

zix | *appriver*

Global Threat Report

Halbjahresbericht 2021



Einleitung

Cyberkriminelle erweitern ständig ihr Repertoire und entwickeln neue Methoden und Techniken, um die Wirksamkeit ihrer Angriffe gegen technologische und menschliche Abwehrmechanismen zu verbessern. Auch diesem Jahr haben die Angreifer weiter aufgerüstet.

Im Jahr 2021 haben wir bereits mehrere neue Methoden im Bereich der Anpassung und Tarnung beobachtet. In diesem Bericht gehen wir beispielhaft auf mehrere neue Entwicklungen ein. Wir untersuchen auch einige altbekannte Angriffsvarianten, die für Unternehmen auf der ganzen Welt weiterhin eine Bedrohung darstellen.

Mehr als die Hälfte des Jahres 2021 liegt bereits hinter uns, aber eines hat sich in dieser Zeit nicht verändert: E-Mails sind nach wie vor weltweit der meistgenutzte Angriffsvektor bei Cyberattacken auf Unternehmen. In der ersten Jahreshälfte haben sich die Phishing-Angriffe weiterentwickelt und sind ausgefeilter als je zuvor. Wir haben erstmals beobachtet, dass Angreifer echte Webzertifikatsdaten nutzen, um ihren Angriffsversuchen durch Anpassung mehr Glaubwürdigkeit zu verleihen. Darüber hinaus investieren die Kriminellen viel Arbeit in die Tarnung ihrer kriminellen Aktivitäten. Ein Beispiel dafür sind Phishing-Angriffe, die die Captcha-Technologie nutzen, um nicht entdeckt zu werden.

Cyberkriminelle gehen bei ihren Täuschungsversuchen einen Schritt weiter und lassen ihre Angriffe aussehen wie Nachrichten von bekannten und vertrauenswürdigen Diensten. Arbeitssuchende und Personalabteilungen von Unternehmen wurden beispielsweise mit Phishing-E-Mails attackiert, die bekannte Job-Webseiten imitiert haben.

IC3 hat kürzlich gemeldet, dass „Business E-Mail Compromise“ (BEC) mit bereinigten Verlusten in Höhe von 1,8 Milliarden US-Dollar die teuerste Betrugsmasche im Jahr 2020 war. Daher überrascht es nicht, dass wir auch in den ersten beiden Quartalen des laufenden Jahres eine große und weiter steigende Anzahl an BEC-Angriffen beobachtet haben. Anzeichen für einen Rückgang der Zahlen gibt es bislang nicht.

Ende Januar ging die Nachricht von den Ermittlungen der Strafverfolgungsbehörden um die Welt, die zur Zerschlagung der Malware-Gruppe Emotet geführt haben – ein leider viel zu seltenes Ereignis. Vor seinem Ende war Emotet eine der fortschrittlichsten, professionellsten und aktivsten Malwares auf dem Markt. Emotet war ursprünglich ein Banking-Trojaner, hat aber im Laufe der Zeit seinen Aktionsradius erweitert und fungierte dann als Loader für Verteiler anderer Malware-Typen. Emotet wurde also in großem Umfang als Malware-as-a-Service (MaaS) genutzt.

Viele der Banking-Trojaner, über die wir im Folgenden berichten, folgen bereits einem ähnlichen Weg. Einige von ihnen scheinen diesen Geschäftsbereich angesichts der gestiegenen Nachfrage nach MaaS-Angeboten nach der Zerschlagung von Emotet weiter ausgebaut zu haben.

Wir werfen auch einen Blick auf einige RAT-Aktivitäten (Remote Access Trojan), die in der ersten Hälfte des Jahres 2021 besonders aktiv waren



Personalisierte Angriffe - Webseiten-Zertifikatsdaten

In unserem [Global Security Report 2020](#) haben wir prognostiziert, dass die Angreifer ihre Vorstöße in diesem Jahr noch stärker personalisieren und anpassen würden. Der folgende Fall ist ein gutes Beispiel dafür. Dieser Phishing-Versuch gibt sich als Zertifikatsfehlermeldung für die Website des Empfängers aus. Das Besondere daran ist, dass die echten Zertifikatsdaten und der A-Datensatz des DNS (Domain Name System) verwendet wurden, um die Phishing-Nachricht an die Domain des Empfängers anzupassen. Die Payload-URL führte zu einer Website zum Abfangen von Anmeldeinformationen, die wie die Admin-Seite der jeweiligen Webplattform aufgebaut war. Bei unseren Tests sind uns die generischen WordPress-Admin-Anmeldeseiten sowie die Shopify-Anmeldeseiten aufgefallen (je nach Ziel).

BEISPIEL 1: ZERTIFIKATFEHLER

Certificate Error on [redacted].com

Let's Encrypt <tlsreport@securemailer.net>
To: [redacted]

Thu 4/15/2021 9:02 AM

Let's Encrypt Error Prevention

Conflict in SSL/TLS Certificate Signature Algorithm

Your e-mail address is registered as the owner of [redacted].com. This domain address is using a R3 certificate, and our systems automatically detect any errors related to your certificates.

As a matter of quality and security, we intensively upgrade our error prevention and reporting services. Currently we're fully integrated to **Shopify Support Team**. You're able to resolve this issue by logging to your Shopify Panel.

[redacted].com Certificate Data
Let's Encrypt / R3
Issuance Date: 2/5/2021 1:10:54 AM / Expiry Date: 5/6/2021 1:10:54 AM
Serial Number: 04:E3:70:DC:26:51:F4:BB:7F:EB:6A:3B:F6:4E:82:6F:EB:E4
DNS A Record: ns1.uniregistry-dns.com

What can happen to [redacted].com?
Your website can show certificate errors to your customers and in critical cases suffer attacks such as POODLE-TLS.

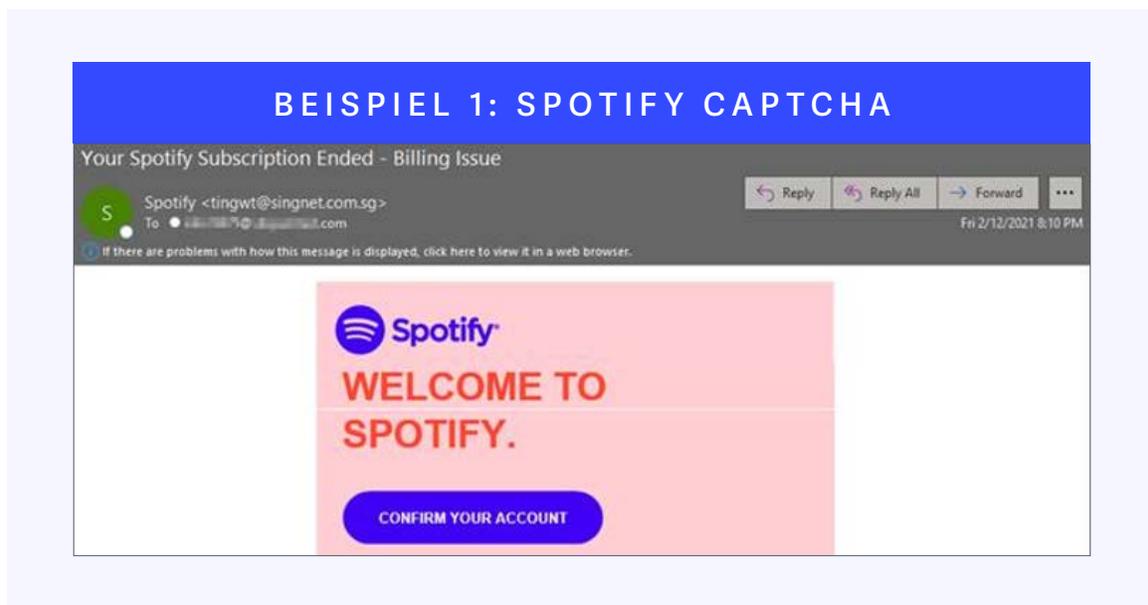
We highly recommend you to fix the issue described in [redacted]

[Start the update process](#)

