MALICIOUS

Classifications: Spyware | Downloader | Exploit

Threat Names: Lokibot | Lokibot.v2 | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Word Document**
File Name	**Purchase Order.doc**
ID	#10614422
MD5	58fa856ae520dc6c6e47f4b459e2de5b
SHA1	89c76a3bcb6a83cb1b343f5ea03cfc2da2214e97
SHA256	425ef5b31a93a014e2ff74d66c148a7b73b0fb2a57ab2e015576cb2272db5dfb
File Size	16.04 KB
Report Created	2024-06-10 06:33 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | ms_office

OVERVIEW

VMRay Threat Identifiers (28 rules, 74 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Lokibot configuration was extracted	1	Spyware
	• A configuration for Lokibot was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• YARA detected "Lokibot" from ruleset "Malware" in memory dump data from (process #10) alpha73882.scr.			
5/5	Data Collection	Tries to read cached credentials of various applications	1	Spyware
	• Tries to read sensitive data of: Bitvise SSH Client, BlazeFTP, Internet Explorer, Microsoft Outlook, SecureFX, Total Commander, Trojita.			
4/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #6) alpha73882.scr reads from (process #10) alpha73882.scr.			
4/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
4/5	Exploit	Exploits a vulnerability in MS Office	1	Exploit
	• Exploits equation editor vulnerability CVE-2017-11882 or CVE-2018-0802 in MS Office.			
4/5	Network Connection	Downloads executable	1	Downloader
	• (Process #4) eqnedt32.exe downloads Windows executable via http from hxxps://dukeenergyltd[.]top/alpha.scr.			
4/5	Network Connection	Downloads file	1	Downloader
	• Downloads file via http from hxxps://dukeenergyltd[.]top/alpha.doc.			
4/5	Network Connection	Attempts to connect through HTTPS	1	-
	• (Process #4) eqnedt32.exe connects to hxxps://dukeenergyltd[.]top/alpha.scr.			
4/5	Heuristics	Document contains a phishing URL	1	-
	• Document "C:\Users\RDhJ0CNFevzX\Desktop\Purchase Order.doc" contains a phishing URL hxxps://dukeenergyltd[.]top/alpha.doc.			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #6) alpha73882.scr.			
4/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #6) alpha73882.scr modifies memory of (process #10) alpha73882.scr.			
4/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #6) alpha73882.scr alters context of (process #10) alpha73882.scr.			
4/5	Reputation	Malicious host or URL detected via reputation	4	-

Score	Category	Operation	Count	Classification
	• Reputation analysis labels the contacted URL "hxxps://dukeenergyltd[.]top/alpha.doc" as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxps://dukeenergyltd[.]top/alpha.scr" which was contacted by (process #4) eqnedt32.exe as Mal/HTMLGen-A. • Reputation analysis labels the contacted URL "hxxps://dukeenergyltd[.]top" as Mal/HTMLGen-A. • Reputation analysis labels the resolved domain "dukeenergyltd.top" as Mal/HTMLGen-A.			
4/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\xaFodrmIsC.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\xaFodrmIsC.exe", to be triggered by REGISTRATION.			
3/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #6) alpha73882.scr enables process privilege "SeDebugPrivilege".			
3/5	Discovery	Reads system data	1	-
	• (Process #10) alpha73882.scr reads the cryptographic machine GUID from registry.			
2/5	Discovery	Possibly does reconnaissance	14	-
	• (Process #10) alpha73882.scr tries to gather information about application "Mozilla Firefox" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Comodo IceDragon" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Safari" by registry. • (Process #10) alpha73882.scr tries to gather information about application "K-Meleon" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Mozilla SeaMonkey" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Mozilla Flock" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Cyberfox" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Total Commander" by registry. • (Process #10) alpha73882.scr tries to gather information about application "NetScape" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Default Programs" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Bitvise SSH Client" by registry. • (Process #10) alpha73882.scr tries to gather information about application "SecureFX" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Postbox" by registry. • (Process #10) alpha73882.scr tries to gather information about application "Trojita" by registry.			
2/5	Discovery	Searches for sensitive browser data	14	-
	• (Process #10) alpha73882.scr searches for sensitive data of web browser "Comodo Dragon" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Maple Studio" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Google Chrome" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Chromium" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Torch" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Yandex Browser" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Epic Privacy Browser" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "CocCoc" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Vivaldi" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Chrome Canary" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Orbitum" by file. • (Process #10) alpha73882.scr searches for sensitive data of web browser "Opera" by file. • (Process #10) alpha73882.scr tries to access sensitive data of web browser "QtWeb Internet Browser" by registry. • (Process #10) alpha73882.scr tries to access sensitive data of web browser "Internet Explorer / Edge" by registry.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #10) alpha73882.scr tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.			

