AVENIQ

Cyber Threat Landscape

Alice Drifte
Professional Cyber Security Consultant

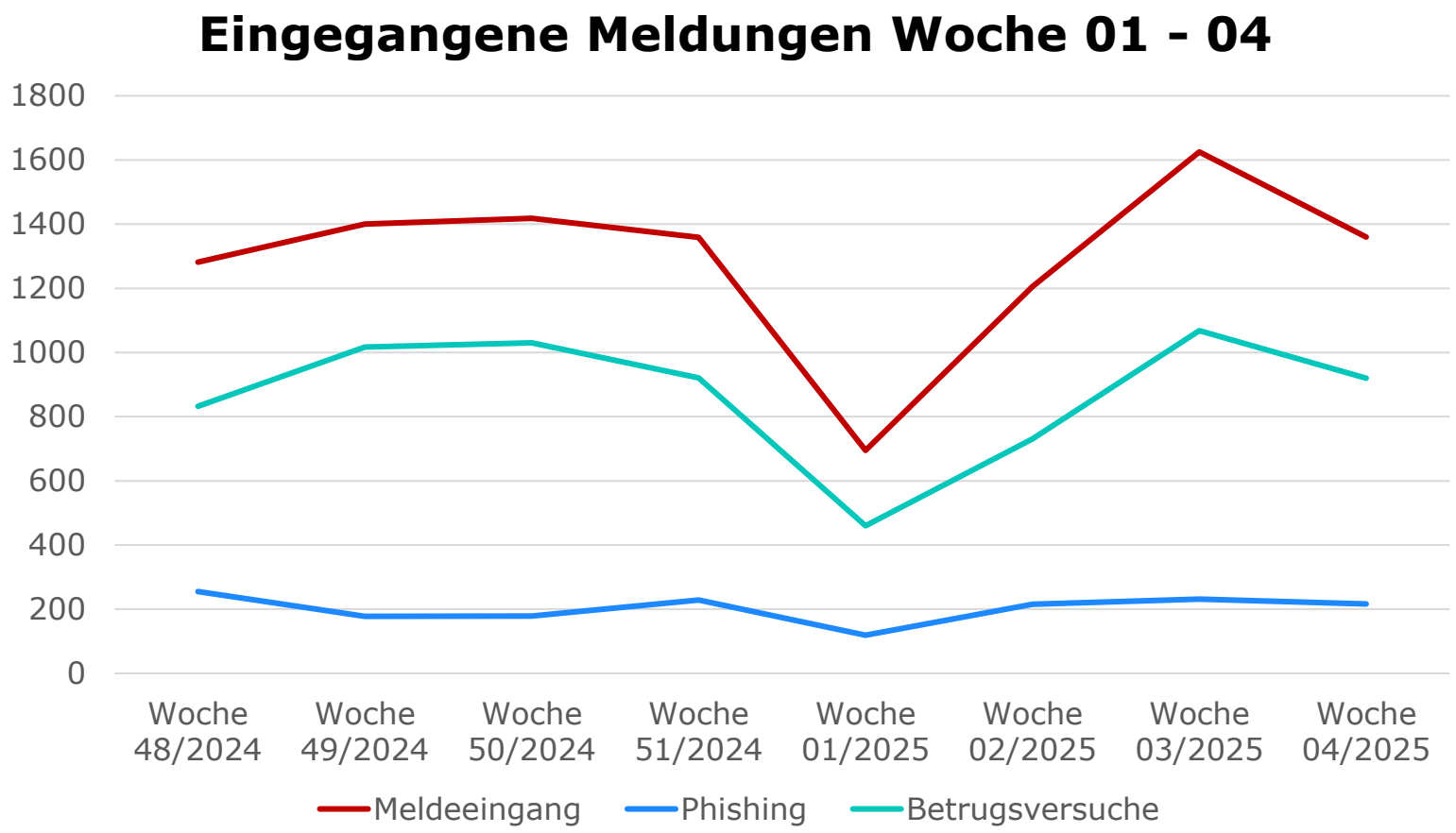
Januar 2025

Agenda

1. Eingegangene Meldungen Januar 2025
2. Thema des Monats
3. Cyber Angriffe des Monats
4. Schwachstellen des Monats
5. Insights aus dem Aveniq Security Team
6. Tactics, Techniques & Procedures
7. Gut zu wissen
8. Anhänge

Eingegangene Meldungen Januar 2025 in der Schweiz

Bundesamt für Cybersicherheit (BACS)



Trends im Januar

Im Vergleich zum Dezember mit 5459 Meldungen sind im Januar 4885 Meldungen eingetreten.

