AVENIQ

Cyber Threat Landscape

Alice Drifte
Professional Cyber Security Consultant

January 2025

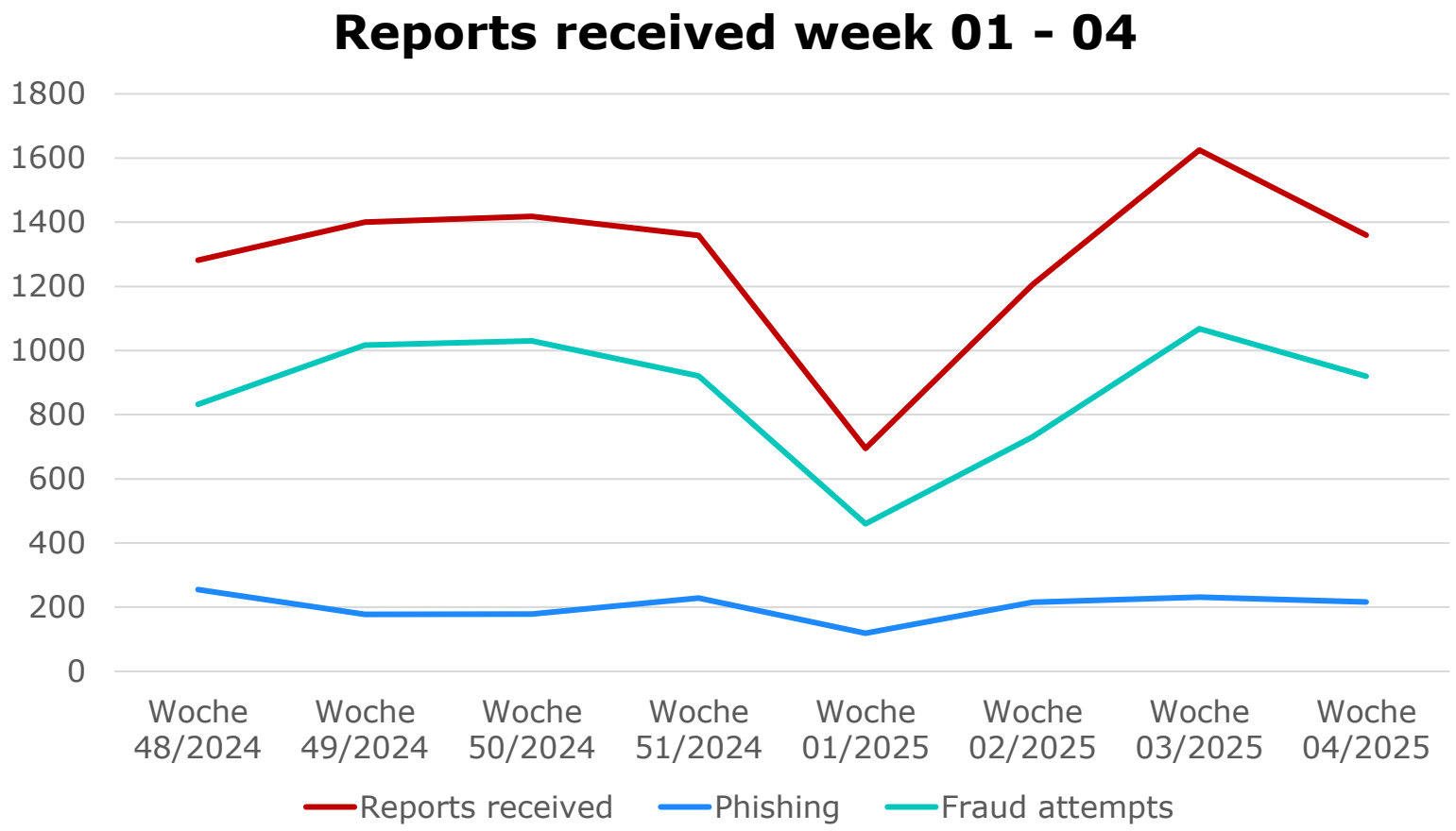
Agenda

1. Reports received January 2025
2. Topic of the month
3. Cyber Attacks of the month
4. Vulnerabilities of the month
5. Insides from the Security Team of Aveniq
6. Tactics, Techniques & Procedures
7. Good to know
8. Appendixes

AVENIQ

Reports received January 2025 in Switzerland

Federal Office of Cybersecurity (BACS)



Trends in January

Compared to December with 5875 reports, 4885 reports occured in January.