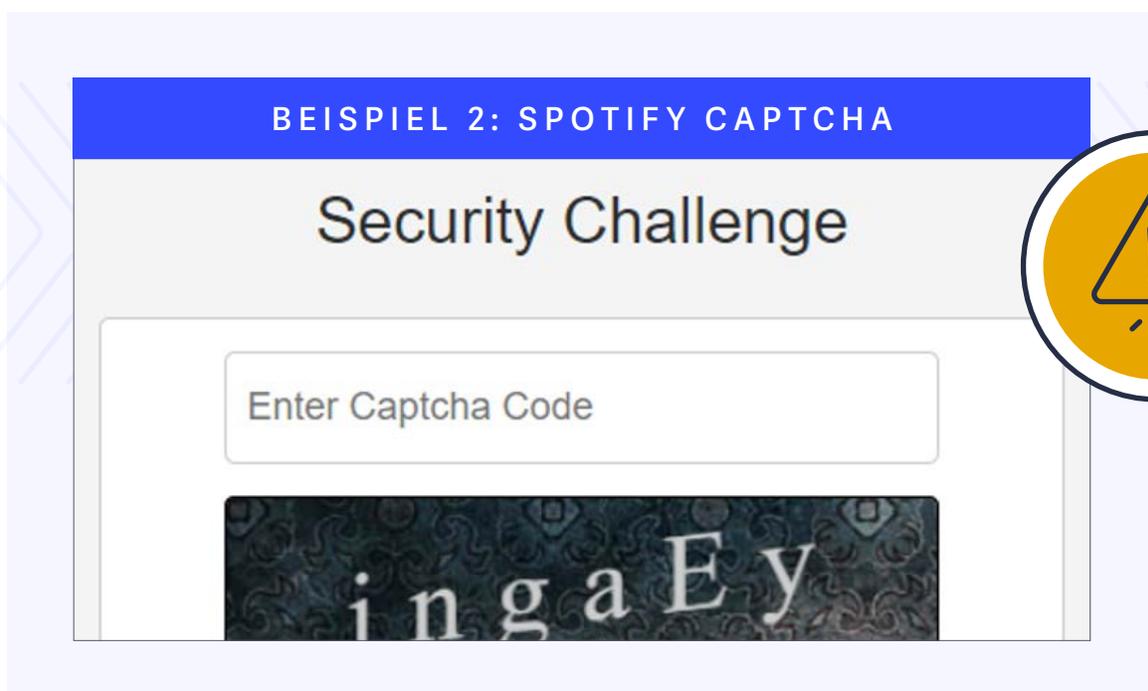
By clicking on the link you agree with Let's Encrypt Terms and Conditions.
If you're not the owner of [redacted].com; please ignore this message.
All data you submit during update process is your responsibility.
Do not reply to this message. This is an automatic message.

Mehr Tarnung – Captcha-Phishing

Im bisherigen Verlauf des Jahres 2021 haben sich Captcha-Technologien bei Phishing-Angriffen immer stärker verbreitet. Im Februar wurden wir auf eine Reihe von Angriffen aufmerksam, die Nachrichten des Streaming-Portals Spotify imitierte und Captchas verwendete. Wir gehen davon aus, dass diese Methode von nun an häufiger vorkommen wird, da die Verwendung von Captchas den Angreifern hilft, den Inhalt ihrer Landingpages vor Web-Scanning-Diensten zu verbergen, die ihn als verdächtig identifizieren könnten.



Klickt man auf den Link „BESTÄTIGEN SIE IHR KONTO“, erscheint diese Captcha-Sicherheitsabfrage, die korrekt beantwortet werden muss, um fortzufahren.



Sobald das Captcha korrekt eingegeben wurde, werden Sie auf eine authentisch aussehende, mit Spotify gebrandete Seite geleitet, auf der Sie Ihre Anmeldeinformationen eingeben sollen.

BEISPIEL 3: SPOTIFY CAPTCHA



To continue, log in to Spotify.

Email address or username 

Password 

Remember me 

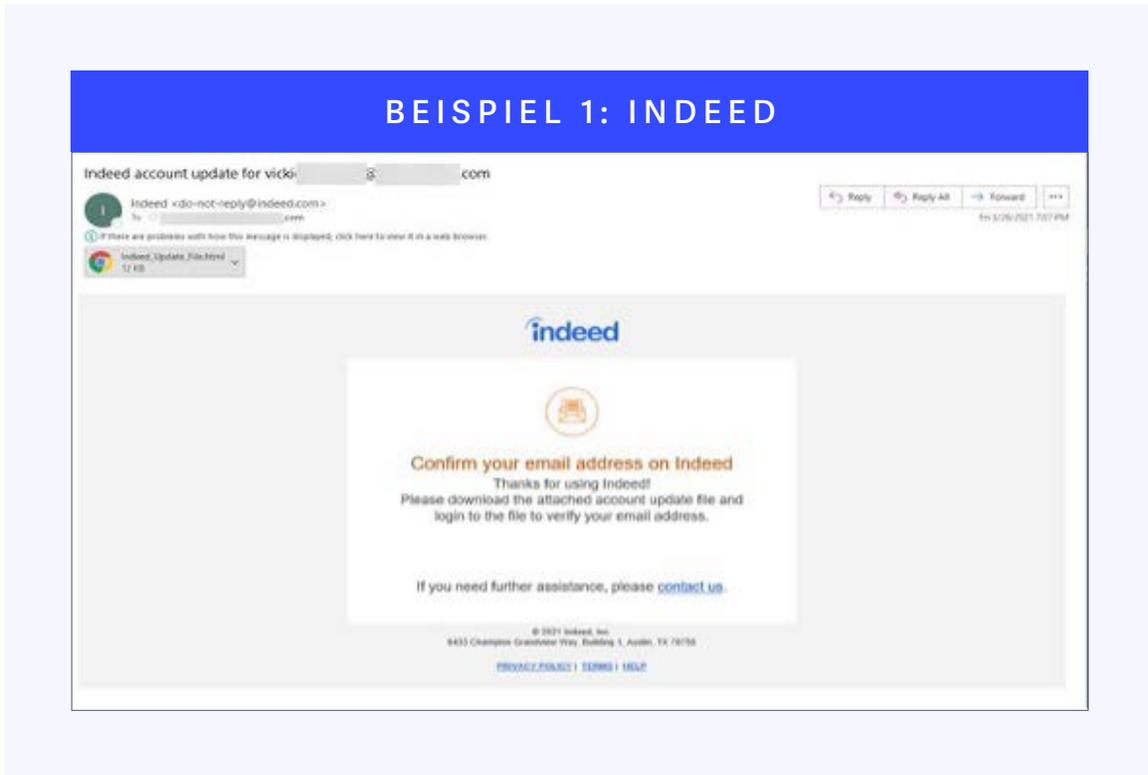
[Forgot your password?](#)

[Terms, Conditions and Privacy Policy.](#)



Arbeitssuchende / Personalabteilungen im Visier

Ende März, als Millionen von Arbeitnehmern nach der Corona-Pandemie wieder ins Berufsleben einsteigen wollten, sind uns vermehrt Phishing-Angriffe aufgefallen, die es auf Nutzer des Online-Jobportals Indeed abgesehen hatten. Diese Angriffe sind nicht nur für Arbeitssuchende gefährlich, sondern auch für Arbeitgeber und insbesondere für Personalabteilungen. Das folgende Beispiel zeigt die per HTML-Anhang übermittelte Phishing-Seite, auf der die persönlichen Daten eingegeben werden sollten.



„Living off the Land“ (LOtL) Phishing-Angriffe

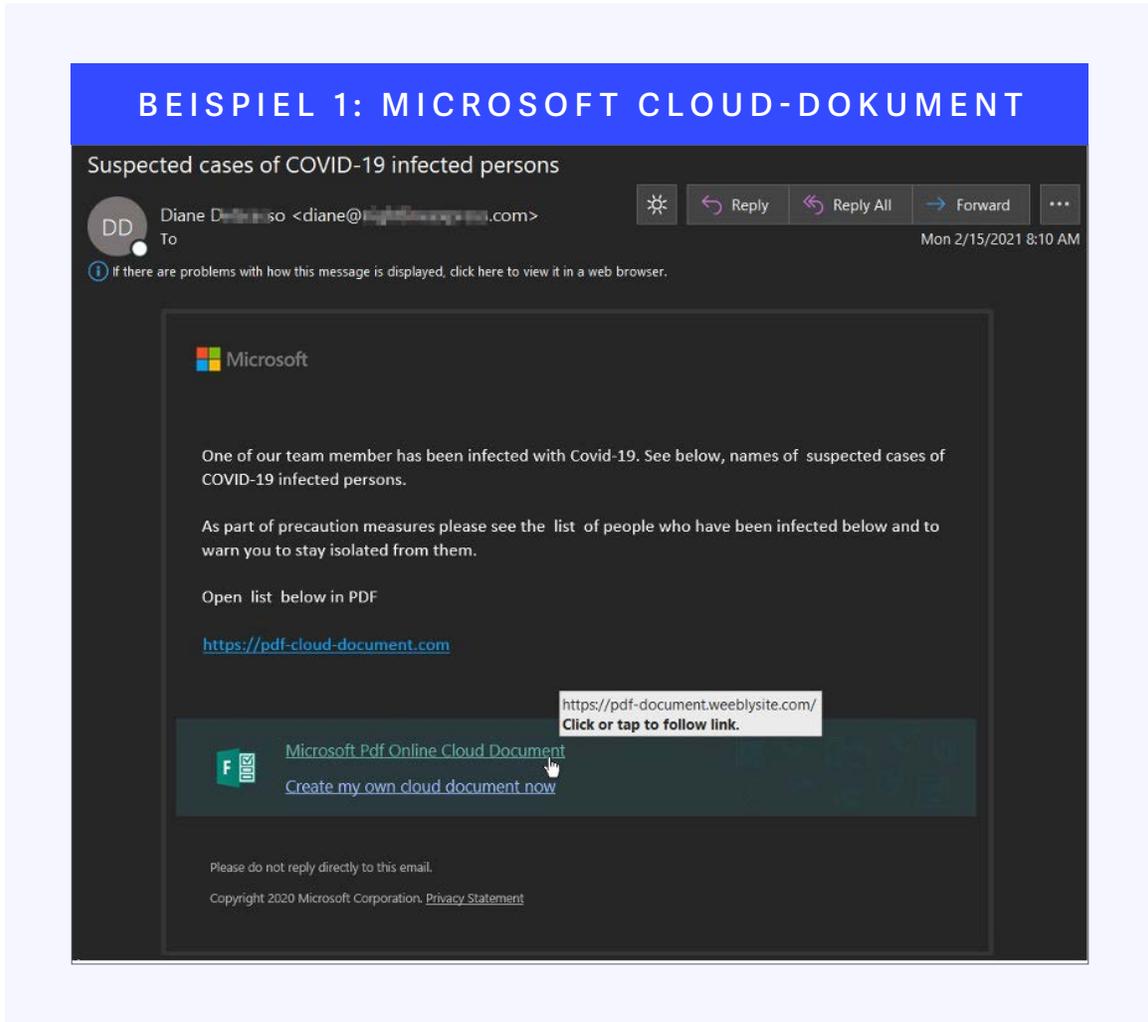
LOtL-Phishing-Angriffe breiten sich immer weiter aus, da die Nutzung legaler Services für illegale Aktivitäten Vorteile für die Cyberkriminellen bieten. Darüber hinaus ist es viel einfacher, Angriffe von seriösen Plattformen aus durchzuführen, da nur wenig oder gar keine zusätzliche Infrastruktur benötigt wird. Wir haben festgestellt, dass einige der erfolgreichsten Angreifer verschiedene Plattformen nutzen, um den Schutz vor diesen Angriffen zu erschweren.

Das sind die 20 Dienste, die bei LOtL-Phishing-Angriffen am häufigsten zur Tarnung genutzt werden (nach E-Mail-Aufkommen).

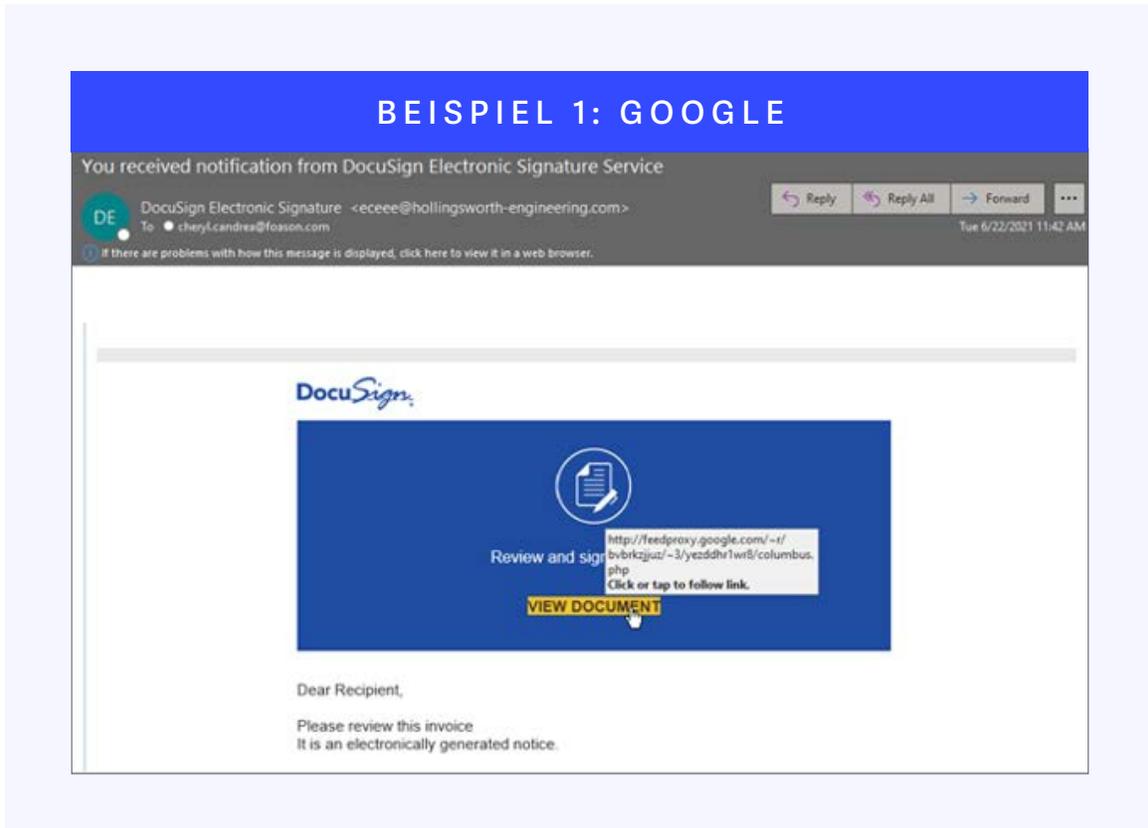
Google APIs	OracleCloud
GoogleDocs	AzureWebsites
AppSpot	WeTransfer
Amazon AWS	FireBaseApp
WebApp (Google)	MySharepoint
PageLink	ReBrandly
FeedProxy	BlogSpot
SendGrid	SurveyMonkey
WindowsNET	AzureEdge
ListManage	GoogleSites



Bei einem LOTL-Angriff zum Thema COVID-19, den wir dokumentiert haben, wurde behauptet, dass „ein Teammitglied mit COVID-19 infiziert wurde“. Man solle sich künftig von den Betroffenen isolieren; deren Namen könne man im beigefügten PDF einsehen. Die Nachricht enthielt einen Payload-Link zu einem „Microsoft PDF Online Cloud Document“. Der Link führte zu einer Phishing-Seite, die wie ein Adobe PDF Online-Cloud-Dokument aufgebaut war. Weebly ist ein Website- und Formularanbieter, der in diesem Jahr vermehrt von LOTL-Angreifern zur Tarnung genutzt wurde.



