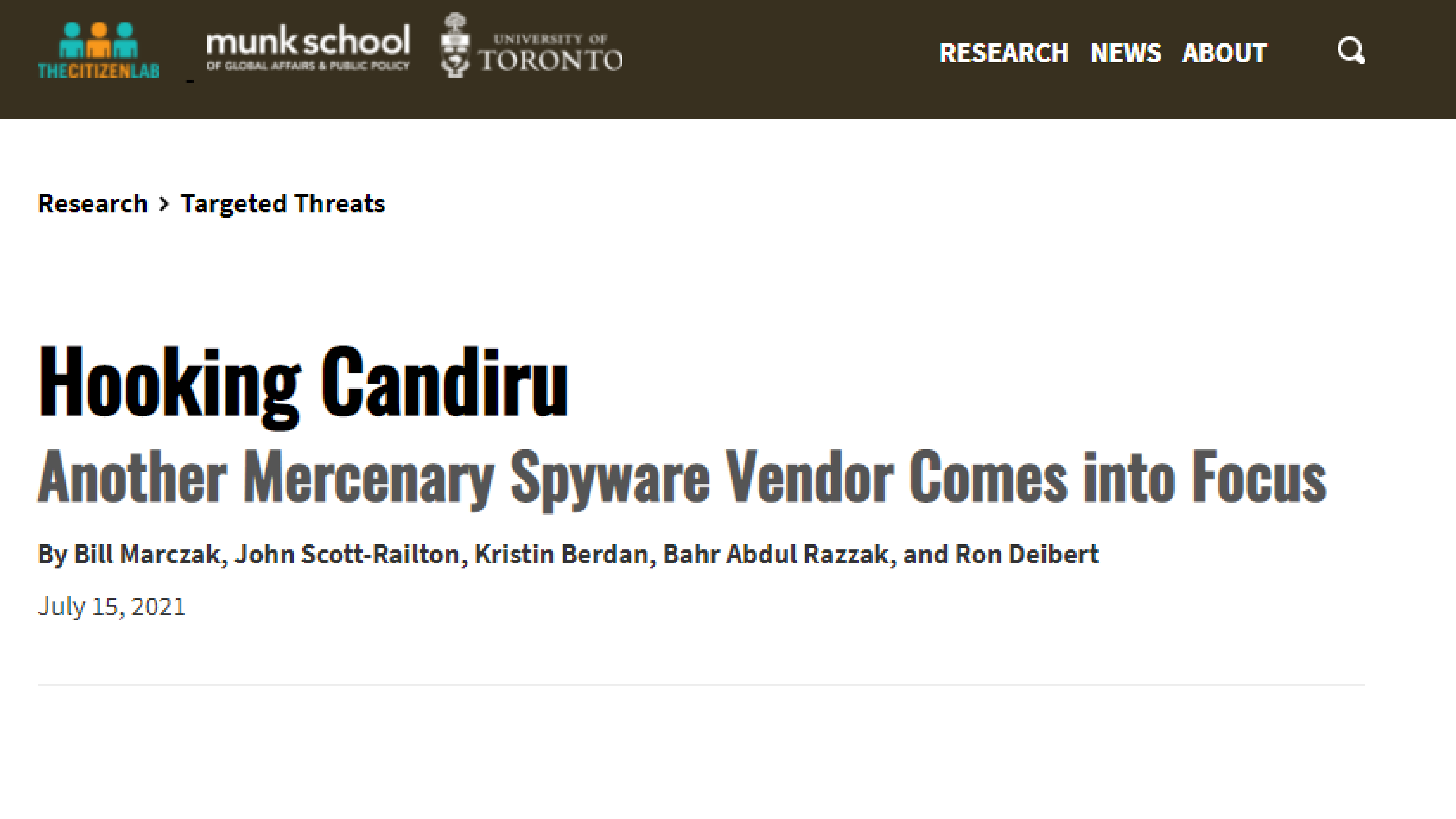
Respeito à Privacidade e aos Direitos Civis



