Joker's Stash, the Largest Carding Marketplace, Shuts Down

January 15, 2021
FacebookTwitterLinkedInReddit

01 / 15 / 2021

Key Findings

- Joker's Stash, the largest dark web marketplace in the underground payment card economy, has announced that it is shutting down.
- While this marketplace was the largest in the carding space, it also exhibited a severe decline in the volume of compromised records posted over the past six months.
- Given this marketplace's high profile, it relied on a robust network of criminal vendors who offered their stolen records on this marketplace, among others. Gemini assesses with a high level of confidence that these vendors are very likely to fully transition to other large, top-tier dark web marketplaces.
- The underground payment card economy is likely to remain largely unaffected by this shutdown.

Background

Joker's Stash, the largest dark web marketplace in the underground payment card economy, has announced that it is shutting down. The announcement, posted on January 15, 2021, claimed that it would remain operational until February 15, 2021, before the administrator, "JokerStash," "goes on a well-deserved retirement." This message was originally posted to Joker's Stash itself, and additionally added to several top-tier dark web forums.

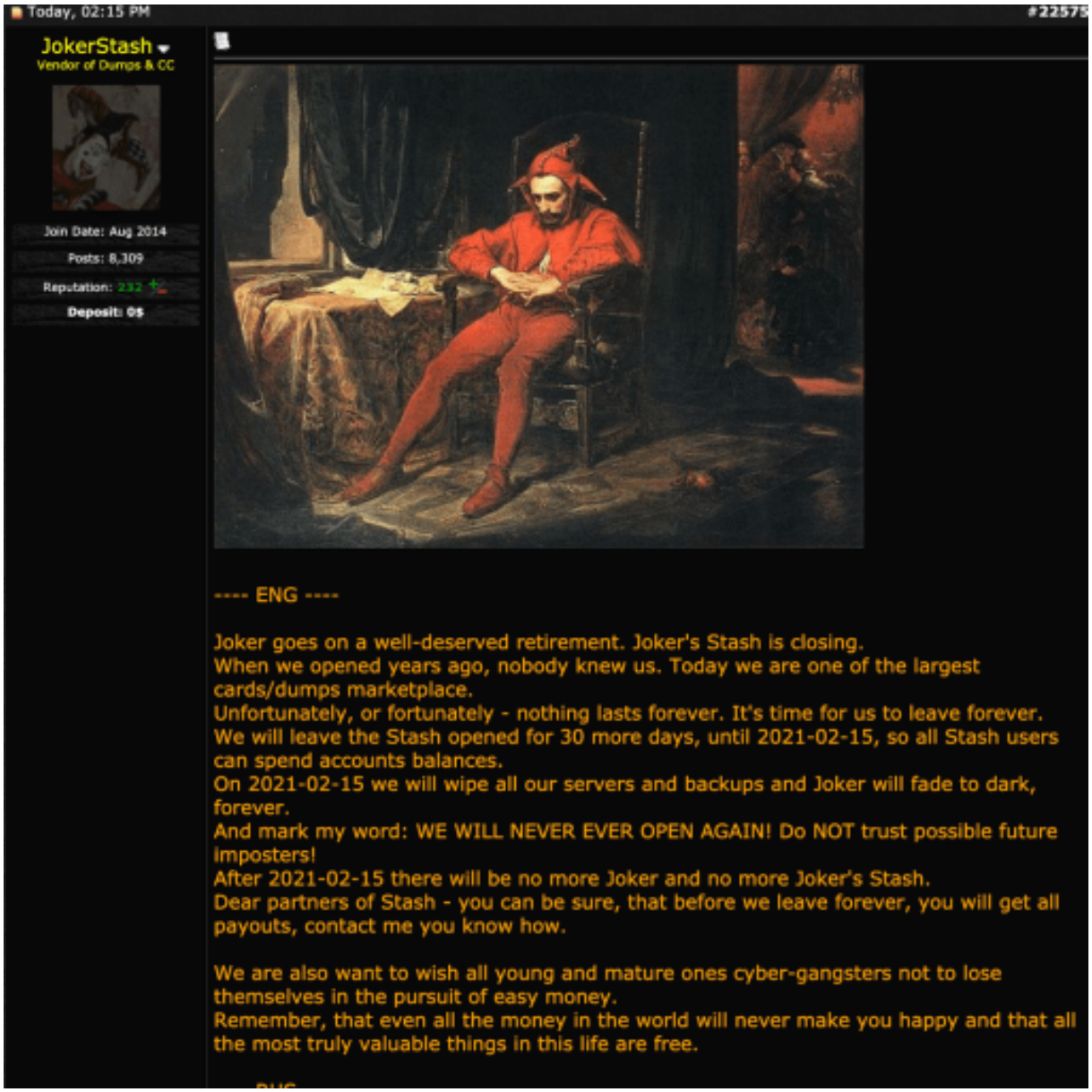

Image 1: JokerStash announces the closure of the Joker's Stash marketplace.

In-Depth Analysis

Reactions

Feedback was mixed; some dark web forum members expressed disappointment to lose access to the marketplace, while others who had been frustrated with its operations were neutral. Certain actors accepted JokerStash's explanation for retirement, while others on dark web forums and hacking-focused Telegram channels speculated that the FBI had detained JokerStash. Several weeks ago, Joker's Stash blockchain domains were temporarily rendered unavailable and replaced with an FBI and Interpol seizure notice. However, the administrator quickly regained control.

Image 2: An FBI and Interpol seizure notice appeared on a Joker's Stash blockchain domain on December 16, 2020.

In late October, the marketplace's routine activities were disrupted. JokerStash posted to claim that this was due to getting COVID-19 and spending more than one week in a hospital.

2020-10-29

Fucking COVID...

--- ENG ---

I got infected with COVID.
14 Days ago i start to feel myself "not so well",
in 2-3 days after begin i start to feel myself terrible - more dead, than alive
Doctors took me to the hospital and after all tests/diagnostics they said - it's COVID.
My health condition was very bad (extensive pneumonia, high temperature, fever, cough, tiredness)
More than week i spent in hospital and ate tons of pills.
I'm much better now. Today is a first day i have normal body temperature and no fever.
Doctor said if temperature will not start grow again - i will be able go home in 1-2 days.

Sorry for this unplanned shit and pause in my work.
We are all humans, sometimes we are weak.
I will back to normal work in 1-2 days and will continue to do regular daily fresh updates.
Thnx for understanding.

Joker.

Image 3: JokerStash claims to have been hospitalized due to COVID-19.

Another event that may have contributed to this threat actor shutting down their marketplace is Bitcoin's recent spike. JokerStash was an early advocate of Bitcoin and claims to keep all proceeds in this cryptocurrency. This actor was already likely to be among the wealthiest cybercriminals, and the spike may have multiplied their fortune, earning them enough money to retire. However, the true reason behind this shutdown remains unclear.

Operations

While this marketplace was the largest in the carding space, it also exhibited a severe decline in the volume of compromised Card Not Present (CNP) and Card Present (CP) records posted over the past six months. Most other top-tier carding marketplaces actually increased their posted data (largely CNP data, while CP data declined during COVID-19 lockdowns) during this time. However, Joker's Stash has received numerous user complaints alleging that card data validity is low, which even prompted the administrator to upload proof of validity through a card-testing service.

