

THREAT LANDSCAPE - C19 RED EDITION

**Sille Laks
Cyber Security Expert
Cyber4Dev
@SilleLaks
22.10.2020**



C19 - attacker's view



Experts warn “Hackers exploit corona virus to spread malware” - 18/2/2020

Singapore Specialist : Corona Virus Safety Measures

 **DT**
Tuesday, 28 January 2020 at 03:51
[Show Details](#)

Dear Sir,

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

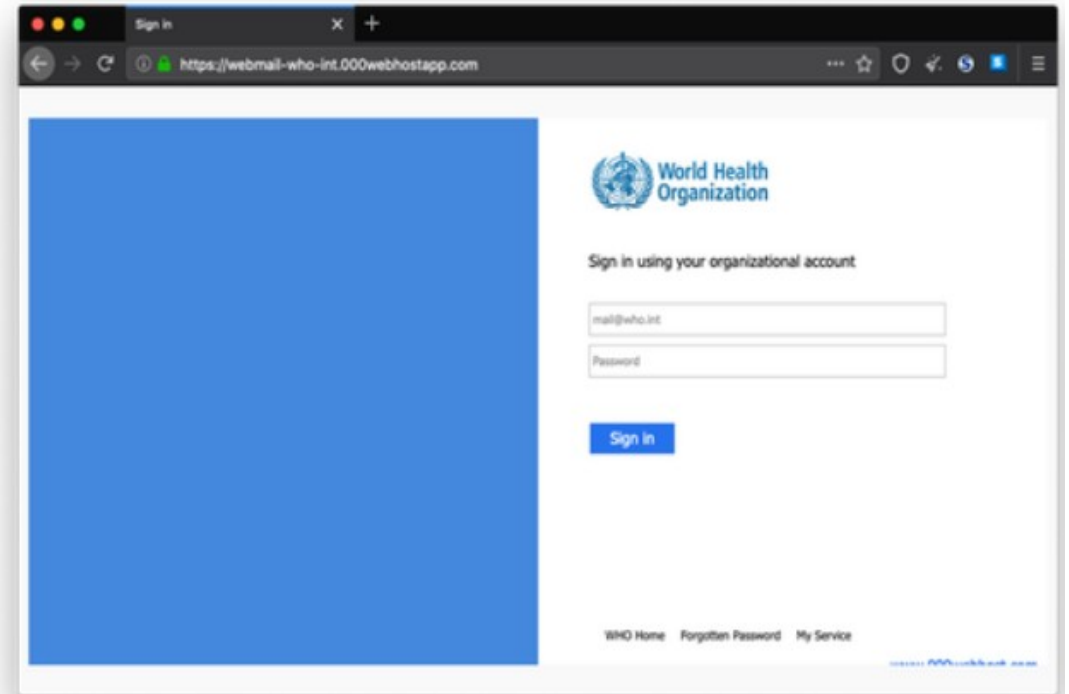
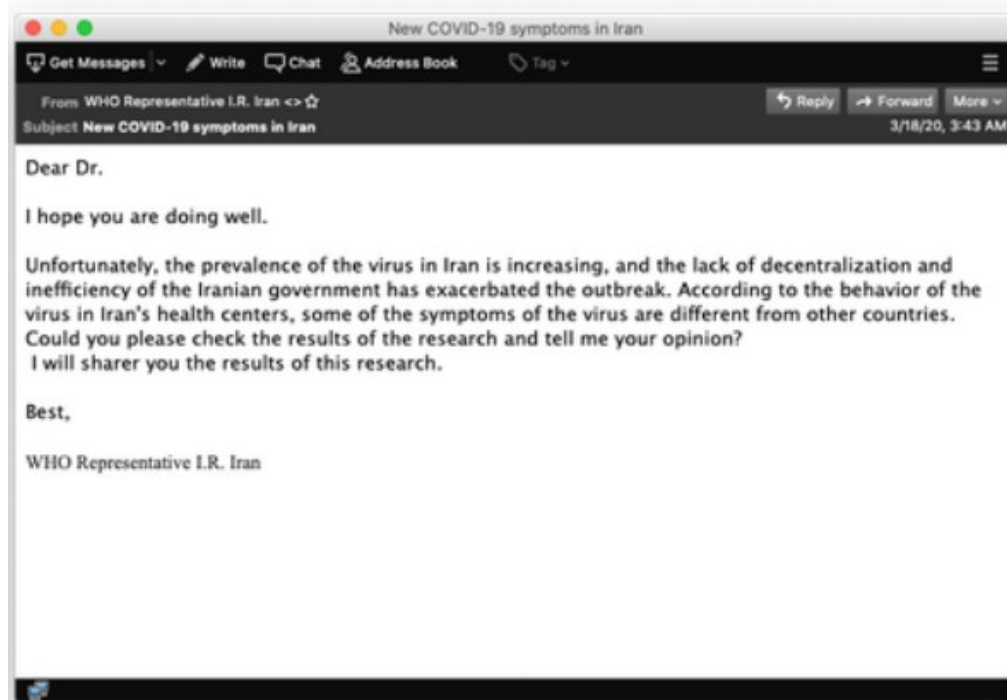
Use the link below to download

[Safety Measures.pdf](#)

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

Regards
Dr 
Specialist wuhan-virus-advisory


KITTENS? HOW CHARMING



PAYMENTS WILL MOVE ONLINE

E-PAYMENT BANK TRANSACTIONS - Message (Plain Text)

File Message Help Tell me what you want to do

Protect Mark Unread Find Zoom Share to Teams Send to OneNote

E-PAYMENT BANK TRANSACTIONS

WS [Redacted] <[Redacted]>
To: undisclosed-recipients:
We removed extra line breaks from this message.
Payment Form for Bank related transactions_zip.arj
1 MB

Reply Reply All Forward ...
Thu 5/7/2020 3:32 PM

Dear Customer,

Due to the COVID-19 virus lockdown affecting countries and businesses, Our Finance HQ will implement online payment banking to all our active vendors/suppliers.

