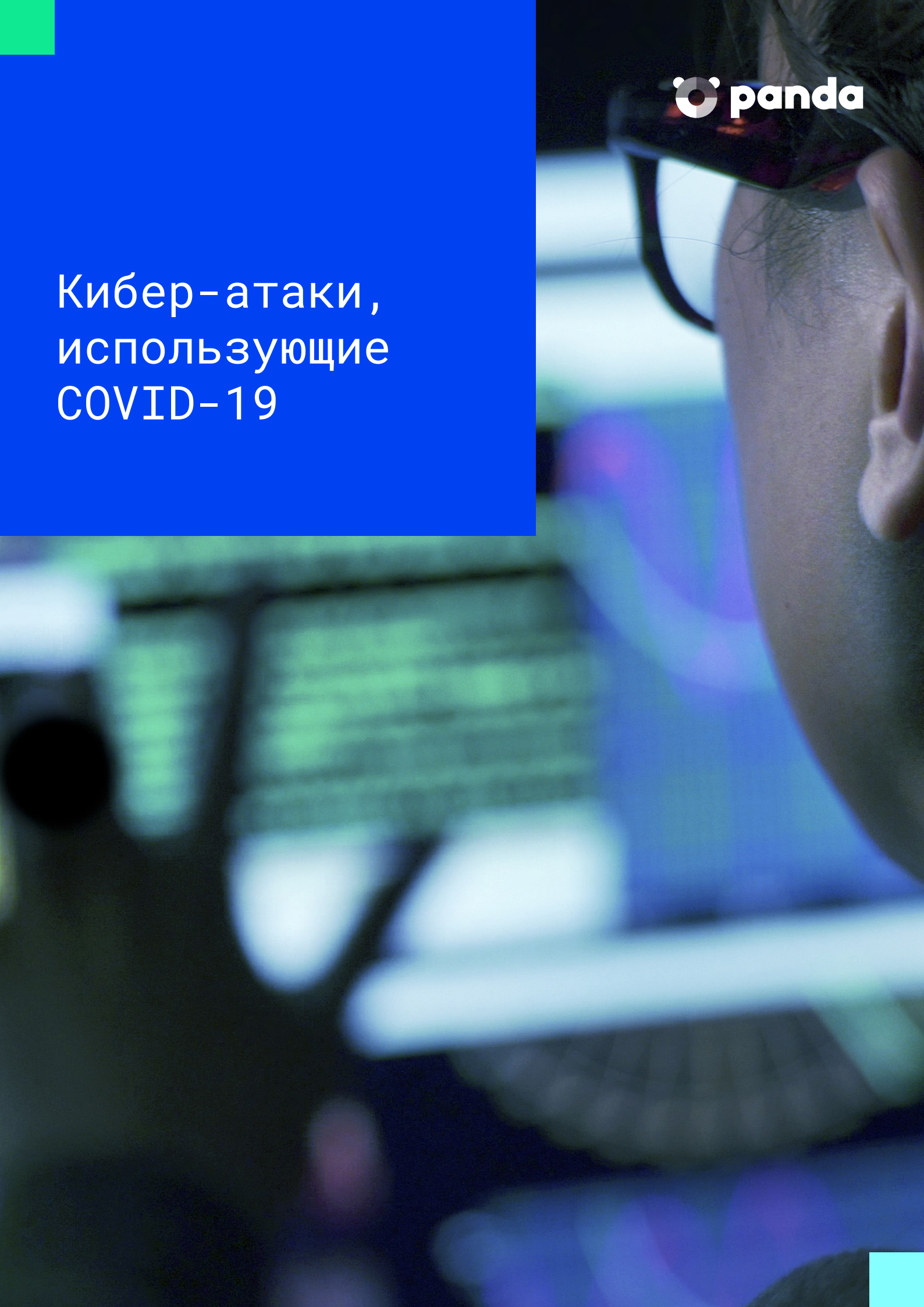
Кибер-атаки, использующие COVID-19



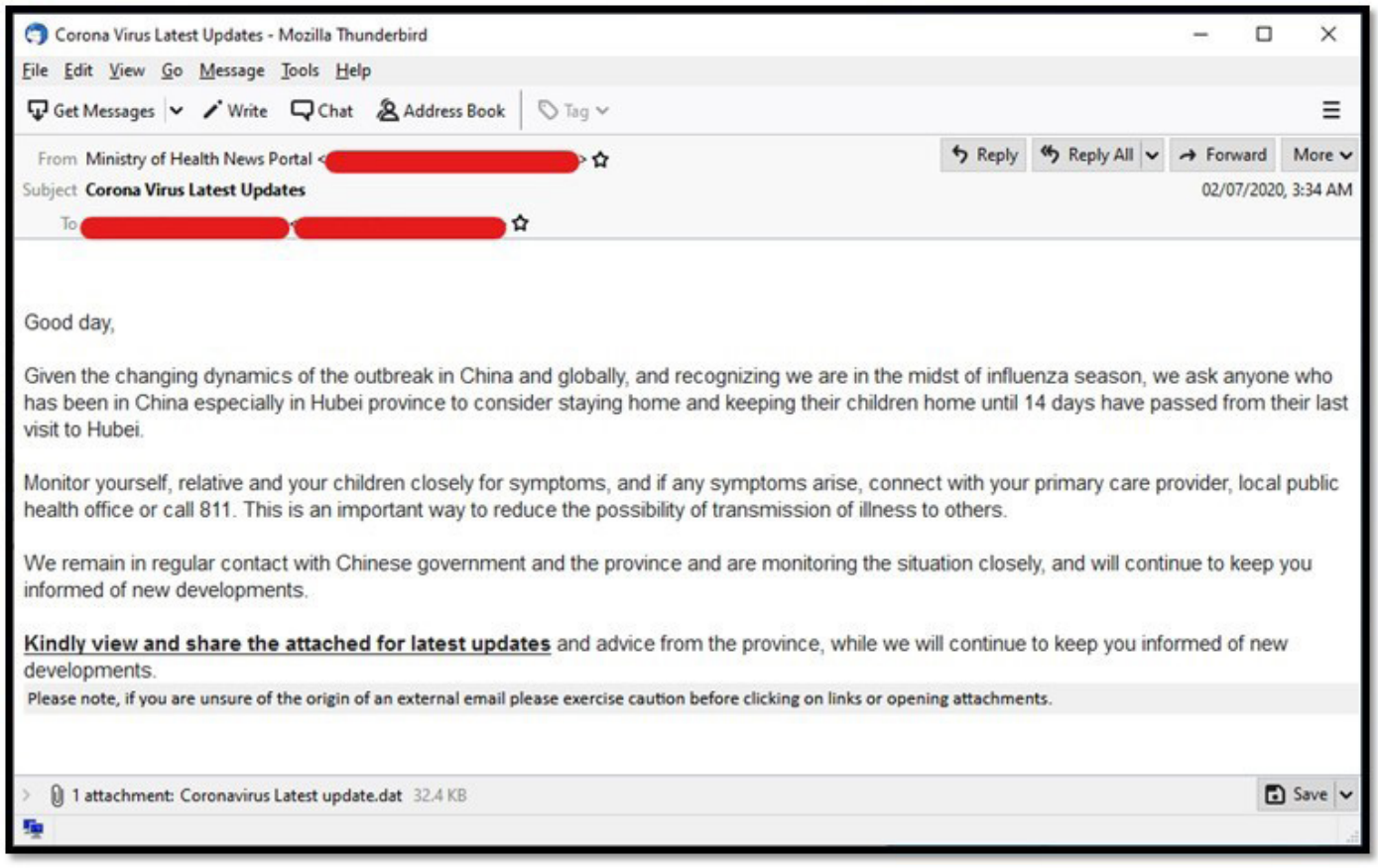
Глобальные кампании с кибер-атаками, использующими COVID-19

Пандемия с коронавирусом COVID-19 используется в качестве приманки во вредоносных кампаниях с применением техник социальной инженерии, включая спам, вредоносные программы, шифровальщики и вредоносные домены. По мере того как количество случаев заражения увеличивается уже тысячами, также набирают обороты и соответствующие вредоносные кампании. Эксперты Panda постоянно находят новые образцы подобных вредоносных кампаний, связанных с коронавирусом.

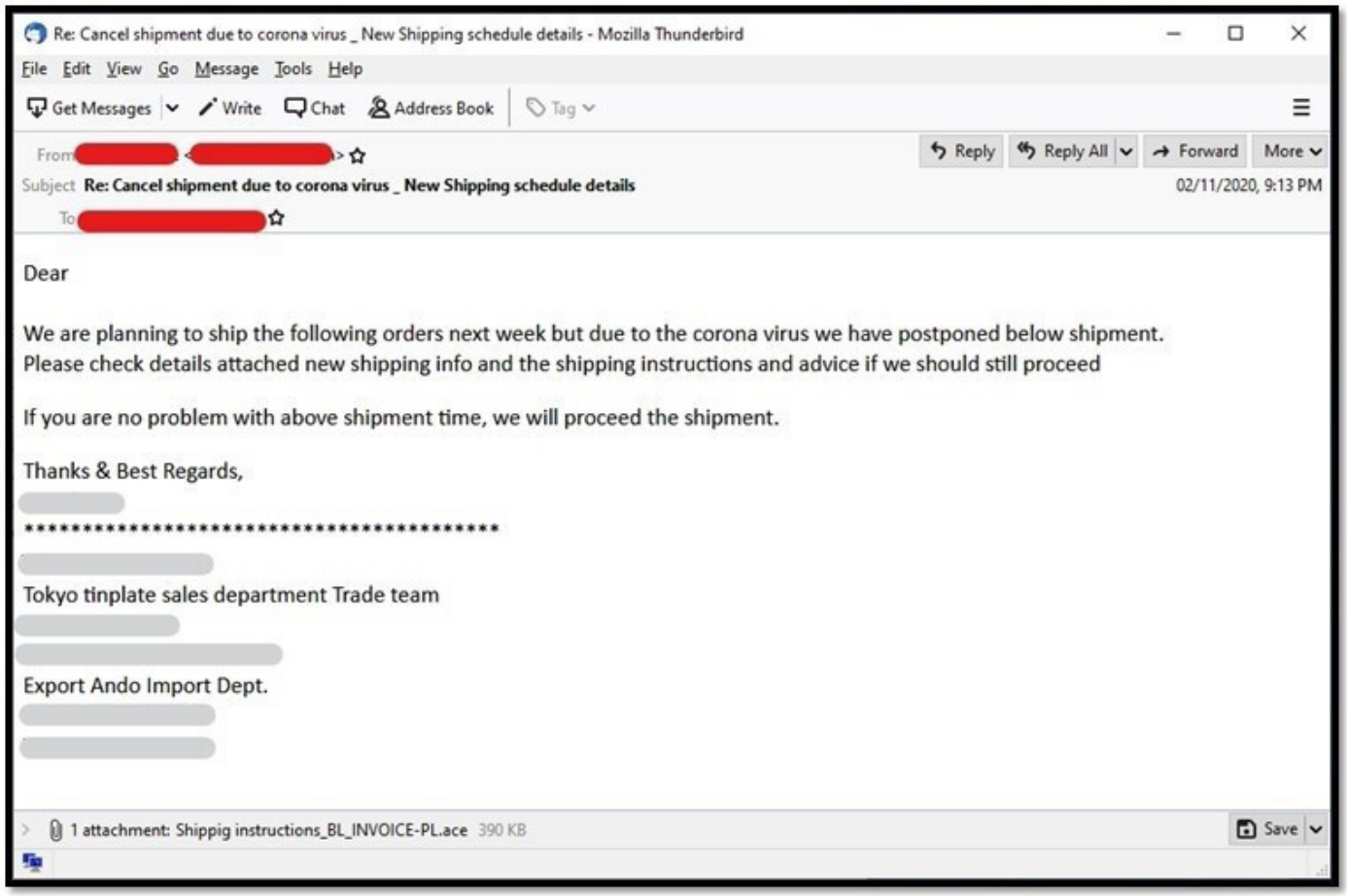
Спам, связанный с коронавирусом

Эксперты Panda обнаружили отправление и получение спамовых писем, связанных с коронавирусом, практически во всем мире, включая и такие страны как США, Японию, Россию и Китай. Во многих из этих писем, которые выглядят так, словно они отправлены из официальных организаций, утверждается, что они содержат обновленную информацию и рекомендации относительно пандемии. Как и большинство спам-кампаний, они также содержат и вредоносные вложения.

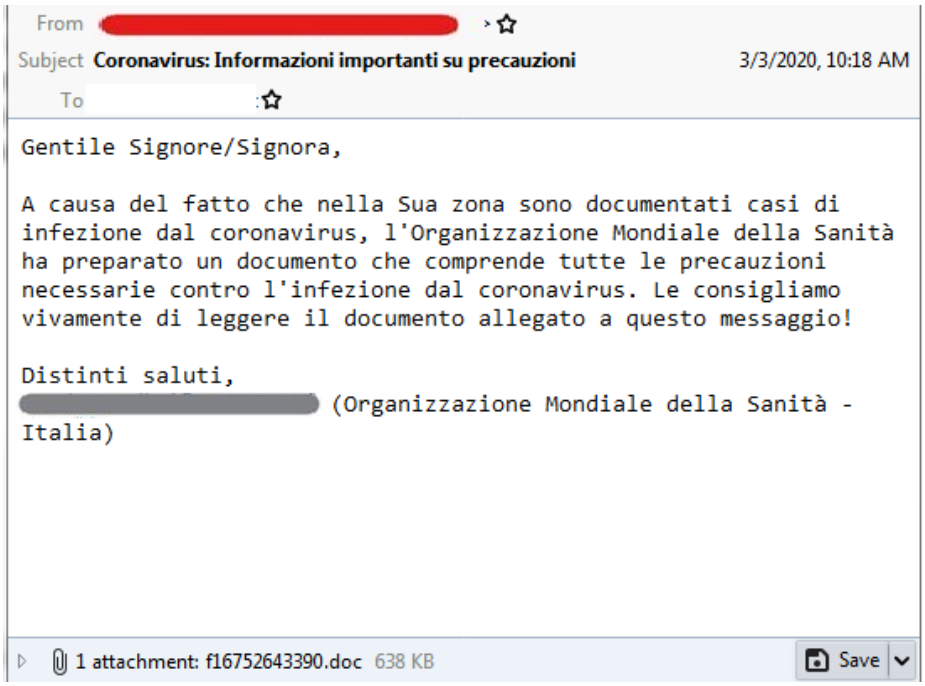
Один из примеров - спам с темой письма **"Corona Virus Latest Updates",** якобы отправленный Министерством здравоохранения. Содержит рекомендации о том, как предотвратить заражение, а в письме имеется вложение, которое якобы содержит обновленную информацию о коронавирусе COVID-19. Впрочем, на самом деле оно содержит вредоносную программу.



Другие спамовые письма про коронавирус связаны с поставками продуктов питания, которые были нарушены в результате распространения инфекции.

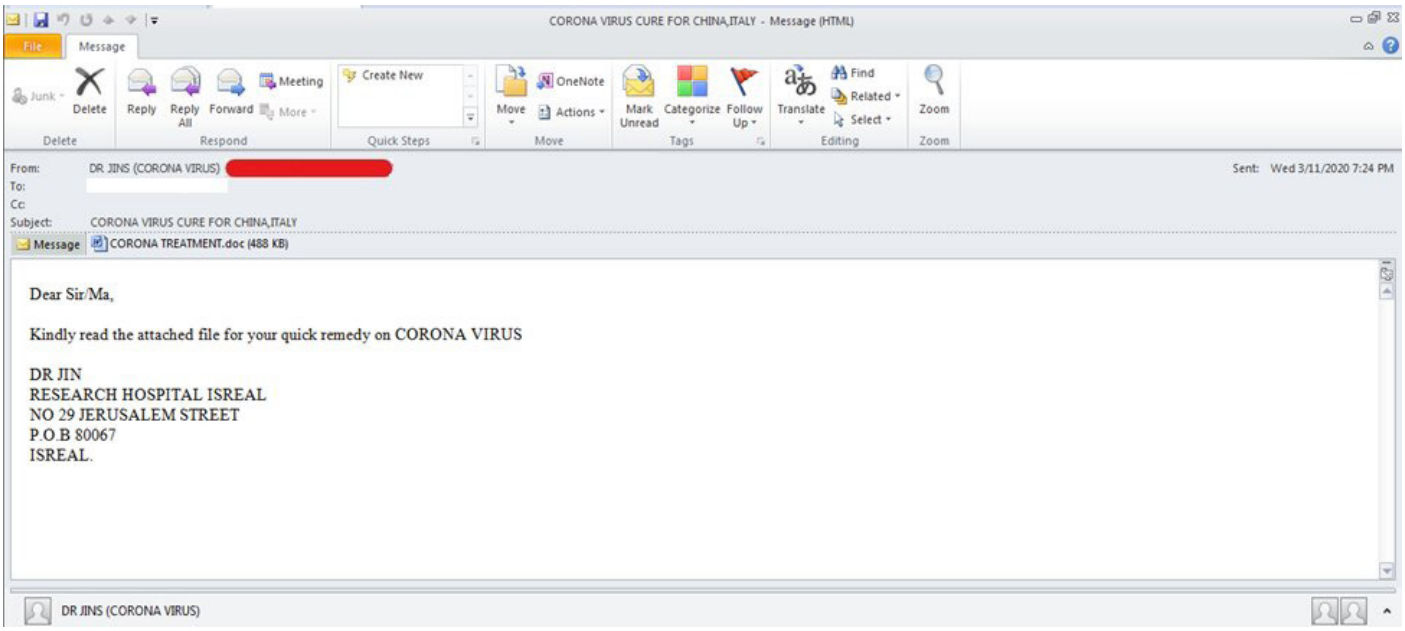


Следующий пример спама на итальянском языке содержит важную информацию о коронавирусе:



Следующее письмо на португальском языке обещает новую информацию о предполагаемой вакцине против COVID-19.

Были случаи, когда в теме спамовых писем упоминались лекарства против коронавируса, чтобы попытаться заставить людей загрузить вредоносное вложение. Иногда таким вредоносным вложением является **HawkEye Reborn** - это вариант трояна HawkEye, который осуществляет кражу информации.



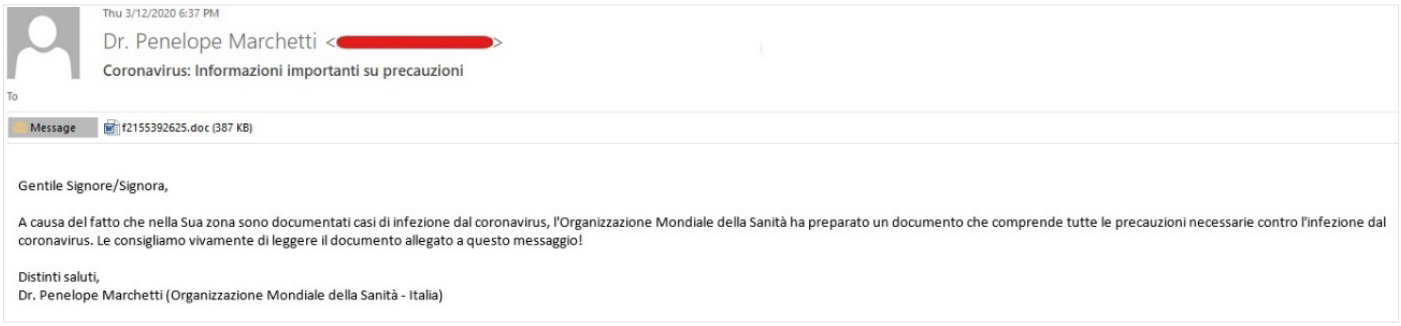
Индикаторы компрометации для вредоносных вложений

