RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Digitaler Wirtschaftsschutz

Unternehmenswerte schützen und verteidigen

Virtueller Kongress “Digitale Sicherheit Rheinland-Pfalz”
Mainz, 19. November 2020

Cyberspionage durch Wellmess / Wellmail

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

Schwere Vorwürfe aus London

17.07.2020, 16:19 Uhr

Russische Hacker sollen Impfstoff-Forscher ausspionieren

Sicherheitsbehörden schlagen Alarm. Der russische Geheimdienst soll auch das Brexit-Abkommen beeinflusst haben. Der Kreml weist die Vorwürfe zurück. VON SEBASTIAN BORGER

Weltweit wird an einem Impfstoff geforscht. FOTO: SAKCHAI LALIT/DPA

Quelle: Der Tagesspiegel

LEBENDIG. SICHER. BÜRGERNAH.

Aktives Monitoring über Realtime-Scanner

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

covid.berlin
coruna.cr
covidjab.co.uk
covid19coronavirus.com
coronavirusvaccinelist.com
hunger-trotz-corona.ch
survivingcorona.org
coronaviruspharma.com
coronavirusmortgagerelief.site
coronavirusbestmasks.com
symptomsofcovid19.com
coronavirusfinancial.net
buycoronakit.com
covid-19-impfstoff.de
coviddefender.com

- lifecorona.com
- www.coronavirus.ginfo.site
- covid19.smshub.co.id
- covid19-api.grupovisual.org
- www.reliefcorona.com
- covidideas.com
- rockstarvirusremoval.com
- www.brocktoncovenantchurch.com
- survivingcovid-19.org
- brocktoncovenantchurch.com
- covid19.allinsoft.net.pe
- pandemicrt.com
- www.pandemicrt.com
- cervezacorona.net
- protivo-virus.ru
- prophecyuncovered.com
- covid19-produkte.de
- www.coronapreferences.de
- corona-raetsel.de
- coronarchiv.de
- coronacommand.com

LEBENDIG. SICHER. BÜRGERNAH.

Maliziöse Web Sites

Activity Leveraging Coronavirus / COVID / Mask as a Theme

1-50 of 336 Results

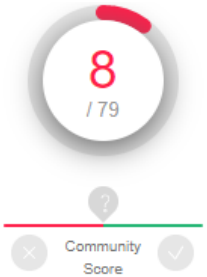
Type	Summary	Owner	Added
Incident	Hacked Data Broker Accounts Fueled Phony COVID Loans, Une...	Technical Blogs and Reports	08-07-2020
Incident	Attentions: YOU HAVE WON RS 7 CRORE AND 2 LAKH RUPEES ...	Spamtastic OSINT	08-04-2020
Incident	Covid19 Emergency Relief Scam	Technical Blogs and Reports	08-04-2020
Incident	Investigate | COVID-19 Cybercrime Weekly Update	Technical Blogs and Reports	08-01-2020
Incident	Discover | COVID-19 Weekly Update	Technical Blogs and Reports	08-01-2020
Incident	FEMA Covid Hazard Pay Facebook Hoax	Technical Blogs and Reports	08-01-2020
Incident	Microsoft COVID-19 Relief Fund Scam	Technical Blogs and Reports	08-01-2020
Incident	Business ID Theft Soars Amid COVID Closures	Technical Blogs and Reports	07-28-2020
Incident	Covid 19 Update 😢	Spamtastic OSINT	07-27-2020
Incident	Nigeria: avoid Covid phishing scams	Spamtastic OSINT	07-27-2020
Incident	COVID-19 RELIEF PARKAGE.	Spamtastic OSINT	07-24-2020
Incident	Couple of interesting Covid-19 related stats, (Tue, Jul 21st)	Technical Blogs and Reports	07-21-2020

Identified Infrastructure Referencing "Corona" or "Covid"

1-50 of 2332

Type	Summary	Owner	Observations	Added
URL	http://u823584jr0.ha004.t.justns.ru/labanquepostal...	OpenPhish	--	08-09-2020
Host	face-mask-coronavirus.com	Firebog Prigent Malware...	--	08-09-2020
Host	facebook.corona-virus-news.xyz	Firebog Prigent Malware...	--	08-09-2020
Host	examenadomiciliocoronavirus.cl	Firebog Prigent Malware...	--	08-09-2020
Host	eventt.19covidd.com	Firebog Prigent Malware...	--	08-09-2020
Host	ent-covid19-gouv.info	Firebog Prigent Malware...	--	08-09-2020
Host	ecialeventfreefire.19covidd.com	Firebog Prigent Malware...	--	08-09-2020
Host	donaldtrumphascoronavirus.com	Firebog Prigent Malware...	--	08-09-2020
Host	doeshappymediumhavethecoronavirus.com	Firebog Prigent Malware...	--	08-09-2020
Host	desinfectercoronavirus.com	Firebog Prigent Malware...	--	08-09-2020
Host	desinfectantes-covid19.com	Firebog Prigent Malware...	--	08-09-2020
Host	deadlycovid19.com	Firebog Prigent Malware...	--	08-09-2020

