Current Events to Widespread Campaigns: Pivoting from Samples to Identify Activity

domaintools.com/resources/blog/current-events-to-widespread-campaigns-pivoting-from-samples-to-identify

> We would like to thank Black Lotus Labs at Lumen for their contributions and assistance in this analysis.

> If you would prefer to listen to The DomainTools Research team discuss their analysis, it is featured in our recent episode of Breaking Badness, which is included at the bottom of this post.

Introduction

Cyber Threat Intelligence (CTI) practitioners can gain insight into adversary operations by tracking conflicts or geopolitical tensions. Similar to a "follow the money" approach in criminal investigations, looking at conflict zones can reveal cyber capabilities deployed as part of events —either by the parties to the conflict itself, or third parties interested in monitoring events for their own purposes.

The above theory is supported by historical incidents linked to geopolitical tensions:

- Russia's invasion of Ukrainian territory leading to, among other events, the 2015 and 2016 Ukraine power incidents, the 2017 NotPetya event, and continuing operations to the present.
- Tensions in the Arabian/Persian Gulf region leading to multiple rounds of wiper malware as well as providing possible "cover" for the 2017 Triton/TRISIS incident.
- Continuing strains on the Korean peninsula providing cover for the 2018 disruptive attack on the Pyeongchang Olympic Games (even if the attacker in this case was not North Korea).

Based on precedent, analysts can identify developments in adversary operations and technical capabilities by tracking identifiers related to major events and conflict zones. Identifying capabilities deployed to take advantage of such items can yield insights into fundamental attacker tradecraft and behaviors, and enable defense and response for incidents which may strike far closer to home at a later date.

Initial Discovery: Caucasus Conflict

With the above thesis in mind, DomainTools researchers examined technical artifacts emerging around the 2020 conflict between Armenia and Azerbaijan in the Caucasus region. While investigating, researchers discovered the following malicious document file on a commercial multi-scanner service:

```
Name: PKK militants in Nagorno-Karabakh.doc
MD5: e00af9b6303460666ae1b4bdeb9503ba
SHA1: ce810173555d6a98ce10c847f16e95575fe13405
SHA256: 7c495c21c628d37ba2298e4a789ff677867521be27ec14d2cd9e9bf55160518f
```

Masquerading as a news article covering details about the Caucasus conflict, the document contains a reference to an external site to fetch additional material to the victim's computer:

Armenia transfers YPG/PKK terrorists to occupied area to train militias against Azerbaijan

Many YPG/PKK terrorists who received training in Iraq and Syria were transferred to Azerbaijan's Nagorno-Karabakh region occupied by Armenia to train Armenian militias against Azerbaijan and ultimately open a new front against Turkey.

The terrorists are expected to provide training to Armenian militias on sabotage, raids and improvised explosive devices (IEDs).

Earlier in September, Armenia proposed to establish a militia of volunteers following tensions with Azerbaijan in the Tovuz region. The YPG/PKK terrorists are expected to train these volunteer fighters.

Armenian Ambassador to Iraq Hrachya Poladian reportedly contacted the YPG/PKK terrorists in Syria and Iraq and convinced them to go to Nagorno-Karabakh for training.

The ambassador also secured an agreement with northern Iraq's Patriotic Union of Kurdistan (PUK), which is led by the Talabani family, for the transfer of terrorists from Iraq.

