AzzaSec, NoName Cyberattackers Join Hands to Potentially Target Pro-Ukriane Allies

thecyberexpress.com/azzasec-noname-join-hands-to-target-ukriane/

June 27, 2024

Amidst the ongoing Russo-Ukrainian war, hackers from Italy have decided to join forces with an infamous cyber attacker group in Russia.

Azzasec is an Italian hacktivist group who has been involved in anti-Israel campaigns and has teamed up with the infamous pro-Russian hacktivists Noname057(16). Azzasec has a large network of partner groups, whereas Noname05716 is selective in their allies.

The alliance between these two nefarious groups signifies a potential increase in the scale and sophistication of cyberattacks on Ukraine and its allies.

Understanding the AzzaSec Ransomware

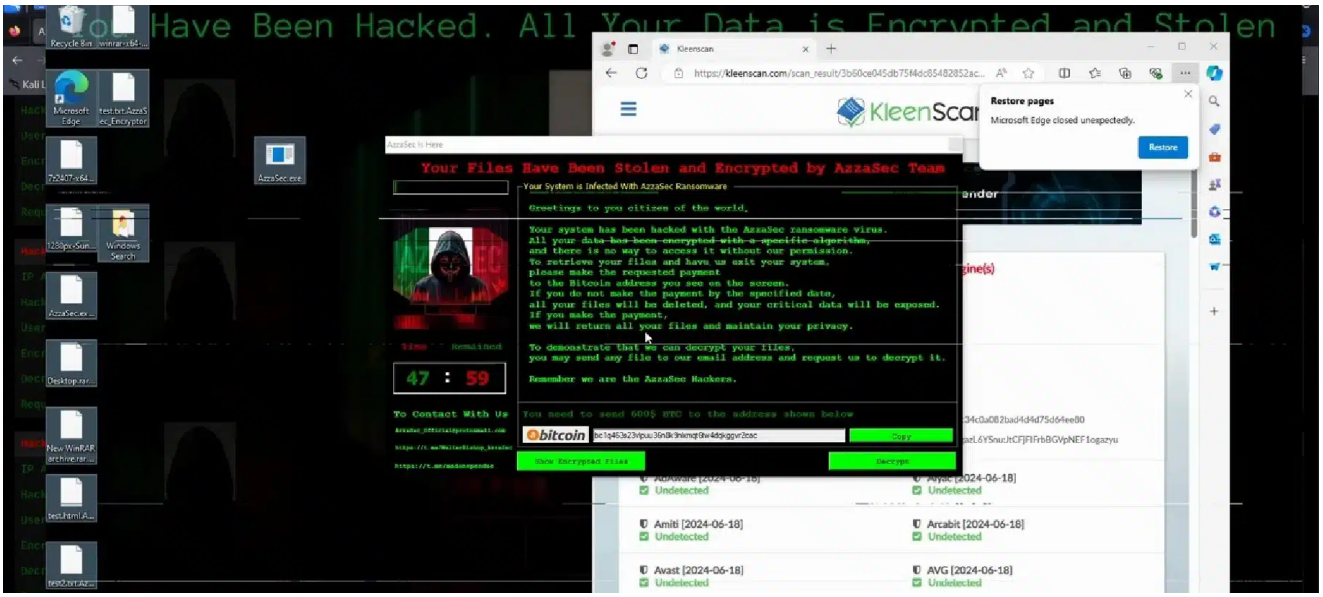
On June 26, 2024, NoName formally announced on its social media channels about the alliance.

“Today we have formed an alliance with the Italian hacker group AzzaSec, which is one of the TOP 3 coolest hack teams in Italy! We are always open to cooperation with various trance around the world!” the post read.

Source: X

AzzaSec is an infamous actor that infects computers and encrypts files. It later demands a ransom for its decryption. Once a computer is infected, AzzaSec assigns the '.AzzaSec' extension to the filenames. It alters files such as '1.png' to '1.png.AzzaSec' and '2.pdf' to '2.pdf.AzzaSec.'

Additionally, it changes the desktop wallpaper and provides a ransom note via a pop-up window like the screenshot below.



Source: X

The group demands ransom through Bitcoin. AzzaSec's sophisticated encryption techniques and the secrecy of cryptocurrency transactions make it increasingly difficult for authorities to crackdown and defuse the cybercriminals.

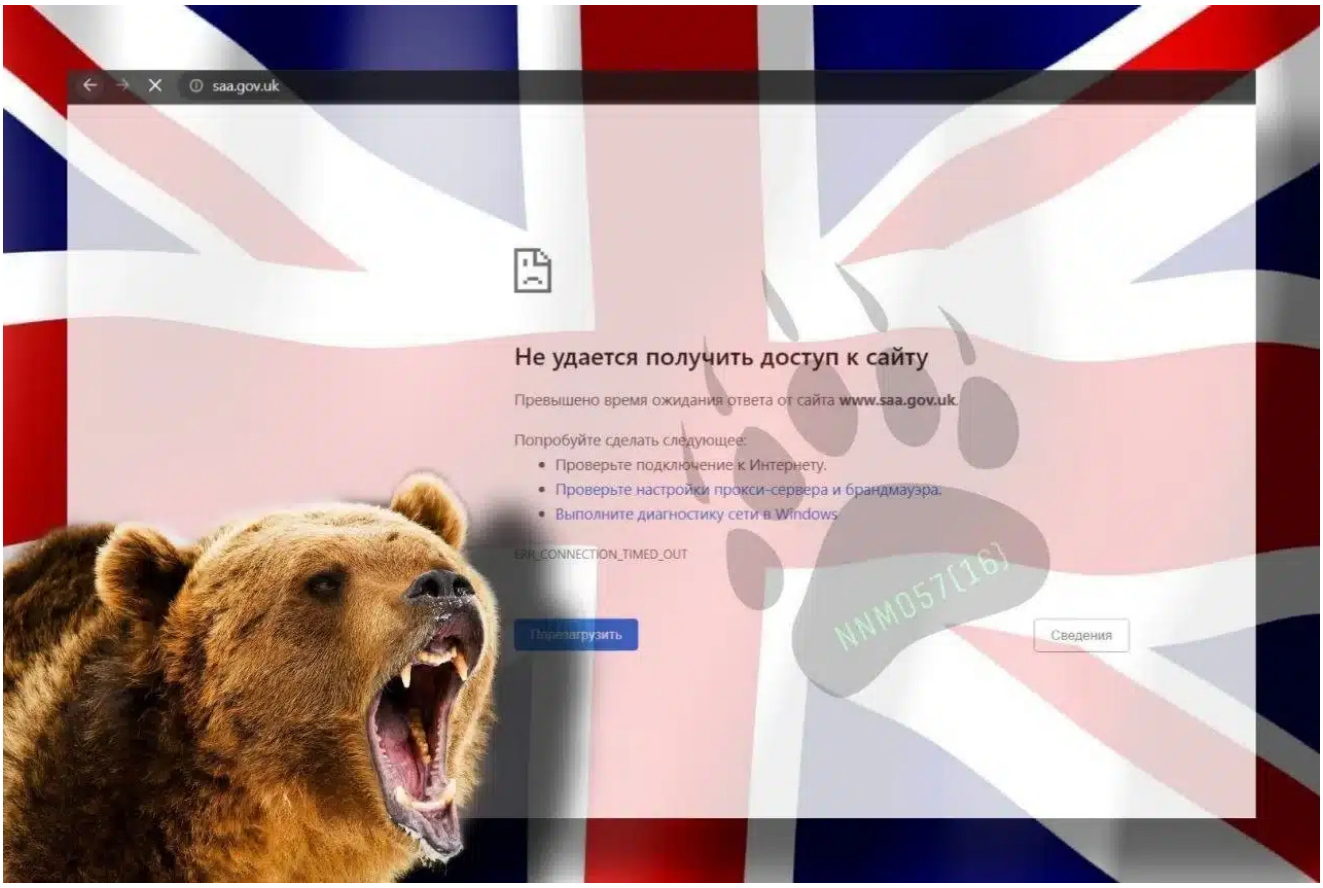
AzzaSec recently announced the release of a Windows ransomware builder. The group claimed that their ransomware could bypass major antivirus solutions such as Windows 10 / 11 Defender, Avast, Kaspersky, and AVG.

AzzaSec's emergence into the ransomware scene signals a reminder for organizations and individuals alike to upgrade their cybersecurity measures and remain vigilant against online threats.

Inglorious Past of NoName

NoName057(16) , on the other hand, first emerged in March 2022 and is known for its cyber-attacks on Ukrainian, American, and European government agencies, media, and private companies. The group is considered one of the biggest unorganised and free pro-Russian activist group.

Renowned for its widespread cyber operations, NoName057(16) has garnered notoriety for developing and distributing custom malware, notably the DDoS attack tool, the successor to the Bobik DDoS botnet.



Source: X

According to a report by Google-owned Mandiant, NoName057(16), along with other Russian state hackers, pose the biggest cyber threat to elections in regions with Russian interest.

“Mandiant is tracking multiple self-proclaimed hacktivist groups primarily conducting DDoS attacks and leaking compromised data in support of Russian interests. These groups claim to have targeted organizations spanning the government, financial services, telecommunications, transportation, and energy sectors in Europe, North America, and Asia; however, target selection and messaging suggests that the activity is primarily focused on the conflict in Ukraine. Relevant groups include KillNet, Anonymous Sudan, NoName057(16), JokerDNR/DPR, Beregini, FRwL_Team (aka “From Russia with Love”), and Moldova Leaks,” Google stated in its threat intelligence report in April.

The alliance between AzzaSec and NoName057(16) raises serious concerns about the evolving cyber threat landscape. With a combined skillset for ransomware deployment and large-scale attacks, these groups pose a significant risk to organizations and governments aligned with Ukraine. As the Russo-Ukrainian war rages on, the digital front is likely to see further escalation in cyberattacks. It is crucial for targeted nations and organizations to bolster their cybersecurity defenses, implement robust incident response plans, and collaborate on international efforts to counter these cyber threats.

Media Disclaimer: This report is based on internal and external research obtained through various means. The information provided is for reference purposes only, and users bear full responsibility for their reliance on it. The Cyber Express assumes no liability for the accuracy or consequences of using this information.