AVENIQ

Cyber Threat Landscape

January 2023

Michael Malsch | Senior Consultant Cyber Security

Cen Magjuni | Senior Consultant Business Resilience

aveniq.ch

Table of contents

Summary of the month 1/2

Summary		Link
PayPal	At the end of December 2022, the payment platform PayPal discovered a hacker attack and reported it to the US Attorney's Office. Almost 35,000 customers are said to have been affected by the data leak. The timely investigation revealed that the hacker attack had already taken place between December 6 and 8. Cybercriminals were able to gain access to names, addresses, social security numbers, tax identification numbers and dates of birth, according to PayPal. Currently, the company is informing affected customers and has reset their passwords. Even though the company claims that there has been no misuse of the data so far, the customers have suffered damage. Once data has been published on the Internet, it can be misused at any time. Anyone who uses payment services automatically handles their data on the Internet. This incident should also be a warning to other companies that protect valuable data or even money only with passwords. Because, if PayPal now improves its security measures, the hackers will try the already stolen passwords on other websites. Therefore, the essential question to all other companies arises: Are you prepared for this?	https://www.datensicherheit.de/paypal-vorfall-warnung-cybersecurity-welt
T-Mobile	The U.S. subsidiary of German Telekom has again fallen victim to a hacker attack. According to initial findings, however, no highly sensitive customer data was captured, the company said. Hackers have gained access to data on around 37 million customers of Telekom subsidiary T-Mobile US. The company made the announcement Thursday after the U.S. stock market closed. The cyber attack was detected on Jan. 5. According to the company, no highly sensitive customer data was affected. According to preliminary findings, phone numbers, birth information and billing addresses may have been captured, but no passwords, credit card or Social Security numbers, it said. Based on the investigation so far, customer accounts and financial data were not directly at risk, T-Mobile said. Nevertheless, the U.S. mobile carrier, which is part of the Bonn-based Deutsche Telekom Group, did not rule out the possibility that the incident, which began on or around Nov. 25, could result in high costs. With the help of external experts, the source of the attack was found and it was stopped within a day of it becoming known in January. Investigations are still ongoing, but there are currently no indications that criminals have managed to penetrate the system or network.	https://www.watson.ch/digital/usa/663384950-cyber-angriff-auf-t-mobile-rund-37-millionen-user-betroffen

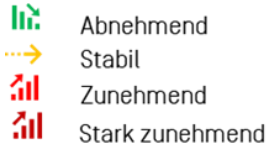
Summary of the month 2/2

Summary		Recommndation	Link
Microsoft	Microsoft has advised its customers to install the latest January 2023 security updates on on-premise Exchange servers. The company is urging IT administrators to patch their Exchange servers to protect their organization from cyberattacks and security threats. Microsoft warns that malicious actors are increasingly exploiting vulnerabilities to compromise unpatched Exchange servers in on-premises environments. This allows attackers to take complete control of unpatched Exchange instances and steal sensitive information. They could also access the address book to launch social engineering attacks.	• IT administrators are advised to run the Exchange Server Health Checker tool to find potential configuration issues that could affect performance. It identifies unpatched Exchange servers and provides instructions on manual actions to take to update the environment. • Administrators can use the Setup Assist script to troubleshoot issues that may arise during the installation process. The Exchange team has also published a troubleshooting guide to help IT administrators resolve common issues they may encounter when installing Exchange Server cumulative and security updates. • Deploy the latest updates to Windows Server and other dependent servers, including DNS and Active Directory.	https://petri.com/microsoft-patch-exchange-servers/
	The National Cyber Security Center (NCSC) is receiving more reports of CEO fraud attacks against companies. The attackers usually obtain information about the victims from publicly available sources in order to elicit the CEOs and financial officers from companies and organizations. By means of an email with a forged sender to the chief financial officer or treasurer of an association, the latter is instructed by the supposed CEO to trigger a payment in an allegedly urgent and confidential matter. In the cases currently reported, the attackers have come up with an additional trick, according to information from the NCSC: they call the person responsible for finance directly and introduce themselves as an alleged employee - "Maître Muller" - of a well-known auditing firm.	• Do not give out any information in case of unusual contact. • If in doubt, ask your supervisors whether the payment should be made. • Make your employees, especially those in the finance department, aware of this fraud scam. • Use a four-eyes principle with collective signature for bank transfers. • Introduce internal control mechanisms: In the case of unusual transfer orders, always have someone check whether the sender address of the e-mail is correct and whether the request for payment originates from the named ordering party.	https://www.computerworld.ch/security/hacking/welle-ceo-betrug-in-westschweiz-2831383.html

Observed Trends in December 2022 (worldwide)

Type of Threats December 2022	Trends compared to	
	November 2022	December 2021
Malware		
Intrusion		
Ransomware		
Phishing		
Web App Attack		
Cryptojacking		
IoT Malware		

Cyber Threat Index	
Critical 850 – 1000 Attacks	
High 700 – 850 Attacks	
Medium 550 – 700 Attacks	← **665 Attacks worldwide** (-1% compared to last Month)
Low 350 – 550	
Lowest 0 – 550 Attacks	



Sources:
https://securitycenter.sonicwall.com/m/page/capture-labs-threat-metrics
https://www.fireeye.com/cyber-map/threat-map.html
https://www.imperva.com/cyber-threat-index/

Topic of the Month

PayPal incident as a warning for the cybersecurity world – 25.01.2023

https://www.datensicherheit.de/paypal-vorfall-warnung-cybersecurity-welt

At the end of December 2022, the payment platform PayPal discovered a hacker attack and reported it to the US Attorney's Office. Almost 35,000 customers are said to have been affected by the data leak. The timely investigation revealed that the hacker attack had already taken place between December 6 and 8. Cybercriminals were able to gain access to names, addresses, social security numbers, tax identification numbers and dates of birth, according to PayPal. Currently, the company is informing affected customers and has reset their passwords. Even though the company claims that there has been no misuse of the data so far, the customers have suffered damage. Once data has been published on the Internet, it can be misused at any time. Anyone who uses payment services automatically handles their data on the Internet.

