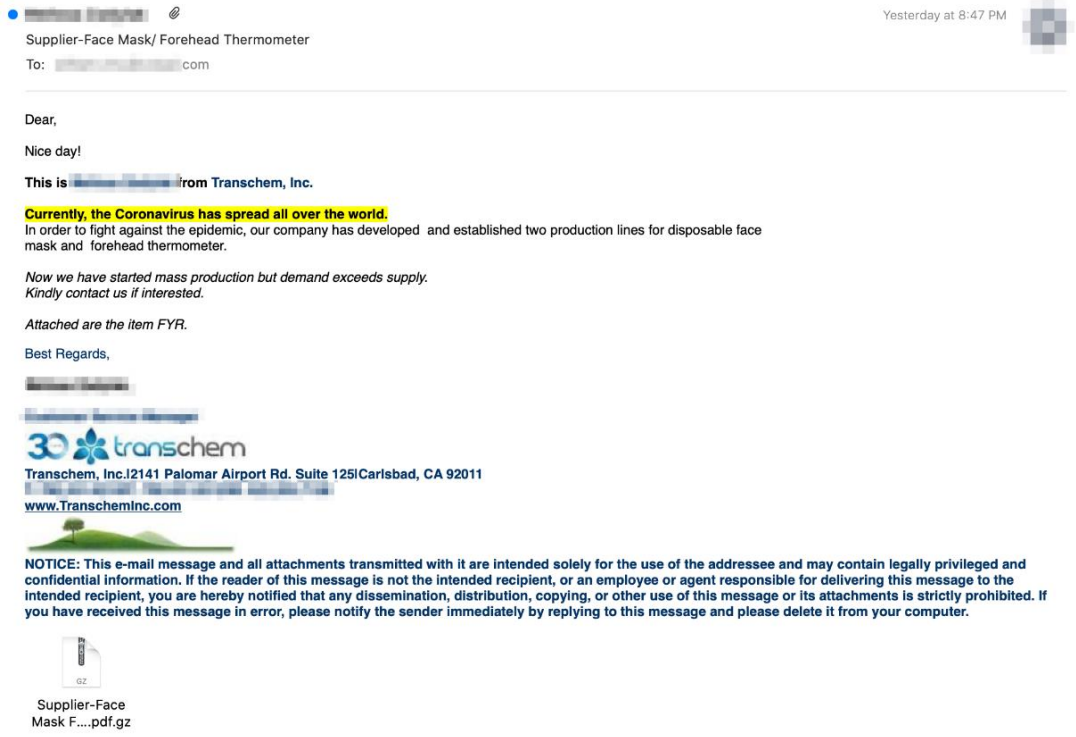
PPE-Themed Phishing Campaign Exploits COVID Shortages to Spread Malware

Executive Summary

A new phishing campaign is using COVID-19 personal protective equipment (PPE)-themed lures to spread Agent Tesla malware. This difficult-to-detect remote access Trojan (RAT) provides attackers with a dashboard to monitor the malware's keylogging and information stealing capabilities. The sophisticated malware campaign uses a 10-day cycle of rotated IP addresses and malware hashes to evade detection and increase the chances that a victim downloads and executes the malware. While the attackers have used a similar email body text throughout the campaign, the phishing emails imitate employees at actual chemical manufacture and import/export companies. Organizations should train their employees to avoid opening and executing email attachments and immediately scan any devices suspected to be infected.

Report

On August 27, 2020, Area 1 Security released a report warning of an ongoing phishing campaign spreading Agent Tesla remote access Trojan (RAT) malware using lures advertising personal protective equipment (PPE) effective against COVID-19. The campaign, which began in May and has since gone through multiple iterations, uses an email body advertising protective masks and forehead thermometers to entice victims to open email attachments containing the RAT. Once the attached compressed file is extracted and the victim clicks on the file "Supplier-Face Mask Forehead Thermometer.pdf.gz," the Agent Tesla malware is deployed. Agent Tesla is a sophisticated RAT that provides attackers with a full dashboard to monitor the keylogging and information-stealing functions of the malware.



Supplier-Face Mask/ Forehead Thermometer

To: [redacted]com

Yesterday at 8:47 PM

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

[redacted]

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.

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

Fig. 1. An example phishing email from the Agent Tesla campaign, using Transchem Inc.'s corporate branding. Source: Agent 1 Security

The included example email uses the branding of a legitimate but unaffiliated company, Transchem, Inc. While the campaign has gone through multiple iterations, the body text has remained consistent. Agent 1 Security also noted that "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." These TTP modifications include rotating IP addresses to avoid filters and modifying the malware itself to change its hash. "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." The attackers include details to make the fraudulent emails appear as real as possible, such as impersonating real chemical manufacture and import/export companies and employees and including the actual contact information for the company in signature blocks.

If organizations suspect a device or network is infected with Agent Tesla, security researchers recommend running a full scan on the system. Employees should be trained to refer unsolicited emails from unknown companies to the security team and to avoid interacting with or open compressed or executable files. Because the attackers have used consistent language in their phishing lures, organizations can also circulate the above example to their employees.

References

https://healthitsecurity.com/news/covid-19-ppe-phishing-campaign-delivers-agent-tesla-rat-malware
https://www.area1security.com/blog/facemask-phishing-agent-tesla-malware/