Operation Ghoul: targeted attacks on industrial and engineering organizations

securelist.com/blog/research/75718/operation-ghoul-targeted-attacks-on-industrial-and-engineering-organizations/

Authors

 Mohamad Amin Hasbini

Introduction

Kaspersky Lab has observed new waves of attacks that started on the 8th and the 27thof June 2016. These have been highly active in the Middle East region and unveiled ongoing targeted attacks in multiple regions. The attackers try to lure targets through spear phishing emails that include compressed executables. The malware collects all data such as passwords, keystrokes and screenshots, then sends it to the attackers.

> #OpGhoul targeting industrial, manufacturing and engineering organizations in 30+ countries
>
> Tweet

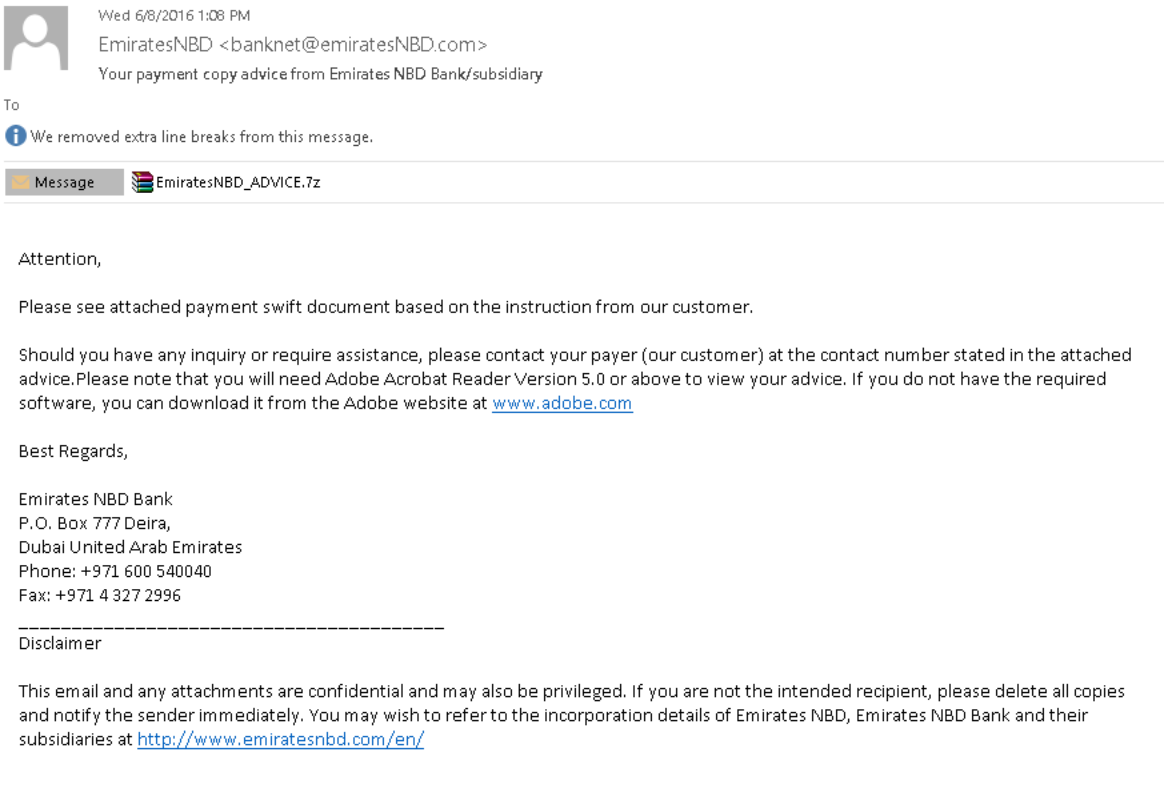
We found that the group behind this campaign targeted mainly industrial, engineering and manufacturing organizations in more than 30 countries. In total, over 130 organizations have been identified as victims of this campaign. Using the Kaspersky Security Network (KSN) and artifacts from malware files and attack sites, we were able to trace the attacks back to March 2015. Noteworthy is that since the beginning of their activities, the attackers' motivations are apparently financial, whether through the victims' banking accounts or through selling their intellectual property to interested parties, most infiltrated victim organizations are considered SMBs (Small to Medium size businesses, 30-300 employees), the utilization of commercial off-the-shelf malware makes the attribution of the attacks more difficult.

> In total, over 130 organizations have been identified as victims of Operation Ghoul #OpGhoul
>
> Tweet

In ancient Folklore, the Ghoul is an evil spirit associated with consuming human flesh and hunting kids, originally a Mesopotamian demon. Today, the term is sometimes used to describe a greedy or materialistic individual.

Main infection vector: malicious emails

The following picture represents emails that are being used to deliver malware to the victims, in what looks like a payment document. The e-mails sent by attackers appear to be coming from a bank in the UAE, the Emirates NBD, and include a 7z file with malware. In other cases, victims received phishing links. A quick analysis of the email headers reveals fake sources being utilised to deliver the emails to victims.



Wed 6/8/2016 1:08 PM
EmiratesNBD <banknet@emiratesNBD.com>
Your payment copy advice from Emirates NBD Bank/subsidiary

To

We removed extra line breaks from this message.

Message EmiratesNBD_ADVICE.7z

Attention,

Please see attached payment swift document based on the instruction from our customer.

Should you have any inquiry or require assistance, please contact your payer (our customer) at the contact number stated in the attached advice.Please note that you will need Adobe Acrobat Reader Version 5.0 or above to view your advice. If you do not have the required software, you can download it from the Adobe website at www.adobe.com

Best Regards,

Emirates NBD Bank
P.O. Box 777 Deira,
Dubai United Arab Emirates
Phone: +971 600 540040
Fax: +971 4 327 2996

Disclaimer

This email and any attachments are confidential and may also be privileged. If you are not the intended recipient, please delete all copies and notify the sender immediately. You may wish to refer to the incorporation details of Emirates NBD, Emirates NBD Bank and their subsidiaries at http://www.emiratesnbd.com/en/

Malicious attachments

In the case of spear phishing emails with an attachment, the 7z does not contain payment instructions but a malware executable (EmiratesNBD_ADVICE.exe). We have observed executables with the following MD5s:

Malware MD5 hashes

fc8da575077ae3db4f9b5991ae67dab1
b8f6e6a0cb1bcf1f100b8d8ee5cccc4c
08c18d38809910667bbed747b2746201
55358155f96b67879938fe1a14a00dd6

Email file MD5 hashes

5f684750129e83b9b47dc53c96770e09
460e18f5ae3e3eb38f8cae911d447590

The spear phishing emails are mostly sent to senior members and executives of targeted organizations, most likely because the attackers hope to get access to core intelligence, controlling accounts and other interesting information from people who have the following positions or similar:

- Chief Executive Officer
- Chief Operations Officer
- General Manager
- General Manager, Sales and Marketing
- Deputy General Manager
- Finance and Admin Manager
- Business Development Manager
- Manager
- Export manager
- Finance Manager
- Purchase manager
- Head of Logistics
- Sales Executive
- Supervisor
- Engineer

Technical details

Malware functionality

The malware is based on the Hawkeye commercial spyware, which provides a variety of tools for the attackers, in addition to malware anonymity from attribution. It initiates by self-deploying and configuring persistence, while using anti-debugging and timeout techniques, then starts collecting interesting data from the victim's device, including:

- Keystrokes
- Clipboard data
- FileZilla ftp server credentials
- Account data from local browsers
- Account data from local messaging clients (Paltalk, Google talk, AIM…)
- Account data from local email clients (Outlook, Windows Live mail…)
- License information of some installed applications

> #OpGhoul malware collects all data such as #passwords, keystrokes and screenshots
>
> Tweet

Data exfiltration

Data is collected by the attackers using primarily:

Http GET posts

> Sent to hxxp://192.169.82.86

Email messages

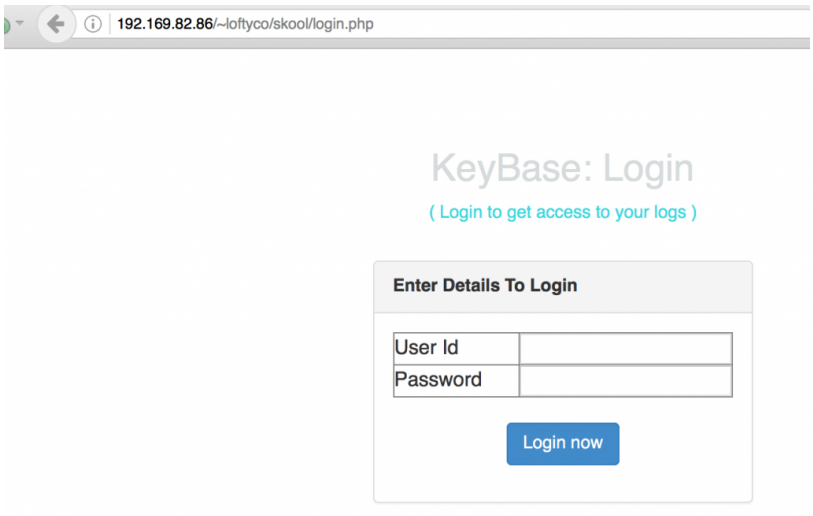
- mail.ozlercelikkapi[.]com (37.230.110.53), mail to info@ozlercelikkapi[.]com
- mail.eminenture[.]com (192.185.140.232), mail to eminfo@eminenture[.]com

