

BfV Cyber-Brief Nr. 02/2017


- Hinweis auf aktuelle Angriffskampagne -



Kontakt:

Bundesamt für Verfassungsschutz

Referat 4D2/4D3

 0221/792-2600

„Operation Cloud Hopper“: Cyber-Angriffskampagne gegen Managed Service Provider

Dem Bundesamt für Verfassungsschutz (BfV) liegen Erkenntnisse über aktuelle Cyberangriffe auf IT-Dienstleister und Wirtschaftsunternehmen vor. Die Angriffe sind den Advanced Persistent Threats (APT) zuzuordnen und stellen eine hohe Bedrohung für betroffene Unternehmen und deren Kunden dar. Das BfV als nationale Spionageabwehrbehörde möchte deutsche Unternehmen auf diesem Wege auf die aktuelle Bedrohungslage aufmerksam machen.

Sachverhalt

Die mutmaßlich chinesische Angreifer-Gruppierung ist unter anderem unter den Namen APT 10, Menupass Team und Stone Panda bekannt. Auch wenn sie seit mindestens 2009 aktiv ist, richteten sich die in der Vergangenheit beobachteten Cyberangriffe vor allem gegen US-amerikanische und japanische Ziele. Seit Ende 2016 scheint sich der Interessenfokus auf Wirtschaftsunternehmen in Europa erweitert zu haben.

APT 10 hat neben dem Hochtechnologie-Bereich Aufklärungsinteresse an folgenden Branchen:

- Energie,
- Transport/Automobil,
- Rohstoffe/Mineralien,
- Chemie,
- Gesundheit,
- Telekommunikation,
- Luft- und Raumfahrt.

Ausgangspunkt der Cyberangriffe sind in der Regel Spear-Phishing Mails, die thematisch auf die jeweiligen Empfänger zugeschnitten sind und maliziöse (Word-) Dokumente enthalten. Als Schadsoftware kommt im Anschluss häufig PlugX (auch unter dem Namen DestroyRAT bekannt) zum Einsatz. Daneben nutzt APT 10 seit Ende 2016 scheinbar exklusiv eine Schadsoftware mit dem Namen ChChes.

Laut einem kürzlich veröffentlichten Bericht von BAE Systems und PwC richten sich die Cyberangriffe der Gruppe derzeit gezielt gegen IT Service Provider – vor allem Cloud Dienstleister – um von dort in die oft besser geschützten Systeme von deren Kunden zu gelangen. Das Vorgehen wird als „Operation Cloud Hopper“ bezeichnet.

Betroffen waren bisher vor allem Organisationen in den USA, Japan, Großbritannien und Indien. Derzeit gibt es Hinweise, dass auch deutsche Unternehmen angegriffen worden sind.

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 eingegangen sind.
- Durchsicht der Netzwerk-Logs nach den in der Anlage aufgeführten netzwerkbasierten 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:

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 folgende Punkte zu beachten und diese auch den Beschäftigten Ihres Unternehmens in geeigneter Weise zur Kenntnis zu geben:

- 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 verschleiert wird.
- Seien Sie grundsätzlich vorsichtig, was das Öffnen von E-Mailanhängen und das Ausführen von Makros in Office-Dokumenten angeht.

Anlage

Netzwerkbasierte Indicators of Compromise (IoC)

www.mobile.2waky.com
mobile.2waky.com
windowsupdate.2waky.com
peopleinfodata.3-a.net
blaaaaaaaaaaaaa.windowsupdate.3-a.net
ipv4.windowsupdate.3-a.net
windowsupdate.3-a.net
contract.4mydomain.com
eu.acmetoy.com
www.twgovernmentinfo.acmetoy.com
www.windowsupdate.acmetoy.com
windowsupdate.acmetoy.com
koala.acsocietyy.com
acsocietyy.com
products.almostmy.com
ap-southeast-1.compute.amazonaws.com
ec2-52-74-203-151.ap-southeast-1.compute.amazonaws.com
www.visualstudio.authorizeddns.net
visualstudio.authorizeddns.net
ctldl.windowsupdate.authorizeddns.org
ctldl.windowsupdate.authorizeddns.us
download.windowsupdate.authorizeddns.org
ipv4.windowsupdate.authorizeddns.org
v4.windowsupdate.authorizeddns.org
www.windowsupdate.authorizeddns.net
www.windowsupdate.authorizeddns.org
windowsupdate.authorizeddns.net
windowsupdate.authorizeddns.org
shrimp.bdoncloud.com
zebra.bdoncloud.com
trout.belowto.com

