CTI/20240627_macOS_PoseidonStealer at main · govcert-ch/CTI

By govcert-ch

Archived: 2026-04-05 15:26:25 UTC

Poseidon Stealer malspam campaign targeting Swiss macOS users

On the evening of the 27th of June 2024, the NCSC has observed a large AGOV themed malspam campaign targeting macOS users in Switzerland with Poseidon Stealer.

AGOV is the public service login for Switzerland. It is not only for use in federal settings, but also when dealing with cantonal and communal authorities, for example when completing your tax return.

The malspam has been sent from Amazon's legitimate outbound email service using the following email subject:

```
AGOV-Zugriff: Ab Juli 2024 für alle öffentlichen Online-Dienste obligatorisch
```

Sending IP addresses (Amazon):

```
 23.251.226.1
23.251.226.2
23.251.226.3
23.251.226.4
23.251.226.5
```

Sender (Email from):

```
AGOV <noreply@ing.automech.com.br>
```

The malspam emails contain a link to `bing.com` from which victim gets redirects to another, mostly likely compromised host, that finally redirects the victim' to a website hosting Poseidon Stealer.

Rogue redirect (probably compromised):

```
https://shop.aishabaker.com/about/
```

Poseidon Stealer payload URLs:

```
 https://register-agov.net /AGOV-Access.dmg
https://register-agov.com/AGOV-Access.dmg
https://agov-ch.com/AGOV-Access.dmg
```

```
https://agov-ch.net/AGOV-Access.dmg
https://agov-access.net/AGOV-Access.dmg
https://agov-access.com/AGOV-Access.dmg
```

Once infected, Poseidon Stealer will steal various information from the victim's machine and exfiltrate it to a botnet C2 located here:

A copy of the Poseidon Stealer malware sample is available for download here:

- https://bazaar.abuse.ch/sample/474ee78c6636ee478ea7f4521559679fbc468bb326357737bfc465e63ed153fa/

MISP event (JSON):

- 20240627_macOS_PoseidonStealer.json