The federal government also warns against phishing in the name of the FTA and fraudulent SMS in the name of Binance (Link).

Topic of the month

«It was only a matter of time before the pro-Russian hacker group NoName057(16) also targeted Switzerland. Welcome to the new reality of cyberattacks!»

Summary		Link
21.01.2025	**Hacker attacks Swiss websites** In January 2025, Switzerland was rocked by a major cyberattack that paralyzed several websites. The pro-Russian hacker group NoName057(16) claimed responsibility for the attacks, which were directed against various Swiss institutions. The affected websites included those of the Zürcher and Vaud cantonal banks as well as the websites of the municipalities of Lucerne, Kriens and Adligenswil. The attacks were carried out using so-called distributed denial-of-service (DDoS) attacks, in which the websites were overloaded by mass requests and were therefore no longer accessible to regular users. While this type of attack doesn't result in data leakage, it can cause significant disruption. The hacker group NoName057(16) has been active since 2022 and specializes in politically motivated cyberattacks. Their attacks are often directed against countries that support Ukraine in the war against Russia. The group communicates mainly via Telegram and announces its goals there. This incident highlights the ongoing threat of cybercrime and the need to continuously invest in cybersecurity to defend against such attacks. The Federal Office for Cybersecurity had already warned of possible attacks in the run-up to the World Economic Forum (WEF), as the risk was estimated to be particularly high during this time.	Link

Cyber Attacks of the month

Summary		Link
08.01.2025	**Casio confirms outflow of customer data** The Japanese electronics manufacturer Casio confirmed that personal data of about 8500 people was exposed in a ransomware attack in October 2024. Mainly employees, business partners and some customers are affected. The stolen data includes names, addresses, phone numbers, and other personal information. Casio is working with external specialists to investigate the incident and prevent further damage.	Continue reading
13.01.2025	**Swissmem compensation fund warns its 200,000 policyholders** The compensation fund Swissmem was the victim of a cyber attack in which data was stolen. The exact extent of the data theft is still unclear, but Swissmem warns its 200,000 policyholders of possible fraudulent contacts. The affected data could be used for phishing attacks or other fraudulent activities. Swissmem is working closely with cybersecurity experts to clarify the incident.	Continue reading
21.01.2025	**Russian hackers paralyze websites of banks and municipalities** Several Swiss websites, including those of the Zürcher and Vaud cantonal banks and the municipalities of Lucerne, Adligenswil, Kriens and Ebikon, have been paralyzed by DDoS attacks by the pro-Russian hacker group NoName057(16). These attacks occurred during the World Economic Forum in Davos and caused significant disruption. The hacker group wanted to attract attention and demonstrated its skills on the net. The Federal Office for Cybersecurity had warned in advance of such attacks.	Continue reading
03.02.2025	**Cyber attack on cantonal road condition website in Graubünden** The cantonal road condition website in Graubünden was paralyzed twice by cyberattacks on 2 February 2025. The attacks took place at 10:00 a.m. and 3:30 p.m. and caused significant disruptions to service. Those responsible are working to close the security gaps and make the website fully functional again. This incident demonstrates the ongoing threat of cybercrime and the need to continuously invest in cybersecurity.	Continue reading

Vulnerabilities of the month

Summary				Recommendation	Learn more about
ivanti	**09.01.2025** **Ivanti**	Security Advisory	Public-facing application exploit can be used to execute remote code.	• Updating the software	Link
FORTINET	**14.01.2025** **Fortinet**	News	Public-facing application exploit can be used to execute remote code.	• Updating the software	Link
Adobe	**14.01.2025** **Adobe**	Security Advisory	SExecute arbitrary code. Using the Exploitation for Client Execution method.	• Updating the software	Link
Microsoft	**15.01.2025** **Microsoft**	Security Advisory	Several vulnerabilities in Microsoft products.	• Updating the software	Link
ORACLE	**21.01.2025** **Oracle**	Security Updates	Several vulnerabilities in Oracle products.	• Updating the software	Link
	27.01.2025 **Google Chrome**	Security Updates	The drive-by compromise method exploits several vulnerabilities.	• Updating the software	Link
SONICWALL	**27.01.2025** **SonicWall**	Security Update	Public-facing application exploit can be used to execute remote code.	• Updating the software	Link
	30.01.2025 **Apple Products**	Security Updates	Execute arbitrary code. Using the Exploitation for Client Execution method.	• Updating the software	Link

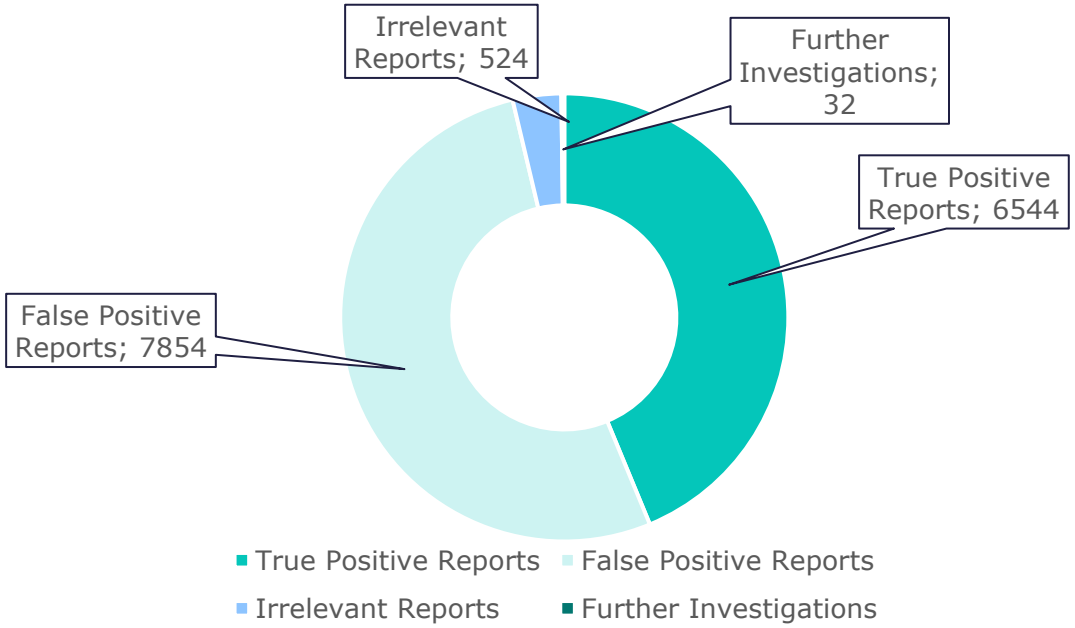
Insides from the Security Team of Aveniq

Interested in our security services?
*More information at **aveniq.ch/cyber-security***

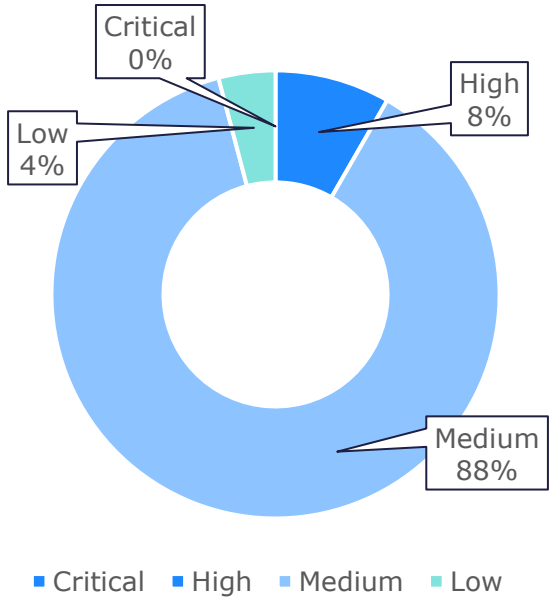
Latest Malware Variants

14.01.2025	WP3.XYZ	Malware	The SS3. XYZ Malware has compromised over 5,000 WordPress websites by creating fake admin accounts, installing malicious plugins, and exfiltrating sensitive data.
15.01.2025	MikroTik	Botnet	A botnet of 13,000 MikroTik devices uses misconfigured SPF DNS records to spread malware via fake DHL invoices.
29.01.2025	Aquabotv3	Botnet	The new Aquabotv3 botnet malware exploits a command injection vulnerability in Mitel SIP phones to integrate them into their botnet.

Reports received in January 2025



Reports processed in January 2025



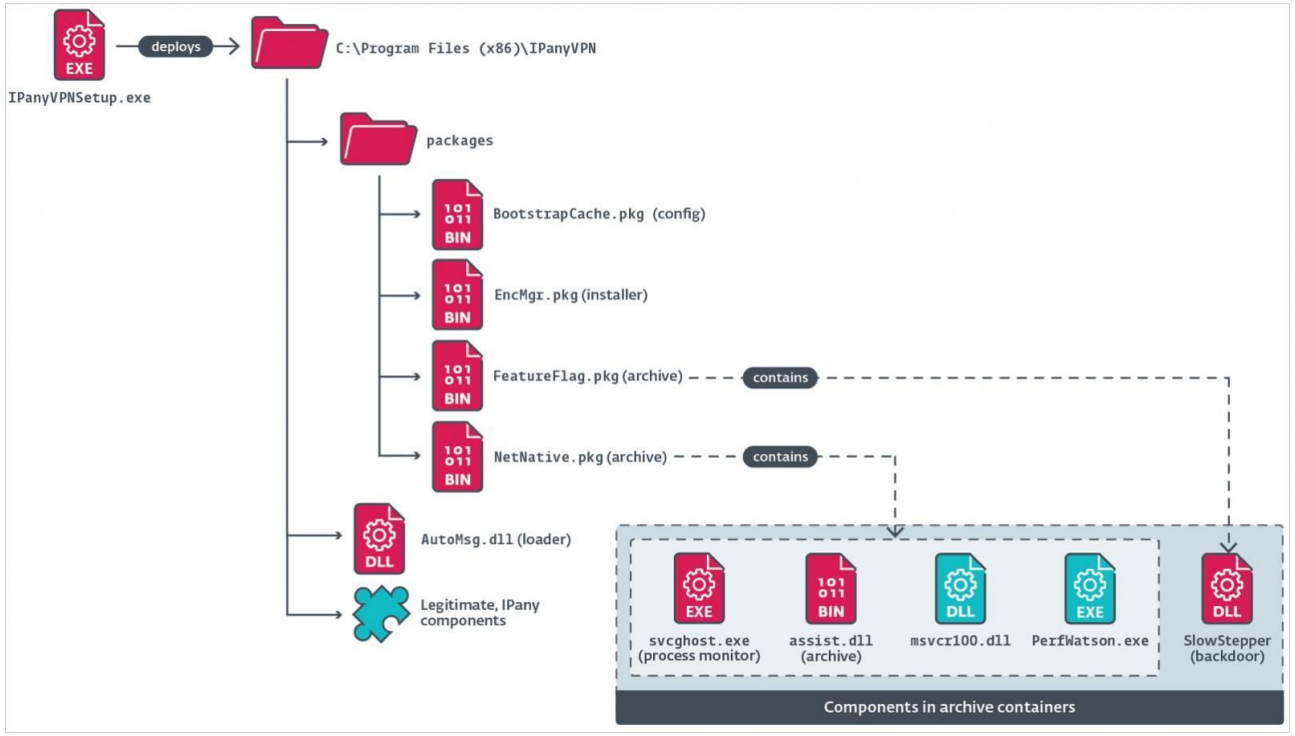
Tactics, Techniques & Procedures 1/2

Summary		Link
22.01.2025	IPany VPN breached in supply chain attack to spread custom malware	Link

In January 2025, South Korean VPN provider IPany fell victim to a supply chain attack carried out by the China-linked hacker group PlushDaemon. This group compromised IPany's VPN installer to distribute the tailor-made 'SlowStepper' malware.

Method

1. **Supply-Chain-Attack**: PlushDaemon exploited a vulnerability in IPany's supply chain by compromising the VPN client's installation process.
2. **Distribution of the malware:** The "SlowStepper" malware has been designed to go unnoticed and burrow deep into the victim's system.
3. **Data Exfiltration:** Once installed, SlowStepper collects sensitive information from the infected system.
4. **Persistence:** To ensure that the malware remains active even after a system reboot, SlowStepper implements persistence mechanisms.
5. **Remote control:** The attackers can control the infected systems remotely by sending commands to the malware.



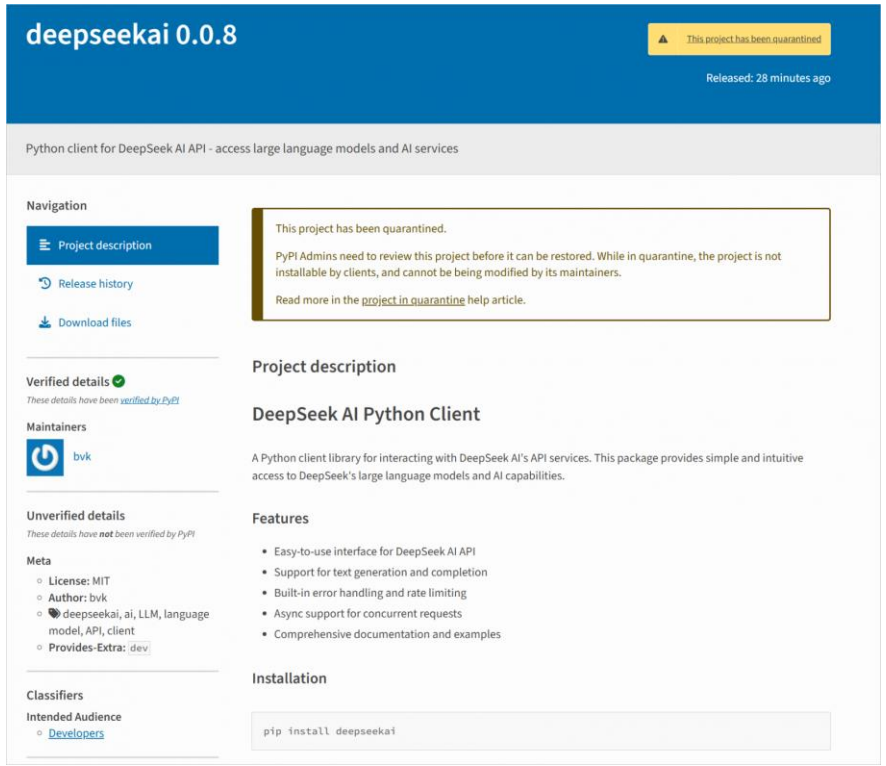
Tactics, Techniques & Procedures 2/2

Summary		Link
03.02.2025	**DeepSeek AI Tools Imitated by Infostealer Malware on PyPI**	Link

In January 2025, threat actors took advantage of DeepSeek's popularity to upload two malicious infostealer packages named 'deepseeek' and 'deepseekai' to the Python Package Index (PyPI). These packages pretended to be developer tools for the AI platform, but stole sensitive information from the developers' machines, including API keys and database credentials.

Method

1. **Supply chain attack:** The attackers took advantage of DeepSeek's growing popularity to upload fake packages to PyPI.
2. **Malware distribution:** The "deepseeek" and "deepseekai" packages were uploaded to PyPI on January 29, 2025.
3. **Data exfiltration:** The stolen information was exfiltrated to a command-and-control server operated through the legitimate Pipedream automation platform.
4. **Persistence:** The malware used various techniques to disguise its presence and ensure that it remains active even after a system reboot.
5. **Remote control:** The attackers were able to control the infected systems remotely by sending commands to the malware.

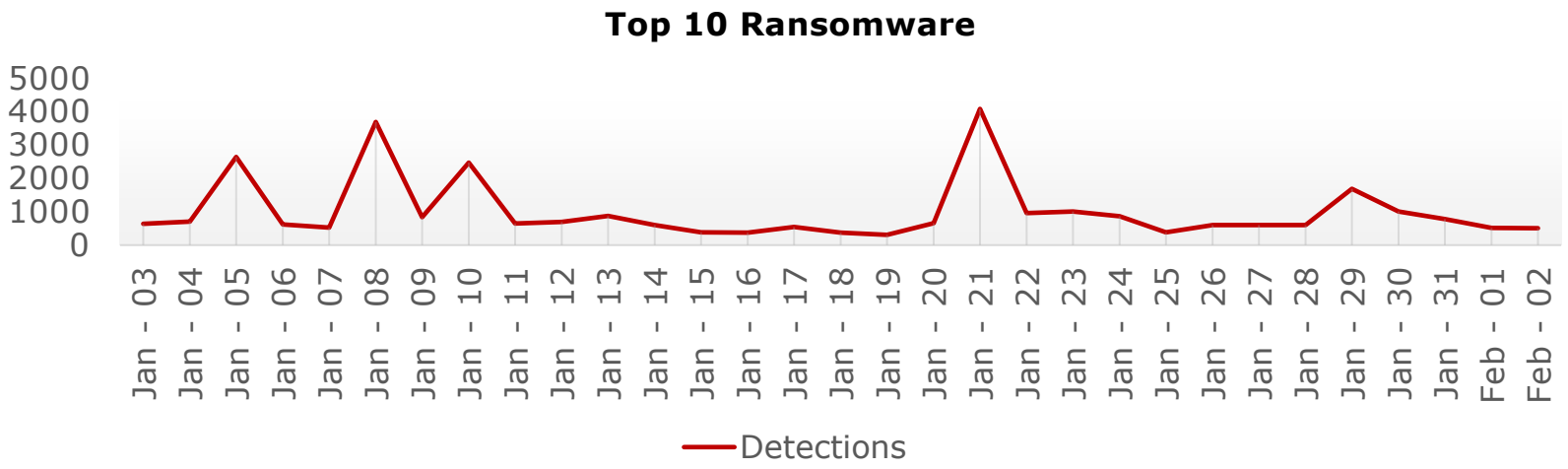


Good to know

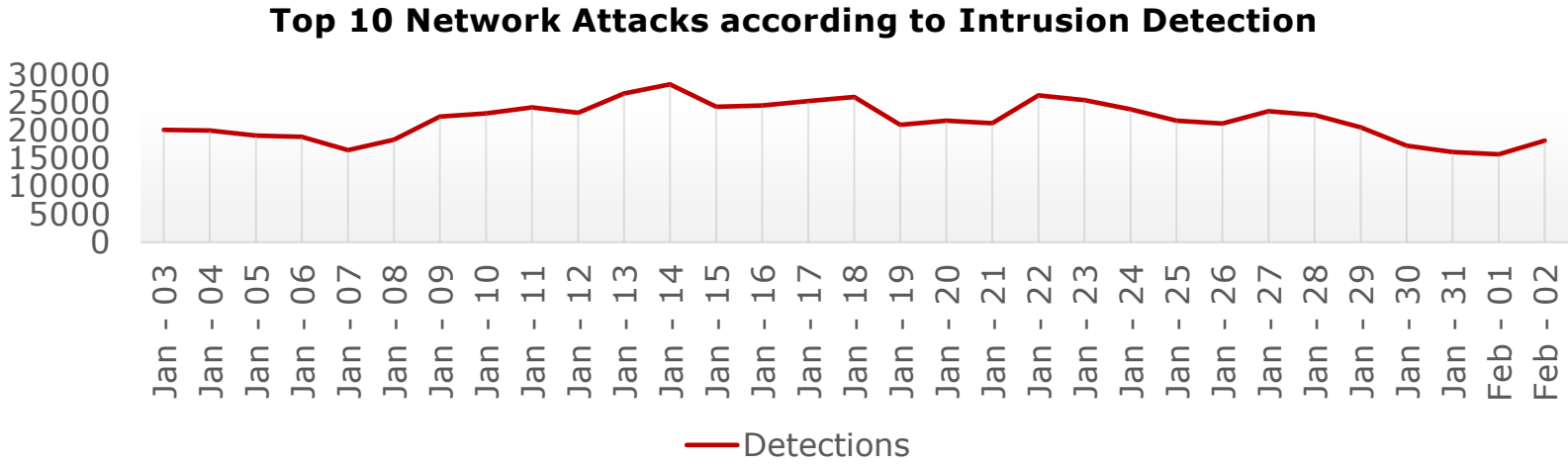
Summary		Link
16.01.2025	**AWS account data ended up on the dark web** In the course of an attack, numerous AWS account data has appeared on the darknet. Kaspersky discovered over 100 compromised data packets for the AWS platform. Although no sensitive information is affected, the incident shows the need for proactive security measures.	Continue reading
21.01.2025	**ChatGPT can be used for DDoS attacks** A security researcher has discovered that ChatGPT can be misused for DDoS attacks. By sending HTTP POST requests to the ChatGPT API, thousands of hyperlinks can be delivered, resulting in congestion on the target web page. OpenAI and Microsoft have not yet responded to the researcher's contact attempts.	Continue reading
23.01.2025	**NTC finds security vulnerabilities in hospital information systems** The National Cybersecurity Test Institute (NTC) has discovered serious security vulnerabilities in three of the most widely used hospital information systems (HIS) in several Swiss hospitals. In total, over 40 moderate to severe vulnerabilities have been identified, including fundamental architectural issues and inadequate encryption. Some vulnerabilities allow full access to patient data within a few hours.	Continue reading
26.01.2025	**Android with new functions against theft** Google has introduced new anti-theft features for Android. The Identity Check feature automatically locks devices if they are in an untrusted location and requires biometric authentication. Another function, "Theft Detection Lock", detects theft attempts on unlocked smartphones and automatically activates the screen lock.	Continue reading

Appendixes

Monthly Top 10 in Switzerland 1/2



Name	%
Trojan-Ransom.AndroidOS.Congur.cw	25.99
Trojan-Ransom.AndroidOS.Small.cj	7.76
Trojan-Ransom.AndroidOS.Svpeng.ac	7.62
Trojan-Ransom.AndroidOS.Congur.ap	6.59
Trojan-Ransom.Win32.Encoder	4.54
Trojan-Ransom.AndroidOS.Svpeng.ah	3.81
Trojan-Ransom.AndroidOS.Svpeng.snt	3.52
Trojan-Ransom.AndroidOS.Svpeng.ab	2.05
Trojan-Ransom.AndroidOS.Congur.bf	1.9
Trojan-Ransom.AndroidOS.Svpeng.ad	1.8

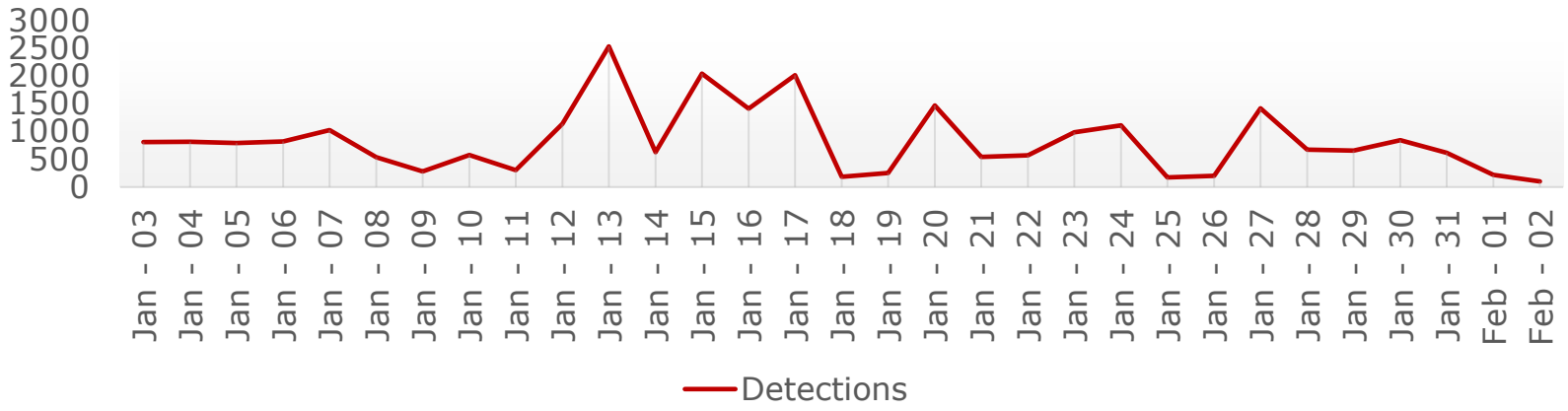


Name	%
Bruteforce.Generic.Rdp.a	47.32
Bruteforce.Generic.Rdp.d	39.84
Scan.Generic.PortScan.UDP	9.27
DoS.Generic.Flood.TCPSYN	1.79
Scan.Generic.PortScan.TCP	1.47
Bruteforce.Generic.Rdp.c	0.07
Intrusion.Generic.CVE-2021-44228.a	0.05
Intrusion.Generic.CVE-2018-11776.a.exploit	0.04
Intrusion.Generic.Win.CMD.exploit	0.04
Intrusion.Win.CVE-2019-0708.a.exploit	0.03

Quelle: https://cybermap.kaspersky.com/stats

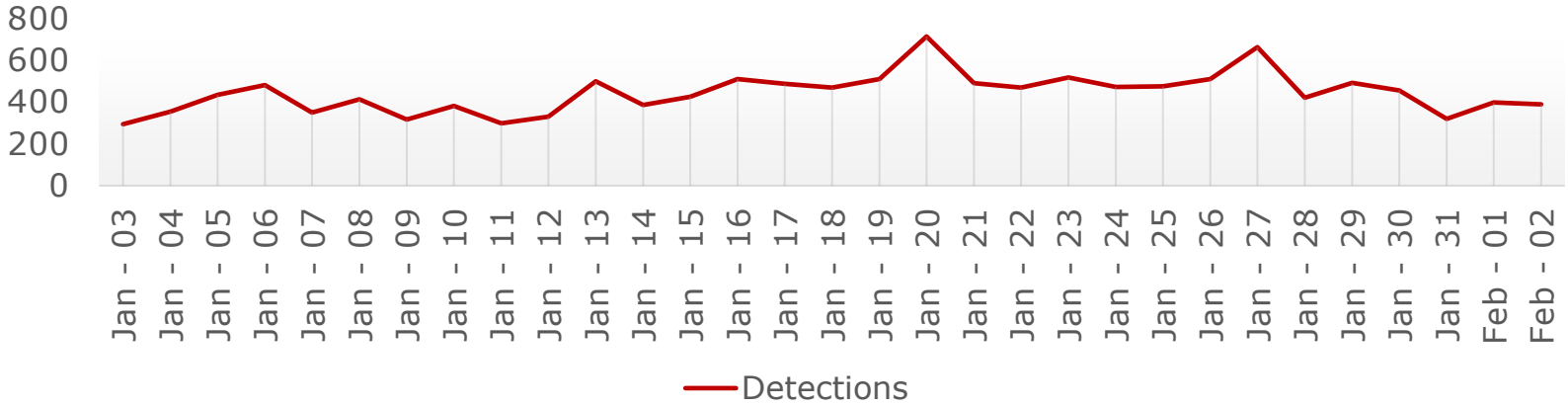
Monthly Top 10 in Switzerland 2/2

Top 10 Infected E-mails



Name	%
Trojan.Script.Generic	15.06
Hoax.Win32.KL-Demo.a	7.36
Packed.Multi.MultiPacked.gen	7.33
Packed.Multi.SuspiciousPacker.gen	6.81
Trojan.MSOffice.Badur.gen	5.76
Trojan.Win32.Badun.gen	4.71
DangerousObject.Multi.Generic	4.38
Backdoor.MSIL.Remcos.gen	3.73
Trojan-Spy.MSIL.Noon.gen	3.1
Trojan-Downloader.Script.Generic	2.81

Top 10 Vulnerabilities



Name	%
Exploit.Win32.CVE-2010-2862.a	94.71
Exploit.Linux.CVE-2017-7308.a	1.01
Exploit.Script.Generic	0.91
Exploit.Win32.Pidief.daa	0.79
Exploit.Win32.CVE-2011-3402.a	0.64
Exploit.AndroidOS.Lotoor.be	0.39
Exploit.Script.CVE-2021-26855.gen	0.34
Exploit.Linux.CVE-2014-3153.a	0.31
Exploit.Win32.Dropper	0.29
Exploit.JS.Agent.a	0.2

Quelle: https://cybermap.kaspersky.com/stats

AVENIQ

Your contact person

Alice Drifte
Professional Cyber
Security Consultant

+41 58 059 41 26

alice.drifte@aveniq.ch