No more cheques will be issued out.

Kindly provide all your bank related details in above attachment form for swift payment process.

Please your urgent feedback is needed for our Finance Team.

Thank you very much.


[Redacted]
Sales Executive
[Redacted]
[Redacted]
TEL: [Redacted]
FAX: [Redacted]

CONFIDENTIAL CORONA CURE

Message


Confidential Cure Solution on Corona virus - Temporary Items

Confidential Cure Solution on Corona virus

 Tuesday, February 4, 2020 at 10:10 AM
[Show Details](#)


Corona virus prevention vaccine and cure medication has been secretly developed by our medical scientist who's names are meant to remain silent for security reasons. We know that the world has been struggling to contain this deadly virus developed and sprayed by wicked scientists to reduce the population of the world so the government will have control over you. The government of China knows the exact cause of this deadly virus, the government of America and other world government also knew about it but they end up blaming animal rodents for the outbreaks.

This corona virus is a weapon created to discredit rivals government health systems or the other way to control the citizens of the world but due to some people like us and our medical teams hate the injustice going in this world. Our secret medical scientist team has developed the cure and prevention to counter this evil act of the world to save lives of innocent people around the world. For those interested to secure their lives kindly reply and get more information about shipping or delivery to you and private distribution.



Dr. Carlos Gerrado sent you a free health guideline

[Click for Corona-Virus Cure Review](#)



Thank You,

YOU DON'T HAVE TO OVERDO IT



The image shows a screenshot of a Microsoft login page. At the top left is the Microsoft logo. Below it is a back arrow and a redacted email address ending in ".com". The main heading is "Enter password". Below that is a message: "Because you're accessing sensitive info, you need to verify your password". There is a "Password" input field with a horizontal line below it. Below the input field is a link that says "Forgot my password". In the bottom right corner, there is a blue button with the text "Sign in".

Google blocked 18M C19 phishing e-mails a week in April

BUSINESS CONTINUITY PLAN

COVID-19 UPDATE // BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MAY 2020. - Message (Plain Text)

File Message Help Tell me what you want to do

Delete Delete Archive

Respond Reply Reply All Forward

Protection Protect

Quick Steps Signature To Manager Team Email

Move Move

Tags Assign Policy Categorize Follow Up

Editing Translate

Speech Read Aloud

Zoom Zoom

Teams Share to Teams

OneNote Send to OneNote

Insights

Protection Report Message

COVID-19 UPDATE // BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MAY 2020.

 CENTER FOR DISEASE CONTROL & MANAGEMENT <[redacted]>
To undisclosed-recipients:

Reply Reply All Forward ...

Wed 5/6/2020 6:47 AM

We removed extra line breaks from this message.

 BUSINESS TRANSACTION NOTICE ON COVID-19 DOCUMENT_pdf.arj
1 MB

Dear Partners,

A MUST READ!!!

Find in the attached everything you need to know about the business continuity plan and management of the deadly Wuhan Coronavirus and as published by the World Health Organisation (WHO).

Endeavour to read through so as to keep you safe from the COVID-19 virus.

A HEALTHY YOU BREEDS A HEALTHY SOCIETY.

