ManageEngine
Log360

Tackling COVID-19 Themed Cyberattacks

Is your organization working from home?
It may be at risk of **COVID-19**-themed attacks.

Introduction

The COVID-19 pandemic has brought with it a unique set of challenges for cybersecurity professionals around the world. In an atmosphere of uncertainty, any apparent information on the ongoing crisis makes potent bait. This is something that malicious actors know and have been exploiting.

The rapid proliferation of COVID-19 has been closely paralleled by a rise in COVID-19-based cyberattacks. Security researches have discovered multiple instances of coronavirus-themed credential stuffing scams, phishing attacks, and malware payloads. According to a study by Check Point Threat Intelligence, "coronavirus-themed domains [are] 50 percent more likely to be malicious."

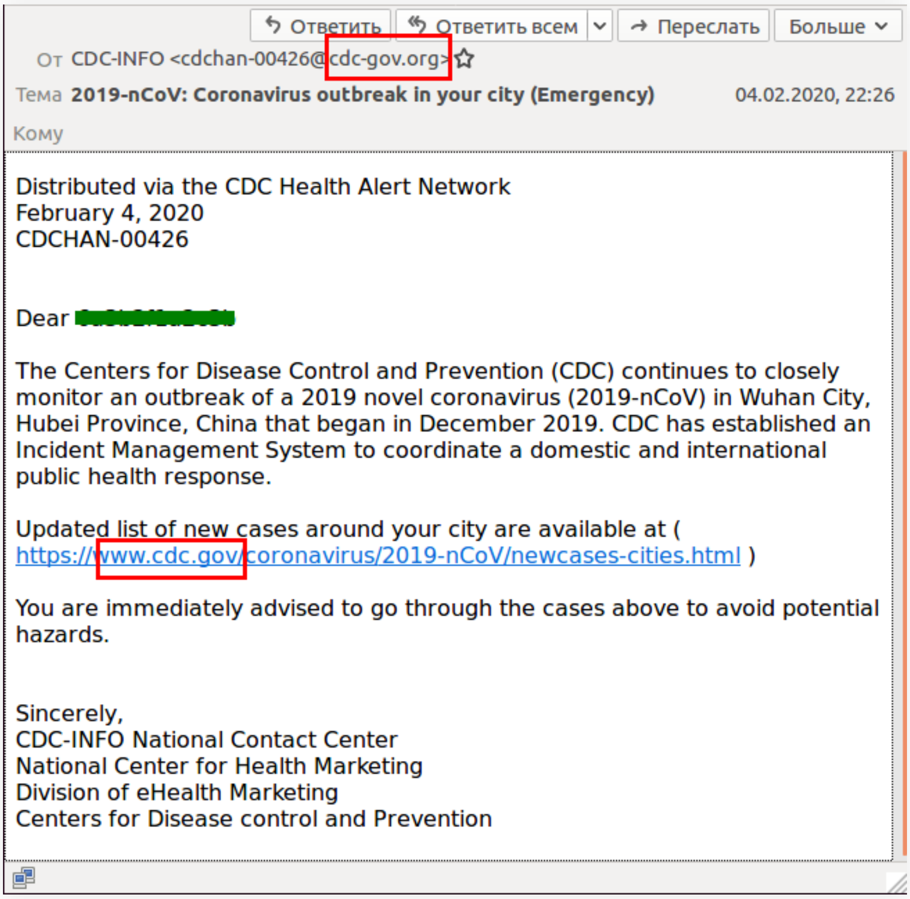
This e-book will give you an overview on the cyberattacks that are happening and experts' tips on how to ramp up your security defenses to combat such attacks. The best course of action for avoiding attacks like these is, of course, not taking the bait. But first, you need to learn how to identify a cybercriminal's bait, so you can effectively avoid it.

Information overload: COVID-19-themed phishing attacks

By now, most of us are no stranger to a barrage of information on COVID-19. Starting with dubious claims on social media like tea being the cure for COVID-19 (it isn't) to emails claiming to have the latest updates, we've seen it all. All of these fall somewhere in the spectrum of mildly annoying and relatively harmless to dangerous malware.

Here are some of the malicious emails that have begun to surface.

1. Emails imitating government organizations.



От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 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.

