DYNAMIC ANALYSIS REPORT

#14956977

MALICIOUS

Classifications:	Injector Exploit Spyware Downloader
Threat Names:	XLoader Mal/HTMLGen-A
Verdict Reason:	-

Sample Type	**RTF Document**
File Name	**schemas.rtf**
ID	#8414598
MD5	0af0eeaac65d4a12706157a59180fde6
SHA1	42e4e2ccfcd54589ac89c02d5dc050e483c8b888
SHA256	0ea61e3db99c96cf0b148d6f2ebab3ed8860c17be0298a7e5469330b0eecb7d7
File Size	2454.29 KB
Report Created	2023-07-17 11:30 (UTC)
Target Environment	win7_64_sp1_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (28 rules, 125 matches)

Score	Category	Operation	Count	Classification
5/5	System Modification	Modifies operating system directory	5	-
	• (Process #6) wmplayer.exe creates file "\??\C:\Windows\SysWOW64\ntdll.dll" in the OS directory. • (Process #7) behind-any-heavy.exe creates file "\??\C:\Windows\SysWOW64\ntdll.dll" in the OS directory. • (Process #7) behind-any-heavy.exe creates file "\??\C:\Windows\SysWOW64\control.exe" in the OS directory. • (Process #6) wmplayer.exe creates file "\??\C:\Windows\SysWOW64\control.exe" in the OS directory. • (Process #8) control.exe creates file "\??\C:\Windows\SysWOW64\ntdll.dll" in the OS directory.			
5/5	Input Capture	Captures clipboard data	1	Spyware
	• (Process #11) explorer.exe reads data from clipboard.			
5/5	YARA	Malicious content matched by YARA rules	3	Spyware
	• YARA detected "XLoader_3" from ruleset "Malware" in memory dump data from (process #8) control.exe. • YARA detected "XLoader_3" from ruleset "Malware" in memory dump data from (process #6) wmplayer.exe. • YARA detected "XLoader_3" from ruleset "Malware" in memory dump data from (process #7) behind-any-heavy.exe.			
5/5	Data Collection	Combination of other detections shows multiple input capture behaviors	1	Spyware
	• (Process #11) explorer.exe captures keyboard and potentially exfiltrates data.			
4/5	Obfuscation	Reads from memory of another process	5	-
	• (Process #5) rundll32.exe reads from (process #6) wmplayer.exe. • (Process #7) behind-any-heavy.exe reads from (process #8) control.exe. • (Process #6) wmplayer.exe reads from (process #7) behind-any-heavy.exe. • (Process #6) wmplayer.exe reads from (process #8) control.exe. • (Process #8) control.exe reads from (process #9) next_story.exe.			
4/5	Anti Analysis	Tries to detect kernel debugger	1	-
	• (Process #6) wmplayer.exe tries to detect a kernel debugger via API "NtQuerySystemInformation".			
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	Performs DNS request	20	-

Score	Category	Operation	Count	Classification
	• (Process #11) explorer.exe resolves hostname "www.noonprince.site" to IP "64.225.91.73". • (Process #11) explorer.exe resolves hostname "www.edirassini.com" to IP "23.231.93.253". • (Process #11) explorer.exe fails to resolve hostname "www.araclarinlav.net" • (Process #11) explorer.exe resolves hostname "www.framedeals.buzz" to IP "104.21.73.200". • (Process #11) explorer.exe resolves hostname "www.gchiase2.click" to IP "52.74.11.229". • (Process #11) explorer.exe resolves hostname "www.3ycgf7x2.com" to IP "156.235.147.223". • (Process #11) explorer.exe resolves hostname "www.sahibinizim.com" to IP "85.159.66.93". • (Process #11) explorer.exe fails to resolve hostname "www.farfetich.com" • (Process #11) explorer.exe resolves hostname "www.darkbert.cloud" to IP "74.208.236.60". • (Process #11) explorer.exe resolves hostname "www.sbys021.cyou" to IP "67.198.197.12". • (Process #11) explorer.exe fails to resolve hostname "www.steanmcomunity.com" • (Process #11) explorer.exe resolves hostname "www.linyapda.com" to IP "104.223.129.53". • (Process #11) explorer.exe resolves hostname "www.camrose.top" to IP "66.29.131.66". • (Process #11) explorer.exe resolves hostname "www.ketomealplann.online" to IP "162.240.81.18". • (Process #11) explorer.exe resolves hostname "www.workationdelsol.com" to IP "81.169.145.159". • (Process #11) explorer.exe resolves hostname "www.solusiphone.com" to IP "202.52.146.246". • (Process #11) explorer.exe resolves hostname "www.qsw17.com" to IP "154.204.182.49". • (Process #11) explorer.exe fails to resolve hostname "www.e-fite.com" • (Process #11) explorer.exe resolves hostname "www.hsph.net" to IP "156.234.184.200". • (Process #11) explorer.exe resolves hostname "www.mcqueen08.shop" to IP "198.252.104.158".			
4/5	Network Connection	Connects to remote host	16	-
	• (Process #11) explorer.exe opens an outgoing TCP connection to host "104.223.129.53:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "156.234.184.200:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "198.252.104.158:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "66.29.131.66:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "52.74.11.229:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "64.225.91.73:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "202.52.146.246:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "154.204.182.49:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "67.198.197.12:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "85.159.66.93:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "23.231.93.253:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "104.21.73.200:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "81.169.145.159:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "162.240.81.18:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "74.208.236.60:80". • (Process #11) explorer.exe opens an outgoing TCP connection to host "156.235.147.223:80".			
4/5	Network Connection	Downloads file	1	Downloader
	• (Process #8) control.exe downloads file via http from hxxp://www[.]sqlite[.]org/2017/sqlite-dll-win32-x86-3180000.zip.			
4/5	Network Connection	Attempts to connect through HTTP	34	-

Score	Category	Operation	Count	Classification
	• (Process #11) explorer.exe connects to hxxp://www[.]darkbert[.]cloud/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]framedeals[.]buzz/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]sbys021[.]cyou/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]solusiphone[.]com/6rpu/?Ppu=faBeZhPX5eU5QXnFE+dc5CPYlMWUyDTtNeptDe6h+cF53wfgkO0luiweZ75MuMUHzFerSygnYX9lViN9G1duoMBKfooktpsWGEWEJ85M6QrA&0ZtwYy=0Hz0YF. • (Process #11) explorer.exe connects to hxxp://www[.]sbys021[.]cyou/6rpu/?Ppu=Rcz2mjU14OA8QPxc1N2OacQW0VRi8xNHbgUYKLKbYTAEagufCdnbRwOPW/Gop3dlJvGGvn9orV1ZZoltHd4LeWC1vTbbcjBsq04JHSaAYe2A&0ZtwYy=0Hz0YF. • (Process #11) explorer.exe connects to hxxp://www[.]linyapda[.]com/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]noonprince[.]site/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]framedeals[.]buzz/6rpu/?Ppu=kYINAY0yQ323qkefT2XXzDAGfk6UP2Z8qRCNSz8Z+f0CQfYwboHLsC+C3xIpdzKwExr+OWy9bbGV1GkwXCaFZfOYVChXXqLqY4/rWEj3RUsR&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]mcqueen08[.]shop/6rpu/?Ppu=8yF31yfwMGrwMgoGkeZJNAXs9+B9vl5goWUEgFES0xLujVmhnvwjmM2B3xNOFxdj+WRtsZIGrVX1sTyq4/MVxCvZ4V21BvasviIPjTali1bE&DZ5B=cD5cmh4y. • (Process #8) control.exe connects to hxxp://www[.]sqlite[.]org/2017/sqlite-dll-win32-x86-3180000.zip. • (Process #11) explorer.exe connects to hxxp://www[.]camrose[.]top/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]gchiase2[.]click/6rpu/?Ppu=mVJlWZfSFHBRFuERTuOklOQuZAXsug76Rb6U1r41UoL2DX3aPzUPzNqBljYL7ti450ag3Bo6lZ1IbJeCG+GGgpjFIX3p2LcfmCwIg5QT40TU&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]hsph[.]net/6rpu/?Ppu=bp/9yUFv9lJJcN4JNIhXerCAgTu6Or+k1MY0Iurax5GDqLc+waTZ9JvidWLEdxfT5I792dN+01Rq7OGIRf0JTNYGmkd4Oz97hk03rUvUIxej&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]ketomealplann[.]online/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQVSyUGXzQpZ/oFi4h3H+24HKXEY2nSdAWJvneOcGgUMami2cKwsJYEJKxKHg8oLM7F69NEQAVQI58PqH8f3g+0+F+5h2vKnRoveqo7gmla&0ZtwYy=0Hz0YF. • (Process #11) explorer.exe connects to hxxp://www[.]linyapda[.]com/6rpu/?Ppu=JNMU5lRt9TQe5nNO1Sbk4VxBCXrLWLA+kd/L3q3uoel7JjKZIKJMPyDJgqUHRkY/QYEd1fE6OYjcL8erFU5Zx1xTZddScdwaDztYO0AT1ncL&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]camrose[.]top/6rpu/?Ppu=N+WSMqmqRmb14d9QzRyAN3xsZDrnSAfhhEAa8OEYiCceR0oEixBRMbPxz1+3q8NVlie0/YhDq1RnPn7pB4JelypIFUJz8NQwEq5o/aBJ34jg&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]noonprince[.]site/6rpu/?Ppu=jJ/+gArpHQbXobQt+1ki5xkEHX4MSTPPinzeMGb0J4bJuhIdtq7hM8JTt7JawuX2uibibnvCsht7tkzSg6k/YHT9h54N81SDw8rE87yE9Zwo&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]workationdelsol[.]com/6rpu/?Ppu=bEVJe5rzh1pqq+KFzm7Z+MzxelhnwO+hrg1lyrCWTePQJ5Zn93SpngadGKgonJqu9tF4GcuUAaTMG+CUi1c4mFrYfPuJEoj4aymWhQI+O0AJ&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]sahibinizim[.]com/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]ketomealplann[.]online/6rpu/?Ppu=YhpgcRwO6+pWSfeSjyLhlLoZP/EzdYlsk0TmHSB5wknwPdVcUjrVLv9VIK7YWCaX0UccOKRnfdC48X7PtpX8/Wj5tY1GsAn75acQ2dSPUiCC&0ZtwYy=0Hz0YF. • (Process #11) explorer.exe connects to hxxp://www[.]sahibinizim[.]com/6rpu/?Ppu=lJq/LhGK9DOZEGMpf2olbPXQGZgyLkip1hmFhlmGKm2rNGuqXmLfg2nedVtlUVUZ0TQZBbOz6gvWTDwJXkmVYYKgAUnwn9bOWCBMGhBnErqQ&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]mcqueen08[.]shop/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]qsw17[.]com/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]workationdelsol[.]com/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQVSyUGXzQpZ/oFi4h3H+24HKXEY2nSdAWJvneOcGgUMami2cKwsJYEJKxKHg8oLM7F69NEQAVQI58PqH8f3g+0+F+5h2vKnRoveqo7gmla&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]hsph[.]net/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]solusiphone[.]com/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]qsw17[.]com/6rpu/?Ppu=JVO1m5e/3foRHFKnRvmKZH7D1Zp5kDwhgVsUBOwS8GWoPpxixj0lRTL1XpPbi2O/iXpzZpAddedLxDwI+fDFr8e+q9qu1LfVAh/O9o1R7V42&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]solusiphone[.]com/6rpu/?Ppu=faBeZhPX5eU5QXnFE+dc5CPYlMWUyDTtNeptDe6h+cF53wfgkO0luiweZ75MuMUHzFerSygnYX9lViN9G1duoMBKfooktpsWGEWEJ85M6QrA&DZ5B=cD5cmh4y. • (Process #11) explorer.exe connects to hxxp://www[.]gchiase2[.]click/6rpu/. • (Process #11) explorer.exe connects to hxxp://www[.]darkbert[.]cloud/6rpu/?Ppu=ZlX90GMmr8OogOg59rJ1Sq68WWCkPNLZb0E+DI3GqNea2L8xU9jjz42bwiq3b+jjRv/wmCHBdMxVdMSvPhr8nNujTmRdkSiXjzcB21PbyZmB&0ZtwYy=0Hz0YF. • (Process #8) control.exe connects to hxxp://www[.]3ycgf7x2[.]com/6rpu/?Ppu=9sSRcqZov6Qtq4zmkSZBGZmXdQYu9z+k6EqEB/Sh3ZqUM3BBgmi3SjlHjOpo7drCVTaguvFHZF5loeh6oTyBKI0lwK6sDJGoLREcMJkpJ4t8&DZ5B=cD5cmh4y&wn=1. • (Process #11) explorer.exe connects to hxxp://www[.]edirassini[.]com/6rpu/.			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #3) cmd.exe.			
4/5	Injection	Writes into the memory of another process	5	Injector

