Threat Actor Profile: TA2719 Uses Colorful Lures to Deliver RATs in Local Languages

proofpoint.com/us/blog/threat-insight/threat-actor-profile-ta2719-uses-colorful-lures-deliver-rats-local-languages

August 25, 2020

Blog

Threat Insight

Threat Actor Profile: TA2719 Uses Colorful Lures to Deliver RATs in Local Languages

August 26, 2020 The Proofpoint Threat Research Team

In late March 2020, Proofpoint researchers began tracking a new actor with a penchant for using NanoCore and later AsyncRAT, popular commodity remote access trojans (RATs). Dubbed TA2719 by Proofpoint, the actor uses localized lures with colorful images that impersonate local banks, law enforcement, and shipping services. To date, Proofpoint has observed this actor send low volume campaigns to recipients in Austria, Chile, Greece, Hungary, Italy, North Macedonia, Netherlands, Spain, Sweden, Taiwan, United States, and Uruguay.

Below are recent lure examples, message volume, geo targeting, and payload details. While lures are customized for various geographies and impersonate individuals associated with the spoofed entities, no vertical targeting has been observed. This actor typically delivers malware via malicious attachments, though URLs linking to malicious files were used as a delivery mechanism in early campaigns. TA2719 often relies on widely available resources, such as commodity malware and free hosting providers, to execute their campaigns.

Lures

Most lures observed appear to be from a real person with a connection to the spoofed organization. Even details like the street address in the alleged sender's signature are often accurate. Combined with the branding, these details attempt to boost legitimacy of the message. They could still appear legitimate to an intended recipient who chooses to search for the sender's name or address before opening the attached file or clicking a link in the message.

Campaigns observed during March-May 2020 were primarily law enforcement-themed. Using local languages and logos from local law enforcement agencies, the subject lines often attempted to create urgency by claiming, "ข้อความด่วนจากสำนักงานตำรวจแห่งชาติ (Urgent

message from the Royal Thai
Police),” or “Последната полициска покана пред апсењето (The last police invitation before the arrest)” (Figures 1, 2).

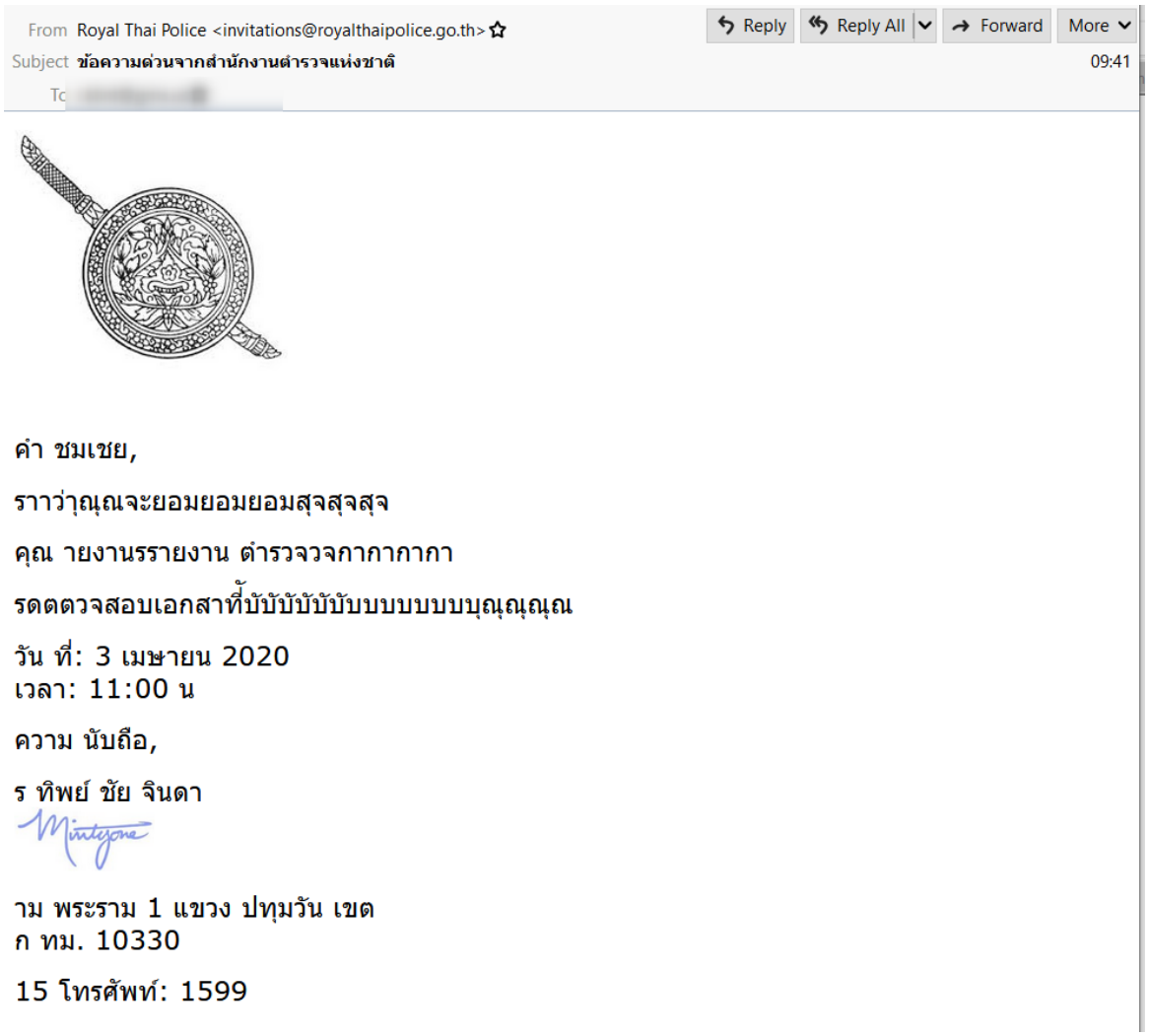


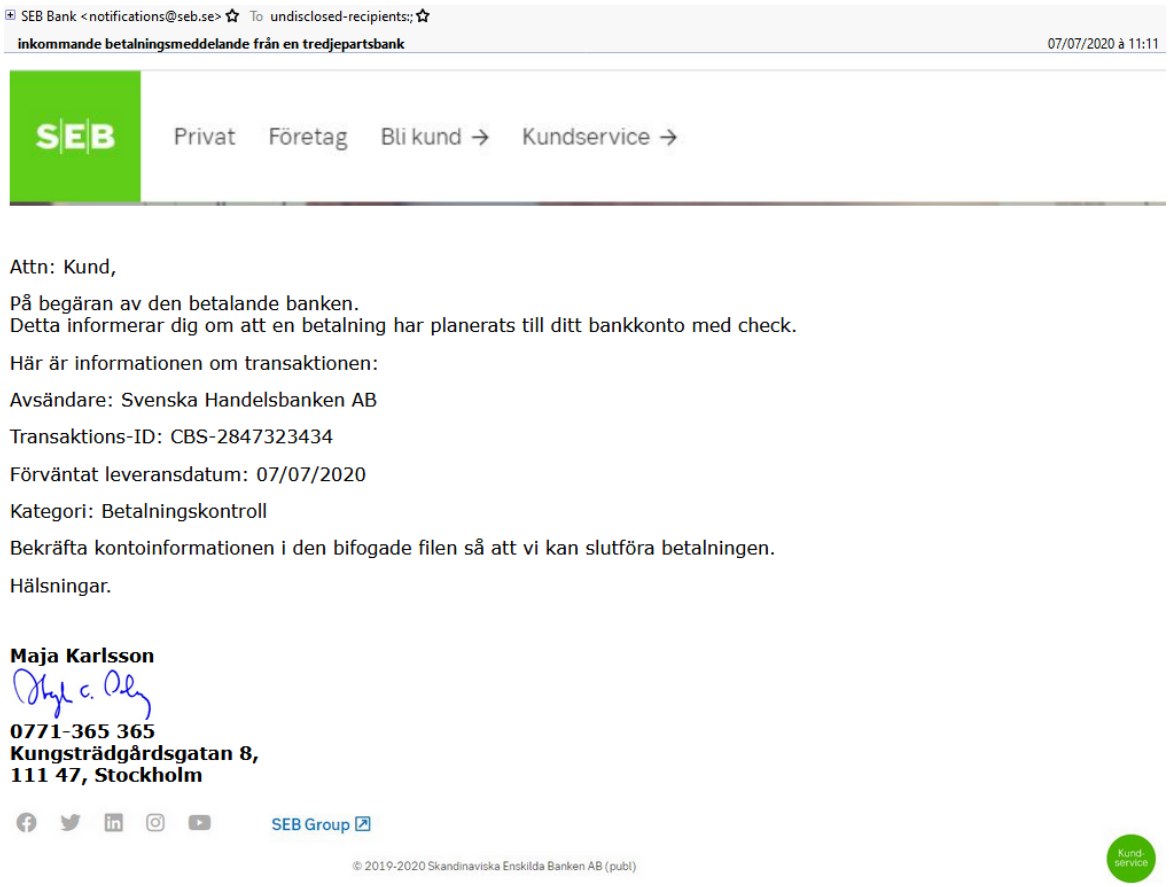
Figure 1: Email lure spoofing Royal Thai Police

Figure 2: Email lure impersonating the Police of North Macedonia, appearing to come from the State Secretary of the North Macedonian Ministry of Internal Affairs

In addition to law enforcement-themed lures, some messages sent during this time spoofed shipping notifications. One early campaign also preyed on COVID-19 fears and impersonated the Taiwan Centers for Disease Control (Figure 3). This campaign was notable not only because of the theme, but also because it leveraged both URLs and attachments to deliver the payload. Typically, TA2719 uses attachments or URLs, but rarely a mix of both in a single campaign.

Figure 3: Email lure impersonating the Taiwan Centers for Disease Control and appearing to be from its director, Jih-Haw Chou

In early June 2020, Proofpoint observed a shift away from law enforcement lures as TA2719 began to use more common bank, shipping, and purchase order lures (Figures 4, 5).



SEB Bank <notifications@seb.se> To undisclosed-recipients:;

inkommande betalningsmeddelande från en tredjepartsbank 07/07/2020 à 11:11

SEB Privat Företag Bli kund → Kundservice →

Attn: Kund,

På begäran av den betalande banken.
Detta informerar dig om att en betalning har planerats till ditt bankkonto med check.

Här är informationen om transaktionen:

Avsändare: Svenska Handelsbanken AB

Transaktions-ID: CBS-2847323434

Förväntat leveransdatum: 07/07/2020

Kategori: Betalningskontroll

Bekräfta kontoinformationen i den bifogade filen så att vi kan slutföra betalningen.

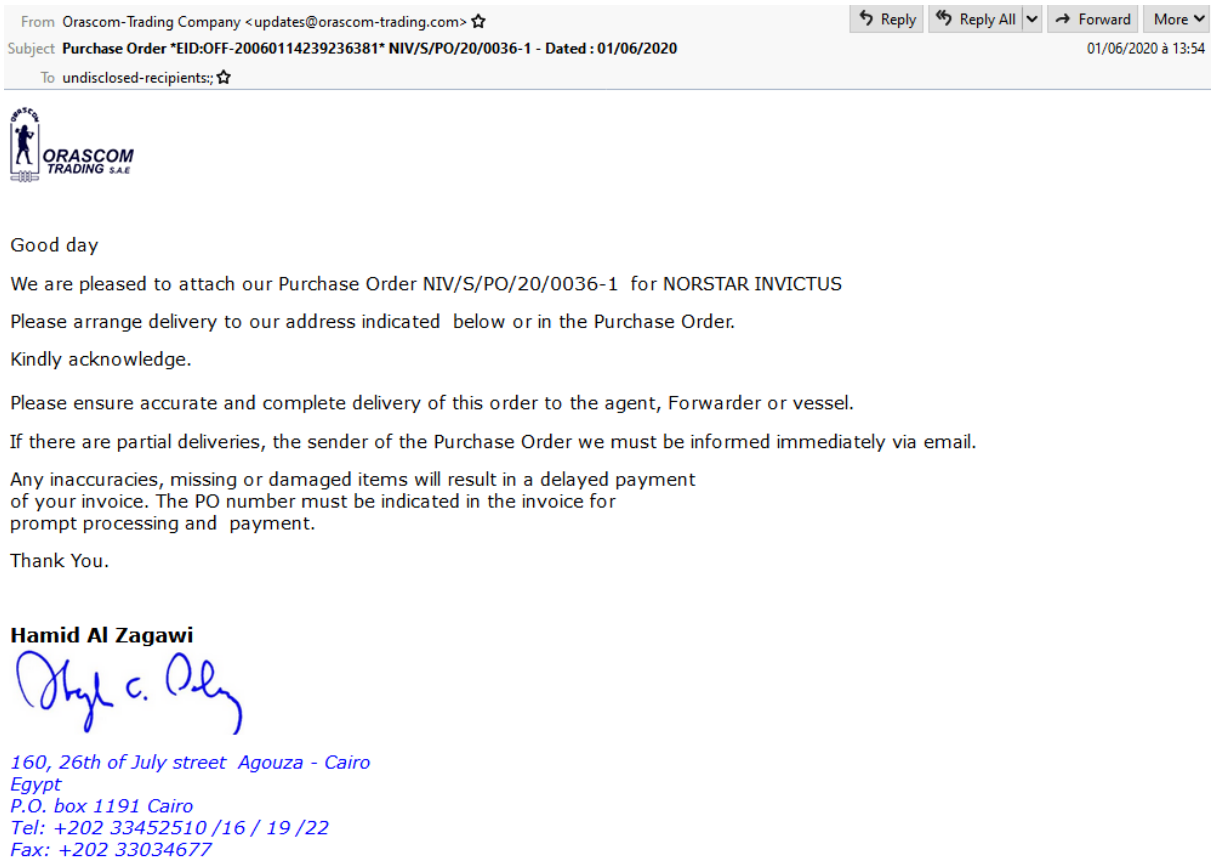
Hälsningar.

Maja Karlsson

0771-365 365
Kungsträdgårdsgatan 8,
111 47, Stockholm

SEB Group

Figure 4: Swedish email lure impersonating SEB, with subject, "incoming payment notification from a third party bank"



From Orascom-Trading Company <updates@orascom-trading.com>
Subject **Purchase Order *EID:OFF-20060114239236381* NIV/S/PO/20/0036-1 - Dated : 01/06/2020**
To undisclosed-recipients:;

Reply | Reply All | Forward | More

01/06/2020 à 13:54

ORASCOM TRADING S.A.E

Good day

We are pleased to attach our Purchase Order NIV/S/PO/20/0036-1 for NORSTAR INVICTUS

Please arrange delivery to our address indicated below or in the Purchase Order.

Kindly acknowledge.

Please ensure accurate and complete delivery of this order to the agent, Forwarder or vessel.

If there are partial deliveries, the sender of the Purchase Order we must be informed immediately via email.

Any inaccuracies, missing or damaged items will result in a delayed payment
of your invoice. The PO number must be indicated in the invoice for
prompt processing and payment.

Thank You.

Hamid Al Zagawi

160, 26th of July street Agouza - Cairo
Egypt
P.O. box 1191 Cairo
Tel: +202 33452510 /16 / 19 /22
Fax: +202 33034677

Figure 5: Email lure with fraudulent purchase order from Orascom Trading

Lures continued to be bank-themed in late June, with subjects like, “Εισερχόμενη επιταγή πληρωμής (Incoming payment notification)” (Figure 6).

Figure 6: Email lure impersonating a Greek bank

As of mid-July, TA2719 shifted to exclusively using package delivery lures, impersonating shipping companies and using subject lines like, “Your parcel from Mrs. Garn has arrived at our office,” or “您从中国寄来的包裹已经到了我们办公室（陈先生的包裹）”(The package you sent from China has arrived at our office (Mr. Chen's package)” (Figure 7).

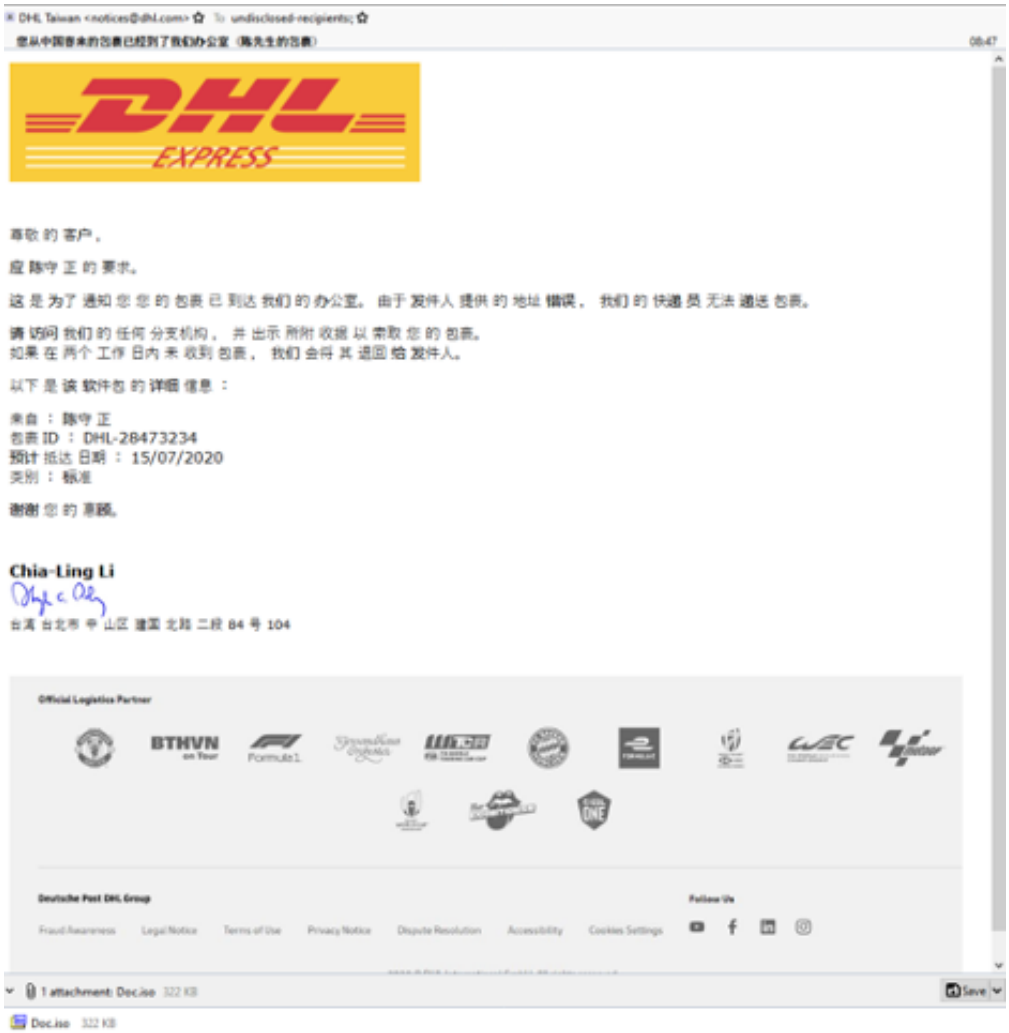
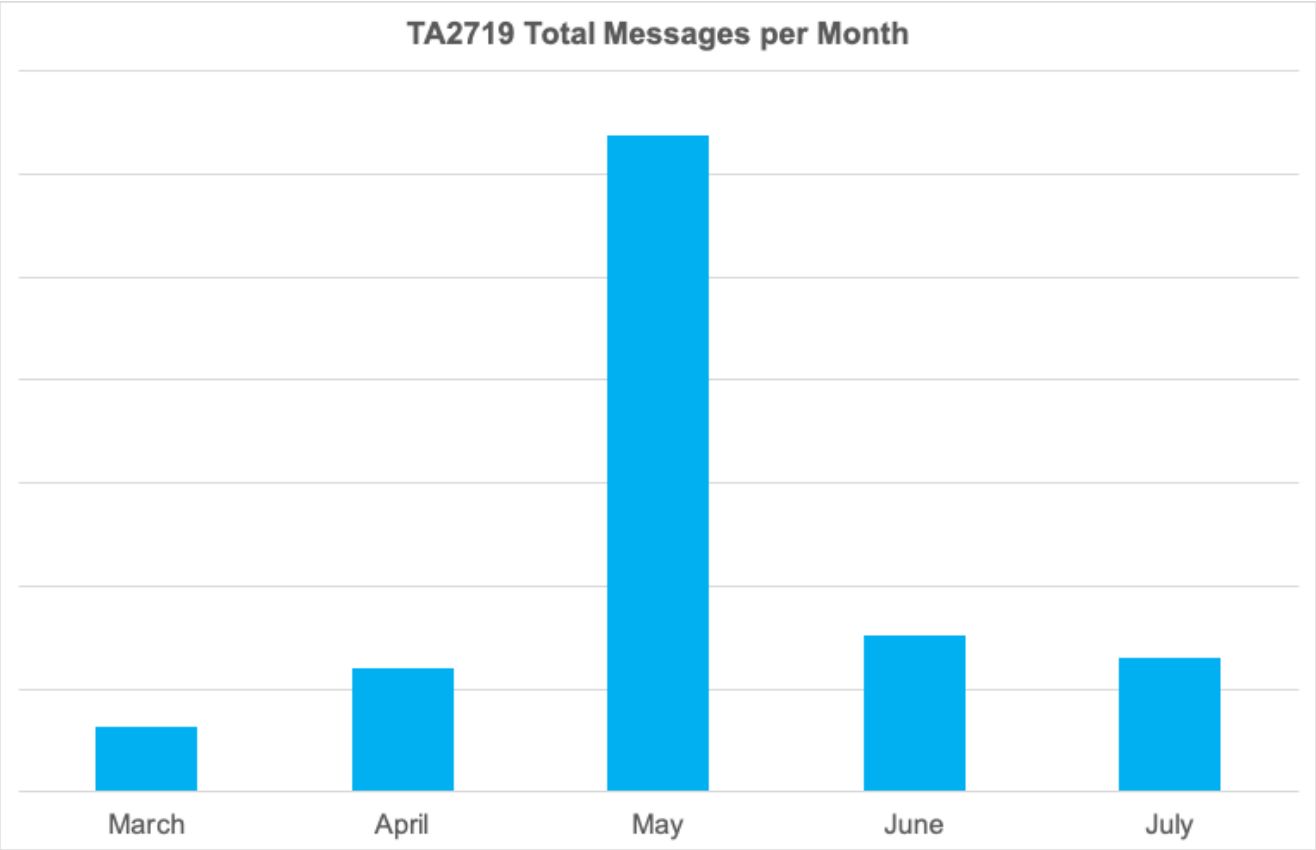


Figure 7: Email lure with fraudulent package notification

Volume

Campaign message volume has been relatively low, with a few dozen or few hundred messages per campaign. Total monthly message volume peaked in May but has since returned to levels closer to those observed in March and April. Since late March, Proofpoint has observed several TA2719 campaigns per month. The message volume spike in May was driven by fewer campaigns with over 2,000 messages each, rather than multiple smaller campaigns seen in other months.



Targeting

Though the campaigns don't appear to have any vertical targeting, they are carefully crafted for specific regions. Various languages and references to legitimate local entities, such as banks or law enforcement organizations, have been observed:

Country	Language	Lure Themes Observed
Austria	German	Police
Chile	Spanish	Shipping
Greece	Greek	Police, banking
Hungary	Hungarian	Police, banking
Italy	Italian	Police
Netherlands	Dutch	Police

North Macedonia	Macedonian	Police, shipping
Singapore	English	Police
Spain	Spanish	Police, shipping
Sweden	Swedish	Police, banking
Taiwan	Chinese	CDC, shipping
Thailand	Thai	Police
Uruguay	Spanish	Police
United States	English	Shipping

Intended recipients often have easily searchable profiles online, and TA2719 also sends to role-based email addresses. This suggests that there is little targeting at the individual recipient level, but that the recipient lists may be more opportunistic in nature and compiled using basic OSINT techniques.

Delivery and Payload

From March to early July, NanoCore was distributed primarily through emailed ISO file attachments. Several campaigns instead used URLs linking to malicious ISO files. Finally, sometimes the actor attempted to deliver a mix of attachments and URLs in the same email. When using URLs, ISO files were hosted on compromised sites or file hosting services.

In mid-July, the actor pivoted from distributing NanoCore to AsyncRAT, another commodity RAT. Like NanoCore, AsyncRAT has been advertised on forums and as of May 2020, appears to still be under active development with new features released May 10, 2020.

Across all campaigns observed by Proofpoint, the ISO files had a generic name, such as ‘Document.iso’ or ‘pdf.iso’. Once the user opens the ISO–which opens like any other folder on the computer–they then must double click the malware executable file inside to run it.

The C&C hostnames and IPs used by TA2719 appear to be relatively stable, changing roughly once per month. This actor sometimes uses free dynamic DNS (DDNS) providers for their C&C.

Conclusion

While not the most advanced lures we've seen, the localization and inclusion of legitimate street addresses and names of real individuals related to the spoofed entities demonstrate this actor's attention to detail. Though TA2719 does not appear to target any particular industry, they tailor their messages to various geographies and send medium-volume campaigns several times per month. Their use of free DDNS providers, reuse of infrastructure, and reliance on commodity malware demonstrate the ease with which threat actors can begin and maintain an operation.

IOCs

NanoCore
Attachment
SHA256: 6489bbcdd9e0588d6e4ee63e5f66346e7d690ac3b7ee5249436fb1db8abc6453
Malware SHA256: 1b93790c002d5216822277c6b8abb36dfd5daf9ebc14553135c992f64f8d949e
C&Cs: 172.111.188[.]199, megaida123.ddns.net

AsyncRAT
Attachment
SHA256: 161eaa18e31aec64433158da81eea99e518659e06ed36e2052508a7cbeb688c6
Malware
SHA256: bcc0be90110b3b960230a366f1be67904704f87645ff5fde69536432d73feace
C&C: 194.5.98[.]8

ET + ETPRO Signatures

NanoCore:
ETPRO MALWARE NanoCore RAT Keep-Alive Beacon - 2816718

AsyncRAT:
ETPRO MALWARE Observed Malicious SSL Cert (AsyncRAT Server) - 2836595

Additional References

Vendetta-new threat actor from Europe

Fake emails in the name of the Spanish national police

Subscribe to the Proofpoint Blog