ID: 440105
Sample Name: plan-1053707320.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:42:12
Date: 24/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

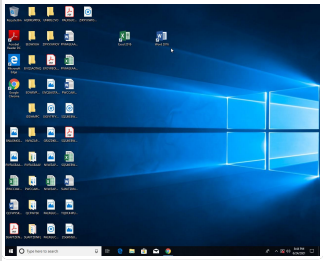
Windows Analysis Report plan-1053707320.xlsb

Overview

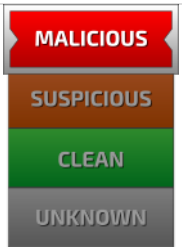
General Information

Sample Name:	plan-1053707320.xlsb
Analysis ID:	440105
MD5:	4854b4dcfa44103.
SHA1:	fa24422834d0f6c..
SHA256:	68741c1f5df351d..
Infos:	

Most interesting Screenshot:



Detection



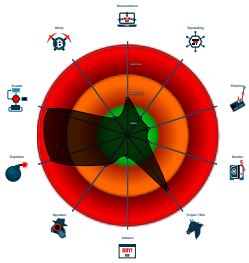
Hidden Macro 4.0 Qbot

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Schedule system p…
- Yara detected Qbot
- Allocates memory in foreign process…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Found abnormal large hidden Excel …

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 3152 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6088 cmdline: regsvr32 ..\gihi1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - explorer.exe (PID: 4784 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
      - schtasks.exe (PID: 5848 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn nowkkbo /tr 'regsvr32.exe -s \'C:\Users\user\gihi1.dll\" /SC ONCE /Z /ST 20:45 /ET 20:57 MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 1276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - regsvr32.exe (PID: 3488 cmdline: regsvr32 ..\gihi2.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - explorer.exe (PID: 5440 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- regsvr32.exe (PID: 4088 cmdline: regsvr32.exe -s 'C:\Users\user\gihi1.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5312 cmdline: -s 'C:\Users\user\gihi1.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 1200 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5312 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- regsvr32.exe (PID: 380 cmdline: regsvr32.exe -s 'C:\Users\user\gihi1.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 2124 cmdline: -s 'C:\Users\user\gihi1.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 4168 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 2124 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Qbot


```
{
  "C2 list": [
    "204.97.97.215:21858",
    "70.154.48.62:44327",
    "70.31.11.245:7267",
    "213.191.161.231:29643",
    "153.239.78.184:38503",
    "78.214.129.166:38539",
    "254.124.232.207:39310",
    "109.164.21.24:64901",
    "141.215.250.177:22875",
    "227.244.119.210:52552",
    "174.179.129.208:15267",
    "111.112.232.190:48521",
    "255.28.73.185:49979",
    "141.103.36.51:3939",
```

```
"116.110.10.187:25167",
"85.180.25.176:32726",
"79.254.143.27:14876",
"235.218.248.190:29975",
"161.4.87.73:5800",
"224.200.240.56:14635",
"9.155.72.32:55392",
"216.67.224.194:53640",
"141.121.237.255:1461",
"121.42.239.196:13549",
"179.179.31.112:63026",
"218.134.37.166:33358",
"239.135.100.181:9787",
"239.242.36.114:27696",
"60.26.149.129:8707",
"114.86.119.195:36123",
"154.85.103.18:33933",
"141.204.72.150:28929",
"229.176.154.40:1991",
"206.193.4.142:60112",
"113.150.134.145:14637",
"182.192.0.153:3039",
"37.235.119.158:25257",
"118.217.148.55:40918",
"157.238.131.159:17525",
"120.231.33.231:39242",
"113.196.247.102:57216",
"39.96.161.153:21974",
"37.95.209.127:37781",
"88.221.119.43:55621",
"49.191.149.88:15536",
"25.203.154.171:56937",
"160.244.29.108:63666",
"227.245.195.188:38491",
"11.191.229.149:48178",
"29.223.190.224:4552",
"144.140.245.179:62583",
"199.3.125.195:31574",
"37.158.174.86:39635",
"19.119.17.26:61415",
"18.218.204.94:25156",
"17.147.2.193:34433",
"232.165.224.232:64576",
"255.113.254.238:35466",
"244.159.158.34:29113",
"6.247.120.152:5539",
"20.23.44.234:12808",
