A Hacker's Viewpoint

PLANNING THE ATTACK

Who are these people?

What in the heck is PRE-ATT&CK???

I'm more of a visual person...

Can you explain that PRE whatever again? o.O

OK...now for the TLDR!

Ummm...I have a question :-)

Let's go around and introduce ourselves!

Kristina Krasnolobova

Title: Cyber Security Analyst

Company: Sentara Healthcare

Role: I look at events to go by, try to make sense of them and occasionally tell people "BAD USER" when they click on the links and put in their password...

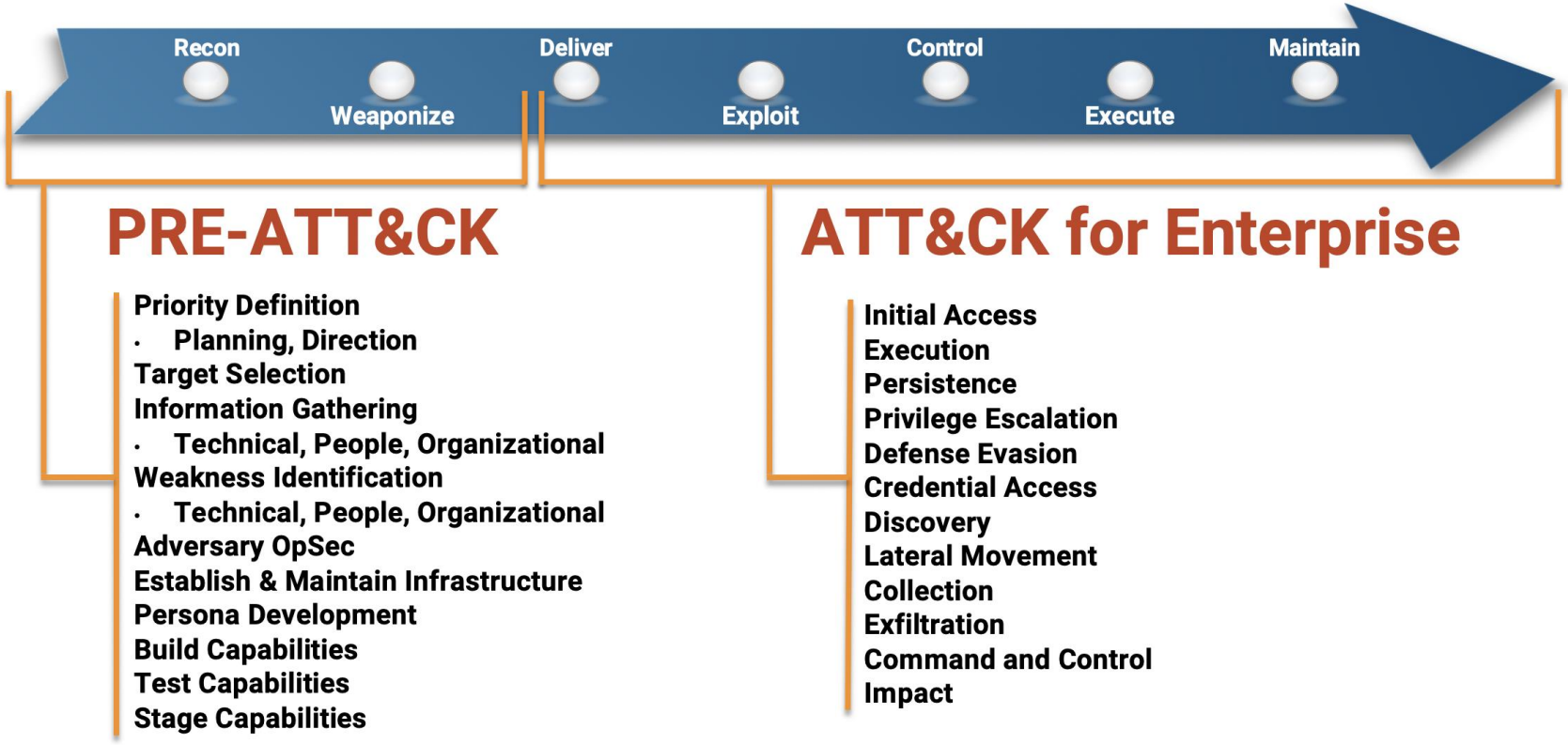
Robert George

Title: Principle Cybersecurity Architect

Company: Sentara Healthcare

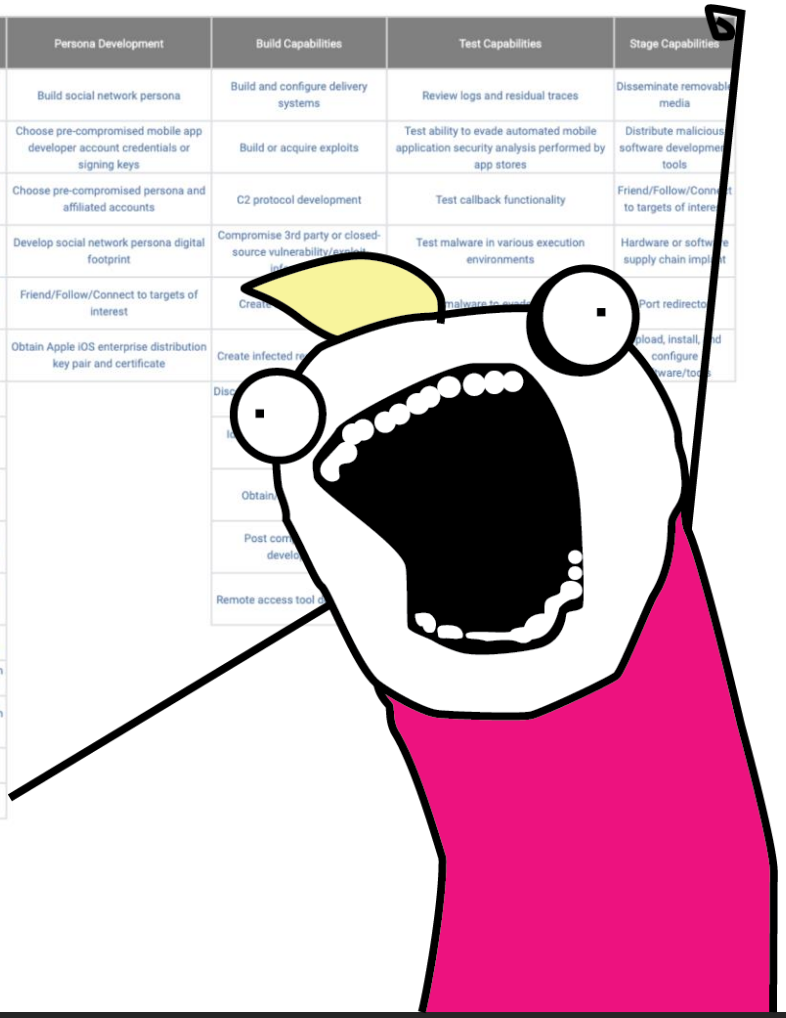
Role: I evaluate security controls and tell people NO a lot... I also evaluate new technologies that never seem to make the budget.

Cyber Kill Chain + CSF + lots more = MITRE ATT&CK!!!




I'm not impressed...

Priority Definition Planning	Priority Definition Direction	Target Selection	Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification	Adversary OPSEC	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities	Stage Capabilities
Assess KITs/KIQs benefits	Assign KITs, KIQs, and/or intelligence requirements	Determine approach/attack vector	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Acquire OSINT data sets and information	Analyze application security posture	Analyze organizational skillsets and deficiencies	Analyze business processes	Acquire and/or use 3rd party infrastructure services	Acquire and/or use 3rd party infrastructure services	Build social network persona	Build and configure delivery systems	Review logs and residual traces	Disseminate removable media
Assess current holdings, needs, and wants	Receive KITs/KIQs and determine requirements	Determine highest level tactical element	Conduct active scanning	Aggregate individual's digital footprint	Conduct social engineering	Analyze architecture and configuration posture	Analyze social and business relationships, interests, and affiliations	Analyze organizational skillsets and deficiencies	Acquire and/or use 3rd party software services	Acquire and/or use 3rd party software services	Choose pre-compromised mobile app developer account credentials or signing keys	Build or acquire exploits	Test ability to evade automated mobile application security analysis performed by app stores	Distribute malicious software development tools
Assess leadership areas of interest	Submit KITs, KIQs, and intelligence requirements	Determine operational element	Conduct passive scanning	Conduct social engineering	Determine 3rd party infrastructure services	Analyze data collected	Assess targeting options	Analyze presence of outsourced capabilities	Acquire or compromise 3rd party signing certificates	Acquire or compromise 3rd party signing certificates	Choose pre-compromised persona and affiliated accounts	C2 protocol development	Test callback functionality	Friend/Follow/Connect to targets of interest
Assign KITs/KIQs into categories	Task requirements	Determine secondary level tactical element	Conduct social engineering	Identify business relationships	Determine centralization of IT management	Analyze hardware/software security defensive capabilities		Assess opportunities created by business deals	Anonymity services	Buy domain name	Develop social network persona digital footprint	Compromise 3rd party or closed-source vulnerability/exploit	Test malware in various execution environments	Hardware or software supply chain implant
Conduct cost/benefit analysis		Determine strategic target	Determine 3rd party infrastructure services	Identify groups/roles	Determine physical locations	Analyze organizational skillsets and deficiencies		Assess security posture of physical locations	Common, high volume protocols and software	Compromise 3rd party infrastructure to support delivery	Friend/Follow/Connect to targets of interest	Create		Port redirector
Create implementation plan			Determine domain and IP address space	Identify job postings and needs/gaps	Dumpster dive	Identify vulnerabilities in third-party software libraries		Assess vulnerability of 3rd party vendors	Compromise 3rd party infrastructure to support delivery	Create backup infrastructure	Obtain Apple iOS enterprise distribution key pair and certificate	Create infected r		pload, install, and configure ware/tool
Create strategic plan			Determine external network trust dependencies	Identify people of interest	Identify business processes/tempo	Research relevant vulnerabilities/CVEs			DNSCalc	Domain registration hijacking		Dis		
Derive intelligence requirements			Determine firmware version	Identify personnel with an authority/privilege	Identify business relationships	Research visibility gap of security vendors			Data Hiding	Dynamic DNS				
Develop KITs/KIQs			Discover target logon/email address format	Identify sensitive personnel information	Identify job postings and needs/gaps	Test signature detection			Dynamic DNS	Install and configure hardware, network, and systems		Obtain		
Generate analyst intelligence requirements			Enumerate client configurations	Identify supply chains	Identify supply chains				Fast Flux DNS	Obfuscate infrastructure		Post co develo		
Identify analyst level gaps			Enumerate externally facing software applications technologies, languages, and dependencies	Mine social media	Obtain templates/branding materials				Host-based hiding techniques	Obtain booter/stressor subscription		Remote access tool		
Identify gap areas			Identify job postings and needs/gaps						Misattributable credentials	Procure required equipment and software				
Receive operator KITs/KIQs tasking			Identify security defensive capabilities						Network-based hiding techniques	SSL certificate acquisition for domain				
			Identify supply chains						Non-traditional or less attributable payment options	SSL certificate acquisition for trust breaking				
			Identify technology usage patterns						OS-vendor provided communication channels	Shadow DNS				
			Identify web defensive services						Obfuscate infrastructure	Use multiple DNS infrastructures				
			Map network topology						Obfuscate operational infrastructure					
			Mine technical blogs/forums						Obfuscate or encrypt code					
			Obtain domain/IP registration information						Obfuscation or cryptography					
			Spearphishing for Information						Private whois services					
									Proxy/protocol relays					
									Secure and protect infrastructure					



But look at all the things...
ALL THE THINGS


Kandy Korn
Home
Cyber Security
Cyber Security
Incident Response Process

Movie Credits

CAST

Hacker - Cameron Walters-Lugo

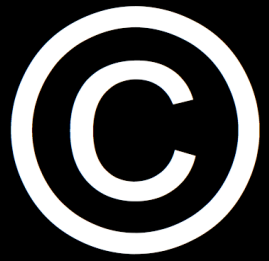
CREW TEAMS

AUDIO CREW

Audio in the hacker video that you can't hear - Ed Muducdoc

COSTUME/DECORATION CREW

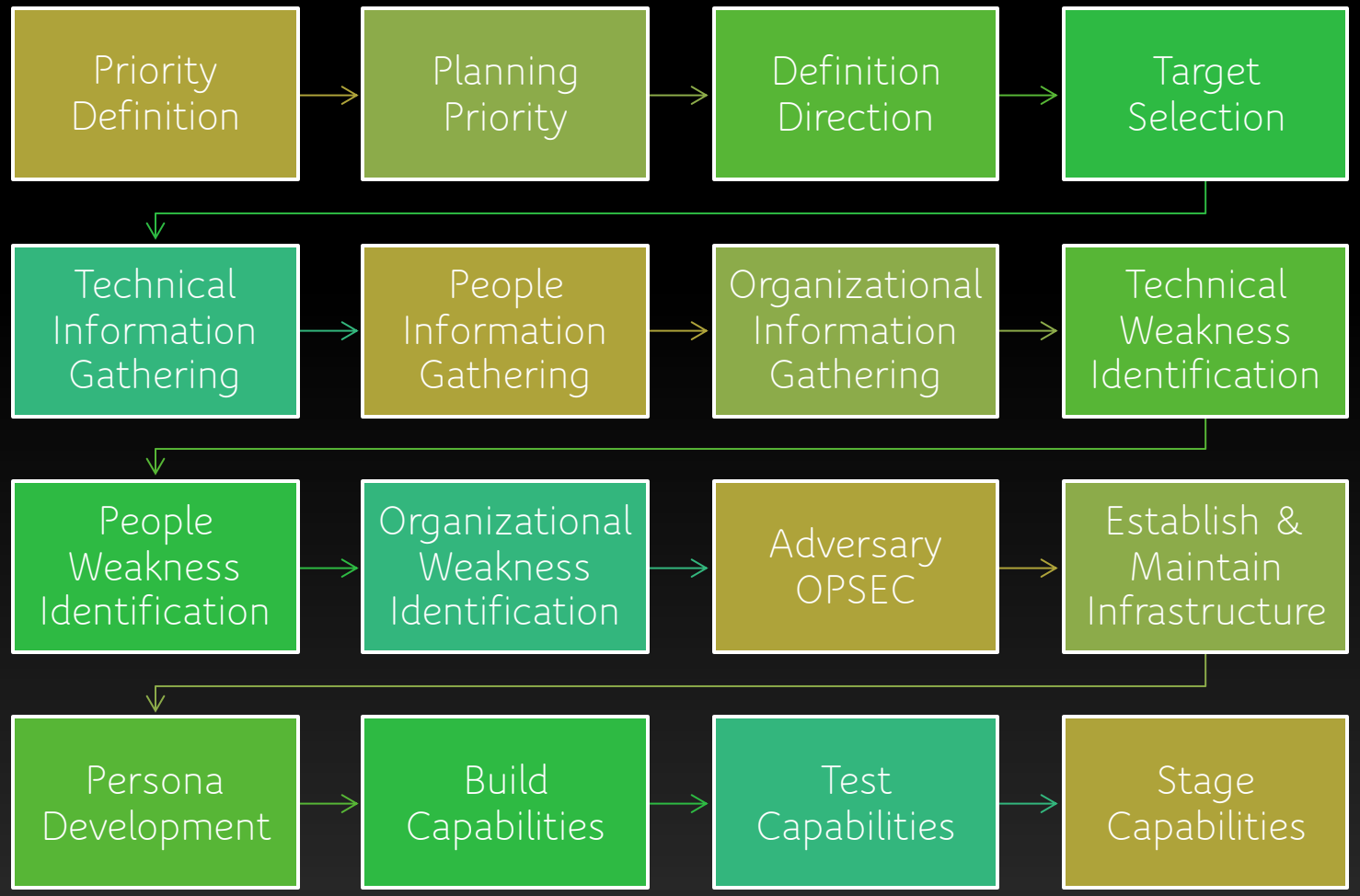
Hacker's laptop -Ed Muducdoc
Hoodie provider - Ken Jensen
Snort Pigs - John DePalma



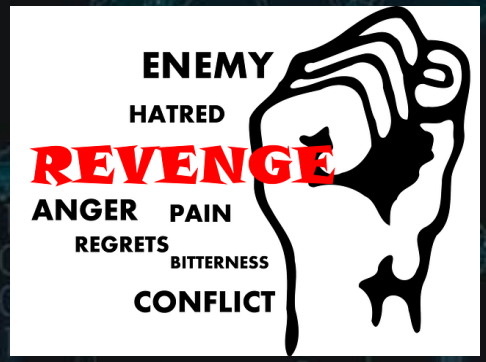
PRE-ATT&CK

...AND WHY YOU SHOULD CARE

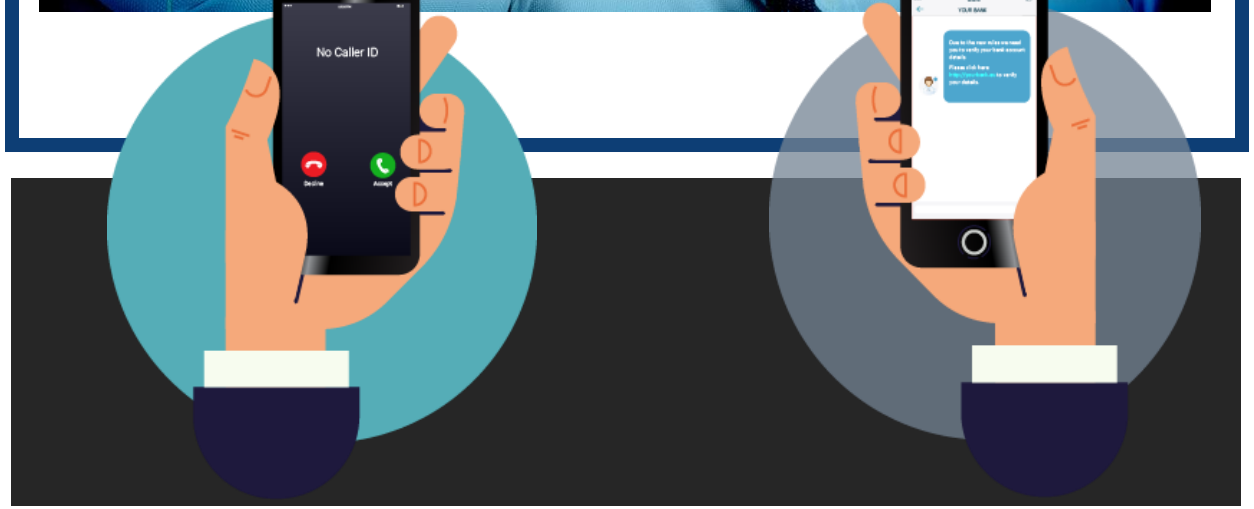
PRE-ATT&CK Categories



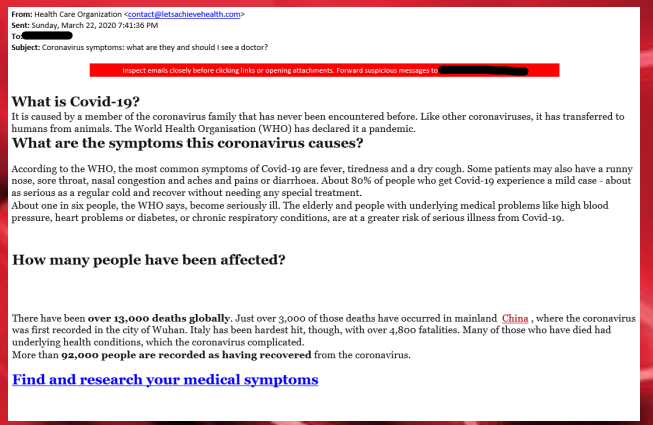
So why do hackers select specific targets?



Priority Definition Planning	Priority Definition Direction	Target Selection



Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification



From: Health Care Organization <contact@letsachievehealth.com>
Sent: Sunday, March 22, 2020 7:41:36 PM
To: [redacted]
Subject: Coronavirus symptoms: what are they and should I see a doctor?