Score	Category	Operation	Count	Classification
2/5	Discovery	Searches for sensitive application data	4	-

- (Process #10) alpha73882.scr searches for sensitive data of application "Pidgin" by file.
- (Process #10) alpha73882.scr tries to access sensitive data of application "KiTTY" by registry.
- (Process #10) alpha73882.scr tries to access sensitive data of application "PuTTY" by registry.
- (Process #10) alpha73882.scr tries to access sensitive data of application "WinChips" by registry.

Score	Category	Operation	Count	Classification
2/5	Discovery	Searches for sensitive FTP data	7	-

- (Process #10) alpha73882.scr tries to access sensitive data of FTP application "LinasFTP" by registry.
- (Process #10) alpha73882.scr searches for sensitive data of FTP application "FileZilla" by file.
- (Process #10) alpha73882.scr searches for sensitive data of FTP application "BlazeFTP" by file.
- (Process #10) alpha73882.scr tries to access sensitive data of FTP application "FAR Manager" by registry.
- (Process #10) alpha73882.scr tries to access sensitive data of FTP application "NCH Fling" by registry.
- (Process #10) alpha73882.scr tries to access sensitive data of FTP application "NCH Classic FTP" by registry.
- (Process #10) alpha73882.scr searches for sensitive data of FTP application "FTP Navigator" by file.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive FTP data	3	-

- (Process #10) alpha73882.scr tries to read sensitive data of FTP application "BlazeFTP" by registry.
- (Process #10) alpha73882.scr tries to read sensitive data of FTP application "Total Commander" by registry.
- (Process #10) alpha73882.scr tries to read sensitive data of FTP application "SecureFX" by registry.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive application data	1	-

- (Process #10) alpha73882.scr tries to read sensitive data of application "Bitvise SSH Client" by registry.

Score	Category	Operation	Count	Classification
2/5	Discovery	Searches for sensitive mail data	4	-

- (Process #10) alpha73882.scr searches for sensitive data of mail application "Pocomail" by file.
- (Process #10) alpha73882.scr tries to access sensitive data of mail application "IncrediMail" by registry.
- (Process #10) alpha73882.scr searches for sensitive data of mail application "Opera Mail" by file.
- (Process #10) alpha73882.scr tries to access sensitive data of mail application "Microsoft Outlook" by registry.

Score	Category	Operation	Count	Classification
2/5	Data Collection	Reads sensitive mail data	2	-

- (Process #10) alpha73882.scr tries to read sensitive data of mail application "Microsoft Outlook" by registry.
- (Process #10) alpha73882.scr tries to read sensitive data of mail application "Trojita" by registry.

Score	Category	Operation	Count	Classification
2/5	Heuristics	Signed executable failed signature validation	1	-

- C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr is signed, but signature validation failed.

Score	Category	Operation	Count	Classification
1/5	Mutex	Creates mutex	2	-

- (Process #6) alpha73882.scr creates mutex with name "jXwztFZgjbeeUxrVPcVRAVtAjVu".
- (Process #10) alpha73882.scr creates mutex with name "B7274519EDDE9BDC8AE51348".

Malware Configuration: Lokibot

Metadata	Key	Extracted Value
Encryption Key	Key Tags Algorithm Mode Iv Key Tags Algorithm	+GrwTafWkea+mP09tlubezd5OJSV+VEl Encryption Key #0 3DES CBC TPh5m1q9osA= /w== Encryption Key #1 XOR
URL	Url Tags Url Tags Url Tags Url Tags Url Tags	alphastand.win/alien/fre.php Encrypted with Key #0 alphastand.trade/alien/fre.php Encrypted with Key #0 kbfvzoboss.bid/alien/fre.php Encrypted with Key #0 alphastand.top/alien/fre.php Encrypted with Key #0 alphabetllc.top/alpha/five/fre.php Encrypted with Key #1
Other: Version Identifier	Tags Value	Identifier in Network Packets ckav.ru

