MALICIOUS

Classifications: Miner | PUA | Backdoor

Threat Names: XMRig | C2/Generic-A | Mal/Generic-S | XMRig.EMB

Verdict Reason: -

Sample Type	**Windows Exe (x86-64)**
File Name	**service.exe**
ID	#10321205
MD5	4ac91d6780cd7a405262a07452efab3f
SHA1	2779333362184c39e210dc21c2b5879cf5201f37
SHA256	a05bf521aa48398ccb4428ebf564cd5c6425b5aa1f530570fac7b711a8f3d401
File Size	1593.50 KB
Report Created	2024-04-28 11:01 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 13 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	XMRig configuration was extracted	1	Miner
	• A configuration for XMRig was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Miner, PUA
	• YARA detected "XMRig_Miner" from ruleset "PUAs" in memory dump data from (process #1) service.exe.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Malicious host or URL detected via reputation	2	-
	• Reputation analysis labels the resolved domain "eu.minerpool.pw" as C2/Generic-A. • Reputation analysis labels the contacted IP address 185.10.68.220 as C2/Generic-A.			
2/5	Discovery	Reads network adapter information	1	-
	• (Process #1) service.exe reads the network adapters' addresses by API.			
2/5	Network Connection	Sets up server that accepts incoming connections	1	Backdoor
	• (Process #1) service.exe starts a TCP server listening on port 49162.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) service.exe creates mutex with name "4pC39Ev2yuzFY8izw76DGDJR".			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #1) service.exe enables process privilege "SeLockMemoryPrivilege".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) service.exe enumerates running processes.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #1) service.exe resolves hostname "eu.minerpool.pw" to IP "185.10.68.123".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #1) service.exe opens an outgoing TCP connection to host "185.10.68.220:443".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) service.exe resolves 307 API functions by name.			

Malware Configuration: XMRig

Metadata	Key	Extracted Value
Socket	Tags	Mining Pool #0
	Address	185.10.68.220
	Port	443
	Network Protocol	tcp
	C2	✔
	Tags	Mining Pool #1
	Address	2.59.220.122
	Port	443
	Network Protocol	tcp
	C2	✔
	Tags	Mining Pool #2
	Address	91.92.248.9
	Port	443
	Network Protocol	tcp
	C2	✔
	Tags	Mining Pool #3
	Address	back123.brasilia.me
	Port	443
	Network Protocol	tcp
	C2	✔
	Tags	Mining Pool #4
	Address	eu.minerpool.pw
	Port	443
	Network Protocol	tcp
	C2	✔
	Tags	Mining Pool #5
	Address	rig.myrms.pw
	Port	443
	Network Protocol	tcp
	C2	✔
	Tags	Mining Pool #6
	Address	rig.zxcvb.pw
	Port	443
	Network Protocol	tcp
	C2	✔
	Tags	Mining Pool #7
	Address	rs.fym5gserobhh.pw
	Port	443
	Network Protocol	tcp
	C2	✔
Credential	Tags	Mining Pool #0
	Username	XmrigBeta2
	Tags	Mining Pool #1
	Username	XmrigBeta2
	Tags	Mining Pool #2
	Username	XmrigBeta2
	Tags	Mining Pool #3
	Username	XmrigBeta2
	Tags	Mining Pool #4
	Username	XmrigBeta2
	Tags	Mining Pool #5
	Username	XmrigBeta2
	Tags	Mining Pool #6
	Username	XmrigBeta2
	Tags	Mining Pool #7
	Username	XmrigBeta2

