Bundeskriminalamt

BKA

Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie

Inhaltsverzeichnis

1. Die COVID-19-Pandemie in Deutschland – und im Cyberspace

Am 11.03.2020 stufte die Weltgesundheitsorganisation die Ausbreitung des Coronavirus (SARS-CoV-2 bzw. COVID-19) als globale Pandemie ein. Seitdem sind weltweit gravierende Auswirkungen auf nahezu alle Lebensbereiche spürbar: anfängliche Grenzschließungen, das umfassende Ausweichen auf Home-Office, die bundesweite Schließung von Schulen, das Kontakt- sowie Veranstaltungsverbot, Social Distancing, die Schließung von Gastronomiebetrieben und anderen Möglichkeiten der Freizeitgestaltung. Corona hat die Gesellschaft bis heute maßgeblich geprägt.

Der Branchenverband Bitkom fand in einer Umfrage[1] heraus, dass durch den Wegfall „analoger Angebote“ die Nutzung ihrer digitalen Pendants zunahm. Im Zuge der COVID-19-Pandemie wurde das Internet zum einen von der Bevölkerung verstärkt als Informationsquelle und Freizeitbeschäftigung genutzt, zum anderen haben die veranlassten Home-Office-Maßnahmen eine verstärkte Nutzung dieses Mediums zur Konsequenz. Vor allem Musik- und Videostreaming-Dienste wurden vermehrt genutzt. Ebenfalls eine logische Konsequenz des Social Distancing: der intensivere Gebrauch von Messengerdiensten, E-Mails und Social Media-Plattformen.

Die IT-Infrastruktur des Landes fungiert gerade in diesen Zeiten als eine grundlegende Säule für die Aufrechterhaltung der öffentlichen Ordnung und der Wirtschaftsprozesse. Sie gewährleistet sowohl den Austausch von Informationen zwischen Forschern und Medizinern als auch die Abwicklung von Versorgungsketten lebenswichtiger Waren und Güter.

Die Gesellschaft weicht im Zuge der Corona-Krise vermehrt auf die digitale Welt aus – ein perfekter Nährboden für Cyberkriminelle.

Cyberkriminelle fanden schnell einen Weg, um die Ausbreitung des Virus, die damit einhergehenden Sorgen und Unsicherheiten in der Bevölkerung sowie die vermehrte Nutzung von digitalen Angeboten für ihre Zwecke zu missbrauchen. Ob durch Phishing-Mails, DDoS-Attacken oder durch die Durchführung und Verbreitung von Desinformationskampagnen, es entwickelten sich zahlreiche neue Varianten für Cyber-Angriffe, welche alle als gemeinsamen Nenner die Corona-Krise als Narrativ ihrer Angriffe nutzten.

So viel vorweg: Bei den Tätern handelt es sich nach hier vorliegenden Erkenntnissen vielfach um bereits auf dem kriminellen Markt aktive Cyberkriminelle, die sich in den meisten bekannten Fällen etablierter Modi Operandi und Angriffsmethoden bedienen. Jedoch: Die verwendete „Geschichte“ hat sich den gesellschaftlichen Umständen angepasst. Die Täter nutzen eine hohe Bandbreite an „typischen“ Cyberangriffswerkzeugen und kombinieren diese mit einer für die Bevölkerung belastenden, emotional wirkenden Thematik.

[1] Abrufbar unter: https://www.bitkom.org/Presse/Presseinformation/Seit-Corona-Ausbruch-Online-Dienste-gefragt-wie-nie

2. Polizeiliche Meldungen

Im Zusammenhang mit der Covid-19-Pandemie vereinbarte das BKA mit den Landeskriminalämtern einen anlassbezogenen Meldedienst, bei dem das zahlenmäßige Aufkommen und Modi Operandi von Cybercrime-Straftaten gesammelt und analysiert werden.

Im Rahmen dieses polizeilichen Meldedienstes wurden bis zum 27.07.2020 folgende Fallzahlen übermittelt:

Bundesland	**CCieS**[2]	**CCiwS**[3]
Baden-Württemberg	8	6
Bayern[4]	32	46
Berlin	1	0
Brandenburg	0	1
Hamburg	0	9
Hessen[5]	3	3
Mecklenburg-Vorpommern	0	0
Niedersachsen	68	258
Nordrhein-Westfalen[6][7]	2	2
Rheinland-Pfalz	0	90

[2] Cybercrime im engeren Sinne: Ausspähen und Abfangen von Daten, Datenveränderung und -sabotage
[3] Cybercrime im weiteren Sinne umfasst Straftaten, bei denen IT-Systeme zur Planung, Vorbereitung und Ausführung verwendet wurden.
[4] Ein Fall kann dabei eine Vielzahl von zusammengehörenden Einzelvorgängen umfassen.
So wurden im Zusammenhang einer Corona-Phishing-Welle mit Stand Montag, 27.07.20, allein in Bayern rund 500 Sachverhalte angezeigt.
[5] Laut Pressemitteilung der Generalstaatsanwaltschaft Frankfurt am Main werden in Hessen über 50 Ermittlungsverfahren wegen des Verdachts von Straftaten im Zusammenhang mit Anträgen auf staatlich finanzierte „Corona-Soforthilfezahlungen“ geführt. Dies wird in der Statistik als ein Fall aufgeführt - siehe Fußnote 4.
[6] Einrichtung einer Ermittlungskommission zum Subventionsbetrug mit mehr als 100 eingegangenen Online-Anzeigen. Ermittlungsverfahren u.a. wegen des Verdachts des gewerbsmäßigen Betruges und des Ausspähens von Daten. Dies wird in der Statistik als ein Fall aufgeführt - siehe Fußnote 4.
[7] Einrichtung einer Ermittlungskommission – zentrale Ermittlungsführung im Zusammenhang mit den Fake-Webseiten zum Thema Corona-Soforthilfe. Siehe hierzu auch die Ausführungen auf der Folgeseite.
Mit Stand vom 27.07.2020 sind hierzu mehr als 1200 Strafanzeigen eingegangen.
Dies wird in der Statistik als ein Fall aufgeführt - siehe Fußnote 4.

Saarland	0	5
Sachsen	7	15
Sachsen-Anhalt	0	7
Schleswig-Holstein	17	34
Thüringen	3	1
Gesamtergebnis	**141 Fälle**	**471 Fälle**

Um eine einheitliche statistische Vorgehensweise zu gewährleisten, flossen verschiedene Sachverhalte als nur ein Verfahren in die obige Zählung ein, auch wenn teilweise Strafanzeigen im vierstelligen Bereich einem Tatkomplex zugeordnet werden konnten.

Das Land Nordrhein-Westfalen (NW) hat Anfang April 2020 eine Ermittlungskommission eingerichtet, die sich mit Fake-Seiten zum Thema Corona - Soforthilfe befasst. Die Staatsanwaltschaft Köln stuft dieses Verfahren als gewerbsmäßigen Betrug im Sinne des §263 StGB ein. Mit Stand vom 14.09.2020 sind bei der Polizei NW mehr als 1.200 Strafanzeigen zu dieser Thematik eingegangen.

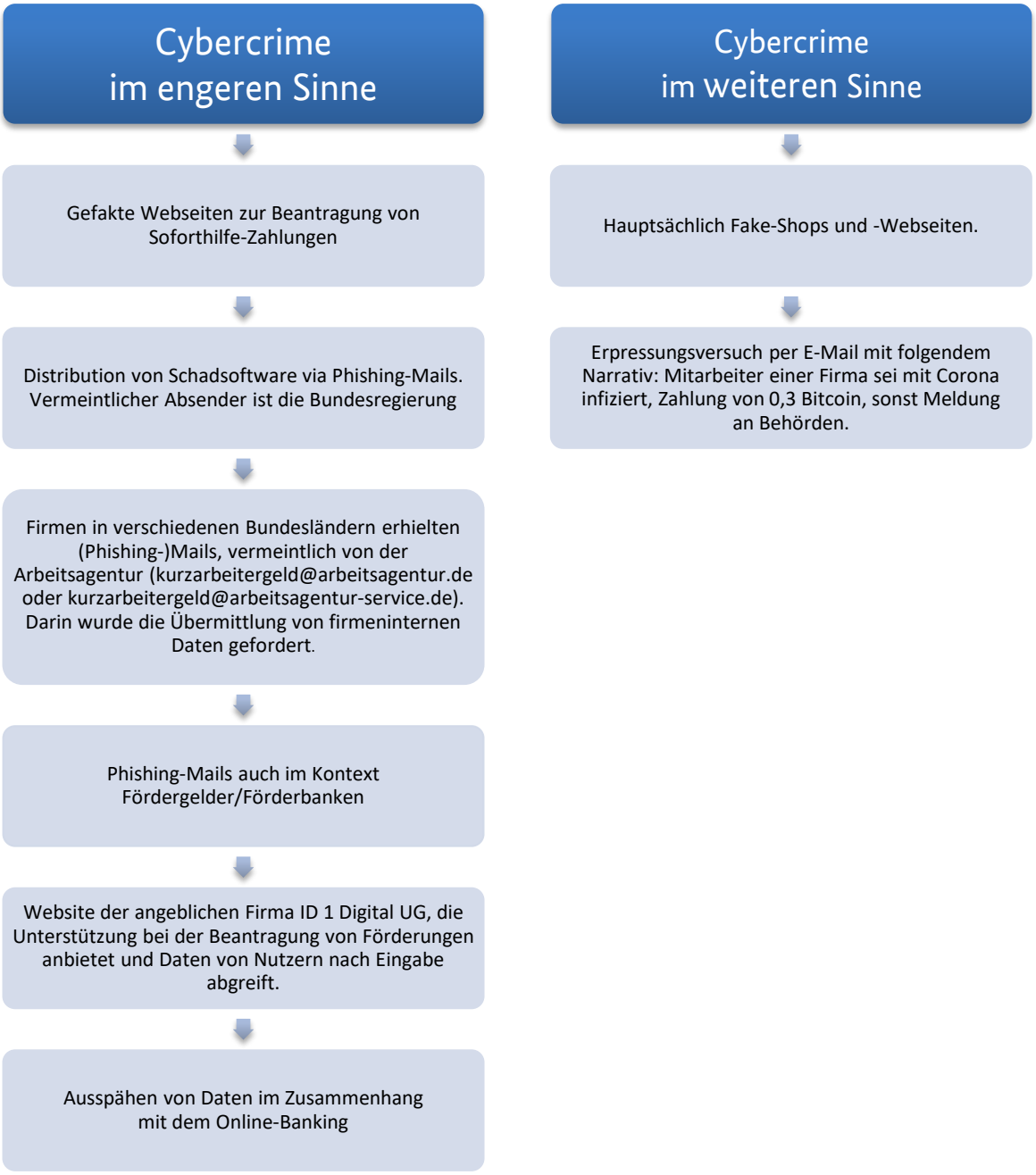
Das LKA NW richtete zudem eine Ermittlungskommission wegen Subventionsbetrugs-Delikten im Zusammenhang Corona-Soforthilfen ein. Hierzu gingen bisher mehr als 100 Online-Anzeigen ein.

Im Zusammenhang mit der Corona-Phishing-Welle wurden in Bayern mit Stand vom 27.07.2020 rund 500 Sachverhalte angezeigt.

Die Zulieferungen der Landeskriminalämter zeigen auf, dass es sich bei den gemeldeten Fällen schwerpunktmäßig um Cybercrime im weiteren Sinne handelt[8]. Die Betrugshandlungen im Zusammenhang mit der Beantragung der Corona-Soforthilfen und dem damit verbundenen kurzzeitigen Stopp der Auszahlungen in einigen Bundesländern sorgten dabei auch für ein hohes mediales Interesse.

[8] Aufgrund veränderter Erhebungsmodalitäten haben sich geringfügige Veränderungen bei den abgebildeten Fallzahlen im Vergleich zur vorherigen Berichterstattung ergeben.

Zu konkreten Phänomenausprägungen meldeten die Landeskriminalämter u. a. folgende Fallbeispiele:



3. Die primäre Bedrohung – Fake-Webseiten, Phishing und Malware Spamming

3.1 Betrug mittels gefälschter Corona-Soforthilfe-Webseiten

Im LKA NW gingen ab dem 08.04.20 vermehrt Anzeigen zu Fake-Webseiten ein, auf denen unbekannte Täter versuchten, Unternehmensdaten auszuspähen, um diese in der Folge für betrügerische Anträge auf Fördergelder einzusetzen. Genutzt wurde hierfür ein von den Tätern auf die Webseite gestelltes Formular, welches dem Originalantrag zur Erlangung der Fördergelder täuschend ähnlich sein sollte. Die Erfolgsaussicht der Täter wurde dadurch erhöht, dass bei einer Google-Suche nach „Soforthilfe NRW“ auch Links und Suchergebnisse erschienen, welche auf die gefälschten Seiten führten. Folgend ein Screenshot besagter Fake-Website:

Abbildung 1: Screenshot der Fake-Webseite zur NRW-Soforthilfe

Das LKA NW konnte im Zuge ihrer Ermittlungen mehrere Domains dieser Art identifizieren, die teilweise kurz nach Bekanntwerden des Sachverhalts durch sog. Abuse-Meldungen des LKA NW vom Netz getrennt werden konnten. Nach derzeitigem Stand gingen beim LKA NW mehr als 1.200 Online-Anzeigen in diesem Zusammenhang ein[9].

Aufgrund dieser massiven Betroffenheit setzte das nordrhein-westfälische Wirtschaftsministerium vorübergehend die Auszahlung von Corona-Soforthilfen für Selbstständige und Unternehmen aus. Die Bundesländer Baden-Württemberg, Hamburg und Sachsen meldeten ähnlich gelagerte Fälle.

[9] Siehe Seite 6

Das BKA als kriminalpolizeiliche Zentralstelle unterstützte die Ermittlungen der Länderdienststellen durch quervergleichende Abklärungen der technischen Spuren hinsichtlich möglicher Täteridentitäten. Ferner war einzukalkulieren, dass durch die unbekannten Täter weitere Phishing-Angriffe erfolgten bzw. beabsichtigt waren, sodass durch die zuständige Landespolizei präventivpolizeiliche Maßnahmen eingeleitet und fortgesetzt wurden.

Die Polizei in Berlin wurde im April 2020 von der dortigen Investitionsbank Berlin über eine Phishing-Webseite, die den Internetauftritt der Bank nachahmt (http://www.ibb.de), informiert. Die weiteren Ermittlungen ergaben, dass täterseitig über eine zusätzlich darüber verlinkte weitere Phishing-Seite[10] ein Online-Formular für die Beantragung von finanziellen Soforthilfen bereitgestellt wurde. Ziel dürfte die unberechtigte Erlangung von personenbezogenen Daten gewesen sein, um damit Folgestraftaten zu begehen.

Bezogen auf diesen Modus Operandi wurden weitere Ermittlungen in Nordrhein-Westfalen, Hamburg, Sachsen und Berlin geführt und durch das BKA als Zentralstelle unterstützt.

Auch international ist seit der COVID-19 -Pandemie die Anzahl an maliziösen Domains und betrügerischen Fake-Shops, welche zum Beispiel „Corona-Virus-Heimtests“ und andere gefälschte Waren anbieten, stark angestiegen.

Eine Auswertung durch TrendMicro[11] ergab, dass von 47.610 Aufrufen maliziöser Corona-spezifischen Domains ca. 9,8 Prozent aus Deutschland erfolgten. Ein Großteil dieser Aufrufe sei auf Spam-Mails zurückzuführen.

Unit42, Kooperationspartner von EC3[12], berichtet im Report „Studying How Cybercriminals Prey on the COVID-19 Pandemic”[13], dass im Zeitraum vom 01.01.2020 bis 31.03.2020 116.357 neu registrierte Domains mit Corona-Bezug identifiziert worden seien. Seit dem 12.03.2020 würden circa 3.000 Domains pro Tag registriert. Von diesen Domains seien 1,74 Prozent (2.022) eindeutig maliziös, während über ein Drittel (40.261) als hochriskant eingestuft würden. Die Anzahl an maliziösen bzw. „high-risk“ Domains sei den Untersuchungen zufolge im Zeitraum Februar und März 2020 um ca. 569 Prozent respektive 788 Prozent gestiegen.

Eine weitere Auswertung seitens Unit42 hinsichtlich der eindeutig maliziösen Domains habe ergeben, dass circa 16 Prozent für Phishing-Angriffe und zum Abgreifen von Nutzerdaten verwendet, während 84 Prozent zum Hosten verschiedener Malware genutzt würden.