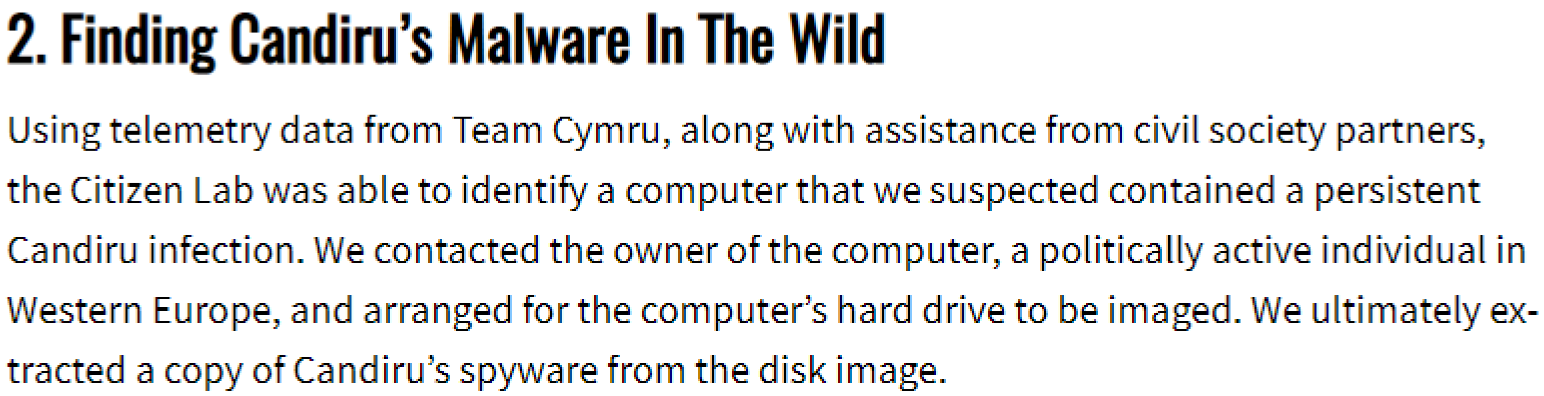
Research › Targeted Threats

Hooking Candiru

Another Mercenary Spyware Vendor Comes into Focus

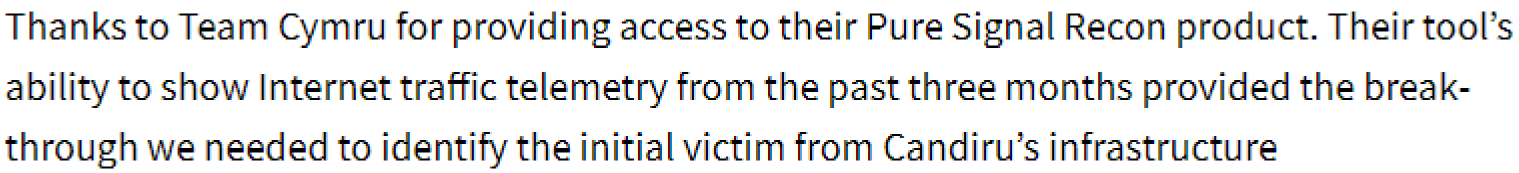
By Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert

July 15, 2021

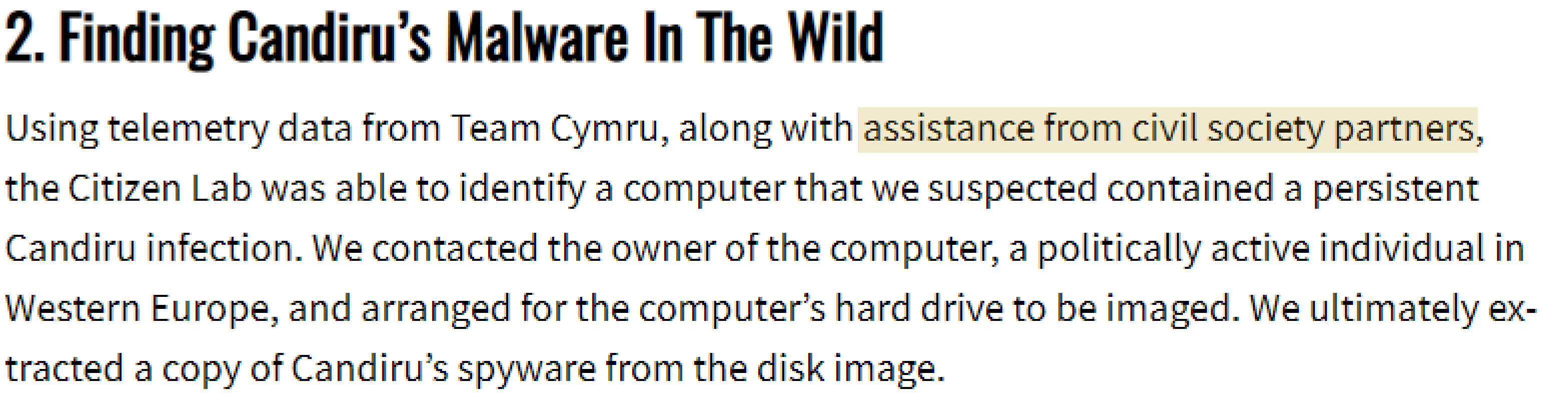


2. Finding Candiru's Malware In The Wild

Using telemetry data from Team Cymru, along with assistance from civil society partners, the Citizen Lab was able to identify a computer that we suspected contained a persistent Candiru infection. We contacted the owner of the computer, a politically active individual in Western Europe, and arranged for the computer's hard drive to be imaged. We ultimately extracted a copy of Candiru's spyware from the disk image.

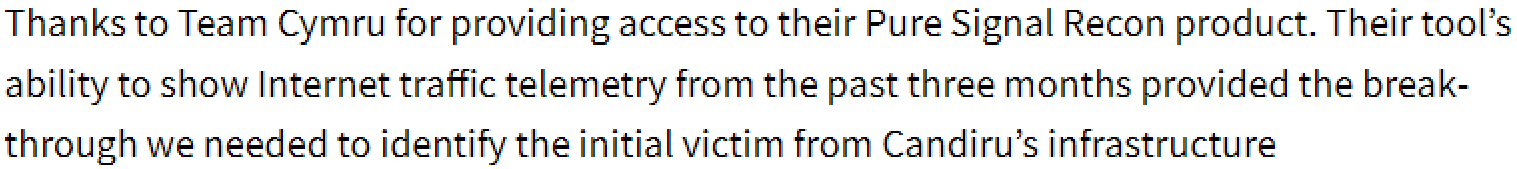


Thanks to Team Cymru for providing access to their Pure Signal Recon product. Their tool's ability to show Internet traffic telemetry from the past three months provided the breakthrough we needed to identify the initial victim from Candiru's infrastructure

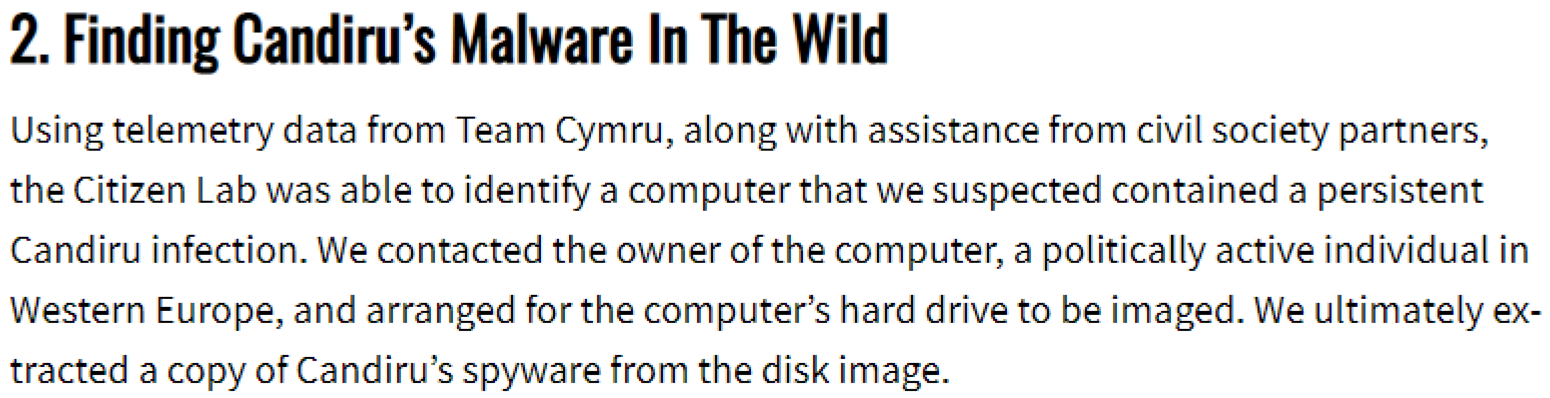


2. Finding Candiru’s Malware In The Wild

Using telemetry data from Team Cymru, along with assistance from civil society partners, the Citizen Lab was able to identify a computer that we suspected contained a persistent Candiru infection. We contacted the owner of the computer, a politically active individual in Western Europe, and arranged for the computer’s hard drive to be imaged. We ultimately extracted a copy of Candiru’s spyware from the disk image.

