Die gängigen Betreffs der aktuellen Angriffswellen mit Malware/SPAM/Phisihing …

Anmerkungen:

1. Nur eine kleine Stichprobe aus den Angriffsversuchen der letzten paar Tage:

2. Wir beobachten:
   a) Massenangriffe, die an sehr viele Kunden geschickt werden. Diese Angriffe sind jedoch technisch auf niedrigem Niveau, leicht zum Abfangen und die "Täuschung" ist leicht zu durchschauen.
   b) Wellen, die sich an spezielle Kundengruppen richten wie Krankenhäuser
   c) Einzelangriffe - gezielt an bestimmte Institutionen, Unternehmen und sogar User

3. Alle hier dargestellten Absender sind E-Mail-Adressen, welche aus den Mail-Header ausgelesen wurden.

   Diese können und werden auch immer wieder gefälscht sein. Zu beachten ist zusätzlich, dass nicht die E-Mail-Adressen sondern die Alias-Namen in der Vorschau der Mailprogramme wie Outlook angezeigt werden. Diese sind frei definierbar und werden gerne zur Täuschung eingesetzt.

Beispiel: gezielter Angriff mit MALWARE auf eine Institution - zum aktuellen Thema Corona & Pandemie

Eingang	Absender (Info aus dem Mailheader, kein Alias)	Betreff	Dateiname	Anlagen:	Scanstatus	Signaturname
31.03.2020	info@_infocompany.gq	**Re: COVID-19 Relief: How to Access Complimentary Products**	Covid-19 (2).001:SHETLAN.EXE	1	VIRUS(APT/IKARUS)	Win32.Outbreak
13.03.2020	8869-488-401440-1489-amt=amt.gv.at@mail.teddybear.rest	**The Natural Way To Fight The Pandemic**	http://bit.do/fu7Zh	0	VIRUS	URL-Category:malware

Beispiel: gezielter Angriff mit MALWARE auf die Buchhaltung einer Institution (kommt jedoch generell sehr oft vor)

gefälschte Anfragen, Angebote, Rechnungen, etc. werden noch immer als Täuschungsversuch angewandt und sind sehr verbreitet

Eingang	Absender (Info aus dem Mailheader, kein Alias)	Betreff	Dateiname	Anlagen:	Scanstatus	Signaturname
23.03.2020	vipecchi@gmail.com	**Re: re: proforma-Rechnung Überarbeitet im Februar um**	Scan-50% _swiftoutput098765456789.zip:Scan-50% _swiftoutput098765456789.exe	1	VIRUS	Trojan.Inject
25.03.2020	serajul@evincebd.com	**Payment**	PAYMENT SWIFT.PDF.r00:PAYMENT SWIFT.PDF.bat	1	VIRUS	Win32.Outbreak

Beispiel: andere gezielte Angriffe auf Firmen mit MALWARE

* Achtung! E-Mail-Adresse des Empfängers taucht im Betreff des Mails auf. Aus Datenschutzgründen wurde sie hier durch die fiktive Adresse office@kundendomain.at ersetzt.

Eingang	Absender (Info aus dem Mailheader, kein Alias)	Betreff	Dateiname	Anlagen:	Scanstatus	Signaturname
16.03.2020	donotreply@myexpresship.com	**Zurückgesandter Versandbeleg für * office@kundendomain.at**	Shipment Verification & Return Form.img:Shipment Verification & Return Form.exe	1	VIRUS(APT/IKARUS)	Win32.SuspectCrc
16.03.2020	donotreply@myexpresship.com	**Zurückgesandter Versandbeleg für * erwin.koch@kundendomain.at**	DHL-Express Shipment Receipts.img:Shipment Verification&Return Form_pdf.exe	01.01.1900	VIRUS	Win32.Outbreak

Beipiel: SPAMs zu aktuellem Thema Corona, Pandemie & Sicherheit

* Achtung! Name und Vorname des Empfängers wurde vom Angreifer auch in der Absenderadresse verwendet (ein gezielter Angriff auf eine bestimmte Person!)
Die beim Absender und Empfänger vorkommenden Namen und Vornamen wurden hier aus Datenschutzgründen durch frei erfundene ersetzt.
Auch die Domain des Kunden wurde durch den Platzhalter "kundendomain.at" ersetzt

Eingang	Absender	Empfänger	Betreff	Größe [KB]	Scanstatus
01.04.2020	* martin.koch@daily.com	* martin.koch@kundendomain.at	**dringend: Ihre Sicherheit ist wichtig**	33,64 KB	SPAM
01.04.2020	* werner.mueller@daily.com	* werner.mueller@kundendomain.at	dringend: Ihre Sicherheit ist wichtig	33,64 KB	SPAM
01.04.2020	* anton.schneider@daily.com	* anton.schneider@kundendomain.at	dringend: Ihre Sicherheit ist wichtig	33,65 KB	SPAM
01.04.2020	osterreich.noreply@naturvalencia.net	xxxxxxxxxx	**Coronavirus-Spezial: Brauchen Sie uns? Hier sind wir**	8,46 KB	SPAM
01.04.2020	osterreich.noreply@naturvalencia.net	xxxxxxxxxx	Coronavirus-Spezial: Brauchen Sie uns? Hier sind wir	8,48 KB	SPAM
01.04.2020	osterreich.noreply@naturvalencia.net	xxxxxxxxxx	Coronavirus-Spezial: Brauchen Sie uns? Hier sind wir	8,43 KB	SPAM
01.04.2020	ffayfk@rceip.com	xxxxxxxxxx	**Re: Thermometer & Surgical & KN95 Mask**	1,14 KB	SPAM
01.04.2020	bounce@heprii.si	xxxxxxxxxx	**Schutzmasken**	13,87 KB	SPAM
31.03.2020	bounce@heprii.si	xxxxxxxxxx	**DESINFEKATIONSMITTEL FÜR HÄNDE - LIEFERUNG BIS 7.4.2020**	50,89 KB	SPAM
30.03.2020	returnmail@sender-005.cafe24.com	xxxxxxxxxx	**(??) Are you looking for masks for COVID-19 Prevention?**	18,35 KB	SPAM
29.03.2020	hardhearted@enjoyshorts.icu	xxxxxxxxxx	**New Corona-virus Mask!**	11,95 KB	SPAM

30.03.2020	hvrtgiqh@wabl.com	xxxxxxxxxx	**Re: OEM medical equipment for you**	1,27 KB	SPAM

Beipiel: SPAMs, die Zweifel schüren sollen über die Sicherheit des eigenen Accounts

Eingang	Absender	Empfänger	Betreff	Größe [KB]	Scanstatus
31.03.2020	djanders@gctel.com	xxxxxxxxxx	**Hohe Gefahr. Ihr Konto wurde gehackt. Ändern Sie Ihr Passwort dringend.**	5,90 KB	SPAM
30.03.2020	bleached@creeps.net	xxxxxxxxxx	**Yoúr accoúnt has sígns of hackíng and blockíng. Please contact wíth Secúríty Department of khmistelbach.at**	9,41 KB	SPAM
30.03.2020		xxxxxxxxxx	**Delivery Status Notification (Failure)**	11,18 KB	SPAM

Beipiel: typische Massenwellen der letzten Tage

* Achtung! E-Mail-Adresse des Empfängers taucht im Betreff des Mails auf. Aus Datenschutzgründen wurde sie hier durch die fiktive Adresse office@kundendomain.at ersetzt.

Eingang	Absender	Empfänger	Betreff	Größe [KB]	Scanstatus
02.03.2020	uwtoxrb@iornades.de	xxxxxxxxxx	**CANNABIS OIL - Stellt es Knorpelgewebe und Gelenke wieder her**	167,84 KB	SPAM
02.03.2020	yqquwxj@maxiroll.art	xxxxxxxxxx	**Höhle der Löwen System macht Deutsche Bürger reich!**	256,23 KB	SPAM
29.03.2020	ihnyqzz@jolomas.art	xxxxxxxxxx	**Deutsche nutzen dieses einfache System, um durchschnittlich 450 /Tag zu verdienen und ihre Jobs zu kündigen!**	452,13 KB	SPAM
30.03.2020	odbicia@sth4u.com.pl	xxxxxxxxxx	*** office@kundendomain.at, wir schätzen Ihre Meinung | Nutzen Sie die aktive Reservierung**	29,72 KB	SPAM
30.03.2020	600708b6448949079be6464b1eb9e530_cd3489b5713bf2c0014892a011c39ab9_d8952ee82da0235e06f287e51095bbe8@imoniukatalogai.com	xxxxxxxxxx	**Kontaktdatenbanken in wenigen Minuten - ÖSTERREICH (2020-03-25) - 50% Rabatt**	70,98 KB	SPAM

Beipiel: "Die Hoffnung schüren" als SPAM-Thema

* Achtung! E-Mail-Adresse des Empfängers taucht im Betreff des Mails auf. Aus Datenschutzgründen wurde sie hier durch die fiktive Adresse office@kundendomain.at ersetzt.

Eingang	Absender	Empfänger	Betreff	Größe [KB]	Scanstatus
02.03.2020	kokuneva@haroldbray.gq	xxxxxxxxxx	**Wir bieten Geschäfts- und Privatkredite an**	0,78 KB	SPAM

ACHTUNG! Zur Erinnerung:

Viele Mailprogramme wie Outlook zeigen in der Vorschau zuerst nur den Alias-Namen des Absenders und **NICHT** die E-Mail-Adresse.
Solch ein gefälschter Alias-Name soll dem User suggerieren, dass das E-Mail von einem "legalen" und vertrauenswürdigen Absender kommt.