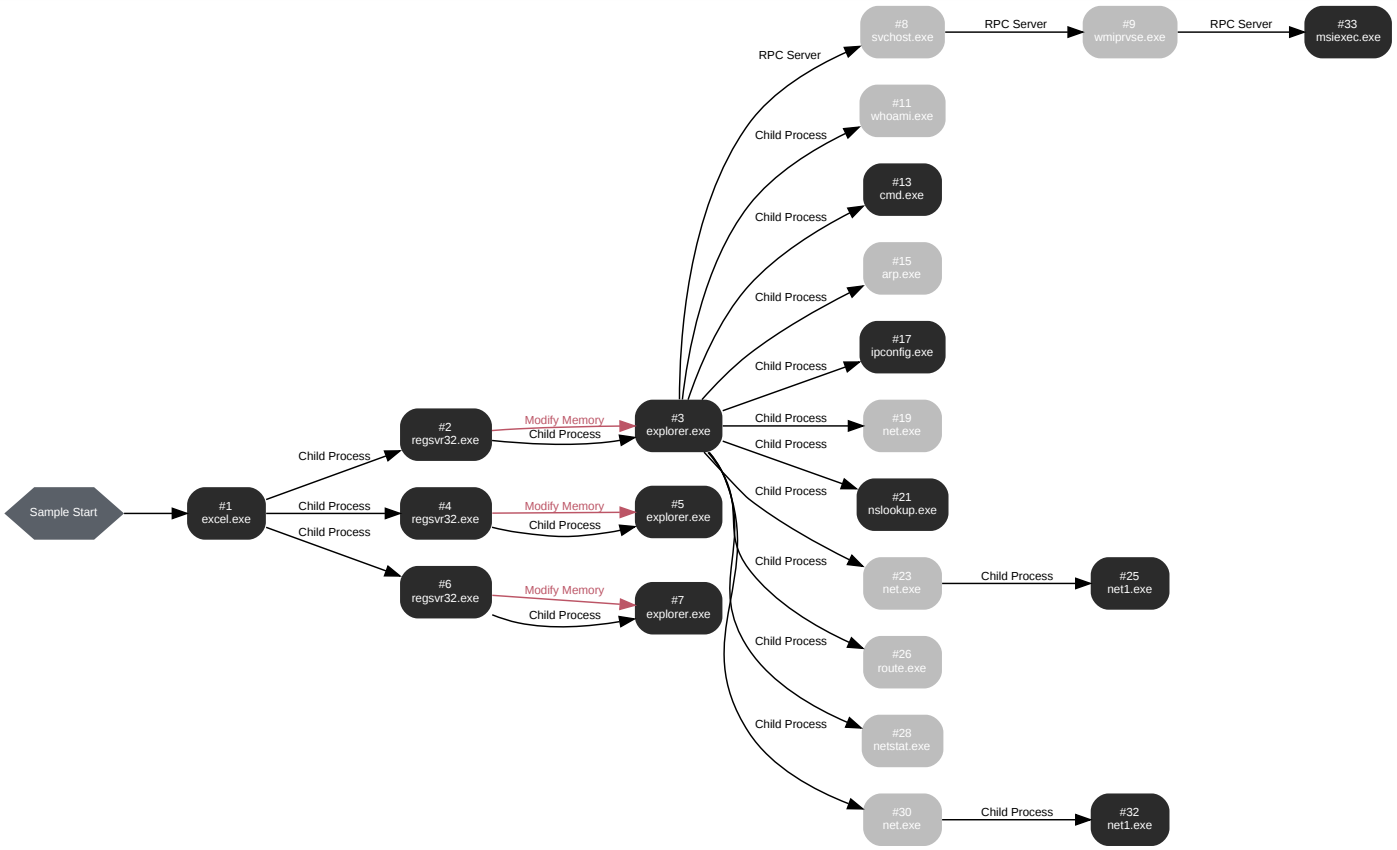
51 sessions, 132.09 KB sent, 1229.57 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://190.14.37.178/44466.8866396991.dat	-	-		0 bytes	NA
GET	http://185.183.96.67/44466.8866396991.dat	-	-		0 bytes	NA
GET	http://185.250.148.213/44466.8866396991.dat	-	-		0 bytes	NA
GET	http://185.183.96.67/	-	-		0 bytes	NA
GET	http://185.250.148.213/	-	-		0 bytes	NA
GET	http://190.14.37.178/	-	-		0 bytes	NA
POST	https://71.74.12.34/t4	-	-		0 bytes	NA
POST	https://120.150.218.241/t4	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: excel.exe

ID	1
File Name	c:\program files (x86)\microsoft office\root\office16\excel.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 57600, Reason: Analysis Target
Unmonitor End Time	End Time: 305504, Reason: Terminated by Timeout
Monitor duration	247.90s
Return Code	Unknown
PID	2924
Parent PID	1636
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Drezd.red	378.00 KB	182cef031bc77e5e5ac38ad2ad27e0eeb926fbba80f01857dfd019242adee5de	✗
-	16.00 KB	4fe7b59af6de3b665b67788cc2f99892ab827efae3a467342b3bb4e3bc8e5bfe	✗
-	512 bytes	076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	✗
C:\Users\RDhJ0CNFevzX\Drezd.red	378.00 KB	42ab0130aea7782ee4f17c64de58d02d5bfa0411abb6366567ba3ef6f16d16a5	✗

Host Behavior

Type	Count
Module	14
Registry	45
Window	37
Keyboard	5
COM	1

Process #2: regsvr32.exe

ID	2
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	regsvr32 -silent ..\Drezd.red
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 92876, Reason: Child Process
Unmonitor End Time	End Time: 106804, Reason: Terminated
Monitor duration	13.93s
Return Code	0
PID	5348
Parent PID	2924
Bitness	32 Bit

Host Behavior

Type	Count
Module	125
Registry	1
-	4
System	14
File	1
Process	116
Environment	4
-	5
-	2
-	1

Process #3: explorer.exe

ID	3
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100676, Reason: Child Process
Unmonitor End Time	End Time: 305504, Reason: Terminated by Timeout
Monitor duration	204.83s
Return Code	Unknown
PID	5368
Parent PID	5348
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\windows\syswow64\regsvr32.exe	0x14f4	0x110000(1114112)	0x21000	✓	1
Modify Memory	#2: c:\windows\syswow64\regsvr32.exe	0x14f4	0x140000(1310720)	0x1ac4	✓	1
Modify Memory	#2: c:\windows\syswow64\regsvr32.exe	0x14f4	0x13d4790(20793232)	0x5	✓	1

Dropped Files (46)

File Name	File Size	SHA256	YARA Match
-	180 bytes	741d79a4b15f920e5a38b7f65b0c451ed28ec6446a6f9bb35c46d2af522af3c9	✗
-	156 bytes	30b53fc3118e12478f2f39da4ba92da8427dc220ad1204456334b013615fa3eb	✗
-	1.16 KB	c76943490d9459d186c4333ce412889d7e5056cf74f5bc70a75ee376f04ca254	✗
-	1.04 KB	f4c311176ad91175d6aa0bf26be00c886e71ca308c150832b3a4afd275191eb8	✗
-	696 bytes	1e394f19b5a12e28cfa740b7adb5fcdef560690fc48146cbb1682e5fe8e1e0d3	✗
-	652 bytes	8df30458f63524cb05d19b8bcc16abe17a66252c6d5a3f7c1ef755f468e59e4d	✗
-	1.14 KB	e69c0209f399c5e28b2c6375800a17ac170e50b81af6c1339439d809e8f4b816	✗
-	908 bytes	5d7b7d44b87cb48121727640ec22cb655e2200d825f8aabdf4a63649f1764e94	✗
-	936 bytes	690aa69da3fc0910ccd1a861f6719f2bea1921f250363682706df67eea274366	✗
-	852 bytes	931d4754f66cd7033f223760ecd3b51bd773478ef40de2cdc7e44f671c5fa15f	✗
-	816 bytes	17587e17d6d62da2664ec62ceffccc0e49ec01f9f2095e43de21fb78ec111951	✗
-	572 bytes	e0feb1830851ac73f28ac5131bf170ff34f5de32efd96d45aae2ade609f8c07b	✗
-	908 bytes	e20ab2c345c8848a2ee7dee3d17c45bb522e22f27ad718ffccbcbd2084c07f3e	✗

File Name	File Size	SHA256	YARA Match
-	940 bytes	54e912c0d0d08fff32c9cbdd981c85c018a9b2dbf3c7526db7e4601e1bf39a6a	✗
-	576 bytes	5e8ed36fd66eafad6283b30ddfee42249eb0cc568c32b134446771104dcacb2b	✗
-	972 bytes	e1c642de1a562436f036844a80eebdfcdf9d52703f6f02993d2d78c4f1289525	✗
-	1.10 KB	1fda3cbf01185b9a045559d1c52a11283f4d095e04243f72491c5008bc92ed41	✗
-	872 bytes	96dfae722a1687b4190e08d5ad6b4dae2dbe335d6d1ddfc40918c0f8007165b8	✗
-	972 bytes	7e1f749b740f33f5a4a7763ce25157fdb841052f40ecb648a2f1ab32a219ea63	✗
-	692 bytes	c7f42acd49fddb1855a619149c633bcde408c62b437e3466e03fe8e4013be9bc	✗
-	576 bytes	389c057654f3d31d5dea75ca25167f1f2837ac019b2804cd923ba0c7adbb2c47	✗
-	880 bytes	6c86156fa85192c752ca66721424dfdfa063b98854690336eda607a68c72f69f	✗
-	1.19 KB	32e5106fee571564dbe7cbf1b858c5d35a5b02764f0ce5202c2549771c21fcf9	✗
-	684 bytes	442caa0905060d24342dbf0e5e1dde8ab8edfcde39f507642840c311d6e37fdd	✗
-	640 bytes	21de40e6d8ed7d606fb3ac5b2bd407143370abb2cc2cbcbc08947db1ec929867	✗
-	872 bytes	2571d2cbdd080283e380d2260a3126d98f154d9e5f8e63415d47c84754c4344e	✗
-	660 bytes	2f4cdf41990890f584db43c487c3c41ac493448285127da480b28f80440372bf	✗
-	1.12 KB	51cf64a1e2c4a6ea218e601d3e4917f97aa800e6ce885e0d3bb8fb77d185a253	✗
-	736 bytes	babb91aa95e8ca5df4c296ec6b5739b420ad457c8d3dfd549c0cd71c5739e9d7	✗
-	944 bytes	17bf116661fe0839884c759952bf971115fc99a900a3125416d50cc1a4263703	✗
-	620 bytes	3c2c5fb0e809713fd7c34287e51483046bb1e3b277d81590310ecb67f12db9ae	✗
-	680 bytes	37c67f1c2c3f15aae5592cf27c42dc0331f2496758dab2193d7e4f7c08b98c78	✗
-	640 bytes	acae48fff5a84e4a1450e69f22901fbef72f7fdd697bcb07201a4e22904cff61	✗
-	740 bytes	fc7092800205440b2ccdadf6a025d70c983a2eeaadfb5997d80199f2390cdb42	✗
-	1.09 KB	08bd9546c1600374b09009115e2545b20ebbcbada5961694580d8ffae9208571	✗
-	680 bytes	c1c1604c67382ee44fd7aef7592eaf4c8bef64e0746342714ab6971ab040a6a8	✗
-	864 bytes	2515413adc270d95080780c9dbd2f30ced49e541f3bd24e4534d988faf45ab95	✗
-	804 bytes	09b6ea31657c6ddf2c54cc6c0c0348e740fae4c87118df9e01992e5d74808a56	✗
-	1.09 KB	537a2ffe5bc774bfdd03c9d8e9062c376ba3c1ba5b723f17ce2e679eef1105fe	✗
-	1.13 KB	62a78d0a2f70c7d3d74f989e0f73d09297d8ff418bbf4edbd47407366fa126a4	✗
-	1.17 KB	760b213ccfd7854f3bddaa847ab739d773d1467fde38a2ab46f7798a3acba653	✗
-	876 bytes	9935ce28bdda01527e072b1a91f54864c3114a7a2c28814108a38e4802b9d6d5	✗

File Name	File Size	SHA256	YARA Match
-	596 bytes	64bfc22c1a60c4422810bc2213d085af70445f7963d465e191e64193d9de99a3	✗
-	604 bytes	1ff04984fa857e8d74161687d62426922212008a5aac8da7a3a2c97c693bcc34	✗
-	1.18 KB	8158f8c518a05abfefebd47f750577a03ec121a633a98d5a00e642e6c7f135f5	✗
-	840 bytes	cac3ccbfb8d040b2f9e7b0f7c5ebcaf85347b65d4b5f38bf8ed3bcae8c67854e	✗

Host Behavior

Type	Count
Module	122
Process	308
System	80115
Registry	14979
File	6875
Mutex	7032
Keyboard	2
-	1
-	355
Window	1
COM	9
-	9

