MALICIOUS

Classifications: Injector | Downloader

Threat Names: Mal/HTMLGen-A | Mal/Generic-S | Pikabot

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**Xjgkkltfdhdfhfjg.exe**
ID	#9928494
MD5	2a3a840641803b101b86e0c321b0a5fe
SHA1	52bc3e121f44c4f9e71b43110f468886294c7fc2
SHA256	b025e37611168c0abcc446125a8bd7cb831625338434929febadfcc9cc4c816e
File Size	3328.09 KB
Report Created	2024-02-22 11:01 (UTC)
Target Environment	windows 10 (64bit 20H1 -EN-) | exe

OVERVIEW

VMRay Threat Identifiers (18 rules, 72 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Pikabot configuration was extracted	1	Downloader
	• A configuration for Pikabot was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	2	Downloader
	• YARA detected "Pikabot_Indirect_Syscalls" from ruleset "Malware" in memory dump data from (process #1) xjgkkltfdhdfhfjg.exe. • YARA detected "Pikabot_FunctionStrings_Feb2024" from ruleset "Malware" in function strings data from (process #2) ctfmon.exe.			
5/5	Anti Analysis	Makes indirect system call to evade hooking based sandboxes	13	-
	• (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtQueryInformationProcess". • (Process #2) ctfmon.exe makes an indirect system call to "NtQueryInformationProcess". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtCreateUserProcess". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtSetContextThread". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtAllocateVirtualMemory". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtClose". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtResumeThread". • (Process #2) ctfmon.exe makes an indirect system call to "NtQueryInformationToken". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtQuerySystemInformation". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtOpenProcess". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtGetContextThread". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtWriteVirtualMemory". • (Process #1) xjgkkltfdhdfhfjg.exe makes an indirect system call to "NtReadVirtualMemory".			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) xjgkkltfdhdfhfjg.exe modifies memory of (process #2) ctfmon.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) xjgkkltfdhdfhfjg.exe alters context of (process #2) ctfmon.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	26	-

Score	Category	Operation	Count	Classification
		• Reputation analysis labels the URL "hxxps://23[.]226[.]138[.]143:2083/api/admin.emoji.addAlias" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://23[.]226[.]138[.]161:5242/api/admin.usergroups.addTeams" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://37[.]60[.]242[.]85:9785/api/admin.emoji.addAlias" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://57[.]128[.]165[.]176:13721/api/admin.users.session.reset" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://86[.]38[.]225[.]105:13721/api/admin.emoji.add" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://86[.]38[.]225[.]106:2221/api/admin.emoji.addAlias" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://89[.]117[.]23[.]185:2221/api/admin.apps.restrict" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://89[.]117[.]23[.]186:5632/api/admin.emoji.addAlias" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://103[.]82[.]243[.]5:13785/api/admin.users.session.reset" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://145[.]239[.]135[.]24:5243/api/admin.users.session.reset" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://154[.]12[.]233[.]66:2224/api/admin.usergroups.addTeams" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://178[.]18[.]246[.]136:2078/api/admin.usergroups.addTeams" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://85[.]239[.]243[.]155:5000/api/admin.users.session.reset" which was contacted by (process #2) ctfmon.exe as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 37.60.242.85 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 178.18.246.136 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 103.82.243.5 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 23.226.138.143 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 57.128.165.176 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 86.38.225.106 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 145.239.135.24 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 154.12.233.66 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 85.239.243.155 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 23.226.138.161 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 89.117.23.186 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 86.38.225.105 as Mal/HTMLGen-A. • Reputation analysis labels the contacted IP address 89.117.23.185 as Mal/HTMLGen-A.		
3/5	Network Connection	Uses HTTP to upload a large amount of data.	1	-
		• (Process #2) ctfmon.exe uploads 114.615KB data using HTTP POST.		
2/5	Anti Analysis	Tries to detect kernel debugger	1	-
		• (Process #1) xjgkkltfdhdfhfjg.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".		
2/5	Anti Analysis	Tries to detect debugger	2	-
		• (Process #1) xjgkkltfdhdfhfjg.exe tries to detect a debugger via API "NtQueryInformationProcess". • (Process #1) xjgkkltfdhdfhfjg.exe tries to detect a debugger via API "CheckRemoteDebuggerPresent".		
2/5	Discovery	Queries a host's domain name	1	-
		• (Process #2) ctfmon.exe queries the host's domain name.		
1/5	Discovery	Enumerates running processes	2	-
		• (Process #1) xjgkkltfdhdfhfjg.exe enumerates running processes. • (Process #2) ctfmon.exe enumerates running processes.		
1/5	Obfuscation	Reads from memory of another process	1	-
		• (Process #1) xjgkkltfdhdfhfjg.exe reads from (process #1) xjgkkltfdhdfhfjg.exe.		
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
		• (Process #1) xjgkkltfdhdfhfjg.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.		

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	1	-
	• (Process #2) ctfmon.exe creates mutex with name "{9ED9ADD7-B212-43E5-ACE9-B2E05ED5D524}".			
1/5	Network Connection	Tries to connect using an uncommon port	15	-
	• Tries to connect to TCP port 2083 at 23.226.138.143. • Tries to connect to TCP port 5242 at 23.226.138.161. • Tries to connect to TCP port 9785 at 37.60.242.85. • Tries to connect to TCP port 13721 at 57.128.165.176. • Tries to connect to TCP port 5000 at 85.239.243.155. • Tries to connect to TCP port 13721 at 86.38.225.105. • Tries to connect to TCP port 2221 at 86.38.225.106. • Tries to connect to TCP port 2221 at 89.117.23.185. • Tries to connect to TCP port 5632 at 89.117.23.186. • Tries to connect to TCP port 13785 at 103.82.243.5. • Tries to connect to TCP port 2223 at 104.129.55.105. • Tries to connect to TCP port 13783 at 104.129.55.106. • Tries to connect to TCP port 5243 at 145.239.135.24. • Tries to connect to TCP port 2224 at 154.12.233.66. • Tries to connect to TCP port 2078 at 178.18.246.136.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) xjgkkltfdhdfhfjg.exe resolves 60 API functions by name.			
1/5	Obfuscation	Overwrites code	1	-
	• (Process #2) ctfmon.exe overwrites code to possibly hide behavior.			

Malware Configuration: Pikabot

Metadata	Key	Extracted Value
Socket	Address	103.82.243.5
	Port	13785
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	86.38.225.105
	Port	13721
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	37.60.242.85
	Port	9785
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	89.117.23.185
	Port	2221
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	104.129.55.106
	Port	13783
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	86.38.225.106
	Port	2221
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	178.18.246.136
	Port	2078
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	154.12.233.66
	Port	2224
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	85.239.243.155
	Port	5000
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	145.239.135.24
	Port	5243
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	23.226.138.161
	Port	5242
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	104.129.55.105
	Port	2223
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	23.226.138.143
	Port	2083
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	57.128.165.176
	Port	13721
	Network Protocol	tcp
	C2	✔
	Listen	✖
	Address	89.117.23.186
	Port	5632
	Network Protocol	tcp
	C2	✔
	Listen	✖

Mitre ATT&CK Matrix

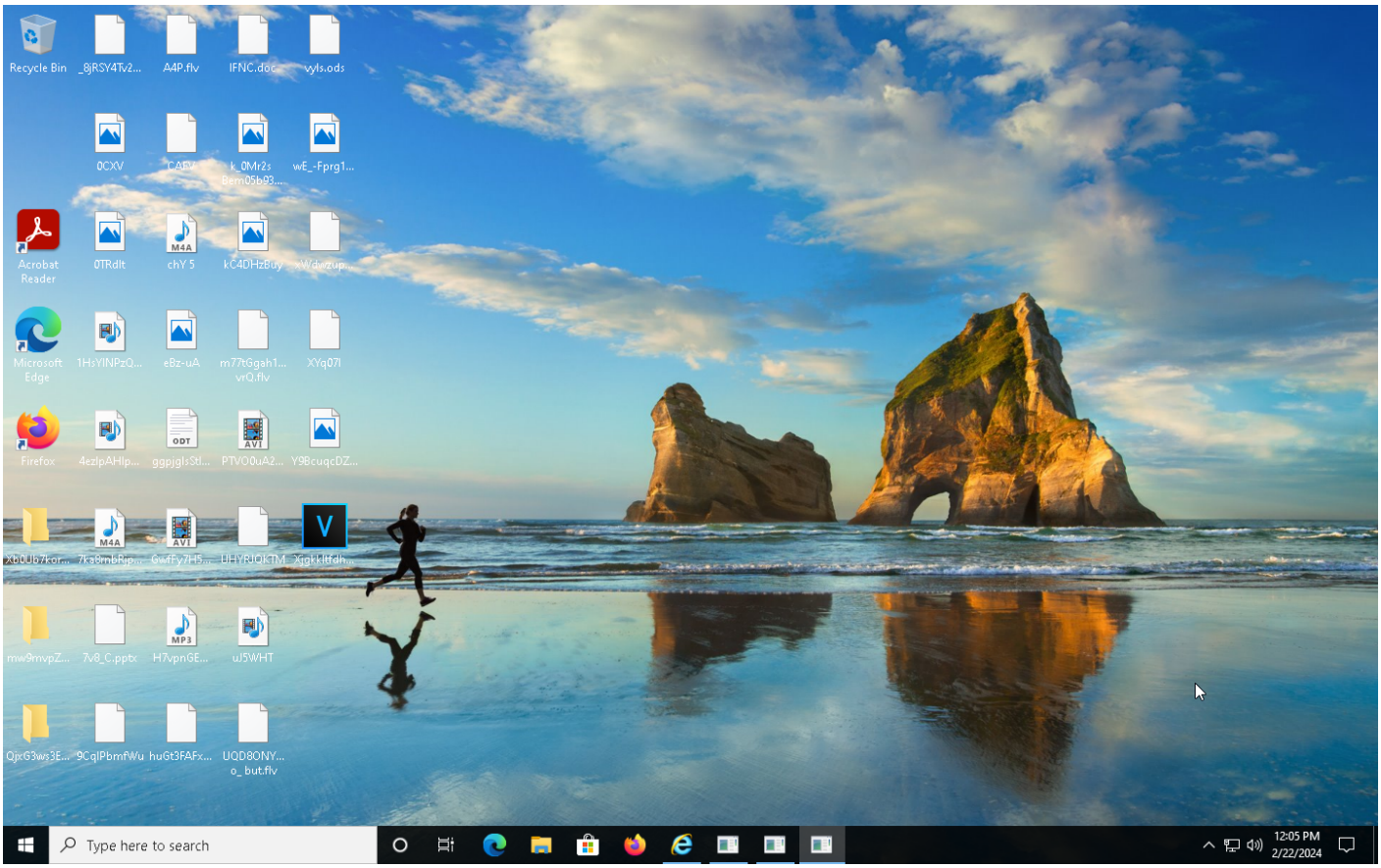
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing		#T1057 Process Discovery			#T1071 Standard Application Layer Protocol	#T1020 Automated Exfiltration	
									#T1065 Uncommonly Used Port		