"68.58.107.122:40009",
"177.71.146.158:14858",
"218.154.172.108:36509",
"59.198.167.253:53302",
"45.116.255.72:7036",
"11.48.233.235:37824",
"181.50.13.209:4123",
"8.141.223.46:63405",
"196.248.106.49:5168",
"123.119.149.61:15034",
"158.237.184.100:6941",
"47.102.246.133:28795",
"245.30.65.166:57241",
"96.17.6.131:61427",
"158.127.33.70:13273",
"171.113.240.107:55225",
"29.188.217.91:11621",
"233.26.116.125:35782",
"103.200.182.78:41414",
"212.166.144.41:13766",
"225.167.47.169:10108",
"218.233.238.210:11757",
"61.149.157.113:33452",
"224.147.98.25:43134",
"215.16.240.69:58681",
"69.158.146.64:33703",
"43.93.98.34:24929",
"94.211.166.245:8677",
"237.58.8.158:44902",
"22.105.125.67:37017",
"228.204.65.194:22014",
"240.58.16.219:55052",
"160.25.48.169:7011",
"48.255.58.190:27057",
"12.207.95.189:15569",
"100.104.109.104:51319",
"154.195.229.221:35588",
"98.133.117.21:26241",
"124.177.25.94:55126",
"59.211.38.81:7832",
"197.103.23.2:43598",
"123.210.126.131:49328",
"192.204.246.62:53778",
"220.178.117.122:65405",
```

```
    "32.177.158.150:9600",
    "186.12.160.146:13500",
    "217.11.103.56:65312",
    "183.137.66.59:24965",
    "73.73.123.212:54786",
    "84.4.148.67:50685",
    "173.176.181.154:13839",
    "216.1.166.66:2080",
    "144.122.242.245:52290",
    "115.127.247.89:14716",
    "25.5.112.94:8779",
    "40.151.136.48:36008",
    "78.114.25.179:8887",
    "185.149.69.37:4676",
    "66.204.28.22:17430",
    "50.138.243.152:7941",
    "195.170.56.121:46373",
    "189.236.221.185:38192",
    "39.35.83.72:15610",
    "213.64.255.229:34462",
    "27.98.20.110:25605",
    "250.34.90.10:20014",
    "55.164.192.159:18516",
    "89.170.84.87:31034",
    "195.228.141.229:32482",
    "67.144.76.43:2062",
    "217.168.11.163:26766",
    "212.238.116.17:9843",
    "109.26.22.183:43143",
    "58.142.103.104:44200",
    "200.39.220.35:59648",
    "115.127.244.231:37553",
    "150.184.143.159:42919",
    "14.29.250.1:10356",
    "86.168.140.17:49045",
    "62.128.177.85:27511",
    "219.13.32.40:17684",
    "60.225.8.42:6650",
    "113.94.94.176:17136",
    "243.196.184.116:25994",
    "168.243.164.189:60510",
    "217.56.43.145:25488"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.237315592.0000000000E00000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000002.00000002.237315592.0000000000E00000.00000004.00000001.sdmp	QakBot	QakBot Payload	kevoreilly	• 0x12623:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 0 8 49 81 ...
00000007.00000002.247270585.0000000000110000.00000040.00000001.sdmp	QakBot	QakBot Payload	kevoreilly	• 0x13223:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 0 8 49 81 ...
00000004.00000002.246220132.0000000004BA0000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000004.00000002.246220132.0000000004BA0000.00000004.00000001.sdmp	QakBot	QakBot Payload	kevoreilly	• 0x12623:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 0 8 49 81 ...

Click to see the 1 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.regsvr32.exe.10000000.3.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
2.2.regsvr32.exe.10000000.3.unpack	QakBot	QakBot Payload	kevoreilly	• 0x12623:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 0 8 49 81 ...
3.2.explorer.exe.510000.0.raw.unpack	QakBot	QakBot Payload	kevoreilly	• 0x13223:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 0 8 49 81 ...
4.2.regsvr32.exe.4ba0000.2.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
4.2.regsvr32.exe.4ba0000.2.unpack	QakBot	QakBot Payload	kevoreilly	• 0x11a23:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 0 8 49 81 ...

Source	Rule	Description	Author	Strings
Click to see the 13 entries				

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

