BLACK KITE

Cybercriminals Prey on Healthcare Workers

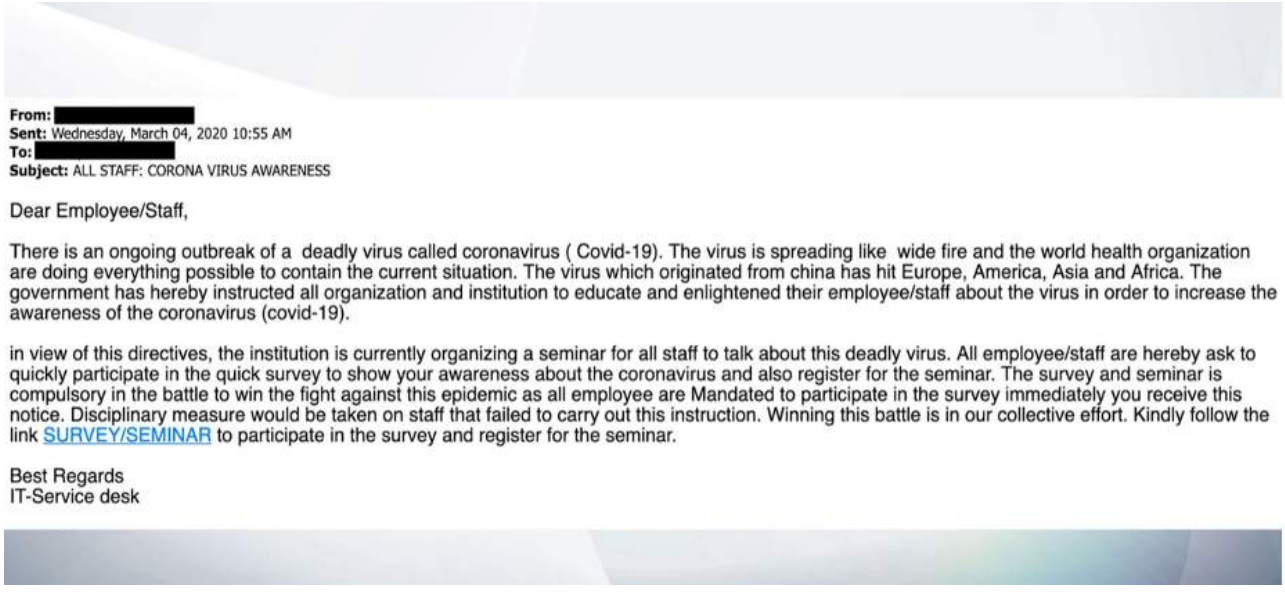
Healthcare employees on the frontlines working to end the COVID-19 global pandemic are now targets for cybercriminals.

Recent email scams sent to a number of healthcare organizations imitating internal IT teams are attempting to capitalize on the already vulnerable landscape.

Black Kite is diving deeper into the security posture of the hospitals combatting the COVID-19 pandemic in **New York.**

"The first thing we want to do is neutralize attacks before they happen. The second is to help any medical organization after they are attacked." - CTI League Founder, Ohad Zaidenberg

Targeted Attacks Towards Healthcare on the Rise



From: [redacted]
Sent: Wednesday, March 04, 2020 10:55 AM
To: [redacted]
Subject: ALL STAFF: CORONA VIRUS AWARENESS

Dear Employee/Staff,

There is an ongoing outbreak of a deadly virus called coronavirus (Covid-19). The virus is spreading like wide fire and the world health organization are doing everything possible to contain the current situation. The virus which originated from china has hit Europe, America, Asia and Africa. The government has hereby instructed all organization and institution to educate and enlightened their employee/staff about the virus in order to increase the awareness of the coronavirus (covid-19).

in view of this directives, the institution is currently organizing a seminar for all staff to talk about this deadly virus. All employee/staff are hereby ask to quickly participate in the quick survey to show your awareness about the coronavirus and also register for the seminar. The survey and seminar is compulsory in the battle to win the fight against this epidemic as all employee are Mandated to participate in the survey immediately you receive this notice. Disciplinary measure would be taken on staff that failed to carry out this instruction. Winning this battle is in our collective effort. Kindly follow the link SURVEY/SEMINAR to participate in the survey and register for the seminar.