[10] http://www.corona-zuschuss-ibb.de/
[11] Erhebungszeitraum: 01.01. – 31.03.2020; online abrufbar unter: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
[12] European Cybercrime Centre von EUROPOL
[13] https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/

3.2 Bundesweite Phishing-Kampagne mit Corona-Bezug

Seit dem 04.05.2020 wurden dem BKA von mehreren Bundesländern Corona-Phishing-Fälle im Zusammenhang mit den Investitionsbanken diverser Bundesländer gemeldet.

Durch die Täter wurden unter Verwendung der E-Mail Adresse „corona-zuschuss@forderbank.de.com“, wobei „Förderbank“ durch die Domain der jeweiligen Landesförderbank ausgetauscht wird (also z.B. corona-zuschuss@ibb.de.com für die Investitionsbank Berlin), Phishing-Mails distribuiert. Bei Aufruf der betrügerischen E-Mail-Domain erfolgte eine Weiterleitung auf die legitimen Webseiten der jeweiligen Förderbanken bzw. der Bundesländer, um Authentizität vorzutäuschen.

In den übersendeten Phishing-Mails wurde eine Drohkulisse hinsichtlich einer Rückförderung von Fördergeldern aufgebaut und das angeschriebene Opfer aufgefordert, Unternehmensdaten für eine Übermittlung an das Finanzamt auszufüllen. In einem zweiten Schritt erfolgte durch die Täter dann die Übermittlung von Kontodaten, auf welche die überschüssig gezahlten Fördergelder zurücküberwiesen werden sollen.

Durch die LKÄ wurden auch in Zusammenarbeit mit verschiedenen Handelskammern entsprechende Warnmeldungen sowohl auf den Webseiten der Förderbanken als auch im Rahmen von Social Media Postings und Pressemitteilungen veröffentlicht.

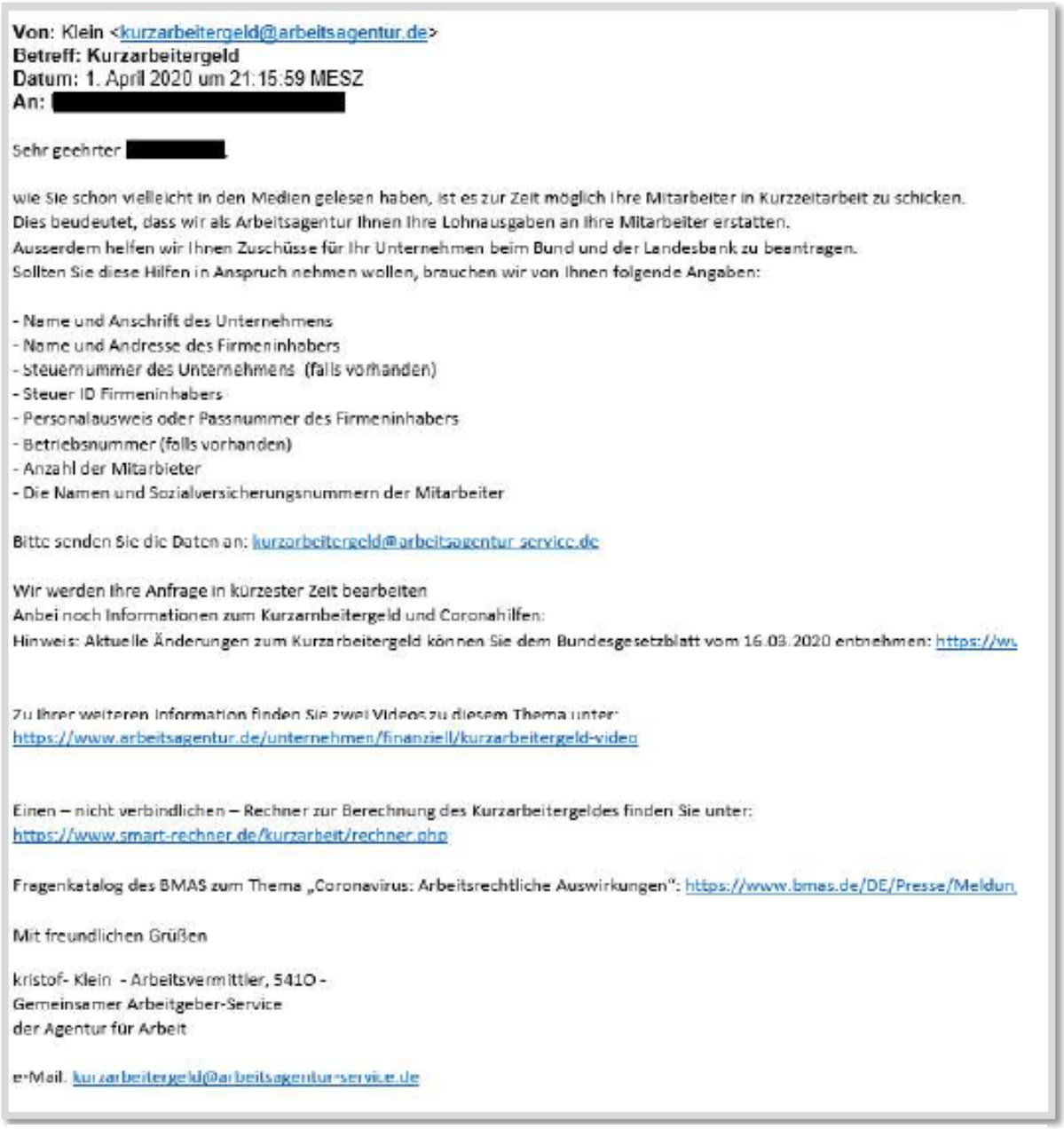
Mehrere Bundesländer sowie das BKA gaben zu diesem Modus Operandi Warnmeldungen heraus.

Im weiteren Verlauf der Ermittlungen wurde bekannt, dass die Schäden, welche im Kontext der Corona-Soforthilfen gemeldet wurden, mit überwiegender Mehrheit dem Subventionsbetrug zuzuordnen sind. Alleine in Berlin ist der dadurch entstandene Schaden auf circa 3,2 Millionen Euro zu beziffern.

Finanzielle Schäden, die durch Phishing-Mails bzw. Fake-Webseiten entstanden, bewegen sich – im Vergleich zum klassischen Subventionsbetrug – im niedrigen Bereich.

3.3 Malware Spamming (Malspam)

Seit Beginn der Covid-19-Pandemie wurden seitens verschiedener Cybercrime-Gruppierungen mehrere Spam- und Phishing-Kampagnen mit internationalem Charakter generiert. Vermeintliche Absender sind Behörden (WHO, Gesundheitsministerium etc.), Dienstleister (Paket- und Lieferdienste) oder als vertrauenswürdig geltende Berufsgruppen (Ärzte, Virologen).
Die Narrative der Phishing-Mails sind dabei auf Unsicherheit, Neugier und das hohe Informationsbedürfnis in der Bevölkerung zugeschnitten. Ziel des Phishings ist dabei, mittels gefälschter Homepages, maliziösen Dokumenten und Schadsoftware an digitale Identitäten bzw. monetäre Mittel zu gelangen. Folgendes Beispiel für derartiges Phishing wurde durch die Behörden des Cyber-AZ identifiziert:



Von: Klein <kurzarbeitergeld@arbeitsagentur.de>
Betreff: Kurzarbeitergeld
Datum: 1. April 2020 um 21:15:59 MESZ
An: [redacted]

Sehr geehrter [redacted]

wie Sie schon vielleicht in den Medien gelesen haben, ist es zur Zeit möglich Ihre Mitarbeiter in Kurzzeitarbeit zu schicken.
Dies beudeutet, dass wir als Arbeitsagentur Ihnen Ihre Lohnausgaben an Ihre Mitarbeiter erstatten.
Ausserdem helfen wir Ihnen Zuschüsse für Ihr Unternehmen beim Bund und der Landesbank zu beantragen.
Sollten Sie diese Hilfen in Anspruch nehmen wollen, brauchen wir von Ihnen folgende Angaben:

