

BfV Cyber-Brief Nr. 04/2016

- Hinweis auf aktuelle Angriffskampagne -



Kontakt:

Bundesamt für Verfassungsschutz

Referat 4D2/4D3

 0221/792-2600

Aktuelle Angriffskampagne gegen Unternehmen der Energiewirtschaft

Unternehmen der Energiewirtschaft laufen derzeit Gefahr, durch eine vermutlich iranische Cyberkampagne attackiert zu werden. Hierzu nutzt die Angreifergruppierung insbesondere gefälschte Seiten von Jobportalen. Die von den Angreifern verwendete Schadsoftware wird von den gängigen Antivirenherstellern bislang noch nicht oder nur unzureichend erkannt.

Mit dieser Angriffskampagne sollen nach Erkenntnissen des Bundesamtes für Verfassungsschutz (BfV) insbesondere europäische Unternehmen der Energiewirtschaft angegriffen werden. Da davon auszugehen ist, dass auch deutsche Unternehmen zum Kreis der potenziellen Ziele der Kampagne gehören, möchte das BfV als nationale Spionageabwehrbehörde auf diesem Wege auf die aktuelle Bedrohung hinweisen.

Sachverhalt

Die mutmaßlich iranische Angreifergruppierung, die seit mindestens 2011 aktiv sein soll und deren Aktivitäten durch IT-Sicherheitsunternehmen unter den Bezeichnungen Newscaster, Ajax Hacking Team und Charming Kitten veröffentlicht wurden, richtet sich nach Hinweisen des BfV derzeit unter anderem gegen Unternehmen der Energiewirtschaft.

Hierzu hat die Gruppierung Domains angelegt, die legitimen Domains von Jobportalen für den Öl- und Gassektor nachempfunden sind. Gleichzeitig wurden Microsoft Word Dokumente, die vermeintliche Jobangebote enthalten, erstellt und mit Schadsoftware versehen. Über Schaltflächen mit Texten wie z.B. „Click to see more details!“ werden weitergehende Informationen zu den jeweiligen Jobangeboten versprochen. Klickt das Opfer nun auf eine dieser Schaltflächen, wird eine Schadsoftware installiert.

Es ist denkbar, dass die Angreifergruppierung per E-Mail, Links unter gefälschten Domains von Jobportalen verschickt, um hiermit die infizierten Word-Dokumente zum Download anzubieten. Auch ein direkter Versand der Dokumente ist nicht ausgeschlossen.

Handlungsempfehlung

Um festzustellen, ob Ihr Unternehmen von dieser Angriffskampagne betroffen ist, empfehlen wir folgende Schritte:

- Suchen Sie in den E-Maileingängen, ob verdächtige E-Mails – insbesondere mit vermeintlichen Stellenangeboten – eingegangen sind.
- Durchsicht der Netzwerk-Logs nach den in der Anlage aufgeführten netzwerkbasierten IoC¹.
- Suche nach den in der Anlage aufgeführten hostbasierten-IoC.

Sollten Sie entsprechende Anhaltspunkte feststellen, besteht die Gefahr der Infizierung Ihrer Rechner. In diesem Fall können wir Ihre Maßnahmen mit zusätzlichen Hintergrundinformationen unterstützen und weitere Hinweise geben. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

1. Indicators of Compromise

Tel.: 0221-792-2600 oder
E-Mail: poststelle@bfv.bund.de
Referat 4D3

Wir sichern Ihnen absolute Vertraulichkeit zu!

