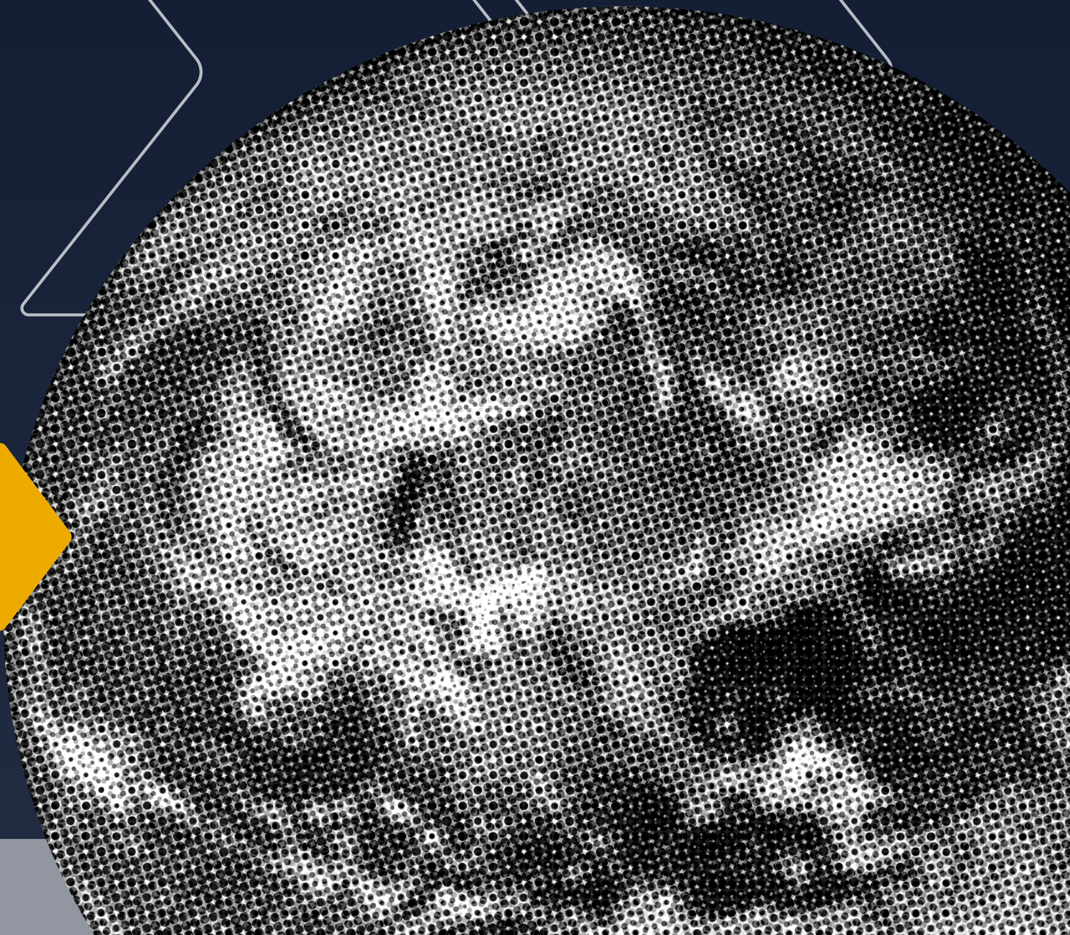
zix | appriver

2020 Mid-Year Global Threat Report



Executive Summary

The Zix | AppRiver Global Security Report for 2020 shares the threats and trends our cybersecurity analysts saw throughout the first half of the year. Perhaps unsurprisingly, attackers were quick to take advantage of the global pandemic, launching scams that played on peoples' anxieties as well as attacks targeting remote workforces. Analysts saw a continued surge of "living off the land" (LotL) attacks—attacks which hijack legitimate services—for phishing and distributing malware. Our analysts also observed a resurgence of banking trojans used by large-scale malware distributors.

In this report, we will take a deep dive into many of email security's top threats and trends. Additionally, we will discuss examples of prevalent attacks and explore their potential impact.

> *In this report, we will take a deep dive into many of email security's top threats and trends.*

Introduction

For much of the first half of 2020, world news was dominated by the COVID-19 pandemic—and so too was the threat landscape. Attackers were quick to embrace everything from personal protective equipment (PPE) offer scams to phony health alerts, which acted as covers for phishing scams or distributing malware. They also turned their attention to targeting remote workforces via scams involving collaboration tools.

Threat actors further embraced the use of legitimate services to deliver attack payloads, a technique known as "living off the land" (LotL). In early 2020, large-scale malware distributors brought banking trojans back to the fore—marking a shift from 2019, which was dominated by remote access trojans (RATs). Finally, ransomware returned to prominence in the email threat landscape and became the second most popular type of malware being distributed.

There's a lot going on in the world, and these changes are leaving their mark on the threat landscape. Next, this report provides an overview of the attack trends to be aware of, as well as tips on how to keep your organization safe.

> *This report provides an overview of the attack trends to be aware of, as well as tips on how to keep your organization safe.*

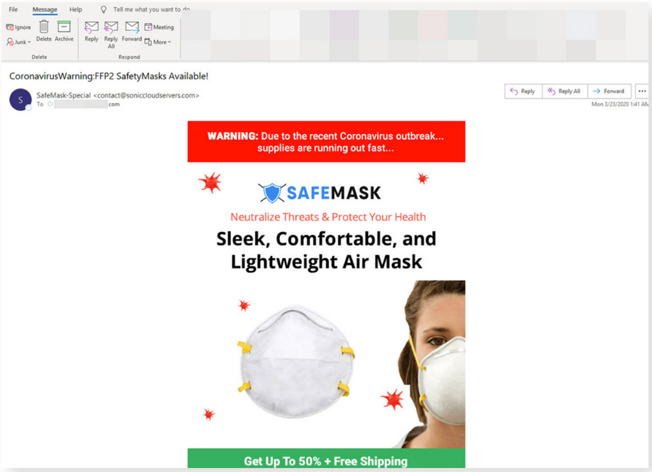
Pandemic and Remote Work Shape Threat Landscape

As the pandemic took hold and businesses worldwide scrambled to deploy remote workers, cybercriminals were quick to take advantage of the situation in every way imaginable. Cybercriminals quickly adapted their tactics to take advantage of peoples' distress. Sadly, this comes as no surprise, as we have seen threat actors work from the same playbook many times before.

For instance, just hours after the bombing of the Boston Marathon in 2013, we saw cybercriminals sending malicious emails claiming to contain footage from the bombing. There are countless examples like this, which is why we have been carefully monitoring—and continue to monitor—the current situation in anticipation of what is to come. So far, threat actors have used a variety of approaches. Some of the earliest attacks took the form of PPE scams but quickly iterated as criminals began to use malware and phishing attacks.

PPE Scams Target Anxious Consumers

Scams involving personal protective equipment arrived early on and blended in seamlessly with the global rush to purchase masks, hand sanitizer, COVID-19 test kits, and other medical supplies. Beginning in early January, we recorded an influx of spam (shown below) which pushed PPE to the general public. In most cases, this PPE does not really exist or it was a bait and switch where the products were inferior. Over time, these scams have become more pervasive. By early summer, the FBI was estimating millions of dollars in losses to these kinds of scams.



CoronavirusWarning:FFP2 SafetyMasks Available!

SafeMask-Special <contact@soniccloudservers.com>
To [redacted] com

Mon 3/23/2020 1:41 AM

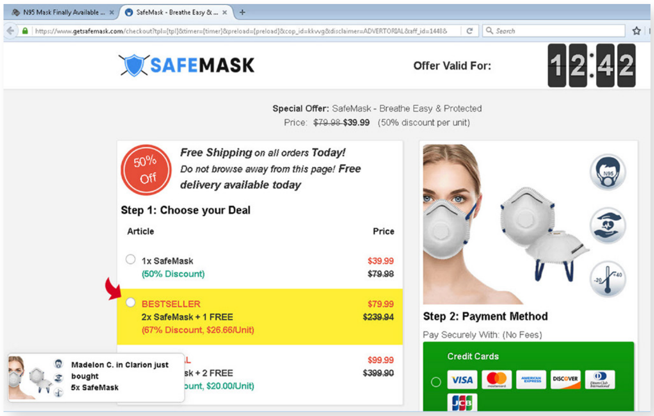
WARNING: Due to the recent Coronavirus outbreak... supplies are running out fast...

