Threat Assessment: Luna Moth Callback Phishing Campaign

unit42.paloaltonetworks.com/luna-moth-callback-phishing/

Kristopher Russo

November 21, 2022

By Kristopher Russo

November 21, 2022 at 3:00 AM

Category: Threat Briefs and Assessments

Tags: BazarLoader, callback phishing, conti ransomware, Cortex, Cortex XDR, Enterprise DLP, Extortion, incident response, Luna Moth, next-generation firewall, Phishing, Silent Ransom Group, threat intelligence

This post is also available in: 日本語 (Japanese)

Executive Summary

Unit 42 investigated several incidents related to the Luna Moth/Silent Ransom Group callback phishing extortion campaign targeting businesses in multiple sectors including legal and retail. This campaign leverages extortion without encryption, has cost victims hundreds of thousands of dollars and is expanding in scope.

By design, this style of social engineering attack leaves very few artifacts because of the use of legitimate trusted technology tools to carry out attacks. However, Unit 42 has identified several common indicators implying that these attacks are the product of a single highly organized campaign. This threat actor has significantly invested in call centers and infrastructure that's unique to each victim.

Cybersecurity awareness training is the most effective defense against these stealthy and discreet attacks. However, Palo Alto Networks customers receive protection from the attacks discussed in this blog through the Next-Generation Firewall and Cortex XDR detecting data exfiltration or connections to suspicious networks.

Related Unit 42 Topics Phishing, BazarLoader

Table of Contents

What Is Callback Phishing?

Callback phishing, also referred to as telephone-oriented attack delivery (TOAD), is a social engineering attack that requires a threat actor to interact with the target to accomplish their objectives. This attack style is more resource intensive, but less complex than script-based attacks, and it tends to have a much higher success rate.

In the past, threat actors associated with the Conti group have had great success with this attack style in the BazarCall campaign. Unit 42 has been tracking these types of attacks since 2021. Early iterations of this attack focused on tricking the victim into downloading the BazarLoader malware using documents with malicious macros.

This new campaign, which Sygnia has attributed to a threat actor dubbed "Luna Moth," does away with the malware portion of the attack. In this campaign, attackers use legitimate and trusted systems management tools to interact directly with a victim's computer, to manually exfiltrate data to be used for extortion. As these tools are not malicious, they're not likely to be flagged by traditional antivirus products.

Please note that the tools named in this post are legitimate. Threat actors often abuse, take advantage of or subvert legitimate products for malicious purposes. This does not imply a flaw or malicious quality to the legitimate product being abused.

The Typical Callback Phishing Attack Chain

The initial lure of this campaign is a phishing email to a corporate email address with an attached invoice indicating the recipient’s credit card has been charged for a service, usually for an amount under $1,000. People are less likely to question strange invoices when they are for relatively small amounts. However, if people targeted by these types of attacks reported these invoices to their organization’s purchasing department, the organization might be better able to spot the attack, particularly if a number of individuals report similar messages.

The phishing email is personalized to the recipient, contains no malware and is sent using a legitimate email service. These phishing emails also have an invoice attached as a PDF file. These features make a phishing email less likely to be intercepted by most email protection platforms.

The attached invoice includes a unique ID and phone number, often written with extra characters or formatting to prevent data loss prevention (DLP) platforms from recognizing it. When the recipient calls the number, they are routed to a threat actor-controlled call center and connected to a live agent.

Under the guise of canceling the subscription, the threat actor agent guides the caller through downloading and running a remote support tool to allow the attacker to manage the victim’s computer. This step usually generates another email from the tool’s vendor to the victim with a link to start the support session.

The attacker then downloads and installs a remote administration tool that allows them to achieve persistence. If the victim does not have administrative rights on their computer, the attacker will skip this step and move directly to finding files for exfiltration.

The attacker will then seek to identify valuable information on the victim’s computer and connected file shares, and they will quietly exfiltrate it to a server they control using a file transfer tool.

In this way, the threat actor is able to compromise organizational assets through a social engineering attack on an individual.

After the data is stolen, the attacker sends an extortion email demanding victims pay a fee or else the attacker will release the stolen information. If the victim does not establish contact with the attackers, they will follow up with more aggressive demands. Ultimately, attackers will threaten to contact victims’ customers and clients identified through the stolen data, to increase the pressure to comply.

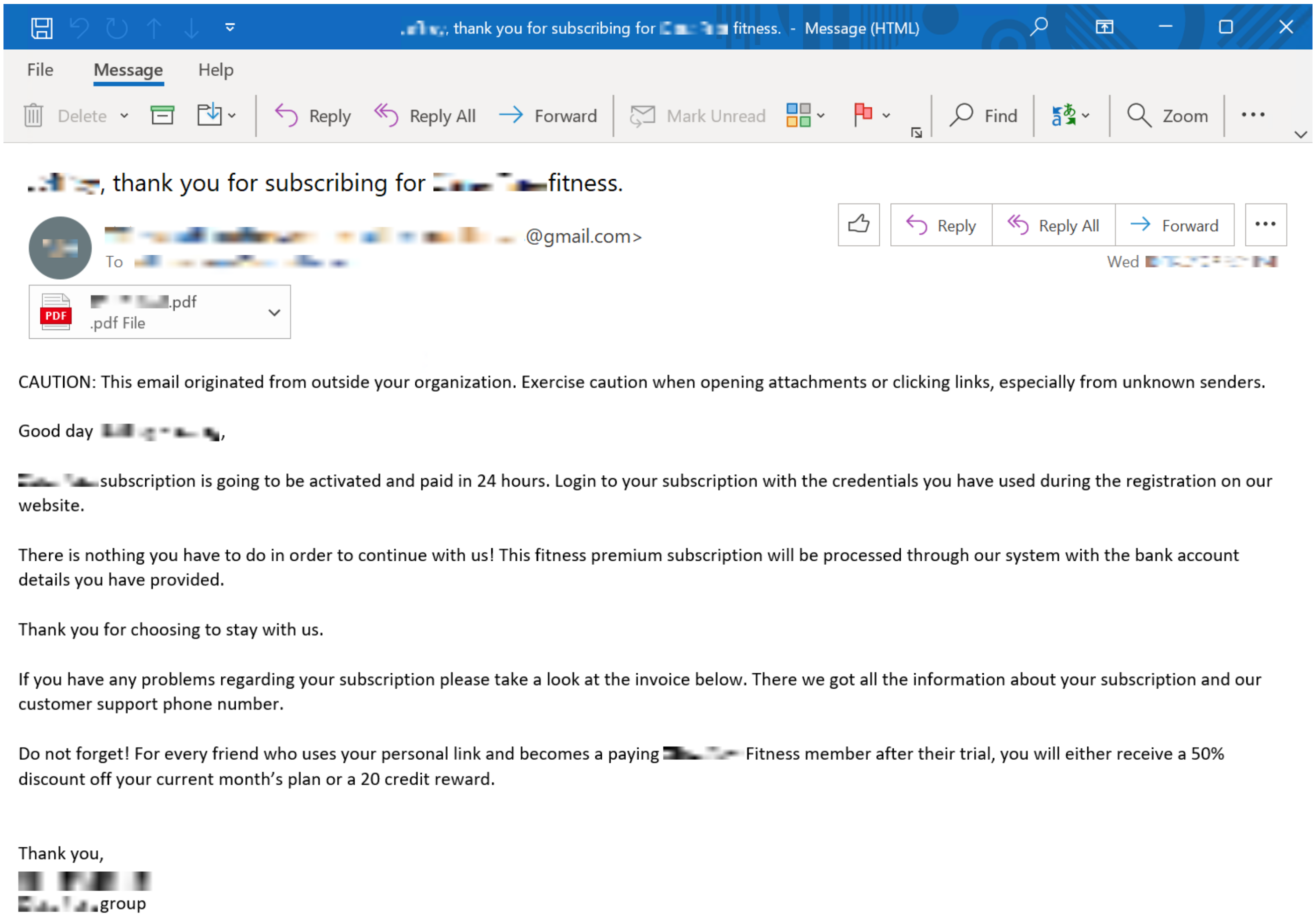
Luna Moth Campaign Analysis

Unit 42 has responded to multiple cases related to a single campaign that occurred from mid-May to late October 2022. ADVIntel attributes this campaign to a threat actor dubbed Silent Ransom with ties to Conti. While Unit 42 cannot confirm Silent Ransom's tie to Conti at this time, we are monitoring this closely for attribution.

These cases show a clear evolution of tactics that suggests the threat actor is continuing to improve the efficiency of their attack. Cases analyzed at the beginning of the campaign targeted individuals at small- and medium-sized businesses in the legal industry. In contrast, cases later in the campaign indicate a shift in victimology to include individuals at larger targets in the retail sector.

During the initial campaign, the phishing email frequently originated from an address using the format FirstName.LastName.[SpoofedBusiness]@gmail[.]com as seen in Figure 1. The attacker often spoofs the names of obscure athletes for these email addresses.

Unit 42 has also observed emails with the format [RandomWords]@outlook[.]co.th.



[redacted], thank you for subscribing for [redacted]fitness.

[redacted] @gmail.com>

To [redacted]

Wed [redacted]

[redacted].pdf
.pdf File

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links, especially from unknown senders.

Good day [redacted],

[redacted] subscription is going to be activated and paid in 24 hours. Login to your subscription with the credentials you have used during the registration on our website.

There is nothing you have to do in order to continue with us! This fitness premium subscription will be processed through our system with the bank account details you have provided.

Thank you for choosing to stay with us.

If you have any problems regarding your subscription please take a look at the invoice below. There we got all the information about your subscription and our customer support phone number.

Do not forget! For every friend who uses your personal link and becomes a paying [redacted] Fitness member after their trial, you will either receive a 50% discount off your current month's plan or a 20 credit reward.

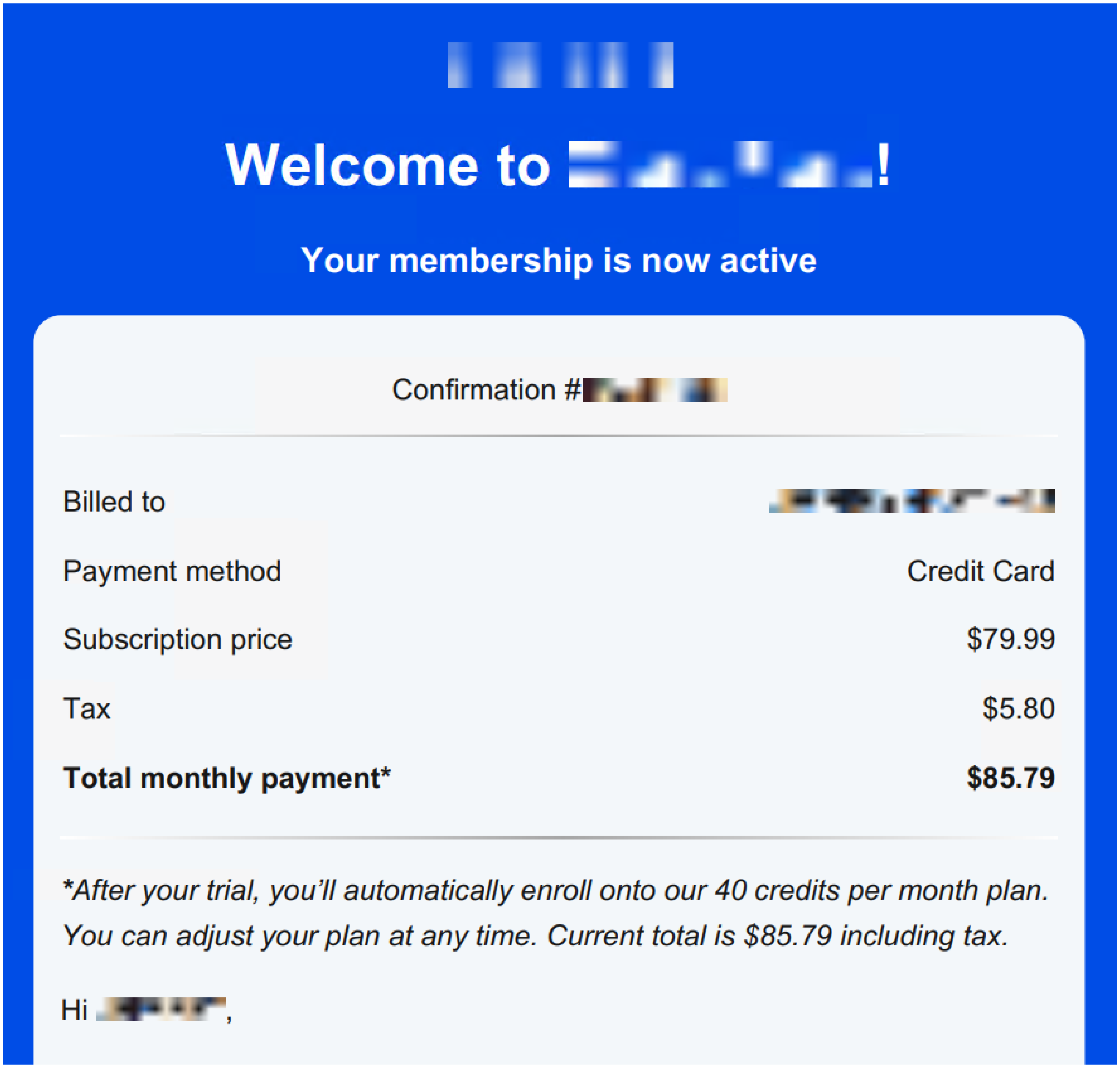
Thank you,
[redacted]
[redacted]group

Figure 1. Redacted phishing email.

The wording in the body of the phishing email has changed throughout the campaign. This was likely done to thwart email protection platforms. Regardless of what wording was used, the email always indicated the victim is responsible for the charges detailed in the attached invoice.

PDF documents containing an invoice number were attached to the phishing emails. Unit 42 observed fake invoices spoofing both an online class platform and a health club aggregator in this campaign.

Early incidents used a logo from one of the spoofed businesses at the top of the invoice. Later cases replaced this with the simple header welcoming the target to the second spoofed business on a plain blue background, as shown in Figure 2. Each invoice features a nine- or 10-digit confirmation number near the top, which is also incorporated into the filename. When the recipient contacts the threat actor, this confirmation number is used to identify them.



[redacted]

Welcome to [redacted]!

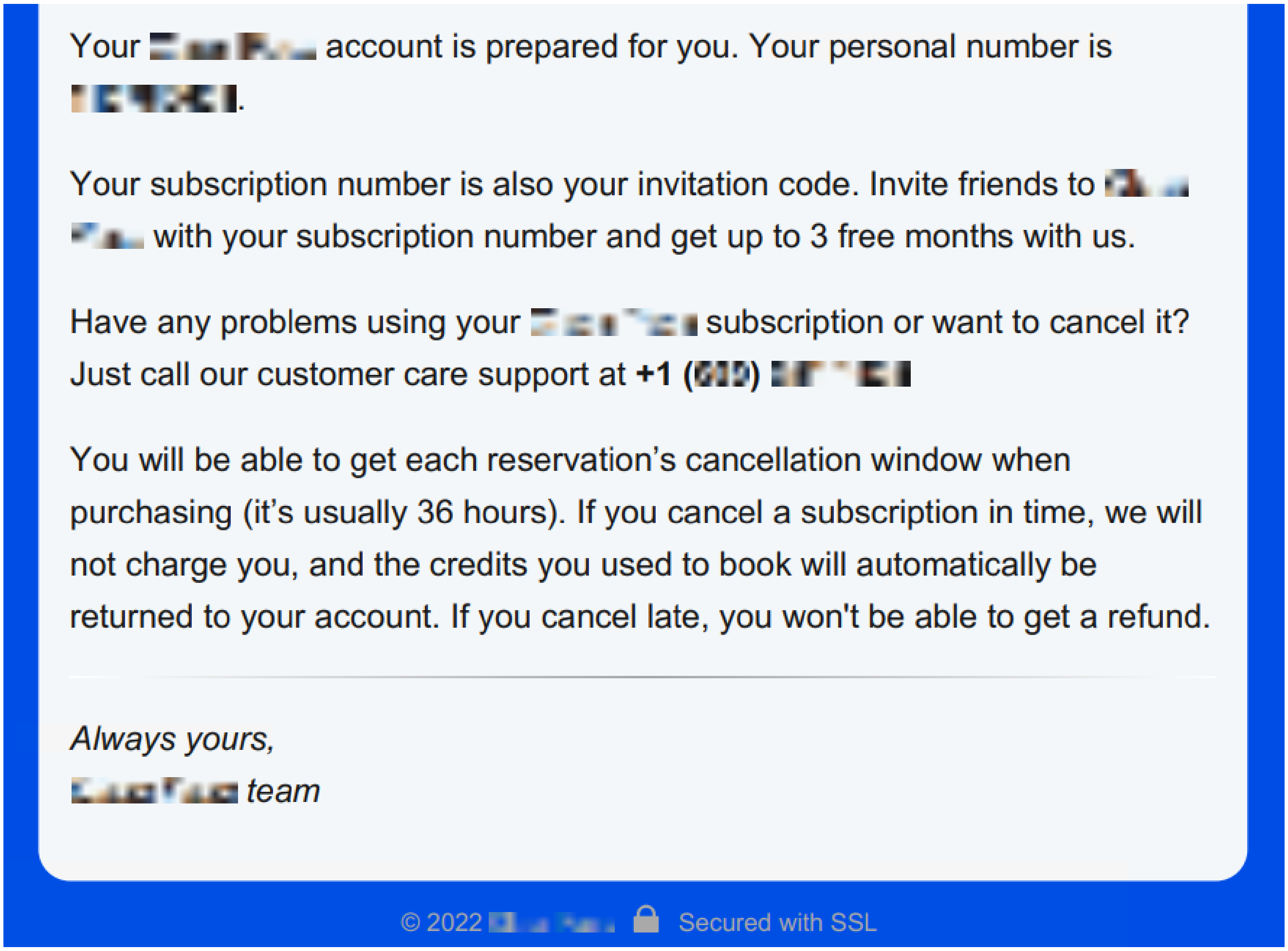
Your membership is now active

Confirmation #[redacted]

Billed to	[redacted]
Payment method	Credit Card
Subscription price	$79.99
Tax	$5.80
Total monthly payment*	**$85.79**

**After your trial, you'll automatically enroll onto our 40 credits per month plan. You can adjust your plan at any time. Current total is $85.79 including tax.*

Hi [redacted],



Your [redacted] account is prepared for you. Your personal number is [redacted].

Your subscription number is also your invitation code. Invite friends to [redacted] with your subscription number and get up to 3 free months with us.

Have any problems using your [redacted] subscription or want to cancel it? Just call our customer care support at **+1 ([redacted]) [redacted]**

You will be able to get each reservation's cancellation window when purchasing (it's usually 36 hours). If you cancel a subscription in time, we will not charge you, and the credits you used to book will automatically be returned to your account. If you cancel late, you won't be able to get a refund.

