AVENIQ

Cyber Threat Landscape

Cen Magjuni Senior Consultant Business Resilience

January 2024

Agenda

1. Current global trends
2. Topic of the month
3. Cyber Attacks of the Month
4. Vulnerabilities of the month
5. Tactics, Techniques & Procedures
6. Good to know
7. Appendixes

Global Trends in December 2023

Type of Threats	Trends compared to	
	November 2023	December 2022
Malware	→	↗
Intrusionen	→	↗
Ransomware	↘	↘
Phishing	↘	↘
Web App Angriffe	↘	↗
Cryptojacking	↘	↗
IoT Malware	↘	↘

Cyber Threat Index

Critical
850 – 1000 Attacks

High
700 – 849 Attacks

Medium
550 – 699 Attacks

Low
350 – 549 Attacks

Lowest
0 – 349 Attacks

← **658 Attacks worldwide**
(-5% compared to last Month)

↘	Abnehmend
→	Stabil
↗	Zunehmend
⇗	Stark zunehmend

Topic of the month

Summary		Link
01.02.2024 DATASPORT	**Hackers sell data of 900,000 Swiss amateur athletes** Around 1.3 million records were recently offered for sale as a data package on a hacker forum. More than 900,000 of these are said to affect Swiss citizens who were captured from the company Datasport. The rest of the data relate to neighbouring countries and other countries. Datasport provides services such as timekeeping, start number allocation and online registration for popular sports events - from the Engadin Ski Marathon to numerous city runs and cycling races. Amateur athletes can also use myDS to collect their performance data and publish it as they wish. On January 23, the company itself reported a cyberattack on its website. According to CEO Thomas Bachofner, as part of the periodic review of technical and organizational measures for data and information security, Datasport has increased geo-redundancy and outsourced the data to another data center for backup purposes. In the course of the implementation, a security-relevant vulnerability must have existed in this data center shortly before January 23. After it was discovered, it was closed by Datasport within minutes. The hacker or hackers must have taken advantage of this short window of opportunity. After the vulnerability was published by the perpetrators, the data was checked again, according to Bachofner. The company estimates that up to 1 million records could theoretically be affected. However, security-relevant information such as passwords or means of payment are not affected by the leak, emphasizes the Datasport CEO. The potentially affected information is posted on Datasport.com by the users themselves and can be viewed by the public. This includes data such as names, postal addresses and dates of birth, but also e-mail addresses and telephone numbers of myDS users. This is confirmed by data samples published by the hacker. However, the myID numbers contained in the data package are only used internally by Datasport in order to avoid user duplication.	Link

Cyber Attacks of the month 1/2

Summary		Link
30.01.2024 Schneider Electric	**Cactus Hacks Schneider Electric** On January 17, the major French electronics company Schneider Electric was attacked by the Cactus ransomware gang. The Sustainability Business department was affected, disrupting part of the cloud platform and still experiencing outages. According to sources, several terabytes of company data were captured by the hackers. Customers of the affected division include Allegiant Travel Company, Clorox, DHL, DuPont, Hilton, Lexmark, PepsiCo and Walmart, among others. The stolen data could include sensitive information about customers' energy consumption, industrial control and automation systems, and compliance with environmental and energy regulations. The hackers threaten to publish the data if a ransom is not paid. Schneider Electric said the attack was limited to its Sustainability Business division, other parts of the company were not affected. The Sustainability Business department is currently carrying out recovery measures and functional tests, so access should be possible again in a few days. The company has hired a cybersecurity firm, reported the incident to the authorities and is conducting a detailed forensic analysis. Schneider Electric already had problems with hackers last year. Using the widespread Moveit vulnerability, the Clop ransomware gang managed to capture the company's data.	Link
25.01.2024 Hewlett Packard Enterprise	**HPE reports cyberattack on its own email system** HPE was infiltrated by Russian hackers who gained access to the email system. The exact extent is still unclear, the cybercriminals were active in the system unnoticed for about half a year. Details are yet to be clarified, but the company believes that Russian attackers Midnight Blizzard, also known as Cozy Bear, are behind the attack. The hackers are said to have infiltrated the company's email system and presumably gained access to HPE's email environment as early as May 2023. The successful attack was only noticed in December last year. According to HPE, the criminals were able to access the mailboxes of some users, including go-to-market and cybersecurity, but more precise figures and content are still pending. It is investigating how the attack was carried out. HPE says the incident had no impact on HPE's financial results.	Link