Score	Category	Operation	Count	Classification
	• (Process #5) rundll32.exe modifies memory of (process #6) wmplayer.exe. • (Process #6) wmplayer.exe modifies memory of (process #7) behind-any-heavy.exe. • (Process #6) wmplayer.exe modifies memory of (process #8) control.exe. • (Process #8) control.exe modifies memory of (process #9) next_story.exe. • (Process #8) control.exe modifies memory of (process #11) explorer.exe.			
4/5	Injection	Modifies control flow of another process	4	-
	• (Process #5) rundll32.exe alters context of (process #6) wmplayer.exe. • (Process #6) wmplayer.exe alters context of (process #7) behind-any-heavy.exe. • (Process #8) control.exe alters context of (process #9) next_story.exe. • (Process #8) control.exe alters context of (process #11) explorer.exe.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	Reputation	Contacts known malicious URL	5	-
	• Reputation analysis labels the URL "hxxp://www[.]framedeals[.]buzz/6rpu/" which was contacted by (process #11) explorer.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://www[.]framedeals[.]buzz/6rpu/?Ppu=kY...aFZfOYVChXXqLqY4/rWEj3RUsR&DZ5B=cD5cmh4y" which was contacted by (process #11) explorer.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQ...8f3g+0+F+5h2vKnRoveqo7gmIa&0ZtwYy=0Hz0YF" which was contacted by (process #11) explorer.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQ...8f3g+0+F+5h2vKnRoveqo7gmIa&DZ5B=cD5cmh4y" which was contacted by (process #11) explorer.exe as Mal/HTMLGen-A. • Reputation analysis labels the URL "hxxp://www[.]edirassini[.]com/6rpu/" which was contacted by (process #11) explorer.exe as Mal/HTMLGen-A.			
4/5	Reputation	Resolves known malicious domain	3	-
	• Reputation analysis labels the resolved domain "www.edirassini.com" as Mal/HTMLGen-A. • Reputation analysis labels the resolved domain "www.framedeals.buzz" as Mal/HTMLGen-A. • Reputation analysis labels the resolved domain "www.steanmcomunity.com" as Mal/HTMLGen-A.			
3/5	Persistence	Installs system startup script or application	2	-
	• (Process #5) rundll32.exe adds "0" to Windows startup via registry. • (Process #8) control.exe adds "C:\Program Files (x86)\Windows Media Player\wmplayer.exe" to Windows startup via registry.			
3/5	Discovery	Enumerates running processes	1	-
	• (Process #5) rundll32.exe enumerates running processes.			
3/5	Anti Analysis	Delays execution	2	-
	• (Process #8) control.exe has a thread which sleeps more than 5 minutes. • (Process #11) explorer.exe has a thread which sleeps more than 5 minutes.			
3/5	Reputation	Contacts known suspicious URL	2	-
	• (Process #11) explorer.exe contacted known malicious URL hxxp://www[.]gchiase2[.]click/6rpu/?Ppu=mVJ...GGgpjFIX3p2LcfmCwIg5QT40TU&DZ5B=cD5cmh4y. • (Process #11) explorer.exe contacted known malicious URL hxxp://www[.]gchiase2[.]click/6rpu/.			
3/5	Reputation	Resolves known suspicious domain	1	-
	• Resolved domain "www.gchiase2.click" is a known suspicious domain.			
2/5	Anti Analysis	Tries to detect debugger	1	-

Score	Category	Operation	Count	Classification
	• (Process #5) rundll32.exe tries to detect a debugger via API "NtQueryInformationProcess".			
2/5	Discovery	Possibly does reconnaissance	2	-
	• (Process #8) control.exe tries to gather information about application "Mozilla Firefox" by registry. • (Process #8) control.exe tries to gather information about application "Mozilla Firefox" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #8) control.exe tries to read credentials of web browser "Internet Explorer" by reading from the system's credential vault.			
2/5	Defense Evasion	Loads a dropped DLL	1	-
	• (Process #8) control.exe loads dropped DLL sqlite3.dll.			
1/5	Mutex	Creates mutex	4	-
	• (Process #6) wmplayer.exe creates mutex with name "0K12-A9Q7G4-282F". • (Process #8) control.exe creates mutex with name "0K12-A9Q7G4-282F". • (Process #8) control.exe creates mutex with name "12L541-4F23B2XB9". • (Process #8) control.exe creates mutex with name "L96NQOTUUVCA42H_".			
1/5	Crash	A monitored process crashed	1	-
	• (Process #2) eqnedt32.exe crashed.			
-	Trusted	Known clean file	4	-
	• Embedded file "sqlite3.def" is a known clean file. • Embedded file "" is a known clean file. • Embedded file "C:\Users\KEECFM~1\AppData\Local\Temp_tcx1h.zip" is a known clean file. • Embedded file "sqlite3.dll" is a known clean file.			

Mitre ATT&CK Matrix

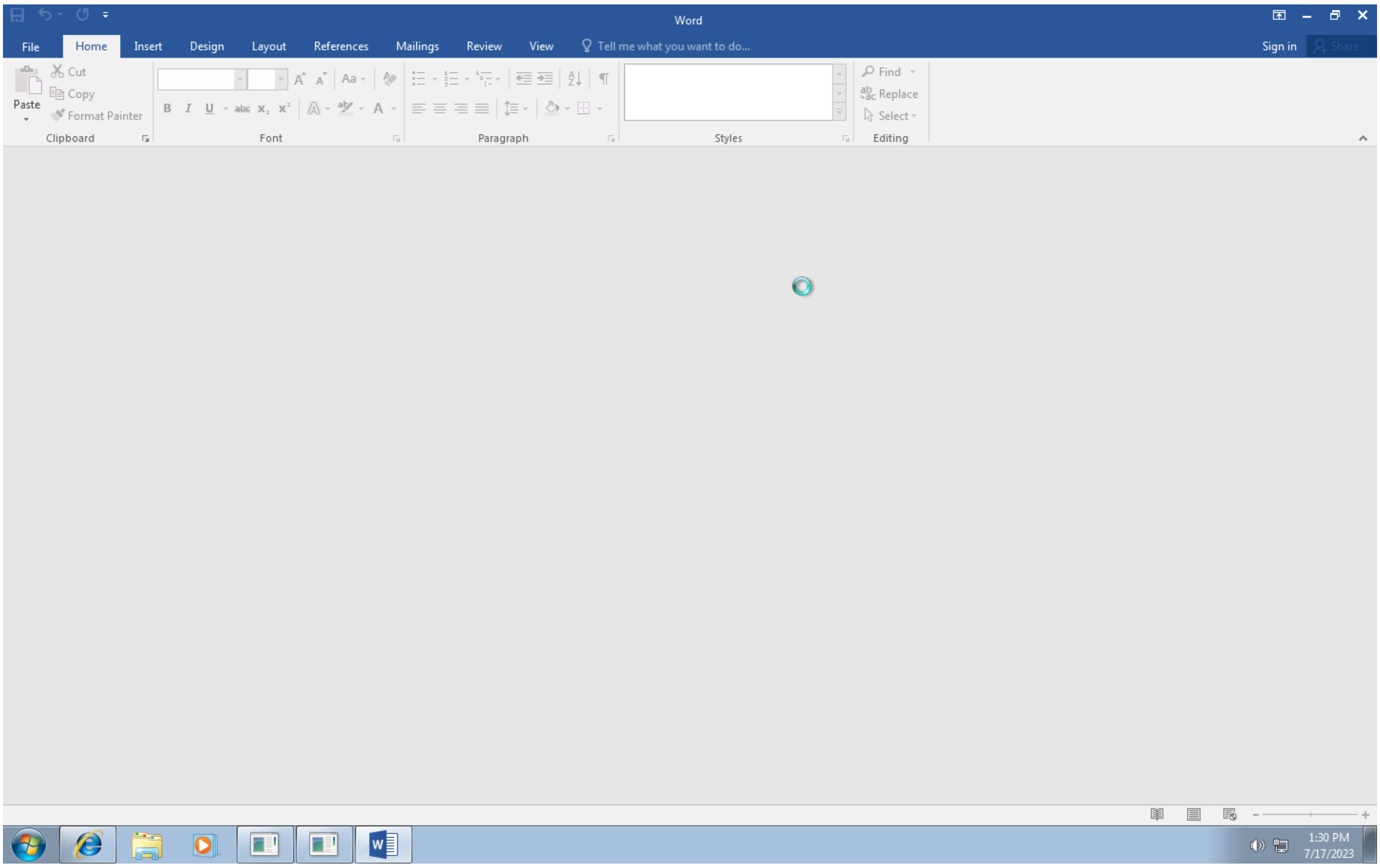
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1203 Exploitation for Client Execution	#T1060 Registry Run Keys / Startup Folder		#T1112 Modify Registry	#T1003 Credential Dumping	#T1057 Process Discovery	#T1105 Remote File Copy	#T1115 Clipboard Data	#T1071 Standard Application Layer Protocol		
					#T1056 Input Capture	#T1012 Query Registry		#T1119 Automated Collection	#T1105 Remote File Copy		
						#T1083 File and Directory Discovery		#T1005 Data from Local System			
								#T1056 Input Capture			

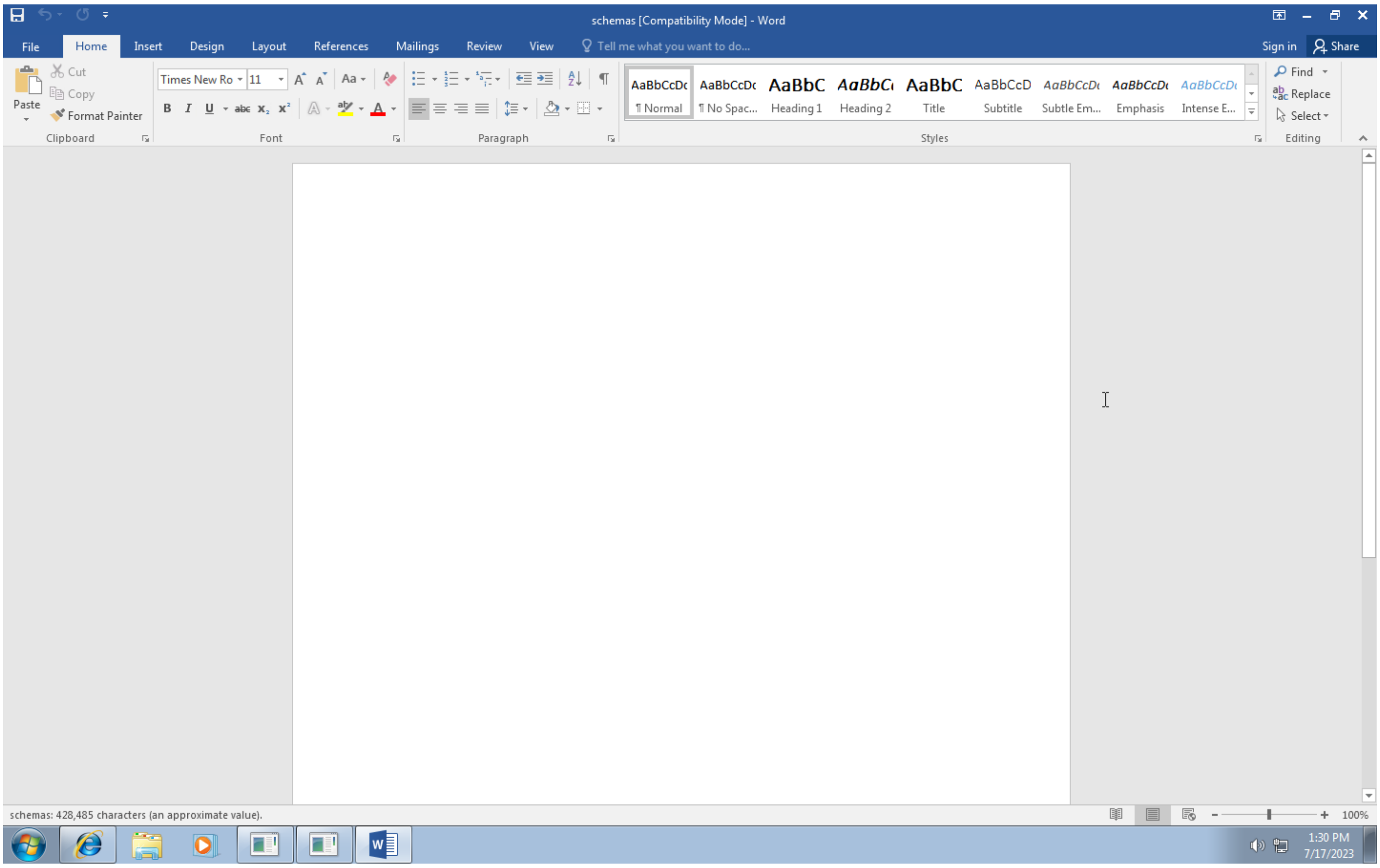
Sample Information

ID	#8414598
MD5	0af0eeaac65d4a12706157a59180fde6
SHA1	42e4e2ccfcd54589ac89c02d5dc050e483c8b888
SHA256	0ea61e3db99c96cf0b148d6f2ebab3ed8860c17be0298a7e5469330b0eecb7d7
SSDeep	12288:WUr0OQL9/JcoDCubwbwl390KE83oqUxIhGUKKR+uQ6:9gOs9BcYCYV0n83ExIhGUKpuQ6
File Name	schemas.rtf
File Size	2454.29 KB
Sample Type	RTF Document
Has Macros	✔

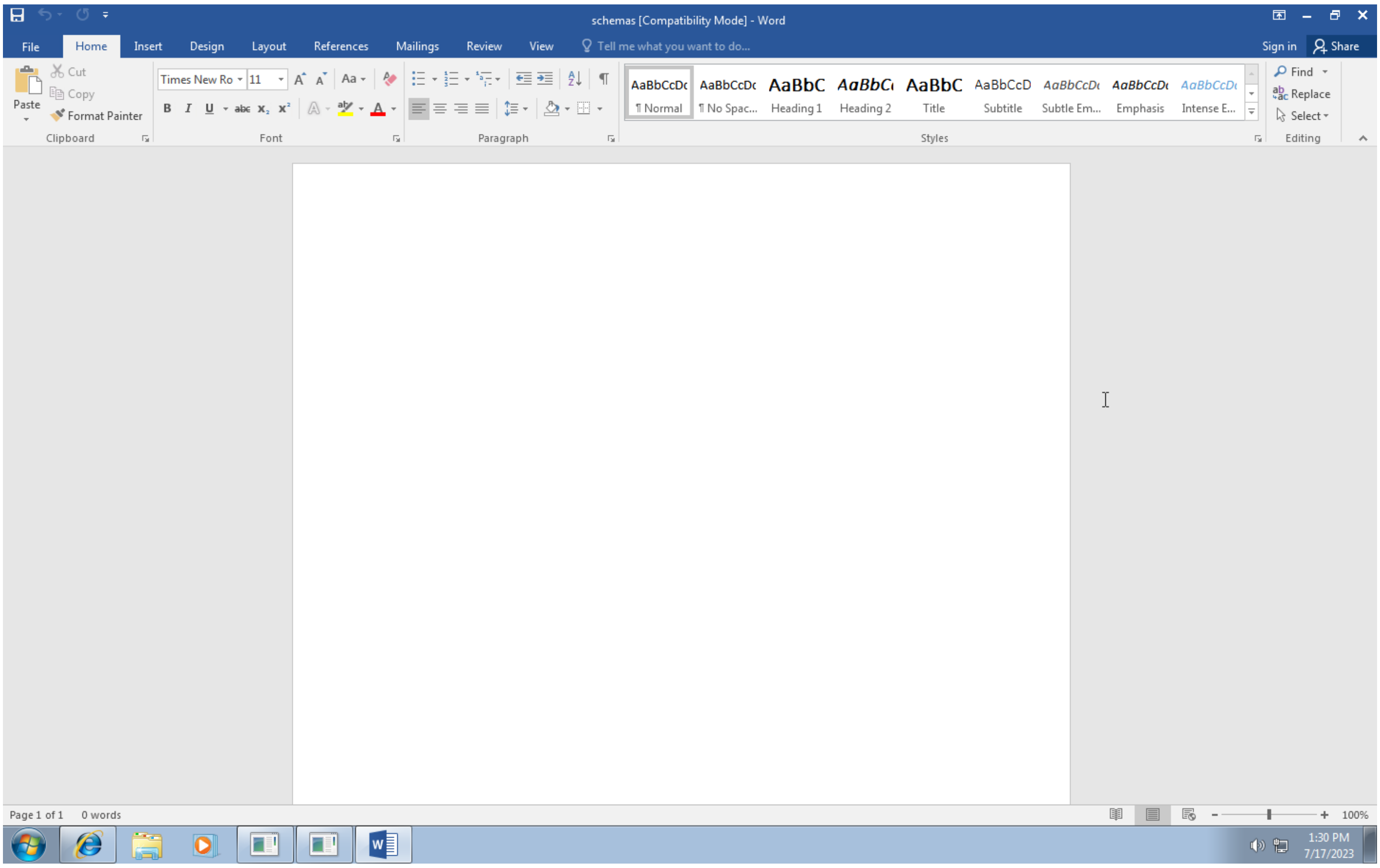
Analysis Information

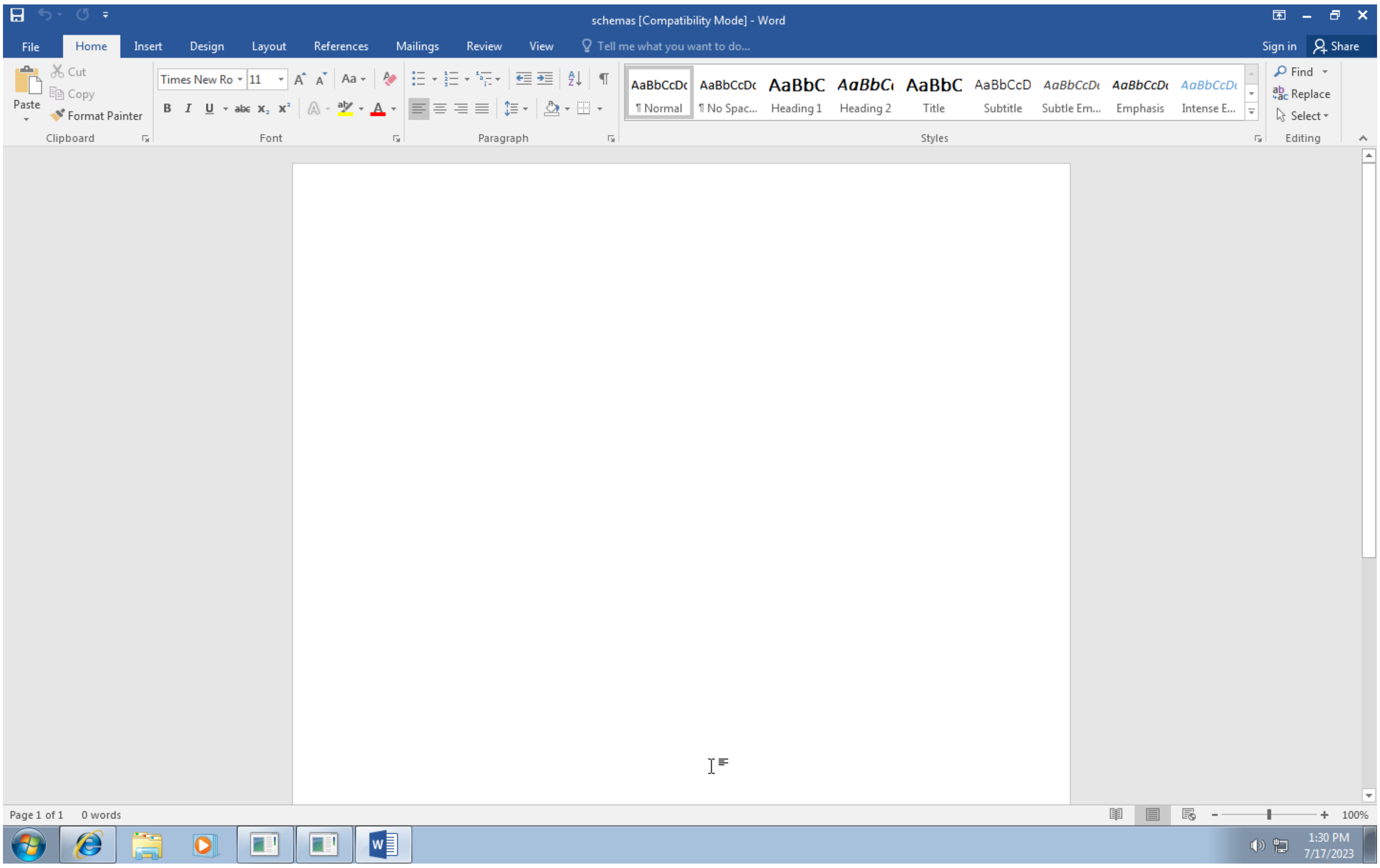
Creation Time	2023-07-17 11:30 (UTC)
Analysis Duration	00:04:02
Termination Reason	Timeout
Number of Monitored Processes	10
Execution Successful	True
Reputation Enabled	✔
WHOIS Enabled	✔
Built-in AV Enabled	✖
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, 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	16





schemas: 428,485 characters (an approximate value).





