# Cosmic Lynx Returns in 2021 with Updated Tricks

agari.com/email-security-blog/cosmic-lynx-returns-2021/

February 11, 2021

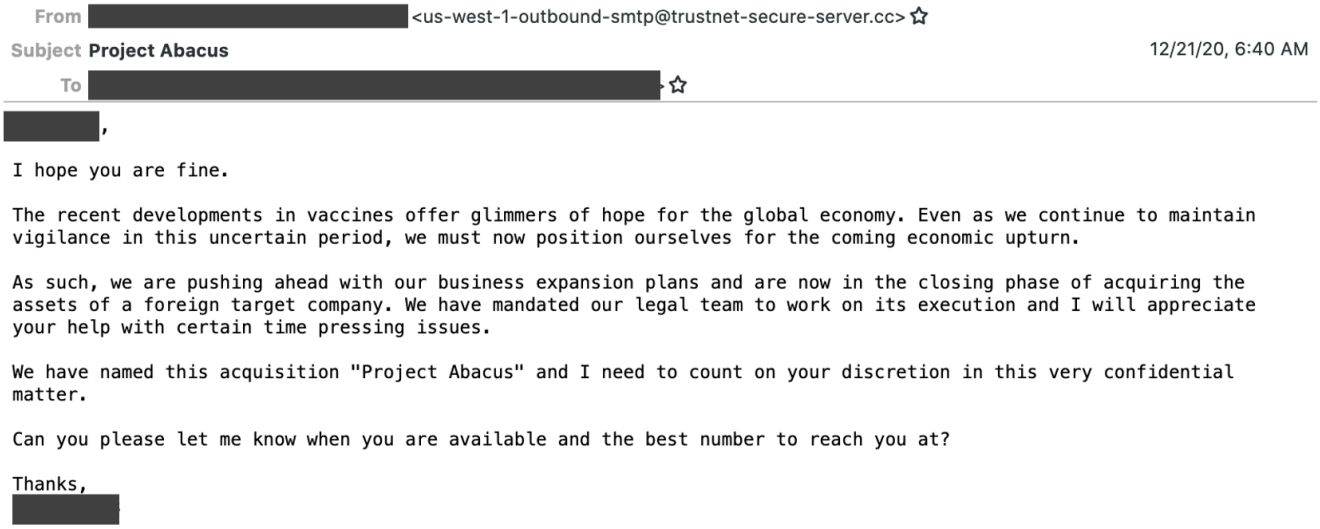
Email Security Blog

Share


In July 2020, we published a report on a Russian-based BEC group we called Cosmic Lynx. In that report, we described the tactics used by the group, which included its targeting of senior executives at large companies with a global footprint and how it uses mergers and acquisitions (M&A) themes in its BEC email lures.

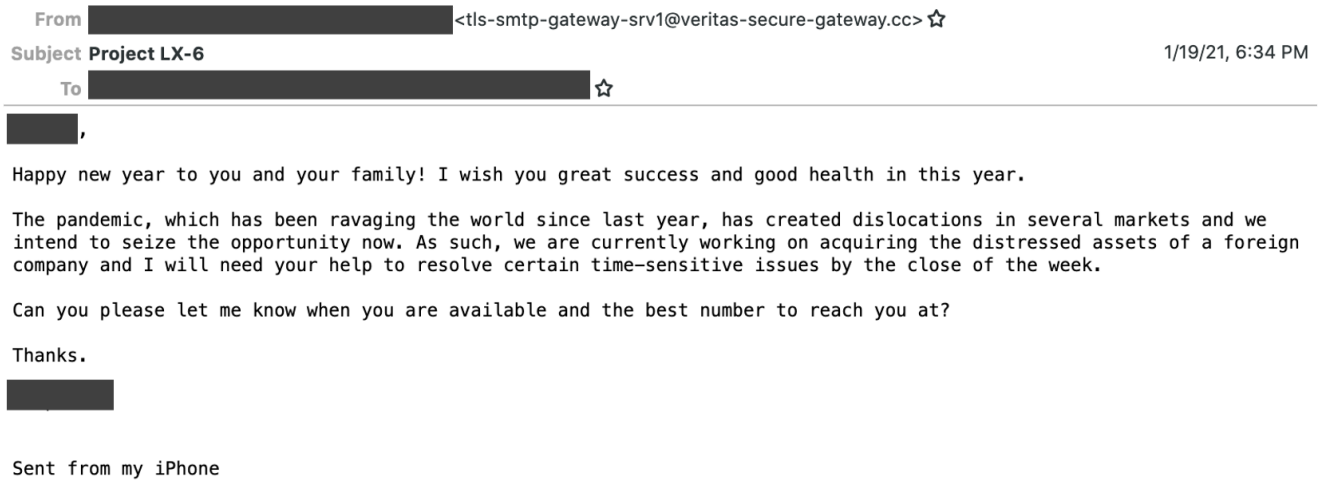
Shortly after we published the report, we saw a significant decrease in Cosmic Lynx activity for more than three months. While we can't conclusively say that our report caused Cosmic Lynx to go on a hiatus, the timing was very notable. In mid-October 2020, though, we started to detect a resurgence in Cosmic Lynx activity, using the same tactics that we had previously observed prior to their disappearance.