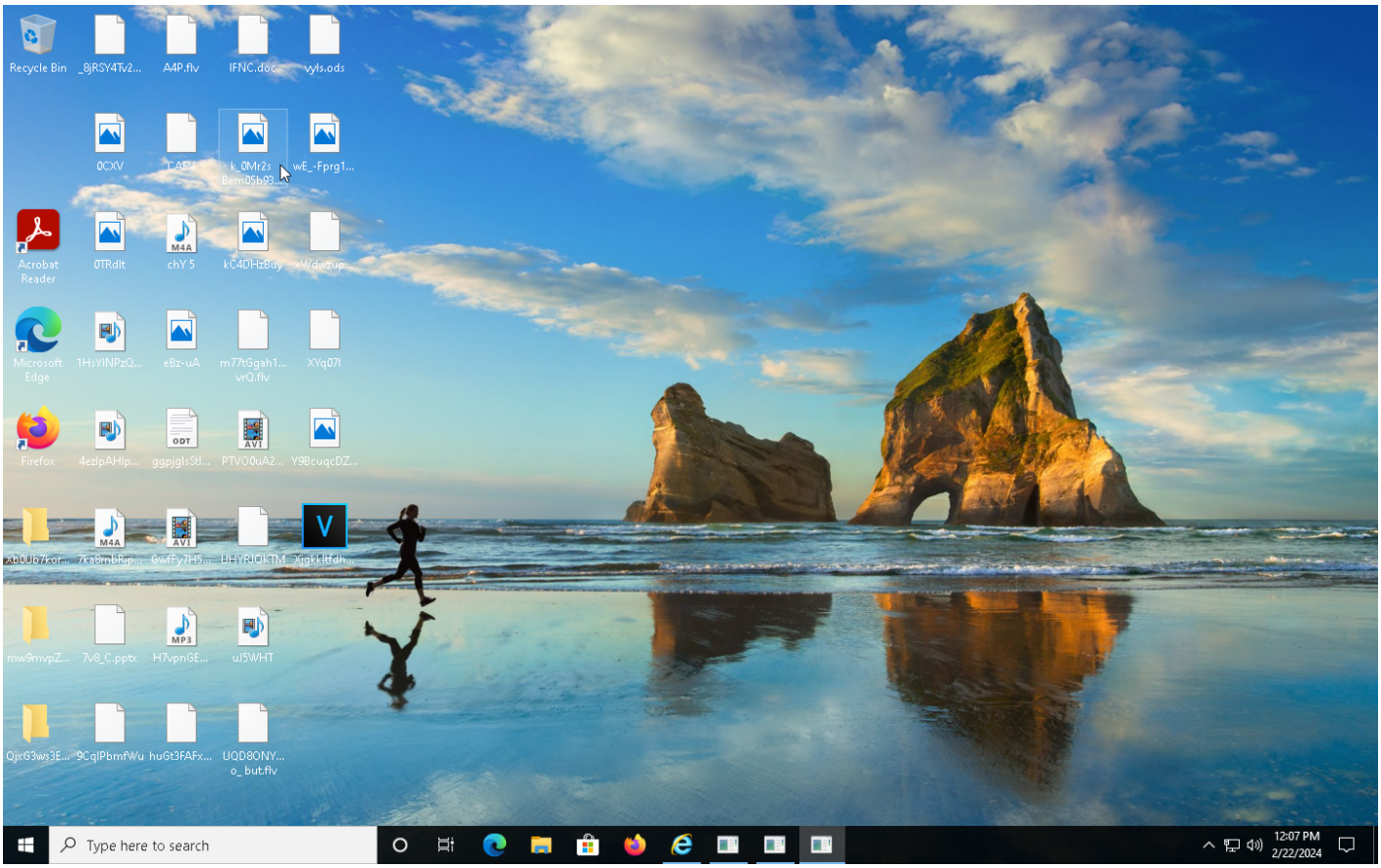
Sample Information

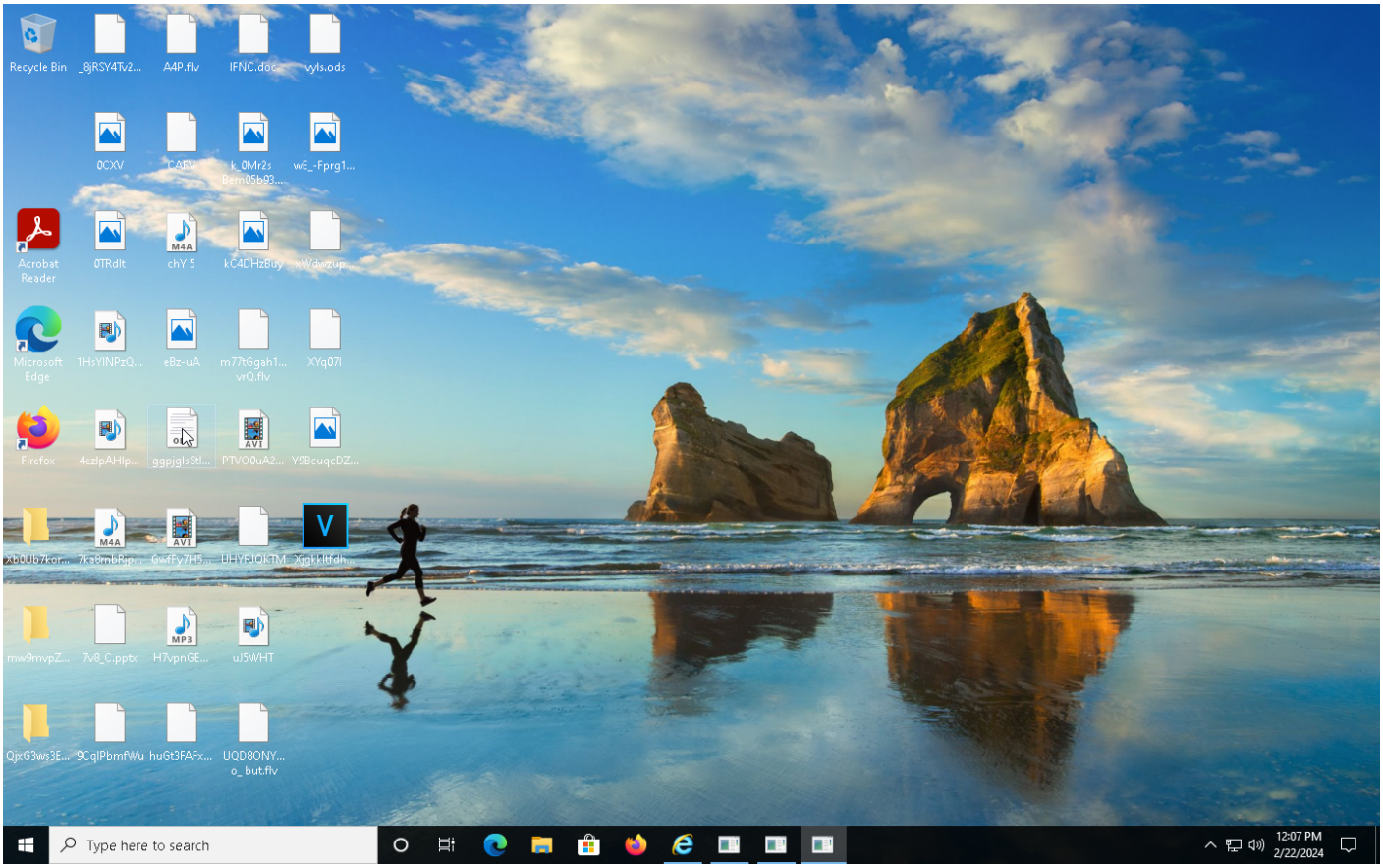
ID	#9928494
MD5	2a3a840641803b101b86e0c321b0a5fe
SHA1	52bc3e121f44c4f9e71b43110f468886294c7fc2
SHA256	b025e37611168c0abcc446125a8bd7cb831625338434929febadfcc9cc4c816e
SSDeep	49152:zCXtvRXOhEc2MgyyuTEGQp8EamZaFChW7ZaxJmLufu4l:zCxRXOhEc2MgJHTp+isL1
ImpHash	5e4731b579fcbf2ee2d5b665a7fef172
File Name	Xjgkkltfdhdfhfjg.exe
File Size	3328.09 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2024-02-22 11:01 (UTC)
Analysis Duration	00:03:29
Termination Reason	Timeout
Number of Monitored Processes	2
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	59