Malicious sample detected (through community Yara rule)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found abnormal large hidden Excel 4.0 Macro sheet

Office process drops PE file

Persistence and Installation Behavior:

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion:

Tries to evade analysis by execution special instruction which cause usermode exception

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Qbot

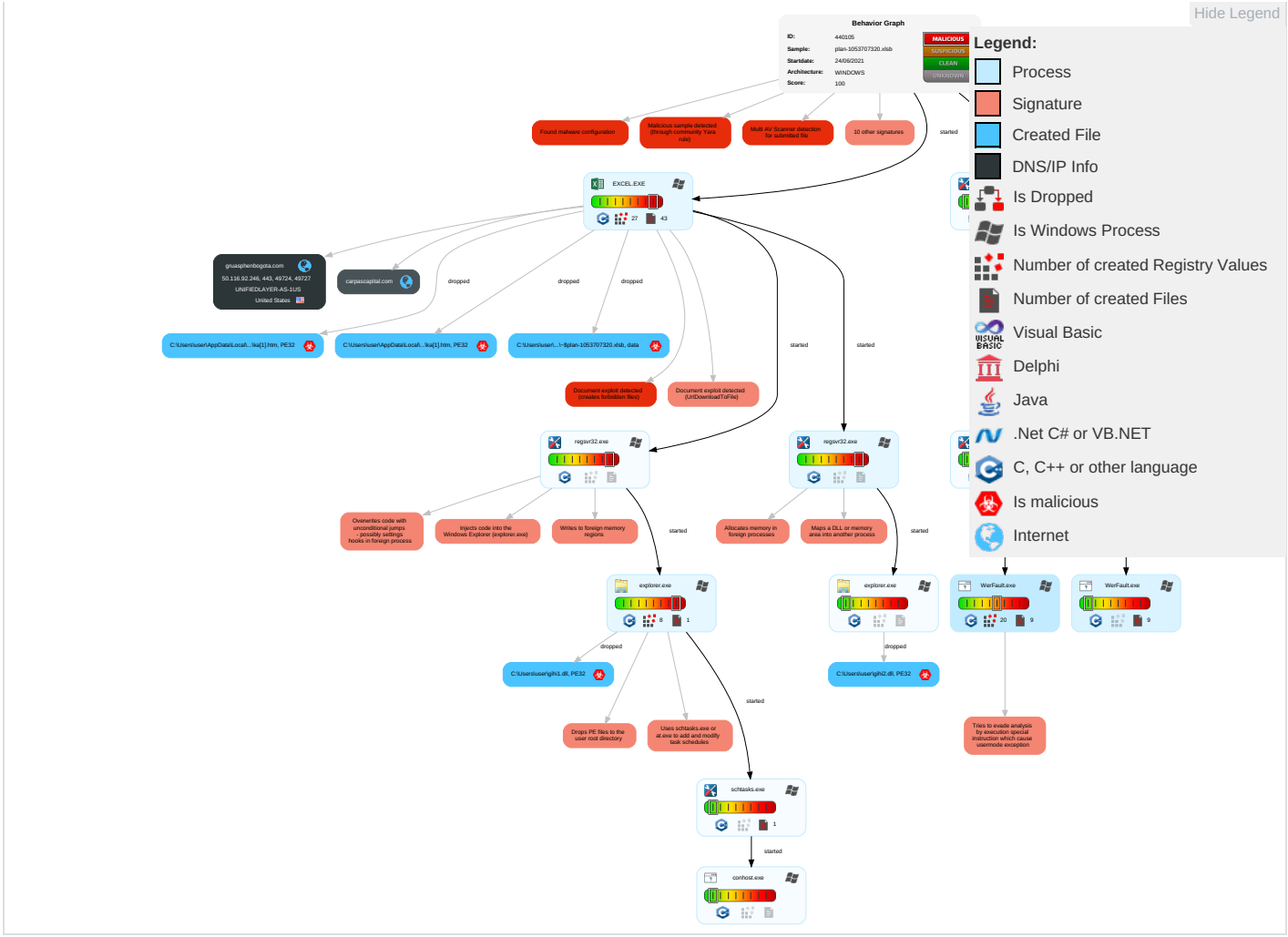
Remote Access Functionality:

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scripting 2	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eaves Insecu Netwo Comm
Default Accounts	Native API 3	Windows Service 3	Windows Service 3	Scripting 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 4 3	Scheduled Task/Job 1	Process Injection 4 1 2	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploi Track Locati
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 2	NTDS	System Information Discovery 1 1 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Service Execution 2	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Regsvr32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

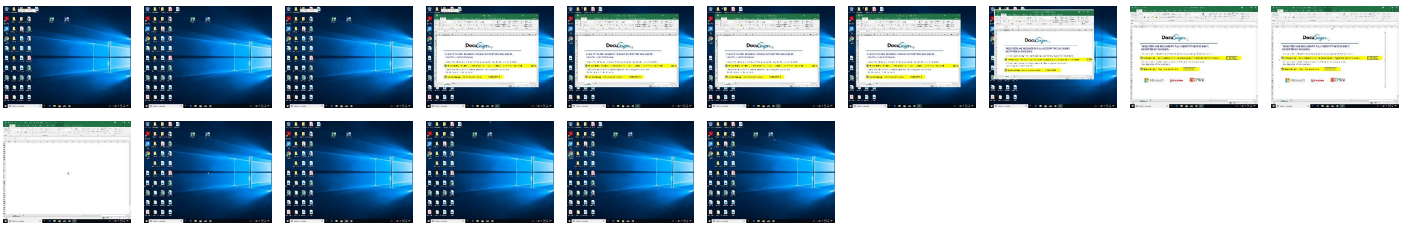
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
plan-1053707320.xlsb	26%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ka[1].htm	100%	Joe Sandbox ML		
C:\Users\user\gihi1.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ka[1].htm	100%	Joe Sandbox ML		
C:\Users\user\gihi2.dll	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.regsvr32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
4.2.regsvr32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
3.2.explorer.exe.510000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
7.2.explorer.exe.110000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

Source	Detection	Scanner	Label	Link
carpascapital.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://gruasphenbogota.com/C74hwGGxi/ka.html	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://carpascapital.com/gBPg8MtsGbv/ka.html%	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
carpascapital.com	50.116.92.246	true	false	• 2%, Virustotal, Browse	unknown
gruasphenbogota.com	50.116.92.246	true	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.116.92.246	carpascapital.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	440105
Start date:	24.06.2021
Start time:	20:42:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	plan-1053707320.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSB@20/18@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 94% (good quality ratio 89.2%) • Quality average: 82.1% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 81% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:43:19	Task Scheduler	Run new task: nowkkbo path: regsvr32.exe s>-s "C:\Users\user\gihi1.dll"

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
50.116.92.246	plan-930205822.xlsb	Get hash	malicious	Browse	
	plan-277786552.xlsb	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
carpascapital.com	plan-930205822.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246
gruasphenbogota.com	plan-930205822.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	factura y factura de la v#U00eda a#U00e9rea.exe	Get hash	malicious	Browse	• 74.220.199.6
	T5gtQGRL8u.exe	Get hash	malicious	Browse	• 162.241.135.156
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	PO 74230360.xlsb	Get hash	malicious	Browse	• 162.241.114.107
	plan-930205822.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	7UXBXIr31E.exe	Get hash	malicious	Browse	• 192.185.198.10
	TW8o2zNu2Q.exe	Get hash	malicious	Browse	• 50.116.109.135
	xwKdahKPn8.exe	Get hash	malicious	Browse	• 108.167.164.216