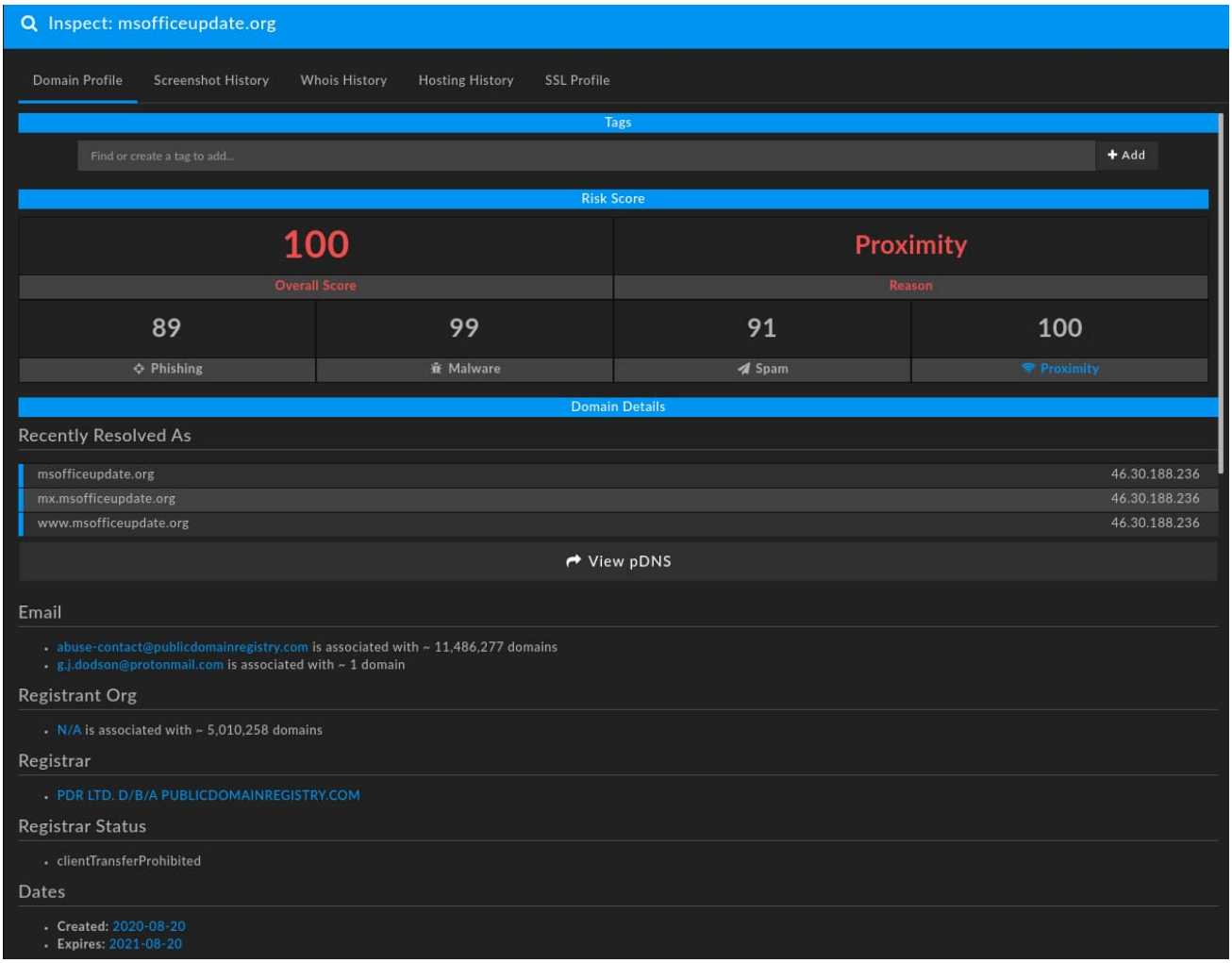
The terrorists followed several different routes to reach their destination, including using Iran as a transit country. One of the routes included the transfer of terrorists from Iraq's Sulaymaniyah to Sabis, then to Kermanshah in Iran. Another group from Mount Qandil in Iraq also passed through Iran's Urmiya on their way to Nagorno-Karabakh.

The head of the Turkey-Azerbaijan Friendship and Solidarity Foundation, professor Aygün Attar, claimed that France is involved in the transfer of YPG/PKK terrorists to train Armenian militias. He noted that there is a center established in France solely for Armenians and YPG/PKK terrorists.

Meanwhile, Istanbul Azerbaijan Cultural Home Association Chairman Hikmet Elp told that the PKK aims to settle in Nagorno-Karabakh and that the Yerevan administration is trying to change the demography of the area by transferring the terrorists and Armenians in Lebanon to the disputed region.

By doing so, Armenia aims to open war on Azerbaijan and train the militias in Karabakh, while the terrorist organization will be able to open a new front and attack Turkey from Armenia or Georgia.

In this specific case, the document attempts to communicate to the domain “msofficeupdate[.]org”:



Overall, the document appears focused on the Armenian-Azerbaijani conflict with dedicated network infrastructure enabling the attack sequence. While we could stop and view this item in isolation, further analysis reveals even more interesting elements.

Identifying Items for Pivoting

Both the document and the domain contain items of interest for further analysis and pivoting. Reviewing lessons from a previous DomainTools blog, we can examine the technical indicators related to this campaign as composite objects with opportunities to discern fundamental adversary behaviors.

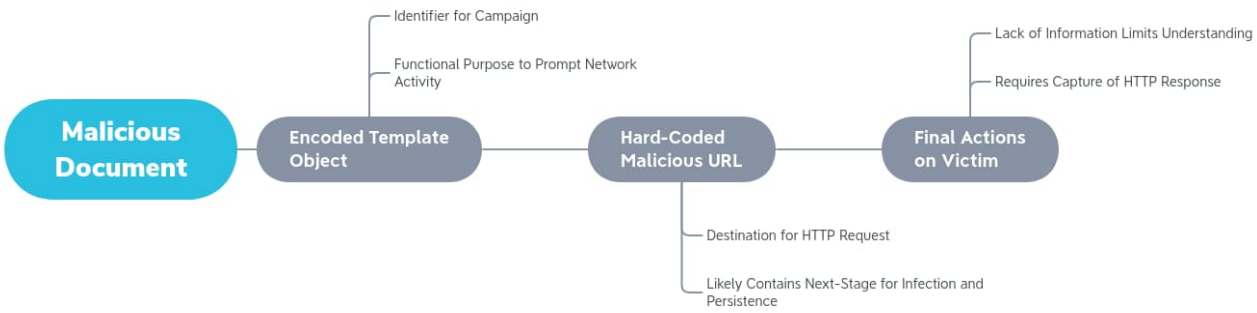
Examining the document, file metadata, shown here using Phil Harvey's ExifTool, indicates the presence of an unusually long string of numbers as a template object:

```
File Size                       : 26 kB
File Modification Date/Time     : 2020:10:13 12:51:05-06:00
File Access Date/Time           : 2020:10:13 12:51:46-06:00
File Inode Change Date/Time     : 2020:10:13 12:51:46-06:00
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                        :
Comments                        :
Template                        : 0000000001000000000200000000030000000040000000005000000000600000000070000000008000000000900000000010000000001100000000120000000013000
0000014000000001500000000160000000017000000001800000000190000000020000000021000000002200000
Last Modified By                :
Revision Number                 : 1
Software                        : Microsoft Office Word
Total Edit Time                 : 0
Create Date                     : 2020:10:05 12:50:00
Modify Date                     : 2020:10:05 12:50:00
Pages                           : 1
Words                           : 300
Characters                      : 1833
Security                        : None
Code Page                       : Unicode (UTF-8)
Company                         :
Lines                           : 15
Paragraphs                      : 4
Char Count With Spaces          : 2129
App Version                     : 15.0000
Scale Crop                      : No
Links Up To Date                : No
Shared Doc                      : No
Hyperlinks Changed              : No
Title Of Parts                  : ,
Heading Pairs                   : Назва, 1, Название, 1
```

Based on the template object and a hard-coded Uniform Resource Locator (URL), the document will attempt to communicate to the domain identified above. The actual functionality of the malicious document hinges on network communication to the attacker domain, with an HTTP request to a resource such as the following:

`hXXps://msofficeupdate[.]org/morgue6visible5bunny6culvert7ambo5nun1illuminate4`

All following functionality appears dependent on a response to this request. At this time, DomainTools does not have any data or other information as to what may be returned from this response. As a result, our analysis is limited to the document itself and identified network infrastructure. However, defenders may find value in the URL pattern in the HTTP request—words divided by single numbers—for developing Network Intrusion Detection System (NIDS) signatures.



Lack of view into follow-on execution aside, we have a search string to use to fingerprint additional file samples or to disposition items that may be related to the original campaign in the template string. Notably, for a malicious document, the item does not contain any active

content (ActiveX objects or Visual Basic for Applications [VBA] macros), limiting our ability to identify further items. However, the template item appears unique enough to serve as a signifier to identify additional samples similarly constructed.

On the infrastructure side, we have several more leads to follow. As previously documented in past blogs on infrastructure hunting and analysis, we have a combination of technical indicators related to domain creation and hosting as well as thematic identifiers related to the domain name itself. For the domain in question, as seen in the previous DomainTools Iris Investigate inspection image above, the following observations hold:

- Leaked registrant email, “g.j.dodson[AT]protonmail[.]com”.
- Domain registration service, “PDR Ltd. d/b/a PublicDomainRegistry.com”.
- Authoritative name server associated with the domain, “bitdomain[.]biz”.
- Hosting on a dedicated server, “46.30.188[.]236”, through the Netherlands-based provider “Web2objects Gmbh”.
- An SSL/TLS certificate obtained through Sectigo with limited identifying information.
- A domain “theme” of mimicking Microsoft Office update services.

While any of the above items in isolation may be relatively limited for identifying adversary tendencies or additional infrastructure—either by being too general or far too specific—in combination, they can yield patterns for further analysis. For example, looking for a combination of privacy-centric email addresses registering domains via PublicDomainRegistry using the name server “bitdomain[.]biz” hosted in Europe with Sectigo SSL/TLS certificates can yield a result set for further analysis. Applying a “thematic” search to the results of such an investigation, such as looking for other Microsoft or Office themes in domain names, can identify additional items for analysis related to this campaign.

Unraveling Additional Infrastructure

Based on the characteristics described in the previous section, DomainTools researchers identified 35 domains matching the patterns associated with the initially observed malicious domain at varying levels of estimative probability or confidence. As shown in the following table, we can observe additional tendencies such as favoring several privacy-oriented email services during registration and an overwhelming focus on European Virtual Private Server (VPS) providers for hosting purposes.

Domain	Date Created	Registrant Email	IP Addr
iphoneupdatecheck[.]com	**2016-05-12**	**louie@brookes.openmailbox.org**	**91.236.1**

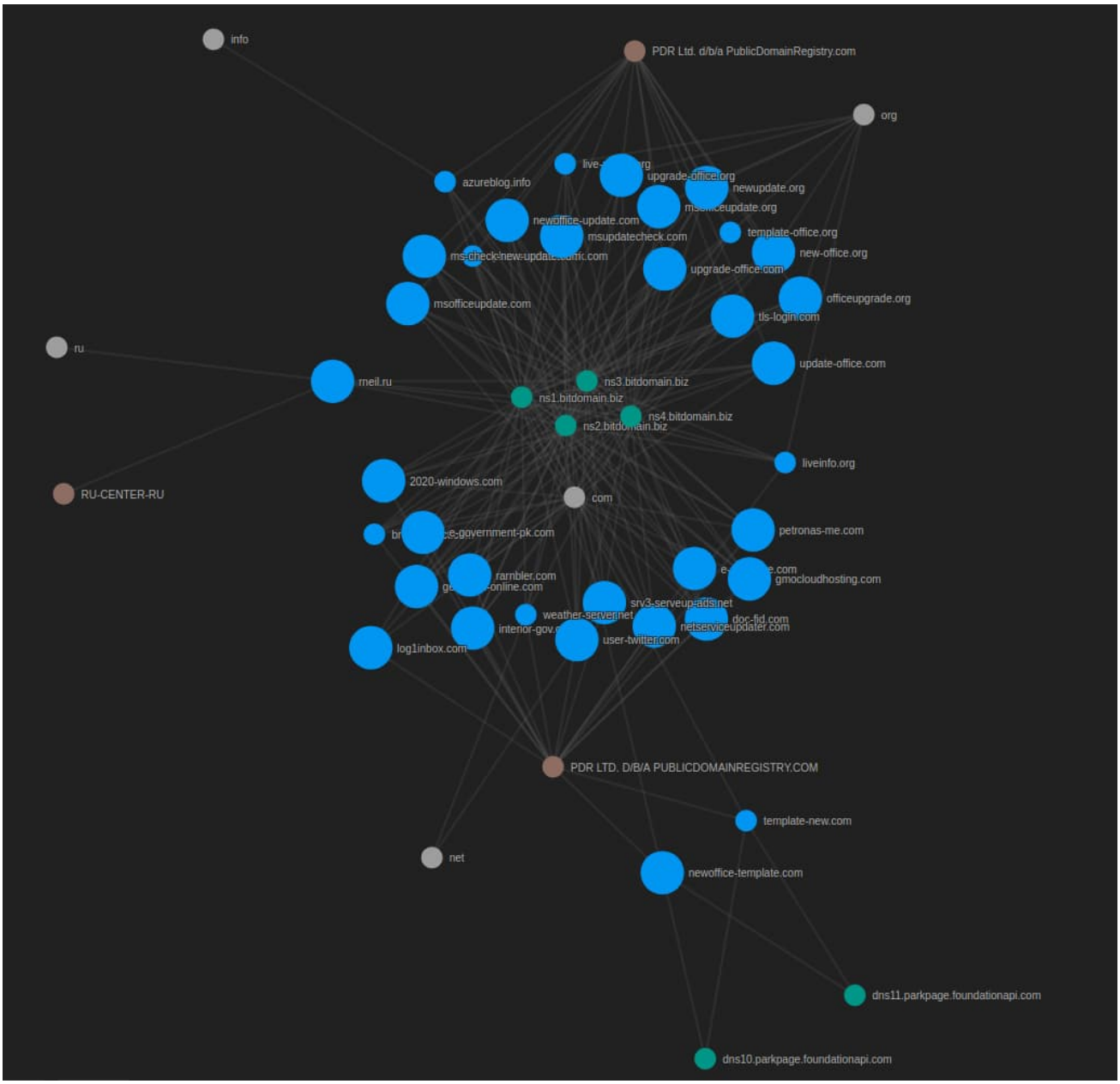
Domain	Date Created	Registrant Email	IP Addr
brexitimpact[.]com	2016-06-23	jaroslav88@tuta.io	185.112.
srv3-serveup-ads[.]net	2019-04-16	salemjoshi@protonmail.com	101.100
newoffice-template[.]com	2019-06-12	j.konnoban@email.cz	147.135
ms-check-new-update[.]com	2019-07-08	stivgarret@protonmail.com	87.121.9
template-new[.]com	2019-08-28	N/A	66.70.21
user-twitter[.]com	2019-11-13	hostmaster@user-twitter.com	N/A
live-media[.]org	2019-11-27	sam.walker@tutanota.com	137.74.1
officeupgrade[.]org	2019-11-29	alex.sval@tutanota.com	198.24.1
template-office[.]org	2020-01-10	s.taylor87@seznam.cz	185.243
get-news-online[.]com	2020-01-15	laptev.vl.90@mail.ru	N/A
liveinfo[.]org	2020-01-15	laptev.vl.90@mail.ru	91.195.2
newoffice-update[.]com	2020-02-11	adam.crowld@protonmail.com	51.161.9
update-office[.]com	2020-03-03	paul_wilsonn@protonmail.com	192.52.1
upgrade-office[.]com	2020-03-18	p.borovin@protonmail.com	158.69.3
tls-login[.]com	2020-03-25	boxerkeen@protonmail.com	103.255
upgrade-office[.]org	2020-04-07	pavel.savin1992@bk.ru	66.248.2

Domain	Date Created	Registrant Email	IP Addr
newupdate[.]org	2020-06-04	and.frolov@bk.ru	46.183.2
2020-windows[.]com	2020-06-19	gmail.chrome.2020@mail.ru	176.107
petronas-me[.]com	2020-07-05	cgog.global@gmail.com	N/A
msupdatecheck[.]com	2020-07-10	mike.barrett@tutanota.com	167.114.
log1inbox[.]com	2020-08-15	vazquezftcathyo5123@gmail.com	N/A
gmocloudhosting[.]com	2020-08-17	hostmaster@gmocloudhosting.com	N/A
msofficeupdate[.]org	2020-08-20	g.j.dodson@protonmail.com	46.30.18
interior-gov[.]com	2020-08-31	gmail.chrome.2020@mail.ru	N/A
e-government-pk[.]com	2020-09-04	gmail.chrome.2020@mail.ru	N/A
e-govoffice[.]com	2020-09-07	hostmaster@e-govoffice.com	N/A
azureblog[.]info	2020-09-25	yshevloin@protonmail.com	N/A
rneil[.]ru	2020-10-01	hostmaster@rneil.ru	N/A
			N/A
weather-server[.]net	2020-10-09	lulgaborova90@protonmail.com	N/A
doc-fid[.]com	2020-10-21	hostmaster@doc-fid.com	N/A
rarnbler[.]com	2020-11-09	nesmali20@cock.li	80.78.22

Domain	Date Created	Registrant Email	IP Addr
msofficeupdate[.]com	2020-11-10	emil.moreu@protonmail.com	185.25.5
netserviceupdater[.]com	2020-11-11	hostmaster@netserviceupdater.com	N/A
new-office[.]org	2020-11-13	moris.pelletier@yahoo.com	51.89.50

While the majority of items were created in 2020, some potentially related network observables date as far back as 2016. When matched against malicious document samples examined in the following section, we begin to see the outlines of a persistent, somewhat lengthy campaign. Although extended in time, the same fundamental network behaviors are reflected in observed items throughout this period.

Observed visually, such as in the DomainTools Iris Investigate visualization below, we see clusters of activity divided between name servers, registrars, and Top Level Domains (TLDs). With an even larger population, we could begin to distill even more aspects of this adversary's methods of operation and potentially devise predictive algorithms for future infrastructure creation.



Locating Additional Samples

In addition to identifying additional network infrastructure, a combination of reviewing the original document as well as pivoting off of observed network infrastructure yields additional malicious document samples. Primarily, the unique Template string of numbers combined with relationship to domains and document themes enable the discovery of additional items. As shown in the following table, these items are linked through both the unique Template string as well as contacting infrastructure related to the analysis provided above on network observables.

