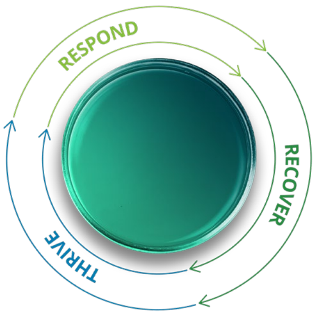
Deloitte.

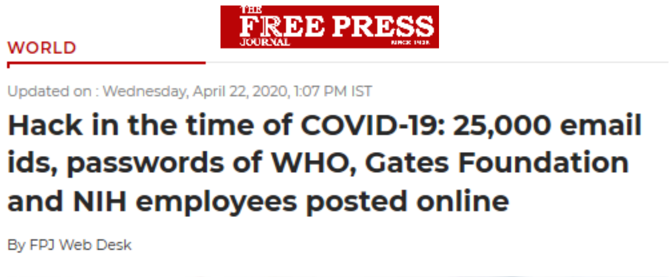
Issue 4| April 29, 2020



The rise of cyber threats in March and April amid COVID-19

A weekly high-level brief that focuses on some of the most current cyber threats and trends as identified by Deloitte Cyber Threat Intelligence (CTI), with near-term recommendations on managing cyber risks to respond, recover and thrive through the COVID-19 global pandemic.

Organizations invest substantial resources in addressing attacks


THE FREE PRESS JOURNAL

WORLD

Updated on : Wednesday, April 22, 2020, 1:07 PM IST

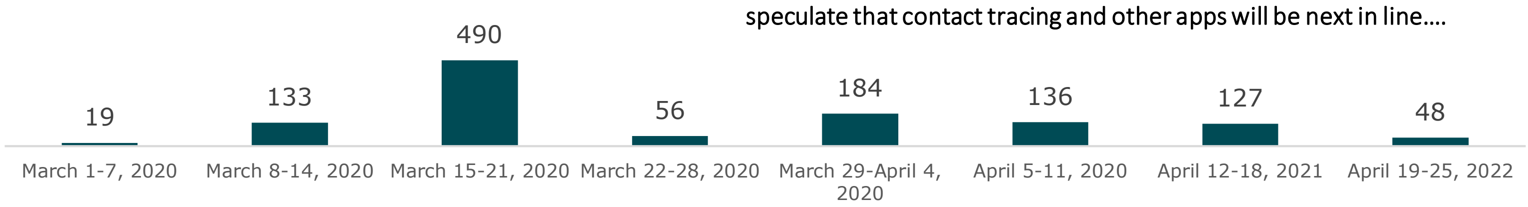
Hack in the time of COVID-19: 25,000 email ids, passwords of WHO, Gates Foundation and NIH employees posted online

By FPJ Web Desk

In the past 30 days, there has been an increase in malware and phishing campaigns related to COVID-19, including targeted attacks on known organizations, such as the WHO and Gates Foundation. While the overall volume of threats isn't increasing, threat actors have increasingly shifted to COVID-19 lures to capitalize on fears around the pandemic. This is evident in the increase of malware samples incorporating COVID-19 themes collected by Deloitte CTI. The lures focused on maps, then personal protective equipment followed by Government incentives.

For employees working remotely, a false sense of security could be an open door of opportunity for cyber adversaries to enter. Tomorrow, we could speculate that contact tracing and other apps will be next in line….

The rise of COVID-19-themed-malware in March and April 2020
(Number of COVID-19 related malware samples)



Malware attacks surge on mobile devices amid COVID-19

From April 15 to April 21, Deloitte CTI observed 14 COVID-19 related malspam campaigns using COVID-19 lures. In addition, Deloitte CTI observed iOS and Android users targeted with malicious apps using COVID-19 lures to deliver spyware. **This week we highlight the rising threats targeting remote workforce and mobile users** (and originally identified in our detailed threat report dated April 18 – April 24).

Spyware threats from malicious mobile app 'Coronavirus updates'

Impact reach: All| Geographies: Global

A malicious app titled "Coronavirus Updates" delivered spyware to unsuspecting users

On April 17, 2020 Deloitte CTI observed researchers at TrendMicro reporting about a malicious app masquerading as "Coronavirus Updates" application delivering a spyware dubbed Project Spy, targeting Android and iOS users. India, Pakistan, Afghanistan, Bangladesh, Iran, Saudi Arabia, Austria, Romania, Grenada, and Russia have observed instances where the app has been downloaded. Spyware is software that enables a user to obtain covert information about another's computer or mobile device activities by transmitting data stealthily from their device.

Threat actors exploit remote workforce by spoofing popular services such as DocuSign and Adobe

Impact reach: All| Geographies: Global

Fake invoice email "Outstanding Invoice" COVID-19 lures to conduct Business Email Compromise (BEC) attacks:

With many organizations around the world opting for a remote workforce during the COVID-19 pandemic, services such as DocuSign are being widely used for authenticating access to sensitive documents. Threat actors are exploiting the current situation by spoofing popular services such as DocuSign, Adobe and other widely used tools for credential phishing attacks. On April 16, 2020, Deloitte CTI observed security vendor MailGuard's report on a phishing campaign spoofing DocuSign to harvest Adobe Cloud credentials. One of the spam emails observed by MailGuard researchers was delivered with the subject line "Outstanding Invoice."

