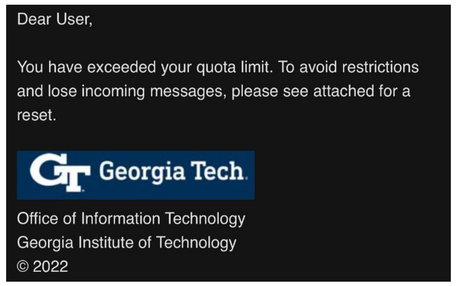
Buy One, Get One Hacked

Investigating a cyber attack against Georgia Tech

Tillson Galloway, Georgia Tech

In a recent phishing attack, criminals stole 500,000 passwords from more than 30 universities, including **Georgia Tech.**



Description	Price	Buy
266k Edu email:pass	$12.00	Buy
648k Edu email:pass	$17.00	Buy

Within hours, the criminals **sold the stolen data** on a popular underground marketplace.

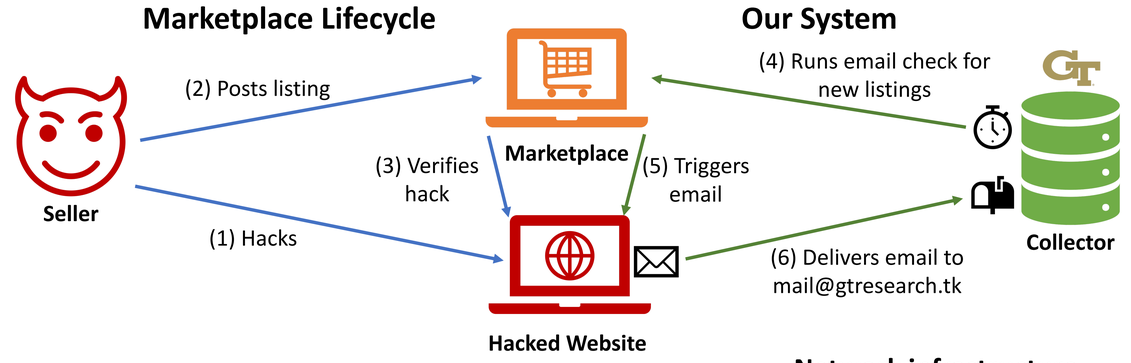
The criminals hosted the attack on **hacked websites** to evade detection, which were purchased on the same marketplace.

On these marketplaces, criminals can buy access to hacked websites for **under $5.00 each**.

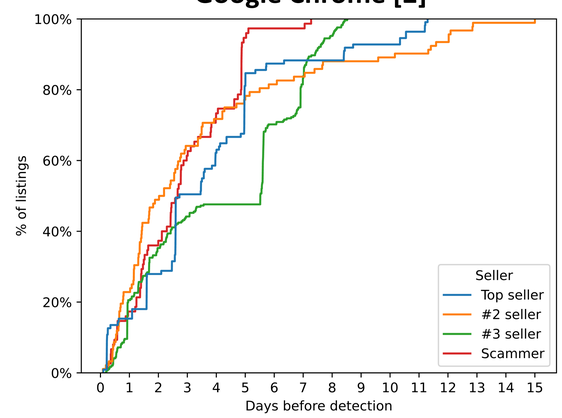
Example listings from a popular marketplace [1]

ID	Country	SSL	TLD	Hosting	Source	Check Send	Price	Check	Seller	Added	Buy
858409	US	http	.com	GoDaddy.com	Hacked	Check Send	5.00	Check	Seller277	2023-01-23 23:42	Buy
858408	ES	https	.org	OVH SAS	Hacked	Check Send	5.00	Check	Seller277	2023-01-23 23:42	Buy
858406	US	https	.co	GoDaddy.com	Hacked	Check Send	5.00	Check	Seller277	2023-01-23 23:41	Buy

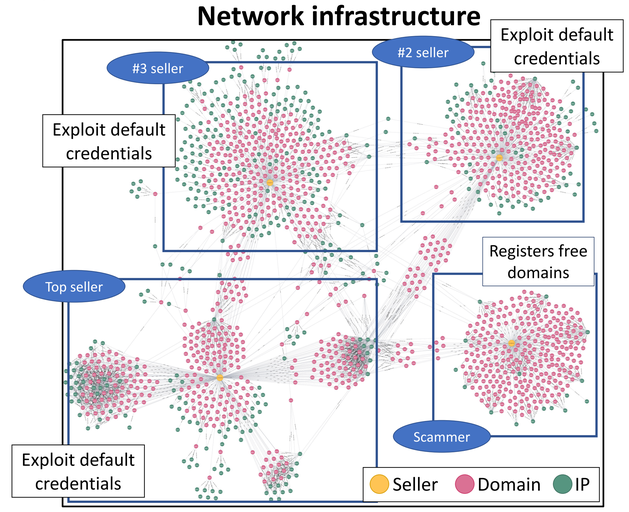
Because marketplaces **leak data** about hacked websites, we can use them to study criminal behavior and to detect attacks faster.



Days between listing and detection by Google Chrome [2]



Network infrastructure



Seller profiles, January 2023

Seller	Sales	Avg. cost	Listings	Servers	Avg. detection time	Technique
Top seller	$44,292	$3.40	13,035	466	3.16 days	Default creds
#2 seller	$35,988	$5.75	6,249	772	4.13 days	Default creds
#3 seller	$33,731	$4.89	6,887	1,190	5.58 days	Default creds
Scammer	$3,345	$3.00	1,145	43	1.81 days	Free domains
All sellers (49)	*$213,968*	*$4.42*	*48,370*	*4,663*	*4.11 days*	-

Conclusions

- Data leaks are a reliable way to detect hacked websites up to 14 days before state-of-the-art systems [2-4]
- High profit margins incentivize most hackers to provide high-quality products
- We will work with Georgia Tech to detect these websites, which would prevent future phishing attacks like this
- In the future, we can use this data to build a ML system that beats the state-of-the-art without access to new leaks

Bibliography

[1] Lufix. https://lufix.to.
[2] Google Safe Browsing. https://developers.google.com/safe-browsing.
[3] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster, "Building a Dynamic Reputation System for DNS.". In *USENIX Security Symposium, 2010*
[4] S. Fernandez, M. Korcynski, and A. Duda. Early detection of spam domains with passive dns and spf. In *International Conference on Passive and Active Network Measurement*, pages 39-49. Springer, 2022