Attackers had tested numerous access data in a so-called credential stuffing attack and were successful in almost 35,000 cases. Credential stuffing is one of the most common cyber attack methods. Previously leaked or illegally obtained credentials are used to try them out en masse for unauthorized access at other services. The attackers assume that users use their login credentials with the same usernames and passwords at multiple services at the same time. According to PayPal's ad, the criminals gained access to customers' names, addresses, social security numbers, tax identification numbers and dates of birth. A notification has since been sent to those affected. PayPal says it has no information so far that there has been any misuse of the data or unauthorized transactions. The danger is now great that there will be fraud attempts with the help of SMS, e-mail or malware. Since there has been major data theft from social media accounts such as Facebook, there is a growing risk that criminals will link personal data. In the worst case scenario, they could ultimately take over consumers' identities and conduct business in the name of the victim. Exploiting a data leak is at the same time a loss of control over one's own data, some of which is sensitive. If the data is hacked, it is always available for criminals to use. The danger lies in the future.

This incident should also be a warning for other companies that protect valuable data or even money only with passwords. Because, if PayPal now improves its security measures, the hackers will try the already stolen passwords on other websites. Therefore, the essential question to all other companies arises: Are you prepared for this?

Cyber Attacks of the Month 1/2

Cyber criminals steal customer data from online pharmacy DocMorris – 27.01.2023

https://www.inside-it.ch/cyberkriminelle-erbeuten-kundendaten-der-online-apotheke-docmorris-20230127

The Dutch online pharmacy DocMorris was the victim of a cyber attack in mid-January. The pharmacy mainly supplies people in Germany. Unknown cybercriminals changed the addresses and customer accounts and ordered medicines in their names. About 20,000 accounts are said to be affected. The affected accounts have been blocked as a precaution and customers have been informed via letters and emails, the company said. Multiple passwords were to blame, it said. "In the attack, computer programs were used to randomly attempt to log into DocMorris customer accounts using credentials captured elsewhere. The attackers take advantage of the fact that access data for online services is unfortunately often used more than once by users. Apparently, this was also the case with your customer account," says the online pharmacy.

The parent company Zur Rose was already the victim of a cyberattack a year ago. On January 18, 2022, customer data of the online store for cosmetics and body care products "zurrose-shop.ch" was allegedly offered on the net. The data allegedly stolen included names, addresses, e-mail addresses and telephone numbers, as well as passwords.

Cyber attack on T-Mobile - around 37 million users affected - 20.01.2023

https://www.watson.ch/digital/usa/663384950-cyber-angriff-auf-t-mobile-rund-37-millionen-user-betroffen

The U.S. subsidiary of German Telekom has again fallen victim to a hacker attack. According to initial findings, however, no highly sensitive customer data was captured, the company said. Hackers have gained access to data on around 37 million customers of Telekom subsidiary T-Mobile US. The company made the announcement Thursday after the U.S. stock market closed. The cyber attack was detected on Jan. 5. According to the company, no highly sensitive customer data was affected. According to preliminary findings, phone numbers, birth information and billing addresses may have been captured, but no passwords, credit card or Social Security numbers, it said. Based on the investigation so far, customer accounts and financial data were not directly at risk, T-Mobile said. Nevertheless, the U.S. mobile carrier, which is part of the Bonn-based Deutsche Telekom Group, did not rule out the possibility that the incident, which began on or around Nov. 25, could result in high costs. With the help of external experts, the source of the attack was found and it was stopped within a day of it becoming known in January. Investigations are still ongoing, but there are currently no indications that criminals have managed to penetrate the system or network.

Cyber Attacks of the Month 2/2

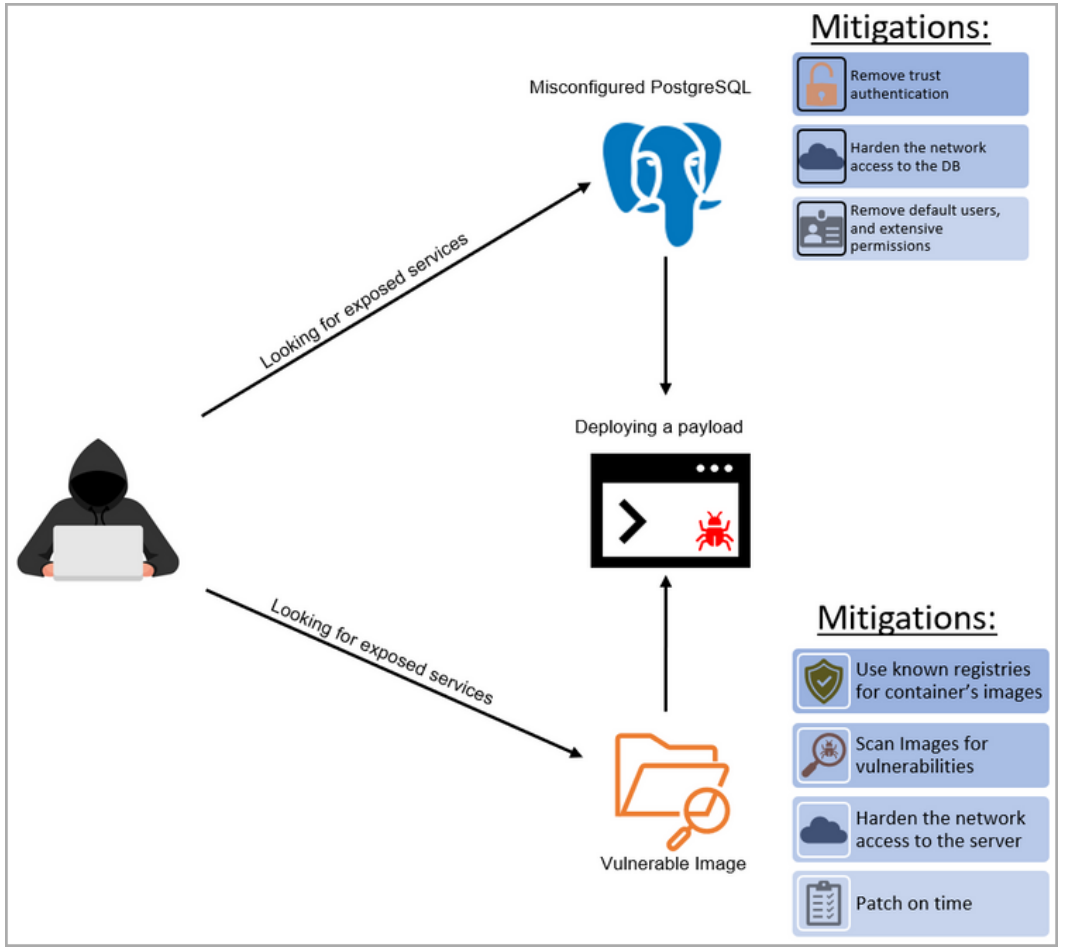
Microsoft: Kubernetes Clusters Hacked in Malware Campaign via PostgreSQL – 11.01.2023

