ID: 440113
Sample Name: plan-1053707320.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:50:58
Date: 24/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

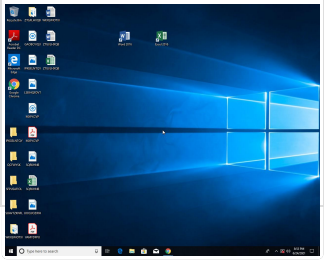
Windows Analysis Report plan-1053707320.xlsb

Overview

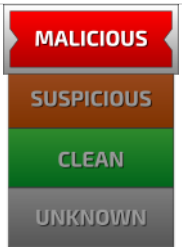
General Information

Sample Name:	plan-1053707320.xlsb
Analysis ID:	440113
MD5:	4854b4dcfa44103.
SHA1:	fa24422834d0f6c..
SHA256:	68741c1f5df351d..
Infos:	

Most interesting Screenshot:



Detection



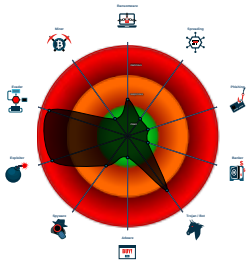
Hidden Macro 4.0 Qbot

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…

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6964 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 3492 cmdline: regsvr32 ..\gihi1.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - explorer.exe (PID: 5800 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
      - schtasks.exe (PID: 6572 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn wtdsqwcv /tr 'regsvr32.exe -s \'C:\Users\user\gihi1.dll\'' /SC ONCE /Z /ST 20:54 /ET 21:06 MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6696 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - regsvr32.exe (PID: 4864 cmdline: regsvr32 ..\gihi2.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - explorer.exe (PID: 7024 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- regsvr32.exe (PID: 6868 cmdline: regsvr32.exe -s 'C:\Users\user\gihi1.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 7092 cmdline: -s 'C:\Users\user\gihi1.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 5044 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7092 -s 652 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- regsvr32.exe (PID: 5824 cmdline: regsvr32.exe -s 'C:\Users\user\gihi1.dll' MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 6700 cmdline: -s 'C:\Users\user\gihi1.dll' MD5: 426E7499F6A7346F0410DEAD0805586B)
    - WerFault.exe (PID: 6372 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6700 -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
00000004.00000002.973589332.0000000001100000.00000040.00000001.sdmp	QakBot	QakBot Payload	kevoreilly	• 0x13223:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...
00000006.00000002.711643542.0000000000F30000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000006.00000002.711643542.0000000000F30000.00000004.00000001.sdmp	QakBot	QakBot Payload	kevoreilly	• 0x12623:$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 08 49 81 ...
00000003.00000002.700614054.0000000001120000.00000004.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000003.00000002.700614054.0000000001120000.00000004.00000001.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 08 49 81 ...
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.explorer.exe.660000.0.raw.unpack	QakBot	QakBot Payload	kevoreilly	• 0x13223:$crypto: 8B 5D 08 0F B6 C2 8A 16 0F B6 1C 18 88 55 13 0F B6 D2 03 CB 03 CA 81 E1 FF 00 00 80 79 08 49 81 ...
3.2.regsvr32.exe.10000000.3.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
3.2.regsvr32.exe.10000000.3.unpack	QakBot	QakBot Payload	kevoreilly	• 0x12623:$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 08 49 81 ...
6.2.regsvr32.exe.10000000.3.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
6.2.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 08 49 81 ...
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