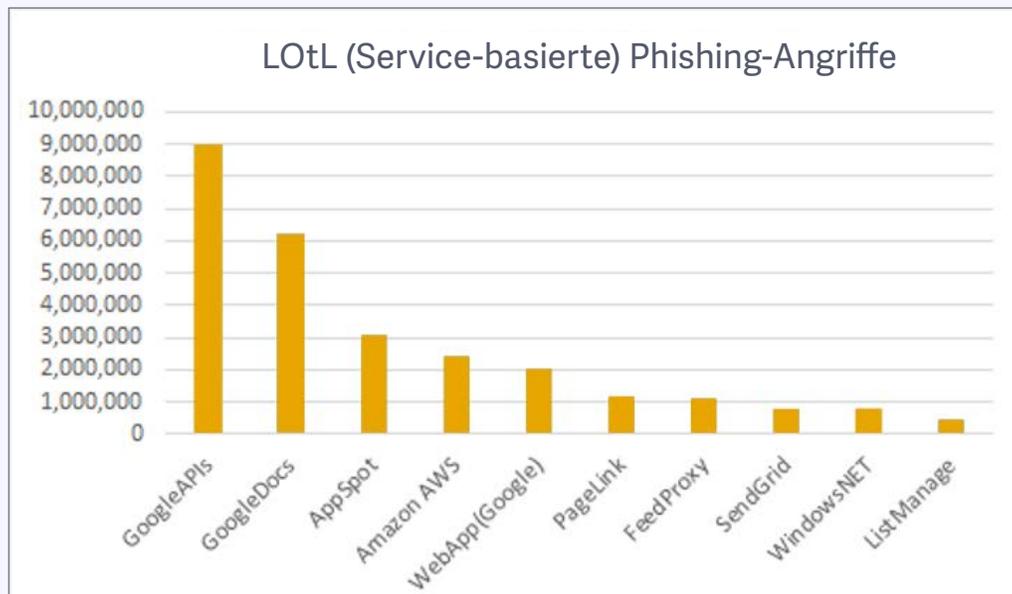
Cyberkriminelle, die bei ihren Angriffen die LOTL-Phishing-Methode anwenden, sind immer auf der Suche nach neuen Diensten, die sie für ihre Zwecke missbrauchen können. Im Juni haben wir einen starken Anstieg der illegalen Verwendung von Googles Feedproxy/Feedburner-Dienst beobachtet. Angreifer haben die Google-Dienste Sites, Docs und APIs (Application Programming Interfaces) genutzt, um ihre Angriffe vor Sicherheitslösungen zu tarnen und ihre gefährlichen Links unverdächtig aussehen zu lassen. Obwohl der Feedburner-Dienst schon längere Zeit existiert, konnten die Angreifer bei ihren Angriffen feedproxy.google.com-Links nutzen, um ihre Opfer auf Phishing-Seiten umzuleiten.



LOtL in Zahlen...

Diese Art des Angriffs wird bei Cyberkriminellen immer beliebter. Die Angreifer versuchen mit dieser Methode, unbemerkt an Sicherheitslösungen vorbeizukommen und ihre potenziellen Opfer mit einer scheinbar ungefährlichen E-Mail zu täuschen. In den ersten sechs Monaten des Jahres 2021 haben wir einen Anstieg von elf Prozent bei dieser Art des Angriffs verzeichnet. Insgesamt haben wir 29,7 Millionen LOtL-Phishing-E-Mails bei den 43 Diensten, die wir aktiv überwachen, erfasst.

Nachfolgend ein Blick auf die Top Ten der E-Mail-Angriffe nach Volumen:



„Business E-Mail Compromise“ (BEC)

Die Kompromittierung geschäftlicher E-Mails zählt zu den rentabelsten Angriffsmethoden dieses Jahres und ist weiterhin eine der bevorzugten Varianten von Cyberkriminellen. Die Angriffe erfordern nur minimalen Zeit- und Geldaufwand und können dem Angreifer große Gewinne einbringen. Im Vergleich mit Malware-Angriffen ist es bei BEC-Angriffen einfacher, die verschiedenen Ebenen von Sicherheitslösungen zu umgehen. Darüber hinaus fallen auch die komplexe Infrastruktur und die Tests weg, die bei Malware-Angriffen normalerweise erforderlich sind. Die Angreifer nutzen dabei eine Vielzahl unterschiedlicher Methoden, um Finanzbetrug zu begehen. Die häufigste Variante, die wir beobachten, beginnt mit Spear-Phishing-E-Mails, die dem Angreifer Zugang zu einem Konto verschaffen sollen.

Sobald die Angreifer Zugang zu einem Konto haben, überwachen sie die Kommunikation und warten auf die richtige Gelegenheit, sich einzuschalten und Zahlungen auf ihre eigenen Konten umzuleiten. Wenn das bei dem Account, in den die Angreifer eingedrungen sind, nicht möglich ist, wechseln sie zu einem anderen, indem sie weitere Phishing-Nachrichten an die Kontaktliste des ersten Accounts senden. So bekommen die Angreifer Zugang zu einem anderen Konto, über das Geldtransfers abgewickelt werden.

Beispiel einer BEC-Nachricht zum Diebstahl von Zugangsdaten (geschwärzt)

BEISPIEL 1: ENTWENDUNG VON ZUGANGSDATEN

Preliminary CD Package Has Been Generated (Review / Download Docs)- for Loan #:XXXX415401 (encrypted)

FA To .com> Reply Reply All Forward Mon 5/17/2021

The **Initial Closing Disclosure (CD)** has been issued to the Borrower(s) and the **Pre-Closing Loan Documents** are available to view for the following loan:
Click on the button to access and upload documents into the secure, password protected document portal. The **Closing Disclosure must be uploaded as soon as possible through this portal.**

<https://georgiamortgage.com/secure>
Click or tap to follow link.

ACCESS DOCUMENT

Financial will engage with the Settlement Agent to finalize fees when the loan documents are drawn. In preparation, please review and/or complete the following:

Settlement Agent:

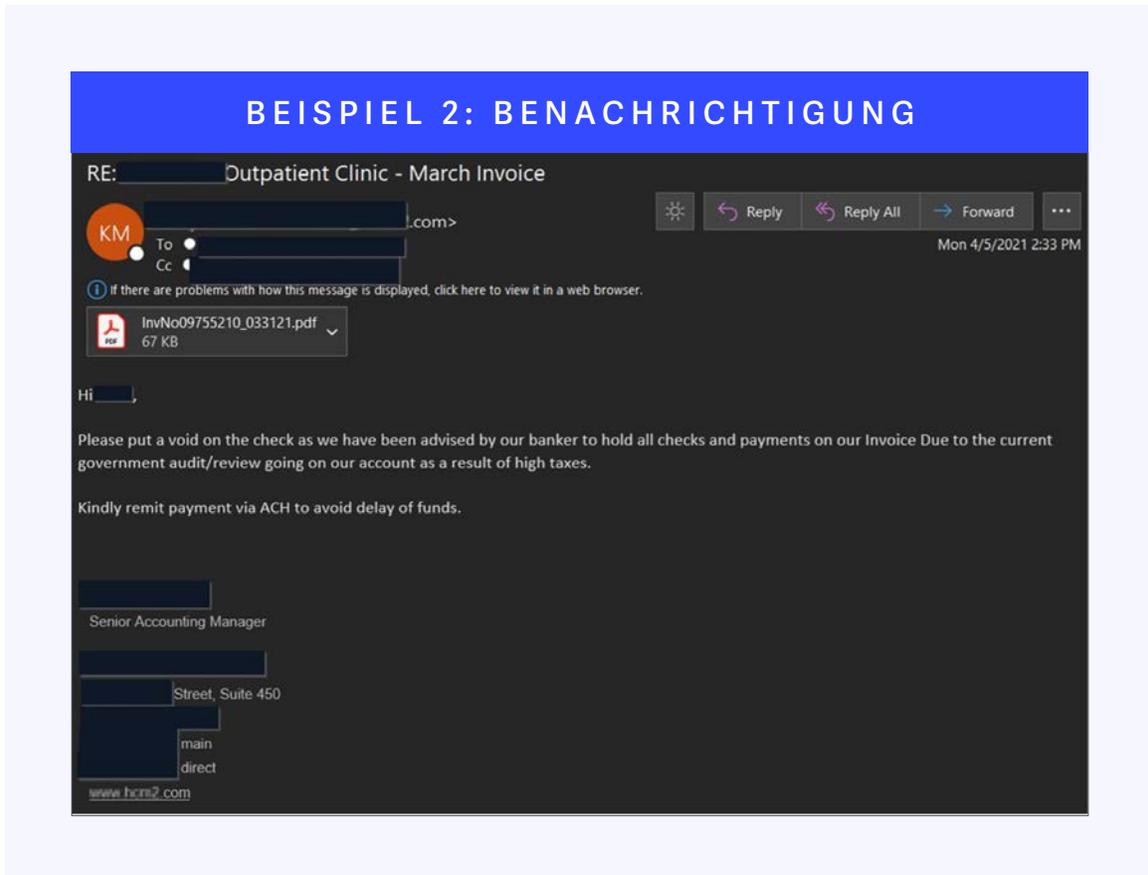
1. Confirm **Vesting**
2. Review **signature lines** and confirm accuracy (No POAs/Trust/AKAs missing, etc.)
3. Provide **State License ID** (Required for Closing Disclosure (CD), Page 5)
4. Review **Closing Disclosure (CD)** for revisions and provide updated **Statement/Closing Disclosure (CD)** to balance the loan

Broker/Processor:

1. Review the **Draft Closing Disclosure** for accuracy of **fees and compensation**
2. **Upload** the following **documents** through the secure, password protected document portal by clicking the link above:
 - Homeowner's Insurance and invoice

If you need assistance or have any questions, please feel free to contact me.

Thank You,
Stephanie Anderson
Closer



Banking-Trojaner – Trickbot

Einer der Banking-Trojaner, die nach der Zerschlagung des Emotet-Botnets Anfang des Jahres verstärkt genutzt wurden, ist Trickbot. Die Inhalte der Angriffe variieren je nach Trickbot-Ableger und reichen von gefälschten Verkehrsverstößen bis hin zu manipulierten Bestellungen. Ist ein Trickbot-Angriff erfolgreich, folgen unter anderem Infizierungen mit Krypto-Mining-Software. Schwerwiegender sind aber häufig die folgenden Ransomware-Infizierungen innerhalb des betroffenen Netzwerks mit Ryuk oder Conti. Die größte Angriffsreihe mit Trickbot, die wir in diesem Jahr beobachtet haben, umfasste etwa 11.300 Nachrichten, die auf Kunden abzielten und wie eine generische Bestellbestätigung aufgebaut waren.

BEISPIEL 1: BESTELLUNG

Re:New PO#87534

Howard <info@...gr>
To: k...@...com

Reply Reply All Forward

Wed 3/31/2021 3:40 PM

P O#87534.7z
10 KB

Good day,

Please find attached our new PO and kindly confirm back if everything looks good on the PO.

Also, please advise on ETA for the shipment.

Thank you.

Best regards,

Howard
採購及資源部-採購員
PNR – Purchaser
Purchasing and Resources
Group Ltd.



Banking-Trojaner – Dridex

Dridex war in diesem Jahr gemessen an der Anzahl der E-Mails mit direkt angehängter Malware die größte Bedrohung. In den ersten beiden Quartalen haben wir über 4,8 Millionen Nachrichten dieser Art erfasst, wobei die meisten aus dem Cutwail-Botnet stammen. Die Angriffe mit Dridex unterscheiden sich in der Regel voneinander, aber die meisten verwenden einen Excel-Anhang als Dropper, um den Dridex-Bankentroyaner zu verbreiten. Fällige Rechnungen oder Kaufbelege sind beliebte Köder für Nachrichten, wobei einige der neueren Beispiele NetSuite, QuickBooks und Office Depot vortäuschen.

BEISPIEL 1: EXCEL-ANHANG

Office Depot Store Receipt #38717-001

OfficeDepotOrders@officedepot.com
To: k@...s.com

Wed 3/24/2021 1:14 PM

Receipt_for_Payment_38717-001.xls
260 KB

Order Confirmation

Thank you for shopping with us.

Attached is your payment receipt.

We are processing your order and will send you an email notification when it ships.

Please note that due to product availability or size, items ordered together may not be shipped together

For your reference, below is a summary of your order:

Expected delivery date: 03/25/2021 8:00 AM - 5:00 PM

Please Note: Delivery fees for shipping to the U.S. Virgin Islands are provided as an estimate. Customers shipping to the U.S. Virgin Islands will be contacted by Office Depot Customer Service.

Order Number: 38717-001
Status: In Process

Order Date: 03/24/2021
Delivery Method: 2 Business Day Delivery

Subtotal:	366.36
Delivery Fee:	0.00
Misc.:	0.00

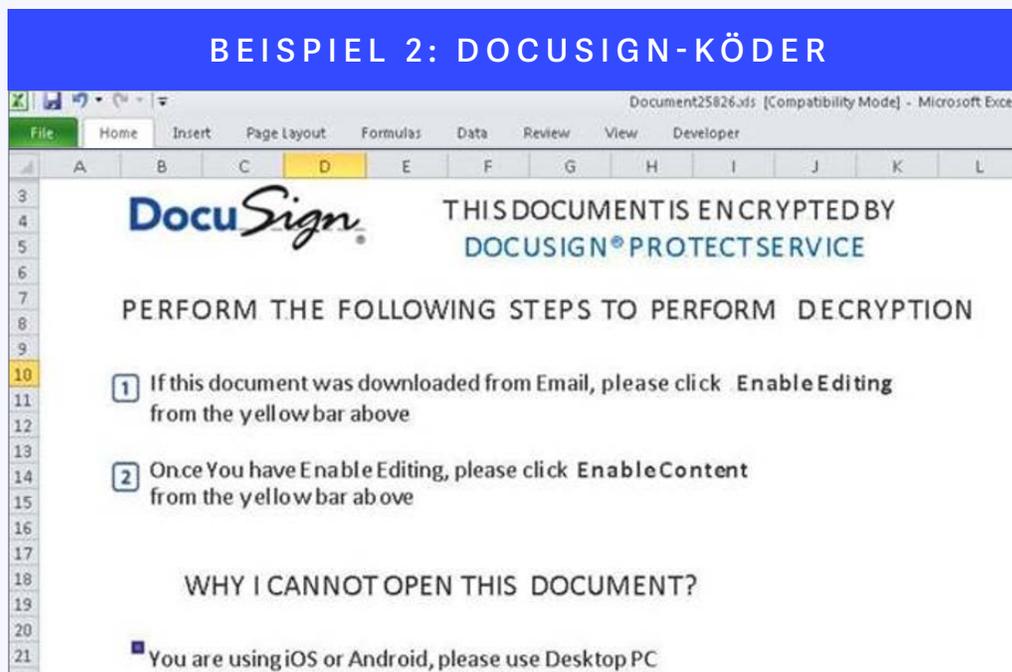
Total:	366.36

Banking-Trojaner – Qakbot

Qakbot ist ein weiterer Banking-Trojaner, der nach der Zerschlagung des Emotet-Botnets häufiger aufgetreten ist. Bislang haben wir im Jahr 2021 E-Mail-Köder-Varianten in verschiedenen Sprachen und mit zahlreichen unterschiedlichen Inhalten entdeckt, die diesen Trojaner verbreiten. Das unten abgebildete Beispiel aus Deutschland enthält einen Qakbot-Excel-Loader in der angehängten Zip-Datei.

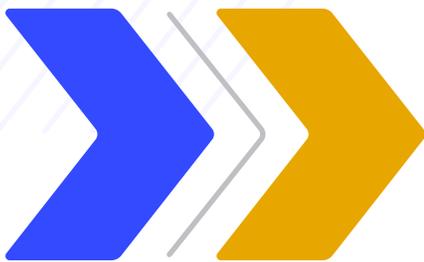
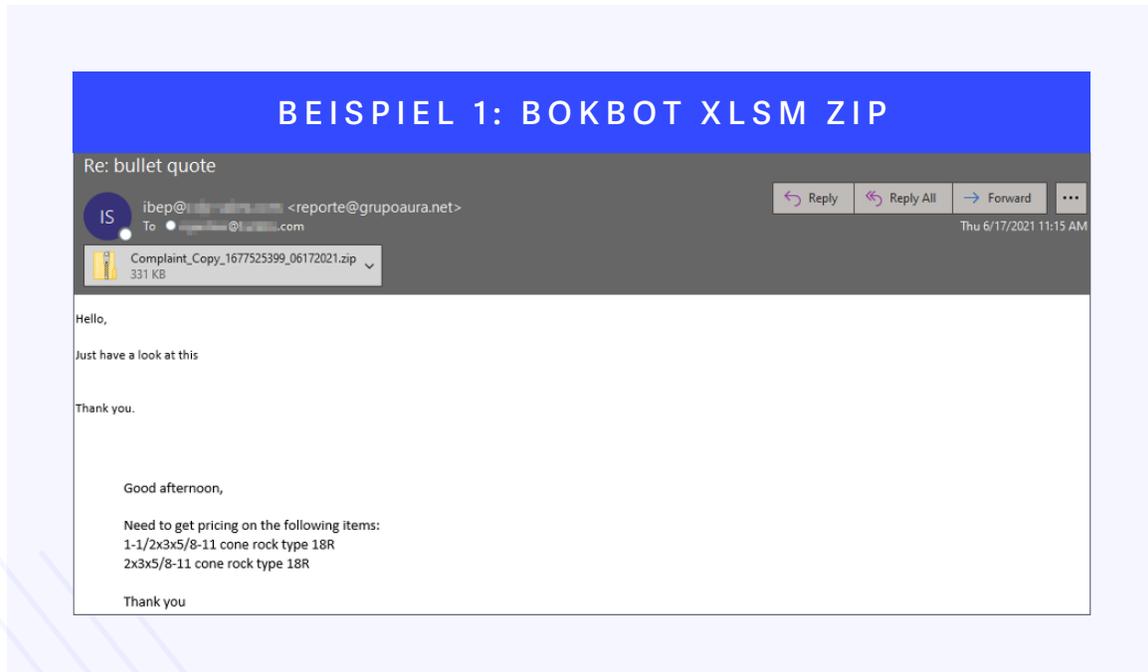


Sobald die Empfänger den Excel-Anhang extrahieren und ausführen, sehen sie einen DocuSign-Köder, der die Benutzer auffordert, die Bearbeitung und den Inhalt zu aktivieren, um die standardmäßig deaktivierten MS-Makros und die geschützte Ansicht zu umgehen. Durch die Aktivierung wird der Rechner infiziert.



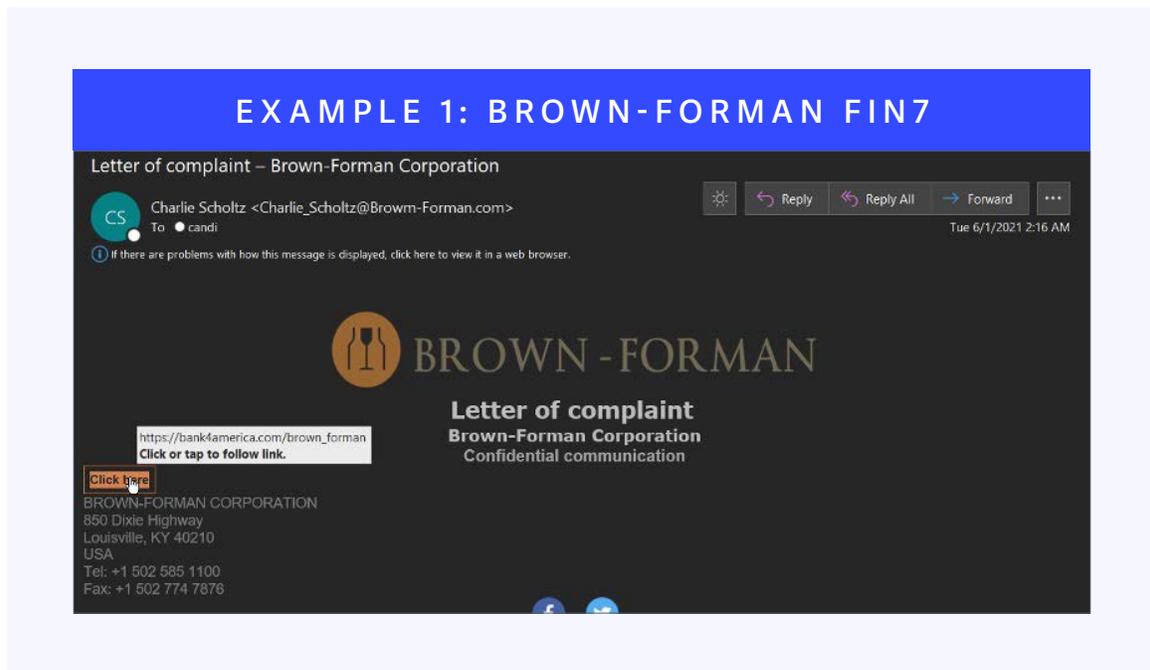
Banking-Trojaner – IcedID (BokBot)

IcedID hat sich von einem Banking-Trojaner zu einem Dropper für andere Malware weiterentwickelt. Die Zerschlagung von Emotet hat diese Entwicklung noch beschleunigt. Bei IcedID handelt es sich um eine modulare Malware, die es in der Vergangenheit auf die Finanzdaten und Anmeldeinformationen der Benutzer abgesehen hatte. Mittlerweile wird die Malware aber immer häufiger als Dropper für andere Malware eingesetzt. Dabei verwenden die Angreifer eine ZIP-Datei, die eine XLSM-Datei (makrofähige Excel-Datei) und Makros enthält, um die Malware zu übermitteln, da XLS-Dateien die bevorzugte Methode zur Datenübermittlung sind.



APT (Advanced Persistent Threat) Spotlight - FIN7 / JSSLoader RAT

FIN7 ist laut Wired eine [milliardenschwere Hackergruppe](#), die in der [Vergangenheit](#) schon mehrere hochkomplexe Angriffe durchgeführt hat. Die Gruppe ist einer der führenden APT-Angreifer, die es auf finanzielle Gewinne abgesehen haben. Eine kürzlich durchgeführte Reihe von Angriffen, die der Gruppe zugeschrieben wird, bestand aus Nachrichten, die als Beschwerdebrief der Brown-Forman Corporation getarnt waren. Die Nachricht forderte die Empfänger dazu auf, auf einen Link zu klicken, um die „vertrauliche Mitteilung“ abzurufen. Sind die Benutzer der Aufforderung gefolgt, wurden sie vom ursprünglichen Payload-Link zu einer Website umgeleitet, die ein Typosquatter der originalen Brown-Forman-Webseite war (Browm-Forman[.]com). Diese Webseite enthielt eine Seite mit der Schaltfläche „Beschwerde anzeigen“, die mit einer .xlsb-Datei (Excel mit binärer Arbeitsmappe) verlinkt war, die wiederum den [JSSLoader-Fernzugriffstrojaner](#) enthielt.



Remcos RAT – Steuerbetrug

Malware-Distributoren haben sich auch mit dem Thema Steuern beschäftigt. Hier haben wir ein Beispiel für Ransomware-Angriffe, die den Remcos RAT verwenden und eine Anfrage für eine Steuererklärung imitiert. Diese Angriffe hatten es ausschließlich auf Wirtschaftsprüfungsbüros abgesehen und ähneln einer Reihe von Attacken, die wir letztes Jahr um die gleiche Zeit beobachtet haben. Der E-Mail sind Bilder der Vorder- und Rückseite eines Führerscheins beigelegt, die mit dem Anzeigenamen und der E-Mail-Signatur des Absenders übereinstimmen. Die passwortgeschützte XLSB-Datei (Excel Binary File) setzt den Remcos RAT frei, nachdem das Passwort zum Öffnen der Datei verwendet wurde und die darin eingebetteten schädlichen Makros ausgeführt wurden.

Bei der Untersuchung stellte sich heraus, dass einige, wenn nicht sogar alle DL-Daten korrekt sind und es sich tatsächlich um eine echte Person handelt, deren Daten kompromittiert wurden. Die Bilder sind hochauflösend, aber wir konnten die Echtheit des Führerscheins nicht eindeutig überprüfen.

BEISPIEL 1: STEUERERKLÄRUNG

Request for Tax Service

Jennifer <postmaster@amarthomesfs.com>
To: recipient

Tax-Document.xlsx 46 KB
image1.jpg 100 KB
image2.jpg 101 KB

Good Day,

I would like to employ your tax services, please take a look at the last page of the attached VTR by carefully. I have about \$250,000-\$300,000 in income to myself personally and to my LLC that I have not yet paid taxes on. I am a SHARED of that there is no 1099 of any kind, it's purely me self-reporting. Do not count the 1099 from Square item including that amount in the self-reported income, as I explain. Very important not to double count that. I am also being all my existing tax documents for 2020, as well as my 2021 return (Due to the confidentiality of details, last document Password: 2021).

NOTE: I have not yet received any tax document from Artek, but I listed the income on the last page. I have also not yet received the 1099 from the 1 selected society for my LLC (\$250,000). You'll see there is a 1099 from them personally. There should be another one coming for the LLC.

Thank you—and please let me know if you have any questions! I know I will owe additional taxes this year, ugh...let's try to minimize as much as possible!

Thanks
Jennifer



Virginia DRIVER'S LICENSE FEDERAL LIMITS APPLY

Customer identifier
C1 0

Name
[REDACTED]

Address
[REDACTED] VA 2

Sex F Class D Date of birth [REDACTED] /1975

Eyes GRN Endorsements NONE Iss REN 11/30/2019

Height 5 FT 2 IN Restrictions C Exp 12/20/2027

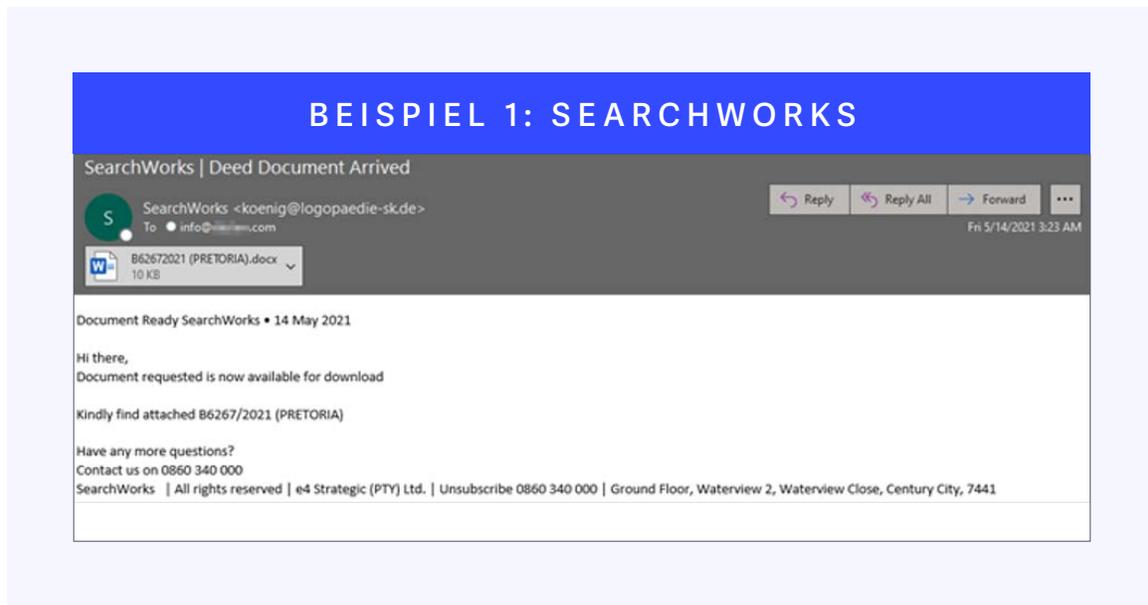
JK
Organ Donor
DD C 6

www.DMV.Nor.com

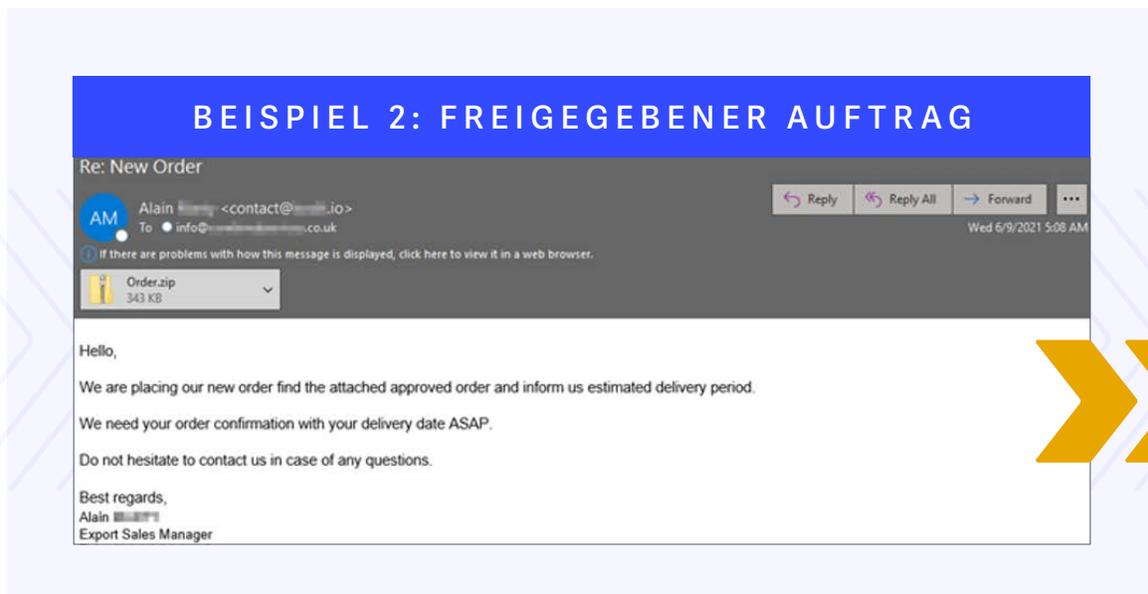
RAT – Formbook

Formbook-Malware, die für den Diebstahl vertraulicher Daten entwickelt wurde, breitet sich in diesem Jahr stark aus. Formbook wird seit 2016 als „Malware as a Service“ (MaaS) verkauft und ist leicht zugänglich. Malware-as-a-Service-Modelle sind äußerst besorgniserregend, da sie umfassenden Support und abgestufte Pakete bieten und es selbst Personen mit wenig oder gar keinem technischen Fachwissen ermöglichen, erheblichen Schaden anzurichten.

Bei den hier als Beispiel angeführten Angriffen wird das Personalvermittlungsunternehmen Search Works imitiert. Formbook wird dabei über Makros angehängt, die in eine als Urkunde getarnte DOCX-Datei eingebettet sind.



Andere Angriffe mit Formbook verbreiteten sich durch eine ZIP-Datei mit dem Titel „approved order“ (freigegebener Auftrag). Die ZIP-Datei enthält eine Datei, die den Rechner infiziert, sobald sie ausgeführt wird.



Snake Keylogger (404 Keylogger)

Die Malware Snake, die vertrauliche Daten der Benutzer abgreift, ist seit etwa 2012 auf dem Markt und verfügt über zahlreiche gefährliche Eigenschaften. Beispielsweise kann Snake sensible Daten des Opfers durch das Aufzeichnen von Tastatureingaben, das Erstellen von Screenshots und das Extrahieren von Informationen aus der Zwischenablage stehlen. Anfang dieses Jahres haben wir eine Reihe von Malware-Angriffen mit dem Namen „Payment Instruction“ (Zahlungsanweisung) beobachtet, bei der eine ausführbare Datei zur Verbreitung dieses Keyloggers verwendet wurde.



BEISPIEL 1: ZAHLUNGSANWEISUNG

RE: PAYMENT INSTRUCTIONS

Administration <administracion@...com>
To: sales@...co.uk

Outlook: blocked access to the following potentially unsafe attachments: **PAYMENT INSTRUCTIONS COPY.exe**

Dear Sir,

Pls Find Attached and confirm payment instruction copy.

We have wired the payment to your account twice and it returned to us.

Please confirm from the attached instruction if there are missing figures in account details and make corrections were necessary so

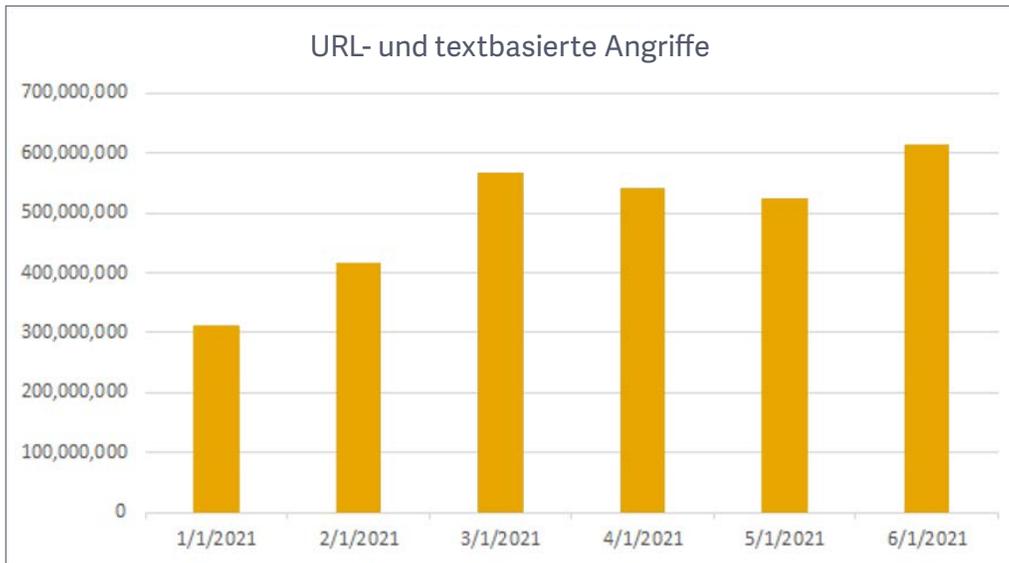
Der folgende Screenshot zeigt, dass die Angreifer etwas in diese ausführbare Datei gepackt haben, von dem wir vermuten, dass es sich um das Offline-Dinosaurierspiel von Google Chrome handelt. In der ausführbaren Datei gibt es Verweise auf „TRexUI“, „RunGameLogic“ und „JumpPressed“, was uns zu dieser Annahme führt. Die Tarnung von schädlichen ausführbaren Dateien als legitime Programme wie Spiele ist eine gängige Praxis.

BEISPIEL 2: VERPACKUNG IN EIN LEGALES PROGRAMM

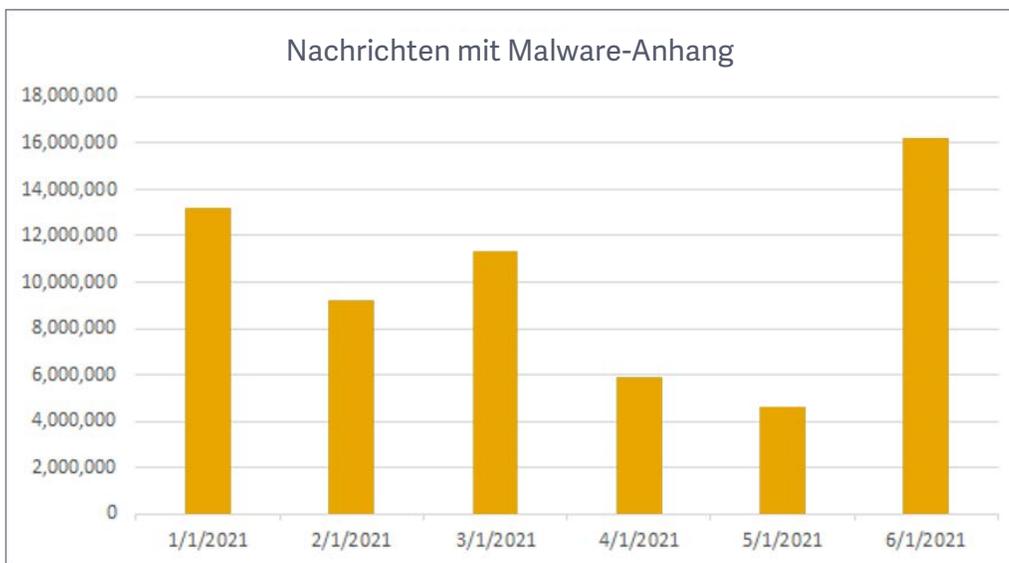
```
ateListOfTrackedObjects>b_4_0<>c__DisplayClass4_0<>c__Di
splayClass4_1<UpdateListOfTrackedObjects>b_1IEnumerable`
l Predicate`1 Stack`1 Comparison`1 List`1 obj1 CS<>S_loca
ls1 vl Int32 obj2 Vector2 v2<>9<Module> B CreateCompatibl
eDC ReleaseDC DeleteDC GetWindowDC TRexUI VK_ARROW_DOWN Sys
tem.IO KEYEVENTF_KEYUP VK_ARROW_UP CAPTUREBLT positionX KEY
EVENTF_EXTENDEDKEY SRCCOPY positionY value_ screenshotArea
mscorlib<>c hdc hdc PerSec RunGameLogic System.Collection
s.Generic nXSrc nYSrc hdcSrc currentId Thread Load Add spee
d dinosaurGroundedButNotCrouche speedFramesTracked CrouchP
ressed JumpPressed id yJumpingThreshold hWnd Find isTouchin
gGround CreateInstance keyCode set_Mode CipherMode get_BigE
ndianUnicode rawBGRAImage DetectObjectsInImage rawImage ima
ge BGRAImageToGrayscale IDisposable CheckAndMarkObstacle Is
PointObstacle Idle RuntimeTypeHandle GetTypeFromHandle Rect
angle Console WriteLine Adope ValueType ObjectType objectTy
pe System.Core get_Culture set_Culture resourceCulture GetG
rayscaleScreenCapture ScreenshotCapture Dispose RunUpdate c
```

Aktuelle Entwicklung

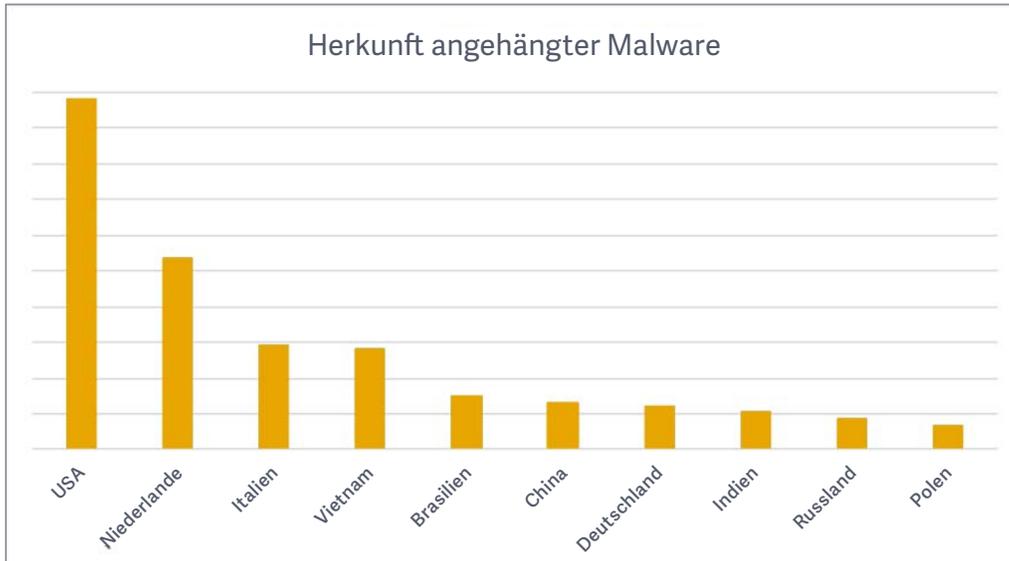
Die Gesamtzahl der E-Mail-Bedrohungen ist in der ersten Hälfte des Jahres 2021 gestiegen. Wir haben im ersten Halbjahr 2021 über 2,9 Milliarden E-Mail-Bedrohungen unter Quarantäne gestellt, was einem Anstieg von 13,5 % gegenüber den vorangegangenen sechs Monaten entspricht.



E-Mails mit Malware als Anhang waren in den ersten fünf Monaten des Jahres 2021 tendenziell rückläufig, bevor sie im Juni wieder anstiegen. Insgesamt haben wir in der ersten Jahreshälfte über 60 Millionen Nachrichten mit Malware im Anhang unter Quarantäne gestellt.



Die USA waren das am häufigsten auftretende Herkunftsland für E-Mails mit schädlichen Anhängen. Nachfolgend sind die zehn häufigsten Herkunftsländer für angehängte Malware im Jahr 2021 aufgeführt.



Nachfolgend finden Sie eine Auflistung der häufigsten Dateitypen von Malware-Anhängen, die von unseren Filtern in der ersten Jahreshälfte 2021 beobachtet wurden. Viele der unten aufgeführten Archivformate enthalten auch andere Dateitypen.