- Name und Anschrift des Unternehmens
- Name und Andresse des Firmeninhabers
- Steuernummer des Unternehmens (falls vorhanden)
- Steuer ID Firmeninhabers
- Personalausweis oder Passnummer des Firmeninhabers
- Betriebsnummer (falls vorhanden)
- Anzahl der Mitarbieter
- Die Namen und Sozialversicherungsnummern der Mitarbeiter

Bitte senden Sie die Daten an: kurzarbeitergeld@arbeitsagentur-service.de

Wir werden Ihre Anfrage in kürzester Zeit bearbeiten
Anbei noch Informationen zum Kurzarbeitergeld und Coronahilfen:
Hinweis: Aktuelle Änderungen zum Kurzarbeitergeld können Sie dem Bundesgesetzblatt vom 16.03.2020 entnehmen: https://w

Zu Ihrer weiteren Information finden Sie zwei Videos zu diesem Thema unter:
https://www.arbeitsagentur.de/unternehmen/finanziell/kurzarbeitergeld-video

Einen – nicht verbindlichen – Rechner zur Berechnung des Kurzarbeitergeldes finden Sie unter:
https://www.smart-rechner.de/kurzarbeit/rechner.php

Fragenkatalog des BMAS zum Thema „Coronavirus: Arbeitsrechtliche Auswirkungen": https://www.bmas.de/DE/Presse/Meldun

Mit freundlichen Grüßen

kristof- Klein - Arbeitsvermittler, 5410 -
Gemeinsamer Arbeitgeber-Service
der Agentur für Arbeit

e-Mail. kurzarbeitergeld@arbeitsagentur-service.de

Abbildung 2: Screenshot einer typischen Phishing-Mail

Das CERT-EU[14] berichtete am 21.04.2020[15], dass beobachtete Phishing-Attacken hauptsächlich die Corona-Narrative als Inhalt der Betreffzeilen verwenden. Gerade zu Beginn der Corona-Krise konnte ein massiver Anstieg an Malspam verzeichnet werden. Ab April allerdings sank die Anzahl bereits wieder und stabilisierte sich in den Folgewochen auf ein „durchschnittliches" Niveau – im Mai und Juni sank die Anzahl der Malspam-Flut noch weiter.

Google meldete am 16. April 2020, dass das Unternehmen pro Tag circa 240 Millionen Spam-Mails und pro Woche circa 18 Millionen Phishing-Mails mit Corona-Narrativen blockiere.[16]

Auch die Anzahl der identifizierten Malware-Familien, welche in spezifischen, auf die Corona-Pandemie angepassten Kampagnen eingesetzt wurden, weist einen ähnlichen Verlauf auf. In der Abbildung[17] unten ist die summierte Häufigkeit der erkannten Malware-Familien dargestellt. Auch hier war zunächst ein starker Anstieg an identifizierten Malware-Familien im März/Anfang April erkennbar, ehe sich diese Zahl ab Ende April auf einem hohen Niveau stabilisierte.

Phishing-Mails der während der Corona-Krise gestarteten Kampagnen enthielten häufig Office-Dokumente, welche als Dropper für Schadsoftware dienten - darunter auch die bekannten und sehr gefährdungsrelevanten Malware-Familien *Emotet*[18], *Agent Tesla*[19] und *Trickbot*[20].

Als Narrative für die Distribution in Deutschland wurden z.B. Antragsformulare für „Familien- und Krankenurlaub" verwendet – als angeblicher Absender wurde das Bundesgesundheits-ministerium[21] verwendet.

[14] Computer Emergency Response Team der EU – zuständig für die Sicherheit aller Netze der EU-Institutionen, Agenturen und Einrichtungen
[15] https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-2020Q1-Threat_Landscape_Report-Executive-Summary-v1.0.pdf
[16] https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
[17] COVID 19 Cyber-Bulletin #10
[18] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/covid-19-malware-makes-hay-during-a-pandemic/
[19] Unit42 bestätigt die Distribution von AgentTesla: https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/
[20] Cyberreason: JUST BECAUSE YOU'RE HOME DOESN'T MEAN YOU'RE SAFE; 18.03.2020; https://www.cybereason.com/blog/just-because-youre-home-doesnt-mean-youre-safe
[21] https://www.heise.de/newsticker/meldung/Warnung-vor-Phishing-Mails-mit-Antragsformular-Familien-und-Krankenurlaub-4701426.html

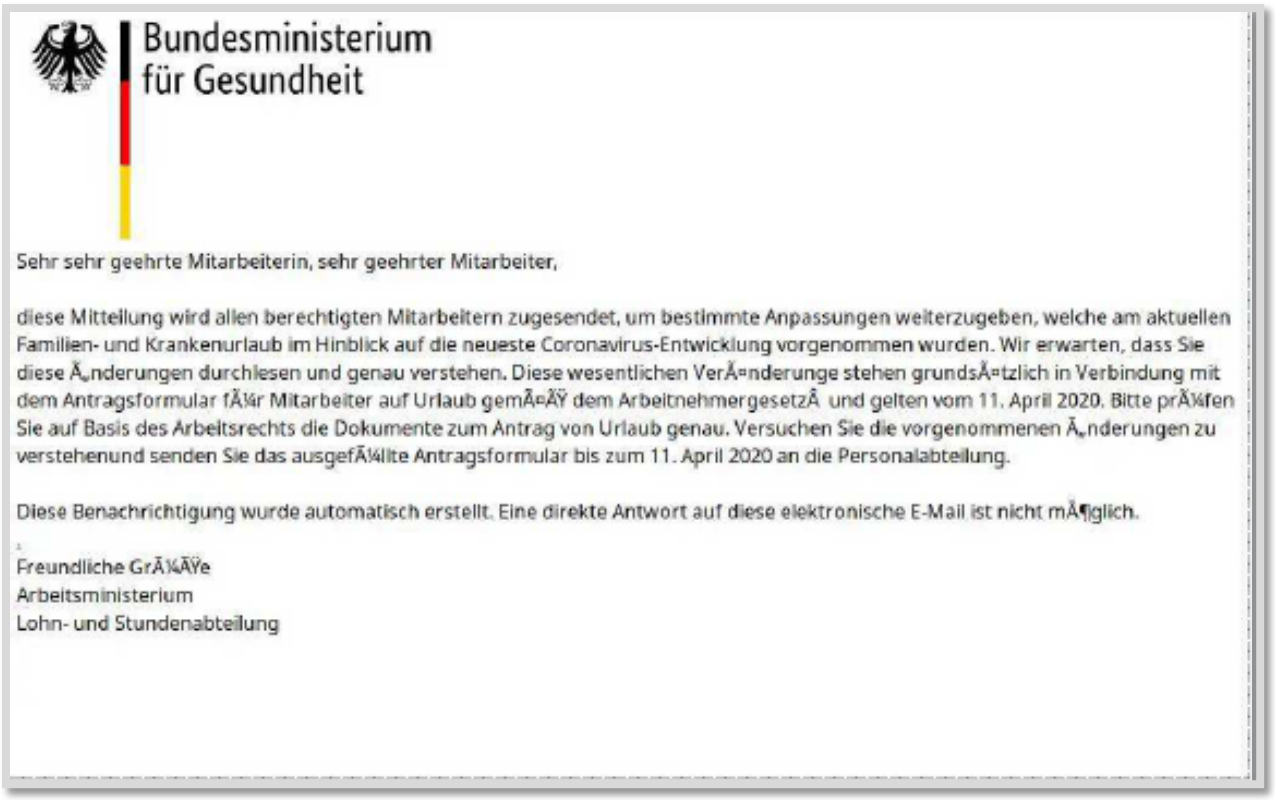


Abbildung 3: Screenshot einer Spam-Mail, in welcher sich der Absender als das Bundesministerium für Gesundheit ausgibt. Narrativ ist ein angeblich neues Urlaubsformular.

Auf ihrem Dashboard[22] veröffentlichen die IT-Sicherheitsforscher von McAfee weitere dort identifizierten Informationen hinsichtlich Cyberangriffen mit COVID-19-Bezug. Demnach wurden im Zeitraum Januar bis Juli 2020 ca. 1,5 Millionen Angriffe mit COVID-19-Narrativen aufgezeichnet, 95.311 davon in Deutschland. Weitere Angaben seitens McAfee legen nah, dass Deutschland im Allgemeinen eines der am häufigsten betroffenen Länder hinsichtlich derartiger Attacken sei.

Auf europäischer Ebene warnte Europol (EC3) vor verschiedenen, möglichen Angriffsvektoren im Zuge der Corona-Pandemie, allen voran der Verbreitung von Fake-Apps oder der Kompromittierung von Webseiten via DNS-Hijacking. In diesem Zusammenhang wurde zudem über die steigende Distribution von Malware (z.B. AZORult), welche über das Aufrufen von inkriminierten Corona-Virus-Dashboards gestreut wird, berichtet. Ziel ist es, Daten wie Passwörter, Kreditkarteninformationen und Usernamen sozialer Medien auszuspähen. Nachfolgend ein Beispiel für ein derartiges Dashboard[23]:

[22] https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html
[23] Abrufbar unter: coronavirus.jhu.edu/map.html

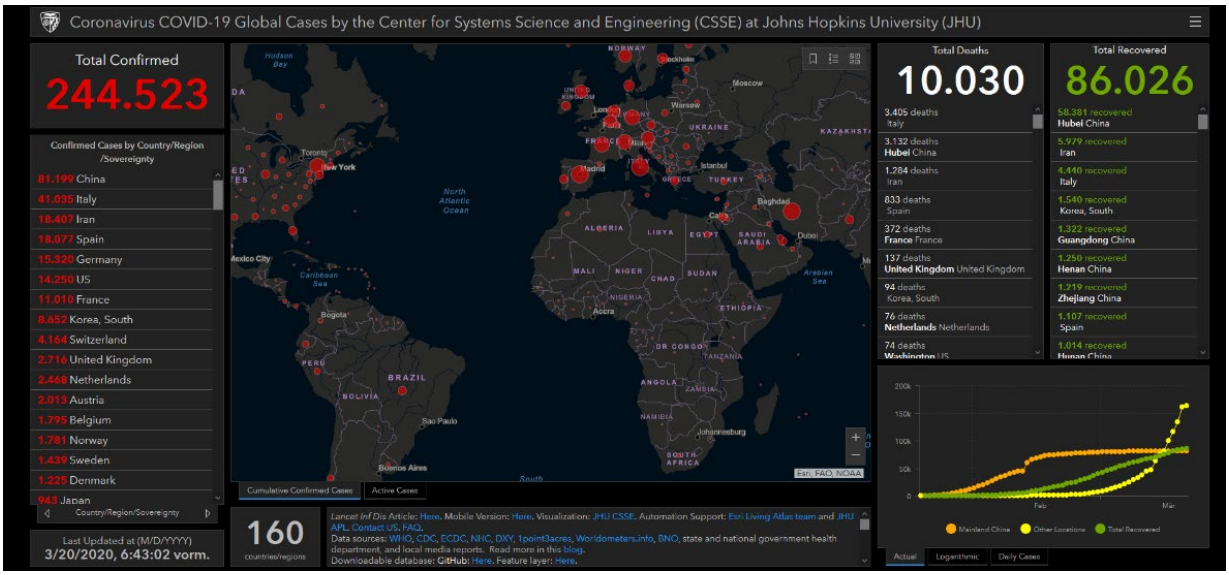


Abbildung 4: Corona-Dashboard – siehe Fußnote 23

Darüber hinaus wurden im Darknet Phishing-Betrugskampagnen beworben, die darauf abzielen, illegitime und maliziöse Apps im Sinne von „Coronavirus Maps“ zu verbreiten[24].

Das CERT-EU gab an, keinen Anstieg an erfolgreichen Cyberangriffen auf EU-Institutionen festgestellt zu haben. Global seien staatliche Akteure und gezielte Infiltrationen in IT-Systeme von Gesundheitseinrichtungen zu verzeichnen. Ebenfalls warnt das CERT-EU vor Desinformationskampagnen via Twitter.

Anfang April veröffentlichte das CERT-US in Zusammenarbeit mit dem US Department of Homeland Security, der Cybersecurity and Infrastructure Security Agency und dem National Cyber Security Centre (NCSC/UK) eine gemeinsame Warnung hinsichtlich möglicher Cyberangriffe im Zuge der Corona-Pandemie[25]. In dem Report warnten die Behörden vor den „typischen“ Angriffsmustern seitens APT[26] und Cyberkriminellen, namentlich Phishing, Malware-Distribution, maliziöse Domains sowie Angriffe auf Telearbeit-Infrastrukturen (z.B. via Remote-Zugriff). Auch diese Behörden warnten vor dem „Corona-Narrativ“, welches das Informationsbedürfnis der Bürger ausnutzt. Im Bereich des Phishings (auch über mobile Endgeräte) wurde konkret vor Mails und SMS mit folgenden Betreffen gewarnt:

- 2020 Coronavirus Updates
- Coronavirus Updates
- 2019-nCov: New confirmed cases in your City
- 2019-nCov: Coronavirus outbreak in your city (Emergency)

[24] EC3
[25] https://www.us-cert.gov/ncas/alerts/aa20-099a
[26] Advanced Persistent Threats – hochprofessionelle Gruppierungen mit besonders hohen Ressourcen-Kapazitäten

Das NCSC/UK identifizierte weiter diverse E-Mails, welche zur Verbreitung des Info-Stealers AgentTesla genutzt werden. Andere Kampagnen beinhalten Excel-Dateien mit DLL-Funktion[27], welche die Malware-Varianten Get2Loader und GraceWire herunterladen.

Interpol warnte indes vor möglichen Tatgelegenheiten (Phishing, Spam-Mails, Betrug etc.) und Ransomware-Angriffen auf mit der Bekämpfung der Covid-19-Pandemie beauftragten Infrastrukturen wie Krankenhäuser und Behörden. Konkret konnte bei Interpol die massive Verbreitung des Android-Trojaners *Cerberus* festgestellt werden.

[27] Dynamic Link Library: Eine Sammlung von Programmen und Funktionen, welche bei Bedarf über ein anderes Programm (hier Excel) aufgerufen und ausgeführt werden können.

5. Auswirkungen der COVID-19-Pandemie auf die Darknet-Szene

Allgemeine Handels- und Markbeschränkungen beeinflussten auch den illegalen Darknet-Handel, was zu Anpassungen bei inkriminierten Angeboten führte:

- Durch die Ausgangs- und Reisebeschränkungen und die damit zusammenhängenden Logistik- und Lieferschwierigkeiten stiegen generell die Verkaufspreise der Waren.
- Der Versand wurde von einigen Vendoren auf das Inland beschränkt.
- Aufgrund der Kontaktbeschränkungen und der verhängten Ausgangssperren nahm der Fußgängerverkehr ab, so dass die für den Versand der inkriminierten Güter notwendige Nutzung von Einwurfbriefkästen mit einem erhöhten Entdeckungsrisiko verbunden war.

Generell reagierten die auf den illegalen Marktplätzen vertretenen Vendoren aber heterogen und abhängig von lokalen Begebenheiten.

Auch wenn einige Vendoren den Verkauf von Waren mit Beginn der Corona-Krise einstellten, war die Lieferung von Waren aus dem Darknet jederzeit möglich.

Bereits zu Beginn der COVID-19-Pandemie wurde ersichtlich, dass nicht nur im Clearnet, sondern auch im Darknet in betrügerischer Absicht eine große Bandbreite von Waren und Tutorials mit Corona-Bezug angeboten wurden: Atemschutzmasken, angebliche Antikörper-Schnelltests, Anti-Malaria-Medikamente, Medikamente zur Stärkung des Immunsystems oder Impfstoffe. Dies umfasste jedoch auch Anleitungen zur Begehung von Betrugsdelikten und zur Erlangung wirtschaftlichen Profits aus der Krise. Ähnlich wie im Clearnet konnte auch im Darknet ein erhöhtes Aufkommen an Betrugsseiten festgestellt werden.

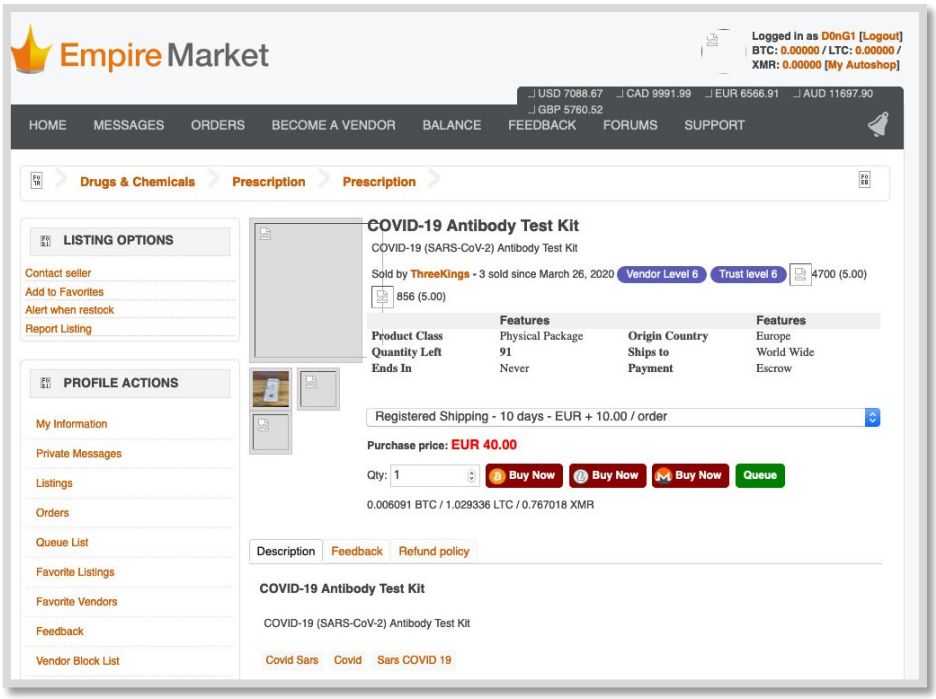


Abbildung 5: Im Darknet zum Verkauf angebotener, angeblicher Antikörper-Test für COVID-19

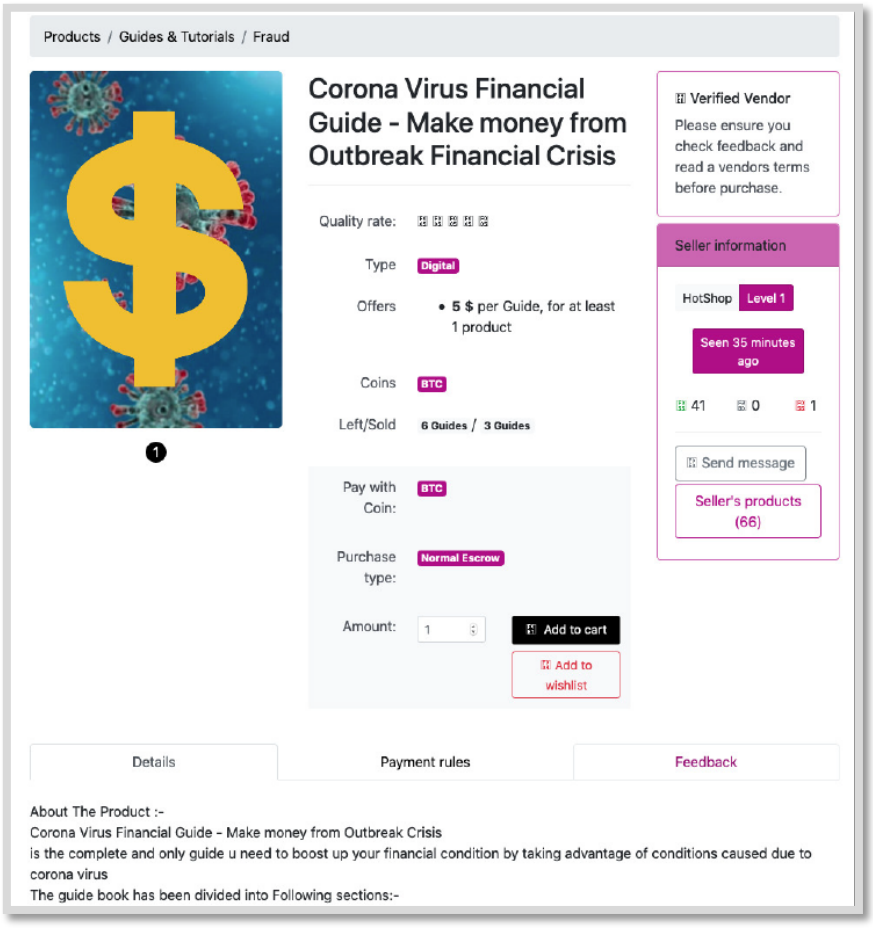


Abbildung 6: Im Darknet angebotener "Corona Virus Financial Guide"

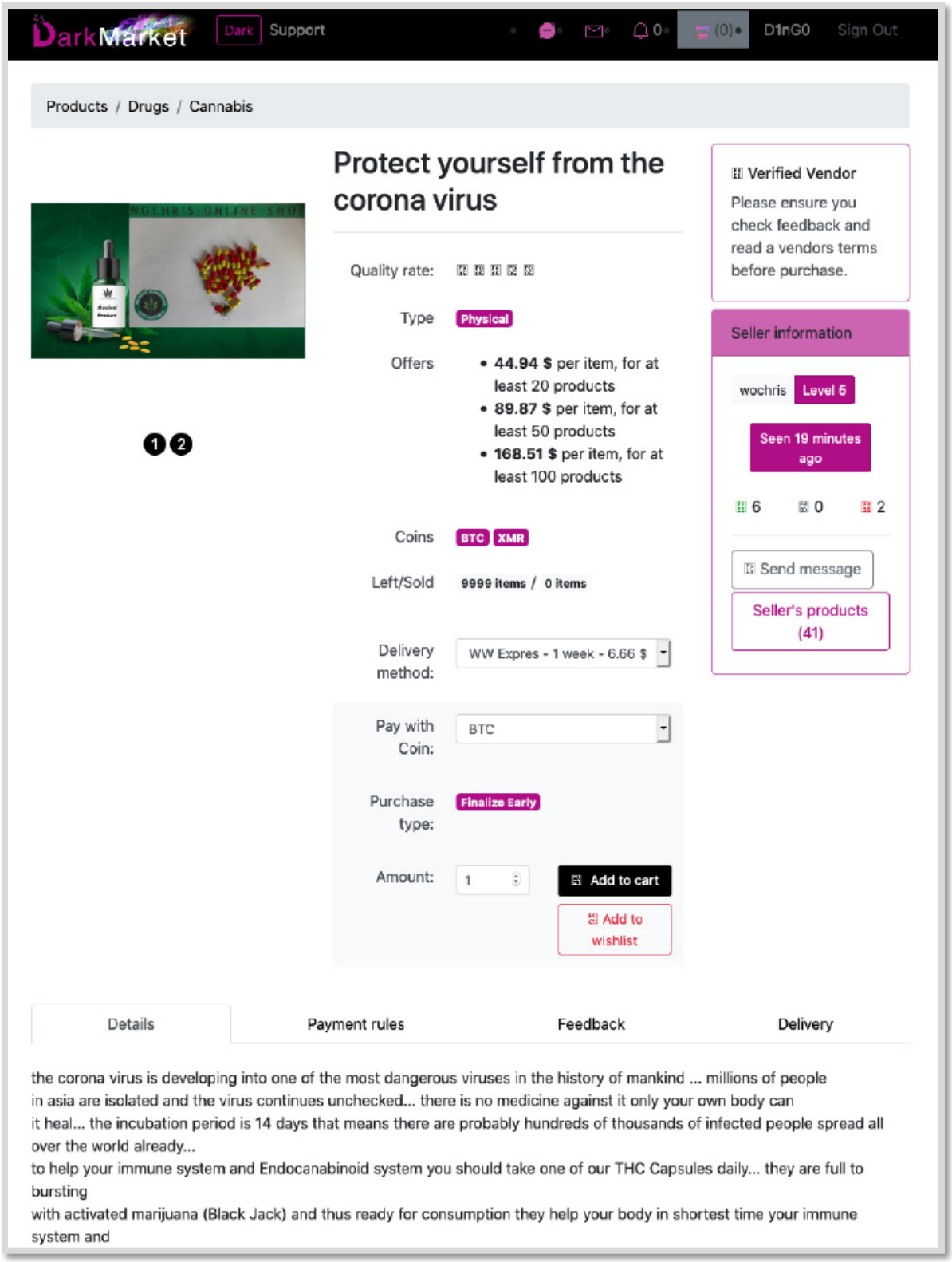


Abbildung 7: Im Darknet angebotene Arznei zum Schutz gegen COVID-19

6. Zahlungskartenkriminalität

Sowohl laut polizeilicher als auch externer Quellen bewegten sich der sogenannte „card not present fraud / CNPF“[28] auf einem gleichbleibend hohen Niveau. Signifikante Veränderungen zu Zeiten vor COVID-19 waren nicht feststellbar.