Network Behavior

Type	Count
HTTPS	51
TCP	38

Process #4: regsvr32.exe

ID	4
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	regsvr32 -silent ..\Drezd1.red
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 105560, Reason: Child Process
Unmonitor End Time	End Time: 117498, Reason: Terminated
Monitor duration	11.94s
Return Code	0
PID	5380
Parent PID	2924
Bitness	32 Bit

Host Behavior

Type	Count
Module	125
Registry	1
-	4
System	14
File	1
Process	116
Environment	4
-	5
-	2
-	1

Process #5: explorer.exe

ID	5
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 114368, Reason: Child Process
Unmonitor End Time	End Time: 117498, Reason: Terminated
Monitor duration	3.13s
Return Code	0
PID	5440
Parent PID	5380
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#4: c:\windows\syswow64\regsvr32.exe	0x1524	0x110000(1114112)	0x21000	✓	1
Modify Memory	#4: c:\windows\syswow64\regsvr32.exe	0x1524	0x140000(1310720)	0x1ac4	✓	1
Modify Memory	#4: c:\windows\syswow64\regsvr32.exe	0x1524	0x13d4790(20793232)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	17
Registry	3
File	26
Mutex	2

Process #6: regsvr32.exe

ID	6
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	regsvr32 -silent ..\Drezd2.red
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 116404, Reason: Child Process
Unmonitor End Time	End Time: 126336, Reason: Terminated
Monitor duration	9.93s
Return Code	0
PID	5464
Parent PID	2924
Bitness	32 Bit

Host Behavior

Type	Count
Module	125
Registry	1
-	4
System	14
File	1
Process	118
Environment	4
-	5
-	2
-	1

Process #7: explorer.exe

ID	7
File Name	c:\windows\syswow64\explorer.exe
Command Line	C:\Windows\SysWOW64\explorer.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 120207, Reason: Child Process
Unmonitor End Time	End Time: 126336, Reason: Terminated
Monitor duration	6.13s
Return Code	0
PID	5572
Parent PID	5464
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\windows\syswow64\regsvr32.exe	0x157c	0x110000(1114112)	0x21000	✓	1
Modify Memory	#6: c:\windows\syswow64\regsvr32.exe	0x157c	0x140000(1310720)	0x1ac4	✓	1
Modify Memory	#6: c:\windows\syswow64\regsvr32.exe	0x157c	0x13d4790(20793232)	0x5	✓	1

Host Behavior

Type	Count
Module	113
System	23
Registry	3
File	32
Mutex	2

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 160839, Reason: RPC Server
Unmonitor End Time	End Time: 305504, Reason: Terminated by Timeout
Monitor duration	144.66s
Return Code	Unknown
PID	836
Parent PID	532
Bitness	64 Bit

Process #9: wmiprvse.exe

ID	9
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 160839, Reason: RPC Server
Unmonitor End Time	End Time: 305504, Reason: Terminated by Timeout
Monitor duration	144.66s
Return Code	Unknown
PID	948
Parent PID	628
Bitness	64 Bit

Process #11: whoami.exe

ID	11
File Name	c:\windows\syswow64\whoami.exe
Command Line	whoami /all
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 173036, Reason: Child Process
Unmonitor End Time	End Time: 176897, Reason: Terminated
Monitor duration	3.86s
Return Code	1
PID	1964
Parent PID	5368
Bitness	32 Bit

Process #13: cmd.exe

ID	13
File Name	c:\windows\syswow64\cmd.exe
Command Line	cmd /c set
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 175552, Reason: Child Process
Unmonitor End Time	End Time: 177748, Reason: Terminated
Monitor duration	2.20s
Return Code	0
PID	4564
Parent PID	5368
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	171
Environment	11
System	1

Process #15: arp.exe

ID	15
File Name	c:\windows\syswow64\arp.exe
Command Line	arp -a
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 176630, Reason: Child Process
Unmonitor End Time	End Time: 178718, Reason: Terminated
Monitor duration	2.09s
Return Code	0
PID	4628
Parent PID	5368
Bitness	32 Bit

Process #17: ipconfig.exe

ID	17
File Name	c:\windows\syswow64\ipconfig.exe
Command Line	ipconfig /all
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 177525, Reason: Child Process
Unmonitor End Time	End Time: 179675, Reason: Terminated
Monitor duration	2.15s
Return Code	0
PID	4656
Parent PID	5368
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	128
Environment	43
System	6
Registry	7

Process #19: net.exe

ID	19
File Name	c:\windows\syswow64\net.exe
Command Line	net view /all
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 178470, Reason: Child Process
Unmonitor End Time	End Time: 192601, Reason: Terminated
Monitor duration	14.13s
Return Code	2
PID	4720
Parent PID	5368
Bitness	32 Bit