Maliziöse Web Sites



8 engines detected this URL

http://coronaviruspharma.com/
coronaviruspharma.com

403 Status | text/html Content Type | 2020-07-21 20:09:15 UTC 9 hours ago

DETECTION DETAILS COMMUNITY

AegisLab WebGuard	Phishing	BitDefender	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Phishing
G-Data	Malware	Kaspersky	Phishing
Sangfor Engine Zero	Malware	Sophos AV	Malicious
DNS8	Suspicious	ESET	Suspicious
ADMINUSLabs	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean

Maliziöse Web Sites

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

1
/ 77

Community Score

One engine detected this URL

http://covid-19-impfstoff.de/
covid-19-impfstoff.de

200
Status

text/html; charset=UTF-8
Content Type

2020-04-06 16:54:34 UTC
3 months ago

DETECTION | DETAILS | COMMUNITY

Fortinet	Phishing	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	AlienVault	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
Avira (no cloud)	Clean	BADWARE.INFO	Clean
Baidu-International	Clean	BitDefender	Clean

LEBENDIG. SICHER. BÜRGERNAH.

DNS Auffälligkeiten

covid19server.unityseguros.com

First Seen 2020-05-17
Last Seen 2020-07-22
Registrar GoDaddy.com, LLC
Registrant Unity Group Holding
Categorize

RESOLUTIONS

1 - 12 of 12 ▾ Sort : Last Seen Descending ▾ 25 / Page ▾

Resolve	Location	Network	ASN	First	Last
54.87.62.224	US	54.87.0.0/16	14618	2020-07-20	2020-07-22
52.1.155.253	US	52.0.0.0/15	14618	2020-07-20	2020-07-22
18.232.20.22	US	18.232.0.0/14	14618	2020-06-11	2020-07-17
52.73.16.6	US	52.72.0.0/15	14618	2020-06-11	2020-07-17
52.4.139.101	US	52.4.0.0/14	14618	2020-07-01	2020-07-01
23.20.7.14	US	23.20.0.0/15	14618	2020-06-08	2020-06-08
3.85.153.239	US	3.80.0.0/12	14618	2020-06-08	2020-06-08
23.22.13.195	US	23.22.0.0/15	14618	2020-05-30	2020-06-06
54.236.250.233	US	54.236.128.0/17	14618	2020-05-28	2020-06-06
34.231.219.204	US	34.224.0.0/12	14618	2020-05-28	2020-05-28
35.169.17.27	US	35.168.0.0/13	14618	2020-05-16	2020-05-17
52.204.246.201	US	52.200.0.0/13	14618	2020-05-16	2020-05-17

Cyberspionage durch Wellmess / Wellmail

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

- Wellmess

  Wird der APT-Gruppierung APT29 zugeschrieben. Sie wird dem FSB zugerechnet.
  Die Malware kann über drei Kommunikationsmethoden mit dem C2-Server kommunizieren, wobei jede individuell aktiviert oder deaktiviert wird. Die drei Methoden sind:

  HTTP

  HTTPS

  DNS

LEBENDIG. SICHER. BÜRGERNAH.

Cyberspionage durch Wellmess / Wellmail

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

- Wellmail

  WellMail ist ein Tool zum Ausführen von Befehlen oder Skripten, wobei die Ergebnisse an einen fest codierten C2-Server (Command and Control) gesendet werden.

  Diese Malware wurde aufgrund von Dateipfaden, die das Wort "Mail" enthalten, und der Verwendung des genutzten Server-Ports 25 "WellMail" genannt.

LEBENDIG. SICHER. BÜRGERNAH.

IOC‘s: YARA-Rules, Hashes und C2 IP-Adressen

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

```
103.103.128.221
103.13.240.46
103.73.188.101
111.90.146.143
111.90.150.176
119.160.234.163
119.81.178.105
120.53.12.132
122.114.197.185
122.114.226.172
141.255.164.29
141.98.212.55
145.249.107.73
146.0.76.37
149.202.12.210
169.239.128.110
176.119.29.37
178.211.39.6
185.120.77.166
```