	plan-277786552.xlsb	Get hash	malicious	Browse	• 50.116.92.246

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order.exe	Get hash	malicious	Browse	• 108.167.183.94
	0rder-bcm_23062021.exe	Get hash	malicious	Browse	• 50.87.249.240
	wdxYcFUCJV.exe	Get hash	malicious	Browse	• 74.220.199.6
	Inv 820984.xlsb	Get hash	malicious	Browse	• 162.144.12.168
	N0vpYgIYpv.exe	Get hash	malicious	Browse	• 162.241.216.218
	droxoUY6SU.exe	Get hash	malicious	Browse	• 192.185.185.25
	idea-22543577.xlsm	Get hash	malicious	Browse	• 108.167.165.249
	idea-22543577.xlsm	Get hash	malicious	Browse	• 108.167.165.249
	Fra8994.exe	Get hash	malicious	Browse	• 162.241.60.126
	WXs8v9QuE7.exe	Get hash	malicious	Browse	• 50.87.146.99

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Oqq8nQNRt0.exe	Get hash	malicious	Browse	• 50.116.92.246
	DocuSign-June-SOA-Dues.261.htm	Get hash	malicious	Browse	• 50.116.92.246
	Invoice 715320 paul@forthebiome.com.html	Get hash	malicious	Browse	• 50.116.92.246
	Quote Requirment R2106131401 .docx	Get hash	malicious	Browse	• 50.116.92.246
	h2GeNTLcFz.xls	Get hash	malicious	Browse	• 50.116.92.246
	iLNAALfs8Y.exe	Get hash	malicious	Browse	• 50.116.92.246
	OsAwg7NTuy.exe	Get hash	malicious	Browse	• 50.116.92.246
	Terms and Conditions pdf.exe	Get hash	malicious	Browse	• 50.116.92.246
	887cPpO46m.exe	Get hash	malicious	Browse	• 50.116.92.246
	Lista degli ordini.exe	Get hash	malicious	Browse	• 50.116.92.246
	GDiwiEVONn.exe	Get hash	malicious	Browse	• 50.116.92.246
	L6AaziH5ts.exe	Get hash	malicious	Browse	• 50.116.92.246
	L6AaziH5ts.exe	Get hash	malicious	Browse	• 50.116.92.246
	A7DmPhc0bs.exe	Get hash	malicious	Browse	• 50.116.92.246
	Invoice_634000.html	Get hash	malicious	Browse	• 50.116.92.246
	Redoslijed na popisu.exe	Get hash	malicious	Browse	• 50.116.92.246
	LtmQGHQsK1.exe	Get hash	malicious	Browse	• 50.116.92.246
	plan-930205822.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	mCzW1o1ZtQ.exe	Get hash	malicious	Browse	• 50.116.92.246
	Receipt_ID544663355899706.js	Get hash	malicious	Browse	• 50.116.92.246

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_d6c4e44bbad4515086a963364165f93d4a33398_7a325c51_04e1cb83\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11460
Entropy (8bit):	3.7742996415536387
Encrypted:	false
SSDEEP:	192:Qzc5mb6VmcH/RS5uGXx3Rjethm/u7sWS274ltUT:ic5Y6VF/RS5n3jeTm/u7sWX4ltUT
MD5:	AA7BCDD80E17C39E90B47691D964DD37
SHA1:	A77C28D8DB3E84F84615879D2127D67AB2F7CEE7
SHA-256:	6B9D3C0D03C2DA12DBDFE7172F814EA9888D1E0A8B942D6C8CA70D192DFFAD28
SHA-512:	FB95085CDAFF4A544D9EBB54D54C5DD053A80A85A2CD008FB05A5B4BC51794C33E0E7423F279057680F0E9B1AC206BB43992E5094C80C3A81C11057DD0C82DF
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_d6c4e44bbad4515086a963364165f93d4a33398_7a325c51_04e1cb83\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.9.0.6.6.2.0.2.4.4.1.7.8.2.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.9.f.a.8.c.5.d.-.7.2.4.2.-.4.a.e.c.-.a.c.a.6.-.a.e.a.0.a.f.b.0.6.4.4.a.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.7.7.f.7.4.3.f.-.7.1.9.1.-.4.2.7.8.-.9.5.c.6.-.e.5.b.8.7.c.2.d.a.6.d.d.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.e.g.s.v.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.4.c.0.-.0.0.0.0.-.0.0.1.7.-.f.6.1.1.-.3.5.3.d.7.4.6.9.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.d.e.8.8.7.2.!.r.e.g.s.v.r.3.2...e.x.e... ..T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.7.1././.0.4././.0.9.:.1.7.:.2.8.:.2.3.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_d6c4e44bbad4515086a963364165f93d4a33398_7a325c51_101b5502\Report.wer	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	11464
Entropy (8bit):	3.776491557452008
Encrypted:	false