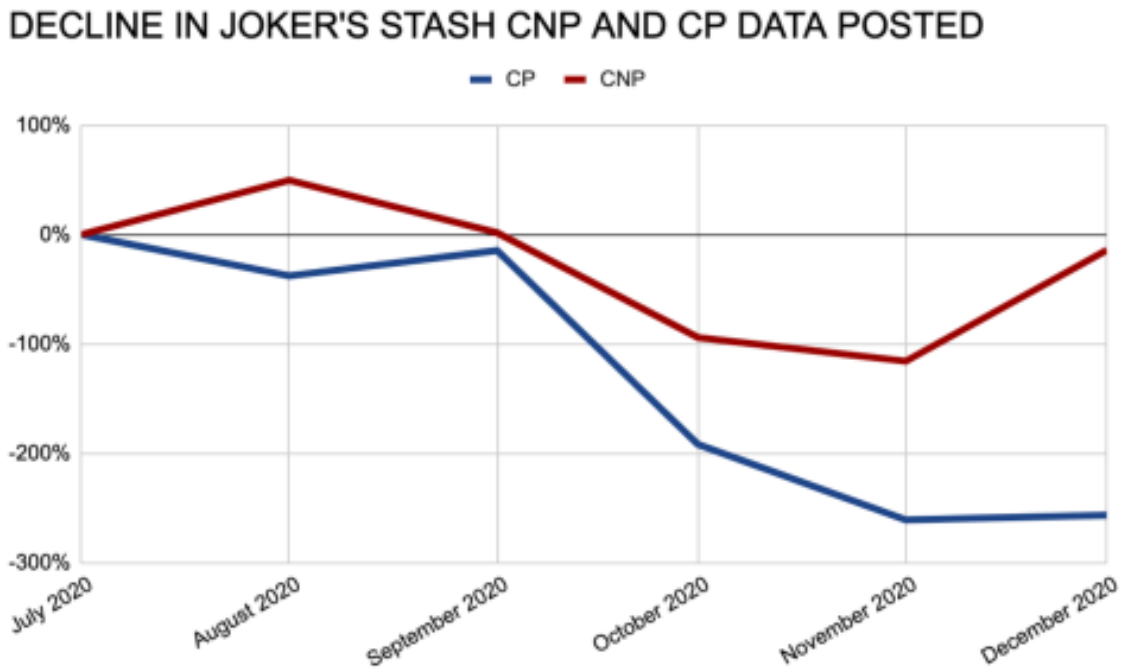

Image 4: Joker's Stash has posted fewer compromised CNP and CP records over the past six months. The graph shows the percentage change in the number of cards posted by comparing each month's level to that of July 2020.

Additionally, JokerStash's tactics, techniques, and procedures (TTPs) involved advertising in advance and then posting high-profile major breaches. The threat actor leveraged media coverage of these breaches to boast about their ability to compromise even major corporations. Most dark web marketplaces eschew such TTPs because they attract undue attention from security

researchers and law enforcement; JokerStash actually celebrated such attention.

Joker's Stash was one of the oldest observed dark web marketplaces and has operated since 2014. In the past year, the marketplace has added over 40 million new records, the majority of which were CP records. CP data was linked to major breaches, such as the "BIGBADABOOM-III" breach that compromised Wawa or the "BLAZINGSUN" breach that compromised Dickey's Barbecue Pit. CNP data was linked to Magecart attacks or occasionally phishing. Gemini calculated that Joker's Stash has generated more than $1 billion USD in revenue over the last several years.

Conclusion

Many criminal groups split the sale of compromised data across numerous marketplaces. For example, Gemini Advisory recently observed the "Keeper" group dividing stolen records among four leading marketplaces (including Joker's Stash). Given Joker's Stash's high profile, it relied on a robust network of criminal vendors who offered their stolen records on this marketplace, among others. Gemini assesses with a high level of confidence that these vendors are very likely to fully transition to other large, top-tier dark web marketplaces.

According to *Wired* research, even the shutdown of the infamous Silk Road dark web marketplace had very little impact on the overall dark web black market. The cybercriminals who sold illicit goods and services there simply shifted to other marketplaces, and the economy continued to function. The underground payment card economy is thus likely to remain largely unaffected by this shutdown.