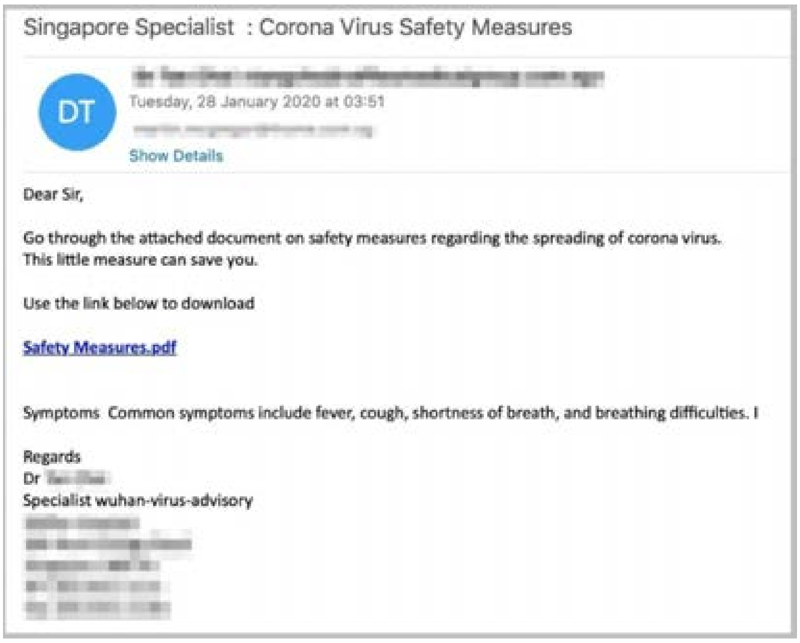
Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Source: Kaspersky

The Centers for Disease Control (CDC) is a United States government organization that is actively involved in fighting the pandemic. Different versions of this email have been surfacing with a similar message: "Get an updated list of cases near you by clicking the link here." If you pay close attention to the domain name, it is **cdc-gov.org.** Government domains end with **.gov**, not **.com** or **.org.**

2. Health tips

For security teams getting started on a data security plan, below are five key areas to focus on:



Singapore Specialist : Corona Virus Safety Measures

[redacted]

Tuesday, 28 January 2020 at 03:51

[redacted]

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.
This little measure can save you.

Use the link below to download

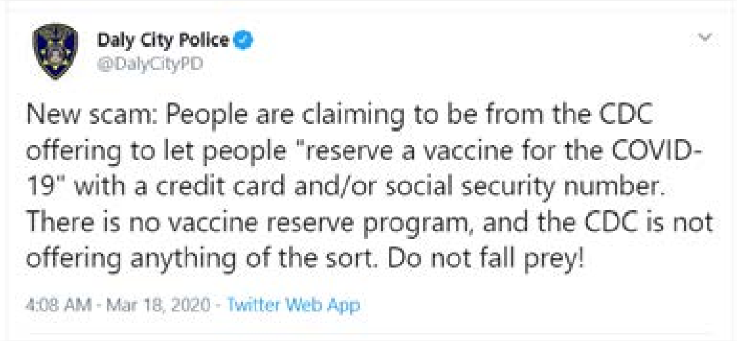
Safety Measures.pdf

Symptoms Common symptoms include fever, cough, shortness of breath, and breathing difficulties. I

Regards
Dr [redacted]
Specialist wuhan-virus-advisory
[redacted]

Source: Norton

Some of these supposed health tips can be packaged with malware like in the email above. In some cases, they even ask you for sensitive information like Social Security numbers or credit card details to "reserve a vaccine when it's available." This scam became so common that Daly City Police in California warned people about it.



Daly City Police
@DalyCityPD

New scam: People are claiming to be from the CDC offering to let people "reserve a vaccine for the COVID-19" with a credit card and/or social security number. There is no vaccine reserve program, and the CDC is not offering anything of the sort. Do not fall prey!

4:08 AM - Mar 18, 2020 - Twitter Web App

Some key takeaways

Avoid opening emails claiming to have COVID-19 updates or heath tips. Create awareness among your employees about the phishing scams, and ask them not to open any emails claiming to have information.

Phishing emails with domains imitating the CDC and World Health Organization (WHO) have been spotted frequently, so instruct your employees to exercise caution while opening non-business emails.