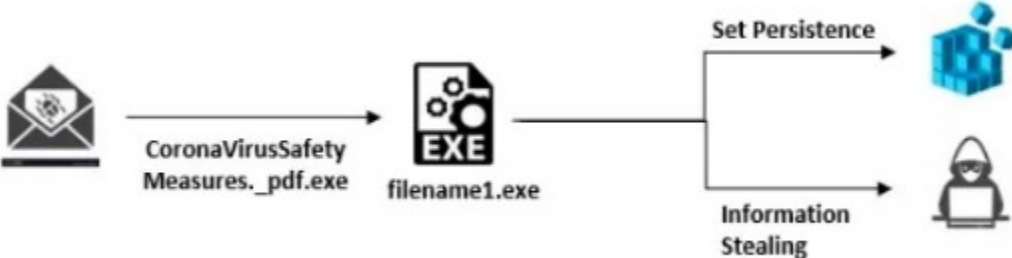
Regards,



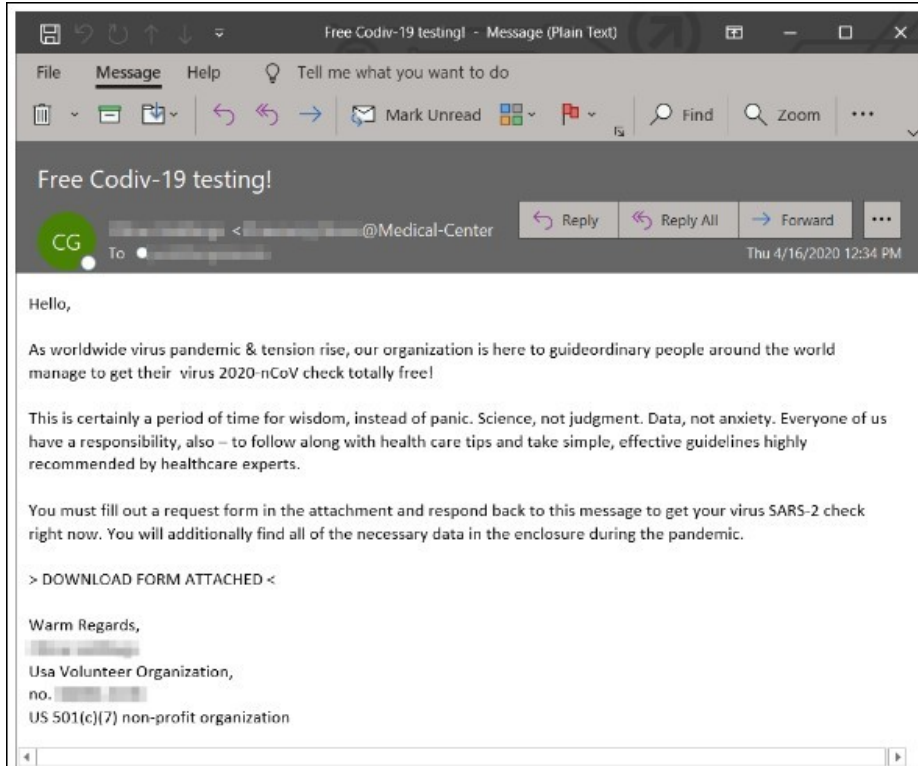
CENTER FOR DISEASE CONTROL



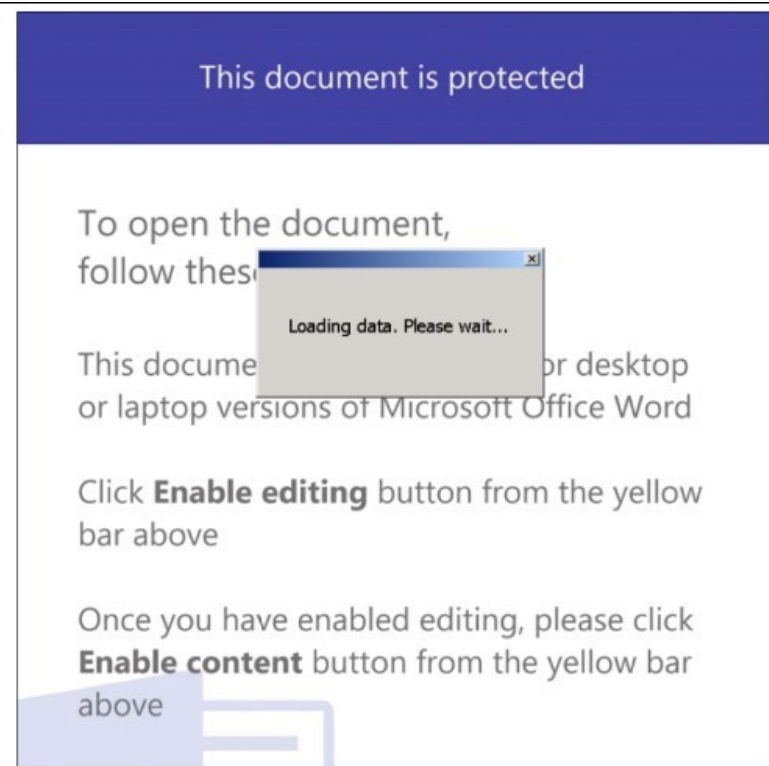
EXECUTE CORONA VIRUS SAFETY MEASURES



FREE! TESTING



Phishing email sample



Malicious macro in action

We got all the protection you need!

Masks, gloves, wipes, sanitizer
Criminals are just waiting
to make a fortune from
COVID-19.

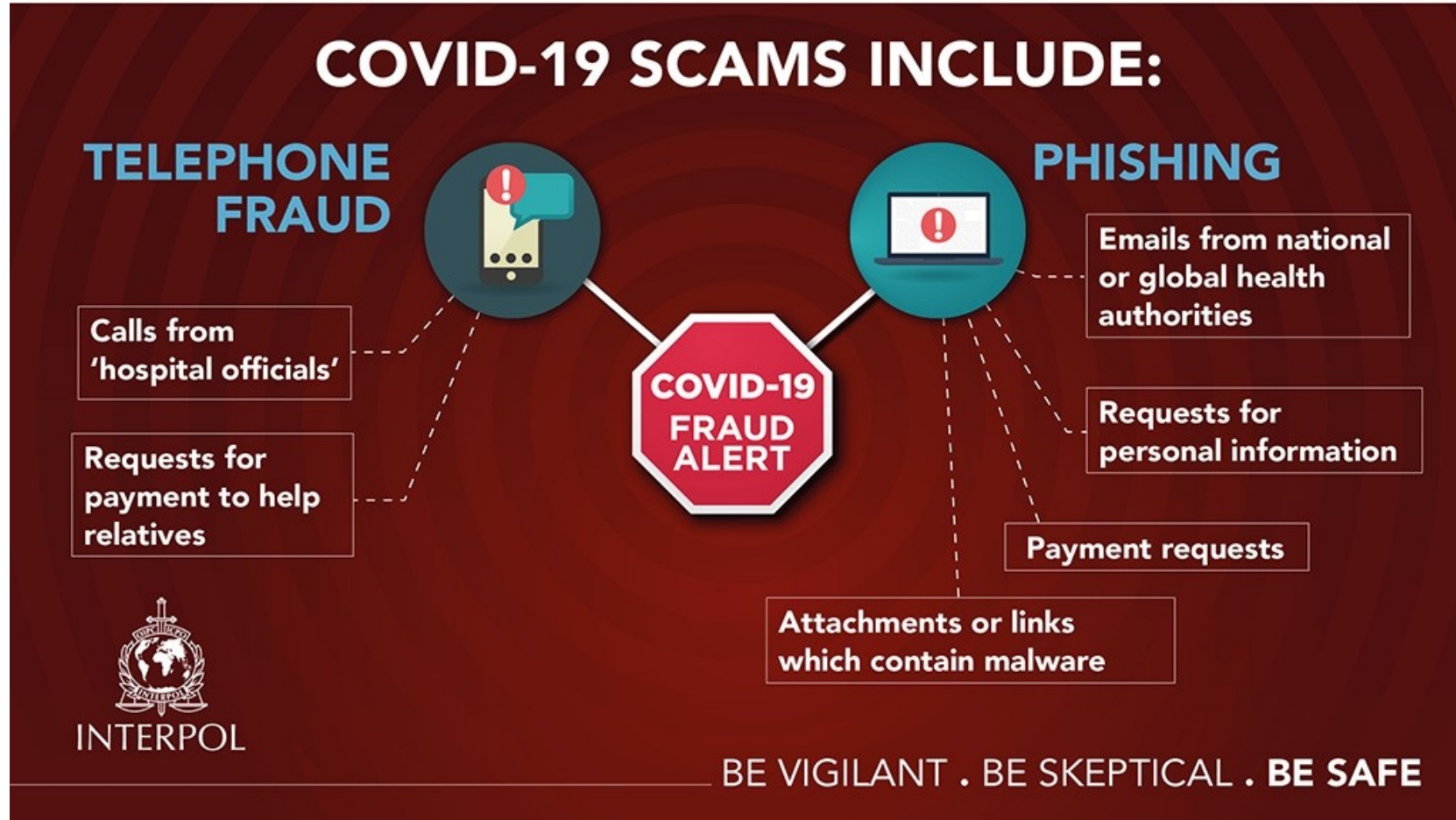
DON'T LET THEM.



INTERPOL

BE VIGILANT . BE SKEPTICAL . **BE SAFE**

Include but not limited to



Australian COVIDSafe app



“REAL COVID” TRACING APP ... OR AN OLD-FASHIONED SMS

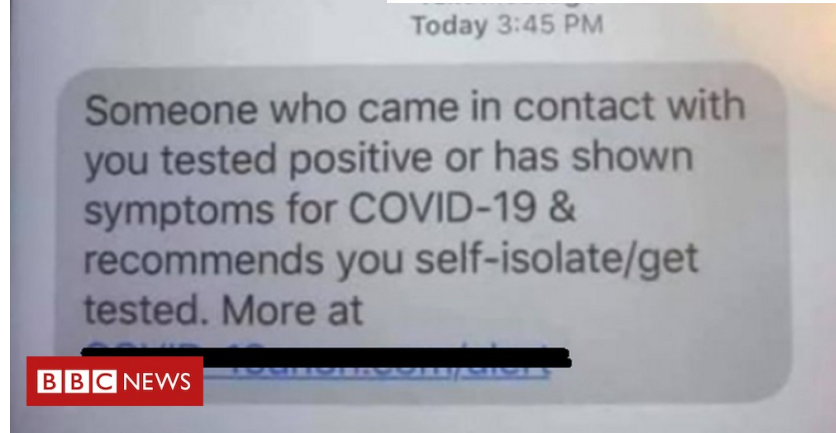
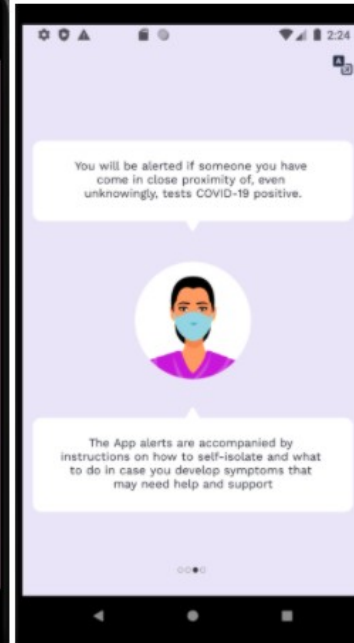
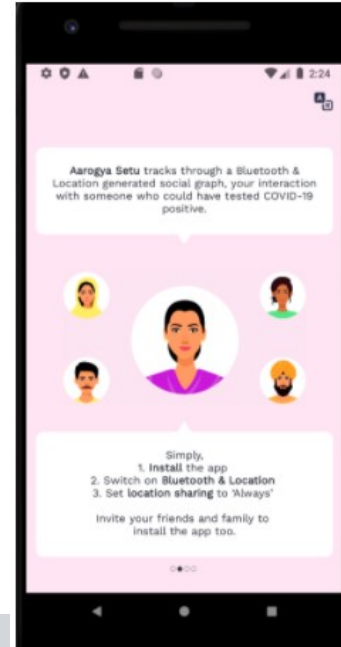


YOUR PHONE IS ENCRYPTED: YOU HAVE 48 HOURS TO PAY 100\$ in BITCOIN OR EVERYTHING WILL BE ERASED

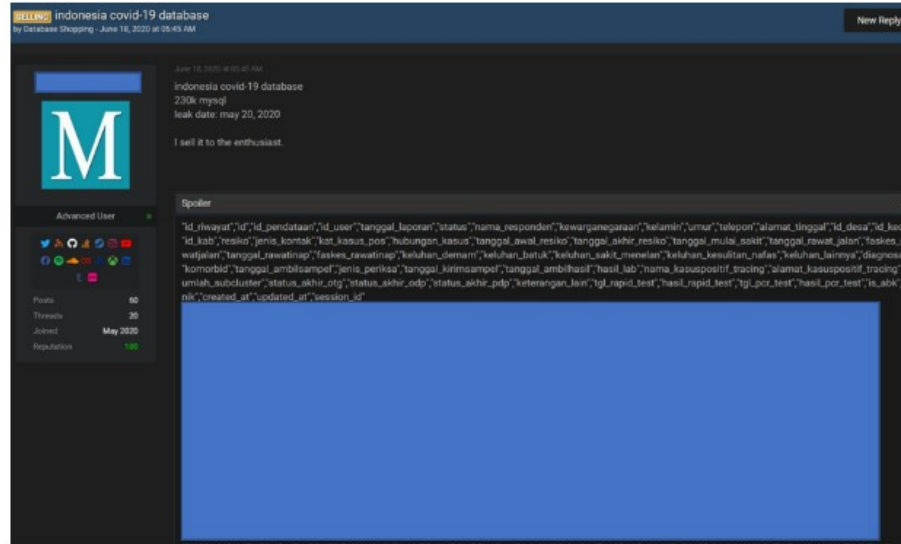
1. What will be deleted? your contacts, your pictures and videos, all social media accounts will be leaked publicly and the phone memory will be completely erased
2. How to save it? you need a decryption code that will disarm the app and unlock your data back as it was before
3. How to get the decryption code? you need to send the 100\$ in bitcoin to the adress below, click the button below to see the code

NOTE: YOUR GPS IS WATCHED AND YOUR LOCATION IS KNOWN, IF YOU TRY ANYTHING STUPID YOUR PHONE WILL BE AUTOMATICALLY ERASED

Web Designius



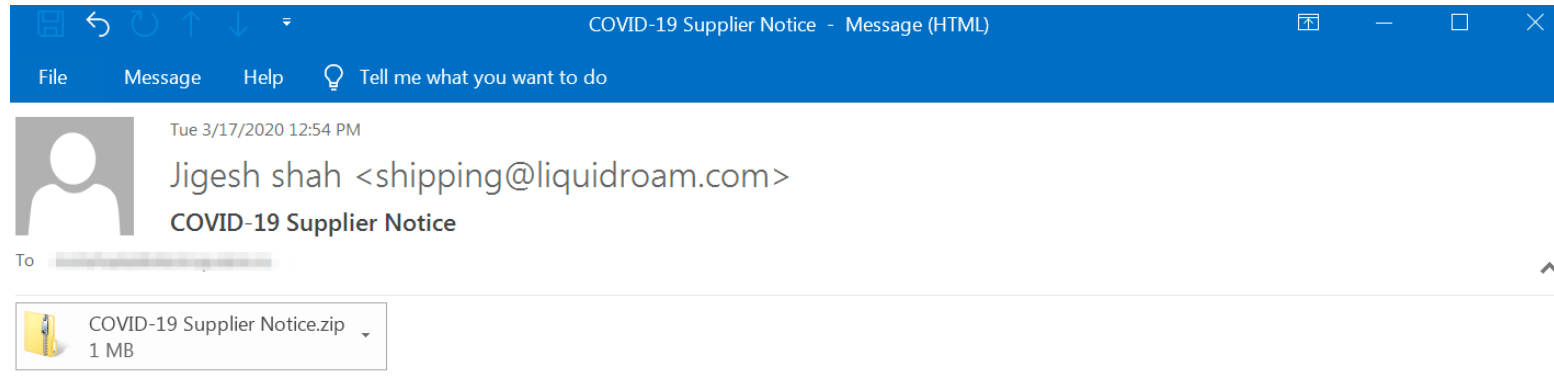
230K C19 PATIENTS PERSONAL DATA IN DARK WEB



The leaked database includes the following fields:

- *name*
- *address*
- *present address*
- *telephone number*
- *citizenship*
- *diagnosis date*
- *result*
- *result date, and many more*

C19 - SUPPLIER NOTIFICATION



Dear Valued Supplier,

Please find attached second notificatio=.

Regards,

Jigesh shah
Senior Buyer,
Worley Landmark=Building,
Building # 5115, Way 4557,
3rd & 4th Floor, 23rd July=Street,
South Al Khuwair,
Post office Box 795,
Postal Code 133,=
Muscat, Sultanate of Oman
T: +968 24473332 M: +968 93299359 | GMT = 4:00 www.worley.com

ALL YOUR FILES ARE BELONG TO US

RASOM20

YOUR PC IS LOCKED

If you want to unlock your files you must send 0.35 BTC (Bitcoin) to this address

1wNyr6A5ZCUxE2fShTvUGPtHfuovT7uBt


After payment send email to : RASOM20@secmail.pro

Insert in message : transaction id - Pc Name - Username



WE ARE CHANGING VENDORS, BAKRUPT BANKS, AND EMPLOYEES

< Inbox





From: **John Smith** <jsmith@acmee.com> (look-alike domain registered) 

To: **Jane Doe** <jdoe@customer.com>

Subject: **Re: Acme Company**

Due to the news of the Corona-virus disease (COVID-19) we are changing banks and sending payments directly to our factory for payments, so please let me know total payment ready to be made so i can forward you our updated payment information.

Kind regards

ZOOM IS EVIL! ZOOM IS DANGEROUS!



ALL CLASSES ARE NOW ONLINE! CREATE AN ACCOUNT IN XYZ ENVIRONMENT



“HELLO! I AM CALLING FROM YOUR BANK, INSURANCE, HR, WHO, PLEASE CONFIRM YOUR CREDIT CARD DETAILS FOR REFUND/ SUPPORT/WINNING?!”



ENISA's fresh publication of TOP 15 cyber threats

TOP 15 CYBER THREATS



1  Malware	2  Web-based attacks	3  Phishing	4  Web application attacks	5  Spam
6  DDoS	7  Identify theft	8  Data breach	9  Insider threat	10  Botnets
11  Physical manipulation, damage, theft and loss	12  Information leakage	13  Ransomware	14  Cyberespionage	15  Cryptojacking



Incident response C-101

Sille Laks
Cyber Security Expert
Cyber4Dev
@SilleLaks
21.10.2020



**When was the first IR team
founded?**

a) 1962

b) 1988

c) 1997

d) 1972

1988 - Morris worm

- The Morris worm was one of the first computer worms distributed via Internet and the first to gain significant mainstream media attention. It was written by a graduate student at Cornell University, Robert Tappan Morris, and launched on **November 2, 1988** to highlight security flaws.
- Exploited **known vulnerabilities** in Unix sendmail, finger, and rsh/rexec, and weak passwords BUT it had a coding error so that the computer could be infected multiple times and each additional process would slow the machine down, eventually to the point of being unusable.
- **60000** computers connected to the Internet – **6000** impacted - **10%** all all the computers in the world

In response - CERT-CC

The Morris worm prompted DARPA to fund the establishment of the **CERT/CC at Carnegie Mellon University**, to give experts a central point for coordinating responses to network emergencies

Phage mailing list to **coordinate** incident response - originally concerned with identifying and eradicating the Morris worm, later reflecting and considering broader issues in computer security

2020

- **CERT** – Computer Emergency Response Team
- **CSIRT** – Computer Security Incident Response Team
- **SOC** – Security Operations Centre
- **IRT** - Incident Response Team
- **RRT** - Rapid Response Team
- **NCSC** - **National Cyber Security Centre**

You need to start an incident response team. What/ who first?

