

INSIGHTS ON CYBERATTACKS

Maik Morgenstern, CTO AV-TEST





- Teil der SWISS IT SECURITY GROUP
- Endpoint/Gateway Tests, APT/Red Team Tests:
- IoT Tests:
- Data Feeds und Statistiken:

[AV-TEST.org](https://www.av-test.org)

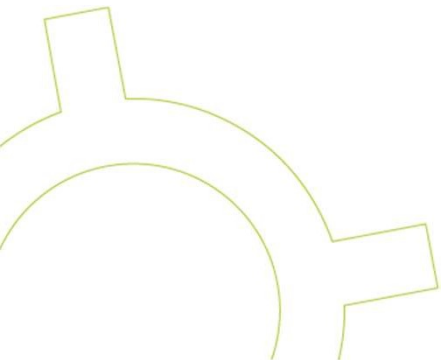
[IoT-TESTS.org](https://www.av-test.org/iot-tests)

[AV-ATLAS.org](https://www.av-test.org/atlas)



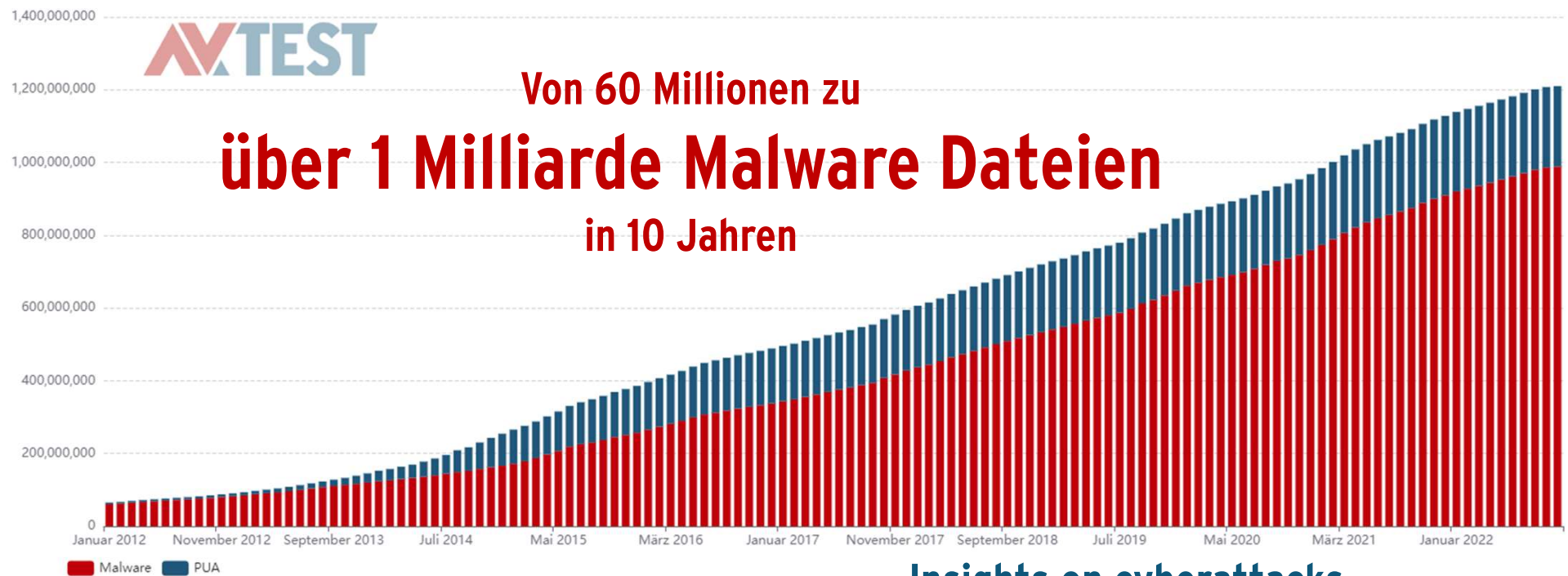
Key Points

- Commodity Malware ist nicht tot
- Foothold und Persistence
 - Alles ist ein Ziel
 - Phishing statt Exploiting
- Ransomware, Ransomware, Ransomware ...
- Ukraine Krieg und Cyberwaffen



Commodity Malware ist nicht tot

GESAMTMENGE VON MALWARE UND PUA



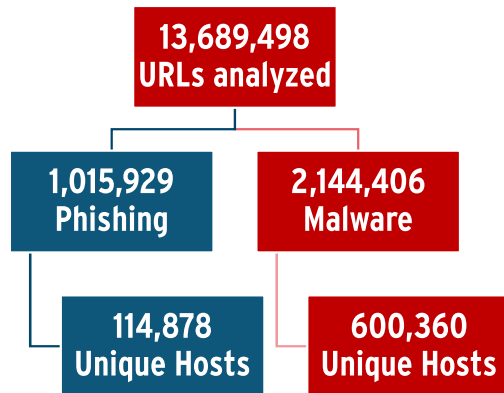
Von 60 Millionen zu
über 1 Milliarde Malware Dateien
in 10 Jahren

Insights on cyberattacks
Atlas by AXTEST

Commodity Malware ist nicht tot

OS	Ende 2018	Ende 2019	Ende 2020	Ende 2021	Okt 2022
 Windows	568.548.134	+18%: 669.508.165	+14%: 765.630.259	+15%: 882.445.394	937.208.812
 Linux	359.867	+108%: 747.535	+45%: 1.082.336	+138%: 2.573.101	4.154.807
 macOS	935.832	+12%: 1.044.704	+67%: 1.745.092	+2%: 1.781.085	1.799.759
 Android	33.565.361	+19%: 39.801.620	+23%: 48.991.197	+11%: 54.557.726	55.787.544