Der Bund zudem warnt vor Phishing im Namen der ESTV und Betrugs-SMS im Namen von Binance (Link).

Thema des Monats

«Es war nur eine Frage der Zeit, bis die pro-russische Hackergruppe NoName057(16) auch die Schweiz ins Visier nimmt. Willkommen in der neuen Realität der Cyberangriffe!»

Zusammenfassung		Link
21.01.2025	**Hackerangriff legt Schweizer Websites lahm**  Im Januar 2025 wurde die Schweiz von einem bedeutenden Cyberangriff erschüttert, der mehrere Websites lahmlegte. Die pro-russische Hackergruppe NoName057(16) bekannte sich zu den Angriffen, die sich gegen verschiedene Schweizer Institutionen richteten. Zu den betroffenen Websites gehörten unter anderem die der Zürcher und Waadtländer Kantonalbank sowie die Internetauftritte der Gemeinden Luzern, Kriens und Adligenswil. Die Angriffe erfolgten mittels sogenannter Distributed Denial-of-Service (DDoS)-Attacken, bei denen die Websites durch massenhafte Anfragen überlastet wurden und somit für reguläre Nutzer nicht mehr erreichbar waren. Diese Art von Angriff führt zwar nicht zum Abfluss von Daten, kann jedoch erhebliche Störungen verursachen. Die Hackergruppe NoName057(16) ist seit 2022 aktiv und hat sich auf politisch motivierte Cyberangriffe spezialisiert. Ihre Angriffe richten sich häufig gegen Länder, die die Ukraine im Krieg gegen Russland unterstützen. Die Gruppe kommuniziert hauptsächlich über Telegram und gibt dort ihre Ziele bekannt. Dieser Vorfall verdeutlicht die anhaltende Bedrohung durch Cyberkriminalität und die Notwendigkeit, kontinuierlich in die Cybersicherheit zu investieren, um solche Angriffe abwehren zu können. Das Bundesamt für Cybersicherheit hatte im Vorfeld des World Economic Forums (WEF) bereits vor möglichen Angriffen gewarnt, da das Risiko während dieser Zeit als besonders hoch eingeschätzt wurde.	Link

Cyber Angriffe des Monats

Zusammenfassung		Link
08.01.2025	**Casio bestätigt Abfluss von Kundendaten** Der japanische Elektronikhersteller Casio bestätigte, dass bei einem Ransomware-Angriff im Oktober 2024 persönliche Daten von etwa 8500 Personen offengelegt wurden. Betroffen sind hauptsächlich Mitarbeiter, Geschäftspartner und einige Kunden. Die gestohlenen Daten umfassen Namen, Adressen, Telefonnummern und weitere persönliche Informationen. Casio arbeitet mit externen Spezialisten zusammen, um den Vorfall zu untersuchen und weitere Schäden zu verhindern.	Weiterlesen
13.01.2025	**Ausgleichskasse Swissmem warnt ihre 200'000 Versicherten** Die Ausgleichskasse Swissmem wurde Opfer eines Cyberangriffs, bei dem Daten gestohlen wurden. Der genaue Umfang des Datendiebstahls ist noch unklar, aber Swissmem warnt ihre 200.000 Versicherten vor möglichen betrügerischen Kontakten. Die betroffenen Daten könnten für Phishing-Angriffe oder andere betrügerische Aktivitäten genutzt werden. Swissmem arbeitet eng mit Cybersicherheitsexperten zusammen, um den Vorfall zu klären.	Weiterlesen
21.01.2025	**Russische Hacker legen Webseiten von Banken und Gemeinden lahm** Mehrere Schweizer Websites, darunter die der Zürcher und Waadtländer Kantonalbank sowie der Gemeinden Luzern, Adligenswil, Kriens und Ebikon, wurden von der pro-russischen Hackergruppe NoName057(16) durch DDoS-Angriffe lahmgelegt. Diese Angriffe erfolgten während des Weltwirtschaftsforums in Davos und führten zu erheblichen Störungen. Die Hackergruppe wollte damit Aufmerksamkeit erregen und demonstrierte ihre Fähigkeiten im Netz. Das Bundesamt für Cybersicherheit hatte im Vorfeld vor solchen Angriffen gewarnt.	Weiterlesen
03.02.2025	**Cyberangriff auf kantonale Strassenzustand-Webseite in Graubünden** Die kantonale Strassenzustands-Website in Graubünden wurde am 2. Februar 2025 zweimal durch Cyberangriffe lahmgelegt. Die Angriffe fanden um 10:00 Uhr und 15:30 Uhr statt und führten zu erheblichen Störungen des Dienstes. Die Verantwortlichen arbeiten daran, die Sicherheitslücken zu schliessen und die Website wieder voll funktionsfähig zu machen. Dieser Vorfall zeigt die anhaltende Bedrohung durch Cyberkriminalität und die Notwendigkeit, kontinuierlich in die Cybersicherheit zu investieren.	Weiterlesen

