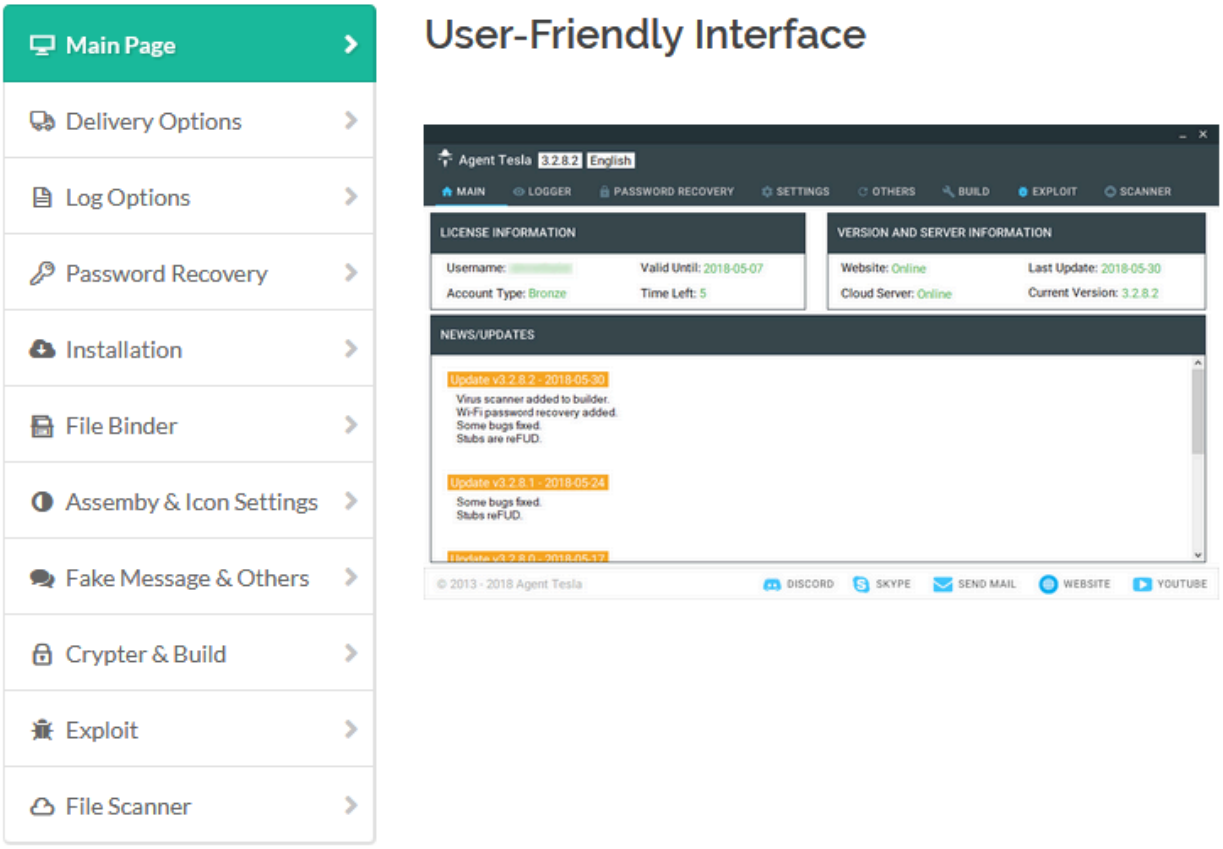
“Face mask manufacturer” supplies Agent Tesla Malware: campaign employs Covid-19 lures and sophisticated evasion techniques

By Elaine Dzuba

Published: 2020-08-27 · Archived: 2026-04-05 17:33:17 UTC

2020-08-27

6 min read



This blog originally appeared in August 2020 on the Area 1 Security website, and was issued in advance of Cloudflare's acquisition of Area 1 Security on April 1, 2022. Learn more.

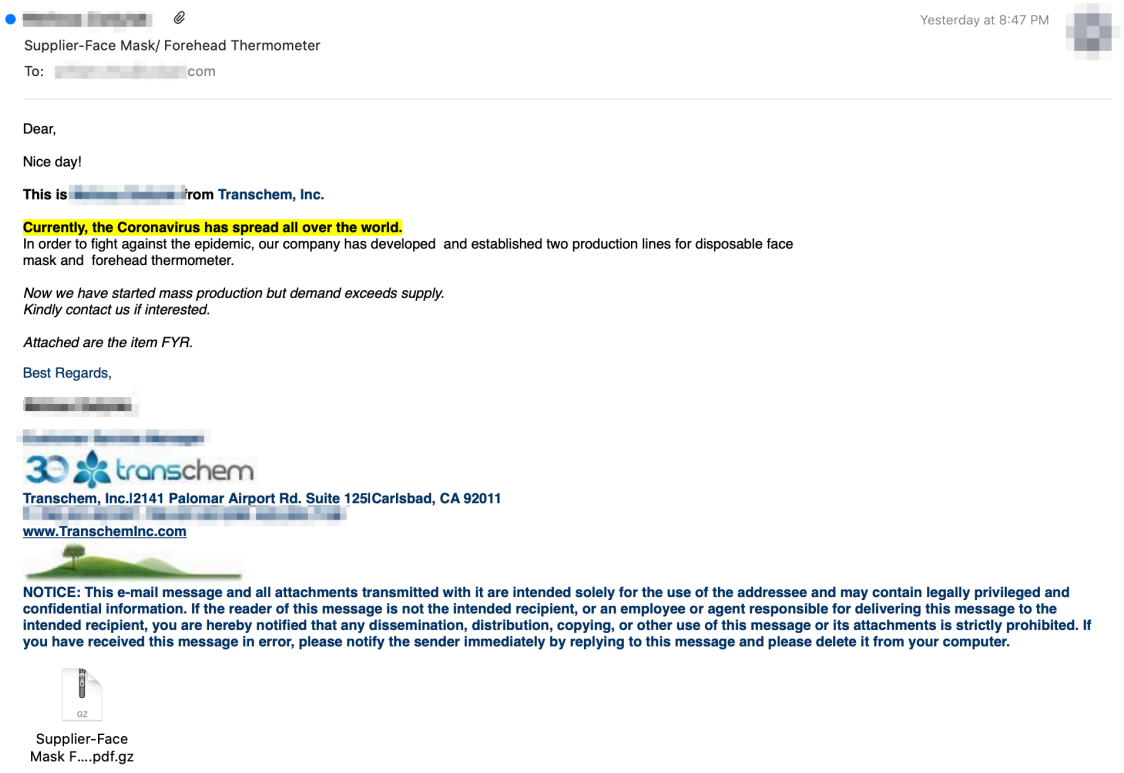
It’s no surprise that the world is currently facing a major shortage of the now-iconic blue surgical mask. Once only seen in hospitals and medical dramas, these masks are now the hottest selling streetwear. New state regulations now have businesses saying, “No Shirt, No Shoes, No Mask, No Service.” The incredible demand has led opportunistic businesses to get into the import/export of this vital article.

Recent phishing campaigns are also capitalizing on this trend by sending email attachments infected with Agent Tesla malware, an advanced Remote Access Trojan (RAT), to various companies under the guise of a mask production business venture. Area 1 Security caught these attacks filled with enticing traps that bypass legacy vendors and would have otherwise made their way into users' inboxes.

Face Mask and Forehead Thermometer Phishing

A prevalent phishing campaign loaded with a malicious executable is attempting to wreak havoc on companies worldwide, spanning numerous industry verticals. This campaign began as early as May, during the start of major lockdowns and mask shortages across the globe due to the COVID-19 pandemic. There have been numerous iterations of the campaign, but the main body of text remains the same.

The attacker lures targets by using language that preys on fears surrounding COVID-19 and claiming to offer face masks and forehead thermometers, products currently in high demand but short supply. To avoid detection, the phishing campaign generally follows a 10-day cycle wherein the threat actor slightly modifies their Tactics, Techniques, and Procedures (TTPs) before launching a new wave of emails. A recent phishing message from this campaign can be found below.



Yesterday at 8:47 PM

Supplier-Face Mask/ Forehead Thermometer

To: [redacted]com

Dear,

Nice day!

This is [redacted] from Transchem, Inc.

Currently, the Coronavirus has spread all over the world.
In order to fight against the epidemic, our company has developed and established two production lines for disposable face mask and forehead thermometer.

Now we have started mass production but demand exceeds supply.
Kindly contact us if interested.

Attached are the item FYR.

Best Regards,

[redacted]

transchem

Transchem, Inc.|2141 Palomar Airport Rd. Suite 125|Carlsbad, CA 92011

www.TranschemInc.com

NOTICE: This e-mail message and all attachments transmitted with it are intended solely for the use of the addressee and may contain legally privileged and confidential information. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution, copying, or other use of this message or its attachments is strictly prohibited. If you have received this message in error, please notify the sender immediately by replying to this message and please delete it from your computer.

GZ

Supplier-Face Mask F....pdf.gz

Transchem Inc. is not associated in any way with this attack

The attacker spoofs chemical manufacturers and import/export businesses to make the phishing message appear more legitimate. Area 1 Security's research shows that the attacker continually revises their phishing messages by periodically spoofing different companies in an effort to evade detection. For the example phish above, the attacker spoofed Transchem Inc., a legitimate chemical supplier. With previously spoofed companies, the attacker

included the real email address of the purported sender in the signature block; however, in this latest campaign, they remove it to reduce the chances of being detected.

To achieve the greatest success in reaching the most inboxes, the attacker uses a dynamic approach to stay one step ahead of common email security defenses:

- With each wave of the campaign, the attacker rotates to a new IP address in a likely attempt to bypass filters that only deny based on known sources of malicious activity;
- Furthermore, the malware in the attachment is continually modified in order to change its hash; and
- With a new hash value, the malware is effectively brand new — legacy detections that are configured to scan for known malicious hashes will not alert on this.

Additionally, due to flaws in the implementation and configuration of email authentication protocols, such as DMARC, SPF and DKIM, the attacker is able to successfully spoof the legitimate sender domains of numerous companies. This demonstrates that the complexity and nuances involved in setting up these protocols can leave you open to attack, and, even when implemented properly, are not enough to protect you from the dynamic phishing attacks that plague companies and individuals.

After bypassing a well-known email gateway and DMARC controls, the only defense left is for the email recipient to recognize this email as a phish. However, the attacker goes to great lengths to present an authentic façade. They:

- Impersonate real employees at various companies to fool unsuspecting targets into downloading purported information on the production of face masks and forehead thermometers;
- Include the legitimate logo of the spoofed company, as well as accurate mailing and contact details; and
- Include the URL in the email's signature block also leading to the legitimate website of the impersonated company.

The attacker is clearly going the extra mile to ensure this spoof will appear as authentic as possible for unsuspecting targets.

Once the email is delivered, recipients are a mere two steps away from executing the Agent Tesla RAT. The target only needs to extract the compressed attachment, then click on the resulting "PDF", which will launch the malware.

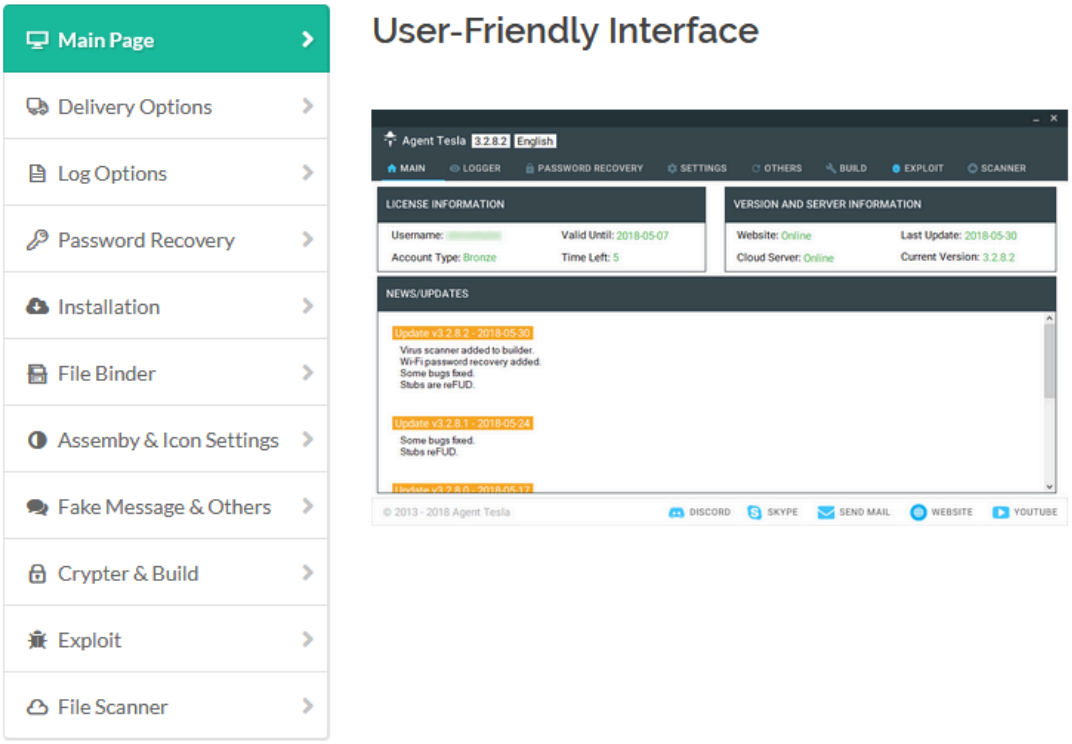
To further reduce suspicion, the attachment's file name is manipulated to make it appear legitimate. More specifically, the attacker always names the attached file "Supplier-Face Mask Forehead Thermometer.pdf.gz". The use of a double extension will often trick targets into thinking the file is a PDF, when in fact it's a compressed executable. This ruse is made possible by the fact that many modern operating systems do not display the file extension (in this case ".gz") for known extensions by default.

Once downloaded, victims may only see "Supplier-Face Mask Forehead Thermometer.pdf", which is the actual file name. To make matters worse, some legacy vendors inspect an attachment's extension *rather than the file*

properties itself, thus allowing compressed executables to bypass rule filtering that is based on file extension.

Analysis of Executable

The attachment is the focal point of this face mask-themed campaign. In order to carry out its information stealing capabilities, this infected attachment requires the target to take action by unzipping and clicking on the resulting file, "Supplier-Face Mask Forehead Thermometer.pdf.exe". If this file is opened, the victim host will be infected with Agent Tesla, a form of Malware-As-A-Service (MaaS), which provides attackers with a dashboard and user interface (UI) to monitor the success of their campaign. Agent Tesla is an advanced RAT that functions as a keylogger and information stealer, and its primary delivery method is via attachments in phishing emails.



What is Agent Tesla?

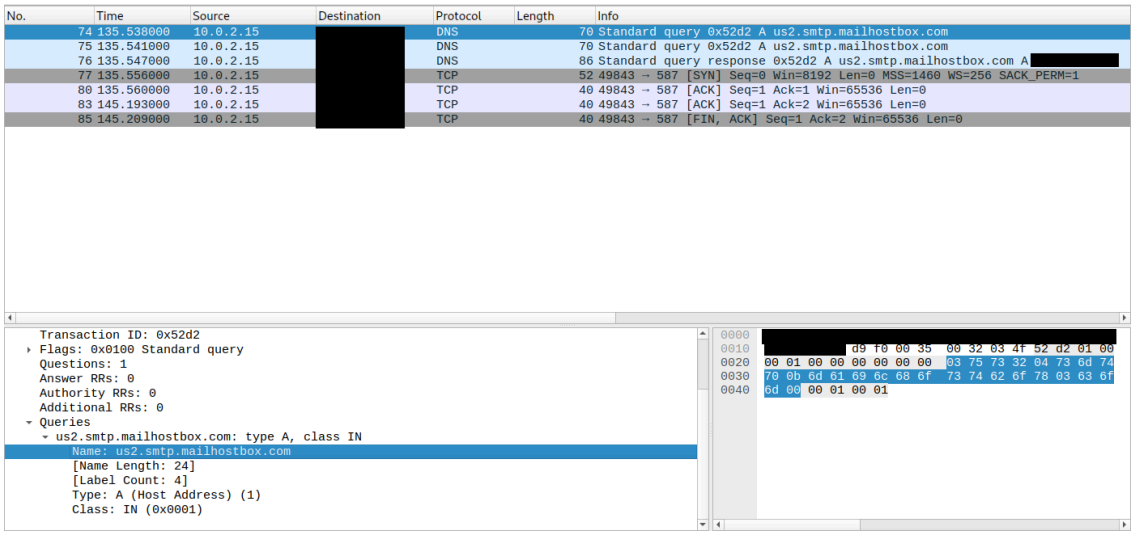
Although Agent Tesla first surfaced in 2014, it is making a resurgence as the preferred MaaS for attackers, superseding even TrickBot and Emotet. The main advantage of Agent Tesla is its ability to adapt and change to avoid detection, providing attackers with a stealthy platform to launch attacks and bypass security measures. Various tiers are available for purchase that provide additional licenses and different functionality. However, in typical internet fashion, there is a torrent available on Russian websites.

For the initial file, the attacker uses a 32-bit Windows executable to ensure that the malware can be executed on common Windows devices. This file is a trojan, appearing as a benign application but containing hidden, malicious functionality. This initial phase determines if it is in a malware analysis environment so the program can decide whether to proceed with the attack or go to sleep.

If the malware detects it is in a target's device, it will make a connection to the attacker's command and control (C2) server located at us2[.]smtp[.]mailhostbox[.]com. This initial connection does not contain any information;

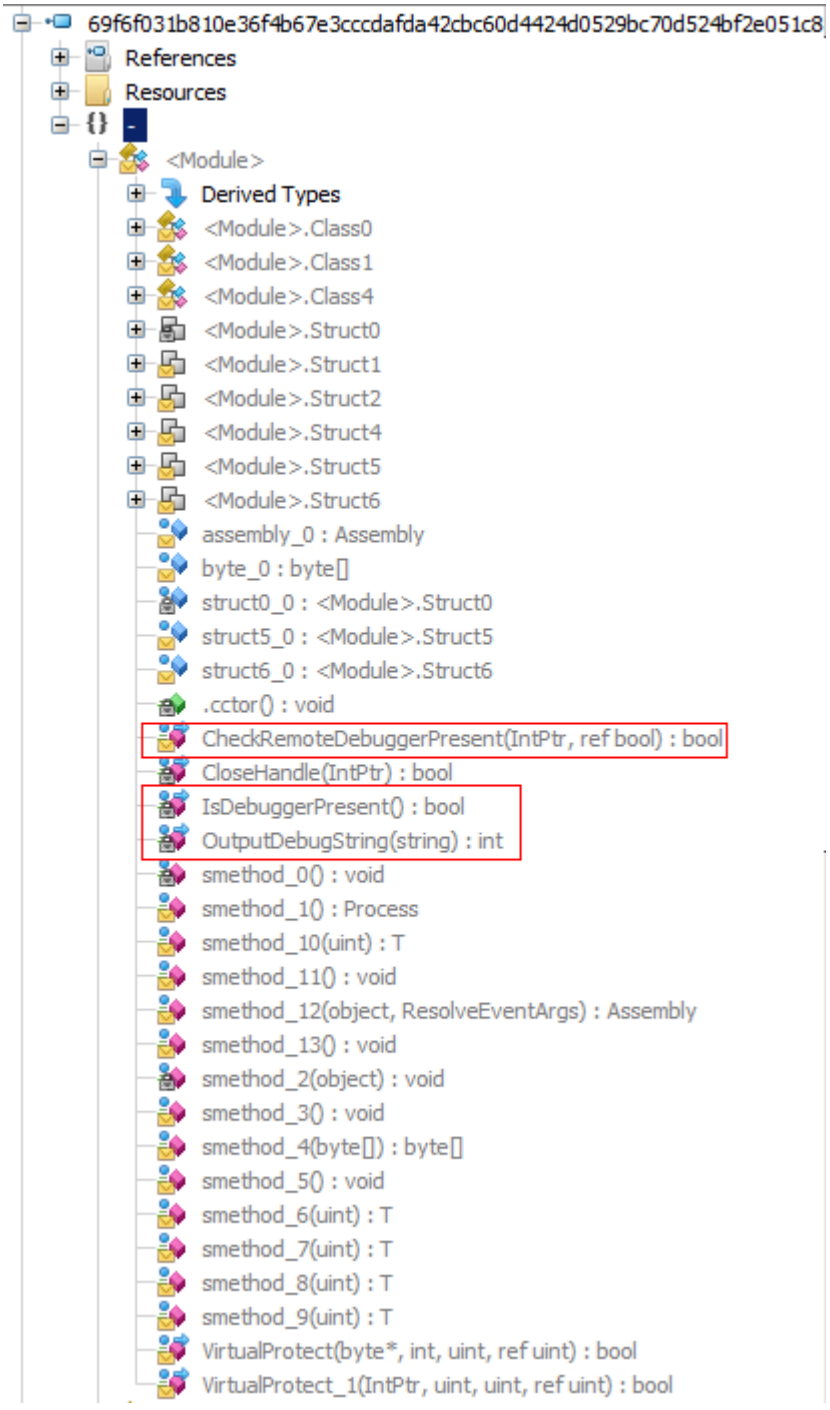
rather, it is only an attempt to provide the attacker with confirmation that the malware successfully ran on the target device.

The malware contains functionality to read the data within a victim's AppData folder, which contains browser credentials and credentials from email clients. The malware will attempt to load missing DLLs and download additional files in order to exfiltrate stolen information from the AppData folder. This data is sent to the C2 via SMTP as seen in packet capture below. This is a common tactic for exfiltration, given outgoing emails containing sensitive information are not likely to be marked as suspicious unless Data Loss Prevention (DLP) software is configured. The exfiltrated victim information is then available to the attacker via the Agent Tesla UI for use in future attacks.



With each new wave of this phishing campaign, the malware is updated by using a number of advanced obfuscation techniques to avoid detection by antivirus software:

- Firstly, the attacker generates a new hash for the attached file in order to circumvent defenses that leverage databases of known malware files. This is done in part by generating executables written for the .NET framework and constantly recompiling with alternative feature sets.
- Secondly, a number of anti-debugging methods are employed to halt any reverse engineering. These methods check if a debugger is present, as well as hiding threads and breakpoints from debugging tools.



Recommendations

If you think your device may have been compromised by malware, it's imperative to run a full scan of your system to check for signs of infection. It's also vital to keep your software and OS secure by installing the latest updates on a routine basis in order to reduce exposure to this "Face Mask Supplier" phishing campaign.

It is not enough to rely on email gateways, cloud email suites and traditional AV to protect against these types of attacks, as the threat actor is continually evolving and finding new ways to leverage commodity malware like Agent Tesla.

As attackers often rely on the end user to download and install malicious executables, it is also vital that employees are aware of common tactics an attacker may use to trick targets into opening malicious files. Unsolicited emails from unknown companies should be regarded as guilty until proven otherwise and reported to the security team. Additionally, any attachments containing compressed files should be handled with extreme caution, and any executable files should not be opened. These extra verifications are just a small precaution but go a long way toward ensuring the safety and security of your organization.

With each wave of the campaign, the malicious files and attacker infrastructure are altered to evade detection. Fortunately, Area 1 Security's comprehensive protection detects and blocks Agent Tesla-based phishing attacks and other targeted campaigns before they can cause any damage.

Area 1 Security's advanced Machine Learning and Artificial Intelligence technology allow our algorithms to uncover new tactics malicious actors are using to bypass legacy vendors and cloud email providers in real time versus waiting days or weeks for signature updates. Our time-zero detections lead the industry with reliable verdicts that stop phishing attempts at delivery time. This has many advantages over post-delivery retraction in that the user is never exposed to the attack.

Indicators of Compromise

Attachment: Supplier-Face Mask Forehead Thermometer.pdf.gz:

MD5: fdfaaf9efb8507262ee9b97324bbb69a

SHA1: 846da85a2f2e6e79ebc7ed84b00ed97af513c80f

SHA256: b419849ce915ede72fda1ea0b566651e233ef5eaffbf8b9211bd44085407ad5e

Executable: Supplier-Face Mask Forehead Thermometer.pdf.exe

MD5: 64bc654373549584f7e596de24e1d8cc

SHA1: 6a39bd3ddaa2c9846e2a4912a80fd718eaee622f

SHA256: 53445247552485c277400bafba84458670f0c1001c91b4f0bcc15935c12d662b

Command and Control Server:

us2[.]smtp[.]mailhostbox[.]com

Sender IP Addresses:

209[.]58[.]149[.]65

203[.]188[.]252[.]14

185[.]66[.]40[.]36

50[.]28[.]40[.]153

62[.]210[.]83[.]136

72[.]32[.]232[.]136

95[.]216[.]16[.]146

209[.]58[.]149[.]66

89[.]33[.]246[.]113

178[.]239[.]161[.]164

156[.]96[.]47[.]65

209[.]58[.]149[.]69

95[.]211[.]208[.]50

209[.]58[.]149[.]87

37[.]48[.]85[.]232

208[.]91[.]199[.]224

Cloudflare's connectivity cloud protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerates any website or Internet application, wards off DDoS attacks, keeps hackers at bay, and can help you on your journey to Zero Trust.

Visit 1.1.1.1 from any device to get started with our free app that makes your Internet faster and safer.

To learn more about our mission to help build a better Internet, start here. If you're looking for a new career direction, check out our open positions.

Email SecurityCloud Email SecurityPhishing