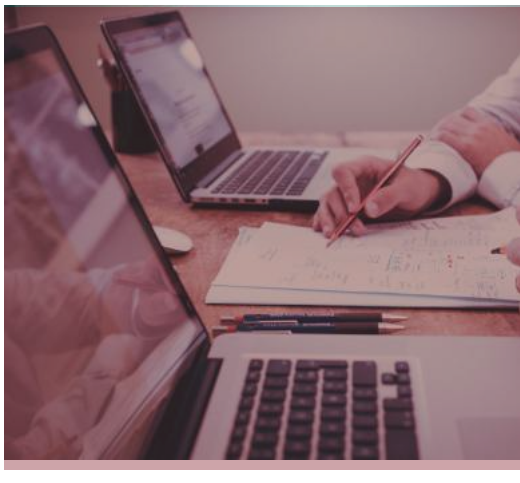
Best Regards
IT-Service desk

Fig-1: An email scam pretending to come from the IT-desk announces a COVID-19 seminar with the subject "ALL STAFF: CORONAVIRUS AWARENESS" [1]

Targeted attacks in the medical sector have dramatically increased since the outbreak of COVID-19, as the increased workload for healthcare employees has left the most more vulnerable. According to Black Kite's study, more than **1,600 credentials have been leaked from 20 top New York hospitals and their related domains, from January 2019 to the present**. Threat actors with various malicious motives craft phishing campaigns as an initial vector in their attacks. In some cases, they even deploy ransomware through inherent cybersecurity vulnerabilities in the hospital IT system.

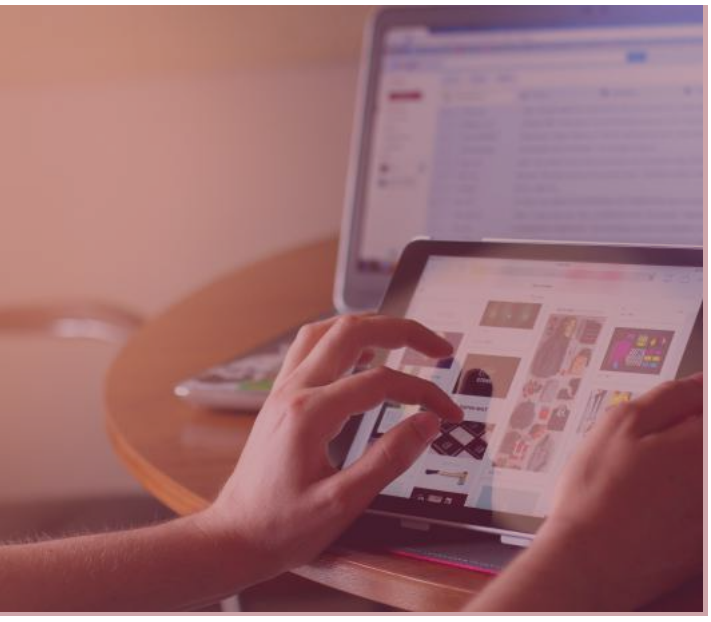
Our Research

The latest attacks against the healthcare sector motivated Black Kite researchers to take a closer look at the cybersecurity of COVID-19 treating hospitals. Our research is scoped to the 20 largest hospitals in New York City.

