Breaking: Elite Cybercrime Forum "Maza" Suffers Breach

flashpoint-intel.com/blog/breelite-cybercrime-forum-maza-breached-by-unknown-attacker/

March 4, 2021

Blogs

Blog

Breaking: Elite Cybercrime Forum “Maza” Breached by Unknown Attacker

On March 3, 2021, Flashpoint detected a breach of the elite Russian cybercrime forum known as “Maza” (originally called “Mazafaka”). This breach follows recent attacks (both attempted and successful) on other Russian cybercrime forums, including the takeover of Russian-language forum Verified.

“Maza” the Latest Russian Cybercrime Forum to Suffer a Breach

On March 3, 2021, Flashpoint detected a breach of the elite Russian cybercrime forum known as “Maza” (originally called “Mazafaka”). This breach follows recent attacks (both attempted and successful) on other Russian cybercrime forums, including the takeover of Russian-language forum Verified.

Known to be in operations as far back as 2003, Maza is a highly-restricted Russian-language cybercrime that built its notoriety over many years, cultivating a community of some of the most sophisticated cybercriminals and financial fraudsters in the criminal underground—many of whom began their respective cybercrime activities as early as the mid- to late-1990s. Little is known at this time about the attackers who successfully compromised Maza. After their successful takeover of Maza, the unknown attackers posted a warning message to forum members reading: *“Your data has been leaked”* and *“This forum has been hacked.”*

Initial Assessment Suggests Breach is Major in Scale

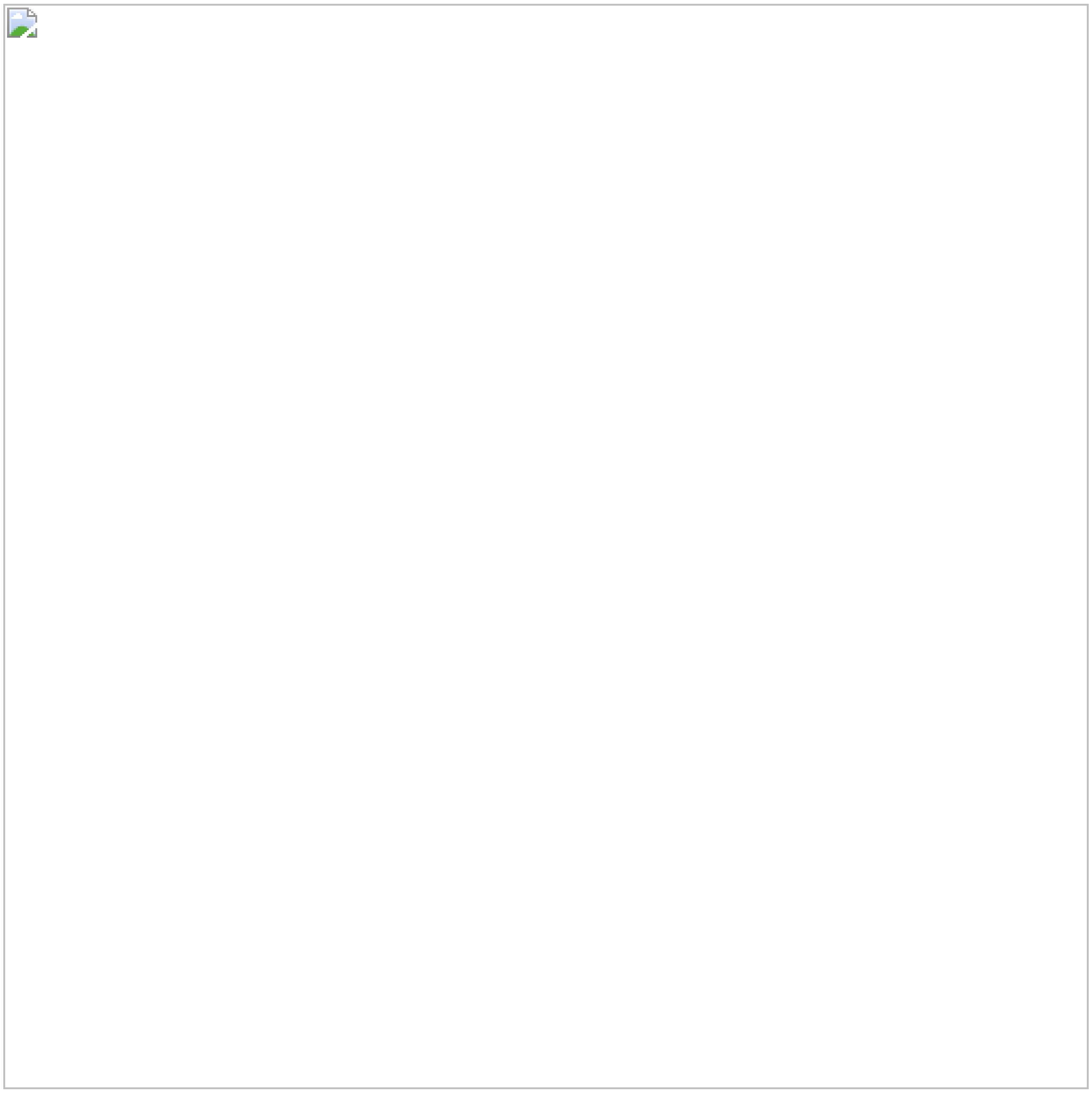
Flashpoint analysts note that the Russian sentences on the warning page were likely translated using an online translator. It is unclear if this automated translation indicates a non-Russian speaking actor is responsible or if this service was used as a misdirection technique.

Details Remain Obfuscated, but Scope of Attack Clearly Large

Flashpoint analysts successfully obtained the purported leaked data. While the compromised data appears to be extensive, it’s worth noting that the passwords have been hashed and most other data fields included in the dump have been hashed or further obfuscated. The leaked Maza data includes the following:

- *User id*
- *Username*
- *email*
- *Password (hashed and obfuscated)*
- *Crt_filename*
- *Crt_pass*
- *Icq (when available)*
- *Aim (when available)*
- *Yahoo (when available)*
- *Msn (when available)*
- *Skype (when available)*

Figure 1: Screenshot of the Maza Breach Warning Posted by the Unknown Attackers



Distressed Cybercriminals Deliberate Options and Exit Strategies

Flashpoint is actively monitoring cybercriminal discussions of Maza across the entire cybercriminal forum ecosystem commenting on the recent disruptions to many elite services and communities. Users on the Exploit forum are discussing moving away from using emails to register on forums as recent disruption efforts may have increased exposure of their online activities. Others are claiming that the database leaked by the attackers is either old or incomplete.

Recent Uptick in Attacks on Russian Cybercrime Forums of Particular Concern to Cybercriminals

Exploit actors also note an increase in attacks over the past months (attempted DDoS of Exploit, Verified compromise, and now Maza), and think the attackers could potentially be forum insiders or law enforcement. Finally, Exploit users note that if the attackers were law enforcement, that this is a new tactic to shut down cybercriminal activity and degrade trust across forums. A user on Exploit warned other users to be careful with registered emails across multiple platforms.

Maza Attackers May Take Similar Approach to Verified Ownership Change

News of the Maza attack comes directly on the heels of another successful breach of the well-established Russian forum Verified on January 20, 2021. Less than a month later on February 18, 2021, the new Verified admins announced the permanent change in ownership and began the deanonymization process of Verified's previous operators, known as "INC," "VR_Support," and "TechAdmin". The new admins noted that the previous administration recorded the IP addresses of every Verified user upon their entrance, which resulted in the collection of a total of 3,801,697 IP addresses.

Whether or not the Maza attackers will pursue a similar ownership takeover remains unclear. Quite interestingly, however, the aforementioned INC admin is (or was) also a Maza moderator.

Forum Breaches Are Not Strong Indicators of Permanent Shutdowns

Maza was previously hacked on February 18, 2011, compromising the data of more than 2,000 cybercriminal users, along with all of their forum correspondence. Shortly following this 2011 Maza breach, another attack was carried out against the Russian cybercrime forum, DirectConnection, whose administrator was the famous "k0pa," Aleksei Burkov.

See Flashpoint Intelligence in Action

Sign up for your risk-free 90-day trial and see how Flashpoint can provide you with the actionable threat intelligence you and your entire team need to identify and respond to threats targeting your organization. When equipped with Flashpoint Intelligence, you move a step ahead of threat actors and the cybercriminals impacting your business and bottom line.