SSDEEP:	192:Lzczb6VYcH/RS5uGXx3Rjethm/u7sxS274ltUA:3c36Vr/RS5n3jeTm/u7sxX4ltUA
MD5:	75B19CEE84F460568309954924B598F2
SHA1:	28C0B1801BBA644220A0BD5628E28C36F1811F36
SHA-256:	4E8549E8D7DC94FADB142E003CCC4B7019815B731BF7A1C6D27A1D25AE61462B
SHA-512:	9F56DC49152B87C6A168AB92FF52D0F51198888895EBC5BAAC6ED266B248630DC6856BEAE0179C8F08A75EC505D2DCF7D00B1287CD3AE910D5A623968DF582A1
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.6.9.0.6.6.3.0.3.1.6.0.3.8.1.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.b.b.b.7.0.e.7.d.-.4.f.e.f.-.4.8.a.f.-.9.4.c.c.-.8.1.0.9.a.b.4.6.3.2.8.3.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.1.d.e.f.5.3.f.-.7.8.8.b.-.4.e.6.a.-.9.5.9.c.-.c.9.4.b.1.1.b.4.7.b.1.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.e.g.s.v.r.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.E.G.S.V.R.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.8.4.c.-.0.0.0.0.-.0.0.1.7.-.f.9.5.b.-.7.2.7.9.7.4.6.9.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.8.8.6.3.0.f.6.0.e.7.3.4.5.4.6.7.0.a.7.d.9.b.6.4.c.9.8.b.4.7.9.8.d.1.d.e.8.8.7.2.!.r.e.g.s.v.r.3.2...e.x.e... ..T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.7.1././.0.4././.0.9.:.1.7.:.2.8.:.2.3.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER510A.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 25 03:45:03 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	35440
Entropy (8bit):	2.5322414467980856
Encrypted:	false
SSDEEP:	192:74XLhRzEEfy+n97S5HwWm78tYgkWr/euP/5RksnRQ:YLXz5fyk9m5alsWr/D/csW
MD5:	FBB9D06C04F9437C97385B87A8790109
SHA1:	7FFCD3C5427C2659DD8508FB175D5FFB52A5735D
SHA-256:	A5E9100C64ED49C6C5C072CA47429BE447236D81D3BC280C0447492072D111AE
SHA-512:	E43273FD82026AEF4052D9A6E079F23B43F57ABE6E1B97A37314DD5CDB1EF6D914E235B3CB1F27E8A93C56FC574C225424F5ADC98A3D23D58654CD168B6F416B
Malicious:	false
Preview:	MDMP..... .....?Q.`.....U.....B.....GenuineIntelW.....T.....L...<Q.`.....@..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1..... .....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER53CA.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8244
Entropy (8bit):	3.690005550288593
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyL656YUmSUugmfJ7SWCpBB89bcfsfq0m:RrlsNie656Y9SUugmfJ7SicEf4
MD5:	C81BDD3AC9D6649F41489D5B59EE1064
SHA1:	DBEA4B2C1DADDA5714EF0EB9639AAF627DB8E7E7
SHA-256:	351F0D2433552DA6AB032FEFDEADBDC9DFC138B8BCC42321AE1161FDE9DE68F6
SHA-512:	68539CFFAE8D64294829C6CF901E29BCD05FFB89DEF8FF6C5EB3F57854C10B948A5D0AEB1FEF85B310C22354429218345BEB53EFE1DEF55132F94DD9664A235D
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WER53CA.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.2.1.2.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C5.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4620
Entropy (8bit):	4.447074870016663
Encrypted:	false
SSDEEP:	48:cvIwSD8zs+JgtWI9lJWSC8Bbs8fm8M4JkH+FvDf+q8VYOIKJYEgd:uITf0C4SNVRJCIkUqYEgd
MD5:	8C5C7C9A48A6306DB76F2811284C6A6F
SHA1:	A9B208978F24D88A37A6CA38E462A01476EAEA9C
SHA-256:	9E3F70B1ABD4E8E712D3A73FDB13DB5F1B039525318DB23CF33133B3F70F78A5
SHA-512:	204C1BA7E40779E6D9A99AA543617FCF557FAD0EBB2FD6DF482437ED7CD297B331D48B5381C78AB302688441BE74CDC9EF9281694AA2CE9FF21C312584B430E1
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1049095" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC79B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Jun 25 03:43:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	34300
Entropy (8bit):	2.5867517653335224
Encrypted:	false
SSDEEP:	192:JOrEIa4PpNu5yWm78tYgkWrpsEmA1rKwgnbn:krEFUDVIsWrOEp1rCb
MD5:	710191DE9840A924F68D90A07E17F862
SHA1:	A37F681AF73D1DEF8D146844AD803F4C8D43A563
SHA-256:	3B5120A64F1BA81CD0B6BC2AF783A2E519A223E5AA3708AD9392F7CFEE8E5033