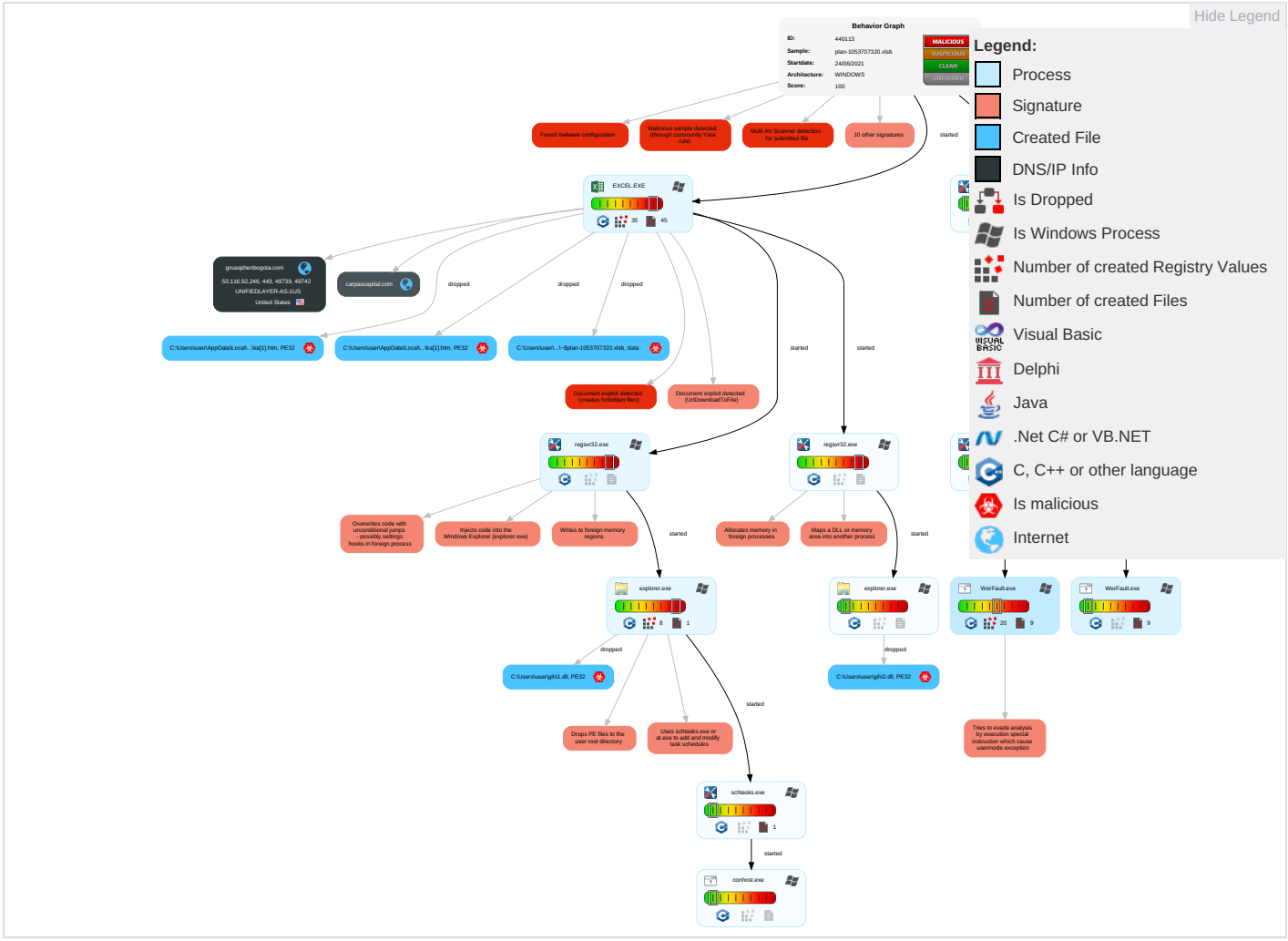
Remote Access Functionality:

- 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 1	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 1	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 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