Process #21: nslookup.exe

ID	21
File Name	c:\windows\syswow64\nslookup.exe
Command Line	nslookup -querytype=ALL -timeout=10 _ldap._tcp.dc._msdcs.WORKGROUP
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 191445, Reason: Child Process
Unmonitor End Time	End Time: 193669, Reason: Terminated
Monitor duration	2.22s
Return Code	0
PID	5764
Parent PID	5368
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Registry	7
System	1
File	5

Network Behavior

Type	Count
UDP	1

Process #23: net.exe

ID	23
File Name	c:\windows\syswow64\net.exe
Command Line	net share
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 192652, Reason: Child Process
Unmonitor End Time	End Time: 194862, Reason: Terminated
Monitor duration	2.21s
Return Code	0
PID	5832
Parent PID	5368
Bitness	32 Bit

Process #25: net1.exe

ID	25
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 share
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193049, Reason: Child Process
Unmonitor End Time	End Time: 194718, Reason: Terminated
Monitor duration	1.67s
Return Code	0
PID	5840
Parent PID	5832
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
File	38
-	3

Process #26: route.exe

ID	26
File Name	c:\windows\syswow64\route.exe
Command Line	route print
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193742, Reason: Child Process
Unmonitor End Time	End Time: 195540, Reason: Terminated
Monitor duration	1.80s
Return Code	0
PID	1200
Parent PID	5368
Bitness	32 Bit

Process #28: netstat.exe

ID	28
File Name	c:\windows\syswow64\netstat.exe
Command Line	netstat -nao
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 194383, Reason: Child Process
Unmonitor End Time	End Time: 196262, Reason: Terminated
Monitor duration	1.88s
Return Code	0
PID	5888
Parent PID	5368
Bitness	32 Bit

Process #30: net.exe

ID	30
File Name	c:\windows\syswow64\net.exe
Command Line	net localgroup
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 195222, Reason: Child Process
Unmonitor End Time	End Time: 197511, Reason: Terminated
Monitor duration	2.29s
Return Code	0
PID	5928
Parent PID	5368
Bitness	32 Bit

Process #32: net1.exe

ID	32
File Name	c:\windows\syswow64\net1.exe
Command Line	C:\Windows\system32\net1 localgroup
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 195722, Reason: Child Process
Unmonitor End Time	End Time: 197158, Reason: Terminated
Monitor duration	1.44s
Return Code	0
PID	2516
Parent PID	5928
Bitness	32 Bit

Dropped Files (1)

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

Host Behavior

Type	Count
Module	3
File	50
User	1

Process #33: msiexec.exe

ID	33
File Name	c:\windows\system32\msiexec.exe
Command Line	C:\Windows\system32\msiexec.exe /V
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 202875, Reason: RPC Server
Unmonitor End Time	End Time: 230246, Reason: Terminated
Monitor duration	27.37s
Return Code	0
PID	6084
Parent PID	532
Bitness	64 Bit