Mitre ATT&CK Matrix

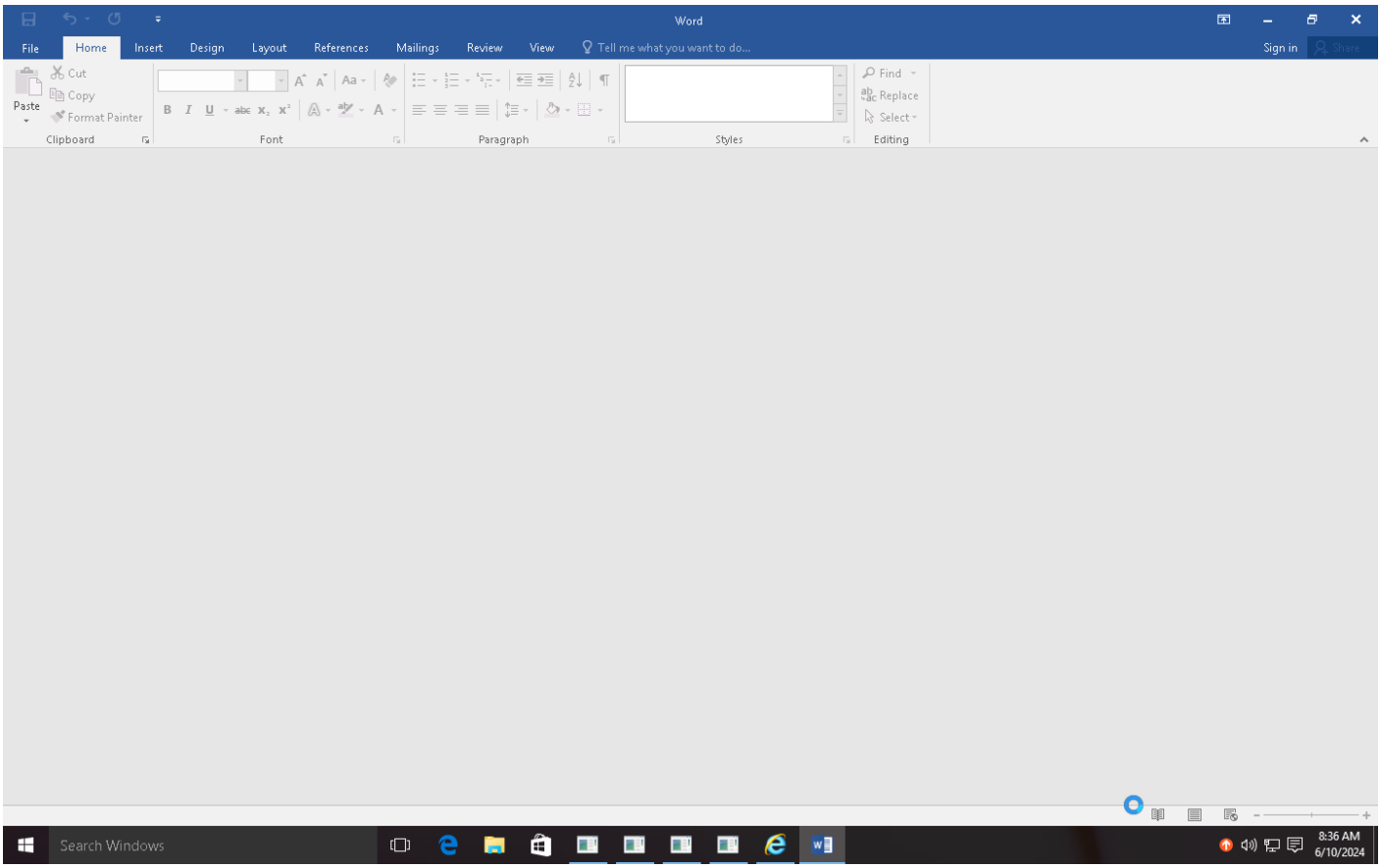
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
#T1193 Spearphishing Attachment	#T1203 Exploitation for Client Execution	#T1053 Scheduled Task	#T1053 Scheduled Task		#T1081 Credentials in Files	#T1082 System Information Discovery	#T1105 Remote File Copy	#T1119 Automated Collection	#T1071 Standard Application Layer Protocol		
	#T1053 Scheduled Task				#T1214 Credentials in Registry	#T1012 Query Registry		#T1005 Data from Local System	#T1105 Remote File Copy		
					#T1003 Credential Dumping	#T1083 File and Directory Discovery			#T1032 Standard Cryptographic Protocol		
						#T1217 Browser Bookmark Discovery					

