SecurityScorecard

Ransomware: a correlation between infection vectors and victims

Doina Cosovan, Catalin Valeriu Lita,
Jue Mo, Ryan Sherstobitoff

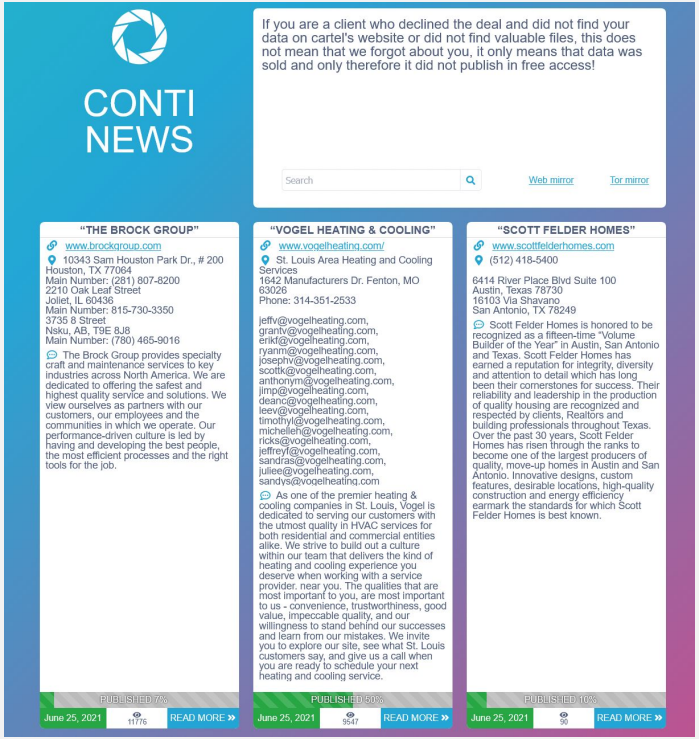
Virus Bulletin 2021

Ransomware Infection Stages

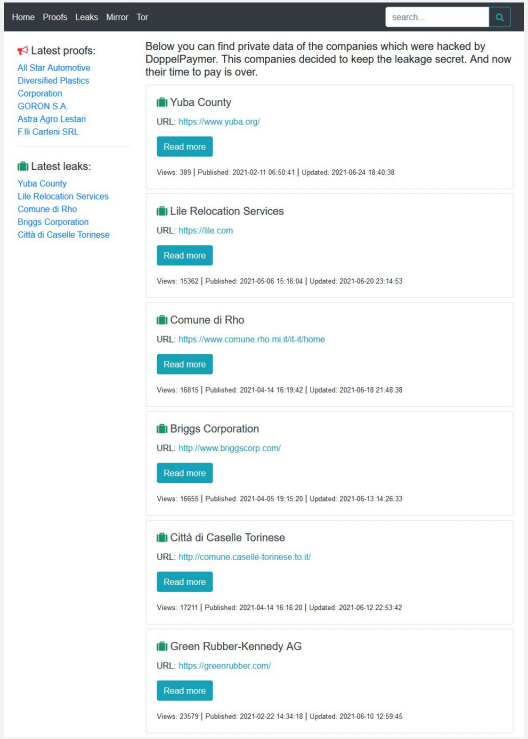
- **Initial access**
- **Local operations**
- **Data exfiltration**
- Data encryption
- Ransom payment or **data leakage**