In late-December 2020, however, we observed a shift in Cosmic Lynx's tactics. First, the group started including references to a COVID-19 vaccine in their initial emails. Cosmic Lynx had previously used COVID themes in their communications earlier in 2020 as a way to build rapport with their targets, but the inclusion of vaccine references indicates the group is continuing to update their lures to reflect items of global interest. Examples of COVID vaccine references in recent Cosmic Lynx BEC campaigns have included lines like "The recent developments in vaccines offer glimmers of hope for the global economy," or "The world economy is approaching a turning point amid hopes for a rapid recovery fueled by an early vaccine."




*Cosmic Lynx email referencing COVID-19 vaccines.*

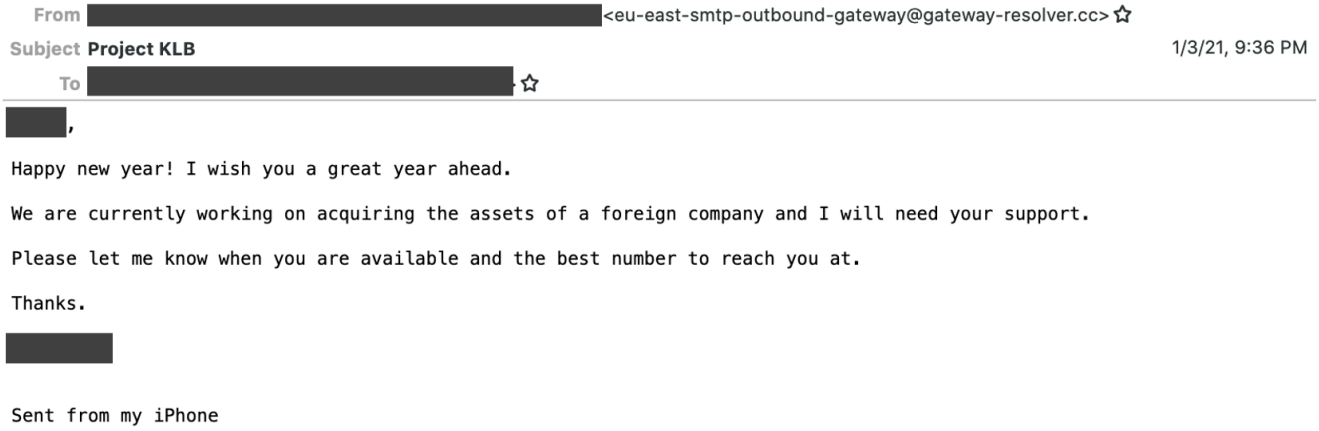
In addition to referencing COVID vaccines, Cosmic Lynx has also continued using other pandemic themes as a way to frame the rationale for the supposed acquisition. In some of their recent campaigns, the group writes that the pandemic “has created dislocations in several markets and we intend to seize the opportunity now” and “We must now position ourselves for the coming economic upturn even as we maintain vigilance in this uncertain period.”




*Cosmic Lynx email containing COVID-19 themes.*

Second, Cosmic Lynx changed the construction of the email addresses they use to send BEC emails. Since mid-2019, the email addresses used by Cosmic Lynx were constructed to mimic secure email and network infrastructure and referenced celestial bodies, like planets and stars. In December 2020, the group started using email addresses that seem to be created to look like more generic email infrastructure, sometimes resembling Amazon Simple Email Service (SES) naming conventions, such as eu-west-smtp-outbound[at]veritas-secure-gateway[.]cc or us-east-tls-smtp-gateway[at]trustnet-server[.]cc.

Finally, instead of continuing communication over email, Cosmic Lynx immediately attempts to redirect a target to phone communication. At the end of their recent BEC emails, Cosmic Lynx now includes a request like, “Can you please let me know when you are available and the best number to reach you at?” While we do not yet have concrete details about how these calls would proceed, it is likely that Cosmic Lynx will use technology to mask the voice of the actor.


From [redacted] <eu-east-smtp-outbound-gateway@gateway-resolver.cc>
Subject **Project KLB** 1/3/21, 9:36 PM
To [redacted]

[redacted],

Happy new year! I wish you a great year ahead.

We are currently working on acquiring the assets of a foreign company and I will need your support.

Please let me know when you are available and the best number to reach you at.

Thanks.

[redacted]

Sent from my iPhone

*Cosmic Lynx email requesting target’s phone number.*

Since the end of December 2020, Cosmic Lynx’s BEC activity has returned to the consistently high volume we saw in early-2020. Since the beginning of 2021, we have observed 43 distinct Cosmic Lynx BEC campaigns targeting executive employees in 19 countries. Since July 2019, we have identified Cosmix Lynx attacks against targets in a total of 53 different countries around the world.

As we noted in our initial Cosmic Lynx report, the entrance of a sophisticated Russian cybercriminal group into the BEC scene shows that actors are realizing that the return on investment for BEC attacks is better than other types of technically sophisticated cyber attacks. Cosmic Lynx has demonstrated the capability to develop much more complex and creative attacks that sets them apart from other BEC groups. To protect against threats like Cosmic Lynx, organizations need to make sure they have defenses in place that are equipped to defend against identity deception attacks that traditional inbound email filters are not equipped to handle.

### Recent Domains Associated with Cosmic Lynx BEC Attacks

email-secure-server[.]cc
email-security-gateway[.]cc
gateway-resolver[.]cc
intranet-gateway[.]cc
intranet-host[.]cc
intranet-server[.]cc
intranetgateway[.]net
intranetserver[.]net

secure-gateway-resolver[.]cc
secure-server-gateway[.]cc
trustnet-secure-server[.]cc
veritas-secure-gateway[.]cc
veritas-secure-host[.]cc

### Recent IP Addresses Linked to Cosmic Lynx Mail Servers

107[.]175[.]38[.]100
107[.]175[.]38[.]108
194[.]5[.]249[.]162
212[.]38[.]166[.]131
212[.]38[.]166[.]35
212[.]38[.]166[.]65
212[.]38[.]166[.]68
23[.]95[.]97[.]33
23[.]95[.]97[.]42
23[.]95[.]97[.]7
23[.]95[.]97[.]8
45[.]79[.]249[.]6
46[.]249[.]59[.]110
46[.]249[.]59[.]111
46[.]249[.]59[.]67
5[.]133[.]179[.]133
5[.]133[.]179[.]65
62[.]182[.]84[.]201
62[.]182[.]84[.]202
93[.]158[.]208[.]104
93[.]158[.]208[.]108
93[.]158[.]208[.]110
94[.]242[.]206[.]17
94[.]242[.]206[.]18
94[.]242[.]206[.]210
94[.]242[.]224[.]203

TAGS

russian bec