Advanced Notification of Cyber Threats against UAE Entities Through Malicious Emails

Security Advisory	AE-Advisory 17-44	**Criticality**	Critical	
Advisory Released On	17 August 2017			

Impact

A malicious file that is being sent via email, when executed it allows the attacker to install a backdoor into the affected system.

Solution

Adhere the advices written under the solution section.

Affected Platforms

- Microsoft Windows

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a newly discovered threat targeting entities in the UAE currently named as “Credit Advice.exe” and it is currently being distributed via spoofed emails.

Threat Details

Our monitoring systems have detected spoofed emails being sent to entities in the UAE. These emails contain a malicious attachment that installs a backdoor shell into the system.

Spoofed e-mail sample:

Dear Customer,

Credit Advice is attached with this e-mail in PDF format.

Note: To view the attached advice you require Adobe Acrobat Reader.

You can download and install Adobe Acrobat Reader free of charge, from the Adobe website - http://www.adobe.com

Thank you for Banking with CBD.

Attijari e-advice

Commercial Bank of Dubai.

For any query or clarification on the Advice, please contact Help-Desk on Tel:04-2121281/2121230. Swift reference number F01722203BBA01

Email Headers

envelope-from="cbd-e-cbd-e-remmitanceadvice@cbd.ae";

x-sender="cbd-e-cbd-e-remmitanceadvice@cbd.ae";

x-conformance=spf_only; x-record-type="v=spf1"

X-IronPort-AV: E=Sophos;i="5.41,366,1498507200";

d="xz'52?pdf'52?exe'52,96?scan'52,96,96,208,52,217";a="68687551"

Received: from mail.tpgserver.ir ([79.175.154.214])

Received: from [45.126.211.200] (UnknownHost [45.126.211.200]) by mail.tpgserver.ir with SMTP;

From: CBD-e-cbd-e-remmitanceadvice@cbd.ae

Reply-To: sunshineslisa1@yahoo.com

Indicators of Compromise

Callback information:

- Server DNS Name: 185.140.53.231
- Service Port: 39560
- Signature Name: Backdoor.NetWire

File created at:

- C:\Documents and Settings\{user-path}\Local Settings\Temp\Credit Advice.exe

  MD5: a1ec803718ed95b3a9b16b6fd26de998

  SHA1: 3bc6f68182ee5471bac9dc26c40f43c876287351

- C:\Documents and Settings\{user-path}\Local Settings\Temp\~DFFBE2.tmp

  MD5: 2de001af8df33ac65bd2e278679fc850

SHA1: 586a5a839ec9895bd753f61bf4e57eea004774d1

- C:\Documents and Settings\{user-path}\Application Data\Imgburn\{current date}

Registry Modified:

- \REGISTRY\USER\S-1-5-21-1409082233-688789844-725345543-1003\Software\Microsoft\Windows\CurrentVersion\Run\"Windows Updates" = C:\Documents and Settings\{user-path}\Application Data\Imgburn\Imgburn.exe
- \REGISTRY\MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{7L0ELK07-YGF8-G2T6-V845-048RE3V61EWC}\"StubPath" = "C:\Documents and Settings\admin\Application Data\Imgburn\Imgburn.exe

Solution

Entities are recommended with the following:

- Block the callback IP Address: 185.140.53.231
- Block emails coming from the IP address: 79.175.154.214
- Set rule to block this email: sunshineslisa1@yahoo.com
- Monitor connections through this port: 39560
- Perform steps to isolate and take immediate action on possible infected machines
- Make sure the SPF check is enabled in your email security to prevent spoofed emails

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae