Targets of Interest | Russian Organizations Increasingly Under Attack By Chinese APTs

Tom Hegel ⁝

SentinelLABS
Targets of Interest | Russian Organizations Increasingly Under Attack By Chinese APTs
By Tom Hegel
READ BLOG >

Executive Summary

- SentinelLabs has identified a new cluster of threat activity targeting Russian organizations.
- We assess with high-confidence that the threat actor responsible for the attacks is a Chinese state-sponsored cyber espionage group, as also recently noted by Ukraine CERT (CERT-UA).
- The attacks use phishing emails to deliver Office documents to exploit targets in order to deliver their RAT of choice, most commonly Bisonal.
- SentinelLabs has also identified associated activity targeting telecommunication organizations in Pakistan leveraging similar attack techniques.

Overview

On June 22nd 2022, CERT-UA publicly released Alert #4860, which contains a collection of documents built with the Royal Road malicious document builder, themed around Russian government interests. SentinelLabs has conducted further analysis of CERT-UA's findings and has identified supplemental Chinese threat activity.

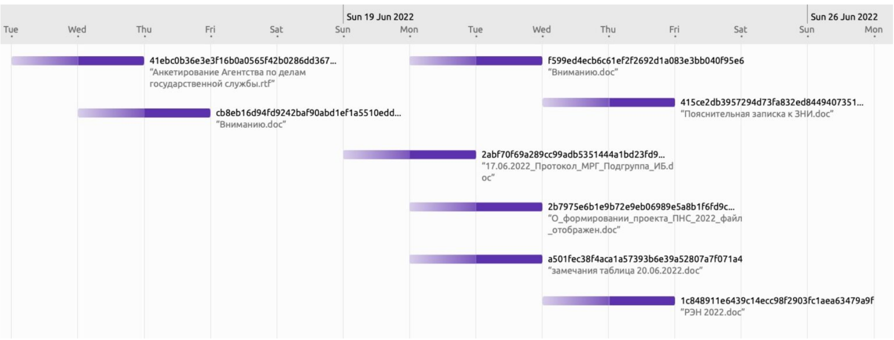
China's recent intelligence objectives against Russia can be observed in multiple campaigns following the invasion of Ukraine, such as Scarab, Mustang Panda, 'Space Pirates', and now the findings here. Our analysis indicates this is a separate Chinese campaign, but specific actor attribution is unclear at this time.

While the overlap of publicly reported actor names inevitably muddies the picture, it remains clear that the Chinese intelligence apparatus is targeting a wide range of Russian-linked organizations. Our findings currently offer only an incomplete picture of this threat cluster's phishing activity, but they serve to provide perspective into an attacker's ongoing operational objectives and a framework for our ongoing research.

Malicious Documents Targeting Russia

On June 22nd , Ukraine's CERT-UA reported several RTF documents containing malicious code exploiting one or more vulnerabilities in MS Office. CERT-UA assessed that the documents, "Vnimaniyu.doc", "17.06.2022_Protokol_MRG_Podgruppa_IB.doc", and "remarks table 20.06.2022_obraza", were likely built with the Royal Road builder and dropped the Bisonal backdoor. Royal Road is a malicious document builder used widely by Chinese APT groups, while Bisonal is a backdoor RAT unique to Chinese threat actors.

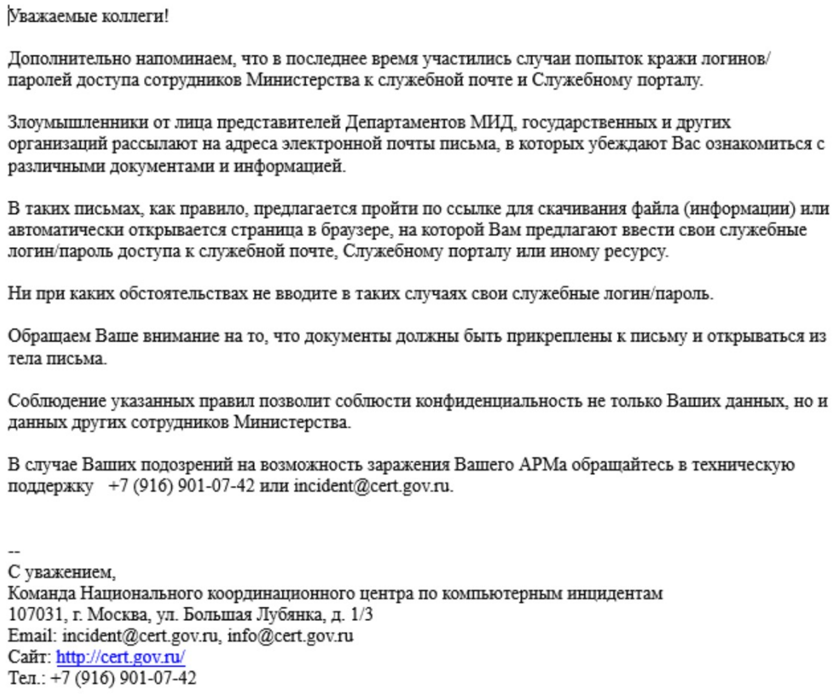
The CERT-UA advisory followed public reporting by our colleagues from nao_sec and Malwarebytes, who identified some of the first indicators and shared related samples and C2 servers. Building off this initial intelligence, SentinelLabs discovered a further related cluster of activity.



Timeline of Royal Road Malicious Documents

As we have observed over the years, Royal Road documents follow content themes relevant to their targets. Following that practice, it's reasonable to assume that the targets in this recent cluster of activity are likely Russian government organizations.

One example of this cluster (f599ed4ecb6c61ef2f2692d1a083e3bb040f95e6) is a fake document mimicking a RU-CERT memo on increased phishing attacks.



Уважаемые коллеги!

Дополнительно напоминаем, что в последнее время участились случаи попыток кражи логинов/паролей доступа сотрудников Министерства к служебной почте и Служебному порталу.

Злоумышленники от лица представителей Департаментов МИД, государственных и других организаций рассылают на адреса электронной почты письма, в которых убеждают Вас ознакомиться с различными документами и информацией.

В таких письмах, как правило, предлагается пройти по ссылке для скачивания файла (информации) или автоматически открывается страница в браузере, на которой Вам предлагают ввести свои служебные логин/пароль доступа к служебной почте, Служебному порталу или иному ресурсу.

Ни при каких обстоятельствах не вводите в таких случаях свои служебные логин/пароль.

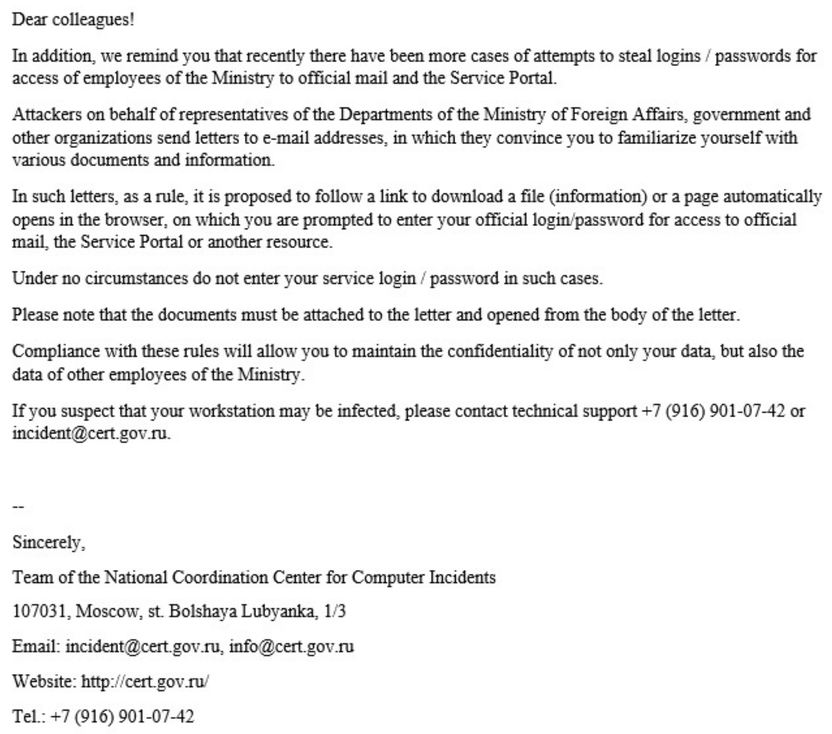
Обращаем Ваше внимание на то, что документы должны быть прикреплены к письму и открываться из тела письма.

Соблюдение указанных правил позволит соблюсти конфиденциальность не только Ваших данных, но и данных других сотрудников Министерства.

В случае Ваших подозрений на возможность заражения Вашего АРМа обращайтесь в техническую поддержку +7 (916) 901-07-42 или incident@cert.gov.ru.

--
С уважением,
Команда Национального координационного центра по компьютерным инцидентам
107031, г. Москва, ул. Большая Лубянка, д. 1/3
Email: incident@cert.gov.ru, info@cert.gov.ru
Сайт: http://cert.gov.ru/
Тел.: +7 (916) 901-07-42

Malicious document mimicking RU-CERT



Dear colleagues!

In addition, we remind you that recently there have been more cases of attempts to steal logins / passwords for access of employees of the Ministry to official mail and the Service Portal.

Attackers on behalf of representatives of the Departments of the Ministry of Foreign Affairs, government and other organizations send letters to e-mail addresses, in which they convince you to familiarize yourself with various documents and information.

In such letters, as a rule, it is proposed to follow a link to download a file (information) or a page automatically opens in the browser, on which you are prompted to enter your official login/password for access to official mail, the Service Portal or another resource.

Under no circumstances do not enter your service login / password in such cases.

Please note that the documents must be attached to the letter and opened from the body of the letter.

Compliance with these rules will allow you to maintain the confidentiality of not only your data, but also the data of other employees of the Ministry.

If you suspect that your workstation may be infected, please contact technical support +7 (916) 901-07-42 or incident@cert.gov.ru.

--

Sincerely,

Team of the National Coordination Center for Computer Incidents

107031, Moscow, st. Bolshaya Lubyanka, 1/3

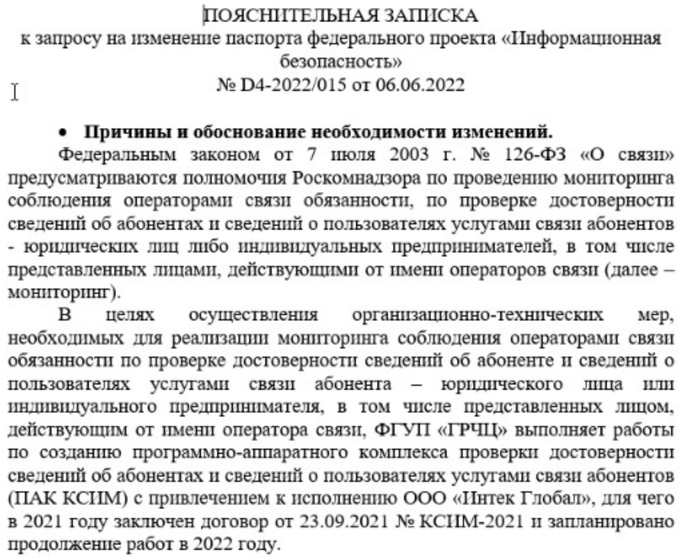
Email: incident@cert.gov.ru, info@cert.gov.ru

Website: http://cert.gov.ru/

Tel.: +7 (916) 901-07-42

Malicious document mimicking RU-CERT (Translated)

Another example is themed around telecommunication organizations (415ce2db3957294d73fa832ed844940735120bae).



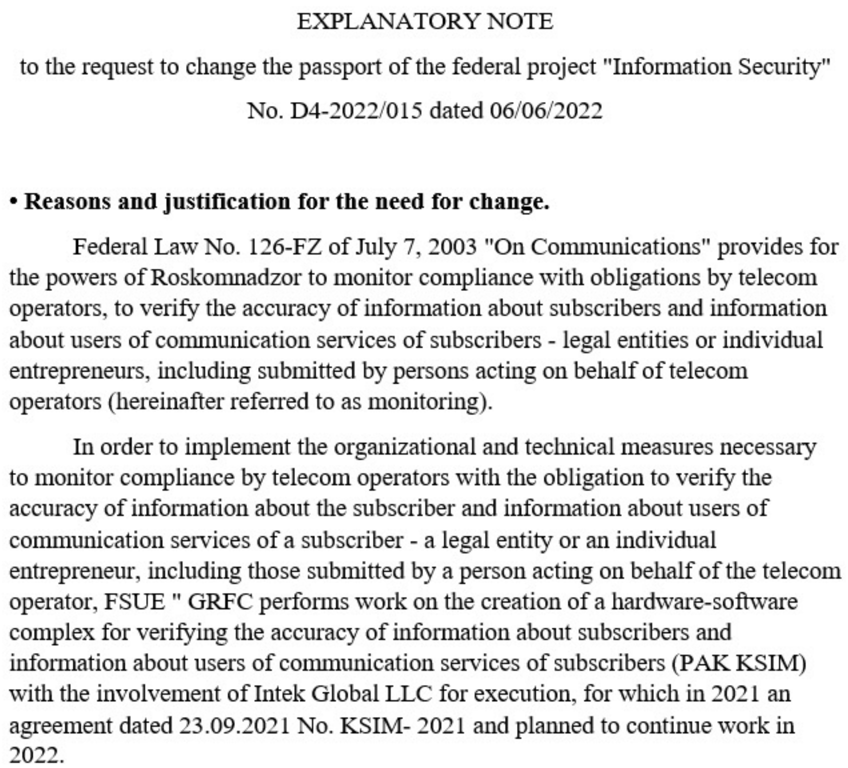
ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к запросу на изменение паспорта федерального проекта «Информационная безопасность»
№ D4-2022/015 от 06.06.2022

- **Причины и обоснование необходимости изменений.**

Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи» предусматриваются полномочия Роскомнадзора по проведению мониторинга соблюдения операторами связи обязанности, по проверке достоверности сведений об абонентах и сведений о пользователях услугами связи абонентов - юридических лиц либо индивидуальных предпринимателей, в том числе представленных лицами, действующими от имени операторов связи (далее – мониторинг).

В целях осуществления организационно-технических мер, необходимых для реализации мониторинга соблюдения операторами связи обязанности по проверке достоверности сведений об абоненте и сведений о пользователях услугами связи абонента – юридического лица или индивидуального предпринимателя, в том числе представленных лицом, действующим от имени оператора связи, ФГУП «ГРЧЦ» выполняет работы по созданию программно-аппаратного комплекса проверки достоверности сведений об абонентах и сведений о пользователях услугами связи абонентов (ПАК КСИМ) с привлечением к исполнению ООО «Интек Глобал», для чего в 2021 году заключен договор от 23.09.2021 № КСИМ-2021 и запланировано продолжение работ в 2022 году.

Malicious Document – Russia Telecom Theme – “Пояснительная записка к ЗНИ.doc”



EXPLANATORY NOTE

to the request to change the passport of the federal project "Information Security"

No. D4-2022/015 dated 06/06/2022

- **Reasons and justification for the need for change.**

Federal Law No. 126-FZ of July 7, 2003 "On Communications" provides for the powers of Roskomnadzor to monitor compliance with obligations by telecom operators, to verify the accuracy of information about subscribers and information about users of communication services of subscribers - legal entities or individual entrepreneurs, including submitted by persons acting on behalf of telecom operators (hereinafter referred to as monitoring).

In order to implement the organizational and technical measures necessary to monitor compliance by telecom operators with the obligation to verify the accuracy of information about the subscriber and information about users of communication services of a subscriber - a legal entity or an individual entrepreneur, including those submitted by a person acting on behalf of the telecom operator, FSUE " GRFC performs work on the creation of a hardware-software complex for verifying the accuracy of information about subscribers and information about users of communication services of subscribers (PAK KSIM) with the involvement of Intek Global LLC for execution, for which in 2021 an agreement dated 23.09.2021 No. KSIM- 2021 and planned to continue work in 2022.

Malicious Document – Russia Telecom Theme – “Пояснительная записка к ЗНИ.doc” (Translated)

The example documents shown above both exploit CVE-2018-0798, a remote execution vulnerability in Microsoft Office to install the embedded malware.

Attribution to Chinese Threat Groups

The collection of files and infrastructure noted above could be considered related to the Tonto Team APT group (*aka* “CactusPete”, “Earth Akhlut”), a Chinese threat group that has been reported on for nearly ten years. However, we assess that link with only medium confidence due to the potential for shared attacker resources that could muddy attribution based on the currently available data. Known targets span the globe, with a particular interest in Northeast Asia, including governments, critical infrastructure, and other private businesses.

The attacker continues their long history of Russian targeting; however, the rate of Russian and Russia-relevant targets in recent weeks may indicate increased prioritization.

There are multiple connections of this activity to Chinese threat actors. As noted above, the documents are built with a commonly known malicious document builder used widely by Chinese APT groups, the shared toolkit often referred to as the “Royal Road” or the “8.t” builder.

These documents often contain metadata indicating the document creator’s operating system was using simplified Chinese, a trait we observed in our previous analysis of Scarab APT activity.

