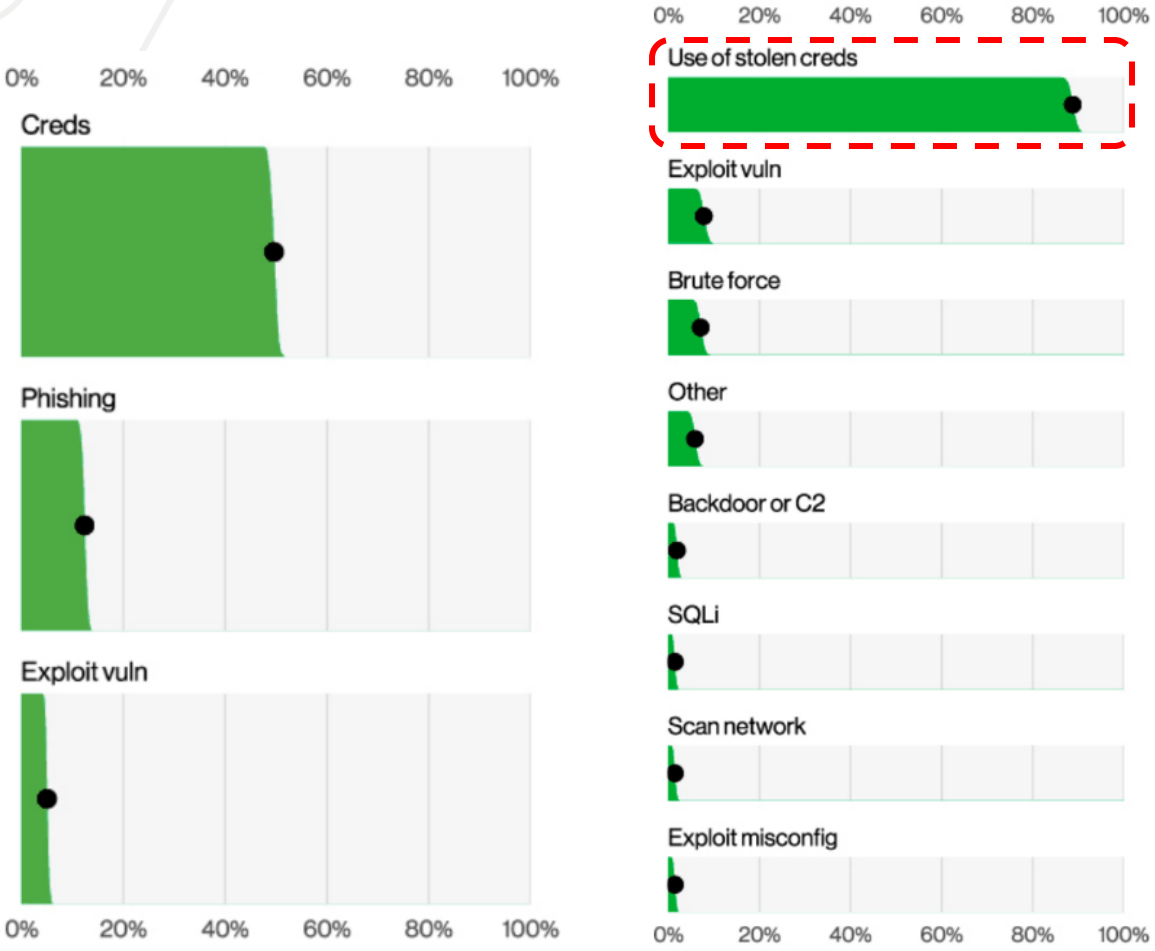
Beyond The Gates: An Empirical Analysis of HTTP-Managed Password Stealers and Operators

Athanasios Avgetidis*, Omar Alrawi*, Kevin Valakuzhy, Charles Lever, Paul Burbage, Angelos D. Keromytis, Fabian Monrose, Manos Antonakakis

The Importance of Stolen Credentials



- **Stolen credentials** are the **primary** way for cybercriminals to gain **initial access** to an organization [1].
- **86%** of recent data web application breaches involve the use of stolen credentials [1].

- Stolen Credentials are important for cybercriminals.
- Cybercriminals are stealing credentials successfully.

[1] 2023 Verizon Data Breach Investigation Report : https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/

Georgia Tech

Password Stealers (PWS) and Credential Stealing

- **Password stealers** (PWS) or information stealers is a family of malware aimed at stealing user credentials.

Usernames

Cookies

Passwords

Remote Access Keys

- Recents reports state that PWS malware is a rising threat!

Georgia Tech

Motivation

Spamalytics: An Empirical Analysis of Spam Marketing Conversion

Chris Kanich* Christian Kreibich† Kir
Geoffrey M. Voelker* Vern Pa

Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones

ngelberth[1], and Felix Freiling[1]

The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns

Brett Stone-Gross[§,⋆], Thorsten Holz[‡,⋆], Gianluca Stringhini[§], and Giovanni Vigna[§,⋆]