Cyber Attacks of the month 2/2

Summary		Link
19.01.2024	**Cyber attack on the cantonal website of the Canton of Basel-Stadt** Since 19.01.2023, the cantonal website of Basel-Stadt (www.bs.ch) has been the target of a cyberattack. At times, the site was unavailable. The cantonal IT experts have taken countermeasures to ensure trouble-free operations again. The DDoS attack, in which a large number of targeted requests are used to bring about a service blockade, began at around 6:30 a.m. The website has been available again since 09.00 a.m. However, impairments are still to be expected. The cybercriminals are not known.	Link
18.01.2024	**Swiss mobile phone supplier Nexus Telecom hacked** The 8Base ransomware gang is said to have captured a large amount of confidential information from Nexus Telecom. The victim delivers network monitoring software to providers worldwide. The criminals threaten to publish the stolen data on their blackmail and leak site on the darknet. The stolen data and the extent of the damage are still being investigated. Nexus Telecom's customers include major European providers such as British Telecommunications (BT) and Deutsche Telekom, as well as others overseas. 8Base is a ransomware group that has been active since March 2022 but only hit the headlines in the summer of 2023 when its activities were just behind the infamous Lockbit gang. Like other well-known ransomware groups, 8Base operates a website on the dark web. It lists hundreds of hacked companies – all victims who have refused to pay ransom so that their stolen data would not be made public. The cybercriminals are considered opportunistic in their choice of victims and attack tools: At the end of last year, IT security researchers discovered that a variant of the Phobos ransomware was used in the hacker attacks on 8Bbase. Phobos is available to cybercriminals as Ransomware as a Service (RaaS). The U.S. cybersecurity agency HC3 told 8Base last November that despite the aggressive portfolio of victims, the origins of the group and the identities of the operators remain a mystery. Cybersecurity researchers believe that the speed and efficiency of current operations do not indicate the beginning of a new group, but rather the continuation of an established and experienced organization.	Link

Vulnerabilities of the month 1/2

Summary		**Recommendations**	**Link**
31.01.2024 ivanti	**Multiple vulnerabilities in Ivanti products could allow remote code execution** Several vulnerabilities have been discovered in Ivanti products, the most serious of which could allow remote code execution: Ivanti Connect Secure, Ivanti Policy Secure (IPS), and Ivanti Neurons for Zero Trust Access (nZTA). Successful exploitation could enable remote code execution in the context of the system. Depending on the rights of the logged-in user, an attacker could then install programs, view, modify, or delete data. Users whose accounts are configured to have fewer privileges on the system may be less affected than users who work with administrative user rights. According to Ivanti, there are reports of targeted exploitation of CVE-2024-21893. Ivanti, CISA, and other sources have reported widespread exploitation of CVE-2024-21887 and CVE-2023-46805.	• Apply the updates provided by Ivanti to vulnerable systems after you have tested them. • Establish and maintain a vulnerability management process: Establish and maintain a documented vulnerability management process for corporate resources. Review and update documentation annually or if there are significant changes in the organization that could affect this protective measure. • Perform automated vulnerability scans of internal company assets on a quarterly or shorter basis. • Build and maintain a secure network architecture. At a minimum, a secure network architecture must take into account segmentation, least privilege, and availability.	Link
23.01.2024	**Multiple vulnerabilities in Apple products could allow arbitrary code execution** Several vulnerabilities have been discovered in Apple products, the most serious of which could allow arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow arbitrary code execution in the context of the logged-on user. Depending on the user's rights, an attacker could then install programs, view, modify, or delete data, or create new accounts with full user privileges. Users whose accounts are configured to have fewer privileges on the system may be less affected than users who work with administrative user rights.	• Establish and maintain a vulnerability management process • Perform penetration testing on applications. For critical applications, authenticated penetration testing is better at detecting vulnerabilities in business logic than code scanning and automated security testing • Apply the principle of least privilege to all systems and services. Run all software as a non-privileged user (without administrative rights) to reduce the impact of a successful attack.	Link

