AVENIQ

Cyber Threat Landscape

Cen Magjuni Senior Consultant Business Resilience

Januar 2024

Agenda

1. Aktuelle weltweite Trends
2. Thema des Monats
3. Cyber Angriffe des Monats
4. Schwachstellen des Monats
5. Tactics, Techniques & Procedures
6. Gut zu wissen
7. Anhänge

Weltweite Trends im Dezember 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

Thema des Monats

Zusammenfassung		Link
01.02.2024	**Hacker verkaufen Daten von 900'000 Schweizer Hobbysportlern** Rund 1,3 Millionen Datensätze wurden kürzlich in einem Hacker-Forum als Datenpaket zum Kauf angeboten. Über 900’000 davon sollen Schweizerinnen und Schweizer betreffen, die bei der Firma Datasport erbeutet wurden. Die restlichen Daten betreffen das benachbarte Ausland und weitere Länder. Datasport erbringt Dienstleistungen wie Zeitmessung, Startnummernvergabe und Online-Anmeldung für Breitensportanlässe - vom Engadin-Skimarathon über zahlreiche Stadtläufe bis hin zu Radrennen. Auch Hobbysportlerinnen und -sportler können mit myDS ihre Leistungsdaten sammeln und nach Belieben veröffentlichen. Am 23. Januar meldete das Unternehmen selbst einen Cyberangriff auf seine Website. Laut CEO Thomas Bachofner hat Datasport im Rahmen der periodischen Überprüfung der technischen und organisatorischen Massnahmen zur Daten- und Informationssicherheit die Georedundanz erhöht und die Daten zu Backup-Zwecken in ein anderes Rechenzentrum ausgelagert. Im Zuge der Umsetzung muss in diesem Rechenzentrum kurz vor dem 23. Januar eine sicherheitsrelevante Schwachstelle bestanden haben. Nachdem diese entdeckt worden war, wurde sie von Datasport innert Minuten geschlossen. Der oder die Hacker müssen dieses kurze Zeitfenster ausgenutzt haben. Nach der Veröffentlichung der Lücke durch die Täter wurden die Daten laut Bachofner nochmals überprüft. Das Unternehmen geht davon aus, dass theoretisch bis zu 1 Million Datensätze betroffen sein könnten. Sicherheitsrelevante Informationen wie Passwörter oder Zahlungsmittel seien vom Leck aber nicht betroffen, betont der Datasport-CEO. Die potenziell betroffenen Informationen werden von den Nutzerinnen und Nutzern selbst auf Datasport.com aufgeschaltet und sind öffentlich einsehbar. Es handelt sich dabei um Daten wie Namen, Postadressen und Geburtsdaten, teilweise aber auch um E-Mail-Adressen und Telefonnummern von myDS-Benutzern. Dies bestätigen vom Hacker veröffentlichte Datensamples. Die im Datenpaket enthaltenen myID-Nummern werden von Datasport jedoch nur intern verwendet, um User-Dobletten zu vermeiden.	Link

Cyber Angriffe des Monats 1/2

Zusammenfassung		Link
30.01.2024	**Cactus hackt Schneider Electric** Am 17. Januar wurde der große französische Elektronikkonzern Schneider Electric von der Ransomware-Gang Cactus angegriffen. Betroffen war die Abteilung Sustainability Business, wodurch ein Teil der Cloud-Plattform gestört wurde und noch immer Ausfälle zu verzeichnen sind. Quellen zufolge wurden mehrere Terabyte an Unternehmensdaten von den Hackern erbeutet. Zu den Kunden der betroffenen Abteilung gehören unter anderem Allegiant Travel Company, Clorox, DHL, DuPont, Hilton, Lexmark, PepsiCo und Walmart. Die gestohlenen Daten könnten sensible Informationen über den Energieverbrauch der Kunden, industrielle Steuerungs- und Automatisierungssysteme und die Einhaltung von Umwelt- und Energievorschriften enthalten. Die Hacker drohen, die Daten zu veröffentlichen, wenn kein Lösegeld gezahlt wird. Schneider Electric erklärte, der Angriff beschränke sich auf die Abteilung Sustainability Business, andere Teile des Unternehmens seien nicht betroffen. Die Abteilung Sustainability Business führt derzeit Wiederherstellungsmaßnahmen und Funktionstests durch, so dass der Zugriff in wenigen Tagen wieder möglich sein sollte. Der Konzern hat eine Cybersicherheitsfirma beauftragt, den Vorfall den Behörden gemeldet und führt eine detaillierte forensische Analyse durch. Bereits im vergangenen Jahr hatte Schneider Electric Probleme mit Hackern. Über die weit verbreitete Moveit-Schwachstelle gelang es der Ransomware-Bande Clop, Daten des Unternehmens zu erbeuten.	Link
25.01.2024	**HPE meldet Cyberangriff auf das eigene E-Mail-System** HPE wurde von russischen Hackern infiltriert, die sich Zugang zum E-Mail-System verschafften. Das genaue Ausmaß ist noch unklar, die Cyberkriminellen waren etwa ein halbes Jahr unbemerkt im System aktiv. Details sind noch nicht geklärt, aber das Unternehmen geht davon aus, dass die russischen Angreifer Midnight Blizzard, auch bekannt als Cozy Bear, hinter dem Angriff stecken. Die Hacker sollen das E-Mail-System des Unternehmens infiltriert und sich vermutlich bereits im Mai 2023 Zugang zur E-Mail-Umgebung von HPE verschafft haben. Bemerkt wurde der erfolgreiche Angriff erst im Dezember vergangenen Jahres. Nach Angaben von HPE konnten die Kriminellen auf die Postfächer einiger Nutzer zugreifen, unter anderem aus den Bereichen Go-to-Market und Cybersicherheit, genauere Zahlen und Inhalte stehen jedoch noch aus. Es wird untersucht, wie der Angriff durchgeführt wurde. HPE teilt mit, dass der Vorfall keine Auswirkungen auf die Finanzergebnisse von HPE hatte.	Link

Cyber Angriffe des Monats 2/2

Zusammenfassung		Link
19.01.2024	**Cyberangriff auf die kantonale Website des Kantons Basel-Stadt** Seit dem 19.01.2023 ist die kantonale Website von Basel-Stadt (www.bs.ch) das Ziel eines Cyberangriffs. Zeitweise war die Seite nicht erreichbar. Die kantonalen IT-Fachleute haben Gegenmassnahmen ergriffen, um den Betrieb wieder störungsfrei sicherzustellen. Der DDos-Angriff, bei dem mit einer Vielzahl von gezielten Anfragen eine Dienstblockade herbeigeführt wird, begann etwa um 06.30 Uhr. Seit 09.00 Uhr ist die Website wieder erreichbar. Nach wie vor ist aber mit Beeinträchtigungen zu rechnen. Die Cyberkriminellen sind nicht bekannt.	Link
18.01.2024	**Schweizer Mobilfunk-Zulieferer Nexus Telecom gehackt** Die Ransomware-Gang 8Base soll von Nexus Telecom eine große Menge vertraulicher Informationen erbeutet haben. Das Opfer liefert Netzwerküberwachungssoftware an Provider weltweit. Die Kriminellen drohen mit der Veröffentlichung der gestohlenen Daten auf ihrer Erpressungs- und Leaksite im Darknet. Die gestohlenen Daten und das Schadensausmass sind noch Gegenstand von Abklärungen. Zu den Kunden von Nexus Telecom gehören unter anderem große europäische Provider wie British Telecommunications (BT) und die Deutsche Telekom, aber auch weitere in Übersee. Bei 8Base handelt es sich um eine Ransomware-Gruppe, die seit März 2022 aktiv ist, aber erst im Sommer 2023 in die Schlagzeilen geriet, als sie mit ihren Aktivitäten nur knapp hinter der berüchtigten Lockbit-Bande lag. Wie andere bekannte Ransomware-Gruppen betreibt 8Base eine Website im Darknet. Dort sind Hunderte von gehackten Unternehmen aufgelistet - allesamt Opfer, die sich geweigert haben, Lösegeld zu zahlen, damit ihre gestohlenen Daten nicht veröffentlicht werden. Die Cyberkriminellen gelten als opportunistisch in der Wahl ihrer Opfer und Angriffswerkzeuge: Ende letzten Jahres stellten IT-Sicherheitsforscher fest, dass bei den Hackerangriffen auf 8Bbase eine Variante der Ransomware Phobos eingesetzt wurde. Phobos steht Cyberkriminellen als Ransomware as a Service (RaaS) zur Verfügung. Die US-amerikanische Cybersicherheitsbehörde HC3 stellte im vergangenen November zu 8Base fest, dass trotz des aggressiven Portfolios an Opfern die Ursprünge der Gruppe und die Identitäten der Betreiber ein Geheimnis bleiben. Cybersicherheitsforscher gehen davon aus, dass die Geschwindigkeit und Effizienz der aktuellen Operationen nicht auf den Beginn einer neuen Gruppe hindeuten, sondern eher auf die Fortsetzung einer etablierten und erfahrenen Organisation.	Link

Schwachstellen des Monats 1/2

Zusammenfassung		Empfehlungen	Link
31.01.2024	**Mehrere Schwachstellen in Ivanti-Produkten könnten eine Remote Code-Ausführung ermöglichen** Mehrere Sicherheitslücken wurden in Ivanti-Produkten entdeckt, von denen die schwerwiegendste die Remotecodeausführung ermöglichen könnte: Ivanti Connect Secure, Ivanti Policy Secure (IPS) und Ivanti Neurons for Zero Trust Access (nZTA). Eine erfolgreiche Ausnutzung könnte Remotecodeausführung im Kontext des Systems ermöglichen. Abhängig von den Rechten des angemeldeten Benutzers könnte ein Angreifer dann Programme installieren, Daten anzeigen, ändern oder löschen. Benutzer, deren Konten so konfiguriert sind, dass sie weniger Rechte auf dem System haben, könnten weniger betroffen sein als Benutzer, die mit administrativen Benutzerrechten arbeiten. Laut Ivanti gibt es Berichte über die gezielte Ausnutzung von CVE-2024-21893. Ivanti, CISA und andere Quellen haben über die weit verbreitete Ausnutzung von CVE-2024-21887 und CVE-2023-46805 berichtet.	• Wenden Sie die von Ivanti bereitgestellten Updates auf anfällige Systeme an, nachdem Sie sie getestet haben. • Einrichtung und Aufrechterhaltung eines Schwachstellenmanagementprozesses: Einführung und Pflege eines dokumentierten Schwachstellen-Management-Prozesses für Unternehmensressourcen. Überprüfen und aktualisieren Sie die Dokumentation jährlich oder wenn wesentliche Änderungen im Unternehmen eintreten, die sich auf diese Schutzmaßnahme auswirken könnten. • Führen Sie vierteljährlich oder in kürzeren Abständen automatisierte Schwachstellen-Scans der internen Unternehmensressourcen durch. • Aufbau und Pflege einer sicheren Netzwerkarchitektur. Eine sichere Netzwerkarchitektur muss mindestens Segmentierung, geringste Rechte und Verfügbarkeit berücksichtigen.	Link
23.01.2024	**Mehrere Schwachstellen in Apple-Produkten könnten eine willkürliche Code-Ausführung ermöglichen** In Apple-Produkten wurden mehrere Sicherheitsanfälligkeiten entdeckt, von denen die schwerwiegendste die Ausführung von beliebigem Code ermöglichen könnte. Eine erfolgreiche Ausnutzung der schwerwiegendsten dieser Sicherheitsanfälligkeiten könnte die Ausführung von beliebigem Code im Kontext des angemeldeten Benutzers ermöglichen. Abhängig von den Rechten des Benutzers könnte ein Angreifer dann Programme installieren, Daten anzeigen, ändern oder löschen oder neue Konten mit vollen Benutzerrechten erstellen. Benutzer, deren Konten so konfiguriert sind, dass sie weniger Rechte auf dem System haben, könnten weniger betroffen sein als Benutzer, die mit administrativen Benutzerrechten arbeiten.	• Einrichtung und Aufrechterhaltung eines Schwachstellen-Management-Prozesses • Durchführen von Penetrationstests für Anwendungen. Bei kritischen Anwendungen sind authentifizierte Penetrationstests besser geeignet, um Schwachstellen in der Geschäftslogik aufzuspüren als Code-Scans und automatisierte Sicherheitstests • Wenden Sie das Prinzip der geringsten Privilegien auf alle Systeme und Dienste an. Führen Sie alle Software als nicht privilegierter Benutzer (ohne administrative Rechte) aus, um die Auswirkungen eines erfolgreichen Angriffs zu verringern.	Link

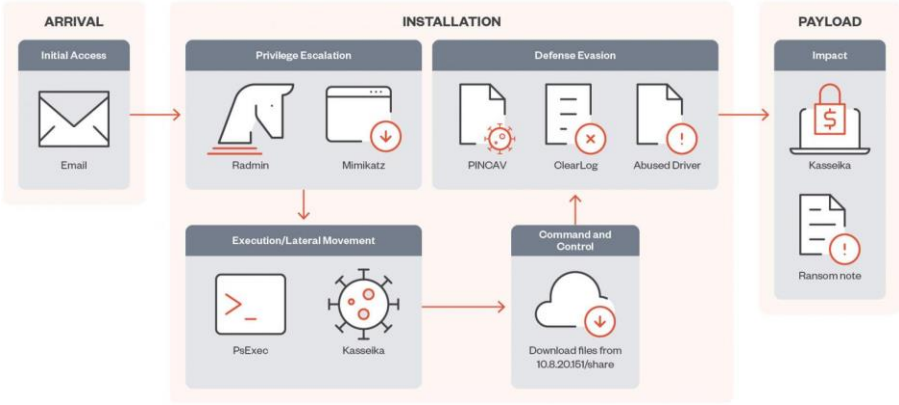
Schwachstellen des Monats 2/2

Zusammenfassung		Empfehlungen	Link
17.01.2024	**Neue Zero-Days in Citrix NetScaler ADC, Gateway unter Beschuss** Die Zero-Day-Lücken CVE-2023-6549 und CVE-2023-6548 wurden am Dienstag bekannt gegeben und gepatcht. CVE-2023-6549 ist eine hochgradige Denial-of-Service-Schwachstelle mit einem CVSS-Wert von 8,2, während CVE-2023-6548 eine mittelschwere Schwachstelle mit einem CVSS-Wert von 5,5 ist, die einem authentifizierten Angreifer die Remoteausführung von Code auf Managementschnittstellen ermöglicht.	• Sofortige Updates für alle betroffenen Versionen • Netzwerkverkehr zur Management-Schnittstelle des Geräts physisch oder logisch vom normalen Netzwerkverkehr trennen • Wenden Sie das Prinzip der geringsten Privilegien auf alle Systeme und Dienste an. Führen Sie alle Software als nicht privilegierter Benutzer (ohne administrative Rechte) aus, um die Auswirkungen eines erfolgreichen Angriffs zu verringern.	Link
17.01.2024	**Eine Schwachstelle in Atlassian Confluence Data Center und Server könnte eine Remote-Code-Ausführung ermöglichen** In Atlassian Confluence Server und Data Center wurde eine Sicherheitslücke entdeckt, die die Ausführung von Remotecode ermöglichen könnte. Eine erfolgreiche Ausnutzung dieser Schwachstelle könnte es einem Angreifer ermöglichen, nicht autorisierte Confluence-Administratorkonten zu erstellen, um auf die Instanz zuzugreifen. Ein Angreifer könnte dann Administrator-Aktionen im Kontext der Confluence-Instanz durchführen. Derzeit gibt es keine Berichte darüber, dass diese Sicherheitslücke ausgenutzt wird.	• Wenden Sie die von Atlassian bereitgestellten Patches und Umgehungslösungen auf anfällige Systeme an, und zwar unmittelbar nach entsprechenden Tests. • Architektur von Netzabschnitten zur Isolierung kritischer Systeme, Funktionen oder Ressourcen. Nutzen Sie die physische und logische Segmentierung, um den Zugriff auf potenziell sensible Systeme und Informationen zu verhindern. Verwenden Sie eine DMZ, um alle dem Internet zugewandten Dienste einzuschließen, die nicht vom internen Netzwerk aus zugänglich sein sollen. Konfigurieren Sie separate Virtual Private Cloud (VPC)-Instanzen, um kritische Cloud-Systeme zu isolieren.	Link
11.01.2024	**Schwachstelle in Cisco Unity Connection könnte eine willkürliche Code-Ausführung ermöglichen** In Cisco Unity Connection wurde eine Sicherheitslücke entdeckt, die die Ausführung von beliebigem Code auf einem Zielhost ermöglichen könnte. Ein erfolgreicher Angriff könnte es einem nicht authentifizierten, entfernten Angreifer ermöglichen, beliebige Dateien auf ein betroffenes System hochzuladen und Befehle auf dem zugrunde liegenden Betriebssystem auszuführen. Derzeit gibt es keine Berichte darüber, dass diese Sicherheitslücke ausgenutzt wird.	• Wenden Sie die von Cisco bereitgestellten Patches auf anfällige Systeme an, nachdem Sie sie getestet haben. • Entfernen Sie unnötige und potenziell anfällige Software oder verweigern Sie den Zugriff darauf, um einen Missbrauch durch Angreifer zu verhindern. • Blockieren der Ausführung von Code auf einem System durch Anwendungskontrolle und/oder Skriptblockierung.	Link

Tactics, Techniques & Procedures 1/2

Zusammenfassung		Link
31.01.2024	**DarkGate-Malware über Microsoft Teams ausgeliefert** Der Kunde hat einen verdächtigen Screenshot einer Phishing-Mail zur Verfügung gestellt. Die darin verwendete Domain “onmicrosoft.com” scheint auf den ersten Blick authentisch zu sein. Das MDR SOC-Team vermutet jedoch, dass der Benutzername und möglicherweise die gesamte Domain von den Angreifern kompromittiert wurden. In der Kundenumgebung wurden mehr als 1.000 “MessageSent”-Ereignisse gefunden, die vom Benutzer generiert wurden. Obwohl die Empfänger-IDs nicht enthalten waren, enthielten sie die Tenant-ID des externen Benutzers. Diese Information ermöglichte es dem Team, “MemberAdded”-Ereignisse zu identifizieren, die auftreten, wenn ein Benutzer einem Team-Chat beitritt1. Die Microsoft 365 Tenant-ID ist eine weltweit eindeutige Kennung, die Organisationen zugewiesen wird. Sie ermöglicht es Mitgliedern verschiedener Organisationen, über Teams zu kommunizieren. Solange beide Chat-Teilnehmer gültige Tenant-IDs haben und der externe Zugriff aktiviert ist, können sie Nachrichten austauschen. Das MDR SOC Team konnte Ereignisse abfragen, die die Tenant-ID des externen Benutzers enthielten und mehrere "MemberAdded"-Ereignisse identifizieren. Diese Ereignisse treten auf, wenn ein Benutzer einem Chat in Teams beitritt. In diesem Fall konnten sie die Ereignisse über das Feld "ChatThreadId" positiv mit dem Angreifer verknüpfen. Der Kunde erhielt eine Liste der Benutzer, die den externen Chat akzeptiert hatten, und konnte potenziell kompromittierte Ressourcen und Konten identifizieren, um das Problem zu beheben. Bei der weiteren Untersuchung entdeckte das MDR SOC-Team drei Benutzer, die eine verdächtige Datei mit einer doppelten Erweiterung heruntergeladen hatten. Die Datei hieß "Navigating Future Changes October 2023.pdf.msi". Dateien mit doppelter Erweiterung werden häufig von Angreifern verwendet, um Benutzer zum Herunterladen bösartiger ausführbarer Dateien zu verleiten. Die zweite Erweiterung, in diesem Fall .msi, wird normalerweise vom Dateisystem verborgen. Der Benutzer glaubt, eine PDF-Datei für geschäftliche Zwecke herunterzuladen, erhält aber stattdessen ein bösartiges Installationsprogramm. Das MDR SOC-Team war in der Lage, den Dateinamen und die zugehörigen Hashes an den Kunden weiterzugeben, der diese Informationen wiederum an seinen EDR-Anbieter (Endpoint Detection and Response) weiterleitete, damit die Datei der Blockliste hinzugefügt werden konnte. Die Informationen zu den Dateidownloads ermöglichten es dem Kunden auch, die betroffenen Ressourcen zu identifizieren, um sie zu isolieren und zu bereinigen.	Link

Tactics, Techniques & Procedures 2/2

Zusammenfassung		Link
23.01.2024	**Kasseika-Ransomware nutzt Antivirentreiber, um andere Antivirenprogramme zu töten** Die Ransomware-Operation "Kasseika" nutzt die Taktik "Bring Your Own Vulnerable Driver" (BYOVD), um Antivirensoftware zu deaktivieren, bevor sie Dateien verschlüsselt. Dabei missbraucht Kasseika den Martini-Treiber (Martini.sys/viragt64.sys), der Teil des VirtIT Agent Systems von TG Soft ist. Die Ransomware zeigt Ähnlichkeiten im Quellcode mit BlackMatter, obwohl dieser seit seiner Abschaltung Ende 2021 nicht öffentlich durchgesickert ist. Kasseika-Angriffe beginnen mit einer Phishing-E-Mail, um Anmeldeinformationen von Mitarbeitern zu stehlen und Zugriff auf das Unternehmensnetzwerk zu erhalten. Anschließend verwenden die Angreifer das Windows PsExec-Tool, um bösartige .bat-Dateien auszuführen und den anfälligen 'Martini.sys'-Treiber herunterzuladen.  Die Ransomware “Kasseika” nutzt die Taktik “Bring Your Own Vulnerable Driver” (BYOVD), um Antivirensoftware zu deaktivieren, bevor sie Dateien verschlüsselt. Dabei missbraucht Kasseika den Martini-Treiber (Martini.sys/viragt64.sys), der Teil des VirtIT Agent Systems von TG Soft ist. Die Ransomware zeigt Ähnlichkeiten im Quellcode mit BlackMatter, obwohl dieser seit seiner Abschaltung Ende 2021 nicht öffentlich durchgesickert ist. Kasseika-Angriffe beginnen mit einer Phishing-E-Mail, um Anmeldeinformationen von Mitarbeitern zu stehlen und Zugriff auf das Unternehmensnetzwerk zu erhalten. Anschließend verwenden die Angreifer das Windows PsExec-Tool, um bösartige .bat-Dateien auszuführen und den anfälligen ‘Martini.sys’-Treiber herunterzuladen. Die Ransomware verschlüsselt Zieldateien mithilfe der Algorithmen ChaCha20 und RSA, fügt den Dateinamen eine pseudozufällige Zeichenfolge hinzu und hinterlässt in jedem verschlüsselten Verzeichnis eine Lösegeldnotiz. Um die Sicherheitsanalyse zu erschweren, löscht Kasseika nach der Verschlüsselung die Systemereignisprotokolle und verwendet Befehle wie ‘wevutil.exe’. Opfer hatten bei den von Trend Micro beobachteten Angriffen 72 Stunden Zeit, um 50 Bitcoins (2.000.000 US-Dollar) zu hinterlegen, wobei alle 24 Stunden Verzögerung zusätzlich 500.000 US-Dollar hinzugefügt wurden.	Link

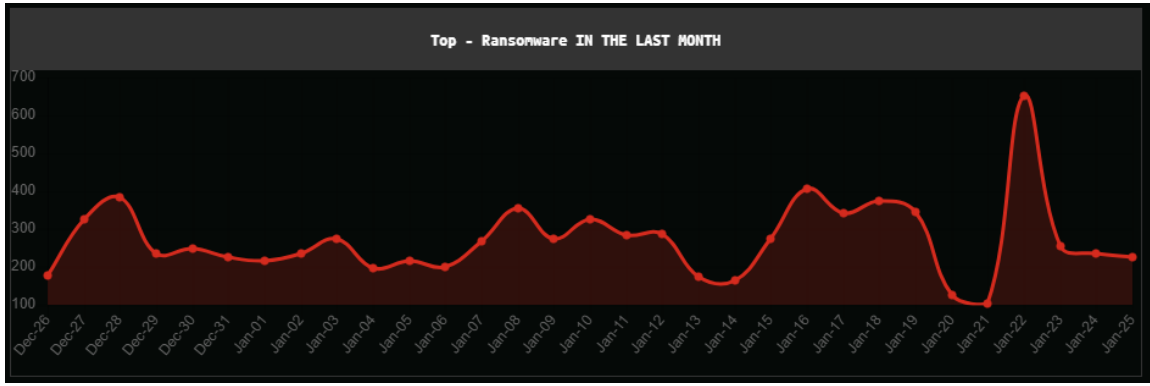
Gut zu wissen

Zusammenfassung		Link
26.01.2024	**Microsoft erklärt, wie russische Hacker seine Führungskräfte ausspioniert haben** Die Ransomware-Operation “Kasseika” nutzt die Taktik “Bring Your Own Vulnerable Driver” (BYOVD), um Antiviren-Software zu deaktivieren, bevor Dateien verschlüsselt werden. Dabei missbraucht Kasseika den Martini-Treiber (Martini.sys/viragt64.sys), der Teil des VirtIT Agent Systems von TG Soft ist. Die Ransomware weist Ähnlichkeiten mit dem Quellcode von BlackMatter auf, obwohl dieser seit seiner Abschaltung Ende 2021 nicht mehr öffentlich geleakt wurde. Kasseika-Angriffe beginnen mit einer Phishing-E-Mail, die darauf abzielt, Anmeldeinformationen von Mitarbeitenden zu stehlen und Zugang zum Unternehmensnetzwerk zu erhalten. Anschließend nutzen die Angreifer das Windows PsExec-Tool, um schädliche .bat-Dateien auszuführen und den anfälligen Treiber ‘Martini.sys’ herunterzuladen. Die Ransomware verschlüsselt die Zieldateien mit den Algorithmen ChaCha20 und RSA, fügt den Dateinamen eine pseudozufällige Zeichenfolge hinzu und hinterlässt in jedem verschlüsselten Verzeichnis eine Lösegeldnachricht. Um eine Sicherheitsanalyse zu erschweren, löscht Kasseika nach der Verschlüsselung die Systemereignisprotokolle und verwendet Befehle wie ‘wevutil.exe’. Bei den von Trend Micro beobachteten Angriffen hatten die Opfer 72 Stunden Zeit, um 50 Bitcoins (2.000.000 US-Dollar) einzuzahlen, wobei alle 24 Stunden weitere 500.000 US-Dollar hinzukamen. Dieser erweiterte Zugang ermöglichte es der Gruppe, weitere bösartige OAuth-Anwendungen und Konten zu erstellen, um Zugang zur Microsoft-Unternehmensumgebung und damit zum Office 365 Exchange Online-Dienst zu erhalten, der den Zugriff auf E-Mail-Postfächer ermöglicht.	Link
26.01.2024	**Digitale Anzeigeerstattung von Cyberdelikten auf Suisse ePolice** Auf der Plattform Suisse ePolice (www.suisse-epolice.ch) können Cyberdelikte rund um die Uhr online angezeigt werden. In 12 Kantonen ist dies bereits möglich, weitere Kantone werden in den nächsten Monaten folgen. Die eingegebenen Strafanzeigen werden direkt an die zuständige Polizeidienststelle weitergeleitet. Bei rund 50 Prozent der Cybercrime-Delikte kann auf den Gang zum Polizeiposten verzichtet werden. Die Nutzung der Plattform ist barrierefrei und kostenlos. Der Dienst ist bereits in folgenden Kantonen verfügbar: AI, AR, BE, FR, GL, GR, LU, NE, SG, SZ, ZG, ZH.	Link

Anhänge

Monatliche Top 10 der Schweiz 1/2

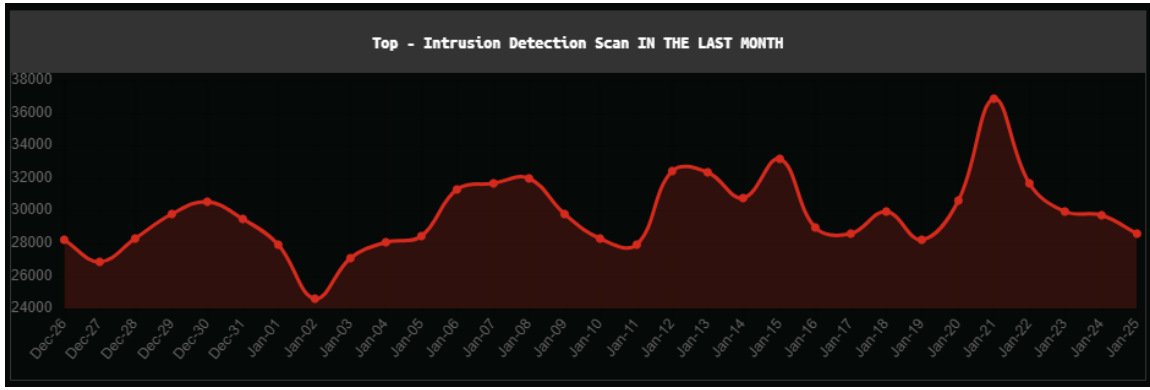
Top 10 Ransomware (Aufkommen/Ranking)



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 Netzwerkangriffe gem. Intrusion Detection (Aufkommen/Ranking)



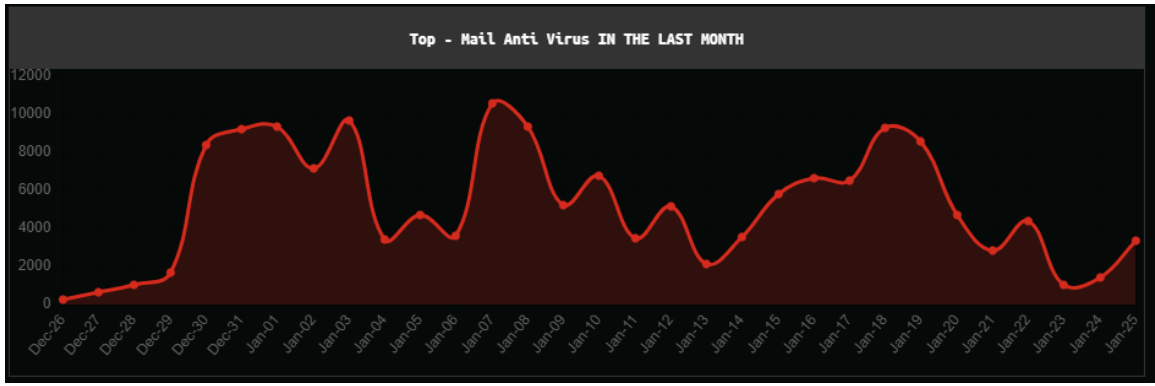
Top - Intrusion Detection Scan IN THE LAST MONTH

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%

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

Monatliche Top 10 der Schweiz 2/2

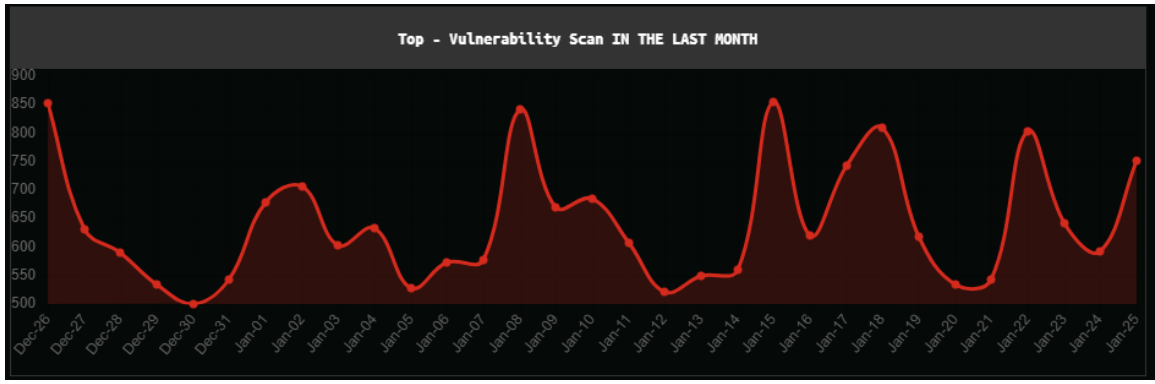
Top 10 Infizierte Mails (Aufkommen/Ranking)



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 Schwachstellen (Aufkommen/Ranking)



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.apqh	0.35%
9	Exploit.Win32.Firehost	0.32%
10	Exploit.SWF.Corrempa.b	0.21%

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

AVENIQ

Ihr Ansprechpartner

Cen Magjuni
Senior Consultant Business Resilience

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