Recycle Bin
Acrobat Reader
Microsoft Edge
Firefox
Type here to search
12:05 PM
2/22/2024





Screenshots truncated

NETWORK

General

137.21 KB total sent

50.38 KB total received

14 ports 5632, 2083, 5000, 13721, 2221, 2223, 2224, 9785, 13783, 13785, 5242, 5243, 445, 2078

16 contacted IP addresses

2 URLs extracted

2 files downloaded

15 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

13 URLs contacted, 13 servers

13 sessions, 128.33 KB sent, 44.62 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxps://85[.]239[.]243[.]155:5000/api/admin.users.session.reset	-	-	-	0 bytes	MALICIOUS
POST	hxxps://104[.]129[.]55[.]106:13783/api/admin.users.session.reset	-	-	-	0 bytes	CLEAN
POST	hxxps://86[.]38[.]225[.]105:13721/api/admin.emoji.add	-	-	-	0 bytes	MALICIOUS
POST	hxxps://104[.]129[.]55[.]105:2223/api/admin.users.session.reset	-	-	-	0 bytes	MALICIOUS
POST	hxxps://89[.]117[.]23[.]185:2221/api/admin.apps.restrict	-	-	-	0 bytes	MALICIOUS
POST	hxxps://145[.]239[.]135[.]24:5243/api/admin.users.session.reset	-	-	-	0 bytes	MALICIOUS
POST	hxxps://23[.]226[.]138[.]143:2083/api/admin.emoji.addAlias	-	-	-	0 bytes	MALICIOUS
POST	hxxps://154[.]12[.]233[.]66:2224/api/admin.usergroups.addTeams	-	-	-	0 bytes	MALICIOUS
POST	hxxps://178[.]18[.]246[.]136:2078/api/admin.usergroups.addTeams	-	-	-	0 bytes	MALICIOUS
POST	hxxps://37[.]60[.]242[.]85:9785/api/admin.emoji.addAlias	-	-	-	0 bytes	MALICIOUS
POST	hxxps://57[.]128[.]165[.]176:13721/api/admin.users.session.reset	-	-	-	0 bytes	MALICIOUS
POST	hxxps://103[.]82[.]243[.]5:13785/api/admin.users.session.reset	-	-	-	0 bytes	MALICIOUS
POST	hxxps://89[.]117[.]23[.]186:5632/api/admin.emoji.addAlias	-	-	-	0 bytes	MALICIOUS
POST	hxxps://23[.]226[.]138[.]161:5242/api/admin.usergroups.addTeams	-	-	-	0 bytes	MALICIOUS
POST	hxxps://86[.]38[.]225[.]106:2221/api/admin.emoji.addAlias	-	-	-	0 bytes	MALICIOUS

BEHAVIOR

Process Graph

Process #1: xjgkkltfdhdfhfjg.exe

ID	1
File Name	c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe
Command Line	"C:\Users\OqXZRaykm\Desktop\Xjgkkltfdhdfhfjg.exe"
Initial Working Directory	C:\Users\OqXZRaykm\Desktop\
Monitor Start Time	Start Time: 213853, Reason: Analysis Target
Unmonitor End Time	End Time: 342514, Reason: Terminated
Monitor duration	128.66s
Return Code	1
PID	3668
Parent PID	-
Bitness	32 Bit

Host Behavior

Type	Count
Module	4200
File	3
Environment	1
System	1460
Keyboard	4687
-	1
-	3
Process	499
-	10
-	3

Process #2: ctfmon.exe

ID	2
File Name	c:\windows\syswow64\ctfmon.exe
Command Line	"C:\Windows\SysWOW64\ctfmon.exe -p 1234"
Initial Working Directory	C:\Windows\SysWOW64[illegible].\??\C:\Windows\SysWOW64\ctfmon.exe\
Monitor Start Time	Start Time: 339354, Reason: Child Process
Unmonitor End Time	End Time: 419540, Reason: Terminated by timeout
Monitor duration	80.19s
Return Code	Unknown
PID	2708
Parent PID	3668
Bitness	32 Bit