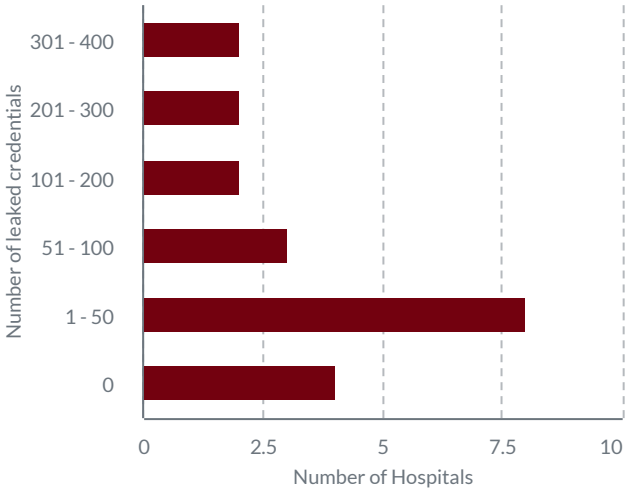


Black Kite's platform runs a passive non-intrusive comprehensive scan for each hospital. Based on the hospital website domain name, researchers were able to derive a comprehensive digital footprint including every related healthcare domain, subdomain, IP address, service, email, etc. Building upon the assets discovered in the digital footprint, common security issues were identified and a cybersecurity score was calculated for each hospital.

Leaked Credentials in Hospital-Related Domains



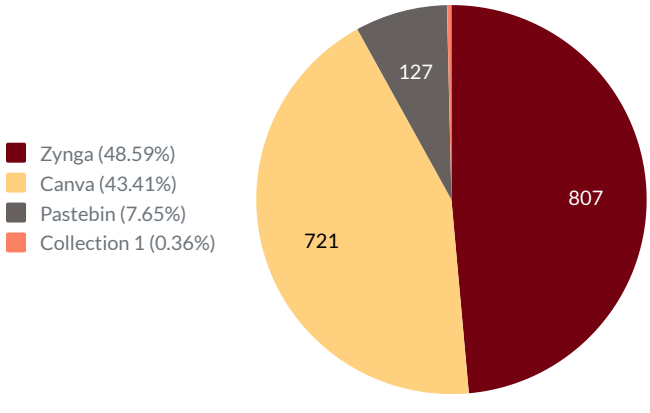
Leveraging breached credentials is often the initial vector of a phishing email campaign. Phishing attacks present a scheme to trick consumers into thinking they are from legitimate sources, such as the IT department or a peer organization they already trust.



As detailed, **1661 credentials have been leaked from the 20 New York hospitals and their healthcare-related domains, from January 2019 to the present**. 2019 was a year of prominent credential breaches, such as Zynga [2] and Canva [3], as well as a mass exposure of credential collections on hacking forums and platforms as in the case of Collection #1 [4].

Sources that Adversaries Utilize

The name of a leaked credential is usually mentioned along with the organization where the data breach originated. The two sources in our research with the most leaked credentials from January 2019 - Present are Zynga (a gaming company) [2] and Canva (graphic design website) [3], common platforms in which subscribers use corporate email addresses and credentials.



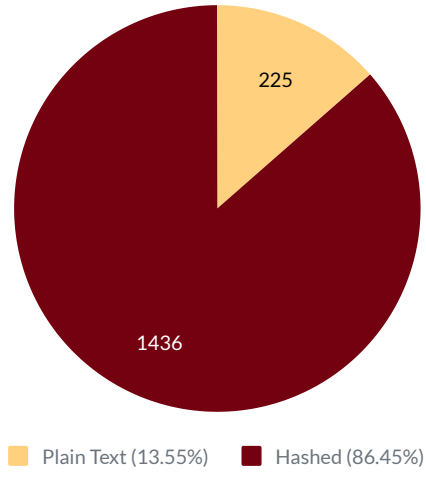
Black Kite identified the email accounts of NYC healthcare workers, **which were used on Zynga and Canva platforms, and have been leaked as part of 2019 breaches.**

The hackers usually sell the credentials on the dark web and do not mind sharing the information with each other.

Why do Previously Compromised Accounts Matter?

Employees often register themselves on the internet under their corporate email addresses, sometimes using the same password they use on corporate accounts. It's called "credential stuffing" and it's common for hackers to leverage these sources (not the company itself) in crafting their attacks. Hackers use the employee information to infiltrate a company's system by using previously breached username/password pairs.

Leaked credentials serve as either a potential target list for their phishing campaigns or a way to access the organization's resources. When plain (unencrypted) passwords are obtained, a hacker might impersonate regular hospital staff to gain access to these internal resources.



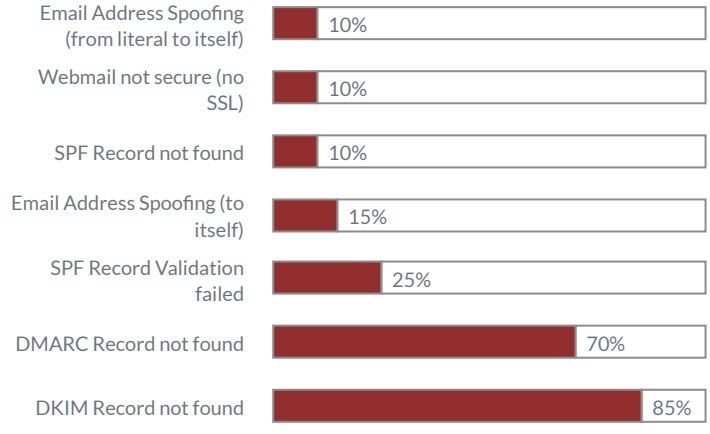
***How hackers leverage these vulnerabilities:** Hackers might leverage these vulnerabilities when crafting spoofed emails to hospital staff, pretending to be from the WHO or the CDC. In the message body, some announce so-called COVID-19 seminars and provide links to malicious sites for registration.*

Simple Steps to Prevent "Credential Stuffing" Attacks

- Keep an eye on credential breaches
- Warn employees against password reuse across different platforms
- Enable two-factor authentication where possible
- Disable macros on Microsoft documents
- Warn employees against clicking links in email bodies

Email Security of the COVID-19 Hospitals

Email configuration is of paramount importance, especially when another entity attempts to send an email on behalf of an organization. Here, we discovered about 85% of the NY Hospitals lack DKIM and 70% of them lack DMARC related controls in their email configurations. DKIM and DMARC records are used together to protect a domain name from being used in phishing and scam emails.



The purpose of an SPF record is to prevent spammers from sending messages forged from addresses of a domain, and in our case, a hospital domain or a trusted party. 25% of the hospitals lack SPF validation and 10% have no SPF record at all.

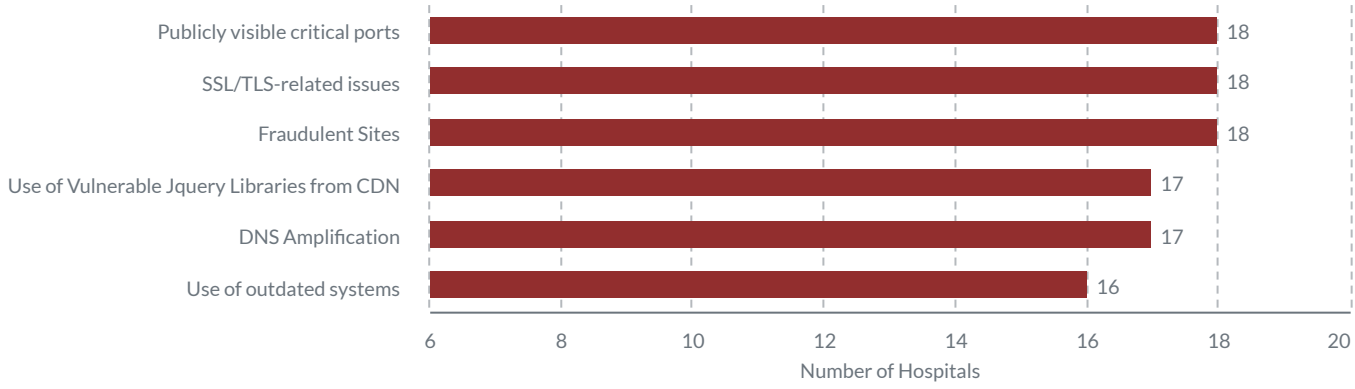
15% of the hospitals on our list are vulnerable to a process called "email address spoofing to itself" which is pretty simple and widespread. In most cases, it doesn't mean the email account has been hacked; instead, someone is able to imitate the hospital in the email address.

Simple Steps to Prevent "Email Spoofing" Attacks

- Ensure DMARC and SPF are in place and set up correctly
- Create DKIM information for every domain that is used to send emails
- Enhance spam filters
- Read message headers, and cross-check IP addresses
- Disable SMTP relay for your domain from the internet
- If you manage your own email, audit it to see how it responds to SPF and DMARC records

Other Common Security Issues - New York City Hospitals

Apart from email configurations and leaked credentials, some common security findings among hospitals relate to Publicly Visible Critical Ports, SSL/TLS-related issues and fraudulent sites.



Publicly Visible Critical Ports

Remote administration is becoming increasingly common and is often used when it is difficult or impractical to be physically near a system in order to use it. Black Kite has identified publicly visible critical ports for 90% of the hospitals' IT systems, regarding some remote administration tools such as RDP, VNC, SSH, Telnet, SNMP.

Simple Steps to Manage Critical Ports

- Keep an eye on credential breaches
- Warn employees against password reuse across different platforms
- Enable two-factor authentication where possible
- Disable macros on Microsoft documents
- Warn employees against clicking links in email bodies

Fraudulent Sites

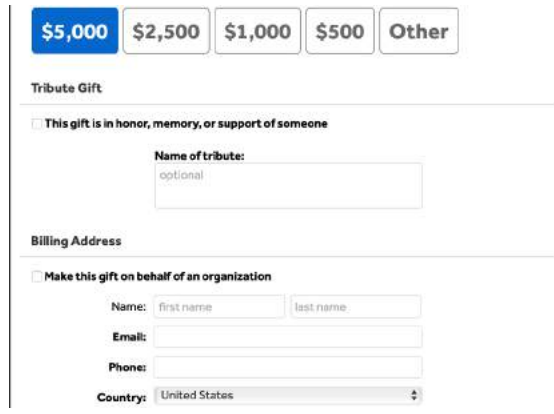
Fraudulent domains and subdomains are look-a-like domains mimicking a company's original site. In the healthcare sector, fraudulent sites could be used as part of a phishing campaign where the cybercriminals could trick the hospital staff while giving away sensitive information (including PHI). With a 90% occurrence ratio, fraudulent domains are one of the most dangerous attack vectors.

Simple Steps to to Prevent Staff from Entering Fraudulent Sites

- Continuously monitor for look-a-like domains
- Continuously check for blacklisted sites related to COVID-19

SSL/TLS-related Issues

Findings related to SSL/TLS issues are perhaps the most common issues we came across during our research. The strength of SSL/TLS determines the resiliency of communication to confidentiality attacks.
Some hospitals are also accepting donations through website payments; another factor in why SSL/TLS is important for the confidentiality of the traffic directed to and from the hospital websites.



Simple Steps to Prevent "Confidentiality" Attacks

- Check for SSL certificates and expiration dates (Renewal becomes available 30 days before its expiration)
- Stop using RC4,DES-like weak algorithms
- Disable support for export cipher suites
- Disable SSLv3
- Use TLS 1.2 and later versions

Recent Statistics on HealthCare Attacks Align with Black Kite's Findings

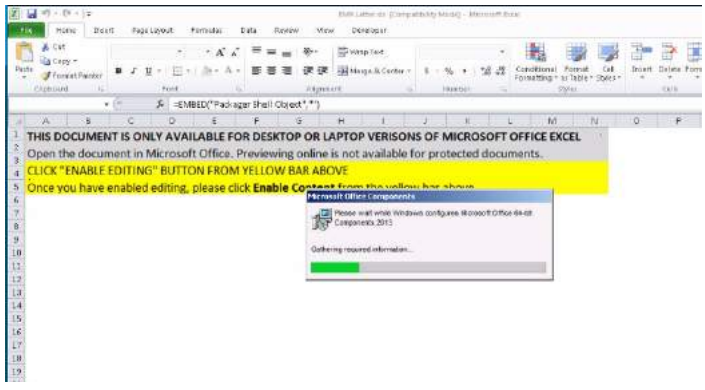


Fig-2: A recently discovered COVID-19 bait attributed to TA505 using a Microsoft Excel document. It requests the user to enable macros [6]