Both ozlercelikkapi[.]com and eminenture[.]com seem to belong to compromised organisations operating in manufacturing and technology services.

Malware command center

The malware connects to 192.169.82.86 to deliver collected information from the victim's PC. This information includes passwords, clipboard data, screenshots…

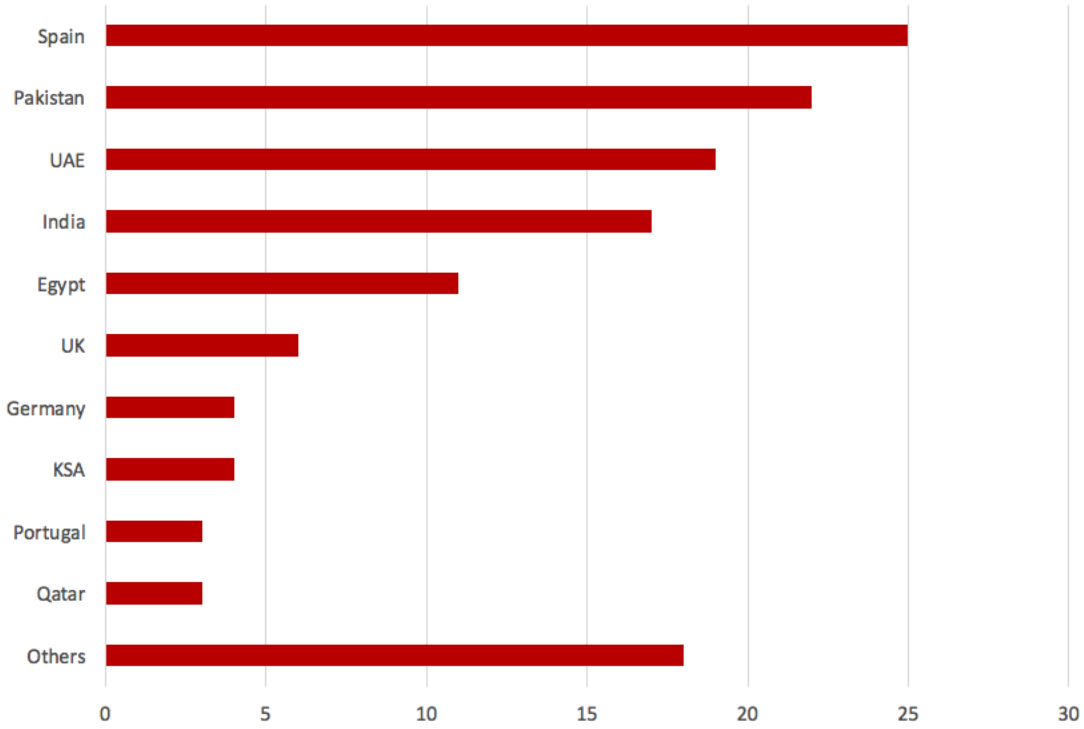
hxxp://192.169.82.86/~loftyco/skool/login.php
hxxp://192.169.82.86/~loftyco/okilo/login.php



The IP address 192.169.82.86 seems to belong to a compromised device running multiple malware campaigns.

Victim information

Victim organizations are distributed in different countries worldwide with attackers focused on certain countries more than others:



