MALICIOUS

Classifications: Spyware

Threat Names: Trojan.GenericKDZ.76753 Gen:Variant.Mikey.113998

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll**
ID	#2782965
MD5	718a7d9b1fe55a72cfa586e869236df8
SHA1	5d870aeb7951ab6af0900ba837924f79e3716936
SHA256	d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222
File Size	1192.00 KB
Report Created	2021-09-28 14:23 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 168 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	5	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) xauypj.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #10) xauypj.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #15) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #59) xauypj.exe as "Gen:Variant.Mikey.113998".			
4/5	Injection	Modifies control flow of another process	4	-
	• (Process #2) xauypj.exe alters context of (process #15) explorer.exe. • (Process #11) xauypj.exe alters context of (process #15) explorer.exe. • (Process #19) xauypj.exe alters context of (process #15) explorer.exe. • (Process #43) xauypj.exe alters context of (process #56) explorer.exe.			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #56) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #56) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #15) explorer.exe creates a new explorer.exe process.			
1/5	Discovery	Reads system data	43	-

Score	Category	Operation	Count	Classification
		• (Process #2) xauypj.exe reads the Windows installation date from registry. • (Process #3) xauypj.exe reads the Windows installation date from registry. • (Process #4) xauypj.exe reads the Windows installation date from registry. • (Process #5) xauypj.exe reads the Windows installation date from registry. • (Process #6) xauypj.exe reads the Windows installation date from registry. • (Process #7) xauypj.exe reads the Windows installation date from registry. • (Process #12) xauypj.exe reads the Windows installation date from registry. • (Process #8) xauypj.exe reads the Windows installation date from registry. • (Process #9) xauypj.exe reads the Windows installation date from registry. • (Process #10) xauypj.exe reads the Windows installation date from registry. • (Process #11) xauypj.exe reads the Windows installation date from registry. • (Process #13) xauypj.exe reads the Windows installation date from registry. • (Process #16) xauypj.exe reads the Windows installation date from registry. • (Process #14) xauypj.exe reads the Windows installation date from registry. • (Process #19) xauypj.exe reads the Windows installation date from registry. • (Process #22) xauypj.exe reads the Windows installation date from registry. • (Process #23) xauypj.exe reads the Windows installation date from registry. • (Process #24) xauypj.exe reads the Windows installation date from registry. • (Process #25) xauypj.exe reads the Windows installation date from registry. • (Process #28) xauypj.exe reads the Windows installation date from registry. • (Process #29) xauypj.exe reads the Windows installation date from registry. • (Process #30) xauypj.exe reads the Windows installation date from registry. • (Process #31) xauypj.exe reads the Windows installation date from registry. • (Process #32) xauypj.exe reads the Windows installation date from registry. • (Process #33) xauypj.exe reads the Windows installation date from registry. • (Process #34) xauypj.exe reads the Windows installation date from registry. • (Process #35) xauypj.exe reads the Windows installation date from registry. • (Process #36) xauypj.exe reads the Windows installation date from registry. • (Process #37) xauypj.exe reads the Windows installation date from registry. • (Process #38) xauypj.exe reads the Windows installation date from registry. • (Process #43) xauypj.exe reads the Windows installation date from registry. • (Process #39) xauypj.exe reads the Windows installation date from registry. • (Process #40) xauypj.exe reads the Windows installation date from registry. • (Process #41) xauypj.exe reads the Windows installation date from registry. • (Process #42) xauypj.exe reads the Windows installation date from registry. • (Process #44) xauypj.exe reads the Windows installation date from registry. • (Process #45) xauypj.exe reads the Windows installation date from registry. • (Process #48) xauypj.exe reads the Windows installation date from registry. • (Process #51) xauypj.exe reads the Windows installation date from registry. • (Process #54) xauypj.exe reads the Windows installation date from registry. • (Process #57) xauypj.exe reads the Windows installation date from registry. • (Process #55) xauypj.exe reads the Windows installation date from registry. • (Process #56) explorer.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	100	-

- (Process #2) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #3) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #4) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) xauypj.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #5) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #12) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #8) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #9) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #10) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #11) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #11) xauypj.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #13) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #16) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #14) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #19) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #22) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #19) xauypj.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #23) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #24) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #25) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #28) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #29) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #30) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #31) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #32) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #34) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #35) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #36) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #37) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #37) xauypj.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #38) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #43) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #38) xauypj.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #39) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #40) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #43) xauypj.exe creates mutex with name "{450ae42e-11c4-9ab5-80d0-f9ecd98a92e9}".
- (Process #41) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #42) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #44) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #45) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #48) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #51) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #54) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #57) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #55) xauypj.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #56) explorer.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #56) explorer.exe creates mutex with name "{298ddcca-efe5-2f07-cbb5-e91e37797537}".
- (Process #56) explorer.exe creates mutex with name "{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}".
- (Process #56) explorer.exe creates mutex with name "{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}".
- (Process #56) explorer.exe creates mutex with name "{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}".
- (Process #56) explorer.exe creates mutex with name "{3efe96e0-aada-6cdc-4854-db5a860aa498}".
- (Process #56) explorer.exe creates mutex with name "{9ffb2102-4ed7-3d87-65ab-805271e438f1}".
- (Process #56) explorer.exe creates mutex with name "{1dda5c84-234c-9dac-e365-31fdf4838be5}".
- (Process #56) explorer.exe creates mutex with name "{42099d9a-d7ef-cbfd-f97f-f2a010acb178}".
- (Process #56) explorer.exe creates mutex with name "{1ea4e5de-7907-947c-5f34-31aa5165b0ee}".
- (Process #56) explorer.exe creates mutex with name "{5bffd7b8-454a-d897-55b3-ba9b73e0f7e8}".
- (Process #56) explorer.exe creates mutex with name "{7ba3817f-aeba-298a-7847-ab3c2bff153d}".
- (Process #56) explorer.exe creates mutex with name "{be62f0b1-7f97-55e-d089-c80cc59559bf}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	5	-

- (Process #2) xauypj.exe reads from (process #15) explorer.exe.
- (Process #11) xauypj.exe reads from (process #15) explorer.exe.
- (Process #19) xauypj.exe reads from (process #15) explorer.exe.
- (Process #43) xauypj.exe reads from (process #56) explorer.exe.
- (Process #55) xauypj.exe reads from (process #56) explorer.exe.