Phishing statt Exploiting

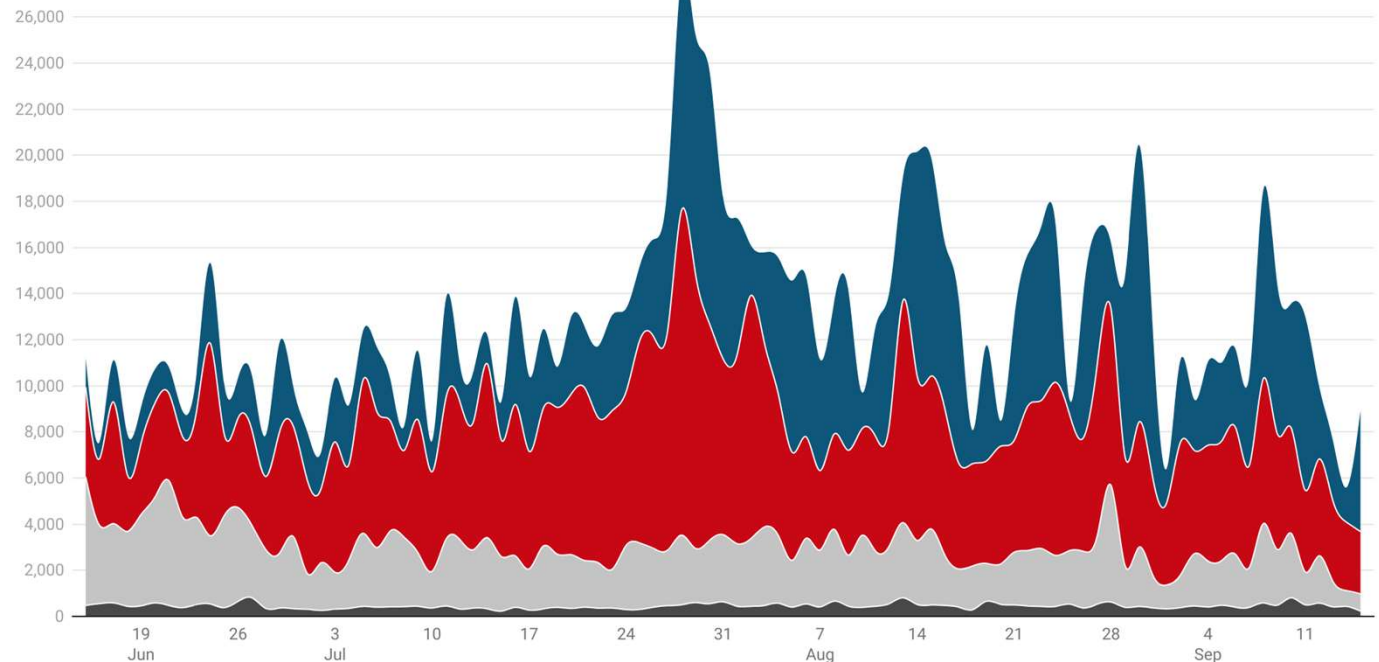


Phishing ist eine wachsende Bedrohung

Über 30% aller verdächtigen Webseiten in AV-ATLAS im Jahr 2022 sind Phishing Webseiten

Malicious and Phishing URLs

■ Malware Payloads ■ Phishing ■ Web Script ■ Other



Ransomware, Ransomware, Ransomware ...

Über 100 öffentlich berichtete Cyberangriffe

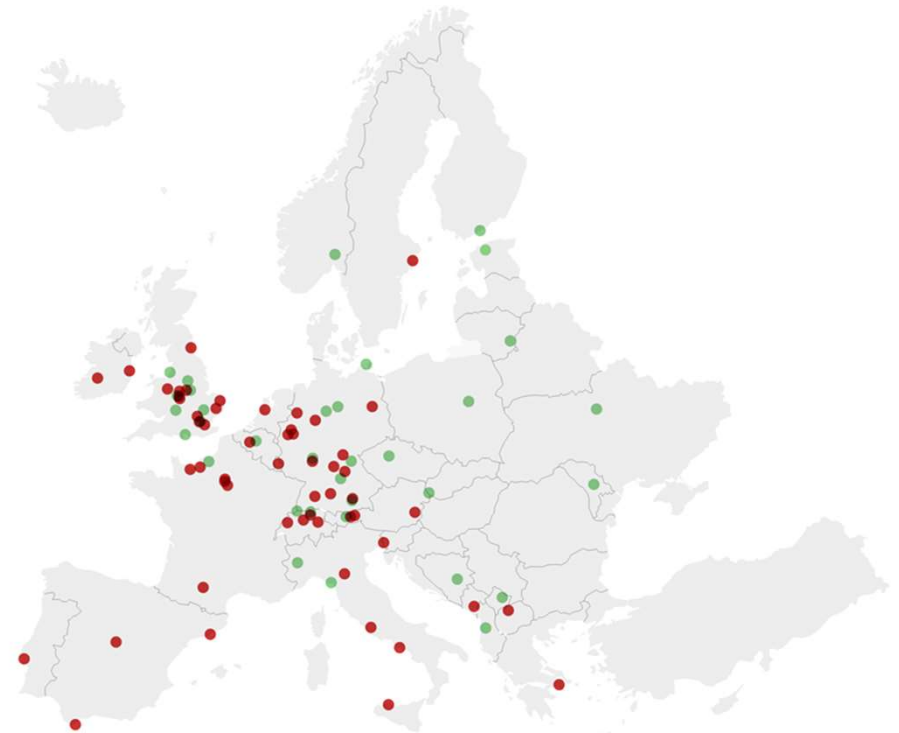
Im Zeitraum Juli 2022 bis Anfang Oktober 2022 in der Presse gemeldet.

**Etwa 60% wurden als
Ransomware identifiziert**

**Westeuropa: Ransomware
Osteuropa: Ukrainekrieg**

Cyberangriffe Juli 2022 - Oktober 2022

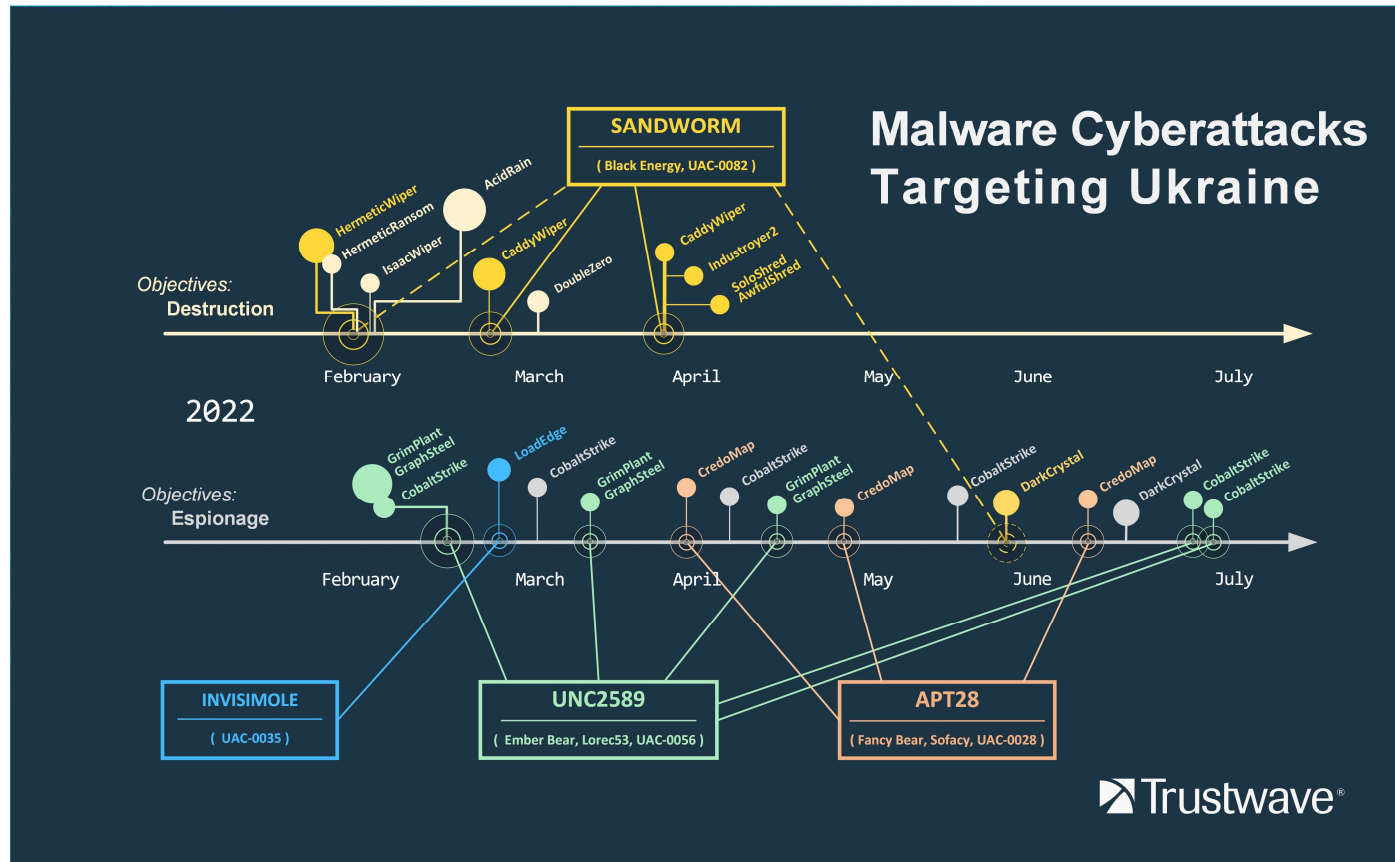
■ Anderes ■ Ransomware



Insights on cyberattacks

atlas by TEST

Ukraine Krieg und Cyberwaffen



Overview of the Cyber Weapons Used in the Ukraine - Russia War:
<https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/overview-of-the-cyber-weapons-used-in-the-ukraine-russia-war/>

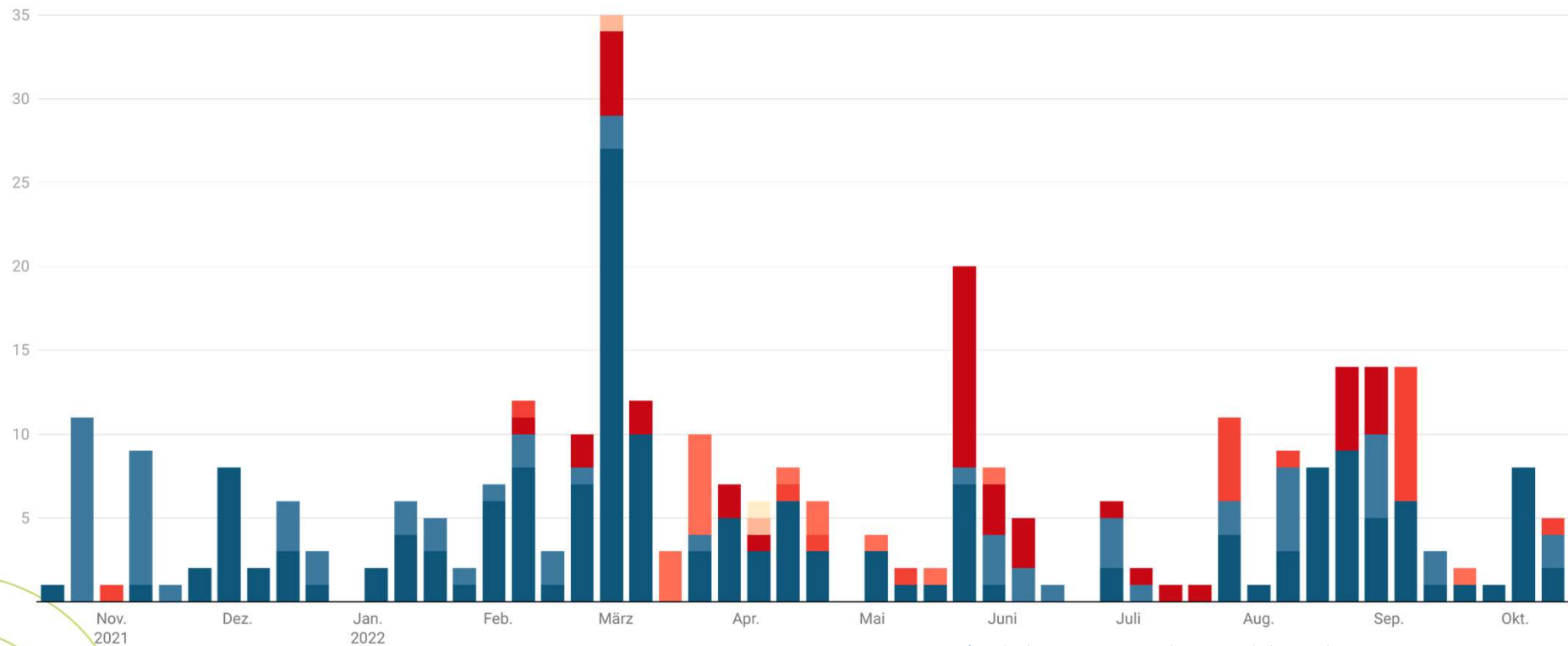
Insights on cyberattacks

atlas by **TEST**

Ukraine Krieg und Cyberwaffen

Wiper Malware

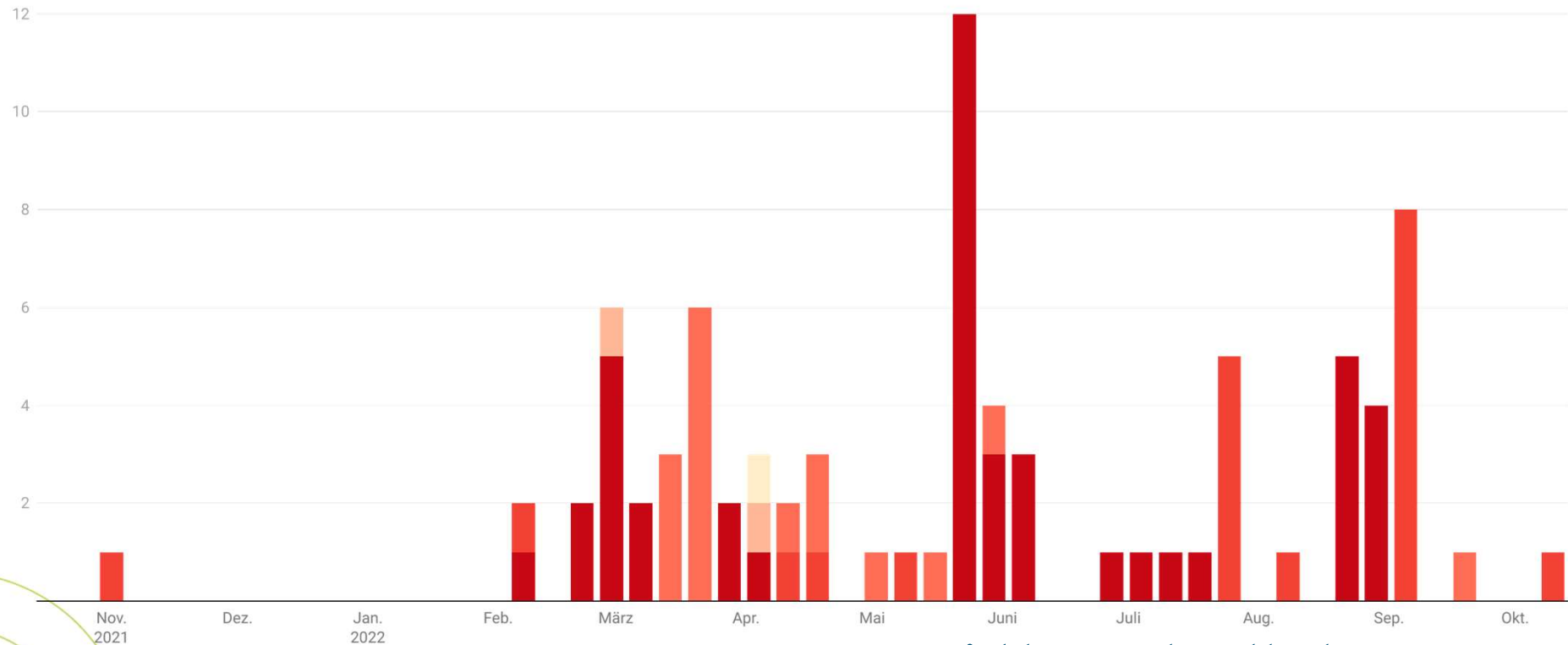
Killdisk Wiperlocker Hermeticwiper Industroyer Caddywiper Isaacwiper Acidrain



Ukraine Krieg und Cyberwaffen

Wiper Malware

Hermeticwiper Industroyer Caddywiper Isaacwiper Acidrain



Vielen Dank für Ihre Aufmerksamkeit!



Insights on cyberattacks

atlas by **AVTEST**