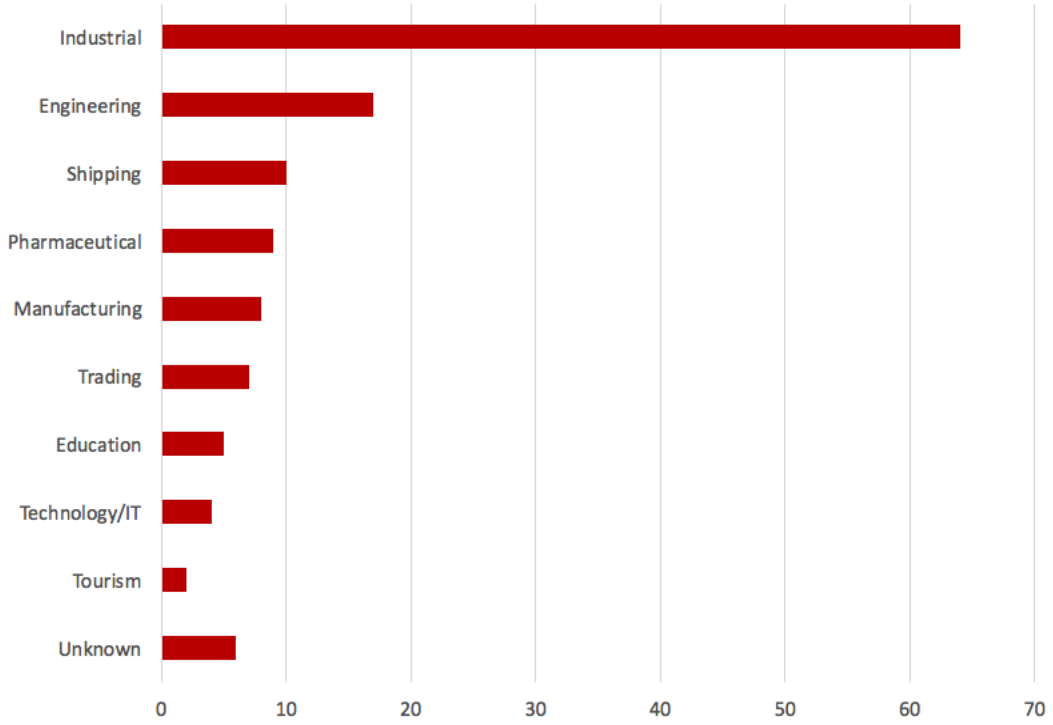
Number of Victim Organisations by Country

Countries marked as “others” have less than three victim organizations each, they are: Switzerland, Gibraltar, USA, Sweden, China, France, Azerbaijan, Iraq, Turkey, Romania, Iran, Iraq and Italy.

Victim industry information

Victim industry types were also indicators of targeted attacks as attackers were looking to infiltrate organizations that belong to the product life cycle of multiple goods, especially industrial equipment.

> #Manufacturing #transportation #travel targets of #OpGhoul
>
> Tweet



Number of Victim Organizations by Industry Type

Victim industry description

Industrial	Petrochemical, naval, military, aerospace, heavy machinery, solar energy, steel, pumps, plastics
Engineering	Construction, architecture, automation, chemical, transport, water
Shipping	International freight shipping
Pharmaceutical	Production/research of pharmaceutical and beauty products
Manufacturing	Furniture, decor, textiles
Trading	Industrial, electronics and food trading
Education	Training centers, universities, academic publishing
Tourism	Travel agencies
Technology/IT	Providers of IT technologies and consulting services
Unknown	Unidentified victims

The last attack waves

Kaspersky Lab user statistics indicate the new waves of attacks that started in June 2016 are focused on certain countries more than others.

> #opghoul highly active in #MiddleEast
>
> Tweet

Hundreds of detections have been reported by Kaspersky Lab users; 70% of the attacked users were found in the United Arab Emirates alone, the other 30% were distributed in Russia, Malaysia, India, Jordan, Lebanon, Turkey, Algeria, Germany, Iran, Egypt, Japan, Switzerland, Bahrain and Tunisia.

Other attack information

Phishing pages have also been spotted through 192.169.82.86, and although they are taken down quickly, more than 150 user accounts were identified as victims of the phishing links sent by the attackers. Victims were connecting from the following devices and inserting their credentials, a reminder that phishing attacks do work on all platforms:

- Windows
- Mac OS X
- Ubuntu
- iPhone
- Android

The malware files are detected using the following heuristic signatures:

Trojan.MSIL.ShopBot.ww
Trojan.Win32.Fsysna.dfah
Trojan.Win32.Generic

Conclusion

Operation Ghoul is one of the many attacks in the wild targeting industrial, manufacturing and engineering organizations, Kaspersky Lab recommends users to be extra cautious while checking and opening emails and attachments. In addition, privileged users need to be well trained and ready to deal with cyber threats; failure in this is, in most cases, the cause behind private or corporate data leakage, reputation and financial loss.

Indicators of Compromise

The following are common among the different malware infections; the presence of these is an indication of a possible infection.

