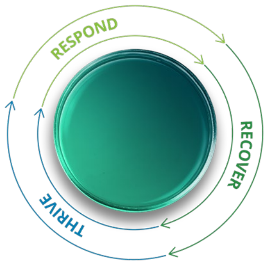
Deloitte.

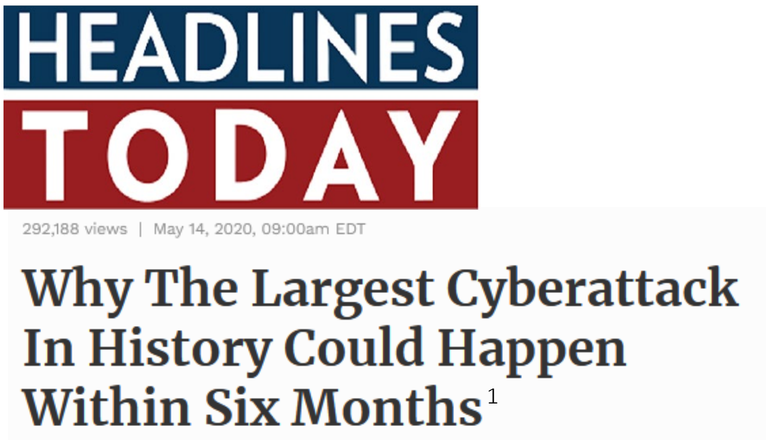
Issue 8 | June 3, 2020

COVID-19 Global Cyber risks: Is a major cyberattack looming?

This is the final issue in a series of high-level briefs that focus 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.



COVID-19 lays the groundwork for a destructive cyberattack. Is your organization prepared?


HEADLINES TODAY

292,188 views | May 14, 2020, 09:00am EDT

Why The Largest Cyberattack In History Could Happen Within Six Months[1]

Over the past few weeks, Deloitte CTI has traced a wide range of cyberattacks related directly to COVID-19. As consistently reported, we assess with high confidence that the pandemic has not resulted in any observable changes to threat actor tactics, techniques, and procedures. What has changed, however, is the level of risk to which organizations are now exposed. The widespread scramble to accommodate remote work has increased the attack surface to unprecedented proportions—**heightening the likelihood of a large-scale cyber incident**. This is because it is within times of chaos and change that the adversary looks to take advantage. Organizations that do not strengthen their cyber maturity now may discover themselves unprepared to effectively protect, detect, and respond to threats specifically targeting their organizations or inadvertently targeting their organization through a third or fourth party.

[1] Source: https://www.forbes.com/sites/stephenmcbride1/2020/05/14/why-the-largest-cyberattack-in-history-will-happen-within-six-months/#31da7160577c

COVID specific cyber attacks continue to increase

Fake Contact Tracing app delivers ransomware

Impact reach: All | Geographies: Europe

On May 27, 2020, Deloitte CTI observed the following incident of threat actors leveraging malicious COVID-19 contact tracing app to deliver ransomware that targeted the life sciences and healthcare industry and academic sector. Security vendor Dottor Marc reporting on a new ransomware dubbed 'Unicorn' that targeted pharmacies, doctors, medical businesses, and universities across Italy. Threat actors leveraged social engineering to lure users into downloading a malicious Coronavirus (COVID-19) contact tracing application. Once the encryption process is completed, an Italian ransom note asking for 300 euros gets displayed onto the infected machine.

Mobile malware COVID threats on the rise

Impact reach: All | Geographies: Global

Mobile malware continuously used in COVID-19 lures to target victims as employees continue to work from home amid the COVID-19 pandemic. Researchers identified four different versions of an Android malware leveraging a Coronavirus (COVID-19) lure to access information such as the contact list and also enable reading SMS data from a victim(s) device. Users should continuously monitor their device and accounts, particularly accounts that are accessed via Android device applications, and promptly report any unrecognized activity or unusual application behavior. Ensure that when Installing mobile apps, plug-ins, and codecs they are from trusted sources such as Google Play Store/Apple store and – if necessary – company portals. Deploy mobile device management (MDM), or enterprise mobility management (EMM) software solutions, to increase security on enterprise mobile devices, including smartphones and tablets.

Phishing attacks target business intelligence

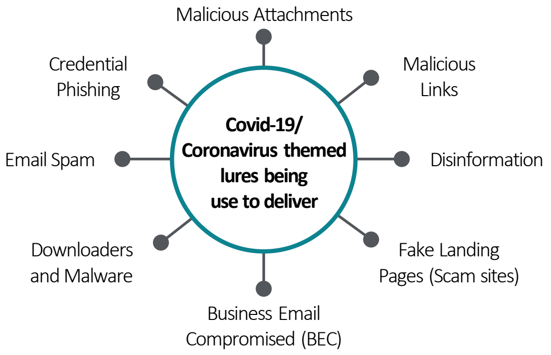
Impact reach: All | Geographies: Europe

On May 27, 2020, Deloitte CTI observed a European-based threat actor named Vendetta targeting individuals in operations to steal business secrets with phishing emails that leveraged COVID-19 themed police investigation letters and detection notices. Embedded macros in Microsoft Office documents should be blocked if macros are not used in your environment, or only allow signed macros that are validated to execute. Recipients of suspicious emails are encouraged to verify the ostensible sender via alternate communication methods, via secure channels and not use the contact information provided in a message.