Screenshots truncated

NETWORK

General

180.79 KB total sent

663.16 KB total received

2 ports 80, 53

18 contacted IP addresses

82 URLs extracted

75 files downloaded

24 malicious hosts detected

DNS

43 DNS requests for 21 domains

1 nameservers contacted

25 total requests returned errors

HTTP/S

33 URLs contacted, 16 servers

100 sessions, 177.41 KB sent, 660.98 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://www[.]margosinc[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]myxxxcentral[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bazararaira[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]litespeedtech[.]com/error-page	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]taxrice[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]alextsoucas[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]sabao-barra[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://workationdelsol[.]com/xmlrpc.php	-	-	-	0 bytes	CLEAN
GET	hxxp://nginx[.]net	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]drsaulson[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]bjjfsd[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]interjetinc[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]conanstower[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://push[.]zhanzhang[.]baidu[.]com/push.js	-	-	-	0 bytes	CLEAN
GET	hxxp://fedoraproject[.]org	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]madfishman[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]smartviolet[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]ithinkhealth[.]com	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://www[.]linyapda[.]com/list-3/4348.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4675.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/3627.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/023.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4905.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/494.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/434.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com//5.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/2544.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/178.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/3383.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/676.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4597.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/033.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com//4.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4047.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/2228.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/968.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/056.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/029.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/127.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4498.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/3459.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4639.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4085.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4997.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/054.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/2807.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/350.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4305.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/94.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/3538.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/039.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/020.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4341.html	-	-	-	0 bytes	CLEAN

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://www[.]linyapda[.]com/list-3/3754.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/050.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/461.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/129.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/3789.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/025.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/647.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/035.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/2063.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/3265.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/3234.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/64.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-3/4455.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]linyapda[.]com/list-4/77.html	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]markstef[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]graciesantos[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]3ycgf7x2[.]com/6rpu/?Ppu=9sSRcqZov6Qtq4zmkSZBGZmXdQYu9z+k6EqEB/Sh3ZqUM3BBgmi3SjlHjOpo7drCVTaguvFHZF5loeh6oTyBKI0lwK6sDJGoLREcMJkpJ4t8&DZ5B=cD5cmh4y&wn=1	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]lacalatruite[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]gunsperu[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]paulciganek[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]gurasi[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]shokugyo[.]com	-	-	-	0 bytes	CLEAN
GET	hxxp://www[.]cniddm[.]com	-	-	-	0 bytes	CLEAN
POST	hxxp://www[.]camrose[.]top/6rpu/	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]sbys021[.]cyou/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]qsw17[.]com/6rpu/?Ppu=JVO1m5e/3foRHFKnRvmKZH7D1Zp5kDwhgVsUBOwS8GWoPpxixj0lRTL1XpPbi2O/iXpzZpAddedLxDwl+fDFr8e+q9qu1LfVAh/O9o1R7V42&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]framedeals[.]buzz/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]hsph[.]net/6rpu/?Ppu=bp/9yUFv9lJJcN4JNIhXerCAgTu6Or+k1MY0Iurax5GDqLc+waTZ9JvidWLEdxfT5I792dN+01Rq7OGlRf0JTNYGmkd4Oz97hk03rUvUIxej&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]workationdelsol[.]com/6rpu/	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]gchiase2[.]click/6rpu/	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]edirassini[.]com/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]sahibinizim[.]com/6rpu/?Ppu=IJq/LhGK9DOZEGMpf2olbPXQGZgyLkip1hmFhlmGKm2rNGuqXmLfg2nedVtlUVUZ0TQZBbOz6gvWTDwJXkmVYYKgAUnwn9bOWCBMGhBnErqQ&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	hxxp://www[.]qsw17[.]com/6rpu/	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]solusiphone[.]com/6rpu/	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]sahibinizim[.]com/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]mcqueen08[.]shop/6rpu/?Ppu=8yF31yfwMGrwMgoGkeZJNAXs9+B9vl5goWUEgFES0xLujVmhnvwjmM2B3xNOFxdj+WRtsZIGrVX1sTyq4/MVxCvZ4V21BvasviIPjTali1bE&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]hsph[.]net/6rpu/	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]linyapda[.]com/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]solusiphone[.]com/6rpu/?Ppu=faBeZhPX5eU5QXnFE+dc5CPYlMWUyDTtNeptDe6h+cF53wfgkO0luiweZ75MuMUHzFerSygnYX9lViN9G1duoMBKfooktpsWGEWEJ85M6QrA&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]ketomealplann[.]online/6rpu/	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]noonprince[.]site/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]framedeals[.]buzz/6rpu/?Ppu=kYINAY0yQ323qkefT2XXzDAGfk6UP2Z8qRCNSz8Z+f0CQfYwboHLsC+C3xIpdzKwExr+OWy9bbGV1GkwXCaFZfOYVChXXqLqY4/rWEj3RUsR&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]sbys021[.]cyou/6rpu/?Ppu=Rcz2mjU14OA8QPxc1N2OacQW0VRi8xNHbgUYKLKbYTAEagufCdnbRwOPW/Gop3dlJvGGvn9orV1ZZoltHd4LeWC1vTbbcjBsq04JHSaAYe2A&0ZtwYy=0Hz0YF	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]mcqueen08[.]shop/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]noonprince[.]site/6rpu/?Ppu=jJ/+gArpHQbXobQt+1ki5xkEHX4MSTPPinzeMGb0J4bJuhldtq7hM8JTt7JawuX2uibibnvCsht7tkzSg6k/YHT9h54N81SDw8rE87yE9Zwo&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]camrose[.]top/6rpu/?Ppu=N+WSMqmqRmb14d9QzRyAN3xsZDrnSAfhhEAa8OEYiCceR0oEixBRMbPxz1+3q8NVlie0/YhDq1RnPn7pB4JelypIFUJz8NQwEq5o/aBJ34jg&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]gchiase2[.]click/6rpu/?Ppu=mVJlWZfSFHBRFuERTuOklOQuZAXsug76Rb6U1r41UoL2DX3aPzUPzNqBIjYL7ti450ag3Bo6IZ1lbJeCG+GGgpjFIX3p2LcfmCwIg5QT40TU&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
POST	hxxp://www[.]darkbert[.]cloud/6rpu/	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]ketomealplann[.]online/6rpu/?Ppu=YhpgcRwO6+pWSfeSjyLhlLoZP/EzdYlsk0TmHSB5wknwPdVcUjrVLv9VIK7YWCaX0UccOKRnfdC48X7PtpX8/Wj5tY1GsAn75acQ2dSPUiCC&0ZtwYy=0Hz0YF	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]linyapda[.]com/6rpu/?Ppu=JNMU5lRt9TQe5nNO1Sbk4VxBCXrLWLA+kd/L3q3uoel7JjKZIKJMPyDJgqUHRkY/QYEd1fE6OYjcL8erFU5Zx1xTZddScdwaDztYO0AT1ncL&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQVSyUGXzQpZ/oFi4h3H+24HKXEY2nSdAWJvneOcGgUMami2cKwsJYEJKxKHg8oLM7F69NEQAVQI58PqH8f3g+0+F+5h2vKnRoveqo7gmIa&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]solusiphone[.]com/6rpu/?Ppu=faBeZhPX5eU5QXnFE+dc5CPYlMWUyDTtNeptDe6h+cF53wfgkO0luiweZ75MuMUHzFerSygnYX9lViN9G1duoMBKfooktpsWGEWEJ85M6QrA&0ZtwYy=0Hz0YF	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]darkbert[.]cloud/6rpu/?Ppu=ZIX90GMmr8OogOg59rJ1Sq68WWCkPNLZb0E+DI3GqNea2L8xU9jjz42bwiq3b+jjRv/wmCHBdMxVdMSvPhr8nNujTmRdkSiXjzcB21PbyZmB&0ZtwYy=0Hz0YF	-	-	-	0 bytes	MALICIOUS

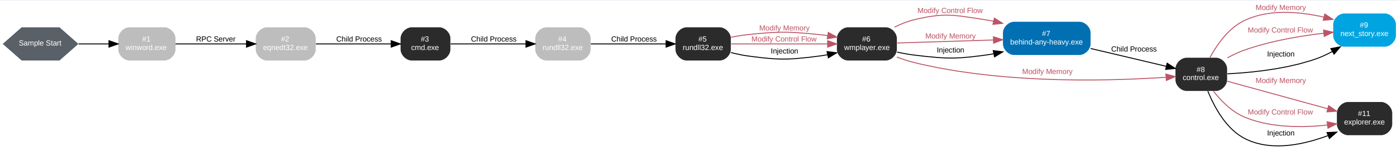
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQVSyUGXzQpZ/oFi4h3H+24HKXEY2nSdAWJvneOcGgUMami2cKwsJYEJKxKHg8oLM7F69NEQAVQI58PqH8f3g+0+F+5h2vKnRoveqo7gmla&0ZtwYy=0Hz0YF	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]workationdelsol[.]com/6rpu/?Ppu=bEVJe5rzh1pqq+KFzm7Z+MzxelhnwO+hrg1lyrCWTePQJ5Zn93SpngadGKgonJqu9tF4GcuUAaTMG+CUi1c4mFrYfPuJEoj4aymWhQI+O0AJ&DZ5B=cD5cmh4y	-	-	-	0 bytes	MALICIOUS
GET	hxxp://www[.]sqlite[.]org/2017/sqlite-dll-win32-x86-3180000.zip	-	-	-	0 bytes	CLEAN
GET	hxxps://zz[.]bdstatic[.]com/linksubmit/push.js	-	-	-	0 bytes	CLEAN
GET	hxxps://domaincntrol[.]com/?orighost=	-	-	-	0 bytes	CLEAN
GET	hxxps://fonts[.]gstatic[.]com	-	-	-	0 bytes	CLEAN
GET	hxxps://hm[.]baidu[.]com/hm.js?fe6a346f32de57f467ca0b7cfd87bfa1	-	-	-	0 bytes	CLEAN
GET	hxxps://nojs[.]domaincntrol[.]com	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	www[.]noonprince[.]site	NO_ERROR	64.225.91.73	-	CLEAN
A	www[.]edirassini[.]com	NO_ERROR	23.231.93.253	-	MALICIOUS
A	www[.]araclarinlav[.]net	NX_DOMAIN	-	-	CLEAN
A	www[.]framedeals[.]buzz	NO_ERROR	104.21.73.200, 172.67.165.207	-	MALICIOUS
A	www[.]farfetich[.]com	-	-	-	CLEAN
A	www[.]gchiase2[.]click, dns[.]ladipage[.]com	NO_ERROR	52.74.11.229, 54.179.30.8, 13.215.123.39	dns[.]ladipage[.]com	SUSPICIOUS
A	www[.]3ycgf7x2[.]com	NO_ERROR	156.235.147.223	-	CLEAN
A	www[.]e-fite[.]com	-	-	-	CLEAN
A	www[.]sahibinizim[.]com, redirect[.]natrocdn[.]com, natroredirect[.]natrocdn[.]com	NO_ERROR	85.159.66.93	redirect[.]natrocdn[.]com, natroredirect[.]natrocdn[.]com	CLEAN
A	www[.]darkbert[.]cloud	NO_ERROR	74.208.236.60	-	CLEAN
A	www[.]sbys021[.]cyou	NO_ERROR	67.198.197.12	-	CLEAN
A	www[.]steanmcomunity[.]com	NX_DOMAIN	-	-	MALICIOUS
A	www[.]linyapda[.]com	NO_ERROR	104.223.129.53	-	CLEAN
A	www[.]camrose[.]top	NO_ERROR	66.29.131.66	-	CLEAN
A	www[.]ketomealplann[.]online, ketomealplann[.]online	NO_ERROR	162.240.81.18	ketomealplann[.]online	CLEAN
A	www[.]sqlite[.]org	NO_ERROR	45.33.6.223	-	CLEAN
A	www[.]workationdelsol[.]com, workationdelsol[.]com	NO_ERROR	81.169.145.159	workationdelsol[.]com	CLEAN
A	www[.]solusiphone[.]com, solusiphone[.]com	NO_ERROR	202.52.146.246	solusiphone[.]com	CLEAN
A	www[.]qsw17[.]com	NO_ERROR	154.204.182.49	-	CLEAN
A	www[.]hsph[.]net	NO_ERROR	156.234.184.200	-	CLEAN
A	www[.]mcqueen08[.]shop, mcqueen08[.]shop	NO_ERROR	198.252.104.158	mcqueen08[.]shop	CLEAN

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\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 31629, Reason: Analysis Target
Unmonitor End Time	End Time: 275230, Reason: Terminated by timeout
Monitor duration	243.60s
Return Code	Unknown
PID	3172
Parent PID	2020
Bitness	64 Bit

Process #2: eqnedt32.exe

ID	2
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: 39693, Reason: RPC Server
Unmonitor End Time	End Time: 48251, Reason: Crashed
Monitor duration	8.56s
Return Code	0
PID	3336
Parent PID	3172
Bitness	32 Bit