Mitre ATT&CK Matrix

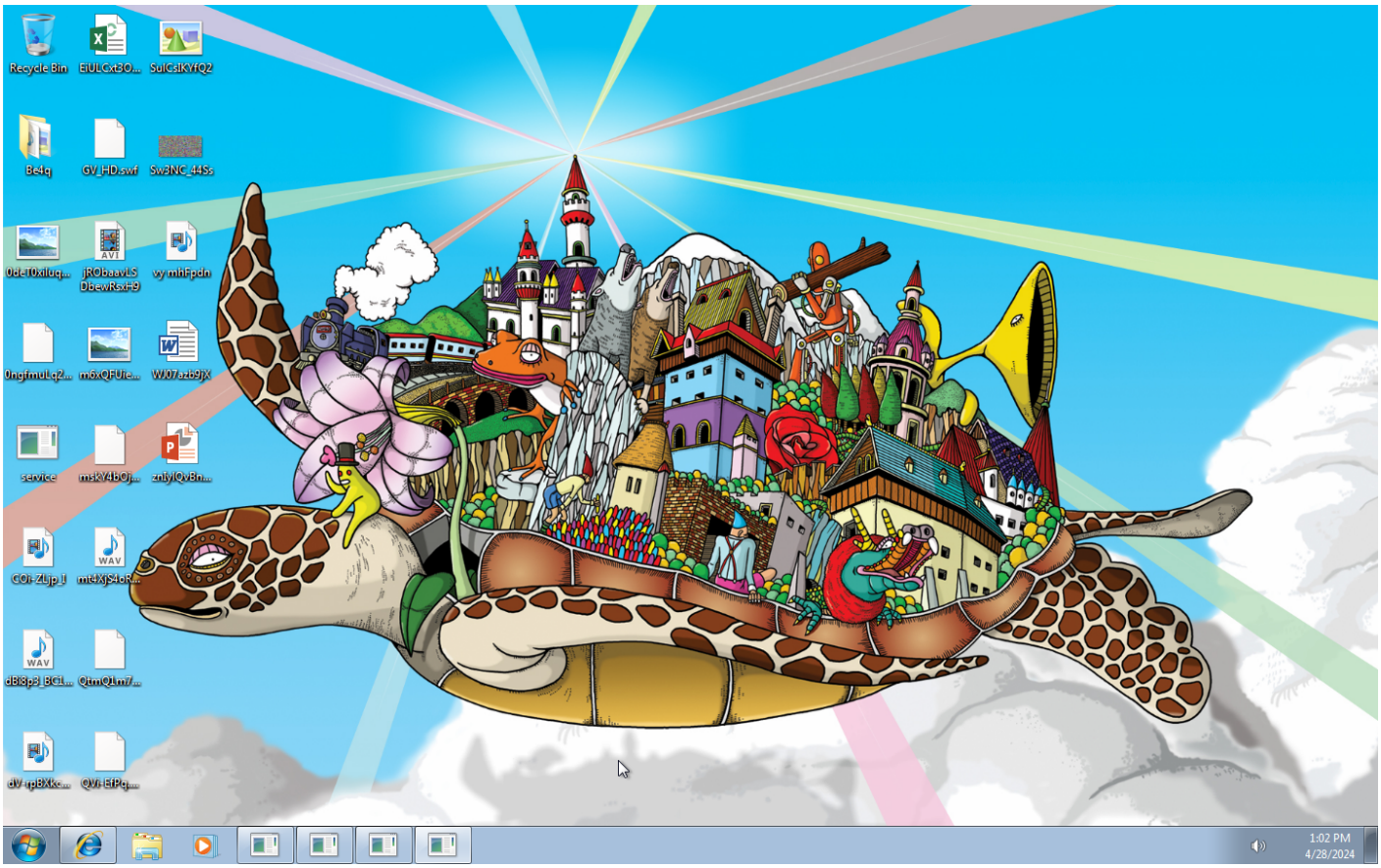
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing		#T1016 System Network Configuration Discovery					
						#T1057 Process Discovery					

