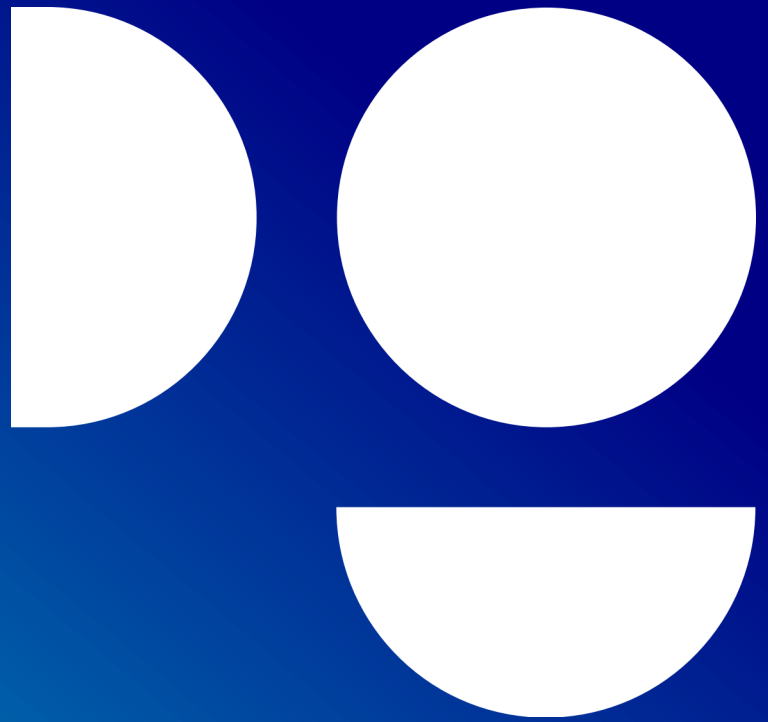
dataglobal group

dataglobal Group

@DFN Betriebstagung



1. Vorstellung
2. Cybercrime in Deutschland
3. eXpurgate E-Mail Security
4. Detection Trends & Beispiele
5. Und weiter?

Vorstellung

Wer sind wir?

Über die dataglobal Group

30 Jahre
Erfahrung in der
Softwareentwicklung
„Made in Germany“

Über 3.000 Kunden

25 Mio. € Umsatz
pro Jahr

Über 220 Mitarbeiter

Fokusmarkt:
Deutschland
Österreich
Schweiz

Softwarelösungen für
den digitalen Arbeitsplatz

dataglobal Group

Brands

eleven

Berlin
40 Mitarbeitende

windream
MANAGING DOCUMENTS

Bochum
95 Mitarbeitende

dataglobal[xx]

Hamburg
Heilbronn
Cluj-Napoca
80 Mitarbeitende

vykon
a dataglobal Group company

München
10 Mitarbeitende

dataglobal Group

Heutige Referenten

Christian Lange

Director Product Management bei

eleven cyber security

Ulrich Jansen

Geschäftsführer

bei eleven cyber security

eleven

Cybercrime

Lage in Deutschland

Cybercrime – die Lage

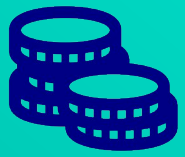
Aktuelle Zahlen

Phishing bleibt eine der häufigsten Cyberbedrohungen:
Laut Verizon (2023) waren 36 % aller erfolgreichen Datenverletzungen auf Phishing zurückzuführen. E-Mails sind das Hauptmedium für diese Art von Angriffen.

E-Mails als Hauptkanal für Malware:
Laut Statista (2023) werden etwa 94 % aller Malware-Angriffe über E-Mails verbreitet. Dies zeigt, dass E-Mails ein bevorzugtes Werkzeug für Cyberkriminelle sind, um Schadsoftware wie Ransomware und Trojaner zu verteilen.

Kundenverluste durch Cyberangriffe:
Laut einer Studie von EY Schweiz verlieren 41 % der betroffenen Unternehmen nach einem Cybervorfall Kunden, da das Vertrauen in die Sicherheit der Daten verloren geht.

Durchschnittliche Kosten eines Datenverlusts:
Eine Studie des BSI gibt an, dass die durchschnittlichen Kosten für die Wiederherstellung von Daten und Systemen nach einem Angriff bei 100.000 Euro für kleinere Unternehmen und bis zu 1 Million Euro für große Unternehmen liegen können.



„Der Schaden der Cyberangriffe in Deutschland betrug im Jahr 2021 etwa 225,3 Mrd. Euro.“*

*Quelle: Bundeskriminalamt - BKA

eXpurgate

E-Mail-Security to keep the Inbox clean

eXpurgate

E-Mail Security Engine

eXpurgate Fakten

- seit 2001 am Markt als Cloud und Inhouse Lösung
- Klassifizierung in ~ 20 verschiedene Kategorien (u.a. Phishing, Malware, Spam, Scam, Newsletter)
- Verarbeitung von 1 Milliarde E-Mails täglich
  - 50% des deutschen privaten E-Mail-Verkehrs
- Einfache und flexible Integration (In-/ Outbound)
  - SMTP-Proxy
  - Milter Plugin (sendmail)
  - spamd Plugin (Postfix)
  - Daemon
  - SDK
  - zusätzlich: einfache Anbindung von 3rd Party AV Engines (Avira, Varist, Ikarus)
- Made & operated in Germany
- Spam-Ordner und Quarantäne adé
  - Hohe Trefferraten und geringe FP-Raten
  - Garantierte Erkennungsrate: >99%
  - Garantierte FP-Rate: <0,00005% (1 von 2 Millionen E-Mails)

eXpurgate

E-Mail Security Engine

Hands off: Einmal eingerichtet übernimmt eXpurgate

- Eigene global gewonnene Daten werden fortlaufend zentral:
  - analysiert
  - angereichert
  - bewertet
- Alle Kunden profitieren von den Daten automatisch:
  - Eigene Pflege von Block-/Allow-Listen kann entfallen
  - Outbreak Detection schließt die Lücken die AV-Engines durch den Update Zyklus haben
  - Newsletter und Graymail werden zuverlässig erkannt
  - Updates passieren automatisch fortlaufend und schnell im Hintergrund
- Optionaler Hands-Off-Ansatz: eXpurgate **kann** bis ins kleinste Detail konfiguriert werden - notwendig ist es nicht.

Detection

Aktuelle Beispiele

Detection

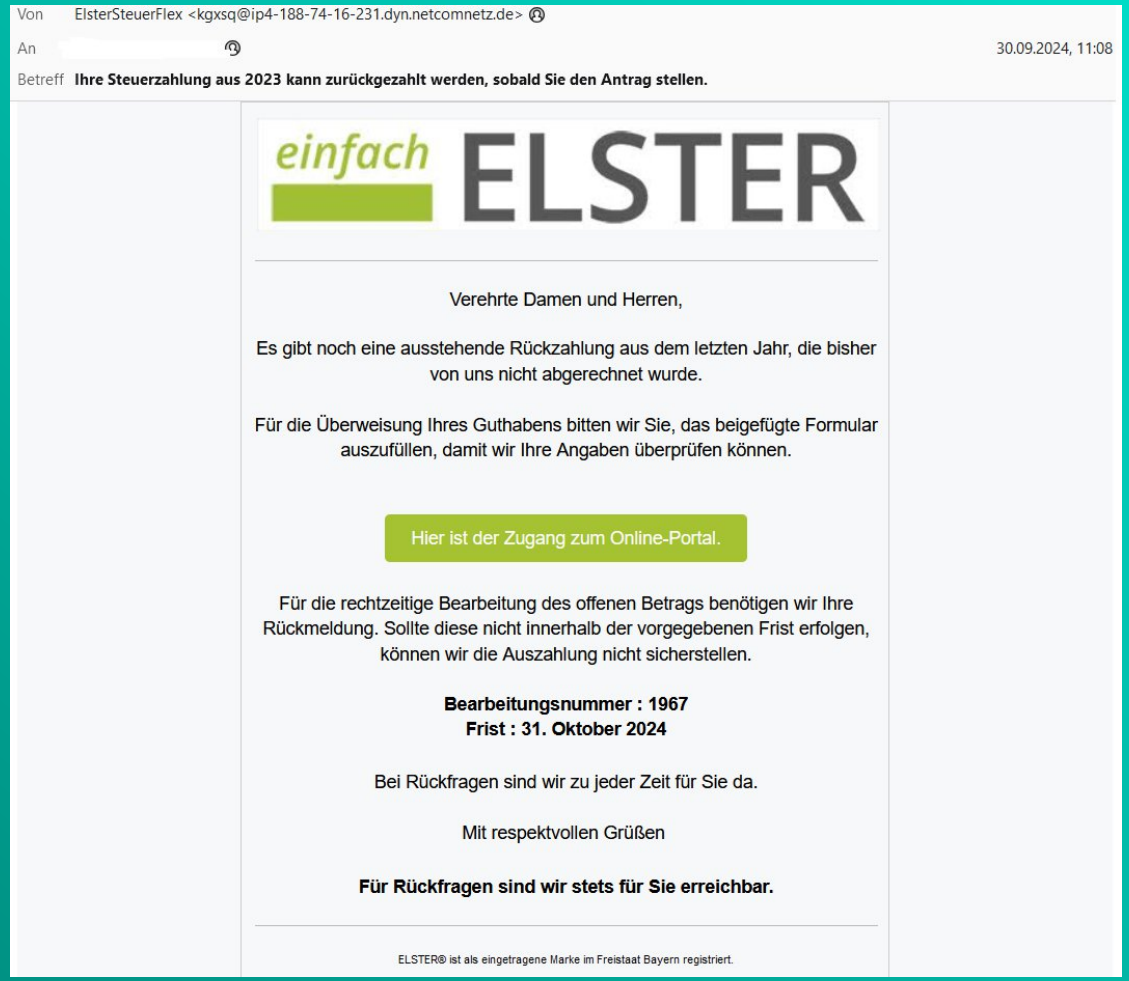
Aktuelle Trends

Wie sich die Techniken verändert haben

- Kurzfristigen Mieten von legitimer Infrastruktur mit „Wegwerf-VMs“ (z.B. bei AWS, Azure, o.ä.)
  - Hebelt IP-Listen aus
  - Spamwellen mit Millionen von E-Mails in kurzer Zeit
  - Botnetze sind dagegen einfacher zu erkennen
- Missbrauch anderer legitimer E-Mail-Infrastrukturen wie z.B. Amazon SES und Office 365
- Ausnutzen modernen CSS- und HTML Techniken zum Verschleiern von Text
- Unicode zur Nutzung von Homoglyph-Attacken
- Missbrauch von vertrauenswürdigen Anbietern (z.B: Docusign, Paypal, Elster)

Detection

Beispiele



Von ElsterSteuerFlex <kgxsq@ip4-188-74-16-231.dyn.netcomnetz.de>

An

30.09.2024, 11:08

Betreff **Ihre Steuerzahlung aus 2023 kann zurückgezahlt werden, sobald Sie den Antrag stellen.**

einfach ELSTER

Verehrte Damen und Herren,

Es gibt noch eine ausstehende Rückzahlung aus dem letzten Jahr, die bisher von uns nicht abgerechnet wurde.

Für die Überweisung Ihres Guthabens bitten wir Sie, das beigefügte Formular auszufüllen, damit wir Ihre Angaben überprüfen können.

Hier ist der Zugang zum Online-Portal.

Für die rechtzeitige Bearbeitung des offenen Betrags benötigen wir Ihre Rückmeldung. Sollte diese nicht innerhalb der vorgegebenen Frist erfolgen, können wir die Auszahlung nicht sicherstellen.

Bearbeitungsnummer : 1967
Frist : 31. Oktober 2024

Bei Rückfragen sind wir zu jeder Zeit für Sie da.

Mit respektvollen Grüßen

Für Rückfragen sind wir stets für Sie erreichbar.

ELSTER® ist als eingetragene Marke im Freistaat Bayern registriert.

Detection

Beispiele

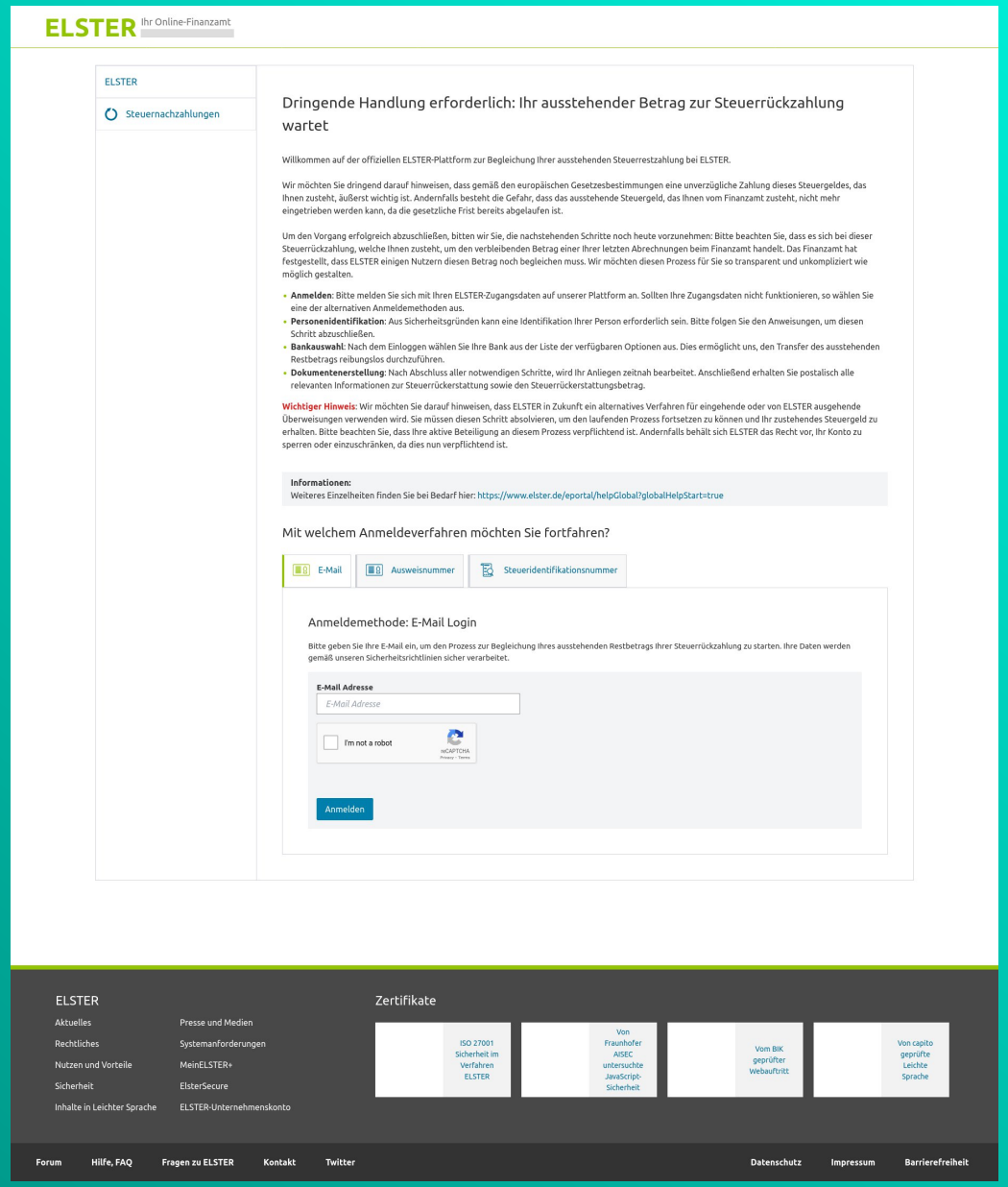
Phishing-Angriff

- Saisonalität
- sehr gut gemachtes Mailing & Landingpage

Ziel:

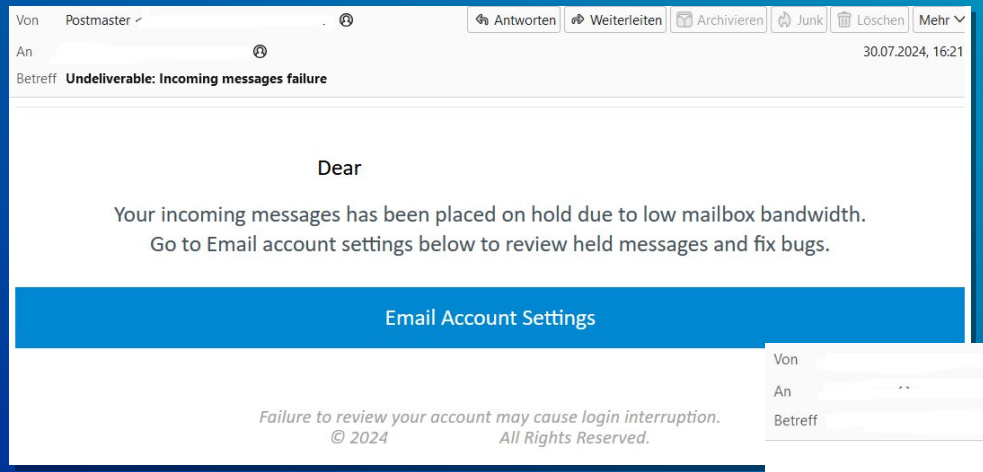
Identitätsdiebstahl für Betrug

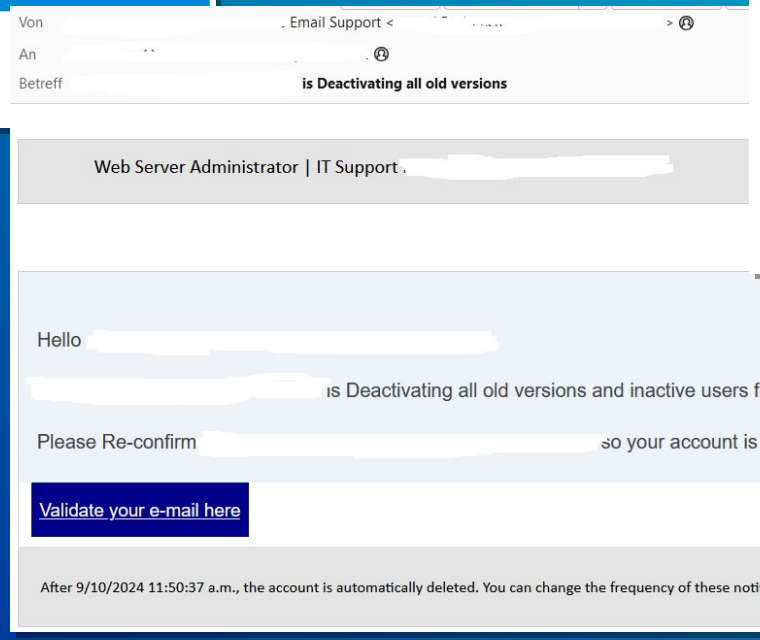
(Adresse, E-Mail, Telefon, Geburtstag, …)

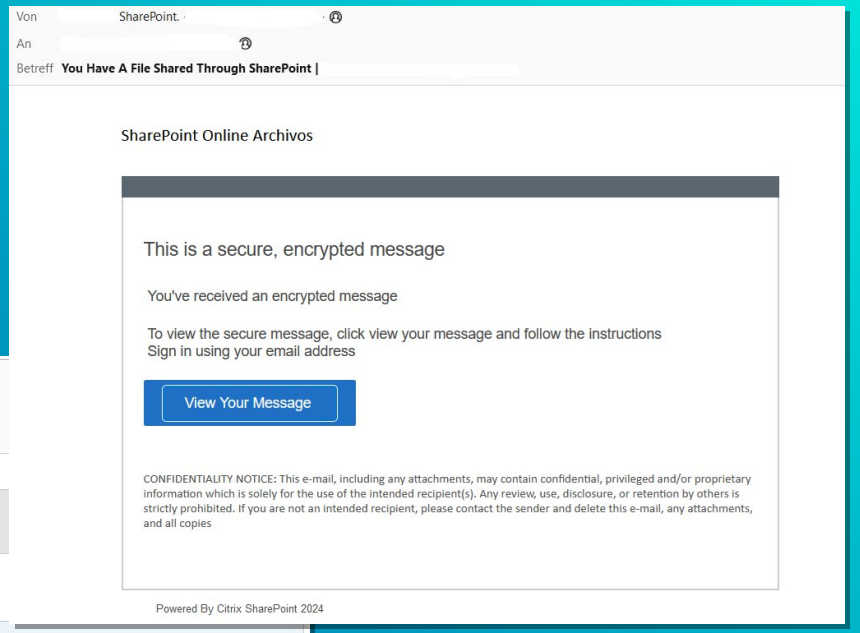


Detection

Beispiele im Uni-Umfeld







Und weiter?

ein Gedankenspiel

eXpurgate

Gedankenspiel

Effizientere Detection für Inbound & Outbound Traffic

- Mehr Detection durch den zusätzlichen Einsatz von eXpurgate
  - Einsatz bei Inbound / Outbound Traffic neben dem DFN-Filter
  - geringe FP-Rate ermöglichen problemloses Chaining
- Pflege von Block-/Allowlists
  - -> wird auf ein Minimum reduziert – eXpurgate kommt regelmäßig ohne aufwändige Listen aus
- Virenscan mit stündlichen Updates
  - -> Outbreak Detection schließt die Lücke zwischen Zero-Day und AV-Update
- Newsletter-Allowlists
  - -> erwünscht/unerwünschte Newsletter („Graymail“) werden in separaten Kategorien erfasst
  - -> kein Extraaufwand Listen zu pflegen
- (mögliche) Mitarbeit für Postmaster durch Sample Reportings und engen Austausch

Fragen

Kontaktdaten

Danke für Ihre Aufmerksamkeit.

Bei Fragen wenden Sie sich gerne an Sebastian Hinz,
Sales eleven cyber security GmbH

Ihre Fragen rund um eXpurgate


dataglobal
group