Ransomware Leaks Websites

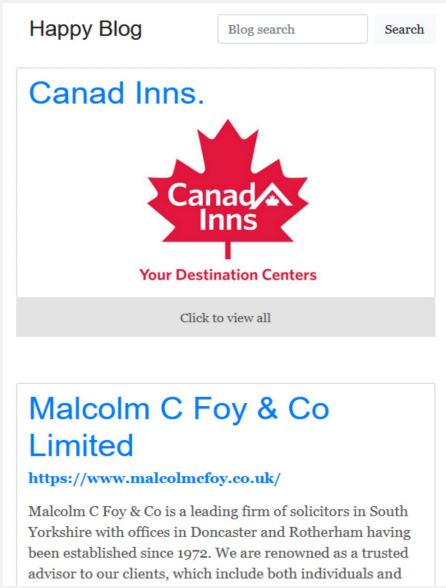
Conti



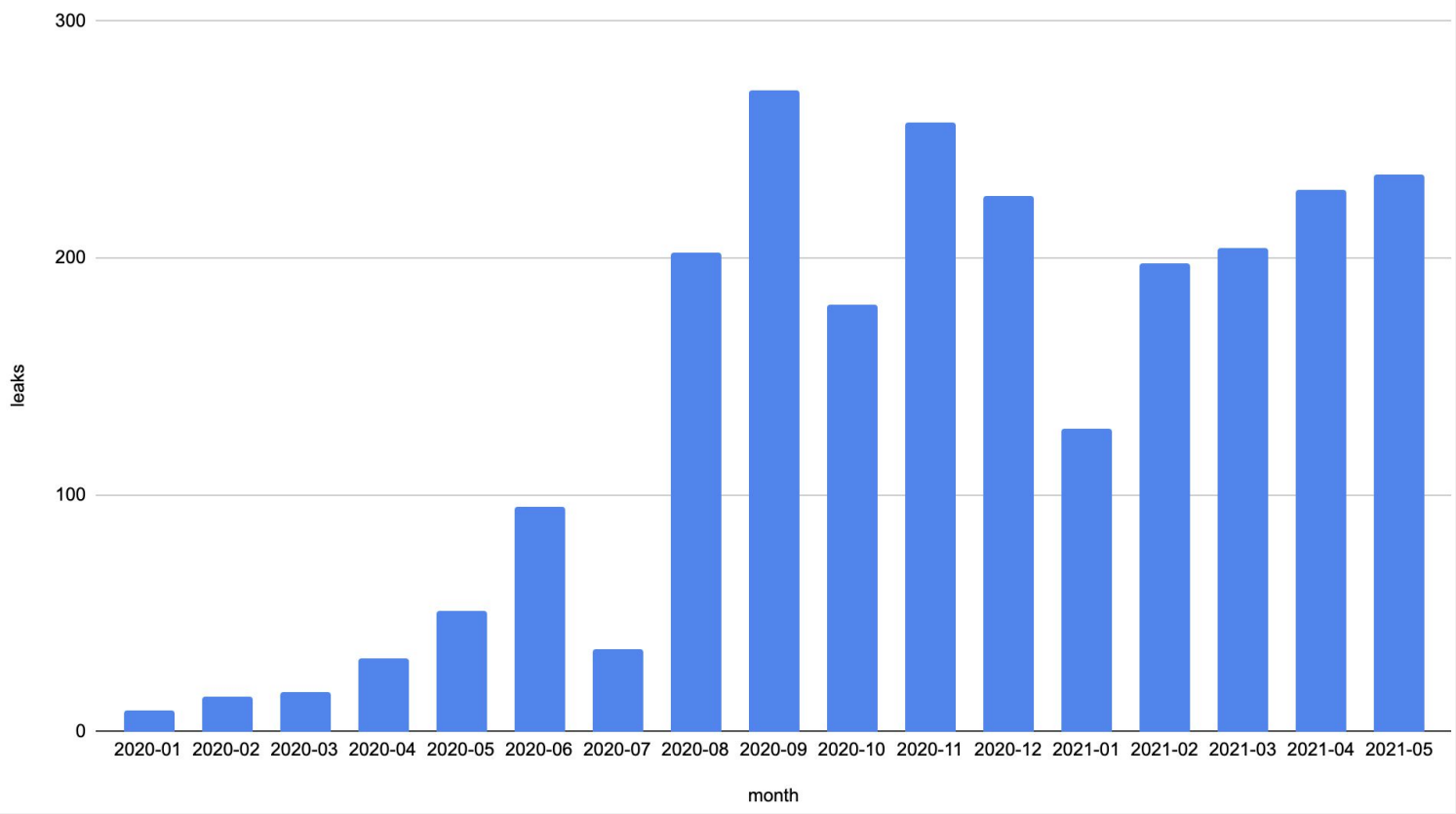
DoppelPaymer



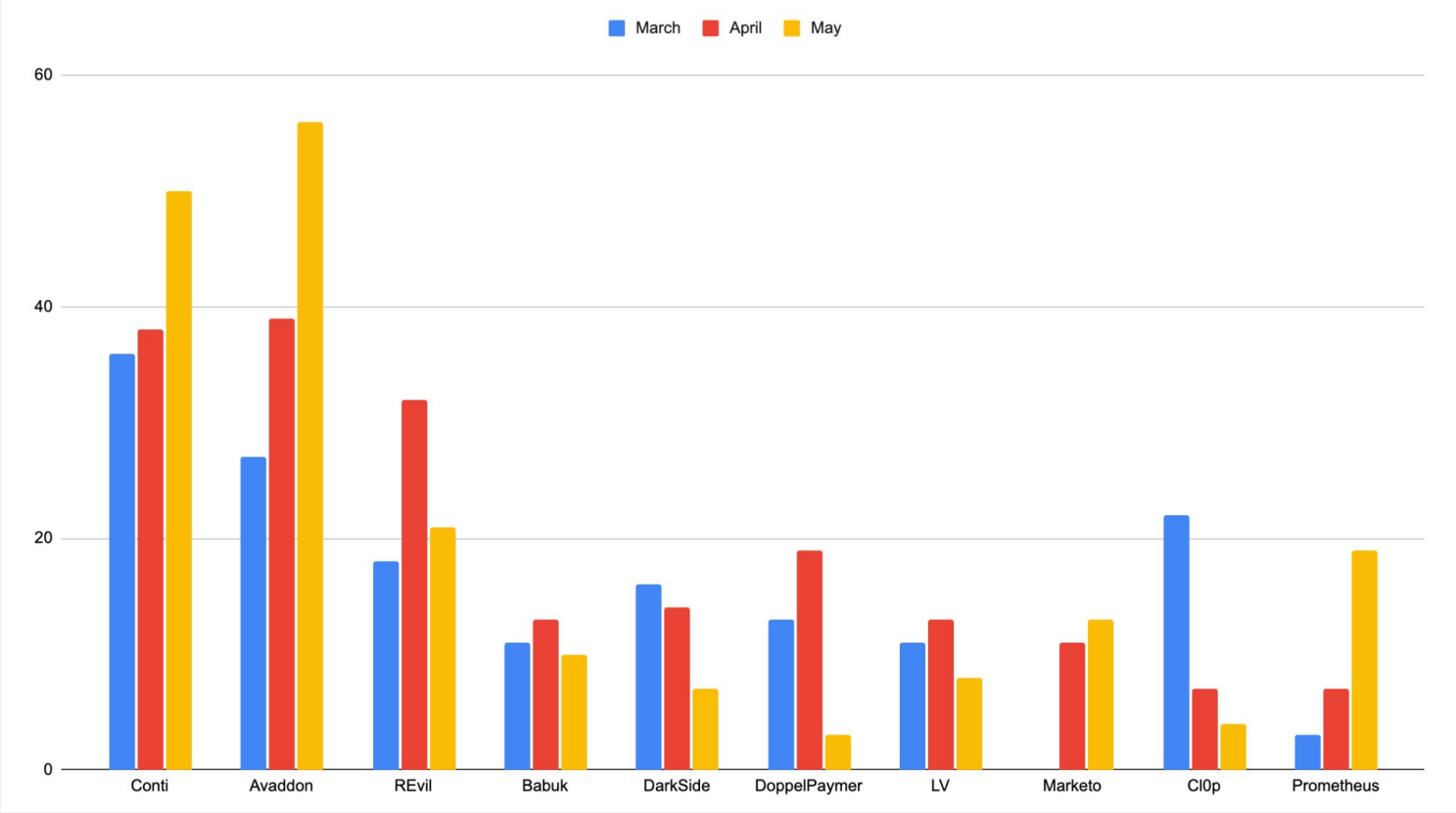
REvil



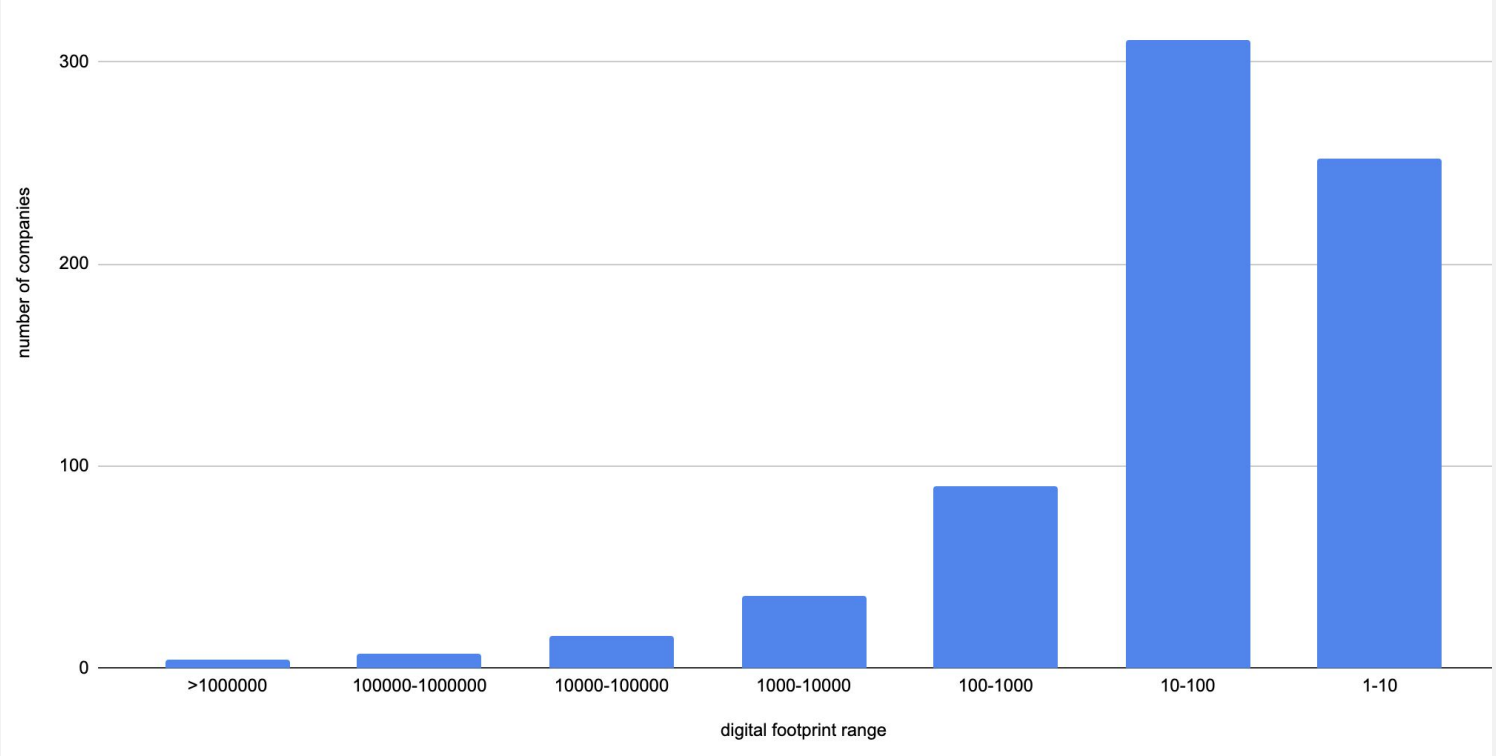
Ransomware leaks per month