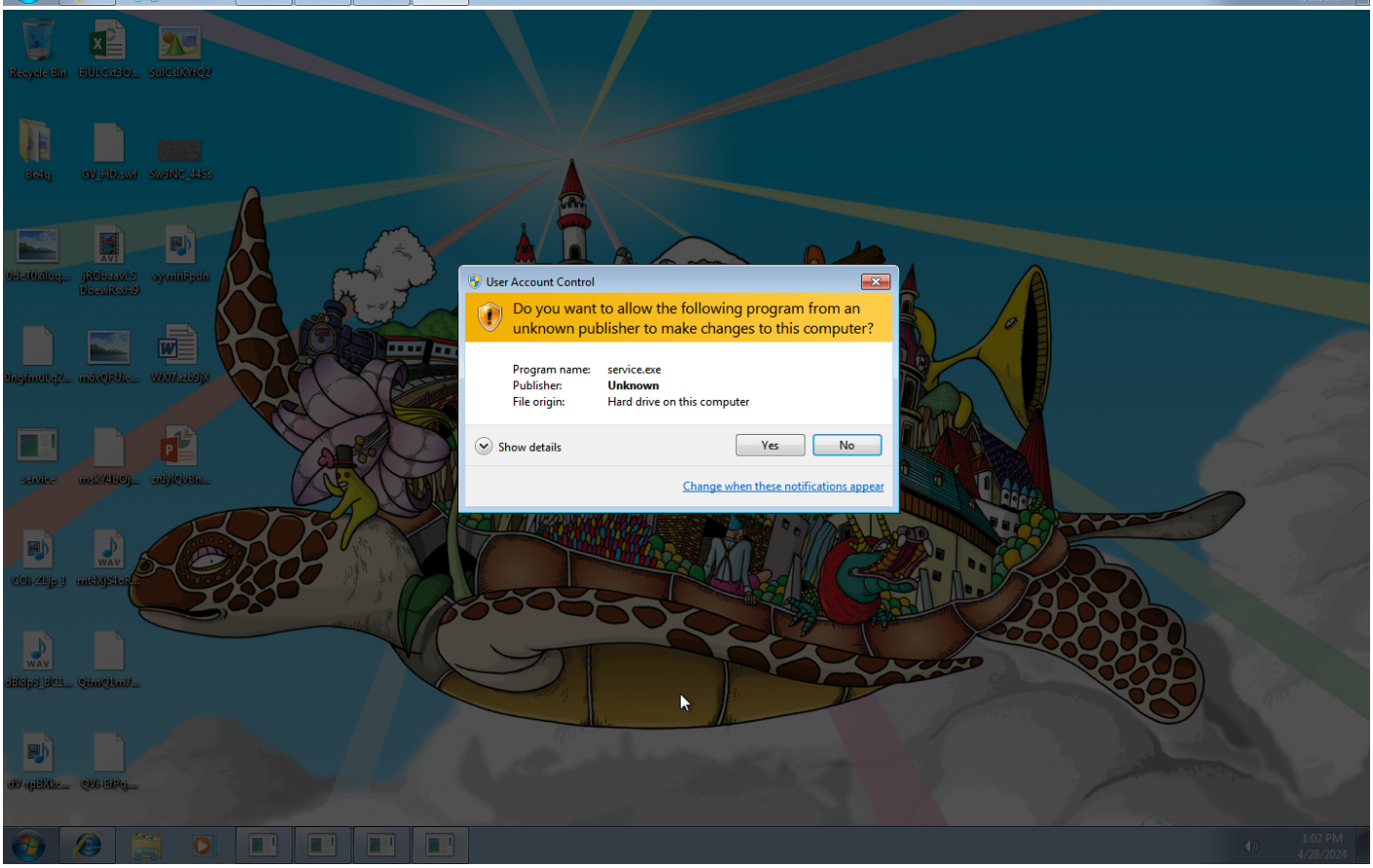
Sample Information

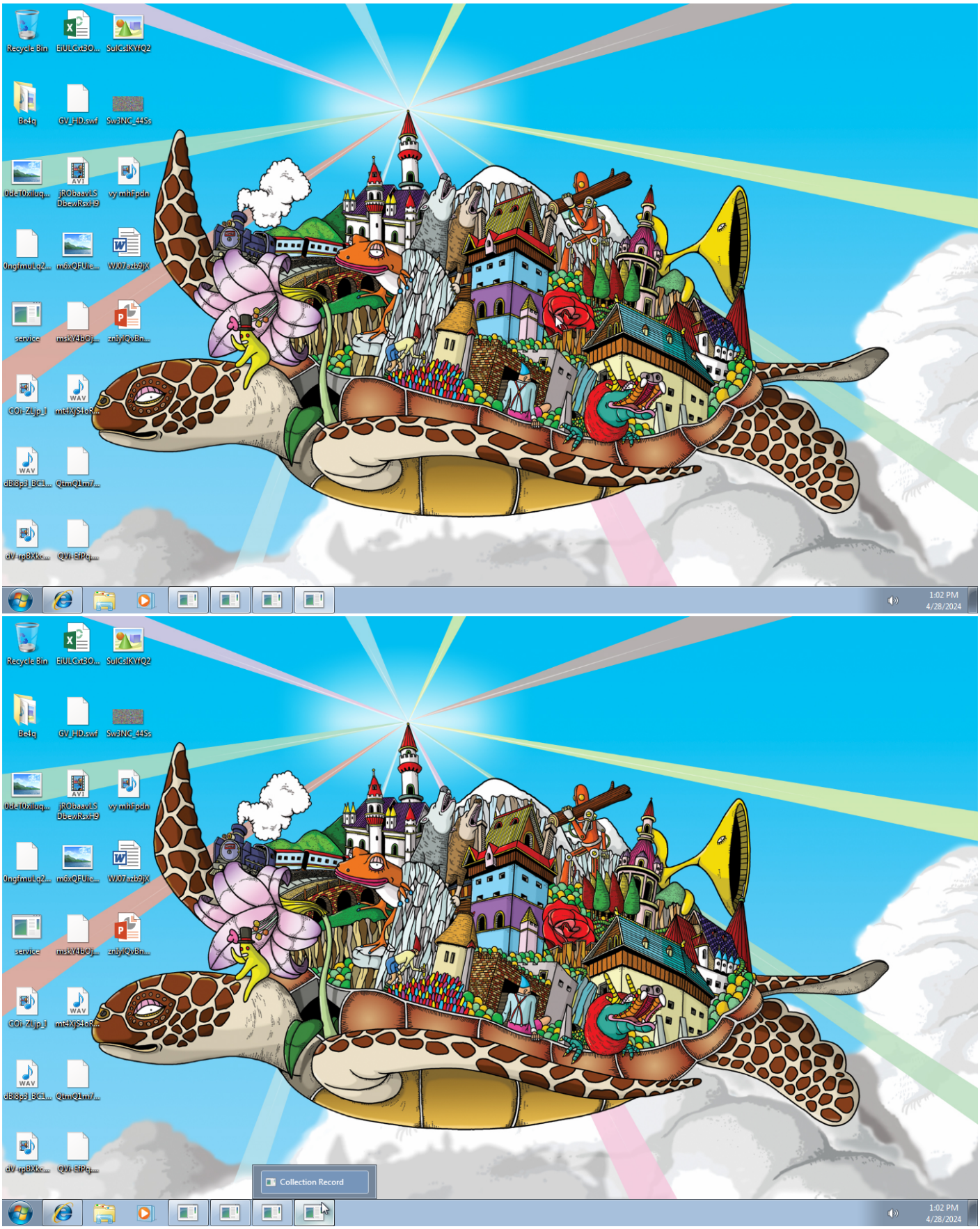
ID	#10321205
MD5	4ac91d6780cd7a405262a07452efab3f
SHA1	2779333362184c39e210dc21c2b5879cf5201f37
SHA256	a05bf521aa48398ccb4428ebf564cd5c6425b5aa1f530570fac7b711a8f3d401
SSDeep	24576:ravo/YFhnivTP0lhLuFEFotb0XUGH0gUu2ZfdOPAklQuYi/XCiN:rEo/Ul0atGYUGHv92ZfY5l3j/yiN
ImpHash	bb388b5fb16beacfa2a7403d25eaa8c4
File Name	service.exe
File Size	1593.50 KB
Sample Type	Windows Exe (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2024-04-28 11:01 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	16
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✖
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	14