Inspect emails closely before clicking links or opening attachments. Forward suspicious messages to [redacted]

What is Covid-19?
It is caused by a member of the coronavirus family that has never been encountered before. Like other coronaviruses, it has transferred to humans from animals. The World Health Organisation (WHO) has declared it a pandemic.

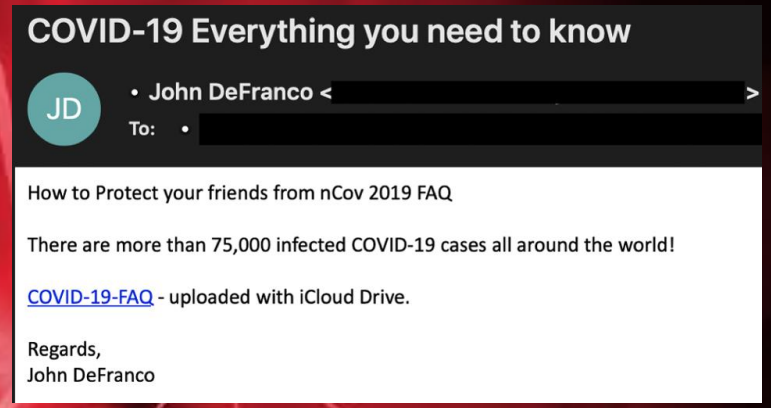
What are the symptoms this coronavirus causes?

According to the WHO, the most common symptoms of Covid-19 are fever, tiredness and a dry cough. Some patients may also have a runny nose, sore throat, nasal congestion and aches and pains or diarrhoea. About 80% of people who get Covid-19 experience a mild case - about as serious as a regular cold and recover without needing any special treatment.
About one in six people, the WHO says, become seriously ill. The elderly and people with underlying medical problems like high blood pressure, heart problems or diabetes, or chronic respiratory conditions, are at a greater risk of serious illness from Covid-19.

How many people have been affected?

There have been **over 13,000 deaths globally**. Just over 3,000 of those deaths have occurred in mainland China , where the coronavirus was first recorded in the city of Wuhan. Italy has been hardest hit, though, with over 4,800 fatalities. Many of those who have died had underlying health conditions, which the coronavirus complicated.
More than **92,000 people are recorded as having recovered** from the coronavirus.

Find and research your medical symptoms



COVID-19 Everything you need to know

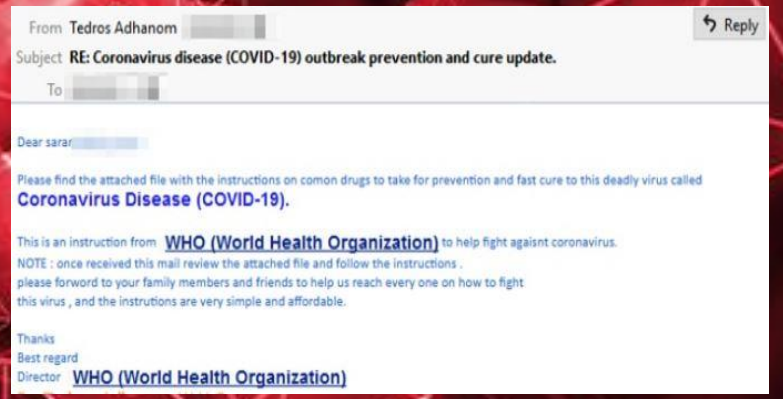
JD • John DeFranco <[redacted]>
To: • [redacted]

How to Protect your friends from nCov 2019 FAQ

There are more than 75,000 infected COVID-19 cases all around the world!

COVID-19-FAQ - uploaded with iCloud Drive.

Regards,
John DeFranco



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

Dear sarar[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 agaisnt coronavirus.
NOTE : once received this mail review the attached file and follow the instructions .
please forword to your family members and friends to help us reach every one on how to fight this virus , and the instrutions are very simple and affordable.

Thanks
Best regard
Director **WHO (World Health Organization)**

03/24/2020-03/25/2020

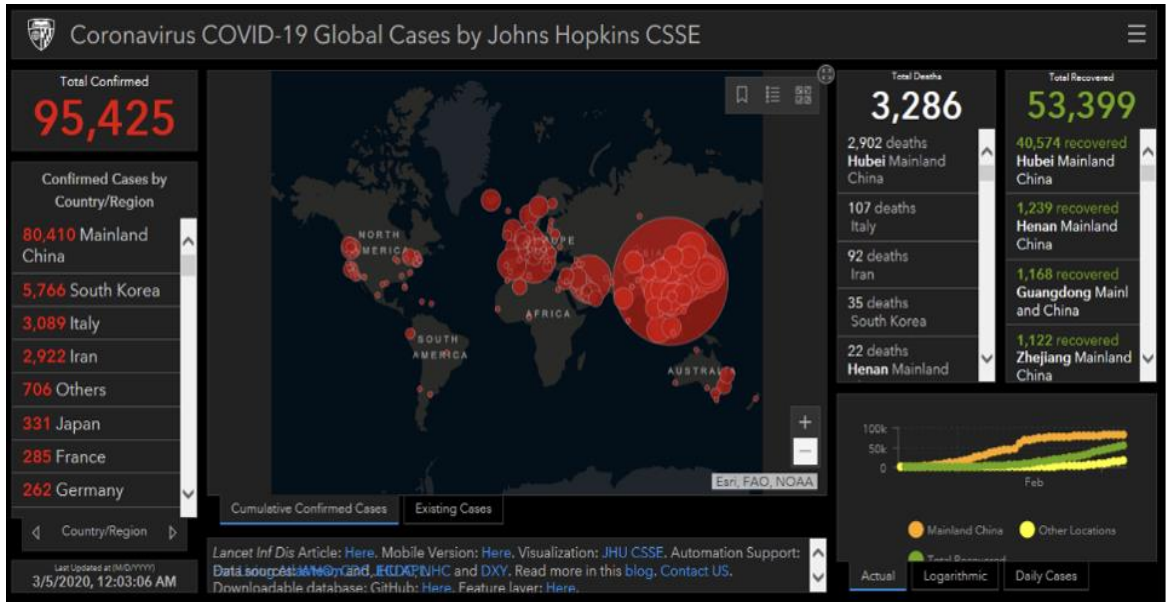
81,189 spam emails

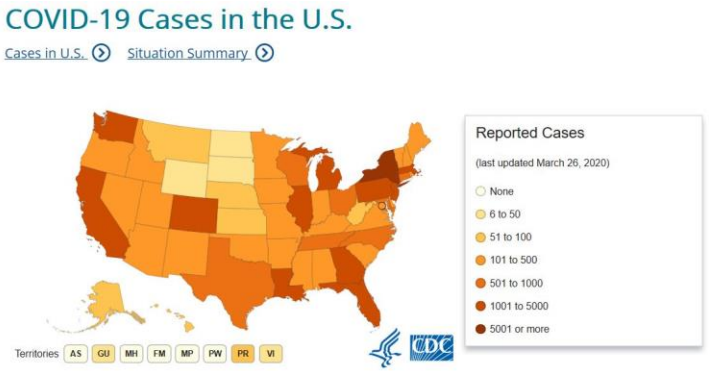
originated from **28,661** unique email domains

Phishing with COVID-19

Technical Information Gathering	People Information Gathering	Organizational Information Gathering	Technical Weakness Identification	People Weakness Identification	Organizational Weakness Identification

Real





Malicious

Registered domains including “coronavirus” in the last 7 days = **5762**

Registered domains including “covid” in the last 7 days = **6155**

Registered domains including “covid-19” in the last 7 days = 934

Registered domains including “covid19” in the last 7 days = **3098**

Adversary OPSEC	Establish & Maintain Infrastructure	Persona Development	Build Capabilities	Test Capabilities	Stage Capabilities

In closing... ULABRR

Use	Use a personal email account to sign up for personal accounts online (non-work accounts).
Limit	Limit the sharing of contact information on social media.
Accept	Only accept connection requests from known and trusted individuals.
Be	Be mindful of the images that are shared publically.
Review	Review social account security and privacy settings to restrict access to private information.
Research	Research your own public data so you know what's out there!


Questions?