



# Nigerian Ransomware: An Inside Look at Soliciting Employees to Deploy DemonWare

On August 12, 2021, we identified and blocked a number of emails sent to Abnormal Security customers soliciting them to become accomplices in an insider threat scheme. The goal was for them to infect their companies' networks with ransomware. These emails allege to come from someone with ties to the DemonWare ransomware group.

DemonWare—also known as Black Kingdom and DEMON—has been around for a few years. Earlier this year, the ransomware was in the news when an actor tried to use it to exploit the significant Microsoft Exchange Vulnerability that was announced in March (CVE-2021-27065).

## The Initial Ask: Sending the Ransomware Request

In this latest campaign, the sender tells the employee that if they're able to deploy ransomware on a company computer or Windows server, then they would be paid \$1 million in bitcoin, or 40% of the presumed \$2.5 million ransom. The employee is told they can launch the ransomware physically or remotely. The sender provided two methods to contact them if the employee is interested—an Outlook email account and a Telegram username.

---

**From** sajid@bpovision.com ☆  
**Subject** Partnership Affiliate Offer 8/12/21, 12:03 PM  
**To** undisclosed-recipients:; ☆

---

if you can install & launch our Demonware Ransomware in any computer/company main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: [cryptonation92@outlook.com](mailto:cryptonation92@outlook.com)

Telegram : madalin8888

*Initial email sent by the threat actor.*

Historically, ransomware has been delivered via email attachments or, more recently, using direct network access obtained through things like unsecure VPN accounts or software vulnerabilities. Seeing an actor attempt to use basic social

engineering techniques to convince an internal target to be complicit in an attack against their employer was notable.

The tactic used by this actor, however, gave us an opportunity to better understand it. Since the actor invited a target to get in touch with him, we did just that. We constructed a fictitious persona and reached out to the actor on Telegram to see if we could get a response. It didn't take long for a response to come back, and the resulting conversation gave us an incredible inside look at the mindset of this threat actor.

## Instructing the Target and Reducing the Ransom

The first message we sent indicated we saw the email and asked what we needed to do to help. A half hour later, the actor responded and reiterated what was included in the initial email, followed by a question about whether we'd be able to access our fake company's Windows server. Of course, our fictitious persona would have access to the server, so we responded that we could and asked how the actor would send the ransomware to us.



**Pablo**

5:37 PM

if you work in an office, you can install  
Ransomware in your company windows server

once the company pays us big cash in Bitcoins,  
you will get %40



5:37 PM

can you access your company windows server?


5:37 PM

*Initial response from ransomware actor reiterating offer.*

Later, the actor sent us two links for an executable file we could download on WeTransfer or Mega.nz, two file sharing sites. The file was named "Walletconnect (1).exe" and based on an analysis of the file, we were able to confirm that it was, in fact, ransomware.

  ✓ 4:00 PM  
k how are you gonna send me the file

 **Pablo** 4:00 PM  
<https://we.tl/t-oQk7YWBEJU>

 ✓ 4:00 PM  
and do i just need to upload it or do i need to do anything else

 **Pablo** 4:00 PM  
<https://mega.nz/file/BxxG2DaY#AyLPiHCxCHp2H1u1dG6wiEzz-IUcdt1VhnErjO-yBq8>

[mega.nz](https://mega.nz)  
20.97 MB file on MEGA



if you can operate the server machine, the server must have a browser? 4:00 PM

 ✓ 4:01 PM  
yea

 **Pablo** 4:01 PM  
or usb port?

*Ransomware actor providing links to ransomware file.*

As the conversation continued, it became clear that the actor was quite flexible in the amount of money he was willing to accept for the ransom. While the initial email insinuated the ransom would be \$2.5 million, the actor quickly lowered expectations by indicating he hoped he could charge our fake company just \$250,000. After our persona mentioned the company we “worked” for had an annual revenue of \$50 million, the actor pivoted and lowered the number even further to \$120,000.



**Pablo**

is it a big company?



**Pablo**

[redacted]  
k, never done anything like this before but im leaving my co...  
i hope we can charge them about \$250,000+



[redacted]  
the company i work for isn't huge but its not small either  
about \$50mil annual revenue



**Pablo**

[redacted]  
about \$50mil annual revenue  
we'll charge them 120,000\$\$+



[redacted]  
im confused about the amount, you said id get 1 mil but ur  
talking about just charging them 120k



**Pablo**

[redacted]  
im confused about the amount, you said id get 1 mil but ur t...  
if you want me to charge them a milli  
we'll charge them a milli

i was just being a little bit considerate for them, lol

*Ransomware actor updating ransom amount expectations.*

Throughout the conversation, the actor repeatedly tried to alleviate any hesitations we may have had by ensuring us that we wouldn't get caught, since the ransomware

would encrypt everything on the system. According to the actor, this would include any CCTV (closed-circuit television) files that may be stored on the server.

The actor also instructed us to dispose of the .EXE file and delete it from the recycle bin. Based on the actor's responses, it seems clear that he 1) expects an employee to have physical access to a server, and 2) he's not very familiar with digital forensics or incident response investigations.



[redacted]  
is there anything i can do to make sure they dont know im the one that uploaded the file

im kinda worried bout that



**Pablo**

[redacted]  
is there anything i can do to make sure they dont kn...  
the Ransomware will cripple all cctv footage, and every shit in the system



**Pablo**

[redacted]  
is there anything i can do to make sure they dont kn...  
once installed in the system, dispose the file in the storage & delete it from the recycle bin



[redacted]  
cctv?



**Pablo**

[redacted]  
cctv?

it will cripl everything stored in the server

so i don't think there will be any traces

any footage or any file, anything stored in the server will be encrypted



**Pablo**

**Pablo**

once installed in the system, dispose the file in the s...  
just delete the software in the storage and recycle bin as soon as possible



**Pablo**

**Pablo**

just delete the software in the storage and recycle b...  
so no traces

once installed

*Ransomware*

*actor provides instructions on how to cover our tracks.*

At one point in the conversation, we asked the actor if he had created the ransomware himself or if he was just using it. The actor told us that he “programmed the software using python language.” In reality, however, all of the code for DemonWare is freely available on GitHub as a “project was made to demonstrate how easy ransomware are [sic] easy to make and how it work [sic].”



ah k

so out of curiosity did u create the file or are u just using it



**Pablo**

i programmed the software

using python language



was it hard

to create



**Pablo**

yes, of course



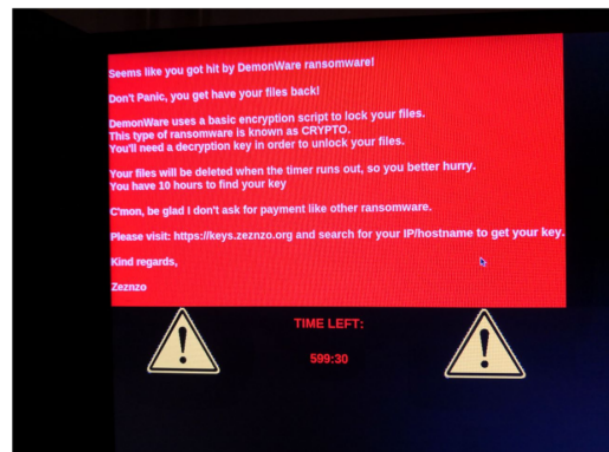
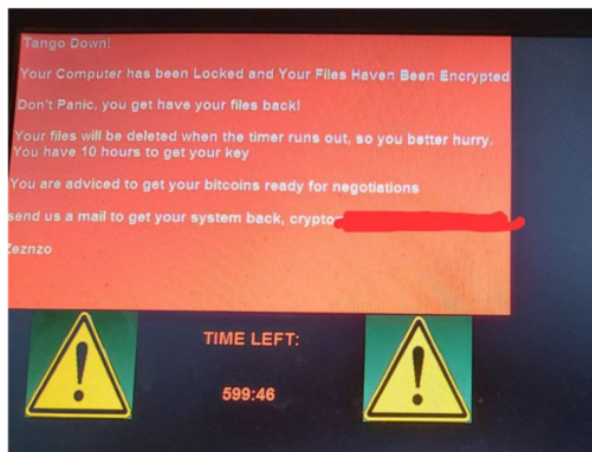
**Pablo**

yes, of course

lol "of course"

*Ransomware actor attesting to writing the malware himself.*

In this case, our actor simply needed to download the ransomware from GitHub and socially engineer someone to deploy the malware for them.



*Ransom demand screen provided by our actor vs. ransom demand screen sample from GitHub DemonWare repository.*

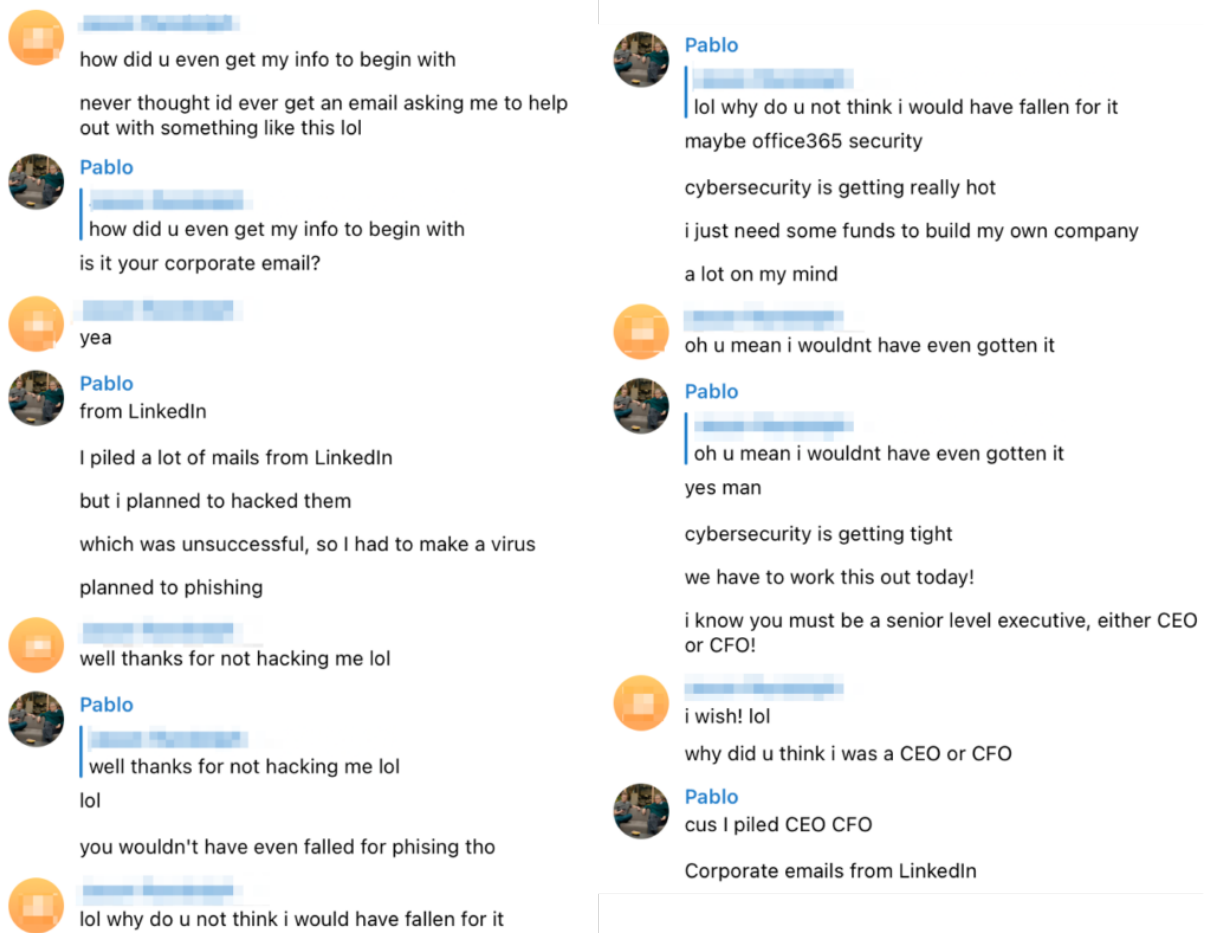
This demonstrates the appeal of ransomware-as-a-service, as it lowers the barrier of entry for less technically-sophisticated actors to get into the ransomware space.

## The LinkedIn Connection: Finding Targets Through Social Networks

When analyzing cyber attacks, one of the biggest questions to ask is *how did an actor initially get the target's contact information?* In this case, since we had our threat actor engaged with us, we thought we should ask him the question directly.

According to the actor, he collects his targeting information from LinkedIn, which, in addition to other commercial services that sell access to similar data, is a common method scammers use to obtain contact information for employees.





*Information about how target contact information was collected by ransomware actor.* According to this actor, he had originally intended to send his targets—all senior-level executives—phishing emails to compromise their accounts, but after that was unsuccessful, he pivoted to this ransomware pretext.

## Digging Deeper: Understanding the Nigerian Scheme

So who is this person? Before starting our conversation with the actor, we conducted some cursory open source research to see if we could get any clues about his identity. Our initial findings suggested that the actor could potentially be Nigerian, based on information found on a Naira (Nigerian currency) trading website and a Russian social media platform website.



██████ **FINANCE**

Dear Customers

Here at ██████ FINANCE LTD

Our Mission:

Our Vision: To create a banking and finance industry

Whatsapp - +234████████████████████

← WhatsApp number with Nigerian prefix

if you have ipip / dtc / MT103-202 / FX4 / MT104  
forward to our email - cryptonation92@████████████████████

← Same username from ransomware email

all contracts are signed and returned within 24 - 48 hours

Thank you! My regards

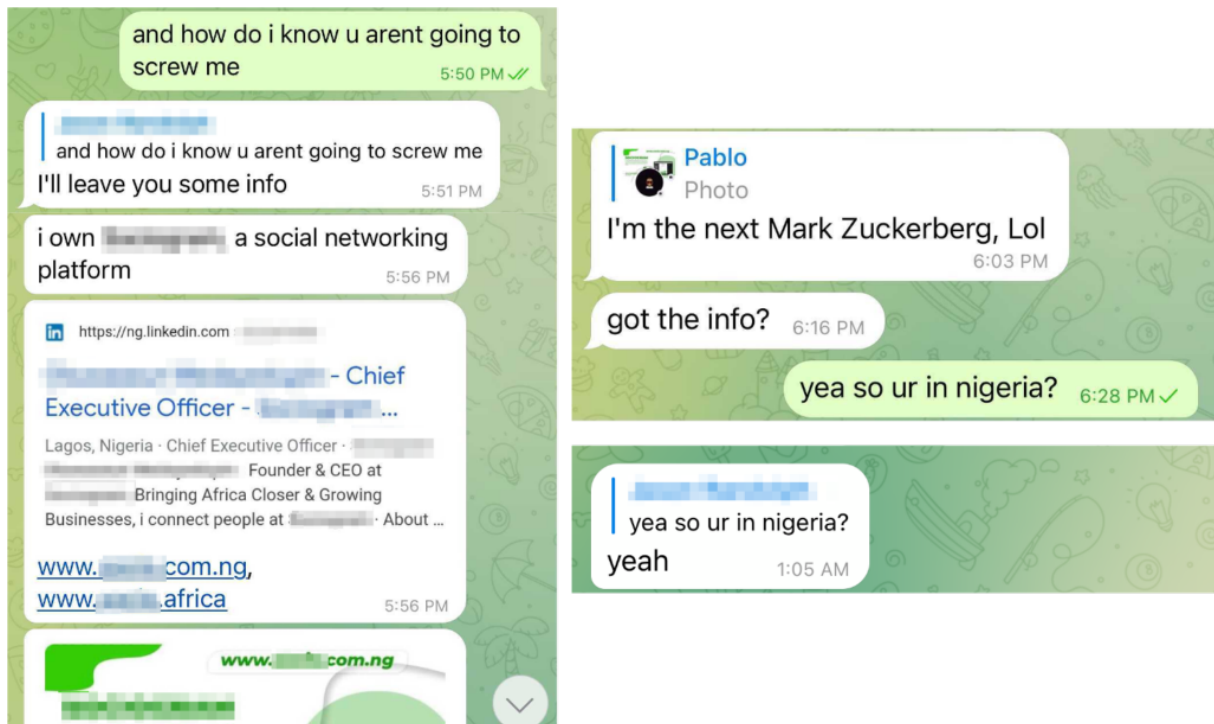
CEO 🧑 Oluwaseun

← Common African first name

*Information found on a Russian social media platform website connecting ransomware actor to Nigeria.*

After our conversation started, though, the actor we were talking to was kind enough to confirm our suspicions. After expressing concerns that the actor might pull one over on us, he provided some information about himself. He confirmed that he was located in Nigeria and was trying to build an African social networking platform, joking he was “the next Mark Zuckerberg.” He also provided a link to his LinkedIn profile containing his full name.

Interestingly, the actor must have had second thoughts about sharing his identity with us because he later deleted those messages from our conversation. However, anticipating this regret, we saved screenshots of this information before he deleted it.



*Attribution details provided by ransomware actor.*

Knowing the actor is Nigerian really brings the entire story full circle and provides some notable context to the tactics used in the initial email we identified. For decades, West African scammers, primarily located in Nigeria, have perfected the use of social engineering in cybercrime activity.

While the most common cyber attack we see from Nigerian actors (and most damaging attack globally) is business email compromise (BEC), it makes sense that a Nigerian actor would fall back on using similar social engineering techniques, even when attempting to successfully deploy a more technically sophisticated attack like ransomware.

## Collecting Intelligence Through Engagement

Our conversation with this ransomware actor took place over the course of five days. Because we were able to engage with him, we were better able to understand his motivations and tactics.

Threat intelligence like this helps us better understand the bigger picture with additional context—something we're unable to do by only examining traditional indicators of compromise and raw data. Using these unique intelligence collection methods, we are able to gain a deeper level of insight to help better understand emerging cyber threats, and to better protect our customers.

*Curious about our additional conversations with this threat actor? Register for our webinar *Deconstructing the Ransomware Landscape: Conversation with a Real Threat Actor* on September 8th for full details.*