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



Screenshots truncated

NETWORK

General

2.21 KB total sent

24.20 KB total received

2 ports 443, 53

2 contacted IP addresses

8 URLs extracted

0 files downloaded

1 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

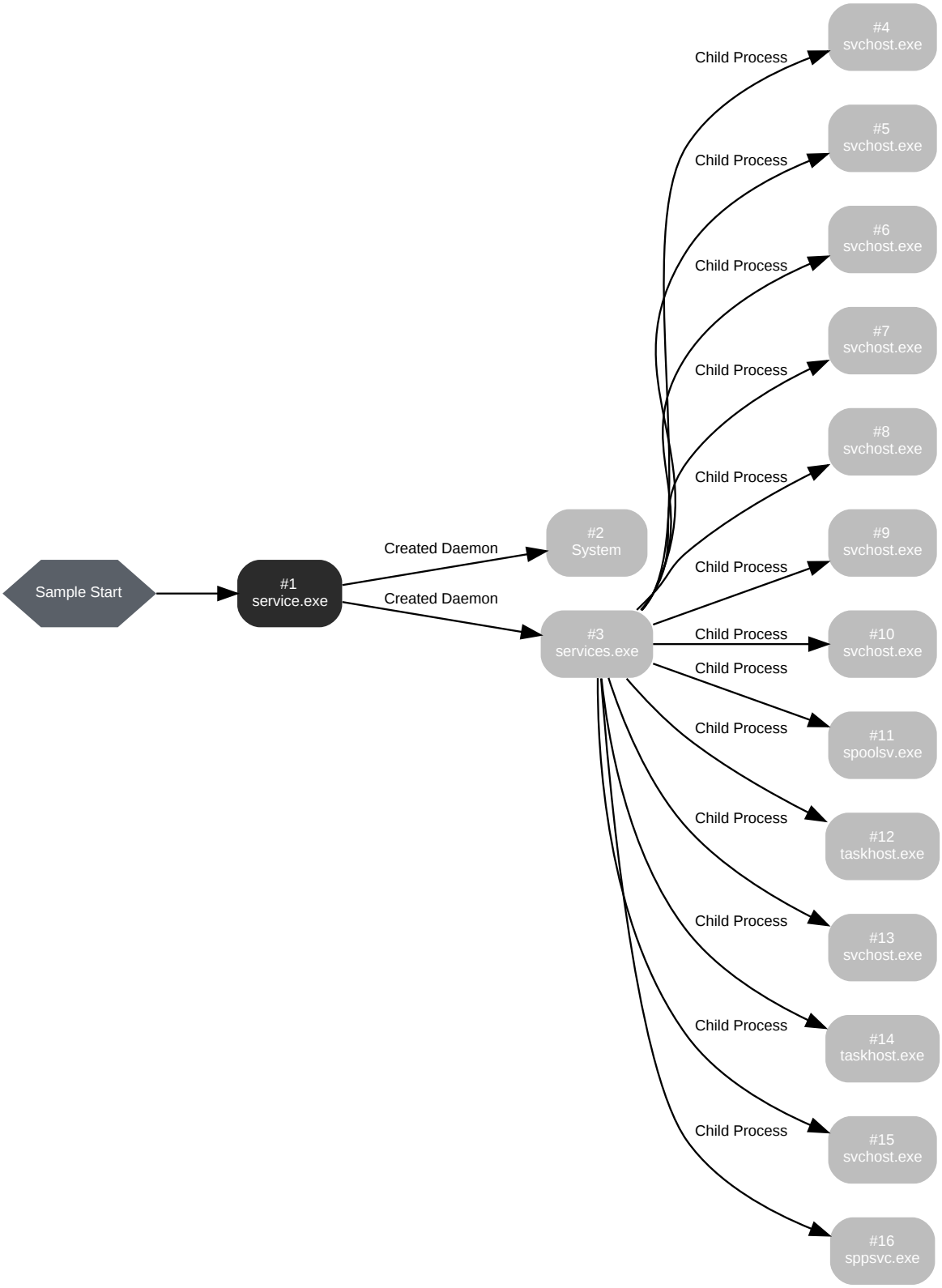
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	eu[.]minerpool[.]pw	NO_ERROR	185.10.68.123, 185.10.68.220, 91.92.248.9	-	MALICIOUS

