



Cybersecurity gestern, heute, morgen

Wolfgang Schwabl
Chief Security Officer
A1 Telekom Austria AG

September 5th 2023

Programming

Author	Donald Knuth
Country	United States
Language	English
Genre	Non-fiction Monograph
Publisher	Addison-Wesley
Publication date	1968– (the book is still incomplete)
Media type	Print (Hardcover)
ISBN	0-201-03801-3
Dewey Decimal	519
LC Class	QA76.75

THE CLASSIC WORK
NEWLY UPDATED AND REVISED

The Art of Computer Programming

VOLUME 1

Fundamental Algorithms

Third Edition

DONALD E. KNUTH

Von Jitze Couperus - Flickr: Supercomputer - The Beginnings, CC BY 2.0,
<https://commons.wikimedia.org/w/index.php?curid=19382150>



Computers in the beginning
of the 80ies

By Jason Sp... - Flickr: IMG_9976, CC BY 2.0,
<https://commons.wikimedia.org/w/index.php?curid=29457452>



Von Stefan_Kögl - Eigenes Werk, CC BY-SA 3.0,
<https://commons.wikimedia.org/w/index.php?curid=466937>

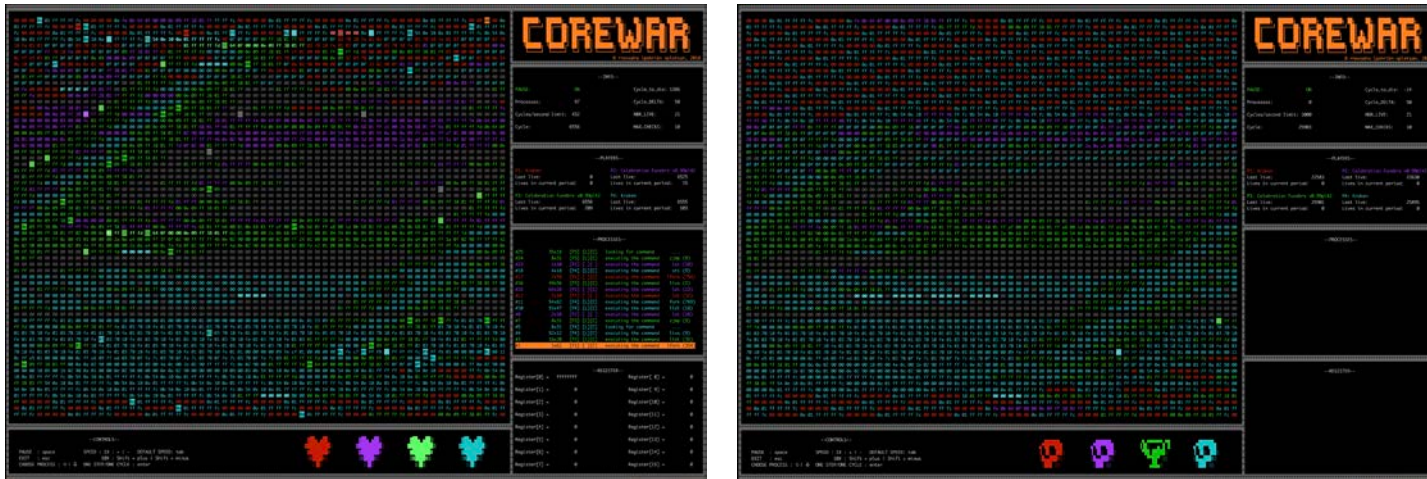
Cybersecurity gestern (Jahre um 1980)

Datensicherung war oberstes Gebot

- Backup der Multiuser-Systeme:
 - tägliches System-Backup im single-user mode durch Operatoren
 - mind. 3 Zyklen Festplatten mit 2 örtlich getrennten, feuerfesten Schränken.
 - Archiv von Software und Daten auf Magnetbändern
- Backup von PCs:
 - Anwendungen
 - Archiv von Software und Daten auf Disketten

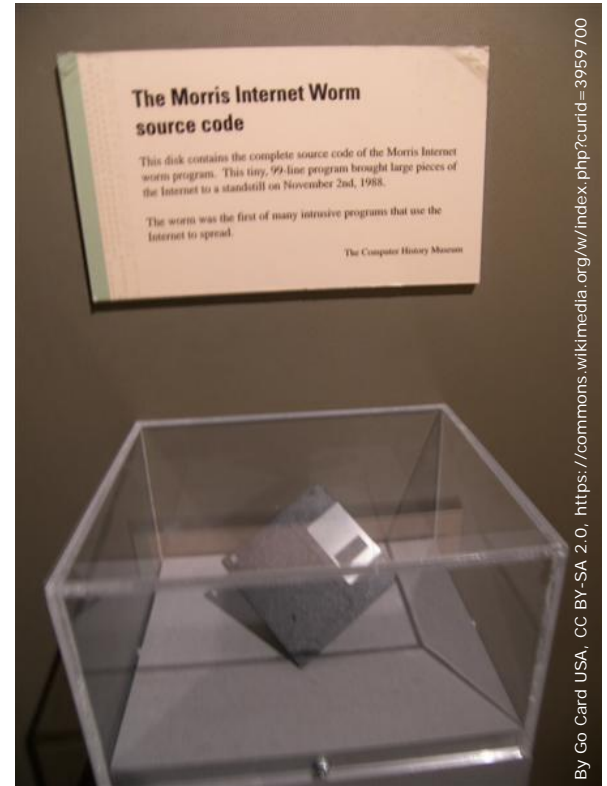
Core War*

- Core War is a 1984 programming game created by D. G. Jones and A. K. Dewdney in which two or more battle programs (called "warriors") compete for control of a virtual computer. These battle programs are written in an abstract assembly language called Redcode.



Morris Worm*

- The Morris worm or Internet worm of November 2, 1988, is one of the oldest computer worms distributed via the Internet, and the first to gain significant mainstream media attention.
- It resulted in the first felony conviction in the US under the 1986 Computer Fraud and Abuse Act.
- It was written by a graduate student at Cornell University, Robert Tappan Morris, and launched on 8:30 pm November 2, 1988, from the Massachusetts Institute of Technology network.



ILOVEYOU*

- ILOVEYOU, sometimes referred to as Love Bug or Love Letter for you, was a computer worm that infected over ten million Windows personal computers on and after 5 May 2000. It started spreading as an email message with the subject line "ILOVEYOU" and the attachment "LOVE-LETTER-FOR-YOU.TXT.vbs".
- Onel de Guzman, a then-24-year-old resident of Manila, Philippines, created the malware. Because there were no laws in the Philippines against making malware at the time of its creation, de Guzman could not be prosecuted.

kindly check the attached LOVELETTER



LOVE-LETTER-FOR-Y
OU.TXT.vbs




coming from me.

A photograph of a server room. The room is filled with rows of server racks. The racks are illuminated with blue and green lights, creating a futuristic atmosphere. In the background, a person is standing in a brightly lit area, possibly a doorway or a window, looking at a device. The overall scene is a mix of dark, industrial-looking server racks and bright, clean light from the background.

Today

**Be prepared
against Cyber Threats**

3 Pillars against Cybercrime

1 People	2 Processes	3 Systems
		
<ul style="list-style-type: none">▪ Proof of good conduct. Security clearances of employees with special duties▪ Data Protection, Compliance, and Security Awareness Trainings▪ Professional Partners Ikarus, Mandiant, KPMG, ...▪ Community of Trust (ATC, CSP, KSÖ, ...)	<ul style="list-style-type: none">▪ InfoSec Policy & Standards, ISMS (Information Security Management System) use it! (→ ISO 27001)▪ Configuration Management▪ A1 CERT▪ SOC (as a service)▪ Sharing Threats & Incidents	<ul style="list-style-type: none">▪ SPAM Defence, Firewalls, Filters, Data Leakage Prevention▪ Vulnerability Scans & Penetration Tests▪ Regular Patching▪ Anti-DDoS Systems▪ Redundant data centers, cables and backups▪ SIEM System▪ Check & Test Effectiveness



Threat Intelligence

Threats

DDoS

Malicious Websites

Phishing

Ransomware

SMS Fraud Scenarios

Threat Intel

Europol EC3

world wide overview
 weekly
 free of charge

Professional Information

CERT.AT
 GSMA
 Scitum
 Microsoft
 ...

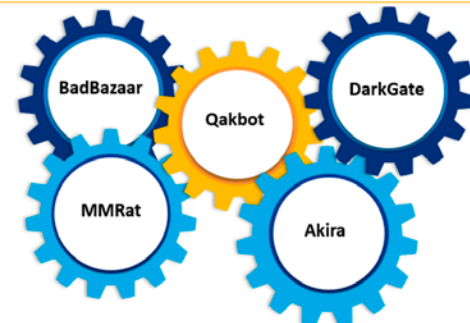
EU Cyber News

- Qakbot botnet infrastructure shattered after international operation.** The malware victimised more than 700 000 computers, with at least EUR 54 million paid in ransoms since 2007. Europol has supported the coordination of a large-scale international operation that has taken down the infrastructure of the Qakbot malware and led to the seizure of nearly EUR 8 million in cryptocurrencies. **Source:** [Europol](#).
- Digital Services Act takes effect for large online platforms.** From now on, 19 platforms and search engines with at least 45 million users will have to comply with the DSA rules concerning data collection, privacy, disinformation, online hate speech and more. The law aims to give users of those platforms, including minors, more rights and influence over their accounts and ensure a high level of privacy and security. **Source:** [EuropeanUnion](#).

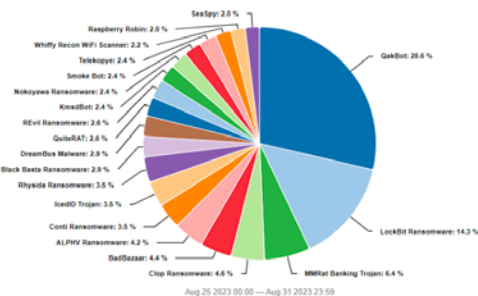
Malware

- Stealthy Android malware MMRat carries out bank fraud via fake app stores.** The Trend Micro Mobile Application Reputation Service (MARS) team discovered a new, fully undetected Android banking trojan, dubbed MMRat, that has been targeting mobile users in Southeast Asia since late June 2023. **Source:** [TrendMicro](#).
- Shining some light on the DarkGate loader.** Recently, Telekom Security CTI was made aware about a new malware campaign that is distributed via phishing emails. The malspam campaign used stolen email threads to lure victim users into clicking the contained hyperlink, which downloaded the malware. **Source:** [Telekom](#).
- BadBazaar espionage tool targets Android users via trojanized Signal and Telegram apps.** ESET researchers have discovered active campaigns linked to the China-aligned APT group known as GREY, distributing espionage code that has previously targeted Uyghurs. Most likely active since July 2020 and since July 2022, respectively, the campaigns have distributed the Android BadBazaar espionage code through the Google Play store, Samsung Galaxy Store, and dedicated websites representing the malicious apps Signal Plus Messenger and FlyGram. **Source:** [WeLiveSecurity](#).
- Akira ransomware targeting VPNs without Multi-Factor authentication.** Cisco is aware of reports that Akira ransomware threat actors have been targeting Cisco VPNs that are not configured for multi-factor authentication to infiltrate organizations, and we have observed instances where threat actors appear to be targeting organizations that do not configure multi-factor authentication for their VPN users. **Source:** [Cisco](#).
- 3 malware loaders you can't (shouldn't) ignore.** Malware loaders are tricky business for SOC teams. Mitigation for one loader may not work for another, even if it loads the same malware. And they're one of the most common tools for a cyber-threat actor to secure initial access to a network, then help drop payloads (remote-access software and post-exploitation tools are popular choices). **Source:** [Reliaquest](#).

Top 5 News Topics of the Week



Trending Malware Families Chart

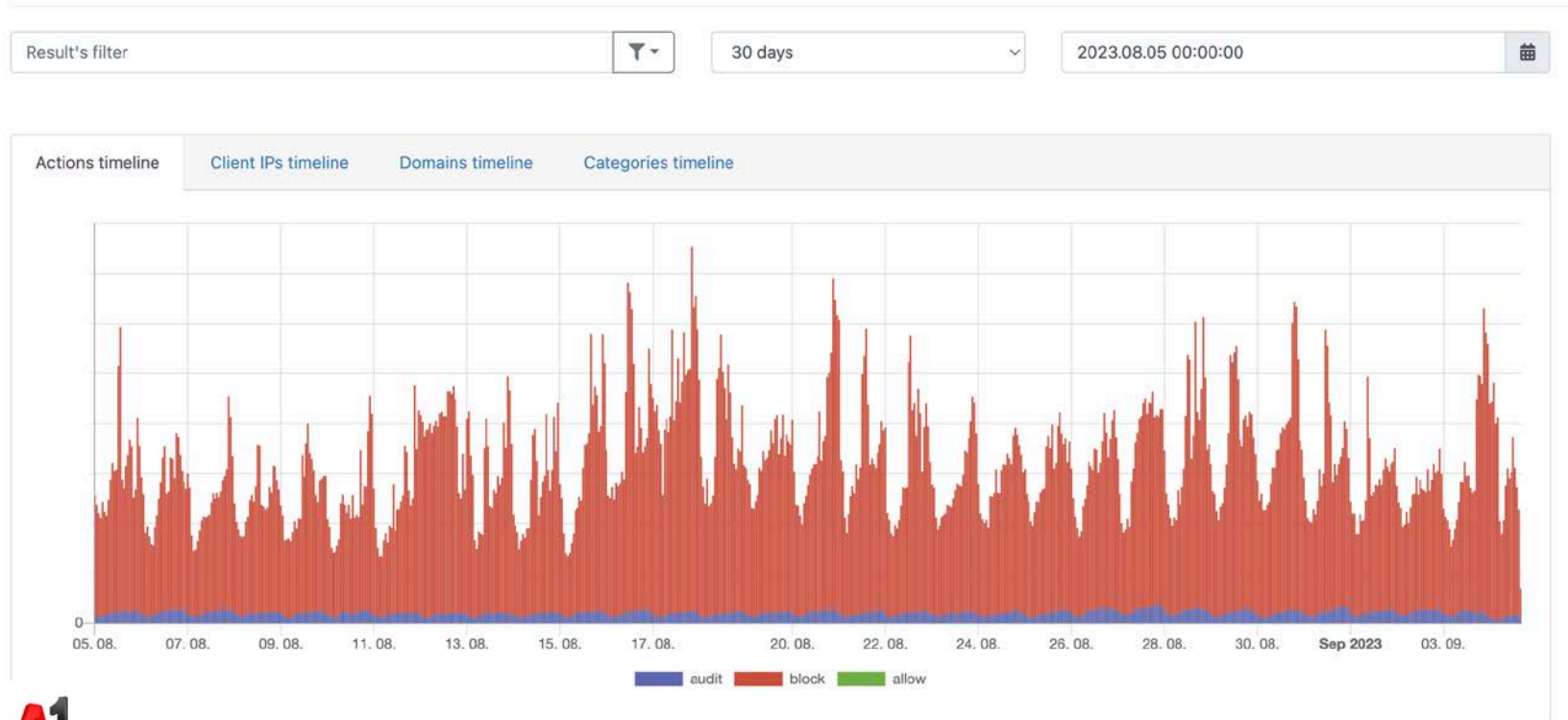


distributed through the Google Play store, Samsung Galaxy Store, and dedicated websites representing the malicious apps Signal Plus Messenger and FlyGram. **Source:** [WeLiveSecurity](#).

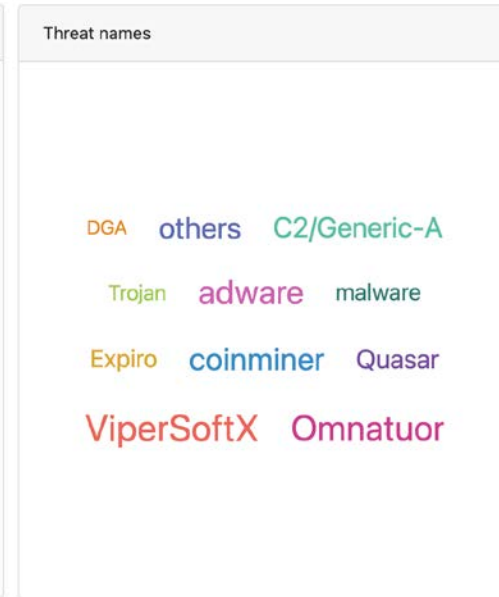
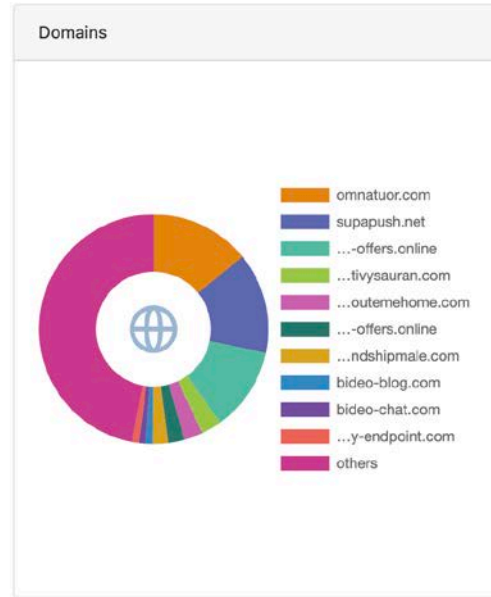
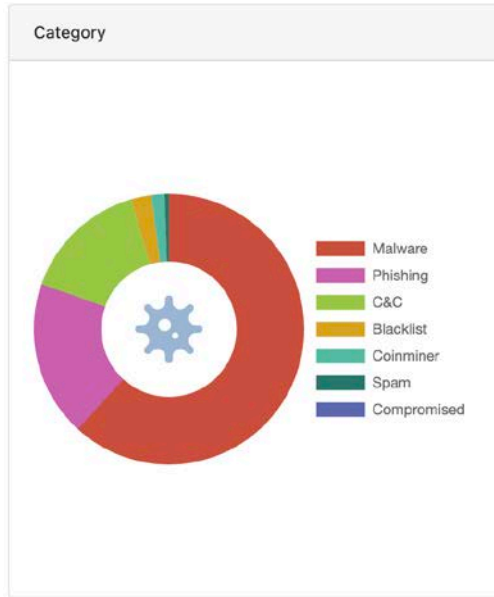
DNS Protection



Overview of threats detected in your DNS traffic



DNS Protection A1 Onlineschutz



DDoS - Distributed Denial of Service attacks (increasing)

Facts (A1 Austria)

within April-Aug 2023:

170+ DDoS attacks / day

192 DDoS > 10 Gbit/s

12 DDoS > 50 Gbit/s



ID ↓	Max Impact	Importance	Alert	Start Time	Classification & Annotations
1967605		High Fast Flood 46,847.0% of 50 Mpps 61.8 Gbps, 5.9 Mpps	DoS Host Alert Incoming Host Alert to 188.1... using Pi-Space Misuse Types: ICMP, IP Fragmentation, UDP, NTP Amplification, DNS Amplification, chargen Amplification	Aug 19 18:52 - 19:00 (0:08)	Possible Attack The "chargen Amplification" host alert signature has been triggered at router "W-PWS-I...". (expected rate: 25.00 Mpps/25.00 Kpps, observed rate: 41.89 Mpps/3.94 Kpps) (by auto-annotation)
1967604		High Fast Flood 43,975.0% of 50 Mpps 58.5 Gbps, 5.6 Mpps	DoS Host Alert Incoming Host Alert to 188.1... using 915231755_A1SrbiJadooBeograd_IPv4_pc Misuse Types: ICMP, IP Fragmentation, Total Traffic, UDP, NTP Amplification, DNS Amplification, chargen Amplification	Aug 19 18:52 - 19:00 (0:08)	Possible Attack TMS mitigation 'Alert 1967604 IPv4 Auto-Mitigation' stopped (by auto-annotation)
1966117		High Fast Flood 186,232.0% of 50 Mpps 249.2 Gbps, 24.1 Mpps	DoS Host Alert Incoming Host Alert to 178.1... using Pi-Space Misuse Types: ICMP, IP Fragmentation, UDP, NTP Amplification, DNS Amplification, chargen Amplification	Aug 16 12:47 - 13:18 (0:31)	Possible Attack The "chargen Amplification" host alert signature has been triggered at router "W-A-IX9071". (expected rate: 25.00 Mpps/25.00 Kpps, observed rate: 29.39 Mpps/2.64 Kpps) (by auto-annotation)
1952029		High Fast Flood 31,840.0% of 50 Mpps 69.7 Gbps, 6.7 Mpps	DoS Host Alert Incoming Host Alert to 77.2... using Pi-Space Misuse Types: ICMP, IP Fragmentation, UDP, DNS Amplification, chargen Amplification	Jul 15 22:10 - 22:18 (0:08)	Possible Attack The "chargen Amplification" host alert signature has been triggered at router "W-PWS-I...". (expected rate: 25.00 Mpps/25.00 Kpps, observed rate: 161.67 Mpps/15.03 Kpps) (by auto-annotation)
1952028		High Fast Flood 26,014.0% of 50 Mpps 55.9 Gbps, 5.3 Mpps	DoS Host Alert Incoming Host Alert to 77.2... using m915231755_VIPMOBILE_OpCo_IPv4_pc Misuse Types: ICMP, IP Fragmentation, Total Traffic, UDP, DNS Amplification, chargen Amplification	Jul 15 22:10 - 22:18 (0:08)	Possible Attack Flowspec mitigation 'Host Alert 1952028 77.2...' 'chargen Amplification' stopped (by auto-annotation)
1952027		High Fast Flood 26,014.0% of 50 Mpps 55.9 Gbps, 5.3 Mpps	DoS Host Alert Incoming Host Alert to 77.2... using 915231755_A1SrbiJadooBeograd_IPv4_pc Misuse Types: ICMP, IP Fragmentation, Total Traffic, UDP, DNS Amplification, chargen Amplification	Jul 15 22:10 - 22:18 (0:08)	Possible Attack TMS mitigation 'Alert 1952027 IPv4 Auto-Mitigation' stopped (by auto-annotation)
1951978		High Fast Flood 20,015.0% of 300 Kpps 684.2 Gbps, 60.0 Mpps	DoS Host Alert Incoming Host Alert to 91.14... using Pi-Space Misuse Types: IP Fragmentation, UDP, DNS Amplification, NetBIOS Amplification, RIPv1 Amplification	Jul 15 18:33 - 18:41 (0:08)	Possible Attack The "NetBIOS Amplification" host alert signature has been triggered at router "W-A-BC...". (expected rate: 25.00 Mpps/25.00 Kpps, observed rate: 59.98 Mpps/5.25 Kpps) (by auto-annotation)
1950883		High Fast Flood 19,805.0% of 30 Kpps 59.6 Gbps, 5.9 Mpps	DoS Host Alert Incoming Host Alert to 85.9... using AS8447_Residential_Prefix Misuse Types: ICMP, IP Fragmentation, IP Private, NTP Amplification, DNS Amplification	Jul 13 04:29 - 04:35 (0:05)	Possible Attack TMS mitigation 'Alert 1950883 IPv4 Auto-Mitigation' stopped (by auto-annotation)
1927393		High Fast Flood 32,868.0% of 10 Kpps 51.5 Gbps, 5.1 Mpps	DoS Host Alert Incoming Host Alert to 91.1... using Pi-Space Misuse Types: ICMP, IP Fragmentation, UDP, NTP Amplification, DNS Amplification, chargen Amplification, CLDAP Amplification	May 27 19:06 - 19:14 (0:08)	Possible Attack The "chargen Amplification" host alert signature has been triggered at router "W-PWS-I...". (expected rate: 25.00 Mpps/25.00 Kpps, observed rate: 58.99 Mpps/5.37 Kpps) (by auto-annotation)
1923697		High Fast Flood 74,409.0% of 10 Kpps 119.4 Gbps, 11.5 Mpps	DoS Host Alert Incoming Host Alert to 89.14... using AS65043_cgNAPT_Mobile Misuse Types: ICMP, IP Fragmentation, IP Private, TCP SYN, TCP RST, UDP, NTP Amplification, DNS Amplification, TCP SYN/ACK Amplification, CLDAP Amplification, Apple Remote Management Service Amplification	May 19 23:26 - May 20 00:28 (1:02)	Possible Attack TMS mitigation 'Alert 1923697 IPv4 Auto-Mitigation' stopped (by auto-annotation)

A1-CERT Playbooks

SPACE SHORTCUTS

Besprechungsnotizen

PAGE TREE

• A1-SecOps Service Catalogue

▼ Core Incident Services

▶ Templates

▼ Incident Detection

▼ Alert Handling & Triage

• Triage Procedure

▼ Playbooks

• **Phishing (Mail/SMS/---)**

▶ Office 365 Alerts

▶ MDE Alerts - (Microsoft Defender for EndPoint)

▶ MDI Alerts (Microsoft Defender for Identity)

▶ MDCA Alerts (Microsoft Defender for Cloud Apps)

▶ MS Azure Alerts

▶ Splunk A1 QV63SR Alerts

• Threat Intelligence based Alerts

• Business ADSL which poses a threat

• Malware and Intrusion related Alerts (e.g. Windows Defender for Endpoint)

• Account Lockouts

• Other Version of PsExec

• Suspicious E-Mail (Phishing/Spam/Malware) was reported via "Send Messa

Pages / ... / Playbooks 128 views

☆ Save for later

👁 Watch

🔗 Share

...

Phishing (Mail/SMS/---)

Created by [redacted] last modified on Aug 31, 2022

1. Analyze Phishing E-Mail

in Explorer (Microsoft 365 Defender Dashboard) malicious E-Mails can be analyzed in depth. Do the following in order to gain attack insights and derive IOCs:

- Analyze the metadata (from, recipient, sender ip, subject, names of attachments,...)
- Download the malicious e-mail
- Extract and analyze malicious attachments (virtual environment)
- Analyse malicious URLs (virtual environment)
- Create, save and analyze the campaign report (best practice: open it directly in Word and then print to PDF, otherwise Statistics are missing in the report; probably a bug)
- Make screenshots (e.g. from phishing sites, or e-mail previews)
- Check the latest delivery location: Is everything quarantined (mitigated successfully) or is something delivered to an Inbox?
- Select Result in Microsoft 365 Defender under "Submissions" (**User is automatically notified with the result**)
- Do an impact analysis and initiate mitigation (as needed)
 - how many users got the phishing E-Mail
 - What exactly is it? Phishing or Malware. What Phishing exactly (O365, A1.net, EBanking,...)? What Malware exactly?
 - Check if someone clicked the link or opened attachments

"A1 Phishing" Check (Check if an official A1 Mail is considered as phishing by users. The following portals contain information about A1 communication)

- A1 Workplace, <https://a1team.workplace.com/>
- A1 Facebook, <https://de-de.facebook.com/A1Fanpage/>
- A1 Coach, [http://\[redacted\].austria.local/a1ta/index.\[redacted\]](http://[redacted].austria.local/a1ta/index.[redacted])
- Intranet, A1 Team
- A1 Homepage, <https://www.a1.net/>
- ask Team Communication, [redacted]@a1.at; in urgent cases contact Teamleader [redacted]
- Infos about Domain <https://centralops.net/co/DomainDossier.aspx>

E-mail Security Advice

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

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

FluBot Malware

Facts

A1 Austria

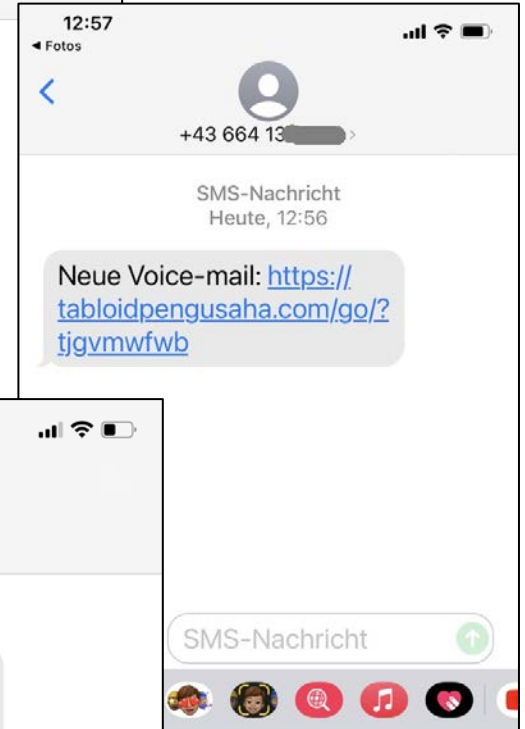
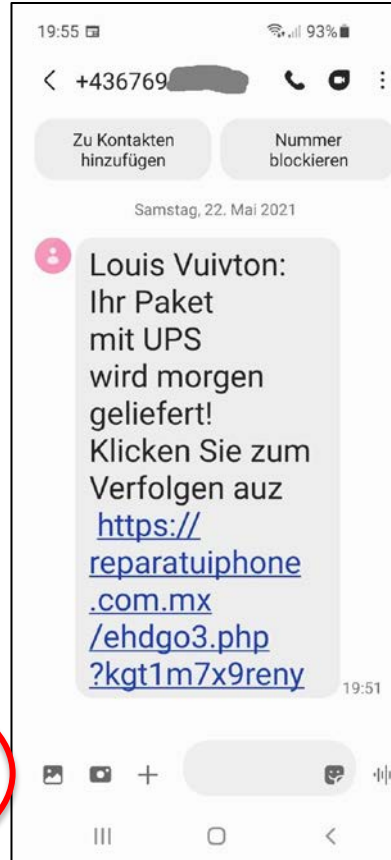
Started ~ May 21

Millions of SMS

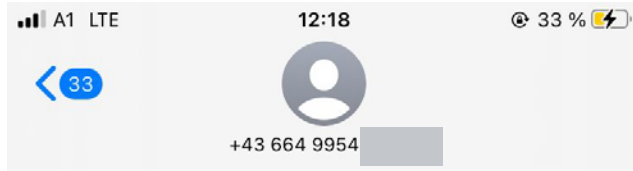
Thousands of
infected
Android
phones

~ May 22:
Botnet shutdown by
Europol cooperation

A1

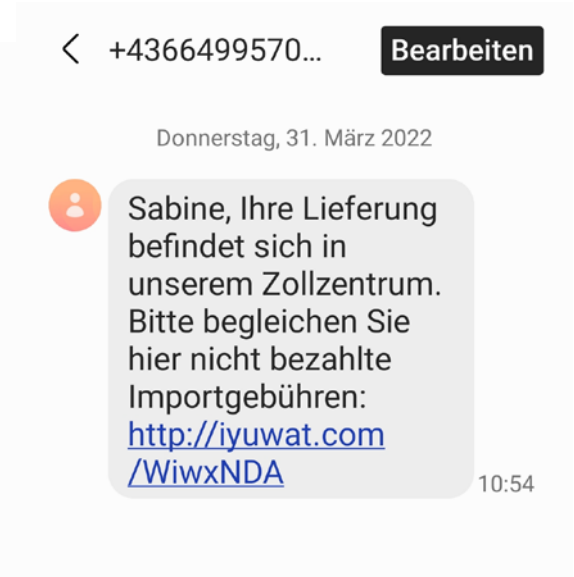


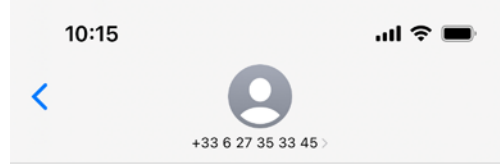
Smishing examples



SMS-Nachricht
Mittwoch, 10:04

Die Lieferung für Melanie wurde gestoppt. Unbezahlte Versandkosten sind ausstehend. Vervollständigen Sie sie hier <http://ifotar.com/rbYjIVl>





SMS-Nachricht
Heute, 09:54

D.H.L - Ihr Paket wartet auf
Lieferung aufgrund zusätzlicher
Zollgebühren.
Die Zusatzkosten sind zu
begleichen bei : [kundenservice-
dhl.de](https://kundenservice-dhl.de)



<https://www.watchlist-internet.at/unserioese-webseiten/phishing-alarm/>

Erstattung durch Ihre Krankenkasse Österreichische Gesundheitskasse 04.09.2023	▼
Geplante Expresszustellung SMS 04.09.2023	▼
Erhöhung der Rente finanzonline.at 01.09.2023	▼
Sozialfonds SMS 01.09.2023	▼
myPayLife Mail: Update erforderlich ! 01.09.2023	▼
BAWAG SMS 28.08.2023	▼
Magenta Wichtig: Unbezahlte Benachrichtigung über Ihren Magenta 28.08.2023	▼
Disney+ Informationen aktualisieren 23.08.2023	▼
Paylife Update erforderlich !! 22.08.2023	▼
A1 Es ist Ihnen nicht mehr möglich, neue E-Mails zu empfangen. #8774960729 21.08.2023	▼
POST EXPRESS (1) Ihre Paketbenachrichtigung 18.08.2023	▼
oesterreich.gv.at Ihre Rückerstattung ist online verfügbar 18.08.2023	▼

Cybersecurity Tomorrow

Cybersecurity Tomorrow

- Know all your IT, systems, devices, network and data
- Manage and monitor all authorizations
- Business-Continuity (e.g. Backup/Restore) is essential
- “Patch me, if you can” -> “Patch me, yes you can”
- Automate maintenance and defense
- Verify continuously
- Have a professional support
- Share and learn

- Crime continues, be aware of “Cyberfraud”



We do a lot to keep
A1 secure



Lessons learned (1 - Passwords)

- Complex passwords are required for all users (A1: 15 chars, UPPER|lower|0-9|+special)
- Don't insist on periodic password changes for all users
- Multifactor Authentication (at least with SMS-TAN) is a strong requirement for all users
- Follow the Microsoft security recommendations, especially for active directory (Tier model)
- Single Sign On – yes, but limited to sets of applications of similar purpose
- Allow long and complex passwords (do not exclude special chars like space or \$/,:;.\$@\()[]{}€)
- Encrypt passwords
- forbid clear text lists of passwords (part of vulnerability check?)
- Password management solutions for corporations are needed

Lessons learned (2)

- “Patch me, if you can”
- DLP is valuable – esp. for the command line logging, distributed searching for files
- SIEM is valuable, sharpen them! (e.g. alarms according to MITRE model)
- SOC and Red/Blue Teams are valuable, Purple Teams are better
- Monitor the traffic, restrict outgoing traffic
- Whitelisting of services is better than blacklisting
- No exceptions!
- Do the security homework always properly! (e.g. see the 18 CIS Controls)
 - Inventory of hardware & software? (Computer Aided Configuration Management)
 - Business Continuity Tests done? (Essential services, Redundancy, Backup/Restore)
 - Time synchronization (< 1s)
- Be prepared for the next attack