Host Behavior

Type	Count
System	42
Module	77

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36	C:\Users\RDhJ0CNFevzX\Desktop\3982ae3e61a6ba86d61bd8f017f6238cc9afeb08b785010d686716e8415b6a36.xlsx.xls	Sample File	126.00 KB	application/vnd.ms-excel	-	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
4fe7b59af6de3b665b67788cc2f99892ab827efae3a467342b3bb4e3bc8e5bfe	c:\users\rdhj0cnfevzx\appdata\local\temp\~df29dbd0834f02d2ce.tmp	Dropped File	16.00 KB	application/octet-stream	-	CLEAN
076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560	c:\users\rdhj0cnfevzx\appdata\local\temp\~dfad4a9cdf69cebb65.tmp	Dropped File	512 bytes	application/octet-stream	-	CLEAN
741d79a4b15f920e5a38b7f65b0c451ed28ec6446a6f9bb35c46d2af522af3c9	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	180 bytes	text/plain	-	CLEAN
42ab0130aea7782ee4f17c64de58d02d5bfa0411abb6366567ba3ef6f16d16a5	C:\Users\RDhJ0CNFevzX\Drezd1.red, C:\Users\RDhJ0CNFevzX\Drezd.red, C:\Users\RDhJ0CNFevzX\Drezd2.red	Dropped File	378.00 KB	application/vnd.microsoft.portable-executable	Read, Create, Access, Write	CLEAN
30b53fc3118e12478f2f39da4ba92da8427dc220ad1204456334b013615fa3eb	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	156 bytes	text/plain	-	CLEAN
c76943490d9459d186c4333ce412889d7e5056cf74f5bc70a75ee376f04ca254	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.16 KB	text/plain	-	CLEAN
f4c311176ad91175d6aa0bf26be00c886e71ca308c150832b3a4afd275191eb8	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.04 KB	text/plain	-	CLEAN
1e394f19b5a12e28cfa740b7adb5fcdef560690fc48146cbb1682e5fe8e1e0d3	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	696 bytes	text/plain	-	CLEAN
8df30458f63524cb05d19b8bcc16abe17a66252c6d5a3f7c1ef755f468e59e4d	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	652 bytes	text/plain	-	CLEAN
e69c0209f399c5e28b2c6375800a17ac170e50b81af6c1339439d809e8f4b816	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.14 KB	text/plain	-	CLEAN
5d7b7d44b87cb48121727640ec22cb655e2200d825f8aabdf4a63649f1764e94	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	908 bytes	text/plain	-	CLEAN
690aa69da3fc0910ccd1a861f6719f2bea1921f250363682706df67eea274366	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	936 bytes	text/plain	-	CLEAN
931d4754f66cd7033f223760ecd3b51bd773478ef40de2cdc7e44f671c5fa15f	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	852 bytes	text/plain	-	CLEAN
17587e17d6d62da2664ec62ceffccc0e49ec01f9f2095e43de21fb78ec111951	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	816 bytes	text/plain	-	CLEAN
e0feb1830851ac73f28ac5131bf170ff34f5de32efd96d45aae2ade609f8c07b	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	572 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
e20ab2c345c8848a2ee7dee3d17c45bb522e22f27ad718ffccbcbd2084c07f3e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	908 bytes	text/plain	-	CLEAN
54e912c0d0d08fff32c9cbdd981c85c018a9b2dbf3c7526db7e4601e1bf39a6a	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	940 bytes	text/plain	-	CLEAN
5e8ed36fd66eafad6283b30ddfee42249eb0cc568c32b134446771104dcacb2b	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	576 bytes	text/plain	-	CLEAN
e1c642de1a562436f036844a80eebdfcdf9d52703f6f02993d2d78c4f1289525	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	972 bytes	text/plain	-	CLEAN
1fda3cbf01185b9a045559d1c52a11283f4d095e04243f72491c5008bc92ed41	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.10 KB	text/plain	-	CLEAN
96dfae722a1687b4190e08d5ad6b4dae2dbe335d6d1ddfc40918c0f8007165b8	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	872 bytes	text/plain	-	CLEAN
7e1f749b740f33f5a4a7763ce25157fdb841052f40ecb648a2f1ab32a219ea63	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	972 bytes	text/plain	-	CLEAN
c7f42acd49fddb1855a619149c633bcde408c62b437e3466e03fe8e4013be9bc	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	692 bytes	text/plain	-	CLEAN
389c057654f3d31d5dea75ca25167f1f2837ac019b2804cd923ba0c7adbb2c47	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	576 bytes	text/plain	-	CLEAN
6c86156fa85192c752ca66721424dfdfa063b98854690336eda607a68c72f69f	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	880 bytes	text/plain	-	CLEAN
32e5106fee571564dbe7cbf1b858c5d35a5b02764f0ce5202c2549771c21fcf9	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.19 KB	text/plain	-	CLEAN
442caa0905060d24342dbf0e5e1dde8ab8edfcde39f507642840c311d6e37fdd	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	684 bytes	text/plain	-	CLEAN
21de40e6d8ed7d606fb3ac5b2bd407143370abb2cc2cbcbc08947db1ec929867	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	640 bytes	text/plain	-	CLEAN
2571d2cbdd080283e380d2260a3126d98f154d9e5f8e63415d47c84754c4344e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	872 bytes	text/plain	-	CLEAN
2f4cdf41990890f584db43c487c3c41ac493448285127da480b28f80440372bf	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	660 bytes	text/plain	-	CLEAN
