



AGARI CYBER
INTELLIGENCE DIVISION

THREAT ACTOR DOSSIER

Cosmic Lynx

The Rise of Russian BEC

AGARI.

© Copyright 2020 Agari Data, Inc.

Executive Summary

“ At some point, Russian and Eastern European cybercriminals are going to start thinking to themselves, ‘Why am I spending all of this time and money setting up infrastructure and hiring malware developers when I can just send someone an email, ask them to send me money, and they’ll do it.’”

For more than a year, this is a line we have used over and over again, expecting that some of the world's most dangerous cybercriminals would move into the world of business email compromise (BEC) because the return on investment for basic social engineering attacks is much higher than more sophisticated malware-based attacks. For the first time, this report shows how these expectations have now become a reality, detailing a Russian criminal organization we call Cosmic Lynx.

We have observed more than 200 BEC campaigns linked to Cosmic Lynx since July 2019, targeting individuals in 46 countries on six continents. Unlike most BEC groups that are relatively target agnostic, Cosmic Lynx has a clear target profile: large, multinational organizations. Nearly all of the organizations Cosmic Lynx has targeted have a significant global presence and many of them are Fortune 500 or Global 2000 companies. The target employees of Cosmic Lynx are senior-level executives. Like other BEC groups, it seems Cosmic Lynx identifies employees to target based on their title. Three quarters of employees targeted by Cosmic Lynx hold the titles of Vice President, General Manager, or Managing Director.

Cosmic Lynx employs a dual impersonation scheme. The pretext of their attacks is that the target organization is preparing to close an acquisition with an Asian company as part of a corporate expansion. First, they impersonate a company's CEO, asking the target employee to work with “external legal counsel” to coordinate the payments needed to close the acquisition. Then, Cosmic Lynx hijacks the identity of a legitimate attorney at a UK-based law firm whose job it is to facilitate the transaction. Cosmic Lynx prefers to use mule accounts in Hong Kong to receive stolen funds. The group is actively resistant to using mule accounts in the United States, but has provided secondary accounts located in Hungary, Portugal, and Romania.

Cosmic Lynx exploits DMARC controls to spoof the email addresses of impersonated CEOs, making their attacks appear much more authentic. For organizations that have implemented an established DMARC policy set to reject (*p=reject*) or quarantine (*p=quarantine*), Cosmic Lynx modifies the display name impersonating a CEO to include their email address, which still gives it the look that the email is coming from the CEO's account.

Domains registered by Cosmic Lynx are named in a way to mimic secure email and network infrastructure (e.g., *secure-mail-gateway[.]cc*, *encrypted-smtp-transport[.]cc*, *mx-secure-net[.]com*). The mailbox referenced in a Cosmic Lynx email address usually references celestial bodies, like planets and stars--hence the “Cosmic” in Cosmic Lynx-- similar to the naming convention of some SMTP or DNS name servers.

To make their infrastructure more resilient and mask their identity in Whois records, Cosmic Lynx has registered a number of their domains with NiceVPS, a bulletproof hosting and anonymous domain provider. Cosmic Lynx's infrastructure has also been linked to other types of malicious activity, including Emotet and Trickbot banking Trojans, Android click fraud malware, a popular carding marketplace, and Russian fake document websites.

Table of Contents

The Missing Lynx

Inside a Cosmic Lynx Attack

4

A Global Threat

A Look at Cosmic Lynx's Targets

9

Hitting D-MARC

How Cosmic Lynx Exploits DMARC Controls

11

Exploiting a Pandemic

How Cosmic Lynx Has Leveraged COVID-19 in Their Attacks

13

Putting the “Cosmic” in Cosmic Lynx

A Look at Cosmic Lynx's Operational Infrastructure

16

Who is Cosmic Lynx?

Exposing Cosmic Lynx's Russian Origin

21

Conclusion

24

Appendix A

Domains Used in Cosmic Lynx BEC Attacks

25

Appendix B

IP Addresses Associated with Cosmic Lynx Mail Servers

26

Appendix C

Email Subject Lines Used in Cosmic Lynx BEC Campaigns

27

The Missing Lynx

Inside a Cosmic Lynx Attack

Every single day, researchers in the Agari Cyber Intelligence Division (ACID) engage with dozens of BEC scammers who have tried (and failed) to target Agari customers. In doing so, we collect rich intelligence that allows us to better understand cybercriminal group operations, uncover the identities of those involved in the criminal schemes, discover and track the evolution of their methods over time, and unravel the financial infrastructure they use to launder stolen proceeds.

Over the last year, ACID has identified more than 200 BEC campaigns targeting businesses all over the world that are attributed to a sophisticated group of BEC actors we refer to as “Cosmic Lynx.” This report details the tactics used by the group as well as our assessment about the attribution of the group’s location.

The pretext used in nearly all Cosmic Lynx BEC attacks is that the company is preparing to close an acquisition with an Asian company as part of corporate expansion. Impersonating the company’s CEO, Cosmic Lynx asks the target employee to work with “external legal counsel” to coordinate the payments necessary to close the acquisition. Of course, due to the sensitive nature of this acquisition, the target employee is asked to keep the details of this transaction confidential until it has been finalized.

From	<secure-mercury@secure-mx-service.cc>	☆
Subject	Matter with law firm	
To	Cheryl	☆
Cheryl,		
<p>There is a time-sensitive corporate matter that needs to be resolved with our appointed law firm by the close of this week. I would like to entrust it to you.</p> <p>Please let me know soonest by email if you can handle this and I will fill you in on the details.</p> <p>Regards,</p> <p>[REDACTED]</p>		
Sent from my iPhone		

Example initial email from Cosmic Lynx.

One of the first things that stands out in a Cosmic Lynx attack is that they are extremely well-written. Unlike most BEC emails that are riddled with misspelled words and grammatical errors, Cosmic Lynx emails are usually very detailed and written in nearly perfect English. In some cases, Cosmic Lynx uses words that are likely not in most people's vocabulary, like "accretive" and "synergistic," and uses them in their proper context. It should be noted that although Cosmic Lynx's targets are located all over the world, nearly all of the emails sent by the group are written in English. The only exception to this we have identified were a handful of emails written in French that were sent to a few targets in France.

From <smtp-uranus@email-gateway-host.cc> ☆
Subject Project Rubicon
To Fred ☆
5/6/20, 4:50 PM

Fred,

I hope this message finds you safe, healthy and staying positive in the wake of the COVID-19 crisis that has turned our world upside down.

While we focus on addressing on the immediate safety and business concerns during this challenging period, we must also look beyond and be ready to pounce on the economic rebound as countries around the world begin to ease the lockdown, businesses reopen and normalcy gradually returns.

In the midst of this crisis, value accretive opportunities are abound and we have been actively looking out for them. After careful due diligence, we have decided to acquire the synergistic assets of a foreign company.

I will require you to assist and support our legal team as we now embark on the closing phase of this acquisition.

For confidentiality reasons, the transaction shall be referred to as "Project Rubicon". This is a highly sensitive matter and I need to count on your discretion.

Please let me know soonest by email if you can handle this and I will fill you in on the specifics.

Best regards,

Sent from my iPhone

Once the "CEO" has introduced the request to the target employee, the next step in a Cosmic Lynx attack is to introduce the "lawyer" that will be assisting with the payments for the fake acquisition. The "lawyer" generally introduces himself in a separate email and gives the target a general overview of how the transaction will proceed.

This is where Cosmic Lynx deploys their second round of impersonation. Instead of developing an independent legal persona, Cosmic Lynx hijacks the identities of real attorneys at high-profile law firms to add another layer of legitimacy to their attack. Nearly all of the attorneys impersonated by Cosmic Lynx are based in the United Kingdom.

From **M&A By** No: CC261013
Subject **To Jane** 4/22/20, 1:54 PM

Privileged & Confidential

Dear Jane [REDACTED],

Please allow me to introduce myself and my firm.

I am [REDACTED], am in charge of M&A for [REDACTED].

Our firm has been retained by [REDACTED] to assist in the acquisition of all assets of a southeast Asia based company.

[REDACTED] has informed me that you will be our contact and will be assisting us in all matters pertaining to this acquisition

According to the terms & agreements signed by the senior executive of your Group who appointed you to handle this case, at the moment you are the only one involved.

Terms & Conditions

Upon receipt of this mail, following the NDA No 2512 signed by the different parties involved, all correspondences relating to this matter will be classified and registered under the case No: CC261013.

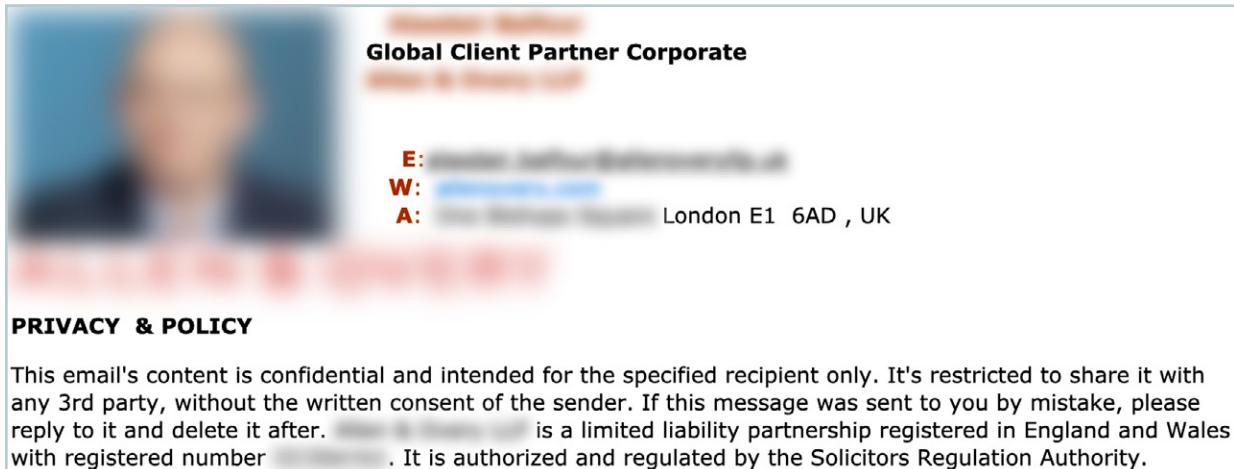
Any disclosures concerning this operation before the official announcement could result in the cancellation of the offer by the Markets Authority. You cannot involve a third party without our prior consent or disclose any information relating to this matter by any means of communication other than this mailbox.

Kind Regards

Introductory email from the “lawyer” in a Cosmix Lynx attack.

Cosmic Lynx employs two strategies to make communications from the impersonated lawyer more convincing. First, the group registers a domain that closely resembles the law firm's actual domain and create an email address on this domain to communicate with a target. For example, if an attorney's real email address is john.doe@lawfirm.com, Cosmic Lynx would create an account like john.doe@lawfirmllp.com to communicate with an employee.

Second, to mimic the impersonated attorney's communication patterns as closely as possible, Cosmic Lynx creates a detailed email signature that contains a picture of the impersonated lawyer, a link to the legitimate law firm's website, and a confidentiality disclaimer. An analysis of the signatures indicates they are likely created using a freely available online signature generator. The attorney's photo is copied directly from the law firm's actual website.



"Lawyer" signature in Cosmic Lynx email.

The final phase of a Cosmic Lynx BEC attack is getting the target employee to send one or more payments to mule accounts controlled by the group. A characteristic of Cosmic Lynx attacks that sticks out is the amount of money they request. The average amount requested in most executive impersonation BEC attacks is [\\$55,000](#). Cosmic Lynx, on the other hand, asks for hundreds of thousands, sometimes millions of dollars.

Based on our engagements with the group, it is clear their preference is to have a target send payments to mule accounts located in Hong Kong, which has become a common source of international mule accounts over the past few years. In every successful engagement we have initiated with Cosmic Lynx, the initial mule account they have provided to us has been located in Hong Kong.

To better understand how a BEC threat actor will adapt, we commonly give them reasons why a payment to their first mule account is not possible. In typical cases, BEC actors who originally provide an international bank account will follow up with a secondary mule account that is located in the US or the same country as the target. For Cosmic Lynx, though, they seem to be consciously resistant to provide mule accounts in certain countries, like the US. Even when we give them no other options, the group actively refuses to disclose mule accounts in the US. This could mean that either the group does not have a supply of mules in the US or for other reasons, they prefer not to use bank accounts in the US to receive illicit funds. Outside Hong Kong, secondary accounts provided by Cosmic Lynx have been located in Hungary, Portugal, and Romania.

From [REDACTED] ☆
Subject Re: M&A By [REDACTED] 5/7/20, 8:17 AM
To Andy [REDACTED] ☆

Privileged & Confidential

Dear Andy [REDACTED],

Thank you for the information, Regarding the financial transaction and your daily limits you can proceed with the amount of \$1,555,770 USD Before cut off time today. It will be great if you could split up the rest with your others resources and do it before cut off time today as well after the first installment.

Please forward me the attached once you've completed the first payment and i will give you the rest of the instructions.

-Below are the recipient details:

BENEFICIARY NAME: [REDACTED]

BENEFICIARY ADDRESS: [REDACTED] SAN PO
KONG KLN HONG KONG

BENEFICIARY BANK: [REDACTED]

BANK ADDRESS: [REDACTED], KOWLOON

BANK CODE: [REDACTED]

ACCOUNT NUMBER : [REDACTED]

SWIFT: [REDACTED]

AMOUNT :\$1,555,770 US DOLLARS

According to the terms & agreements signed by the senior executive of your Group who appointed you to handle this case, at the moment you are the only one involved.

Initial mule account provided in Cosmic Lynx attack.

A Global Threat

A Look at Cosmic Lynx's Targets

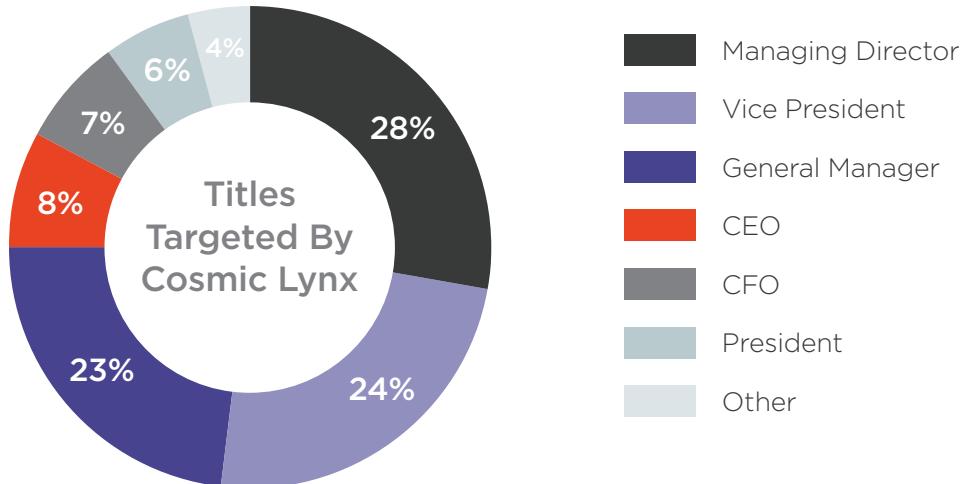
Typical BEC groups tend to be agnostic when selecting targets for their attacks. They are more interested in identifying employees who have access to money, regardless if they work for a small, five-person company or an organization with thousands of employees. In contrast, Cosmic Lynx has a clear target preference: large, multinational organizations. Nearly all of the target organizations we have identified have a global presence and many of them are Fortune 500 or Global 2000 companies. These target organizations are headquartered in 20 countries; however, because most of the organizations are global, employees targeted by Cosmic Lynx BEC campaigns are located in 46 countries on six continents. Even employees in countries not typically seen in phishing campaign targeting sets, like Namibia and Mongolia, were targeted by Cosmic Lynx.



Map of Cosmic Lynx targets.

To identify employees to target with BEC attacks, groups generally use legitimate commercial services that allow them to conduct a finely tuned search for employees based on a number of variables, such as title, location, and company revenue. Based on a review of employees targeted by Cosmic Lynx, it is clear that they are using a similar service to identify targets specifically by their title.

All of the employees targeted in Cosmic Lynx BEC campaigns are senior-level employees at a company. Three quarters of employees targeted hold the titles of Vice President, General Manager, or Managing Director at a company. Other positions explicitly targeted by Cosmic Lynx include CEO (generally, subsidiary or country-level CEOs), CFO, and President. Because Cosmic Lynx is focused on large, global companies, another interesting aspect of their attacks is that they rarely target employees multiple times. Instead, they will target employees with the same title at a company located in different countries.



Hitting D-MARC

How Cosmic Lynx Exploits DMARC Controls

The [DMARC](#) standard was created to prevent malicious actors from directly spoofing an organization's domain when sending an email. The standard was published in 2012 and allows organizations to authenticate legitimate email messages and sources for their email-sending domains and publish explicit policies that instruct mailbox providers what to do with inauthentic messages. The most aggressive DMARC policy is "reject" ($p=reject$), which means that email messages that do not pass DMARC authentication will be rejected by a mail server and not delivered to a user. In essence, with an effective DMARC policy at reject, cybercriminals are not able to directly spoof an organization's domain.

While spoofed domains can be used to create very realistic-looking phishing emails, very few BEC attacks leverage spoofed domains. In our latest quarterly [Email Fraud & Identity Deception Trends report](#), we found that 96% of all BEC attacks used free webmail accounts or registered domains to send malicious emails.

Cosmic Lynx, though, is part of the 4% of attacks to exploit organizations that do not have an established DMARC policy. This enhances the authenticity of their emails by directly spoofing the email addresses of CEOs when possible. Based on our analysis of historical Cosmic Lynx attacks, it is clear that the group is aware of which target organizations have implemented an effective DMARC policy and which organizations have not.

If a company has not implemented a DMARC policy or has a policy set to monitor-only ($p=none$), Cosmic Lynx will directly spoof the CEO's email address and set the Reply-To email to their operational email account they use to actually correspond with a victim. If an organization has an established DMARC policy set to reject or quarantine ($p=quarantine$), Cosmic Lynx will not spoof the sending email address. Instead, the group changes the display name impersonating the CEO to include their email address, which still gives the look that the email is coming directly from the CEO's account (e.g., "John Smith - jsmith@acme.com").



From ☆
Subject Resolve matter with law firm 1/16/20, 9:57 AM
Reply to <secure-uranus@secure-mx-gateway.cc>☆
To Scott ☆

Scott,

I'm following up with you regarding the email I sent to you previously about the corporate matter with our appointed law firm.

This matter needs to be resolved within the next few days and I would like you to be in charge of it.

Please let me know soonest by email if you can handle this and I will provide more details.

Regards,

Sent from my iPhone

From ☆
Subject Law firm matter <secure-neptune@mx-gateway-host.cc>☆ 3/18/20, 4:38 AM
To ☆

Lars,

We are working on a corporate matter with our appointed law firm and a time-sensitive issue has arisen that needs to be resolved promptly.

As there are regulatory and stakeholders' concerns to be addressed, it must be sorted out by close of business tomorrow and I would like you to take charge.

Please reply me soonest by email if you can handle this and I will fill you in on the specifics.

Regards,

Sent from my iPhone

Spoofed (top) vs. non-spoofed (bottom) Cosmic Lynx emails.

Exploiting a Pandemic

How Cosmic Lynx Has Leveraged COVID-19 in Their Attacks

Phishing attacks exploiting the COVID-19 pandemic started to skyrocket in March 2020. Malware campaigns, [credential phishing lures](#), and [BEC attacks](#) all started adopting COVID-19 themes as a way to increase the success rate of their attacks. Cosmic Lynx was no different.

In late-March, the group began inserting language referencing the pandemic into their BEC campaign emails as a social-engineering icebreaker that preceded their main request. Because COVID-19 has impacted nearly everyone in the world, it afforded Cosmic Lynx an opportunity to disarm a target's suspicions by building rapport with them at the beginning of an initial email regardless of where the target was located. Some of the pandemic-themed content used by Cosmic Lynx included the following:



The COVID-19 pandemic is a truly unprecedented situation which affects us all but we are doing everything possible to provide a safe working environment to our people, and to minimize its negative impact on our business.



With the unpredictable and fluid situation around COVID-19, the world is navigating through an uncertain period with few precedents. We are deeply concerned about the pandemic's impact on our business and our employees' health and have rolled out several mitigation measures.



I trust this emails (sic) finds you safe and well. The current situation with the COVID-19 virus has all of us worried.

As the peak of the pandemic passed for most countries by late-May, Cosmic Lynx shifted their tone and began referencing the reopening of global economies as an introduction to their emails. Like the earlier references to COVID-19, these introductions are meant to get a target to put down their defenses before the Cosmic Lynx actor gets to what they really want. Some of the introductions used by Cosmic Lynx after the COVID-19 peak included the following:



As the world emerges from lockdown restrictions, we are cautiously optimistic that the worst is finally behind us.



"As countries around the world gradually ease lockdown restrictions and companies resume business, we must now look beyond the crisis and position ourselves for the economic recovery."



"The last many weeks have been very challenging but the worst is most likely over as normalcy is gradually returning with countries easing restrictions. We anticipate a robust rebound in the economy and are seizing the opportunity to further develop our business."

Prior to the global rise of COVID-19, Cosmic Lynx's emails were rather generic, which makes their pivot to pandemic themes that much more notable. Like many cybercriminals out there, this indicates they are savvy enough to pay attention to global events and adapt their attacks to exploit them.



From <tls-sirius-net@mx-gateway-host.cc> ☆
Subject Potential corporate transaction 4/20/20, 7:27 AM
To ☆

Allan,

I certainly hope this email finds you well. With the unpredictable and fluid situation around COVID-19, the world is navigating through an uncertain period with few precedents. We are deeply concerned about the pandemic's impact on our business and our employees' health and have rolled out several mitigation measures.

As we brace for further disruptions during this uncertain period, we must also seize the opportunity to prepare for the eventual business recovery once the crisis abates.

We have thus embarked on a major project which involves our legal team and bankers and I will require your assistance and support.

This matter requires strict confidentiality and I need to count on your discretion. Please let me know by email if you can handle this.

Regards,

Sent from my iPhone

From <smtp-neptune@mail-transport-protection.cc> ☆
Subject Project Cyclone 6/9/20, 5:52 PM
To ☆

Dear Maria,

I hope all is well.

As countries lift restrictions, normalcy is gradually returning and we are hopeful that the worst is over.

Within every crisis, the seeds of opportunity are sowed. I am pleased to share that we are seizing the moment and are pressing ahead to acquire the assets of a distressed company. Our legal team is currently working on closing the transaction and I need you to work closely with them on certain time-sensitive issues.

We have named this acquisition "Project Cyclone". This is a highly sensitive and confidential matter and I would appreciate your discretion.

Please let me know soonest by email if you can assist and I will provide further instructions.

Cheers,

Sent from my iPhone

Examples of COVID-19-themed Cosmic Lynx emails.

Putting the “Cosmic” in Cosmic Lynx

A Look at Cosmic Lynx’s Operational Infrastructure

Attacker infrastructure is another one of the key differences between Cosmic Lynx and other BEC groups. While most BEC actors tend to gravitate to free webmail accounts or remotely-hosted cloud services, Cosmic Lynx consistently chooses to host their own email infrastructure with a small number of hosting providers. By hosting, managing, controlling, and running their own email infrastructure, Cosmic Lynx is able to be more resistant to law enforcement operations which may target their campaigns.

Putting the “Cosmic” in Cosmic Lynx

Email addresses created by Cosmic Lynx to send their campaigns seem to mimic secure email and network infrastructure. The mailbox referenced in a Cosmic Lynx email address (the part of an email address before the "@") usually references celestial bodies, like planets and stars--hence the “Cosmic” in Cosmic Lynx--similar to the naming convention of some SMTP or DNS name servers. Examples of these mailbox names include “smtp-mars,” “mx-taurus,” “tls-sirius,” and gateway-mercury.”

Similarly, domains registered by Cosmic Lynx are named in a way to impersonate secure email infrastructure (e.g., secure-mail-gateway[.]cc, encrypted-smtp-transport[.]cc, mx-secure-net[.]com). In some cases, Cosmic Lynx has referenced Fortinet, a US-based cybersecurity that offers endpoint security and secure email gateway products, in their domains (e.g., fortinet-host-protection[.]cc, fortinet-server[.]cc, fortinet-gateway[.]cc).

See Appendix A for a full list of domains linked to Cosmic Lynx attacks.

Manipulating Email Flow, Not Just for Email Engineers

Most BEC actors simply purchase a domain or use a free webmail account, with attackers frequently cycling through accounts and domains as they’re taken down. Cosmic Lynx purchases domains too; however, they put much more work and effort into securing the infrastructure from outsiders investigating the domains.

Cosmic Lynx makes heavy use of DNS MX records for their email accounts to manipulate mail flow. After Cosmic Lynx registers their domain for a specific campaign, the attackers point the top-level domain (TLD) at Cloudflare to make the domain appear more legitimate. Next, the attackers create a subdomain to use as the MX record, or the place where emails will be sent and delivered. By modifying the IP address that the subdomain is pointing to, Cosmic Lynx is able to point part of the domain at seemingly legitimate infrastructure, while running scams under the subdomain.

This is a key differentiator when comparing traditional BEC actors and Cosmic Lynx, as true understanding of how email flow and editing DNS records is a skill that far exceeds traditional BEC actors.

DMARC: Not Just for the Good Guys

While Cosmic Lynx is more than happy to spoof email infrastructure to target an organization with a BEC attempt, the attackers aren't fans of having someone else spoof their infrastructure. Cosmic Lynx is able to monitor for any attempts at spoofing their domain by using properly-configured DMARC policies on their domain infrastructure. In a vast majority of cases, Cosmic Lynx DMARC domains are configured to send spoofs to abuse@[domain], with variations including legal@[domain] and dmarc@[domain]. By using these email accounts, not only does Cosmic Lynx receive a copy of any person trying to spoof them, but they could fool unsuspecting users into reporting fraud attacks to them, too.

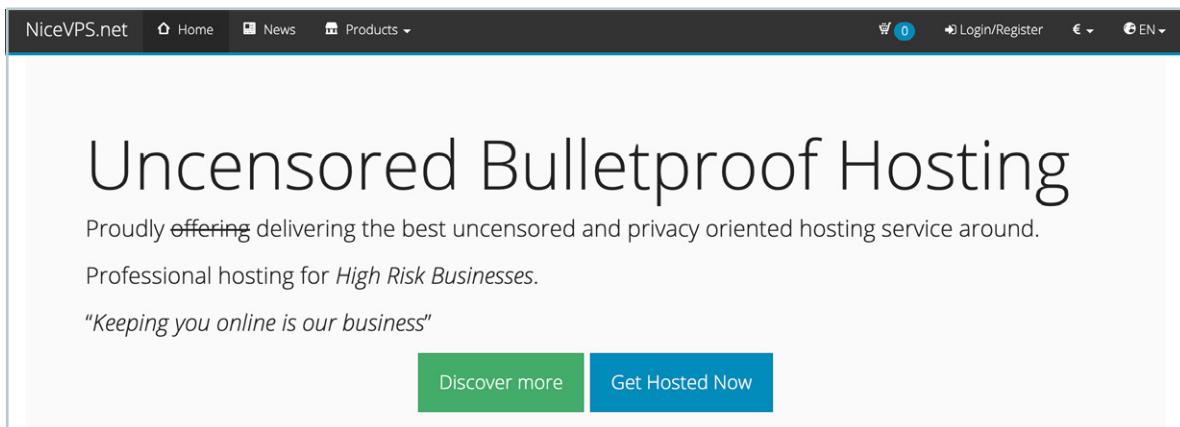
Additionally, if DMARC is not enabled, anyone is able to spoof the origins of the sending domain. By having this security feature disabled, spam bots and other parties are able to piggy-back on the reputation of the sending domain, which would negatively impact the reputation of the sending domain. In the case of Cosmic Lynx, their entire existence in the BEC space relies on emails landing in the inboxes of users, and if their delivery domains have poor Senderbase Reputation Scores (SBRs), most security appliances will refuse or flag these emails as being suspicious.

```
"v=DMARC1; p=reject; rua=mailto:abuse@mail-transport-agent.cc"
"v=DMARC1; p=reject; rua=mailto:abuse@mail-transport-gateway.cc"
"v=DMARC1; p=reject; rua=mailto:abuse@mail-transport-host.cc"
"v=DMARC1; p=reject; rua=mailto:dmarc@mx-gateway-host.cc"
"v=DMARC1; p=reject; rua=mailto:abuse@mx-secure-email-server.cc"
"v=DMARC1; p=reject; rua=mailto:abuse@mx-secure-net.com"
"v=DMARC1; p=reject; rua=mailto:abuse@node-protection.cc"
"v=DMARC1; p=reject; rua=mailto:abuse@secure-email-delivery.cc"
"v=DMARC1; p=reject; pct=100; rua=mailto:dmarc-abuse@secure-email-provider.cc"
"v=DMARC1; p=reject; rua=mailto:abuse@secure-mail-gateway.cc"
```

Cosmic Lynx DMARC policies.

Fortifying Infrastructure with Bulletproof Hosting

In order to make their infrastructure more resilient and mask their identity in WHOIS records, Cosmic Lynx has registered a number of their domains with NiceVPS, a bulletproof hosting and anonymous domain provider. Based on a review of other domains registered with NiceVPS, it is clear that the service caters to cybercriminals.



The screenshot shows the NiceVPS.net website. At the top, there's a navigation bar with links for Home, News, Products, a login/register button, and language selection (EN). The main heading is "Uncensored Bulletproof Hosting". Below it, a sub-headline says "Proudly offering delivering the best uncensored and privacy oriented hosting service around." followed by "Professional hosting for *High Risk Businesses*". A quote "Keeping you online is our business" is also present. At the bottom of the main section are two buttons: "Discover more" (green) and "Get Hosted Now" (blue).

NiceVPS homepage.

Instead of using basic Whois privacy when registering a domain, NiceVPS registers a domain on their customers' behalf with their anonymous domain name service, adding an additional layer of anonymity between the domain and Cosmic Lynx. Instead of showing masked registrant details, a domain's Whois record will just show contact details for NiceVPS, under the organization name "Nice IT Services Group Inc." NiceVPS also does not require registrants to provide any personal information when registering a domain and purchases can be made using bitcoin, making it even harder to track someone's identity.



The screenshot shows a service offer for "Anonymous Domains". It features a yellow background with the title "Anonymous Domains" and the subtitle "Confidential domain ownership service". A bulleted list of benefits includes: ✓ Highest confidentiality - 100% Anonymous, ✓ Managed DNS Hosting, ✓ DNSSEC Support, ✓ Domain and email forwarding, and ✓ Glued name-servers support. Below this, the price is listed as "Starting from €4.99 per year". At the bottom is a green button labeled "Register Bitcoin Domain".

Anonymous domain service from NiceVPS.

To make the infrastructure more friendly for scammers, NiceVPS makes use of a warrant canary, which will let users know if information has been subpoenaed or requested by law enforcement. If the warrant canary is not updated after a pre-determined period of time, this will tip the users of the infrastructure off that law enforcement intervention may be happening, giving attackers time to react and clean up their tracks.

The screenshot shows the NiceVPS.net website with a blue header bar. The header includes links for Home, News, Products, a shopping cart icon with '0', a Login/Register button, and language selection for EN. The main content area has a title 'Warrant Canary' and a breadcrumb navigation 'HOME / CANARY'. Below this, a statement in a box claims the service is safe and lists update dates: February 1, May 1, August 1, and November 1.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: RIPEMD160

NiceVPS confirms that our service IS SAFE to be used normally and has not received any undemocratic court order or secret subpoena.