Schwachstellen des Monats

Zusammenfassung				Empfehlung	Link
ivanti	**09.01.2025** **Ivanti**	Security Advisory	Mittels Public-Facing Application Exploit kann Remote-Code ausgeführt werden.	• Aktualisieren der Software	Link
FORTINET	**14.01.2025** **Fortinet**	News	Mittels Public-Facing Application Exploit kann Remote-Code ausgeführt werden.	• Aktualisieren der Software	Link
Adobe	**14.01.2025** **Adobe**	Security Advisory	Ausführung von beliebigem Code. Mittels Exploitation for Client Execution Methode werden mehrere Schwachstellen auf den Client-Devices ausgenutzt.	• Aktualisieren der Software	Link
Microsoft	**15.01.2025** **Microsoft**	Security Advisory	Mehrere Schwachstellen in Microsoft Produkte.	• Aktualisieren der Software	Link
ORACLE	**21.01.2025** **Oracle**	Security Updates	Mehrere Schwachstellen in Oracle Produkte.	• Aktualisieren der Software	Link
	27.01.2025 **Google Chrome**	Security Updates	Ausführung von beliebigem Code. Mittels Drive-By Compromise Methode werden mehrere Schwachstellen ausgenutzt.	• Aktualisieren der Software	Link
SONICWALL	**27.01.2025** **SonicWall**	Security Update	Mittels Public-Facing Application Exploit kann Remote-Code ausgeführt werden.	• Aktualisieren der Software	Link
	30.01.2025 **Apple Products**	Security Updates	Mittels Exploitation for Client Execution Methode werden mehrere Schwachstellen ausgenutzt.	• Aktualisieren der Software	Link

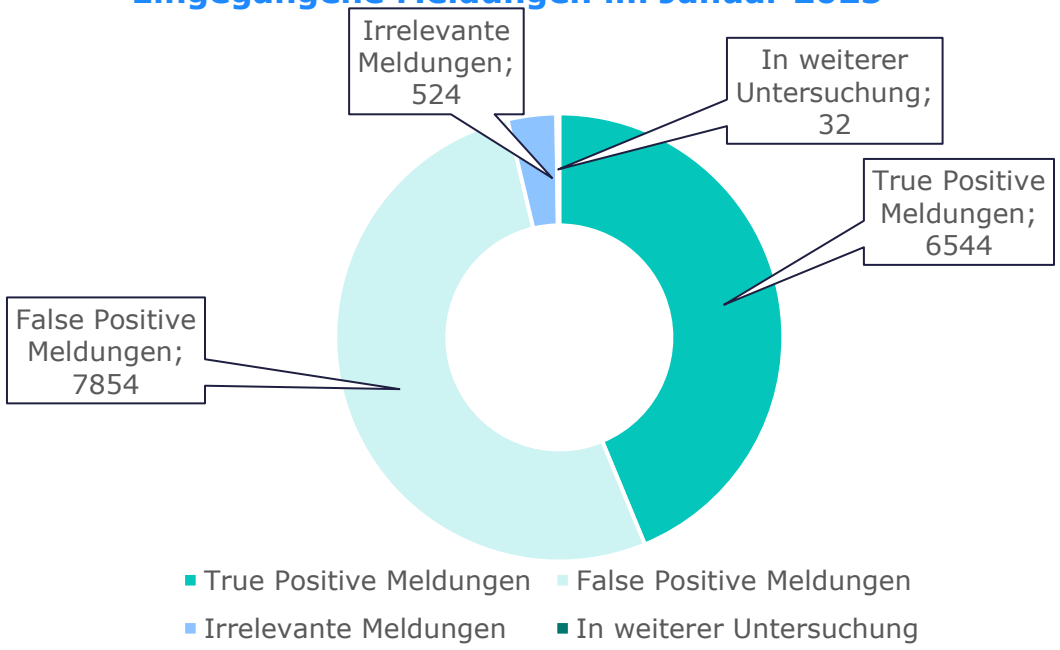
Insights aus dem Aveniq Security Team

Interessiere an unsere Security Services?
*Weitere Infos unter **aveniq.ch/cyber-security***

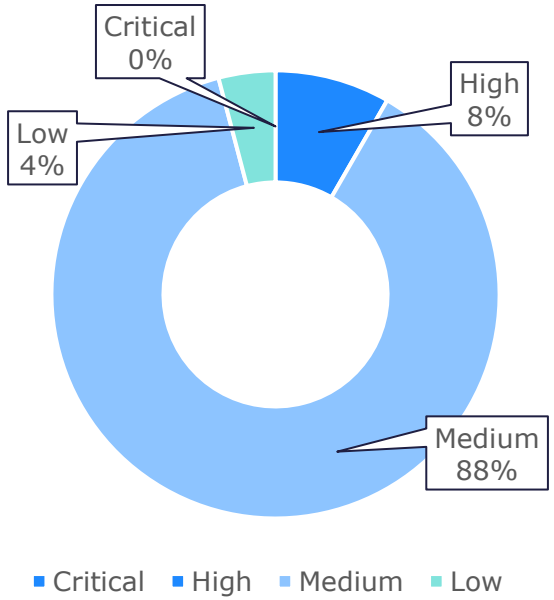
Neuste Malware-Varianten

14.01.2025	WP3.XYZ	Malware	Die WP3.XYZ-Malware hat über 5.000 WordPress-Websites kompromittiert, indem sie gefälschte Admin-Konten erstellt, bösartige Plugins installiert und sensible Daten exfiltriert.
15.01.2025	MikroTik	Botnet	Ein Botnet aus 13.000 MikroTik-Geräten nutzt falsch konfigurierte SPF-DNS-Einträge, um Malware über gefälschte DHL-Rechnungen zu verbreiten.
29.01.2025	Aquabotv3	Botnet	Die neue Aquabotv3-Botnet-Malware nutzt eine Befehlsinjektionsschwachstelle in Mitel SIP-Telefonen aus, um diese in ihr Botnetz zu integrieren.

Eingegangene Meldungen im Januar 2025



Bearbeitete Meldungen im Januar 2025



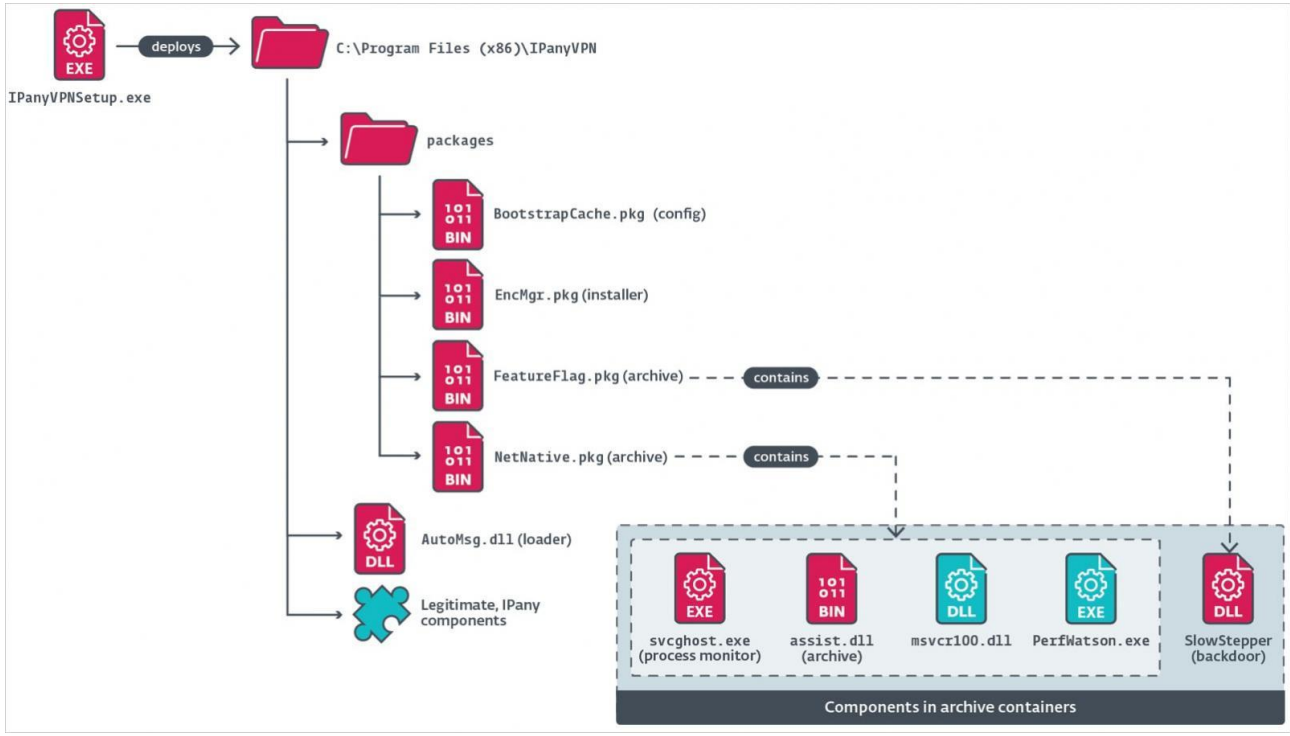
Tactics, Techniques & Procedures 1/2

Zusammnfasung		Link
22.01.2025	**IPany VPN bei Supply-Chain-Angriff verletzt, um benutzerdefinierte Malware zu verbreiten**	Link

Im Januar 2025 wurde der südkoreanische VPN-Anbieter IPany Opfer eines Supply-Chain-Angriffs, der von der China-verbundenen Hackergruppe "PlushDaemon" durchgeführt wurde. Diese Gruppe kompromittierte den VPN-Installer von IPany, um die massgeschneiderte Malware "SlowStepper" zu verbreiten.

Methode

1. **Supply-Chain-Angriff**: PlushDaemon nutzte eine Schwachstelle in der Lieferkette von IPany aus, indem sie den Installationsprozess des VPN-Clients kompromittierten.
2. **Verbreitung der Malware**: Die Malware "SlowStepper" wurde so konzipiert, dass sie unbemerkt bleibt und sich tief in das System des Opfers eingräbt.
3. **Datenexfiltration**: Einmal installiert, sammelt SlowStepper sensible Informationen vom infizierten System.
4. **Persistenz**: Um sicherzustellen, dass die Malware auch nach einem Neustart des Systems aktiv bleibt, implementiert SlowStepper Mechanismen zur Persistenz.
5. **Fernsteuerung**: Die Angreifer können die infizierten Systeme aus der Ferne steuern, indem sie Befehle an die Malware senden.



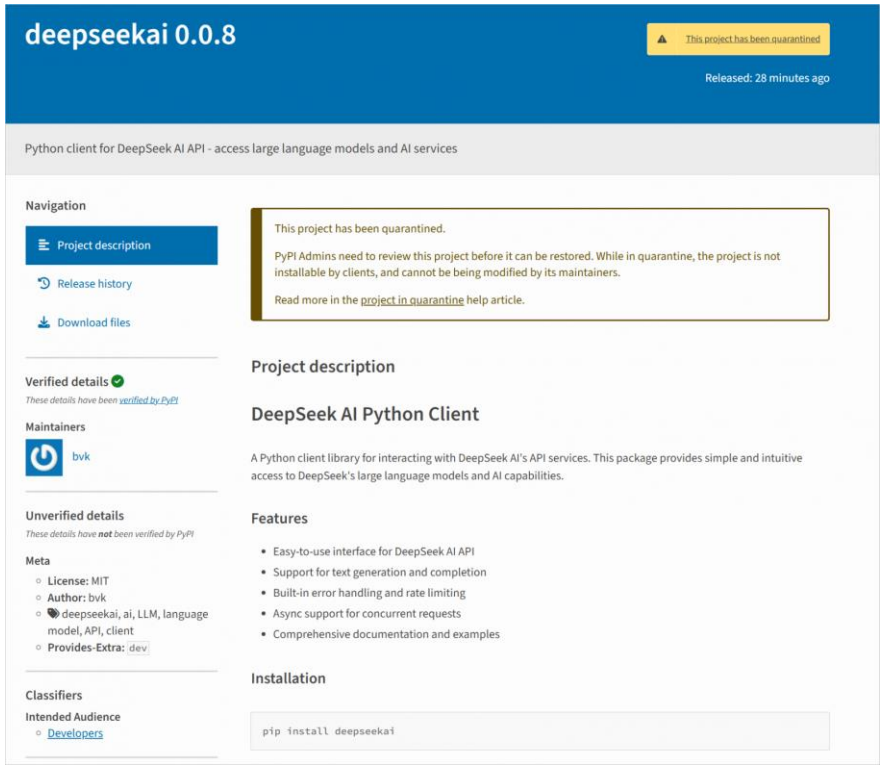
Tactics, Techniques & Procedures 2/2

Zusammenfassung		Link
03.02.2025	**DeepSeek KI-Tools, die von Infostealer-Malware auf PyPI imitiert werden**	Link

Im Januar 2025 nutzten Bedrohungsakteure die Popularität von DeepSeek aus, um zwei bösartige Infostealer-Pakete namens "deepseeek" und "deepseekai" auf dem Python Package Index (PyPI) hochzuladen. Diese Pakete gaben vor, Entwickler-Tools für die AI-Plattform zu sein, stahlen jedoch sensible Informationen von den Maschinen der Entwickler, einschliesslich API-Schlüssel und Datenbank-Anmeldeinformationen.

Methode

1. **Supply-Chain-Angriff**: Die Angreifer nutzten die wachsende Beliebtheit von DeepSeek, um gefälschte Pakete auf PyPI hochzuladen.
2. **Verbreitung der Malware**:Die Pakete "deepseeek" und "deepseekai" wurden am 29. Januar 2025 auf PyPI hochgeladen.
3. **Datenexfiltration**:Die gestohlenen Informationen wurden an einen Command-and-Control-Server exfiltriert, der über die legitime Automatisierungsplattform Pipedream betrieben wurde.
4. **Persistenz**:Die Malware nutzte verschiedene Techniken, um ihre Anwesenheit zu verschleiern und sicherzustellen, dass sie auch nach einem Neustart des Systems aktiv bleibt.
5. **Fernsteuerung**:Die Angreifer konnten die infizierten Systeme aus der Ferne steuern, indem sie Befehle an die Malware sendeten.



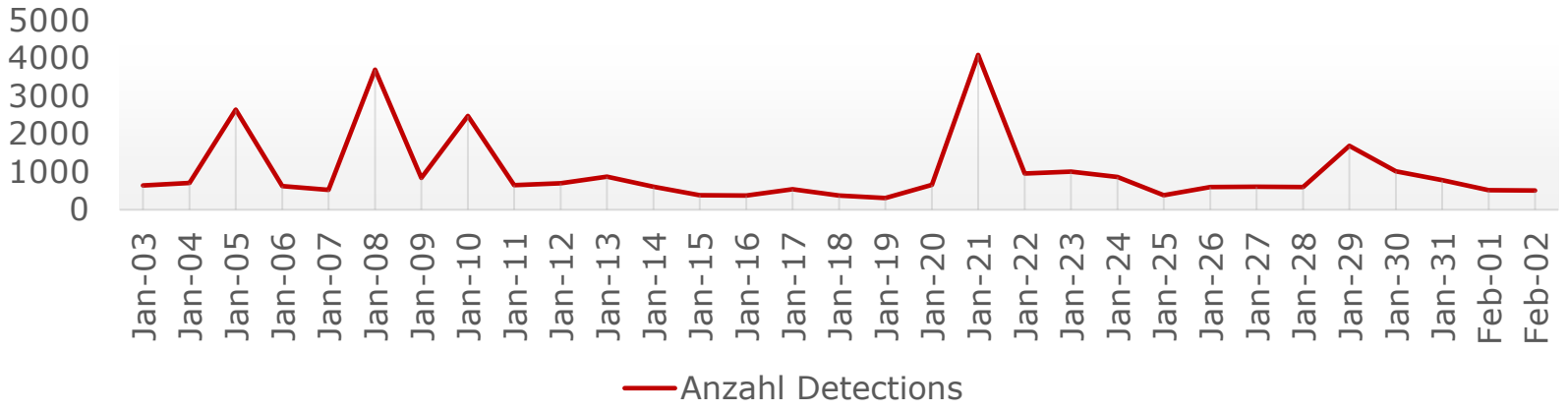
Gut zu wissen

Zusammenfassung		Link
16.01.2025	**AWS-Account-Daten im Darknet gelandet** Im Zuge eines Angriffs sind zahlreiche AWS-Account-Daten im Darknet aufgetaucht. Kaspersky entdeckte über 100 kompromittierte Datenpakete für die AWS-Plattform. Obwohl keine sensiblen Informationen betroffen sind, zeigt der Vorfall die Notwendigkeit proaktiver Sicherheitsmassnahmen.	Weiterlesen
21.01.2025	**ChatGPT lässt sich für DDoS-Angriffe zweckentfremden** Ein Sicherheitsforscher hat entdeckt, dass ChatGPT für DDoS-Angriffe missbraucht werden kann. Durch das Senden von HTTP-POST-Anfragen an die ChatGPT-API können Tausende von Hyperlinks übermittelt werden, was zu einer Überlastung der Zielwebseite führt. OpenAI und Microsoft haben bisher nicht auf die Kontaktversuche des Forschers reagiert.	Weiterlesen
23.01.2025	**NTC findet Sicherheitslücken in Klinikinformationssystemen** Das Nationale Testinstitut für Cybersicherheit (NTC) hat in mehreren Schweizer Spitälern schwerwiegende Sicherheitslücken in drei der meistgenutzten Klinikinformationssysteme (KIS) entdeckt. Insgesamt wurden über 40 mittlere bis schwere Schwachstellen identifiziert, darunter grundlegende Architekturprobleme und unzureichende Verschlüsselung. Einige Schwachstellen ermöglichen den vollständigen Zugriff auf Patientendaten innerhalb weniger Stunden.	Weiterlesen
26.01.2025	**Android mit neuen Funktionen gegen Diebstahl** Google hat neue Diebstahlschutzfunktionen für Android eingeführt. Die Funktion "Identity Check" sperrt Geräte automatisch, wenn sie sich an einem nicht vertrauenswürdigen Standort befinden, und verlangt eine biometrische Authentifizierung. Eine weitere Funktion, "Theft Detection Lock", erkennt Diebstahlversuche bei entsperrten Smartphones und aktiviert automatisch die Displaysperre.	Weiterlesen

Anhänge

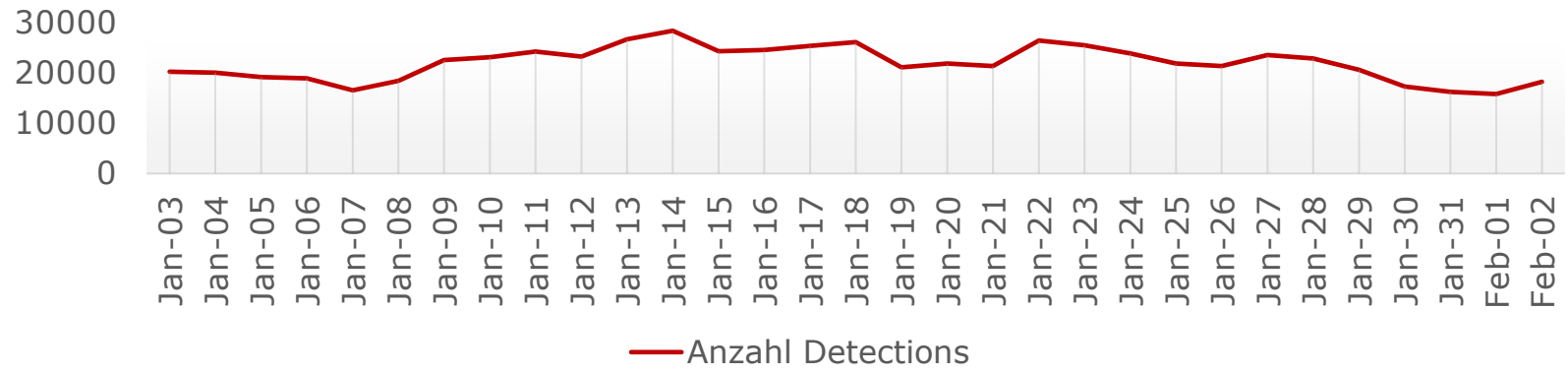
Monatliche Top 10 der Schweiz 1/2

Top 10 Ransomware (Aufkommen/Ranking)



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

Top 10 Netzwerkangriffe gem. Intrusion Detection (Aufkommen/Ranking)

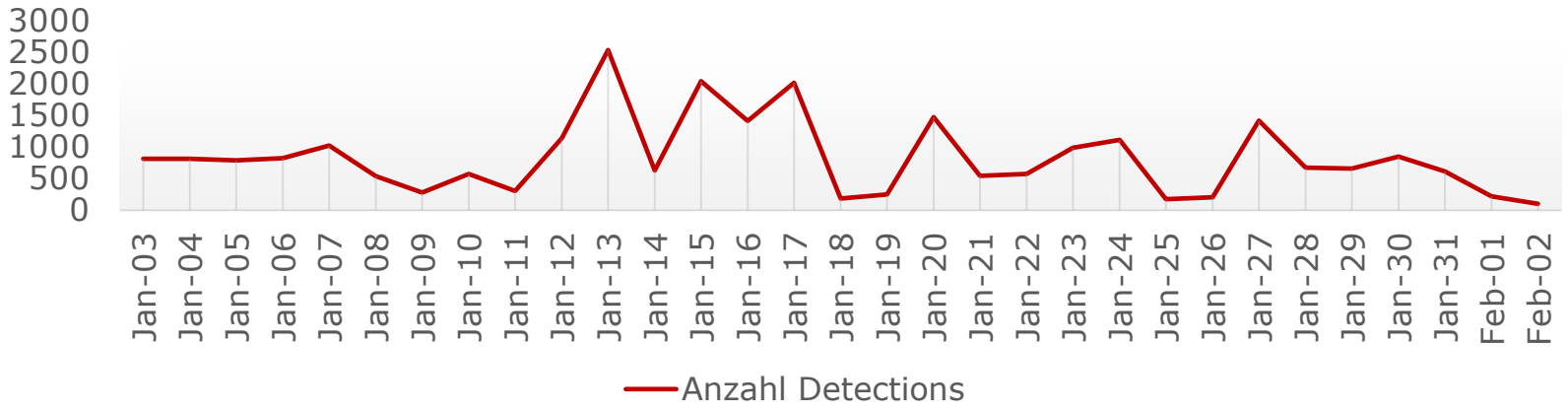


Name	%
Bruteforce.Generic.Rdp.a	47.32
Bruteforce.Generic.Rdp.d	39.84
Scan.Generic.PortScan.UDP	9.27
DoS.Generic.Flood.TCPSYN	1.79
Scan.Generic.PortScan.TCP	1.47
Bruteforce.Generic.Rdp.c	0.07
Intrusion.Generic.CVE-2021-44228.a	0.05
Intrusion.Generic.CVE-2018-11776.a.exploit	0.04
Intrusion.Generic.Win.CMD.exploit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

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

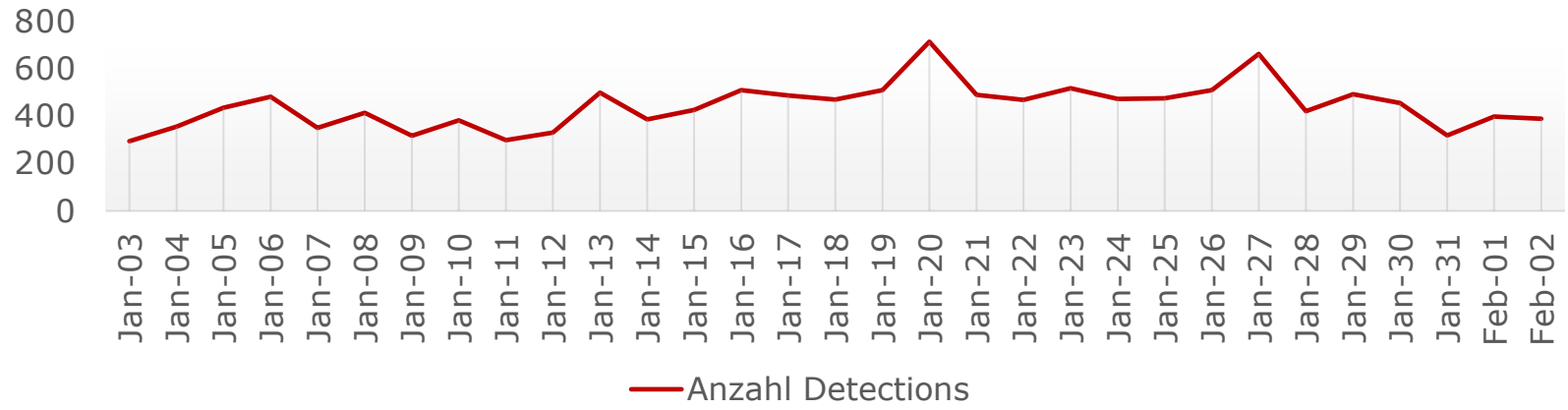
Monatliche Top 10 der Schweiz 2/2

Top 10 Infizierte Mails (Aufkommen/Ranking)



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 Schwachstellen (Aufkommen/Ranking)



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

Ihr Ansprechpartner

Alice Drifte
Professional Cyber
Security Consultant

+41 58 059 41 26

alice.drifte@aveniq.ch