niggardingproving.havinglives.camdvr.org
havinglives.camdvr.org
hamiltion.catholicmmb.com
dick.ccfchrist.com
edgar.ccfchrist.com
fabian.ccfchrist.com
gavin.ccfchrist.com
chibashiri.com
cloud-kingl.com
www.fukuoka.cloud-maste.com
fukuoka.cloud-maste.com
hukuoka.cloud-maste.com
www.kawasaki.cloud-maste.com
kawasaki.cloud-maste.com
sappore.cloud-maste.com
www.sapporo.cloud-maste.com
sapporo.cloud-maste.com
ukuoka.cloud-maste.com
www.cloud-maste.com
tophost.dynamicdns.co.uk
mircsoft.compress.to
nz.compress.to
kmd.crabdance.com
myblog.csproject.org
cwinatonal.com
www.helpus.ddns.info
helpus.ddns.info
www.machine.ddns.ms
mmy.ddns.us
un.ddns.info
download.windowsupdate.dedgesuite.net
v4.windowsupdate.dedgesuite.net
windowsupdate.dedgesuite.net
windowsupdate.dns05.com

imap.dnset.com
ctldl.windowsupdate.dnset.com
download.windowsupdate.dnset.com
ipv4.windowsupdate.dnset.com
v4.windowsupdate.dnset.com
www.windowsupdate.dnset.com
windowsupdate.dnset.com
un.dnsrd.com
ftp.malware.dsmtip.com
www.micrsoftware.dsmtip.com
micrsoftware.dsmtip.com
www.twsslpopservupro.dynssl.com
messagea.emailfound.info
www.findme.epac.to
findme.epac.to
windowsupdate.esmtip.biz
www.essashi.com
essashi.com
film.everydayfilmlink.com
musicinfo.everydayfilmlink.com
everydayfilmlink.com
cia.ezua.com
msg.ezua.com
windowsupdate.ezua.com
www.imitate.faqserv.com
ipv4.windowsupdate.fartit.com
windowsupdate.fartit.com
fastmail2.com
mx.feerlookik.org
webmail.feerlookik.org
lennon.fftpoor.com
malcolm.fftpoor.com
smo.gadskysun.com
ad.getfond.info

dailyblog.god.jp
microsoft.got-game.org
referred.gr8domain.biz
realnews.home.kg
idpmus.hostport9.net
bak.ignorelist.com
ijica.in
apple.ikwb.com
fuck.ikwb.com
improvejpease.com
cdn.incloud-go.com
www.msn.incloud-go.com
msn.incloud-go.com
www.incloud-go.com
www.yahoo.incloud-go.com
yahoo.incloud-go.com
zebra.incloud-go.com
incloud-obert.com
dailyheadline.info.tm
ctldl.applemusic.itemdb.com
applemusic.itemdb.com
www.microsoftmusic.itemdb.com
microsoftmusic.itemdb.com
ctldl.itunesimages.itsaol.com
images.itunesimages.itsaol.com
ipv4.itunesimages.itsaol.com
v4.itunesimages.itsaol.com
usa.itsaol.com
ctdl.windowsupdate.itsaol.com
download.windowsupdate.itsaol.com
v4.windowsupdate.itsaol.com
www.windowsupdate.itsaol.com
windowsupdate.itsaol.com
ixrayeye.com

jap.japanmusicinfo.com
japanmusicinfo.com
jica-go-jp.bike
jica-go-jp.biz
jimin.jimindaddy.com
jimin-jp.biz
sstday.jkub.com
jpcert.org
sendmsg.jumpingcrab.com
stone.jumpingcrab.com
back.jungleheart.com
www.feed.jungleheart.com
feed.jungleheart.com
availability.justdied.com
newsreport.justdied.com
app.lehigtapp.com
ipv4.windowsupdate.lflink.com
windowsupdate.lflink.com
ctldl.windowsupdate.lflinkup.com
download.windowsupdate.lflinkup.com
ipv4.windowsupdate.lflinkup.com
v4.windowsupdate.lflinkup.com
tfa.longmusic.com
nsa.mefound.com
meiji-ac-jp.com
document.methoder.com
drives.methoder.com
mofa-go-jp.com
christjihad.moood.com
justnews.moood.com
www.microsoftmirror.mrbasic.com
microsoftmirror.mrbasic.com
ipv4.microsoftupdate.mrbasic.com
www.nmr.x.mrbonus.com

nmx.mrbonus.com
fire.mrface.com
maffc.mrface.com
microsoft.mrface.com
windowsupdate.mrface.com
be.mrslove.com
cnnews.mylftv.com
ipv4.windowsupdate.mylftv.com
windowsupdate.mylftv.com
ftp.jimin.mymom.info
jimin.mymom.info
www.twx.mynumber.org
twx.mynumber.org
balk.n7go.com
jcie.mofa.ns01.info
send.mofa.ns01.info
mofa.ns01.info
nsatcdns.com
www.headline.ocry.com
sky.oldbmwy.com
oldbmwy.com
commons.onedumb.com
ea.onmypc.info
www.microsoftstore.onmypc.net
microsoftstore.onmypc.net
sdmsg.onmypc.org
uk.dynamicdns.org.uk
www.latestnews.organiccrap.com
latestnews.organiccrap.com
mediapath.organiccrap.com
osaka-jpgo.com
nttdata.otzo.com
outlook.otzo.com
singed.otzo.com