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	2	-

- (Process #15) explorer.exe resolves 25 API functions by name.
- (Process #56) explorer.exe resolves 26 API functions by name.

Score	Category	Operation	Count	Classification
1/5	Crash	A monitored process crashed	5	-

- (Process #15) explorer.exe crashed.
- (Process #11) xauypj.exe crashed.
- (Process #19) xauypj.exe crashed.
- (Process #37) xauypj.exe crashed.
- (Process #38) xauypj.exe crashed.

Mitre ATT&CK Matrix

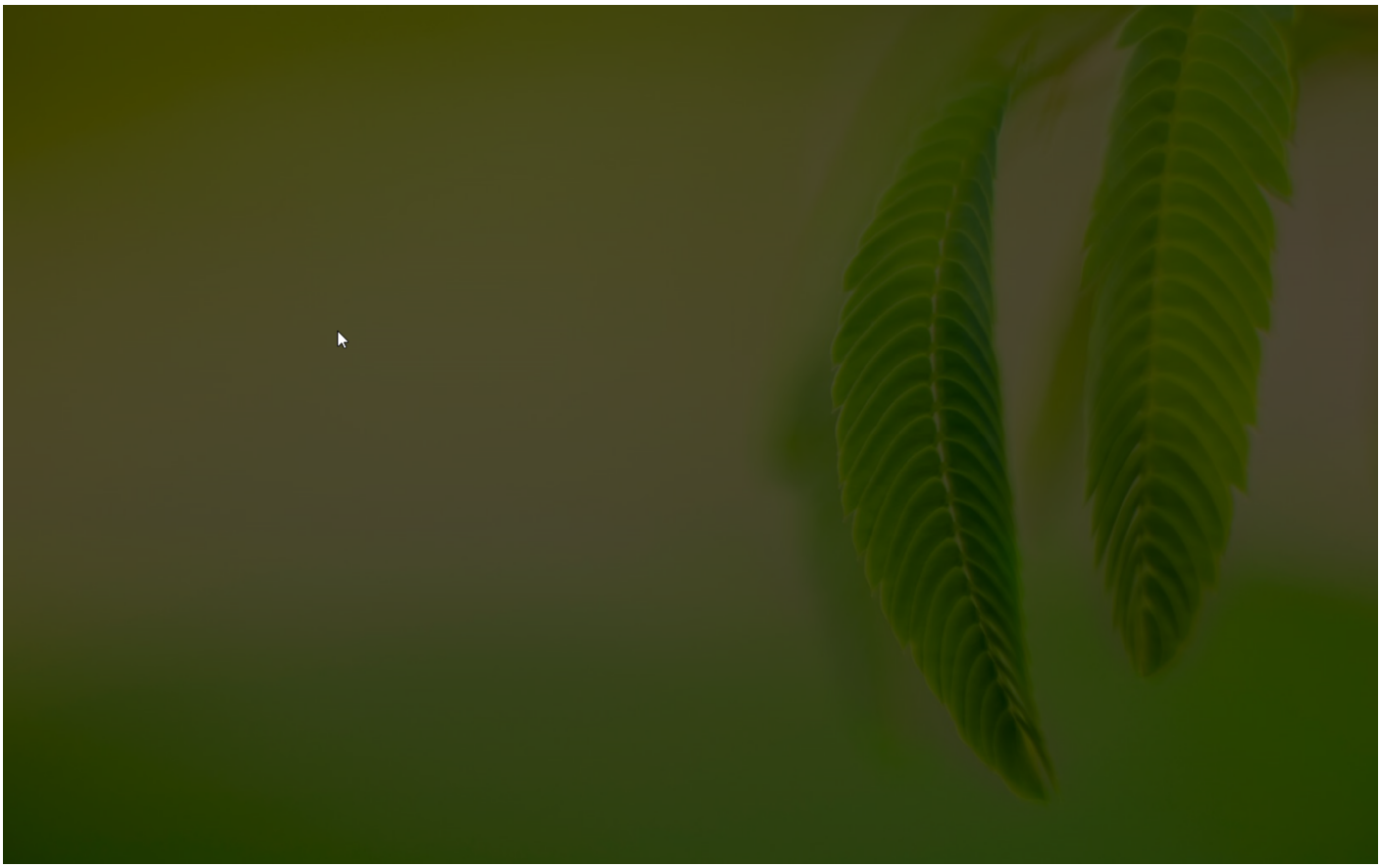
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
						#T1012 Query Registry		#T1005 Data from Local System			
						#T1083 File and Directory Discovery					