https://linuxsecurity.com/news/cloud-security/microsoft-kubernetes-clusters-hacked-in-malware-campaign-via-postgresql

The Kinsing malware is now actively breaching Kubernetes clusters by leveraging known weaknesses in container images and misconfigured, exposed PostgreSQL containers. While these tactics aren't novel, Microsoft's Defender for Cloud team reports they have seen an uptick lately, indicating that the threat actors are actively looking for specific entry points.

Kinsing is a Linux malware with a history of targeting containerized environments for crypto mining, using the breached server's hardware resources to generate revenue for the threat actors. The threat actors behind Kinsing are known for exploiting known vulnerabilities like Log4Shell, and, more recently, an Atlassian Confluence RCE to breach targets and establish persistence. When exploiting image vulnerabilities, the threat actors hunt for remote code execution flaws that enable them to push their payloads. The second initial attack pathway that Microsoft's security experts observed was an uptick in the targeting of misconfigured PostgreSQL servers. One of the most common misconfigurations the attackers leverage is the 'trust authentication' setting, which instructs PostgreSQL to assume that "anyone who can connect to the server is authorized to access the database."

Mitigating this problem is as simple as using the latest available versions of the images you wish to deploy and only sourcing these images from official repositories and trustworthy locations. Microsoft also suggests minimizing access to exposed containers by using IP allow lists and following least privilege principles.



The two attack methods of Kinsing *(Microsoft)*

Vulnerabilities of the Month 1/3

VMware Confirms Exploit Code Released for Critical vRealize Logging Vulnerabilities – 31.01.2023

https://www.securityweek.com/vmware-confirms-exploit-code-released-for-critical-vrealize-logging-vulnerabilities/

VMware confirmed the publication of exploit code in an update to its VMSA-2023-0001 bulletin and called on customers using its VMware vRealize Log Insight product to implement mitigations as a matter of urgency. The vulnerabilities, tracked as CVE-2022-31706, CVE-2022-31704 and CVE-2022-31710, are rated critical with CVSS severity scores of 9.8 out of 10. The security defects affect users of its VMware vRealize Log Insight and could be exploited by an unauthenticated attacker to take full control of a target system. VMware described the flaws as directory traversal and broken access control issues with dangerous implications and warned that "an unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution." The bulletin update follows the publication of a technical deep-dive by automated penetration testing firm Horizon3.ai that included demo exploit code. The company also released IOCs (indicators of compromise) to help defenders hunt for signs of compromise. VMware's VRealize Log Insight is a log collection and analytics virtual appliance used by administrators to collect, view, manage and analyze syslog data.

Lexmark printers enable code smuggling – 30.01.2023

https://www.netzwoche.ch/news/2023-01-30/lexmark-drucker-ermoeglichen-codeschmuggel

The American printer manufacturer Lexmark warns about a critical security vulnerability in its devices. The vulnerability allows attackers to inject and execute their own code. This vulnerability (CVE-2023-23560) only affects "newer" printers. Lexmark lists about a hundred models that are affected by the vulnerability. A patched firmware version is already available for all of them. Affected are printers with a firmware version below XXXX.081.233, patched are the firmware versions XXXX.081.234 and up.

While this critical vulnerability only affects the "newer" Lexmark devices, the manufacturer warns of a second vulnerability (CVE-2023-22960), which also affects older devices. However, this vulnerability is described as only moderately severe. The devices have a protection mechanism that temporarily locks an account if too many log-in attempts fail. Malicious users could bypass this protection and thus launch a brute-force attack on credentials. Again, a patched firmware version is already available. Firmware versions as of XXXX.081.233 contain the fix for this vulnerability. However, owners of a "newer" Lexmark, such as the Lexmark CX944, should make sure that they have also installed the second firmware update to be protected against both vulnerabilities.

Vulnerabilities of the Month 2/3

Microsoft urges admins to patch on-premises Exchange servers – 27.01.2023

https://petri.com/microsoft-patch-exchange-servers/

Microsoft has recommended customers to deploy the latest January 2023 security updates on on-premises Exchange servers. The company urges IT admins to keep their Exchange servers patched to protect their organization from cyberattacks and security threats. Microsoft raised an alarm that malicious actors are increasingly leveraging vulnerabilities to compromise unpatched Exchange servers in on-premises environments. It enables attackers to take complete control over unpatched Exchange instances and steal sensitive information. Moreover, they could access the address book to launch social engineering attacks.
Recommendations:

- IT admins are advised to run the Exchange Server Health Checker tool to find potential configuration issues that could impact the performance. It identifies unpatched Exchange servers and provides instructions about manual actions that need to be performed for updating the environment.
- Administrators can use the SetupAssist script to fix any problems that might occur during the installation process. The Exchange team also published a troubleshooting guide to help IT admins address common problems that could occur during the installation of Exchange server cumulative and security updates.
- Deploy the latest updates for Windows Server and other dependent servers, including DNS and Active Directory.

Thousands of Sophos Firewall devices at risk of RCE attacks – 17.01.2023

https://www.scmagazine.com/brief/device-security/thousands-of-sophos-firewall-devices-at-risk-of-rce-attacks

More than 4,000 internet-connected Sophos Firewall devices continue to have the critical remote code execution flaw, tracked as CVE-2022-3236, unpatched despite the release of hotfixes last September and the issuance of official patches in December. Over 99% of more than 88,000 internet-facing Sophos Firewalls have not been updated to versions with the official fix. While a proof-of-concept exploit for the vulnerability is yet to be released, threat actors could potentially reproduce the exploit based on available technical data, as done by Baines, to conduct a new wave of attacks, which Baines noted could be hindered by required CAPTCHAs during authentication.

Vulnerabilities of the Month 3/3

Cisco warns of security vulnerabilities it will not patch – 13.01.2023

https://www.infosecurity-magazine.com/news/cisco-vulnerability-in-end-of-life/

In a warning about critical vulnerabilities in several routers from Cisco, the manufacturer writes that it "has not released or will not release updates" - although proof-of-concept code for one of the vulnerabilities is already available. Cisco gives two reasons for this. The four small business router models RV016, RV042, RV042G and RV082 are affected. Incorrect validation of user input in incoming HTTP packets allows attackers to bypass authentication on the devices (CVE-2023-20025). Neither vulnerability can be exploited unless attackers can access the management interface. A patch would not be made available because the routers have already reached their end of life (EOL)

Recommendation:

- Cisco refers to the workaround of blocking both ports 443 and 60443

UEFI vulnerabilities threaten ARM devices like Microsoft Surface – 10.01.2023

https://www.heise.de/news/UEFI-Sicherheitsluecken-bedrohen-ARM-Geraete-wie-Microsoft-Surface-7454141.html

Attackers could bypass the Secure Boot protection mechanism on Lenovo ThinkPads and Microsoft Surface. Security researchers from Binarly have discovered several vulnerabilities in the reference code of UEFI firmware from Qualcomm and Lenovo for ARM-based computers. Since many PC manufacturers use the code, supply chain attacks are conceivable. Lenovo has already reacted and released security updates. If attackers successfully exploit three vulnerabilities (CVE-2022-40516 "high", CVE-2022-40517 "high", CVE-2022-40520 "high"), they could trigger memory errors due to insufficient input checks, according to the researchers. Subsequently, it should be possible to disable Secure Boot. In a warning message, Lenovo states that it has closed the gaps in firmware 1.47. Qualcomm lists the gaps in a post. It is not yet known if and when the other affected manufacturers will provide security updates.

Tactics, Techniques & Procedures 1/3

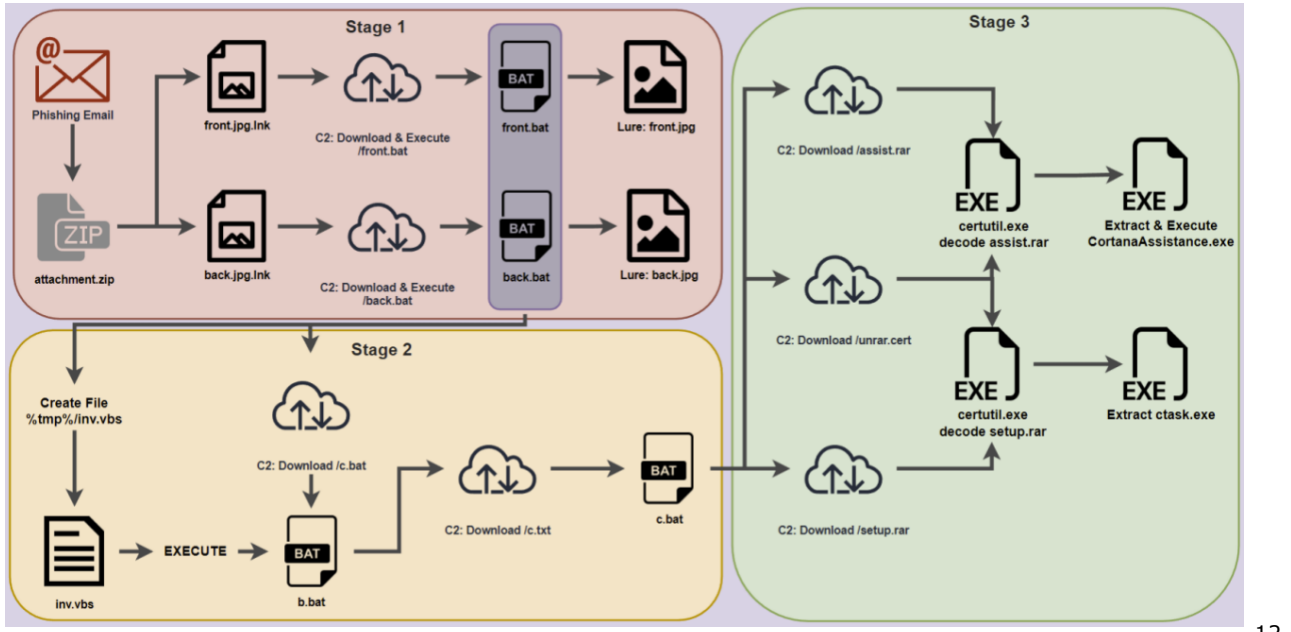
New stealthy Python RAT malware targets Windows in attacks – 27.01.2023

https://www.bleepingcomputer.com/news/security/new-stealthy-python-rat-malware-targets-windows-in-attacks/

A new Python-based malware has been spotted in the wild featuring remote access trojan (RAT) capabilities to give its operators control over the breached systems. Named PY#RATION by researchers, the new RAT uses the WebSocket protocol to communicate with the command and control (C2) server and to exfiltrate data from the victim host. RAT is actively developed with multiple versions of it since August when the PY#RATION campaign started.The PY#RATION malware is distributed via a phishing campaign that uses password-protected ZIP file attachments containing two shortcut .LNK files disguised as images, namely front.jpg.lnk and back.jpg.lnk. When launched, the shortcuts victim sees the front an back of a driver's license. However, malicious code is also executed to contact the C2 (Pastebin in later attacks) and download two .TXT files ('front.txt' and 'back.txt') which are eventually renamed to BAT files to accommodate the malware execution. Upon launch, the malware creates the 'Cortana' and 'Cortana/Setup' directories in the user's temporary directory and then downloads, unpacks, and runs additional executable files from that location. Persistence is established by adding a batch file ('CortanaAssist.bat') into the user's startup directory. The use of Cortana, Microsoft's personal assistant solution on Windows, aims at disguising the malware entries as system files.

features seen in version 1.6.0 of the PY#RATION RAT are the following:

- Perform network enumeration
- Perform file transfers from the breached system to the C2
- Perform keylogging to record the victim's keystrokes
- Execute shell commands
- Perform host enumeration
- Extract passwords and cookies from web browsers
- Steal data from the clipboard
- Detect anti-virus tools running on the host



The campaign's complete infection chain (Securonix)

Tactics, Techniques & Procedures 2/3

NCSC warns: criminals increasingly scam with QR codes – 25.01.2023

NCSC warnt: Kriminelle betrügen vermehrt mit QR-Codes (inside-it.ch)

The National Cyber Security Center (NCSC) warns of increased abuses using QR codes. Typically, fraudsters search hacked email accounts for sent invoices and payment instructions. If they find what they are looking for, they copy and manipulate the invoice: the IBAN number is changed and the victim is sent the invoice again in the name of the actual invoicing party. The recipient's account "has changed" and the recipient should "now pay into the new account". Now the cybercriminals are resorting to a new scam: in a recently reported case, not only was the IBAN swapped, but the QR code was also adjusted accordingly. Furthermore, the victim was supposed to deposit the amount into a Swiss account. Recommendation:

- Make employees aware and do not follow up on unusual requests for payment.
- Employees within the company should verify the accuracy of such invoices by consulting them by telephone.

Wave of CEO fraud in western Switzerland – 18.01.2023

https://www.computerworld.ch/security/hacking/welle-ceo-betrug-in-westschweiz-2831383.html

The National Cyber Security Center (NCSC) is receiving more reports of CEO fraud attacks against companies. The attackers usually obtain information about the victims from publicly available sources in order to elicit the CEOs and financial officers from companies and organizations. By means of an email with a forged sender to the chief financial officer or treasurer of an association, the latter is instructed by the supposed CEO to trigger a payment in an allegedly urgent and confidential matter. In the cases currently reported, the attackers have come up with an additional ruse, according to information from the NCSC: they call the financial officer directly and introduce themselves as an alleged employee - "Maître Muller" - of a well-known auditing firm. Recommendations:

- Do not give out any information in case of unusual contact.
- If in doubt, ask your superiors whether the payment should be made.
- Check what information about your own company is available online.
- Make your employees, especially those in the finance department, aware of this scam.
- Use a four-eyes principle with collective signature for bank transfers.
- Introduce internal control mechanisms: In the case of unusual transfer orders, always have someone check whether the sender address of the e-mail is correct and whether the request for payment originates from the named ordering party.

Tactics, Techniques & Procedures 3/3

AL2023_04 New malware targets Linux machines and installs cryptocurrency miners and IRC bots – 12.01.2023

https://cirt.gy/Malware-targets-Linux-machines-and-installs-cryptocurrency-miners-and-IRC-bots

A new Shell Script Compiler (SHC) malware has been spotted targeting Linux machines, infecting these systems with cryptocurrency miners and adding them to an IRC botnet. The SHC malware is a generic shell script compiler that is responsible for converting Bash shell scripts into ELF (executable and linkable format) files for Linux machines. Bash is a basic shell in Linux operating systems, and commands supported by Bash can be compiled in script format. This allows threat actors to convert malicious bash shell scripts into executable ELF files. This method of converting the bash to ELF files after infiltrating a device is a way of avoiding file detection. The malicious scripts in SHC ELF executables are also encoded using the RC4 algorithm and this also helps in evading detection as well. When the SHC malware is executed, it fetches multiple malware payloads. The first and main payload downloaded is the XMRig cryptocurrency miner. It is downloaded as a TAR archive from a remote URL, extracted to '/usr/local/games/' and executed. The XMRig miner is an open-source, cross platform GPU/CPU cryptocurrency miner designed for mining cryptocurrencies such as Monero or Bitcoin. In this case, XMRig is set to mine Monero currency using the compromised server's available computational resources. Recommendation:

- administrators should use passwords that are difficult to guess for their accounts and change them periodically to protect the Linux server from brute force attacks and dictionary attacks and update to the latest patch to prevent vulnerability attacks.
- Administrators should also use security programs such as firewalls for servers accessible from outside to restrict access by attackers.

Microsoft: Cuba ransomware hacking Exchange servers via OWASSRF flaw – 14.01.2023

https://www.cybersecurity-insiders.com/cuba-ransomware-gang-hacking-microsoft-exchange-servers/

Microsoft issued a press update that Cuba Ransomware gang were after its exchange servers after exploiting critical server-side request forgery (SSRF) vulnerability. Incidentally, the same flaw is also being exploited by 'Play' Ransomware group that hacked into the cloud servers of Rackspace via an OWASSRF exploit. Windows OS giant says that the threat actors were striking the servers after bypassing ProxyNotShell URL rewrite abilities. FBI issued an advisory in December last year stating that the Cuba gang is after US Critical infrastructure, as they have already targeted 49 organizations, including companies that are into generation and distribution of power and a water utility. As the impact was minimal, the activity went unnoticed by the media, but was notified to the Biden administration.

Argentina's Judiciary of Cordoba, Belgium City of Antwerp, Rackspace and the German H-Hotels are some of its targeted companies for now.

Good to Know 1/2

Cybercrime job ads on the dark web pay up to $20k per month – 30.01.2023

https://www.bleepingcomputer.com/news/security/cybercrime-job-ads-on-the-dark-web-pay-up-to-20k-per-month/

In a new report by Kaspersky, which analyzed 200,000 job ads posted on 155 dark websites between March 2020 and June 2022, hacking groups and APT groups seek to hire mainly software developers (61% of all ads), offering very competitive packages to entice them. The highest-paying job seen by Kaspersky's analysts included a monthly salary of $20,000, while ads for capable attack specialists topped at $15,000/per month. Hacking groups also seek to fill other roles, including data analysts, malware and tool developers, initial compromise actors, reverse engineers, website and phishing email designers, malware testers, and IT administrators. The median pay for IT pros ranged between $1,300 and $4,000 per month, with designers receiving the lower amounts and reverse engineers being positioned at the higher end of the median pay spectrum. In one-third of the job postings, the recruiters offered candidates full-time employment, and an equal percentage allowed a flexible schedule. In some cases (8%), the remote workers would be offered paid vacation and sick leave, which shows that some dark web employers care about making their proposals as attractive as possible.

As part of the hiring process, cybercriminal recruiters conduct test assignments created to determine an applicant's level of competency in the claimed field. In some cases, the recruiters also look into the provided CV or portfolio, and in one out of four postings, there's an interview session conducted with the job seeker. In characteristic examples spotted by Kaspersky, one job posting promised to pay candidates roughly $300 in BTC for a test assignment. Another job offer laid out a multi-step screening process where the candidate would be asked to encrypt a test DLL in 24 hours, making it fully undetectable by AVs (max of 3 minor AV runtime detects). As cybercrime enterprises adopt business-like operations, we will continue to see the dark web as a recruiting tool for threat actors looking for a stable income. Some software developers may see these opportunities as a lifeline during difficult times of political unrest, poor economies, or a lack of job opportunities in their region. However, it is vital to understand the potential risks of working for a dark web employer, ranging from being scammed to getting framed, arrested, prosecuted, and imprisoned.

Cyberattacks in Switzerland have more than doubled – 19.01.2023

https://www.inside-it.ch/cyberangriffe-in-der-schweiz-haben-sich-mehr-als-verdoppelt-20230109

Cybersecurity firm Check Point has released a new report on the number of cyberattacks last year. Globally, these have increased by 38%. Broken down by region, North America leads the way (up 52%), ahead of Latin America (up 29%) and Europe (up 26%). According to the survey, the increase in Switzerland is above the global average. Here, a 61% increase in cyberattacks on organizations was recorded compared to the previous year, it said. The NCSC had also recently published its figures for 2022: with a total of over 34,000 reports, there was no longer a doubling of the previous year's figure of 21,714 reports, but the increase in absolute terms was still greater than the year before, at 13,000 reports.

According to Check Point, the manufacturing industry is the most affected in Switzerland, with an average of 725 attacks per week. This is followed by the financial industry (623), government/military (529), healthcare (455) and the communications sector (397). Compared to the previous year, only the manufacturing industry recorded a decrease (minus 24%). The highest increases were in the financial industry and the communications sector, up 120% and 200%, respectively. With AI technologies such as ChatGPT, cybercriminals could generate malicious code and phishing emails even faster and more automatically in the future.

Good to Know 2/2

Product Security Incident Response: Key Strategies and Best Practices – 18.01.2023

https://www.bleepingcomputer.com/news/security/product-security-incident-response-key-strategies-and-best-practices/

In today's digital landscape, it is essential to implement proactive measures to ensure the security of your organization's products. But even with good practices in place, the dynamic nature of vulnerability identification, and ever-increasing attack tools and techniques, vulnerabilities can escape the best defenses and make their way into released products. As such, organizations should have a plan to identify and address vulnerabilities in their products. This is where the role of a Product Security Incident Response Team (PSIRT) comes into play. A PSIRT is responsible for identifying, assessing, and addressing vulnerabilities in a product or service. There are several key strategies and best practices to create an effective PSIRT. Recommendations:

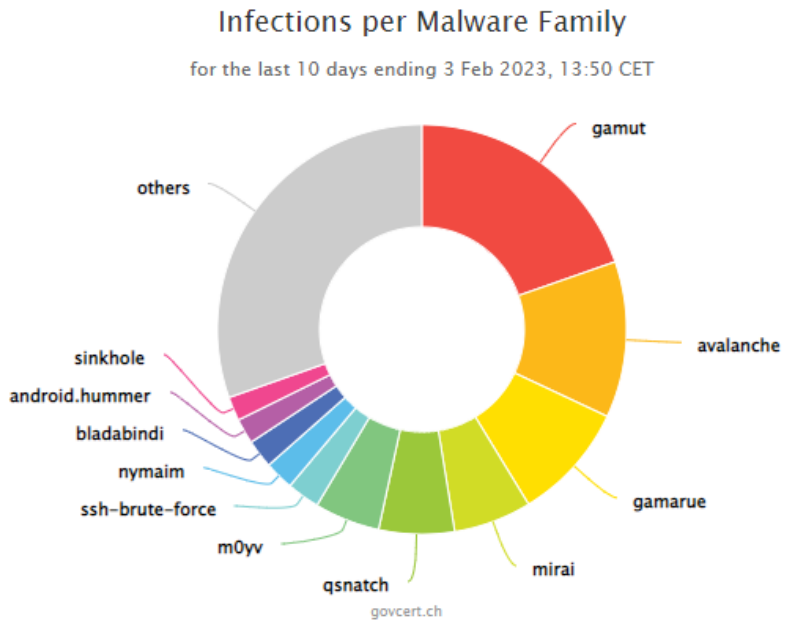
1. **Respond Proactively:** When a vulnerability is discovered, the clock is ticking. The PSIRT should initiate its response process quickly, including notifying internal and external stakeholders. The moment a vulnerability is shared with an organization is the moment responsibility and due diligence start being measured, as additional phases of the PSIRT begin. Formalize the response in a manner that is documented, logged, and preserves the chain of custody for all communications.
2. **Clearly State Your Embargo Policy:** Take a clear and transparent stance on defining your organization’s embargo policy. Embargo of a security issue means that the issue will not be publicly disclosed for some time by the vendor/discoverer while a fix is being generated. A best-practice embargo period is between one and ten weeks. The embargo should be defined depending on the severity of the vulnerability. Vulnerabilities should be classified into a tracking system with the identification of a severity score based on the Common Vulnerability Scoring System (CVSS) and handled in a confidential way during a defined and communicated embargo period. Your PSIRT should be prepared to communicate this information downstream to customers as soon as it is available via advisory publications.
3. **Partner with Researchers and Security Vendors:** Researchers and security tool vendors are vital partners in the fight to secure the supply chain. Cybersecurity researchers constantly search for vulnerabilities in software and hardware using the latest tools and technology and are key inputs into improving PSIRT, while security vendors make new tools for identifying vulnerabilities. The more inputs into your PSIRT identification process, the more access to knowledge, tools, and resources. Build collaborative relationships with researchers and security vendors to better integrate your vulnerability sighting and advisory notification process with them.
4. **Optimize Your Investigation and Remediation Process:** An effective investigation is important for ensuring that the PSIRT can identify affected code and that the risk posed can be communicated to customers in a timely manner. The steps of the investigation process should be formally documented, measured, and optimized for continuous improvement. A good PSIRT should have an array of tools, automation, and methods to determine the extent to which the vulnerable code may exist in all products. Verification of remediation is quintessential to ensure the risks have been appropriately addressed. A formalized “sign-off stage gate” is important to capture remediation's approval and internal certification. By ensuring that all patches or fixes have been properly implemented and applied, you can have confidence that your customers are protected from potential security threats.

By following these best practices, your organization's PSIRT can effectively identify and collaboratively address product vulnerabilities.

Appendencies

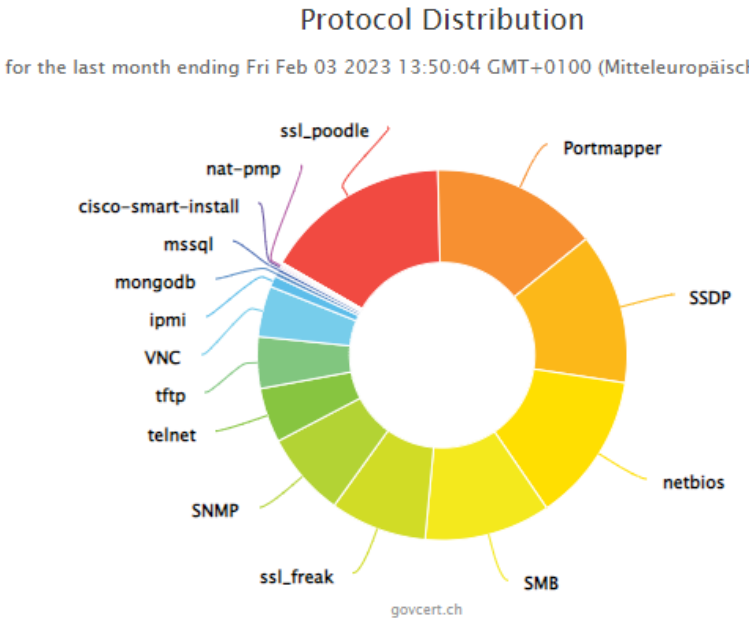
Malware & Vulnerable Systems - Switzerland

Malware Statistics



These statistics originate from a database containing infected systems in Switzerland that have been active the last 48h. This database is fed by different sources, mostly DNS sinkholes operated by different organizations, where infected clients connect to.

Vulnerable Systems

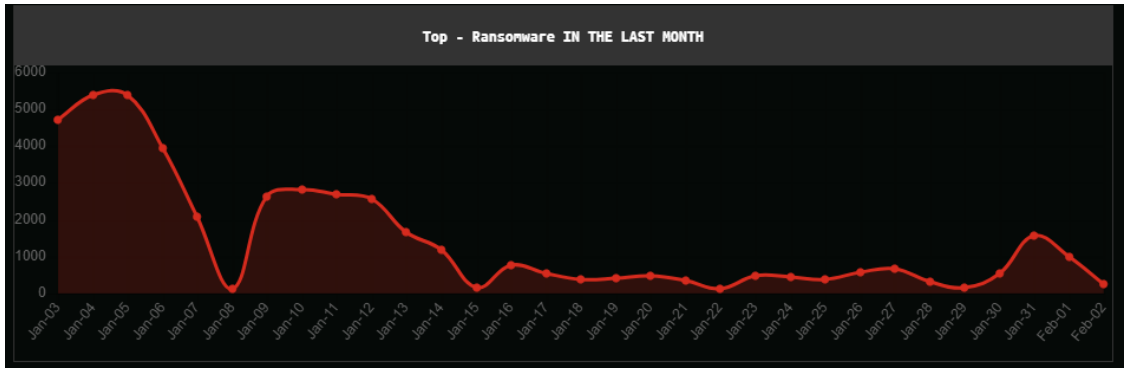


These statistics originate from a database containing systems in Switzerland that can be potentially abused for DDoS amplification and reflection attacks or are otherwise seriously vulnerable on the protocol level.

Source: https://www.govcert.ch/statistics/malware/

Monthly Top 10’s Switzerland 1/2

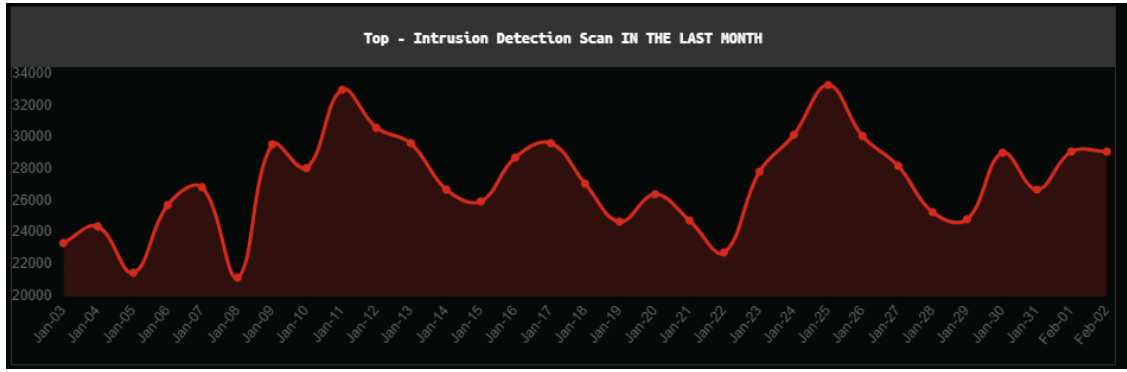
Top 10 Ransomware



Top - Ransomware IN THE LAST MONTH

1	trojan-ransom.win32.Crypren.gen	82.63%
2	Trojan-Ransom.Win32.Encoder	3.18%
3	Trojan-Ransom.Win32.Crypmodng.gen	2.4%
4	Trojan-Ransom.NSIS.Onion.lts	1.44%
5	Trojan-Ransom.Win32.Shade.xh	1.44%
6	Trojan-Ransom.Win32.Cryakl.aje	1.42%
7	Trojan-Ransom.NSIS.Onion.jfe	1.33%
8	Trojan-Ransom.Win64.Magni.gen	1.21%
9	Trojan-Ransom.Win32.Gimemo.pef	0.47%
10	Trojan-Ransom.Win32.PornoAsset.pef	0.19%

Top 10 Network attacks according to Intrusion Detection Scans



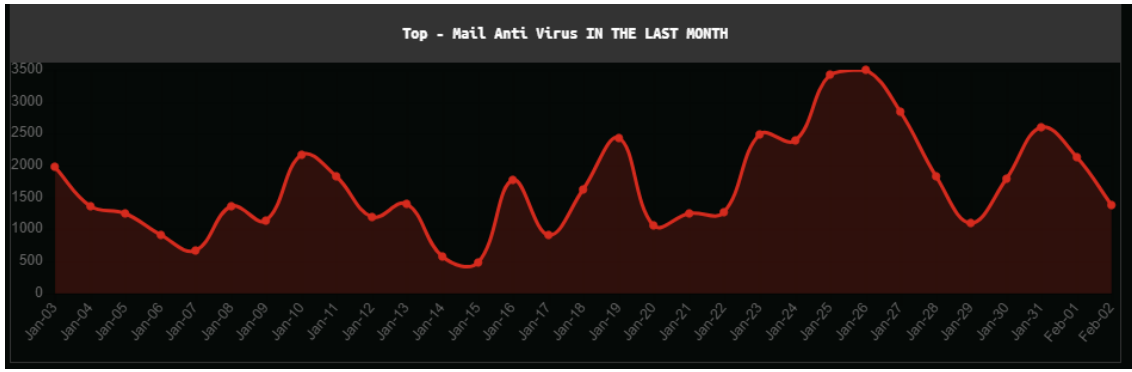
Top - Intrusion Detection Scan IN THE LAST MONTH

1	Bruteforce.Generic.Rdp.d	56.75%
2	Bruteforce.Generic.Rdp.a	31.56%
3	DoS.Generic.Flood.TCPSYN	5.99%
4	Bruteforce.Generic.Rdp.c	2.16%
5	Scan.Generic.PortScan.TCP	1.75%
6	Scan.Generic.PortScan.UDP	1.63%
7	Intrusion.Win.MS17-010.o	0.06%
8	Intrusion.Generic.CVE-2021-44228.a	0.04%
9	Intrusion.Win.CVE-2019-0708.b.exploit	0.02%
10	Intrusion.Generic.CVE-2021-44228.b	0.01%

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

Monthly Top 10’s Switzerland 2/2

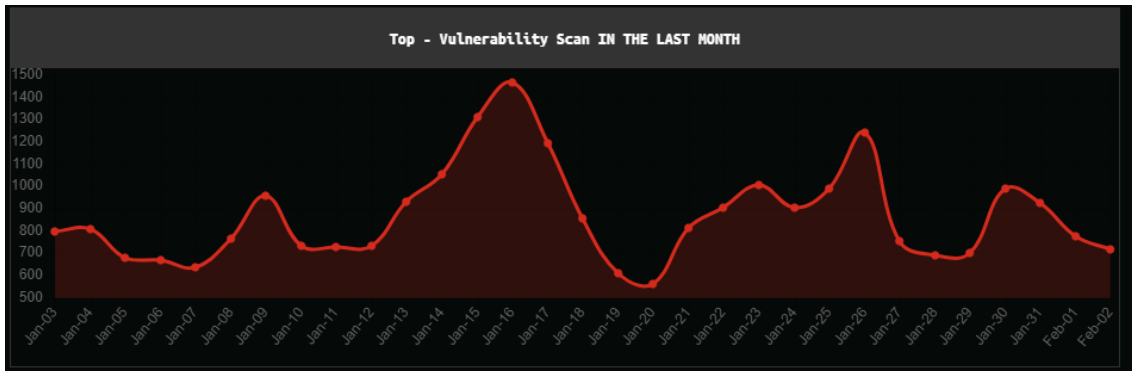
Top 10 Infected Mails



Top - Mail Anti Virus IN THE LAST MONTH

1	Hoax.Script.Scaremail.gen	15.73%
2	Trojan.Script.Generic	11.48%
3	Trojan.MSOffice.Emotet.gen	7.07%
4	DangerousObject.Multi.Generic	5.29%
5	Trojan.Win32.Badun.gen	4.78%
6	Trojan-Downloader.Script.Agent.gen	4.1%
7	Backdoor.Win32.Androm.gen	3.42%
8	Trojan.PDF.Badur.gen	3.18%
9	Virus.Win32.PolyRansom.b	2.93%
10	Hoax.HTML.Phish.gen	2.18%

Top 10 Vulnerabilities



Top - Vulnerability Scan IN THE LAST MONTH

1	Exploit.Win32.CVE-2010-2862.a	82.04%
2	Exploit.SWF.Agent.gen	5.08%
3	Exploit.Win32.MS05-036	4.96%
4	Exploit.Multi.Desert.gen	3.99%
5	Exploit.MSWord.Agent.gen	0.98%
6	Exploit.Win32.Generic.msf	0.56%
7	Exploit.HTTP.CVE-2017-5638.gen	0.3%
8	Exploit.MSOffice.CVE-2017-11882.gen	0.19%
9	Exploit.Java.Generic	0.16%
10	Exploit.Script.Blocker	0.16%

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

AVENIQ

Michael Malsch
Senior Consultant Cyber Security

T +41 58 059 41 80
E michael.malsch@aveniq.ch

Aveniq AG
Bruggerstrasse 68
CH-5401 Baden
T +41 58 411 77 77

Cen Magjuni
Senior Consultant Business Resilience

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

Aveniq AG
Bruggerstrasse 68
CH-5401 Baden
T +41 58 411 77 77