A newly established group of cybersecurity professionals called "COVID-19 Cyber Threat Coalition" concentrate their efforts on coronavirus related cyber-attacks. According to their initial findings, the most common coronavirus threats are [5] credential phishing (33%), scams (30%), and malicious documents as attachments (18%). Several of these malicious files were identified in the form of Microsoft Word Document files and 7-zip compressed files. Although the details are not fully known at this stage, the threats are assumed to have created an initial intrusion to enable further system exploitation, persistence, and exfiltration.

Over the past week, security researchers observed a campaign from TA505, using coronavirus lure as part of a downloader campaign [7]. While the group previously targeted retail and finance, their new targets became U.S. healthcare, manufacturing, and pharmaceutical industries.

It is also noted that a number of ransomware groups are hunting for exposed VPN servers, which hospitals frequently use to support remote-working administration staff.

Black Kite's findings on the cybersecurity of New York City hospitals also align with these recent attack vectors against healthcare. Vulnerabilities in Email Configurations, Leaked Credentials, and Publicly Visible Critical Ports, which are among the most common security findings of Black Kite, are merely invitations for hackers whose motive is to turn this crisis into an opportunity.

What Are the Specific Motives of Cybercriminals?

Cybercriminals execute attacks towards healthcare workers for different reasons. Here is a shortlist of those motivations:

- To exfiltrate information, any treatment methodology, or novel research regarding COVID-19, including testing of existing drugs or vaccination studies
- To infiltrate IT systems of the hospitals and exfiltrate as many PHI (protected health information) as possible
- To exfiltrate personal information other than PHI to sell on the dark web
- Immediate monetization through ransomware attacks

Takeaways

As “ruthless” as it may seem under these circumstances, it is no surprise that cybercriminals are taking advantage of a worldwide crisis and preying on the most critical element to human survival at the time.

This research reveals healthcare staff is only a click away from giving a hacker access to critical resources or allowing cybercriminals to install ransomware that could shut down the systems entirely. Despite these unfortunate conditions, simple steps can be taken to prevent further attacks.

5 Takeaways

- Educate staff; awareness is the first line of defense
- Check continuously for leaked credentials, warn staff against password reuse, enable MFA where possible
- Invest in strong Email Security. Make sure SPF, DMARC, and DKIM controls are in place and properly set up. Enable SSL on webmail.
- Beware of cleartext transmission on web site; disable any vulnerable versions of SSL/TLS.
- Manage critical ports externally and internally; disable unnecessary services and ports

References

[1] https://news.sky.com/story/coronavirus-cybercriminals-target-healthcare-workers-with-email-scam-11956617
[2] https://thehackernews.com/2019/09/zynga-game-hacking.html
[3] https://www.cisomag.com/nearly-140-million-user-data-leaked-in-canva-hack/
[4] https://www.wired.com/story/collection-leak-usernames-passwords-billions/
[5] https://www.computerweekly.com/news/252481298/Coronavirus-threats-ramp-up-as-more-hospitals-come-under-attack
[6] https://otx.alienvault.com/pulse/5ea06a3ce9030e041b86dbb5
[7] https://blog.cyberint.com/covid-19-ongoing-cyber-updates

How To Rate Your Cyber Ecosystems

Black Kite's platform aims to provide full visibility into a cyber ecosystem. The platform enables enterprises to continuously assess third-party risks, assigns a letter grade to each vendor, correlates findings with industry standards to inform compliance requirements, and determines the probable financial impact if a third-party experiences a breach.

Learn more at www.blackkitetech.com

The Black Kite (formerly known as NormShield) Platform's intuitive interface compiles reports and communicates risks in qualitative, quantitative, and easy-to-understand business terms for executives. The interface also allows IT-security teams to drill down to the technical details in each risk category.
With the alerting mechanism, the users of the platform become aware of the security vulnerabilities within a cyber ecosystem promptly and can take immediate action.