Als vorbeugende Maßnahmen zum Schutz vor Infektionen empfehlen wir konkret die folgenden Punkte zu beachten und diese auch an die Beschäftigten Ihres Unternehmens in geeigneter Weise weiterzutragen:

- Klicken Sie keine in E-Mails enthaltenen Links an, wenn Sie nicht sicher sind, wer Urheber der E-Mail ist.
- Überprüfen Sie insbesondere, ob Links wirklich auf die Seite verweisen, die Sie hinter dem Link erwarten, oder ob das tatsächliche Ziel durch irreführende Subdomains wie z.B. [www.microsoftsubsystem.com-adm\[.\]in](http://www.microsoftsubsystem.com-adm[.]in) verschleiert werden.
- Seien Sie misstrauisch, wenn vermeintliche Stellenangebote in anderen Dokumenten „verpackt“ sind.
- Seien Sie grundsätzlich vorsichtig, was das Öffnen von E-Mailanhängen und das Ausführen von Makros in Office-Dokumenten angeht.

Anlage

Netzwerkbasierte IoC

www6.chrome-up[.]date:3014/java.js
www6.chrome-up[.]date:9528/dwn/java.js
www5.chrome-up[.]date:4040/cs
www4.chrome-up[.]date
www3.chrome-up[.]date
www7.chrome-up[.]date
www6.chrome-up[.]date
www5.chrome-up[.]date
www1.chrome-up[.]date
https://www5.chromeup[.]date:4005/download/
chrome-up[.]date
service.chrome-up[.]date:8080/WebService.asmx
www3.chrome-up[.]date:4443/IDCJB
www1.chrome-up[.]date:8080/p
www1.chrome-up[.]date:8080/P
service1.chrome-up[.]date
serviceupdate[.]net
webmaster.serveirc[.]com
service.chrome-up[.]date
service1.chrome-up[.]date/r.exe
microsoftsubsystem.com-adm[.]in
microsoftsubsystem.com-adm[.]in:9528/owa/certificate.exe
microsoftsubsystem.comadm[.]in:9528/download/spool.exe
argaam.com-adm[.]in
mol.com-adm[.]in
mainlink[.]club
maildelivery1[.]com
maildelivery2[.]com
maildelivery3[.]com
maildelivery4[.]com
maildelivery5[.]com

maildelivery6[.]com
maildelivery7[.]com
maildelivery8[.]com
msrv.maildelivery2[.]com
zombiebooks[.]top
mail.knewfte[.]top
ze3aeoi.knewfte[.]top
knewfte[.]top
com-adm[.]in
aleoryu2.flownat[.]top
webconfig.serveirc[.]com
servicesystem.serveirc[.]com
autodiscover.sama.gov.sa.owa.auth-log[.]in
analytics-google[.]org
syn.timezone[.]live
mainlink[.]club
pranktube[.]club
pranktube[.]club/jq.js
pranktube[.]club/Video/88
ns1.mails[.]rocks
ns2.mails[.]rocks
sitemainlink[.]club
mail.ldry7[.]club
webhost.ldry7[.]club
mails[.]rocks
ldry[.]club
Sitemainlink[.]club/d3qg2o/1434/1/22029/1421/38/263
googleanalytics.ddns[.]net
mail.flownat[.]top
easygo[.]link
msservice[.]site
Mails[.]rocks:8080/38/263/286/1/22041/1.jpg
analytics-google[.]org:69/checkFile.aspx
mails.[.]services

globalscript.sytes[.]net
globalscript.sytes[.]net:8089/jquery.js
googlecheck[.]biz
vagupdate[.]net
ns4.adlaim[.]ru
supports.co[.]com
msrv.supports.co[.]com
luberef[.]com/en/cv/cv-luberef.doc
w3school.ddns[.]net
auth-log[.]in
go-microsft[.]com
5.9.53[.]123
5.39.222[.]5
5.254.100[.]200
23.254.211[.]96
45.32.39[.]78
45.32.154[.]163/certi.bat
45.32.155[.]151
45.32.180[.]169
45.58.34[.]196
45.58.34[.]196:8080/b32
45.58.34[.]196:8080/b64
45.58.34[.]196:8080/p
45.58.34[.]196:8080/rpi
45.58.46[.]225
46.17.96[.]202
46.17.97[.]6
66.228.51[.]94
69.28.88[.]126
69.64.147[.]242
69.87.221[.]90
69.87.222[.]166
72.41.40[.]122
96.126.96[.]228

104.218.120[.]165
104.219.55[.]37
104.238.184[.]252
104.245.33[.]172
107.170.21[.]85
107.170.246[.]112
108.61.220[.]25
138.68.58[.]227
139.59.182[.]31
139.162.225[.]240
159.203.42[.]18
162.220.53[.]136
162.220.55[.]159
185.5.172[.]103
185.73.37[.]81
185.73.37[.]81:3104
185.73.37[.]81:3014/java.js?LOOL=...
185.73.38[.]112
192.64.81[.]122
192.64.81[.]209
192.241.237[.]219
212.71.246[.]204
216.15.213[.]184
216.198.213[.]229

Hostbasierte IoC (MD5)

3b3aa592dfdbadfa6272641644eda9ac
230901b4219068cda90b91cf5e460b0f
18fde9b6e5e6cdaf7c15ac43d41cf47c
79258459e6d02a87463284b645aebb84
44ac06837f4ff06f90128554c256c193
8342e909e4f7840a676d03221f489847
f292e2b1371e957bc3700a00e3dcf81a
fc94d56641c3df902a556749b4a7fe74
2a0e9160f6656895ecfa613790bb462d
0e572f9ed0a20f7651c34aae23ae68cc
1a056f16b9d872fa1f5d346e8cc0b619
46984f669522d545f2c0aef85520c4a4
8fcbcd6230dd6d901b32b2dac8ffbd8
a9d85fba12518dadf821e769cf5755b3
636471b334e1e3e0dc142365bcd89605
1f79f7be271630b257a9ac9e7a069778
3911b67621291025eae704a4191ae466
230901b4219068cda90b91cf5e460b0f
bcb445b72228e26378488a110432d775
20aa161972b06e9a28dc95432818aa69
650aaab31b7bc4bf5bb28675141c0eb5
81a19e5eeb67023cd3436e71c41777f4
012f79570f720b997b9ef4ef327dd2da
cced9d843cd9dce4a835777798c58904
fad5197c84ac081e03babb558b2d6235
c153a4ef6622a5c1553690bf3dcf045d
92b41f01ea9ed5268cc6c35774bef399
ab12cfdd53d7ed4e0ea449abb4c668a3
dc938f6d94cec4e229402b47e53f46a7
cb9ecb5a73d009cbc8d65532216989cc
94c053324907ce48303f483abbfb483d
ad1063351ef32575b8260fc110c49caf
ab59ba909a34ec973045dcad6e867276

1305a56769dabd98c32599b189c99670
83cbf0374f33942e87156bf16be9fdaa
17a7504c2bbb7b0666c757a3a73b3628
805e542c70f4dddbc913a284f509f56d
9634d4c7ae1432d20f3867c057b5b8fa
2c60f38f94dedee47aed8dc1f8969a2b
25bf953cd6591d125dceb52162f426ef
d2e5f99a715019056b87193e73a0dcdb
710caf14c1417fe866ce084864c11b04
839567d62f1be253fc5a2daf1ab71bc8
b0833f957f6f1f359ab4ccd04dbb9da9
28468f9fa9a14de8dcb9eb04c6798011
559674ae5e5de9b6c35ebed07e91c944
3c8a142d2e3b84fb0d210250af77cc9b
07d6406036d6e06dc8019e3ade6ee7de
1abdb66c83179d7d6896f8d0defdba65
ed743ae8e5c7e8c6953ff9133a28f88a
b36d17390de4bc1d74ff55f2bd8dc1cb
5e2dc647b403a5b90a0a1fa5ad057202
7243ab4937eb43d8b232e0a4cab6fb7d
17f31cb5106e01c1e03d61265f66d2be
86426a55ca7dec5d78333d2af1f2c6ec