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	CmD.exe /C rundll32 %tmp%\Client.log,IEX A␒␌C
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 41534, Reason: Child Process
Unmonitor End Time	End Time: 44466, Reason: Terminated
Monitor duration	2.93s
Return Code	0
PID	3360
Parent PID	3336
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	9
File	6
Process	1

Process #4: rundll32.exe

ID	4
File Name	c:\windows\syswow64\rundll32.exe
Command Line	rundll32 C:\Users\KEECFM~1\AppData\Local\Temp\Client.log,IEX A␒␌C
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 41730, Reason: Child Process
Unmonitor End Time	End Time: 44431, Reason: Terminated
Monitor duration	2.70s
Return Code	0
PID	3384
Parent PID	3360
Bitness	32 Bit

Process #5: rundll32.exe

ID	5
File Name	c:\windows\system32\rundll32.exe
Command Line	rundll32 C:\Users\KEECFM~1\AppData\Local\Temp\Client.log,IEX AC
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 41836, Reason: Child Process
Unmonitor End Time	End Time: 44196, Reason: Terminated
Monitor duration	2.36s
Return Code	0
PID	3392
Parent PID	3384
Bitness	64 Bit

Host Behavior

Type	Count
File	1
Module	4
-	3
Registry	2
Process	24
-	3
-	6

Process #6: wmplayer.exe

ID	6
File Name	c:\program files (x86)\windows media player\wmplayer.exe
Command Line	rundll32 C:\Users\KEECFM~1\AppData\Local\Temp\Client.log,IEX AC
Initial Working Directory	C:\Program Files (x86)\Windows Media Player\
Monitor Start Time	Start Time: 42561, Reason: Injection
Unmonitor End Time	End Time: 52182, Reason: Terminated
Monitor duration	9.62s
Return Code	0
PID	3420
Parent PID	3392
Bitness	32 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#5: c:\windows\system32\rundll32.exe	0xd44	0x70000(458752)	0x31000	✔	1
Modify Memory	#5: c:\windows\system32\rundll32.exe	0xd44	0x7efde008(2130567176)	0x8	✔	1
Modify Control Flow	#5: c:\windows\system32\rundll32.exe	0xd44 / 0xd60	0x7efde008(2130567176)	-	✔	1
Modify Memory	#5: c:\windows\system32\rundll32.exe	0xd44	0x70000(458752)	0x200	✔	1

Host Behavior

Type	Count
File	8
-	1
-	1
System	10
Module	15
User	1
Mutex	1
Environment	1
Process	3
-	8
-	2

Process #7: behind-any-heavy.exe

ID	7
File Name	c:\program files\windows photo viewer\behind-any-heavy.exe
Command Line	"C:\Program Files\Windows Photo Viewer\behind-any-heavy.exe"
Initial Working Directory	C:\Program Files\Windows Photo Viewer\
Monitor Start Time	Start Time: 44085, Reason: Injection
Unmonitor End Time	End Time: 275230, Reason: Terminated by timeout
Monitor duration	231.15s
Return Code	Unknown
PID	2208
Parent PID	3420
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\program files (x86)\windows media player\wmplayer.exe	0xd60	0x930000(9633792)	0xf4000	✔	1
Modify Control Flow	#6: c:\program files (x86)\windows media player\wmplayer.exe	0xd60 / 0x8a4	0x994d97(10046871)	-	✔	1
Modify Control Flow	#6: c:\program files (x86)\windows media player\wmplayer.exe	0xd60 / 0x8a4	0x8c(140)	-	✔	1

Host Behavior

Type	Count
File	5
Process	2
-	1

Process #8: control.exe

ID	8
File Name	c:\windows\syswow64\control.exe
Command Line	"C:\Windows\SysWOW64\control.exe"
Initial Working Directory	C:\Program Files\Windows Photo Viewer\
Monitor Start Time	Start Time: 44431, Reason: Child Process
Unmonitor End Time	End Time: 275230, Reason: Terminated by timeout
Monitor duration	230.80s
Return Code	Unknown
PID	3456
Parent PID	2208
Bitness	32 Bit

Injection Information (2)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#6: c:\program files (x86)\windows media player\wmplayer.exe	0xd60	0xb0000(720896)	0x2e000	✔	1
Modify Memory	#6: c:\program files (x86)\windows media player\wmplayer.exe	0xd60	0xe10000(14745600)	0x1f000	✔	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	4.88 KB	c5edf6afd22dd7fd0efa2996716f25cd739731caea328532a8fd6ec64600e630	✖
C:\Users\KEECFM~1\AppData\Local\Temp_tcx1h.zip	433.21 KB	d01c69d09282f9050f6b113c45884fe9b9abf3bdf5bd93b45927d9b6bfb233fe	✖
-	828.29 KB	5ea67d6b7f67301ca214af511740f26b9e6cc9e16b2c0ec7bba071d05b9bde78	✖

Host Behavior

Type	Count
File	102
-	1
-	1
System	11974
User	1
Mutex	3
Registry	11784
Module	22
Process	7
-	1
-	11
COM	2

Network Behavior

Type	Count
HTTP	2
TCP	1

Process #9: next_story.exe

ID	9
File Name	c:\program files (x86)\windows defender\next_story.exe
Command Line	"C:\Program Files (x86)\Windows Defender\next_story.exe"
Initial Working Directory	C:\Program Files (x86)\Windows Defender\
Monitor Start Time	Start Time: 57262, Reason: Injection
Unmonitor End Time	End Time: 275230, Reason: Terminated by timeout
Monitor duration	217.97s
Return Code	Unknown
PID	2116
Parent PID	3456
Bitness	32 Bit

Injection Information (3)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#8: c:\windows\syswow64\control.exe	0xd84	0x25c0000(39583744)	0x2328000	✔	1
Modify Memory	#8: c:\windows\syswow64\control.exe	0xd84	0x820000(8519680)	0x124000	✔	1
Modify Control Flow	#8: c:\windows\syswow64\control.exe	0xd84 / 0x848	0x8b4d77(9129335)	-	✔	1

Process #11: explorer.exe

ID	11
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 73108, Reason: Injection
Unmonitor End Time	End Time: 275230, Reason: Terminated by timeout
Monitor duration	202.12s
Return Code	Unknown
PID	2020
Parent PID	-
Bitness	64 Bit

Injection Information (4)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#8: c:\windows\syswow64\control.exe	0xd84	0xbb60000(196476928)	0x2328000	✔	1
Modify Memory	#8: c:\windows\syswow64\control.exe	0xd84	0x9310000(154206208)	0x106000	✔	1
Modify Control Flow	#8: c:\windows\syswow64\control.exe	0xd84 / 0x7e8	0xffffffff(4294967295)	-	✔	1
Modify Control Flow	#8: c:\windows\syswow64\control.exe	0xd84 / 0x7e8	0xfc(252)	-	✔	1