Vulnerabilities of the month 2/2

Summary		Recommendations	Link
17.01.2024 Citrix NetScaler	**New Zero-Days in Citrix NetScaler ADC, Gateway Under Attack** The zero-day vulnerabilities CVE-2023-6549 and CVE-2023-6548 were announced and patched on Tuesday. CVE-2023-6549 is a high-level denial-of-service vulnerability with a CVSS score of 8.2, while CVE-2023-6548 is a moderate vulnerability with a CVSS score of 5.5 that allows an authenticated attacker to remotely execute code on management interfaces.	• Immediate updates for all affected versions • Physically or logically separate network traffic to the device's management interface from normal network traffic • Apply the principle of least privilege to all systems and services. Run all software as a non-privileged user (without administrative rights) to reduce the impact of a successful attack.	Link
17.01.2024 ATLASSIAN Confluence	**A Vulnerability in Atlassian Confluence Data Center and Server Could Allow Remote Code Execution** A vulnerability has been discovered in Atlassian Confluence Server and Data Center that could allow remote code execution. Successful exploitation of this vulnerability could allow an attacker to create unauthorized Confluence administrator accounts to access the instance. An attacker could then perform administrator actions in the context of the Confluence instance. Currently, there are no reports of this vulnerability being exploited.	• Apply Atlassian's patches and workarounds to vulnerable systems immediately after testing. • Architecture of network sections to isolate critical systems, functions, or resources. Leverage physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to include all internet-facing services that you don't want to be accessible from the internal network. Configure separate Virtual Private Cloud (VPC) instances to isolate critical cloud systems.	Link
11.01.2024 CISCO	**Vulnerability in Cisco Unity Connection Could Allow Arbitrary Code Execution** A vulnerability has been discovered in Cisco Unity Connection that could allow arbitrary code execution on a target host. A successful attack could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system. Currently, there are no reports of this vulnerability being exploited.	• Apply the patches provided by Cisco to vulnerable systems after you have tested them. • Remove or deny access to unnecessary and potentially vulnerable software to prevent misuse by attackers. • Block code execution on a system through application control and/or script blocking.	Link

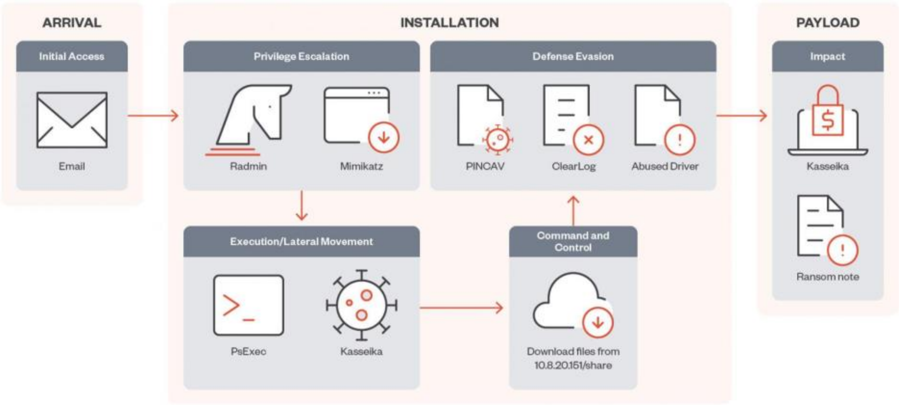
Tactics, Techniques & Procedures 1/2

Summary		Link
31.01.2024	**DarkGate malware delivered via Microsoft Teams** The customer has provided a suspicious screenshot of a phishing email. The domain "onmicrosoft.com" used in it seems authentic at first glance. However, the MDR SOC team suspects that the username and possibly the entire domain were compromised by the attackers. More than 1,000 user-generated MessageSent events were found in the customer environment. Although the recipient IDs were not included, they contained the tenant ID of the external user. This information allowed the team to identify "MemberAdded" events that occur when a user joins a team chat1. The Microsoft 365 tenant ID is a globally unique identifier that is assigned to organizations. It allows members of different organizations to communicate through Teams. As long as both chat participants have valid tenant IDs and external access is enabled, they can exchange messages. The MDR SOC team was able to query events that contained the external user's tenant ID and identify multiple MemberAdded events. These events occur when a user joins a chat in Teams. In this case, they were able to positively link the events to the attacker using the ChatThreadId field. The customer was given a list of users who had accepted the external chat and was able to identify potentially compromised resources and accounts to resolve the issue. Upon further investigation, the MDR SOC team discovered three users who had downloaded a suspicious file with a duplicate extension. The file was called "Navigating Future Changes October 2023.pdf.msi". Double-extension files are often used by attackers to trick users into downloading malicious executables. The second extension, in this case .msi, is usually hidden by the file system. The user believes they are downloading a PDF file for business purposes but receives a malicious installer instead. The MDR SOC team was able to pass the filename and associated hashes to the customer, who in turn forwarded this information to their Endpoint Detection and Response (EDR) provider so that the file could be added to the blocklist. The information about the file downloads also allowed the customer to identify the affected resources in order to isolate and clean them up.	Link

Tactics, Techniques & Procedures 2/2

Summary		Link
23.01.2024	**Kasseika Ransomware Uses Antivirus Drivers to Kill Other Antivirus Programs**	Link

The "Kasseika" ransomware operation uses the "Bring Your Own Vulnerable Driver" (BYOVD) tactic to disable antivirus software before encrypting files. In doing so, Kasseika abuses the Martini driver (Martini.sys/viragt64.sys), which is part of TG Soft's VirtIT Agent System. The ransomware shows similarities in source code with BlackMatter, although the latter has not been publicly leaked since its shutdown in late 2021. Kasseika attacks start with a phishing email to steal employee credentials and gain access to the corporate network. Then, the attackers use the Windows PsExec tool to execute malicious .bat files and download the vulnerable 'Martini.sys' driver.



The "Kasseika" ransomware uses the "Bring Your Own Vulnerable Driver" (BYOVD) tactic to disable antivirus software before encrypting files. In doing so, Kasseika abuses the Martini driver (Martini.sys/viragt64.sys), which is part of TG Soft's VirtIT Agent System. The ransomware shows similarities in source code with BlackMatter, although the latter has not been publicly leaked since its shutdown in late 2021. Kasseika attacks start with a phishing email to steal employee credentials and gain access to the corporate network. Then, the attackers use the Windows PsExec tool to execute malicious .bat files and download the vulnerable 'Martini.sys' driver. The ransomware encrypts targeted files using the ChaCha20 and RSA algorithms, adds a pseudo-random string to the filenames, and leaves a ransom note in each encrypted directory. To complicate security analysis, Kasseika deletes the system event logs after encryption and uses commands such as 'wevutil.exe'. Victims had 72 hours to deposit 50 bitcoins ($2,000,000) in the attacks observed by Trend Micro, with an additional $500,000 added every 24-hour delay.

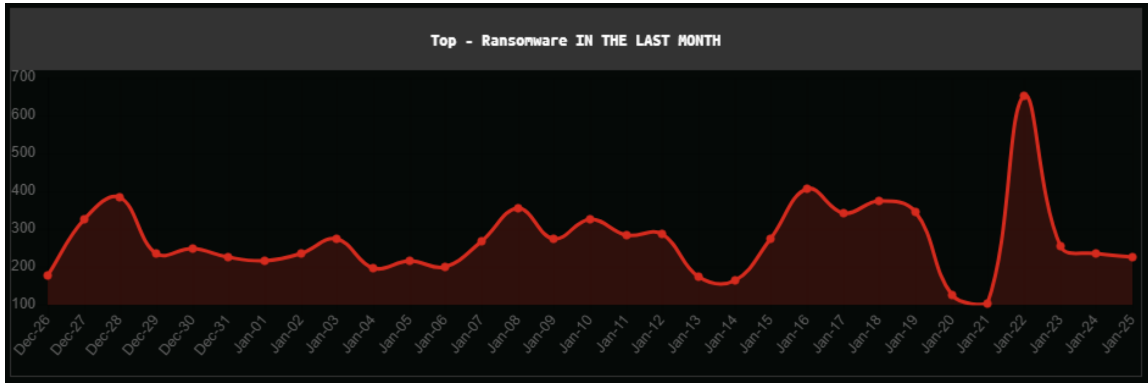
Good to know

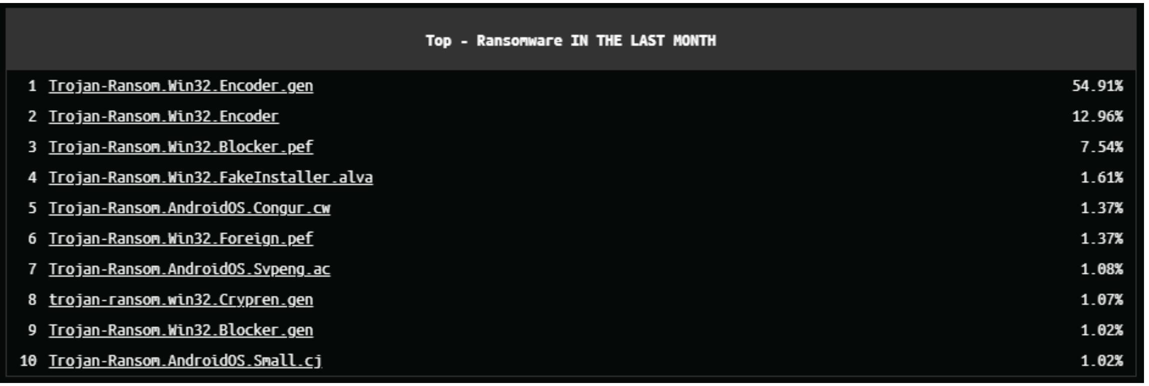
Summary		Link
26.01.2024	**Microsoft explains how Russian hackers spied on its executives** The "Kasseika" ransomware operation uses the "Bring Your Own Vulnerable Driver" (BYOVD) tactic to disable antivirus software before encrypting files. In doing so, Kasseika abuses the Martini driver (Martini.sys/viragt64.sys), which is part of TG Soft's VirtIT Agent System. The ransomware shares similarities with BlackMatter's source code, although it has not been publicly leaked since its shutdown in late 2021. Kasseika attacks begin with a phishing email that aims to steal employee credentials and gain access to the corporate network. The attackers then use the Windows PsExec tool to execute malicious .bat files and download the vulnerable driver 'Martini.sys'. The ransomware encrypts the targeted files using the ChaCha20 and RSA algorithms, adds a pseudo-random string to the filenames, and leaves a ransom message in each encrypted directory. To make security analysis more difficult, Kasseika deletes the system event logs after encryption and uses commands such as 'wevutil.exe'. In the attacks observed by Trend Micro, victims had 72 hours to deposit 50 bitcoins ($2,000,000), with another $500,000 added every 24 hours. This expanded access allowed the group to create more malicious OAuth applications and accounts to gain access to the Microsoft enterprise environment and thus the Office 365 Exchange Online service that provides access to email mailboxes.	Link
26.01.2024	**Digital reporting of cyber crimes on Suisse ePolice** On the Suisse ePolice (www.suisse-epolice.ch) platform, cyber crimes can be reported online around the clock. This is already possible in 12 cantons, and other cantons will follow in the coming months. The criminal complaints filed will be forwarded directly to the relevant police station. In around 50 percent of cybercrime offences, there is no need to go to the police station. The use of the platform is barrier-free and free of charge. The service is already available in the following cantons: AI, AR, BE, FR, GL, GR, LU, NE, SG, SZ, ZG, ZH.	Link

Appendixes

Monthly Top 10 in Switzerland 1/2

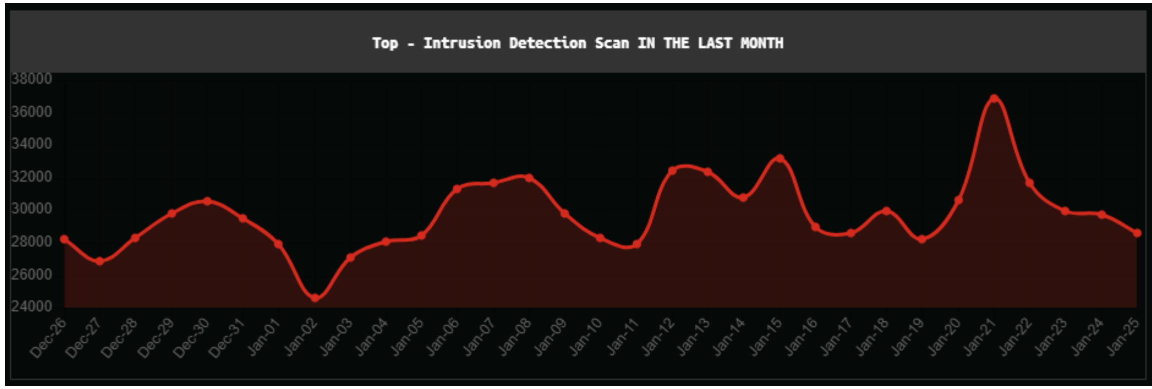
Top 10 Ransomware

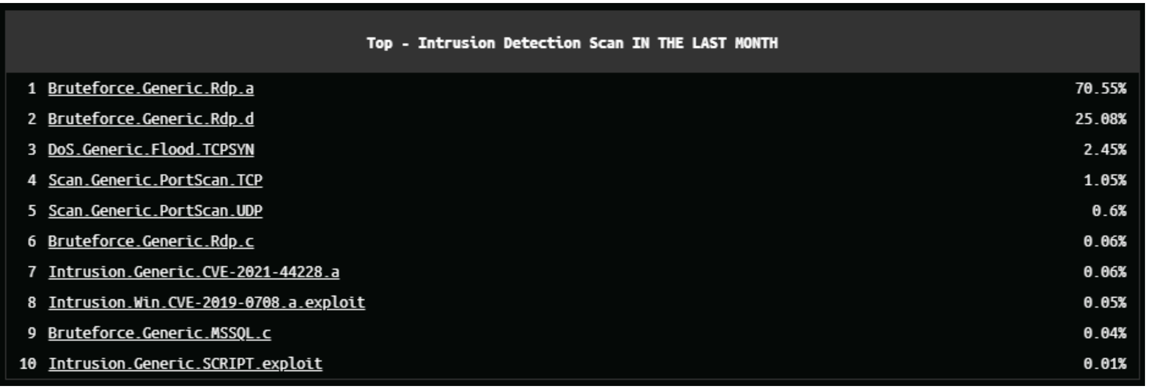

Top - Ransomware IN THE LAST MONTH


Top - Ransomware IN THE LAST MONTH

1	Trojan-Ransom.Win32.Encoder.gen	54.91%
2	Trojan-Ransom.Win32.Encoder	12.96%
3	Trojan-Ransom.Win32.Blocker.pef	7.54%
4	Trojan-Ransom.Win32.FakeInstaller.alva	1.61%
5	Trojan-Ransom.AndroidOS.Congur.cw	1.37%
6	Trojan-Ransom.Win32.Foreign.pef	1.37%
7	Trojan-Ransom.AndroidOS.Svpeng.ac	1.08%
8	trojan-ransom.win32.Crypren.gen	1.07%
9	Trojan-Ransom.Win32.Blocker.gen	1.02%
10	Trojan-Ransom.AndroidOS.Small.cj	1.02%

Top 10 Network Attacks according to Intrusion Detection


Top - Intrusion Detection Scan IN THE LAST MONTH

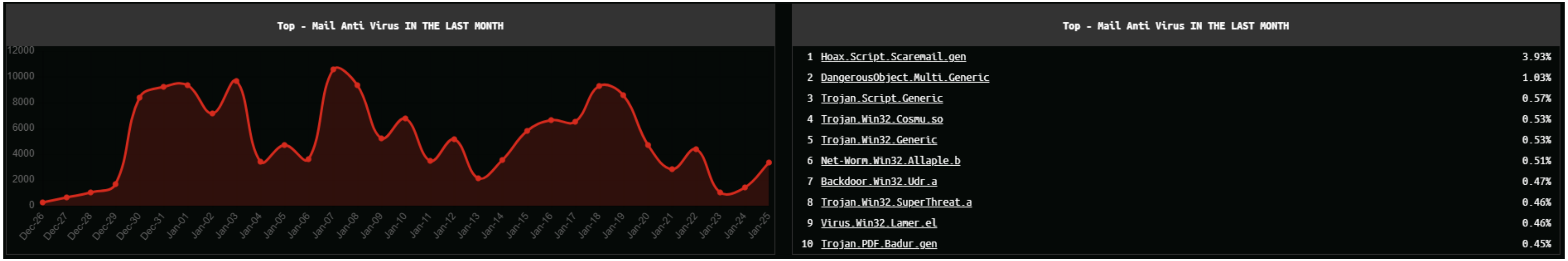

Top - Intrusion Detection Scan IN THE LAST MONTH

1	Bruteforce.Generic.Rdp.a	70.55%
2	Bruteforce.Generic.Rdp.d	25.08%
3	DoS.Generic.Flood.TCPSYN	2.45%
4	Scan.Generic.PortScan.TCP	1.05%
5	Scan.Generic.PortScan.UDP	0.6%
6	Bruteforce.Generic.Rdp.c	0.06%
7	Intrusion.Generic.CVE-2021-44228.a	0.06%
8	Intrusion.Win.CVE-2019-0708.a.exploit	0.05%
9	Bruteforce.Generic.MSSQL.c	0.04%
10	Intrusion.Generic.SCRIPT.exploit	0.01%

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

Monthly Top 10 in Switzerland 2/2

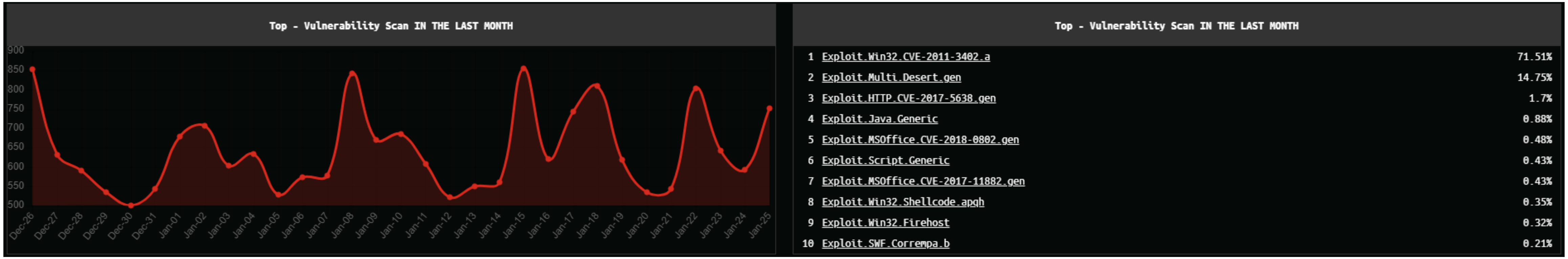
Top 10 Infected E-mails



Top - Mail Anti Virus IN THE LAST MONTH

1	Hoax.Script.Scaremail.gen	3.93%
2	DangerousObject.Multi.Generic	1.03%
3	Trojan.Script.Generic	0.57%
4	Trojan.Win32.Cosmu.so	0.53%
5	Trojan.Win32.Generic	0.53%
6	Net-Worm.Win32.Allaple.b	0.51%
7	Backdoor.Win32.Udr.a	0.47%
8	Trojan.Win32.SuperThreat.a	0.46%
9	Virus.Win32.Lamer.el	0.46%
10	Trojan.PDF.Badur.gen	0.45%

Top 10 Vulnerabilities



Top - Vulnerability Scan IN THE LAST MONTH

1	Exploit.Win32.CVE-2011-3402.a	71.51%
2	Exploit.Multi.Desert.gen	14.75%
3	Exploit.HTTP.CVE-2017-5638.gen	1.7%
4	Exploit.Java.Generic	0.88%
5	Exploit.MSOffice.CVE-2018-0802.gen	0.48%
6	Exploit.Script.Generic	0.43%
7	Exploit.MSOffice.CVE-2017-11882.gen	0.43%
8	Exploit.Win32.Shellcode.apgh	0.35%
9	Exploit.Win32.Firehost	0.32%
10	Exploit.SWF.Corrempa.b	0.21%

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

AVENIQ

Your contact person

Cen Magjuni
Senior Consultant Business Resilience

T +41 58 411 79 11
E cen.magjuni@aveniq.ch