Ransomware leaks March-May 2021



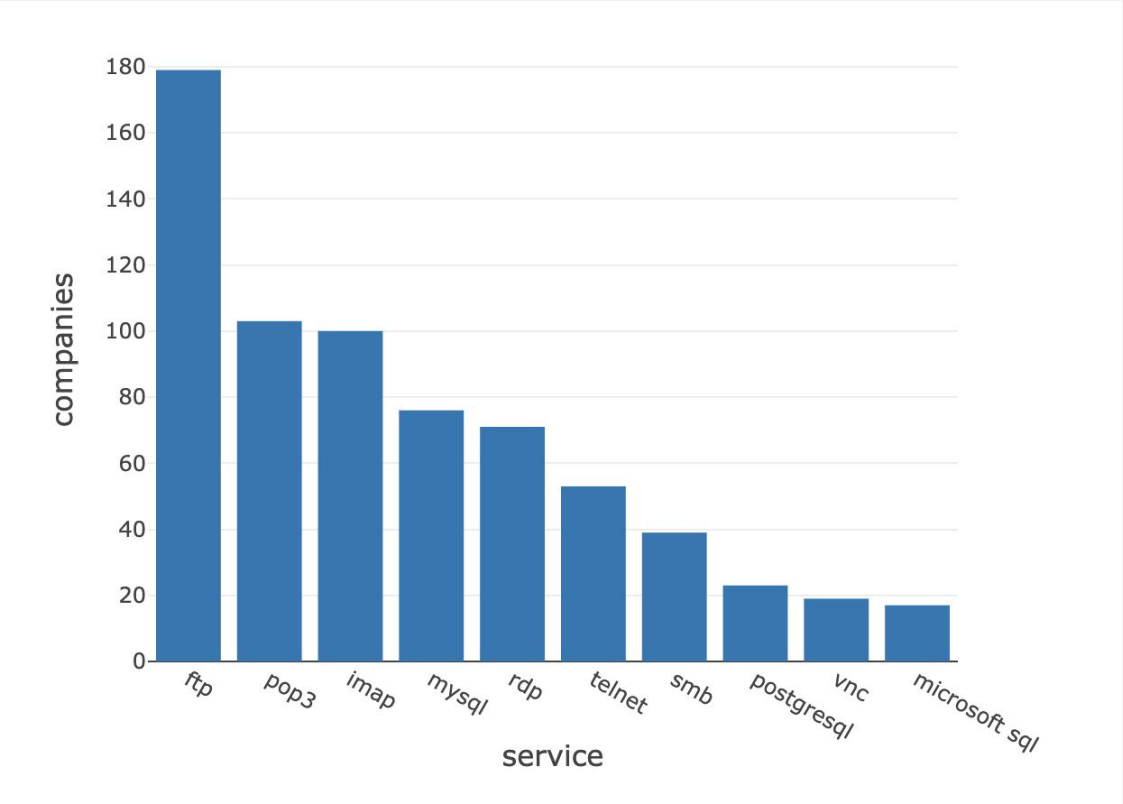
Digital Footprint



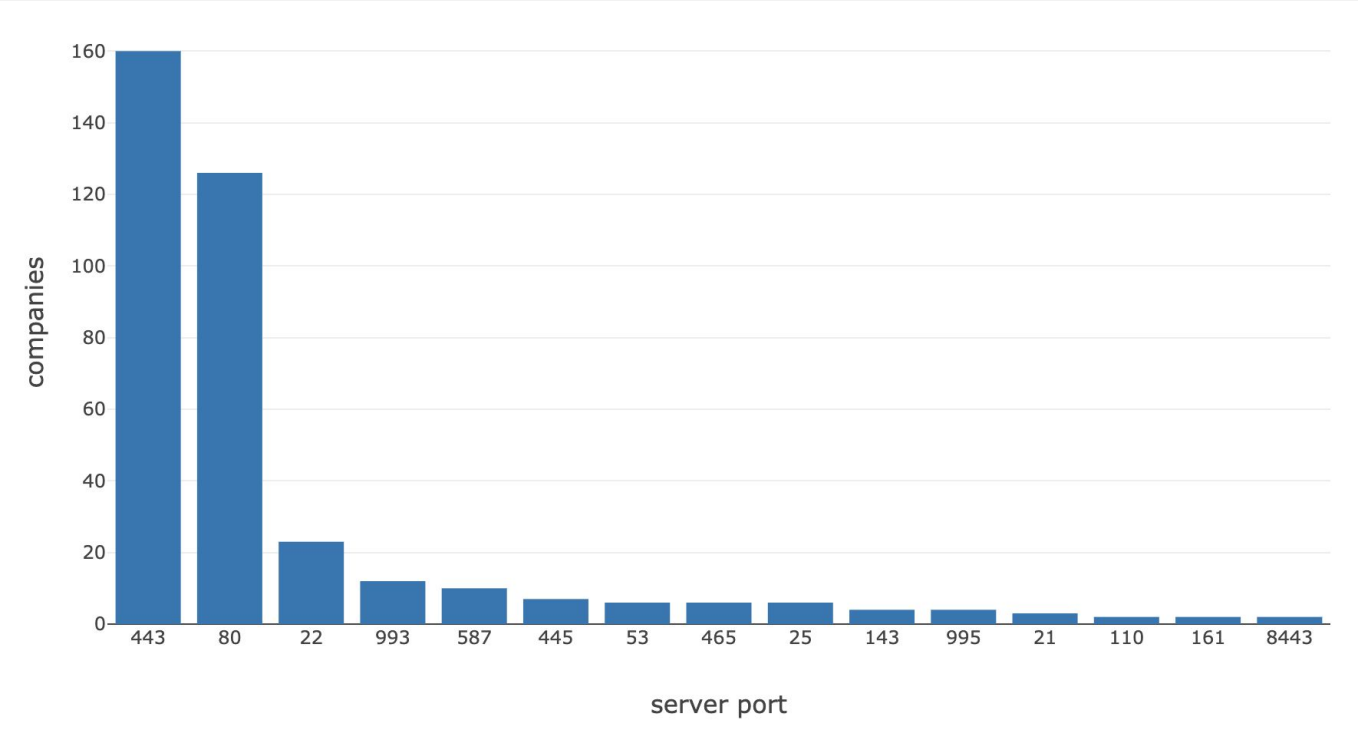
Initial Access

- Exposed services
- Vulnerabilities
- Spam
- Leaked Credentials
- Application Security
- Malware Infections