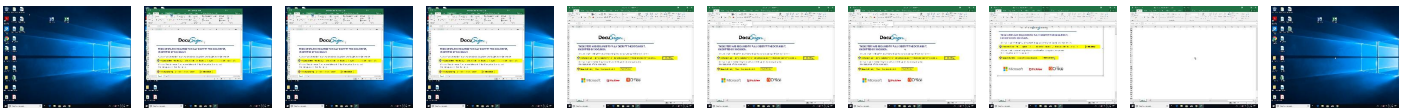
Behavior Graph



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
plan-1053707320.xlsb	28%	ReversingLabs	Document-Excel.Downloader.EncDoc	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\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\2WF3MMUU\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
6.2.regsvr32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
4.2.explorer.exe.1100000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
3.2.regsvr32.exe.10000000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
13.2.explorer.exe.660000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File

Domains

Source	Detection	Scanner	Label	Link
carpascapital.com	2%	Virustotal		Browse
gruasphenbogota.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://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://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://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://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://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
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	

Source	Detection	Scanner	Label	Link
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	
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	• 2%, Virustotal, Browse	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:	440113
Start date:	24.06.2021
Start time:	20:50:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 59s
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:	33

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@20/19@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 60.8% (good quality ratio 57.1%) • Quality average: 79% • Quality standard deviation: 28.6%
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
20:52:13	Task Scheduler	Run new task: wtdsqwcv 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-1053707320.xlsb	Get hash	malicious	Browse	
	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-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	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	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	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

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	plan-1053707320.xlsb	Get hash	malicious	Browse	• 50.116.92.246
	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

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_d6c4e44bbad4515086a963364165f93d4a33398_7a325c51_13ef4904\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):	3.7741173117335585
Encrypted:	false
SSDEEP:	192:zzclb6VwcH/RS5uGXx3RjetA/u7saS274ItUt:Pch6VT/RS5n3jeC/u7saX4ItUt

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_regsvr32.exe_d6c4e44bbad4515086a963364165f93d4a33398_7a325c51_13ef4904\Report.wer	
MD5:	15F762162A144362E720C1547D2B9C20
SHA1:	07C57885EBAD5FBAEE82E3A63852A00823C1B542
SHA-256:	2C61000AF99003333633BAFF4D9233C38AA4A4FD5F759920116E3FFD847B89D8
SHA-512:	CE261BC172FE673A2BBAC8B4101DD643CF51954747DB7C93D780AE333461D4BEAA41B07D9591407A111F77DACE3E4B307CA5C623E64796ED58422FF4C6B171 0
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.=.1.3.2.6.9.0.3.4.3.3.9.2.6.2.4.2.2.4.....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.=.d.f.8.3.d.b.4.2.-.1.a.3.7.-.4.4.1.4.-.a.2.5.1.-.3.6.0.3.5.8.a.2.0.6.a.7.....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.=.d.d.c.1.3.a.9.6.-.8.4.0.8.-.4.2.b.b.-.9.5.0.9.- .b.c.d.c.7.b.9.d.1.6.9.f.....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.b.b.4.-.0.0.0.0.-.0.0.1.b.-.1.1.f.1.-.b.e.0.b.2.a.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_18b8e3a9\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):	3.773207090548546
Encrypted:	false
SSDEEP:	192:Gzc1Gb6VrcH/RS5uGXx3RjetA/u7szS274ItU3:Acm6VY/RS5n3jeC/u7szX4ItU3
MD5:	B8504E07BB98A9D64FDEFBDF41F194D5
SHA1:	202315861F4D0805683956B4421BEC4844871BA0
SHA-256:	C0CA2062F7E533046149967CF764CBB505F0FB7D8FC8D0A9381B4C6665ABA9EF
SHA-512:	1B06CC46BECB26BF63C31F242165B2A634EC8B393F1D3807868E9BF836D7EF05041DBB3230229D1E6E1E17EDF7D8C04BD0884F9B70654046CE863E737B2A77D
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.=.1.3.2.6.9.0.3.4.4.4.4.6.9.9.6.3.2.6.....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.=.f.5.6.a.1.e.0.b.-.3.0.c.1.-.4.a.2.6.-.9.6.0.2.-.c.c.e.e.6.4.6.7.d.e.0.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.=.5.d.a.7.8.d.b.4.-.1.9.b.0.-.4.4.6.d.-.a.2.c.d.-.4.f. 3.3.7.d.4.9.7.1.8.7.....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.a.2.c.-.0.0.0.0.-.0.0.1.b.-.3.d.f.c.-.6.5.4.b.2.a.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\WER3993.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 24 18:52:20 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	34208
Entropy (8bit):	2.6006270724495497
Encrypted:	false
SSDEEP:	192:cUNV+FKctFAK58zi/LWHQMW+N8MLOglhcH8xNzudDnn5z:KKGFAK/6H7GuhcHGNyFn5z
MD5:	17AD30916C50EA6F0F1F9B852E3C23C9
SHA1:	88637E18C09D821EE93D7EA5FF68CB8626F4CE01
SHA-256:	6B0849C5A3AA9AE4DFC4207CD1D074A38AE95B467098D2AF1EB18598856BC9F8
SHA-512:	07F1B9B19DDE2E6DEA46B4F48684F482DF33CDBCEB1110BDEA3CFA3F3230AD2CD9B1734F180900257262739769B2EE8A23974C244EA7CA15D270D0341E600C 9
Malicious:	false
Preview:	MDMP..... .....d..`.....U.....B.....GenuineIntelW.....T.....]..`.....@..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e..... .....W... .E.u.r.o.p.e. .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\WER400C.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):	8248
Entropy (8bit):	3.69375614707593
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiDP6iQe6YfCSUDgmfJ7Sqx+pBB89begsfaKm:RrlsNir606YaSUDgmfJ7Sqpezfu
MD5:	1830660BB14C11F682D01FDFCB1A65E7
SHA1:	5D37220F3D7049C206092E9D4ECA4BF2CBADCA9C
SHA-256:	E8072C1D35E368BEB6A0290D2C072B13C15022330BA27C12B35B650917224032