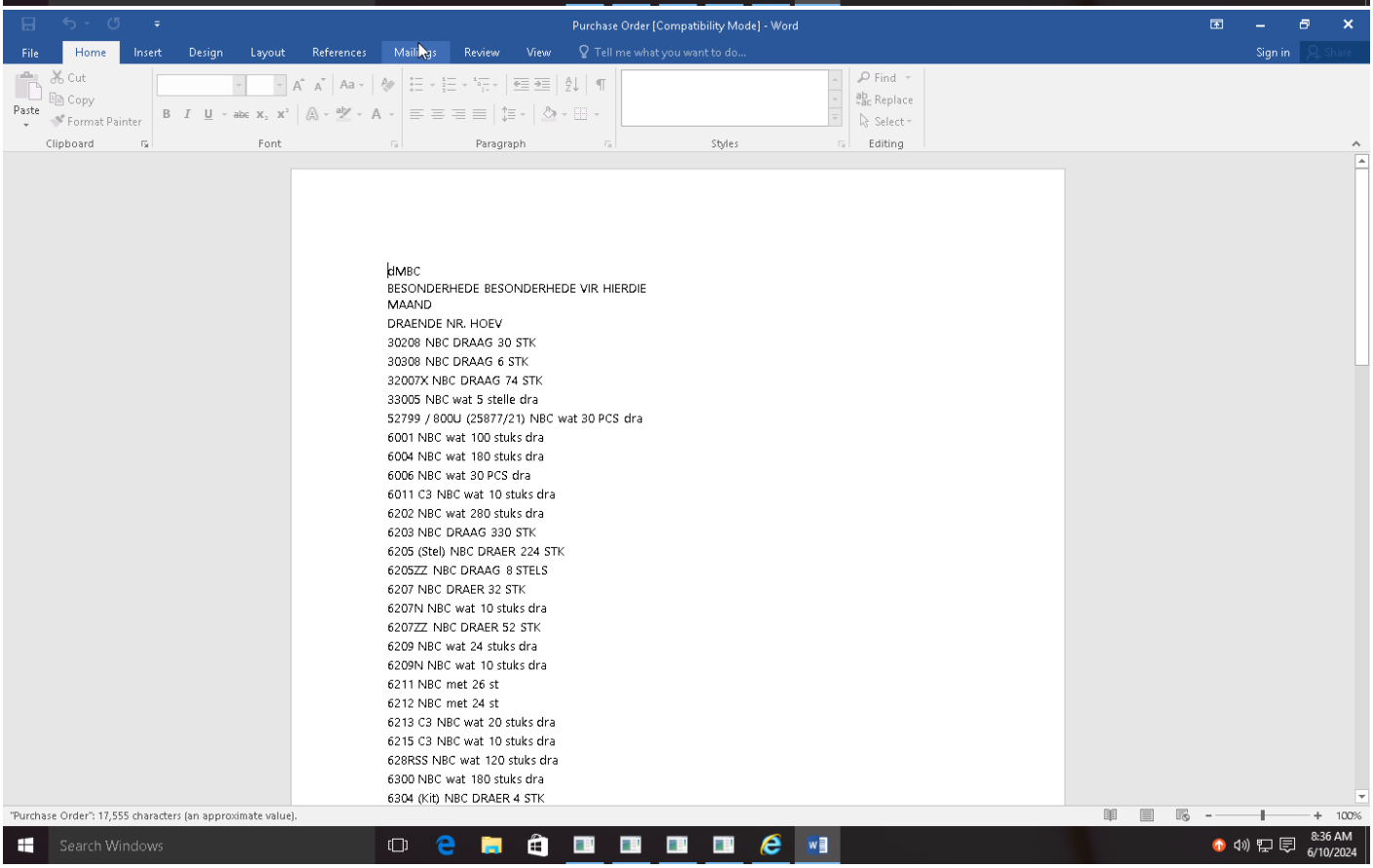
Sample Information

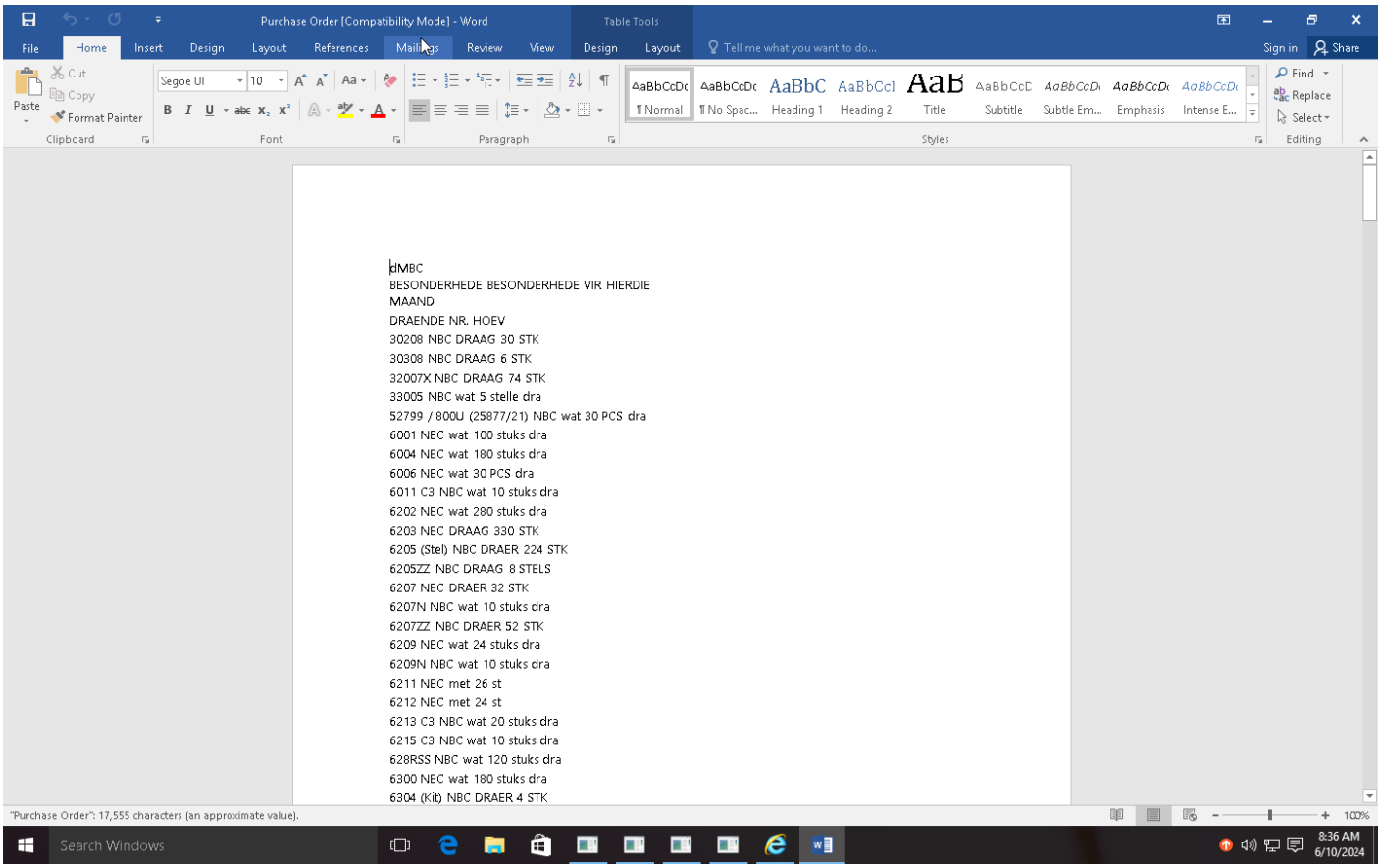
ID	#10614422
MD5	58fa856ae520dc6c6e47f4b459e2de5b
SHA1	89c76a3bcb6a83cb1b343f5ea03cfc2da2214e97
SHA256	425ef5b31a93a014e2ff74d66c148a7b73b0fb2a57ab2e015576cb2272db5dfb
SSDeep	384:IyXnXK3Wgs8PL8wi4OEwH8TIbE91r2fRcJYzviML2nkPt:Icnyb5P3DOqnYJamvtL2nkF
File Name	Purchase Order.doc
File Size	16.04 KB
Sample Type	Word Document
Has Macros	✔