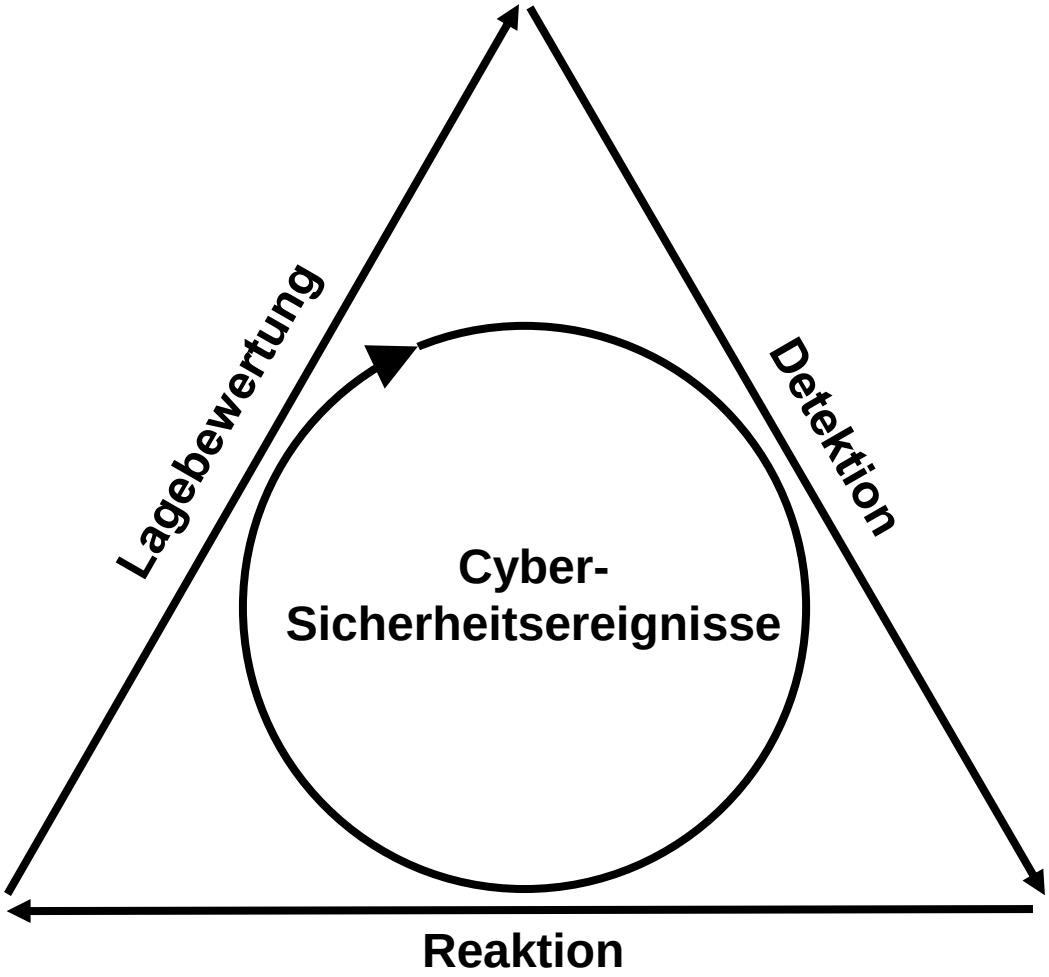
```
rule wellmess_dotnet_unique_strings {
meta:
description = "Rule to detect WellMess .NET"
author = "NCSC"
hash = "2285a264ffab59ab5a1eb4e2b9bcab9baf26750b6c544ee3094af5"
strings:
$s1 = "MaxPostSize" wide
$s2 = "HealthInterval" wide
$s3 = "Hello from Proxy" wide
$s4 = "Start bot:" wide
$s5 = "Choise" ascii wide
condition:
uint16(0) == 0x5a4d and uint16(uint16(0x3c)) == 0x4550 and 3 of them
}
```

```
00654dd07721e7551641f90cba832e98c0acb030e2848e5efc0e1752c067ec07
0322c4c2d511f73ab55bf3f43b1b0f152188d7146cc67ff497ad275d9dd1c20f
03e9adae529155961f1f18212ff70181bde0e3da3d7f22961a6e2b1c9da2dd2e
0b8e6a11adaa3df120ec15846bb966d674724b6b92eae34d63b665e0698e0193
14e9b5e214572cb13ff87727d680633f5ee238259043357c94302654c546cad2
1fed2e1b077af08e73fb5ecffd2e5169d5289a825dcaf2d8742bb8030e487641
21129ad17800b11cdb36906ba7f6105e3bd1cf44575f77df58ba91640ba0cab9
```

LEBENDIG. SICHER. BÜRGERNAH.

Triage-Prozess für Cyber-Sicherheitsereignisse

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT



LEBENDIG. SICHER. BÜRGERNAH.

Triage-Prozess für Cyber-Sicherheitsereignisse

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

- Detektion:
  Ziel des Aufgabengebiets "Detektion" ist, sicherheitsrelevante Ereignisse zeitnah und zuverlässig zu erkennen.

- Reaktion:
  Bei der Aufarbeitung von Cyber-Sicherheitsvorfällen werden geeignete Maßnahmen vorgeschlagen.

  Dazu gehört bspw. Auch die Warnung der von Cyber-Vorfällen (potenziell) betroffenen Unternehmen und Organisationen.

LEBENDIG. SICHER. BÜRGERNAH.

Triage-Prozess für Cyber-Sicherheitsereignisse

RheinlandPfalz
MINISTERIUM DES INNERN UND FÜR SPORT

- Lagebewertung:
  Erkenntnisse über Cyber-Gefahren, insbesondere über Bedrohungen, Schwachstellen und Vorfälle, werden im Aufgabengebiet "Lage" erfasst, analysiert, aufbereitet und kommuniziert.

  Ergänzt werden diese Lage-Informationen durch Warnungen vor aktuellen Cyber-Gefahren.

LEBENDIG. SICHER. BÜRGERNAH.