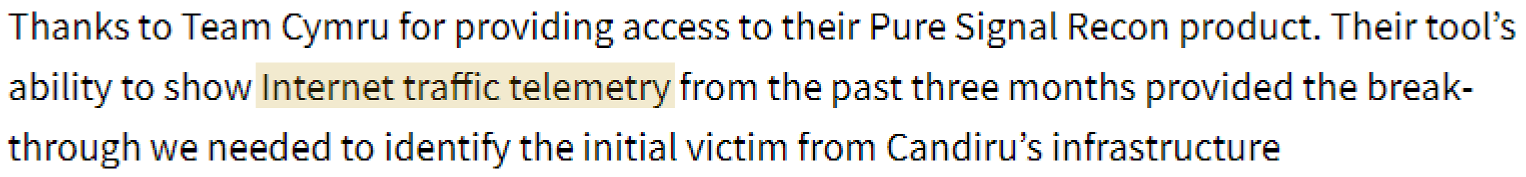


Thanks to Team Cymru for providing access to their Pure Signal Recon product. Their tool’s ability to show Internet traffic telemetry from the past three months provided the breakthrough we needed to identify the initial victim from Candiru’s infrastructure

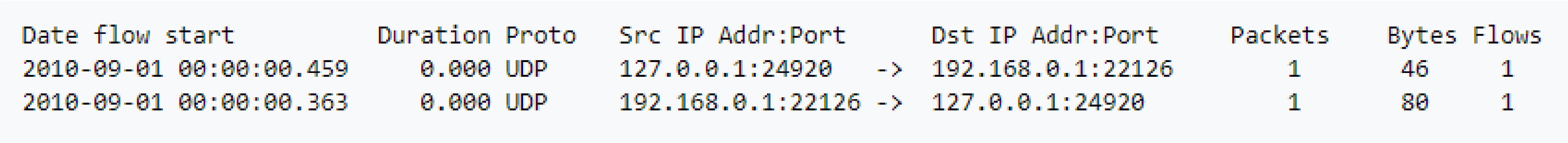


2. Finding Candiru’s Malware In The Wild

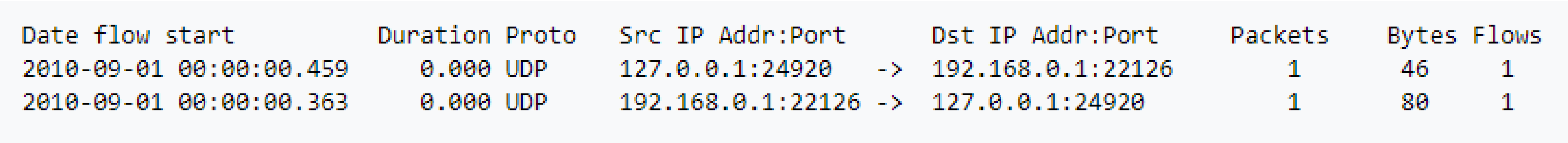
Using telemetry data from Team Cymru, along with assistance from civil society partners, the Citizen Lab was able to identify a computer that we suspected contained a persistent Candiru infection. We contacted the owner of the computer, a politically active individual in Western Europe, and arranged for the computer’s hard drive to be imaged. We ultimately extracted a copy of Candiru’s spyware from the disk image.



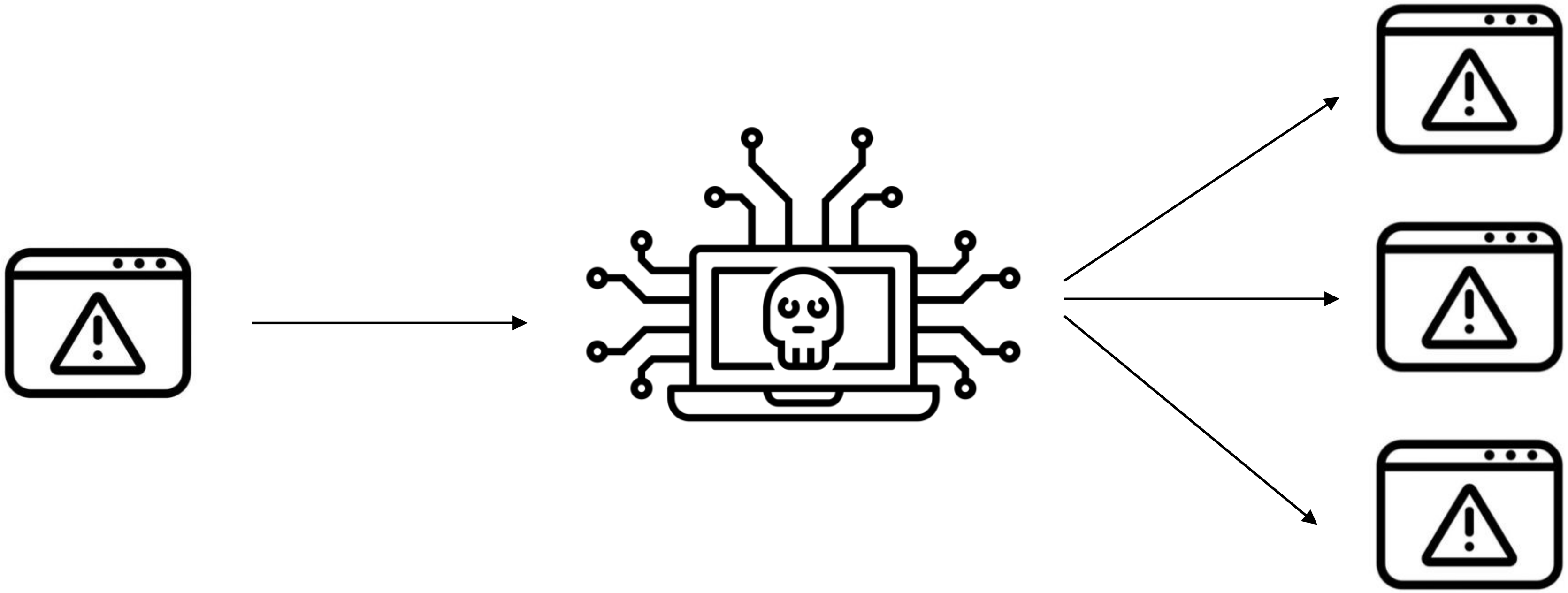
Thanks to Team Cymru for providing access to their Pure Signal Recon product. Their tool’s ability to show Internet traffic telemetry from the past three months provided the breakthrough we needed to identify the initial victim from Candiru’s infrastructure

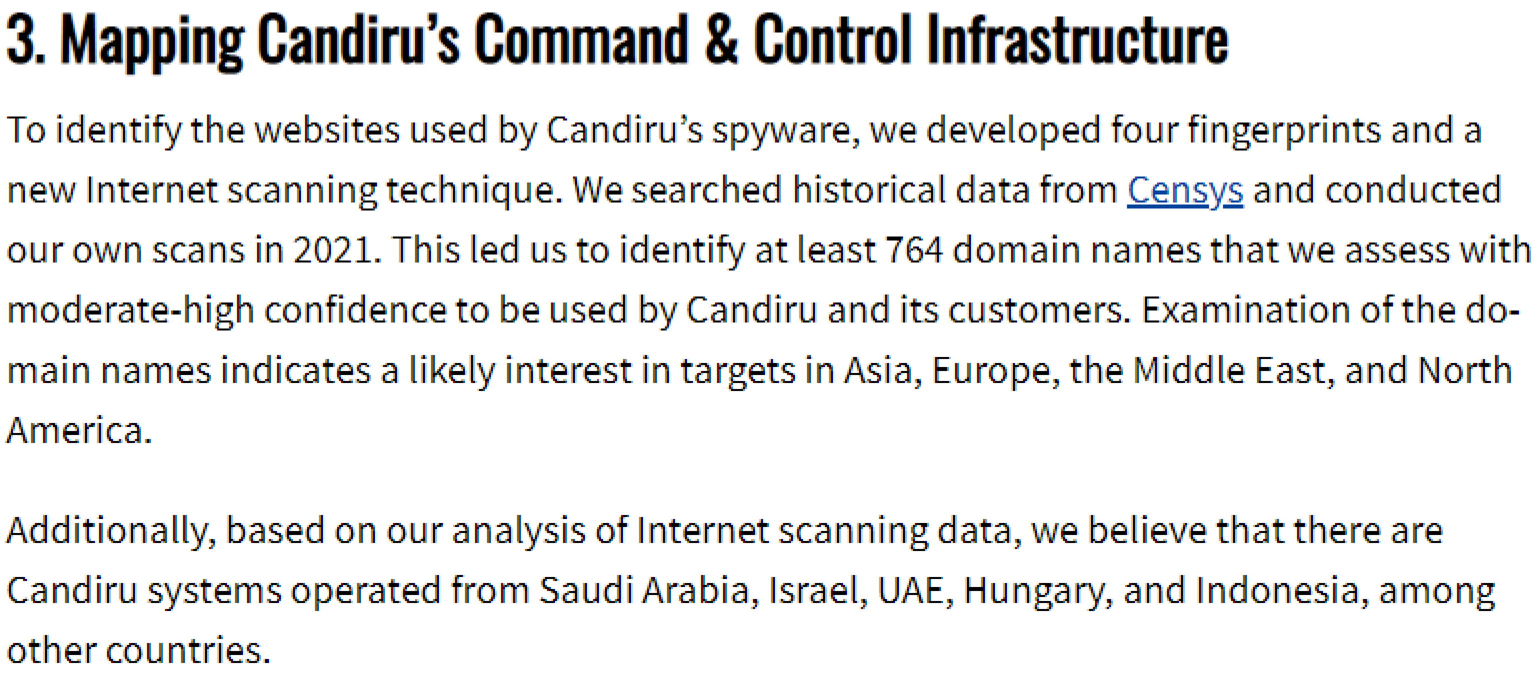


```
Date flow start          Duration Proto   Src IP Addr:Port      Dst IP Addr:Port     Packets    Bytes Flows
2010-09-01 00:00:00.459     0.000 UDP     127.0.0.1:24920   ->  192.168.0.1:22126        1       46     1
2010-09-01 00:00:00.363     0.000 UDP     192.168.0.1:22126 ->  127.0.0.1:24920          1       80     1
```



```
Date flow start          Duration Proto      Src IP Addr:Port       Dst IP Addr:Port      Packets     Bytes Flows
2010-09-01 00:00:00.459     0.000 UDP        127.0.0.1:24920    -> 192.168.0.1:22126          1        46     1
2010-09-01 00:00:00.363     0.000 UDP        192.168.0.1:22126 -> 127.0.0.1:24920             1        80     1
```