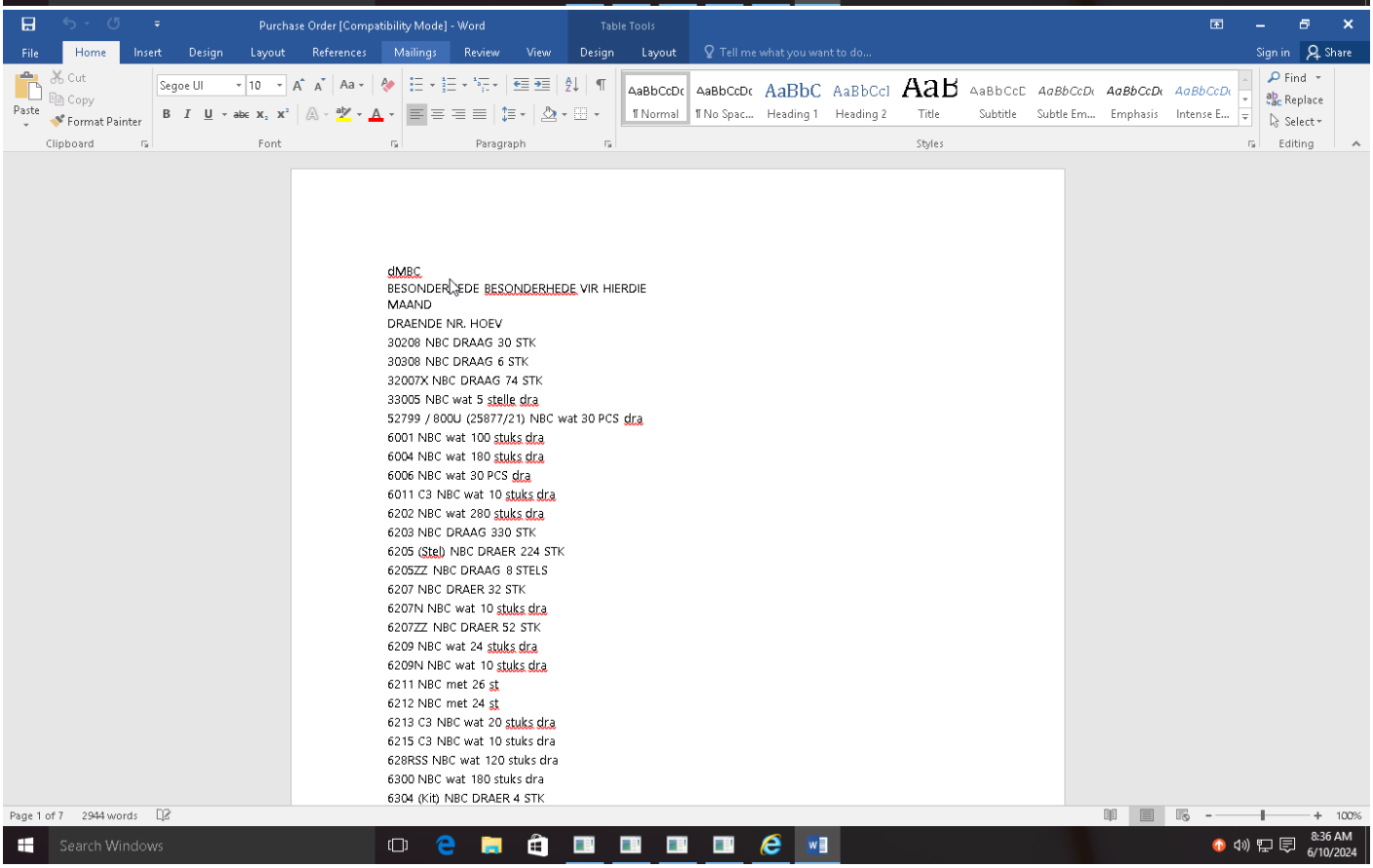
Analysis Information

Creation Time	2024-06-10 06:33 (UTC)
Analysis Duration	00:04:02
Termination Reason	Timeout
Number of Monitored Processes	8
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	1


Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
Search Windows
8:36 AM
6/10/2024


Purchase Order [Compatibility Mode] - Word
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Font
Paragraph
Styles
Find
Replace
Select
Editing
dMBC
BESONDERHEDE BESONDERHEDE VIR HIERDIE MAAND
DRAENDE NR. HOEV
30208 NBC DRAAG 30 STK
30308 NBC DRAAG 6 STK
32007X NBC DRAAG 74 STK
33005 NBC wat 5 stelle dra
52799 / 800U (25877/21) NBC wat 30 PCS dra
6001 NBC wat 100 stuks dra
6004 NBC wat 180 stuks dra
6006 NBC wat 30 PCS dra
6011 C3 NBC wat 10 stuks dra
6202 NBC wat 280 stuks dra
6203 NBC DRAAG 330 STK
6205 (Stel) NBC DRAER 224 STK
6205ZZ NBC DRAAG 8 STELS
6207 NBC DRAER 32 STK
6207N NBC wat 10 stuks dra
6207ZZ NBC DRAER 52 STK
6209 NBC wat 24 stuks dra
6209N NBC wat 10 stuks dra
6211 NBC met 26 st
6212 NBC met 24 st
6213 C3 NBC wat 20 stuks dra
6215 C3 NBC wat 10 stuks dra
628RSS NBC wat 120 stuks dra
6300 NBC wat 180 stuks dra
6304 (Kit) NBC DRAER 4 STK
"Purchase Order": 17,555 characters (an approximate value).
100%
Search Windows
8:36 AM
6/10/2024





Screenshots truncated

NETWORK

General

5.07 KB total sent

1057.75 KB total received

2 ports 443, 53

2 contacted IP addresses

5 URLs extracted

2 files downloaded

1 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

3 URLs contacted, 1 servers

3 sessions, 9.97 KB sent, 1517.18 KB received

HTTP Requests

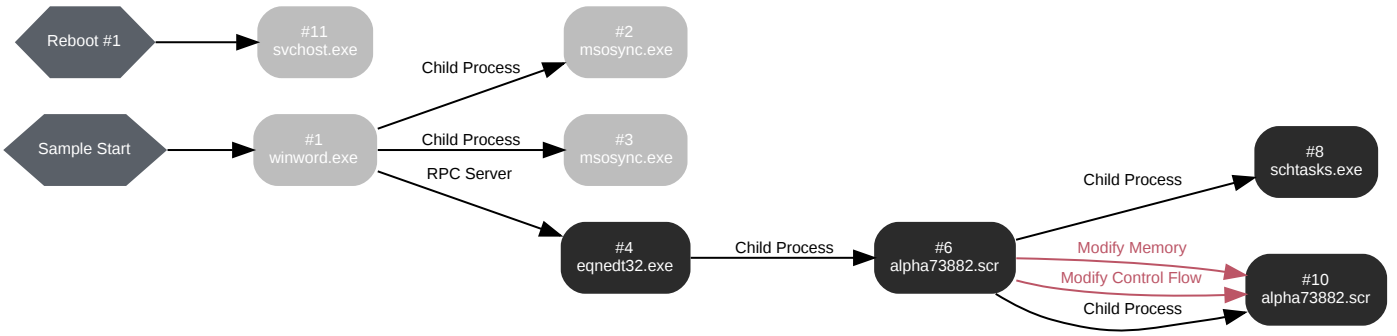
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://dukeenergyltd[.]top/alpha.doc	-	-	-	0 bytes	MALICIOUS
GET	hxxps://dukeenergyltd[.]top/alpha.scr	-	-	-	0 bytes	MALICIOUS
OPTIONS	hxxps://dukeenergyltd[.]top	-	-	-	0 bytes	MALICIOUS

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	dukeenergyltd[.]top	NO_ERROR	172.67.134.136, 104.21.25.202	-	MALICIOUS

BEHAVIOR

Process Graph



Process #1: winword.exe

ID	1
File Name	c:\program files\microsoft office\office16\winword.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 133678, Reason: Analysis Target
Unmonitor End Time	End Time: 327062, Reason: Terminated
Monitor duration	193.38s
Return Code	0
PID	4884
Parent PID	-
Bitness	64 Bit