51cf64a1e2c4a6ea218e601d3e4917f97aa800e6ce885e0d3bb8fb77d185a253	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.12 KB	text/plain	-	CLEAN
babb91aa95e8ca5df4c296ec6b5739b420ad457c8d3dfd549c0cd71c5739e9d7	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	736 bytes	text/plain	-	CLEAN
17bf116661fe0839884c759952bf971115fc99a900a3125416d50cc1a4263703	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	944 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3c2c5fb0e809713fd7c34287e51483046bb1e3b277d81590310ecb67f12db9ae	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	620 bytes	text/plain	-	CLEAN
37c67f1c2c3f15aae5592cf27c42dc0331f2496758dab2193d7e4f7c08b98c78	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	680 bytes	text/plain	-	CLEAN
acae48fff5a84e4a1450e69f22901fbef72f7fdd697bcb07201a4e22904cff61	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	640 bytes	text/plain	-	CLEAN
fc7092800205440b2ccdadf6a025d70c983a2eeaadfb5997d80199f2390cdb42	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	740 bytes	text/plain	-	CLEAN
08bd9546c1600374b09009115e2545b20ebbcbada5961694580d8ffae9208571	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.09 KB	text/plain	-	CLEAN
c1c1604c67382ee44fd7aef7592eaf4c8bef64e0746342714ab6971ab040a6a8	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	680 bytes	text/plain	-	CLEAN
2515413adc270d95080780c9dbd2f30ced49e541f3bd24e4534d988faf45ab95	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	864 bytes	text/plain	-	CLEAN
09b6ea31657c6ddf2c54cc6c0c0348e740fae4c87118df9e01992e5d74808a56	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	804 bytes	text/plain	-	CLEAN
537a2ffe5bc774bfdd03c9d8e9062c376ba3c1ba5b723f17ce2e679eef1105fe	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.09 KB	text/plain	-	CLEAN
62a78d0a2f70c7d3d74f989e0f73d09297d8ff418bbf4edbd47407366fa126a4	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.13 KB	text/plain	-	CLEAN
760b213ccfd7854f3bddaa847ab739d773d1467fde38a2ab46f7798a3acba653	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.17 KB	text/plain	-	CLEAN
9935ce28bdda01527e072b1a91f54864c3114a7a2c28814108a38e4802b9d6d5	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	876 bytes	text/plain	-	CLEAN
64bfc22c1a60c4422810bc2213d085af70445f7963d465e191e64193d9de99a3	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	596 bytes	text/plain	-	CLEAN
1ff04984fa857e8d74161687d62426922212008a5aac8da7a3a2c97c693bcc34	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	604 bytes	text/plain	-	CLEAN
8158f8c518a05abfefebd47f750577a03ec121a633a98d5a00e642e6c7f135f5	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	1.18 KB	text/plain	-	CLEAN
cac3ccbfb8d040b2f9e7b0f7c5ebcaf85347b65d4b5f38bf8ed3bcae8c67854e	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\hztfec57\t4[1]	Dropped File	840 bytes	text/plain	-	CLEAN
182cef031bc77e5e5ac38ad2ad27e0eeb926fbba80f01857dfd019242adee5de	C:\Users\RDhJ0CNFevzX\Drezd1.red, C:\Users\RDhJ0CNFevzX\Drezd.red, 44466.8866396991.dat, C:\Users\RDhJ0CNFevzX\Drezd2.red	Downloaded File	378.00 KB	application/vnd.microsoft.portable-executable	Read, Create, Access, Write	CLEAN
d30b441ab0e88a1487f29a80d63e2a4865a3f5df7854fb8359b354397f807e2c	0.JPG	Embedded File	83.67 KB	image/jpeg	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Drezd.red	Downloaded File, Dropped File	Read, Create, Access, Write	CLEAN
C:\INTERNAL__empty	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\regsvr32.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\explorer.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\amstream.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDhJ0CNFevzX\Drezd.red.cfg	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\lkuqna	Accessed File	Create, Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\lkuqna\tozrlqis.mdj	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Drezd1.red	Downloaded File, Dropped File	Read, Create, Access, Write	CLEAN
C:\Users\RDhJ0CNFevzX\Drezd2.red	Downloaded File, Dropped File	Read, Create, Access, Write	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\net1.exe	Accessed File	Access	CLEAN
c:\hiberfil.sysss	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\lkuqna\cfdircmne32.dll	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\lkuqna\fdircmne32.dll	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://71.74.12.34/t4	-	71.74.12.34	-	POST	MALICIOUS
https://120.150.218.241/t4	-	120.150.218.241	-	POST	MALICIOUS
http://190.14.37.178/44466.8866396991.dat	-	190.14.37.178	-	GET	CLEAN
http://185.183.96.67/44466.8866396991.dat	-	185.183.96.67	-	GET	CLEAN
http://185.250.148.213/44466.8866396991.dat	-	185.250.148.213	-	GET	CLEAN
http://185.183.96.67	-	-	-	GET	CLEAN
http://185.250.148.213	-	-	-	GET	CLEAN
http://190.14.37.178	-	-	-	GET	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
120.150.218.241	-	Australia	TLS, TCP	MALICIOUS
192.168.0.1	-	-	DNS, UDP	CLEAN
71.74.12.34	-	United States	HTTP, TCP	CLEAN
185.250.148.213	-	Moldova	HTTP, TCP	CLEAN
185.183.96.67	-	Netherlands	HTTP, TCP	CLEAN