Host Behavior

Type	Count
System	331
-	39
File	18

Network Behavior

Type	Count
HTTP	99
DNS	25
TCP	100

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
aab5207a37210231eb636a0ce8663e61840fcc105ea59e5b1d847f92879da2eb	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
d1694016d7e737dacb539993da81070dd0c61fa7887a8224bfe81d459d4f59a0	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
f674463cde22abbbf52bb5af52496a4839a03b838e889f5c8b2764250d4ef445	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
d66458e76d9c2bbd7251e73b553cb9ca9ae16494329c5eeefa589b79a6f7bcba	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
25416d3fb3dad23c916f5feeb597a36fc3ac7ba667c509d91ed835b832e737ae	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
60df76e67edba8b37521d0f9602563f7b1af273d30b5741defec2f7852b55f50	-	Memory Dump	196.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
2142268967e96dd3ea917d68564195ad15c5b23c386e45bb4179527b4f969404	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
7e6262a5531806d8c68176a21d4867440d5478d190c7c663a202e346be059f61	-	Memory Dump	976.00 KB	application/octet-stream	-	MALICIOUS
0ea61e3db99c96cf0b148d6f2ebab3ed8860c17be0298a7e5469330b0eecb7d7	C:\Users\kEecfMwgj\Desktop\schemas.rtf	Sample File	2454.29 KB	text/rtf	-	MALICIOUS
8c54b804c62f7999c0b2326b48ffd1ceb27f6b24851bae601d921fee183fe706	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
ea94733f694c39b78970c3d1ad4ac04f68eb7fa1e68d9daff69be185d3219b6f	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
325cd15afce75f0404887cae52d53b82feae9d6f5ce18b03ced15d5d0c5c4dce	-	Memory Dump	976.00 KB	application/octet-stream	-	MALICIOUS
f1212cc5741fa30c9305dfcdaa75829e63b9bf0430344c353566d96b358d519a	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
4d81645bd48c56d6696b3869fabe8268d7e779aa5016c783685015245dd4599b	-	Memory Dump	976.00 KB	application/octet-stream	-	MALICIOUS
06a1cb91c8cdde3acbc45d94ea3254a7728aa394f696c8d692ee2d85ac63d0f7	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
3dc6a71c59bee11e3993c00963a391509a243d1c257de6ed12d30ab654bc4b19	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
ad5ef651c1b0b3dc87318f9530823ab574b6704a8c34d83fbf14b53ba1b4557a	-	Memory Dump	184.00 KB	application/octet-stream	-	MALICIOUS
d01c69d09282f9050f6b113c45884fe9b9abf3bdf5bd93b45927d9b6bfb233fe	C:\Users\KEECFM~1\AppData\Local\Temp_tcx1h.zip, c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\sqlite-dll-win32-x86-3180000[1].zip	Downloaded File	433.21 KB	application/zip	Access, Create	SUSPICIOUS
5ea67d6b7f67301ca214af511740f26b9e6cc9e16b2c0ec7bba071d05b9bde78	sqlite3.dll, c:\users\keecfmwgj\appdata\local\temp\sqlite3.dll	Archive File	828.29 KB	application/vnd.microsoft.portable-executable	-	SUSPICIOUS
8cabab28c552a673cdec3b0cf100753a486a10ed030fcbaad5fba62053d77277	-	Downloaded File	8.54 KB	text/html	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d3dc34a197341b4e5e089f3034d65b685b9098d03233e00223e877309a4abb21	-	Downloaded File	8.00 KB	text/html	-	CLEAN
668d19dd59d951fc5298d1fdb90d005a66b06e206f63040fe5d51a48cb5f6ef8	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
66aec8e88abc0e3478714b25fcff2b1b936f692de1f19057c44dd1b6a29a806f	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
5dc1ae0b875dc0d78dbc5532226f5f31b762b4d1229984f605d27bf895ab6807	-	Downloaded File	1.21 KB	text/html	-	CLEAN
3a593be1e2b16bdb1f4eb2d3fdb8d1945cbbfc03e72106813e25977ead9205b0	-	Downloaded File	336 bytes	text/plain	-	CLEAN
73f3bcb688474ce336efff25f73e963083fbbcbf90f86acd16b72eaf8e43fec5	-	Downloaded File	336 bytes	text/plain	-	CLEAN
9e8756bdc95f4227166cf7b6d054b0e6def9ff6561b481d05b6e190182f8badf	-	Downloaded File	636 bytes	text/plain	-	CLEAN
19c90f9f8d5892b6d5b646045957d8d1fb905cbec0be290f4dff87efd84b21b2	-	Downloaded File	336 bytes	text/plain	-	CLEAN
63001f4fcbcce8816b4aa76d90d927bf11a6a6920d348d933a6bb556268384b9	-	Downloaded File	11.07 KB	text/html	-	CLEAN
866b370ff5a2568bc04e6b8a01b70d6dd63e98435cf55dc89b0a9d38106e1bc2	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
ff3cc78438cd7aaf852f136bfe301b0fdf1518ab03713390fd3728ed2039489e	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
6edf9704b24f53df8e4a998b42ff09d03e546655c004a66ae27ad10d4d005dd4	-	Downloaded File	336 bytes	text/plain	-	CLEAN
6b4475635131ff4e1b507af867c9946a4d6a4c7be215f4e6d8febb7cee7743ae	-	Downloaded File	336 bytes	text/plain	-	CLEAN
396d5a0eea5e0fda8bc47558d1f8a8d3960c03a861fceaa398ba494c48762417	-	Extracted File	35.94 KB	image/png	-	CLEAN
8efee8c14157ee1e4a1fc3d575c47ab1151b40c8a9c3a741df4c71b1fcd7e7c2	-	Downloaded File	1.25 KB	text/html	-	CLEAN
bb99ea9bc045fb68dac61c4b04206e94a111fbfe51058b2bbad27680bfb649ae	-	Downloaded File	936 bytes	text/plain	-	CLEAN
90cb9fe49a0a32c1c48eef5c88ff86ae64baaf7a456626eb25255b65eac912a1	-	Downloaded File	1.45 KB	text/plain	-	CLEAN
f4ee0edb614fe1d174f8a6b703f0714d1707b2680f0cea63201c4f37d54dc878	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
c5edf6afd22dd7fd0efa2996716f25cd739731caea328532a8fd6ec64600e630	sqlite3.def, c:\users\keecfmwgj\appdata\local\temp\sqlite3.def	Archive File	4.88 KB	text/plain	-	CLEAN
8c87ec7759236eca4daad974b4f11dd30431b5486851f6aa104176418ca4b86b	-	Downloaded File	188 bytes	text/plain	-	CLEAN
016d9c43e3bb24db9d9f9b502ba6053967537aa2882994caf48501e6881e256c	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
1bca668d5d122dc944cc5a54047a0a80636debdfc7224637531e0d1771d285f9	-	Downloaded File	188 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2e36fc7965b8a3495ad4aeb379f93df4906e787e1db1079b166ced59e791aceb	-	Downloaded File	2.21 KB	text/plain	-	CLEAN
a8291f2137138c4a5b317d055de81ae8f40410e0b004a39ee376b3401f0679b6	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
0310703470d216b010c7b1ea8049df27624adbdd6c095c84b006610bff31c584	-	Downloaded File	188 bytes	text/plain	-	CLEAN
333cd6f23812770a0d0383e0b50d5f7b260751e0c35489b4e0bb174ccb20d467	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
34e95ef48aee8af0ffbe0ad651ea2a758c2ec9d65859c6c9fbe6649ab53dd0ff	-	Downloaded File	3.42 KB	text/html	-	CLEAN
1ff0982b45d0f2f0a015640dbd5082fb7557666639b12dddcc65818e1ac1598e	-	Extracted File	26.99 KB	image/png	-	CLEAN
7df196b204950e3afb23fa548303eb358010bd846a404f0afe0f715c2e1394de	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
662c95ab3a6d996380d317cba4cc2644652629adfa4124006b94f68c3750c76c	-	Downloaded File	188 bytes	text/plain	-	CLEAN
7392749832c70fcfc2d440d7afc2f880000dd564930d95d634eb1199fa15de30	-	Downloaded File	593 bytes	text/html	-	CLEAN
c06a91f75af500ae461afa0936bf0b221c5dc6aa01cf2d34d641c1fdfc76662f	-	Downloaded File	188 bytes	text/plain	-	CLEAN
11017aed5bb0dc7beab781884b86e2c9c033b541265742230a9768c8ddec7124	-	Downloaded File	17.33 KB	text/html	-	CLEAN
4ae03599dab2776fe60770c26a681772adff840a15f42c51eede6ffb3cada5ae	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
5c2866bf9a3715cad85cda5401fdce8b58553d2811f17a07d8b04a6b21f96aff	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
761795d88168bf0c8843ee677afa4bc062887f947c5859b8b1453b3ce1b74cf3	-	Downloaded File	2.33 KB	text/plain	-	CLEAN
4fe5b7d3f7b58acd60527573fa28459bb591c27aa8c9cda72fd8cb229cf37bfa	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
3c5c0554c0dfecebcb2e2079bb8dcad6d74bec0fbe7753067502ed098fc574c5	-	Downloaded File	8.53 KB	text/html	-	CLEAN
74ac52d11c9bb070670a89aa26554c6cb8ad9bf69376b970b119471459d9ceaf	-	Downloaded File	626 bytes	text/html	-	CLEAN
b247588eac52856f03e2b2638541a86933b387040e31583e425300661dd5d07b	-	Downloaded File	188 bytes	text/plain	-	CLEAN
7f4ddfe1388169265d75968984680ff70b4d24f0ad3b529fa43872c96f7c8212	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
56e91ebbf6b455d5118b71295a7b7772ae32957b5b6c048766f6da1eab4d2123	-	Downloaded File	1.45 KB	text/plain	-	CLEAN
37a4e56c497e170de6e152bc479624eb8d7ccb35bad5a190f2fdb17ac699cffa	-	Downloaded File	708 bytes	text/html	-	CLEAN
597822560c88bae1905e3cd029c4e607dc0bf98abe3dcac69d60b3595b2be782	-	Downloaded File	336 bytes	text/plain	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7d04f7431bbfa41a04bcc7e6b98b9de0d919756c4c671c5785c99fff45f16402	-	Downloaded File	13 bytes	text/plain	-	CLEAN
2a999def46397a0b61e43331e03d9e1f10af284a5dee8da77d8f75d16ef748b7	-	Downloaded File	188 bytes	text/plain	-	CLEAN
f8ea8df569cc34ccb663cc77fc7b31bbb3d9af80d054a9652e22d8965d8acd29	-	Downloaded File	636 bytes	text/plain	-	CLEAN
7f8c7f918148b32820b0c39f8904de975147f2a5d34a3f676298a691ae857284	-	Downloaded File	3.56 KB	text/html	-	CLEAN
a9fa386e483bfaa1c66968145cc2ae564c56b298dff9efd3005aae921cc11f26	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
88f788f6d8f482bbe5db00bed9872ae3edd99547f1ab94f0b4756ac58ca4c839	-	Downloaded File	2.21 KB	text/plain	-	CLEAN
77d609a14fb139047d5732049f650c90490f7d69d97454755fa4c60744bfaf45	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
d749f89f753bb2f9b43d0e7079999798a38dc4972f4099d33e869bf62707a328	-	Downloaded File	188 bytes	text/plain	-	CLEAN
fc20222674c7c79cd598e99b1d0bef3522224ee9e8bc9b7a8272c2b83f2026c6	-	Downloaded File	188 bytes	text/plain	-	CLEAN
1cac6b4d71c810845995320580597bf6c494885fc2f570bc8c248a0690bac90d	-	Downloaded File	1.45 KB	text/plain	-	CLEAN
78bb47a24e0d3efa0e99e0830fb8d234fad0d37c8961c2d3bdc1ce22346aef7b	-	Downloaded File	336 bytes	text/plain	-	CLEAN
e5fceef1e5b8a800a62a5e1df12254a569b281a86befda4cb9f49f7e4309d9bd	-	Downloaded File	2.32 KB	text/plain	-	CLEAN
78f0414c1b612b9609357c2cff962cf8cfa3c60a2aa728b7f6f72d98dbc26e42	-	Downloaded File	188 bytes	text/plain	-	CLEAN
d130061346747c43f73ab0956fd626f657f485f9eb1f19bdaa6696bf443050e7	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
df68bc5677cecff63bf08e972e57b822a1577d0d4b685b6ed4561a7be31a36e8	-	Downloaded File	188 bytes	text/plain	-	CLEAN
e95b6352c3a5a7d9ed74f3b2f21336373282ac96d76e240bc871b91528686882	-	Downloaded File	336 bytes	text/plain	-	CLEAN
56489013fc13adceecac297998a70d4bb0bc99527ef8e01e6ca12a0065060d41	-	Downloaded File	336 bytes	text/plain	-	CLEAN
9b342ae7f25d65bdb817d8c995f3211ac398e41575fc5d149d994c1dcb008f0a	-	Downloaded File	1.14 KB	text/html	-	CLEAN
07306b21988085c2bcc5f2c8715ad71494d1fa300cb6d5502718d4737a0b21f1	-	Downloaded File	188 bytes	text/plain	-	CLEAN
fc96b639f05fad089b30bf2737ca12f1709912f2b13f0da427a8b4e8175754f6	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
87a9323ac85ce28867d5d7ce590c8f29b8d1a999961fca71bb33adef48683691	-	Downloaded File	166 bytes	text/html	-	CLEAN
04b4a505219ac79883742c94cf173228fc368534fd7976d0fbadf247d1427af4	-	Downloaded File	389 bytes	text/html	-	CLEAN

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
0d069336c69c77c310b58bdf6e00536c105d153605be2137718953f47560a8a0	-	Downloaded File	1.45 KB	text/plain	-	CLEAN
417754d30f20886abc1d0216efc09bae7e4de22e7850b5b0a0814d904dbd6dba	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
ff06d11f01e006a20723e9aadf5483af9e535628a81efdb56266578908cdf519	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
d4638586159427f4c7e5827bf6501629d2782f053759b3693e5e44860d0fb747	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
f70c13835fbe4b1d2de63707b16498df0107eb9d22b146cf360f2d77787a68b7	-	Downloaded File	3.11 KB	text/plain	-	CLEAN
eee0525b2681d294f50c8e6cc41743fec9aedd84df2541c616e26f85651ae8d7	-	Downloaded File	188 bytes	text/plain	-	CLEAN
e40506547551e9b3e4c4714d9f3bb65fdb77e943b7804c3df2ee64ce230b6fb9	-	Downloaded File	188 bytes	text/plain	-	CLEAN
1fbf916e641e62c1f712fbe786919ea8da6147420e0c85f3670ef9e6a4777e25	-	Downloaded File	2.32 KB	text/plain	-	CLEAN
5e0b0a2df310ad006c3915218a9ef44030e681d687737dc4d51792d83ab27cf6	-	Downloaded File	1.16 KB	text/plain	-	CLEAN
e829bdc9a6d04b8dbb7ca238ed25c9a64749ee8e8af33d616f2a3fdb05c03b5b	-	Downloaded File	188 bytes	text/plain	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\schemas.rtf	Sample File	-	MALICIOUS
\??\C:\Program Files\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Chromium\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Kinza\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CCleaner Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\7Star\7Star\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\BraveSoftware\Brave-Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CentBrowser\User Data	Accessed File	Access	CLEAN
\??\C:\Windows\SysWOW64\ntdll.dll	Accessed File	Access, Create, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Elements Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\uCozMedia\Uran\User Data	Accessed File	Access	CLEAN
c:\users\keecfmwgj\appdata\local\temp\sqlite3.dll	Dropped File, Extracted File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CocCoc\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Comodo\Dragon\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Kometa\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Google\Chrome\User Data\	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Blisk\User Data	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\QIP Surf\User Data	Accessed File	Access	CLEAN
\??\C:\Program Files (x86)\Mozilla Firefox\Firefox.exe	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Slimjet\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Chedot\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Yandex\YandexBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Coowon\Coowon\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Vivaldi\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Fenrir Inc\Sleipnir5\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\liebao\User Data	Accessed File	Access	CLEAN
sqlite3.def	Miscellaneous File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CatalinaGroup\Citrio\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\SalamWeb\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Iridium\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Torch\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Opera Software\Opera Neon\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\MapleStudio\ChromePlus\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Amigo\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\360Chrome\Chrome\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\AVG\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Sputnik\Sputnik\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Edge\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Orbitum\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Opera Software\Opera Stable	Accessed File	Access	CLEAN
c:\users\keecfmwgj\appdata\local\temp\sqlite3.def	Dropped File, Extracted File	-	CLEAN
sqlite3.dll	Miscellaneous File	-	CLEAN
\??\C:\Program Files (x86)\Windows Media Player\wmplayer.exe	Accessed File	Access, Create, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Local\URBrowser\User Data	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp_tcx1h.zip	Accessed File, Downloaded File, Extracted File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\AVAST Software\Browser\User Data	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Opera Software\User Data	Accessed File	Access	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\x9ohk109\sqlite-dll-win32-x86-3180000[1].zip	Downloaded File, Extracted File	-	CLEAN
\??\C:\Windows\SysWOW64\control.exe	Accessed File	Access, Create, Read	CLEAN
0	Miscellaneous File	-	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Epic Privacy Browser\User Data	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://www[.]framedeals[.]buzz/6rpu/	Extracted, Contacted	104.21.73.200, 172.67.165.207	United States	POST	MALICIOUS
hxxp://www[.]framedeals[.]buzz/6rpu/?Ppu=kYINAY0yQ323qkefT2XXzDAGfk6UP2Z8qRCNSz8Z+f0CQfYwboHLsC+C3xIpdzKwExr+OWy9bbGV1GkwXCaFZfOYVChXXqLqY4/rWEj3RUsR&DZ5B=cD5cmh4y	Extracted, Contacted	104.21.73.200, 172.67.165.207	United States	GET	MALICIOUS
hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQVSyUGXzQpZ/oFi4h3H+24HKXEY2nSdAWJvneOcGgUMami2cKwsJYEJKxKHg8oLM7F69NEQAVQI58PqH8f3g+0+F+5h2vKnRoveqo7gmIa&0ZtwYy=0Hz0YF	Extracted, Contacted	23.231.93.253	United States	GET	MALICIOUS
hxxp://www[.]edirassini[.]com/6rpu/?Ppu=ImQVSyUGXzQpZ/oFi4h3H+24HKXEY2nSdAWJvneOcGgUMami2cKwsJYEJKxKHg8oLM7F69NEQAVQI58PqH8f3g+0+F+5h2vKnRoveqo7gmIa&DZ5B=cD5cmh4y	Extracted, Contacted	23.231.93.253	United States	GET	MALICIOUS
hxxp://www[.]edirassini[.]com/6rpu/	Extracted, Contacted	23.231.93.253	United States	POST	MALICIOUS
hxxp://www[.]gchiase2[.]click/6rpu/?Ppu=mVJlWZfSFHBRFuERTuOkIOQuZAXsug76Rb6U1r41UoL2DX3aPzUPzNqBIjYL7ti450ag3Bo6IZ1IbJeCG+GGgpjFIX3p2LcfmCwIg5QT40TU&DZ5B=cD5cmh4y	Extracted, Contacted	52.74.11.229, 54.179.30.8, 13.215.123.39	Singapore	GET	SUSPICIOUS
hxxp://www[.]gchiase2[.]click/6rpu/	Extracted, Contacted	52.74.11.229, 54.179.30.8, 13.215.123.39	Singapore	POST	SUSPICIOUS
hxxp://www[.]shokugyo[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]darkbert[.]cloud/6rpu/	Extracted, Contacted	74.208.236.60	United States	POST	CLEAN
hxxp://www[.]linyapda[.]com/list-3/3234.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://workationdelsol[.]com/xmlrpc.php	Extracted	81.169.145.159	Germany	-	CLEAN
hxxp://www[.]smartviolet[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/2544.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/2063.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]sbys021[.]cyou/6rpu/	Extracted, Contacted	67.198.197.12	United States	POST	CLEAN
hxxps://fonts[.]gstatic[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]solusiphone[.]com/6rpu/?Ppu=faBeZhPX5eU5QXnFE+dc5CPYIMWUyDTtNeptDe6h+cF53wfgkO0luiweZ75MuMUHzFerSygnYX9lViN9G1duoMBKfooktpsWGEWEJ85M6QrA&0ZtwYy=0Hz0YF	Extracted, Contacted	202.52.146.246	Indonesia	GET	CLEAN
hxxp://www[.]sbys021[.]cyou/6rpu/?Ppu=Rcz2mjU14OA8QPxc1N2OacQW0VRi8xNHbgUYKLKbYTAEagufCdnbRwOPW/Gop3dIJvGGvn9orV1ZZoltHd4LeWC1vTbbcjBsq04JHSaAYe2A&0ZtwYy=0Hz0YF	Extracted, Contacted	67.198.197.12	United States	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-4/033.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4498.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://nginx[.]net	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/3459.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/023.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4305.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4047.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxps://domaincntrol[.]com/?orighost=	Extracted	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://www[.]linyapda[.]com/list-3/461.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]margosinc[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]paulciganek[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/94.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxps://nojs[.]domaincntrol[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/3789.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/050.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/968.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/6rpu/	Extracted, Contacted	104.223.129.53	United States	POST	CLEAN
hxxp://www[.]linyapda[.]com/list-4/434.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]ithinkhealth[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]noonprince[.]site/6rpu/	Extracted, Contacted	64.225.91.73	United States	POST	CLEAN
hxxp://www[.]cniddm[.]com	Extracted	-	-	-	CLEAN
hxxps://zz[.]bdstatic[.]com/linksubmit/push.js	Extracted	-	-	-	CLEAN
hxxp://www[.]madfishman[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4597.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/035.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/350.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]mcqueen08[.]shop/6rpu/?Ppu=8yF31yfwMGrwMgoGkeZJNAXs9+B9vl5goWUEgFES0xLujVmhnvwjmM2B3xNOFxdj+WRtsZIGrVX1sTyq4/MVxCvZ4V21BvasviIPjTali1bE&DZ5B=cD5cmh4y	Extracted, Contacted	198.252.104.158	United States	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-4/025.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]gurasi[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]sqlite[.]org/2017/sqlite-dll-win32-x86-3180000.zip	Extracted, Contacted	45.33.6.223	United States	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-3/2807.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4085.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]camrose[.]top/6rpu/	Extracted, Contacted	66.29.131.66	United States	POST	CLEAN
hxxps://hm[.]baidu[.]com/hm.js?fe6a346f32de57f467ca0b7cfd87bfa1	Extracted	-	-	-	CLEAN
hxxp://push[.]zhanzhang[.]baidu[.]com/push.js	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/3538.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/020.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]hsph[.]net/6rpu/?Ppu=bp/9yUFv9lJJcN4JNIhXerCAgTu6Or+k1MY0Iurax5GDqLc+waTZ9JvidWLEdxfT5I792dN+01Rq7OGlRf0JTNYGmkd4Oz97hk03rUvUIxej&DZ5B=cD5cmh4y	Extracted, Contacted	156.234.184.200	Hong Kong	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4675.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4341.html	Extracted	104.223.129.53	United States	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://www[.]linyapda[.]com/list-3/3383.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]ketomealplann[.]online/6rpu/	Extracted, Contacted	162.240.81.18	United States	POST	CLEAN
hxxp://www[.]linyapda[.]com	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]interjetinc[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/129.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/6rpu/?Ppu=JNMU5lRt9TQe5nNO1Sbk4VxBCXrLWLA+kd/L3q3uoel7JjKZIKJMPyDJgqUHRkY/QYEd1fE6OYjcL8erFU5Zx1xTZddScdwaDztYO0AT1ncL&DZ5B=cD5cmh4y	Extracted, Contacted	104.223.129.53	United States	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-4/77.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4905.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]gunsperu[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]camrose[.]top/6rpu/?Ppu=N+WSMqmqRmb14d9QzRyAN3xsZDrnSAfhhEAa8OEYiCceR0oEixBRMbPxz1+3q8NVlie0/YhDq1RnPn7pB4JelypIFUJz8NQwEq5o/aBJ34jg&DZ5B=cD5cmh4y	Extracted, Contacted	66.29.131.66	United States	GET	CLEAN
hxxp://www[.]lacalatruite[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4639.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/647.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]noonprince[.]site/6rpu/?Ppu=jJ/+gArpHQbXobQt+1ki5xkEHX4MSTPPinzeMGb0J4bJuhIdtq7hM8JTt7JawuX2uibibnvCsht7tkzSg6k/YHT9h54N81SDw8rE87yE9Zwo&DZ5B=cD5cmh4y	Extracted, Contacted	64.225.91.73	United States	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-3/3754.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]workationdelsol[.]com/6rpu/?Ppu=bEVJe5rzh1pqq+KFzm7Z+MzxelhnwO+hrg1IyrCWTePQJ5Zn93SpngadGKgonJqu9tF4GcuUAaTMG+CUi1c4mFrYfPuJEoj4aymWhQI+O0AJ&DZ5B=cD5cmh4y	Extracted, Contacted	81.169.145.159	Germany	GET	CLEAN
hxxp://www[.]bazararaira[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com//4.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]sahibinizim[.]com/6rpu/	Extracted, Contacted	85.159.66.93	Turkey	POST	CLEAN
hxxp://www[.]drsaulson[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]ketomealplann[.]online/6rpu/?Ppu=YhpgcRwO6+pWSfeSjyLhlLoZP/EzdYlsk0TmHSB5wknwPdVcUjrVLv9VIK7YWCaX0UccOKRnfdC48X7PtpX8/Wj5tY1GsAn75acQ2dSPUiCC&0ZtwYy=0Hz0YF	Extracted, Contacted	162.240.81.18	United States	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-3/3265.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]litespeedtech[.]com/error-page	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/127.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/039.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4997.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]alextsoucas[.]com	Extracted	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://www[.]sahibinizim[.]com/6rpu/?Ppu=lJq/LhGK9DOZEGMpf2olbPXQGZgyLkip1hmFhlmGKm2rNGuqXmLfg2nedVtlUVUZ0TQZBbOz6gvWTDwJXkmVYYKgAUnwn9bOWCBMGhBnErqQ&DZ5B=cD5cmh4y	Extracted, Contacted	85.159.66.93	Turkey	GET	CLEAN
hxxp://www[.]linyapda[.]com/list-4/029.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/2228.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://fedoraproject[.]org	Extracted	-	-	-	CLEAN
hxxp://www[.]mcqueen08[.]shop/6rpu/	Extracted, Contacted	198.252.104.158	United States	POST	CLEAN
hxxp://www[.]qsw17[.]com/6rpu/	Extracted, Contacted	154.204.182.49	Hong Kong	POST	CLEAN
hxxp://www[.]sabao-barra[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]workationdelsol[.]com/6rpu/	Extracted, Contacted	81.169.145.159	Germany	POST	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4348.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]hsph[.]net/6rpu/	Extracted, Contacted	156.234.184.200	Hong Kong	POST	CLEAN
hxxp://www[.]solusiphone[.]com/6rpu/	Extracted, Contacted	202.52.146.246	Indonesia	POST	CLEAN
hxxp://www[.]linyapda[.]com/list-3/676.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]qsw17[.]com/6rpu/?Ppu=JVO1m5e/3foRHFKnRvmKZH7D1Zp5kDwhgVsUBOwS8GWoPpxixj0lRTL1XpPbi2O/iXpzZpAddedLxDwl+fDFr8e+q9qu1LfVAh/O9o1R7V42&DZ5B=cD5cmh4y	Extracted, Contacted	154.204.182.49	Hong Kong	GET	CLEAN
hxxp://www[.]taxrice[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/4455.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/64.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/054.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]solusiphone[.]com/6rpu/?Ppu=faBeZhPX5eU5QXnFE+dc5CPYlMWUyDTtNeptDe6h+cF53wfgkO0luiweZ75MuMUHzFerSygnYX9lViN9G1duoMBKfooktpsWGEWEJ85M6QrA&DZ5B=cD5cmh4y	Extracted, Contacted	202.52.146.246	Indonesia	GET	CLEAN
hxxp://www[.]conanstower[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]graciesantos[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-3/3627.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]myxxxcentral[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]darkbert[.]cloud/6rpu/?Ppu=ZlX90GMmr8OogOg59rJ1Sq68WWCkPNLZb0E+DI3GqNea2L8xU9jjz42bwiq3b+jjRv/wmCHBdMxVdMSvPhr8nNujTmRdkSiXjzcB21PbyZmB&0ZtwYy=0Hz0YF	Extracted, Contacted	74.208.236.60	United States	GET	CLEAN
hxxp://www[.]3ycgf7x2[.]com/6rpu/?Ppu=9sSRcqZov6Qtq4zmkSZBGZmXdQYu9z+k6EqEB/Sh3ZqUM3BBgmi3SjIHjOpo7drCVTaguvFHZF5loeh6oTyBKI0lwK6sDJGoLREcMJkpJ4t8&DZ5B=cD5cmh4y&wn=1	Extracted, Contacted	156.235.147.223	Hong Kong	-	CLEAN
hxxp://www[.]bjjfsd[.]com	Extracted	-	-	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/494.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com/list-4/056.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]markstef[.]com	Extracted	-	-	-	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://www[.]linyapda[.]com/list-3/178.html	Extracted	104.223.129.53	United States	-	CLEAN
hxxp://www[.]linyapda[.]com//5.html	Extracted	104.223.129.53	United States	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www[.]framedeals[.]buzz	104.21.73.200, 172.67.165.207	United States	HTTP, DNS, TCP	MALICIOUS
www[.]edirassini[.]com	23.231.93.253	United States	HTTP, DNS, TCP	MALICIOUS
www[.]steanmcomunity[.]com	-	-	-	MALICIOUS
www[.]gchiase2[.]click	52.74.11.229, 54.179.30.8, 13.215.123.39	Singapore	HTTP, DNS, TCP	SUSPICIOUS
mcqueen08[.]shop	198.252.104.158	United States	HTTP, DNS, TCP	CLEAN
domaincntrol[.]com	-	-	-	CLEAN
www[.]margosinc[.]com	-	-	-	CLEAN
www[.]drsaulson[.]com	-	-	-	CLEAN
nojs[.]domaincntrol[.]com	-	-	-	CLEAN
www[.]bazararaira[.]com	-	-	-	CLEAN
dns[.]ladipage[.]com	52.74.11.229, 54.179.30.8, 13.215.123.39	Singapore	HTTP, DNS, TCP	CLEAN
www[.]e-fite[.]com	-	-	-	CLEAN
nginx[.]net	-	-	-	CLEAN
solusiphone[.]com	202.52.146.246	Indonesia	HTTP, DNS, TCP	CLEAN
www[.]conanstower[.]com	-	-	-	CLEAN
www[.]solusiphone[.]com	202.52.146.246	Indonesia	HTTP, DNS, TCP	CLEAN
www[.]gurasi[.]com	-	-	-	CLEAN
www[.]sqlite[.]org	45.33.6.223	United States	HTTP, DNS, TCP	CLEAN
fedoraproject[.]org	-	-	-	CLEAN
www[.]markstef[.]com	-	-	-	CLEAN
www[.]farfetich[.]com	-	-	-	CLEAN
www[.]alextsoucas[.]com	-	-	-	CLEAN
fonts[.]gstatic[.]com	-	-	-	CLEAN
www[.]smartviolet[.]com	-	-	-	CLEAN
www[.]paulciganek[.]com	-	-	-	CLEAN
push[.]zhanzhang[.]baidu[.]com	-	-	-	CLEAN
www[.]mcqueen08[.]shop	198.252.104.158	United States	HTTP, DNS, TCP	CLEAN
www[.]sabao-barra[.]com	-	-	-	CLEAN
www[.]qsw17[.]com	154.204.182.49	Hong Kong	HTTP, DNS, TCP	CLEAN
www[.]ketomealplann[.]online	162.240.81.18	United States	HTTP, DNS, TCP	CLEAN
zz[.]bdstatic[.]com	-	-	-	CLEAN
www[.]madfishman[.]com	-	-	-	CLEAN