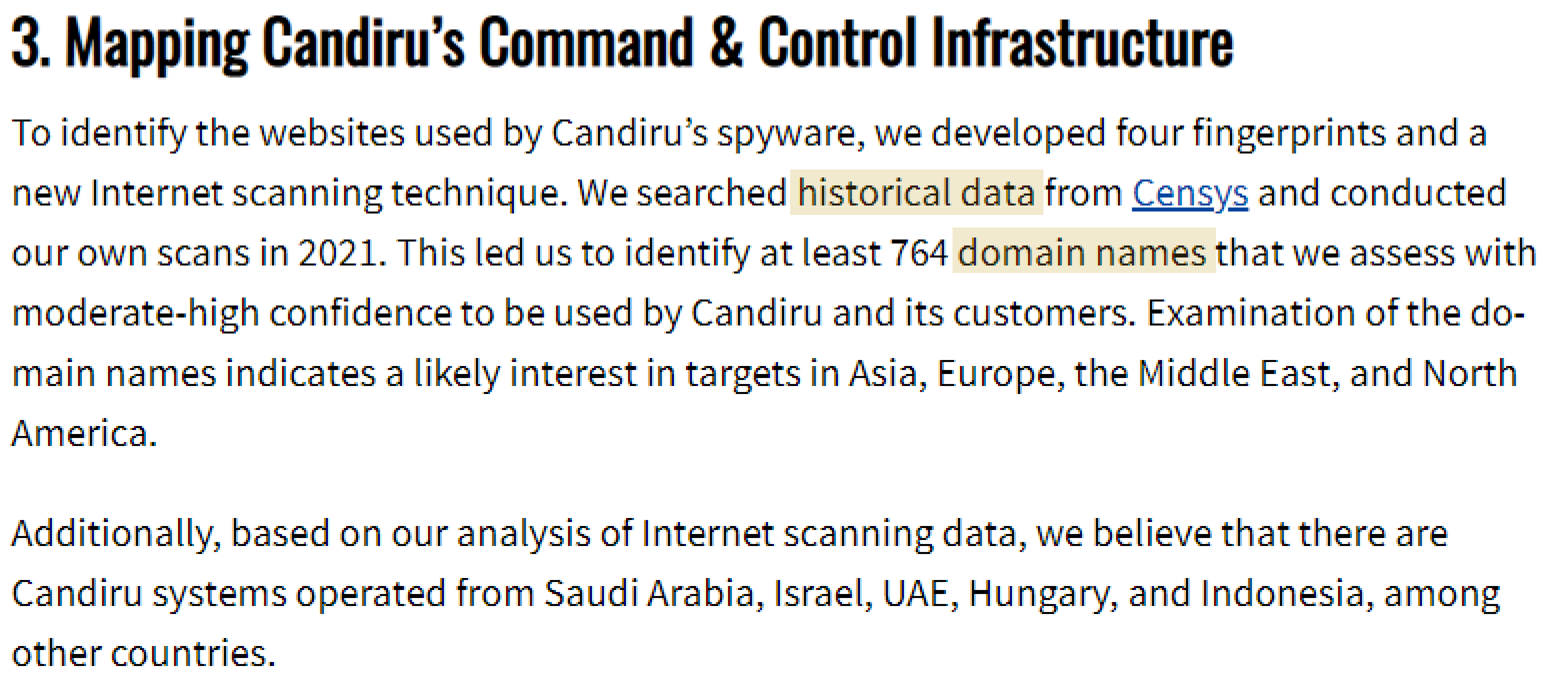




3. Mapping Candiru’s Command & Control Infrastructure

To identify the websites used by Candiru’s spyware, we developed four fingerprints and a new Internet scanning technique. We searched historical data from Censys and conducted our own scans in 2021. This led us to identify at least 764 domain names that we assess with moderate-high confidence to be used by Candiru and its customers. Examination of the domain names indicates a likely interest in targets in Asia, Europe, the Middle East, and North America.

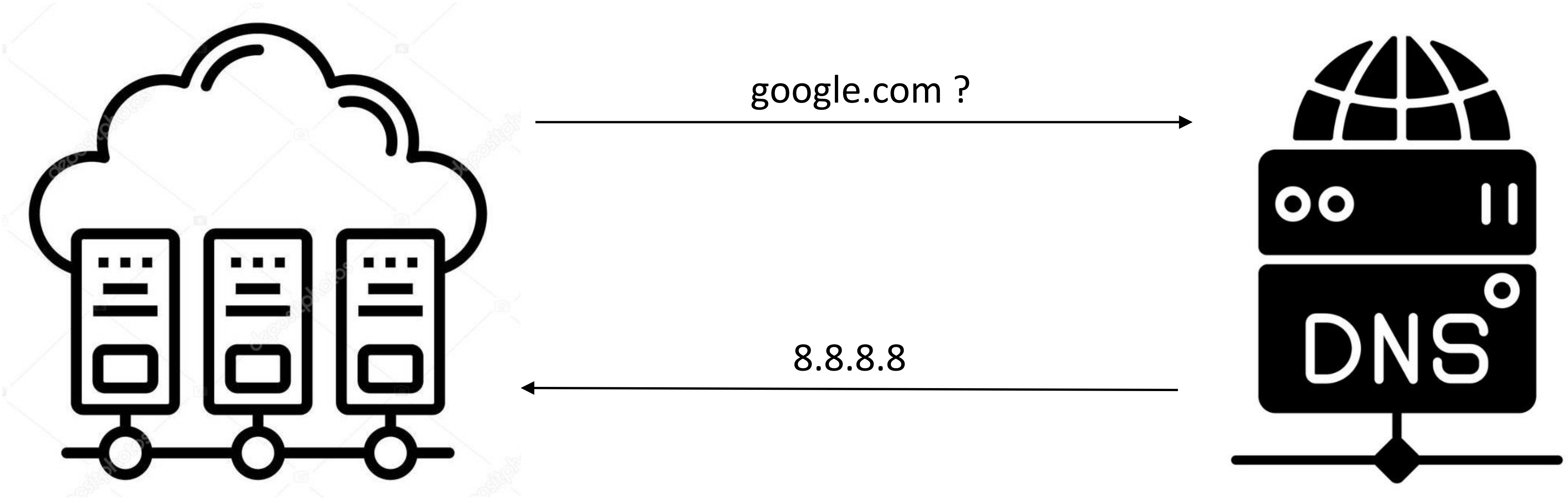
Additionally, based on our analysis of Internet scanning data, we believe that there are Candiru systems operated from Saudi Arabia, Israel, UAE, Hungary, and Indonesia, among other countries.



3. Mapping Candiru’s Command & Control Infrastructure

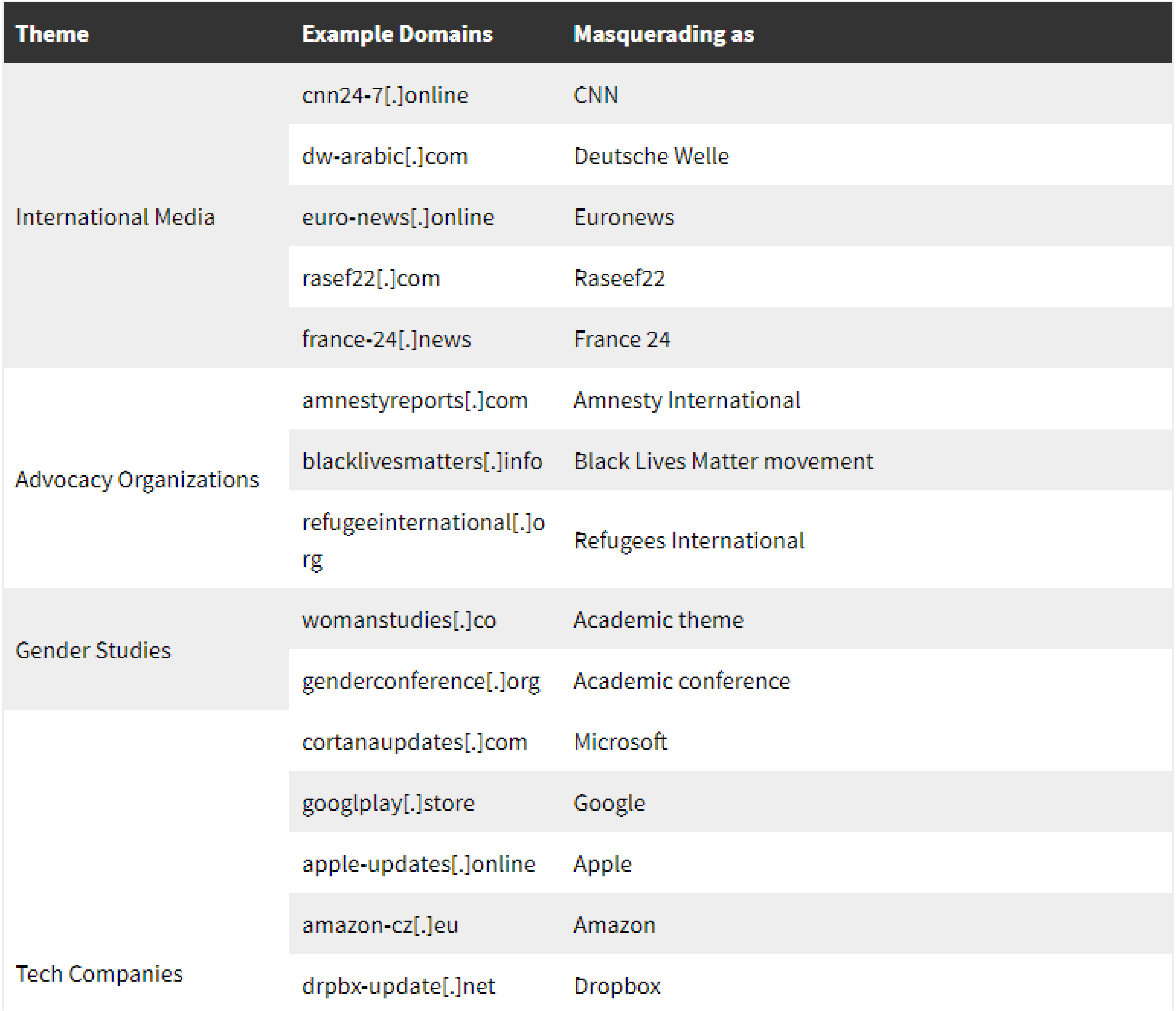
To identify the websites used by Candiru’s spyware, we developed four fingerprints and a new Internet scanning technique. We searched historical data from Censys and conducted our own scans in 2021. This led us to identify at least 764 domain names that we assess with moderate-high confidence to be used by Candiru and its customers. Examination of the domain names indicates a likely interest in targets in Asia, Europe, the Middle East, and North America.

Additionally, based on our analysis of Internet scanning data, we believe that there are Candiru systems operated from Saudi Arabia, Israel, UAE, Hungary, and Indonesia, among other countries.



google.com ?

8.8.8.8



Theme	Example Domains	Masquerading as
International Media	cnn24-7[.]online	CNN
	dw-arabic[.]com	Deutsche Welle
	euro-news[.]online	Euronews
	rasef22[.]com	Raseef22
	france-24[.]news	France 24
Advocacy Organizations	amnestyreports[.]com	Amnesty International
	blacklivesmatters[.]info	Black Lives Matter movement
	refugeeinternational[.]org	Refugees International
Gender Studies	womanstudies[.]co	Academic theme
	genderconference[.]org	Academic conference
Tech Companies	cortanaupdates[.]com	Microsoft
	googlplay[.]store	Google
	apple-updates[.]online	Apple
	amazon-cz[.]eu	Amazon
	drpbx-update[.]net	Dropbox

Respeito à Privacidade e aos Direitos Civis

Cooperação

Telemetria de tráfego de rede

Histórico de registros de domínios