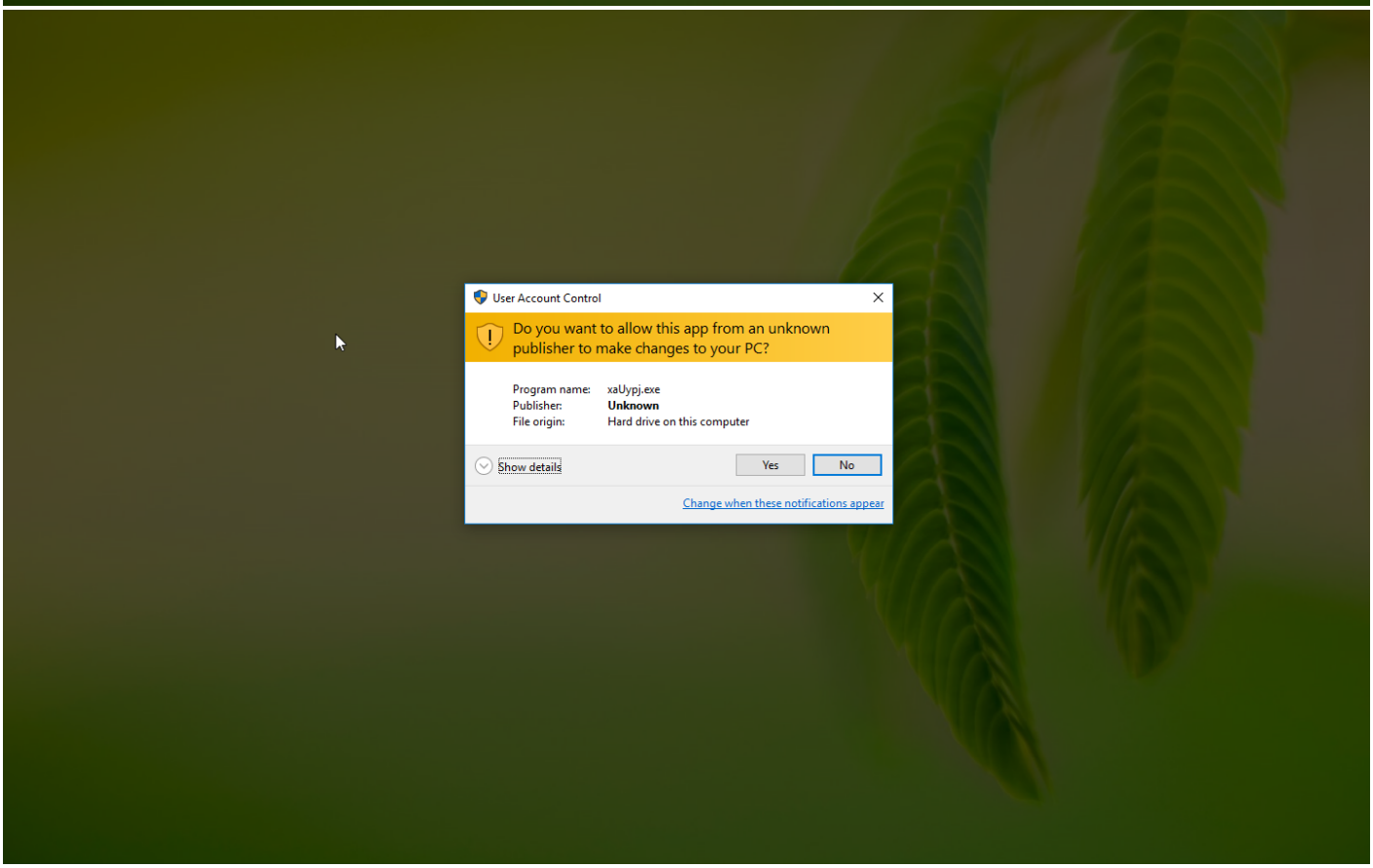
Sample Information

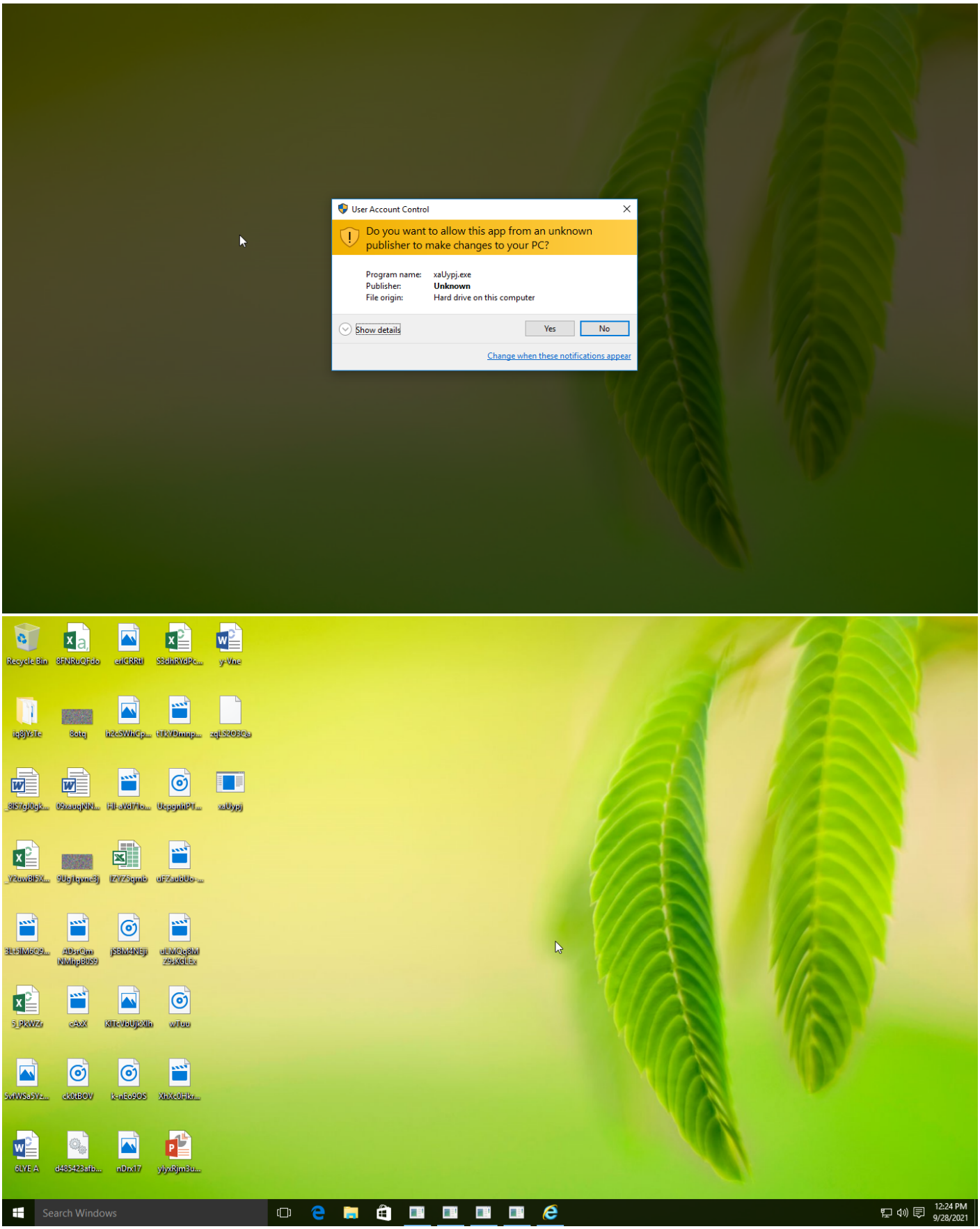
ID	#2782965
MD5	718a7d9b1fe55a72cfa586e869236df8
SHA1	5d870aeb7951ab6af0900ba837924f79e3716936
SHA256	d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222
SSDeep	12288:0Vl0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:xfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll
File Size	1192.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:23 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	60
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	5
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0