This statement will be updated approximately on the following dates:
* February 1
* May 1
* August 1
* November 1
```

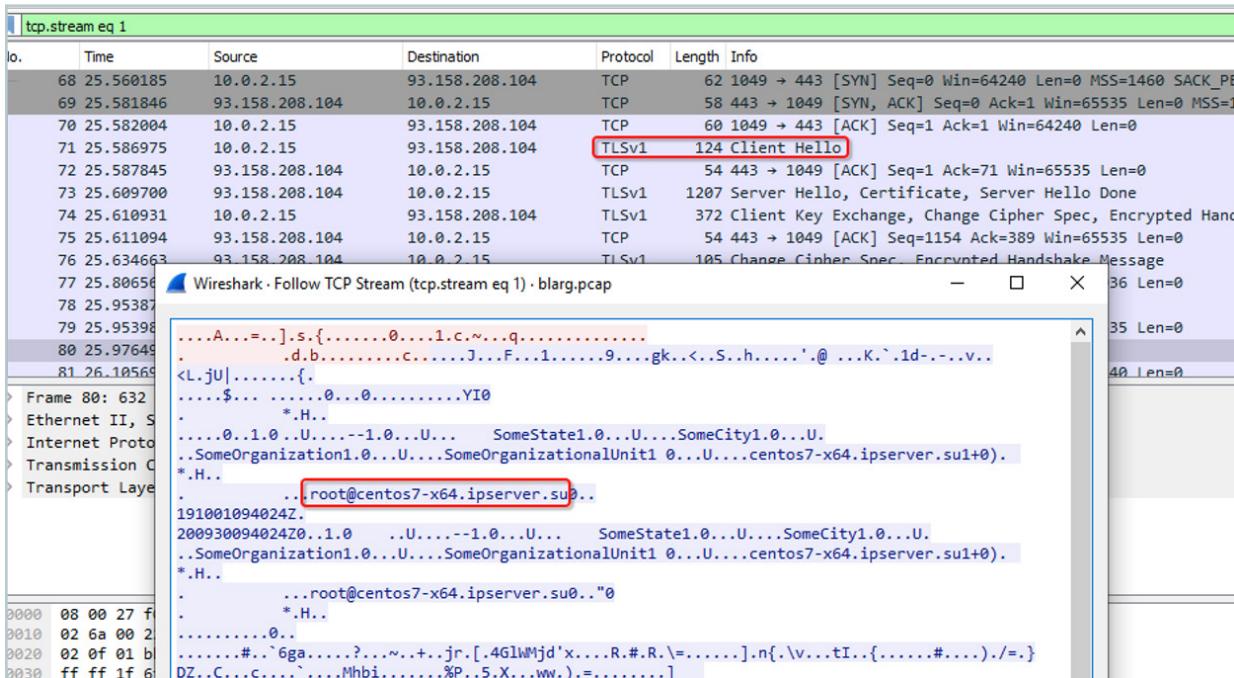
NiceVPS warrant canary message.

Trickbot, Emotet, and BEC...Oh My!

One of the more notable aspects of Cosmic Lynx's BEC infrastructure is its links to other types of malicious activity, particularly malware infrastructure. Because Cosmic Lynx controls their infrastructure so closely, this may indicate deeper connections to the criminal underground that have not been observed by previous BEC actors.

Between December 2019 and April 2020, two of Cosmic Lynx's mail servers, vmc[.]fortinet-protection[.]cc and cx[.]fortinet-gateway[.]cc, were hosted on IP address 46[.]249[.]62[.]202. This time frame overlaps with two other domains, adsclubpartners[.]ru and 00xff[.]net, hosted at this IP address that were used to host configuration files for Russian [click fraud malware](#) targeting Android mobile devices.

Between December 2019 and January 2020, one of Cosmix Lynx's mail servers, vs[.]secure-mx-gateway[.]cc, was hosted on IP address 93[.]158[.]208[.]104. In October 2019, two months prior to Cosmic Lynx infrastructure pointed to the IP address, a sample of Trickbot, one of today's most active banking Trojans, was seen making SSL connections to this IP address, indicating this address may have been used as a command and control (C2) server.



PCAP of Trickbot sample connecting to 93[.]158[.]208[.]104 (Source: VirusTotal).

Between March 2020 and April 2020, one of Cosmic Lynx's mail servers, mail[.]mx-secure-net[.]com, was hosted on IP 139[.]162[.]120[.]155. Between October and December 2019, multiple malicious word documents linked to the Emotet banking Trojan were observed being downloaded from the IP address.

Between January 2020 and February 2020, one of Cosmic Lynx's mail servers, vs[.]mx-gateway-host[.]cc resolved to IP address 46[.]249[.]59[.]67. Around June 2019, this IP address was hosting Azorult malware, which is capable of stealing chat messages, browser history, and financial information. Between March 2019 and October 2019, this IP address also hosted mrgreen[.]ws, a carding marketplace that has been in operation since 2014.

Malware authors and other cybercriminals frequently cycle through infrastructure and in some cases, infrastructure is used for a single attack or campaign, so we cannot link Cosmic Lynx actors to these other malicious activities directly. Associations to infrastructure connected to more sophisticated malicious activity across multiple service providers is notable, though, because we generally do not see these types of links with other BEC groups.

Who is Cosmic Lynx?

Exposing Cosmic Lynx's Russian Origin

Historically, a vast majority of BEC attacks have [originated from actors in Nigeria](#). Looking at Cosmic Lynx's attacks, though, it is clear they are a different breed than other active cybercriminal groups conducting BEC operations. Our assessment finds that Cosmic Lynx is likely composed of Russia-based actors, based on analysis of their attacks and infrastructure.

The first piece of evidence that ties back to a Russian nexus is the time/date stamp in the email headers of some of the Cosmic Lynx attacks. Generally, the Date field in an email header reflects the time and date an email was sent and usually includes a UTC offset. While this UTC offset can be modified by either the sender or routing infrastructure, in many cases this offset will reflect the time zone of the sender. For many of the Cosmic Lynx attacks we have analyzed, the UTC offset in the email headers are set to +0300 (MSK), which corresponds to Moscow Standard Time. Moscow Standard Time is only observed in the eastern parts of Russia, as well as Belarus and very small parts of Georgia and Ukraine. Since none of the routing infrastructure used by Cosmic Lynx or their targets are located in Russia, and it is unlikely an actor would spoof an MSK offset, we assess that this is the likely time zone of the sender(s) of these messages.