Initial Access: Exposed Services



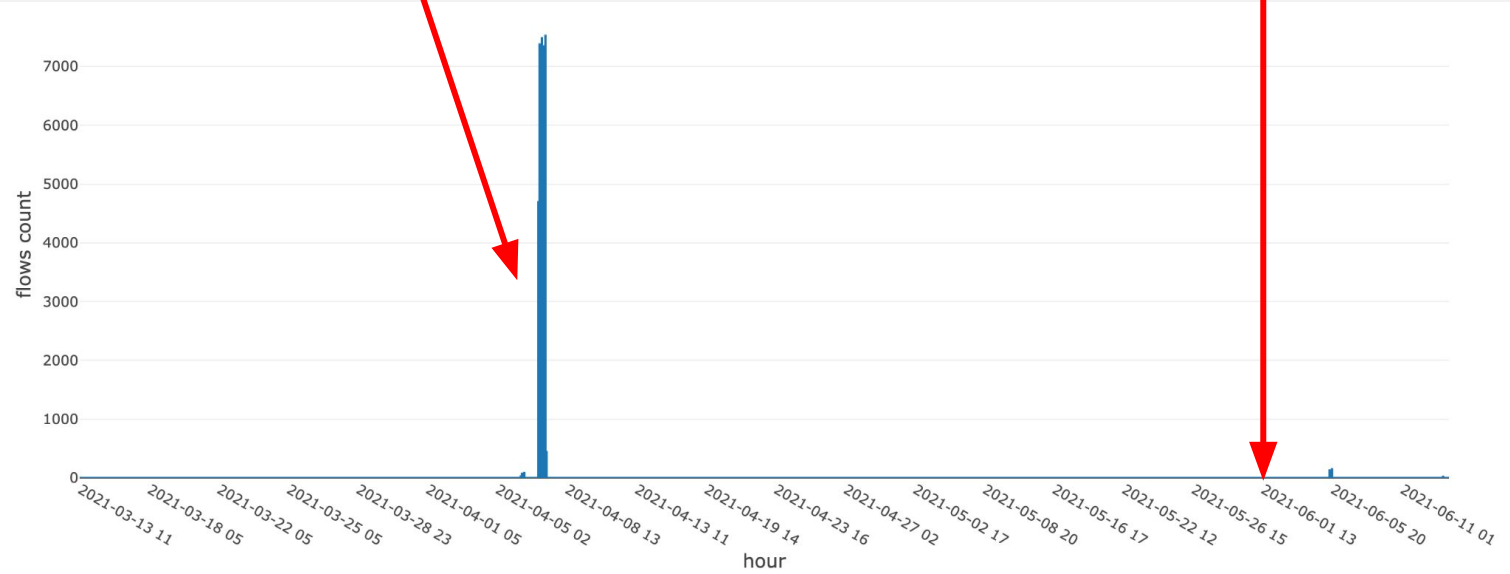
Initial Access: Abused Services



Use Case: SSH Brute Forcing

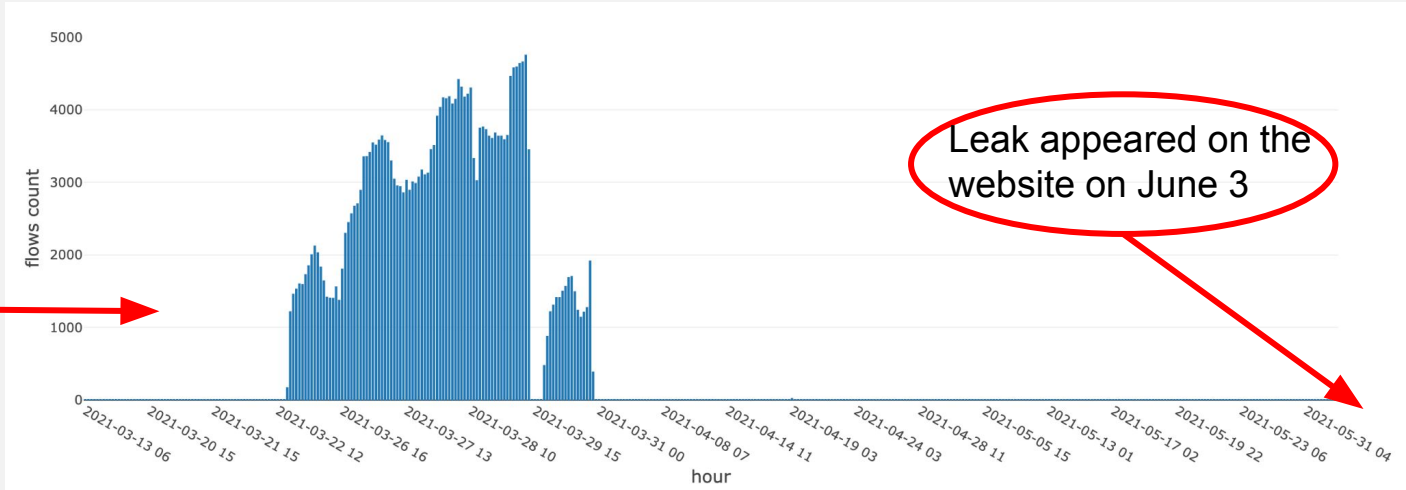
SSH brute forcing on April 7 between 7 AM and 12 AM

Leak appeared on website on May 30



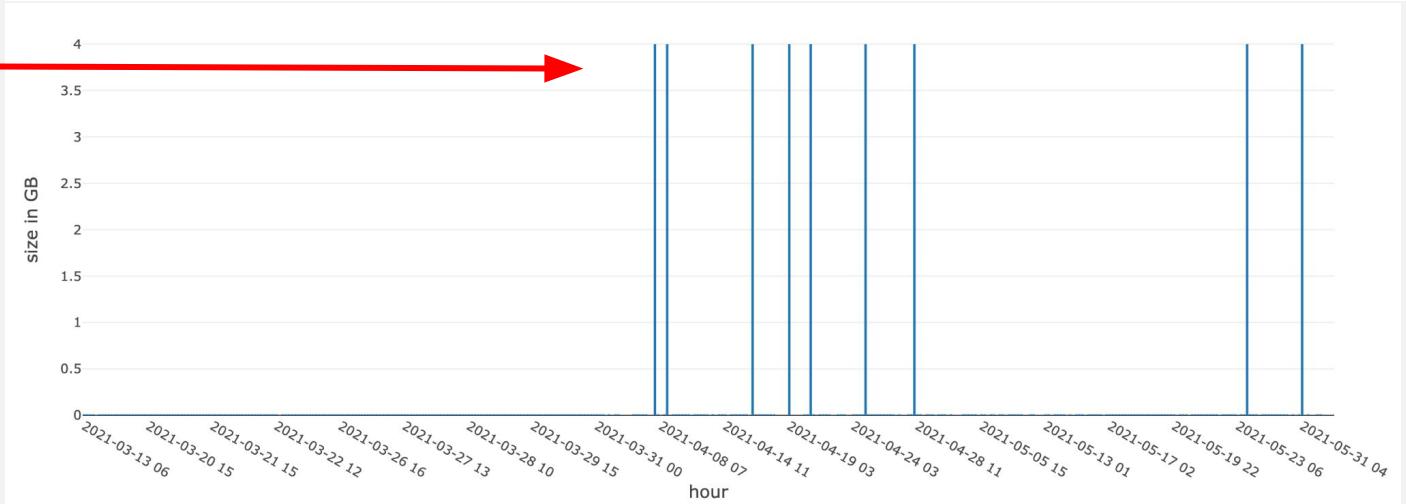
Use Case: RDP

RDP brute forcing between March 25 and March 30

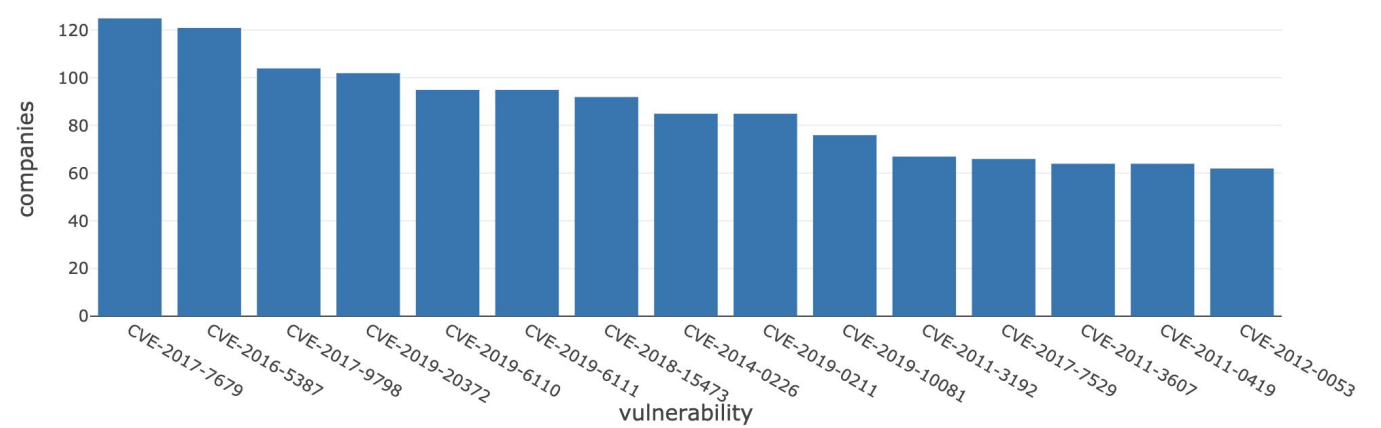


Leak appeared on the website on June 3

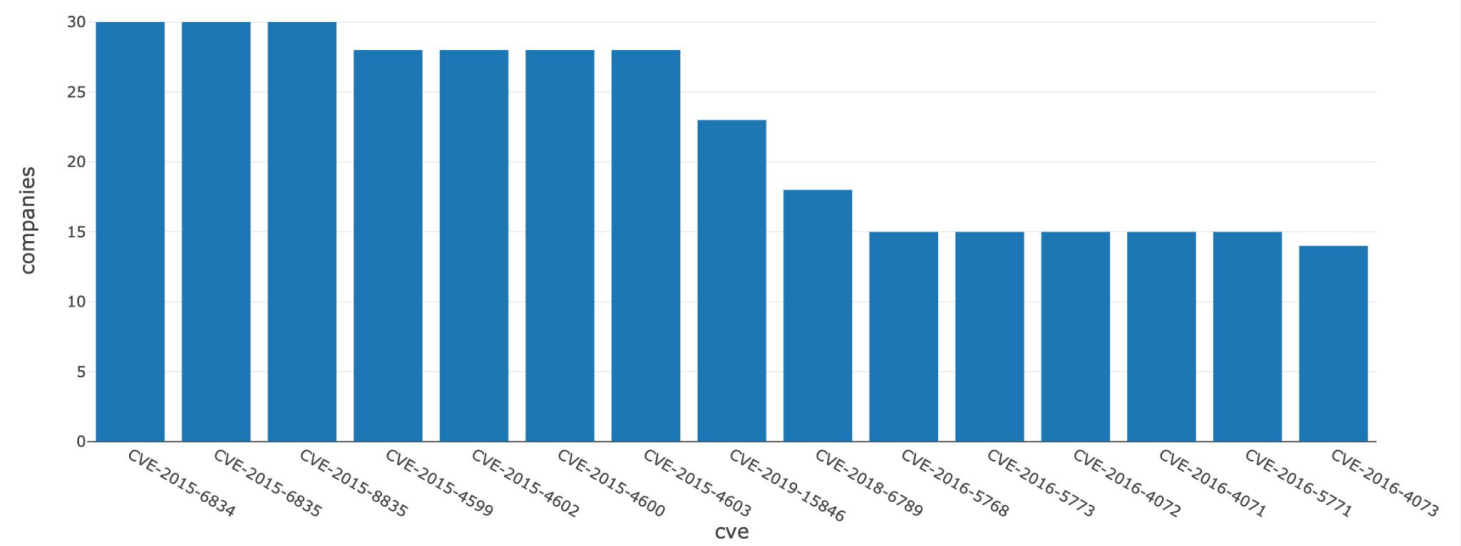
RDP exfiltration between April 25 and April 30



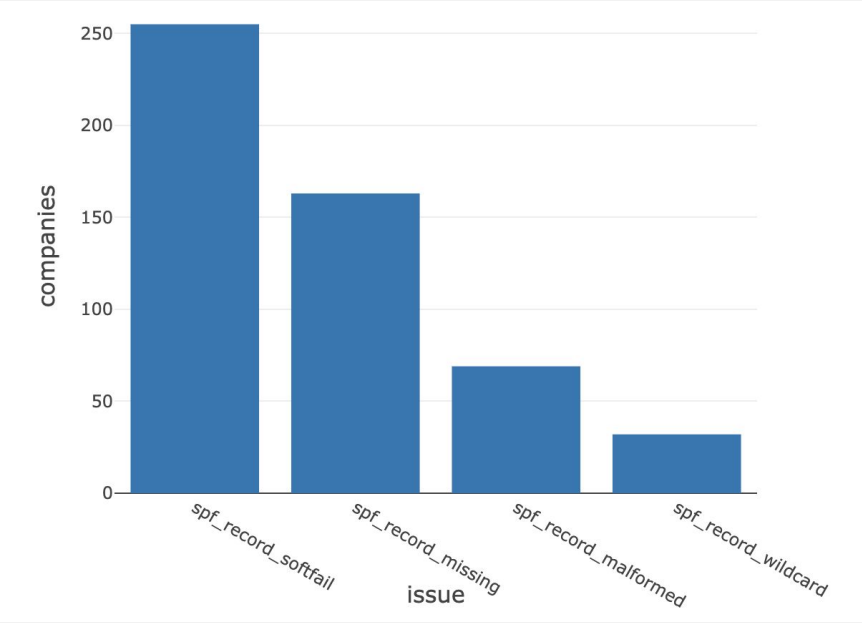
Initial Access: CVEs with POC



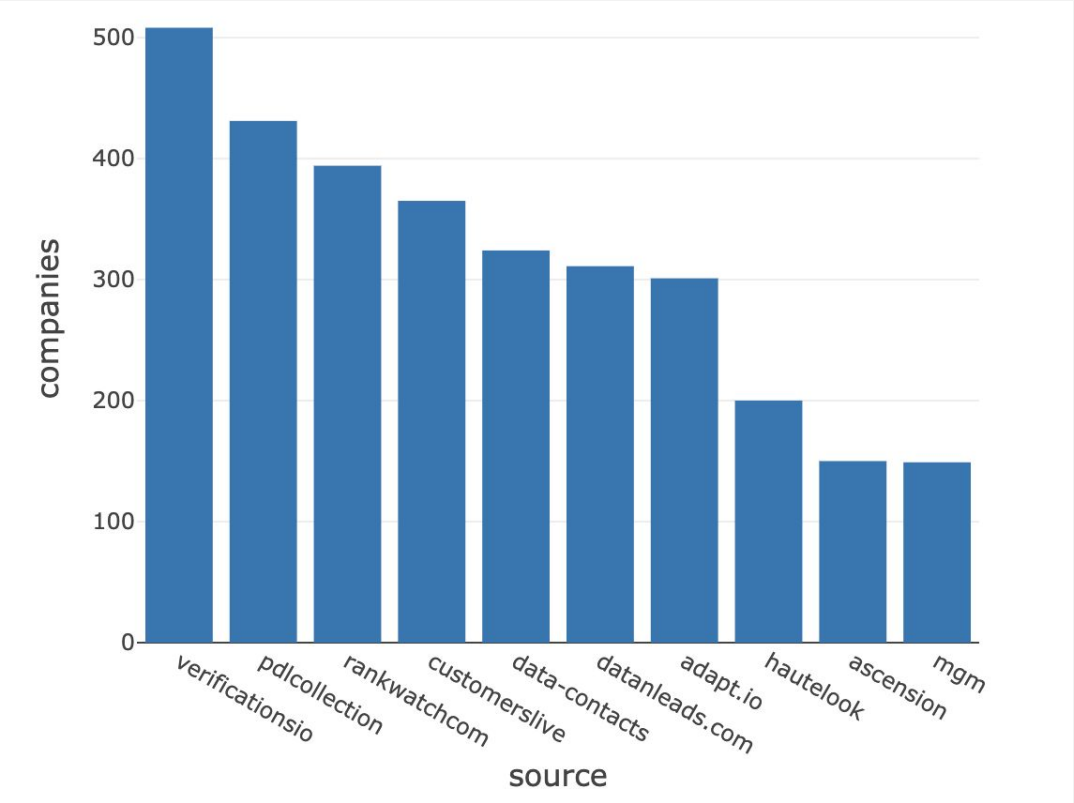
Initial Access: RCE CVEs



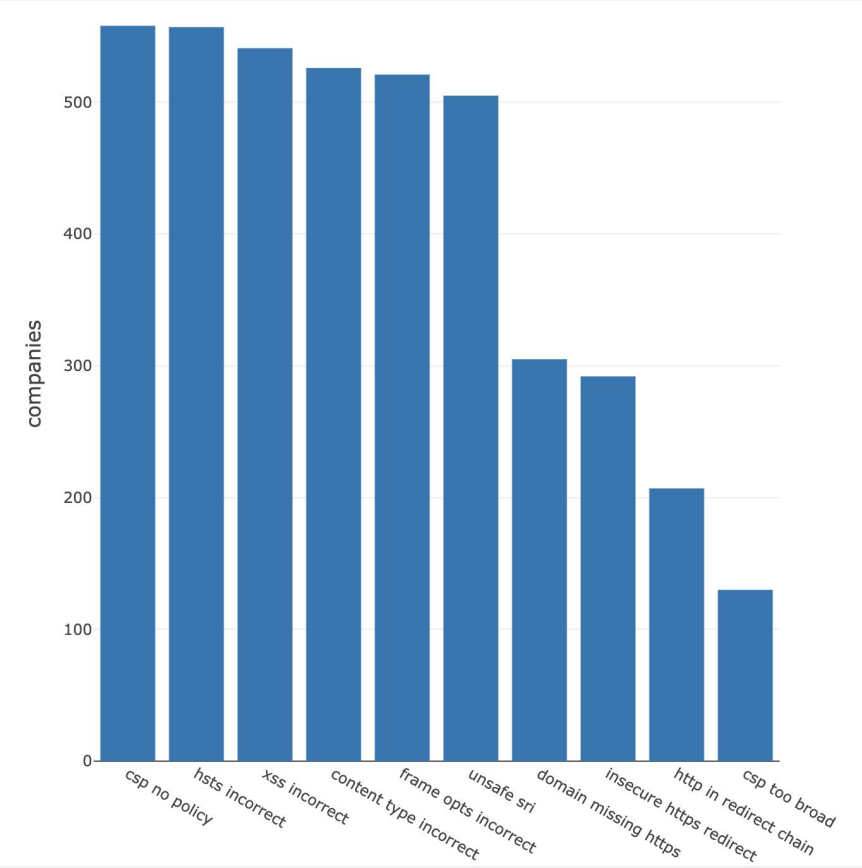
Initial Access: Spam



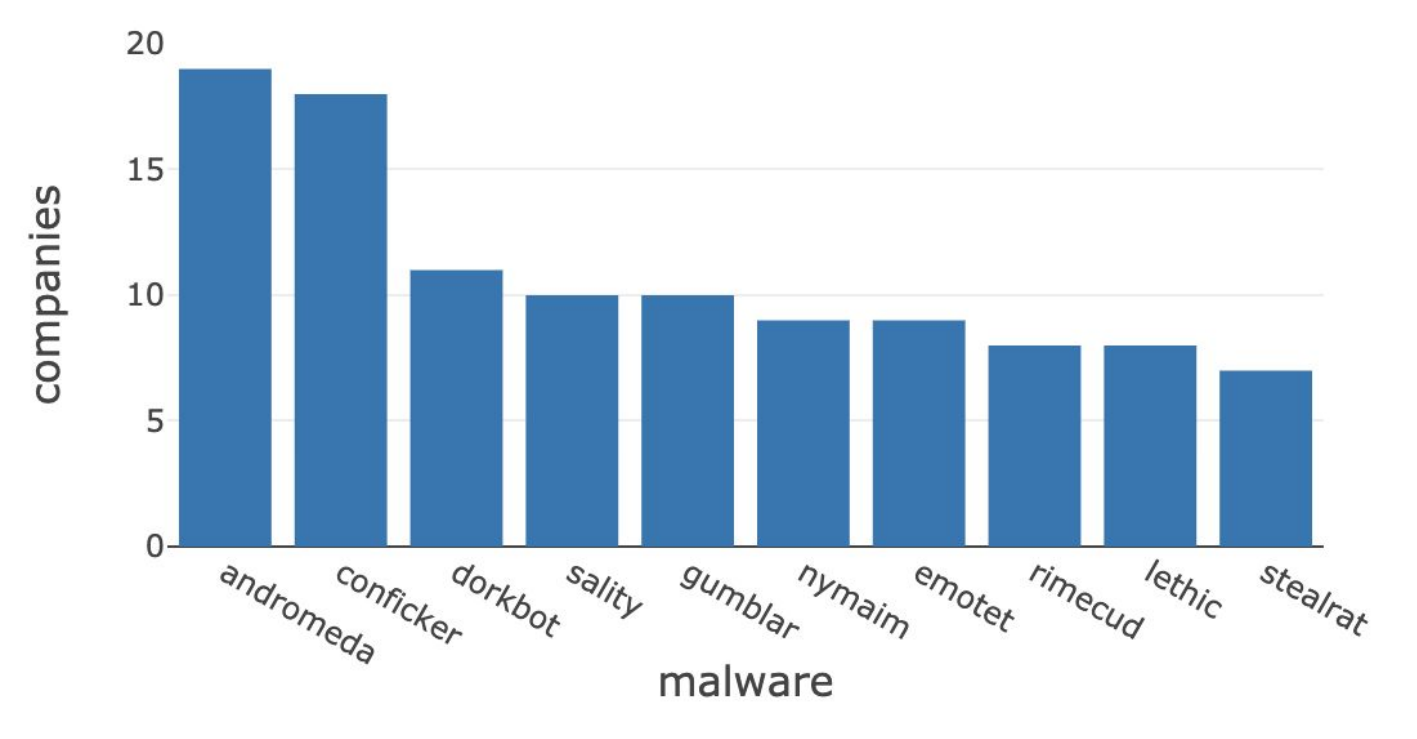
Initial Access: Leaked Credentials



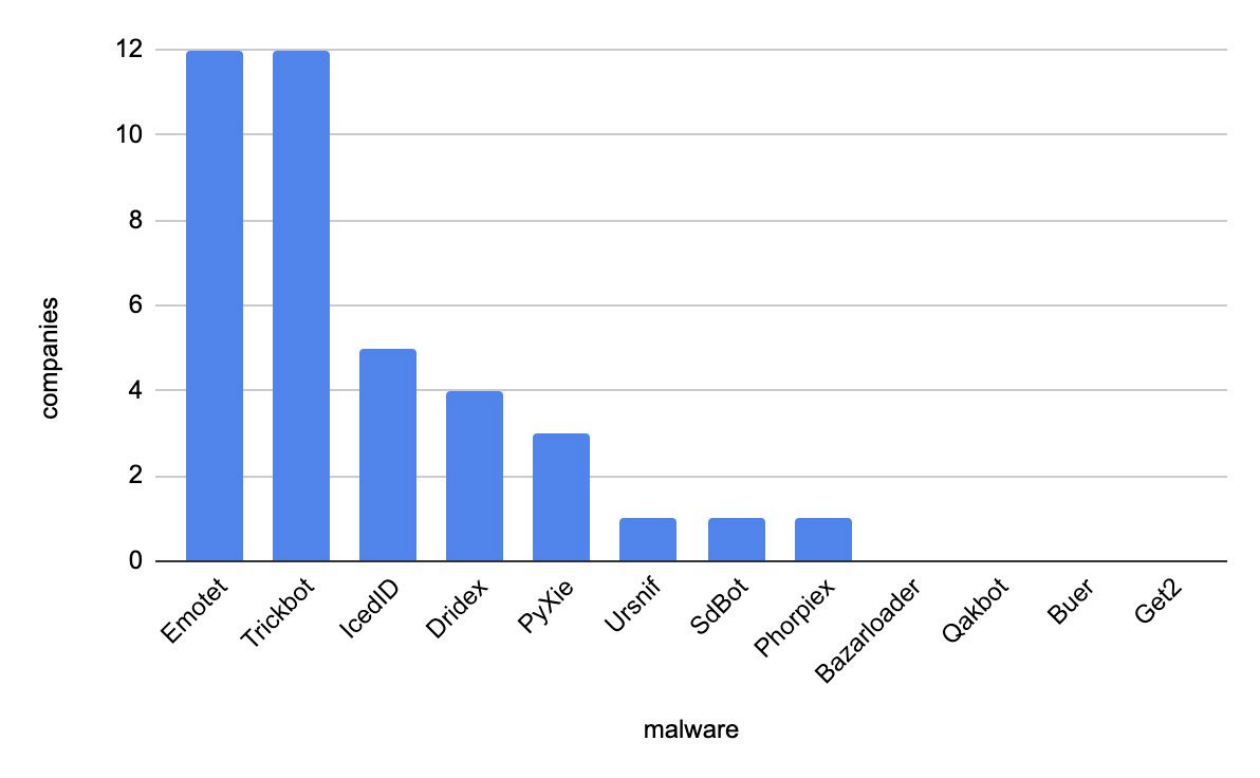
Initial Access: Application Security



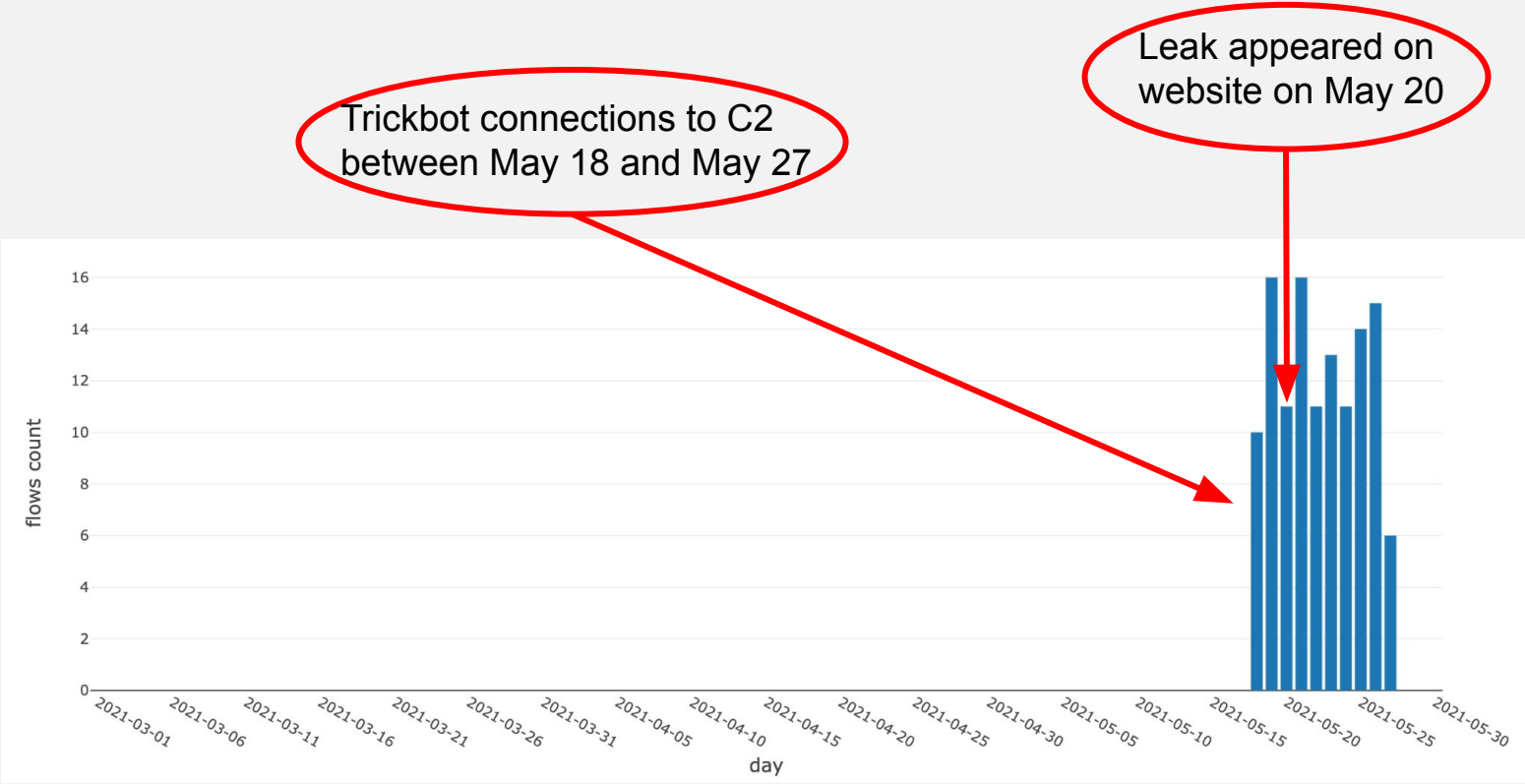
Initial Access: Malware from sinkholes



Initial Access: Ransomware related malware from netflow

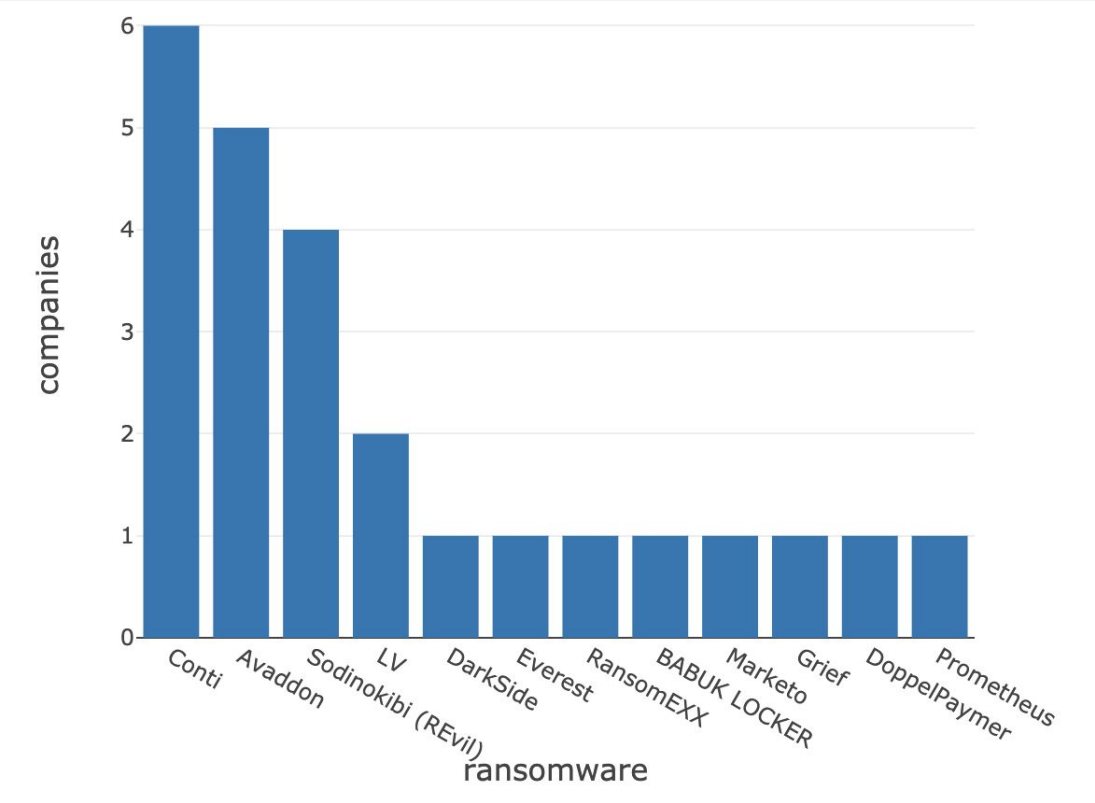