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



Screenshots truncated

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

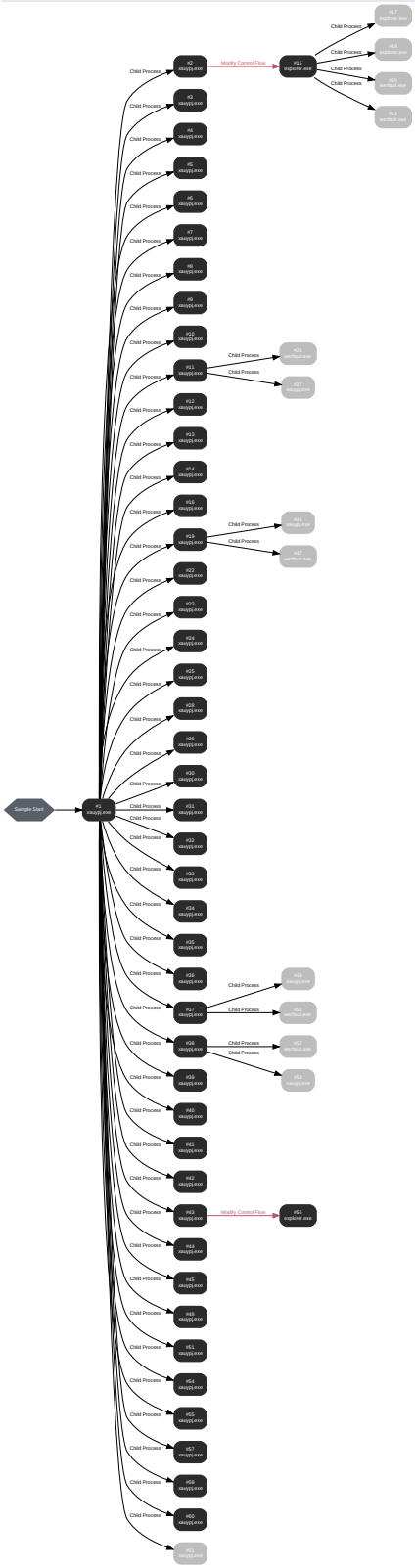
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: xauypj.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmppy3pshh5" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72289, Reason: Analysis Target
Unmonitor End Time	End Time: 321729, Reason: Terminated by Timeout
Monitor duration	249.44s
Return Code	Unknown
PID	1164
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	45

Process #2: xauypj.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=IsInteractiveUserSession
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94793, Reason: Child Process
Unmonitor End Time	End Time: 165955, Reason: Terminated
Monitor duration	71.16s
Return Code	0
PID	2532
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	35
Environment	2
Registry	789
Mutex	6
Process	2
-	59
-	32
-	142

Process #3: xauypj.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=QueryActiveSession
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 97356, Reason: Child Process
Unmonitor End Time	End Time: 126323, Reason: Terminated
Monitor duration	28.97s
Return Code	0
PID	1980
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #4: xauypj.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=QueryUserToken
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 99157, Reason: Child Process
Unmonitor End Time	End Time: 133112, Reason: Terminated
Monitor duration	33.95s
Return Code	0
PID	3716
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #5: xauypj.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=RegisterUsertokenForNoWinlogon
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 101343, Reason: Child Process
Unmonitor End Time	End Time: 134898, Reason: Terminated
Monitor duration	33.55s
Return Code	0
PID	1288
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #6: xauypj.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSCloseServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 104635, Reason: Child Process
Unmonitor End Time	End Time: 138939, Reason: Terminated
Monitor duration	34.30s
Return Code	0
PID	4872
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #7: xauypj.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSConnectSessionA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109249, Reason: Child Process
Unmonitor End Time	End Time: 147798, Reason: Terminated
Monitor duration	38.55s
Return Code	0
PID	1300
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #8: xauypj.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSConnectSessionW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 115268, Reason: Child Process
Unmonitor End Time	End Time: 153335, Reason: Terminated
Monitor duration	38.07s
Return Code	0
PID	4928
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #9: xauypj.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSCreateListenerA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119488, Reason: Child Process
Unmonitor End Time	End Time: 155182, Reason: Terminated
Monitor duration	35.69s
Return Code	0
PID	3788
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #10: xauypj.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSCreateListenerW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 123005, Reason: Child Process
Unmonitor End Time	End Time: 164775, Reason: Terminated
Monitor duration	41.77s
Return Code	0
PID	552
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #11: xauypj.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSDisconnectSession
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 127650, Reason: Child Process
Unmonitor End Time	End Time: 205181, Reason: Crashed
Monitor duration	77.53s
Return Code	1114
PID	1752
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	767
Mutex	6
Process	2
-	60
-	1
-	116
Window	1

Process #12: xauypj.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnableChildSessions
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 132268, Reason: Child Process
Unmonitor End Time	End Time: 150915, Reason: Terminated
Monitor duration	18.65s
Return Code	0
PID	3364
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #13: xauypj.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateListenersA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 137548, Reason: Child Process
Unmonitor End Time	End Time: 174584, Reason: Terminated
Monitor duration	37.04s
Return Code	0
PID	1188
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	785
Mutex	7

Process #14: xauypj.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateListenersW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 142549, Reason: Child Process
Unmonitor End Time	End Time: 180084, Reason: Terminated
Monitor duration	37.53s
Return Code	0
PID	2968
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #15: explorer.exe

ID	15
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 142858, Reason: Injection
Unmonitor End Time	End Time: 237122, Reason: Crashed
Monitor duration	94.26s
Return Code	3221225477
PID	1600
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (150)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xe38	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xe7c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xf28	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xfac	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xc34	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xc24	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x864	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xb2c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x494	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xb4c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x238	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x6e4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xcd0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x398	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x560	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x5c0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0xce8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x1030	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x10bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x10d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x12e0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x1368	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x137c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x138c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x1394	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x13b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x13f8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb28bab580(140716696843648)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xb28 / 0x684	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xe38	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xe7c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xf28	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xfac	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xc34	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xc24	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x864	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xb2c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x494	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xb4c	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x238	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x6e4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xcd0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x398	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x560	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x5c0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xce8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x1030	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x10bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x10d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x12e0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x1368	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x137c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x138c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x1394	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x13b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0x13f8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#11: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x894 / 0xc38	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#19: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0xffc / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1