C:\ProgramData\Microsoft\Windows\WER\Temp\WER400C.tmp.WERInternalMetadata.xml	
SHA-512:	1C62B2BBB157F583A8BD9CABFA733D4A3F6006F0B073F94BB5775E7BF07E2D8066EC6519488CC987A0A9517A55A2291CB7C5F267AFC683F75A04E1CBE97A85E7
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.>.7.0.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER44C1.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):	4.450374572187856
Encrypted:	false
SSDEEP:	48:cvIwSD8zs1JgtWI9+RaPhWSC8B78fm8M4JkH+FhL+q8VYl+0KJYGgd:uITfPxVSNKJCSkoqYGgd
MD5:	A5B1288A547EEE136D2F09E10142DDA9
SHA1:	8B7CBF924B4F1C65A78FA570E69DEFFF5AD42427
SHA-256:	C62F43EE967BF8D6F07D6EEE57C605D9C32A91EFAD615D68E00AC26224DBD6B3
SHA-512:	0F6589301777CFD64F231AF020A1FA792B128057814C80992F455F54C7844B7438508A70CCB45A512C46D753E2100852B4B4F336C4C357FC5937C40F3F2CDD3B
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="1048563" />.. <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\WERD571.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Jun 24 18:54:06 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	34060
Entropy (8bit):	2.6074160567654263
Encrypted:	false
SSDEEP:	192:PlEZpIjo7oukkDRVlGTtW+N8MLOglhcRuIXZina:twljWllnlGTnGuhcoUga
MD5:	899EA0F9B3658B5A6CBCDE388DDD87EA
SHA1:	E6AE09FDBB78C3574F568F9A66294526E6E07F1D
SHA-256:	85C8876F48013E6696DA42267FA52DB78EB0384C49E73DA89DA49515F50FB894
SHA-512:	2117864D8107504717FC927D62DC45DC6333E43B83C5B4A795C429CF486B7A719681E1716EB038FD8F70A67FF3BFDB2CD4E1056156AADE50E8957167267FB576
Malicious:	false
Preview:	MDMP..... .....`.....U.....B.....GenuineIntelW.....T.....`.....@..1.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERDBDA.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):	8248
Entropy (8bit):	3.6920438867043095
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiGH6v6YUhSUUgmfJ7Sqx+pBB89b1zsfHnm:RrlsNi26v6YaSUUgmfJ7Sqp1YfG
MD5:	24537AA59C8A9FD673996B251C39DF65
SHA1:	58403CB37FB659C2946440CB15D403F106872780
SHA-256:	A84B497332A7DB46AE23866DAC6016EE700E45A3847825CB1A6B2B6B36761922
SHA-512:	A181D4B291EEF4D7B7DD194A359384E2F7A7BD490AD891BE0BBB60D125FE0C365EBF984D3C327A59861B09B6CCC227187DE9B573EF3A9663565F8B4FBB9E51C
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDBDA.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.>.6.7.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERDE3D.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):	4.448979618906682
Encrypted:	false
SSDEEP:	48:cvIwSD8zsQJgtWI9+RaPhWSC8By8fm8M4JkH+Fd+q8VYv0KJYkgd:uITfWxVSNRJCik1qYkgd
MD5:	DF34FAC632E99E2364AA9BF692327B38