Injection Information (9)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0xe0000(917504)	0x400	✔	1
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0xe1000(921600)	0xdc00	✔	1
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0xef000(978944)	0x2c00	✔	1
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0xf2000(991232)	0x1e00	✔	1
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0xf4000(999424)	0x200	✔	1
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0xf5000(1003520)	0x200	✔	1
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0xf6000(1007616)	0x1600	✔	1
Modify Control Flow	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0 / 0x6b0	0x77d13670(2010199664)	-	✔	1
Modify Memory	#1: c:\users\oqxzraykm\desktop\xjgkkltfdhdfhfjg.exe	0xdf0	0x3fc008(4177928)	0x4	✔	1

Host Behavior

Type	Count
Module	8
Mutex	1
-	66
Process	246
User	2
System	4

Network Behavior

Type	Count
HTTPS	15
TCP	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b025e37611168c0abcc446125a8bd7cb831625338434929febadfcc9cc4c816e	C:\Users\OqXZRaykm\Desktop\XjgkkltfdhdfhfjG.exe	Sample File	3328.09 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
f83602d9c77a7a3a61058f6b2aaecbe0237346972dbab4b0750d56476c2019b9	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
5e92e51f91b6ca831cd69e4c9598e069f778933864beade21caf387ea93721ef	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b0f4d4e844518babfefd8bd59b9e1765d9b7bcfac9bfb86076b10ac986befb5d	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
5141198c8bd52c60e07e330d1773865c22037b7ecfe16be31488f760f83fa712	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
04f191979f0cc68a7a11134a8d787f371667af0ca167611c395a9a8d80fd1a81	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
b904317a3220a76ec571db7d9e5a48dd91493ad3e514007ae73a32a70b503704	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
2af1ab90c7b09660ffbfeb3b31d3f6dd500393c830938aeb157f9e00d6633963	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
4e99b8fba162948153bd30382bd2c9fa73308e319ee54be571f975137cdaf9d9	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
4d191d4b6b6f239d7af2abf10f4d30130dd599fda9898d06ebdc7bc2242f2821	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
7eaf8469518a59171cd115da67643ab31e100aadc4d067da975607fc7bac46a9	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
ec9f44a31c0be3076072153014c993871bf6269bd529906da80cf4af5c0b8187	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a89e8e09aabe0b3add9082a448a897e09cd123ae285f02e6b2f5fe1234e1c644	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
664ce9a6e2fc47c7ffb6199376c181e18385138da02e7739fb728b06c57df725	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
f791e931ba9878e28d99751826f46df72d53d9f237822e8e414afa34ed72ff35	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
34a5279830bcd192b197d2a69207f65f5543ddb680c565d1da53af6324aa03b9	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
fb242e53483aa2a9975b649898e3610905400743447c9f61217db82b957e5d1a4	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0e42930948b4dd5471a7fdbea09e589f5d553601499f0653341104e5cd120878	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c2e49b39b8accd4798152c23cb51c192e9ec8346bdd0d5ba63e9ec3c401358ae	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
418f3f4080f176f80638dbd532bb5d9bace11b56951b5181dd1f628bf69b4684	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
32f699329104e9bb55cef42a10aa2cc352942b3e734842c18fbdc5fc653fbfeb	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8285419ab9f0d8bbbc7ce73c795497e838aad9da7965d2abd921d5466f694681	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
6d0d3fb4d34c620204544ffcdd6c35a66bc9d61484a805cfaa3cc9753c4d205f	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
c0bbf2703fd7ca7e84d03cc38e17a3bb686b275fedee6ab27ebef88f342c7c1d	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
1b8f8ebd195c301ebbdda9e0aa576c60fc72236331ad0f0f562e3e8d53ee8649	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e2ab7fc883bbd5acacd4c048505c041bc4e34895d77082a2f0c1161c9d40dc0d	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
89aedd0e9057f27486b5b531d0658ae9336ae7d91724868f16f2da8323b47cfd	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
6a96741d54e6906e494d549cbd152e07839709bb7e850d6cfaed8141e3b02db3	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
3593143fa301c8ccc6e5c6090b09bbd77c8bf0c6436745266e86a69aff6cad8a	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
9c7dd13bdeae6861be84c30870c0fe79a5f1332b3c3d684ffcc7c1f1683a2c40	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
084ad50a09cf56f259c05a00890a489d0a03e01a431b6115df344cf3939a450f	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
92ca5e3b93b03639d4f3d642c32274402077ce5a9ab78a3825a1c6d4d044017b	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e4f0ab2c56b6821a163d3cee830f7841a3fb9a340dda21194cd6ea130043db4c	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8710c78e1d7ecb3d260c508950600571285ab5c03a51b88804d8f3a165aa4cb4	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
864ebaf3986e3086446ab3b3d114b79395fb5e80cbbe43707a1ae172cd502c3f	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
9a7d88c5939b46428c5b609f17a31d854332e772958be1b53bc930eae0e48425	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
71a70f57ff04bba6ddbc01114bcc78626905824b59040cc4066f158b8daaf445	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
50b0810156942325f69eecd23a41ffe49015553a1fb443324629a4e4c7c9c3a1	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e6aed3a8dfeb99ce0fc6ff7121d65f9f0ba01838c7b2e5aa50e3e265f689897c	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
6cda844e5e38449f3f6003333e3c10d7c64b9ed0659e1573801a353dd89b4164	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
54172ddc51303308c33a1d341b720830c41c4c2b2f094442de57de71da25bcad	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
5f4b2dd4c24d58b71a3d5cf0aabbb01e2c1cc1faa25d02a479b1db1b728b871c	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3d66e95f4b798c931cb321ff65327aa179a2ecaebc89c587180dbc0fb54cebb0	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
aef09e00b1cebca03a0ee872cc9481915b9438733940c938d2070d2bccc7e2f0	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a672eb90e76c0cfb4df88823593f061f749c9ecc4b04612e78e029e20cb53b83	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
26447370ee0a08474bb6cf6e608d14274a238d62d82094a0083ac33477d23701	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e47dff8e4fa01e848c9d3ec30629849da9240ba2d537af4e0f6fb7c7e2a189ef	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
faca0cc75510d7ece45e1fae7001fe0c2e549211917bb5b2775293813b40a8dc	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
d2deb2059355d5d40dc1c3e9591ac76555b5c0f4a6f88aebd99d34470253f847	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
99a017b00abb19cd9b25f94041d2874db6bf296673020d90b368657c4e2ac5ca	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
9c0457858ca37e693b631f1187f5ecae0f7c4f5d096a60df37a501f4087f0518	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
e752f938e5ec1423a0de218467195f530f21a34d1504b3db777d557f3d750902	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
38ed6ea6fef18ee65ad81fce59a1724264528463bdeea7f14a3562d21404f216	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a2936836368451e36fdb259dc88dd66caaafc5bad99b44817edf26e2e52d27c2	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
9f5b46b611db8746cecbbdb913d2fa00960961f98ecacbad678abadc1ad69d0c	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
0a1d3f89ea930f38543c030605d39cd91f97c78ec14e0082a5bf2fe6b9e14cd0	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
df7f797a426d60c10f09b05fe25cc4bd1271c392c06f6b30a7aa3708ee384698	-	Memory Dump	208.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
a3df83e7b8091e37d738a2f9fa99d4cfffef20d270ed6ef24e47c9c284e6a5db	-	Memory Dump	1024.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
ad991fedff4ae8471f5f8ba1efe55b4efe1aec6104680f6ae0d90fcdb9bf1ba8	-	Memory Dump	196.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
dd770c0d8301a5bf7408d98be823da7ec0ee7a30793b6f3e43a3f7f66bb779c3	-	Downloaded File	7.46 KB	application/octet-stream	-	CLEAN
5fd55da8747d933410bb637571802aca2eedf3314039722e2b9d6f37afdad97e	-	Downloaded File	552 bytes	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\OqXZRaykm\Desktop\XjgkkItfdhdfhfjg.exe	Accessed File, Sample File	Access	MALICIOUS