SHA-256
b9e5849d3ad904d0a8532a886bd3630c4eec3a6faf0cc68658f5ee4a5e803be

В этом случае индикаторы компрометации такие:

SHA-256
6cc5e1e72411c4f4b2033ddafe61fdb567cb0e17ba7a3247acd60cbd4bc57bfb
7c12951672fb903f520136d191f3537bc74f832c5fc573909df4c7fa85c15105

Еще одна спамовая кампания была направлена против пользователей в Италии - стране, которая сильно пострадала в результате пандемии. В теме и теле писем содержится текст “Coronavirus: important information on precautions” (Коронавирус: важная информация о мерах предосторожности). В теле письма утверждается, что вложение в письме - это документ от Всемирной организации здравоохранения (ВОЗ), а потому настоятельно рекомендуется скачать этот вложенный документ Microsoft Word, который содержит в себе трояна.


Thu 3/12/2020 6:37 PM

Dr. Penelope Marchetti <[redacted]>

Coronavirus: Informazioni importanti su precauzioni

To

Message f2155392625.doc (387 KB)

Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus, l'Organizzazione Mondiale della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie contro l'infezione dal coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggio!

Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

Когда пользователь открывает этот документ, то показывается следующее сообщение, заставляющее пользователя включить макросы:

Индикаторы компрометации (IOC)

SHA-256
dd6cf8e8a31f67101f974151333be2f0d674e170edd624ef9b850e3ee8698fa2

Вредоносные программы и шифровальщики, связанные с коронавирусом

Благодаря нашему сервису 100% классификации, антивирусная лаборатория PandaLabs сумела идентифицировать и заблокировать следующие вредоносные исполняемые файлы, связанные с этими кампаниями:

Название файла	SHA 256
CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm	ab533d6ca0c2be8860a0f7fbfc7820ffd 595edc63e540ff4c5991808da6a257d
	17161e0ab3907f637c2202a384de67fca 49171c79b1b24db7c78a4680637e3d5
	315e297ac510f3f2a60176f9c12fcf9 2681bbad758135767ba805cdea830b9ee
CoronaVirusSafetyMeasures_pdf.exe	c9c0180eba2a712f1aba1303b90cbf12c11 17451ce13b68715931abc437b10cd
	29367502e16bf1e2b788705014d0142 d8bcb7fcc6a47d56fb82d7e333454e923
LIST OF CORONA VIRUS VICTIM.exe	3f40d4a0d0fe1eea58fa1c71308431b5c2c e6e381cacc7291e501f4eed57bfd2
POEA HEALTH ADVISORY re-2020 Novel Corona Virus.pdf.exe	3e6166a6961bc7c23d316ea9bca87d82 87a4044865c3e73064054e805ef5ca1a
POEA Advisories re-2020 Novel Corona Virus.2.pdf.exe	b78a3d21325d3db7470fbf1a6d254e23d34 9531fca4d7f458b33ca93c91e61cd

Другие исследователи видели, как кибер-преступники использовали онлайн-карты мониторинга заболевания коронавирусом, подменяя их фейковыми веб-сайтами, с которых загружались и устанавливались вредоносные программы. Ниже приведены хэши таких вредоносных приложений:

SHA 256
2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307
0b3e7faa3ad28853bb2b2ef188b310a67663a96544076cd71c32ac088f9af74d
13c0165703482dd521e1c1185838a6a12ed5e980e7951a130444cf2feed1102e
fda64c0ac9be3d10c28035d12ac0f63d85bb0733e78fe634a51474c83d0a0df8
126569286f8a4caeeaba372c0bdba93a9b0639beaad9c250b8223f8ecc1e8040

Новый вариант шифровальщика CoronaVirus использовал для своего распространения фейковый сайт по оптимизации системы. Жертвы неосознанно скачивали с этого сайта файл **WSGSetup.exe**. Затем этот файл работал как загрузчик двух видов вредоносных программ: шифровальщик CoronaVirus и троян для кражи паролей **Trojan Kpot**.

Данная кампания является частью последней тенденции, наблюдаемой среди шифровальщиков: она сочетает шифрование данных с кражей информации.

Более того, был замечен еще один шифровальщик под названием **CovidLock,** ныне поражающий пользователей мобильных устройств. Этот шифровальщик появился из вредоносного приложения для Android, которое якобы помогает отслеживать случаи заражения COVID-19. Шифровальщик блокирует сотовый телефон своей жертвы, предоставляя ему всего 48 часов для оплаты выкупа в размере **100 долларов США в биткоинах** для восстановления доступа к своему устройству. Иначе жертве угрожают удалить все данные с телефона и украсть данные их аккаунтов в соцсетях.

Домены, связанные с коронавирусом

Кроме того, **заметно увеличилось** число доменных имен, использующих в своем названии слово "корона" (corona). Ниже мы приводим список таких вредоносных доменов:

- acccorona [.] com
- alphacoronavirusvaccine [.] com
- anticoronaproducts [.] com
- beatingcorona [.] com
- beatingcoronavirus [.] com
- bestcorona [.] com
- betacoronavirusvaccine [.] com
- buycoronavirusfacemasks [.] com
- byebyecoronavirus [.] com
- cdc-coronavirus [.] com
- combatcorona [.] com
- contra-coronavirus [.] com
- corona-blindado [.] com
- corona-crisis [.] com
- corona-emergencia [.] com
- corona explicada [.] com
- corona-iran [.] com
- corona-ratgeber [.] com
- coronadatabase [.] com
- coronadeathpool [.] com
- coronadetect [.] com
- coronadetection [.] com

Как работают эти атаки

Дело в том, что все эти атаки используют векторы проникновения, которые можно рассматривать как "традиционные". Мы в Panda видим, что все эти векторы могут быть закрыты традиционными антивирусными решениями для защиты конечных устройств. Мы в этом случае использует следующие механизмы для обнаружения и блокировки угроз:

- **Сервис 100% классификации**, который классифицирует каждый бинарный файл и разрешает запуск только тем из них, кто проверен нашей облачной системой с искусственным интеллектом
- EDR-технологии, особенно система обнаружения **Индикаторов атак (IoA) по поведению и контексту.**

Из того, что мы видим в нашей лаборатории, наиболее распространенным примером атак является почтовые спамовые письма с использованием технологий социального инжиниринга. Такие письма содержат дроппер, который загружает бинарный файл здесь:

C:\Users\user\AppData\Local\Temp\qeSw.exe
Хэш: 258ED03A6E4D9012F8102C635A5E3DCD
Решения Panda обнаруживают дроппер как Trj/GdSda.A

Данный бинарный файл шифрует компьютер (процесс: vssadmin.exe) и удаляет теневые копии с использованием процесса conhost.exe.

Официальные источники IoC

Испанский национальный криптографический центр имеет исчерпывающий список индикаторов компрометации (IoC) на уровне хэшей, IP-адресов и доменов:
https://www.ccn.cni.es/index.php/en/.

Информация может быть доступна здесь:
https://loreto.ccn-cert.cni.es/index.php/s/oDcNr5Jqqpd5cjn

Как защитить себя от этих и других кибер-угроз

Благодаря **сервису 100% классификации,** который классифицирует все бинарные файлы до их запуска и блокирует запуск любых вредоносных бинарных файлов, решения Panda по защите конечных устройств с опциями расширенной защиты очень эффективны для остановки таких вредоносных кампаний, как и многих других.

Этот сервис использует высокоэффективный механизм для обнаружения и удаления вредоносных программ и шифровальщиков еще до их запуска независимо от того, являются ли они новыми вариантами угроз или новыми вредоносными доменами, как в случае с вредоносными объектами, связанными с COVID-19.

Поведенческие и контекстуальные индикаторы атак (IoA) обнаруживают и блокируют необычные шаблоны поведения на защищенных устройствах: например, загрузка исполняемого файла из Word или попытка доступа к неизвестным или вредоносным URL. Любая попытка компрометации устройства немедленно блокируется, а выполнение вредоносных действий и подключение к вредоносным доменам останавливается.


panda
30
year
anniversary