SHA1:	012B4B7C31FC1C326FC6E58EFF056F0D608E41EC
SHA-256:	80B809F00095397594C3B5D4068CD96145C915364638AA1EA2A871BE1D06BDEB
SHA-512:	8855D849B6B56E50B6B4DA1FE66C0B980702FBF0D24BB300B7BF93D6EFA22EAA3626FC9F8730E28854493C9917FC2034850741F815AAD57D48B0865551444C98
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="1048564" />.. <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\A1BC798F-5F72-4EA3-BE7B-898818256BFB	
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):	5.367850460063856
Encrypted:	false
SSDEEP:	1536:KcQIKNgeBXA3gBwlpQ9DQW+z7Y34ZliKWXboOidX5E6LWME9:GEQ9DQW+zvXO1
MD5:	03B5A85182D5248D0EB0960BC5338E31
SHA1:	09F017611A33578A990E1F714212B2A4158DE7E8
SHA-256:	6843F38B0F450A390FB39DB999FE2896170EEE8F192D282A49A302A97A17BBE9
SHA-512:	14F73A61113E3833D52310E6FFF76CEDD13B2C5600CB8A7792F72041D84F21E045CF9308F5DE81B11A3D96E498E3214301BD612AFE74E17610D844F367EA6395
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-24T18:51:55">.. 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\7716717F.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.If.,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\2WF3MMUU\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):	302512
Entropy (8bit):	6.5099091174634305
Encrypted:	false
SSDEEP:	6144:EYtPEybzPqbV7WQY6n519eBvQfMN46aCsowDvVJa:TtPZ7qbV7XY6nl8lfMNcCHkv/
MD5:	E1CE7B3C5E793A6C5A2BE7801695DB58
SHA1:	633801464F9C064D6BDE4FA568177872F2354532
SHA-256:	2C93B9A196190AD2E08D31102BEC4FC3AC3B6B732D3B5F6EEF3E1BF5FD017C4B
SHA-512:	5AF5CB784AB47208904D8D00BC5EAE9638779FD48D6EDAC3F74301E729131491AA6F46B5545534389F814FA4E9A8DB2175C5F06948D5E5EA1207249C224C2ABD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\Microsoft\Windows\INetCache\IE\OR0WKIO1\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):	302521
Entropy (8bit):	6.509780411812991
Encrypted:	false
SSDEEP:	6144:EYtPEybzPqbV7WQY6n519eBvQfMN46aCsowDvVJa:TtPZ7qbV7XY6nl8lfMNcCHkv/
MD5:	35D8C462B24EABCEEB247BF5C6FF07C2
SHA1:	AF7E0EDE0EEB55F094D689E3C493FFAFAFD8A49F
SHA-256:	4ACA6B14EA5A7CD1D61F615D6B0665DA8870981C57DDD10203DD1C2E52D5190B
SHA-512:	56E5E27043E850BEF5ED86419131D2D2100F1A98A58CC68E64325391B96C4D1076F32BAB3D0320F83C0ABC38792AAEB0974E8A5F78ED8F9E1087E150F56378C6
Malicious:	**true**
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\Temp\F5C40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	113223
Entropy (8bit):	7.875783115355491
Encrypted:	false
SSDEEP:	1536:PKYUOtOpEknvGrnxJQVyZEbrMj34410mHyL9c988gHhX8jCNnKfl5ncVCd:PKY45br0o45GUgHhX8jC9ySVC
MD5:	E7CDABA9352809BC7F9AECA6A7909863
SHA1:	F2591E410316D5970C33974E1E9B5BEAACEB2955