Process #2: msosync.exe

ID	2
File Name	c:\program files\microsoft office\office16\msosync.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 143522, Reason: Child Process
Unmonitor End Time	End Time: 338493, Reason: Terminated
Monitor duration	194.97s
Return Code	1073807364
PID	4436
Parent PID	4884
Bitness	64 Bit

Process #3: msosync.exe

ID	3
File Name	c:\program files\microsoft office\office16\msosync.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 143634, Reason: Child Process
Unmonitor End Time	End Time: 147907, Reason: Terminated
Monitor duration	4.27s
Return Code	0
PID	5024
Parent PID	4884
Bitness	64 Bit

Process #4: eqnedt32.exe

ID	4
File Name	c:\program files\common files\microsoft shared\equation\eqnedt32.exe
Command Line	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 153025, Reason: RPC Server
Unmonitor End Time	End Time: 161889, Reason: Terminated
Monitor duration	8.86s
Return Code	0
PID	3532
Parent PID	4884
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr	579.51 KB	91a9acd38a970ddf7fe35f9477d415e9b9befc760c85a4f8e15b045b42a9d689	✖

Host Behavior

Type	Count
Module	6
File	1
Process	1

Network Behavior

Type	Count
HTTPS	1

Process #6: alpha73882.scr

ID	6
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 159447, Reason: Child Process
Unmonitor End Time	End Time: 331359, Reason: Terminated
Monitor duration	171.91s
Return Code	0
PID	3656
Parent PID	3532
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB75D.tmp	1.56 KB	9f09da042e0b44a70976b514e26040c38cca89661c63056072a5fca6562e557c	✖
C:\Users\RDhJ0CNFevzX\AppData\Roaming\xaFodrmIsC.exe	579.51 KB	91a9acd38a970ddf7fe35f9477d415e9b9befc760c85a4f8e15b045b42a9d689	✖

Host Behavior

Type	Count
Registry	4
Module	41
Window	6
File	28
Mutex	2
User	2
System	18
Process	2
-	3
-	8

Process #8: schtasks.exe

ID	8
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xaFodrmIsC" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB75D.tmp"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 300662, Reason: Child Process
Unmonitor End Time	End Time: 314357, Reason: Terminated
Monitor duration	13.70s
Return Code	0
PID	4684
Parent PID	3656
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
COM	1
File	10

Process #10: alpha73882.scr

ID	10
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 314356, Reason: Child Process
Unmonitor End Time	End Time: 337802, Reason: Terminated
Monitor duration	23.45s
Return Code	1073807364
PID	5064
Parent PID	3656
Bitness	32 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr	0xe4c	0x400000(4194304)	0x400	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr	0xe4c	0x401000(4198400)	0x13800	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr	0xe4c	0x415000(4280320)	0x4200	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr	0xe4c	0x41a000(4300800)	0x200	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr	0xe4c	0x4a0000(4849664)	0x2000	✔	1
Modify Memory	#6: c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr	0xe4c	0x300008(3145736)	0x4	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\appdata\roaming\alpha73882.scr	0xe4c / 0x12b8	0x4139de(4274654)	-	✔	1