Zunächst war ein genereller Rückgang von Zahlungskarten-Transaktionen feststellbar, was im Zusammenhang mit den Ausgangsbeschränkungen und vieler geschlossener Geschäfte/Betriebe nicht überraschte.

Außerdem war eine erhöhte Anzahl von Geldautomatentransaktionen zu verzeichnen. Ursächlich hierfür dürfte die zur Anfangszeit der Pandemie festgestellte „Flucht“ ins Bargeld“ sein, wobei betrügerische Transaktionen in diesem Zusammenhang nicht bekannt wurden.

Die auch für dieses Jahr geplanten, internationalen Kontrolltage im Bereich der Zahlungskartenkriminalität von EUROPOL/EC3 unter dem Schirm von EMPACT[29] wurden aufgrund der Covid-19-Pandemie abgesagt. Diese Kontrollaktionen finden jedes Jahr statt und befassen sich mit dem betrügerischen Einsatz von Kreditkartendaten und CNPF. Der Ausfall dieser Aktionen könnte nach Einschätzung des zuständigen BKA-Fachbereichs deutliche Auswirkungen auf die Bekämpfung des Kriminalitätsphänomens haben.

[28] Eine Transaktion, bei der der Karteninhaber die Zahlungskarte nicht physisch vorlegen muss
[29] European Multidisciplinary Platform Against Criminal Threats = EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität

7. Home-Office als Stresstest – DDoS-Angriffe

Die eingangs bereits erwähnten Folgen der Corona-Pandemie für die Gesellschaft sorgten für einen deutlichen Anstieg des Home-Office – und damit des Datenverkehrs in Deutschland. Der deutsche Internetknoten DE-CIX verzeichnete einen Anstieg von 10 Prozent bzgl. der Gesamtdatenrate gegenüber dem Niveau vor Beginn der COVID-19-Pandemie.

Auch wenn ein Engpass aufgrund ausreichender Reservekapazitäten seitens der Provider nicht zu erwarten war, boten das Home-Office und die damit zum kritischen Element gewordenen VPN-Server attraktive Angriffsziele für Cyberkriminelle.

Vor diesem Hintergrund bedarf es laut des IT-Sicherheitsdienstleisters Link11, Mitglied des German Competence Centers G4C e.V., „nur geringen Aufwands, um Server und Online-Dienste (...) zu überlasten und, je nach Ausgestaltung des Angriffs, einen VPN-Server oder eine Firewall zum Absturz zu bringen“. Dadurch steige die Gefahr, mit einem relativ einfach auszuführenden DDoS-Angriff alle Mitarbeitenden eines Unternehmens gleichzeitig an ihrer Arbeit zu hindern.

DDoS-Angriffe (oder deren Androhung) erhielten während der durch die Pandemie forcierten Home-Office-Maßnahmen insgesamt ein höheres Bedrohungspotenzial.

Link11 fasst die Bedrohungslage durch DDoS-Angriffe während der Corona-Krise wie folgt zusammen:

- Im ersten Quartal 2020 betrug die größte Angriffsbandbreite 406 Gbps.
  Dies ist ein Zuwachs von 81 Prozent im Vergleich zum ersten Quartal 2019.
- Die durchschnittliche Bandbreite der Angriffe im ersten Quartal 2020 betrug 5,0 Gbps, im ersten Quartal 2019 4,3 Gbps.

Auch das BSI stellte eine gestiegene Intensität von DDoS-Angriffen fest[30]. Ferner wurde vor Attacken auf Fernzugriffe, insbesondere die Kompromittierung des Windows-RDP-Protokolls, gewarnt. Diese haben seit Beginn der Corona-Krise um 127 Prozent zugenommen.

[30] Fortlaufender Untersuchungszeitraum

8. Ransomware

International betrachtet war, neben Regierungsbehörden, das Gesundheitswesen ein attraktives Ziel für Cyberkriminelle während der Corona-Pandemie: Wie der Cybersecurity-Dienstleister Unit42 berichtete, wurden z. B. kanadische Gesundheitseinrichtungen und Universitäten, welche an der Bekämpfung von COVID-19 beteiligt sind, mit Ransomware-Varianten angegriffen.[31] Durch die Notwendigkeit der Aufrechterhaltung der Patientenversorgung war es gerade für Akteure von Ransomware attraktiv, diese Ziele anzugreifen, um deren Notlage und Auslastung für eine hohe Lösegeldforderung auszunutzen. Derartige Angriffe auf Kritische Infrastrukturen waren zwar auch in der Vergangenheit zu verzeichnen[32] - in der besonderen Situation der Pandemie steht jedoch zu befürchten, dass die Auswirkungen solcher Angriffe gravierender ausfallen.

Verschiedene Quellen[33] berichteten von einer (internationalen) Zunahme von Ransomware-Angriffen auf das Gesundheitswesen[34]. Eingesetzt wurden hiernach die Ransomware-Familien *Maze, Sodinokibi* und *Ryuk*[35].

Der IT-Security-Dienstleister Coveware berichtete[36], dass im ersten Quartal 2020 v.a. IT-Dienstleister, Einrichtungen des Gesundheitswesens und des öffentlichen Dienstes die bevorzugten Ziele von Ransomware-Angriffen darstellten. Coveware zufolge sei dies ungewöhnlich, da der öffentliche Dienst (v.a. Schulen und Bildungseinrichtungen) erfahrungsgemäß erst im Sommer vermehrt Opfer von Cyberangriffen werde.

Es ist insgesamt davon auszugehen, dass Cyberkriminelle die Notlage von KRITIS-Einrichtungen (v.a. aus dem Bereich des Gesundheitswesens) ausnutzen, um hohe bzw. erhöhte Lösegeldforderungen zu verlangen.

Während der Corona-Pandemie wurden ferner neue Ransomware-Familien identifiziert:

Die Ransomware *„CovidLock“* tarnt sich z.B. als legitime App für mobile Endgeräte, welche vermeintlich eine HeatMap über die aktuelle Verbreitung der Krankheit anzeigen soll. Nach der Installation verschlüsselt CovidLock das betroffene System und droht mit der Veröffentlichung der kryptierten Daten sowie der permanenten Löschung des Telefonspeichers[37].

Eine weitere aufgetretene Ransomware in diesem Zusammenhang ist *„CoronaVirus“*[38]. „CoronaVirus“ ist als sog. Wiper einzustufen. Bisherigen Erkenntnissen zufolge sind die Akteure hinter dieser Schadsoftware nicht an Lösegeldforderungen interessiert, da kein Lösegeld verlangt wird, sondern ausschließlich Daten des betroffenen Systems überschrieben werden. Eine Wiper-Malware dient somit zuvorderst der Sabotage von Systemen.

---

[31] https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/
[32] Vgl. Spiegel, 2019. Hacker-Attacke trifft mehrere Krankenhäuser.
[33] Exemplarisch: https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
[34] Vgl. Artikel von IT-Daily vom 23.03.2020: Fünfmal mehr Malware zu Coronavirus
[35] 26.03.2020 - bleepingcomputer: Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic; online abrufbar unter: https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/
[36] https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
[37] Techrepublic: Covidlock ransomware exploits coronavirus with malicious Android app; 17.03.2020; https://www.techrepublic.com/article/covidlock-ransomware-exploits-coronavirus-with-malicious-android-app/
[38] Sonicwall: Coronavirus Trojan Overwritung The MBR, 31.03.2020; abrufbar unter: https://security-news.sonicwall.com/xmlpost/coronavirus-trojan-overwriting-the-mbr/

9. Exkurs: Straftaten in Zusammenhang mit Videokonferenzanwendungen

Am 14.04.2020 wurde bekannt, dass Cyberkriminelle Login-Daten für den Videokonferenzdienst „Zoom“ errungen haben. Gemäß eigenen Angaben habe die IT-Sicherheitsfirma Cyble im Darknet und in einschlägigen Untergrundforen hunderttausende ausgespähter Zugangsdatensätze entdeckt, die dort zum Kauf angeboten wurden.

Wie von Zoom selbst bestätigt wurde[39] erlangten die Täter diese Zugangsdatensätze durch sog. „Credential Stuffing“. Bei „Credential Stuffing“ handelt es sich um eine Methode, bei der Zugangsdaten aus älteren Datenleaks bei anderen Diensten dahingehend getestet werden, ob auch dort mittels dieser Zugangsdaten eine Anmeldung möglich ist.

Da die genutzten Zugangsdaten aus anderen Leaks stammen, ist es wahrscheinlich, dass diese bereits an anderer Stelle bekannt geworden sind. Eine vollständige Liste aller kompromittierten Accounts liegt nicht vor.

Laut dem US-CERT, dem FBI[40] und OSINT-Quellen wie Malwarebytes[41] nutzen Cyberkriminelle verschiedene Schwachstellen der App, welche z.B. Zugriff auf User-Videos erlauben. Besonders häufig sei aber das sog. Zoombombing festzustellen. Hierbei verschaffen sich Unberechtigte Zugang zu Zoom-Videoschaltkonferenzen (VSKen), indem sie entweder die Meeting-IDs erraten oder sich anderweitig beschaffen. Der Schaden durch Zoombombing sei bislang auf das Stören der jeweiligen VSK begrenzt. Die Dimension dieser Störungen kann unterschiedlich ausfallen: Aus Nordrhein-Westfalen (Bonn) wurde ein Sachverhalt übermittelt, in welchem durch Zoombombing kinderpornografisches Material während eines Webinars ausgestrahlt wurde[42].

Cyberkriminelle nutzten die Corona-Krise und die damit verbundenen Home-Office-Maßnahmen für ihre Zwecke auch aus, indem sie maliziöse Versionen der VSK-App Zoom erstellen. Laut Open Source-Quellen beinhalten diese maliziösen Versionen, die vornehmlich von Webseiten von Drittanbietern heruntergeladen werden, sog. Coinminer[43], RATs[44] oder Adware[45]. Laut IT-Security-Dienstleister Bitdefender ist die Anzahl an Downloads der „Fake-Zoom“-App in Deutschland aber eher gering.

Die (IT-)Nachrichtenseite Threatpost warnte zudem vor Phishing-Mails, welche auf das Abgreifen von Userdaten für Skype abzielten[46].

---

[39] https://www.heise.de/security/meldung/Videokonferenz-Plattform-Zoom-Veroeffentlichte-Login-Daten-aus-Credential-Stuffing-Angriffen-4702677.html (Abrufdatum 15.04.2020)
[40] https://www.us-cert.gov/ncas/current-activity/2020/04/02/fbi-releases-guidance-defending-against-vtc-hijacking-and-zoom
[41] https://blog.malwarebytes.com/how-tos-2/2020/04/keep-zoombombing-cybercriminals-from-dropping-a-load-on-your-meetings/
[42] EPOST-Nachricht 2020-0006188392 vom 20.04.2020
[43] https://blog.trendmicro.com/trendlabs-security-intelligence/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer/
[44] https://blog.trendmicro.com/trendlabs-security-intelligence/webmonitor-rat-bundled-with-zoom-installer/
[45] https://labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users/
[46] https://threatpost.com/skype-phishing-attack-targets-remote-workers-passwords/155068/

Das Cyber-AZ[47] berichtete in diesem Zuge von der Erstellung von mit schadhaftem Code angereicherten Versionen legitimer Apps. Dies betraf u. a. eine in Italien eingesetzte App, welche das Infektionsrisiko durch Kontaktüberwachung bewerten soll, sowie Corona-Dashboards, welche die Ausbreitung des Virus darstellen. So identifizierte Bitdefender im Mai eine App, welche sich als Informationsplattform über das Virus tarnte, sich aber als Screen-Locker herausstellte. „About Koronavirus" blockiert das Android-Smartphone und fordert zur Entschlüsselung eine Lösegeldzahlung. Ferner berichtete Bitdefender am 18.05.2020, dass verschiedene maliziöse Apps im Umlauf seien, welche nach Installation durch den User SMS und Kontaktdaten stehlen.

[47] Nationales Cyber-Abwehrzentrum – Kooperation deutscher Sicherheitsbehörden auf Bundesebene

10. Gesamtbewertung und Ausblick

Die gesellschaftlichen und wirtschaftlichen Auswirkungen der Pandemie sowie die damit in Zusammenhang stehenden staatlichen Hilfsmaßnahmen bieten für Cybertäter spezifische Angriffsmöglichkeiten. Die Strafverfolgungsbehörden haben zunehmend Versuche festgestellt, diese Lage auszunutzen. Aufgrund des weiter bestehenden Gefahrenpotenzials der Pandemie für Staat und Gesellschaft und der anhaltenden Verschiebungen diverser Lebensbereiche in den virtuellen Raum wird die thematische Bedrohungslage im Cyberbereich als andauernd hoch eingestuft.

Dieser Gefährdungseinschätzung liegen folgende Erkenntnisse und Bewertungen zugrunde:

Cyberkriminelle greifen bei ihren Aktivitäten auf bewährte Modi Operandi und Malware-Familien zurück. Die Corona-Pandemie zeigt dabei einmal mehr auf, dass die Täter sehr rasch gesellschaftliche Entwicklungen aufgreifen und zu kriminellen Zwecken ausnutzen.

Die hauptsächliche Bedrohung geht weiterhin von Phishing und maliziösen/kriminellen Domains aus. Neben der Erstellung von Fake-Webseiten im Zusammenhang mit der Beantragung der Corona-Soforthilfe wurden bundesweite Phishing-Wellen festgestellt, die jeweils zum Ziel hatten, persönliche Daten von Antragstellern zu erlangen und in der Folge für mutmaßliche Betrugsdelikte nutzen zu können. In mehreren Bundesländern nahmen diese Modi Operandi konkreten Einfluss auf die staatliche Auszahlung von Corona-Soforthilfen.

Es häufen sich ausländische, sicherheitsbehördliche und externe Hinweise, dass Cybertäter die Corona-Krise für die Verbreitung der Schadsoftware *TrickBot* ausnutzen. Eine mögliche Verbreitung auch in Deutschland und das in der Vergangenheit bekannt gewordene „Zusammenspiel“ der Malware-Varianten *TrickBot, Ryuk* und *Emotet* stellen ein bedeutsames Gefahrenpotenzial dar.

Es ist einzukalkulieren, dass Transaktionen nicht nur vermehrt online vorgenommen werden, sondern auch der Handel mit Kryptowährungen ansteigen wird. Cyberkriminelle können dies ausnutzen und vermehrt Online-Geschäfte und diesbezügliche Zahlungssysteme attackieren.

Bislang bewegt sich das Aufkommen versuchter Cyberangriffe auf hohem, die Zahl erfolgreicher Cyberstraftaten in Deutschland auf mittlerem Niveau.

Dieser Umstand ist nach hiesiger Einschätzung auch auf die technischen Sicherheitsmaßnahmen und die durchgeführten Präventions- und Sensibilisierungsmaßnahmen in Deutschland zurückzuführen.

Jedoch: Die globale Corona-Pandemie ist noch nicht überstanden.

Einer proaktiven Lagebeobachtung sowie einer engen Zusammenarbeit der Polizei mit ihren Partnern kommt in diesem Zusammenhang weiterhin eine herausragende Bedeutung zu.

Die Resilienz der Bevölkerung und Unternehmen gegenüber Social Engineering wird weiter auf die Probe gestellt, da potenziell jeder - unabhängig von seinem beruflichen und gesellschaftlichen Status - von der Thematik betroffen sein kann.

Impressum

Herausgeber
Bundeskriminalamt, 65173 Wiesbaden

Stand
September 2020

Gestaltung
Bundeskriminalamt, 65173 Wiesbaden

Bildnachweis
Bundeskriminalamt

Weitere Publikationen des Bundeskriminalamtes zum Herunterladen finden Sie ebenfalls unter:
www.bka.de/Lagebilder

Diese Publikation wird vom Bundeskriminalamt im Rahmen der Öffentlichkeitsarbeit herausgegeben.
Die Publikation wird kostenlos zur Verfügung gestellt und ist nicht zum Verkauf bestimmt.

Nachdruck und sonstige Vervielfältigung, auch auszugsweise,
nur mit Quellenangabe des Bundeskriminalamtes
(Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie, Seite X).