Agent Tesla Targeting United States & Australia: Revealing the Attackers' Identities

By ramanl

Published: 2024-04-02 · Archived: 2026-04-09 02:00:15 UTC

Research by: Antonis Terefos, Raman Ladutska

Part I from the series E-Crime & Punishment

Introduction

When considering a notoriously famous topic known for quite a long time, it may feel like there is nothing new to add to this area anymore – all paths traced, all words said, all "i"s dotted. Is it worth an investigation to begin with? As it turns out, there are new discoveries with previously hidden information of valuable significance that can be built into the already-painted picture.

In this research series conducted by Check Point Research (CPR), the **Agent Tesla** malware acts as the master villain. It is an example of an advanced remote access trojan (**RAT**) specializing in the theft and infiltration of sensitive information from infected machines. This malware can collect various types of data, including keystrokes and login credentials used in browsers (such as Google Chrome and Mozilla Firefox) and email clients used on infected machines. Agent Tesla is a malware family with a rich and infamous history in the cyber landscape: it has been repeatedly included in the monthly reports of top 10 prevalent malware families since 2020.

A Deadly Agent (Tesla)

Check Point Research uncovered a recent malware campaign of Agent Tesla operation aimed against **American** and **Australian** organizations. On the 7th of November 2023, an Agent Tesla campaign started against Australian organizations, and the same actor performed another campaign targeting mainly Australian entities. Phishing campaigns mainly target organization **email credentials** to access entities and perform further campaigns but with the next goal, to execute the malware samples of Agent Tesla. In this case, the attack base constituted **62,000 emails**. 2 subsequent spam campaigns were launched on the 8th and 30th of November.

After further investigation, CPR tracked down the activity of **2 cyber-crime actors** behind Agent Tesla operations with the evidence of being connected with each other:

- Bignosa (main threat actor)
- Gods

The main actor appears to be a part of a group operating malware and phishing campaigns, targeting organizations, which is testified by the US and Australian email business databases, as well as individuals. Apart from campaigns originating from companies' victims, the group maintains a large number of servers, which are

used either for **RDP** connections or for malware campaigns using **Round Cube** – separate machines are used for consequent steps in the cyber-operations.

The malicious campaigns were all conducted in the same manner. The spam emails are prepared abusing the formal mail from with the topic of purchasing goods and order delivery, social engineered in a way to increase the probability of the victim to click the button and initiate the infection chain.

Upon clicking on the email, the Agent Tesla sample protected by the **Cassandra Protector** is downloaded to the victim's machine and executed. The Cassandra protector is designed to work exclusively with .NET samples and introduces various features: anti-AV and anti-emulation tricks or signing the resulting file with the certificate – to name a few. We will describe this protector in more details in the section linked to the "Bignosa" actor.

Below, we present the details of the investigation, reveal clues that allowed us to draw connections between various pieces of information, make breakdowns of steps and timeframes during the malicious campaigns, link actors with each other, and uncover their identities.

Campaigns

The malware campaigns were meticulously prepared, rather than simply initiating the spam with a single click, The diagram below shows the times of preparation and execution steps:

Image 1 – Activity of the "Bignosa" threat actor shown on the timeline

Phishing texts used in these campaigns appear to be taken from the following sites:

- https://www.dailylifedocs.com/sales-letter-samples.html
- https://www.writeexpress.com/

Malware campaigns 7-8th of November

On the 7th of November, the main threat actor "Bignosa" launched a malware campaign targeting more than 11,000 Australian companies. The actor **possesses** email databases focused on different attack targets, and for this campaign, Australian recipients have been chosen:

- US Businesses (”USA Database 2.txt”)
- AU Businesses (”AU B2B Lead.txt”/”Australia Mail list.doc”)
- Educational (”Edu Email.txt”)

The campaign was performed by “Bignosa” using the email support@chserver.top with an attachment PDF.IMG, which is a disguised Agent Tesla sample, is protected with the Cassandra Protector.

Image 2 – Malware campaign targeting AU 7th of November

The server `chserver.top-172.81.60.206` is a server that belongs to the actor, he installed Plesk and Round Cube to perform the campaign on the previous day at 19:57:46. “Bignosa” connected to it with SSH using an IP from Kenya `41.90.185.44`. The actor used RDP to connect to the machine `91.215.152.7`, logged in to Webmail, and launched the spam campaign.

