2020-06-18

GLOBAL COVID 19-RELATED PHISHING CAMPAIGN BY NORTH KOREAN OPERATIVES LAZARUS GROUP EXPOSED BY CYFIRMA RESEARCHERS

Reporting Date: 18 June 2020

Assessment Period: 1 to 16 June 2020

Subject: Hacker groups are planning a large-scale phishing campaign targeted at more than 5M individuals and businesses (small, medium, and large enterprises) across six countries and multiple continents

Motivation: Financial Gains

Method: The hacking campaign involved using phishing emails under the guise of local authorities in charge of dispensing government-funded Covid-19 support initiatives. These phishing emails are designed to drive recipients to fake websites where they will be deceived into divulging personal and financial information.

Executive Summary:

CYFIRMA Researchers have been tracking the Lazarus Group, a known hacker group sponsored by North Korea, for many years. Investigations into the Group's activities have revealed detailed plans indicating an upcoming global phishing campaign.

There is a common thread across six targeted nations in multiple continents – the governments of these countries have announced significant fiscal support to individuals and businesses in their effort to stabilize their pandemic-ravaged economies. The following are some of the government-funded programs:

> Singapore, a small nation-state in Southeast Asia, has announced almost SGD 100B financial aid in various forms to stem unemployment and keep businesses afloat;

paying foreigners;

> Indian government has announced Rs 20 lakh crore (US$307B) of credit, finance and collateral-free loans to micro, small and medium enterprises, as well as welfare packages for citizens;

> America has set aside trillions of dollars to design Economic Impact Payment or Stimulus Payments as well as Paycheck Protection Program to prop up its economy; and

> As part of the UK government COVID-19 recovery strategy, a number of support programs have been made available, such as Coronavirus Job Retention Scheme, and Self-Employment Income Support Scheme. The Government's package has also been complemented by further contributions from the Bank of England.

The Lazarus Group's upcoming phishing campaign is designed to impersonate government agencies, departments, and trade associations who are tasked to oversee the disbursement of the fiscal aid.

The hackers plan to capitalize on these announcements to lure vulnerable individuals and companies into falling for the phishing attacks.

Given the potential victims are likely to be in need of financial assistance, this campaign carries a significant impact on political and social stability.

CYFIRMA Researchers first picked up the lead on June 1, 2020, and have been analyzing the planned campaign, decoding the threats, and gathering evidence. Evidence points to hackers planning to launch attacks in six countries across multiple continents over a two-day period. Further research uncovered seven different email templates impersonating government departments and business associations.

As of time of reporting (18 Jun), we have not seen the phishing or impersonated sites defined in the email templates. But our research shows the hackers were planning to set that up in the next 24 hours.

We also observed that hackers are planning to spoof or create fake email IDs impersonating various authorities. These are some of the emails discussed in their phishing campaign plan:

> covid19notice@usda.gov

> ccff-applications@bankofengland.co.uk

> covid-support@mom.gov.sg

> covid-support@mof.go.jp

> ncov2019@gov.in

> fppr@korea.kr

Campaign Launch Dates:

According to the hackers plans as observed by CYFIRMA Research, the phishing campaigns are scheduled to launch in the following countries across multiple continents on the stated dates.

Country Name	Campaign Launch Date	Target
USA	20 June 2020	Individuals
UK	20 June 2020	Businesses
Japan	20 June 2020	Individuals
India	21 June 2020	Individuals
Singapore	21 June 2020	Businesses
South Korea	21 June 2020	Individuals

Phishing Theme:

USA: Hackers claimed to have 1.4M curated email IDs. The Plan is to send the email below via a spoofed USDA email account luring them with fake Direct Payment of USD 1000 and inciting them to provide personal detail. Pls see email evidence below.

UK: Hackers claimed to have 180,000 business contacts. The plan is to send email below via a spoofed Bank of England email account and luring them to provide business details, pressing them to provide before 26 June 2020. Pls see email evidence below.

Japan: Hackers claimed to have 1.1M individual email IDs and planning to send phishing email from a spoofed Ministry of Finance, Japan email account offering additional payment of JPY 80,000 for all citizens and residents of Japan. Pls see email evidence below.

India: Hackers claimed to have 2M individual email IDs. The plan is to send emails free COVID-19 testing for all residence of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad inciting them to provide personal information. Pls see email evidence below.

South Korea. Hackers claimed they have 700,000 individual email IDs and will send phishing email to all citizens announcing an additional 1M Won payment in cash and shopping vouchers. The fake email will be spoofed to impersonate the South Korean Government. Pls see email evidence below.

Phishing Email Targeting the US

Dear Fellow Americans,

We are going through unprecedented times because of Covid-19 pandemic.

Your Federal Government wants to reassure you we are with you in this difficult time.

We have created Direct-pay Government Benefits schemes, which can provide you support up to $1000 per person in your family. We recommend you update your personal and bank details using link [ ].

Direct-pay benefit program is on top of grant schemes;
Supplemental Nutrition Assistance Program (SNAP)
Subsidized Housing, Housing Voucher and Public Housing program
Welfare or Temporary Assistance for Needy Families (TANF)

Under direct payment schemes all USA citizens will paid $1000 into their bank accounts, if you don't have access to you bank, a cheque will send to your communication address.

Regards,
USDA,
United States
Call the USDA National Hunger Hotline at 1-866-3-HUNGRY (1-866-348-6479)
or 1-877-8-HAMBRE (1-877-842-6273). Information is available in English and Spanish.
The hotline operates Monday through Friday, 7:00 AM to 10:00 PM Eastern Time.

Phishing Email Targeting the UK

Sir/Madam,

Today HM Treasury announced a number of measures designed to support businesses. The Chancellor set out a package of temporary, timely and targeted measures to support public services, people and businesses through this period of disruption caused by Covid-19.

The joint HM Treasury and Bank of England lending facility, named the Covid Corporate Financing Facility (CCFF). The facility is designed to support liquidity among larger firms, helping them to bridge coronavirus disruption to their cash flows through the purchase of short-term debt in the form of commercial paper.

You can register your business by clicking the link below []

Last date to register your business is 26 June 2020 by 2pm.

Thank you very much,
Bank of England, Threadneedle Street, London, EC2R 8AH, Switchboard: +44(0)20 3461 4444, Enquiries: +44(0)20 3461 4878

Phishing Email Targeting Japan

住民

日本の大蔵省は本日、日本のすべての居住者への支援資金の追加80,000円を発表しました。 前回からの手続きを簡単にするために、今回はリンク[]を使用してオンラインで申請できます。 今日申し込む

2020年7月15日までに、支払いは銀行口座に直接送られるか、小切手は指定された通信アドレスに送られます。

日本政府はすべての市民と居住者の福祉に取り組んでいます。

どうもありがとうございました、
日本財務省
100100-8940東京都千代田区霞ヶ関3-1-1 Tel：03-3581-4111

Phishing Email Targeting India

Dear Citizens,

The ministry of health and family welfare, government of India has announced a mandatory COVID-19 testing for all residents of Delhi, Mumbai, Hyderabad, Chennai and Ahmedabad above age of 40 years.

Government of India has decided to reimburse testing cost incurred.

A medical staff will come to your residence to collect samples.

Please immediately register using link below for all free COVID-19 test. Do not forget to provide complete contact details with PAN no.

Link ()

Thank you for your support in keeping India's fight against COVID-19.

Thank You;
Ministry of Health and Family Welfare (MOHFW)
Nirman Bhavan, Maulana Azad Road
New Delhi 110011

Phishing Email Targeting Singapore

新加坡商业联合会会员，

感谢您在COVID19断路器期间的长期支持。我们了解您在过去两个月或更长时间内遭受的痛苦和折磨，这使您无法开展业务。

在过去的几个月中，我们宣布了许多由新加坡政府支持的商业友好计划。此外，新加坡人力部（MOM）今天宣布了一项新的财务计划，根据工作支持计划（JSS）为每位员工提供750新元的一次性补贴。

请注册您的公司，不要忘记提供您的公司银行信息，以便我们能够自动转移资金。

立即索取利益：[]

谢谢，
人力部[MOM]新加坡
MOM服务中心
1500 Bendemeer Road，新加坡339946
就业准证服务中心
金河路，20上环路，＃04-01 / 02，新加坡邮政编码058416

Phishing Email Targeting South Korea

한국 시민 여러분

2020 년 3 월 경제 및 재무부 장관 발표와 더불어 오늘날 보건 복지부 (MOHW)는 시민과 주민을위한 2 단계 구호 기금을 발표했다. 이 구호 기금에 따라 모든 시민과 주민은 최대 100 만 원의 현금 및 쇼핑 바우처를받을 수 있습니다.

현금 지급을 받으려면 모든 시민이 오늘 등록해야합니다.

여기서 신청할 수 있습니다 ()

감사합니다,
보건 복지부
세종시 둘 4로 13 (30113) 대한민국
도움말 센터 82-129

Phishing Email Targeting Singapore

Anggota Persekutuan Perniagaan Singapura,

Terima kasih atas sokongan jangka panjang anda semasa pemutus litar COVID19. Kami memahami keperitan dan penderitaan yang anda alami selama dua bulan atau lebih, yang telah menghalang anda daripada menjalankan perniagaan.

Dalam beberapa bulan terakhir, kami telah mengumumkan banyak program persahabatan perniagaan yang disokong oleh pemerintah Singapura. Sebagai tambahan, Kementerian Tenaga Manusia (MOM) Singapura hari ini mengumumkan rancangan kewangan baru yang memberikan subsidi satu kali sebanyak S $ 750 bagi setiap pekerja di bawah Pelan Sokongan Kerja (JSS).

Daftarkan syarikat anda dan jangan lupa memberikan maklumat bank syarikat anda supaya kami dapat memindahkan dana secara automatik.

Tuntut faedah anda dengan segera: []

Terima kasih,
Kementerian Tenaga Manusia [MOM] Singapura
Pusat Servis MOM
1500 Bendemeer Road, Singapura 339946
Pusat Perkhidmatan Pas Pekerjaan
Sinhe Road, 20 Upper Ring Road, # 04-01 / 02, Singapura 058416

Pls contact CYFIRMA if you'd like a deeper technical discussion on how we can assist your organization to discover threats at the early planning stage.

Get In Touch

Have a burning question for us? Want to decode threats and deploy the best cybersecurity strategy for your organization?

Contact Us