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

By gmcdouga

Published: 2024-04-03 · Archived: 2026-04-14 02:16:42 UTC

Highlights

- Check Point Research (CPR) uncovered **three recent malicious campaigns** of one of the most prevalent malware in the market – **Agent Tesla**. These operations were aimed against US and Australian organizations and exploited the topics of goods purchasing and order delivery as their lures
- Upon investigation, we discovered that these threat actors had a database of **62,000 emails**, including individuals and organizations from different spheres
- Apart from campaigns originating from victims of companies, the group maintains a large number of servers, which are used for protection of their identity
- Despite the efforts of threat actors to keep their anonymity, CPR **revealed their true identities and source**, re-constructed their steps in the conducted attacks, with continued monitoring of their activity

Long-known malware

Agent Tesla malware is 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 has an infamous history in the cyber landscape, repeatedly included in the monthly reports of top 10 prevalent malware families since 2020.

The Source : Two cyber-crime actors

CPR tracked down the activity of 2 cyber-crime actors behind Agent Tesla operations with the evidence of them being connected with each other :

- "Bignosa" (main threat actor)
- "Gods"

The main actor, "Bignosa" appears to be 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 ordinary individuals. "Bignosa" employed Cassandra Protector for obfuscation and utilized various malware families, signaling a secondary level of cyber-crime tactics and tools.

With a dual identity, "Gods" also known online as "Kmarshal" earlier involved in phishing attacks, later transitioned to malware campaigns. He also demonstrated capabilities in web design and phishing operations.

During our investigation, we tracked the links between various clues, drew connections and secured the identities of these two threat actors, including their pictures from their LinkedIn pages. They appeared to be of African origin, with one of them holding legitimate assignments within their business.

Their technical level looked to be different, with “Gods” being more experienced, and both communicate via Jabber, open technology for instant messaging, with ‘Gods” providing assistance to “Bignosa” in matters of varying difficulty. Using Agent Tesla, however, was not an obstacle for both of them. We also tracked their malicious activity behind Agent Tesla and shared all the discoveries with the relevant law enforcement agencies.

Recent campaigns

The malware campaigns were meticulously prepared, rather than simply initiating the spam with a single click. Utilizing phishing emails with topics related to purchasing goods and order delivery, the attackers attempted to social engineer victims into initiating the malware infection. These emails were sent from the servers deployed by the threat actors right before the campaigns with the main purpose of anonymity. The malware itself was protected by the Cassandra Protector, adding in anti-detection capabilities to make it harder to get caught.

The diagram below shows the times of preparation and execution steps for these attacks:

he principal scheme of the first two operations is shown in the diagram below:

The principal scheme for the third attack is similar to the first ones, except for the different addresses used in the attacking machines:

To get further information and follow our investigation step-by-step with full details around the threat actors discovered, please visit the dedicated page in the Research blog.

Conclusion and 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.*

For more details, visit the CPR blog.
