Deloitte.

Global Cyber COVID-19 weekly executive cyber briefing

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.

Issue 3| May 2020

Data protection and privacy in the age of COVID-19

This week we highlight a **few of the issues and related cyber threats** (and originally identified in our detailed threat report dated April 11 – April 16) impacting consumers, non-profit organizations as well as healthcare organizations globally. Threat actors are exploiting fear around COVID-19 to target users with information-stealing malware, with the aim of obtaining Personally Identifiable Information (PII), financial information, or credentials to facilitate further access. The ongoing COVID-19 pandemic has amplified risk factors by increasing the volume of attacks that target user data and impact their privacy. In addition, the Research from Deloitte Cyber Threat Intelligence (CTI) indicates COVID-19 pandemic responses by healthcare providers and research institutes are hampered by cyber adversaries who are launching cyber-attacks around the globe targeted at critical health care infrastructure.

Intellectual property theft

Impact reach: Life sciences | Geographies: Canada, Japan

Agent Tesla Malware used on medical research facility to identify future IP theft targets

From March to April 2020, Deloitte CTI observed a COVID-19 themed phishing campaign targeting medical research facilities located in Japan and Canada using information stealing malware. In this campaign, phishing emails were delivered to targets using subject lines such as "COVID-19 Supplier Notice" or a "Corporate advisory" and included malicious ZIP files "COVID-19 Supplier Notice.zip" as an attachment. When opened, the malware was loaded on to the victims' machines.

The Agent Tesla malware can perform screen capturing, password stealing, webcam recording and downloading additional malware. The threat actors almost certainly targeted these organizations to gain access to their networks to conduct reconnaissance and facilitate future IP theft.

Suggested top actions:

1. Ensure proper deployment and update of anti-phishing, anti-virus, and web-filtering security controls.
2. Be on alert as spam messages may also look legitimate or purport to be from official sources and may use subject line themes associated with COVID-19 or Coronavirus.
3. 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.

Theft of Consumer Personal Information

Impact reach: Consumer | Geographies: Global

Fraudsters pose as charities and organizations to process fake donation payments and target personal login credentials in various campaigns

Deloitte CTI assesses with high confidence that COVID-19 related themes are increasingly and effectively used to facilitate the theft of Personally Identifiable Information (PII) or financial information. Turn-key phishing kits and Phishing-as-a-Service (PhaaS) products are increasing the number of threats as there is no longer a technical barrier to becoming a threat actor – only a financial one. Between February and April 2020:

- A series of phishing kits were distributed that imitate legitimate websites / organizations to enable fraudulent transactions. Users are tricked into providing sensitive information such as login credentials to view COVID-19 related policies. Alternatively, they may facilitate fraud by processing "donation" payments for charities or other COVID related institutions which do not exist.
- Multiple COVID-19 related watering hole attacks were launched to steal information such as browser cookies, history, payment information, form autofill information and saved login credentials. **A watering hole attack** is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit.

Suggested top actions:

1. Enable two-factor authentication for any third-party logins, vendor logins, and remote user logins.
2. Monitor and limit the number of login attempts allowed by a user to get into a system. After a threshold is passed, disable the account and implement the second channel of verification to re-enable the account.
3. Implement Access Control (AC) and Identity Access Management (IAM) in order to limit network privileges and shared drive permissions to contain endpoint ransomware infections. Grant users the minimum local privileges that they need in their roles.
4. Avoid clicking on attachments or links embedded in email messages with subject lines purporting to contain information related to COVID-19 or Coronavirus.

Top Data Protection and Privacy considerations amid COVID-19

In the UK, NHS gave supermarkets data about vulnerable patients to prioritize deliveries to those most in need. The information covered **at least 1.5 million people.**

What data protection and privacy measures should be taken for public health?

The US may leverage the National Syndromic Surveillance Program, which is a voluntary collaboration between the Centers for Disease Control and Prevention and various state and local health departments that **draws data from more than 4,000 health care facilities.**

Does the processing of health data by public authorities open the door to surveillance?

Analysis of eCommerce transactions found that purchases for cold, cough & flu products have **increased 198%,** while online purchases for pain relievers **increased 152%.**

What are the consequences of processing highly sensitive data?

Apple and Google unveiled tools that would allow smartphone users to know if they have crossed paths with anyone who has COVID-19. This technology could inject valuable new support into contact tracing, a strategy public health officials say is essential to allowing people to return to work and normal life while containing the spread of the pandemic.

If monitoring citizens, what measures should be taken to anonymously monitor?

PHI is more valuable to fraudsters than PII from other industries because of the greater amount of detail that it contains, such as dates of birth and Social Security numbers. The detail level in PHI facilitates identity theft, such as fraudulent applications for lines of credit, insurance fraud, and the fraudulent acquisition of prescription medications.