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://23[.]226[.]138[.]143:2083/api/admin.emoji.addAlias	Extracted, Contacted	23.226.138.143	United States	POST	MALICIOUS
hxxps://23[.]226[.]138[.]161:5242/api/admin.usergroups.addTeams	Extracted, Contacted	23.226.138.161	United States	POST	MALICIOUS
hxxps://37[.]60[.]242[.]85:9785/api/admin.emoji.addAlias	Extracted, Contacted	37.60.242.85	Germany	POST	MALICIOUS
hxxps://57[.]128[.]165[.]176:13721/api/admin.users.session.reset	Extracted, Contacted	57.128.165.176	United Kingdom	POST	MALICIOUS
hxxps://86[.]38[.]225[.]105:13721/api/admin.emoji.add	Extracted, Contacted	86.38.225.105	United States	POST	MALICIOUS
hxxps://86[.]38[.]225[.]106:2221/api/admin.emoji.addAlias	Extracted, Contacted	86.38.225.106	United States	POST	MALICIOUS
hxxps://89[.]117[.]23[.]185:2221/api/admin.apps.restrict	Extracted, Contacted	89.117.23.185	United States	POST	MALICIOUS
hxxps://89[.]117[.]23[.]186:5632/api/admin.emoji.addAlias	Extracted, Contacted	89.117.23.186	United States	POST	MALICIOUS
hxxps://103[.]82[.]243[.]5:13785/api/admin.users.session.reset	Extracted, Contacted	103.82.243.5	Indonesia	POST	MALICIOUS
hxxps://145[.]239[.]135[.]24:5243/api/admin.users.session.reset	Extracted, Contacted	145.239.135.24	France	POST	MALICIOUS
hxxps://154[.]12[.]233[.]66:2224/api/admin.usergroups.addTeams	Extracted, Contacted	154.12.233.66	United States	POST	MALICIOUS
hxxps://178[.]18[.]246[.]136:2078/api/admin.usergroups.addTeams	Extracted, Contacted	178.18.246.136	Germany	POST	MALICIOUS
hxxps://85[.]239[.]243[.]155:5000/api/admin.users.session.reset	Extracted	85.239.243.155	United States	-	MALICIOUS
hxxps://104[.]129[.]55[.]105:2223/api/admin.users.session.reset	Extracted, Contacted	104.129.55.105	United States	POST	CLEAN
hxxps://104[.]129[.]55[.]106:13783/api/admin.users.session.reset	Extracted	104.129.55.106	United States	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
23.226.138.143	-	United States	HTTPS, TCP	MALICIOUS
23.226.138.161	-	United States	HTTPS, TCP	MALICIOUS
37.60.242.85	-	Germany	HTTPS, TCP	MALICIOUS
57.128.165.176	-	United Kingdom	HTTPS, TCP	MALICIOUS
86.38.225.105	-	United States	HTTPS, TCP	MALICIOUS
86.38.225.106	-	United States	HTTPS, TCP	MALICIOUS
89.117.23.185	-	United States	HTTPS, TCP	MALICIOUS
89.117.23.186	-	United States	HTTPS, TCP	MALICIOUS
103.82.243.5	-	Indonesia	HTTPS, TCP	MALICIOUS
104.129.55.105	-	United States	HTTPS, TCP	MALICIOUS
145.239.135.24	-	France	HTTPS, TCP	MALICIOUS
154.12.233.66	-	United States	HTTPS, TCP	MALICIOUS
178.18.246.136	-	Germany	HTTPS, TCP	MALICIOUS
85.239.243.155	-	United States	TCP, TLS	MALICIOUS