Image 3 – RDP connection to 91.215.152.7 to connect to the mail server

The principal scheme of this operation is shown in the diagram below:

Image 4 – Attack scheme for these two campaigns

Malware campaign 29-30th of November

On the 29th of November, the threat actor from `41.90.177.10` connected via SSH to `192.236.236.35` and installed Plesk & Round Cube once again. Using his Bulgarian RDP connection, `91.215.152.7`, he created an email address and logged into Webmail. Around 16:00, the machine was ready for the campaign.

Image 5 – Test email after installation

On the 30th of November, “Bignosa” executed the campaign targeting multiple organizations in Australia and United States. The file attachment was once again an Agent-Tesla with the same C&C as the campaign earlier in the month.

Image 6 – Malspam text and attachment

The principal scheme of this operation is shown in the diagram below:

Image 7 – Attack scheme for this campaign

The schemes are similar in both campaigns except for the addresses of the server where Plesk and RoundCube were installed – these are the only differences between the attacks.

Cassandra Protector

During both campaigns “Bignosa” used Cassandra Protector to obfuscate the samples’ initial code and later convert the executables into ISO. The actor has been a customer of Cassandra Protector since 24/6/2023 (with that specific email):

Image 8 – "Bignosa" account details for Cassandra Protector

Cassandra Protector has been used to "protect" 67 samples:

Image 9 – Actor's protected samples, time, and filename – dates correlate with the campaigns launch time

Cassandra Protector supports only .NET samples and provides various functionalities such as (as described on the sales site):

1. Injection method.
2. Persistence method.
3. Anti-Virus & Emulation.
4. Delaying execution.
5. Signing protected with a Certificate.
6. Icon Change.
7. Pop-up message box with custom text.
8. Custom Assembly features.
9. Create and execute downloader.

10. Protection options.

Image 10 – Cassandra Protector options

Cassandra Protector allows the end user to choose a file to be downloaded and/or executed after launch, lets configure sleep time before continuing execution and choose a fake message box to be shown.

Under the hood the Protector has the capabilities of putting itself to Defender exclusion via `Powershell:Add-MpPreference -ExclusionPath` command. It can *copy* itself to the "AppData" folder, set the file as `hidden/system` and set a new ACL (Access Control List). For persistence Cassandra Protector adds the file to Scheduled Tasks.

The injection option is also configurable, it can be a PE Hollowing or .NET Reflection to itself:

Image 11 – Cassandra Protector "Injection Persistence" options

Once the sample was "protected", the actor used ISO Burner to convert the .NET into an ISO file with ".img" extension and attached the resulting file to spam emails.

Threat actors

We have covered the technical aspects of the campaigns; now we will examine the profiles of threat actors linked to these campaigns, starting with the main one – "Bignosa."

First Threat Actor – Bignosa

The Threat Actor "**Bignosa**" was behind the described campaigns. "Bignosa" appears to have been using Agent Tesla for quite a while and performing phishing attacks in the past as well.

This actoruses another alias as well as a name which gives an indication of where he is originally from. The nickname that was also observed was **Nosakhare** which is of Nigerian origin and means *"What God say will be/is destiny"*.

The further profile description is tightly connected with the other Threat Actor who appears to be assisting "Bignosa" in allegedly taking the first steps into the malware world on the rights of a seemingly more experienced one. The nickname of the other Threat Actor is "Gods." A bright example of the interaction between the two is shown on the Skype excerpt where "Bignosa"gets advice from "Gods" (`live:.cid.1b6f75099c70b269`) regarding which malspam text to use for the campaign.

Image 12 – "Gods" provides a text to be used in the malicious campaign to "Bignosa"

The actors have been observed to communicate via Jabber – a service for instant messaging via an open protocol used since 1999 – where, in multiple instances, “Bignosa” wasn’t able to clean his machine from the Agent Tesla test infections and provided a Team Viewer access to “Gods” for assistance in cleaning up the machine.

Image 13 – Bignosa & Gods Jabber conversations

The following screenshot shows how “Gods” connected via Team Viewer to the “Bignosa” machine to remove Agent Tesla infection:

Image 14 – “Gods” in the process of removing Agent-Tesla test-infection from the “AppData” folder

Initially, we considered the collaboration between “Bignosa” and “Gods” to be solely in the form of a “student-mentor” role model. However, later findings suggest a closer collaboration between the two actors and show evidence of them performing as a group. We will get back to this after we take a closer look at the profile of the “God’s” threat actor right in the next section.

We summarize the information mapped to the activities of “Bignosa” in the diagram below:

Image 15 – The map of traces linked to “Bignosa”

According to the name “Nosakhare” that was used by the threat actor, the “NG” acronym in Skype, Kenyan traces in the malicious campaigns, and several other clues – we can draw a conclusion that we’re dealing with a Kenyan

man Nosakhare Godson. There is a LinkedIn profile revealing the photo of this person:

Image 16 – LinkedIn profile of Nosakhare Godson

Other bits of interest to add to his profile come from examining his RDP desktop:

Image 17 – RDP desktop with many links to examine

We can spot three other malware families on this desktop: **Quasar**, **Warzone,** and **PureCrypter**. Quasar and Warzone are available in the public access, and Quasar is even open-sourced, so the “modified” suffix in the folder name implies that the malware code could be edited to suit the needs of the actor. There is a tutorial in a separate file describing the usage of PureCrypter.

There are separate files with the emails of Australian and miscellaneous customers, as well as the whole folder with the USA victims. *Grammarly* is also part of the actor’s toolkit in his spam activities. *SuperMailer* is seen as (likely) the test tool as it was not used in the malicious campaigns. The application was not bought as evidenced by the crack for it also seen in the desktop – probably to save money whenever possible for maximum profit from malicious activities. Another piracy evidence is the folder with the name “activator.”

Having familiarized ourselves with the main actor, it's time to investigate the activities of the one using the "Gods" alias – the mentor of "Bignosa".

Second Threat Actor – Gods/Kmarshal

This Threat Actor has been performing phishing attacks since March 2023 and then transitioned to malspam and malware operations around June 2023. Those phishing attacks appear to have been reporting the data to "logteam@netc.eu":

Image 18 – Phishing attacks with the email logteam@netc.eu used by "Gods" threat actor

The campaign conducted around June 2023 involved several widely used services, Microsoft sign-in form as one of the vivid examples:

Image 19 – The phishing page and the code behind it

On the 15th of August "Gods" appears to have performed a malware campaign connecting via RDP to VDS server `79.110.48.6` and then to Webmail. This campaign targeted a mix of Australian and UK companies using "Agent

Tesla” as well.

This actor uses two nicknames more frequently than the others – “Gods” and “Kmarshal” – as present in the threat actor’s Jabber account:

Image 20 – “Gods” and “Kmarshal” in one Jabber account

This fact potentially allows us to assume that there could possibly be, at least two persons behind this threat actor. However, future findings proved that all the nicknames belonged to one person. Let us see the clues we have gathered regarding this threat actor.

We identified that two machines related to “Gods”had usernames with prefixes “**km**” and “**KM**”:

Image 21 – "KM" prefix in the machine name

One of the machines has the name "**KM-MacBook-Pro**". He is part of a chat group in Jabber where 10 other contacts are present:

We found that the email that is used by "Gods" threat actor – `unlimitedsendertech@gmail.com` – appears to be the same as from the YouTube channel "8 Letter Tech":

Image 23 – email address of “Gods” on the YouTube channel

This channel contains videos on setting up RoundCube and Zimbra Mail:

Image 24 – “8 Letter Tech” channel on YouTube

The same email appears in one of the videos on the channel:

Image 25 – The “Gods” registration email appears in the video

All of this means that the channel is directly related to the “Gods” threat actor.

Alas, these facts did not help us with de-anonymizing the actor. At this point, we decided to summarize all the data bits we had about him:

Image 26 – The map of traces linked to “Gods/Kmarshal”

The interesting fact is that although there are a lot of Turkish IP addresses. These addresses are likely connected with the past of the actor where he must have studied at the Turkish university – as evidenced by our later findings. The actor does not speak Turkish and uses ChatGPT via an RDP machine to translate spam messages to this language:

Image 27 – ChatGPT used to translate spam messages to Turkish

Before we proceed with the de-anonymization of “Gods,” let us first investigate a close connection between “Bignosa” and “Gods,” extending more than a “student-mentor” relationship.

Collaboration between the “Bignosa” and “Gods”

Let us consider the following receipt, which is VDS paid by “Bignosa” under one of his aliases, “Andrei Ivan”:

Image 28 – Swiss VDS paid by “Bignosa”

As a side note, the same phone number as in the receipt is used for 2FA for his “work” Gmail account. What drew our interest besides this fact was the history of VDS account operations:

Image 29 – History of operations for the VDS

We spotted the “sterdiffa-steel.ddndsfree.com” site that has its IP set to one used by “Gods” – 80.68.159.15:

Image 30 – Dynamic DNS service used by “Gods”

We know this IP belongs to “Gods” from the fact that the email used in DynuDNS service is the one linked to him:

Image 31 – DynuDNS service account with the email used by “Gods”

Also, we spotted an administrator change. At first, the administrator email was set to the address used by “Bignosa” – “lwork6356@gmail.com”:

Image 32 – The administrator address set to the email of “Bignosa”

Within 2 days, this Plesk instance “changed” hands and went under the government of “Gods” with his address “unlimitedsendertech@gmail.com”:

Image 33 – The administrator address set to the email of "Gods"

We managed to link their collaboration as early back as March 2023 when they performed phishing attacks targeting email credentials. The earliest indications for the use of malware in their campaigns appear to be in June 2023.

Further connections and de-anonymization via social media

In the course of the investigation, we saw relations in these attacks to the following previously unseen nicknames:

1. GODINHO
2. TAMEGURUS

We will focus on the 2nd one as it is crucial for the research, as it turned out to be. *TAMEGURUS* appears to be related to *Tamedevelopers* according to the search in Google:

Image 34 – "Tamegurus" tag encountered in the TikTok account

Only one video from the TikTok network has this tag, and in this video, the author speaks about an ongoing web project for the actor's legitimate job in relation to Chinese customers:

Image 35 – “Tamegurus” tag in the video related to Chinese customers

It’s important to state that this activity is not related to the malicious one, on the contrary, it is a part of this legitimate job, a web-design project related to China, hence we see this connection.

On another social media network, Instagram, we find the account of “tamedevelopers”, who is a Web Designer from Nigeria somehow connected to Turkey:

Image 36 – "Tamedevelopers" account on Instagram

From earlier on, we saw that a lot of Turkish IP addresses were connected to "Gods". @Tamedevelopers' account on the social network Fiverr, where he goes by his name Fredrick Peter, demonstrates the clue to such a connection: he studied at the Turkish University, and the threat actor "Gods" probably studied there as well:

Image 37 – "Tamedevelopers" account on Fiverr

@Tamedevelopers is followed by another Instagram account *@8LetterStudio* (remember that "8 Letter Tech" is the YouTube channel), where a post mentioning him was made:

Image 38 – Post by “8LetterStudio” mentioning “Tamedevelopers”

@8letterstudio, in its turn, is being followed by another known name – @king_kmarshal (King KM), which is frequently used by “Gods”:

Image 39 – “king_kmarshal” following “8LetterStudio”

We feel like we are on the right track, as many details are starting to link together. The next step is to search for “8 Letter Studio” in other social media, for example, Facebook:

Image 40 – “8LetterStudio”page on Facebook

We see the connection to Chinese customers right at the top post on the page, just what we started with when we encountered the “Tamedevelopers” account in TikTok. As we mentioned previously, this part is probably related to his legitimate job – a web-design project related to the customers from Hong Kong.

On this page, we see that in 2015, it was created under a different name:

Image 41 – “Kmbrand Design” is the former name for “8 Letter Studio”

Searching for the name “Kmbrand Design” we encounter the page on Fiverr network:

Image 42 – “kmbranddesign” in the Fiverr network

He states his knowledge of Turkish is basic, which explains the usage of ChatGPT for translation:

Image 43 – Language knowledge of Kingsley F

The videos on his page are the same as on the YouTube channel “8 Letter Tech”. At one point, the email `unlimitedsendertech@gmail.com` – used by “Gods” – is seen in the video:

Image 44 – Email used by “Gods” in the video by Kingsley F

Now the things are really getting hot. We almost know the name of “Gods”. Further search leads to the page on Behance network (that uses the same profile photo as in the Fiverr network) which explains the relationship

between “tamedevelopers” and “Gods” – he must be part of the web-designers team:

Image 45 – The profile of Kingsley Fredrick on Behance network

This page also reveals the name of the man behind “Gods” alias – Kingsley Fredrick. Yet another cross-link connection to the beginning of de-anonymizing research is the Instagram profile of this man following “tamedevelopers”:

Image 46 – The profile of Kingsley Fredrick on Instagram network

Recent Activity, 6th March

The story of the described threat actors is not yet finished; on the contrary, it’s just getting started. We have spotted them launching a phishing campaign in December 2023 and January 2024. One the 6th of March 2024 one of the organizations that was mimicked during this attack is the Furman University in South Carolina:

Image 47 – The phishing page and the code behind it

We linked this campaign to the “GODINHO” alias (remember the start of the de-anonymization process for “Gods”), which appears to be yet another skin for the “Gods” actor. Several HTML pages used in this attack are uploaded to VT with the following hashes:

- 8ba55cc754638714764780542eefd629c55703ecf63ae20d5eb65b8c14d3e645
- 87709f72683c5ffc166f348212b37aadb7943b5653419f2f0edf694fb50f1878
- 691761d401a6650872d724c30b7ef5972e3792e9a2ba88fdca98b4312fb318d8

We can surmise that legal activity like web design is not enough, as when it comes to making profits, any means of additional income, even those not so innocent in nature, will suffice for the cyber-crime actors – be it malware usage or classical phishing. We continue to monitor the ongoing activities of evil-oriented minds and are actively collaborating with the legal authorities to stop this group and other threats.

Conclusion

As seen from the description of these threat actors’ actions, no rocket science degree is required to conduct the cyber-crime operations behind one of the most prevalent malware families in the last several years. It’s an unfortunate course of events caused by the low-entry level threshold so that anyone willing to provoke victims to launch the malware via spam campaigns can do so.

There is an upside to this though: multiple traces left by cyber-crime actors allowed us to pinpoint them, re-create their actions, and get a peek into their daily activities. There are occasional data pieces on the web: seemingly tiny and unimportant pieces of data can sum up the big picture and reveal the truths that usually prefer to remain hidden. In this case, these pieces allowed us to reveal the identities of cyber-crime actors from Africa, re-create steps and timeframes when the main actor conducted his malicious campaigns, understand the pattern, and provide protection against these and future attacks. The power of social media blossomed in all its beauty to help us in the chase.

CPR managed to predict and prevent occurring as well as future campaigns targeting our customers. As a note of importance, we have worked closely with law enforcement on this investigation. The research about Agent Tesla will continue in the 2nd part of the series, stay tuned for the updates!

Recommendations

This research highlights the importance of vigilance in cybersecurity. The identification of these threat actors was made possible through meticulous analysis of digital footprints, demonstrating the power of digital forensics.

To mitigate the risks of being affected by such threats, it is essential to:

– Keep operating systems and applications updated, through timely patches and other means.

– Be cautious of unexpected emails with links, especially from unknown senders.

– Enhance cybersecurity awareness among employees.

– Consult security specialists for any doubts or uncertainties.

Protections

Check Point customers remain protected against the threat described in this research.

Check Point Threat Emulation and Harmony Endpoint provide comprehensive coverage of attack tactics, file-types, and operating systems and protect against the type of attacks and threats described in this report.

- Spyware.Win32.Tesla.TC.*
- AgentTesla.TC.*

IOCs

Alias	Personal/VPN IPs	Associated Emails/Jabbers	Associated Phones	Malicious Infrastructure
Bignosa	105.160.122.192 105.161.75.138 105.161.81.79 197.237.92.228 41.90.176.165 41.90.177.10 41.90.179.140 41.90.180.123 41.90.180.219 41.90.181.104 41.90.185.44 41.90.186.173	admin@dllserver.top andrewbailey@sent.com baileyandrewjr@mailo.com contact@chserver.top dickson@outlook.com enquires@dllserver.top felixjensen84@gmail.com felixjensenjr@gmail.com felixreederjr@gmail.com iamhere@mailo.com info@chserver.top info@sterdiffa-wat.site	+1 5623757370 +254 105051021 +254 741439531	142.202.190.222 172.81.60.206 192.236.146.12 192.236.194.247 192.236.236.35 80.68.159.15 91.215.152.7

	41.90.186.247 41.90.186.248 41.90.188.113 41.90.189.214 91.215.152.7	iwork@hot-chilli.net lwork6356@gmail.com nosakharegodson@gmail.com peterdave@mailo.com peterdavejr@gmail.com peterdavejr@mailo.com sales@kenyapride.co.ke support@chserver.top support@cloverleave.info support@dllserver.top support@sterdiffa-wat.site		
Gods	147.189.161.184 149.0.216.243 149.0.91.214 176.218.220.145 192.223.25.77 192.223.25.85 212.133.214.104 31.155.119.217 46.2.179.191 46.2.181.103 46.2.254.164 46.2.35.156 79.110.48.6 84.38.130.226 91.92.244.255	account-security@eutrade.top dfk@dtdc.eu.org gods@openim.eu info@eutrade.top j.klaus@johnokimattorney.eu.org kmarshal101@hotmail.com kmarshal@jabbers.one kmarshal@sure.im legal@johnokimattorney.eu.org logteam101@gmail.com logteam@netc.eu msgate@net-c.ca no-replu@hlgroup.eu.org no-reply@hlgroup.eu.org noreply@grillminings.tech onye.oma50@gmail.com smtps@hlgroup.eu.org unlimitedsendertech@gmail.com	+1 7024041730	142.202.188.238 147.189.161.184 156.227.0.187 45.38.135.112 79.110.48.6 80.68.159.15 84.38.130.226 91.210.166.29

Source: https://research.checkpoint.com/2024/agent-tesla-targeting-united-states-and-australia/