```
Date: Tue, 5 May 2020 01:05:28 +0300 (MSK)
From: <gateway-atlas@encrypted-host.cc>
To:
Message-ID: <2017797638.3.1588629928227@[REDACTED]
Subject: Project Indigo
```

Cosmic Lynx email header with Moscow Standard Time UTC offset.

As we discussed earlier, some of the infrastructure used by Cosmic Lynx to send BEC emails overlaps with infrastructure used by Trickbot and Emotet malware, which is believed to be tied to Russian actors. In addition to these potential connections, we have also observed multiple instances where IP addresses linked to Cosmic Lynx's BEC domain have overlapped with infrastructure used to host Russian fake document websites. These sites, which seem to be catering to individuals in Russia and Ukraine, sell a variety of false Russian-language documents, such as diplomas, birth certificates, and death certificates.

Информация
Преимущества
Доставка

Мой документ
мы знаем, как важно иметь правильный документ

+7(925)629-61-57
info@diplomssale.com

Соцсети:

ДИПЛОМЫ » АТТЕСТАТЫ СВИДЕТЕЛЬСТВА СЕРТИФИКАТЫ СПРАВКИ УДОСТОВЕРЕНИЯ ЗАКАЗАТЬ

АТТЕСТАТЫ

о среднем (полном) общем образовании (11 классов)
о неполном среднем образовании (9 классов)

ОРИГИНАЛЬНЫЙ БЛАНК

Мы используем только оригинальные бланки Гознак, Спецбланк, такие же, как выдают в учебных и других организациях.

БОЛЬШОЙ ОПЫТ

Мы работаем более 20 лет на рынке изготовления документов. Знания и опыт необходимы для правильного заполнения документов.

КАЧЕСТВО

Все документы выполнены на самом современном оборудовании, с учетом всех правил изготовления защищенной продукции.

САМЫЕ ПОПУЛЯРНЫЕ ДОКУМЕНТЫ

Смотреть все

- Аттестат о среднем образовании РСФСР 1993
- Справка об обучении в ВУЗе, колледже, техникуме, школе
- Аттестат о среднем (полном) общем образовании 1994-2006
- Аттестат об основном общем образовании 2014-2019 (9 классов)
- Украинский диплом магистра образца 2011-2013 года
- Свидетельство о рождении

Screenshots from Russian fake document website linked to Cosmic Lynx infrastructure.

The final piece of evidence pointing to Russian attribution comes from the metadata of documents sent by Cosmic Lynx in some of their BEC attacks. During one of our engagements with Cosmic Lynx, they sent us a document containing wire transfer instructions for a payment, as well as a fake non-disclosure agreement. A review of the metadata of these documents shows they were last saved by user "Serge Devant" prior to being sent to us. Serge Devant is the name of a DJ from Saint Petersburg, Russia. While the name of this user can be easily changed to reflect any name, using the name of a Russian DJ, regardless of whether it is legitimate or not, is notable. It should be noted that we have no evidence that the real Serge Devant is associated with Cosmic Lynx activity.

NON-DISCLOSURE AGREEMENT

Page 1/3

Monday, 18th May 2020

THIS AGREEMENT is made between:

1. [REDACTED]
2. [REDACTED]

RECITALS

A. The Receiving Party understands that the Disclosing Party has disclosed or may disclose information relating to [REDACTED] matter, which to the extent previously, presently, or subsequently disclosed to the Receiving Party is hereinafter referred to as "Proprietary Information" of the Disclosing Party.

OPERATIVE PROVISIONS

1. In consideration of the disclosure of Proprietary Information by the Disclosing Party, the Receiving Party hereby agrees: (i) to hold the Proprietary Information in strict confidence and to take all reasonable precautions to protect such Proprietary Information (including, without limitation, all precautions the Receiving Party employs with respect to its own confidential materials), (ii) not to disclose any such Proprietary Information or any information derived therefrom to any third person, (iii) not to make any use whatsoever at any time of such Proprietary Information except to evaluate internally its relationship with the Disclosing Party, and (iv) not to copy or reverse engineer any such Proprietary Information. The Receiving Party shall procure that its employees,

Created: Wednesday, August 14, 2019 at 11:13 AM
Modified: Thursday, June 11, 2020 at 10:50 AM
Printed: Wednesday, August 14, 2019 at 11:14 AM
Last saved by: Serge Devant
Revision number: 6
Total editing time: 2 Minutes

Fake Cosmic Lynx NDA and metadata with references to Serge Devant.

While none of these pieces of evidence on their own would warrant a solid attribution case, we believe looking at the totality of evidence together builds a strong circumstantial argument that some, if not all, Cosmic Lynx actors are based in Russia.

Conclusion

Business email compromise has become the predominant cyber threat businesses face today. Since 2016, businesses have lost at least [\\$26 billion](#) as a result of BEC attacks and, based on the most recent [FBI IC3 report](#), losses from BEC attacks grew another 37 percent in 2019, accounting for 40 percent of all cybercrime losses over the course of the year. Evidence that more sophisticated threat groups are adding BEC to their attack repertoire should concern everyone. Unlike traditional BEC groups, Cosmic Lynx has demonstrated the capability to develop much more complex and creative attacks that sets them apart from other more generic BEC attacks we see everyday.

To protect against threats like these, organizations first need to understand and accept the state of today's cyber threat landscape. Most email-based threats today, like BEC attacks, are very simple social engineering attacks that are technically unsophisticated. To effectively protect against these threats, companies need to make sure they have defenses in place that are equipped to detect identity deception attacks that traditional inbound filters are not accustomed to handling. Additionally, organizations should have good internal processes in place, so payment requests, regardless of source, are verified before they are processed.

Since 2016, businesses have lost at least

\$26B

as a result of BEC attacks

losses from BEC attacks grew another