SHA-256:	212B90AE445DFA7DFE07681DAE33A2BDB4AC75305D6F593C1676731B87F40614
SHA-512:	1C216AD9E63291FB9EBCC2F39161CCF670168E9A34837CC8D74487D65BA24214EFF4DB2C8CAFEACB4B2DD0BF9880712DFB76359AE4E0D08F78442DFE1540B6DD
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....l.)..W....'r....X.8..@..W.....PK..... ....!.j.9.....[Content_Types].xml ...(..... ....MO.0...H.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.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:RFXl6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
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):	302512
Entropy (8bit):	0.011582753180433458
Encrypted:	false
SSDEEP:	3:WlWUqt/vllXl+YZcFTS9gXeF+X32ZpbYtfhZ8hZy+FAv73A/Ol9qnErqDlblthtg:idq2Vg3F+X322ChMQAjQObV66DTyi8G
MD5:	593AD3F06697E915B547987B0E753705
SHA1:	A855AC5D2979AA4782D21B0E8F731AB4ACC56E30
SHA-256:	E2A91304AE5407AE1FC1FD8E4D670543F4191B4A858E4DB13516FFDA1239B421
SHA-512:	39B85662AA13A582987668954A6F8A14755357F00648406282CD8E2DEBB7045E109DBF4E77EB646D7684F4E2657A11F7D9FC64FAA262B4E5E12D331E210BD815
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):	302521
Entropy (8bit):	0.011582436694389499
Encrypted:	false
SSDEEP:	3:WlWUqt/vllXl+YZcFTS9gXeF+X32ZpbYtfhZ8hZy+FAv73A/Ol9qnErqDlblthtg:idq2Vg3F+X322ChMQAjQObV66DTyi8G
MD5:	57692E0E3077E0016A5038DD174CFD4C
SHA1:	B999DB831EB947D8CAABFDBB00F6BA1CFEFE3697
SHA-256:	B737EBBBF7E6380296E2DF93A6545C528B9B63579124D16EBDB630BC9085F391
SHA-512:	ABB81617B8D80BAFFCE47B1033CD625C3252A427BDE374FE6B01B4EE5B0CA8BB996F8B16BB99E800314BDEF575E046C01D033C57A113E4C5AE7F7F8DC34360E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\gihi2.dll	
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
SHA512:	a51e5f92409f4f5dc564c26b2b95659865ae56cf643ea5b b846cbac56a760374aa16cdb7972819e2a3c816632c2e1 834ea65be2848f0a8140ac67eb119125a87
SSDEEP:	1536:OlHoxJQVyZEbrMj34410mHyL9c988gHhX8jCNnK fl5ncjv0/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 20:51:59.018085957 CEST	192.168.2.4	8.8.8.8	0x2b13	Standard query (0)	carpascapital.com	A (IP address)	IN (0x0001)
Jun 24, 2021 20:52:00.620779991 CEST	192.168.2.4	8.8.8.8	0xaad0	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 20:51:59.214350939 CEST	8.8.8.8	192.168.2.4	0x2b13	No error (0)	carpascapital.com		50.116.92.246	A (IP address)	IN (0x0001)
Jun 24, 2021 20:52:00.675678015 CEST	8.8.8.8	192.168.2.4	0xaad0	No error (0)	gruasphenbogota.com		50.116.92.246	A (IP address)	IN (0x0001)
Jun 24, 2021 20:54:10.390286922 CEST	8.8.8.8	192.168.2.4	0xe13a	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

