Caught Beneath the Landline: A 411 on Call Center Scams

proofpoint.com/us/blog/threat-insight/caught-beneath-landline-411-telephone-oriented-attack-delivery

October 29, 2021

Blog
Threat Insight
Caught Beneath the Landline: A 411 on Call Center Scams

November 04, 2021 Selena Larson, Sam Scholten and Timothy Kromphardt

Key Takeaways

- Proofpoint researchers observe tens of thousands of telephone oriented cyberattacks daily.
- There are two types of these threats regularly observed by Proofpoint. One features traditional call center fraud, such as fake tech support, to steal money. The second leverages call centers to distribute malware that could be used for secondary compromises.
- Proofpoint is aware of individual victims losing nearly $50,000 per attack. It is likely that number is greater.
- Malware distributed in some of the observed campaigns could lead to ransomware and pose a greater risk to business operations.

Overview

Proofpoint researchers have observed an increase in attacks perpetuated by threat actors leveraging a robust ecosystem of call center-based email threats. The attacks rely on victims to call the attackers directly and initiate the interaction. Email fraud supported by call center customer service agents is prolific and profitable. In many cases, victims lose tens of thousands of dollars stolen directly from their bank accounts.

There are two types of call center threat activity regularly observed by Proofpoint. One uses free, legitimate remote assistance software to steal money. The second leverages the use of malware disguised as a document to compromise a computer and can lead to follow-on malware. The second attack type is frequently associated with BazaLoader malware and is often referred to as BazaCall. Both attack types are what Proofpoint considers **telephone-oriented attack delivery (TOAD).**

TOAD

	Fraud	BazaCall
Phone-based	X	X
Initial objective: financial gain	X	
Initial objective: malware installation		X
Uses commercially available remote access software	X	
Leads to follow on activity		X

In recent attacks, threat actors email a victim claiming to be representatives from entities like Justin Bieber ticket sellers, computer security services, COVID-19 relief funds, or online retailers, promising refunds for mistaken purchases, software updates, or financial support. The emails contain a phone number for customer assistance. When the victims call the number for help, they are connected with a malicious call center attendant directly and the attack begins.

Proofpoint detects and blocks tens of thousands of email threats related to TOAD every day. Our researchers tracked down the perpetrators to multiple areas of operations, and through email data, phone conversations, and message and infrastructure artifacts, can now provide an exclusive look at how the thriving call center threat business profits on lies.

Call Center Threats

Most consumers are familiar with phone-based fraud and regularly receive unsolicited phone calls from people pretending to be, for instance, tech support or the Department of Motor Vehicles. According to a 2021 study conducted by Truecaller, nearly 60 million Americans have reportedly lost money due to phone fraud, losing $29.8 billion between 2020 and 2021. The recent spike in TOAD threats observed by Proofpoint is a subset of these threats, combining old-fashioned phone fraud with unsolicited emails as an initial communication vector.

These types of attacks include elaborate infection chains requiring significant victim interaction to infiltrate a victim's computer or smartphone. The threat actor sends an email typically with a receipt for a large purchase masquerading as a company or organization and instructs the recipient to call the number in the email to cancel or dispute their purchase. The email address is usually a Gmail, Yahoo, or other freemail account. If the user calls the

phone number provided in the email, a customer service representative will verbally guide the user to visit a website or mobile app store. They will guide them through different types of user interaction such as downloading a malicious file, allowing them to remotely access their machine, or downloading a malicious application for remote access.

While the two distinct TOAD types begin the same – victim receives an email and is directed to call a customer service representative – the attack paths diverge depending on the objective.

Financial extortion actors typically use invoice lures associated with companies like Amazon, Paypal, or security software. Once a person calls the number listed in the email, the actor will direct the victim to install remote access software such as AnyDesk, Teamvier, Zoho, etc. and provide them access to interact with the machine under the guise of customer service. Often, the victim is directed to login to their bank account to get a refund, or purchase gift cards. Once the attacker is connected, they blackout the screen to hide their activities. They might edit the HTML of the banking webpage to show a different amount or attempt to steal the money directly.

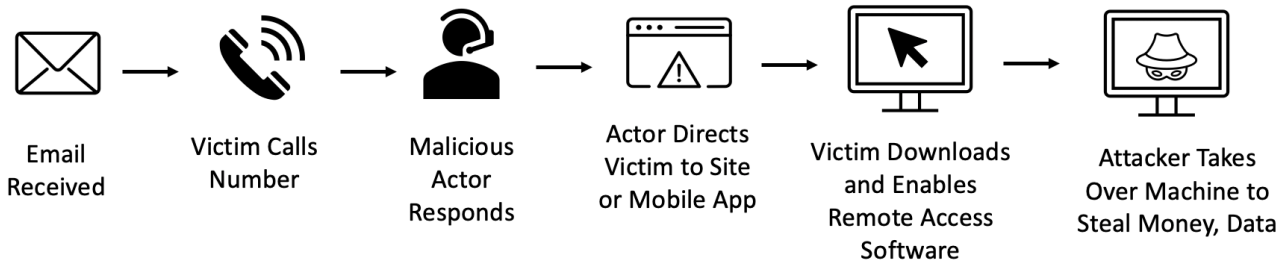

Figure 1: Financially motivated attack path.

In malware focused attacks like BazaCall, the invoice lures are often more elaborate, including themes such as Justin Bieber concerts, lingerie, and fake movie sites. The victim is directed to a malicious website where they are told to download a document to facilitate a refund, but instead are infected with malware.

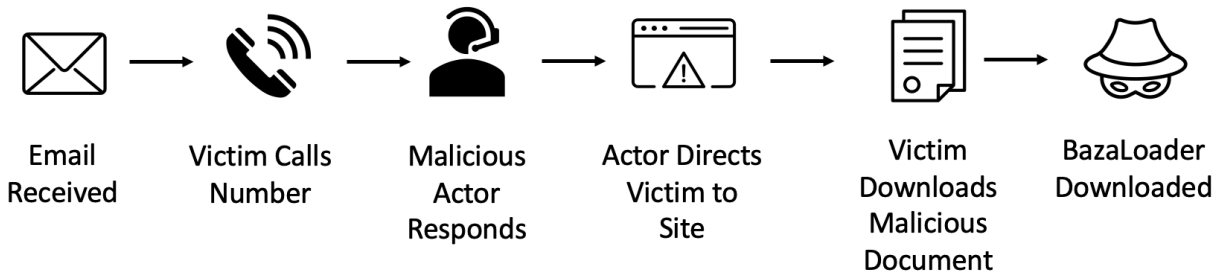

Figure 2: BazaCall attack path.

Once the attackers have obtained access to the device, they can access banking, email, and other private accounts or download follow-on malware including ransomware. By leveraging attack chains that require a lot of human interaction, threat actors can bypass some automated threat detection services that only flag on malicious links or attachments in email.

Popular Call Center Lures

The lures and themes threat actors send to victims vary, from very low effort attempts to leveraging legitimate branding and document downloads. Our researchers frequently engage with threat actors to better understand the attack paths and behaviors exhibited by these actors.

PayPal Lure

For example, our researcher identified a financially motivated TOAD threat masquerading as a PayPal invoice from a U.S. weapons manufacturer.