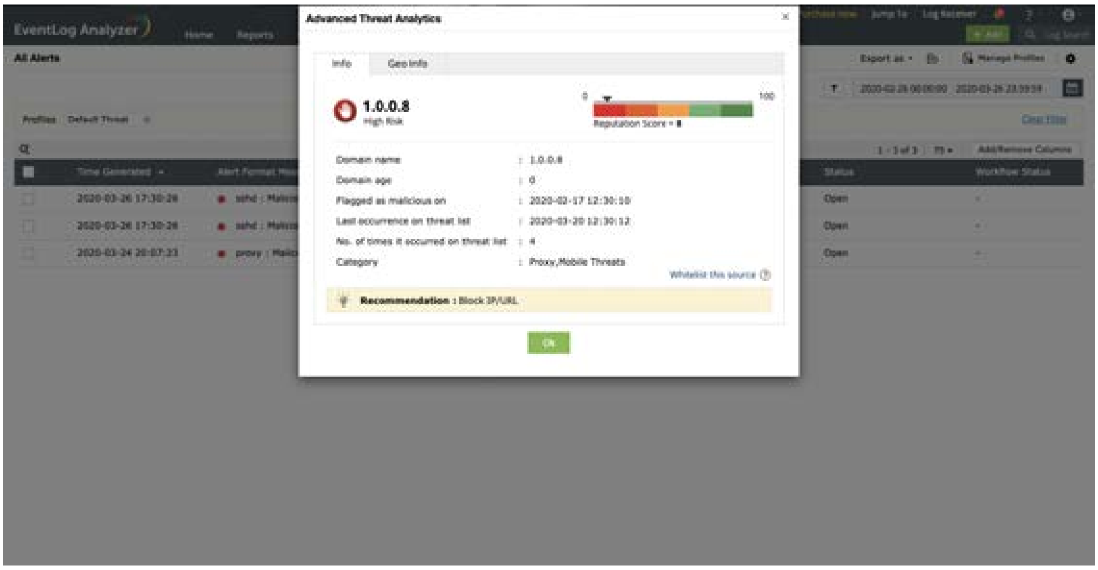
For instance, the URLs below have been flagged as malicious:

- http://bodica.com.ru/office/coronavirus/-act-today-or-people-will-die-f4d3d9cd99ca
- http://uk-covid-19-relieve.com
- https://chase-covid19s.com

These are just three examples of the hundreds of malicious COVID-19-themed domains out there. Some malicious domains even have **https://**, but that doesn't guarantee that they're safe.

Tip: Log360, a comprehensive security information and event management (SIEM) solution, has a built-in threat intelligence platform that gets dynamically updated with the latest information on malicious domains and URLs, including the recent COVID-19-themed ones. With this solution, you can easily get real-time alerts when a user is trying to contact or download something from these sites. Check out our Advanced Threat Analytics add-on here.

Log360's Advanced Threat Analytics add-on uses reputation-based scoring to assess the severity of threats. Each domain that interacts with your network will be assessed based on its reputation and history. If a domain has no recorded history of malicious activity or association with malicious domains, the reputation score will be high. Conversely, if the domain has been flagged for malicious behavior or is associated with suspicious domains, the reputation score for that domain will be low. This information can be crucial in making informed decisions like setting the firewall policies for a network.