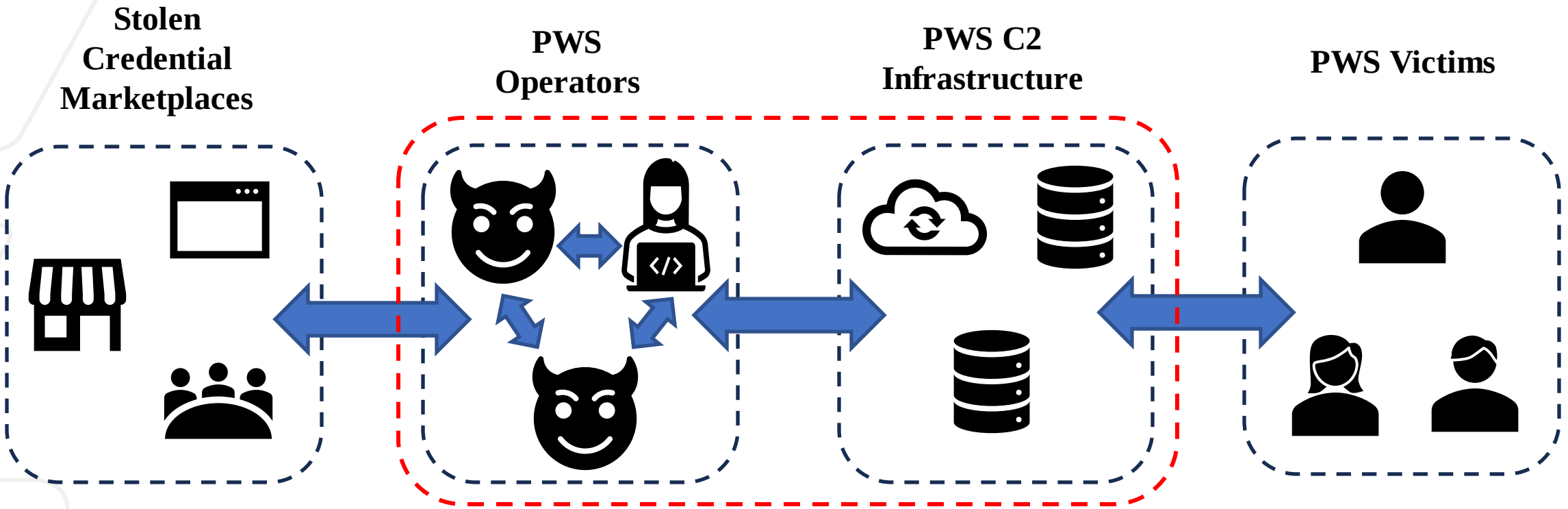
Re: CAPTCHAs – Understanding CAPTCHA-Solving Services in an Economic Context

chenko, Chris Kanich, Damon McCoy,
oelker and Stefan Savage
f California, San Diego
, dlmccoy, voelker, savage}@cs.ucsd.edu

Sunrise to Sunset:
Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale

Adam Oest*, Penghui Zhang*, Brad Wardman†,
Eric Nunes†, Jakub Burgis†, Ali Zand‡, Kurt Thomas‡, Adam Doupé*, and Gail-Joon Ahn*,§