BEHAVIOR

Process Graph



Process #1: service.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\service.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\service.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49372, Reason: Analysis Target
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	244.09s
Return Code	Unknown
PID	3936
Parent PID	-
Bitness	64 Bit

Host Behavior

Type	Count
Module	379
System	1209
File	10
Environment	1
Mutex	1
-	3
User	2
COM	1
-	1
Process	46173
-	6

Network Behavior

Type	Count
DNS	1
TCP	1

Process #2: System

ID	2
File Name	System
Command Line	-
Initial Working Directory	-
Monitor Start Time	Start Time: 63062, Reason: Created Daemon
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	4
Parent PID	-
Bitness	64 Bit

Process #3: services.exe

ID	3
File Name	c:\windows\system32\services.exe
Command Line	C:\Windows\system32\services.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Created Daemon
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	472
Parent PID	3936
Bitness	64 Bit

Process #4: svchost.exe

ID	4
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	596
Parent PID	472
Bitness	64 Bit

Process #5: svchost.exe

ID	5
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k RPCSS
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	664
Parent PID	472
Bitness	64 Bit

Process #6: svchost.exe

ID	6
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	712
Parent PID	472
Bitness	64 Bit

Process #7: svchost.exe

ID	7
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	824
Parent PID	472
Bitness	64 Bit

Process #8: svchost.exe

ID	8
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	876
Parent PID	472
Bitness	64 Bit

Process #9: svchost.exe

ID	9
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1020
Parent PID	472
Bitness	64 Bit

Process #10: svchost.exe

ID	10
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k NetworkService
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1040
Parent PID	472
Bitness	64 Bit

Process #11: spoolsv.exe

ID	11
File Name	c:\windows\system32\spoolsv.exe
Command Line	C:\Windows\System32\spoolsv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1136
Parent PID	472
Bitness	64 Bit

Process #12: taskhost.exe

ID	12
File Name	c:\windows\system32\taskhost.exe
Command Line	"taskhost.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1168
Parent PID	472
Bitness	64 Bit

Process #13: svchost.exe

ID	13
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1200
Parent PID	472
Bitness	64 Bit

Process #14: taskhost.exe

ID	14
File Name	c:\windows\system32\taskhost.exe
Command Line	taskhost.exe $(Arg0)
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1812
Parent PID	472
Bitness	64 Bit

Process #15: svchost.exe

ID	15
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1696
Parent PID	472
Bitness	64 Bit

Process #16: sppsvc.exe

ID	16
File Name	c:\windows\system32\sppsvc.exe
Command Line	C:\Windows\system32\sppsvc.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 63062, Reason: Child Process
Unmonitor End Time	End Time: 293467, Reason: Terminated by timeout
Monitor duration	230.41s
Return Code	Unknown
PID	1328
Parent PID	472
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
a05bf521aa48398ccb4428ebf564cd5c6425b5aa1f530570fac7b711a8f3d401	C:\Users\kEecfMwgj\Desktop\service.exe	Sample File	1593.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
9dfdb84e771af677eb9382303720174f0eb20932ba1a66fc1ea7a736234985c1	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8e39641862cf180d60b1f049245e7e6560f740d64a17014bdfdf38813dc3dc9b	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c41103ca551b74ab1d6a7ef82084cef0a11c544908c54723a805ce6a2cc8be64	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c311de84665ce7d075dd117dfdbc43480320b231af50df9ea660c7f37b712836	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
affaaf78ed13469bd4e29cf48c824c996105f491937043c0cc3195399fa91fce	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
1dba46d171dd0c1f9a4ae1df3f7b5805a0ecb73ea4a268870d250706ab754e25	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b857fcb3c11c8ead27f95ab05f737ddc3b38219672c6dbfa93f3840dd82ebdb6	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
eee396d6292120c418259fe77494dfccef8d24be1039d8ce67cbcd29d340aae6	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
00d33b874ede59d08c3562d6d3f473c35b1368ff66e00e4306414df4bc49139c	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
daee04efe81abdfbf35405115272ea8bcd5f815f97de661745808d134ccaea73	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
453cc558b5a2ce891ae9bbf3ee4745b5b443ce8ae5369d81d301ee6edfe5fa80	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8d472e71ed86ee344e0eb7a7fda67cebbfa004405dadbb88f8f69ff8b90bb1cb	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
d3131faae54af4766944514bb11fda502620659f89e81dbe26d5328ace2951e3	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
6e623de8e77d8c76834084cc9c150b304a5bf98e0ba7cabd10135e96f1db1fd6	-	Memory Dump	7428.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\service.exe	Accessed File, Sample File	Access	MALICIOUS
C:\Program Files\Common Files\SSL/openssl.cnf	Accessed File	Access	CLEAN
\\.\WinRing0_1_2_0	Accessed File	Access	CLEAN
-	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://185[.]10[.]68[.]220:443	Extracted	185.10.68.220	Seychelles	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://2[.]59[.]220[.]122:443	Extracted	2.59.220.122	-	-	MALICIOUS
hxxp://91[.]92[.]248[.]9:443	Extracted	91.92.248.9	Bulgaria	-	MALICIOUS
hxxp://back123[.]brasilia[.]me:443	Extracted	-	-	-	MALICIOUS
hxxp://eu[.]minerpool[.]pw:443	Extracted	91.92.248.9, 185.10.68.220, 185.10.68.123	Bulgaria, Seychelles	-	MALICIOUS
hxxp://rig[.]myrms[.]pw:443	Extracted	-	-	-	MALICIOUS
hxxp://rig[.]zxcvb[.]pw:443	Extracted	-	-	-	MALICIOUS
hxxp://rs[.]fym5gserobhh[.]pw:443	Extracted	-	-	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
eu[.]minerpool[.]pw	91.92.248.9, 185.10.68.220, 185.10.68.123	Bulgaria, Seychelles	TCP, DNS, TLS	MALICIOUS
back123[.]brasilia[.]me	-	-	-	CLEAN
rig[.]myrms[.]pw	-	-	-	CLEAN
rig[.]zxcvb[.]pw	-	-	-	CLEAN
rs[.]fym5gserobhh[.]pw	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.10.68.220	eu[.]minerpool[.]pw	Seychelles	TCP, DNS, TLS	MALICIOUS
185.10.68.123	eu[.]minerpool[.]pw	Seychelles	DNS	CLEAN
91.92.248.9	eu[.]minerpool[.]pw	Bulgaria	DNS	CLEAN
2.59.220.122	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
4pC39Ev2yuzFY8izw76DGDJR	access	service.exe	CLEAN

Process

Process Name	Commandline	Verdict
service.exe	"C:\Users\kEecfMwgj\Desktop\service.exe"	MALICIOUS
System	-	CLEAN
services.exe	C:\Windows\system32\services.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k RPCSS	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted	CLEAN
svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskhost.exe	taskhost.exe $(Arg0)	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalService	CLEAN

Process Name	Commandline	Verdict
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation	CLEAN
sppsvc.exe	C:\Windows\system32\sppsvc.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k NetworkService	CLEAN
spoolsv.exe	C:\Windows\System32\spoolsv.exe	CLEAN
taskhost.exe	"taskhost.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	CLEAN

YARA / AV

YARA (14)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5
PUAs	XMRig_Miner	XMRig mining software	Memory Dump	-	Miner, PUA	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	windows 7 (64bit SP1 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
YARA Built-in Ruleset Version	2024.2.1.18

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp

System Root	C:\Windows