IP Address	Domains	Country	Protocols	Verdict
190.14.37.178	-	Panama	HTTP, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Global\{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}	access	explorer.exe	CLEAN
{DE3A2553-AB1B-4C85-9686-F3F136EBACE2}	access	explorer.exe	CLEAN
{61969771-19E3-435D-AE55-CFB18F1249EF}	access	explorer.exe	CLEAN
eahrqgzlvtqtlrmoknrvvoqdzbad	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\MdiMaximized	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\GridWidth	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\GridHeight	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ShowGrid	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\AlignToGrid	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\SaveBeforeRun	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ShowToolTips	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\CollapseWindows	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\UpgradeVBX	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ReadOnlyMode	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\BackgroundProjectLoad	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\FolderView	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Tool	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\PropertiesWindow	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\UI	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Dock	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\VBE\6.0\Addins	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\Designers	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\ToolboxControls	access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\CtlsShowSelected	read, access	excel.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\DsnShowSelected	read, access	excel.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common\MainWindow	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\Clsid\{C62A69F0-16DC-11CE-9E98-00AA00574A4F}\Instance CLSID	read, access	excel.exe	CLEAN
HKEY_CLASSES_ROOT\.red	access	regsvr32.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey	create, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\abb28c95	read, access, write	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1560258661-3990802383-1811730007-1000	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1560258661-3990802383-1811730007-1000\ProfileImagePath	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\9e2d5cdb	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\a9f3ace9	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\114fcb8c	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\6c478406	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\d4fbe363	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\59d85448	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\130eebf0	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\e164332d	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\e3251351	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\3665b42c	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\2caa5c0b	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\3e1ff3e5	read, access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\f3d19cc3	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}\Dhcpv6ClassId	read, access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{E25A642B-6CEB-4194-8F83-8BC82AF94F5A}\DhcpClassId	read, access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}\Dhcpv6ClassId	read, access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{C2998852-8A8B-426B-AAB1-8880E47F8B1A}	access	ipconfig.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters	access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DNSLookupOrder	read, access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Domain	read, access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DhcpDomain	read, access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\DNSClient	access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SearchList	read, access	nslookup.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DhcpSearchList	read, access	nslookup.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\3fa6462	read, access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Fdircmnenyyey\4317bc6f	access, write	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
regsvr32.exe	regsvr32 -silent ..\Drezd.red	SUSPICIOUS
explorer.exe	C:\Windows\SysWOW64\explorer.exe	SUSPICIOUS
regsvr32.exe	regsvr32 -silent ..\Drezd1.red	SUSPICIOUS
regsvr32.exe	regsvr32 -silent ..\Drezd2.red	SUSPICIOUS
ipconfig.exe	ipconfig /all	SUSPICIOUS
excel.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\EXCEL.EXE"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -Embedding	CLEAN
whoami.exe	whoami /all	CLEAN
cmd.exe	cmd /c set	CLEAN
arp.exe	arp -a	CLEAN
net.exe	net view /all	CLEAN
nslookup.exe	nslookup -querytype=ALL -timeout=10 _ldap._tcp.dc._msdcs.WORKGROUP	CLEAN
net.exe	net share	CLEAN
net1.exe	C:\Windows\system32\net1 share	CLEAN
route.exe	route print	CLEAN
netstat.exe	netstat -nao	CLEAN
net.exe	net localgroup	CLEAN
net1.exe	C:\Windows\system32\net1 localgroup	CLEAN
msiexec.exe	C:\Windows\system32\msiexec.exe /V	CLEAN

YARA / AV

Antivirus (1)

File Type	Threat Name	File Name	Verdict
Memory Dump	Gen:Variant.Bulz.604474	-	MALICIOUS

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 18:53:08+00:00
Built-in AV Database Records	10474020

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