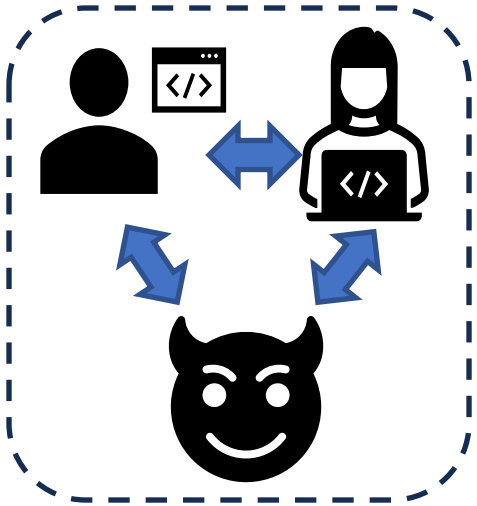
PWS Ecosystem Overview

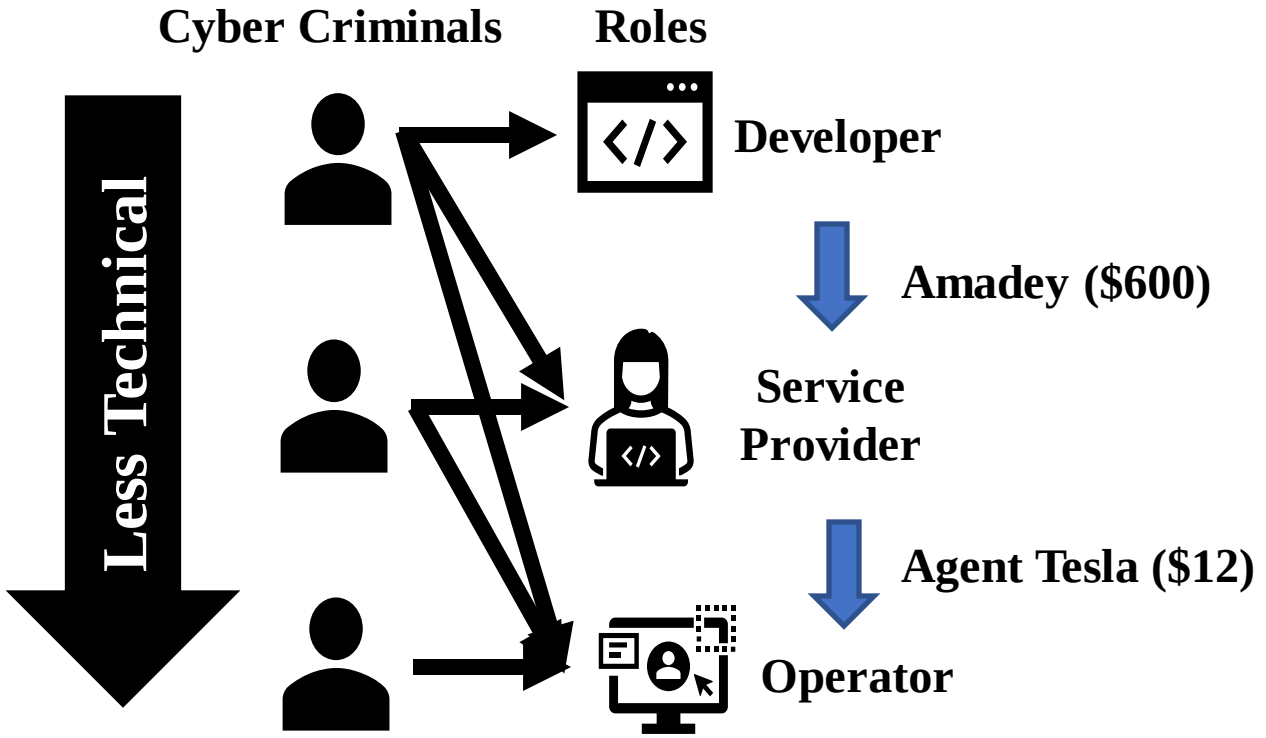


What tactics do operators employ?

- What are their roles and relationships?
- How profitable are they?
- How effective are we in detecting them?