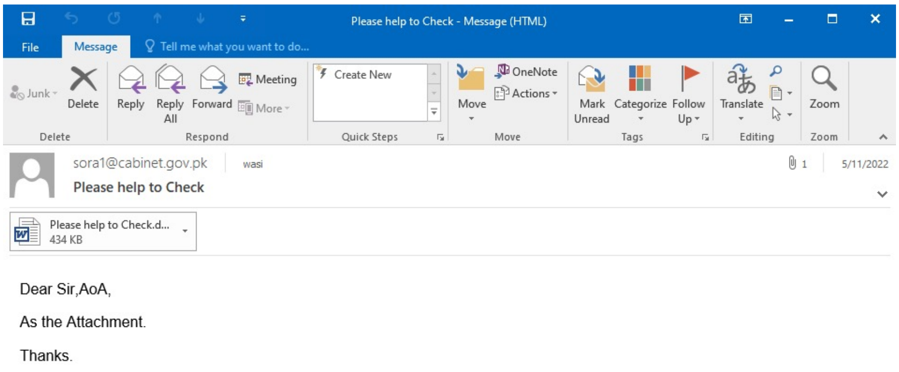
The malicious documents are generally used for the delivery of custom malware, such as the Bisonal RAT, which as noted by CERT-UA, is unique to Chinese groups, including Tonto Team. Bisonal has a uniquely long history of use and continued development by its creators, such as expanding features for file searching and exfiltration, anti-analysis and detection techniques, and maintaining generally unrestricted system control.

Additionally, the collection of C2 infrastructure associated with these various samples fall under a larger umbrella of known Chinese APT activity.

Related Activity of Interest

It’s also worth noting that there are still ongoing related attacks focused on non-Russian organizations, such as those against Pakistan.

For example, one file uploaded to VirusTotal (91ca78231bcacab0d5e6194041817b96252e65bf) from Pakistan is a May 2022 email message file to the Pakistan Telecommunication Authority, sent from a potentially compromised account in the Cabinet Division of the Pakistani government. This email contains the Royal Road attachment “Please help to Check.doc” (f444ff2386cd3ada204c3224463f4be310e5554a), dropping 85fac143c52e26c22562b0aaa80ffe649640bd29 and beaconing outbound to instructor.giize[.]com (198.13.56[.]122).



sora1@cabinet.gov.pk wasi

1 5/11/2022

Please help to Check

Please help to Check.d...
434 KB

Dear Sir,AoA,

As the Attachment.

Thanks.

Phishing email containing malicious document

Conclusion

We assess with high confidence that the Royal Road-built malicious documents, delivered malware, and associated infrastructure are attributable to Chinese threat actors. Based on our observations, there's been a continued effort to target Russian organizations by this cluster through well-known attack methods– the use of malicious documents exploiting n-day vulnerabilities with lures specifically relevant to Russian organizations. Overall, the objectives of these attacks appear espionage-related, but the broader context remains unavailable from our standpoint of external visibility.

Indicators of Compromise

IOC	Description
f599ed4ecb6c61ef2f2692d1a083e3bb040f95e6	6/21/2022 Royal Road Document"Вниманию.doc"
cb8eb16d94fd9242baf90abd1ef1a5510edd2996	6/16/2022 Royal Road Document "Вниманию.doc"
41ebc0b36e3e3f16b0a0565f42b0286dd367a352	6/15/2022 (Estimate) Royal Road Document"Анкетирование Агентства по делам государственной службы.rtf"
2abf70f69a289cc99adb5351444a1bd23fd97384	6/20/2022 Royal Road Document"17.06.2022_Протокол_МРГ_Подгруппа_ИБ.doc"
supportteam.lingrevelat[.]com	C2 Domain
upportteam.lingrevelat[.]com	C2 Domain for cb8eb16d94fd9242baf90abd1ef1a5510edd2996
2b7975e6b1e9b72e9eb06989e5a8b1f6fd9ce027	6/21/2022 Royal Road Document"О_формировании_проекта_ПНС_2022_файл_отображен.doc"
a501fec38f4aca1a57393b6e39a52807a7f071a4	6/21/2022 Royal Road Document"замечания таблица 20.06.2022.doc"
415ce2db3957294d73fa832ed844940735120bae	6/23/2022 Royal Road Document"Пояснительная записка к ЗНИ.doc"
news.wooordhunts[.]com	C2 Domain for 415ce2db3957294d73fa832ed844940735120bae
137.220.176[.]165	IP Resolved for C2 Domains news.wooordhunts[.]com supportteam.lingrevelat[.]com upportteam.lingrevelat[.]com
1c848911e6439c14ecc98f2903fc1aea63479a9f	6/23/2022 Royal Road Document"РЭН 2022.doc"
91ca78231bcacab0d5e6194041817b96252e65bf	5/12/2022 Phishing Email File
f444ff2386cd3ada204c3224463f4be310e5554a	5/12/2022 Royal Road Document"Please help to Check.doc"
instructor.giize[.]com	C2 Server for f444ff2386cd3ada204c3224463f4be310e5554a