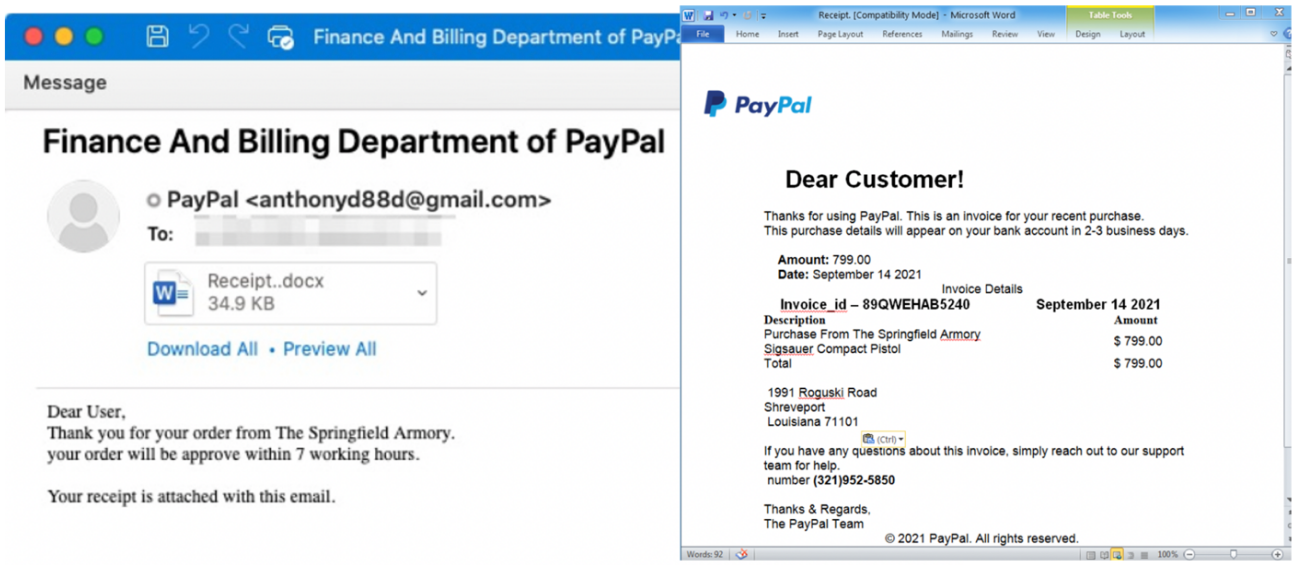

Figure 3: PayPal lure masquerading as the U.S. company Springfield Armory.

Our researcher called the number in the invoice and connected with “David” pretending to be a PayPal representative. “David” followed a script and told our researcher to download AnyDesk and login to his bank account. The attacker also claimed that someone had tried to purchase a weapon using his PayPal account and warned him that “hackers” regularly access people’s accounts to make purchases. In total, the conversation took approximately an hour.

Justin Bieber Lure

Other campaigns use pop culture themed lures, including posing as ticket sellers to The Weeknd concerts or the upcoming 2022 Justin Bieber world tour. These lures are associated with BazaCall threats. When our researcher called the number in the Justin Bieber email, he

was immediately placed on hold with the pop star's music.

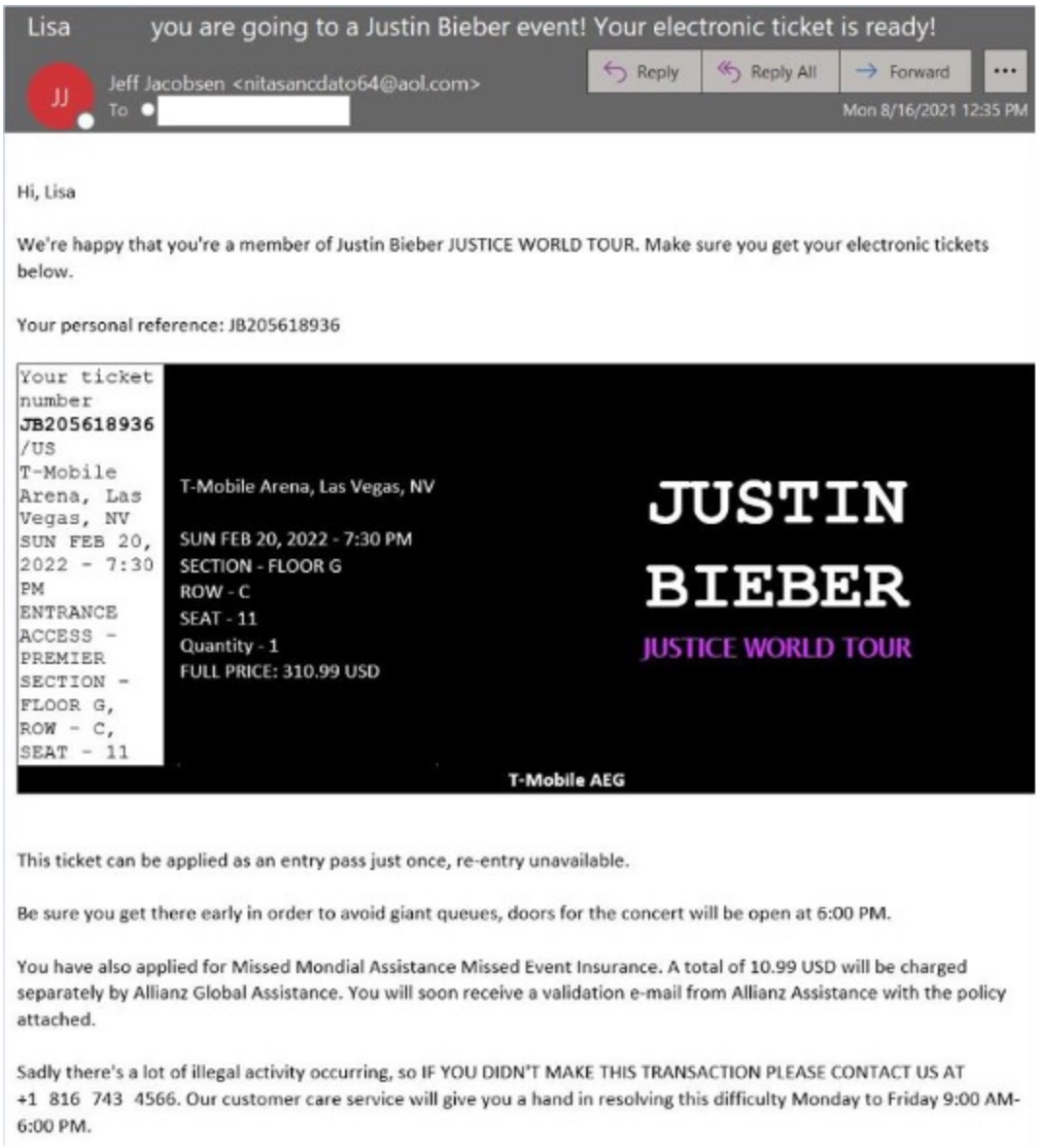

Figure 4: Justin Bieber themed email purporting to be tickets for an upcoming concert.

When our researcher called the BazaCall threat actors, a person named "John Edwards" claimed someone had erroneously placed an order on his credit card and to visit ziddat[.]com/code.exe to get a refund. Our researcher downloaded the executable in a virtual machine, and told "John" nothing came up on the screen. BazaLoader was successfully downloaded, and "John" said he could take care of the issue before abruptly hanging up. In total, the call took approximately 10 minutes.

Threat Actors

Although it is difficult to narrow down activity into specific threat activity groups associated with TOAD threats, Proofpoint researchers have identified multiple activity clusters located in India. Most of the activity occurs in three cities: Kolkata, Mumbai, and New Delhi.

Proofpoint was able to pin down multiple physical locations of activity clusters based on the threat actors' interactions with Proofpoint researchers as well as open-source information shared on fraud forums and YouTube. The following map represents a sample of identified call centers.

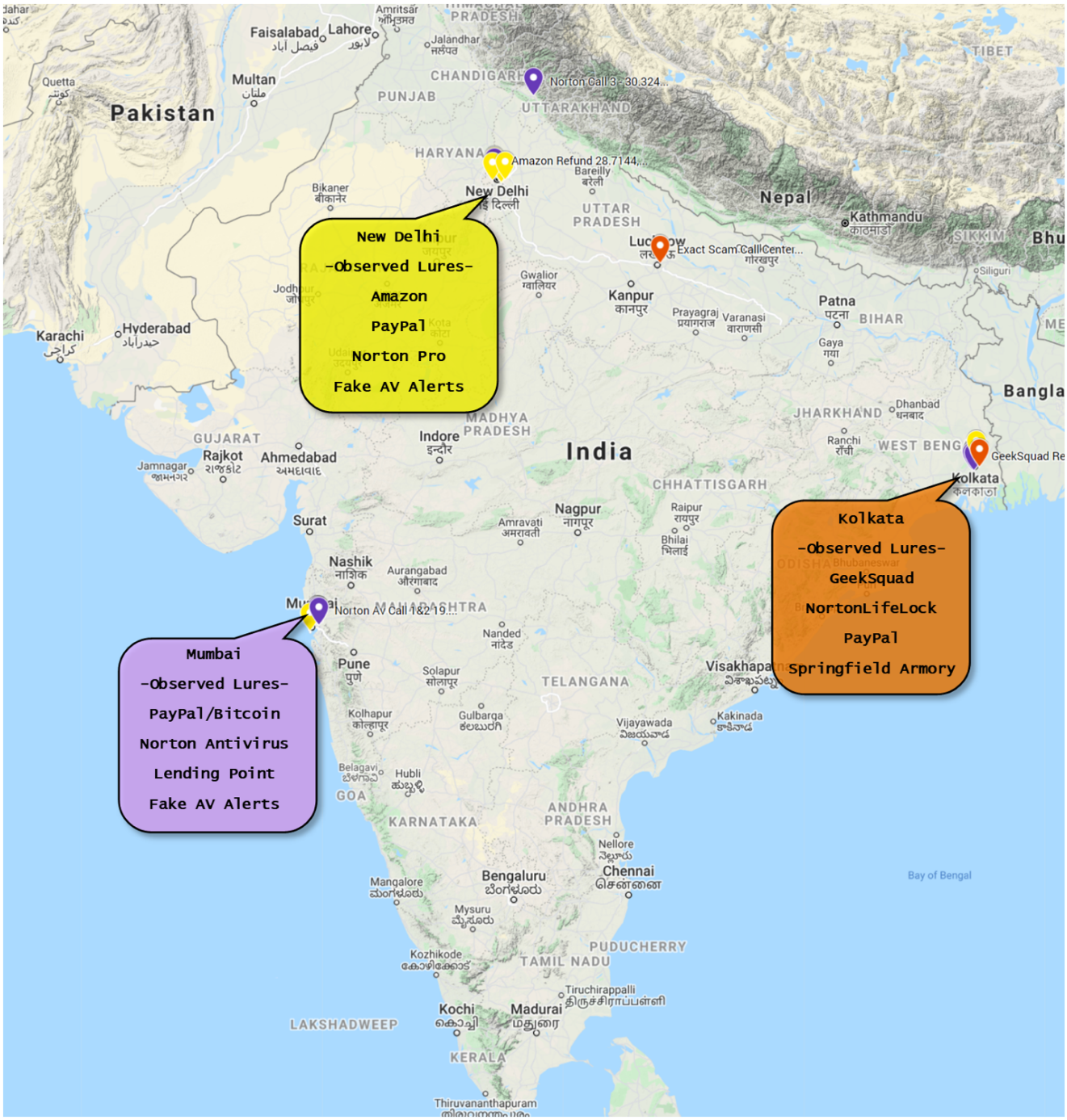

Figure 5: Locations of TOAD threat operators.

During our research, threat actors accessed researchers' computers directly, and Proofpoint researchers were able to siphon data such as IP information from the remote access connections. Additionally, some independent "scam baiters" have remote access to threat actors' physical location and share their findings on YouTube and TikTok.

Based on publicly available information, Proofpoint was able to identify the office allegedly used by one cluster of tech support TOAD actors located in Kolkata.

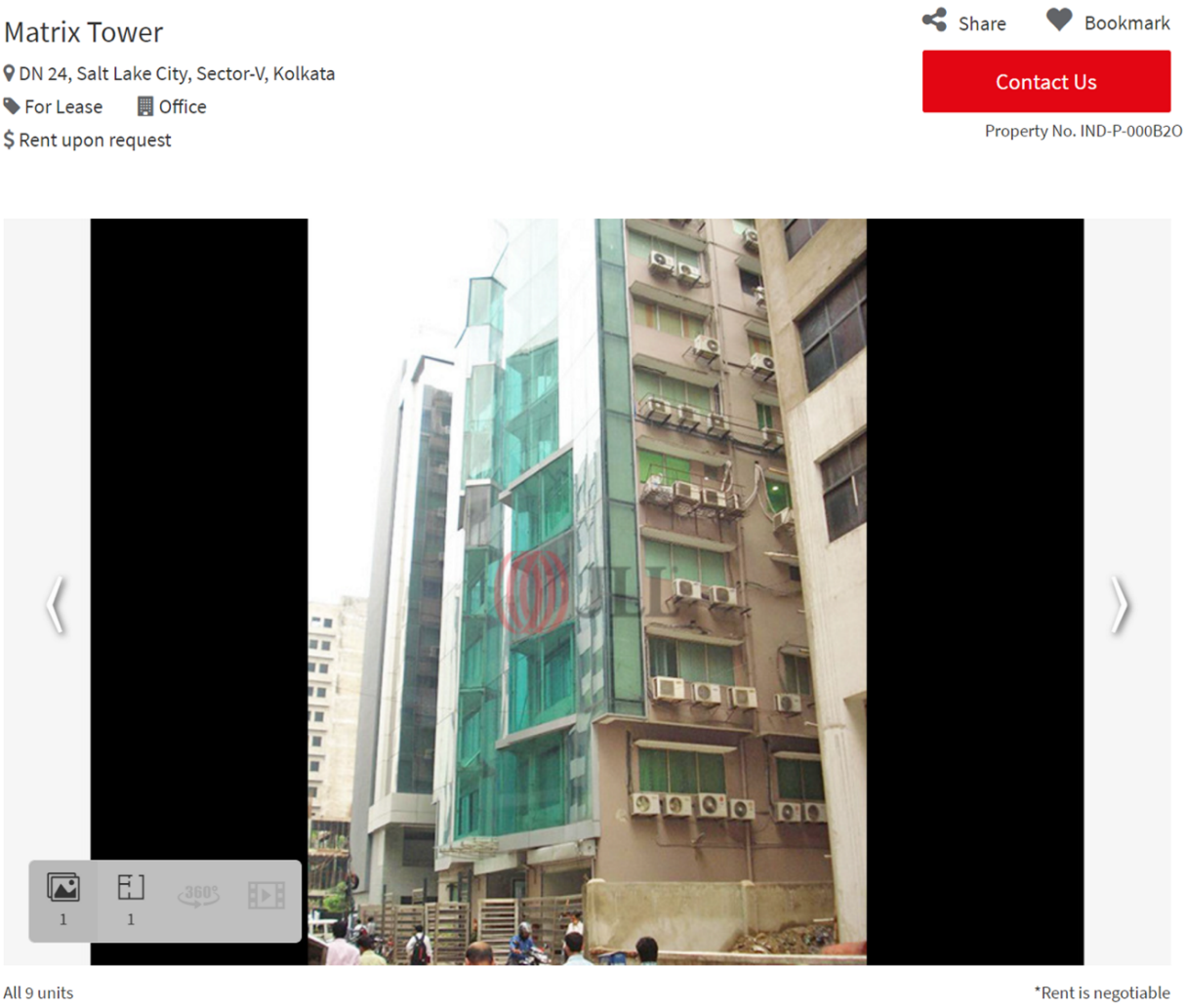

Figure 6: Matrix Tower in Kolkata where TOAD threat actors allegedly operate listed on a property management company website.

These threat actors reportedly targeted people in Germany, the U.S., Australia, and India with fraudulent tech support claims.

Malicious call centers are architected like legitimate businesses. Owners sign leases on buildings purporting to be telemarketers or other phone-based businesses, and recruit local jobseekers to support the operation. Due to job scarcity in areas of operation and potential for higher earnings than alternative employment, the lucrative phone fraud jobs are alluring. While conducting calls with the threat actors, Proofpoint researchers overheard floor managers guiding employees through a script on how to speak to victims. Employees' pay varies. According to the BBC, earnings may start at 1 rupee for every $1 stolen and increase to $50,000 per month.

While financially motivated and malware-focused TOAD actors have similar techniques, Proofpoint researchers have observed that BazaLoader threat actors do not appear to use physical call center facilities, and fake customer service agents are usually not located in India. Proofpoint assesses with moderate confidence the actors use inbound call center software then route the calls to geographically dispersed customer service agents. The agents distributing BazaLoader do not remotely access victims' machines; rather they direct them to a website to download a malicious file that loads the malware. Thus, the fake customer service agents do not require as much technical aptitude as other cybercrime actors.

The increasingly widespread adoption of threats requiring victims to initiate engagement with their attackers indicates that participants in the cybercriminal ecosystem likely learn from each other and will shape tactics, techniques, and procedures (TTPs) based on efficacy observed by their fellow threat actors.

Victimology

Call center-based email threat actors do not appear to specifically target people via demographics, jobs, location, etc., but likely procure their contact lists from legitimate data brokerages or other telemarketer resources. And while the public typically hears about activities impacting victims from vulnerable communities including the elderly and disabled, according to the 2021 TrueCaller report, men are impacted more than women, and younger men are more likely than older men to be victims of a phone scam. (*Analyst note: This data includes all phone-based spam and scams and are not specific to call center-based email threats.)*

Like many victims of crime, people who lose money to cyberattacks may feel ashamed and embarrassed, and do not share details of what occurred. This makes it difficult for researchers, law enforcement, and the public to understand the true number of people impacted by call center-based email fraud. But the losses can be life-altering. Proofpoint is aware of victims losing nearly $50,000 in one attack, with the threat actor masquerading as a NortonLifeLock representative. And the fallout of cybercrime – like the financial toll, and emotional well-being – reportedly disproportionally impact Black, Indigenous, and people of color (BIPOC) communities.

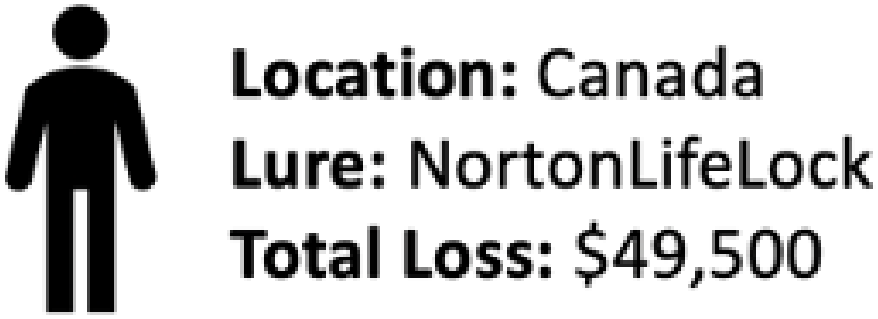

Figure 7: Known victim of TOAD threat.

Impacts to Organizations

TOAD threat actor targeting is indiscriminate and includes both personal email accounts – Gmail, Yahoo, Hotmail, etc. – and corporate email addresses. Proofpoint has observed BazaCall operators targeting employees of large organizations, and a successful infection could compromise the entire enterprise network leading to follow on attacks such as ransomware.

Targeting individuals' private email addresses could have follow-on impacts to corporations. For example, as COVID-19 has caused a shift to remote work, more people are accessing personal information online from work devices or accounts. Additionally, TeamViewer and AnyDesk are legitimate enterprise software services that may be already installed on corporate machines; if the software allows external connections, the activity could bypass other enterprise security protections that may be in place to detect and block remote access attempts. A threat actor may successfully obtain remote access to a corporate managed device and install malware that could facilitate follow-on activity such as ransomware.

Proofpoint assesses small and medium-sized businesses are at greatest risk for TOAD threats impacting the corporate environment.

APPENDIX

The following is a list of company names Proofpoint regularly observes in call center-based email threat campaigns.

- Norton
- Mcafee
- Ebay
- Nort-Pro
- PayPal
- GeekSquad
- NortonLifeLock

- Covid-19 relief /AOL Fund
- AOL Committee
- VakıfBank
- Santander Bank
- IMF Giving
- Amazon
- Justin Bieber Justice World Tour
- The Weeknd T O U R
- Springfield Armory
- Symantec
- Meagher Auto Insurance

Subscribe to the Proofpoint Blog