Stealer Cybercriminal Roles

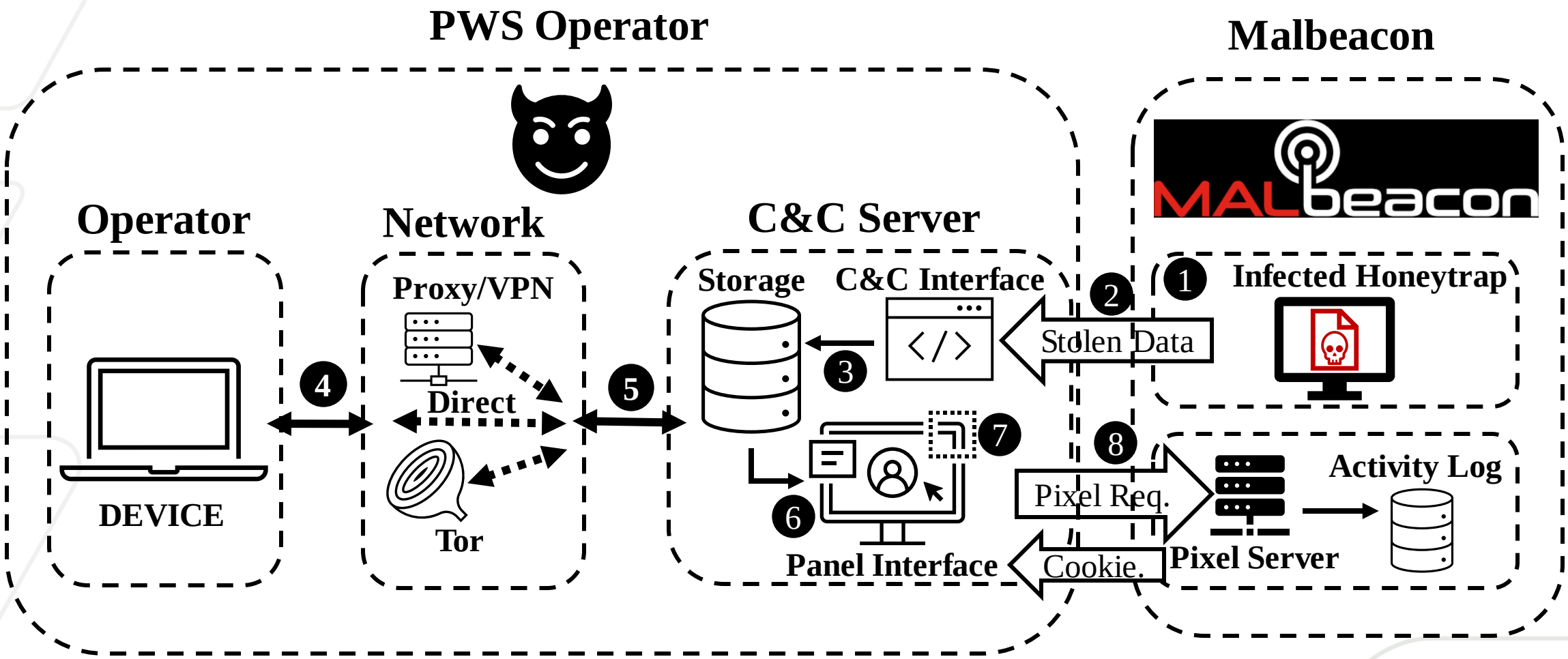




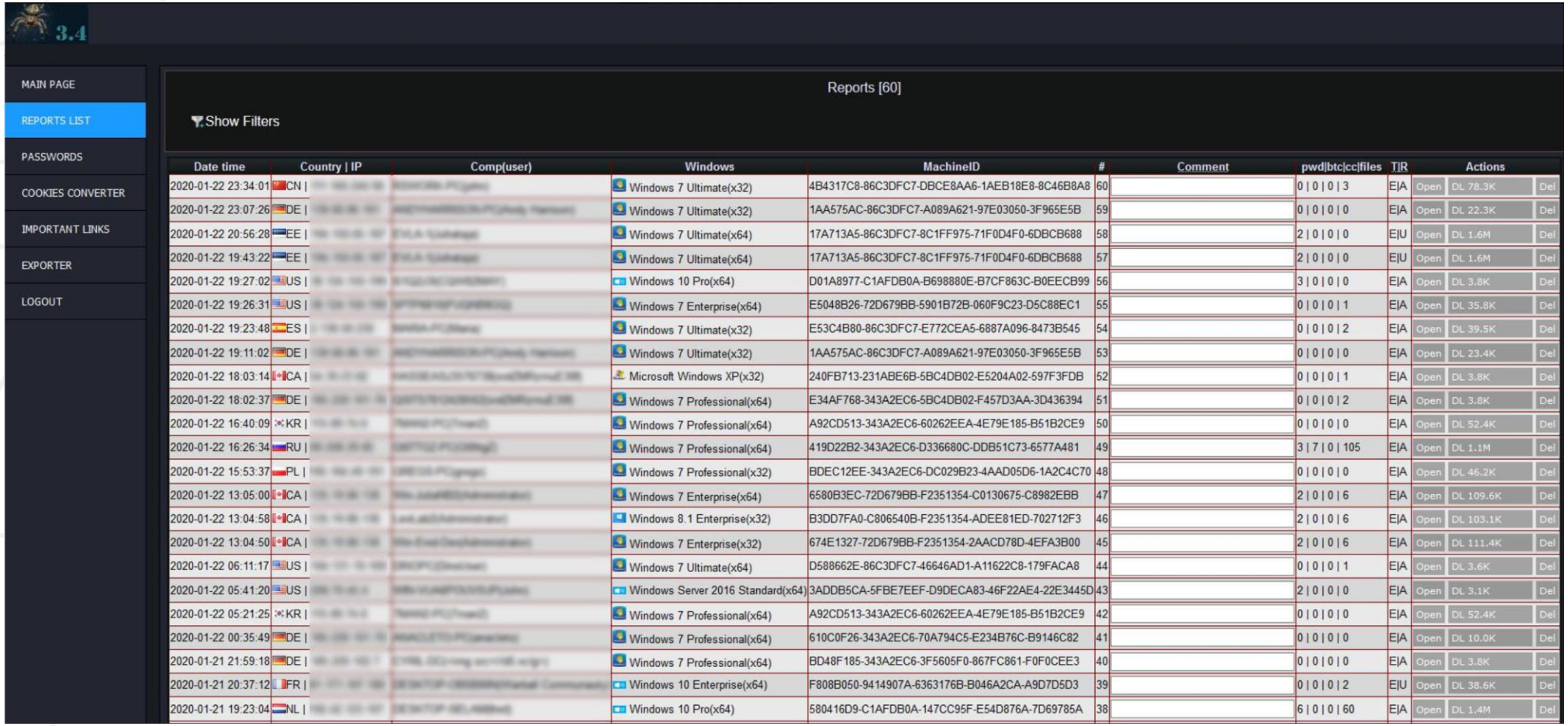
- The Stealers market is **mature** and **competitive.**
- The technical and financial **entry** barrier is **low**.

Georgia Tech

Stealer Dataset Collection



Operator Perspective: Panel Example (AZORult)



Date time	Country | IP	Comp(user)	Windows	MachineID	#	Comment	pwd|btc|cc|files	T|R	Actions
2020-01-22 23:34:01	CN |		Windows 7 Ultimate(x32)	4B4317C8-86C3DFC7-DBCE8AA6-1AEB18E8-8C46B8A8	60		0 | 0 | 0 | 3	E|A	Open DL 78.3K Del
2020-01-22 23:07:26	DE |		Windows 7 Ultimate(x32)	1AA575AC-86C3DFC7-A089A621-97E03050-3F965E5B	59		0 | 0 | 0 | 0	E|A	Open DL 22.3K Del
2020-01-22 20:56:28	EE |		Windows 7 Ultimate(x64)	17A713A5-86C3DFC7-8C1FF975-71F0D4F0-6DBCB688	58		2 | 0 | 0 | 0	E|U	Open DL 1.6M Del
2020-01-22 19:43:22	EE |		Windows 7 Ultimate(x64)	17A713A5-86C3DFC7-8C1FF975-71F0D4F0-6DBCB688	57		2 | 0 | 0 | 0	E|U	Open DL 1.6M Del
2020-01-22 19:27:02	US |		Windows 10 Pro(x64)	D01A8977-C1AFDB0A-B698880E-B7CF863C-B0EECB99	56		3 | 0 | 0 | 0	E|A	Open DL 3.8K Del
2020-01-22 19:26:31	US |		Windows 7 Enterprise(x64)	E5048B26-72D679BB-5901B72B-060F9C23-D5C88EC1	55		0 | 0 | 0 | 1	E|A	Open DL 35.8K Del
2020-01-22 19:23:48	ES |		Windows 7 Ultimate(x32)	E53C4B80-86C3DFC7-E772CEA5-6887A096-8473B545	54		0 | 0 | 0 | 2	E|A	Open DL 39.5K Del
2020-01-22 19:11:02	DE |		Windows 7 Ultimate(x32)	1AA575AC-86C3DFC7-A089A621-97E03050-3F965E5B	53		0 | 0 | 0 | 0	E|A	Open DL 23.4K Del
2020-01-22 18:03:14	CA |		Microsoft Windows XP(x32)	240FB713-231ABE6B-5BC4DB02-E5204A02-597F3FDB	52		0 | 0 | 0 | 1	E|A	Open DL 3.8K Del
2020-01-22 18:02:37	DE |		Windows 7 Professional(x64)	E34AF768-343A2EC6-5BC4DB02-F457D3AA-3D436394	51		0 | 0 | 0 | 2	E|A	Open DL 3.8K Del
2020-01-22 16:40:09	KR |		Windows 7 Professional(x64)	A92CD513-343A2EC6-60262EEA-4E79E185-B51B2CE9	50		0 | 0 | 0 | 0	E|A	Open DL 52.4K Del
2020-01-22 16:26:34	RU |		Windows 7 Professional(x64)	419D22B2-343A2EC6-D336680C-DDB51C73-6577A481	49		3 | 7 | 0 | 105	E|A	Open DL 1.1M Del
2020-01-22 15:53:37	PL |		Windows 7 Professional(x32)	BDEC12EE-343A2EC6-DC029B23-4AAD05D6-1A2C4C70	48		0 | 0 | 0 | 0	E|A	Open DL 46.2K Del
2020-01-22 13:05:00	CA |		Windows 7 Enterprise(x64)	6580B3EC-72D679BB-F2351354-C0130675-C8982EBB	47		2 | 0 | 0 | 6	E|A	Open DL 109.6K Del
2020-01-22 13:04:58	CA |		Windows 8.1 Enterprise(x32)	B3DD7FA0-C806540B-F2351354-ADEE81ED-702712F3	46		2 | 0 | 0 | 6	E|A	Open DL 103.1K Del
2020-01-22 13:04:50	CA |		Windows 7 Enterprise(x32)	674E1327-72D679BB-F2351354-2AACD78D-4EFA3B00	45		2 | 0 | 0 | 6	E|A	Open DL 111.4K Del
2020-01-22 06:11:17	US |		Windows 7 Ultimate(x64)	D588662E-86C3DFC7-46646AD1-A11622C8-179FACA8	44		0 | 0 | 0 | 1	E|A	Open DL 3.6K Del
2020-01-22 05:41:20	US |		Windows Server 2016 Standard(x64)	3ADDB5CA-5FBE7EEF-D9DECA83-46F22AE4-22E3445D	43		2 | 0 | 0 | 0	E|A	Open DL 3.1K Del
2020-01-22 05:21:25	KR |		Windows 7 Professional(x64)	A92CD513-343A2EC6-60262EEA-4E79E185-B51B2CE9	42		0 | 0 | 0 | 0	E|A	Open DL 52.4K Del
2020-01-22 00:35:49	DE |		Windows 7 Professional(x64)	610C0F26-343A2EC6-70A794C5-E234B76C-B9146C82	41		0 | 0 | 0 | 0	E|A	Open DL 10.0K Del
2020-01-21 21:59:18	DE |		Windows 7 Professional(x64)	BD48F185-343A2EC6-3F5605F0-867FC861-F0F0CEE3	40		0 | 0 | 0 | 0	E|A	Open DL 3.8K Del
2020-01-21 20:37:12	FR |		Windows 10 Enterprise(x64)	F808B050-9414907A-6363176B-B046A2CA-A9D7D5D3	39		0 | 0 | 0 | 2	E|U	Open DL 38.6K Del
2020-01-21 19:23:04	NL |		Windows 10 Pro(x64)	580416D9-C1AFDB0A-147CC95F-E54D876A-7D69785A	38		6 | 0 | 0 | 60	E|A	Open DL 1.4M Del

https://twitter.com/CryptoInsane/status/1231258175766220800

Georgia Tech

Datasets

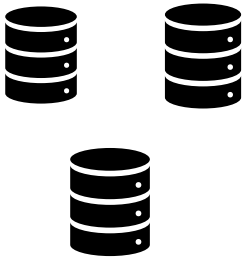
PWS Panel Callbacks (20 Months)

Field Name	Unique
Timestamp	202,538
IP Address	21,812
User-Agent	1,484
Cookie ID	5,552
Referrer Field	27,823

- 10 different PWS families
- 3,613 and 1,195 panel instances of Lokibot and Formbook

+

DNS



Active & Passive DNS

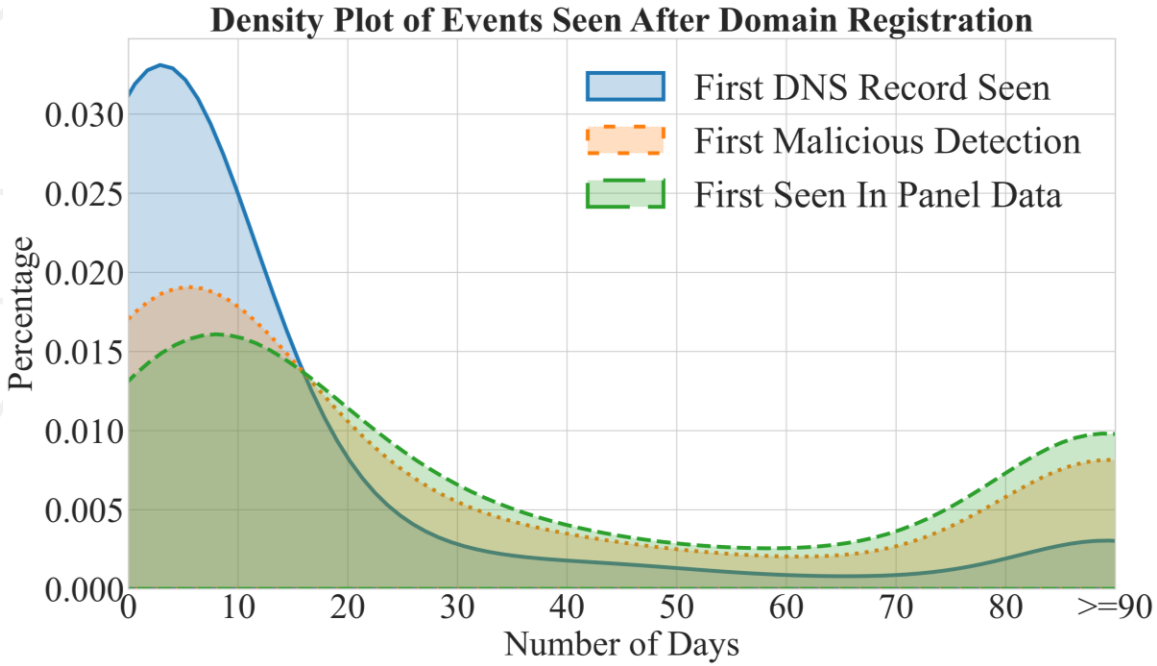
Threat & IP Intel

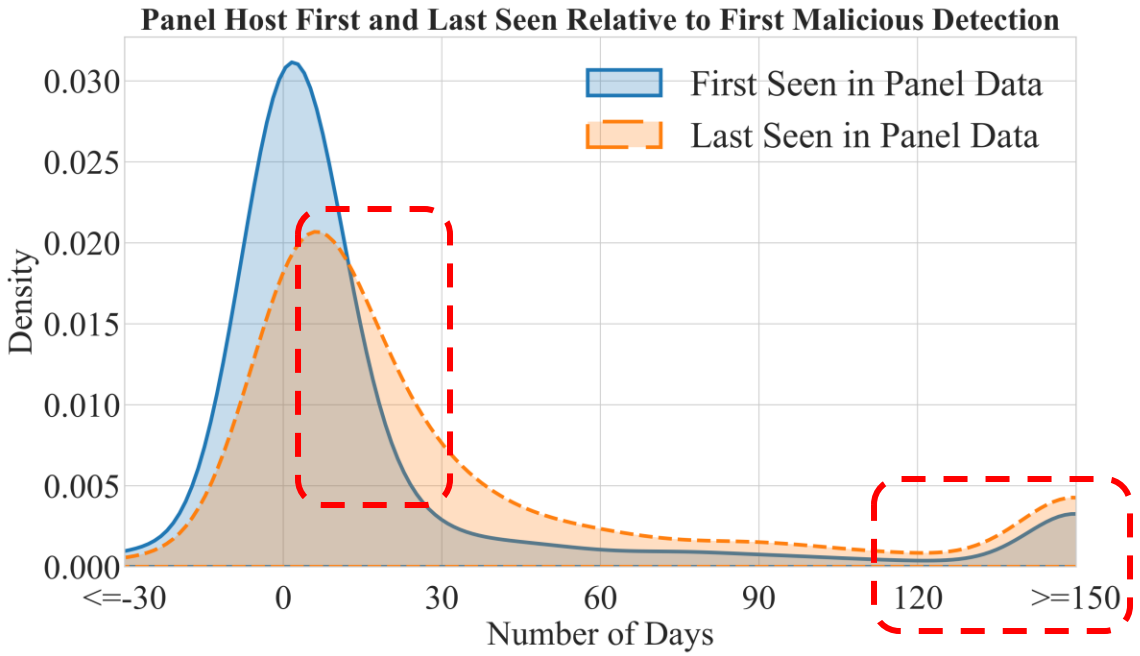
VIRUSTOTAL

urlscan.io
A sandbox for the web

Georgia Tech

Stealers Operations





- C2 Provisioning: **15** days
- Detection Lag: **64** days

- **69.03%** of operators stop accessing the panels within **30** days of detection.

Georgia Tech

Operator Network Characterization

Country	IPs	Mobile Proxy[1]	Res. Proxy [2]	Tor
Nigeria	11,375	4,326 (**38.03%**)	1,181 (**10.38**%)	0 (0%)
USA	1,936	161 (8.32%)	36 (1.86%)	15 (0.77%)
Great Britain	908	153 (16.85%)	65 (7.16%)	7 (0.77%)
South Korea	812	170 (20.93%)	14 (1.72%)	0 (0%)
Germany	496	40 (8.06%)	47 (9.47%)	10 (2.01%)

- Stealer operators make frequent use of VPN services including mobile and residential proxies make attribution difficult.
- Most operator devices are active during weekdays suggesting operators perform Stealer ops as a full-time job.

[1] X. Mi, S. Tang, Z. Li, X. Liao, F. Qian, and X. Wang, "Your phone is my proxy: Detecting and understanding mobile proxy networks," in Proc. of the 2021 NDSS, Virtual, Feb. 2021.

[2] X. Mi, X. Feng, X. Liao, B. Liu, X. Wang, F. Qian, Z. Li, S. Alrwais, L. Sun, and Y. Liu, "Resident evil: Understanding residential ip proxy as a dark service," in Proc. of the 40th S&P Oakland, May 2019.

Georgia Tech

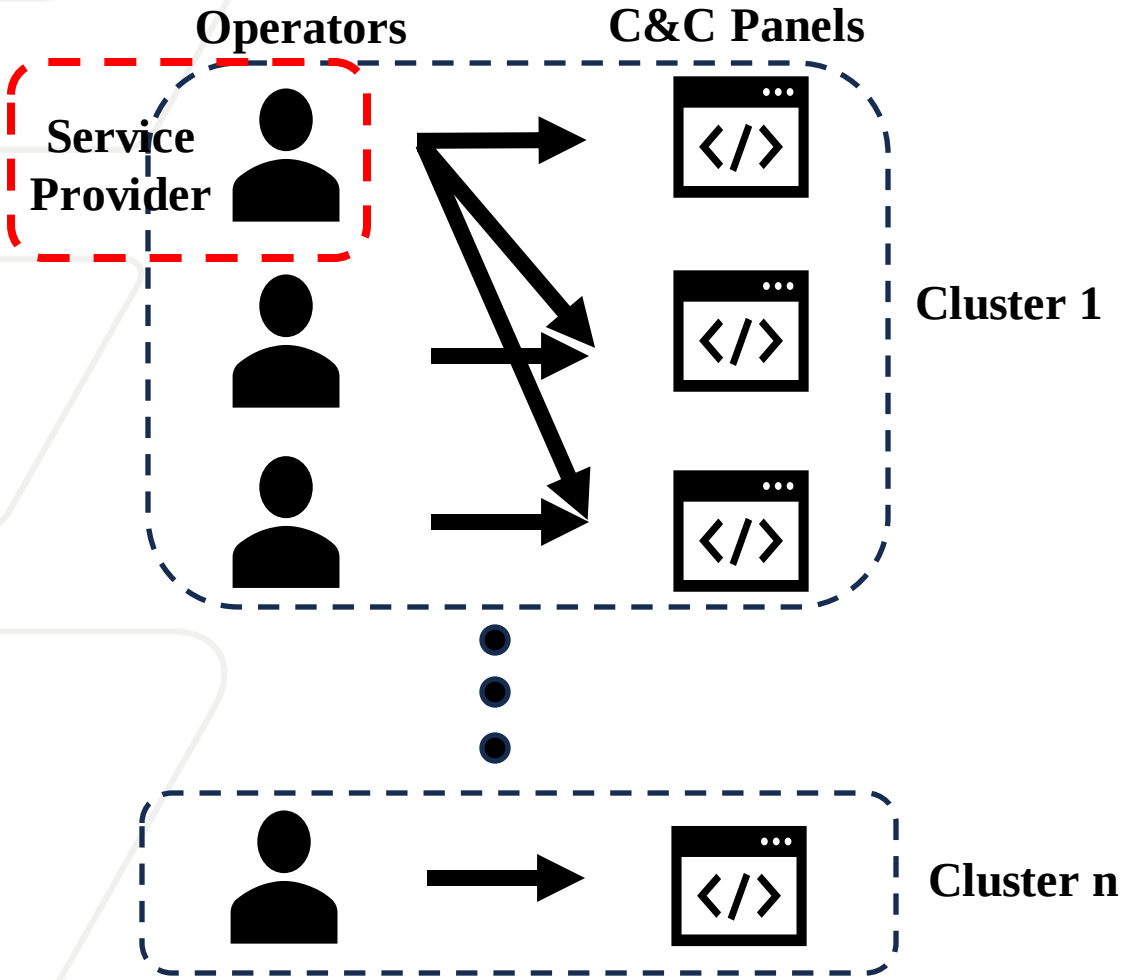
Stealer Targeting

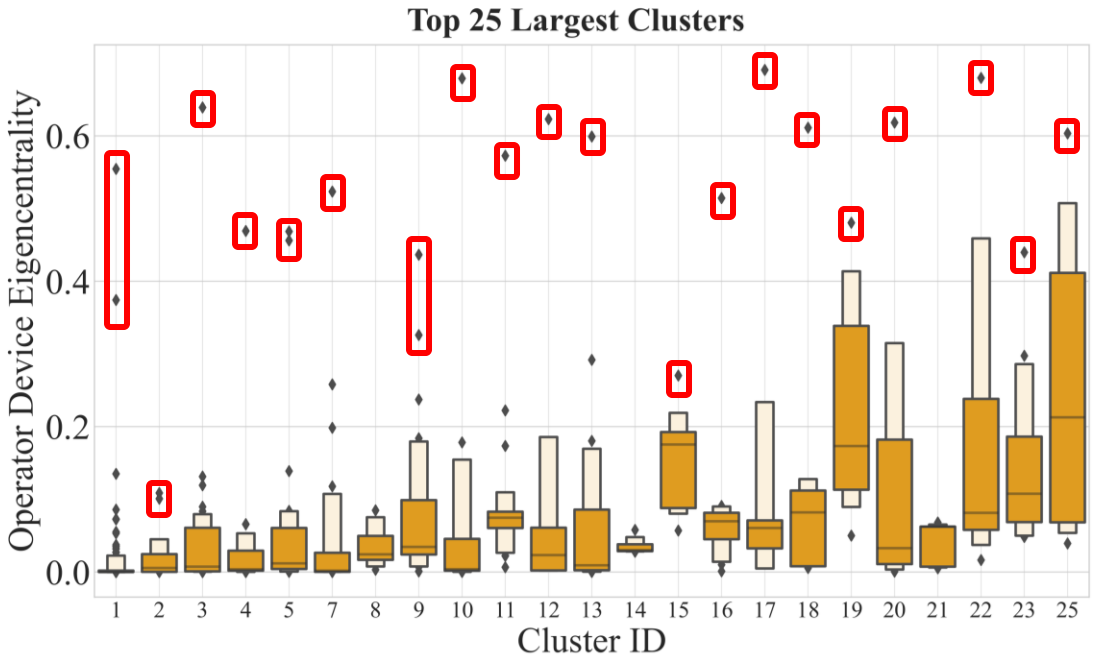
Client Networks		Business Networks		Government Networks	
Type	Count(%)	Countries	Count(%)	Countries	Count(%)
Hosting	67,958 (40.5)	U.S.A	25,315 (92.8)	U.S.A	113 (54.6)
ISP/Telco	37,463 (22.3)	Vietnam	619 (2.2)	Canada	14 (6.7)
Residential	29,595 (17.6)	U.K.	309 (1.1)	China	8 (3.8)
Business	27,269 (16.1)	S. Korea	152 (0.5)	Italy	6 (2.9)
Education	5,143 (3.0)	India	117 (0.4)	Indonesia	5 (2.4)
Government	207 (0.1)	Nigeria	108 (0.4)	Israel	4 (1.9)
Health	188 (0.1)	China	69 (0.2)	India	4 (1.9)

- United States account for most of the business and governmental network targeting.

Georgia Tech

Operator Characterization

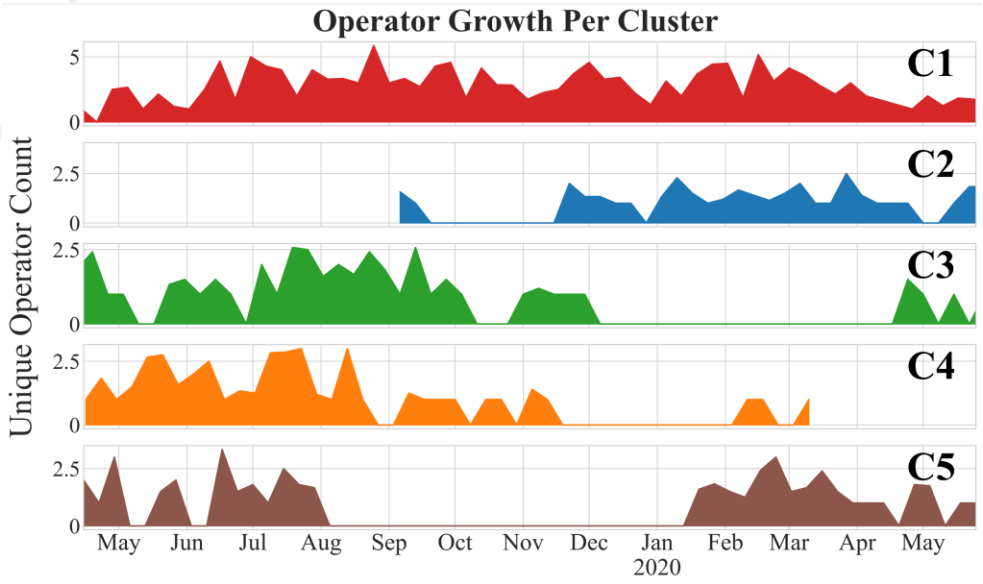




- Each service provider has **1 to 2** most influential operators.
- The largest **1%** service providers account for most of the activities.

Georgia Tech

Top 5 Stealer Clusters



- The top service providers appear to operate for over a year and enjoy **high profit margins** with most over **90%**.
- The profit margins range from approximately **$2,000** to **$11,000** per month for the top service providers.

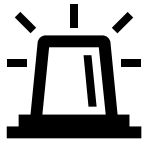
Name	Size	Days Seen	Operators	One-Off Cost	Hosting Cost	Revenue	Profit	Margin
C1	285	689	127	$5,481	$923	$11,834	$10,910	92.2%
C2	84	468	15	$595	$200	$5,440	$5,240	96.33%
C3	72	418	37	$963	$37	$2,579	$2,541	98.55%
C4	68	332	24	$121	$638	$3,440	$2,801	81.45%
C5	57	415	26	$2,592	$89	$1,930	$1,841	95.39%

Georgia Tech

Findings and Takeaways

The PWS market is **mature** with a **low** technical and financial **entry barrier**.

The security community needs to pay more **attention** to stealers attacks as their stolen credentials are often used in **future data breaches**.



The security community detection of PWS **lags** for an average of **64** days after C2 provisioning.

Researchers can use tailored Internet-wide **scanning** to identify PWS C&C panels faster.

PWS service providers enjoy large **profit margins** of over **90%** with profits from **$2,000** to **$11,000** per month.

We make 6 months of the PWS dataset along with code available at: https://github.com/Astrolavos/stealer-sec23

Georgia Tech