New Threat Actor Spoofs Philippine Government, COVID-19 Health Data in Widespread RAT Campaigns

proofpoint.com/us/blog/threat-insight/new-threat-actor-spoofs-philippine-government-covid-19-health-data-widespread

October 25, 2021

Blog
Threat Insight
New Threat Actor Spoofs Philippine Government, COVID-19 Health Data in Widespread RAT Campaigns

October 27, 2021 Selena Larson and Joe Wise

Key Findings

- Proofpoint identified a new cybercriminal threat actor, TA2722.
- This group impersonates Philippine health, labor, and customs organizations as well as other entities based in the Philippines.
- TA2722 typically targets Shipping/Logistics, Manufacturing, Business Services, Pharmaceutical, and Energy entities, among others. Geographic targeting includes North America, Europe, and Southeast Asia.
- TA2722 distributes Remcos and NanoCore remote access trojans (RATs).

Overview

Proofpoint identified a new and highly active cybercriminal threat actor, TA2722, colloquially referred to by Proofpoint threat researchers as the Balikbayan Foxes. Throughout 2021, a series of campaigns impersonated multiple Philippine government entities including the Department of Health, the Philippine Overseas Employment Administration (POEA), and the Bureau of Customs. Other related campaigns masqueraded as the Manila embassy for the Kingdom of Saudi Arabia (KSA) and DHL Philippines. The messages were intended for a variety of industries in North America, Europe, and Southeast Asia, with the top sectors including Shipping, Logistics, Manufacturing, Business Services, Pharmaceutical, Energy, and Finance.

Proofpoint assesses this actor is targeting organizations directly or indirectly engaged with the Philippine government based on a continuous pattern of spoofing email addresses and delivering lures designed to impersonate government entities. For example, the shipping, transportation, and logistics companies would frequently engage with customs officials at ports of call. Additionally, the manufacturing and energy companies support and maintain large supply chain operations, likely requiring correspondence with both labor and customs organizations.

All the campaigns distributed either Remcos or NanoCore remote access trojans (RATs). Remcos and NanoCore are typically used for information gathering, data theft operations, monitoring and control of compromised computers. While the malware's associated infrastructure changed over time, the sender emails were reused for a long period of time.

In 2020, Philippine government entities issued multiple alerts warning users of the activity related to lures using themes such as COVID-19 infection information in the Philippines and the POEA labor information.

Campaign Details

Proofpoint researchers identified a series of campaigns distributing Remcos and NanoCore RATs masquerading as the Kingdom of Saudi Arabia (KSA) embassy in Manila and the Philippine Overseas Employment Administration (POEA) in mid-2021. Upon further investigation, Proofpoint identified additional, separate campaigns distributing the same malware masquerading as the Philippine Department of Health and Bureau of Customs.

Proofpoint separated campaigns into two distinct threat activity clusters. In all cases, message lures were in English. They contained multiple threat distribution mechanisms including:

- OneDrive URLs linking to RAR files with embedded UUE files
- PDF email attachment with an embedded OneDrive link or other malicious URL leading to compressed executables (.iso files) that download and run malware
- Compressed MS Excel documents containing macros which, if enabled, download malware

Remcos is a commodity remote access tool available for purchase online. NanoCore is also commodity malware and written in .NET by "Aeonhack". The code is obfuscated with Eazfuscator.NET 3.3. NanoCore RAT is sold on various hack forums. NanoCore includes many features and plugins. Both Remcos and NanoCore RAT are distributed by numerous cybercrime threat actors with many different delivery techniques and lures.

Threat Cluster Shahzad73

Proofpoint named the first identified cluster Shahzad73 based on the command and control (C2) domains used by the threat actor:

shahzad73[.]ddns[.]net

shahzad73[.]casacam[.]net

Although Proofpoint began regularly tracking this activity cluster in April 2021, historic data suggests the activity dates as far back as August 2020. The threat actor generally leverages themes purporting to be labor-related messages, including spoofing the Philippine Overseas Employment Administration (POEA) and the Saudi Arabian consulate in Manila. Other, less frequent threats observed in Shahzad73 campaigns were associated with billing/invoice lures. The messages impacted hundreds of customers globally including entities in the Transportation, Energy, Construction, Manufacturing, Finance, and Business Services industries.

Messages purported to be, for example:

From: POEA <info1@poea.gov.ph>

Subject: "POEA ADVISORY ON DELISTED AGENCIES."

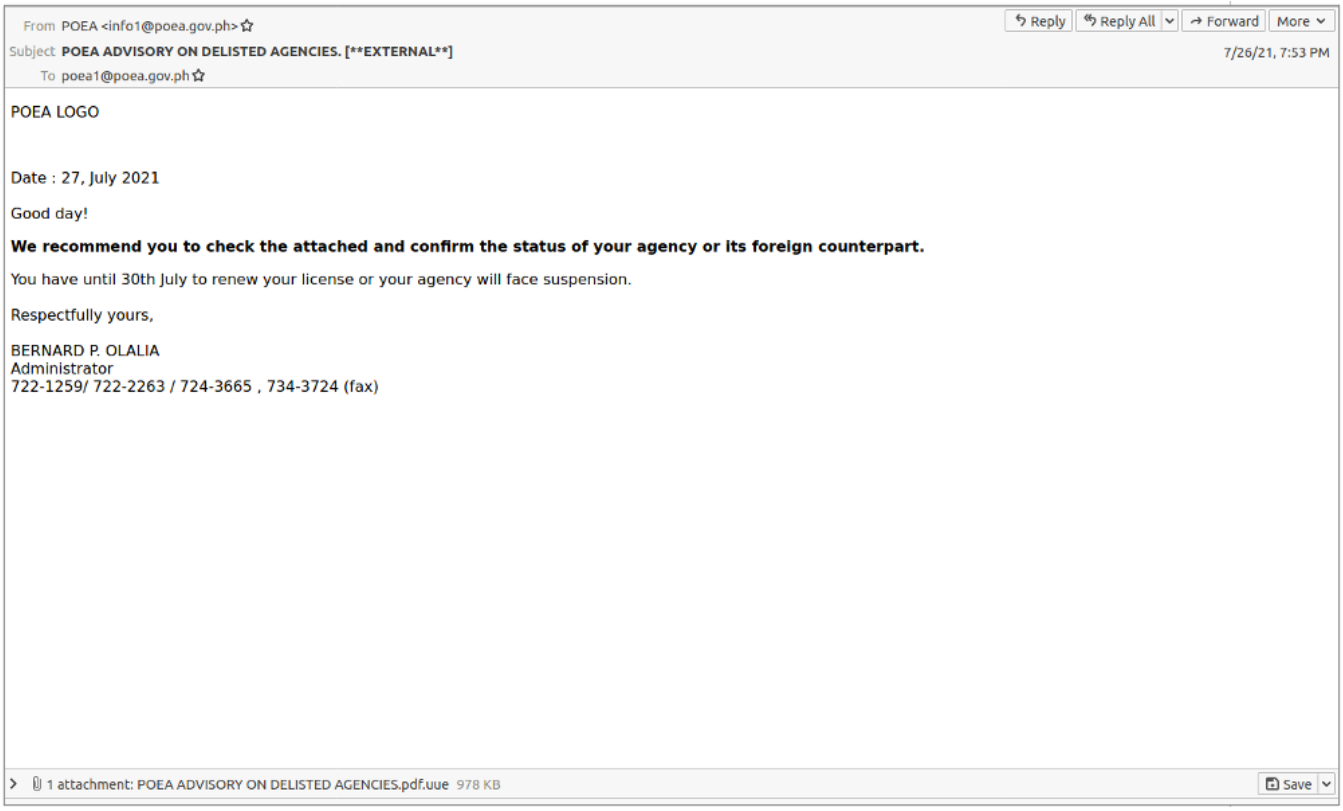

Figure 1: Email sample purporting to be from Philippine Overseas Employment Administration (POEA).

Additional samples include:

From: "ksa.Consulate manila " <consulate_ksa_emb@gmail.com>

Subject: "Memorandum from the Saudi Embassy"