Bulk PII records from non-health care organizations may sell for as little as

$0.10 *USD per record*

whereas PHI records may sell for as much as

$5 *USD per record*

Recover and Thrive: Considerations for protecting privacy while ensuring safety

WHAT QUESTIONS ORGANIZATIONAL LEADERS SHOULD BE ASKING AROUND DATA PRIVACY AS WE SHIFT TO THE "NEXT NORMAL"

As society transitions, whenever their governments deem the timing right, traditional organizations have some tough decisions to make around how to bring employees and customers back into their businesses. Do they take temperatures, wait for antibody testing, do they ask for health disclosures? Whichever path they choose, there will be decisions to be made around data privacy.

Globally, there is tension around the topic of privacy and pandemic management. Questions around ethics in data collection, analysis and privacy are raised. What questions should organizations begin asking around data privacy to get to the answers they need in order to identify a path forward for their workforce, customers and citizens? Perhaps they should consider the following:

Data lifecycle	Considerations for organizations navigating 'Respond and Recover'?	Considerations for organizations to 'Thrive' in the next normal?
Create or collect	**Anonymization –** What non-identifying information can be collected for your organization's purposes in combating COVID-19 (e.g., geographic location, demographics)?	**Consent –** Meaningful consent is an essential element of building trust with customers/employees. In an urgent surge to collect data 'now', how can your organization ensure meaningful consent and outline how the information will be used/stored/destroyed during COVID-19 and in the 'next normal'?
Store and process	**Inventory –** Do you have a dynamic approach to inventorying customer/employee data collected for the purposes of COVID-19 related activity?	**Secure data storage –** The more data organizations collect, the greater a target these data havens become to external malicious attackers. How will organizations aim to limit the collection, use and disclosure of personal information to what is necessary to help prevent and manage the spread of COVID-19, and take reasonable steps to keep personal information secure?
Analyze and use	**Analytic approaches –** COVID-19 has increased the complexity of data analytics strategies. How can organizations determine readiness of data for consumption based on analytics techniques? Are there standards around ethical use of data?	**Use –** Is data being used in accordance with published commitments, the organization's legal basis for processing, and international regulations? Does the enterprise have a governance model for data use and analysis?
Share or transfer	**Secure data sharing –** COVID-19 has inspired data sharing between research institutes and international organizations, for example in support of a vaccine. How should organizations consider examining if their aggregated data contains confidential or restricted information, and how are they securing the transfer of that data?	**Monitor data transfers –** How is confidential IP, PII and PHI data consumption and transfer monitored during COVID-19 and in the 'next normal'?
Retain and destroy	**Retention and data monetization –** If your organization has plans to monetize data collected amid COVID-19, does your organization have a data monetization strategy that is aligned with your data retention framework?	**Data retention –** Should data collected during COVID-19 be retained to allow for data mining or modeling in the 'next normal,' or destroyed after a pre-defined timeframe?

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

Relevant Deloitte reads:

- **On-Demand Webcast:** Responding to COVID-19 with business resilience, trust, and security
- **Article:** Ransoming government
- **Article:** COVID-19 response capabilities for health care organizations
- **Article:** The heart of resilient leadership: Responding to COVID-19

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.

Deloitte China Cyber Risk Partners


Xue, Tonny
National Cyber Risk Leader
Tel: +86 10 8520 7315
Email: tonxue@deloitte.com.cn


Jiang, David Wei
Eastern Region
Tel: +86 21 2312 7088
Email: davidjiang@deloitte.com.cn

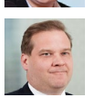

He, Tommy Xiaoming
Northern Region
Tel: +86 10 8512 5312
Email: the@deloitte.com.cn

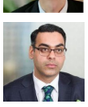

Kwok, Eva Yee Ngar
Southern Region, Hong Kong
Tel: +852 2852 6304
Email: evakwok@deloitte.com.hk


Feng, Steven Ye
Eastern Region
Tel: +86 21 6141 1575
Email: stefeng@deloitte.com.cn


Shih, Nathan Pei-en
Eastern Region
Tel: +86 21 3313 8366
Email: nathanshih@deloitte.com.cn


Xiao, Frank Tengfei
Northern Region
Tel: +86 10 8512 5858
Email: frankxiao@deloitte.com.cn


Pihkanen, Miro
Southern Region, Hong Kong
Tel: +852 2852 6778
Email: miropihkanen@deloitte.com.hk


Kukreja, Puneet
Eastern Region
Tel: +86 21 3313 8338
Email: puneetkukreja@deloitte.com.cn


Zhang, Boris Zhen
Eastern Region
Tel: +86 21 6141 1505
Email: zhzhang@deloitte.com.cn


He, Vivi Wei
Southern Region
Tel: +86 755 3353 8697
Email: vhe@deloitte.com.cn


Ma, Luke Kwok Kwan
Southern Region, Hong Kong
Tel: +852 2852 1086
Email: lukema@deloitte.com.hk

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