32GUARDS RESEARCH NOTE #1-2023

Was wir aus dem Spam- und Malware-Jahr 2022 lernen können

Das 32Guards-Research-Team von Net at Work zieht in dieser Research Note ein Resümee mit Erkenntnissen aus der Abwehr von Spam und Malware im Jahr 2022 und legt dabei einen besonderen Fokus auf den E-Mail-Verkehr im deutschsprachigen Raum. Die Einschätzungen und konkreten Empfehlungen sind für alle E-Mail-Administratoren und andere Verantwortliche für IT-Sicherheit von hohem Wert – unabhängig davon, welche Produkte für Mail Security sie einsetzen.

Tschüss Heimdall, hallo 32Guards.

Was vor einigen Jahren als Projekt Heimdall begann, ist nun vollends ausgereift und tritt unter dem Produktnamen 32Guards ins Rampenlicht. Von der Version 14 an gehört 32Guards zum Standardproduktumfang der Mail Security Suite NoSpamProxy sowohl in der On-Premises-Version als auch im Cloud Service.

Doch als Erinnerung: Was genau ist 32Guards und wie funktioniert es? Alle teilnehmenden Instanzen der NoSpamProxy-Suite für E-Mail-Sicherheit – das sind mehrere Tausend bei Unternehmen, Verwaltungen und anderen Organisationen in Deutschland, Österreich und der Schweiz (DACH-Region) – teilen ihre Beobachtungen via 32Guards untereinander. So profitieren alle angeschlossenen Nutzer nahezu in Echtzeit von Erkenntnissen über erkannte Bedrohungen und Anomalien. Zudem ist so eine mächtige Datenbasis zur mittel- und langfristigen Analyse und Auswertung von Angriffsformen und -mustern entstanden. Regelmäßig werden vollständig anonym und im Einklang mit der EU-DSGVO die Metadaten von vielen Millionen Mails, Links und Anhängen gesammelt und nach Abweichungen, Trends und Mustern ausgewertet.

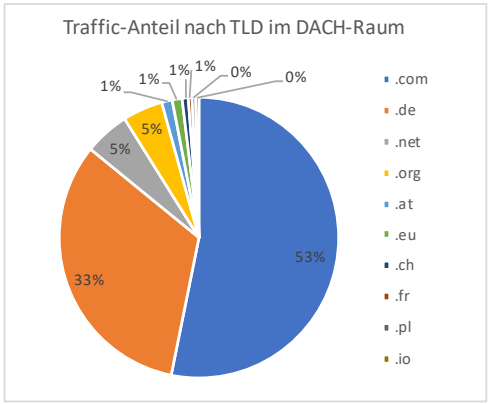
Um insbesondere auch lokale Trends und Muster gezielt finden zu können, steht dabei bewusst der geschäftliche E-Mail-Traffic im DACH-Raum im Fokus. Damit unterscheidet sich 32Guards deutlich von anderen Analyseansätzen, bei denen lokale Trends im geschäftlichen E-Mail-Verkehr im deutschsprachigen Raum oft in einer Flut privater E-Mail-Nutzer oder im Grundrauschen vieler internationaler Business-Nutzer untergehen.

Neue Erkenntnisse fließen automatisiert in Echtzeit in den Schutz der an 32Guards angeschlossenen Kunden ein, werden aber auch der Allgemeinheit in Form von Alerts und Research Notes bereitgestellt.

Aus welchen Top Level Domains kommt der Traffic in der DACH-Region?

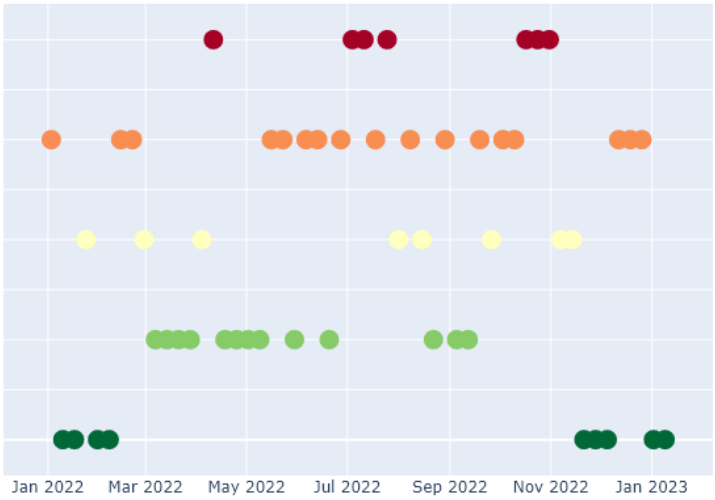
Nicht überraschend kommt der überwiegende Anteil des Traffics von den beiden TLDs *.com* und *.de*, die zusammen mehr als 85% des Traffics ausmachen. Der Traffic aus den großen direkten Nachbarstaaten wie Frankreich und Polen ist marginal. Da viele Unternehmen *.com*-Domains nutzen, unterliegt diese Betrachtung jedoch einer gewissen Unschärfe.

Traffic-Anteil	
TLD	2023
.com	53,2%
.de	32,7%
.net	5,2%
.org	4,6%
.at	1,2%
.eu	1,1%
.ch	0,7%
.fr	0,4%
.pl	0,4%
.io	0,4%



Das Malware-Aufkommen schwankte auch 2022 im Jahresverlauf deutlich

Im Jahresverlauf schwankt das Aufkommen an E-Mails und auch das Auftreten von Malware ganz erheblich. In der Grafik sehen wir den Zeitverlauf über das Jahr mit je einem Punkt pro Woche. Die horizontale Achse in der Mitte stellt einen normalen Gefährdungslevel dar. Die in Rottönen dargestellten Punkte oberhalb repräsentieren Wochen mit besonders hohem Gefährdungspotential, die grün dargestellten Punkte unterhalb Wochen mit besonders geringer Gefahrenlage.

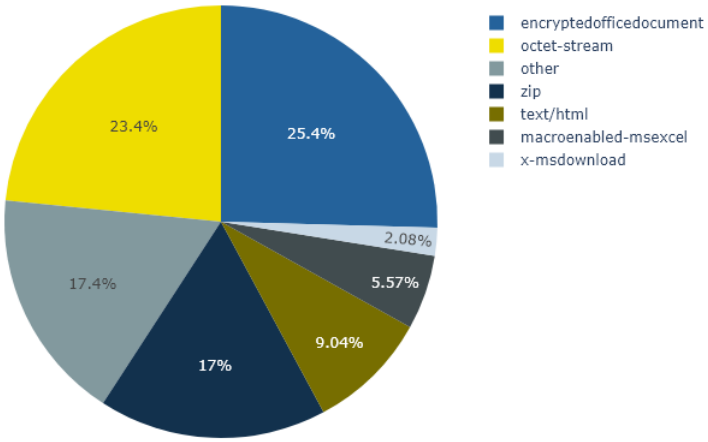


Im Jahr 2022 hatten wir zwei signifikante Spitzen mit besonders hohem Spam-Aufkommen Anfang Juli und Ende Oktober mit einem besonders hohen Anteil an bösartigen E-Mails. Besonders ruhig war es dagegen – wie auch in den Vorjahren – insbesondere in den ersten beiden Januarwochen. Eine Erklärung dafür bieten die diversen Feiertage. Interessant ist jedoch, dass Spammer und Angreifer versuchen, den Jahresendstress und den Shopping-Hype vor Weihnachten noch einmal gezielt mit diversen Kampagnen auszunutzen.

Empfehlung: Verfestigen sich diese zeitlichen Spitzen, kann es Sinn machen, in den erwarteten Hochphasen für Malware besonders strikte Policies scharf zu schalten und beispielsweise Anhangstypen mit höherem Risikopotential abzulehnen oder durch Content Disarming zu entschärfen. Auch sollten im Vorfeld regelmäßiger Peaks gezielt die Awareness-Trainings für Mitarbeitende verstärkt werden. Die Verwendung schnell adaptiv reagierender Services wie 32Guards hilft dabei – insbesondere bei unregelmäßigen und spontanen Wellen.

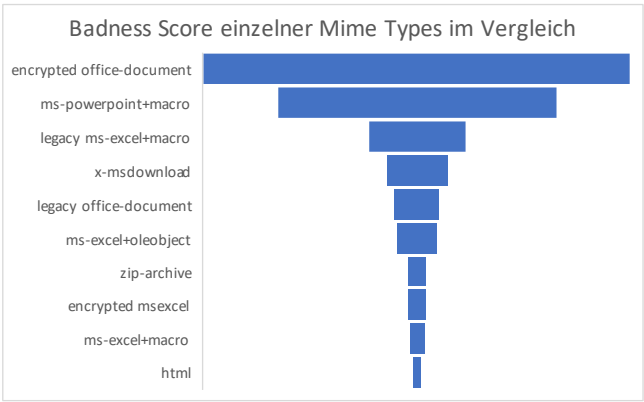
Encrypted Office Files waren 2022 Malware-Spitzenreiter bei Anhängen

Auch im Jahr 2022 stellten E-Mail-Anhänge ein häufig versuchtes Einfallstor für Malware dar. Die Grafik zeigt, wie sich Malware-Erkennungen im Jahr 2022 auf die unterschiedlichen Dateitypen verteilten. Spitzenreiter war die Gruppe verschlüsselter Office-Dateien, gefolgt von der Gruppe *octet-stream*, die viele Image- und Archiv-Formate zusammenfasst. Besonders häufig waren auch klassische ZIP-Dateien sowie Text/HTML.



Angreifer nutzen gerne verschlüsselte Dateiformate, um es Sicherheitslösungen zu erschweren, den enthaltenen Schadcode zu erkennen. Office-Dateien sind dabei besonders beliebt, weil sie weit verbreitet sind und damit die Empfänger daran gewöhnt sind, diese zu öffnen. Durch die Möglichkeit von Makros ist es in Office-Dateien zudem auch nicht schwer, Schadcode zu entwickeln. Wir berechnen in unseren Analysen die Gefährlichkeit einzelner Mime-Typen in einem sogenannten *Badness Score*.

In der Grafik zum Badness Score wird die Top 10 der bösartigen Mime-Types dargestellt. Aus den Werten ergibt sich beispielsweise, dass im deutschsprachigen Raum die Wahrscheinlichkeit, dass ein E-Mail-Anhang bösartig ist, bei verschlüsselten Office-Dokumenten rund 20 Mal höher ist, als bei einfachen ZIP-Archiven.



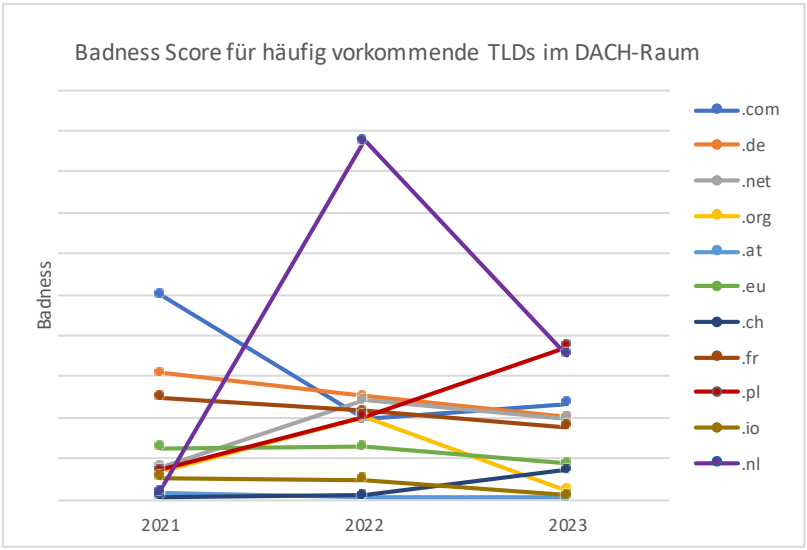
Selbst die zu Recht in Verruf geratenen alten Excel-Formate mit Makros bergen statistisch nur ein Viertel so viel Risiko wie verschlüsselte Office-Dateien.

Empfehlung: Bei der Pflege der entsprechenden Filtereinstellungen sollten Administratoren ein besonderes Augenmerk auf verschlüsselte Office-Dateien legen. Ggf. können diese per Policy intensiver geprüft oder per se von der Zustellung ausgeschlossen werden.

Welche Top Level Domains waren bei bösartigen URLs in 2022 besonders auffällig?

Neben E-Mail-Anhängen sind URLs ein zweiter wichtiger Angriffsvektor. Auch hier errechnen wir einen *Badness Score*, in den sowohl das Aufkommen der Domäne im gesamten Traffic als auch die Anzahl der als bösartig klassifizierten URLs einfließen. Die Grafik zeigt, wie sich der Badness Score für URLs bei den am häufigsten auftretenden TLDs über die vergangenen drei Jahre verändert hat.

URL Badness Score			
TLD	2021	2022	2023
.com	0,997	0,392	0,469
.de	0,617	0,505	0,401
.net	0,156	0,485	0,395
.org	0,131	0,403	0,047
.at	0,027	0,013	0,007
.eu	0,249	0,256	0,175
.ch	0,012	0,020	0,145
.fr	0,499	0,430	0,356
.pl	0,143	0,404	0,744
.io	0,108	0,097	0,020
.nl	0,041	1,752	0,704



Zum Vergleich haben wir noch die TLD *.nl* aufgeführt. Hier hat es in 2022 eine interessante Spitze gegeben. Der Grund dafür waren extensive Spam-Kampagnen aus der niederländischen TLD, bei denen die zugehörigen Domänen-Namen auf Deutsch lauteten, also speziell auf den DACH-Raum zielten. Generell sind die TLDs *.ch* und *.at* eher als unkritisch zu betrachten, während die anderen beiden direkten Anrainer *.fr* und *.pl* zusammen mit *.com* häufiger auffällig waren.

In Summe bleibt festzuhalten, dass der Anteil böshafter E-Mails bei etablierten TLDs konstant bleibt oder teilweise sogar rückläufig erscheint. Die vielen Anstrengungen zur Abwehr und Vermeidung von Spam und Malware bei Unternehmen und Organisationen im DACH-Raum zeigen offenbar langsam Wirkung.

Ein völlig anderes Bild zeigt sich bei den Top 10 der TLDs mit dem höchsten Anteil an bösartigen E-Mails, also hohem Badness Score: Der Spitzenreiter *.fun* hat einen rund 28 Mal höheren Badness Score als der schlechteste Vertreter aus der Gruppe der etablierten TLDs.

Bemerkenswert ist auch der ausgesprochen hohe Badness Score bei den polnischen Domains *waw.pl* und *net.pl*. Vom Volumen her machen die E-Mails der Top 10 Bad TLDs weniger als ein Prozent vom Gesamt-Traffic an geschäftlichen E-Mails in der DACH-Region aus.

Empfehlung: E-Mails mit URLs, die auf TLDs mit schlechter Reputation verlinken, sollten mehr als kritisch bewertet werden. Das gilt besonders, wenn Sender von vertrauenswürdigen Domains aus senden, aber die Links zu TLDs mit geringer Reputation verweisen. Dafür gibt es in der Regel keinen guten Grund. Ggf. sollten für diese Konstellation explizit Whitelists geführt werden.

Top 10 Bad TLDs	
TLD	2022
.fun	14,4
.bid	12,7
.wiki	12,0
.co.in	11,7
.live	10,8
.net.pl	9,6
.xyz	9,4
.waw.pl	9,2
.click	8,6
.website	8,5

Ein Trend 2022: Dateiendungen verschleiern

Bei der Suche nach bösartigen Anhängen sind oft die Endungen im Dateinamen von besonderem Interesse. Da Windows-Systeme die eigentliche Endung – also den Teil nach dem letzten Punkt – nicht anzeigen, besteht bei Angreifern die Hoffnung, die wahre Natur ihrer E-Mail-Anhänge vor Nutzenden verschleiern zu können.

Es wird beispielsweise versucht, eine verdächtige Endung wie *.img*, *.001* oder *.iso* durch harmlose Endungen wie *.pdf* oder *.jpg* zu maskieren. So wird aus *Cartoon.img* durch die Umbenennung in *Cartoon.pdf.img* aus Sicht des unbedarften Windows-Nutzers plötzlich der harmlos aussehende Anhang *Cartoon.pdf*. Klickt der Nutzende darauf, öffnet das Betriebssystem die Installationsdatei. Der Trick ist alt, erfreute sich aber nach wie vor großer Beliebtheit. In der Tabelle finden sich die beliebtesten Kombinationen im Jahre 2022.

Empfehlung: Gute E-Mail-Sicherheitslösungen prüfen alle Anhänge auf ihren tatsächlichen Dateityp und erkennen solche Versuche sofort. Administratoren sollten die entsprechenden Filter einschalten und solche Mails abweisen.

Dateiendungen-Maskierung Top 10 2022
pdf.img
jpg.img
pdf.001
pdf.ISO
pdf.z
docs.zip
doc.rar
pdf.gz
pdf.arj
docs.rar

Über 32Guards

32Guards nutzt das Prinzip der Schwarmintelligenz zur Abwehr von Gefahren: Alle teilnehmenden NoSpamProxy-Instanzen teilen dabei ihre Erfahrungen untereinander – insbesondere im Hinblick auf erkannte Bedrohungen und Anomalien – und profitieren so vom Wissen aller. Neben diesem Echtzeit-Schutz für alle angeschlossenen Kunden entsteht so zusätzlich eine Datenbasis zur mittel- und langfristigen Analyse und Auswertung von Angriffsformen und -mustern. Jede Woche werden vollständig anonym und im Einklang mit der EU-DSGVO die Metadaten von vielen Millionen Mails, Links und Anhängen gesammelt und nach Abweichungen, Trends und Mustern ausgewertet.

Dabei steht bewusst der geschäftliche E-Mail-Traffic in Deutschland, Österreich und der Schweiz (DACH-Region) im Fokus, um auch lokale Trends und Muster gezielt finden zu können. Damit unterscheidet sich 32Guards deutlich von anderen Analyseverfahren, bei denen lokale Trends im deutschsprachigen Raum oft in einer Flut privater E-Mail-Empfänger oder im Grundrauschen vieler internationaler Nutzer untergehen.

Neue Erkenntnisse fließen sofort automatisiert in den Schutz der angeschlossenen Kunden ein, werden aber auch der Allgemeinheit in Form von Alerts und Research Notes bereitgestellt. 32Guards gehört seit der Version 14 zum Standard der NoSpamProxy Mail Security Suite.

Aktuelle Datenbasis (Stand 05/2023) pro Woche:

34,0 Mio. E-Mails | **10,0 Mio. Anhänge** | **300 Mio. Links**

Über NoSpamProxy und Net at Work

Net at Work unterstützt als IT-Unternehmen seine Kunden mit Lösungen und Werkzeugen für die digitale Kommunikation und Zusammenarbeit. Der Geschäftsbereich Softwarehaus entwickelt und vermarktet mit NoSpamProxy ein innovatives Secure E-Mail-Gateway mit erstklassigen Funktionen für Anti-Spam, Anti-Malware und E-Mail-Verschlüsselung, dem weltweit mehr als 4.000 Kunden die Sicherheit ihrer E-Mail-Kommunikation anvertrauen. Die mehrfach ausgezeichnete Lösung – unter anderem Testsieger im unabhängigen techconsult Professional User Ranking – wird als Softwareprodukt und Cloud-Service angeboten. Mehr zum Produkt unter: www.nospamproxy.de

Die Kunden von Net at Work finden sich deutschlandweit im gehobenen Mittelstand wie beispielsweise Diebold-Nixdorf, CLAAS, Miele, Lekkerland, SwissLife, Uni Rostock, Würzburger Versorgungs- und Verkehrsbetriebe und Westfalen Weser Energie. Net at Work wurde 1995 gegründet und beschäftigt derzeit mehr als 130 Mitarbeiter in Paderborn und Berlin. Gründer und Gesellschafter des inhabergeführten Unternehmens sind Uwe Ulbrich als Geschäftsführer und Frank Carius, der mit www.msxfaq.de eine der renommiertesten Websites zu den Themen Office 365, Exchange und Skype for Business betreibt. www.netatwork.de

www.nospamproxy.de | Net at Work GmbH | anfragen@netatwork.de