SHA256	File Na

SHA256	File Na
1f117d5f398e599887ec92a3f8982751ceb83f2adb85d87a2c232906104e8772	C. Bay
4ad0e64e8ebed1d15fac85cd7439bb345824f03d8b3c6866e669c24a42901daa	Scanda 346 pe
68bde4ec00c62ffa51cef3664c5678f1f4985eb6054f77a5190b4d62bd910538	xyz.do
7ba76b2311736dbcd4f2817c40dae78f223366f2404571cd16d6676c7a640d70	Фадее
7c495c21c628d37ba2298e4a789ff677867521be27ec14d2cd9e9bf55160518f	PKK m Nagorr Karaba
89503c73eadc918bb6f05c023d5bf777fb2a0de1e0448f13ab1003e6d3b71fef	О пост зенитн ракетн С-400.c
c630aa8ebd1d989af197a80b4208a9fd981cf40fa89e429010ada56baa8cf09d	Планир расход 2020(1)
e5a4957d0078d0bb679cf3300e15b09795167fdcfa70bbeab6de1387cd3f75bf	Strateg and Se Review SDSR).
7a1effd3cfeecdba57904417c6eeaa7a74d60a761138885b338e8dc17f2c3fbc	Справ АП_26.
0b116f5b93046c3ce3588bb2453ddbb907d990c2053827600375d8fd84d05d8b	Новые Госпро перече (вст. в 01.07.2
79c0097e9def5cc0f013ba64c0fd195dae57b04fe3146908a4eb5e4e6792ba24	N/A

SHA256	File Na
d8f13e6945b6a335382d14a00e35bfefadbdfb625562e1120e5ed0b545f63e11	N/A
348b25023c45ed7b777fa6f6f635cb587b8ffbf100bfa6761d35610bba525a11	Минтр госслу
93279005aa4c8eddf01020b31bc2b401fe1366cbcc9bb2032ffaeb2984afcd79	Минтр госслу

As described in greater detail in the following section, these items largely feature themes related to conflict in the Caucasus or continuing conflict in Ukraine. Additionally, they extend from December 2019 through November 2020, indicating this activity has continued without significant change for nearly a year.

In addition to these items, DomainTools researchers also identified a second set of documents, all originating from France, with a “testing” theme but matching various characteristics of the above items, such as the unique Template string:

SHA256	File Names
29b49fc728510b8d10a84edbd884cd23a0c453c1158551dbd2d266539d5d09b5	testmv
da43472f3bced232ae8f905e819339fb75da0224a31fb1c394110c77b3318b09	testmv
6478821432b8458053d953b6cff7d1b49f4349f5da366278778c87bc8789b65c	testmv
4285a05a993359b8418b590d3309a361f2c42ef7bc29216c0209e57b74513adb	testmv
40b21a2cd054e01cf37eb22d041ef2ea652eaaeae0ba249439fa7ec07a4e9765	testmv

SHA256	File Names
282c805363469440eef082ac0f2a52dbdd47a8cdaecc08df4c1b4c073c5a8256	testmv
df2a85d84daf10b4dcf8d8fdd83493f3c04f2ac7b3edaf4730df0522cc52009f	testmv

The items above stand out from the other documents for several reasons:

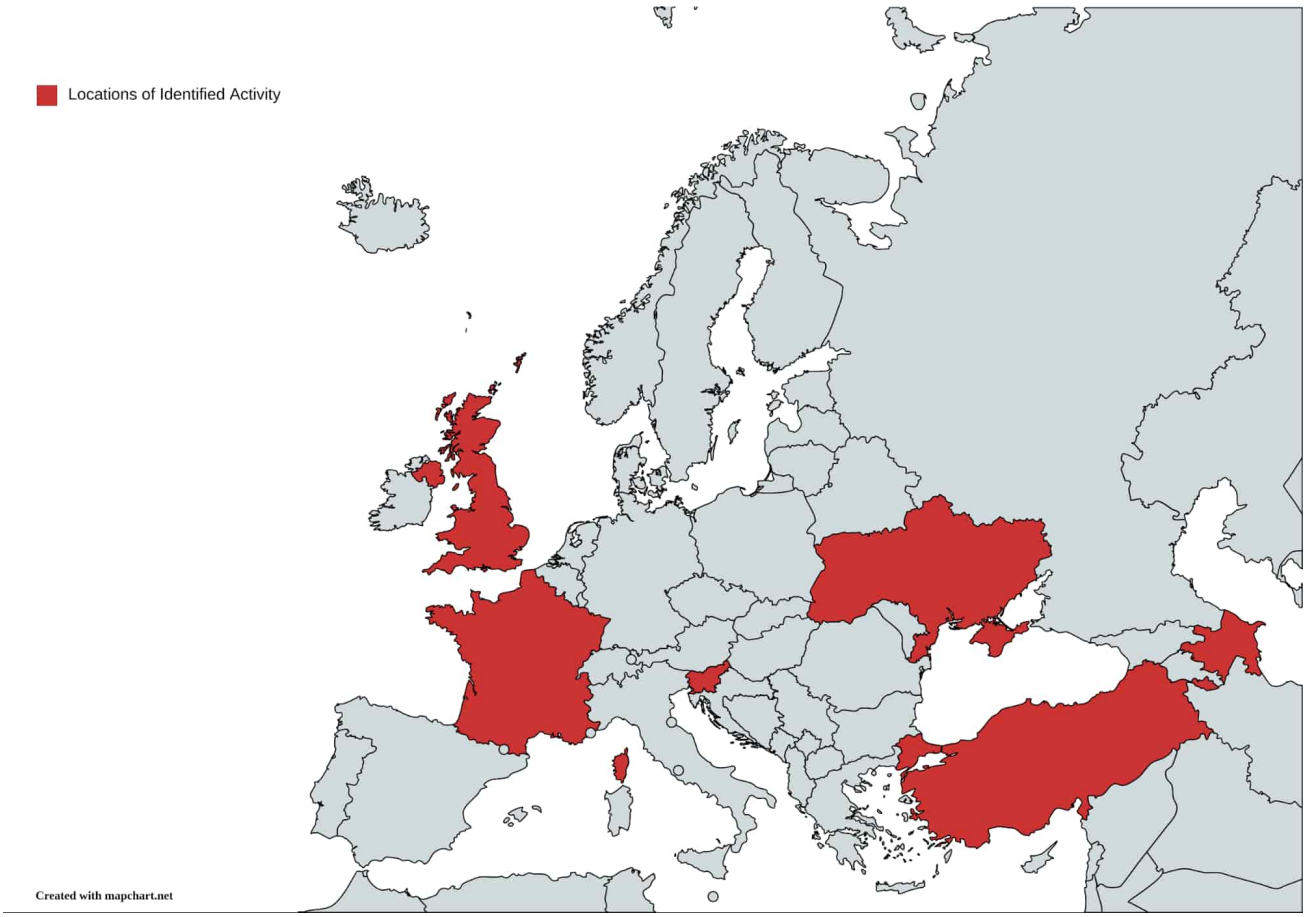
- All were submitted to the same multiscanner service on the same day.
- The items appear to be iterative given the file naming schema (testmw2, testmw3, etc.).
- Analysis of the files indicates fuzzing or alteration of capability among them, in line with the iterative nature of the file names.

An initial conclusion would be these are “testing” runs for a malicious document format or template which would emerge in later campaigns. However, the timing is off for this conclusion to hold as the “test” items appear in mid-September when items using the same template (functionality and lure document) first appear in December 2019.

Overall, this batch of items remains somewhat a mystery as there are no obvious signs linking it to other campaigns. Additionally, some of the items in question are non-functional or lack other components linked to the activity in the first set of documents associated with a likely persistent campaign. DomainTools does not possess any additional information to disposition these items at this time, so they remain somewhat of a mystery relative to the other malicious documents which appear more clearly designed for espionage purposes.

Motivations and Attribution

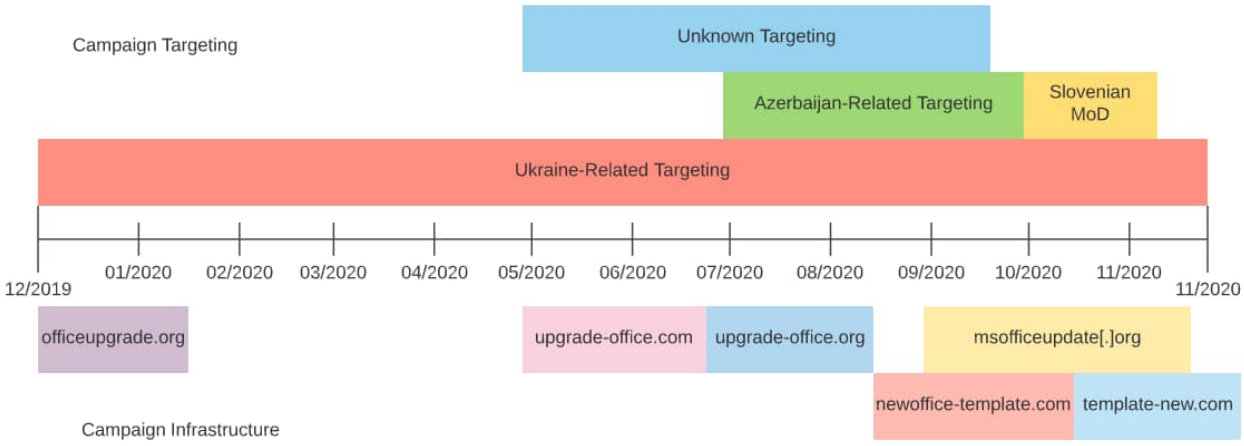
The identified documents emerge from multiple locations but overwhelmingly focus on Azerbaijan and Ukraine.



More interesting still are the themes associated with the documents in their text and titles. In addition to the document which sparked this investigation and its themes centering on the recent conflict on the Caucasus, identified topics include the following:

- C. Bayramov.doc: references the Azerbaijani foreign minister, Ceyhun Bayramov.
- Фадеев М1.doc: presents itself as a fundraising advertisement for a documentary filmmaker covering events in the Donetsk region of Ukraine, an area of conflict.
- О поставке зенитных ракетных систем С-400.doc: masquerades as a report on the S-400 air defense system, produced by Russia and sold to multiple countries.
- Планируемые расходы 2020(1).doc: “Planned Expenses 2020”, a document that appears to show personnel expenses for a Ukrainian local government entity.
- Strategic Defence and Security Review (2021 SDSR).doc: a strategic defense planning document intended for the Slovenian defense ministry. Notably, this document appears related to a phishing email sent to an individual who appears to be the Slovenian military attache to the country’s embassy in the Russian Federation.
- Справочник АП_26.10.2020_.doc: a planning document from the Russian-backed but unrecognized breakaway Donetsk People’s Republic.
- Новые поправки к Госпрограмме переселения в РФ (вст. в силу 01.07.2020).doc: a document on internal resettlement within the Russian Federation.
- Минтруд госслужба.doc:a document from the Russian-backed but unrecognized breakaway Luhansk People’s Republic.

Overall, documents appear related to political, military, and related subjects largely in conflict zones such as the Caucasus and the Russian-backed breakaway regions of eastern Ukraine. Additional items, such as the Slovenian defense document which DomainTools researchers were able to link to a phishing email, strongly imply state-sponsored interests for espionage or similar purposes as motivating this campaign.



In October 2020, several researchers noticed some of the documents identified in this report and linked it to a group referred to in public reporting as “Cloud Atlas” or “Inception.” While data available at present does not completely align with prior Cloud Atlas activity, the following commonalities are observed:

- Targeting focusing on Russian near-abroad regions.
- Use of template objects for initial activity through malicious documents.
- Likely reliance on network communication to retrieve second-stage tooling for follow-on activity.

The response to the HTTP requests sent by the documents would presumably be the key for aligning the above campaigns to the Cloud Atlas actor, but absent this evidence DomainTools can neither confirm nor deny association to this group at present.

Irrespective of specific attribution, possible links to a known Advanced Persistent Threat (APT) actor (Cloud Atlas) combined with campaign themes that are highly political in nature with no obvious mechanism for monetization make the discovered campaign a likely state-sponsored or state-directed espionage campaign. While targeting in this case may imply Russian-related interests, it is important to note that earlier Cloud Atlas activity has also targeted entities in the Russian Federation. One possible alternative hypothesis given the targeting in Russia, as well as a focus on breakaway regions in Ukraine, is that the activity represents Ukraine-sponsored cyber espionage activity. Although interesting, again insufficient evidence exists to support this hypothesis at this time.

While the activity described above is certainly concerning, available information at this time does not support even weak attribution to any state interest, with only plausible (but as yet unproven) links to the Cloud Atlas entity. Although specific attribution may not be possible, we can nonetheless conclude with high confidence that this activity represents cyber espionage activity directed by some, as yet unknown, state actor.

Conclusion

Tracking themes related to geopolitical events can be quite fruitful for discovering active campaigns likely related to state-sponsored interests. In the above example, searching for items related to the Armenia-Azerbaijan conflict in the Caucasus in late 2020 yielded a malicious document. Further analysis of this document and related infrastructure then led to the discovery of additional items which outlined an entire campaign stretching back to 2019.

While the victims of this campaign appear geographically limited, largely focusing on Ukraine and Azerbaijan, the lessons drawn from the analysis of both the malicious documents and related network infrastructure can be used to further defense against similar types of attacks. By monitoring for these types of event-specific incidents, CTI analysts can gain insight into emerging APT activity and deploy defensive countermeasures shortly after discovery.

To learn how to identify and track adversary operations in DomainTools Iris Investigate visit our product page.

Learn More

The DomainTools Security Research Team Discusses Their Analysis: