

Nigerian Tesla: 419 scammer gone malware distributor unmasked

blog.malwarebytes.com/threat-intelligence/2022/05/nigerian-tesla-419-scammer-gone-malware-distributor-unmasked/

Threat Intelligence Team

May 5, 2022



Agent Tesla is a well-known data stealer written in .NET that has been active since 2014 and is perhaps one of the most popular payloads observed in malspam campaigns.

While looking for threats targeting Ukraine, we identified a group we call “Nigerian Tesla” that has been dabbling into phishing and other data theft activities for a number of years. Ironically, one of the main threat actors seemingly compromised his own computer with an Agent Tesla binary.

In this blog, we expose some of the activities from a scammer who started off with classic advance-fee schemes and is now successfully running Agent Tesla campaigns. In the past two years, this threat actor was able to collect close to a million credentials from his victims.

Spam campaign

Our investigation started with an email targeting titled *Остаточний платіж.msg* (Ukrainian for *Final payment.msg*). It contained a link to a file sharing site that downloads an archive containing an executable file.

Доброго ранку,

Перевірте доданий документ, щоб підтвердити остаточну оплату рахунку-фактури.
Ваша швидка відповідь буде оцінена, оскільки ми маємо намір платити наступного тижня.

З найкращими побажаннями
Іван Миколайович
Менеджер облікового запису

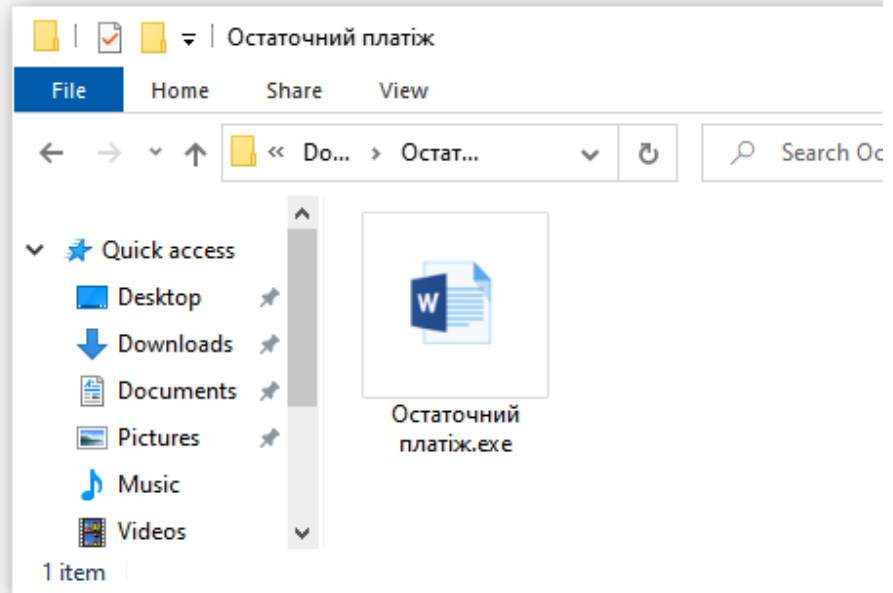
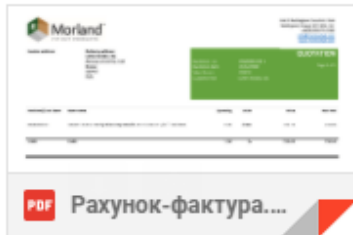


Figure 1: Spam email with Agent Tesla

This executable is actually an Agent Tesla stealer, capable of exfiltrating data in multiple ways, though most commonly using SMTP. The technique is really simple as it only requires an email account that sends messages to itself containing stolen credentials for each victim that executed the malware on their computer.

Test successful!

The attacker sent a number of messages containing the body “Test successful!” from the same machine. Those emails should have been deleted for obvious reasons but this threat actor did not and leaked his own IP address allowing us to locate them in Lagos, Nigeria.

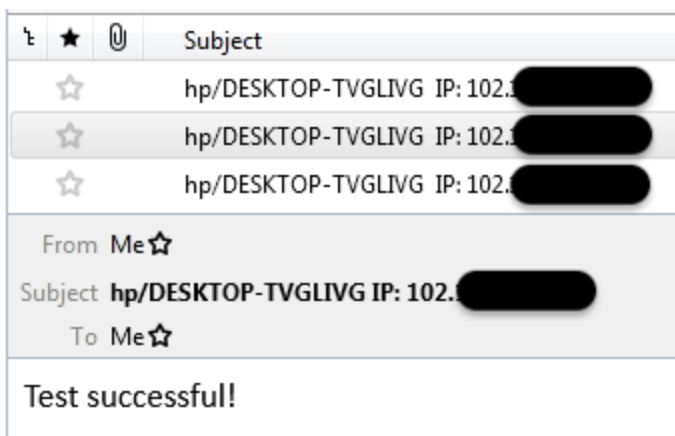


Figure 2: Test emails sent by the attacker

These messages are checks done by the threat actor to make sure communication with Agent Tesla is configured properly. This is typical and is often described in hacking forums where users ask for help with the 'software'.

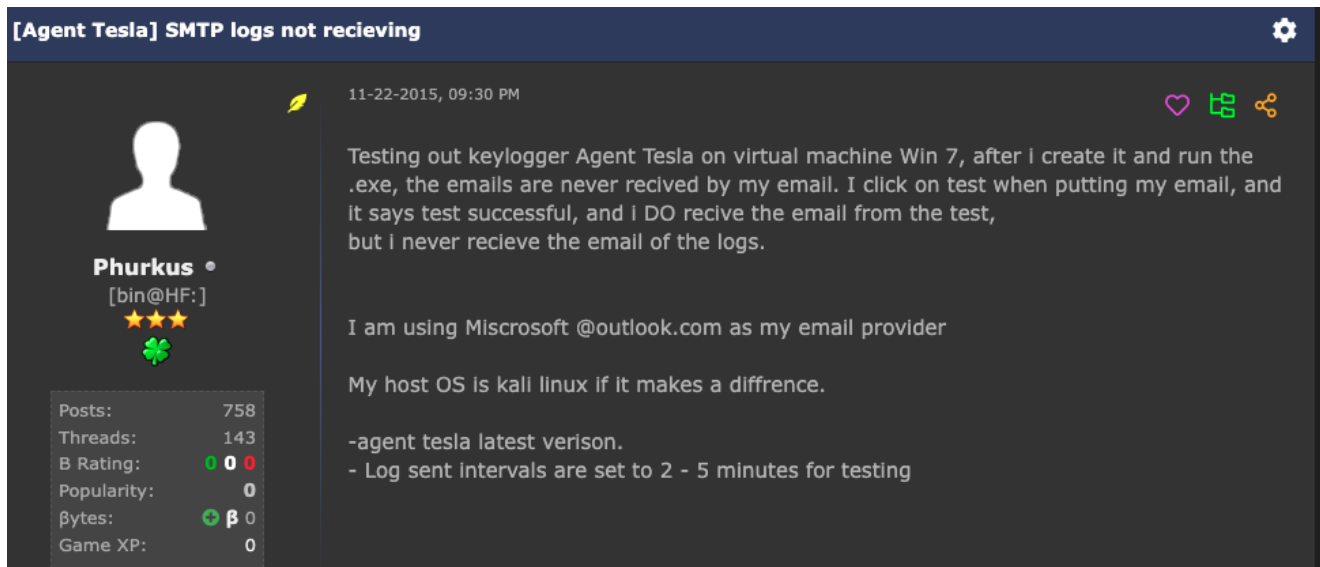


Figure 3: Forum post complaining about issue not receiving logs

There were an additional 26 emails sent from the same IP address that weren't test emails but came from a real Agent Tesla execution. We don't know exactly how, but the attacker managed to infect his own machine.

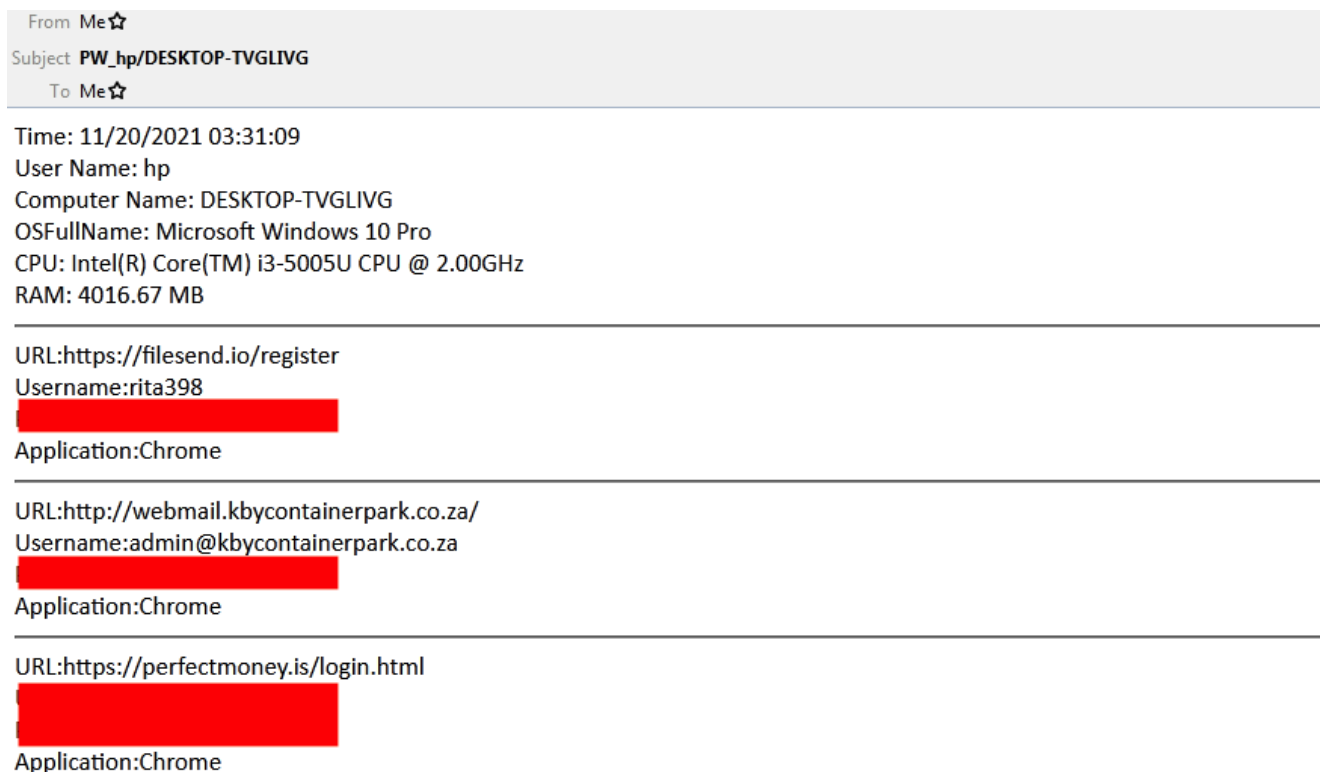


Figure 4: Information exfiltrated from the attacker's machine

Here is a list containing some of the services that the Nigerian Tesla threat actor used:

- PerfectMoney

- Glassdoor signupanywhere (could be a source to get victims emails)
- omail.io (service for extracting emails)
- warzone.ws (Warzone RAT)
- worldwiredlabs (NetWire RAT)
- le-vpn.com and bettervpn.com zenmate.com tigervpn hotvpn (VPN provider)
- securitycode.eu cassandra.pw (Code Protector)
- esco.pw (office document protection)
- monovm hostwinds.com firevps dynu 4server.su (VPS and dedicated servers)
- dnsomatic.com cloudns.net (DNS services)
- spam-lab.su
- filesend.io 4shared (hosting files)
- avcheck.net (offline av test)
- bitshacking.com
- archive.org (used like cloud storage)
- xss.is hackforums.net exploit.in
- titan.email (.pw accounts, various scams)

Rita Bent, Lee Chen and John Cooper are some of the names that have been used in the past along with dozens of different email accounts with passwords containing the string '1985'. The following image shows the activity from user rita398 in hackforums asking about Esco Crypter:

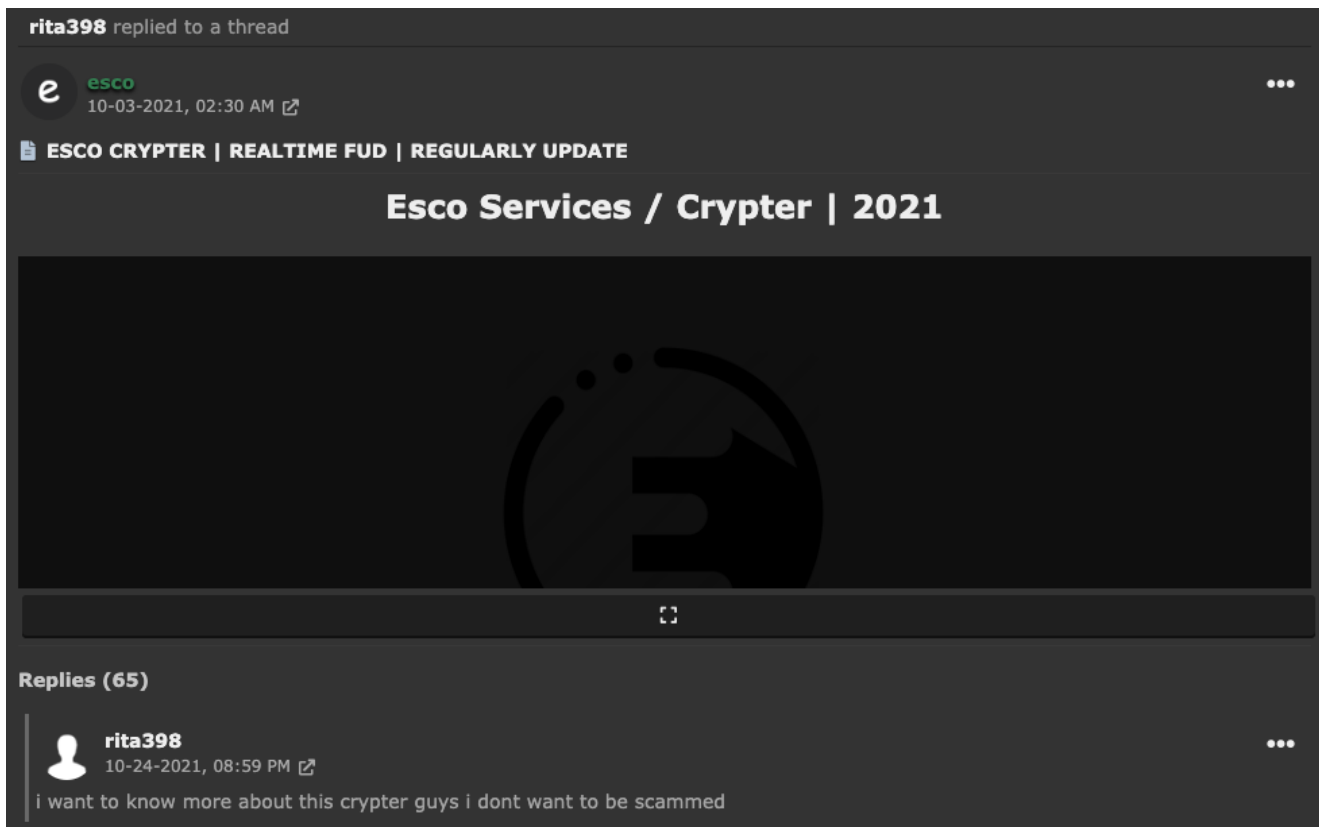



Figure 5: Rita398 interested in Esco Crypter

In that case, we see Rita complaining about some RDP suspension that happened eventually to one of his registered domains.

 rita bent (Owner) 📅 Thursday, August 12th, 2021 (17:49)

Registration Date: Tuesday, June 15th, 2021
Next Due Date: Sunday, August 15th, 2021
Recurring Amount: \$14.95 USD
Billing Cycle: Monthly
Payment Method: Perfect Money
Suspension Reason: We have detected malicious requests from this IP
the reason u gave is not true. i didnt use the rdp for anything like that




Figure 6: RDP shutdown complain

The following email accounts were used in various phishing and data stealing operations:

- along.aalahajirazak.ibrahim@gmail.com
- administracion@romexpert.es
- administracioneforce@eforce.es
- soceanwave244@gmail.com
- barristeradamssetien@gmail.com
- catalinafuster@palmaprocura.com
- david01smith@yandex.com
- davidsmith.ntx31@yandex.com
- davids27smith@yandex.com
- elisabet.valenti@ag.barymont.com
- gestor3@afectadosvolkswagenabogados.com
- info@borrellacerrajeros.com
- info@crmarismas.org
- info@cristaleriagandia.com
- infogestinsur@grupogestinsur.com
- instalaciones@gopamar.com
- isabel@grupoatu.com
- m.lopez@forestadent.es
- nacho@alavigilnevot.com
- restaurante@elsecretodechimiche.com
- soceanwave244@gmail.com
- tienda@di-tempo.com
- torremolinos3@copiplus.es
- v.reino@gooddental.es
- victor@sugesol.com
- vives@viveselectricitat.com

Based on these profiles, we can see this threat actor has an extensive criminal record starting at least from 2014. Back then, they performed classic scams under the Rita Bent moniker.

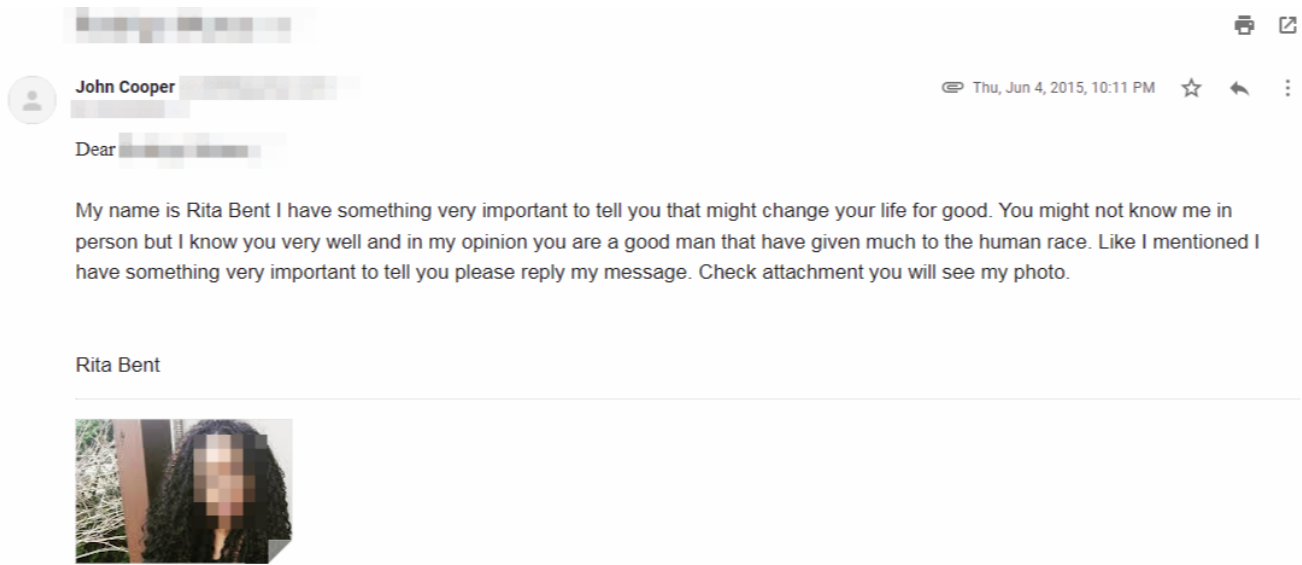


Figure 7: Scam conducted by the same attacker in the past
One of their preferred scams was phishing for Adobe login pages. We have records indicating that several Adobe fake pages were deployed from 2015 until recently. Landing pages looked like the following:

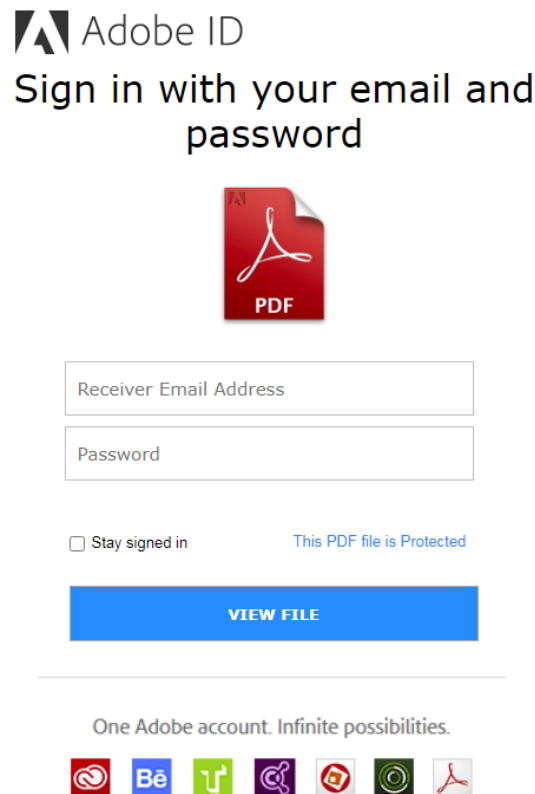
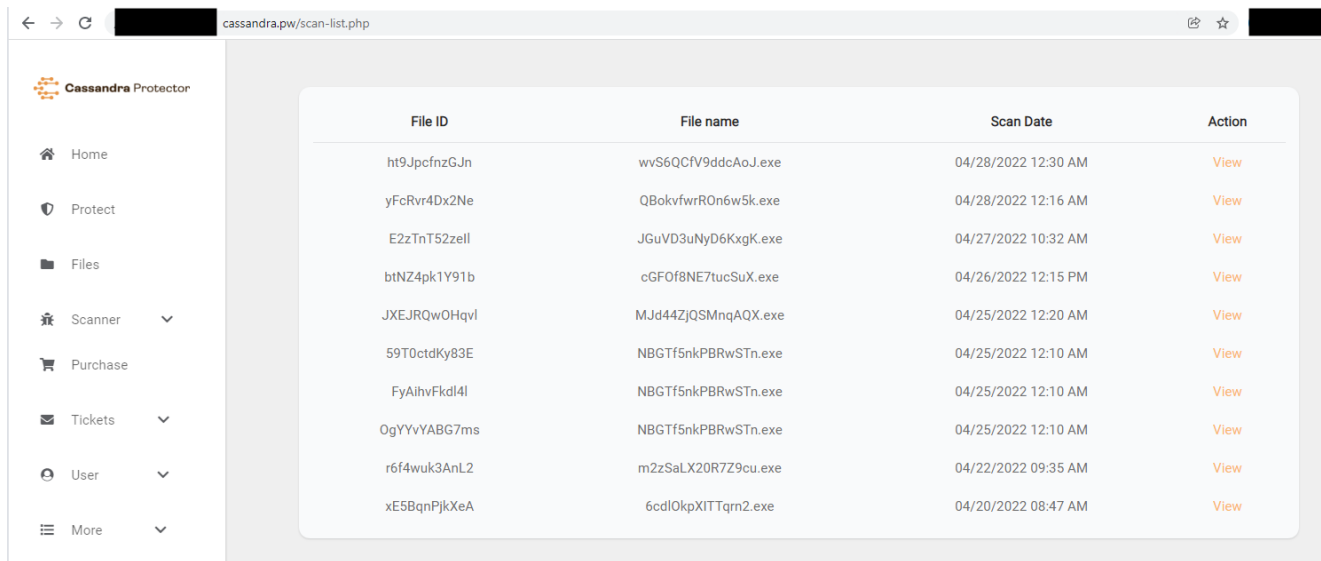


Figure 8: Fake Adobe login page

Fast forward to 2020, and the threat actor has graduated to malware distributor. He protects his binaries with the Cassandra Protector obfuscator and then checks them against AVcheck[.]net.



The screenshot shows the Cassandra Protector web interface. The browser address bar displays 'cassandra.pw/scan-list.php'. The interface includes a sidebar with navigation options: Home, Protect, Files, Scanner, Purchase, Tickets, User, and More. The main content area features a table with the following data:

File ID	File name	Scan Date	Action
ht9JpcfzGJn	wvS6QCFV9ddcAoJ.exe	04/28/2022 12:30 AM	View
yFcRvr4Dx2Ne	QBokvwrR0n6w5k.exe	04/28/2022 12:16 AM	View
E2zTnT52zell	JGuVD3uNyD6KxgK.exe	04/27/2022 10:32 AM	View
btNZ4pk1Y91b	cGF0f8NE7tucSuX.exe	04/26/2022 12:15 PM	View
JXEJRQwOHqvl	MJd44ZjQSMnqAQX.exe	04/25/2022 12:20 AM	View
59T0ctdKy83E	NBGTf5nkPBRwSTn.exe	04/25/2022 12:10 AM	View
FyAihvFkdI4l	NBGTf5nkPBRwSTn.exe	04/25/2022 12:10 AM	View
OgYYvYABG7ms	NBGTf5nkPBRwSTn.exe	04/25/2022 12:10 AM	View
r6f4wuk3AnL2	m2zSaLX20R7Z9cu.exe	04/22/2022 09:35 AM	View
xE5BqnPjkXeA	6cdl0kpXITTqrm2.exe	04/20/2022 08:47 AM	View

Figure 9: Cassandra Protector

File Name	Detection Rate	Result	Scan Date
wvS6QCfV9ddcAoJ.exe	0/26	Clean	04/28/2022 00:30:42

Antivirus	Result
adaware	Clean
ahnlab	Clean
alyac	Clean
avast	Clean
avg	Clean
avira	Clean
bitdef	Clean
bullguard	Clean
clam	Clean
comodo	Clean
drweb	Clean
emsisoft	Clean

Figure 10: AVcheck[.]net

Who is behind these attacks?

The threat actor shared photos of himself back in 2016 and for some reason forgot about them.



Figure 11: Photos of the threat actor

E.K. was born in 1985 according to his driver license. Remember that 1985 was used in a lot of passwords collected from accounts that conducted these illegal activities.



Figure 12: Threat actor's drivers license

At the moment, we do not have much information about other members in the team. But E. K. seems to be the most relevant figure, at least the one who started the scheme.

From 419 scams to Agent Tesla

Nigerian Tesla stole more than 800,000 different credentials from about 28,000 victims. This shows how simple and yet effective running one of these campaigns can be. In this case we see an interesting evolution from a threat actor that was performing the classic advance-fee scam (419 scam) before moving into the malware distribution world, more or less for the same end goal.

Malwarebytes users are protected against Agent Tesla. We detect this sample as Spyware.Password.Stealer.