Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	4. März 2021
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN, BAG, Swissmedic

Aktuelles (Februar 2021)

Die Situation im Bereich Cyber-Sicherheit bleibt aufgrund von aktuellen Angriffen auf kritische Infrastrukturen und im Speziellen auf Organisationen im Gesundheitssektor angespannt.

- Die von uns detektierten Malspam-Wellen bleiben auf einem hohen Niveau.
- Betrüger versuchen vermehrt, an Regierungs- und Nicht-Regierungsorganisationen angeblicher «Impfstoff» zu verkaufen.
- Staatliche Akteure haben versucht, Daten zum Pfizer-Impfstoff zu stehlen.
- Auch im Februar 2021 wurden Spitäler erneut Opfer von Ransomware-Angriffen.

Betrug mit vermeidlichen Impfstoffen

Anfangs Februar 2021 wurden dem NCSC Informationen zugetragen, wonach Betrüger den aktuell europaweit herrschenden Engpass von Impfstoffen auszunutzen, um sich offensichtlich finanziell zu bereichern. Dem NCSC sind Fälle im In- und Ausland bekannt, wo Cyberkriminelle via E-Mail an Regierungs- und Nicht-Regierungsorganisationen herangetreten sind mit dem Angebot, Impfstoffe zu liefern. Dazu haben die Betrüger gut klingende Domain-Namen registriert, von welchen dann Kontakt mit den vermeidlichen Opfern aufgenommen wurde. Die besagten E-Mails sind in Englisch geschrieben und bieten die Lieferung eines nicht näher spezifizierten Impfstoffes an.

Das NCSC empfiehlt gegenüber E-Mails von Unbekannten skeptisch zu sein und in solchen allenfalls vorhandenen Dateianhängen nicht zu öffnen sowie keinen Links zu folgen. Zudem sollten verdächtige E-Mails in jedem Falle direkt dem GovCERT gemeldet werden:

incidents@govcert.ch

Wieder Cyber-Angriff auf europäische Spitäler

Im Februar 2021 kam es erneut zu erfolgreichen Cyber-Angriffen auf Spitäler weltweit. Auch Gesundheitseinrichtungen in Europa blieben von Cyber-Angriffen nicht verschont. So wurden beispielsweise gleich zwei Spitäler in Frankreich Opfer von Ransomware Angriffen. Das L'Hôpital Nord-Ouest in Villefranche-sur-Saône wurde am 15. Februar Opfer der Ransomware «Ryuk». Gemäss Medienberichten[1] mussten als Folge des Cyber-Angriffs Patienten von den Notfallstationen in andere Spitäler verlegt werden. Der Zugang zu diversen Diensten, inkl. Telefonie und Webseite des Spitals, war für mehrere Tage eingeschränkt bzw. nicht möglich.

Auch in der Schweiz gab es in der Vergangenheit erfolgreiche Angriffe durch die Ransomware Ryuk. Als Infektionsvektor wird in der Regel die Malware «TrickBot» verwendet, welche sich über schädliche Office-Dokumente (docx, xlsx) in E-Mails verbreitet.

Über ein weiteres Ransomware Opfer in Frankreich, Spital «Dax», wurden keine weiteren Details bekannt. Jedoch musste gemäss Medienberichten als Folge des Angriffs ein Impfzentrum geschlossen werden.

Staatliche Akteure versuchen an Daten des Pfizer Impfstoffes zu gelangen

Medienberichten zufolge[2] versuchten im Februar staatliche Akteure, vermeintlich aus Nordkorea, an Impfstoff-Daten des Impfstoffherstellers Pfizer zu gelangen. Dazu hätten Angreifer versucht, in Computersysteme südkoreanischer Arzneimittelhersteller einzudringen, wie die südkoreanische Nachrichtenagentur Yonhap berichtet. Sie beruft sich auf Abgeordnete, die in einer geschlossenen Sitzung vom südkoreanischen Geheimdienst NIS unterrichtet worden waren.

Neben Impfstoff-Daten von Pfizer sind wohl auch weitere Impfstoff-Anbieter von ähnlichen Cyber-Angriffen betroffen. So haben gemäss Reuters ebenfalls staatliche Akteure versucht, mittels Social-Engineering, an Daten des Impfstoff-Entwicklers Astra Zeneca zu gelangen[3].

[1] https://www.inside-it.ch/de/post/immer-mehr-ransomware-attacken-auf-krankenhaeuser-20210217

[2] https://www.heise.de/news/Nordkorea-versuchte-angeblich-Pfizers-Impfstoff-Daten-zu-stehlen-5056656.html

[3] https://www.bbc.com/news/technology-56084575

Interview mit einem Ransomware-Betreiber

Der IT-Sicherheitsdienstleister TALOS veröffentlichte ein Interview[4] mit den Ransomware-Betreibern von «LockBit», welches interessante Einblicke in deren Tätigkeit bietet:

- **Spitäler «einfaches Ziel»:** Die Akteure hinter «LockBit» erachten Spitäler als «einfache Ziele». Diese seien in den allermeisten Fällen gewillt, den von den Cyberkriminellen gestellten Lösegeldforderungen nachzukommen. Die Akteure beziffern die Erfolgschancen, dass ein Spital Lösegeld bezahlt, zwischen 80% und 90%.
- **Verwundbare Systeme:** Cyberkriminelle erachten ungepatchte und somit Verwundbare Systeme weiterhin als eine der einfachsten Möglichkeiten für einen erfolgreichen Angriff. Dies, obwohl für die Sicherheitslücken bereits entsprechende Patches vorhanden sind, welche die Sicherheitslücke schliessen würden.
- **DSGVO:** Die strengen Datenschutzbestimmungen in der EU (DSGVO / GDPR) spielen den Angreiffern in die Hände. Europäische Unternehmen, welche Opfer von Ransomware Angriffen werden, sind eher bereit, den Lösegeldforderungen der Cyberkriminellen nachzukommen, um den rechtlichen Konsequenzen bei einer allfälligen Veröffentlichung der Daten zu entgehen.

(10:47:35 PM) **REDACTED:** I told you that I don't like to focus on quantity and don't after everything
(10:49:43 PM) **Talos Analyst :** There are laws in the US that force the victim to publicly disclose breaches – something like the Sarbanes-Auxley Act and alike
(10:50:20 PM) **REDACTED:** they definitely don't disclose everything
(10:50:38 PM) **REDACTED:** but in reality the ransom payout is a bit more difficult in the US recently

(10:51:09 PM) **Talos Analyst :** because everyone has insurance now?
(10:51:19 PM) **REDACTED:** actually those who have insurance pay up quickly
(10:51:24 PM) **REDACTED:** because the insurance covers it
(10:52:16 PM) **REDACTED:** but I hear that there will soon be a law that will ban victims from paying ransomware

(10:52:29 PM) **Talos Analyst :** what about in Europe?
(10:52:45 PM) **REDACTED:** Europe pays, they are scared of GDPR

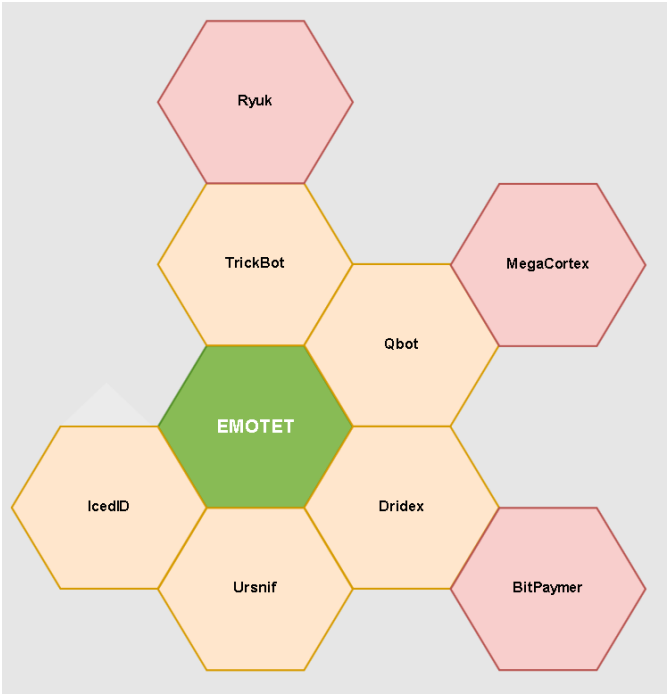
Auszug aus dem Interview mit den Urhebern der Ransomware "LockBit" (Quelle: TALOS)

TrickBot, Qbot und Dridex

Seit Mitte Januar 2021 das «Emotet»-Botnetz von Strafverfolgungsbehörden im Rahmen der Operation Ladybird[5] unschädlich gemacht wurde, ist auch ein beliebter Eintrittsvektor für Ransomware verschwunden. Gemäss unseren Einschätzungen hat dies jedoch die Ransomware-Aktivität, wenn überhaupt, nur bedingt beeinflusst. Andere Malware Familien sind weiterhin aktiv und werden, wie der zuvor genannte Cybervorfall beim L'Hôpital Nord-Ouest zeigt, für die kompromittierung mit Ransomware verwendet. Die folgende Grafik zeigt die bisherige Rolle von «Emotet»:

[4] https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf

[5] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action



Quelle: https://twitter.com/pollo290987/status/1214596853771227137

Bis Januar 2021 wurde «Emotet» von dessen Urhebern vor allem im Darkweb als «Pay-Per-Install» (PPI) vermarktet. Andere, oben ebenfalls ersichtliche Akteure, konnten sich so den Zugang zu mit «Emotet» infizierten Systemen erkaufen, welche dann dazu verwendet wurde, um ihre eigene Malware auf dem System zu platzieren. Diese wurde dann üblicherweise für das Auskundschaften des infiltrierten Netzwerkes verwendet, bevor die Cyberkriminellen schliesslich die Systeme mit Ransomware verschlüsselt haben.

Seit dem Wegfall von «Emotet» müssen sich nun verschiedene Akteure vermehrt selber um das Verbreiten, das heisst: die Infektion von neuen Systemen, kümmern. Als Folge davon beobachten wir eine Zunahme von Malspam Kampagnen, welche direkt versuchen, den Empfänger mit TrickBot, Qbot (aka Quakbot) oder Dridex zu infizieren. Der Modus Operandi ist jedoch immer derselbe: Cyberkriminelle versenden schädliche Excel oder Word Dokumente, welche bei einer Ausführung der darin enthaltenen Makros das System mit Malware infizieren, wobei diese meist zur Laufzeit von einem weiteren Server aus dem Internet heruntergeladen wird.

Empfehlungen:

- Sperrung von IP-Adressen bekannter Botnetz Command&Control Server (C&Cs) durch Implementierung des **MELANI BGP Feeds** (Kontakt: outreach@govcert.ch). Ob Sie oder Ihr Provider diese bereits einsetzen, kann mit einem Aufruf der folgenden Test-Einträge mittels Web-Browser überprüft werden. Schlägt die Verbindung fehl, sind Sie bereits geschützt:
  - http://ip-protection.govcert.ch
  - http://melbl-protection.govcert.ch

- Sperren von Domain-Namen bekannter Botnetz Command&Control Server (C&Cs) durch Implementierung der **MELANI RPZ** oder des **Secure DNS Resolvers** (Kontakt: outreach@govcert.ch)

- Blockieren Sie den Empfang von **gefährlichen E-Mail-Anhängen** auf Ihrem E-Mail-Gateway, dazu zählen auch **Office-Dokumente mit Makros**. Eine Empfehlung von zu sperrenden Dateianhängen finden Sie hier:
  - https://www.govcert.ch/downloads/blocked-filetypes.txt

- Erstellen **Sie regelmässig Sicherungskopien (Backups)** Ihrer Daten. Nutzen Sie dabei das Generationenprinzip (täglich, wöchentlich, monatlich - mindestens 2 Generationen). Stellen Sie jeweils sicher, dass Sie das Medium, auf welchem Sie die Sicherungskopie erstellen, nach dem Backup-Vorgang vom Computer bzw. Netzwerk **physisch trennen und sicher aufbewahren**.

- Sicherstellen, dass genügend Logdateien vorhanden sind (aufgerufene URLs auf den Proxyservern, Active Directory Logs, Sichtbarkeit auf den Endgeräten mit Hilfe von SysMon oder einem Remote Forensik Werkzeug).

- Einsatz einer Liste wie URLHaus[6], um das Nachladen von Malware zu verhindern.

Kontakt GovCERT

Im Falle eines IT-Sicherheitsvorfalles, von verdächtigen E-Mails, etc. steht Ihnen das GovCERT jederzeit gerne zur Verfügung:

E-Mail: incidents@govcert.ch
Pikett-Telefon: +41 79 152 20 80 (**nur in Notfällen!**)

Für Rückfragen technischer Art oder Implementierung von NCSC Dienstleistungen:

outreach@govcert.ch

[6] https://urlhaus.abuse.ch/