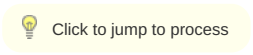
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jun 24, 2021 20:51:59.543297052 CEST	50.116.92.246	443	192.168.2.4	49739	CN=*.carpascapital.com CN=R3, O=Let's Encrypt, C=US CN=ISRG Root X1, O=Internet Security Research 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 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Thu Aug 19 05:30:14 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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 20:52:00.996279955 CEST	50.116.92.246	443	192.168.2.4	49742	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 Fri Sep 04 02:00:00 CEST 2020 Wed Jan 20 20:14:03 CET 2021	Sun Aug 08 05:47:53 CEST 2021 Mon Sep 15 18:00:00 CEST 2025 Mon Sep 30 20:14:03 CEST 2024	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					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: 6964 Parent PID: 800

General

Start time:	20:51:53
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:	0xc70000
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: 3492 Parent PID: 6964

General

Start time:	20:52:01
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi1.dll
Imagebase:	0x13b0000
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: 00000003.00000002.700614054.0000000001120000.00000004.00000001.sdmp, Author: Joe Security • Rule: QakBot, Description: QakBot Payload, Source: 00000003.00000002.700614054.0000000001120000.00000004.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 5800 Parent PID: 3492

General

Start time:	20:52:10
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x12b0000
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: 00000004.00000002.973589332.0000000001100000.00000040.00000001.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: 4864 Parent PID: 6964

General

Start time:	20:52:11
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 ..\gihi2.dll
Imagebase:	0x13b0000
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: 00000006.00000002.711643542.0000000000F30000.00000004.00000001.sdmp, Author: Joe Security • Rule: QakBot, Description: QakBot Payload, Source: 00000006.00000002.711643542.0000000000F30000.00000004.00000001.sdmp, Author: kevoreilly
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: schtasks.exe PID: 6572 Parent PID: 5800

General

Start time:	20:52:12
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 wtdsqwcv /tr 'regsvr32.exe -s \'C:\Users\user\gihi1.dll\'' /SC ONCE /Z /ST 20:54 /ET 21:06
Imagebase:	0x1390000
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: 6696 Parent PID: 6572

General

Start time:	20:52:12
Start date:	24/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: regsvr32.exe PID: 6868 Parent PID: 968

General

Start time:	20:52:13
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:	0x7ff65e5f0000
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: 7092 Parent PID: 6868

General

Start time:	20:52:13
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\gihi1.dll'
Imagebase:	0x13b0000
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: explorer.exe PID: 7024 Parent PID: 4864

General

Start time:	20:52:15
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x12b0000
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: 0000000D.00000002.713096999.0000000000660000.00000040.00000001.sdmp, Author: kevoreilly

Reputation:	high

File Activities — Show Windows behavior

File Written

File Read

Analysis Process: WerFault.exe PID: 5044 Parent PID: 7092

General

Start time:	20:52:16
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7092 -s 652
Imagebase:	0xa60000
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: 5824 Parent PID: 968

General

Start time:	20:54:00
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:	0x7ff65e5f0000
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: 6700 Parent PID: 5824

General

Start time:	20:54:00
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\gihi1.dll'
Imagebase:	0x13b0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WerFault.exe PID: 6372 Parent PID: 6700

General

Start time:	20:54:02
Start date:	24/06/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6700 -s 652
Imagebase:	0xa60000
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