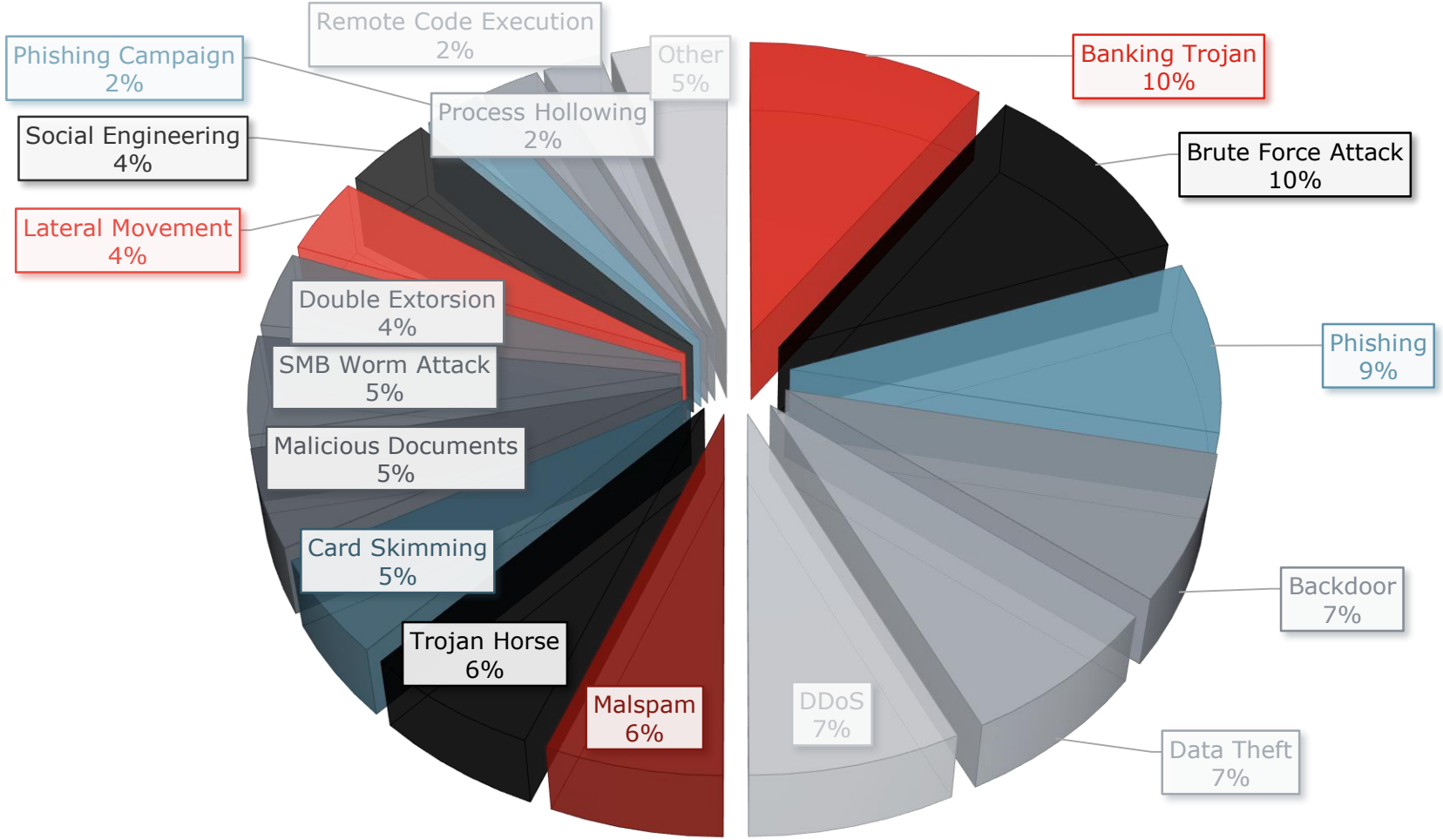
Neues aus dem Bereich der Cyberangriffe

Wolfgang Schwabl, CSO

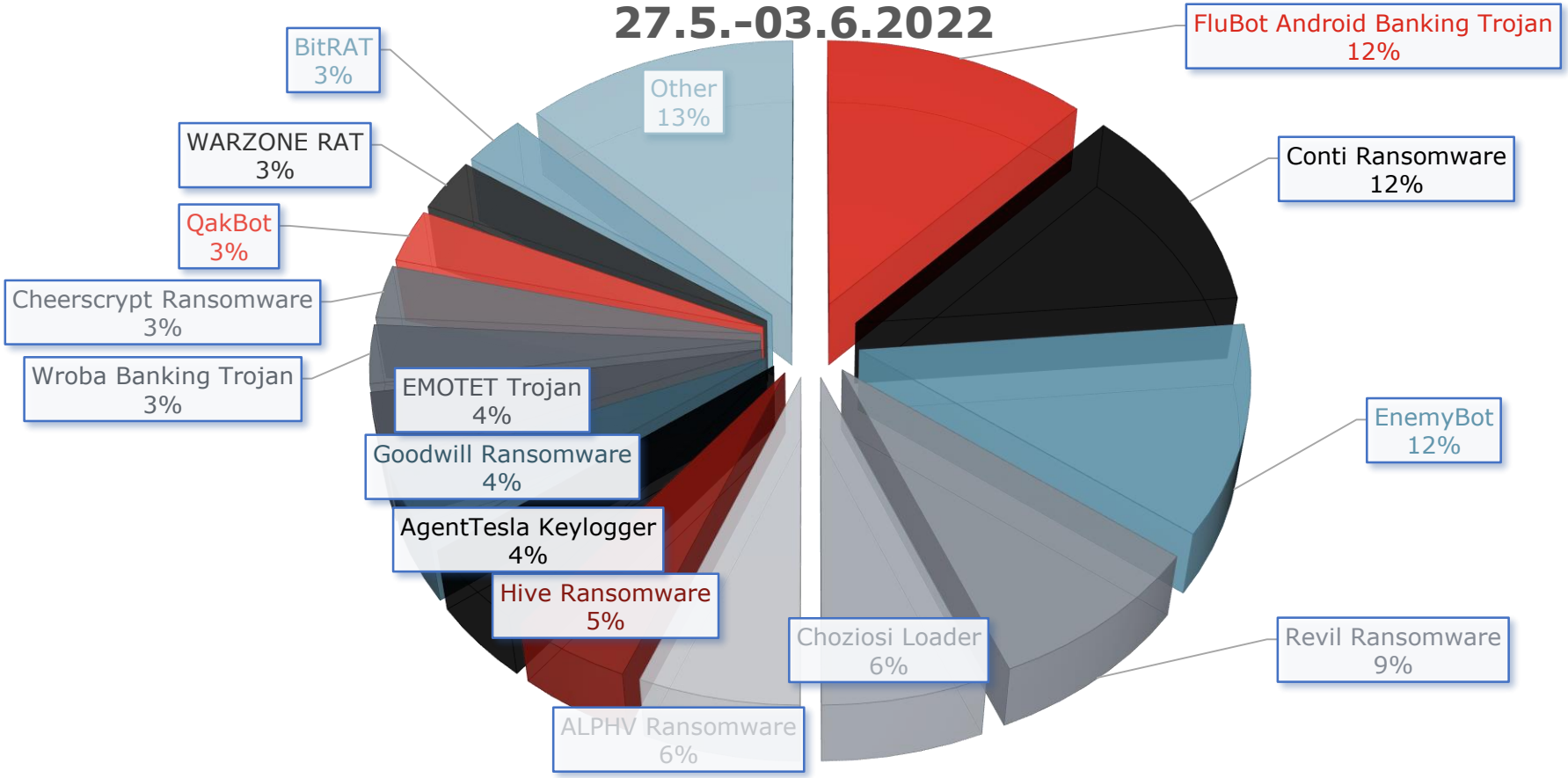
June 9th 2022

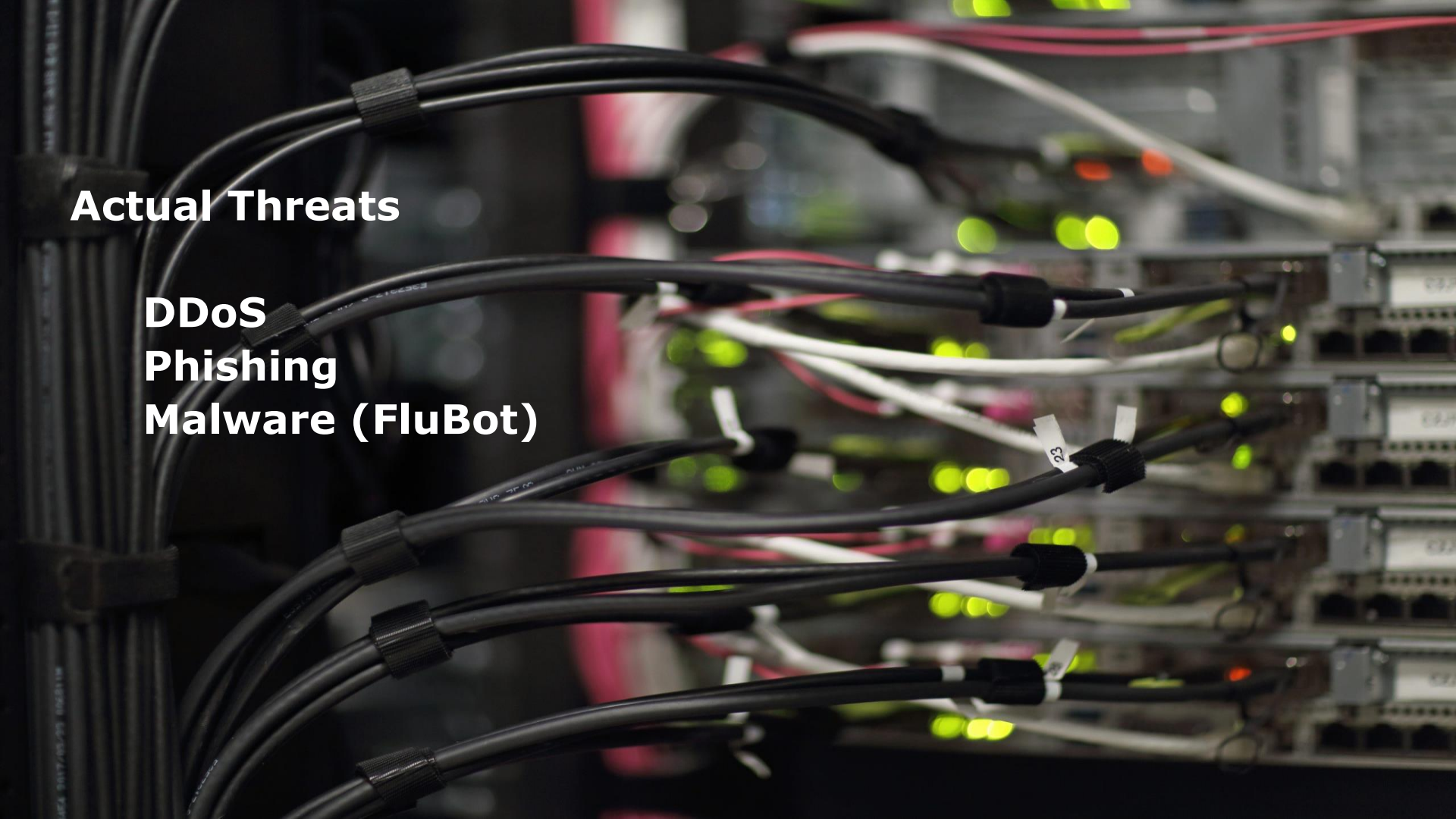
Threats

ATTACK TYPES - EUROPOL 25.6.-2.7.2021



ATTACK STATISTICS - EUROPOL/MENTIONS GRAPH
27.5.-03.6.2022





Actual Threats

DDoS
Phishing
Malware (FluBot)

DDoS - Distributed Denial of Service attacks

Facts (A1 Austria)

~ 100 DDoS attacks / day

Falling trend within last 6 months (comparision 1H21 – 1H22)

500 → 250 DDoS > 10 Gbit/s
100 → 20 DDoS > 50 Gbit/s

Max Impact	Importance	Alert	Start Time
	High Fast Flood 56,464.0% of 50 Mbps 75.3 Gbps, 7.2 Mpps	DoS Host Alert Incoming Host Alert to 91.23[redacted] using PI-Space Misuse Types: ICMP, IP Fragmentation, DNS, UDP, DNS Amplification, Apple Remote Management Service Amplification	Jun 12 05:25 - 13:40 (8:15)
	High Fast Flood 6,641.0% of 400 Kpps 143.5 Gbps, 12.7 Mpps	DoS Host Alert Incoming Host Alert to 185.37.[redacted] using [redacted]Beograd_IPv4_pc Misuse Types: IP Fragmentation, Total Traffic, UDP	Jun 1 17:00 - 17:10 (0:09)
	High Fast Flood 6,641.0% of 400 Kpps 143.5 Gbps, 12.7 Mpps	DoS Host Alert Incoming Host Alert to 185.37[redacted] using [redacted]VIPMOBILE_OpCo_IPv4_pc Misuse Types: IP Fragmentation, Total Traffic, UDP	Jun 1 17:00 - 17:10 (0:09)
	High Fast Flood 8,857.0% of 300 Kpps 143.5 Gbps, 12.7 Mpps	DoS Host Alert Incoming Host Alert to 185.[redacted] using PI-Space Misuse Types: IP Fragmentation, UDP	Jun 1 17:00 - 17:10 (0:09)
	High 3,436.0% of 400 Kpps 333.2 Gbps, 39.6 Mpps	DoS Host Alert Incoming Host Alert to 46.123.[redacted] using A[redacted]A1SI-Mobile-Customers[redacted] Misuse Types: UDP, mDNS Amplification	May 31 00:49 - 01:04 (0:14)
	High Fast Flood 13,197.0% of 300 Kpps 333.2 Gbps, 39.6 Mpps	DoS Host Alert Incoming Host Alert to 46.123.2[redacted] using PI-Space Misuse Types: UDP, mDNS Amplification	May 31 00:48 - 01:03 (0:15)
	High Fast Flood 19,795.0% of 200 Kpps 333.2 Gbps, 39.6 Mpps	DoS Host Alert Incoming Host Alert to 46.123.2[redacted] using [redacted]_A1Slovenijadd_IPv4_sc Misuse Types: UDP	May 31 00:48 - 01:03 (0:15)
	High Fast Flood 19,795.0% of 200 Kpps 333.2 Gbps, 39.6 Mpps	DoS Host Alert Incoming Host Alert to 46.123.[redacted] using [redacted]A1Slovenijadd_OpCo_IPv4_c Misuse Types: UDP	May 31 00:48 - 01:03 (0:15)
	High 11,843.0% of 400 Kpps 566.6 Gbps, 57.8 Mpps	DoS Host Alert Incoming Host Alert to 46.123.2[redacted] using [redacted]A1SI-Mobile-Customers-[redacted] Misuse Types: UDP	May 31 00:30 - 00:38 (0:07)
	High Fast Flood 19,277.0% of 300 Kpps 566.6 Gbps, 57.8 Mpps	DoS Host Alert Incoming Host Alert to 46.123.[redacted] using PI-Space Misuse Types: IP Fragmentation, UDP	May 31 00:28 - 00:37 (0:08)

Cyber Security Incidents

Phishing for Microsoft IDs (Dec. 2018)

IT Help desk: Action Required - Nachricht (Nur-Text)

Datei Nachricht Was möchten Sie tun?

IT Support <it@sprt.co> IT Support 1 04:42

IT Help desk: Action Required

Diese Nachricht hat unnötige Zeilenumbrüche.

Activation Guide.pdf
303 KB

Due to frequent phishing attack, take a minute to activate the upgraded Spam Filter. Set up and guide attached.

Everyone MUST activate the upgraded spam filter service no later than today.

Regards,

IT Department

https://babiesices.info/iolk/frcuzspqbonij29tg4ywdemlvx

Sign In

Microsoft

Sign in

Email, Phone or Skype

No account? Create one!

Next

Terms of use

Pri

E-mail Security

Check “Sender”

A1-Scam-Samples - wolfgang.schwabl@A1.at - Outlook

Datei | Start | Senden/Empfangen | Ordner | Ansicht | ADOBE PDF | Was möchten Sie tun?

Alle | Ungelesen

A1-Scam-Samples durchsuchen (Strg+E) | Aktueller Ordner

VON	SENDER	AN	BETREFF	ERHALTEN	GRÖ...
Schwabl Wolfgang		Thomas C. Stubbings...	Beitrag zum CERT Bericht	Mo. 06.05.2019 11:54	57 KB
Human Resources	kmiedich@napleton.com	employees@hr.com	Employee's Compliance to Reviewed Polic...	Di. 30.04.2019 15:44	11 KB
98039427@student.uts.edu.au	98039427@student.uts.edu.au	India Bennett	€ 2.000.000,00 Euro	Mi. 24.04.2019 13:06	27 KB
iTunes	git@replay.com	schwabl@aon.at	Ihre Apple-ID wurde für den Zugriff auf i...	Di. 16.04.2019 13:00	23 KB
A1telekom	khurshid.tsd@orion-group.net	Schwabl Wolfgang	Rechnung 63250543581 (A1telekom)	Do. 11.04.2019 11:35	16 KB
Anonymer Hacker	anneliese87@c.anonymerhackerz.rocks	Schwabl Wolfgang	Das ist meine letzte Warnung wolfgang.s...	Do. 11.04.2019 11:35	19 KB
Service	478738748378473@p131server.hostpoint.ch	schwabl@aon.at	PayPal: Account verification required	Mo. 08.04.2019 21:08	23 KB
A1 | Support	hr.schlumpf@intergga.ch		Die Schließung Ihres Kontos wird am 04.0...	Mo. 08.04.2019 18:54	14 KB
Raiffeisen	28@586239298046.hostingkunde.de	schwabl	Wichtige Mitteilung	Fr. 05.04.2019 03:55	16 KB
card complete	info@completesecure-services.info	schwabl	Neue Mitteilung	Di. 02.04.2019 04:02	41 KB
IT Support	it@sprt.co	IT Support	IT Help desk: Action Required	Do. 06.12.2018 04:42	314 KB

emente: 11 | Alle Ordner sind auf dem neuesten Stand. | Verbunden mit Microsoft Exchange

FluBot Malware

Facts

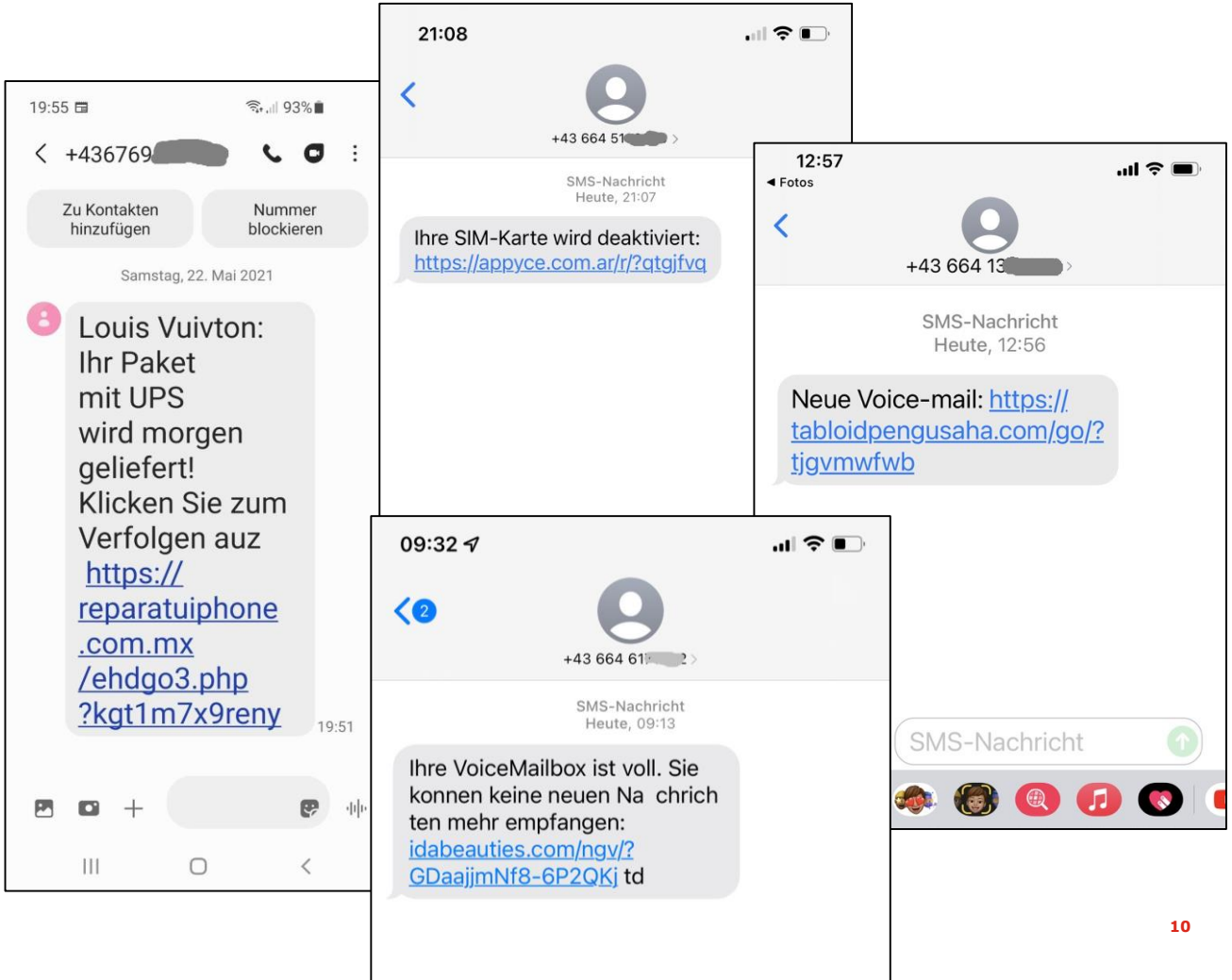
A1 Austria

Started ~ May 21

Millions of SMS

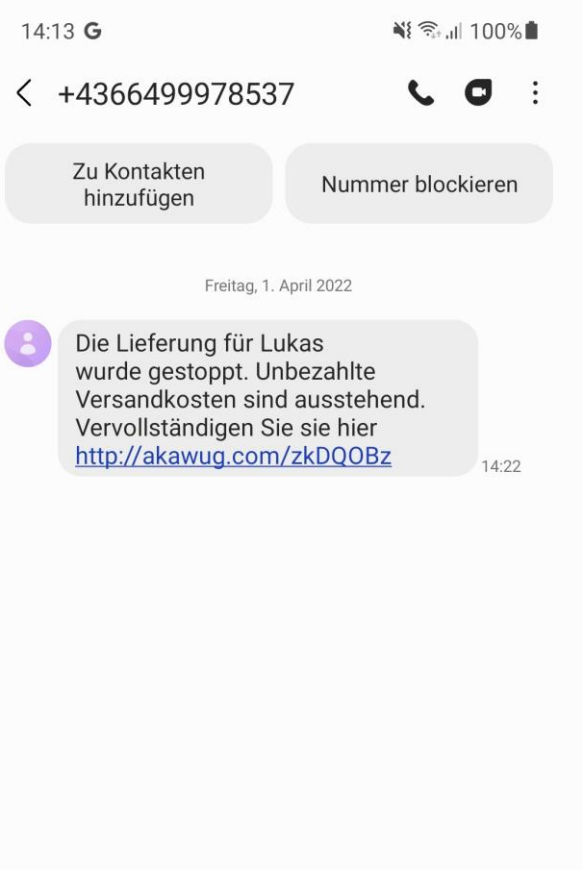
Thousands of infected Android phones

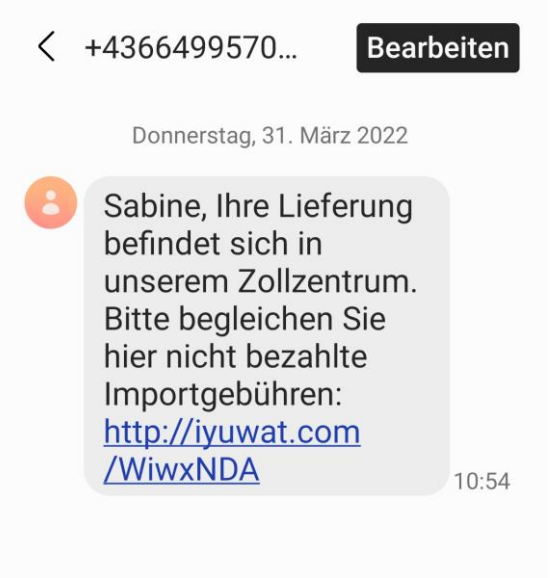
A national botnet



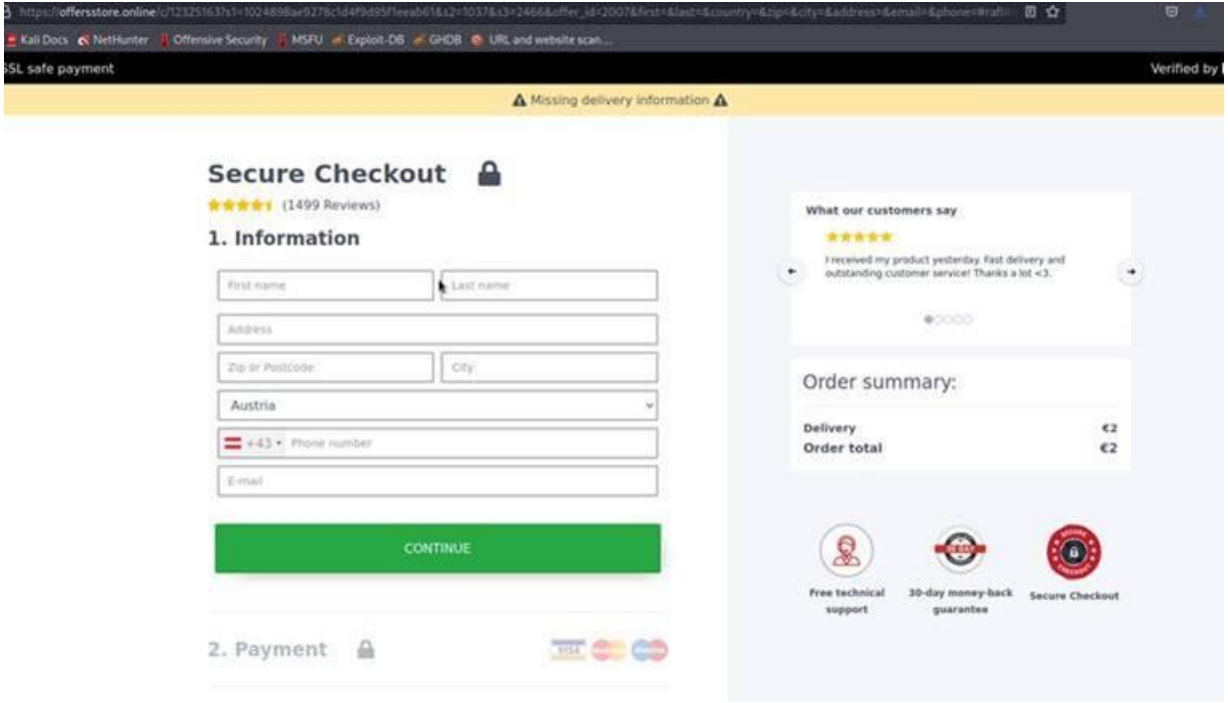
TLP:AMBER

Smishing examples





Website Click 4



Prevention – Mobile Phones

MAM - Mobile Application Management (Microsoft Intune)

Outlook
Teams
SharePoint
OneDrive
Power BI
Edge
Acrobat Reader
…

Only private use

Alexa
Dropbox
LinkedIn
Apple Mail
…

Actual Fraud Cases

A1 Shop Fraud

Procurement Fraud

Anlagentools

Neuanmeldung - Nachricht (HTML)

Datei | Nachricht | Anlagen | Was möchten Sie tun?

Mo 11.04.2022 17:31

mustafa omerovic <office.smakgmbh@gmail.com>

Neuanmeldung

An [redacted] Mario

Aufbewahrungsrichtlinie A1 - E-Mail-Policy: Default - remove after 3 years (3 Jahre) Läuft ab 15.04.2025

SMAK Gewerbeschein 2.pdf
134 KB

Sehr geehrte Damen und Herren,

nach Telefonischen Auskunft habe ich mich entschlossen bei Ihnen A1 Business Kunden zu werden.
Im Anhang finden Sie die Gewerbeschein. Des weiteren wurde mir mitgeteilt, dass minus Prozente(Bonus) gebe ist dies noch Aktuell?

Ich bitte Sie für folgende Geräte in Teilzahlung (24 Monate Laufzeit) mit der Tarif A1 Business Mobil Unlimited 5G zu übermitteln:

Das Angebot für folgende Geräte:

1. Samsung Galaxy S22 Ultra 5G 256GB

2. Iphone 13 Pro Max 256GB in Weiß oder Sierra Blau

3. Iphone 13 Pro Max 256 GB in Graphit (oder in Ausführung in der es lagernd ist)

Bitte übermitteln Sie mir das Angebot.
Vielen Dank im Voraus.

(- Des weiteren wurde mir mitgeteilt am Telefon, dass man für Apple Watch Serie 7 einen Extra Vertrag abschließen muss zu einer der Verträge. Daher bitte einen extra Antrag für Apple Watch 7/ 45mm.)

Mit freundlichen Grüßen
S.M.A.K GmbH

Procurement fraud is not only a technical issue

e.g. request to change a bank account

We do a lot to keep A1 secure