**Spoofed Email Take is :**

Received: from PH7PR19MB5920.namprd19.prod.outlook.com (::1) by

MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Mon, 14 Aug 2023 11:20:14

+0000

Received: from FR3P281CA0021.DEUP281.PROD.OUTLOOK.COM (2603:10a6:d10:1c::11)

by PH7PR19MB5920.namprd19.prod.outlook.com (2603:10b6:510:1db::17) with

Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.6678.24; Mon, 14 Aug

2023 11:20:12 +0000

Received: from VI1EUR05FT049.eop-eur05.prod.protection.outlook.com

(2603:10a6:d10:1c:cafe::a5) by FR3P281CA0021.outlook.office365.com

(2603:10a6:d10:1c::11) with Microsoft SMTP Server (version=TLS1\_2,

cipher=TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384) id 15.20.6699.13 via Frontend

Transport; Mon, 14 Aug 2023 11:20:12 +0000

Authentication-Results: spf=softfail (sender IP is 221.238.162.115)

smtp.mailfrom=gmail.com; dkim=none (message not signed)

header.d=none;dmarc=fail action=none header.from=gmail.com;compauth=fail

reason=001

Received-SPF: SoftFail (protection.outlook.com: domain of transitioning

gmail.com discourages use of 221.238.162.115 as permitted sender)

Received: from mail.cistsec.com.cn (221.238.162.115) by

VI1EUR05FT049.mail.protection.outlook.com (10.233.242.225) with Microsoft

SMTP Server id 15.20.6699.13 via Frontend Transport; Mon, 14 Aug 2023

11:20:10 +0000

X-IncomingTopHeaderMarker:

OriginalChecksum:5E3D08407E034407DF458A8F26C5FD5A9FC9C0F165801BD58ACB83BB2D40A22E;UpperCasedChecksum:9C9ABB51EFFFF602248EFA96D3512DF9D2C34AAAE71D5BF1F37C5A74E632B61D;SizeAsReceived:512;Count:10

Received: from [147.78.103.148] (unknown [172.16.200.2])

by mail.cistsec.com.cn (Postfix) with ESMTP id 854BB1CB1295

for <phishing@pot>; Mon, 14 Aug 2023 19:59:03 +0800 (CST)

Content-Type: text/plain; charset="iso-8859-1"

Content-Transfer-Encoding: quoted-printable

Content-Description: Mail message body

Subject: PURE LOAN

To: phishing@pot

From: triumphantfinance@gmail.com

Date: Mon, 14 Aug 2023 11:20:01 -0700

Reply-To: info.triumphantfinance@gmail.com

X-IncomingHeaderCount: 10

Message-ID:

<c9c6f5e9-009f-4633-bead-dd8647a458bb@VI1EUR05FT049.eop-eur05.prod.protection.outlook.com>

Return-Path: triumphantfinance@gmail.com

X-MS-Exchange-Organization-ExpirationStartTime: 14 Aug 2023 11:20:11.1932

(UTC)

X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit

X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000

X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit

X-MS-Exchange-Organization-Network-Message-Id:

93205f7b-008a-4bb7-a42b-08db9cb86c89

X-EOPAttributedMessage: 0

X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0

X-MS-Exchange-Organization-MessageDirectionality: Incoming

X-MS-PublicTrafficType: Email

X-MS-TrafficTypeDiagnostic:

VI1EUR05FT049:EE\_|PH7PR19MB5920:EE\_|MN0PR19MB6312:EE\_

X-MS-Exchange-Organization-AuthSource:

VI1EUR05FT049.eop-eur05.prod.protection.outlook.com

X-MS-Exchange-Organization-AuthAs: Anonymous

X-MS-UserLastLogonTime: 8/14/2023 11:19:38 AM

X-MS-Office365-Filtering-Correlation-Id: 93205f7b-008a-4bb7-a42b-08db9cb86c89

X-MS-Exchange-EOPDirect: true

X-Sender-IP: 221.238.162.115

X-SID-PRA: TRIUMPHANTFINANCE@GMAIL.COM

X-SID-Result: FAIL

X-MS-Exchange-Organization-PCL: 2

X-MS-Exchange-Organization-SCL: 5

X-Microsoft-Antispam: BCL:0;

X-MS-Exchange-CrossTenant-OriginalArrivalTime: 14 Aug 2023 11:20:10.8338

(UTC)

X-MS-Exchange-CrossTenant-Network-Message-Id: 93205f7b-008a-4bb7-a42b-08db9cb86c89

X-MS-Exchange-CrossTenant-Id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa

X-MS-Exchange-CrossTenant-AuthSource:

VI1EUR05FT049.eop-eur05.prod.protection.outlook.com

X-MS-Exchange-CrossTenant-AuthAs: Anonymous

X-MS-Exchange-CrossTenant-FromEntityHeader: Internet

X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg:

00000000-0000-0000-0000-000000000000

X-MS-Exchange-Transport-CrossTenantHeadersStamped: PH7PR19MB5920

X-MS-Exchange-Transport-EndToEndLatency: 00:00:03.3037115

X-MS-Exchange-Processed-By-BccFoldering: 15.20.6678.022

X-Microsoft-Antispam-Mailbox-Delivery:

abwl:0;wl:0;pcwl:0;kl:0;dwl:0;dkl:0;rwl:0;ucf:0;jmr:0;ex:0;psp:0;auth:0;dest:J;OFR:SpamFilterAuthJ;ENG:(5062000305)(920221119095)(90000117)(920221120095)(90005022)(91005020)(91035115)(9050020)(9100341)(944500132)(2008001134)(2008121020)(4810010)(4910033)(8820095)(9610025)(9560006)(10180021)(9320005)(9245025)(120001);RF:JunkEmail;

X-Message-Info:

6hMotsjLow8rbft1SPm/AT9skYFgIq0xggPZxXnj4dE2MZF0Ywo8pqyBQp1xTc42ZMJ5CCoqzQGmDV+kfKyZEonNmy13q4VlOdU56QywXJ7cuQR/GjNLa2X0u9us5wgoLEkH1blofjwPG+soX+XMhQ4NQUFbzDsQFj5be2/yAVnfN8dal59tteg20AGMxrN8xfn1PnTsfmSVsHJtV4pIdg==

X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MjtHRD0zO1NDTD02

X-Microsoft-Antispam-Message-Info:

=?iso-8859-1?Q?09L8Z8ccqpFpaMFcVPiVacWssfEh0VhZd81HhtYgzBWXLDovH5Sp+YuURe?=

=?iso-8859-1?Q?JV5myO14lsGW+YvOpXZEgi6mvo30BC7u2HxlO4fL9gVzFXLQdfEBTU2A3d?=

=?iso-8859-1?Q?GcZ5Tf/0AyHDteuxpleX5G0mtXjqvctS1H2wFyOJBUfPncFy5murFrnIxq?=

=?iso-8859-1?Q?LOrCaDVguKrF5+47GKegyJjmIdnO6oUle7fbIjlffjrpW5wtbaAkq1PXmq?=

=?iso-8859-1?Q?Iz3h3Z7EtbbQ8cLuVC3jL54B0POId9neKqkLCVKVyOrCK/BTMAuad/5Fzo?=

=?iso-8859-1?Q?zDzINi9l8iSIT/cFfje2Jxv+0JkpWbWgm6HjPlxM4B9DU/j3a59bJdVkUZ?=

=?iso-8859-1?Q?NEKVjLIVyDER9dJz33elVx8u0A2T02xfgtcmYC97XtfE819zGfu0cyENo8?=

=?iso-8859-1?Q?gYHIcFT8TzQRkSFfojQXaM/vESPcmtDkjbVR0gGS6R/CIOSZDZP9mF6l+2?=

=?iso-8859-1?Q?JQOH4Kqq5ZPHU1fGYYL9uX+qBEWnRe8pG5LbbpGgNVfRTCe5QwsZeMZ3NA?=

=?iso-8859-1?Q?DJtGqzl2dD5kz2vunV189uVz9V3NY44YeJ7QzLZPCjUjGi+KvYOLcTLOnt?=

=?iso-8859-1?Q?QTRq3EZ+w8TbAG4/ORQOtJuaCfUQUlEGyBy9O5oOZEVl0y9P7iw2ZU8NA5?=

=?iso-8859-1?Q?vXVwdf+v7Q96+M1f2PGsJX5+d03bL1U/vObOrCQjpyFWTcK44YjT/hilN0?=

=?iso-8859-1?Q?8uNlaAoZHSbFLj8Xmx/bprYpwXBSrAkJfjxRzZ80sAUHjdg8cQQG0j9ibC?=

=?iso-8859-1?Q?y510J+G10ojxBhIvz5q5H/vfPmcMpKkSivavibb8+6kAbaAfgan/LqT/o5?=

=?iso-8859-1?Q?WmG2w6Be5+Q8oUMot/IQ6eG97GPvWzDCxuUuwdAIfiD4oNuKkRWuT3zoCZ?=

=?iso-8859-1?Q?Pax7VEY5SvK49b0jh105nHuE9RbFDtAQQCDdqlrvxPfDFAOE+dL4rC6ja+?=

=?iso-8859-1?Q?rqifZ2zIzdar0c12BpOMxXmtSUNA8LZnxMSfjx+o7RaFpZYH9+vi64NK/v?=

=?iso-8859-1?Q?uhBiE15xbRO1BBxMuIIiN5Qf5/F24lYkEA6S3GWLHo3d3WWg5qrLRFcsyu?=

=?iso-8859-1?Q?SMdMRMo8GMDrFtatWCjlt4Iv1UECEdkyBa0AB+aZXZJcv835M47Wvy/RNE?=

=?iso-8859-1?Q?iN294uHsGD4jD/Qv8coIcJaGCAoD9Gn0DeghNdaRfLRaWyj550l9ewUlfB?=

=?iso-8859-1?Q?0XKKDJtS7nzYW8tRGGN4uZP1gRCrVyqxmp8q26IhJ0x+yMmBRwDd7IxX/2?=

=?iso-8859-1?Q?pISqPuGd7xbNXMhx9r5a/7WAB4FFuruKtXbFJSmIao/vp9bPkDazrGZEqr?=

=?iso-8859-1?Q?s+aF4wE+TJx68Qt8D+JofB7YvTFVQhHsySG0rlztczk6nC829BtXTz3g1n?=

=?iso-8859-1?Q?RY3oAhtfYSX5DJOCsOmf5prIjhdlQkznpkChTEZIbUfdZZaVCjU8jLDtf+?=

=?iso-8859-1?Q?fjwd645SnZqOK77GIyv+eX9jm2If87ahS2MDmjxqG3sIhP1rRCbNevAacI?=

=?iso-8859-1?Q?1Wv0/iAosqARg5UqrD1qIVTz3ebiN0cJmFHLxEFuZKHjXROdQKRBj93zKd?=

=?iso-8859-1?Q?cY1ua2KqcZuEiznRXecZTqcmjdCxfky5sTUaq9Lhf6F3+Ut0Uhuh+ByULF?=

=?iso-8859-1?Q?yyXkHClo1qRIVLVz2InuwbXx9vvxt00VfHHqg7xPMlW1Vhyh5pCP0RZbwl?=

=?iso-8859-1?Q?tTaZqzoibliIcHY/e7LyMgYblVFxxYXKgcjRxfOFmMmP2v8OnQDC02//Pp?=

=?iso-8859-1?Q?+on0aPkh6z4yH2/8lGVIntxHJkSFq1SFp+/bCKpaEpr1m/PxEfN4v+No89?=

=?iso-8859-1?Q?yfjWi4JEt7+L6kStLcTCCEf3zJJdQin/4cz6j0ZmHOdQ1+al9dXwcMFrmk?=

=?iso-8859-1?Q?OpJyNYVnompsWeisBPT5/Csiga2iQBvetHiRBppNjflx56+cMVCIgGWK27?=

=?iso-8859-1?Q?+RIKu+joLXoZex+kuqhfirQiS99V/QgUt9IwidwoHiBL04CVivJDIoYe9/?=

=?iso-8859-1?Q?NuFrvlGHE4gS8hy5YDVaV/PshNDfOwMciQ2JMsHb0vRp9sqA0st95hmH1W?=

=?iso-8859-1?Q?lDouTuXWwiwgB/iOVPm4btemXSacS8jC9+i5sP0AjxIFsDMgqrssrh4bBC?=

=?iso-8859-1?Q?sfMwSjJdPWtMMUnHKm?=

MIME-Version: 1.0

Hello,

I hope this email finds you in good health and high spirits. I am reaching =

out to you today to discuss an exciting opportunity for financing that may =

be of interest to you.

At our reputable financial institution, we understand the challenges and fi=

nancial constraints that individuals and businesses often face when pursuin=

g their projects or expanding their operations. We are pleased to inform yo=

u that we offer an outstanding loan without collateral funding option, prov=

iding you with the necessary financial support without the need for collate=

ral. This financing solution comes with a highly competitive interest rate =

of 3% per annum, ensuring affordability and ease of repayment.

Whether you have a large-scale project or a small business venture, our loa=

n offer can cater to your financing needs. We have the capacity to provide =

funding ranging from 10,000 to 100 million (USD/EUR/POUNDS), giving you the=

flexibility to obtain the necessary capital required for your endeavor.

Additionally, we have an opportunity for you to act as a broker and earn a =

commission of 2% for every successful referral you make to us. By sharing t=

his financing offer with your network and connecting us with potential borr=

owers, you can earn a substantial commission while helping others access th=

e funding they require.

If you are interested in learning more about the details of our financing o=

ffer or the broker referral program, please reply to this email. Our dedica=

ted team will be more than happy to provide you with comprehensive informat=

ion, answer any questions you may have, and guide you through the applicati=

on process.

We believe that financial support should be accessible and beneficial, allo=

wing individuals and businesses to achieve their goals. Therefore, we invit=

e you to take advantage of this opportunity and explore the possibilities t=

hat our financing solution can offer.

Thank you for your time, and we look forward to the possibility of assistin=

g you in realizing your project or business ambitions.

**Examining sender's email address:**

The attacker made the From: and Return-Path: fields to look like Gmail, but the headers prove it was actually sent from mail.cistsec.com.cn (221.238.162.115), not from Google’s mail servers.

**Email headers for discrepancies**

Authentication-Results:

spf=softfail (sender IP is 221.238.162.115) smtp.mailfrom=gmail.com;

dkim=none (message not signed) header.d=none;

dmarc=fail action=none header.from=gmail.com;

compauth=fail reason=001

Not authenticated

**Malicious Links**

https://microsoft.com but the hover shows [http://malicious-domain[.]ru[/] login](http://malicious-domain[.]ru[/%5d%20login)

**Language**

No urgent or threatening language in the email body

**Spelling mistakes**

no obvious spelling mistakes

**Phishing Traits Found in the Email**

Suspicious Sender

Failed Email Authentication

Too-Good-To-Be-True Offer

Unverified Contact Info / Reply-to:

Reply-to is another Gmail address (info.triumphantfinance@gmail.com). Legitimate institutions use official domains.

Technical Anomalies

Received headers show email originating from unusual IPs (221.238.162.115) and internal networks not related to a financial institution.