Host Behavior

Type	Count
Module	40
File	109
System	2
Registry	322

Process #16: xauypj.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 151691, Reason: Child Process
Unmonitor End Time	End Time: 174639, Reason: Terminated
Monitor duration	22.95s
Return Code	0
PID	4936
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	775
Mutex	7

Process #17: explorer.exe

ID	17
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 158905, Reason: Child Process
Unmonitor End Time	End Time: 234678, Reason: Terminated
Monitor duration	75.77s
Return Code	259
PID	1872
Parent PID	1600
Bitness	64 Bit

Process #18: explorer.exe

ID	18
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 161899, Reason: Child Process
Unmonitor End Time	End Time: 226448, Reason: Terminated
Monitor duration	64.55s
Return Code	259
PID	4048
Parent PID	1600
Bitness	64 Bit

Process #19: xauypj.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesExA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 164358, Reason: Child Process
Unmonitor End Time	End Time: 253877, Reason: Crashed
Monitor duration	89.52s
Return Code	1114
PID	4956
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	35
Environment	2
Registry	766
Mutex	6
Process	2
-	60
-	32
-	144
Window	1

Process #20: werfault.exe

ID	20
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1600 -s 5804
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 164585, Reason: Child Process
Unmonitor End Time	End Time: 190551, Reason: Terminated
Monitor duration	25.97s
Return Code	0
PID	4764
Parent PID	1600
Bitness	64 Bit

Process #21: werfault.exe

ID	21
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1600 -s 2352
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 164875, Reason: Child Process
Unmonitor End Time	End Time: 226289, Reason: Terminated
Monitor duration	61.41s
Return Code	0
PID	4952
Parent PID	1600
Bitness	64 Bit

Process #22: xauypj.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesExW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 171910, Reason: Child Process
Unmonitor End Time	End Time: 193041, Reason: Terminated
Monitor duration	21.13s
Return Code	0
PID	2300
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #23: xauypj.exe

ID	23
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 173909, Reason: Child Process
Unmonitor End Time	End Time: 197942, Reason: Terminated
Monitor duration	24.03s
Return Code	0
PID	4912
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #24: xauypj.exe

ID	24
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateServersA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 176318, Reason: Child Process
Unmonitor End Time	End Time: 200378, Reason: Terminated
Monitor duration	24.06s
Return Code	0
PID	916
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	774
Mutex	7

Process #25: xauypj.exe

ID	25
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateServersW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 180486, Reason: Child Process
Unmonitor End Time	End Time: 205557, Reason: Terminated
Monitor duration	25.07s
Return Code	0
PID	4088
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #26: werfault.exe

ID	26
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1752 -s 700
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 182342, Reason: Child Process
Unmonitor End Time	End Time: 200421, Reason: Terminated
Monitor duration	18.08s
Return Code	0
PID	328
Parent PID	1752
Bitness	64 Bit

Process #27: xauypj.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSDisconnectSession
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 182582, Reason: Child Process
Unmonitor End Time	End Time: 200470, Reason: Terminated
Monitor duration	17.89s
Return Code	259
PID	4848
Parent PID	1752
Bitness	64 Bit

Process #28: xauypj.exe

ID	28
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183462, Reason: Child Process
Unmonitor End Time	End Time: 209464, Reason: Terminated
Monitor duration	26.00s
Return Code	0
PID	4156
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #29: xauypj.exe

ID	29
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsExA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186330, Reason: Child Process
Unmonitor End Time	End Time: 212714, Reason: Terminated
Monitor duration	26.38s
Return Code	0
PID	4248
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #30: xauypj.exe

ID	30
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsExW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 188543, Reason: Child Process
Unmonitor End Time	End Time: 213260, Reason: Terminated
Monitor duration	24.72s
Return Code	0
PID	4312
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #31: xauypj.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 191270, Reason: Child Process
Unmonitor End Time	End Time: 215564, Reason: Terminated
Monitor duration	24.29s
Return Code	0
PID	4408
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #32: xauypj.exe

ID	32
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSFreeMemory
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193765, Reason: Child Process
Unmonitor End Time	End Time: 216317, Reason: Terminated
Monitor duration	22.55s
Return Code	0
PID	4448
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	768
Mutex	7

Process #33: xauypj.exe

ID	33
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSFreeMemoryExA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 195661, Reason: Child Process
Unmonitor End Time	End Time: 217242, Reason: Terminated
Monitor duration	21.58s
Return Code	0
PID	4484
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	8

Process #34: xauypj.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSFreeMemoryExW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 199896, Reason: Child Process
Unmonitor End Time	End Time: 220412, Reason: Terminated
Monitor duration	20.52s
Return Code	0
PID	4576
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	779
Mutex	7

Process #35: xauypj.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSGetChildSessionId
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 204965, Reason: Child Process
Unmonitor End Time	End Time: 225188, Reason: Terminated
Monitor duration	20.22s
Return Code	0
PID	4616
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #36: xauypj.exe

ID	36
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSGetListenerSecurityA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 208253, Reason: Child Process
Unmonitor End Time	End Time: 229222, Reason: Terminated
Monitor duration	20.97s
Return Code	0
PID	4708
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #37: xauypj.exe

ID	37
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSGetListenerSecurityW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 211894, Reason: Child Process
Unmonitor End Time	End Time: 254324, Reason: Crashed
Monitor duration	42.43s
Return Code	1114
PID	4796
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	33
File	117
System	6
Environment	2
Registry	778
Mutex	6
Process	1
Window	1

Process #38: xauypj.exe

ID	38
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSIsChildSessionsEnabled
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 214870, Reason: Child Process
Unmonitor End Time	End Time: 258220, Reason: Crashed
Monitor duration	43.35s
Return Code	1114
PID	3784
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	33
File	117
System	6
Environment	2
Registry	786
Mutex	6
Process	1
Window	1

Process #39: xauypj.exe

ID	39
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSLogoffSession
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 217873, Reason: Child Process
Unmonitor End Time	End Time: 242033, Reason: Terminated
Monitor duration	24.16s
Return Code	0
PID	3300
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #40: xauypj.exe