Trickbot infection



Lateral Movement

Lateral movement: Cobalt Strike

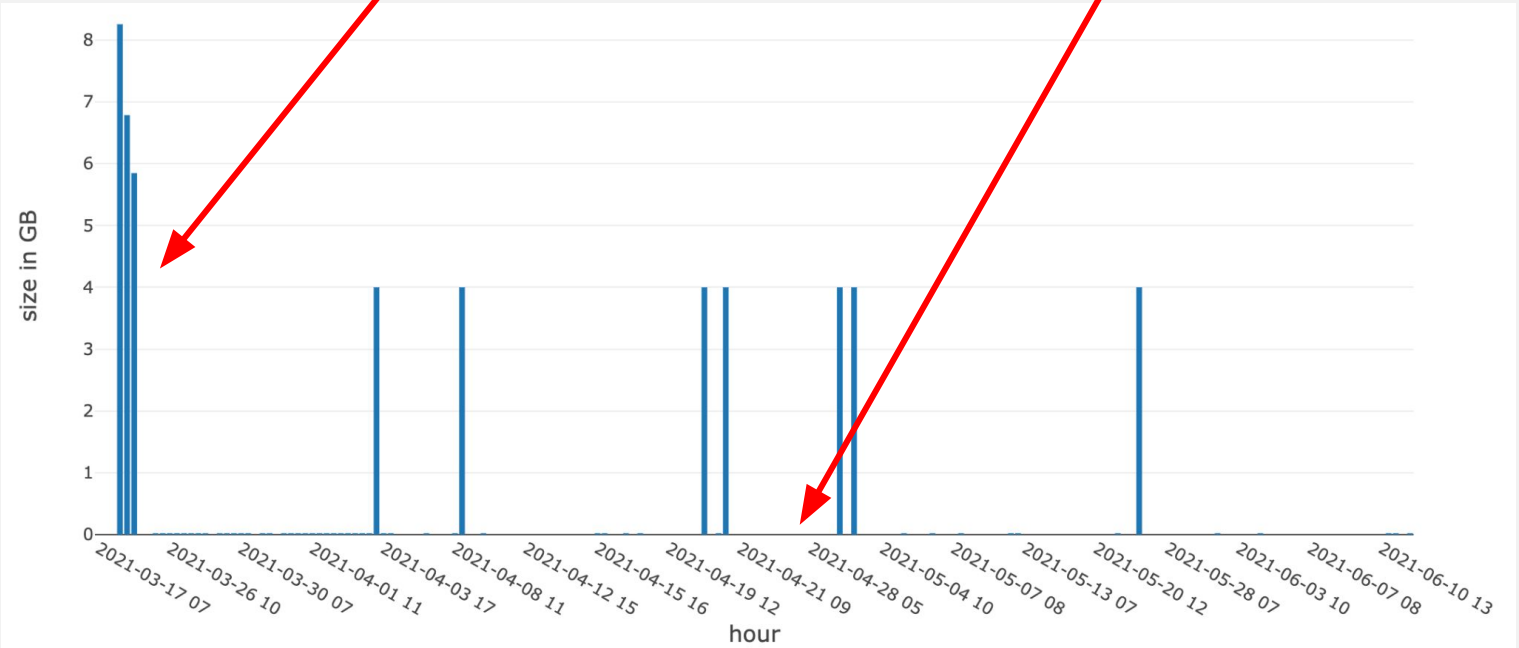


Exfiltration

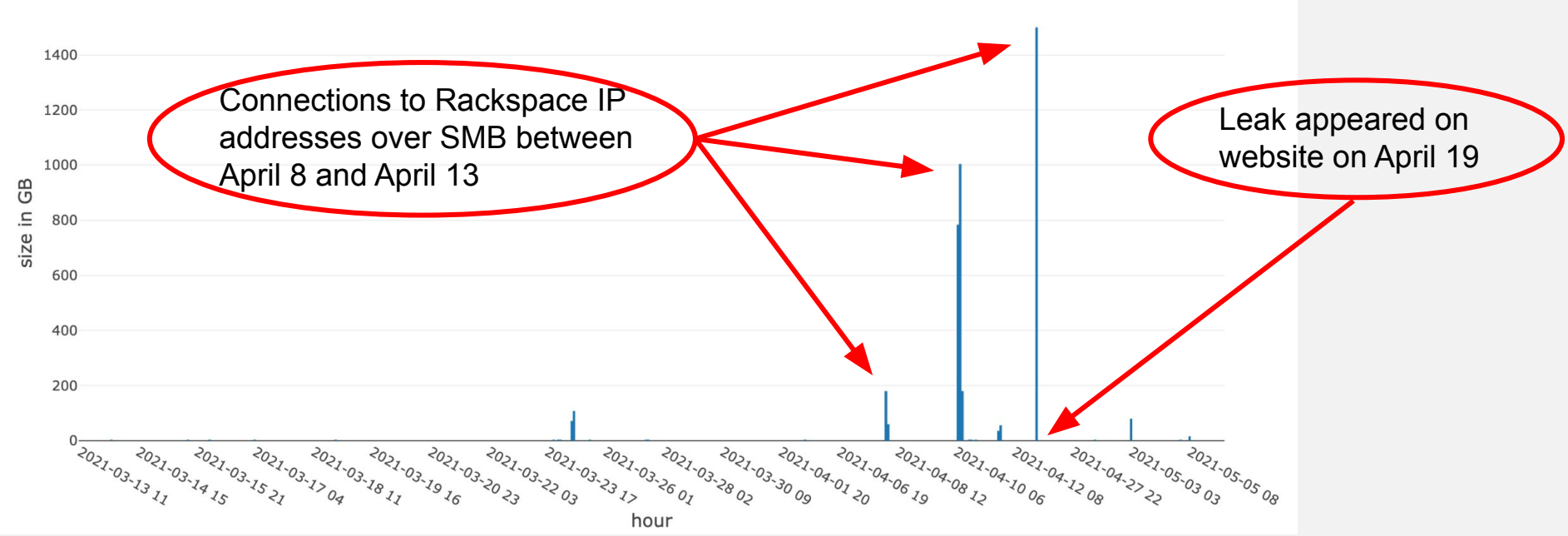
REvil exfiltration to Mega over HTTPS

Connections to 3 Mega IP addresses on March 21 between 3 AM and 3 PM

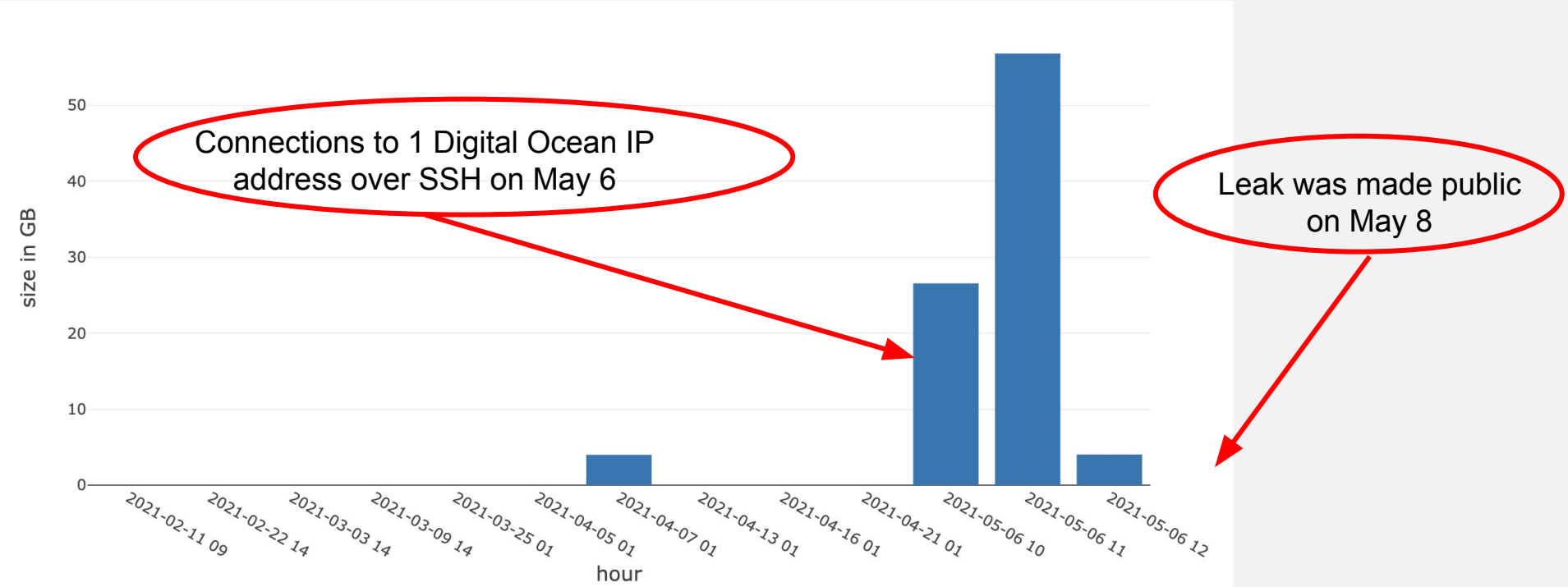
Leak appeared on website on April 26



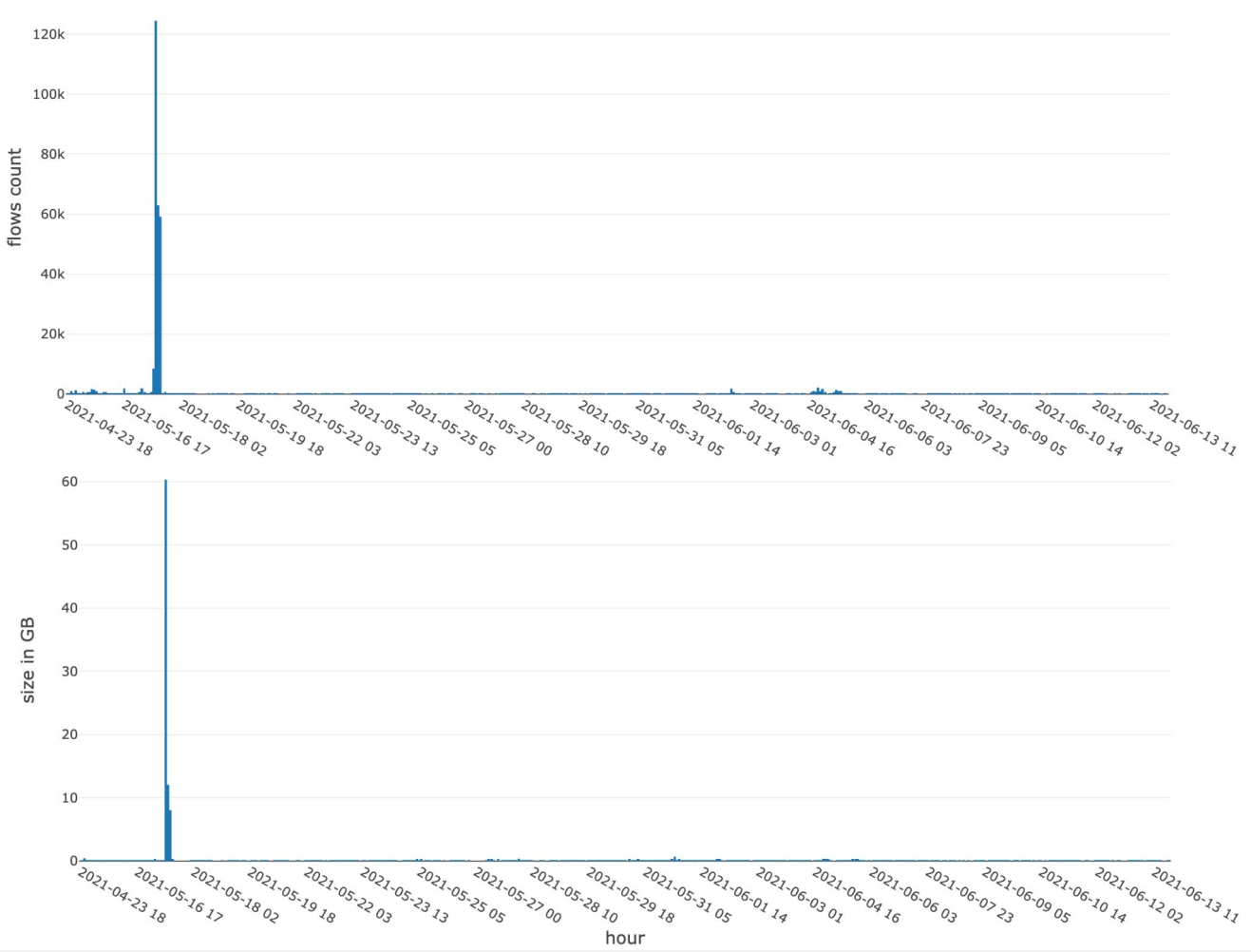
LV exfiltration to Rackspace over SMB



DarkSide exfiltration to Digital Ocean over SSH



Post Leak Exfiltration


flows count
120k
100k
80k
60k
40k
20k
0
2021-04-23 18
2021-05-16 17
2021-05-18 02
2021-05-19 18
2021-05-22 03
2021-05-23 13
2021-05-25 05
2021-05-27 00
2021-05-28 10
2021-05-29 18
2021-05-31 05
2021-06-01 14
2021-06-03 01
2021-06-04 16
2021-06-06 03
2021-06-07 23
2021-06-09 05
2021-06-10 14
2021-06-12 02
2021-06-13 11
size in GB
60
50
40
30
20
10
0
hour

HTTPS

Recommendations

- **Credentials**: don’t reuse credentials, use strong passwords, use a password manager, use Multi Factor Authentication, don’t make your phone number and email address easily accessible.
- **Exposed services**: minimize the exposed digital footprint, use strong authentication where applicable, put services behind VPN where applicable.
- **Vulnerabilities**: patch them immediately especially if they provide Remote Code Execution or Privilege Escalation and if there is a publicly or commercially available proof of concept.
- **Malware**: use an up-to-date Anti-Malware product.
- **Exfiltration**: use an Intrusion Detection System (IDS) / Intrusion Prevention System (IPS) / Firewall, monitor for and block large outgoing amounts of data.

Conclusions