SHA-512:	6CB613678132619CDE432C232C9659A52B716A990FFB044A2E24976845DCF8D86629F333AEA9664E7DFCC4F995E3C55F89F76FE66FC158E162FDBBD3F1D5BD9
Malicious:	false
Preview:	MDMP..... .....P.`.....U.....B.....GenuineIntelW.....T.....P.`.....@..1.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....d.b.g.c.o.r.e...i.3.8.6.,.1.0...0...1.7.1.3.4...1.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERC9CF.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8246
Entropy (8bit):	3.6888562416777
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiSo6cQe6YrnSUNgmfJ7SWCpBB89bX0sffdm:RrlsNi96K6YLSUNgmfJ7SiXnfI
MD5:	4E0577A72B2D9112E7A41EB0F7479793
SHA1:	8DD960FAC91D0C5F8B3E44E70BA0513F8962EFE2
SHA-256:	431F19E79F9E1F75C488919AF7B4FEE091B1810145BE4884C0E6A7DB4C49B46D
SHA-512:	8ACDA86A75DF6007A43EDF37D64ED95C40E0C91282172A144170170D04D509D13A3F6B799DF7C1EC432C81FEF3EBA5F6656DA7DD7942C454033A6DB2A19B18
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.3.1.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERCA8B.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4620
Entropy (8bit):	4.446745396800481
Encrypted:	false
SSDEEP:	48:cvIwSD8zsVJgtWI9lJWSC8B68fm8M4JkH+Fk+q8VY5ZwKJYjgd:uITfvC4SN9JCjkRqYjgd
MD5:	124D90655DB36885C564B4316031D7F9
SHA1:	18A7DC6B62C13F4FFFA59A16AAFA771330C3C0C6
SHA-256:	A507E8C6BA3D29A254E5ACF8EE223825C4573D8DCB6FCD321E21A0479732746D
SHA-512:	19A11E1CA4404C967191E92E9C0FD395D08AF7BA3CEBA4D15EB42602F2683D3402F535AF132C2BC64D310727538E88F7A6390B3DE366C3F95568968437C1BB5D
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1049094" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\83AEEBD5-3CD1-4EBB-B8A2-37AF63012E6F	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134914
Entropy (8bit):	5.367842811187943
Encrypted:	false
SSDEEP:	1536:vcQIKNgeBXA3gBwlpQ9DQW+z7Y34ZliKWXboOidX5E6LWME9:vEQ9DQW+zvXO1
MD5:	57F1CF624BDBC422FA17A144E981B0E3
SHA1:	16C43CD4017BB9482CDD3E5BE7E101A9232D288D
SHA-256:	AB4509C0B65290403A2E0A039E192AF873ED97DC017BF5FF04CE9C47B53BE300
SHA-512:	0ACFA0EE60D24085FE70E05FEEA3DDF95EA1B39F8A2C2A4FDC41FE8D81721A28606D0ADF711A315367F99E4BF48ED255A91F60822F5A73A33F8181129534FD3
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-24T18:43:04">.. Build: 16.0.14222.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\9A86AAF3.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1133 x 589, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	75711
Entropy (8bit):	7.915372969602997
Encrypted:	false
SSDEEP:	1536:gxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncT:7br0o45GUgHhX8jC9yST
MD5:	8296338A43942E3107802E3062AC1270
SHA1:	46E67A586ED8A961AF7FD03140547C1CB2BAC227
SHA-256:	BE5F61F2AE8E4C9F9ADBCE5EC33D4C01A331734FFC5818AA8E45CF60456C5ABD
SHA-512:	C2179050A009C990CBFE6EA45E44AA6307AAC938E3EA523D31713F657E09131B07ACEBB31FC353C5A23E7D6323C4EC01736CFF092ACA1D49B58E71A07F1171AD
Malicious:	false
Preview:	.PNG.....IHDR...m...M.....p.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.....g.....q.|.....<...'r....-^..c.lf..ffX1K.[....Z....V.LO5L..J+...z.]]u..>.==.....Q.....(.....p.t.....8.:.....g@G.....3.....Q.....(.....p.t.....8.:.....g@G.....3.....Q.....(.....p.t.....j.7ZP...:...0S...z5T.....).WU =j.*.$H.B.P.)l.6Q..'.l..7..k..J.o..._....6..{C...r.\|2W.[a...m.BI.?...5.....D....4;B...@b.HiP.jfj}@.S9..E.*J...O..BA5.e:...q!.SP....w....(..._,..l.\|a.7+>.....A#.....3v..37.....w(..j.. .C.R..H3.f.Q....0....h~...)aM..).vQ.1..+J@Q.....Oa+...!5.e.b...V..\|..d../.....vC..&..=9...n.....^6-.tRj...O..{j.e.N....o..~..^.....#!...T...C.#.>.E,[,.....E....h~B.Y./....(2.....(...`....~w#.% ..R..{.....N.Z....k]8>..dW..^s....U...9...W.e...]...W...i.{u.>.s.,L.>1..)....f..b..Z.nai$.Q.."...W2.....Q...G...z....Ea.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ka[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	297733
Entropy (8bit):	6.57868186999486
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ka[1].htm	
SSDEEP:	6144:EYtPEybzPqbV7WQY6n519eBvQfMN46aCsowDvVJa:TtPZ7qbV7XY6nl8IfMNcCHkv/
MD5:	128E7CC006666F6C6BDDBB3543B34124
SHA1:	F00A2063A88CFC56A990E7C761C3693ADD3B4000
SHA-256:	4B5CE6C6A2602321E4334248DFC69E5A49D909B61D719B099CF27B894A61E09D
SHA-512:	A044B7F2C0673CB87FBC7015F9610E9E195C8732A63B9456861173CBF7460DB32CAC5F18135CC6FFCDBC1293C187EE677FB6B0DCC5551DE551C1D695B74000
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
IE Cache URL:	http://https://gruasphenbogota.com/C74hwGGxi/ka.html
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]e.....$.....Rich.....PE..L...I..`.....!.....&.....1a.. ..... .....`..... ..Q...4R..d.....R..4.....code..... ..`.edata ..Q.... .....@..@.rdataf..#...0...$.....@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\ka[1].htm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	297724
Entropy (8bit):	6.578812169784556
Encrypted:	false
SSDEEP:	6144:EYtPEybzPqbV7WQY6n519eBvQfMN46aCsowDvVJa:TtPZ7qbV7XY6nl8IfMNcCHkv/
MD5:	EBA56F3596493DEF206D4002CE4B6D4B
SHA1:	218CB664CC0CE70C90D4F6299BBA02C4099A88EC
SHA-256:	B4E7C6D0AEAD218FECF64229ED0355D03B92D056AC303D8EA56E73601D0CEDD0
SHA-512:	4955BACB5EA18EF7F9232155398C9BD8B5D47429CAD7921D3C0AE7EB067C020D2C2EBA6C9E7E568FF7CCC72F9A0E21A6715F6085BC8825EFB0DA16BE1495D 67
Malicious:	**true**
IE Cache URL:	http://https://carpascapital.com/gBPg8MtsGbv/ka.html
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]e.....$.....Rich.....PE..L...I..`.....!.....&.....1a.. ..... .....`..... ..Q...4R..d.....R..4.....code..... ..`.edata ..Q.... .....@..@.rdataf..#...0...$.....@..... ....

C:\Users\user\AppData\Local\Temp\8A810000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	113222
Entropy (8bit):	7.87582096597083
Encrypted:	false
SSDEEP:	1536:PKYUOtOpEknvGrnxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncVC:PKY45br0o45GUgHhX8jC9ySVC
MD5:	D6512EF97214AE0394239764EFA59EB1
SHA1:	8B61DBFB041780FB61237ACDCF5D618782524AD2
SHA-256:	25F08DFC74107D0B84531F66A7A05C036419CB5CD7CF1BD799D51B652C61237D
SHA-512:	0DE9F1870E54D97E749D27FF0386DF2D402EF591BC165C3A879362DC16FC07CF2600F7D9CC537698E10E13E0341233F83BDB717B953D567916AC6B39E2A62CF
Malicious:	false
Preview:	...N.1....x...h.EUU..h. .>..>.X.M>....3....U...../....#&2.....U/~..h...2x.6x...I\-.>....a..^.9.R....u!..eH.2.....By9.}.*..>..x...;.....z..;..W....W.za\.vyP.....h...s..^..jG...u..&.9..#...fz.0. nx1....B.?.1..X....>.uw.P:jq..v4 ..J...E....$U%...xG...k.ri....oSG1!.j.lWfR.'8*..b|.....L.e>z(....W..@.[.....3.J. .....?N_...X.....".%...W....I.)..W....'r....X.8..@..W.....PK..... ....!.j.9.....[Content_Types].xml ...(..... ....MO.0...H.....

C:\Users\user\Desktop\~$plan-1053707320.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF

C:\Users\user\Desktop\~$plan-1053707320.xlsb	
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C 7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\gihi1.dll	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	297724
Entropy (8bit):	0.011753714816979547
Encrypted:	false
SSDEEP:	3:WlWUqt/vllXl+YZcFTS9gXeF+X32ZpbYtfhZ8hZy+FAv73A/Ol9qnErqDlblthtg:idq2Vg3F+X322ChMQAjQObV66DTyi8G
MD5:	6C285CDB4B48856C1EE7BD15394E3C59
SHA1:	E22FF7D6F0AE9C33C846C04CEC92FF37867EF11F
SHA-256:	3BA903A7B2B5856A2E44C682E19DA2834D4412BAF27F7218F59760F687F3A719
SHA-512:	89679705CB501F64FFDE39FBD26C9D9465FA5928B60EF0CA1C9E95D756A035C07BD0A7252758F52EEC6AAEE594252E8EFE82C34F22913AF77A9A2E6CAD91D9 A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]e.....$.....Rich.....PE..L...I..`.....!.....&.....1a.. ..... .....`..... ..Q...4R..d.....R..4.....code..... ..`.edata ..Q.... .....@..@.rdataf..#...0...$.....@..... ....