Filenames and paths related to malware

C:\Users\%UserName%\AppData\Local\Microsoft\Windows\bthserv.exe
C:\Users\%UserName%\AppData\Local\Microsoft\Windows\BsBhvScan.exe
C:\Users\%UserName%\AppData\Local\Client\WinHttpAutoProxySync.exe
C:\Users\%UserName%\AppData\Local\Client\WdiServiceHost.exe
C:\Users\%UserName%\AppData\Local\Temp\AF7B1841C6A70C858E3201422E2D0BEA.dat
C:\Users\%UserName%\AppData\Roaming\Helper\Browser.txt
C:\Users\%UserName%\AppData\Roaming\Helper\Mail.txt
C:\Users\%UserName%\AppData\Roaming\Helper\Mess.txt

C:\Users\%UserName%\AppData\Roaming\Helper\OS.txt
C:\ProgramData\Mails.txt
C:\ProgramData\Browsers.txt

List of malware related MD5 hashes

55358155f96b67879938fe1a14a00dd6
f9ef50c53a10db09fc78c123a95e8eec
b8f6e6a0cb1bcf1f100b8d8ee5cccc4c
07b105f15010b8c99d7d727ff3a9e70f
ae2a78473d4544ed2acd46af2e09633d
21ea64157c84ef6b0451513d0d11d02e
08c18d38809910667bbed747b2746201
fc8da575077ae3db4f9b5991ae67dab1
8d46ee2d141176e9543dea9bf1c079c8
36a9ae8c6d32599f21c9d1725485f1a3
cc6926cde42c6e29e96474f740d12a78
6e959ccb692668e70780ff92757d2335
3664d7150ac98571e7b5652fd7e44085
d87d26309ef01b162882ee5069dc0bde
5a97d62dc84ede64846ea4f3ad4d2f93
5a68f149c193715d13a361732f5adaa1
dabc47df7ae7d921f18faf685c367889
aaee8ba81bee3deb1c95bd3aaa6b13d7
460e18f5ae3e3eb38f8cae911d447590
c3cf7b29426b9749ece1465a4ab4259e

List of malware related domains

Indyproject[.]org
Studiousb[.]com
copylines[.]biz
Glazeautocaree[.]com
Brokelimiteds[.]in
meedlifespeed[.]com
468213579[.]com
468213579[.]com
357912468[.]com
aboranian[.]com
apple-recovery[.]us
security-block[.]com
com-wn[.]in
f444c4f547116bfd052461b0b3ab1bc2b445a[.]com
deluxepharmacy[.]net
katynew[.]pw
Mercadojs[.]com

Observed phishing URLs

hxxp://free.meedlifespeed[.]com/ComCast/
hxxp://emailreferentie.appleid.apple.nl.468213579[.]com/
hxxp://468213579[.]com/emailreferentie.appleid.apple.nl/emailverificatie-40985443/home/login.php
hxxp://verificatie.appleid.apple.nl.referentie.357912468[.]com/emailverificatie-40985443/home/lo…
hxxp://192.169.82.86/~gurgenle/verify/webmail/
hxxp://customer.comcast.com.aboranian[.]com/login
hxxp://apple-recovery[.]us/
hxxp://apple.security-block[.]com/Apple%20-%20My%20Apple%20ID.html
hxxp://cgi.ebay.com-wn[.]in/itm/2000-Jeep-Wrangler-Sport-4×4-/?ViewItem&item=17475607809
hxxp://https.portal.apple.com.idmswebauth.login.html.appidkey.05c7e09b5896b0334b3af1139274f266b2hxxp://2b68.f444c4f547116bfd052461b0b
hxxp://www.deluxepharmacy[.]net

Other malware links

Malware links observed on 192.169.82.86 dating back to March and April 2016:

hxxp://glazeautocaree[.]com/proforma-invoice.exe
hxxp://brokelimiteds[.]in/cdn/images/bro.exe
hxxp://brokelimiteds[.]in/cdn/images/onowu.exe
hxxp://brokelimiteds[.]in/cdn/images/obe.exe
hxxp://brokelimiteds[.]in/wp-admin/css/upload/order.exe
hxxp://brokelimiteds[.]in/wp-admin/css/upload/orders.exe
hxxp://papercuts[.]info/SocialMedia/java.exe
hxxp://studiousb[.]com/mercadolivrestudio/f.zip
hxxp://copylines[.]biz/lasagna/gate.php?request=true

For more information on how you can protect your business from similar attacks, please visit this post from Kaspersky Business.