IP Address	Domains	Country	Protocols	Verdict
104.129.55.106	-	United States	TCP, TLS	MALICIOUS

Mutex

Name	Operations	Parent Process Name	Verdict
{9ED9ADD7-B212-43E5-ACE9-B2E05ED5D524}	access	ctfmon.exe	CLEAN

Process

Process Name	Commandline	Verdict
xjgkkltfdhdfhfjg.exe	"C:\Users\OqXZRaykm\Desktop\Xjgkkltfdhdfhfjg.exe"	MALICIOUS
ctfmon.exe	"C:\Windows\SysWOW64\ctfmon.exe -p 1234"	SUSPICIOUS

YARA / AV

YARA (59)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_FunctionStrings_Feb2024	Pikabot Function Strings	Function Strings	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5
Malware	Pikabot_Indirect_Syscalls	Pikabot's function to resolve and call NT APIs via indirect system calls	Memory Dump	-	Downloader	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_20h1_en_base
Description	windows 10 (64bit 20H1 -EN-)
Architecture	x86 64-bit
Operating System	Windows 10 20H1
Kernel Version	10.0.19041.208 (dc9233f8-5819-e3d0-929a-7bde0b87f0b9)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.1.2
Dynamic Engine Version	2024.1.2 / 02/16/2024 05:23
Static Engine Version	2024.1.2.0 / 2024-02-16 04:00:11
AV Exceptions Version	2024.1.2.24 / 2024-02-12 14:04:13
Link Detonation Heuristics Version	2024.1.2.26 / 2024-02-15 15:11:55
Smart Memory Dumping Rules Version	2024.1.2.24 / 2024-02-12 14:04:13
Config Extractors Version	2024.1.2.26 / 2024-02-15 15:11:55
Signature Trust Store Version	2024.1.2.24 / 2024-02-12 14:04:13
VMRay Threat Identifiers Version	2024.1.2.26 / 2024-02-15 15:11:55
YARA Built-in Ruleset Version	2024.1.2.26

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	Not installed
Microsoft Office Version	Not installed
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.207.19041.0
Chrome Version	Not installed
Firefox Version	108.0
Flash Version	Not installed
Java Version	8.0.3610.9

System Information

Sample Directory	C:\Users\OqXZRaykm\Desktop
Computer Name	PXTHFFRYO7
User Domain	PXTHFFRYO7
User Name	OqXZRaykm
User Profile	C:\Users\OqXZRaykm
Temp Directory	C:\Users\OQXZRA~1\AppData\Local\Temp

System Root	C:\Windows