Domain	IP Address	Country	Protocols	Verdict
www[.]gunsperu[.]com	-	-	-	CLEAN
www[.]darkbert[.]cloud	74.208.236.60	United States	HTTP, DNS, TCP	CLEAN
www[.]ithinkhealth[.]com	-	-	-	CLEAN
redirect[.]natrocdn[.]com	85.159.66.93	Turkey	HTTP, DNS, TCP	CLEAN
www[.]noonprince[.]site	64.225.91.73	United States	HTTP, DNS, TCP	CLEAN
www[.]sbys021[.]cyou	67.198.197.12	United States	HTTP, DNS, TCP	CLEAN
www[.]3ycgf7x2[.]com	156.235.147.223	Hong Kong	DNS, TCP	CLEAN
www[.]shokugyo[.]com	-	-	-	CLEAN
www[.]camrose[.]top	66.29.131.66	United States	HTTP, DNS, TCP	CLEAN
www[.]araclarinlav[.]net	-	-	-	CLEAN
www[.]lacalatruite[.]com	-	-	-	CLEAN
www[.]litespeedtech[.]com	-	-	-	CLEAN
www[.]workationdelsol[.]com	81.169.145.159	Germany	HTTP, DNS, TCP	CLEAN
www[.]myxxxcentral[.]com	-	-	-	CLEAN
www[.]graciesantos[.]com	-	-	-	CLEAN
www[.]taxrice[.]com	-	-	-	CLEAN
www[.]sahibinizim[.]com	85.159.66.93	Turkey	HTTP, DNS, TCP	CLEAN
www[.]linyapda[.]com	104.223.129.53	United States	HTTP, DNS, TCP	CLEAN
hm[.]baidu[.]com	-	-	-	CLEAN
www[.]cniddm[.]com	-	-	-	CLEAN
natroredirect[.]natrocdn[.]com	85.159.66.93	Turkey	HTTP, DNS, TCP	CLEAN
www[.]bjjfsd[.]com	-	-	-	CLEAN
ketomealplann[.]online	162.240.81.18	United States	HTTP, DNS, TCP	CLEAN
www[.]interjetinc[.]com	-	-	-	CLEAN
www[.]hsph[.]net	156.234.184.200	Hong Kong	HTTP, DNS, TCP	CLEAN
workationdelsol[.]com	81.169.145.159	Germany	HTTP, DNS, TCP	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
162.240.81.18	ketomealplann[.]online, www[.]ketomealplann[.]online	United States	HTTP, DNS, TCP	MALICIOUS
104.21.73.200	www[.]framedeals[.]buzz	-	HTTP, DNS, TCP	MALICIOUS
85.159.66.93	www[.]sahibinizim[.]com, natroredirect[.]natrocdn[.]com, redirect[.]natrocdn[.]com	Turkey	HTTP, DNS, TCP	MALICIOUS
156.234.184.200	www[.]hsph[.]net	Hong Kong	HTTP, DNS, TCP	MALICIOUS
66.29.131.66	www[.]camrose[.]top	United States	HTTP, DNS, TCP	MALICIOUS
52.74.11.229	dns[.]ladipage[.]com, www[.]gchiase2[.]click	Singapore	HTTP, DNS, TCP	MALICIOUS
81.169.145.159	www[.]workationdelsol[.]com, workationdelsol[.]com	Germany	HTTP, DNS, TCP	MALICIOUS

IP Address	Domains	Country	Protocols	Verdict
23.231.93.253	www[.]edirassini[.]com	United States	HTTP, DNS, TCP	MALICIOUS
202.52.146.246	solusiphone[.]com, www[.]solusiphone[.]com	Indonesia	HTTP, DNS, TCP	MALICIOUS
74.208.236.60	www[.]darkbert[.]cloud	United States	HTTP, DNS, TCP	MALICIOUS
104.223.129.53	www[.]linyapda[.]com	United States	HTTP, DNS, TCP	MALICIOUS
198.252.104.158	mcqueen08[.]shop, www[.]mcqueen08[.]shop	United States	HTTP, DNS, TCP	MALICIOUS
156.235.147.223	www[.]3ycgf7x2[.]com	Hong Kong	DNS, TCP	MALICIOUS
64.225.91.73	www[.]noonprince[.]site	United States	HTTP, DNS, TCP	MALICIOUS
67.198.197.12	www[.]sbys021[.]cyou	United States	HTTP, DNS, TCP	MALICIOUS
154.204.182.49	www[.]qsw17[.]com	Hong Kong	HTTP, DNS, TCP	MALICIOUS
13.215.123.39	dns[.]ladipage[.]com, www[.]gchiase2[.]click	Singapore	DNS	CLEAN
54.179.30.8	dns[.]ladipage[.]com, www[.]gchiase2[.]click	Singapore	DNS	CLEAN
45.33.6.223	www[.]sqlite[.]org	United States	HTTP, DNS, TCP	CLEAN
172.67.165.207	www[.]framedeals[.]buzz	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
12L541-4F23B2XB9	access	control.exe	CLEAN
0K12-A9Q7G4-282F	access	wmplayer.exe, control.exe	CLEAN
L96NQOTUUVCA42H_	access	control.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\QN0LCH6PBTDD	write, access	control.exe	SUSPICIOUS
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\WindowsUpdate	write, access	rundll32.exe	SUSPICIOUS
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\4b31ac339b3c6047a5607d10314f5a05	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	read, create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000003	read, create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\15.0\Outlook\Profiles\Outlook	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001	create, access	control.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\ae0727370bd4364ea1d3e75390877e70	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000002	read, create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook_2016	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\94ba7772fb349a48ba2cc741623a1549	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\c1b3326b5fa84f45970fa09da288db37	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\81fb1dc666658c4bb96e792ef5ce3051	create, access	control.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	read, create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\22165c4f0be62c48b2e3e9aef6ce3db3	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\a44d88fba08a5547a1aaad50659b22d8	create, access	control.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\00000001	read, create, access	control.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	access	rundll32.exe	CLEAN
HKEY_USERS\S-1-5-21-4219442223-4223814209-3835049652-1000\SOFTWARE\Microsoft\Internet Explorer\IntelliForms\Storage2	read, create, access	control.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	control.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Firefox	create, access	control.exe	CLEAN

Process

Process Name	Commandline	Verdict
behind-any-heavy.exe	"C:\Program Files\Windows Photo Viewer\behind-any-heavy.exe"	SUSPICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
rundll32.exe	rundll32 C:\Users\KEECFM~1\AppData\Local\Temp\Client.log,IEX A␒␌C	SUSPICIOUS
wmplayer.exe	rundll32 C:\Users\KEECFM~1\AppData\Local\Temp\Client.log,IEX A␒␌C	SUSPICIOUS
control.exe	"C:\Windows\SysWOW64\control.exe"	SUSPICIOUS

Process Name	Commandline	Verdict
winword.exe	"C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n	CLEAN
eqnedt32.exe	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding	CLEAN
cmd.exe	CmD.exe /C rundll32 %tmp%\Client.log,IEX A␒␌C	CLEAN
rundll32.exe	rundll32 C:\Users\KEECFM~1\AppData\Local\Temp\Client.log,IEX A␒␌C	CLEAN
next_story.exe	"C:\Program Files (x86)\Windows Defender\next_story.exe"	CLEAN

YARA / AV

YARA (16)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5
Malware	XLoader_3	XLoader	Memory Dump	-	Spyware	5/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
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	2023.3.1
Dynamic Engine Version	2023.3.1 / 07/17/2023 04:23
Static Engine Version	2023.3.1.0 / 2023-07-17 03:00:15
AV Exceptions Version	2023.3.1.2 / 2023-07-01 17:20:29
Link Detonation Heuristics Version	2023.3.1.2 / 2023-07-01 17:20:29
Smart Memory Dumping Rules Version	2023.3.1.2 / 2023-07-01 17:20:29
Config Extractors Version	2023.3.1.4 / 2023-07-07 07:05:07
Signature Trust Store Version	2023.3.1.2 / 2023-07-01 17:20:29
VMRay Threat Identifiers Version	2023.3.1.4 / 2023-07-07 07:05:07
YARA Built-in Ruleset Version	2023.3.1.4

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