- People?
- Procedures?
 - Money?
- Equipment?
- Constituency?
 - Partners?
- Legal aspects?

People are always the most important component

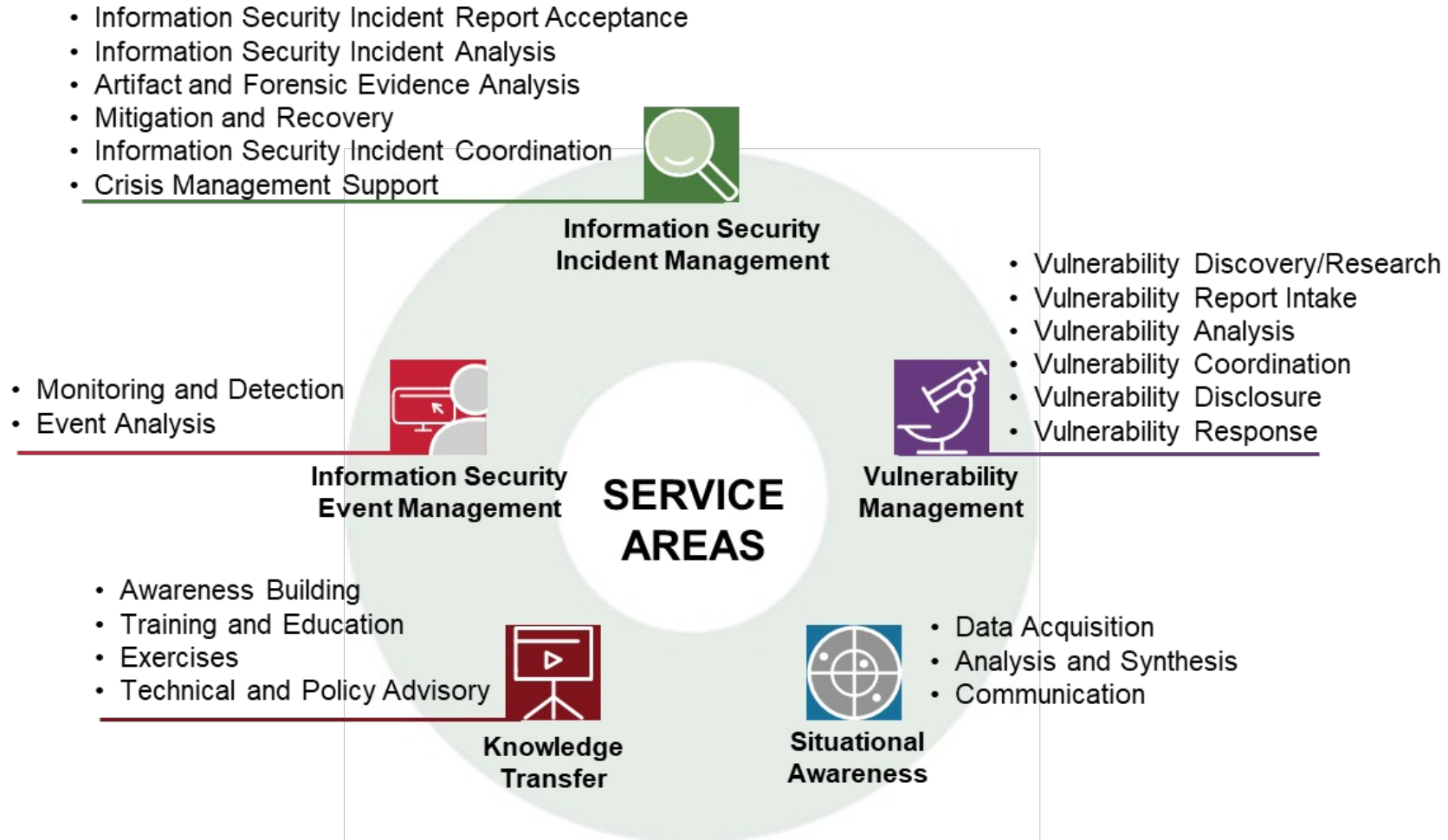
- ... will determine how much funding will you receive,
- ... how many people can you have for the incident response team,
- ... establish the procedures,
- ... define your constituency and legal aspects, and
- ... establish partners and trust within the constituency

