Data Sheet

DTS SOLUTION
CYBER SECURITY REDEFINED

Pandemic COVID-19 Outbreak
Cyber Security Implications

As the world is trying to deal with the **coronavirus pandemic**, it seems hackers, fraudsters, and spammers; all flourish and they are not on lockdown. The situation has proven to be a blessing for them. The attackers find new ways to take advantage of the human fear and to target victims with scams or malware campaigns.

Cyber criminals are showing more signs of exploiting public concern and they are trying to leverage the emergency by sending out **"phishing"** emails that lure internet users to click on malicious links or files. These emails are not only being distributed to phish for passwords but are also urging recipients to donate Bitcoin for research into a Coronavirus vaccine.

In this pandemic, many people panic because of **COVID-19**, so attackers take advantage of the situation. How does it work? The attacker sends emails claiming to be from legitimate organizations with information related to coronavirus. The email messages ask the person to open an attachment to see the latest updates. The malware allows the attacker to take control of your computer, log your keystrokes, or access your personal information and financial data, which could lead to identity theft.

It is recommended for individuals to stay alert about browsing of messages, sites, even online calls, before clicking or downloading. Try not to tap on things where you don't have a clue about the sender, you don't have the foggiest idea where it's from, just utilize extremely quality sources, so in the event that you are googling something see the source and check whether it's been confirmed.

Challenges of Coronavirus attack in an organization:

In terms of cyber security:

DATA SECURITY

UNPATCHED ENDPOINTS

PHISHING ATTEMPTS

- **Data Security:** When People who are working from their PC's or from home share their files containing sensitive information by using non-standard tool or applications or using personal emails etc. through unsecured way without using VPNs since all companies can't afford to build or provide a secured network for all of their employees, this may initiate unsecured data transmission.
- **Unpatched Endpoints:** Any home computer used for work that is not up-to-date or without applying mandatory security patches, uses an outdated operating system (such as Windows 7), contains the evidence of an insecure history of browsing or is not under solid password management policies has become a threat to the corporate environment. Also unknown firewall rules or possibly a firewall with an outdated firmware which provides a point of entry for an outside attacker.
- **Phishing Attempts:** A marking consequence of the virus outbreak will certainly increase phishing attempts by scammers through emails and fake websites masquerading as government announcements. If you receive any email detailing information about the spreading of the virus or healthcare information be cautious before you click any link.

Others

- **Business Impact:** Affects the hidden costs like Lost value of customer relationships, Operational disruption or destruction, Revenue and Income loss. While financial hit, leakage of data, unavailability of service are apparent impacts of cyberattacks, intangible things like business reputation, client business relationship also gets impacted. Similarly, a pandemic situation like this may have hidden consequences in the form of recession, market instability for quite some time.
- **Organizational Impact:** Cyberattacks not only impacts the cybersecurity team of an organization but the entire organization, its employees, its customers, and clients when we work as a team. Everyone plays a role in securing an organization.

How do organizations survive such attack with the existing solutions?

1. **FortiMail** gateway solutions can be used to block definite file types. Then it can send the attachments to FortiSandbox solution (ATP), either on-premises or in the cloud, to check whether the file is showing any malicious behavior. FortiGate firewalls with anti-virus enabled having valid subscription are also able to detect and block COVID-19 threats.
2. **Check Point** protects users from multiple websites known to be related to malicious activities and directs to their websites with discussions around the virus, healthcare as well as from scam websites that claim to sell face masks, vaccines, and home tests that can detect the virus as well as regarding precautionary measures.
3. **Sophos** XG Firewall and SD-RED devices provide various solutions for secure remote connectivity also Sophos Endpoint Protection is designed to secure everyone, whether the employees working from home or if they are office based.
4. **Palo Alto** is capable of preventing COVID-19 threats, especially works on the messages and mails that trick users into opening attachments and clicking malicious links. Palo Alto Networks is frequently updating the latest COVID-19 related cyber threats.

How do we prepare ourselves from an unknown problem?

01 UNDERSTAND THREATS TO ORGANIZATION

02 TRAINING & AWARENESS TO EMPLOYEES

03 ISOLATION & PROTECTION OF ENDPOINTS

04 PREPARE A RESPONSE PLAN

05 INCIDENT RESPONSE

06 SECURE VPN DEPLOYMENT

07 BE EXTRA VIGILANT ON VERIFICATION

1. Understand the threats to your organization

Employees are the first and primary line of defense against Cyber Threats. Cyber criminals are becoming more focused on users of the company networks as a weak link in the security infrastructure chain.

Companies can protect themselves by encouraging personnel to avoid doubtful emails from unknown senders or unfamiliar sources who do not usually communicate directly with you. Cybersecurity teams should work with fraud risk management teams to coordinate detection-and-response activities. The authorized personnel should work with their security teams to identify attack vectors through various methodologies, as a result of more employees working from home and prioritize the protection of their most sensitive information and business-critical applications.

2. Provide cyber security training /awareness to employees

Employees working from home must be provided with the knowledge to identify cyber-attacks such as awareness against phishing emails, risks associated with the use of public Wi-Fi, to ensure the security of the devices being used for work.

Send regular reminders to the employees who are working remotely to avoid any fake-lucrative offers or informative emails (phishing emails) or not to engage with unknown people over suspicious calls that are made to steal their credentials or confidential information. And a frantic search for health advice is such an opportunity. So you should always make sure that you look for information about COVID-19 on trusted sources such as WHO.int or theconversation.com.

3. Isolation and Protection of Endpoints

Isolation and quarantine mechanism — Isolate the files from endpoints that are infected with coronavirus cyber attack also ensure to monitor the suspected files/endpoints. Protect devices against standard and advanced malware. Harden and patch your devices.

4. Have a Response Plan

Calamities like virus outbreaks are unavoidable both in the world of security and the world itself. A response plan provides an organized process for handling the unavoidable virus outbreaks and keeping the chaos under control. For example: A zero-day exploit is prejudicial because there are no signatures available to detect and prevent them. But as soon as a pattern or an indicator gets identified, the signature is released.

Response Plan should include steps like Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned. Through the organized lessons learned from previous simulations can be utilized to close gaps in the created response plan.

5. Incident Response

Continuous monitoring of alerts for any cyber threats, validation of remote connections being made to the core systems or network and early detection of the attacks could save the organization from potential threats.

The security around these can be implemented by web gateways, Proxies, firewalls or IDS (intrusion detection systems) etc. The respective team have to continuously work on implementing updated security measures and identify the loopholes in the existing measures which may result because of some unexpected changes to firmware, software and even hardware.

6. Secure VPN Deployment

Adopt a secure VPN or provide a secure connection between the employee's home to your organization's network and strengthen your network security layer subsequently (Inspect & Adapt). Make sure the ongoing access to corporate tools thus provides additional protection against phishing and malware attacks, the same way like Corporate VPNs.

Implement multi-factor authentication for VPN access. Limits on remote desktop protocol (RDP) access and added special monitoring of remote network connections, thus strengthens the remote access management policy and procedures. Also encourage employees to use cloud services since this will reduce the risk to data as it is not stored locally.

7. Be extra vigilant on verification

Phishing emails contain links to dangerous websites with the aim of intercepting the user's access data. A lot of emails with malicious software, executables are being sent right now during times of uncertainty. Please refrain from opening any mails containing an attachment. If you don't know or trust the sender, don't open it. Better yet: delete it. e.g. Emails that might seem regarding coronavirus death toll being totally exaggerated or hints at a conspiracy involving rogue states setting free the virus as some kind of biological weapon to offer advice from government organizations or WHO (World Health Organization) might not be what they seem. They may be cyberattacks aimed at entering your system to fetch your personal data and might exploit it.

Always use a secure medium of communication for official purposes. Make sure that security protocols such as DMARC are set in your email domain to secure the medium against any attempt of spoofing or abuse. Don't put it off- Create a stronger line of defense against increasingly sophisticated Novel Coronavirus cyber threats now. Prevent at least one employee from making an honest mistake and clicking on the wrong link could save the business from reputational and financial losses. You should also bear in mind that how many such cyber-crime cases or attempts breakout during this pandemic outbreak and how the organizations & businesses were affected or how did they tackle those attacks. Cyber criminals use every opportunity available to exploit weaknesses in cyber security.

Let's stand together to support each other in these difficult times and make sure that we stay proactive and alert against Cyber Crimes.

DTS SOLUTION
CYBER SECURITY REDEFINED

DUBAI: Office 4, Oasis Center, Sheikh Zayed Road, Dubai, United Arab Emirates
T: +971 4 338 3365 | **E:** info@dts-solution.com

☎ 800 HACKED

ABU DHABI: Office 253, Al Bateen C6 Tower - Bainunah, King Abdullah Bin Abdulaziz Al Saud Street | **T:** 971 2 2076777
LONDON: 160 Kemp House, City Road, London, EC1V 2NX, United Kingdom | **T:** +44 2081230 387 (DTS)
www.dts-solution.com