Advanced Threat Analytics

1.0.0.8
High Risk

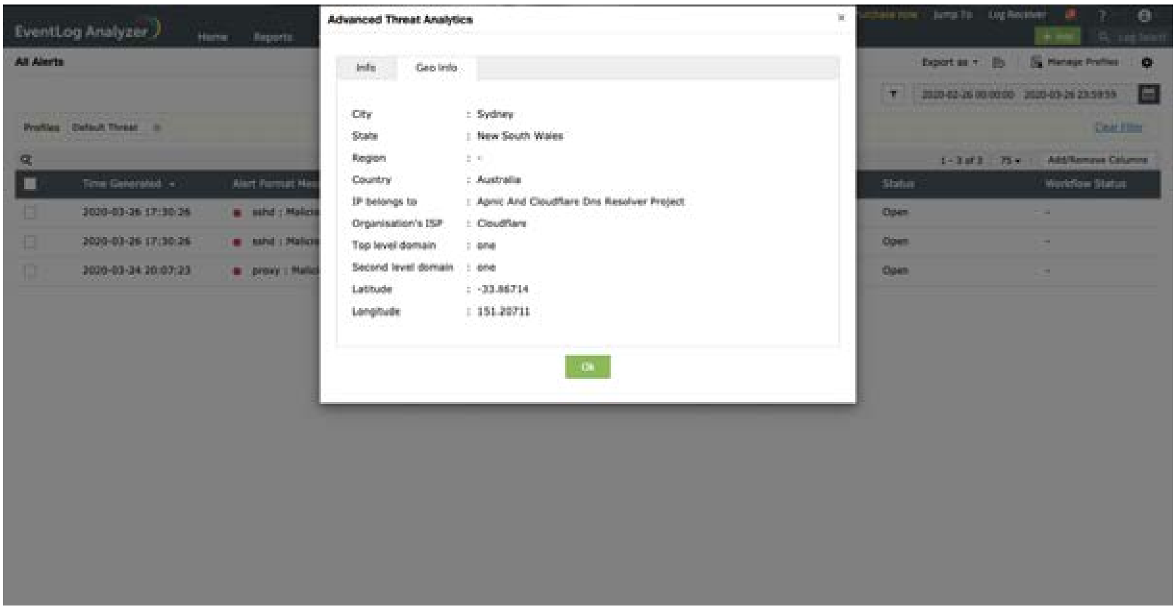
Reputation Score = 8

Domain name	: 1.0.0.8
Domain age	: 0
Flagged as malicious on	: 2020-02-17 12:30:10
Last occurrence on threat list	: 2020-03-20 12:30:12
No. of times it occurred on threat list	: 4
Category	: Proxy,Mobile Threats

Recommendation : Block IP/URL

Time Generated	Alert Format Mes	Status	Workflow Status
2020-03-26 17:30:28	sshd : Malici	Open	-
2020-03-26 17:30:28	sshd : Malici	Open	-
2020-03-24 20:07:23	proxy : Malici	Open	-

Additionlly, you can get information on the location of the domain, the ISP of the organization that owns the domain, and more. In a situation where you are under attack, every bit of information about the attacker will help.



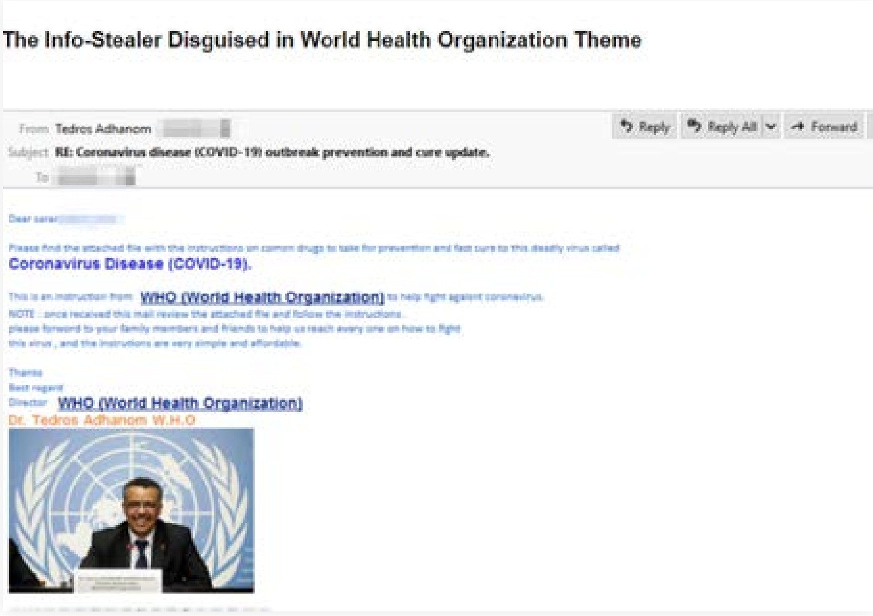
Advanced Threat Analytics

City	: Sydney
State	: New South Wales
Region	: -
Country	: Australia
IP belongs to	: Apnic And Cloudflare Dns Resolver Project
Organisation's ISP	: Cloudflare
Top level domain	: one
Second level domain	: one
Latitude	: -33.86714
Longitude	: 151.20711

2020-03-26 17:30:26	sshd : Malicio	Open	-
2020-03-26 17:30:26	sshd : Malicio	Open	-
2020-03-24 20:07:23	proxy : Malici	Open	-

Users often fall for new phishing scams. So, what's the plan for when they do?

In spite of your best efforts, an employee may unwittingly click on a link that can steal their credentials. What happens next? Is there still a way to protect your network after an employee's credentials have been compromised? Yes, there is. Let's dive into the details of how using an example.



The Info-Stealer Disguised in World Health Organization Theme

From Tedros Adhanom [redacted]
Subject RE: Coronavirus disease (COVID-19) outbreak prevention and cure update.
To [redacted]

Dear sara[redacted]

Please find the attached file with the instructions on comon drugs to take for prevention and fast cure to this deadly virus called
Coronavirus Disease (COVID-19).

This is an instruction from WHO (World Health Organization) to help fight against coronavirus.
NOTE : once received this mail review the attached file and follow the instructions.
please forward to your family members and friends to help us reach every one on how to fight
this virus , and the instructions are very simple and affordable.

Thanks
Best regard
Director WHO (World Health Organization)
Dr. Tedros Adhanom W.H.O

Source: IBM X-Force Exchange

An investigation by IBM X-Force Exchange has found that malicious actors are using WHO-themed phishing emails to spread malware called Agent Tesla. This malware can log keystrokes, steal credentials from browsers, and send this information back to attackers.

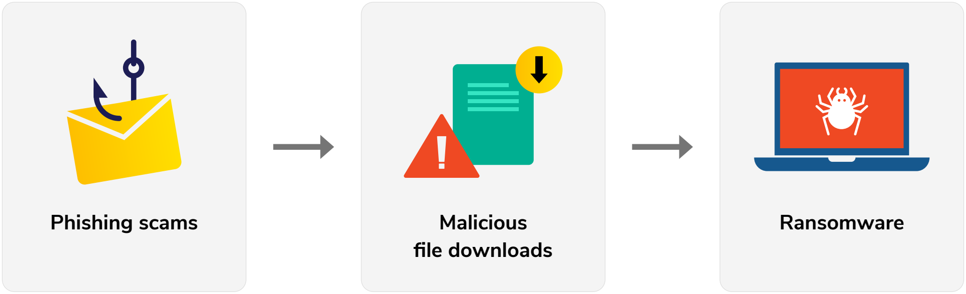
Agent Tesla will be downloaded into the host system when the email attachment **Coronavirus Disease (COVID-19) CURE.exe** is opened.

Assume an employee in your organization has clicked on the email. Your network can still be protected if you're able to spot malware the moment it gets downloaded and installed.

Setting up your defenses for a scenario like this

- Monitor software installations in endpoint devices.
- Not all file installations are malicious, so how would you differentiate a legitimate software installation from a suspicious one? Any software installation followed by a change in registry values is most likely an attack, so it's important to watch this metric closely after new software installations. Most SIEM solutions capture this using correlation rules.
- Configure automated workflows to kill malicious processes identified by the correlation rules. This can instantly stop the attack before it causes any damage to your network.

The pattern of COVID-19 themed attacks



Phishing scams → Malicious file downloads → Ransomware

How to discover and stop these attacks

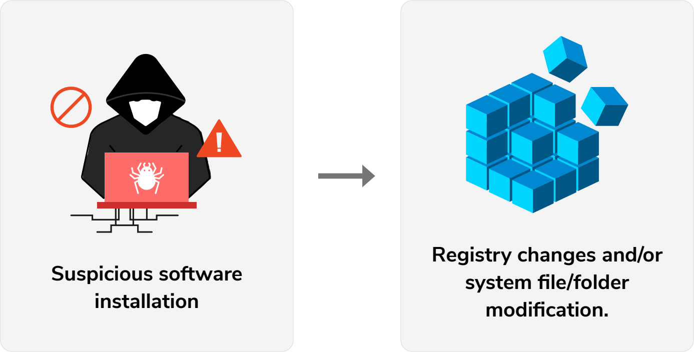
Here are some ways to tackle some common COVID-19-based attacks using threat intelligence, correlation rules, and automated workflows.

To tackle phishing scams:

Threat intelligence feeds capture traffic from suspicious sites. Stop communication with these malicious entities by blocking the domain, URL, or IP address.

Responding to downloaded malicious software:

Correlation rule:



Suspicious software installation

Registry changes and/or system file/folder modification.

Associated workflow:

Kill the malicious process.

Wrapping up

The novel scams discussed in this e-book are just a few instances of the multitudes of potential attacks that have emerged in recent days. Watching out for attacks like these and making the necessary changes to your security architecture will be crucial in the days to come. If you think a security information and event management (SIEM) solution will help, you can try out Log360. You can download it and start using it right away. In case you need help in configuring it, reach out to us anytime.

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote

⤓ Download