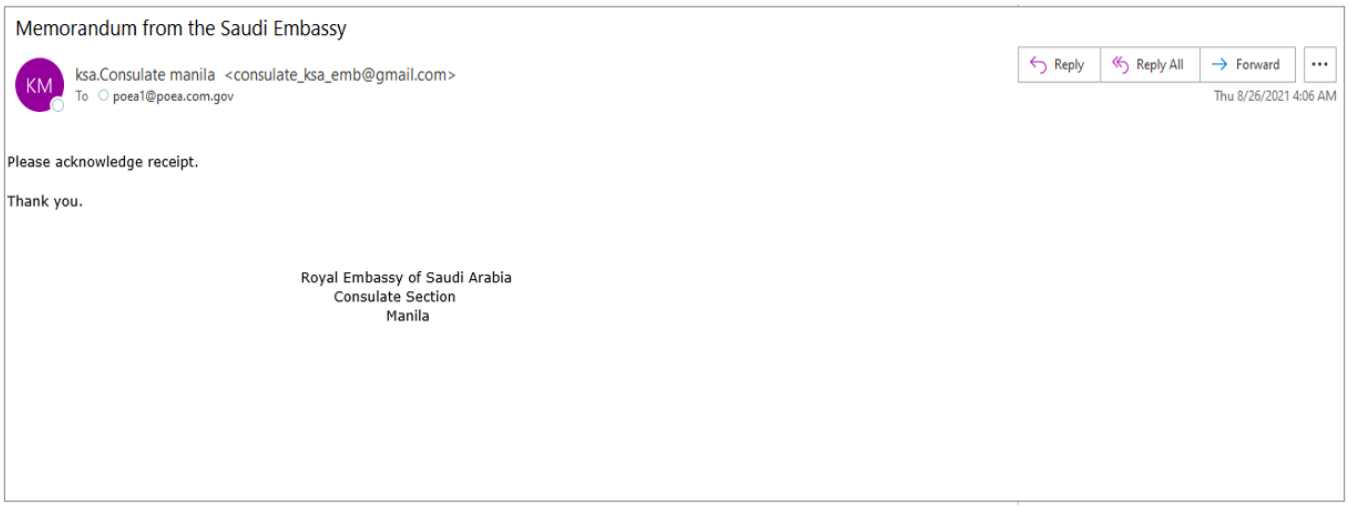

Figure 2: Email sample purporting to be from the Kingdom of Saudi Arabia (KSA) consulate.

Saudi Arabia is reportedly one of the most popular destinations for the country's overseas workers, with over one million Filipinos working there. In May 2021, the Philippines temporarily suspended sending workers to the Kingdom after receiving reports Filipino workers were being charged for COVID-19 testing and quarantine. Proofpoint identified a campaign spoofing the KSA embassy in Manila targeting transportation entities, among others, around the same time.

Most of these messages contain either UUE or RAR attachments ultimately leading to the installation of Remcos remote access trojan (RAT) or NanoCore RAT. Each campaign featured a dynamic DNS C2 domain containing the keyword shahzad73.

Example attachment file names:

memorandum from the saudi embassy.pdf.uue.rar

Memorandum from the Saudi Embassy.pdf.uue

POEA Memo-Circular No 019-22.pdf.uue

POEA Memo-Circular No 002-06.pdf.exe

poea memo on delisted agencies ! reminder.uue.rar

poea advisory on delisted agencies.pdf.uue

swiftusd33,980_soa005673452425.uue.rar

The observed Remcos samples included the following example configuration:

C2: shahzad73[.]casacam[.]net:2404

C2: shahzad73[.]ddns[.]net:2404

license: 9C98D5D48F9EA32282C07700F23815A0

version: 2.7.2 Pro

Observed NanoCore RAT samples included the following example configuration:

GCThreshold: 10485760

KeyboardLogging: True

WanTimeout: 8000

Version: 1.2.2.0

Mutex: Global\{a58bb08a-85df-4191-824c-1b90cbce1024}

RestartDelay: 5000

BackupDnsServer: 8.8.4.4

PrimaryDnsServer: 8.8.8.8

ConnectionPort: 9036

MaxPacketSize: 10485760

BufferSize: 65535

ClearZoneIdentifier: True

DefaultGroup: ENDING-JUNE

LanTimeout: 2500

BackupConnectionHost: shahzad73[.]ddns[.]net

BuildTime: 2021-07-26 13:34:18 UTC

UseCustomDnsServer: True

MutexTimeout: 5000

KeepAliveTimeout: 30000

PrimaryConnectionHost: shahzad73[.]casacam[.]net

TimeoutInterval: 5000

PreventSystemSleep: True

ConnectDelay: 4000

Threat Cluster CPRS

Proofpoint named the second identified threat cluster CPRS based on the actor regularly spoofing the Philippines Bureau of Customs - Client Profile Registration System (CPRS) in ongoing campaigns. The identified Remcos RAT campaigns impacted nearly 150 customers globally, with a focus on Shipping and Logistics, Manufacturing, Industry, and Energy sectors.

Proofpoint began tracking this activity cluster in December 2019. The actor appeared to conduct multiple campaigns per month through October 2020. Activity restarted again in September 2021. Historic data suggests the activity dates as far back as 2018. The threat actor generally leverages themes purporting to be entities related to the Philippine government, most frequently the Bureau of Customs CPRS. Other emails masqueraded as the country's Department of Health distributing COVID-19 information. Other, less frequently observed threats in related campaigns were associated invoice, shipping, or Finance/Treasury themes.

Messages purported to be, for example:

From: cprs@customs[.]gov[.]ph

Subject: "E-Mail Alert for Status: PROVISIONAL GOODS DECLARATION REFERENCE NO.C-1075027-21"

Figure 3: Email purporting to be a Bureau of Customs declaration.

Other message samples include:

From: COVID-19@doh.gov.ph

Subject: "Covid-19 Data Cases Report in Your Location-The Department of Health (DOH)"

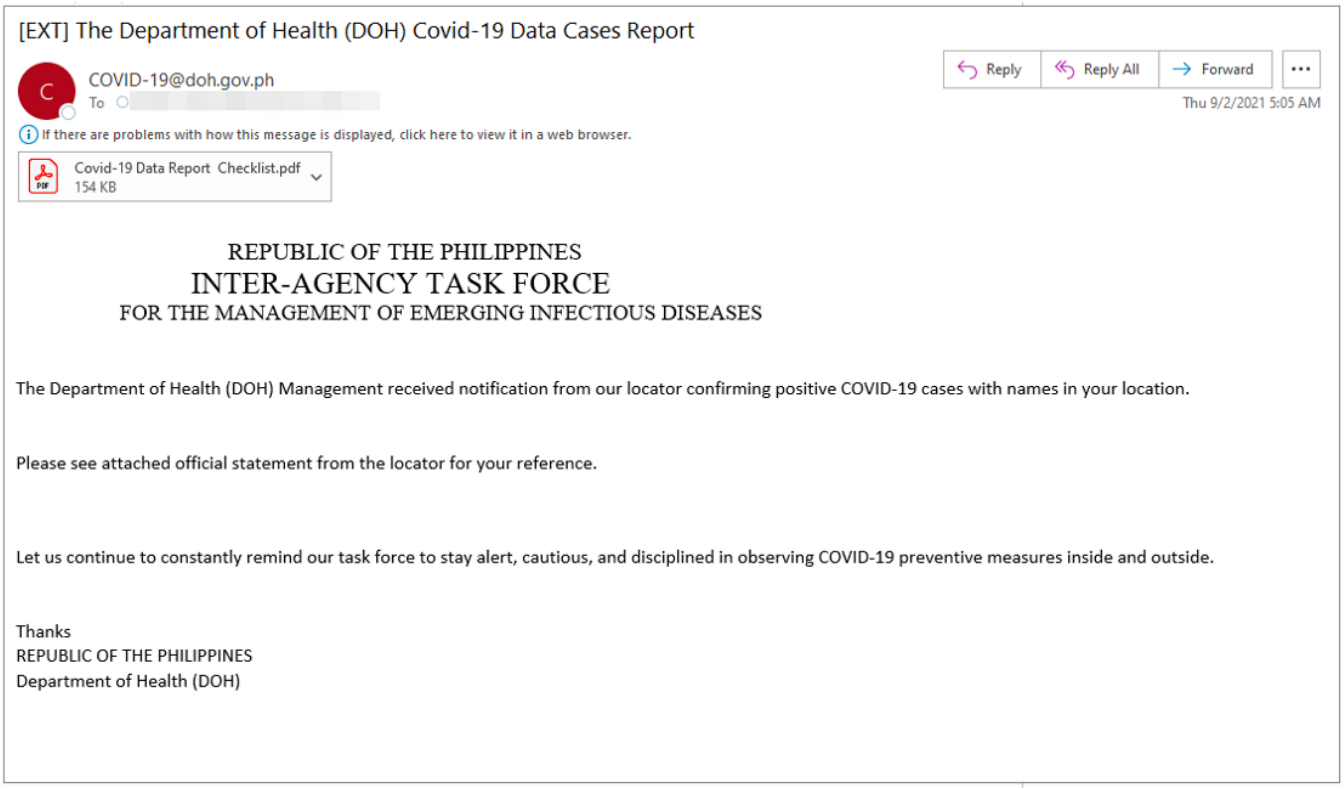

Figure 4: Message purporting to be COVID-19 information from the Philippine Department of Health.

Example attachment file names:

covid-19 pcr test report checklist.pdf

covid-19 data cases report.pdf

notice to submit.pdf

The emails contain either a OneDrive URL or a PDF attachment with a OneDrive URL leading to the download of a compressed executable (e.g. Covid-19 Data Report Checklist_pdf.iso) which, if executed, leads to Remcos RAT.

The most recent Remcos configuration is as follows:

C2: cato[.]fingusti[.]club

License: 4E7867F67DE525ADF9F3A74DBEB02869

Version: 2.7.2 Pro

Mutex: nan

use_tls: nan

2020 campaigns included the following Remcos configuration:

C2: remcos[.]got-game[.]org:2265:pass

license: D77341DCD207EB897C3383385A6676C2

version: 2.5.0 Pro

On 27 September 2021, the threat actor appeared to change tactics. Proofpoint researchers observed corporate credential capture attempts targeting many of the same companies as previously observed Remcos activity. The phishing emails masqueraded as the Philippines Bureau of Customs CPRS and contained actor-hosted URLs linking to a credential harvesting page.

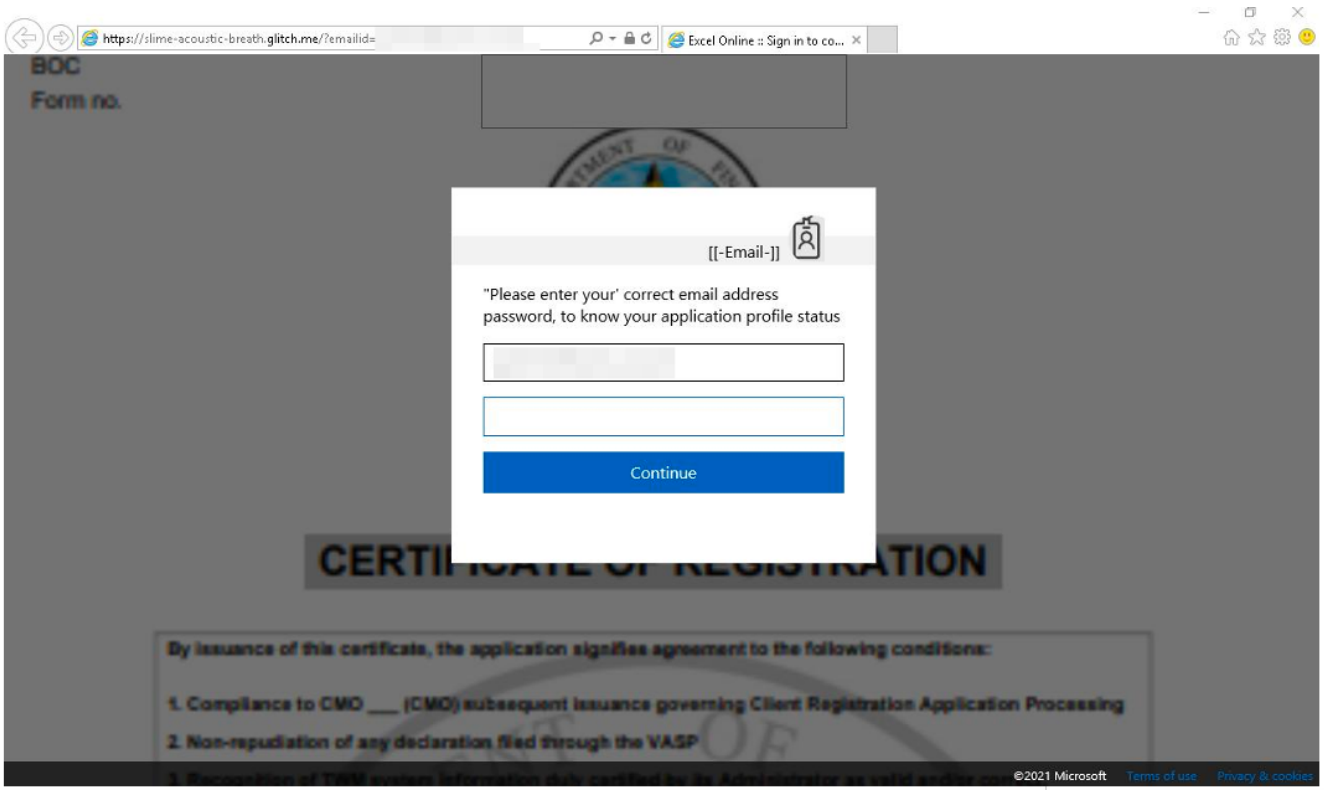

Figure 5: Credential capture landing page.

Despite an expansion of TTPs to include credential harvesting campaigns, Proofpoint assesses with high confidence credential capture activities are likely temporary and the threat actor maintains ongoing high levels of malware distribution activity.

Threat Cluster Overlap

Proofpoint assesses with high confidence the two observed threat clusters are associated with the same threat actor, TA2722. Of note, both clusters targeted a frequently overlapping set of customers, and shared the same sender IP address. Based on observed infrastructure, the two clusters share similar hosting providers, netblocks, and registrars. There are also dozens of unrelated domains that appear to distribute RATs hosted on the same infrastructure.

Threat Cluster	C2 IP	Last Seen	First Seen	ASN	Host Org	Netblock	Country	Registrar
CPRS	185.140.53[.]189	9/22/21	9/22/21	AS208476 - PRIVACYFIRST	Danilenko, Artyom	185.140.53[.]0/24	SE	RIPE
CPRS	79.134.225[.]107	9/20/21	9/7/21	AS6775 - FINK-TELECOM-SERVICES	Andreas Fink trading as Fink Telecom Services GmbH	79.134.224[.]0/19	CH	RIPE
CPRS	79.134.225[.]92	8/11/21	1/22/21	AS6775 - FINK-TELECOM-SERVICES	Andreas Fink trading as Fink Telecom Services GmbH	79.134.224[.]0/19	CH	RIPE
CPRS	185.244.30[.]70	1/9/21	1/6/21	AS208476 - PRIVACYFIRST	Danilenko, Artyom	185.244.30[.]0/24	NL	RIPE
CPRS	185.140.53[.]225	12/27/20	12/14/20	AS208476 - PRIVACYFIRST	Danilenko, Artyom	185.140.53[.]0/24	SE	RIPE

Shahzad73	185.140.53[.]8	9/23/21	8/9/21	AS208476 - PRIVACYFIRST	Danilenko, Artyom	185.140.53[.]0/24	SE	RIPE
Shahzad73	185.19.85[.]139	7/29/21	5/11/21	AS48971 - DATAWIRE-AS	DATAWIRE AG	185.19.84[.]0/22	CH	RIPE
Shahzad73	79.134.225[.]9	5/10/21	4/7/21	AS6775 - FINK-TELECOM-SERVICES	Andreas Fink trading as Fink Telecom Services GmbH	79.134.224[.]0/19	CH	RIPE
Shahzad73	91.212.153[.]84	4/4/21	2/2/21	AS24961 - MYLOC-AS	myLoc managed IT AG	91.212.153[.]0/24	DE	RIPE

Additionally, Proofpoint identified a common registration email associated with multiple command and control IPs and domains that overlapped with the observed activity:

anthony.marshall.1986@gmail[.]com

This email was previously associated with Adwind RAT campaigns reported in 2017.

Conclusion

Proofpoint assesses with high confidence TA2722 is a highly active threat actor leveraging Philippine government themes and targeting a variety of organizations in Southeast Asia, Europe, and North America. It is likely this threat actor is attempting to gain remote access to target computers, which could be used for information gathering or to install follow-on malware or engage in business email compromise (BEC) activity.

Example indicators of compromise:

Indicator	Description
de5992f7c92351d1011fbece2d4bf74ecfc3b09f84aedb12997a2c3bf869de2c	Remcos SHA256
098fe3c8d0407e7438827fb38831dac4af8bd42690f8bd43d4f92fd2b7f33525	NanoCore SHA256
shahzad73[.]casacam[.]net	Remcos/NanoCore C2
shahzad73[.]ddns[.]net	Remcos/NanoCore C2
cato[.]fingusti[.]club	Remcos C2
remcos[.]got-game[.]org	Remcos C2
info1@poea[.]gov[.]ph	Sender Email
cprs@customs[.]gov[.]ph	Sender Email
consulate_ksa_emb@gmail[.]com	Sender Email
de5992f7c92351d1011fbece2d4bf74ecfc3b09f84aedb12997a2c3bf869de2c	Remcos SHA256
66.248.240[.]80	Sender IP