SAFEMASK

Neutralize Threats & Protect Your Health

Sleek, Comfortable, and Lightweight Air Mask

Get Up To 50% + Free Shipping



https://www.getsafemask.com/checkout?tpl={tpl}&timer={timer}&preload={preload}&cop_id=kkvvg&disclaimer=ADVERTORIAL&aff_id=1448&

SAFEMASK

Offer Valid For: 12:42

Special Offer: SafeMask - Breathe Easy & Protected
Price: ~~$79.98~~ $39.99 (50% discount per unit)

50% Off

Free Shipping on all orders Today!
Do not browse away from this page! Free delivery available today

Step 1: Choose your Deal

Article	Price
○ 1x SafeMask (50% Discount)	$39.99 ~~$79.98~~
○ BESTSELLER 2x SafeMask + 1 FREE (67% Discount, $26.66/Unit)	$79.99 ~~$239.94~~
L sk + 2 FREE ount, $20.00/Unit)	$99.99 ~~$399.90~~

Madelon C. in Clarion just bought 5x SafeMask

Step 2: Payment Method

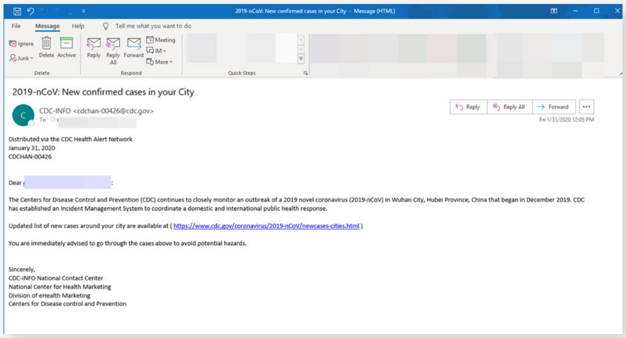
Pay Securely With: (No Fees)

Credit Cards

○ VISA DISCOVER JCB

Phishing and Malware Attacks Proliferate

Not long after the PPE scams arrived on the scene, we began seeing phishing and malware attacks make use of the pandemic. Many of the early phishing attacks preyed upon peoples' fascination with and fear of COVID-19 as it spread. On any given day, we were quarantining hundreds of thousands of phishing attempts posing as the U.S.'s Centers for Disease Control and Prevention (CDC) notifications. One particular attack (pictured) purported to contain information about cases at the addressee's location.



2019-nCoV: New confirmed cases in your City

CDC-INFO <cdchan-00426@cdc.gov>
To [redacted]

Fri 1/31/2020 12:05 PM

Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]:

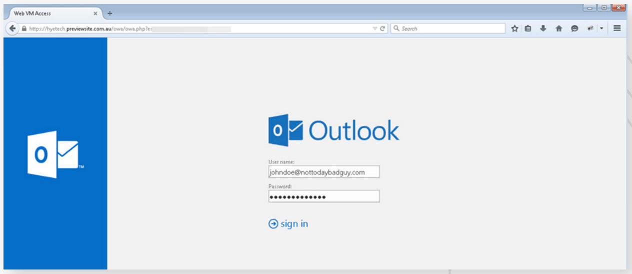
The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

The links in these messages led to phishing pages designed to harvest users' email credentials. Attackers would in turn use these credentials to launch more targeted phishing attacks, wire fraud scams, and to distribute malware.



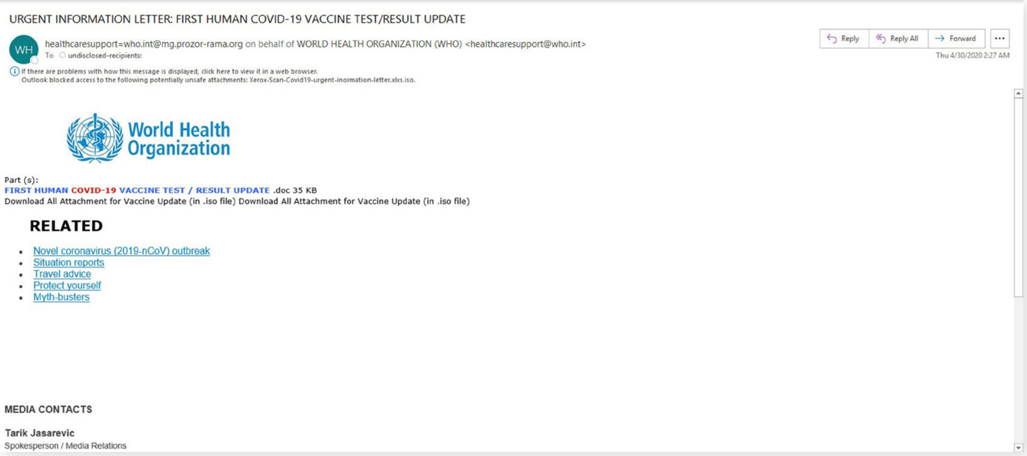
https://hyetech.previewsite.com.au/owa/owa.php?e= [redacted]

User name: johndoe@nottodaybadguy.com

Password: ••••••••••••••

By mid-March, we were seeing a large influx of email attacks attempting to deliver malware while operating under the guise of the pandemic. Threat actors utilized a number of variations on the pandemic theme to accomplish their goals. Some of the most popular formats included health alerts from the CDC or World Health Organization (WHO) or offers of relief funds, such as loans from the Small Business Administration (SBA). The most prominent malware type in these attacks was spyware/RATs, which we'll explore in more detail in the malware section below.

Other types of attacks such as business email compromise (BEC) wire transfer, gift card, and direct deposit-change scams also began to shift tactics slightly by adopting remote work and pandemic themes. These attacks were well-positioned to succeed during these events as they rely on humans taking the email at face value and not communicating with the ostensible sender, which would expose the scam. Stuck at home, users were less likely to meet friends and family face-to-face to be able to verify these claims.



URGENT INFORMATION LETTER: FIRST HUMAN COVID-19 VACCINE TEST/RESULT UPDATE

healthcaresupport=who.int@mg.prozor-rama.org on behalf of WORLD HEALTH ORGANIZATION (WHO) <healthcaresupport@who.int>
To ○ undisclosed-recipients:

Thu 4/30/2020 2:27 AM

If there are problems with how this message is displayed, click here to view it in a web browser.
Outlook blocked access to the following potentially unsafe attachments: Xerox-Scan-Covid19-urgent-inormation-letter.xlxs.iso.

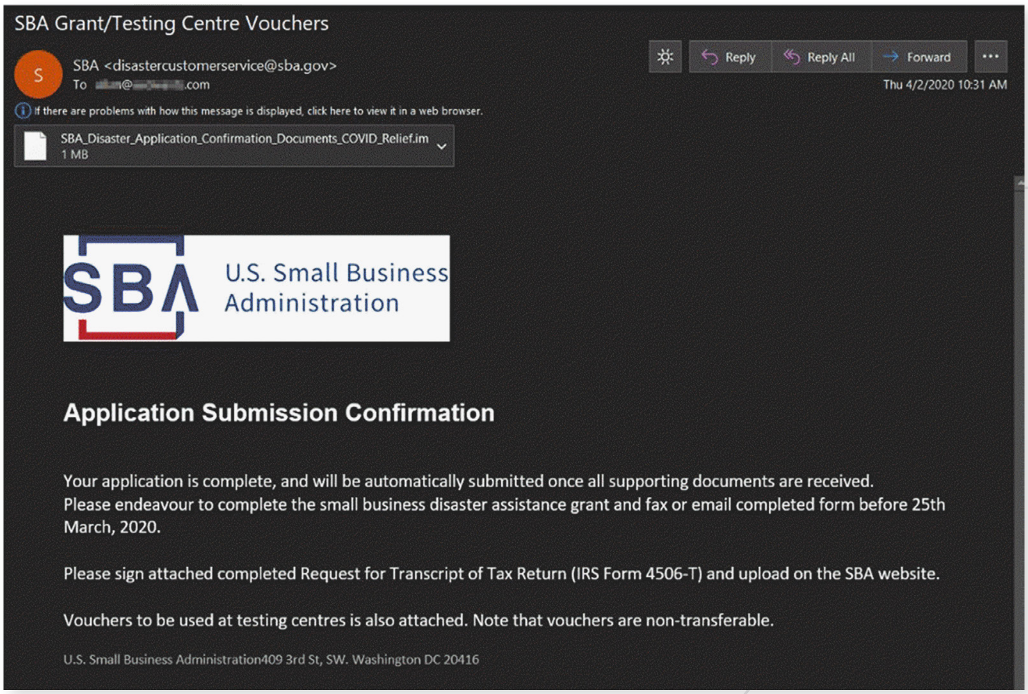
Part (s):
FIRST HUMAN COVID-19 VACCINE TEST / RESULT UPDATE .doc 35 KB
Download All Attachment for Vaccine Update (in .iso file) Download All Attachment for Vaccine Update (in .iso file)

RELATED

- Novel coronavirus (2019-nCoV) outbreak
- Situation reports
- Travel advice
- Protect yourself
- Myth-busters

MEDIA CONTACTS

Tarik Jasarevic
Spokesperson / Media Relations



SBA Grant/Testing Centre Vouchers

SBA <disastercustomerservice@sba.gov>
To [redacted]@[redacted].com

Thu 4/2/2020 10:31 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

SBA_Disaster_Application_Confirmation_Documents_COVID_Relief.im
1 MB

Application Submission Confirmation

Your application is complete, and will be automatically submitted once all supporting documents are received.
Please endeavour to complete the small business disaster assistance grant and fax or email completed form before 25th March, 2020.

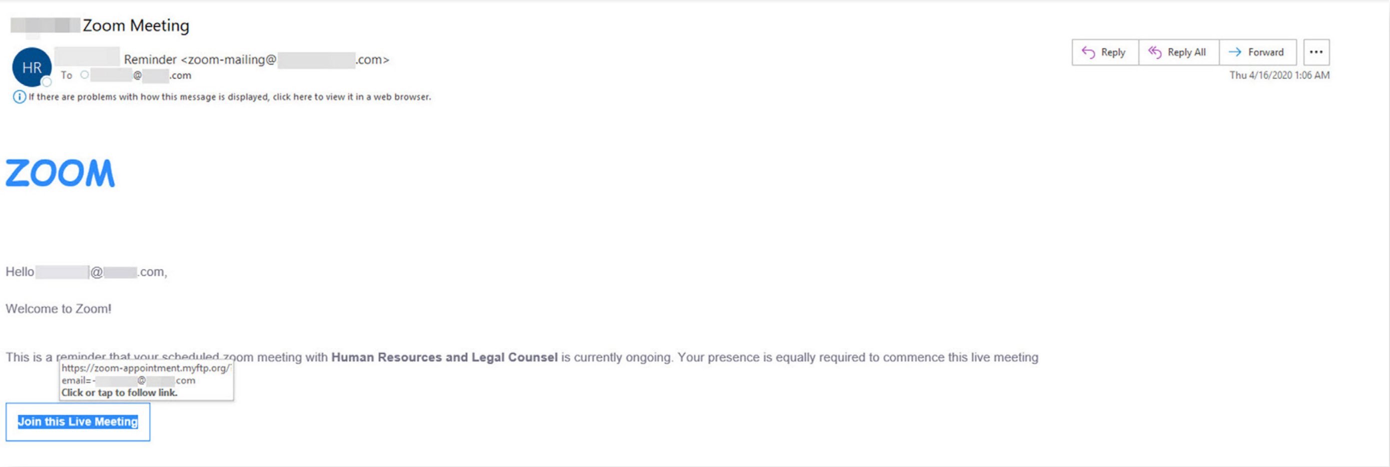
Please sign attached completed Request for Transcript of Tax Return (IRS Form 4506-T) and upload on the SBA website.

Vouchers to be used at testing centres is also attached. Note that vouchers are non-transferable.

U.S. Small Business Administration409 3rd St, SW. Washington DC 20416

Work From Home Exploited

Through the first half of 2020, we observed an uptick in attacks posing as collaboration and productivity solutions. Perhaps the most prominent and relevant were attacks leveraging the Zoom brand. Taking advantage of the "Zoom boom" was a no-brainer as its usage skyrocketed—Zoom gained more new users in the first few months of 2020 than it did in all of the previous year. Many of those new users were rookies to the platform and were therefore more susceptible to attacks posing as legitimate Zoom notifications. This example (pictured below) was one of the many attacks we captured attempting to pose as a Zoom notification.



[redacted] Zoom Meeting

HR [redacted] Reminder <zoom-mailing@[redacted].com>

To [redacted]@[redacted].com

ⓘ If there are problems with how this message is displayed, click here to view it in a web browser.

Thu 4/16/2020 1:06 AM

Hello [redacted]@[redacted].com,

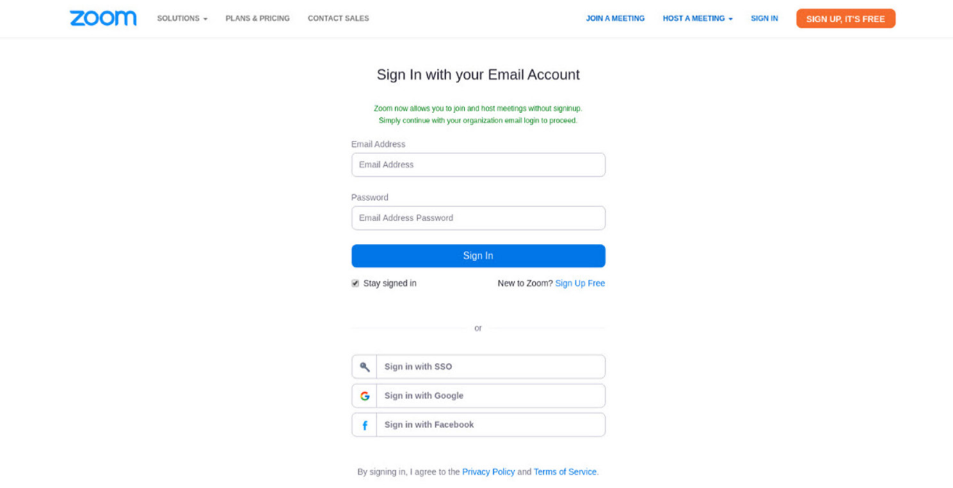
Welcome to Zoom!

This is a reminder that your scheduled zoom meeting with **Human Resources and Legal Counsel** is currently ongoing. Your presence is equally required to commence this live meeting

https://zoom-appointment.myftp.org/
email=-[redacted]@[redacted]com
Click or tap to follow link.

Join this Live Meeting

The link in the message in this case, led to another credential harvesting site.



Sign In with your Email Account

Zoom now allows you to join and host meetings without signinup.
Simply continue with your organization email login to proceed.

Email Address
Email Address

Password
Email Address Password

Sign In

☑ Stay signed in

New to Zoom? Sign Up Free

or

Sign in with SSO

Sign in with Google

Sign in with Facebook

By signing in, I agree to the Privacy Policy and Terms of Service.

Every day it seems more evident COVID-19 will be with us for a considerable time, so we expect these attacks to continue to evolve as new opportunities present themselves. Organizations should focus on reducing the risk associated with these attacks by making employees aware of what to look for. Additionally, businesses may want to revisit acceptable use policies and update them for the reality of long-term remote work.

Malware Threats

While many threat groups have transitioned to business email compromise (BEC) attacks, malware remains a major email threat for businesses of all sizes. In the early half of 2020, banking trojans and ransomware were the favorites of botnets, whereas remote access trojans (RATs) were preferred by other threat actors. While in previous years, ransomware distribution models seemed to be trending to non-email methods, in early 2020, we saw a return to email distribution by some ransomware distributors.

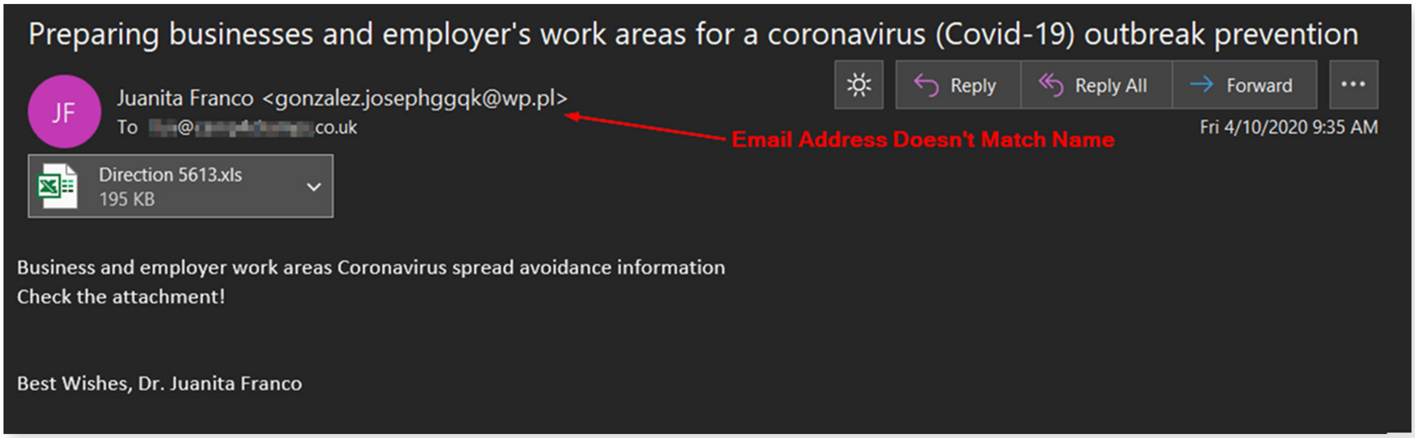
Banking Trojan - Dridex

Over the first half of this year, the top malware caught by our filters was the Dridex banking trojan. In the first six months of 2020 alone, we captured over 1.5 million malicious messages which contained loaders to deploy this malware on customers' machines. Most of the messages took the form of innocuous-looking Microsoft Excel attachments using .xls or .xlsm file extensions. These attachments were intended to be opened on Windows machines.

Dridex's capabilities include:

- Infiltrating web browsers (typically to steal banking credentials)
- Sending unauthorized money transfers
- Keylogging user input
- Capturing screenshots

But that's not all. Cybercriminals often use Dridex to gain an initial foothold before they load DoppelPaymer or BitPaymer ransomware into a corporate environment. Some recent reports indicate that threat actors may also be shifting more towards WastedLocker, a new ransomware, as a follow-up attack. Worryingly, many of their ransom demands directed against enterprise targets range well into the millions of dollars. The U.S. Department of Justice has placed a bounty of $5 million on each of the two suspected actors behind the Dridex malware.



Preparing businesses and employer's work areas for a coronavirus (Covid-19) outbreak prevention

Juanita Franco <gonzalez.josephggqk@wp.pl>
To [redacted]@[redacted]co.uk

Email Address Doesn't Match Name

Fri 4/10/2020 9:35 AM

Direction 5613.xls
195 KB

Business and employer work areas Coronavirus spread avoidance information
Check the attachment!

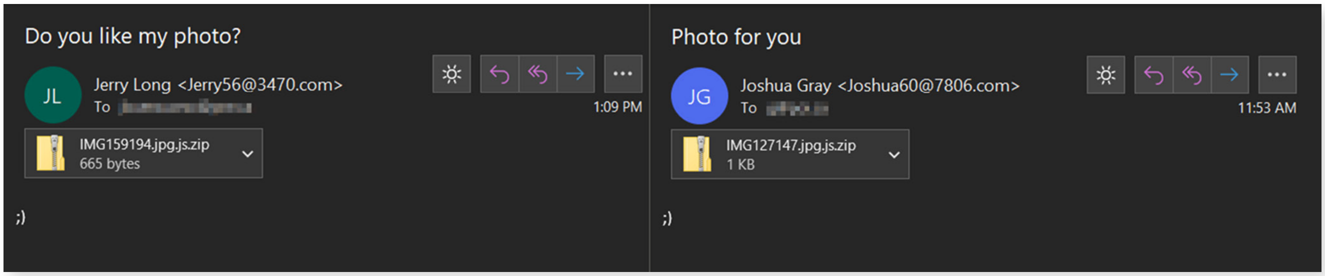
Best Wishes, Dr. Juanita Franco

Dridex Email Example

Ransomware - Avaddon

Coming in close behind Dridex, the second-highest volume of malware attempts over the first half of the year came from Avaddon ransomware attacks. This new ransomware was distributed by the Phorphiex (also known as Trik) botnet in campaigns that exceeded 300,000 messages per day. The name Avaddon is a nod to the Hebrew word *abaddon*, meaning doom or destruction.

The emails themselves used relatively simple lures enticing the recipient with a subject line such as, "Do you like my photo?" or "Photo for you"—and nothing except a wink emoticon in the body. Attached to each message was a zip file that contained the malicious JavaScript that used both PowerShell and Bitsadmin commands to pull down the Avaddon ransomware payload.



Do you like my photo?

JL Jerry Long <Jerry56@3470.com>
To [redacted]
1:09 PM

IMG159194.jpg.js.zip
665 bytes

;)

Photo for you

JG Joshua Gray <Joshua60@7806.com>
To [redacted]
11:53 AM

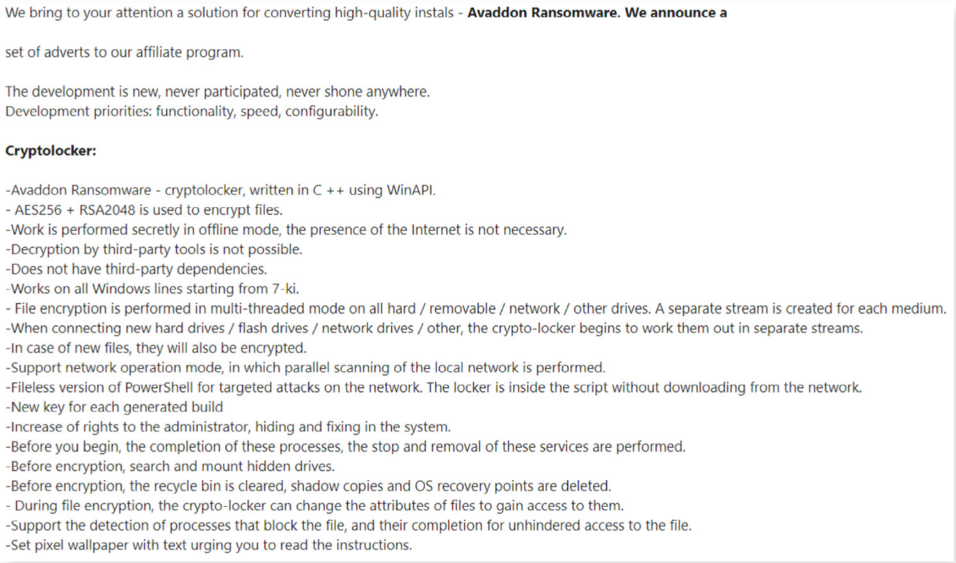
IMG127147.jpg.js.zip
1 KB

;)

Avaddon Email Examples

In addition to distribution via Phorphix botnet, Avaddon creators used a ransomware as a service (RaaS) affiliate payment model to recruit talent for distribution. Affiliates would receive 65% of the ransom paid by victims and the creators would receive a 35% cut.

The creators advertised their service on a popular Russian dark web forum. Like many other groups that operate out of the Commonwealth of Independent States (CIS)—an intergovernmental organization comprised of Russia and other post-Soviet republics—the creators forbade affiliates from targeting users in CIS member states. We noticed that an IP address the attackers had used for command and control communication 217.8.117[.]63 was also used in previous Predator the Thief attacks. This is not the first time it has been advertised on Russian dark web forums.



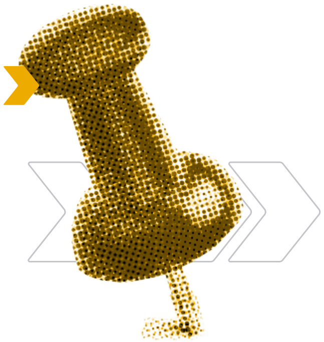
We bring to your attention a solution for converting high-quality instals - **Avaddon Ransomware. We announce a**

set of adverts to our affiliate program.

The development is new, never participated, never shone anywhere.
Development priorities: functionality, speed, configurability.

Cryptolocker:

-Avaddon Ransomware - cryptolocker, written in C ++ using WinAPI.
- AES256 + RSA2048 is used to encrypt files.
-Work is performed secretly in offline mode, the presence of the Internet is not necessary.
-Decryption by third-party tools is not possible.
-Does not have third-party dependencies.
-Works on all Windows lines starting from 7-ki.
- File encryption is performed in multi-threaded mode on all hard / removable / network / other drives. A separate stream is created for each medium.
-When connecting new hard drives / flash drives / network drives / other, the crypto-locker begins to work them out in separate streams.
-In case of new files, they will also be encrypted.
-Support network operation mode, in which parallel scanning of the local network is performed.
-Fileless version of PowerShell for targeted attacks on the network. The locker is inside the script without downloading from the network.
-New key for each generated build
-Increase of rights to the administrator, hiding and fixing in the system.
-Before you begin, the completion of these processes, the stop and removal of these services are performed.
-Before encryption, search and mount hidden drives.
-Before encryption, the recycle bin is cleared, shadow copies and OS recovery points are deleted.
- During file encryption, the crypto-locker can change the attributes of files to gain access to them.
-Support the detection of processes that block the file, and their completion for unhindered access to the file.
-Set pixel wallpaper with text urging you to read the instructions.



Avaddon Dark Web Recruitment Ad

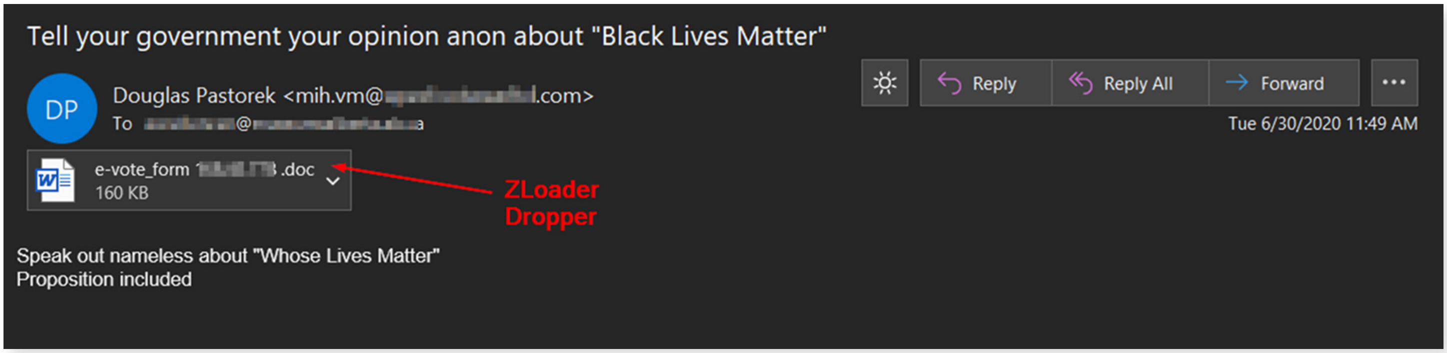
Banking Trojan - ZLoader

The ZLoader banking trojan, a variant derived from the original ZeuS trojan from 2006, has been extremely active this year. Ever since the source code for the Zeus trojan leaked in 2011, there have been quite a few variants based on this code. This newer ZLoader trojan is under active development by threat actors who typically use Excel or Word document extensions as their droppers.

Email lures cover a diverse range of topics, including:

- Coronavirus scams (and how to avoid them)
- Black Lives Matter
- Generic invoices
- CVs and resumes
- FMLA forms
- Local government and postal services spoofing

Recent examples of ZLoader infections have also loaded the Parasite HTTP remote access trojan to give actors a deeper foothold into the infected environment.



Tell your government your opinion anon about "Black Lives Matter"

Douglas Pastorek <mih.vm@[redacted].com>
To [redacted]@[redacted]

Tue 6/30/2020 11:49 AM

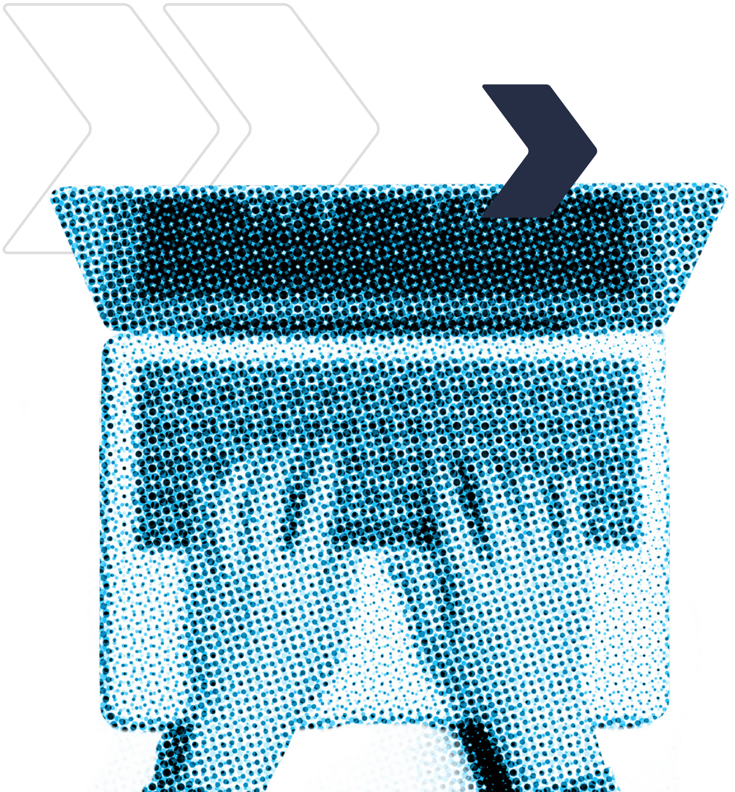
e-vote_form [redacted].doc
160 KB

Speak out nameless about "Whose Lives Matter"
Proposition included

ZLoader Email Example

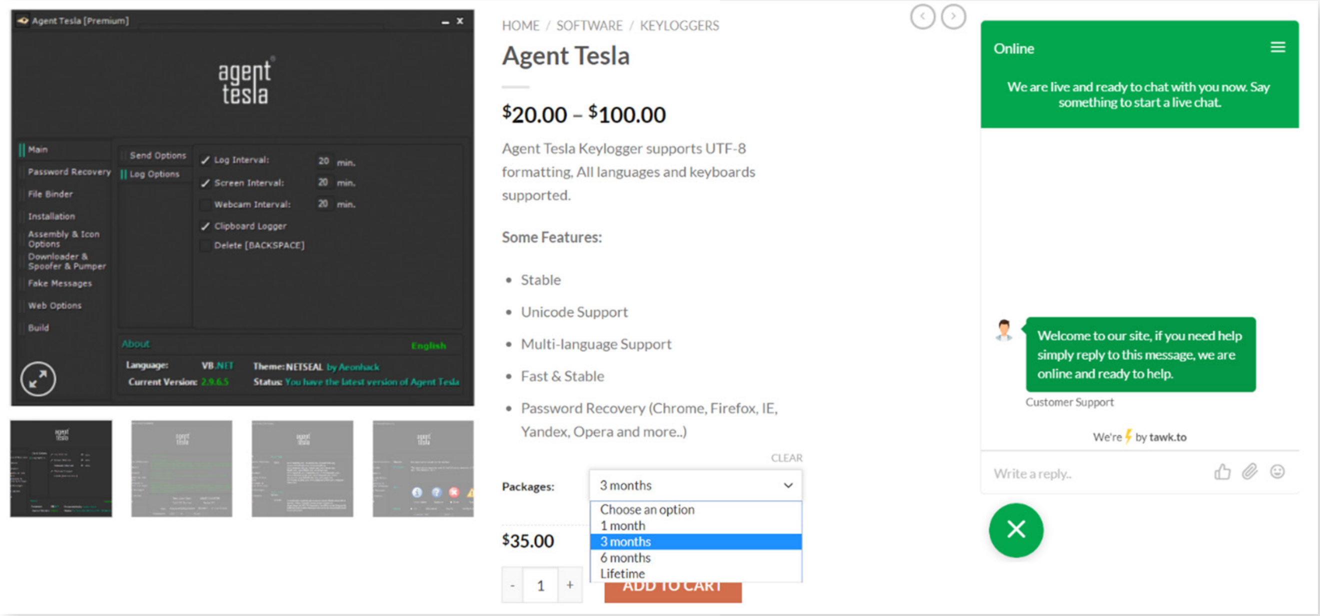
Remote Access Trojans

Remote access trojans (RATs) remain a popular attack vector to gain a foothold into a target system. They allow threat actors to conduct reconnaissance before deciding whether to deploy additional resources to victims such as follow-up payloads, privilege escalation steps, and lateral movement through a network. While 2019 was a banner year for RAT attacks, this tactic still remains a popular approach in 2020 that is only eclipsed by banking trojan campaigns distributed via the larger botnets. That said, most malicious actors who were not using botnets preferred to distribute RATs as the initial payload for their targeted attacks.



Remote Access Trojan - Agent Tesla

Agent Tesla is the most utilized RAT we have seen this year so far. Although it has been used by threat actors since 2014, it remains an extremely popular attack vector due to its powerful keylogger/RAT combination which is simple to deploy and maintain with little monetary expenditure. In addition to logging keystrokes, it has the ability to steal clipboard contents and screenshots. Further, Agent Tesla can conduct password theft for web browsers, mail clients, and popular FTP software. As illustrated in the Agent Tesla advertisement (pictured), it can be obtained for as little as $20 USD for a one-month license or $100 USD for a lifetime license.



✓ Log Interval: 20 min.
✓ Screen Interval: 20 min.
□ Webcam Interval: 20 min.
✓ Clipboard Logger
□ Delete [BACKSPACE]

Language: VB.NET
Theme: NETSEAL by Aeonhack
Current Version: 2.9.6.5
Status: You have the latest version of Agent Tesla

Agent Tesla

$20.00 – $100.00

Agent Tesla Keylogger supports UTF-8 formatting, All languages and keyboards supported.

Some Features:

- Stable
- Unicode Support
- Multi-language Support
- Fast & Stable
- Password Recovery (Chrome, Firefox, IE, Yandex, Opera and more..)

Packages: 3 months

Choose an option
1 month
3 months
6 months
Lifetime

$35.00

- 1 +

We are live and ready to chat with you now. Say something to start a live chat.

Welcome to our site, if you need help simply reply to this message, we are online and ready to help.

Agent Tesla Advertisement

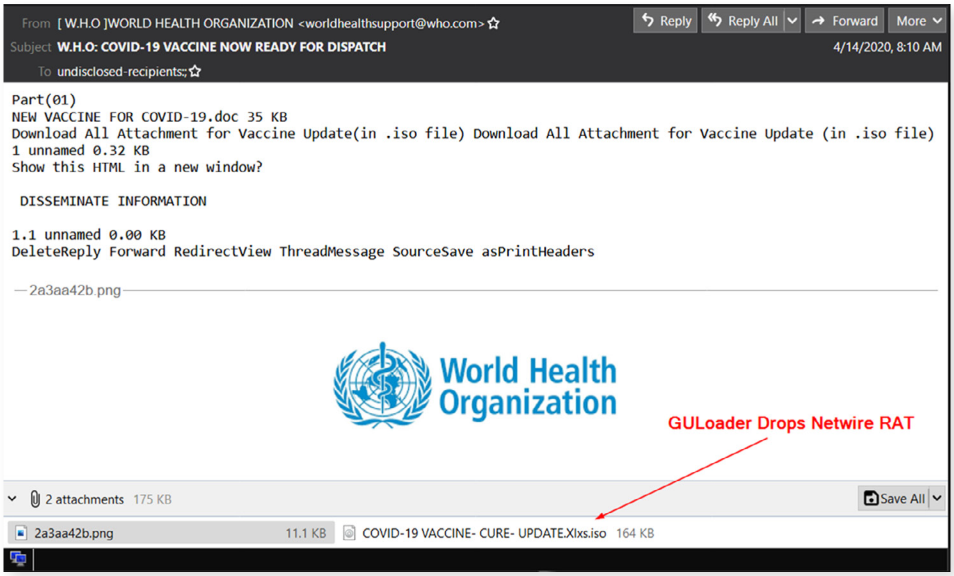
The malware developers behind Agent Tesla continue to actively update its capabilities and advertise it widely on both the dark and clear webs—so it is easy for virtually anyone to obtain. One of the most recent additions is a WiFi stealer module. This is the first step toward what may eventually become a RAT equal to the Emotet banking trojan. Emotet began with similar capabilities before eventually utilizing a WiFi worm module to spread throughout connected wireless networks.

Remote Access Trojan – NetWire

The NetWire RAT emerged from the wild in 2012 and has been used by threat actors ever since. Email campaigns attempting to deploy NetWire on victims' machines cover a full spectrum of lures. Here are just a few examples of lures we have captured attempting to distribute the NetWire RAT:

- IRS spoofing
- Fake invoices
- Sales quotations
- Purchase orders
- A supposed vaccine for coronavirus from the WHO

One of the biggest benefits for threat actors—besides availability and ease of use—is that it's a cross-platform trojan. This means it has the capability to function on infected machines in Windows, macOS, Linux, Android, and even Solaris environments without the need for any extra dependencies. It can steal passwords, keystrokes, and bank card data; take screenshots; and use the victim's webcam to spy on them. In addition, it allows for remote file execution to deploy additional malware payloads on a system. Banking trojans and ransomware are cybercriminals' most preferred follow-up payloads post-RAT deployment.



From [W.H.O]WORLD HEALTH ORGANIZATION <worldhealthsupport@who.com>
Subject W.H.O: COVID-19 VACCINE NOW READY FOR DISPATCH
To undisclosed-recipients;
4/14/2020, 8:10 AM

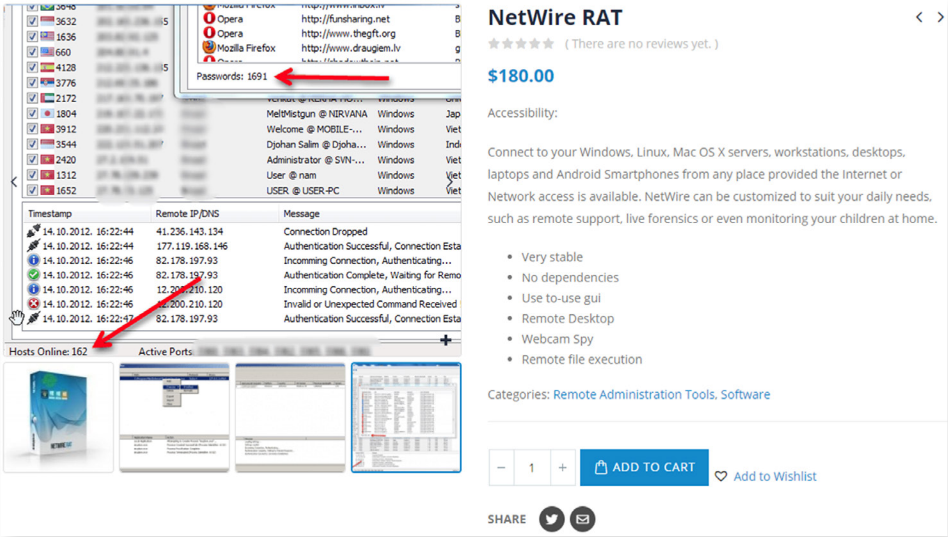
```
Part(01)
NEW VACCINE FOR COVID-19.doc 35 KB
Download All Attachment for Vaccine Update(in .iso file) Download All Attachment for Vaccine Update (in .iso file)
1 unnamed 0.32 KB
Show this HTML in a new window?

 DISSEMINATE INFORMATION

1.1 unnamed 0.00 KB
DeleteReply Forward RedirectView ThreadMessage SourceSave asPrintHeaders
```

2a3aa42b.png

GULoader Drops Netwire RAT

2 attachments 175 KB

2a3aa42b.png 11.1 KB
COVID-19 VACCINE- CURE- UPDATE.Xlxs.iso 164 KB



Opera	http://funsharing.net		
Opera	http://www.thegft.org		
Mozilla Firefox	http://www.draugiem.lv		

Passwords: 1691

☑ 3632	[redacted]			
☑ 1636	[redacted]			
☑ 660	[redacted]			
☑ 4128	[redacted]			
☑ 3776	[redacted]			
☑ 2172	[redacted]			
☑ 1804	[redacted]	MeltMistgun @ NIRVANA	Windows	Jap
☑ 3912	[redacted]	Welcome @ MOBILE-...	Windows	Viet
☑ 3544	[redacted]	Djohan Salim @ Djoha...	Windows	Ind
☑ 2420	[redacted]	Administrator @ SVN-...	Windows	Viet
☑ 1312	[redacted]	User @ nam	Windows	Viet
☑ 1652	[redacted]	USER @ USER-PC	Windows	Viet

Timestamp	Remote IP/DNS	Message
14.10.2012. 16:22:44	41.236.143.134	Connection Dropped
14.10.2012. 16:22:44	177.119.168.146	Authentication Successful, Connection Esta
14.10.2012. 16:22:46	82.178.197.93	Incomming Connection, Authenticating...
14.10.2012. 16:22:46	82.178.197.93	Authentication Complete, Waiting for Remo
14.10.2012. 16:22:46	12.200.210.120	Incomming Connection, Authenticating...
14.10.2012. 16:22:46	12.200.210.120	Invalid or Unexpected Command Received
14.10.2012. 16:22:47	82.178.197.93	Authentication Successful, Connection Esta

Hosts Online: 162 Active Ports [redacted]

NetWire RAT

☆☆☆☆☆ (There are no reviews yet.)

$180.00

Accessibility:

Connect to your Windows, Linux, Mac OS X servers, workstations, desktops, laptops and Android Smartphones from any place provided the Internet or Network access is available. NetWire can be customized to suit your daily needs, such as remote support, live forensics or even monitoring your children at home.

- Very stable
- No dependencies
- Use to-use gui
- Remote Desktop
- Webcam Spy
- Remote file execution

Categories: Remote Administration Tools, Software

Phishing and LotL

Threat actors have increasingly exploited legitimate services to launch living off the land attacks. These types of attacks can be used for malware and phishing campaigns. Attackers prefer to launch attacks abusing these platforms from accounts that were previously compromised. This way, the sender's IP and legitimate originating infrastructure raises less suspicion to email filters and recipients.

Attackers will often preserve the compromised users' signature and images, such as company logos. Certain threat actors have found that leveraging CRM software provides additional intelligence to increase attack success rates. These platforms provide analytics such as who opens an email and link-click rates.

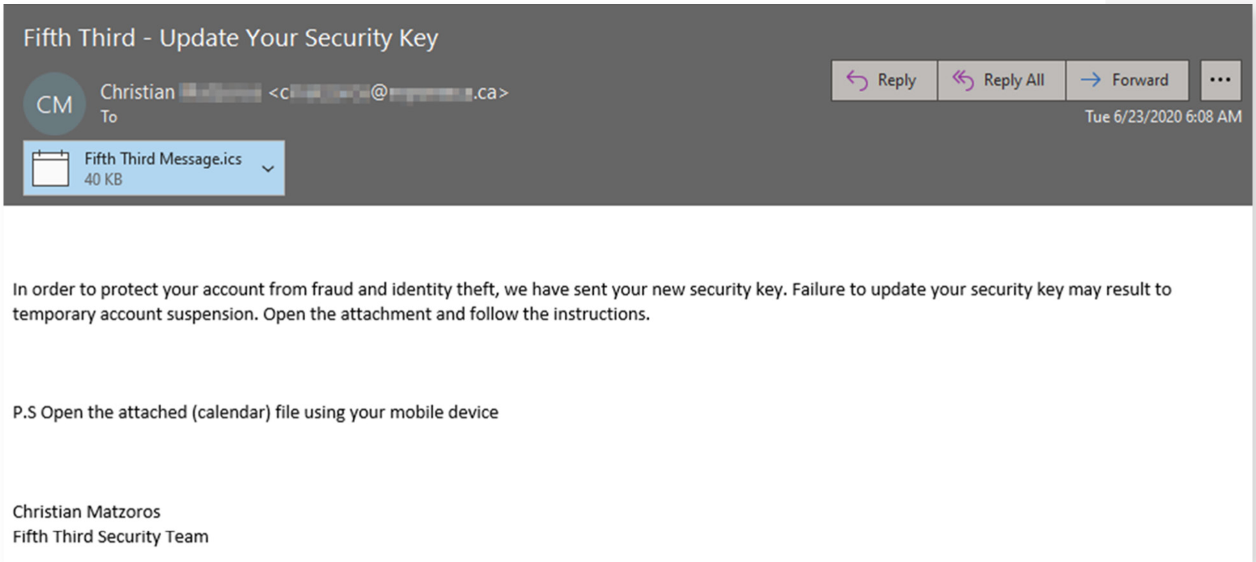
These links either lead directly to a credential harvesting page or host an image that redirects to another site (often an exploited site) that is hosting the credential harvesting page. If an unsuspecting recipient enters their email credentials on one of said pages, the stolen credentials are sent back to the attackers. Since their ultimate goal is financial fraud, this credential theft is necessary for attackers to identify and target employees and vendors who handle monetary transactions.

Most Abused Services in Order (Last Month)

1. Page.link
2. Storage.googleapis.com
3. Sendgrid.net
4. Amazonaws.com
5. Sharepoint.com
6. Forms.gle
7. Onedrive.live.com / 1drv.ms
8. Rebrand.ly
9. App.box.com
10. Sites.google.com
11. Surveygizmo.com
12. Firebaseapp.com
13. Gitbook.io
14. File.dn
15. Genial.ly

Additionally, we recently observed a resurgence of phishing utilizing .ics (Internet Calendaring and Scheduling Core Object Specification) files. These contain a phishing link that eventually leads to a branded credential harvesting page. Sharepoint.com has been the phishing lure of choice in these campaigns.

To date, threat actors using .ics have stuck to a banking alert theme including the banks Wells Fargo and Fifth Third Bank. Here's an example email from the more recent Fifth Third variant:



Fifth Third - Update Your Security Key

CM Christian [redacted] <c[redacted]@[redacted].ca>
To

Fifth Third Message.ics
40 KB

Tue 6/23/2020 6:08 AM

In order to protect your account from fraud and identity theft, we have sent your new security key. Failure to update your security key may result to temporary account suspension. Open the attachment and follow the instructions.

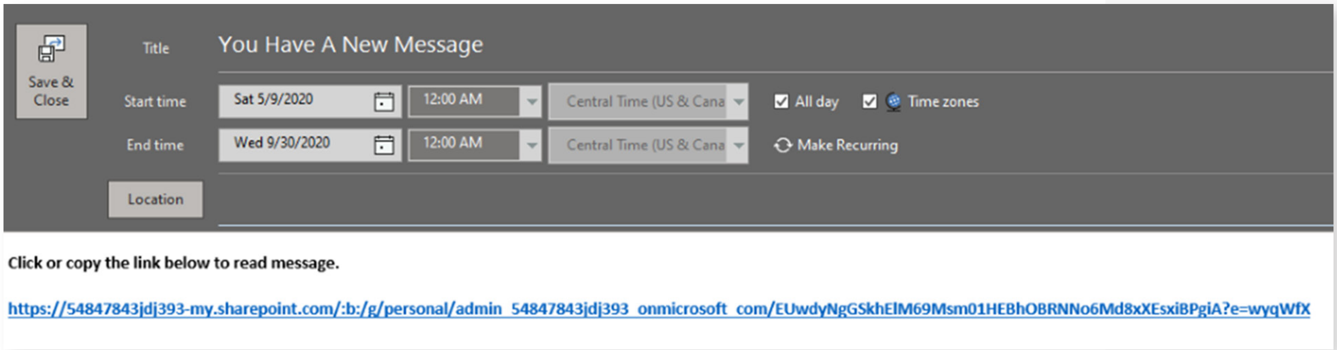
P.S Open the attached (calendar) file using your mobile device

Christian Matzoros
Fifth Third Security Team

This email exhibits a common phishing tactic—a sense of urgency—which is created by the threat to suspend your account. An additional red flag: The sender urges the recipient to open the .ics on their mobile device, likely an attempt to avoid business security solutions from picking up on it. To give the appearance of legitimacy, the threat actors address this email from "alert@wellsfargo.alert.com."

Notice the empty "To" field—another common phishing tactic where bad actors abuse the BCC (Blind Carbon Copy) email functionality. This means no one can see who the email is addressed to. We advise users to proceed with caution when interacting with any email that's been addressed to undisclosed (BCC'd) recipients.

Here is a look at the .ics file once it is opened in Outlook:



Title: You Have A New Message

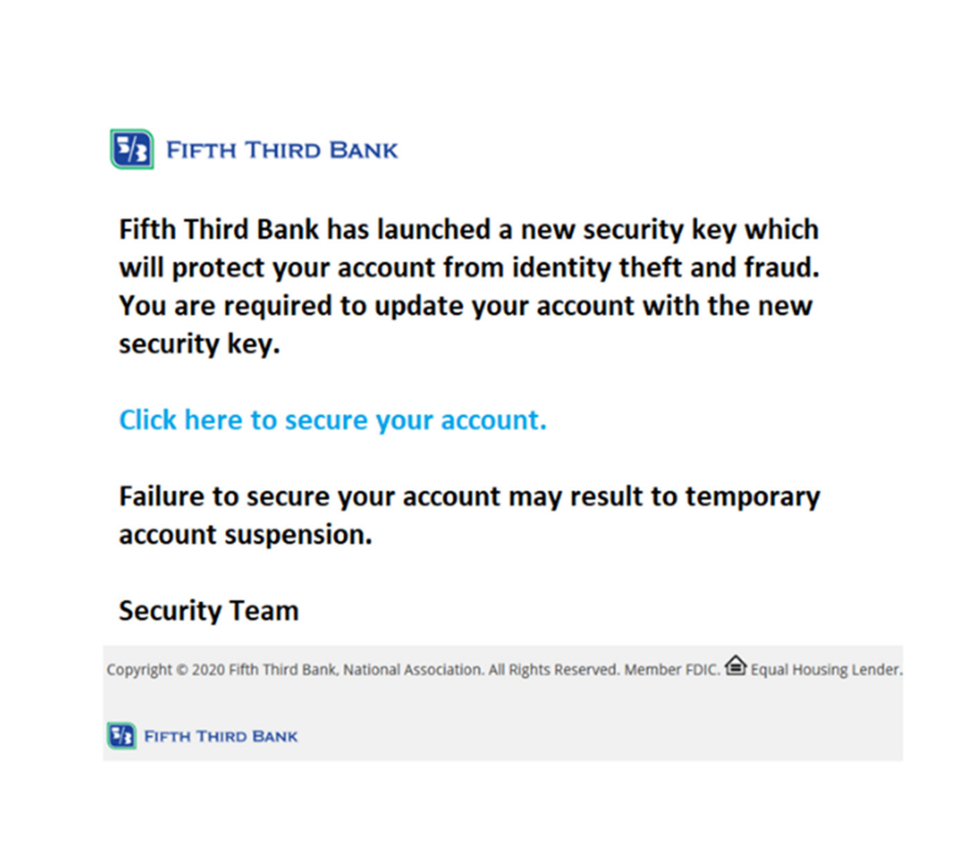
Start time: Sat 5/9/2020 | 12:00 AM | Central Time (US & Cana | ☑ All day ☑ Time zones

End time: Wed 9/30/2020 | 12:00 AM | Central Time (US & Cana | Make Recurring

Click or copy the link below to read message.

https://54847843jdj393-my.sharepoint.com/:b:/g/personal/admin_54847843jdj393_onmicrosoft_com/EUwdyNgGSkhElM69Msm01HEBhOBRNNo6Md8xXEsxiBPgiA?e=wyqWfX

Below is the image being hosted on OneDrive which redirects to storage.googleapis.com:



FIFTH THIRD BANK

Fifth Third Bank has launched a new security key which will protect your account from identity theft and fraud. You are required to update your account with the new security key.

Click here to secure your account.

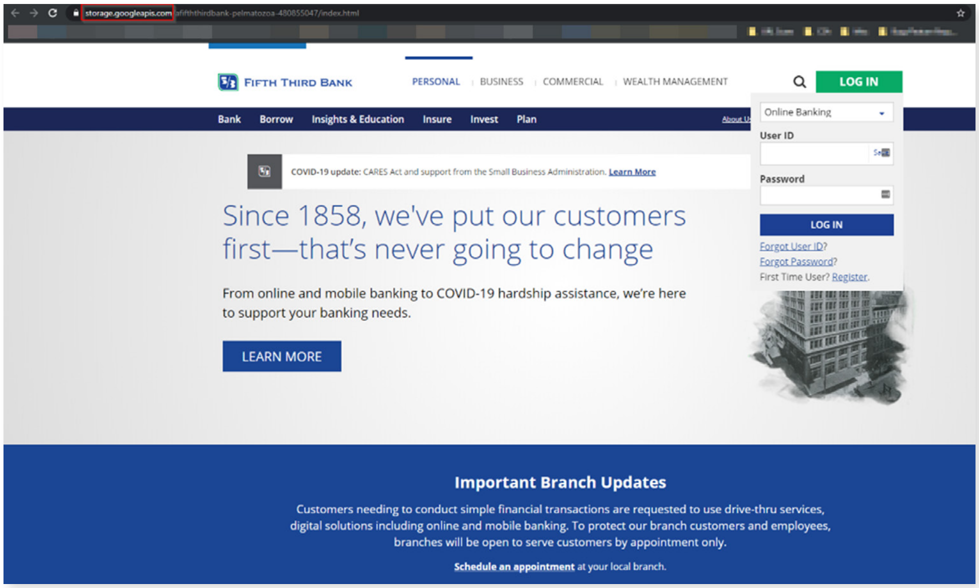
Failure to secure your account may result to temporary account suspension.

Security Team

Copyright © 2020 Fifth Third Bank, National Association. All Rights Reserved. Member FDIC. Equal Housing Lender.

FIFTH THIRD BANK

Finally, we are brought to a well-crafted Fifth Third Bank credential harvesting page being hosted on storage.googleapis.com:



storage.googleapis.com/fifththirdbank-pelmatozoa-480855047/index.html

[redacted]

Online Banking

User ID

Password

LOG IN

Forgot User ID?
Forgot Password?
First Time User? Register.

COVID-19 update: CARES Act and support from the Small Business Administration. Learn More

Since 1858, we've put our customers first—that's never going to change

From online and mobile banking to COVID-19 hardship assistance, we're here to support your banking needs.

Important Branch Updates

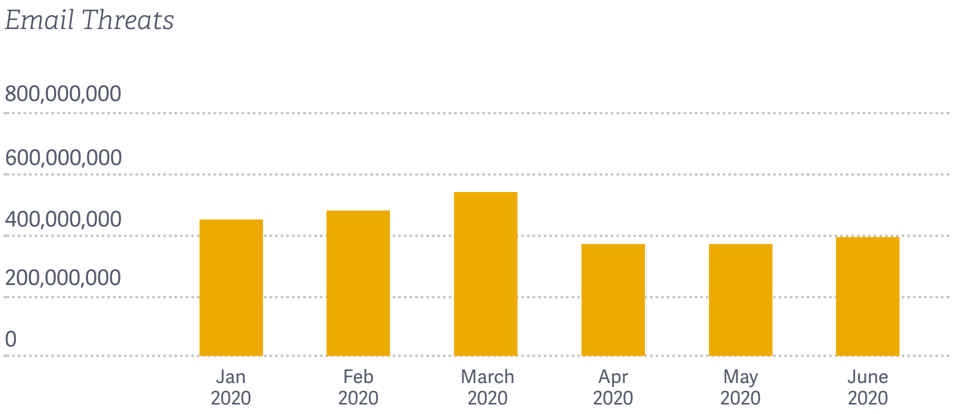
Customers needing to conduct simple financial transactions are requested to use drive-thru services, digital solutions including online and mobile banking. To protect our branch customers and employees, branches will be open to serve customers by appointment only.

Schedule an appointment at your local branch.

Metrics

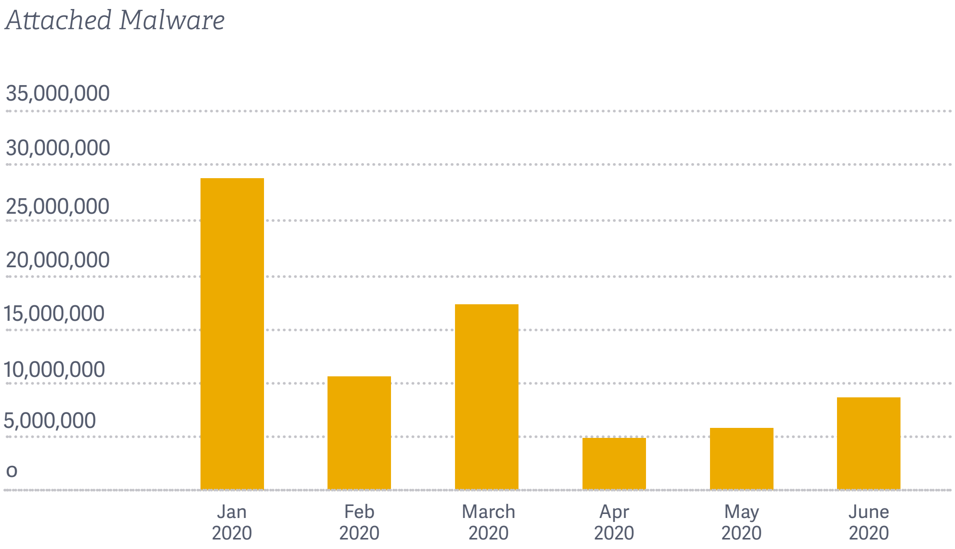
URL- and Text-Based Attack Traffic

The following chart depicts the volume of all other quarantined email traffic caught by our email filters. The majority of quarantined traffic were phishing attacks that contained URL-based malware. We also saw a good amount of text-based attacks, which rely on social engineering tactics. In all we quarantined 3.1 billion of these types of messages through the first half of 2020.



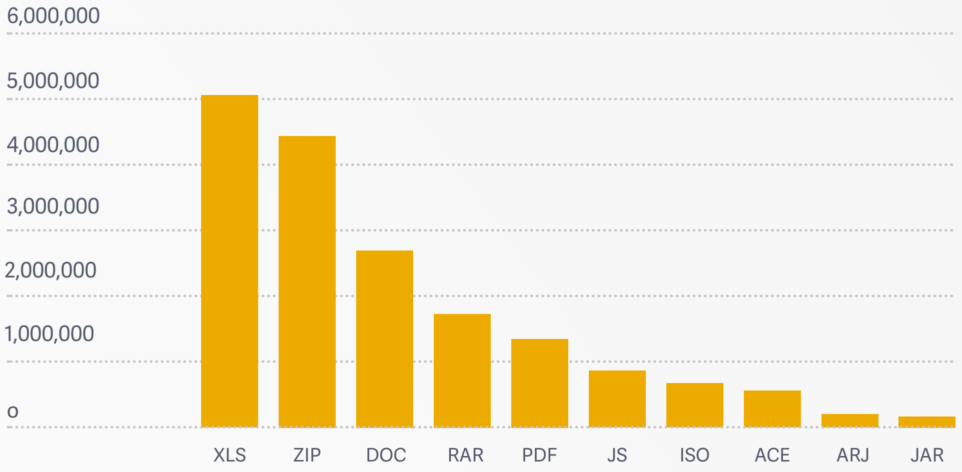
Malware Traffic

During the first half of the year, the volume of malware being delivered via attachment surged in January and March. Threat actors leaned more heavily toward malicious links in the remaining months. Throughout the year to date, Zix | AppRiver's Advanced Email Threat Protection email security quarantined about 87 million emails containing malware in a message attachment.



Below are the top 10 most prevalent attachment types of malware distribution. For several years, the most popular malware attachment type was doc (and docx). This year's malicious traffic was markedly different in that threat actors embraced XLS (spreadsheets) as the most popular malicious attachment type.

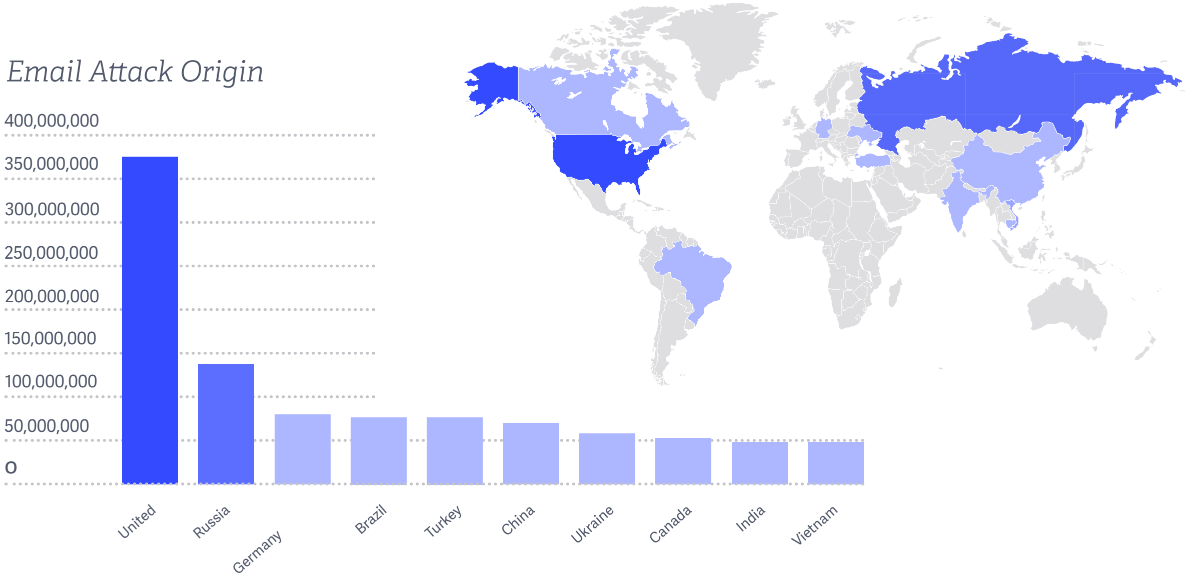
Malware Extension



Top Ten

Of the billions of bad email messages quarantined thus far in 2020, the majority originated in one of these 10 countries. As the chart below depicts, the most common origination point for email-based attacks in the first six months of 2020 was the United States. The most noteworthy change was a drop-off in attacks emanating from China, which fell by just over 50% from the previous six months. During this same period, attacks emanating from Russia ramped up—propelling it to the second most common point of origin.

Email Attack Origin



Timely & Timeless Security Tips

- ○ **Set reminders** to stay vigilant of social engineering attacks.
- ○ **Tune your email security solution** to catch impersonation attacks.
- ○ **Ensure** your security solution can dynamically analyze email attachments.
- ○ **Limit** the use of third-party services.
- ○ **Implement a VPN** for all remote workers (but avoid using a free VPN service as they often monetize your private data).
- ○ **Practice** the method of least privilege.
- ○ **Leverage cloud technology** to scale remote operations, but don't go it alone.
- ○ **Never reuse the same password** on different services. If one is compromised, attackers will try that password on others.
- ○ **Use a password manager,** this way you can create more complex and secure passwords. Ideally, a secure password should be a minimum of 12 characters mixed with uppercase, lowercase, numbers, and symbols or special characters.
- ○ **Always use multi-factor authentication** for any service that offers it. While not infallible, it can greatly reduce the risk of compromise.
- ○ **If there is any suspicion** about a message or transaction, it never hurts to call the sender. Most will be glad that you have security protocols to help you both prevent fraud.
- ○ **Avoid clicking links** whenever possible. Instead, navigate directly to a website and login without utilizing a link inside an email.
- ○ **Establish and update** Business continuity plans. Resilience during a security incident is vital to the business' continuity and minimizes downtime, disruption, or data loss.
- ○ **Use end-to-end email encryption** for any message containing confidential or personally identifiable information (PII).
- ○ **Update remote workers' home router firmware and software**. It's the main gatekeeper for home networks and often overlooked by security updates. If automatic updates are an option, enable them and set them for times (if possible) that wouldn't impact critical devices if the internet goes down during an update.

Learn more about Zix Email Security at Zix.com.

zix® | appriver®