

# Mass email campaign with a pinch of targeted spam

SL [securelist.com/agent-tesla-malicious-spam-campaign/107478/](https://securelist.com/agent-tesla-malicious-spam-campaign/107478/)



Authors

- **Expert** [Roman Dedenok](#)
- **Expert** [Artem Ushkov](#)

Most mass malicious mailing campaigns are very primitive and hardly diverse, with the content limited to several sentences offering the user to download archives that supposedly contain some urgent bills or unpaid fines. The email messages may contain no signatures or logos, with typos and other errors being fairly common. These mailings may target individual users or large corporations, with no significant differences in message content.



umairmahmood@  
PENDING INVOICE & SOA



Dear Sir/Ma,

Please find attached Invoice and SOA.

Best Regards...

### Example of a mass malicious mailing message

Things have started to change recently, though, as spammers began employing techniques that are typical of targeted attacks. In particular, they have been sending emails in the name of real companies, copying the senders' writing style and signatures.

### Customer email with an Easter egg inside

We discovered a noteworthy email message recently. In it, someone posing as a Malaysian prospect and using a fairly odd variety of English, asks the recipient to review some customer requirements and get back with the requested documents. The general format complies with the corporate correspondence standards: there is a logo that belongs to a real company and a signature that features sender details. Overall, the request looks legit, while the linguistic errors easily can be attributed to the sender being a non-native speaker.



Good morning  
My name is [redacted] (Procurement Dept) from [redacted] I would like to procure and request for quotation for the attached.  
The detail requirement and specifications attach for your references.  
Kindly provide us the below documentation as well  
a) Company Brochure  
b) Payment Terms  
If you have any inquiries, you can contact me directly thru email or phone. Your feedback are highly valuable.  
Appreciate your cooperation to promptly feedback on this inquiry latest by today



Procurement Officer  
[redacted] SMC  
[redacted] Puteri, Johor Bahru

\*Disclaimer:  
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error, please notify the system manager. This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. If you are not the intended recipient, you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

### ***The email from the “Malaysian prospect,” with a malicious attachment***

The only thing about the email that smells fishy is the sender’s address (newsletter@trade\*\*\*.com), as “newsletter” is typically used for news, not procurement. Besides, the sender’s domain name is different from the company name in the logo.

In another email, a purported Bulgarian customer inquires about the availability of some products and offers to discuss the details of a deal. The requested products list is said to be in the attachment, as in the previous specimen. The sender’s address, similarly suspicious, belongs to a Greek, not Bulgarian, domain, which apparently has no relation to the company whose name is used by the spammers.




 BULGARIA  <g.menis@.gr>  
 RE: RFQ

 RFQ 202207354RS.zip  
426 KB

Good morning,

We were directed by one of your clients to contact you.  
Please confirm use if you have the following in stock and return to us and also give us your best prices.  
I look forward to your prompt confirmation.

Thank you and best wishes.

 Sofia  
Mobile:+359   
Fax: +359 

### ***The email from the “Bulgarian customer,” with a malicious attachment***

What these two messages have in common is both the mailing scenario and the fact that neither looks generated by a machine. Looking closely at the message headers, we noticed that they shared a structure: a sequence of headers, MSGID format and email client were the same. Besides, the messages originated within a limited range of IP addresses. This suggested that they were part of one massive email campaign.

```
1 Received: [redacted]
2 From: "Mei, Gong" <Gong.Mei@[redacted]>
3 To: [redacted]
4 Subject: [redacted]
5 Date:
6 Message-ID: <20220630182439.233EA1467987716F@[redacted]>
7 MIME-Version:
8 Content-Type: multipart/mixed;
9     boundary="-----_NextPart_000_0012_F98335C7.B18BB244"
10

1 Received: [redacted]
2 From: "KAUFLAND BULGARIA FOOD & CO KD" <g.menis@[redacted]>
3 To: [redacted]
4 Subject: [redacted]
5 Date:
6 Message-ID: <20220630183712.B292358FD41A7F92@[redacted]>
7 MIME-Version:
8 Content-Type: multipart/mixed;
9     boundary="-----_NextPart_000_0012_0FB7D931.027F475F"
10
11
12
```

## Comparing the message headers of two malicious emails

Unlike the IP addresses and headers, the content varies. The spammers have been sending malicious archives addressed from a large number of companies, with the “request” text changing as well. This suggests that the operators invested quite some effort into preparations, which is uncharacteristic of this kind of campaigns.

## Statistics

---

From April till August, our systems detected 739,749 messages attributed to the campaign. The email activity peaked in June, with 194,100 detected messages, dropping to 178,510 in July and to 104,991 in August.

*Malicious email dynamics, April through August 2022 ([download](#))*

## Payload: Agent Tesla malware

---

We studied the contents of the archives attached to the emails, finding it to contain one of two unique files that belong to the same family. It is the widespread Agent Tesla malware, written in .NET and known since 2014. Its main objective is to fetch passwords stored in browsers and other applications, and forward these to the operator. While Agent Tesla most frequently forwards data via email, there are versions that drop the stolen data into a Telegram secret chat, on a website operated by the attackers or on an FTP server. The Agent Tesla version being spread by the campaign at hand is one the latest, capable of ripping password from the following applications.

- Browsers: Chrome, Edge, Firefox, Opera, 360 Browser, 7Star, Amigo, Brave, CentBrowser, Chedot, Chromium, Citrio, Cốc Cốc, Comodo Dragon, CoolNovo, Coowon, Elements Browser, Epic Privacy, Iridium Browser, Kometa, Liebao Browser, Orbitum, QIP Surf, Sleipnir 6, Sputnik, Torch Browser, Uran, Vivaldi, Yandex.Browser, QQ Browser, Cyberfox, IceDragon, Pale Moon, SeaMonkey, Waterfox, IceCat, K-Meleon.
- Email clients: Becky!, Opera Mail, Foxmail, Thunderbird, Claws, Outlook, The Bat!, eM Client, Mailbird, IncrediMail, Postbox, Pocomail
- FTP/SCP clients: WinSCP, WS\_FTP, FTPGetter, SmartFTP, FTP Navigator, Core FTP
- Databases: MySQL Workbench

- Virtual network computing clients: RealVNC, TightVNC, TigerVNC, UltraVNC, Windows RDP, cFTP
- VPN clients: NordVPN, OpenVPN
- Instant messaging programs: Psi/Psi+, Trillian

Agent Tesla is also capable of making screenshots, intercepting clipboard contents and logging keystrokes.

## Agent Tesla attack geography

---

Agent Tesla targets users around the world. According to our observations, the malware’s activity from May till August 2022 was the highest in Europe, Asia and Latin America. The largest number of victims (20,941) was recorded in Mexico. It was followed by Spain, with 18,090 users’ devices registering infection attempts, and Germany, where 14,880 users were affected.

Ten most-attacked counties by number of affected users:

Countries/territory	Users affected
Mexico	20,941
Spain	18,090
Germany	14,880
Turkey	13,326
Russian Federation	12,739
Italy	12,480
Malaysia	10,092
Vietnam	9,760
Brazil	8,851
Portugal	8,739

## Conclusion

---

The spam campaign we discovered is clear proof that cybercriminals can invest significant effort even in mass attacks. The email messages we studied appear to be high-quality imitations of business inquiries by real companies, only given away by the inappropriate

sender addresses. In all likelihood, these emails were composed and sent out manually. That said, our systems were detecting more than a hundred thousand of these emails each month, which targeted organizations all around the world.

The payload spread by the attackers is capable of stealing login data from an imposing number of applications. The data may be offered for sale on darkweb forums or used in targeted attacks against organizations. Agent Tesla is notably a long-known stealer, detected by most cybersecurity products. It is assigned the verdict Trojan-PSW.MSIL.Agensla by Kaspersky products.

## Indicators of compromise

---

### MD5 hashes of attached archives:

ddc607bb993b94c543c63808bebf682a  
862adb87b0b894d450f8914a353e3e9c  
a1ae8b0d794af648908e0345204ea192  
9d0364e1f625edb286b0d5541bb15357  
eee70de3ac0dc902b99ed33408e646c9

### MD5 hashes of the executables and details of attackers' email accounts used for sending and receiving data stolen by the sample:

64011a7871abb873c822b8b99082e8ab  
Mail from: info(a)essentialapparatus.co.ke  
Password: Info@2018  
Mail to: sales1.nuozhongsteel(a)gmail.com  
Mail server: mail.essentialapparatus.co.ke:587

b012cb8cfee0062632817d12d43f98b4  
Mail from: quality(a)keepprojects.in  
Password: quality#@!  
Mail to: quality(a)keepprojects.in  
Mail server: mail.keepprojects.in:587

- Agent Tesla
- Malicious spam
- Spam Letters
- Spammer techniques
- Thematic spam
- Trojan
- Trojan-stealer

Authors

- **Expert** Roman Dedenok
- **Expert** Artem Ushkov

Mass email campaign with a pinch of targeted spam

---

Your email address will not be published. Required fields are marked \*