A Sticky Situation Part 2

domaintools.com/resources/blog/a-sticky-situation-part-2

August 18, 2022

In May 2022, we reported on the Caramel skimmer-as-a-service and how the proliferation of online credit card skimmers support fraud. Evidence suggests CaramelCorp, the group behind the Caramel skimmer, does not limit their cybercrime activities to skimming. Instead, this group appears to pivot frequently in search of profitable new lines of business using different aliases with a documented history spanning several years. Such behavior is not unusual; rather, this appears to be a trend where cybercriminals are quicker to adapt–and expand to offer new services–in response to market forces.

Several factors contribute to this trend, but three are especially pertinent to this investigation. First, cybercrime threat actors can (temporarily) avoid scrutiny from law enforcement by appearing to be a small operation–a target simply not worth the effort to address, given the significant increase in cybercrime and limited resources available to deter such behavior. A cybercrime group that convincingly "appears small" can realize rich dividends. Second, savvy cybercrime threat actors closely monitor the underground economy and evaluate new opportunities in response to market forces. Third, increased specialization and reliance on third party services within the underground economy makes expanding into new types of cybercrime economical with minimal learning curve. The potential harm this trend can cause for business and consumer alike should not be discounted, nor should adversary creativity or their willingness to pivot in search of profits.

Despite its upside, such a trend is not without additional risk for cybercriminals. In exchange for additional capabilities and revenue, cybercrime actors often increase exposure. One helpful way to understand this relationship is through the lens of network defense and to consider exposure in terms of attack surface: increased complexity and reliance on third party services creates risk. If realized, that risk can become exploitable. Such is the case with CaramelCorp, and these footholds help bring into focus a cluster of activity beyond selling access to an online credit card skimmer. Instead, a portrait of a more ambitious group with forays into stealer malware, dubious video game "hacks," and cryptocurrency scams begins to appear.

Domain Registrant "Ozil Verfig" and a Trail of Badness

The seeming simplicity of whois data belies immense complexity. Relationships between registrant data and how domains relate can offer helpful insights when used judiciously. Commonality – whether infrastructure or artifact – does not necessarily mean association or shared endeavor. Not all roads lead to Rome and not all threads of an investigation lead to the same suspect or conclusion. The art of threat intelligence is the ability to see *multum in parvo* ("much in little") without losing sight of the big picture. To do so is to be comfortable with ambiguity, something cybercrime investigations are often fraught with. The domains in CaramelCorp's orbit and how they overlap with the domain registrant "Ozil Verfig" typify this "big picture" approach.

In this case, several roads lead to CaramelCorp. Whois records for caramelcorp[.]cc offer several useful initial footholds, the most helpful being:

Registrant Name: Ozil Verfig

Registrant Organization: Ozil Verfig

Registrant Street: Krasnaya Ploshad

Registrant City: Moscow

Registrant Postal Code: 101000

Registrant Country: RU

Registrant Phone: +495.1234321

Registrant Fax: +495.1234321Registrant Email: [.]com

Notably, the caramelcorp[.]cc domain appears to be controlled by a single registrant for its entire history. The registrant organization name “Ozil Verfig ” and email address “[.]com” seem distinctive. Further, the OSINT footprint associated with this registrant is narrow but deep.

A review of caramelcorp[.]xyz, one of CaramelCorp’s earlier domains, also has “Ozil Verfig” listed as the domain registrant’s organization. The name “Ozil Verfig” is unusual. Thus, the relatively small footprint of domains with registrants and registrant organizations using the name suggest relatedness. Further, many of these domains appear to fall into three categories: (1) impersonation of financial institutions, (2) cryptocurrency scams, and (3) malware domains, whether for propagation or administration (with possible ties to a notable Redline stealer campaign). Given the cybercrime nexus, distinctive name, targeting behavior, and frequently used domain registrars, it appears more likely than not that a single threat actor or group is behind these domain registrations. Another factor to consider is whether any similar domain naming conventions exist.

Registrant “Ozil Verfig” domains follow several consistent naming conventions for several likely domain purpose groups. Some of these domains include:

Domain	Registrant	Registrar	Date
Dashed domains:			
accounts-cooperative[.]com	Ozil Verfig	NiceNIC	Nov. 2021
acounts-service[.]com	Ozil Verfig	NiceNIC	Nov. 2021
cdn-googlestatic[.]com	Ozil Verfig	NiceNIC	Feb. 2022
docs-file[.]com	Ozil Verfig	NiceNIC	Mar. 2022
downloads-drive[.]com	Ozil Verfig	NiceNIC	Mar. 2022
downloads-safe[.]com	Ozil Verfig	NiceNIC	Mar. 2022
drive-file[.]com	Ozil Verfig	Cloudflare	Mar. 2022
file-office[.]com	Ozil Verfig	NiceNIC	Mar. 2022
redhat-dev[.]com	Ozil Verfig	NiceNIC	June 2022
spotify-account[.]xyz	Ozil Verfig	DNSPod	April 2022
static-microsoft[.]com	Ozil Verfig	NiceNIC	June 2022
storage-drive[.]com	Ozil Verfig	NiceNIC	Mar. 2022
Gaming “hacks” and scams:			
fortnightcheat[.]com	Ozil Verfig	NiceNIC	Mar. 2022
robloxforu[.]com	Ozil Verfig	NiceNIC	Mar. 2022
skinchangenow[.]com	Ozil Verfig	NiceNIC	Mar. 2022
valorannow[.]com	Ozil Verfig	NiceNIC	Mar. 2022
Typosquatting and lookalike domains:			
bllockchaln[.]online	Ozil Verfig	DNSPod	May 2020
certcodeplus[.]top	Ozil Verfig	NiceNIC	Nov. 2020
certicode[.]xyz	Ozil Verfig	NiceNIC	Oct. 2020
certicodeplus[.]club	Ozil Verfig	DNSPod	Oct. 2020
certicodeplus[.]group	Ozil Verfig	139.com	Oct. 2020

certicodeplus[.]online	Ozil Verfig	DNSPod	Oct. 2020
certicodeplus[.]top	Ozil Verfig	NiceNIC	Sept. 2020
certicodplus[.]site	Ozil Verfig	NiceNIC	Oct. 2020
certlcodeplus[.]top	Ozil Verfig	NiceNIC	Oct. 2020
firstechfed[.]site	Ozil Verfig	NiceNIC	Oct. 2020
flrstechfed[.]com	Ozil Verfig	NiceNIC	Oct. 2020
flrstechfed[.]group	Ozil Verfig	139.com	Oct. 2020
flrsttechfed[.]group	Ozil Verfig	139.com	Oct. 2020
lloyids[.]com	Ozil Verfig	NiceNIC	Oct. 2020

Panels:

caramelcorp[.]cc	Ozil Verfig	NiceNIC	Dec. 2020
caramelcorp[.]xyz	Ozil Verfig	NiceNIC	Dec. 2020
bezpecnost[.]tech	Ozil Verfig	NiceNIC	April 2022
bezpieczenstwo[.]app	Ozil Verfig	NiceNIC	Dec. 2021
bezpieczenstwo[.]tech	Ozil Verfig	DNSPod	April 2022
gotxest[.]top	Ozil Verfig	NiceNIC	Oct. 2020
panel-smm[.]top	Ozil Verfig	NiceNIC	Jan. 2022

Likely malware:

ahf4ycvea439tt9rq[.]site	Ozil Verfig	NiceNIC	March 2022
awqwywewfs56843[.]top	Ozil Verfig	DNSPod	Jan. 2021
batroslunk[.]top	Ozil Verfig	DNSPod	Dec. 2020
blctrsb[.]site	Ozil Verfig	NiceNIC	July 2020
fitollday[.]site	Ozil Verfig	NiceNIC	April 2020
gaweawgeaweg232[.]top	Ozil Verfig	NiceNIC	Jan. 2021
ghslitvompj[.]top	Ozil Verfig	NiceNIC	Nov. 2020

regisbrow[.]site	Ozil Verfig	NiceNIC	July 2020
windows-upgraded[.]com	Ozil Verfig	NiceNIC	Jan. 2022
wornegmot[.]top	Ozil Verfig	NiceNIC	Oct. 2020

* For purposes of this table, domain registrant and domain registrant organization are combined.

Consistent domain naming conventions across several domain registrations and clustered during specific time periods help define a nexus between CaramelCorp and whois records that include “Ozil Verfig.” But how many of these domains are a signal instead of noise, and does that signal relate to CaramelCorp? The answer is simple. One can begin to identify a person in a crowd – even when everyone looks the same – based on their activities *outside* of that crowd.

Forum presence of CaramelCorp promoter “letsz0ck3r”

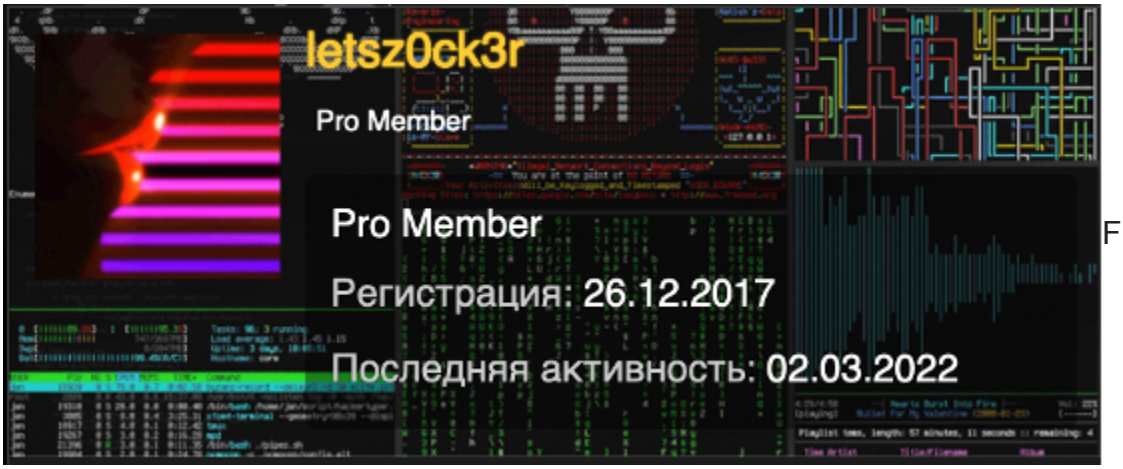

Figure 1: UfoLabs Russian-language hacking forum profile card for user “letsz0ck3r.”

First mentioned in our earlier report, the actor “letsz0ck3r” (also known as “Zocker” and likely “or1kstar”) has a history of offering and promoting services on Russian-language cybercrime forums (Figures 1-2). Some of these may include:

· Selling “Star Stealer” malware that sends stolen data via Telegram (Figures 3-4)

· Likely use of popular off-the-shelf malware (Anubis, Redline, Arkei)

· Offering cash-out and laundering services using US-based financial institutions (Figure 5)

· Selling malware encryption and digital signature services

· Promoting a hidden virtual network computing (hVNC) module for sale

· Video game mods and cheat systems (Figure 6)

Given the background of the Caramel skimmer, such products and services make sense contextually. Of this list, most services are no longer offered. This could be in response to market forces, improved technical abilities, and/or more profitable cybercrime niches.

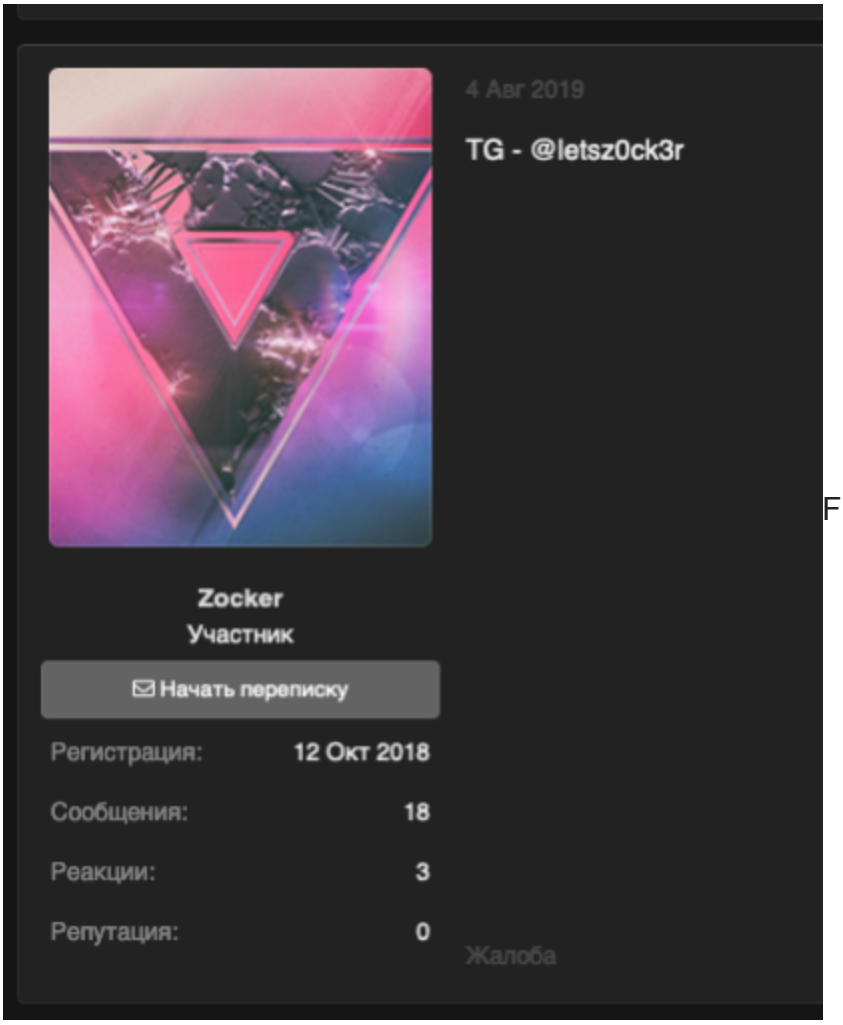

Figure 2: A SkyNetZone post where actor “Zocker” shares the Telegram handle @letsz0ck3r as part of their contact information.

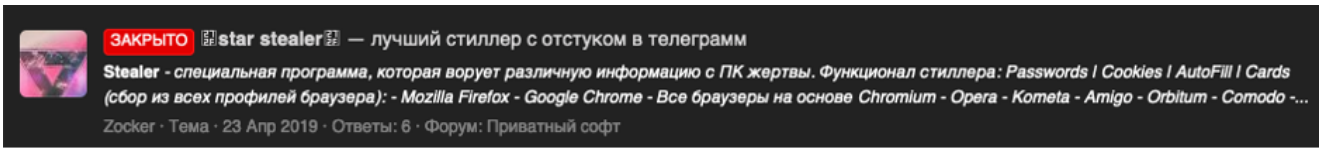

Figure 3: A SkyNetZone hacking forum post summary promoting Star Stealer malware by user “Zocker.”

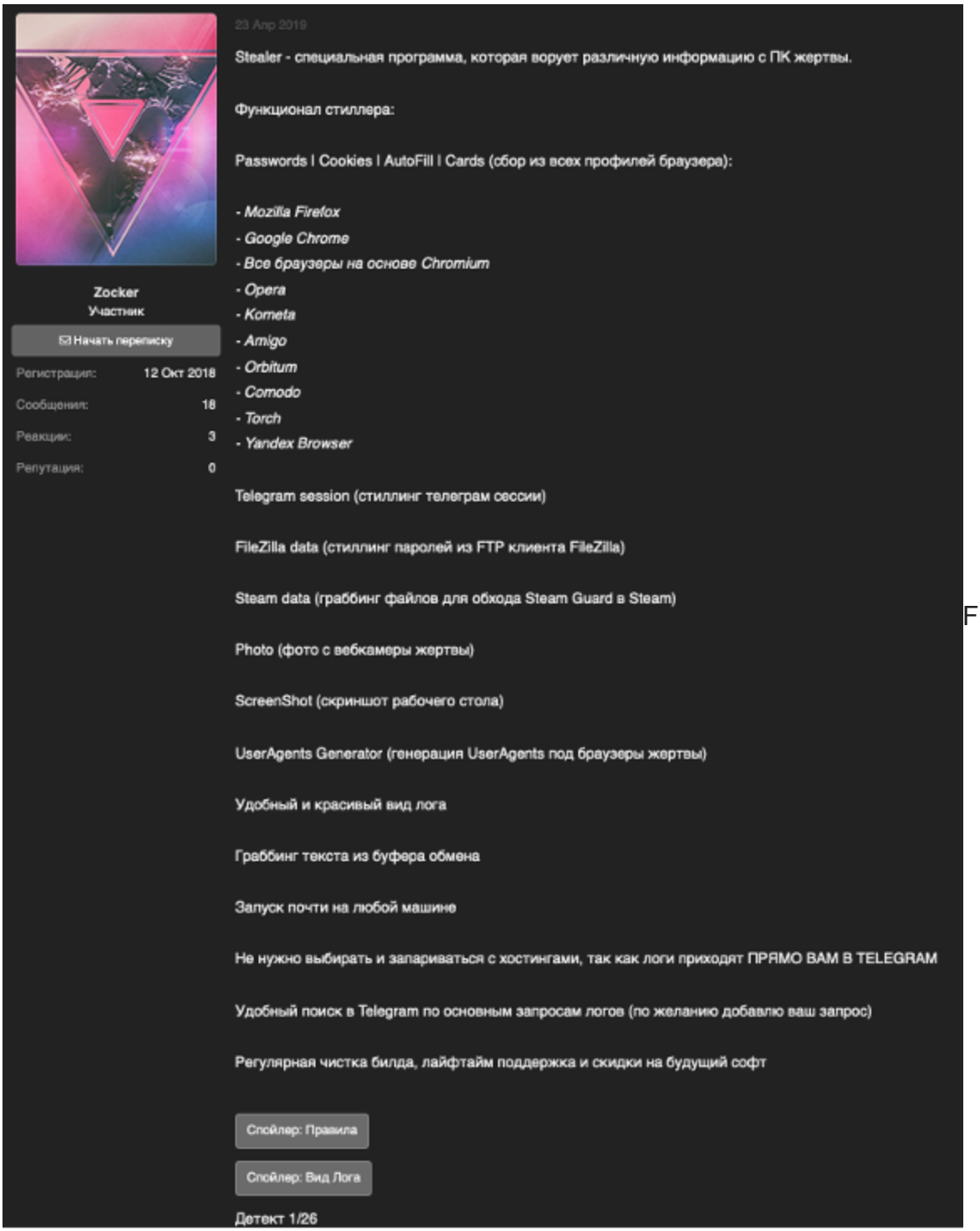

Figure 4: SkyNetZone hacking forum post promoting “Star Stealer,” which claims to steal a wide array of data and be largely undetectable by antivirus services.

Effective methods of cashing out balance sheets.
✳Accounts are not blocked after the first attempts, as is the case with revolution and merch.✳
We can make up to $12,000 from an account at a time, the conditions are negotiated separately.
Almost always connected
We guarantee that money with VCC will not hang anywhere, as is often the case with similar services.

Figure 5: Translation

of actor “Zocker” promoting their cash-out services.

Along with a Russian-language hacking forum presence, “letsz0ck3r” appears interested in video game mods and cheat systems. Unsurprisingly, this actor maintains a presence on the Phoenix video game hacking forum (Figure 6). They also appear to be a customer, which could suggest an interest in gaming beyond exploitation. This activity proved to be especially helpful in this investigation.

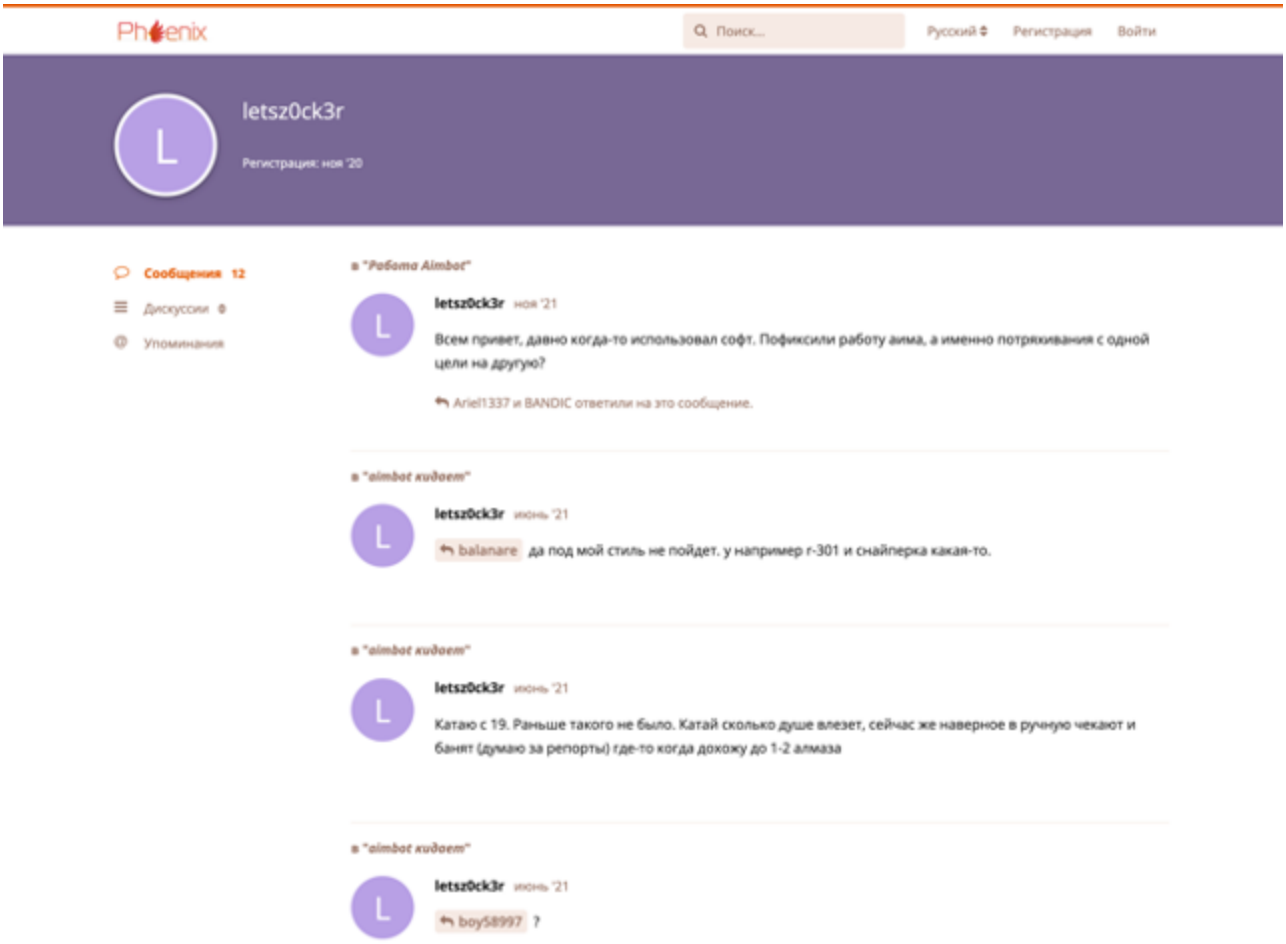

Figure 6: Examples of “letsz0ck3r” presence on the Phoenix video game hacking forum.

Notably, their activity appears to center around aimbots–videogame cheats that vastly improve a player’s reaction time and aim by modifying game configuration files via code

injection as well as using other methods. These modifications almost always violate multiplayer game terms of service.

Video game mods and cheat systems represent a tiny fraction of the underground economy, but their context deserves particular attention. Video game mods are frequent malware propagation vectors. Sometimes threat actors pair a game cheat system with malware; others are rudimentary and simply install malware. The prospect of an unfair advantage in online competitive games makes prospective targets much more likely to install them and ignore antivirus alerts (see Figure 7 for an illustrative example). Because such cheat systems often use code injection to operate, requests to disable Windows Defender entirely and run the program with administrator-level privileges seem credible to prospective targets. Malicious video game mods will often install stealer malware. Notably, DomainTools Research monitors several Redline campaigns that use this precise propagation vector.

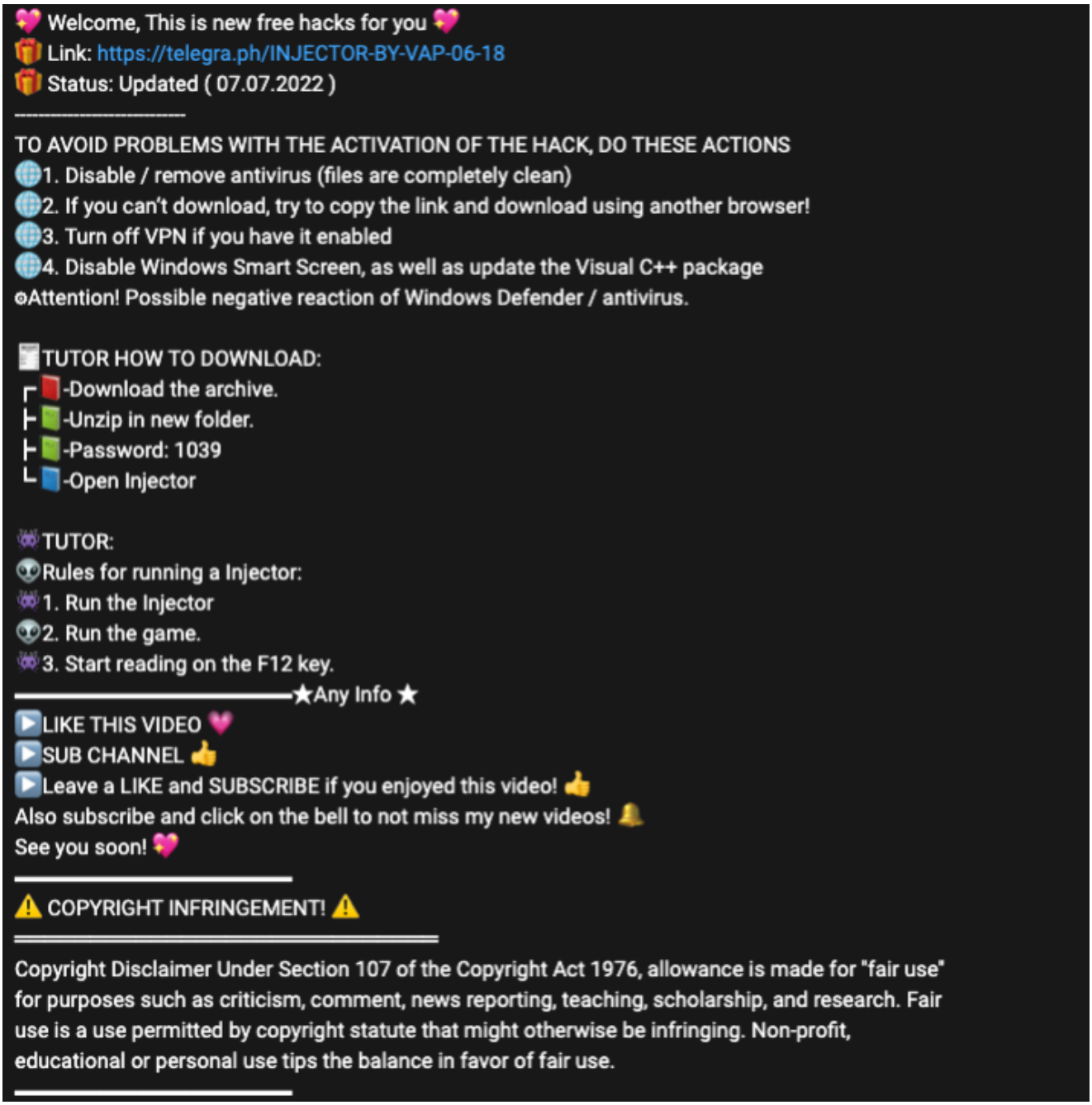

Figure 7: Description of an almost certainly malicious videogame cheat system from a recently uploaded YouTube video. Used for illustrative purposes and without apparent ties to CaramelCorp. After claiming "files are completely clean," the guide then requests potential victims disable Windows Smart Screen and Defender.

Several domains associated with CaramelCorp offer likely malicious video game mods and cheat systems. These domains use the domain registrant organization "Ozil Verfig." Some examples include the domains valorannow[.]com and fortnightcheat[.]com (Figures 8-9). Both appear to be slightly modified clones of other very suspicious video game mod services.

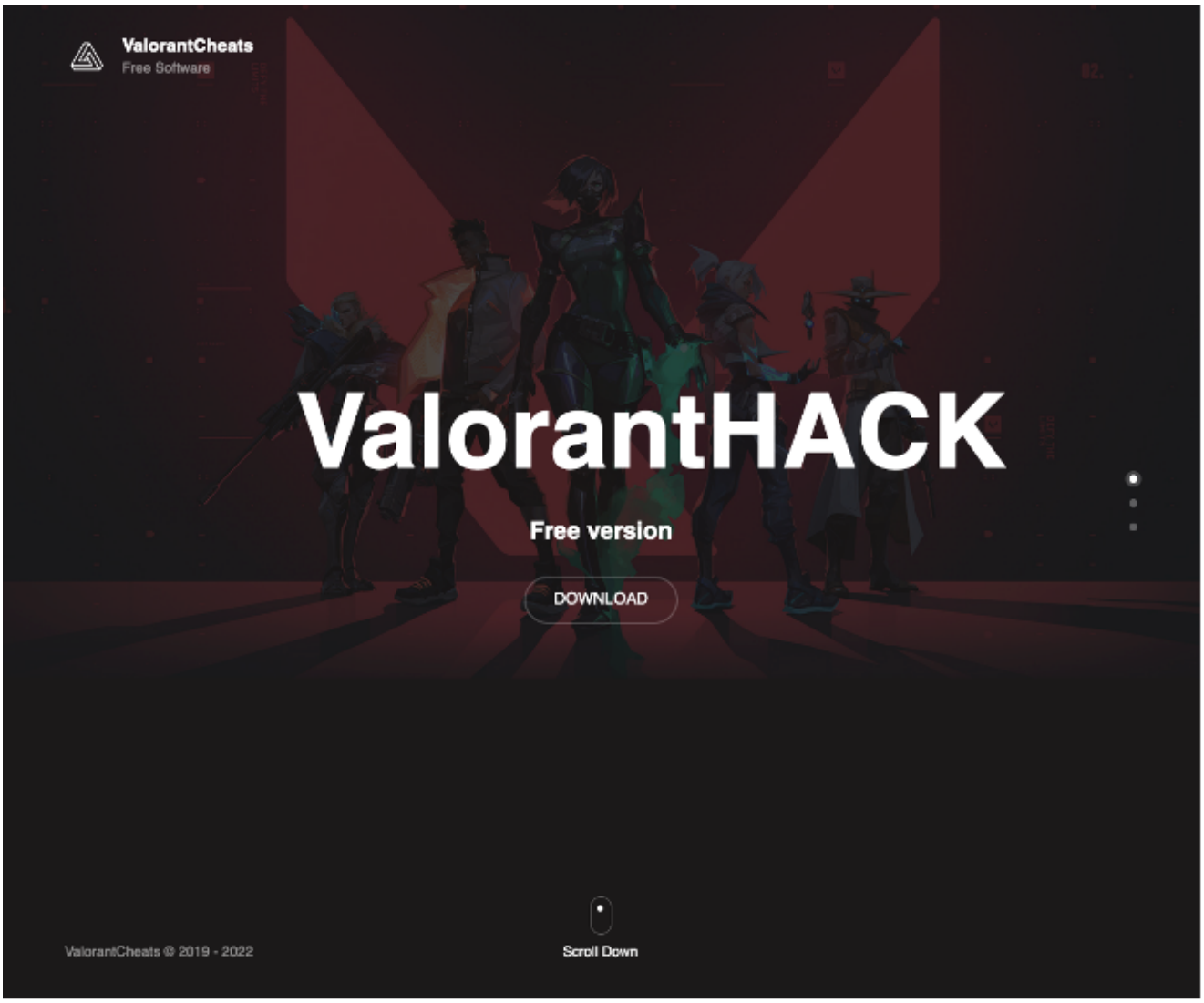

Figure 8: Screenshot of CaramelCorp-associated valorannow[.]com. Likely tied to malware activity, this game cheat engine targets Valorant players.

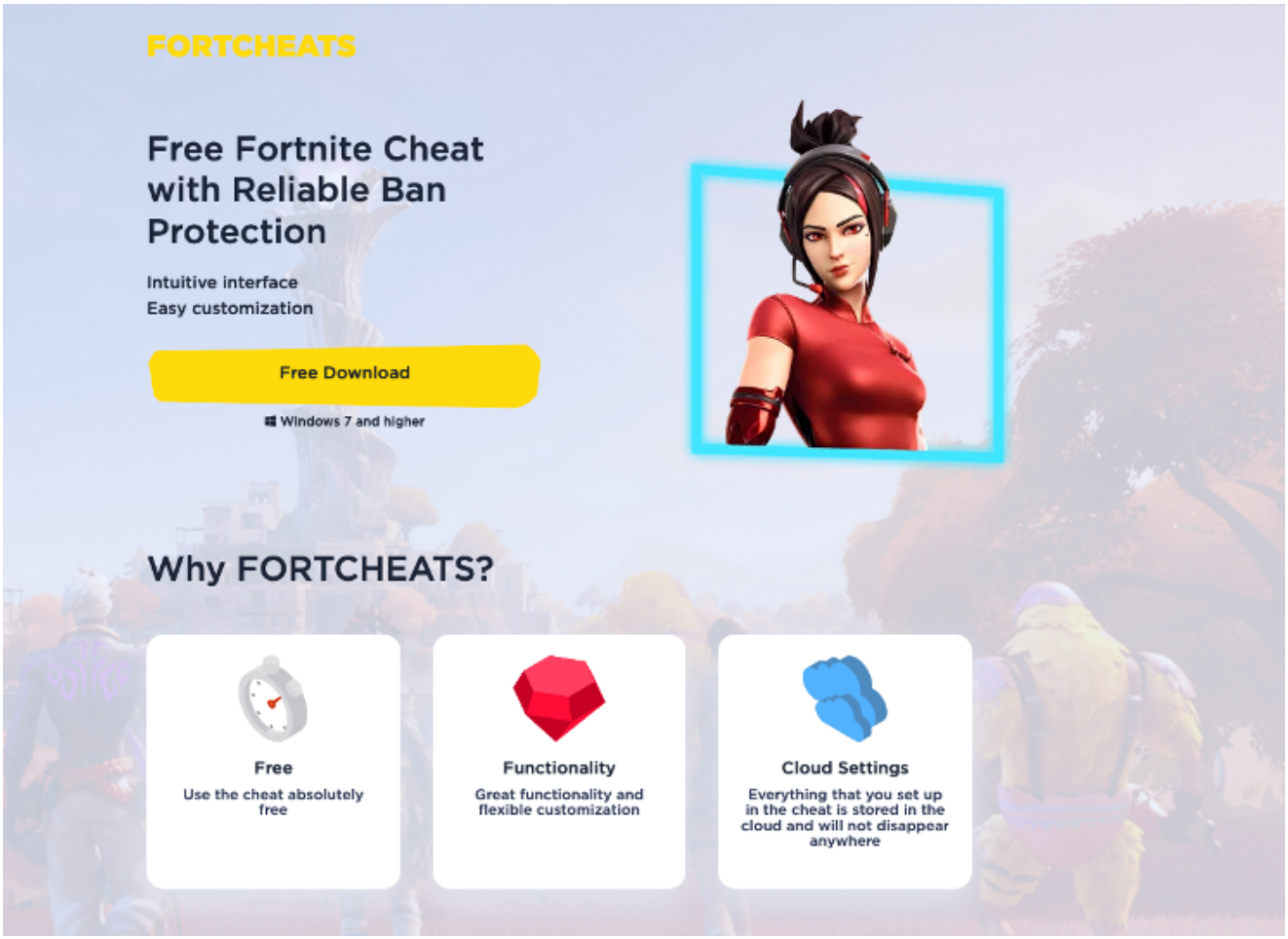

Figure 9: Screenshot of CaramelCorp-associated fortnightcheat[.]com. Likely tied to malware activity, this game cheat engine targets Fortnite players.

But what more can one learn from domains and why would that matter? Sometimes threat actors inadvertently reveal additional cybercrime activity. Here, a minor OPSEC mistake suggests “letsz0ck3r” also has a keen interest in cryptocurrency scams. Their mistake: using one domain for two very different types of scam.

Cryptocurrency scams

Cryptocurrency scams are legion, and CaramelCorp’s adoption of them should surprise no one. The purpose of a cryptocurrency scam is primarily cryptocurrency theft (or, in some cases, an attempt to install malware). More advanced cryptocurrency scams, referred to as “drainers,” not only steal credentials and wallet recovery phrases–they also empty cryptocurrency wallets and transfer the funds to an attacker-controlled wallet long before a victim even realizes their mistake. These stolen funds are almost certainly unrecoverable when transferred and, especially when laundered using privacy-focused cryptocurrencies, exceedingly difficult to track by investigators.

A simpler cryptocurrency scam uses “airdrops,” “money flips,” and “crypto giveaways” as lures to defraud victims. Each of these scams rely on the ruse that sending cryptocurrency somewhere will result in a massive short-term return on investment. Victims lose all the

cryptocurrency they send, which is then laundered by fraudsters. Like drainers, funds stolen using this scam are almost certainly unrecoverable. As economists have long said, there is no free lunch.

And why are these scams becoming so commonplace? The answer is painfully straightforward: they succeed, with victim losses in the billions of dollars. Another key driver in the increasing popularity of cryptocurrency scams is decentralized finance ("DeFi") paired with the vast swath of cryptocurrency projects and services operating in the DeFi space. Separating legitimate DeFi services from malicious ones can become difficult for even experienced cryptocurrency traders.

A clearer picture of CaramelCorp with blurred lines

Importantly, overlap in cybercrime activity can occur on the same domain and help further define a nexus of activity related to an actor group. Here, domains associated with CaramelCorp have historical screenshots of both likely malicious video game cheats and cryptocurrency scams within a relatively brief timeframe (Figures 10-11). The domain skinchangenow[.]com is by no means the exception.

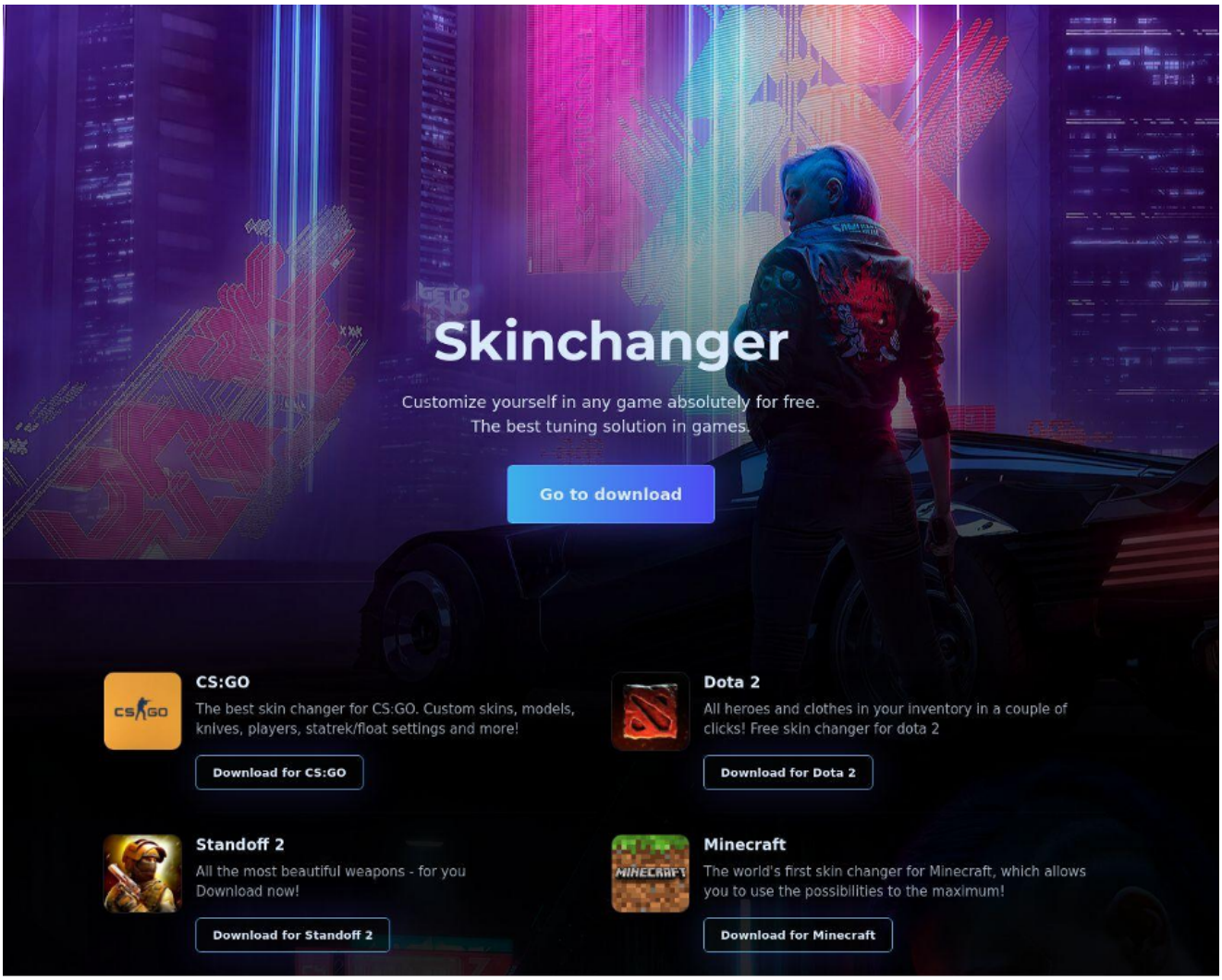

Figure 10: Likely malicious “Skinchanger” video game mod at skinchangenow[.]com.

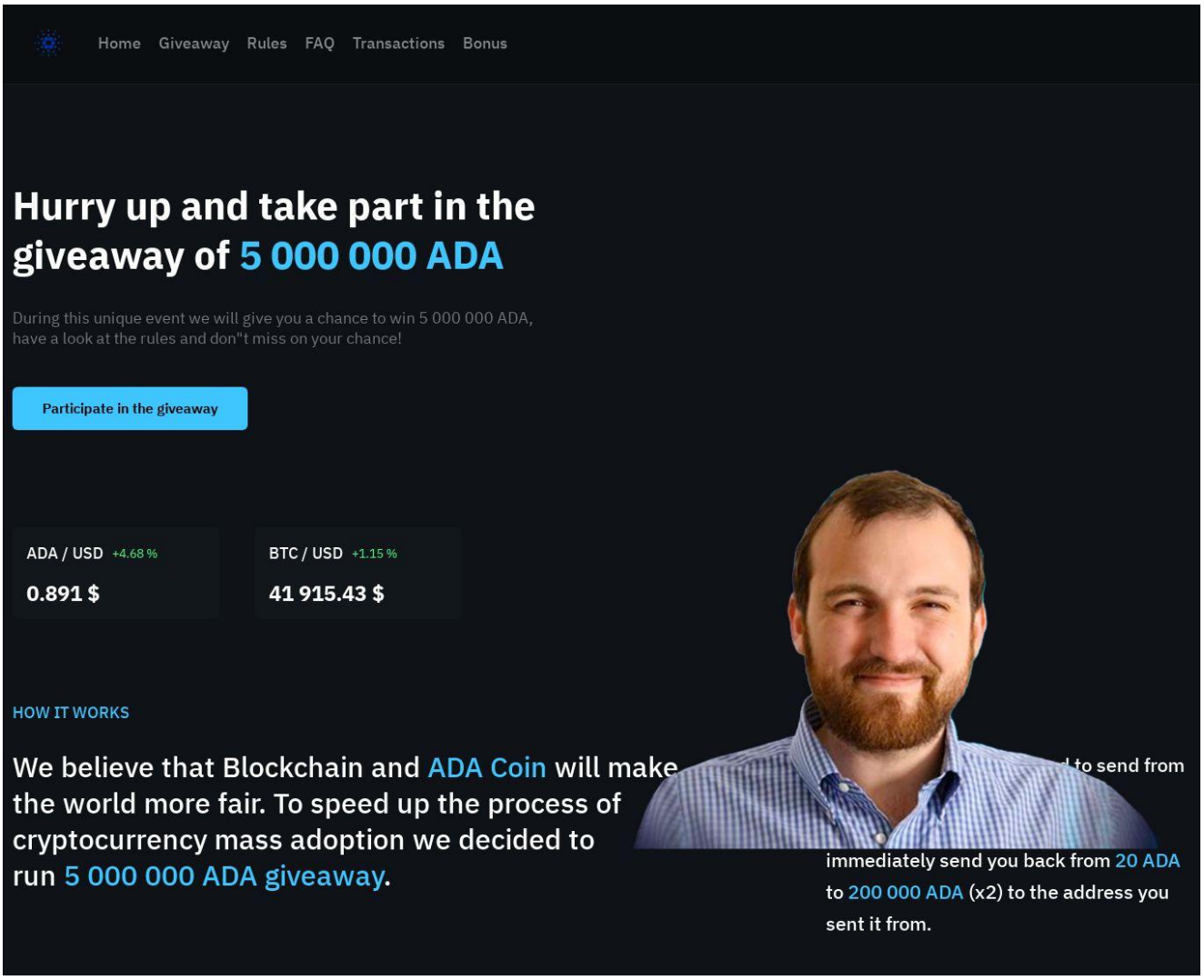

Figure 11: Cryptocurrency giveaway scam targeting Cardano holders at skinchangenow[.]com.

The CaramelCorp-associated domain valorannow[.]com featured a cryptocurrency scam that was replaced weeks later with a landing page for the very suspicious “ValorantCheats” website (Figure 12).

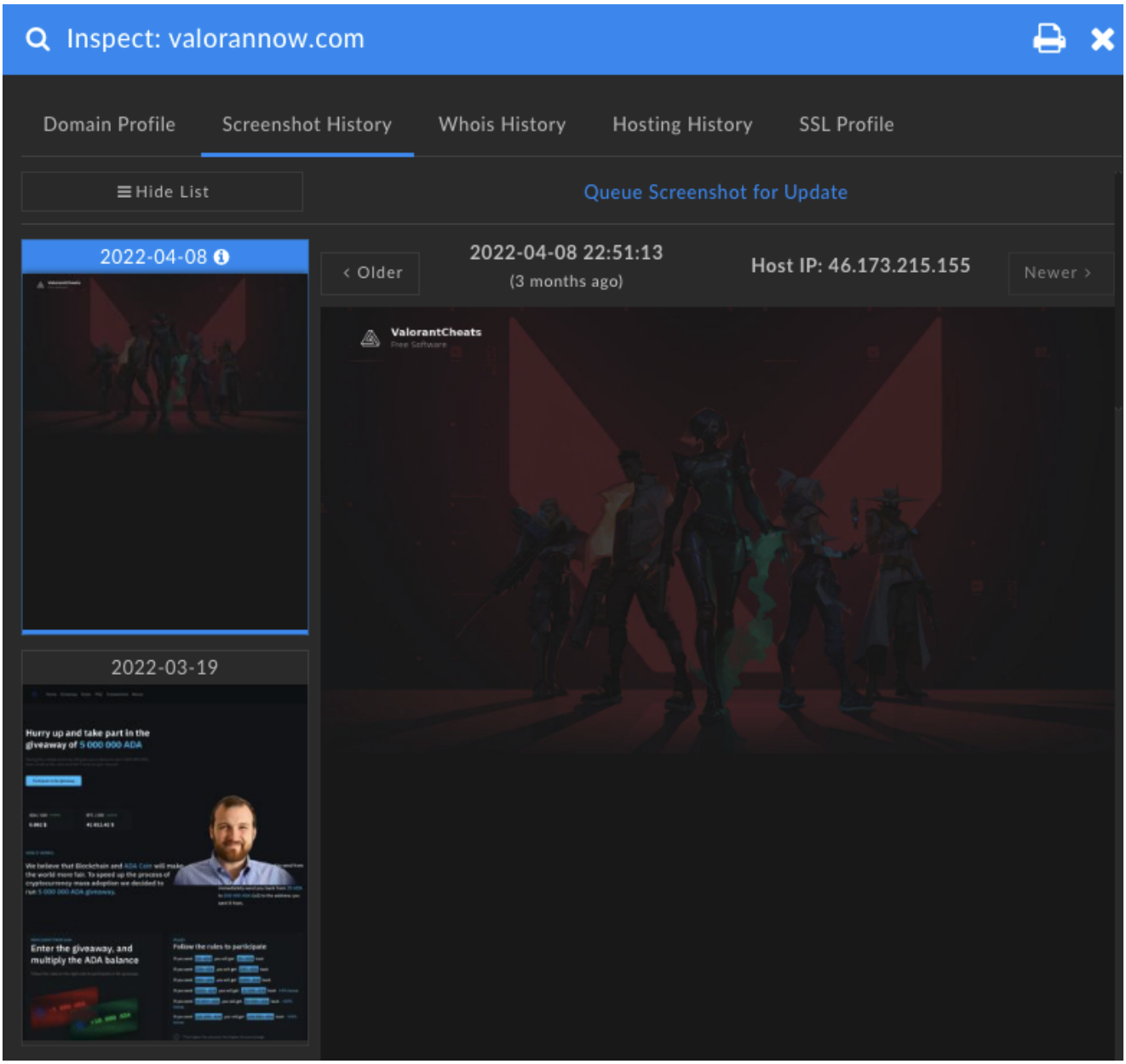

Figure 12: DomainTools Iris Investigate screenshot history feature reveals how the domain valorannow[.]com first began as a cryptocurrency giveaway scam.

Interestingly, a historical screenshot of another CaramelCorp-associated domain appears to show a data table viewable by an unauthenticated user. The domain in question is gotxest[.]top. This data table's columns suggests its purpose was to collect skimmed payment data (Figure 13):

```
ID
URI
BIN
Number
Expired
CVV
Billing
ZIP
Cardholder
Phone
UAgent
```

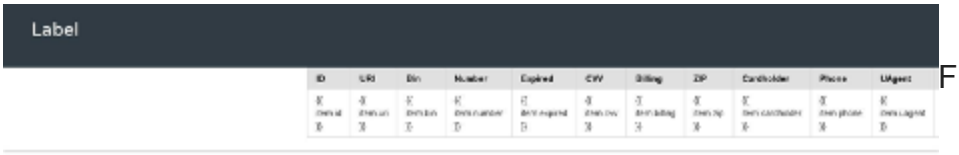

Figure 13: What appears to be a table for skimmed card data exposed to the public web at gotxest[.]top, another domain associated with CaramelCorp.

Given CaramelCorp's interest in online credit card skimming, this historical screenshot of gotxest[.]top' helps solidify further the nexus between "Ozil Verfig" domains and CaramelCorp's activities as a whole.

Taken together, a detailed portrait of CaramelCorp comes into focus. Instead of a skimmer-as-a-service vendor, CaramelCorp represents a group focused on profit maximization that pivots based on market signals, and–more importantly–one willing to learn from years of experience. CaramelCorp's behavior in this regard appears to be part of a trend, but not all is lost for defenders. An analyst mindset combined with quality data sets allow defenders to define, detect, and defend against threats promptly when threat actors pivot (or expand) activities based on market shifts in the underground economy. Happy hunting.

These cookies will be stored in your browser only with your consent. You also have the option to opt-out of these cookies. But opting out of some of these cookies may affect your browsing experience.

Necessary cookies are absolutely essential for the website to function properly. These cookies ensure basic functionalities and security features of the website, anonymously.

Cookie	Duration	Description
cookielawinfo-checkbox-analytics	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookie is used to store the user consent for the cookies in the category "Analytics".
cookielawinfo-checkbox-functional	11 months	The cookie is set by GDPR cookie consent to record the user consent for the cookies in the category "Functional".
cookielawinfo-checkbox-necessary	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookies is used to store the user consent for the cookies in the category "Necessary".
cookielawinfo-checkbox-others	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookie is used to store the user consent for the cookies in the category "Other.
cookielawinfo-checkbox-performance	11 months	This cookie is set by GDPR Cookie Consent plugin. The cookie is used to store the user consent for the cookies in the category "Performance".
viewed_cookie_policy	11 months	The cookie is set by the GDPR Cookie Consent plugin and is used to store whether or not user has consented to the use of cookies. It does not store any personal data.

Functional cookies help to perform certain functionalities like sharing the content of the website on social media platforms, collect feedbacks, and other third-party features.

Performance cookies are used to understand and analyze the key performance indexes of the website which helps in delivering a better user experience for the visitors.

Analytical cookies are used to understand how visitors interact with the website. These cookies help provide information on metrics the number of visitors, bounce rate, traffic source, etc.

Advertisement cookies are used to provide visitors with relevant ads and marketing campaigns. These cookies track visitors across websites and collect information to provide customized ads.

Other uncategorized cookies are those that are being analyzed and have not been classified into a category as yet.