appledownload.ourhobby.com
www.mseupdate.ourhobby.com
mseupdate.ourhobby.com
art.p6p6.net
cap.p6p6.net
flea.poulsenv.com
lizard.poulsenv.com
scorpion.poulsenv.com
ftp.server1.proxydns.com
www.server1.proxydns.com
server1.proxydns.com
availablegoo.qc.to
ctldl.microsoftupdate.qhigh.com
microsoftupdate.qhigh.com
www.contractus.qpoe.com
contractus.qpoe.com
www2.qpoe.com
jp.rakutenmusic.com
rakutenmusic.com
nunluck.re26.com
salvaiona.com
kikimusic.sellclassics.com
91music.servemp3.com
products.serveuser.com
center.shenajou.com
commissioner.shenajou.com
development.shenajou.com
document.shenajou.com
glicense.shenajou.com
interpreter.shenajou.com
license.shenajou.com
sindeali.com
www.sqrl.to
shoppingcentre.station155.com

station155.com
ibmmsg.strangled.net
bmore.sv9u.com
james.tffghelth.com
kennedy.tffghelth.com
sz.thedomais.info
ftp.cia.toh.info
www.cia.toh.info
cia.toh.info
tokyo-gojp.com
ewe.toshste.com
whale.toshste.com
se.toythieves.com
home.trickip.org
bk56.twilightparadox.com
headlines.twilightparadox.com
images.tyoto-go-jp.com
www.ut-portal-u-tokyo-ac-jp.tyoto-go-jp.com
www.kawasaki.unhamj.com
kawasaki.unhamj.com
www.sakai.unhamj.com
sakai.unhamj.com
www.unhamj.com
urearapetsu.com
usffunicef.com
ms.ecc.u-tokyo-ac-jp.com
style.u-tokyo-ac-jp.com
ftp.iphone.vizvaz.com
www.iphone.vizvaz.com
iphone.vizvaz.com
www.vmmmini.com
vmmmini.com
vscue.com
www.foal.wchildress.com

foal.wchildress.com
www.lion.wchildress.com
lion.wchildress.com
www.wchildress.com
windowsupdate.wcwname.com
wdsupdates.com
sc.weboot.info
fiveavmers.websego.net
music.websego.net
sbuudd.webssl9.info
eu.wha.la
balance1.wikaba.com
fr.wikaba.com
globalnews.wikaba.com
wheelbuy.wschandler.com
area.wthelpdesk.com
zebra.wthelpdesk.com
ctldl.windowsupdate.x24hr.com
download.windowsupdate.x24hr.com
ipv4.windowsupdate.x24hr.com
v4.windowsupdate.x24hr.com
www.windowsupdate.x24hr.com
windowsupdate.x24hr.com
read.xxuz.com
newdata.ygto.com
www2.zyns.com
ftp.2014.zzux.com
www.2014.zzux.com
2014.zzux.com
eu.zzux.com
file.zzux.com
www2.zzux.com

104.224.165.122
107.170.42.7
107.181.160.109
108.61.183.111
109.237.108.150
109.237.108.202
109.237.111.119
109.237.111.175
109.248.222.101
109.248.222.85
110.10.176.181
117.11.148.9
123.1.186.28
138.68.19.47
142.4.121.139
142.4.121.141
142.4.121.204
151.101.100.73
151.236.20.16
151.236.23.159
158.255.208.170
158.255.208.189
158.255.208.61
160.202.163.78
160.202.163.79
160.202.163.81
160.202.163.82
160.202.163.90
160.202.163.91
162.243.6.98
162.248.242.115
169.239.128.143
172.246.160.76
172.246.160.80

172.246.160.81
172.246.160.89
173.224.115.141
175.126.148.108
175.126.148.111
185.117.88.124
185.117.88.77
185.117.88.78
185.117.88.80
185.117.88.81
185.117.88.82
185.133.40.63
185.133.40.63
185.14.185.189
185.141.25.33
185.61.149.140
199.189.86.232
199.189.86.233
199.193.252.219
209.126.112.214
209.126.118.11
209.126.118.128
209.126.118.164
211.110.17.209
23.252.105.137
31.184.197.215
31.184.197.227
31.184.198.23
31.184.198.38
37.235.52.18
45.32.251.112
45.32.35.253
45.76.209.232
45.76.220.73

45.76.99.124
46.108.39.134
52.74.203.151
52.76.51.54
54.169.171.178
54.238.50.84
61.97.241.239
71.19.146.87
78.153.149.130
78.153.151.222
83.217.26.203
86.106.102.117
86.106.102.132
86.106.102.3
89.34.237.11
92.242.144.2
95.183.52.57
95.183.53.49
95.47.156.86