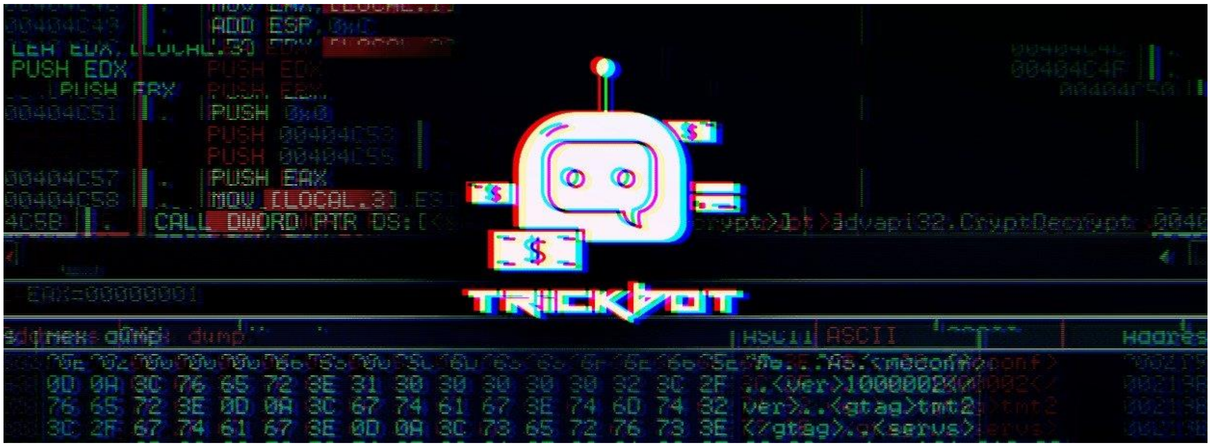
Trickbot in hundreds of unique COVID-19 lures per week

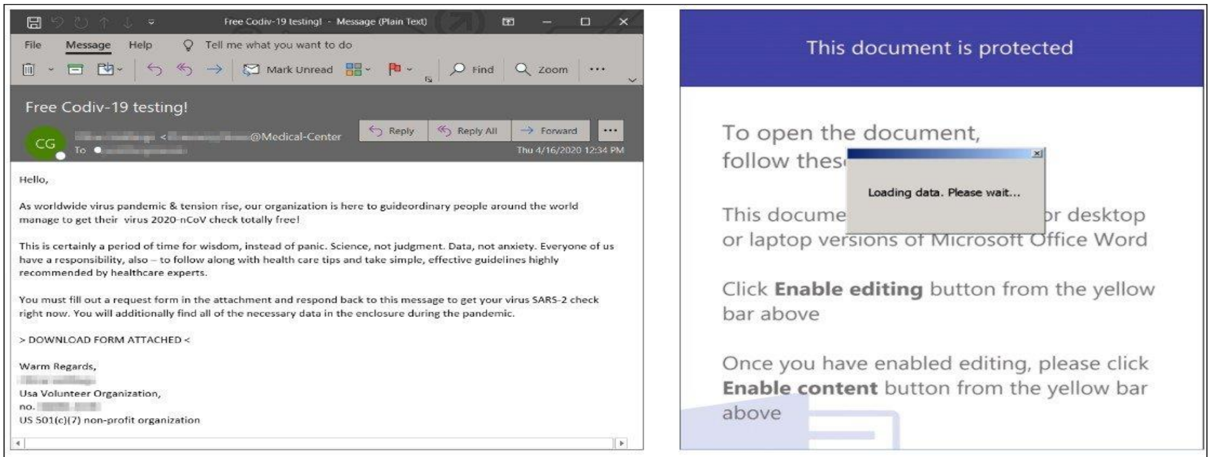


TrickBot is, at the moment, the malware showing up in the highest number of unique COVID-19 related malicious emails and attachments delivered to potential victims' inboxes based on Microsoft's Office 365 Advanced Threat Protection (ATP) data.

"Based on Office 365 ATP data, Trickbot is the most prolific malware operation using COVID-19 themed lures," according to a tweet from Microsoft's global network of security experts.

"This week's campaign uses several hundreds of unique macro-laced document attachments in emails that pose as message from a non-profit offering free COVID-19 test."

The macros used by the TrickBot gang are still using a delay before downloading the malicious payloads to evade sandbox analysis and emulation.


Free Codiv-19 testing! - Message (Plain Text)
File
Message
Help
Tell me what you want to do
Mark Unread
Find
Zoom
Reply
Reply All
Forward
CG

Free Codiv-19 testing!

[redacted] <[redacted]@Medical-Center
To [redacted]
Thu 4/16/2020 12:34 PM

Hello,

As worldwide virus pandemic & tension rise, our organization is here to guideordinary people around the world manage to get their virus 2020-nCoV check totally free!

This is certainly a period of time for wisdom, instead of panic. Science, not judgment. Data, not anxiety. Everyone of us have a responsibility, also – to follow along with health care tips and take simple, effective guidelines highly recommended by healthcare experts.

You must fill out a request form in the attachment and respond back to this message to get your virus SARS-2 check right now. You will additionally find all of the necessary data in the enclosure during the pandemic.

> DOWNLOAD FORM ATTACHED <

Warm Regards,
[redacted]
Usa Volunteer Organization,
no. [redacted]
US 501(c)(7) non-profit organization

This document is protected

To open the document, follow thes

Loading data. Please wait...

This docume r desktop or laptop versions of Microsoft Office Word

Click **Enable editing** button from the yellow bar above

Once you have enabled editing, please click **Enable content** button from the yellow bar above

Phishing email sample

Malicious macro in action

About a week ago, Microsoft said that it has already spotted 76 threat variants using COVID-19 themed lures since these attacks have started, with the TrickBot malware being the most active.

Roughly 60,000 attacks out of millions of targeted messages come with COVID-19 related malicious attachments or URLs per Microsoft, based on data collected from thousands of email phishing campaigns every week.

"In a single day, SmartScreen sees and processes more than 18,000 malicious COVID-19-themed URLs and IP addresses," Microsoft said.

Coronavirus-themed campaigns and upgrades
In late-March, the TrickBot gang was spotted while using a malicious Android app for bypassing two-factor authentication (2FA) protection used by various banks after stealing transaction auth numbers.

Right at the start of January, the TrickBot Trojan was seen switching to a new Windows 10 UAC bypass that allows it to execute itself with elevated privileges without ever having to show a User Account Control prompt in the process.

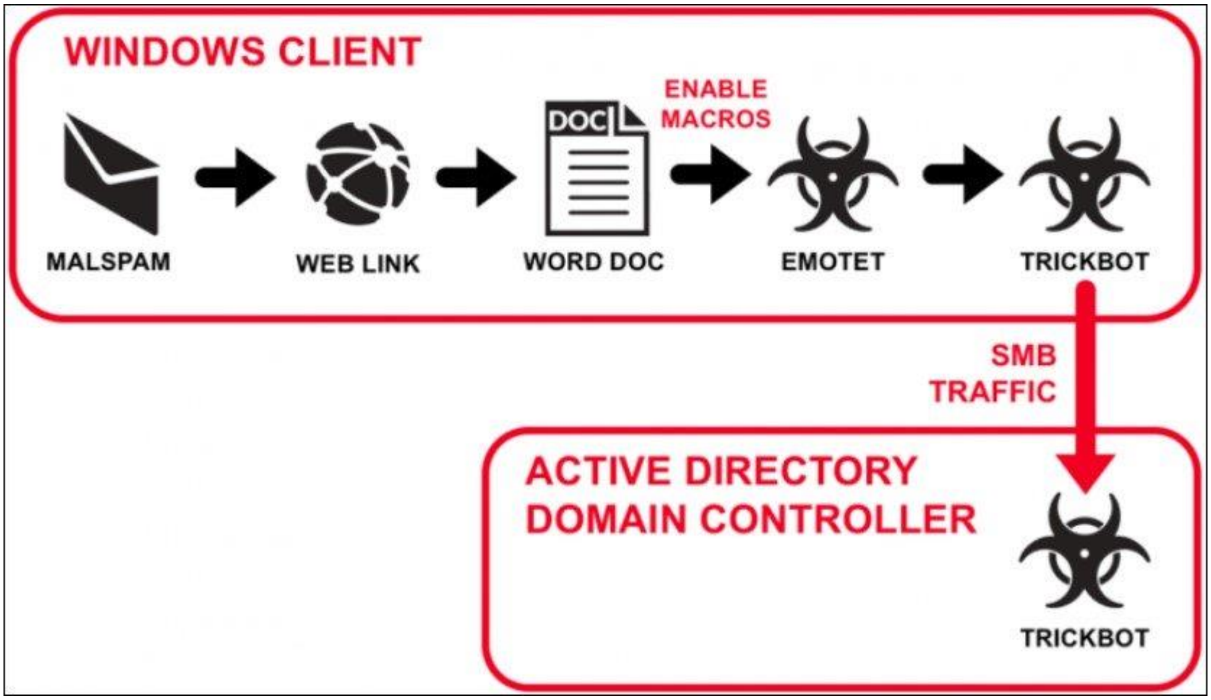
TrickBot was previously deployed as part of a spam campaign that impersonated a doctor at the World Health Organization (WHO) to take advantage of the public's fears surrounding the coronavirus pandemic to target Italians.

During February, both the TrickBot and Emotet Trojans started using strings with text from Coronavirus news stories attempting to bypass security solutions that use machine learning and artificial intelligence to detect malware.

Two days ago, Google announced that Gmail's built-in malware scanners blocked around 18 million phishing and malware emails using COVID-19-themed lures within a single week.

Regularly updated malware
TrickBot is malware strain initially developed as modular banking malware and continuously upgraded by its authors with new modules and capabilities since October 2016 when it was initially spotted in the wild.

Even though at first it was used only for harvesting and exfiltrating sensitive data, TrickBot has now evolved into a popular malware dropper that will further compromise infected systems by delivering other, usually a lot more dangerous, malware payloads.



TrickBot is typically delivered through Emotet and is commonly employed as part of multi-stage attacks to drop other malicious tools, with Ryuk ransomware being one of the most notable.

This normally happens after all potentially useful info —system info, credentials, interesting files — has been already stolen and delivered to its operators.

TrickBot is especially dangerous to enterprises as it can propagate throughout corporate networks and, if it gets admin access to a domain controller, it will steal the Active Directory database to collect other network credentials.

https://www.bleepingcomputer.com/news/security/microsoft-trickbot-in-hundreds-of-unique-covid-19-lures-per-week/?&web_view=true