ID	40
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 220469, Reason: Child Process
Unmonitor End Time	End Time: 246967, Reason: Terminated
Monitor duration	26.50s
Return Code	0
PID	2612
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #41: xauypj.exe

ID	41
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerExA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 221370, Reason: Child Process
Unmonitor End Time	End Time: 246978, Reason: Terminated
Monitor duration	25.61s
Return Code	0
PID	3012
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #42: xauypj.exe

ID	42
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerExW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 222079, Reason: Child Process
Unmonitor End Time	End Time: 247812, Reason: Terminated
Monitor duration	25.73s
Return Code	0
PID	872
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #43: xauypj.exe

ID	43
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 222811, Reason: Child Process
Unmonitor End Time	End Time: 310965, Reason: Terminated
Monitor duration	88.15s
Return Code	0
PID	1488
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	35
Environment	2
Registry	786
Mutex	6
Process	2
-	11
-	32
-	46

Process #44: xauypj.exe

ID	44
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryListenerConfigA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 226488, Reason: Child Process
Unmonitor End Time	End Time: 250805, Reason: Terminated
Monitor duration	24.32s
Return Code	0
PID	4000
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #45: xauypj.exe

ID	45
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryListenerConfigW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 227098, Reason: Child Process
Unmonitor End Time	End Time: 253341, Reason: Terminated
Monitor duration	26.24s
Return Code	0
PID	1840
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	618
Mutex	7

Process #46: xauypj.exe

ID	46
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesExA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 228899, Reason: Child Process
Unmonitor End Time	End Time: 249043, Reason: Terminated
Monitor duration	20.14s
Return Code	259
PID	1248
Parent PID	4956
Bitness	64 Bit

Process #47: werfault.exe

ID	47
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4956 -s 700
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 228966, Reason: Child Process
Unmonitor End Time	End Time: 248097, Reason: Terminated
Monitor duration	19.13s
Return Code	0
PID	2564
Parent PID	4956
Bitness	64 Bit

Process #48: xauypj.exe

ID	48
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQuerySessionInformationA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 229621, Reason: Child Process
Unmonitor End Time	End Time: 253657, Reason: Terminated
Monitor duration	24.04s
Return Code	0
PID	3220
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #49: xauypj.exe

ID	49
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSGetListenerSecurityW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 230904, Reason: Child Process
Unmonitor End Time	End Time: 250763, Reason: Terminated
Monitor duration	19.86s
Return Code	259
PID	1976
Parent PID	4796
Bitness	64 Bit

Process #50: werfault.exe

ID	50
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4796 -s 492
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 231359, Reason: Child Process
Unmonitor End Time	End Time: 250743, Reason: Terminated
Monitor duration	19.38s
Return Code	0
PID	1772
Parent PID	4796
Bitness	64 Bit

Process #51: xauypj.exe

ID	51
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQuerySessionInformationW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 234178, Reason: Child Process
Unmonitor End Time	End Time: 257268, Reason: Terminated
Monitor duration	23.09s
Return Code	0
PID	3592
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #52: werfault.exe

ID	52
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 3784 -s 492
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 236725, Reason: Child Process
Unmonitor End Time	End Time: 254719, Reason: Terminated
Monitor duration	17.99s
Return Code	0
PID	1648
Parent PID	3784
Bitness	64 Bit

Process #53: xauypj.exe

ID	53
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSIsChildSessionsEnabled
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 236892, Reason: Child Process
Unmonitor End Time	End Time: 254934, Reason: Terminated
Monitor duration	18.04s
Return Code	259
PID	1292
Parent PID	3784
Bitness	64 Bit

Process #54: xauypj.exe

ID	54
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryUserConfigA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 241650, Reason: Child Process
Unmonitor End Time	End Time: 261208, Reason: Terminated
Monitor duration	19.56s
Return Code	0
PID	3780
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	777
Mutex	7

Process #55: xauypj.exe

ID	55
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryUserConfigW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 248097, Reason: Child Process
Unmonitor End Time	End Time: 321729, Reason: Terminated by Timeout
Monitor duration	73.63s
Return Code	Unknown
PID	3660
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	37
File	118
System	7
Environment	2
Registry	778
Mutex	5
Process	2
-	2
-	1

Process #56: explorer.exe

ID	56
File Name	c:\windows\explorer.exe
Command Line	explorer.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 250679, Reason: Injection
Unmonitor End Time	End Time: 321729, Reason: Terminated by Timeout
Monitor duration	71.05s
Return Code	Unknown
PID	2000
Parent PID	512
Bitness	64 Bit

Injection Information (36)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x79c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x8b8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0xfdc	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x508	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x704	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x504	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x1060	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x5a8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#43: c:\users\rdhj0cnfevzx\desktop\xauypj.exe	0x4f0 / 0x67c	0x7ffb2623ce60(140716653399648)	-	✔	1

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	53 bytes	e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	✗
-	1.42 KB	680fc9cc119369263e40cc810c716a3d367aed75e09d2a9659824f8c366b7cde	✗
-	1.42 KB	4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	✗
-	1.42 KB	34cbc604bed93cbd541c8f639999d089e597bfa366077ed4224547e8cd69eabb	✗

Host Behavior

Type	Count
Module	44
File	211
System	124
Process	79
Registry	13882
Environment	1
-	18
Mutex	391

Process #57: xauypj.exe

ID	57
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryUserToken
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 252959, Reason: Child Process
Unmonitor End Time	End Time: 261475, Reason: Terminated
Monitor duration	8.52s
Return Code	0
PID	2500
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #59: xauypj.exe

ID	59
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSRegisterSessionNotification
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 257720, Reason: Child Process
Unmonitor End Time	End Time: 321729, Reason: Terminated by Timeout
Monitor duration	64.01s
Return Code	Unknown
PID	3680
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #60: xauypj.exe

ID	60
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSRegisterSessionNotificationEx
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 259637, Reason: Child Process
Unmonitor End Time	End Time: 321729, Reason: Terminated by Timeout
Monitor duration	62.09s
Return Code	Unknown
PID	2856
Parent PID	1164
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2