C:\Users\user\gihi2.dll	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	297733
Entropy (8bit):	0.011753388532788709
Encrypted:	false
SSDEEP:	3:WlWUqt/vllXl+YZcFTS9gXeF+X32ZpbYtfhZ8hZy+FAv73A/Ol9qnErqDlblthtg:idq2Vg3F+X322ChMQAjQObV66DTyi8G
MD5:	FFFF91220A3A21506959B3758C9CB9CF
SHA1:	FCB3EBCB0355FFEFEA97D172FED7A120D346C9A7
SHA-256:	B1DFC17F6A96F209EDE077D3CD07B1B83DDE10AF92EA40F58AA4F932B32D8614
SHA-512:	78814EB6177DE6EC4587BF1479EE17B4E60917F6D11BE3421920EC863D6EC94D1085970D490DF8AA7E227F69078DBFC076CC320733C14381A4E488E3240B7F38
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....]e.....$.....Rich.....PE..L...I..`.....!.....&.....1a.. ..... .....`..... ..Q...4R..d.....R..4.....code..... ..`.edata ..Q.... .....@..@.rdataf..#...0...$.....@..... ....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.836349486539577
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	plan-1053707320.xlsb
File size:	90078
MD5:	4854b4dcfa441032f2f54bf2834e894f
SHA1:	fa24422834d0f6ce6d3e35a8b0f15a906cdf9823
SHA256:	68741c1f5df351dc186805c2c30a79653fd52ce21e2fb2a a34ff0687120343cf

General

SHA512:	a51e5f92409f4f5dc564c26b2b95659865ae56cf643ea5bb846cbac56a760374aa16cdb7972819e2a3c816632c2e1834ea65be2848f0a8140ac67eb119125a87
SSDEEP:	1536:OlHoxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncjv0/Ci:WDbr0o45GUgHhX8jC9ySa
File Content Preview:	PK.....!..#.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "plan-1053707320.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 24, 2021 20:43:07.441231012 CEST	192.168.2.3	8.8.8.8	0x715f	Standard query (0)	carpascapital.com	A (IP address)	IN (0x0001)
Jun 24, 2021 20:43:09.029701948 CEST	192.168.2.3	8.8.8.8	0x524d	Standard query (0)	gruasphenbogota.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 24, 2021 20:43:07.620865107 CEST	8.8.8.8	192.168.2.3	0x715f	No error (0)	carpascapital.com		50.116.92.246	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 24, 2021 20:43:09.209028959 CEST	8.8.8.8	192.168.2.3	0x524d	No error (0)	gruasphenbogota.com		50.116.92.246	A (IP address)	IN (0x0001)
Jun 24, 2021 20:45:06.071314096 CEST	8.8.8.8	192.168.2.3	0xbfe2	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

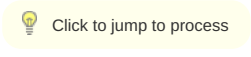
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 24, 2021 20:43:07.948056936 CEST	50.116.92.246	443	192.168.2.3	49724	CN=*.carpascapital.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri May 21 05:30:14 CEST 2021	Thu Aug 19 05:30:14 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		
Jun 24, 2021 20:43:09.527966976 CEST	50.116.92.246	443	192.168.2.3	49727	CN=gruasphenbogota.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research Group, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon May 10 05:47:53 CEST 2021	Sun Aug 08 05:47:53 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=ISRG Root X1, O=Internet Security Research Group, C=US	Fri Sep 04 02:00:00 CEST 2020	Mon Sep 15 18:00:00 CEST 2025		
					CN=ISRG Root X1, O=Internet Security Research Group, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Jan 20 20:14:03 CET 2021	Mon Sep 30 20:14:03 CEST 2024		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 3152 Parent PID: 792

General

Start time:	20:43:02
Start date:	24/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x1350000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 6088 Parent PID: 3152

General

Start time:	20:43:09
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi1.dll
Imagebase:	0xf40000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000002.00000002.237315592.0000000000E00000.00000004.00000001.sdmp, Author: Joe Security • Rule: QakBot, Description: QakBot Payload, Source: 00000002.00000002.237315592.0000000000E00000.00000004.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 4784 Parent PID: 6088

General

Start time:	20:43:13
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x12f0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: QakBot, Description: QakBot Payload, Source: 00000003.00000002.508377992.0000000000510000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: regsvr32.exe PID: 3488 Parent PID: 3152

General

Start time:	20:43:15
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi2.dll
Imagebase:	0xf40000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000004.00000002.246220132.0000000004BA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: QakBot, Description: QakBot Payload, Source: 00000004.00000002.246220132.0000000004BA0000.00000004.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: schtasks.exe PID: 5848 Parent PID: 4784

General

Start time:	20:43:16
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn nowkkbo /tr 'regsvr32.exe -s \'C:\Users\user\gihi1.dll\'' /SC ONCE /Z /ST 20:45 /ET 20:57
Imagebase:	0xe90000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 1276 Parent PID: 5848

General

Start time:	20:43:17
Start date:	24/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 5440 Parent PID: 3488

General

Start time:	20:43:18
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x12f0000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: QakBot, Description: QakBot Payload, Source: 00000007.00000002.247270585.0000000000110000.00000040.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: regsvr32.exe PID: 4088 Parent PID: 528

General

Start time:	20:43:19
Start date:	24/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\gihi1.dll'
Imagebase:	0x7ff71fcf0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 5312 Parent PID: 4088

General

Start time:	20:43:19
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\gihi1.dll'
Imagebase:	0xf40000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 1200 Parent PID: 5312

General

Start time:	20:43:21
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5312 -s 652
Imagebase:	0x320000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 380 Parent PID: 528

General

Start time:	20:45:00
Start date:	24/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\gihi1.dll'
Imagebase:	0x7ff6b8c40000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 2124 Parent PID: 380

General

Start time:	20:45:00
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\gihi1.dll'
Imagebase:	0x1370000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: 4168 Parent PID: 2124

General

Start time:	20:45:02
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 2124 -s 652
Imagebase:	0x10b0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Disassembly

Code Analysis