Host Behavior

Type	Count
Module	853
Registry	180
Mutex	1
File	268
System	14

Process #11: svchost.exe

ID	11
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: 376533, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 376883, Reason: Terminated by timeout
Monitor duration	0.35s
Return Code	Unknown
PID	996
Parent PID	4684
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
425ef5b31a93a014e2ff74d66c148a7b73b0fb2a57ab2e015576cb2272db5dfb	C:\Users\RDhJ0CNFevzX\Desktop\Purchase Order.doc	Sample File	16.04 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
91a9acd38a970ddf7fe35f9477d415e9b9befc760c85a4f8e15b045b42a9d689	C:\Users\RDhJ0CNFevzX\AppData\Roaming\xaFodrmIsC.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr, c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\fqx74zx9\alpha[1].scr	Downloaded File	579.51 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
5b1ea6b3597ad66466174d4ac7487a92d8a5e202ca8cd4bbb2cbbeb46d30f4a2	-	Memory Dump	648.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
f743a86539017023aae3ea9c35d42f092b42dc9ea8bc90154e4b88c6f57fd1f1	-	Downloaded File	421.77 KB	text/rtf	-	CLEAN
f6797c5f8ded41e638543afccb2ef254dfb2b61e8eddf5f23e8e0bac7c0a99f6	-	Extracted File	6.34 KB	image/png	-	CLEAN
9f09da042e0b44a70976b514e26040c38cca89661c63056072a5fca6562e557c	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB75D.tmp	Dropped File	1.56 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\Purchase Order.doc	Sample File	-	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\xaFodrmIsC.exe	Accessed File, Downloaded File, Extracted File	Access, Create, Write	MALICIOUS
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\fqx74zx9\alpha[1].scr	Downloaded File, Extracted File	-	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr	Accessed File, Downloaded File, Extracted File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB75D.tmp	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.config	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://dukeenergyltd[.]top/alpha.doc	Extracted, Contacted	104.21.25.202, 172.67.134.136	United States	HEAD, GET	MALICIOUS
hxxps://dukeenergyltd[.]top/alpha.scr	Extracted, Contacted	104.21.25.202, 172.67.134.136	United States	GET	MALICIOUS
hxxps://dukeenergyltd[.]top	Extracted, Contacted	104.21.25.202, 172.67.134.136	United States	OPTIONS	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://alphastand[.]win/alien/fre.php	Extracted	-	-	-	MALICIOUS
hxxp://alphastand[.]trade/alien/fre.php	Extracted	-	-	-	MALICIOUS
hxxp://kbfvzoboss[.]bid/alien/fre.php	Extracted	-	-	-	MALICIOUS
hxxp://alphastand[.]top/alien/fre.php	Extracted	-	-	-	MALICIOUS
hxxp://alphabetllc[.]top/alpha/five/fre.php	Extracted	-	-	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
dukeenergyltd[.]top	104.21.25.202, 172.67.134.136	United States	HTTPS, DNS, TCP	MALICIOUS
alphastand[.]win	-	-	-	CLEAN
alphastand[.]trade	-	-	-	CLEAN
kbfvzoboss[.]bid	-	-	-	CLEAN
alphastand[.]top	-	-	-	CLEAN
alphabetllc[.]top	-	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
172.67.134.136	dukeenergyltd[.]top	United States	HTTPS, DNS, TCP	CLEAN
104.21.25.202	dukeenergyltd[.]top	-	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
jXwztFZgjbeeUxrVPcVRAVtAjVu	access	alpha73882.scr	CLEAN
B7274519EDDE9BDC8AE51348	access	alpha73882.scr	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\ComodoGroup\IceDragon\Setup\SetupPath	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Apple Computer, Inc.\Safari\InstallDir	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\K-Meleon\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\mozilla.org\SeaMonkey\CurrentVersion	read, access	alpha73882.scr	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\SeaMonkey\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Flock\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox86\RootDir	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\8pecxstudios\Cyberfox\Path	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Pale Moon\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Waterfox\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\LinasFTP\Site Manager	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\FlashPeak\BlazeFtp\Settings\LastPassword	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Ghisler\Total Commander\FtpIniName	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\AppDataLow	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\IM Providers	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Netscape	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\ODBC	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Policies	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\RegisteredApplications	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Wow6432Node	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Classes	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Far\Plugins\FTP\Hosts	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Far2\Plugins\FTP\Hosts	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Bitvise\BvSshClient\LastUsedProfile	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\VanDyke\SecureFX\Config Path	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\Fling\Accounts	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\Fling\Accounts	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\NCH Software\ClassicFTP\FTPAccounts	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\NCH Software\ClassicFTP\FTPAccounts	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\9bis.com\KiTTY\Sessions	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\SimonTatham\PuTTY\Sessions	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\9bis.com\KiTTY\Sessions	access	alpha73882.scr	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\IncrediMail\Identities	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\IncrediMail\Identities	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Martin Prikryl	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\Software\Martin Prikryl	access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Postbox\Postbox\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\FossaMail\CurrentVersion	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\WinChips\UserAccounts	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\2db91c5fd8470d46b1a5bc5efab4cae7\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\6c29d51f56390b45a924b3b787013a66\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8763203907727d498bce4b981b157d7b\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\893893ade607c44aa338ac7df5d6cb42\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	access	alpha73882.scr	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Email Address	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Server	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User Name	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP User	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Server	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User Name	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 User	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Email Address	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP User Name	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Server	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Server	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User Name	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP User	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP User	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Server URL	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail User Name	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Server	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Port	read, access	alpha73882.scr	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Port	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Port	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password2	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password2	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password2	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTPMail Password2	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password2	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\POP3 Password	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\IMAP Password	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\NNTP Password	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\HTTP Password	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002\SMTP Password	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\dc48e7c6d33441458035ee20beefe18a\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\e57f6d0b27b6134693ca7113a4ab34a6\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f35c115766b7c94cb080da6869ae8f9d\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Email	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\imap.auth.pass	read, access	alpha73882.scr	CLEAN
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita\msa.smtp.auth.pass	read, access	alpha73882.scr	CLEAN

Process

Process Name	Commandline	Verdict
alpha73882.scr	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr"	MALICIOUS
eqnedt32.exe	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	SUSPICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\xaFodrmIsC" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpB75D.tmp"	SUSPICIOUS
alpha73882.scr	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\alpha73882.scr"	SUSPICIOUS
winword.exe	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n	CLEAN
msosync.exe	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"	CLEAN
msosync.exe	"C:\Program Files\Microsoft Office\Office16\MsoSync.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	Lokibot	Lokibot Stealer	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.29 / 2024-05-11 04:28:14
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.27 / 2024-05-02 14:06:04
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.31 / 2024-05-17 05:43:49
YARA Built-in Ruleset Version	2024.2.1.32

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows