Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	2. Februar 2021
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN

Aktuelles (Januar 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.
- In den ersten Januar Wochen 2021 war «Emotet» erneut sehr aktiv
- Am 27. Januar wurde in einer weltweit koordinierten Aktion das «Emotet» Botnetz ausgeschaltet und tatverdächtige Personen verhaftet.
- Wir beobachteten vereinzelte DDoS Angriffe, welche aber nicht spezifisch gegen einen bestimmten Sektor gerichtet sind.
- Ebenfalls gibt es viele Angriffe gegen Cloud Accounts wie z.B. O365. In diesem Zusammenhang empfehlen wir die flächendeckende Nutzung einer 2 Faktor Authentisierung, gerade auch für so exponierte Dienste sowie das Einbinden dieser Dienste in das Security Monitoring.
- Mitte Januar gab es eine grössere Cyber Attacke auf ein europäisches Spital.

Takedown des «Emotet»-Botnetzes

Die Schadsoftware (Malware) «Emotet» war über 2 Jahre lang aktiv und wurde unter anderem dazu verwendet, in Firmennetze und andere Einrichtungen weltweit einzudringen und danach mit Ransomware zu verschlüsseln. Nach Einschätzungen von Sicherheitsexperten und dem NCSC war «Emotet» in den Jahren 2019 und 2020 die gefährlichste Schadsoftware weltweit. Auch diverse Spitäler waren in den vergangenen 12 Monaten von diesen Angriffen betroffen. Die von «Emotet» versursachten Schäden belaufen sich nach Einschätzungen auf einen dreistelligen Millionenbetrag.

Bereits seit längerem verfolgen wir eine proaktive Strategie, um die Gefahr durch «Emotet» für Bürgerinnen und Bürger, aber auch für Firmen und insbesondere Gesundheitseinrichtungen in der Schweiz mit Hilfe von technischen Massnahmen zu minimieren. Wir sind

der Überzeugung, dass sich diese Massnahmen bewährt haben und dadurch die Anzahl von grösseren Cyber-Sicherheitsvorfällen in der Schweiz massgeblich reduziert werden konnte.

Am 27. Januar 2021 hat EUROPOL in Zusammenarbeit mit Strafverfolgungsbehörden aus verschiedenen Ländern, darunter den Niederlanden, Deutschland, Frankreich und dem Vereinigten Königreich einen Schlag gegen «Emotet» durchgeführt[1]. Dabei wurden Botnetz-Infrastrukturen, welche von der Täterschaft für die Steuerung und Verwaltung von mit «Emotet» infizierten Computer verwendet wurden, ausgeschaltet («takedown») oder durch die Behörden beschlagnahmt. Die folgende Statistik zeigt die Anzahl aktiver «Emotet» Botnetz Command&Control Server (C&Cs), welche in den vergangenen Tagen durch den MELANI BGP Feed blockiert wurden. Darauf klar erkennbar ist der Einbruch der Zahl aktiver C&C Server zwischen dem 25. Januar und 26. Januar:

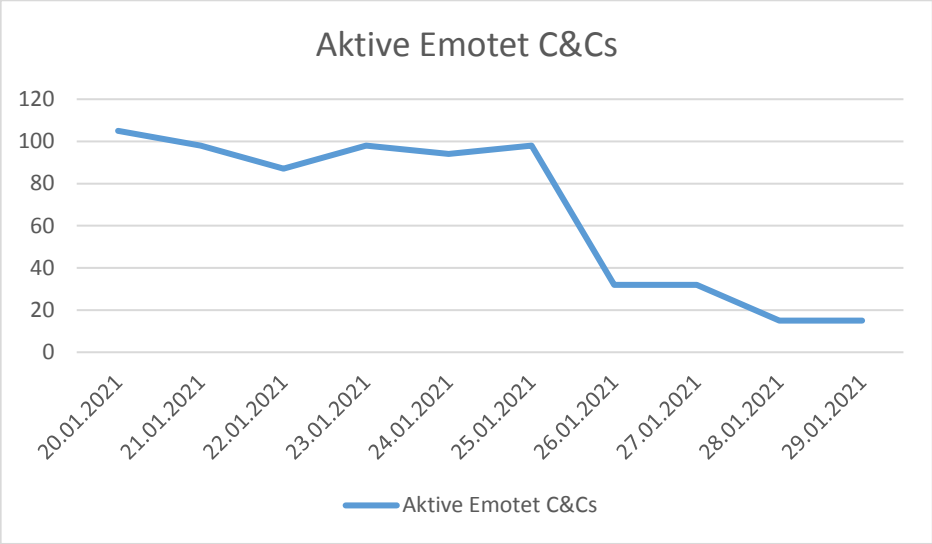

Figure 1 - Aktive Emotet C&Cs in den letzten 10 Tagen

Zudem wurden mutmasslich an «Emotet» und deren Verbreitung beteiligten Personen verhaftet und an die Justiz überführt. Seit einigen Tagen erhält GovCERT.ch Informationen über mit «Emotet» infizierte IP Adressen in der Schweiz und benachrichtigt die zuständigen Internet Service Provider (ISPs), sodass diese wiederum die betroffenen Endkunden zwecks Bereinigung der Infektion informieren können.

Aus technischer Sicht beurteilt NCSC die von den Behörden durchgeführte Aktion als sehr Erfolgreich. Obwohl nicht alle Akteure hinter «Emotet» identifiziert und verhaftet werden konnten, wurde deren Infrastrukturen Massgeblich zerschlagen. Wir gehen jedoch davon aus, dass sich die Akteure in den kommenden Monaten mit einer überarbeiteten Schadsoftware und neuer Infrastruktur zurückmelden werden. Bis dahin gibt es aber erstmal eine Verschnaufpause, die dazu genutzt werden sollte, weitere Schutzvorkehrungen zu planen und umzusetzen, wie z.B. dem Schutz / der Blockierung von Makros oder die Sichtbarkeit auf Endgeräten. Es ist auch zu beachten, dass mit Emotet geschaffene Zugänge in Netzwerke verkauft worden sind und somit andere Tätergruppierungen bereits weitere, von Emotet unabhängige Malware installiert haben können.

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

Das NCSC beobachtet «Emotet» weiterhin und nutzt dabei nicht nur Daten aus eigenen Sensoren und Analysen, sondern setzt auch auf eine intensive internationale Zusammenarbeit mit Partnerstaaten. Dies erlaubt es uns jederzeit und zeitnah auf neue Entwicklungen im Cyberspace zu reagieren und umgehend entsprechende mitigierende Massnahmen einzuleiten.

Erneuter Cyber-Angriff auf ein europäisches Spital

Mitte Januar 2021 wurde bekannt, dass erneut ein europäisches Spital Opfer einer grossen Cyber-Attacke wurde. Unbekannte haben sich dabei Zugriff auf das Netzwerk des Spitals und deren Server verschafft, wobei diese mit Ransomware verschlüsselt wurden. Die Auswirkungen auf die Tätigkeit des Spitals und die Verfügbarkeit deren Dienstleistungen ist «signifikant». Als Eintrittstor wurden gestohlene VPN-Zugangsdaten eruiert. NCSC warnt bereits seit Monaten vor der Gefahr durch gestohlenen VPN Zugangsdaten sowie Sicherheitslücken in VPN-Diensten und hat dazu bereits entsprechende Empfehlungen abgegeben:

- Remote-Zugänge wie **Citrix, RDP und VPN**-Server müssen **konsequent auf dem aktuellen Patchlevel gehalten werden**
- Sämtliche Zugänge, welche durch ein Login (z.B. Benutzername und Passwort) aus dem Internet erreichbar sind müssen zwingend mit einer **zwei Faktor Authentisierung (2FA)** abgesichert werden. Dies betrifft die eben bereits erwähnten Remote-Zugänge wie **Citrix, RDP und VPN**-Server jedoch auch beispielsweise der Zugang auf **Webmail** oder **Sharepoint**

Weitere Cyberbedrohungen

Viele der uns gemeldeten Cybervorfälle sind auf kompromittierte Zugangsdaten zurück zu führen. Diese wurden zuvor gestohlen oder mittels Brute-Forcing-Angriff «geknackt». Während Brute-Forcing-Angriffe technisch relativ einfach zu detektieren sind hilft jedoch vor allem die Implementierung einer Zwei-Faktor-Authentisierung (2FA) die Risikoexposition zu minimieren. Prinzipiell empfehlen wir die Implementierung von 2FA für sämtliche aus dem Internet erreichbare Dienste (wie z.B. Remote Access, Terminservices, Webmail, VPN, etc) sowie sämtliche Clouddienste. Zudem sollten Login versuche sollte aufgezeichnet und regelmässig ausgewertet werden.

Während die Cyberbedrohungslage durch den takedown des Emotet Botnetz reduziert werden konnte, stehen weitere Akteure bereit um in die Bresche zu springen. Das NCSC beobachtet beispielsweise regelmässig «Dridex» Malspam Kampagnen, welche mittels schädlichen Excel-Dateianhängen oder links auf kompromittierte Webseiten versuchen, den Computer des Opfers mit «Dridex» zu infizieren.

Im Januar konnten wir zudem eine Zunahme von Infrastruktur feststellen, welche von einer Threat Actor bekannt als UNC1878 verwendet wird. UNC1878 wurde vor allem durch die Verwendung der Ryuk Ransomware gegen Universal Health Service (UHS) im Oktober 2020[2] bekannt.

Uns bekannte Dridex und UNC1878 Botnetz C&C Server werden auf der MELANI Botnetz Liste (MELBL) gelistet wodurch das von diesen Botnetzen ausgehende Risiko für Benutzer von MELBL minimiert wird.

[2] https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

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