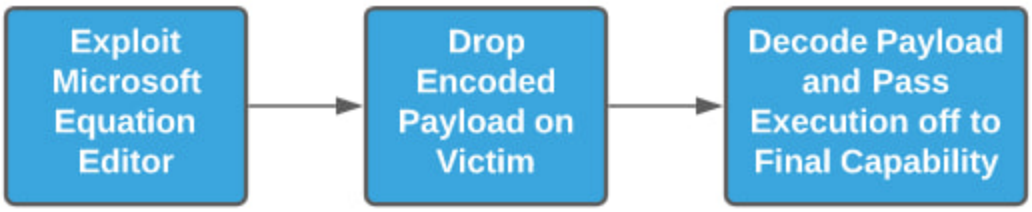
An Undersea Royal Road: Exploring Malicious Documents and Associated Malware

domaintools.com/resources/blog/an-undersea-royal-road-exploring-malicious-documents-and-associated-malware

Background

Since at least 2017, various threat actors, generally associated with or assessed to be located in the People's Republic of China (PRC), utilized a malicious document builder referred to as Royal Road as part of phishing activity. Observed in conjunction with multiple, distinct threat actors, Royal Road provides a mechanism to embed malicious, encoded objects within Rich Text Format (RTF) files. Code execution and object delivery relies on exploiting one of several vulnerabilities in the Microsoft Equation Editor.

As documented by several researchers, multiple adversaries utilize Royal Road to target various industries for the delivery of diverse payload types in victim environments.

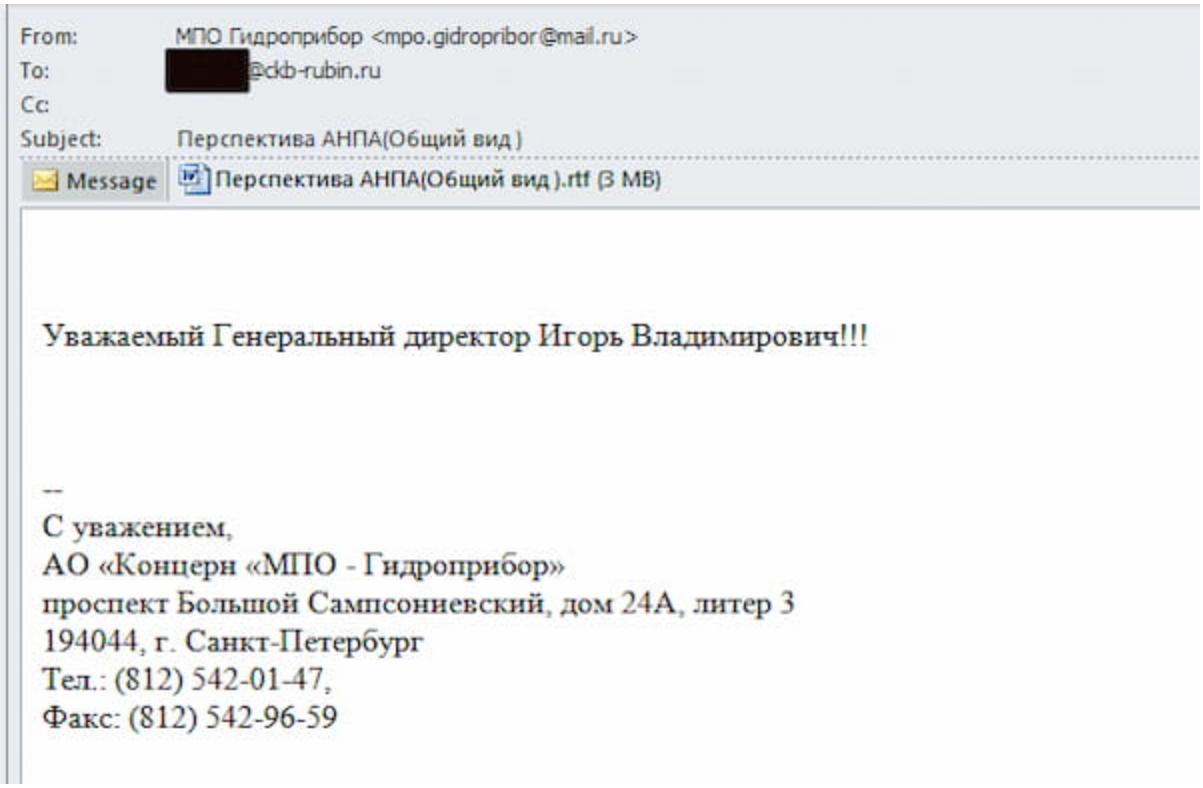


As of this writing, over seven distinct threat groups are assessed to use Royal Road documents for initial access operations, with incidents primarily targeting East and Southeast Asia as well as Russian entities.

In April 2021, DomainTools researchers identified a malicious document matching Royal Road characteristics in a commercial malware database. Further research indicated initial discovery by researchers from Proofpoint. Aside from representing an evolution in Royal Road-related documents and post-exploitation behaviors, available information indicates interesting targeting emphasis for the identified campaign.

Email and Dropper Documents

Although DomainTools initially discovered the activity in question via a malicious document, review of various sources linked the document to an email as the delivery vector:



While technically nondescript—the message is just a brief note with the malicious RTF attached—other contextual details are quite interesting. Examining the actual content and addressing, the following observations emerge:

- For timing and context purposes, the email was sent on 01 April 2021.
- The message sender uses a mail.ru address, but attempts to spoof the legitimate Gridroprobor underwater technology and weapons research center associated with military research and development for the Russian Federation.
- The message recipient is the general contact address for the Rubin Design Bureau, one of three submarine design bureaus supporting the Russian navy.
- Although sent to a general contact address, the message is addressed to General Director “Igor Vladimirovich,” likely referring to Rubin’s current director Igor V. Vilnit.
- The message subject and attachment name references Autonomous Underwater Vehicles (AUVs).
- The email signature references the address and contact information for Gridroprobor in Saint Petersburg.

While all of these items could be identified via open source research and analysis, they represent a level of specificity in theme and likely targeting for the message. Based on the available details, the entity responsible for constructing and sending this message went to some effort to mimic an existing relationship between state-directed organizations researching submarine and underwater weapons technologies on behalf of the Russian Federation. These themes carry over into the malicious RTF itself:

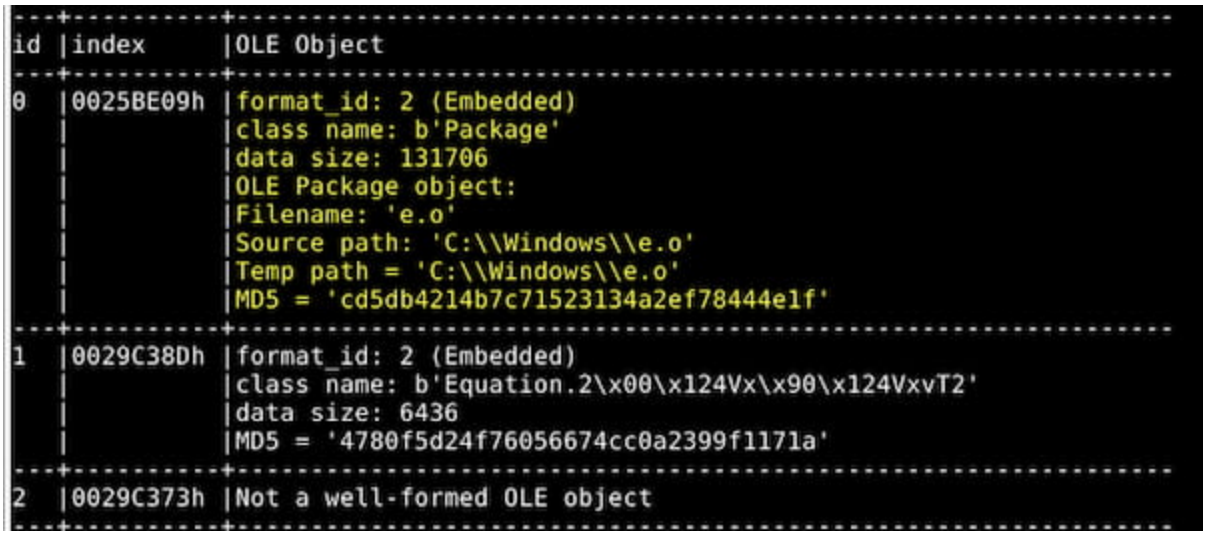
The document, “preliminary design results for the AUV,” is simple with a banner graphic and several perspectives of what appear to be an AUV design. The document has the following identifying characteristics:

```
MD5: 027f5ae272bbb6bbc3e1fdf230a4e3f6

SHA1: 57142832e5453cb0e2c3e6c1a3d7536131b3ed72

SHA256: 774a54300223b421854d2e90bcf75ae25df75ba9f3da1b9eb01138301cdd258f
```

Reviewing document metadata shows several interesting characteristics:

- An original document creation timestamp of 25 May 2007, indicating either the use of deliberate manipulation of timestamps or refreshing an existing template for malicious use.
- An “Author” value of “pc-1.”
- A primary document character set of Simplified Chinese.

Further examination of the document (using the OLEtools framework) reveals embedded objects following the same patterns (although with slightly different naming conventions) as historical Royal Road activity:



```
id |index     |OLE Object
---+----------+-------------------------------------------------------------
0  |0025BE09h |format_id: 2 (Embedded)
   |          |class name: b'Package'
   |          |data size: 131706
   |          |OLE Package object:
   |          |Filename: 'e.o'
   |          |Source path: 'C:\\Windows\\e.o'
   |          |Temp path = 'C:\\Windows\\e.o'
   |          |MD5 = 'cd5db4214b7c71523134a2ef78444e1f'
---+----------+-------------------------------------------------------------
1  |0029C38Dh |format_id: 2 (Embedded)
   |          |class name: b'Equation.2\x00\x124Vx\x90\x124VxvT2'
   |          |data size: 6436
   |          |MD5 = '4780f5d24f76056674cc0a2399f1171a'
---+----------+-------------------------------------------------------------
2  |0029C373h |Not a well-formed OLE object
---+----------+-------------------------------------------------------------
```

The first OLE object is a file containing obfuscated code, while the second contains the Microsoft Equation Editor exploit. When opened in a vulnerable version of Microsoft Word, the document will write the first OLE object to disk to the following location:

```
C:\Users\[Executing User]\AppData\Local\Temp\e.o
```

Next, the Equation Editor will launch, decode the content of “e.o”, and write a Dynamic-Link Library (DLL) object in the form of a Microsoft Office add-in item to disk:

```
C:\Users\[Executing User]\AppData\Roaming\Microsoft\Word\STARTUP\winlog.wll
```

In addition to writing the above file, the “e.o” object is also removed as part of this process. At this point, behavior from the weaponized document ceases and no further, direct action takes place from exploitation.

Identifying Malware Execution and Persistence Mechanisms

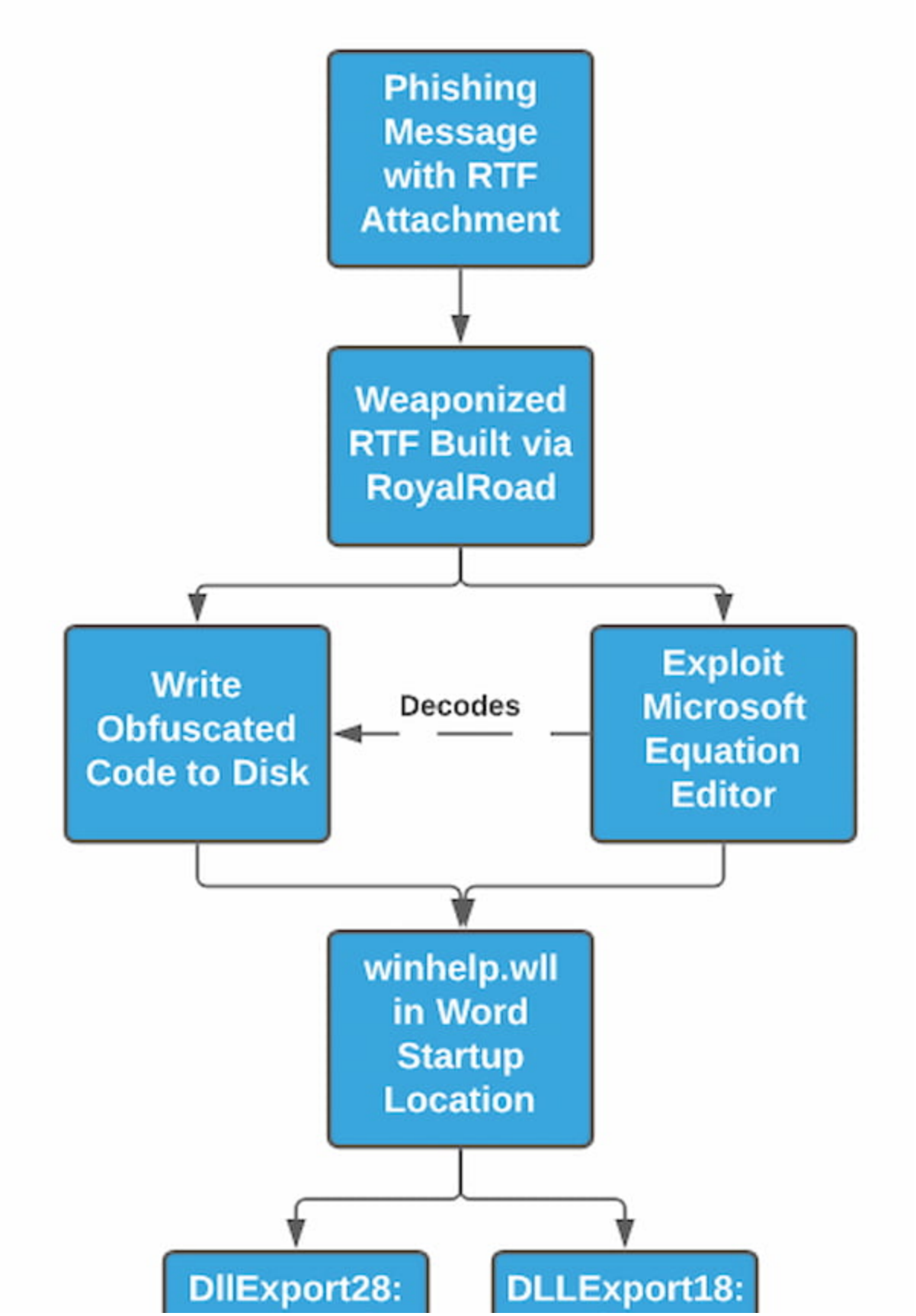
The penultimate action described above, writing the “winlog.wll” DLL to the Word STARTUP location, represents the next stage of execution as well as persistence within the victim environment. As previously documented with respect to Royal Road, the use of WLL file types—typically associated with Microsoft Word add-in objects—ensures the execution of the malicious DLL every time Microsoft Word launches in the future.

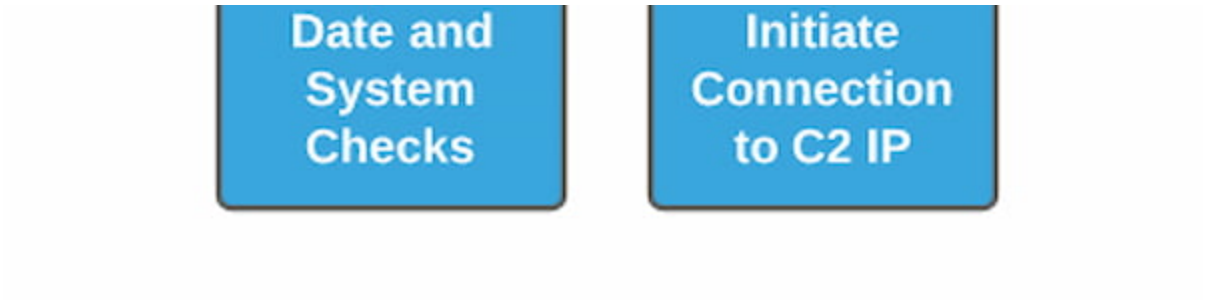
In this specific case, winlog.wll is called via the following convention:

```
Rundll32.exe winlog.wll,DllEntry28 [Current System Time in Unix Timestamp Format]
```

When analyzed, the DLL (specifically the “DllEntry28” export) contains a number of system and analysis checks, preventing execution in monitored environments. However, further analysis of the file indicates that direct functionality can be triggered by calling export “DllEntry18” with no parameters. This combination of follow-on execution taking place the

next time Word is opened combined with the checks present in the default DLL export called during startup provide a relatively simple, if effective, mechanism to evade sandbox and behavioral analysis. Overall execution flow aligns with the following:





Malware Analysis and Infrastructure

The malicious DLL merits further investigation. The file appears compiled mere days before the phishing email was sent (27 March 2021), and has the following characteristics:

```
MD5: 70da6872b6b2da9ddc94d14b02302917

SHA1: b2da45913353bfc66d189455f9ad80ef26968143

SHA256: 2d705f0b76f24a18e08163db2f187140ee9f03e43697a9ea0d840c829692d43c
```

While “DllExport18” and “DllExport28” are the only functional exports for the DLL, the DLL references a total of 34 exported functions (from “DllExport00” to “DllExport33”). Aside from the two already discussed, the remainder have no associated functionality, and potentially represent a diversion or another anti-analysis technique.

When executed via “DllExport18,” the malware sends a single beacon via TCP 443 to the following IP address:

```
45.63.27[.]162
```

Hosted in Australia and part of the Vultr or CHOOPA hosting service, a review of DomainTools Passive DNS (pDNS) data shows no active domain resolutions since November 2020.

Query	Type	Source	Count	Response	First Seen	Last Seen
bgqt.common-faced.com	A	D	16	45.63.27.162	2020-10-27, 12:03	2020-11-20, 23:04
bgqt-7af335.klafive.com	A	D	2	45.63.27.162	2020-09-12, 16:23	2020-09-12, 16:23
bgqt-775077.korea-injured.com	A	D	2	45.63.27.162	2020-09-12, 15:31	2020-09-12, 15:31
bgqt-5b3d94.penny-karen.com	A	D	2	45.63.27.162	2020-09-12, 11:35	2020-09-12, 11:35
bgqt-71fff8.sought.fun	A	D	2	45.63.27.162	2020-09-12, 11:11	2020-09-12, 11:11
bgqt-76012a.dense-favor.net	A	D	2	45.63.27.162	2020-09-12, 09:04	2020-09-12, 09:04
bgqt-2d8e90.cd-n.net	A	D	2	45.63.27.162	2020-09-12, 04:41	2020-09-12, 04:41
bgqt-7e5270.hopcdn.com	A	D	2	45.63.27.162	2020-09-11, 15:03	2020-09-11, 15:03
bgqt.korea-injured.com	A	D	2	45.63.27.162	2020-09-11, 09:12	2020-09-11, 09:12
bgqt-76012a.cd-n.net	A	D	2	45.63.27.162	2020-09-11, 08:28	2020-09-11, 08:28
bgqt-306ea1.fourqt.com	A	D	2	45.63.27.162	2020-09-10, 12:26	2020-09-10, 12:26

Since late 2020, the IP address appears to be dormant until incorporation into this campaign in early 2021.

Examining the DLL further identifies potential additional functionality through plaintext strings. Specifically, there appear to be references for building HTTP headers, including items such as hard-coded User Agent strings, for additional communication:

```
CONNECT %s:%d HTTP/1.0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362

Proxy-Connection: Keep-Alive

Content-Length: 0

HOST: %s

Pragma: no-cache

%s:%s
```

Based on analysis of the DLL, functionality appears to be determined by receiving a response to the initial beacon. The strings identified above indicate the DLL may then respond via HTTP CONNECT methods for subsequent Command and Control (C2) communication.

Additional Document Files

DomainTools researchers attempted to identify additional samples that might be indicative of a wider campaign with similar characteristics. While we were unable to identify any additional samples of the malicious DLL, further searching on document metadata identified two additional documents with identical functionality:

SHA256	File Name
b60c9b59e03101277196bce597701eab5cfb0fd6b37442a5029673a11ffb9295	Перспекти
aec6271de4436ddf0067e67c389cbddb82f73d749e4713f5c8b375ad0ee7da9c	N/A

While the documents have the same ultimate functionality (including identical embedded OLE objects), the presentation of the documents themselves is somewhat different. One features just the diagram portion of the item originally analyzed in this report, while the other features a limited text snippet.

Observation dates indicate visibility after the construction and delivery of the original RTF analyzed in this report (01 April 2021), this information only indicates when the items appeared in third-party datasets as opposed to their actual creation or construction. One possibility is that these less well-formed documents are testing or similar variants for the more refined item delivered in the phishing campaign. How they ended up in a commercial malware repository would be unknown, although we would also need to consider these documents being used in other, unidentified phishing campaigns as well. Irrespective of origin, these documents tentatively indicate a wider scope to this activity than a single phishing email attachment.

Conclusion

The identified activity represents an evolution of Royal Road malicious RTF functionality, including a new naming schema for embedded OLE objects and a DLL payload that appears noticeably different from previous objects delivered via this technique. From a defender’s perspective, this campaign leverages a number of items that can be identified, prevented, or potentially forbidden via policy: using updated Microsoft Office software to eliminate the vulnerability; tracking odd process execution chains such as rundll32.exe spawned from a Microsoft Office process; or identifying odd communication items such as a direct-to-IP HTTP CONNECT observations.

While defensive countermeasures to this campaign are within reach for many organizations, the targeting and possible intent behind this document are curious. Given the email delivery address, themes, and document contents, DomainTools concludes with high confidence that this campaign targets underwater research and weapon development organizations in

the Russian Federation. Furthermore, the historical pattern of activity associated with Royal Road operations combined with the observed language set used in the primary document analyzed in this report would strongly suggest a relationship to at minimum Chinese language entities, if not the PRC itself. However, insufficient evidence exists given paucity of samples and minimal observed targeting and communication to make such a link at anything greater than low confidence.

Irrespective of attribution, the identified phishing instance shows the continued use and evolution of a malicious document framework widely deployed by many threat actors. Combined with the sensitive targeting and the attempts at hardening the ultimate payload, it appears the adversary went to some effort to evade analysis of their activity as well. Although this campaign appears specifically targeted to an entity in the Russian Federation, the underlying behaviors of this campaign—from malicious document usage through binary execution guardrails and controls—provide helpful insight into adversary tradecraft from which all defenders can learn valuable lessons.