Always yours,
[redacted] *team*

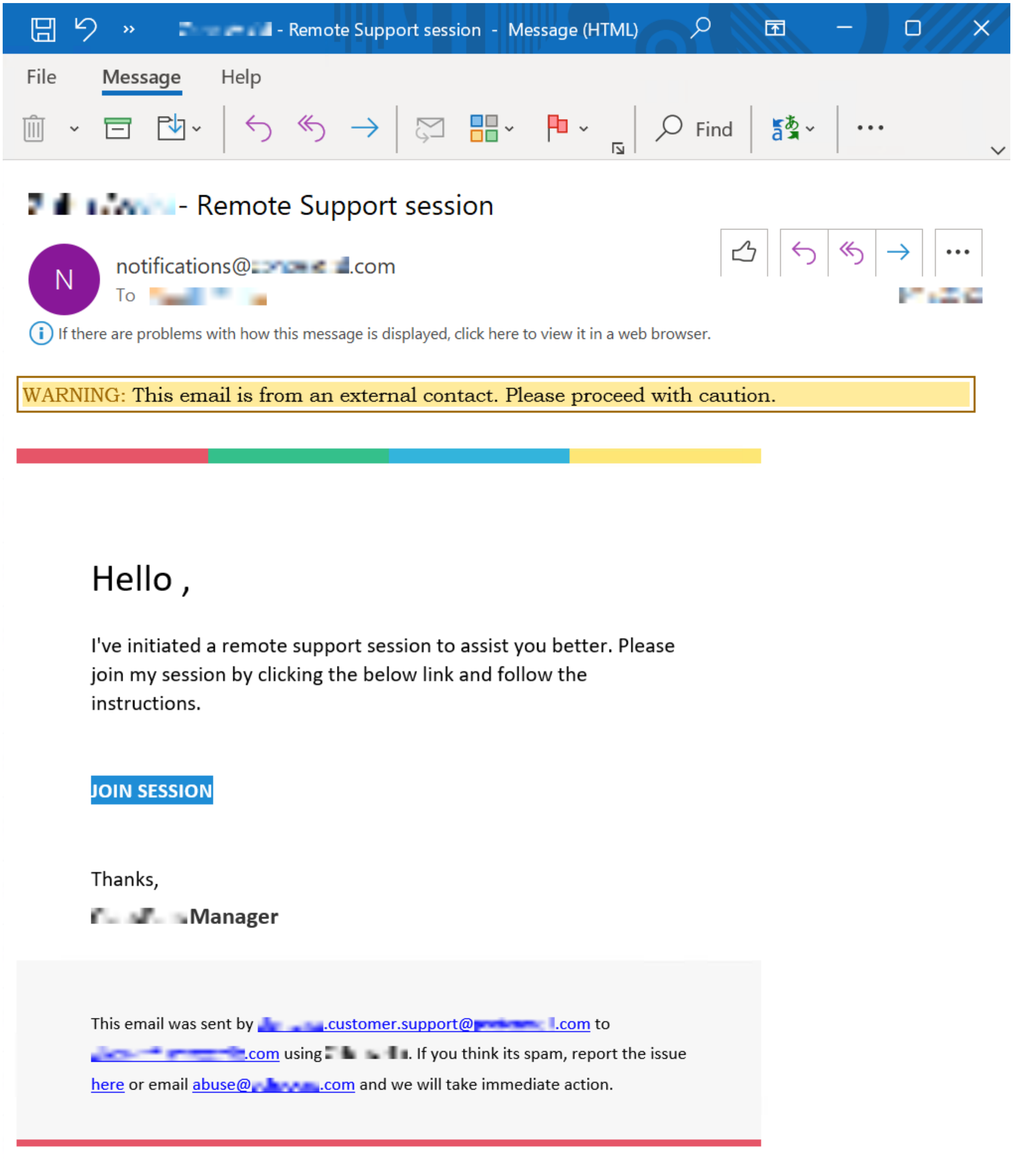
© 2022 [redacted] 🔒 Secured with SSL

Figure 2. Redacted fake invoice.

Early iterations of the extortion campaign recycled phone numbers, but later attacks either used a unique phone number per victim, or victims would be presented with a large pool of available phone numbers in the invoice.

The attacker registered all of the numbers they used via a Voice over IP (VoIP) provider. When the victim called one of the attacker's numbers, they were placed into a queue and eventually connected with an agent who sent a remote assist invitation for the remote support tool Zoho Assist.

The footer of these invitation emails (shown in Figure 3) revealed the email address the threat actor used to register with Zoho. In most incidents, the attacker chose an address from an encrypted email service provider to masquerade as the same vendor used in the fake invoice.



[redacted] - Remote Support session

notifications@[redacted].com
To [redacted]

[redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

WARNING: This email is from an external contact. Please proceed with caution.

Hello ,

I've initiated a remote support session to assist you better. Please join my session by clicking the below link and follow the instructions.

JOIN SESSION

Thanks,
[redacted] Manager

This email was sent by [redacted].customer.support@[redacted].com to [redacted].com using [redacted]. If you think its spam, report the issue here or email abuse@[redacted].com and we will take immediate action.

Figure 3. Redacted remote assistance invitation.

Once the victim connected to the session, the attacker took control of their keyboard and mouse, enabled clipboard access, and blanked out the screen to hide their actions.

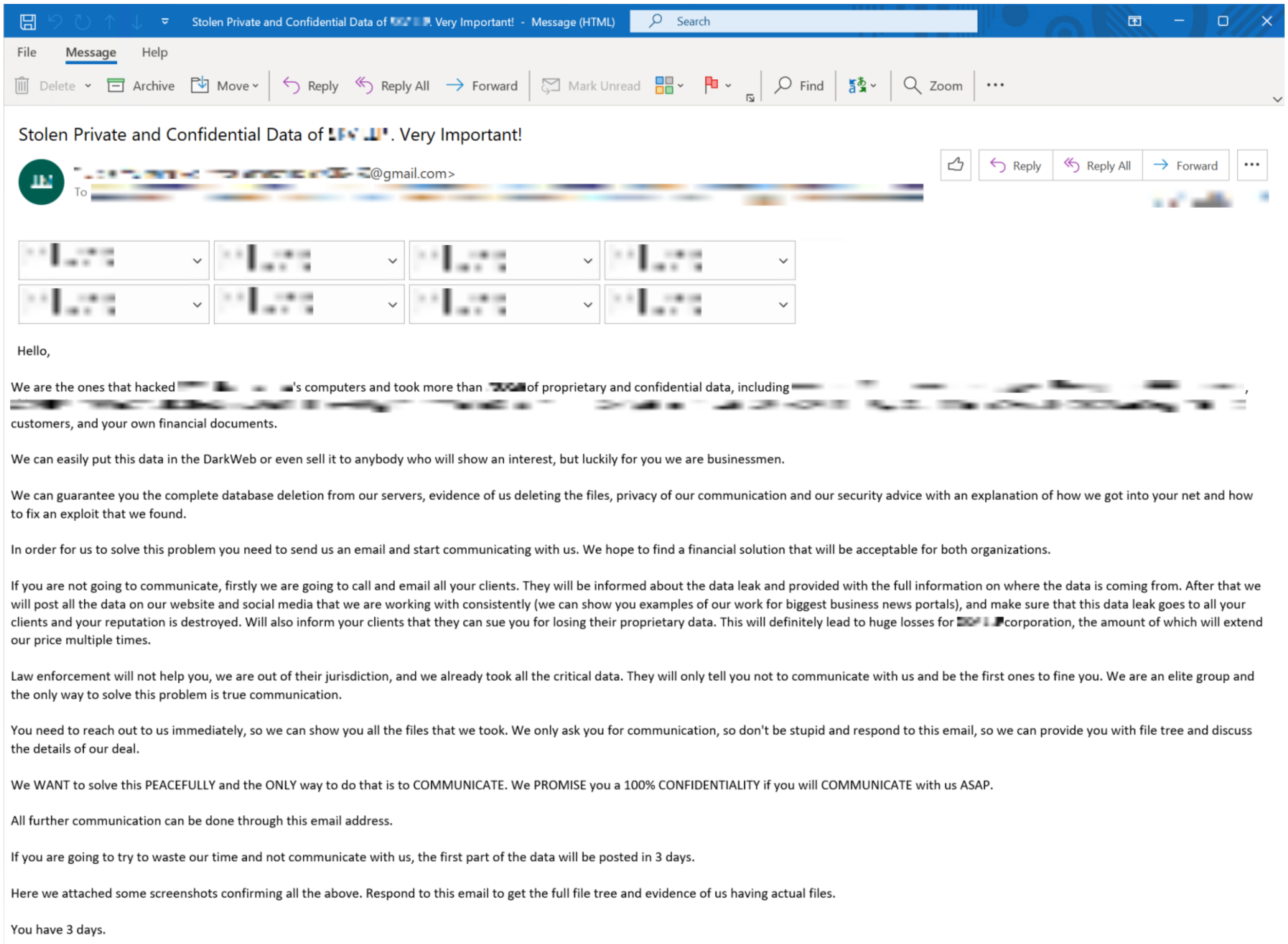
Once the attacker blanked the screen, they installed remote support software Syncro for persistence and open source file management tools Rclone or WinSCP for exfiltration. Early cases also included remote management tools Atera and Splashtop, but recently the attacker appears to have tightened their toolset.

In cases where the victim did not have administrative rights to their operating system, the attacker skipped installing software to establish persistence. Attackers instead downloaded and executed WinSCP Portable, which does not require administrative privileges and is able to run within the user's security context.

In cases where the attacker established persistence, exfiltration occurred hours to weeks after initial contact. Otherwise, the attacker only exfiltrated what they could during the call. The attacker exfiltrated data shortly before the attack.

The domains used early in the campaign were random words with a top-level domain (TLD) of .xyz. Later in the campaign, domains consistently followed the format of [5 letters].xyz. All observed domains fell into the 192.236.128[.]0/17 network range.

Exfiltration was followed with an extortion email, as shown in Figure 4. Like in other templates used in this campaign, the wording and format in the extortion email has evolved over time. In the cases Unit 42 investigated, the attacker claimed to have exfiltrated data in amounts ranging from a few gigabytes to over a terabyte.



Stolen Private and Confidential Data of [redacted]. Very Important!

[redacted]@gmail.com>

To [redacted]

[redacted]

Hello,

We are the ones that hacked [redacted]'s computers and took more than [redacted] of proprietary and confidential data, including [redacted], [redacted] customers, and your own financial documents.

We can easily put this data in the DarkWeb or even sell it to anybody who will show an interest, but luckily for you we are businessmen.

We can guarantee you the complete database deletion from our servers, evidence of us deleting the files, privacy of our communication and our security advice with an explanation of how we got into your net and how to fix an exploit that we found.

In order for us to solve this problem you need to send us an email and start communicating with us. We hope to find a financial solution that will be acceptable for both organizations.

If you are not going to communicate, firstly we are going to call and email all your clients. They will be informed about the data leak and provided with the full information on where the data is coming from. After that we will post all the data on our website and social media that we are working with consistently (we can show you examples of our work for biggest business news portals), and make sure that this data leak goes to all your clients and your reputation is destroyed. Will also inform your clients that they can sue you for losing their proprietary data. This will definitely lead to huge losses for [redacted]corporation, the amount of which will extend our price multiple times.

Law enforcement will not help you, we are out of their jurisdiction, and we already took all the critical data. They will only tell you not to communicate with us and be the first ones to fine you. We are an elite group and the only way to solve this problem is true communication.

You need to reach out to us immediately, so we can show you all the files that we took. We only ask you for communication, so don't be stupid and respond to this email, so we can provide you with file tree and discuss the details of our deal.

We WANT to solve this PEACEFULLY and the ONLY way to do that is to COMMUNICATE. We PROMISE you a 100% CONFIDENTIALITY if you will COMMUNICATE with us ASAP.

All further communication can be done through this email address.

If you are going to try to waste our time and not communicate with us, the first part of the data will be posted in 3 days.

Here we attached some screenshots confirming all the above. Respond to this email to get the full file tree and evidence of us having actual files.

You have 3 days.

Figure 4. Redacted extortion email.

The threat actor created unique Bitcoin wallets for each victim's extortion payments. These wallets contained only two or three transactions and were emptied immediately after funding.

Attacker's monetary demands ranged from 2-78 BTC. They researched the target organization's revenue and used it to justify this extortion amount. However, attackers were quick to offer discounts of approximately 25% for prompt payment.

Paying the attacker did not guarantee they would follow through with their promises. At times they stopped responding after confirming they had received payment, and did not follow through with negotiated commitments to provide proof of deletion.

Prevention and Detection

The threat actors behind this campaign have taken great pains to avoid all non-essential tools and malware, to minimize the potential for detection. Since there are very few early indicators that a victim is under attack, employee cybersecurity awareness training is the first line of defense.

People should always be cautious of messages that invoke fear or a sense of urgency. Do not respond directly to suspicious invoices. Contact the requester directly via the channels made available on the vendor's official website. People should also consult internal support channels before downloading or installing software on their corporate computers.

The second line of defense against this attack type is a robust security technology stack designed to detect behavioral anomalies in the environment. Palo Alto Networks customers receive protection from the attacks discussed in this blog through the Next-Generation Firewall and Cortex XDR detecting data exfiltration or connections to suspicious networks.

Conclusion

Unit 42 expects callback phishing attacks to increase in popularity due to the low per-target cost, low risk of detection and fast monetization. While groups that can establish infrastructure to handle inbound calls and identify sensitive data for exfiltration are likely to dominate the threat landscape initially, a low barrier to entry makes it probable that more threat actors will enter the fray.

Common observables suggest a pervasive multi-month campaign that is actively evolving. Therefore, organizations in currently targeted industries, such as legal and retail, should be particularly vigilant to avoid becoming victims.

All organizations should consider strengthening cybersecurity awareness training programs with a particular focus on unexpected invoices, as well as requests to establish a phone call or to install software. Additionally, expand investments in cybersecurity tools designed to detect and prevent anomalous activity, such as installing unrecognized software or exfiltrating sensitive data.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Additional Resources

Get updates from Palo Alto Networks!

Sign up to receive the latest news, cyber threat intelligence and research from us