37%

in 2019, accounting for

40%

of all cybercrime losses over the course of the year

Appendix A:

Domains Used in Cosmic Lynx BEC Attacks

cloud-front-gateway[.]cc	secure-email-server[.]cc
confidential-privileged[.]com	secure-email-server[.]net
email-gateway-host[.]cc	secure-email-service[.]com
encrypted-gateway[.]cc	secure-mail-cast[.]com
encrypted-host[.]cc	secure-mail-gateway[.]cc
encrypted-mail-gateway[.]cc	secure-mail-host[.]cc
encrypted-mail-server[.]com	secure-mail-host[.]com
encrypted-network[.]cc	secure-mail-net[.]cc
encrypted-smtp-transport[.]cc	secure-mail-net[.]com
eu-1-host-protection[.]cc	secure-mail-provider[.]cc
fortinet-gateway[.]cc	secure-mail-provider[.]com
fortinet-host-protection[.]cc	secure-mail-server[.]cc
fortinet-host[.]cc	secure-mx-gateway[.]cc
fortinet-protection[.]cc	secure-mx-host[.]com
fortinet-server[.]cc	secure-mx-provider[.]cc
mail-transport-agent[.]cc	secure-mx-server[.]cc
mail-transport-gateway[.]cc	secure-mx-service[.]cc
mail-transport-host[.]cc	secure-server-smtp[.]cc
mail-transport-protection[.]cc	secure-smtp-delivery[.]cc
mx-gateway-host[.]cc	secure-smtp-gateway[.]cc
mx-secure-email-host[.]cc	secure-smtp-host[.]cc
mx-secure-email-server[.]cc	secure-smtp-host[.]com
mx-secure-net[.]com	secure-smtp-provider[.]cc
node-protection[.]cc	secure-smtp-server[.]cc
privileged-secured[.]com	secure-smtp-server[.]com
relay-secure-smtp[.]com	secure-smtp-service[.]cc
secure-email-delivery[.]cc	secure-smtp-service[.]com
secure-email-gateway[.]cc	secure-ssl-sec[.]com
secure-email-host[.]cc	smtp-gateway-host[.]cc
secure-email-host[.]com	smtp-secure-gateway[.]cc
secure-email-net[.]cc	smtp-secure-service[.]cc
secure-email-provider[.]cc	smtp-server-relay[.]com
secure-email-provider[.]com	

Appendix B:

IP Addresses Associated with Cosmic Lynx Mail Servers

5[.]133[.]179[.]37	94[.]242[.]206[.]166
5[.]133[.]179[.]43	94[.]242[.]206[.]195
5[.]133[.]179[.]55	94[.]242[.]206[.]204
23[.]95[.]97[.]12	94[.]242[.]206[.]210
23[.]95[.]97[.]19	94[.]242[.]206[.]219
23[.]95[.]97[.]30	94[.]242[.]206[.]68
23[.]95[.]97[.]37	95[.]154[.]199[.]159
23[.]95[.]97[.]47	95[.]154[.]199[.]191
23[.]95[.]97[.]52	134[.]119[.]191[.]53
23[.]95[.]97[.]58	139[.]162[.]120[.]155
45[.]90[.]58[.]30	139[.]162[.]184[.]177
46[.]19[.]137[.]132	139[.]162[.]199[.]16
46[.]19[.]137[.]138	139[.]162[.]97[.]171
46[.]19[.]137[.]142	172[.]105[.]175[.]51
46[.]249[.]59[.]122	172[.]105[.]213[.]70
46[.]249[.]59[.]67	172[.]105[.]39[.]21
46[.]249[.]59[.]81	172[.]105[.]40[.]251
46[.]249[.]59[.]99	172[.]105[.]67[.]170
46[.]249[.]62[.]202	179[.]43[.]159[.]20
46[.]249[.]62[.]207	179[.]43[.]160[.]34
46[.]249[.]62[.]213	194[.]5[.]250[.]131
46[.]249[.]62[.]239	194[.]5[.]250[.]133
51[.]75[.]223[.]210	194[.]5[.]250[.]195
89[.]105[.]202[.]103	194[.]5[.]250[.]220
89[.]105[.]202[.]79	194[.]5[.]250[.]33
93[.]158[.]208[.]102	212[.]38[.]166[.]152
93[.]158[.]208[.]104	212[.]38[.]166[.]184
93[.]158[.]208[.]106	212[.]38[.]166[.]199
94[.]242[.]206[.]123	212[.]38[.]166[.]34
94[.]242[.]206[.]137	212[.]38[.]166[.]4
94[.]242[.]206[.]153	

Appendix C:

Email Subject Lines Used in Cosmic Lynx BEC Campaigns

July 2019 - August 2019

“Discussion today”
 “Discussion today - corporate development”
 “Follow-up discussion”
 “Important - Urgent discussion”
 “Urgent Discussion”

September 2019 - November 2019

“Follow-up: Liaise with external legal counsel”
 “Follow-up: Working with legal counsel”
 “Liaise With External Legal Counsel”
 “Liaise With Legal Advisors”
 “Liaise with legal counsel”
 “Liaising with external legal counsel”
 “Working with legal counsel”

December 2019 - January 2020

“Assignment With Law Firm”
 “Assignment with Legal Firm”
 “Follow-up on law firm matter”
 “Follow-Up: Liaise With External Legal Firm”
 “Handle Matter With Law Firm”
 “Law firm matter”
 “Legal Firm Matter”
 “Liaise with external legal counsel”
 “Liaise with legal firm”
 “Liase with external law firm”
 “Matter With External Legal Counsel”
 “Matter with external legal firm”
 “Matter with law firm”
 “Matter With Legal Advisors”
 “Matter With Legal Firm”
 “Work on matter with legal advisors”

January 2020 - March 2020

“Corporate action matter with law firm”
 “Corporate matter”
 “Corporate matter follow up”
 “Corporate matter to resolve”
 “Corporate matter with law firm”
 “Law firm matter”
 “Law firm matter follow up”
 “Matter with law firm”
 “Request Law firm matter”
 “Resolve matter with law firm”

March 2020 - April 2020

“Corporate development project”
 “Corporate matter Action needed”
 “New corporate development initiative”
 “New corporate development project”
 “Possible corporate action”
 “Possible corporate transaction”
 “Potential corporate action”
 “Potential corporate transaction”

April 2020 - June 2020

“Project XXX” (“XXX” is replaced with a random word for each BEC campaign. For example, “Project Gemini,” “Project Pegasus,” or “Project Viking.”)



AGARI CYBER
INTELLIGENCE DIVISION

About ACID

The Agari Cyber Intelligence Division (ACID) is the only counterintelligence research team dedicated to worldwide BEC and spearphishing investigation. ACID supports Agari's unique mission of protecting digital communications so that humanity prevails over evil. ACID uncovers identity deception tactics, criminal group dynamics, and relevant trends in advanced email attacks. Created by Agari in 2018, ACID helps to impact the cyber threat ecosystem and mitigate cybercrime activity by working with law enforcement and other trusted partners.

Learn more at acid.agari.com

About Agari

Agari is the market share leader in phishing defense solutions for the enterprise. Through applied science, the Agari Identity Graph™ delivers valuable business context to every email risk decision. Agari ensures outbound email from the enterprise cannot be spoofed, increasing deliverability and preserving brand integrity. It also protects the workforce from devastating inbound BEC, VEC, spearphishing, and account takeover-based attacks, reducing business risk and restoring trust to the inbox.

Learn more at www.agari.com