Business email compromise (BEC) target relief funds

Impact reach: All| Geographies: United States

Deloitte CTI observed threat actors conducting Business Email Compromise (BEC) attacks leveraging COVID-19 lures that specifically related to COVID-19 relied funds provided by the CARES Act as well as the U.S. unemployment system. One example, a Nigerian threat actor group, Scattered Canary, used a lure related to the Coronavirus (COVID-19) pandemic using various Internal Revenue Service (IRS), and state unemployment websites to file fraudulent claims by abusing the Gmail "dot accounts" feature, to create hundreds of fake accounts. Warn employees against clicking on attachments or links embedded in email messages with subject lines purporting to contain information related to COVID-19 or Coronavirus


Covid-19/ Coronavirus themed lures being use to deliver

Malicious Attachments

Malicious Links

Disinformation

Fake Landing Pages (Scam sites)

Business Email Compromised (BEC)

Downloaders and Malware

Email Spam

Credential Phishing

A reminder on perpetual resilience

- Looked at in isolation, the COVID-19-related threat incidents are worrying but not unexpected. Looked at in the aggregate, however, and we start seeing a pattern of attack targeting a reeling society's weakest links—threatening the cyber integrity of organizations in every country and every sector of the economy.
- Businesses still shudder to remember the NotPetya attack of 2017 which began in the Ukraine but spread beyond its intended target in seconds, ultimately affecting organizations from Russia and Denmark to the UK and the US.
- Cyberattacks can compromise countless devices and spread across global networks at a breathtaking pace, rendering servers and endpoints inoperable.
- If enterprise systems were already at risk before the outbreak of COVID-19, just imagine the threat organizations face now that a solid percentage of the world's population is connecting to corporate networks and sharing confidential information over weak, unsecured, and unstable systems.
- **In light of these realities, even organizations with fundamentally sound cyber risk management programs should reconsider and look to improve cyber readiness, response, and recovery as it could require a new approach to support post-COVID operations and organization.**

Recover and thrive: To work from anywhere, you need cyber everywhere

As the attack surface exponentially grows in the era of COVID-19, threat actors are increasingly targeting an organization's weakest links—from its operational systems to its backup servers—often in highly sophisticated ways. This has opened the door to enterprise-wide destructive cyberattacks. To mitigate these risks, organizations must adopt new educational tools, technical solutions, and business strategies. Here are a few places to start:

Review and revise incident response plan. Create a Synchronized Cyber Incident Response Plan to define how cyber incident response processes would interlace with COVID-19 crisis teams.

Enhance access management. An effective identity and access management (IAM) security framework should improve your stance across five key domains: identification, authentication, authorization, access governance, and accountability. As the shift to remote work continues, organizations will also need to adopt a security-first cloud strategy to strengthen privilege access management.

Improve cyber hygiene. Poor cyber hygiene has a direct impact on enterprise security. To up your game, it's critical to patch all software, ensure all systems are properly configured, fully deploy all security tools, and adopt effective asset discovery and tracking processes.

Segment and zone. Flat networks allow adversaries to easily maneuver across your various systems. To limit the impact of these attacks, look at improving your segmentation and zoning to prevent an attacker's lateral movement into your enterprise.

Strengthen IT asset management. The rush to remote work has seen organizations adopt a chaotic array of new—and likely untested—applications, operating systems, and devices. To limit your attack surface, you must take steps to audit your dispersed assets and bring them under central supervision – this may now need to include personal devices that employees are now using for work output that should have some level of security controls. You can't protect what you don't know about

Streamline backups. Traditional recovery tends to result in aggressive data redundancy for critical systems. When malware is introduced, this backup environment can accelerate the spread of an attack. To address this issue, look at setting up a storage vault to house backup data and other critical materials and a streamlined data recovery zone that allows you to reconstruct your environments from the vault.

Questions Organizational Executives can ask to foster effective conversations between business leaders and Chief Information Security Officers (CISOs):

- Have roles and responsibilities related to cybersecurity been clearly defined and communicated at every level of the organization up to the CEO and Board?
- Do business leaders understand what the organizations most valuable assets are and the level of cyber risk they are accepting?
- Are technology solutions designed, integrated and operated with security and privacy in mind?
- Does the business incentivize the adoption of secure-by-design-and default practices on the businesses and products in which it invests?
- Are third-party, even fourth-party cyber risks factored into vendor contracts and remediation processes?

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

Relevant Deloitte Reads:

- Update crisis playbook to reflect COVID-19 lessons learned
- Reopening the workplace: The resilient leader's guide
- Deloitte Insights: Establishing the road to a global consumer recovery
- COVID-19: Privacy and security in the next normal

Deloitte Cyber drives progress in a dynamic, connected world, solving complex problems to build confident futures. Using human insight, technological innovation, and comprehensive cyber solutions, we manage cyber everywhere, so society – and your organization – can thrive 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

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.