Framework

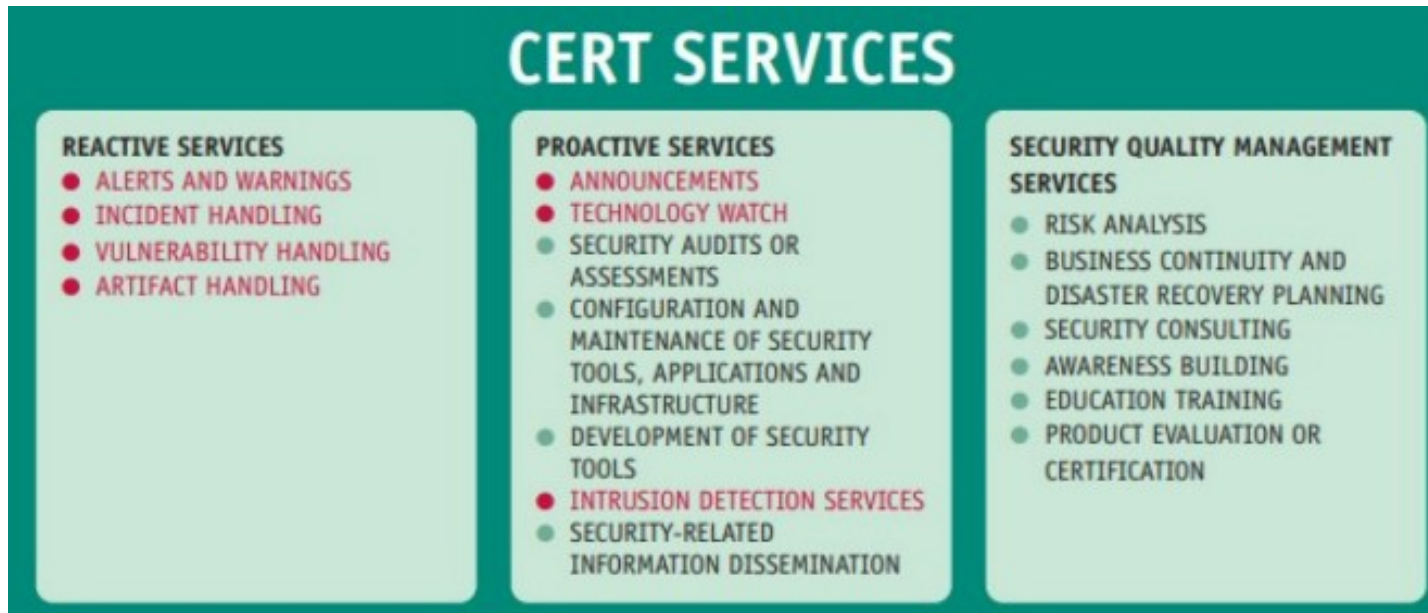
- **Mission statement** – serves the organization or entire constituency not just IT department, reflect important business assets, and preferably also quality assurance!
- **Constituency** - IP range, AS, domain name, free text
- **Responsibilities and mandate** – defines the matters and extent of incident response. Clearly described and sanctioned by the management. What can CERT do and what cannot CERT do!
- **Organizational framework** – escalations, CISO, crisis management, human resources
- **Services provided** – reactive services, proactive services, security quality management services



FIRST CSIRT Services Framework Service Areas and Services



ENISA Incident Management Guide



Information Security Incident Management services

- Information security incident report acceptance
- Information security incidents analysis
- Artefact and forensic evidence analysis
- Mitigation and recovery
- Information security incident coordination
- Crisis management support

Information Security Incident Analysis functions

- Information security incident triage (prioritization and categorization)
- Information collection
- Detailed analysis coordination
- Information security incident root cause analysis
- Cross-incident correlation

Artifact and forensic evidence analysis

- The context required of the artefact to run and to perform its intended tasks, whether malicious or not
- How the artefacts may have been utilized for the attack: uploaded, downloaded, copied, executed, or created within an organization's environments or components
- Which systems have been involved locally and remotely to support the distribution and actions
- What an intruder did once access to the system, network, organization, or infrastructure was established: from passively collecting data, to actively scanning and transmitting data for exfiltration purposes, or collecting new action requests, updating itself or making a lateral movement inside a compromised (local) network
- What a user, user process, or user system did once the user account or user device was compromised
- What behavior characterizes the artefacts or compromised systems, either in standalone mode, in conjunction with artefacts or components, connected to a local network or the Internet, or in any combination
- How the artefacts or compromised systems establish connectivity with the target (e.g., intrusion path, initial target, or detection evasion techniques);
- What communication architecture (peer-to-peer, command-and-control, both) has been utilized
- What were the actions of the threat actors, what is their network and systems footprint
- How the intruders or artefacts evaded detection (even over long periods of time which may include reboot or reinitialization)

Establishing an incident response plan

- Determine the business impact of the information security incident
- Determine the business requirements and timeframe for a successful recovery
- Define decision processes and criteria (if not already defined by policies)
- Identify the objects to be recovered: environments, systems, applications, systems, transversal functions, etc.
- Identify required support and actions by internal and external entities
- Determine a response plan that provides for a meaningful response within the desired business requirements and timeframe based on available resources and the technical scope of required actions

Incident response - ad-hoc measures and containment

- Temporarily remove access for users/systems/services/networks
- Temporarily disconnect systems or networks from networks or backbones
- Temporarily disable services
- Require users to change their passwords or crypto credentials
- Monitor for signs of intrusions and indicators of compromise
- Verify that all users/systems/services/networks are unaffected

Incident response - coordination | Communication

- Communication
 - Notification distribution
 - Relevant information distribution
 - Activities coordination
 - Reporting
 - Media communication
- Internal and external communication
 - Reporting and recommendations
 - Implementation
 - Dissemination / integration / information sharing
 - Management of information sharing

Workflow

- Detection - identification, classification
- Triage – significance, time constraints, severity, is it our constituency (no -> inform responsible constituency), mandate, speed of spreading, how many (possibly) impacted, who should handle this incident?
- Analysis – technical analysis, possible impact analysis, business criticality, characteristics, details matter!
- Incident Response - information and response coordination, mitigation, information gathering, details matter, chronological order

Incident lifecycle – occurrence -> detection-> diagnostics-> repair -> recovery -> restoration -> closure

Details matter!

- Detailed contact information
- Detailed description of the incident
- Incident classification (suggested by the reporter/ actual)
- Logs/ images
- Chronology -> keep a logbook in chronological order!
- As many technical details about impacted systems as possible
- Security systems checkup
- Incident severity (for the impacted party)

C19 - challenges

- COVID-19 can already be classified as the **largest-ever** cybersecurity threat (Security Weekly, March 2020; Panda security, August 2020)
- Econsult Solutions study finds that companies spend an average of **0.06%** of their revenue on cybersecurity
- Cyber attacks most prevalent in the **healthcare** and **financial industries**.
- Email phishing attacks are the most common source of data breaches → lateral movement
- Ransomware → Pay or we publish your data



C19 - challenges

- Remote work
- Financial limitations
- Capacity limitations
- HR limitations
- Legislation limitations



1. 47% of employees cited distraction as the reason for falling for a phishing scam while working from home. ([Tessian](#))
2. Web application breaches account for 43% of all breaches and have doubled since 2019. ([Verizon](#))
3. 52% of legal and compliance leaders are concerned about third-party cyber risks due to remote work since COVID-19. ([Gartner](#))
4. Remote work has increased the average cost of a data breach by \$137,000. ([IBM](#))
5. 81% of cybersecurity professionals have reported their job function changed during the pandemic. ([\(ISC\)²](#))
6. In April, 83% of tech firms reported new customer inquiries, 36% of which within the cybersecurity sector. ([CompTIA](#))
7. The search term "how to remove a virus" increased by 42% in March. ([Google Trends](#))
8. From January to March there was an increase of 8.3% in mobile VPN usage. ([WatchGuard](#))
9. 76% of remote workers say working from home would increase the time to identify and contain a breach. ([IBM](#))



Scams increased by **400%** over the month of March, making **COVID-19 the largest-ever security threat.**

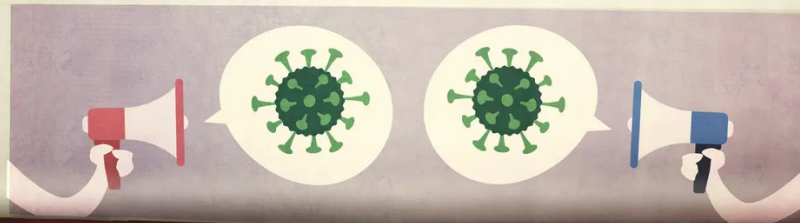
Source: ReedSmith

THE DAILY

CORONAVIRUS

FAKE NEWS

The spread of COVID-19 fake news





<https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents>

<https://www.pymnts.com/news/security-and-risk/2020/big-spike-in-ceo-fraud/>

<https://www.who.int/about/communications/cyber-security>

<https://cisomag.eccouncil.org/data-breaches-on-e-learning-platforms/>

<https://latinamericanpost.com/15225-wannacry-cyberattack-numbers-in-latin-america>

<https://www.elfinancierocr.com/tecnologia/firmas-locales-reportan-diversos-ataques-informaticos-en-costa-rica-pero-no-de-wannacry/ZXDDVITDDJAW5GEVFLY5BLOALE/story/>

<https://qcostarica.com/when-it-comes-to-ransomware-its-sometimes-best-to-pay-up/>

<http://country.eiu.com/article.aspx?articleid=105661194&Country=Costa+Rica&topic=Economy&oid=723778656&aid=1>

<https://www.darkreading.com/vulnerabilities---threats/fake-covid-19-contact-tracing-apps-infect-android-phones/d/d-id/1338047>

<https://www.businessinsider.com/coronavirus-fake-app-ransomware-malware-bitcoin-android-demands-ransom-domain-tools-2020-3>

<https://www.globenewswire.com/news-release/2020/06/10/2046381/0/en/Anomali-Threat-Research-Detects-Fake-COVID-19-Contact-Tracing-Apps-Spreading-Malware.html>

<https://www.welivesecurity.com/2016/09/02/ceo-fraud-stay-protected-modern-day-deception/>

<https://www.welivesecurity.com/2020/03/13/415pm-urgent-message-ceo-fraud/>

<https://www.pymnts.com/news/security-and-risk/2020/big-spike-in-ceo-fraud/>

<https://securityboulevard.com/2020/02/emotet-attacks-spread-alongside-fears-of-coronavirus/>

<https://orange cyberdefense.com/uk/covid-19-and-cyberdefense/>

<https://securityaffairs.co/wordpress/99669/cyber-crime/bec-coronavirus-themed-attacks.html>

<https://securityaffairs.co/wordpress/98420/malware/south-korea-corona-19.html>

<https://www.bleepingcomputer.com/news/security/microsoft-trickbot-in-hundreds-of-unique-covid-19-lures-per-week/>

<https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html>

<https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/>

<https://cybleinc.com/2020/06/21/230k-indonesian-covid-19-patients-personal-information-leaked-in-the-darknet/>

<https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/>

<https://www.theguardian.com/australia-news/2020/apr/28/guardian-essential-poll-suspicious-about-tracing-app-offset-by-approval-of-covid-19-response>

<https://www.infosecurity-magazine.com/news/cybercrime-growing-alarming-pace/>

https://info.abnormalsecurity.com/rs/231-IDP-139/images/AS_Qtrly_BEC_Report_061120.pdf

<https://www.bleepingcomputer.com/news/security/gmail-blocked-18m-covid-19-themed-phishing-emails-in-a-week/>

<https://www.bleepingcomputer.com/news/security/microsoft-trickbot-in-hundreds-of-unique-covid-19-lures-per-week/>

<https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/>

<https://www.bleepingcomputer.com/news/security/us-consumers-report-12m-in-covid-19-scam-losses-since-january/>

<https://www.ic3.gov/media/2020/200320.aspx>

<https://securityboulevard.com/2020/02/emotet-attacks-spread-alongside-fears-of-coronavirus/>

<https://www.who.int/about/communications/cyber-security>

<https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/>

<https://www.bleepingcomputer.com/news/security/nation-backed-hackers-spread-crimson-rat-via-coronavirus-phishing/>

<https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/>

<https://testguild.com/podcast/security/s14-marko/>