Organizational oversight of cyber risk management around COVID-19 malware and phishing exploits

Deloitte recommends the following for guarding against cyber attacks:

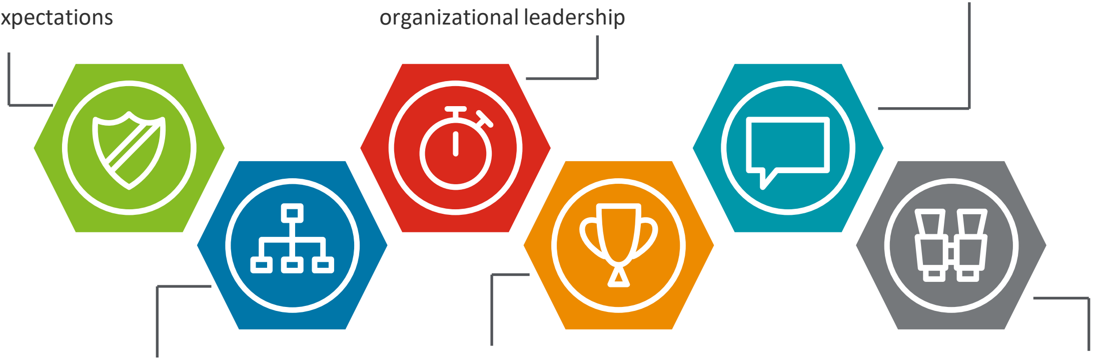
PROACTIVELY PRE-PLAN	**Refreshed playbook?** • Review Cyber incident response playbooks and adapt necessary activities or steps for a remote working model. Anticipate COVID-19 attack scenarios.	**How to engage the right stakeholders?** • Identify critical technical, business, and strategic stakeholders to be engaged remotely during an incident. Ensure primary and secondary contact details are updated and readily available. • Educate them on the potential modus operandi and COVID-19 lures.
DILIGENTLY MONITOR	**How to guide remote collaboration securely?** • Guide and monitor how teams are collaborating remotely, ensure employees are notified and aware of the tools and their authorized processes.	**How to monitor and implement change in operating models?** • Optimize the ability to perform remote investigation and analysis activities within the context of an incident response. • Perform proactive threat monitoring and hunting for COVID-19 themed phishing attacks. • Make use of the most recently updated monitoring dashboard designed for COVID-19.
REFRESH SECURITY CONTROLS	**How to authenticate and update security controls?** • Enforce the use of Multi-Factor Authentication for remote access. technologies (e.g. VPN) and email services (e.g. Office 365). • Accelerate the deployment for all internet facing websites.	**How to update security controls?** • Improve logging details and retention periods for data sources that would need to be leveraged during a potential investigation. • Review security controls for tools and technologies used for remote access at the organization, including but not limited to, Office 365 (email) and VPN services.

Recover and Thrive: Top of mind for preparing for a cyber incident during social distancing

In preparing for the inevitable cyber incident involves more than preparing to react— to merely neutralize a one-off attack. It involves the ability to respond effectively and repeatedly—to plan proactively, to defend your critical systems and data assets vigorously, to get ahead of evolving threats, and to recover thoroughly when attacks do occur. During this time of COVID-19, cyberattacks can increasingly take a toll on corporate balance sheets when they can least afford it. A strong cyber incident response (CIR) capability adapted to social distancing restrictions becomes essential for businesses. Cyber adversaries are looking for opportunities and will exploit opportunities presented by the COVID-19 phases.

Just as organizations and governments quickly moved to shift strategy and procedures when the coronavirus locked down their cities and countries, so should they review and adjust incident response playbooks, protocols and security controls to keep pace with increasing cyber or they may face vulnerabilities that can leave them exposed for months, or years.

In order to prepare, organizations can consider six key areas:



Defensibility advisory

Virtually review and ensure business continuity programs, pandemic scenarios and management practices are defensible and in alignment with applicable cyber security and privacy requirements, fiduciary duties and industry expectations

Cyber, crisis and pandemic incident response

Ensure crisis management programs are updated to effectively develop and manage remote cyber, crisis and pandemic response. As a first step, establish remote crisis management offices and supporting organizational leadership

Remote training and assessments

Educate and engage remote users with training and awareness of evolving organizational processes and the increased cyber risk associated with COVID-19

Third Party risk and supply chain management

Understand critical vendors, their cyber risk and contingency plans and include them into your contingency strategy

Threat management and situational awareness

Remotely assess and deploy technology to improve threat visibility and protection across your infrastructure amid a remote workforce

Threat Intelligence

Monitor the dark web to identify organizational exposures and historical, active and planned attacks against your organization. Perform sentiment analysis to improve COVID-19 staff, supplier and customer communications

We're by your side to help you through COVID-19

Relevant Deloitte reads:

- **Podcast:** Resilient podcast: How businesses can confront the COVID-19 crisis
- **Article:** Management checklist for COVID-19 crisis
- **Article:** Crisis management for a resilient enterprise

Deloitte Cyber helps organizations perform better, solving complex problems so they can build confident futures. Smarter, faster, more connected futures—for business, for people, and for the planet. As a recognized leader in cybersecurity consulting, Deloitte Cyber can help better align cyber risk strategy and investments with strategic business priorities, improve threat awareness and visibility, and strengthen our clients' ability to thrive in the face of cyber incidents. Deloitte Cyber uses human insight, technological innovation and comprehensive cyber solutions, to manage cyber everywhere, so society can go anywhere.

Emily Mossburg
Global Cyber Leader
+1 571 766 7048
emossburg@deloitte.com

Amir Belkhelladi
Canada
+1 514 3937035
abelkhelladi@deloitte.ca

Simon Owen
North South Europe
+44 20 7303 5133
sxowen@deloitte.co.uk

Deborah Golden
US
+1 571 882 5106
debgolden@deloitte.com

James Nunn-Price
Asia Pacific
+61 293227971
jamesnunnprice@deloitte.com.au

Peter Wirnsperger
Central Europe
+49 40320804675
pwirnsperger@Deloitte.de

Nicola Esposito
Spain
+34 918232431
niesposito@deloitte.es

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber