

## New Threat Actor Uses Spanish Language Lures to Distribute Seldom Observed Bandook Malware

[proofpoint.com/us/blog/threat-insight/new-threat-actor-uses-spanish-language-lures-distribute-seldom-observed-bandook](https://proofpoint.com/us/blog/threat-insight/new-threat-actor-uses-spanish-language-lures-distribute-seldom-observed-bandook)

July 15, 2021

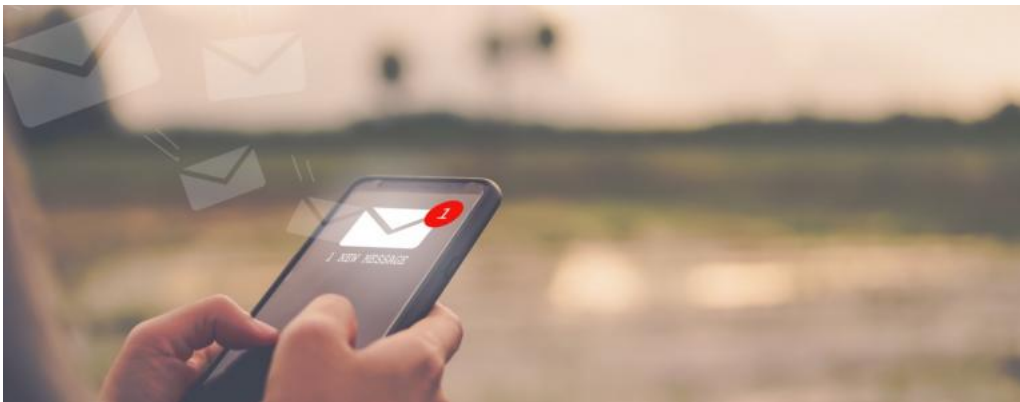




[Blog](#)

[Threat Insight](#)

New Threat Actor Uses Spanish Language Lures to Distribute Seldom Observed Bandoob Malware



July 19, 2021 Joe Wise, Konstantin Klinger, Selena Larson and the Proofpoint Threat Research Team

## Key Findings

- Proofpoint researchers identified a new group, TA2721 distributing Spanish-language email threats.
- The group often targets individuals with Spanish-language surnames at global organizations representing multiple different industries.
- The infection chain features a PDF containing a URL that leads to an encrypted RAR file which installs Bandook malware.
- The threat actor tends to use the same command and control (C2) infrastructure for weeks or months at a time. Proofpoint has only seen three different C2 domains in the last six months.
- Bandook is an old malware that is not used by many threat actors.

## Overview

Proofpoint researchers identified a new and highly active threat group, TA2721, also colloquially referred to by our researchers as Caliente Bandits. The group targets multiple industries from finance to entertainment. The group uses Spanish-language lures to distribute a known – but infrequently used – remote access trojan (RAT) called Bandook. Proofpoint researchers nicknamed the group Caliente Bandits for their use of Hotmail email accounts – “caliente” is the Spanish word for “hot.”

Proofpoint researchers began tracking this group in January 2021 and have observed TA2721 distribute email threats delivering Bandook every week since April. The campaigns are low volume, with fewer than 300 messages per campaign. The threats target entities globally, but the threat actors mostly impact individuals with Spanish surnames at these organizations. Cybersecurity firm ESET first published details of the malware used by this group.

## Campaign Details

TA2721 leverages the same type of budget or payment-themed lures throughout its campaigns to prompt a user to download a PDF.

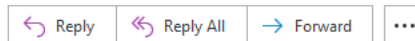
### COTIZACION REFRI TODO INTERNACIONAL, C.A



cuentasporpagar cpp <cuentasporpagar@refritodo.com>

To

Bcc



Sun 6/20/2021 10:26 PM



COTIZACION REFRI TODO INTERNACIONAL, C.A.pdf  
35 KB

**Buenas tardes, Sres. Refritodo Internacional.**

Reciba un cordial saludo de nuestra parte.

En los archivos adjuntos encontrará los siguientes documentos:

- COTIZACION y PRESUPUESTO con sello de pagado.

[Gracias por confiar una vez más en nosotros.](#)

Sin más que agregar.

Se despide por:

Figure 1: Email sample masquerading as a budget/quotation proposal.

The attached PDF contains an embedded URL and password that, when clicked, leads to the download of a password protected compressed executable that contains Bandook.



**COTIZACION JUNIO 21**



Figure 2: PDF containing a malicious link and password that leads to the download Bandook.

Proofpoint researchers observed TA2721 sending low-volume campaigns impacting less than 100 organizations at a time since January 2021. Targets include entities in manufacturing, automotive, food and beverage, entertainment and media, banking, insurance, and agriculture. Targeted organizations included entities in the U.S., Europe, and South America, both multinational organizations as well as smaller businesses. Only a handful of individuals are targeted at each organization, and most have Spanish-language surnames, such as Pérez, Castillo, Ortiz, etc.

The targeting suggests TA2721 conducts reconnaissance and attack planning to obtain employee data and contact information. The group appears to target individuals that may speak Spanish, increasingly the likelihood of a successful compromise.

### Delivery and Installation

---

Proofpoint researchers have observed this actor distributing two different Bandook variants. Bandook is commodity malware, but the tactics used in the campaigns demonstrate some attempts to evade detection and add additional effort for the attacker. The password-protection of the malicious archive is an easy way to make detection by automatic analysis products harder, and the specific focus on Spanish-language surnames coupled with low volume targeting suggests the threat actor conducted reconnaissance before deploying campaigns.

Nearly all observed campaigns contained PDF attachments containing links to the Bandook download, however in one June campaign the threat actor began using URLs in the messages directly.

TA2721 sends Spanish-language messages masquerading as companies located in South America, typically Venezuela, and Mexico. They are sent from Hotmail or Gmail email addresses. Subjects and filenames typically contain the terms "PRESUPUESTO (Budget)", "COTIZACION (Quotation)", and "rcibo de pago (receipt of payment)".

TA2721 generally uses the same command and control (C2) infrastructure for weeks or months at a time. For example:

- "s1[.]megawoc[.]com" was used in January.
- "d1[.]ngobmc[.]com" was used from March to June.
- "r1[.]panjo[.]club" was used since June.

The URLs observed from January through June 2021 used shortener URLs such as bit[.]ly and rebrand[.]ly links. These redirect to spideroak[.]com, an enterprise security file sharing platform. The URLs lead to the download of a password protected RAR file that installs Bandook.

### Malware Analysis

---

Bandook is a commercially available RAT written in Delphi and has been seen in the wild since at least 2007. Researchers have published details about multiple now publicly-[available variants](#). Bandook can capture screenshots, video, keylogging, and audio on the host, and can be used for information gathering operations.

Despite its availability and age of use, Proofpoint does not observe any other threat actor currently using this malware. In fact, since 2015, Proofpoint has observed around 40 total campaigns distributing this malware, with the 2021 TA2721 campaigns making up more than 50% of the observed activity. According to [MITRE ATT&CK's malware wiki](#), Bandoock is not widely used.

The following is an example of a TA2721 attack chain with the identified sample:

Subject: COMPROBANTE DE PAGO LOGSITICA CARACAS CA

Sender: logvencs@doca-safety[.]com

Attachment: comprobante de pago corporacion alfeca, c.a..pdf

PDF: 5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e

Bandoock: 561cb93118fef1966a3233ae7ffd31017823dd5aaad5dc1b2542e717055c197a

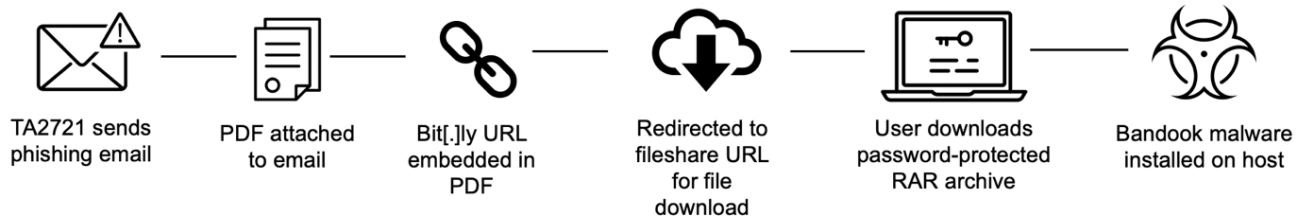


Figure 3: TA2721 attack chain.

The email contains a PDF attachment. A URL inside the PDF leads to a password protected RAR archive. The password for the RAR can be found in the initial PDF attachment (123456). Although the threat actors have changed URL shorteners and C2 domains, the archive password remains the same in every campaign.



Figure 4: PDF containing a link to malware hosted on the Spider Oak filesharing service.

The PDF contains the following URL:

hxxps[:]//bit[.]ly/bcomprob-sbaa1



192[.]168[.]0[.]107	IP address of infected machine
XTWGHENV	Computer name
dwrsApXT	Username
Seven	Operating System (Windows 7, Windows 10, etc.)
0d 3h 24m	Uptime
0	Unknown
5.2	Unknown, possible Bandoock versioning
JN2021	Unknown, possible campaign date or ID
21/6/2021	Current date

Proofpoint identified a third C2 server which pointed to a localhost address in all Bandoock samples associated with TA2721.

hxxp[://localhost:9991/KBL/

Proofpoint believes that this an artifact of the actor testing the malware that was mistakenly included by the actor after testing and attacking victims in real campaigns.

## Conclusion

Proofpoint assesses TA2721 will continue to use of a limited set of Bandoock malware variants, similar infection chain, and a select few C2 domains . The specific targeting suggests the threat actor conducts some reconnaissance on target entities before sending email threats.

Proofpoint researchers anticipate this actor will continue to use similar email lures, infection chains, and passwords while rotating through C2 domains.

## Indicators of Compromise (IOCs)

IOC	IOC Type	Description
ba1355c5e24c431a34bae10915f7cc9b4b1a8843dc79d9c63f1a13f0f9d099f7	SHA256 Hash	"cotizacion corporacion PDF June 21st
hxxps[://bit[.]ly/acotiz-abaa1	URL	URL inside PDF June 2
hxxps[://spideroak[.]com/storage/OVPXG4DJMRSXE33BNNPWC5LUN5PTMNBSHE2TM/shared/1764556-1-1105/COTIZACION 21[.]rar?17afe9bc9463ab5de84bd956cf4dfa9e	URL	Unshortened Bitly URL
a37c79c57ae9e2d681e5f9ef92798278d2bec68bcd91f08d96768e3fe8d5af19	SHA256 Hash	"COTIZACION 21.rar" Downloaded Rar archiv 21st (password: 123456
561cb93118fef1966a3233ae7ffd31017823dd5aad5dc1b2542e717055c197a	SHA256 Hash	"COTIZACION 21.exe" inside Rar June 21st
r3[.]panjo[.]club:7893	C2	Primary C2 of Bandoock 21st
hxxp[://ladvsa[.]club/Hayauaia/	C2	Fallback C2 of Bandoock 21st

5eaa1f5305f4c25292dff29257cd3e14ba3f956f6f8ddb206c0ee3e09af8244e	SHA256 Hash	"comprobante de pago c.a..pdf" PDF June 21st
hxxps[:]//bit[.]jy/bcomprob-sbaa1	URL	URL inside PDF June 2
hxxps[:]//spideroak[.]com/storage/OVPXG4DJMRSXE33BNNPWC5LUN5PTMNBSHE2TM/shared/1764556-1-1104/COMPROBANTE[.]rar?e22cde1331099985a6339fac899e3ebe	URL	Unshortened Bitly URL
39ce7b1e2dc1d4fe3bee24a9be8bea52bcb9028b50090731e5fff586106c264f	SHA256 Hash	"COMPROBANTE.rar" Downloaded Rar archiv 21st (password: 123456
561cb93118fef1966a3233ae7ffd31017823dd5aad5dc1b2542e717055c197a	SHA256 Hash	"COMPROBANTE.exe" inside Rar June 21st

## ET Signatures

2003549 - ET MALWARE Bandoock v1.2 Initial Connection and Report

2003550 - ET MALWARE Bandoock v1.2 Get Processes

2003551 - ET MALWARE Bandoock v1.2 Kill Process Command

2003552 - ET MALWARE Bandoock v1.2 Reporting Socks Proxy Active

2003553 - ET MALWARE Bandoock v1.2 Reporting Socks Proxy Off

2003554 - ET MALWARE Bandoock v1.2 Client Ping Reply

2003555 - ET MALWARE Bandoock v1.35 Initial Connection and Report

2003556 - ET MALWARE Bandoock v1.35 Keepalive Send

2003557 - ET MALWARE Bandoock v1.35 Keepalive Reply

2003558 - ET MALWARE Bandoock v1.35 Create Registry Key Command Send

2003559 - ET MALWARE Bandoock v1.35 Create Directory Command Send

2003560 - ET MALWARE Bandoock v1.35 Window List Command Send

2003561 - ET MALWARE Bandoock v1.35 Window List Reply

2003562 - ET MALWARE Bandoock v1.35 Get Processes Command Send

2003563 - ET MALWARE Bandoock v1.35 Start Socks5 Proxy Command Send

2003564 - ET MALWARE Bandoock v1.35 Socks5 Proxy Start Command Reply

2003565 - ET MALWARE Bandoock v1.35 Get Processes Command Reply

2003937 - ET MALWARE Bandoock iwebho/BBB-phish trojan leaking user data

2805272 - ETPRO MALWARE Bandoock Variant CnC Checkin

2810120 - ETPRO MALWARE Bandoock Retrieving Payloads set

2810121 - ETPRO MALWARE Bandoock Retrieving Payloads

2810122 - ETPRO MALWARE Bandoock Initial HTTP CnC Beacon

2810123 - ETPRO MALWARE Bandoock Initial HTTP CnC Beacon Response

2810124 - ETPRO MALWARE Bandoock HTTP CnC Beacon M1

2810125 - ETPRO MALWARE Bandoock HTTP CnC Beacon M2

2810126 - ETPRO MALWARE Bandoock HTTP CnC Beacon M3

2810127 - ETPRO MALWARE Bandoock HTTP CnC Beacon Response



2810128 - ETPRO MALWARE Bandook TCP CnC Beacon  
2810129 - ETPRO MALWARE Bandook TCP CnC Beacon Response  
2814671 - ETPRO MALWARE Bandook Retrieving Payload (cap)  
2814672 - ETPRO MALWARE Bandook Retrieving Payload (tv)  
2839949 - ETPRO MALWARE Bandook v0.5FM TCP CnC Beacon  
2841218 - ETPRO MALWARE Bandook TCP CnC Beacon  
2841802 - ETPRO MALWARE Suspected Bandook CnC M1  
2841803 - ETPRO MALWARE Suspected Bandook CnC Response  
2845793 - ETPRO MALWARE Suspected Bandook CnC M2  
2848605 - ETPRO MALWARE Bandook TCP CnC Beacon Keep-Alive (Inbound)  
2848616 - ETPRO MALWARE Bandook TCP CnC Beacon Keep-Alive (Inbound)  
2848728 - ETPRO MALWARE Bandook v0.5FM TCP CnC Beacon M2  
[Subscribe to the Proofpoint Blog](#)