Process #61: xauypj.exe

ID	61
File Name	c:\users\rdhj0cnfevzx\desktop\xauypj.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSSendMessageA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 288436, Reason: Child Process
Unmonitor End Time	End Time: 321729, Reason: Terminated by Timeout
Monitor duration	33.29s
Return Code	Unknown
PID	4876
Parent PID	1164
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222	C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll, C:\Users\RDhJ0CNFevzX\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll	Sample File	1192.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
e641ff8107a4197ded9f558d1891e716811e9a7f109f14e876f5a8394844dc34	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	53 bytes	application/octet-stream	-	CLEAN
680fc9cc119369263e40cc810c716a3d367aed75e09d2a9659824f8c366b7cde	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN
4459de34f31d879717f63fcf0b48c4b322ee763c7e60d4b0e2a2a61a7805cf43	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN
34cbc604bed93cbd541c8f639999d089e597bfa366077ed4224547e8cd69eabb	c:\users\rdhj0cnfevzx\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-1560258661-3990802383-1811730007-1000\3d3578a85286f88c6cd9d151e4412949_03845cb8-7441-4a2f-8c0f-c90408af5778	Dropped File	1.42 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmppy3pshh5	Accessed File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Windows\explorer.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\Microsoft\Internet Explorer\UserData\Low\whCs	Accessed File	Access, Create	CLEAN
C:\Windows\system32\BdeHdCfg.exe	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\MSBuild\outlook.exe	Accessed File	Access, Read	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	xauypj.exe	CLEAN
{54137ce8-d76d-e7fc-dec3-c85f290e5b98}	access	xauypj.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{450ae42e-11c4-9ab5-80d0-f9ecd98a92e9}	access	xauypj.exe	CLEAN
{298ddcca-efe5-2f07-cbb5-e91e37797537}	access	explorer.exe	CLEAN
{0d9f601a-1a9d-9a0d-3d48-16d30afad3e9}	access	explorer.exe	CLEAN
{2fb46568-32c9-06dc-d0b5-f1ab83aee93b}	access	explorer.exe	CLEAN
{25390bbd-f8e2-0cdc-c922-ea2f65111ff1}	access	explorer.exe	CLEAN
{3efe96e0-aada-6cdc-4854-db5a860aa498}	access	explorer.exe	CLEAN
{9ffb2102-4ed7-3d87-65ab-805271e438f1}	access	explorer.exe	CLEAN
{1dda5c84-234c-9dac-e365-31fdf4838be5}	access	explorer.exe	CLEAN
{42099d9a-d7ef-cbfd-f97f-f2a010acb178}	access	explorer.exe	CLEAN
{1ea4e5de-7907-947c-5f34-31aa5165b0ee}	access	explorer.exe	CLEAN
{5bffd7b8-454a-d897-55b3-ba9b73e0f7e8}	access	explorer.exe	CLEAN
{7ba3817f-aeba-298a-7847-ab3c2bff153d}	access	explorer.exe	CLEAN
{be62f0b1-7f95-755e-f089-c901cc59559b}	access	explorer.exe	CLEAN
{51d35644-0b88-f048-7f15-371b35fe4778}	access	explorer.exe	CLEAN
{e586b9b5-2211-73a5-584c-e90e373ec95a}	access	explorer.exe	CLEAN
{32a904a8-538e-8343-5555-6f0b1e713173}	access	explorer.exe	CLEAN
{e5989899-a3a9-fd79-a5ea-ef089b7275da}	access	explorer.exe	CLEAN
{232ac131-2ad9-0e6d-8224-fcb2c2b31979}	access	explorer.exe	CLEAN
{362882c5-03e2-fd0f-928d-c1120ad9c64f}	access	explorer.exe	CLEAN
{1bc6a851-4ae7-d17d-9611-affa9e1d58b2}	access	explorer.exe	CLEAN
{dd3a2c55-a2c7-6b31-3779-8694c5a66a4f}	access	explorer.exe	CLEAN
{a2e3a1c4-1044-26ac-2fa3-30ee391a0657}	access	explorer.exe	CLEAN
{7cc6ae5f-2c94-8c18-e20d-28bccdbd00c3}	access	explorer.exe	CLEAN
{d1575404-3469-2df0-db6b-3bcf4439344f}	access	explorer.exe	CLEAN
{ed001072-33d5-3038-e41a-46149c4b6966}	access	explorer.exe	CLEAN
{6a858a42-f46d-62bb-e142-0d99eeaf1f91}	access	explorer.exe	CLEAN
{822894df-44a8-add7-294a-a446b174fbef}	access	explorer.exe	CLEAN
{c42c174a-1be2-3a72-8667-a20ecc356e75}	access	explorer.exe	CLEAN
{a05f0669-d546-7c4b-c5ff-6ad44aa5f2b6}	access	explorer.exe	CLEAN
{95c38542-2405-0d06-534c-428190efb4c6}	access	explorer.exe	CLEAN
{e28905fd-15de-b796-44d3-7a7876237780}	access	explorer.exe	CLEAN
{fef37f2e-4f56-9012-852a-59484b5fed7e}	access	explorer.exe	CLEAN
{53be0c1d-6845-1fb9-9acf-69f1a3b7921b}	access	explorer.exe	CLEAN
{6d23ed51-38ca-5cb0-6eab-e5ee861c8501}	access	explorer.exe	CLEAN
{4055b8dd-d64d-bfbf-12c7-e1fd01a226ba}	access	explorer.exe	CLEAN
{d65528a1-3ef5-a115-0995-914008bd9a62}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{e722aca1-f311-7487-c06a-2f0c9ed96cf8}	access	explorer.exe	CLEAN
{2cfae193-d714-b1b7-9d1d-a23c5e456f45}	access	explorer.exe	CLEAN
{35809dca-c072-ec81-460e-44a0ad984eb0}	access	explorer.exe	CLEAN
{dc1a7d14-4f5e-2174-ea64-bc3105102601}	access	explorer.exe	CLEAN
{9259e53a-cc3a-456a-651a-d3997a588de6}	access	explorer.exe	CLEAN
{ae95a48c-b720-0f34-3b85-420610a06b44}	access	explorer.exe	CLEAN
{43e20c5c-a5aa-e3ba-7ba5-289bd79d768d}	access	explorer.exe	CLEAN
{91752076-8b21-43c3-9b1b-6d06b0370ec3}	access	explorer.exe	CLEAN
{18f3145b-23c3-2dd9-e680-9519534e72bf}	access	explorer.exe	CLEAN
{fdb83606-4ef7-5a58-ba85-687f05c6dbcf}	access	explorer.exe	CLEAN
{e56de5ae-6e94-b096-e03b-36d0cec5d3a6}	access	explorer.exe	CLEAN
{6444f54d-a127-9551-45b8-6703303ab458}	access	explorer.exe	CLEAN
{a5a67534-fa42-ee17-0f42-7894e1acd27e}	access	explorer.exe	CLEAN
{d4fcd5f8-e7e4-8c73-c2e5-9dea809ffc9a}	access	explorer.exe	CLEAN
{6ff03553-8c1f-eaac-a9cf-dffee1d0e05c}	access	explorer.exe	CLEAN
{14001fd5-42cb-a1e0-69b0-ab1633b2ae68}	access	explorer.exe	CLEAN
{9b6e053f-0de2-32a4-79d5-d31fb6cfceba}	access	explorer.exe	CLEAN
{0fe620b0-69ae-dee7-2d6b-018cf8c7d19c}	access	explorer.exe	CLEAN
{65566846-a504-a163-286e-1e2de15b09b5}	access	explorer.exe	CLEAN
{79e05e71-7171-8afb-009d-5d2b446994a0}	access	explorer.exe	CLEAN
{7fc82242-34f1-e1df-ba3b-ade8e9d124e8}	access	explorer.exe	CLEAN
{01d9346c-01cc-1ba0-e2c5-537a12d7529d}	access	explorer.exe	CLEAN
{481f3da2-a9f4-99d5-8d3f-8b79aaa5165f}	access	explorer.exe	CLEAN
{238ff016-c2ab-294d-d37f-36516ac88376}	access	explorer.exe	CLEAN
{b45fb1cc-a6de-1292-8450-230aeff75872}	access	explorer.exe	CLEAN
{7dd56f30-d26e-904c-dc7f-63812c4c902b}	access	explorer.exe	CLEAN
{e8b5559e-6677-afe6-1109-8fbaafa74ea9}	access	explorer.exe	CLEAN
{beed53fc-d0e8-3d49-9e5d-3458950fecb2}	access	explorer.exe	CLEAN
{76b6a7d9-30bc-f0ad-183d-792e6db4470b}	access	explorer.exe	CLEAN
{f608a101-330f-aefc-d398-04f5aa5a0542}	access	explorer.exe	CLEAN
{f3d66484-fbd0-fc9d-4667-437e9739f284}	access	explorer.exe	CLEAN
{3b7ec73b-c511-a202-2a05-a90bb554c574}	access	explorer.exe	CLEAN
{b419202c-7566-1987-fa50-e6543f7b60e5}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	access, create	xauypj.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	access, read	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	xauypj.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	access, read	xauypj.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	access, read	xauypj.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	access, read	xauypj.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EnableLUA	access, read	xauypj.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ConsentPromptBehaviorAdmin	access, read	xauypj.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\PromptOnSecureDesktop	access, read	xauypj.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InstallDate	access, read	xauypj.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8C45A918-B075-FEF6-0DED-B5C899623EB0}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{61E3425B-6B05-A459-B4FE-174B2D84DE94}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{026F08C5-341A-9406-8117-0A9B26B9732B}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{98DFD738-1E78-D107-2616-FA30049BD427}\ShellFolder	access, create	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1384CAC3-17AC-E069-EB5C-4E613FCC6FE4}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5E441BBB-4FA0-7A47-C898-77D45B377F36}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{28ABA520-2C1D-6C61-C0C7-A14CF6B906F1}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{62E4E317-0062-79DE-48F0-1E0765BB0FBB}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\InstallDate	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3588360E-206F-AD4B-5FE2-CA87B137A0AE}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD715941-4DC5-0356-AE8C-CD7DA56A3E36}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2576763A-EFDC-256B-2964-9C5E743B0B1B}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{92405BE0-7F95-9DE5-BB58-67AC75F6DB46}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5CFB38CB-4922-AAF5-9C1E-F3F5A6338105}\ShellFolder\{396DCAA3-9C2C-B4CA-BD78-E818B9F43367}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{ABEF8FF5-5E25-CC62-E6D8-05FBE04DAA0F}\ShellFolder\{DBD7D865-B33B-1126-2D36-346A9AFEB1C1}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A13D7EA4-5D34-8684-2E14-FDAFDFB3E2D8}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4D2056E1-92AF-EC5C-2615-AA80579018DA}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{368B1D7B-EAC9-2EB9-9178-5819EFDD132A}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9D74D8D1-A2C2-8A4E-2A5F-EBAAE5390403}\ShellFolder	access, create	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
explorer.exe	explorer.exe	SUSPICIOUS

Process Name	Commandline	Verdict
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmppy3pshh5" /s	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=IsInteractiveUserSession	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=QueryActiveSession	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=QueryUserToken	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=RegisterUsertokenForNoWinlogon	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSCloseServer	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSConnectSessionA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSConnectSessionW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSCreateListenerA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSCreateListenerW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSDisconnectSession	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnableChildSessions	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateListenersA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateListenersW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesExA	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1600 -s 5804	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1600 -s 2352	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesExW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateProcessesW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateServersA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateServersW	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1752 -s 700	CLEAN

Process Name	Commandline	Verdict
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsExA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsExW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSEnumerateSessionsW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSFreeMemory	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSFreeMemoryExA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSFreeMemoryExW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSGetChildSessionId	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSGetListenerSecurityA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSGetListenerSecurityW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSIsChildSessionsEnabled	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSLogoffSession	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerExA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerExW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSOpenServerW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryListenerConfigA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryListenerConfigW	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4956 -s 700	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQuerySessionInformationA	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4796 -s 492	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQuerySessionInformationW	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 3784 -s 492	CLEAN

Process Name	Commandline	Verdict
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryUserConfigA	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryUserConfigW	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSQueryUserToken	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSRegisterSessionNotification	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSRegisterSessionNotificationEx	CLEAN
xauypj.exe	"C:\Users\RDhJ0CNFevzX\Desktop\xaUypj.exe" /dll="C:\Users\RDHJ0C~1\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll" /fn_id=WTSSendMessageA	CLEAN

YARA / AV

Antivirus (5)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	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	2021-09-28 08:04:18+00:00
Built-in AV Database Records	10477558

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