Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

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

Aktuelles (November)

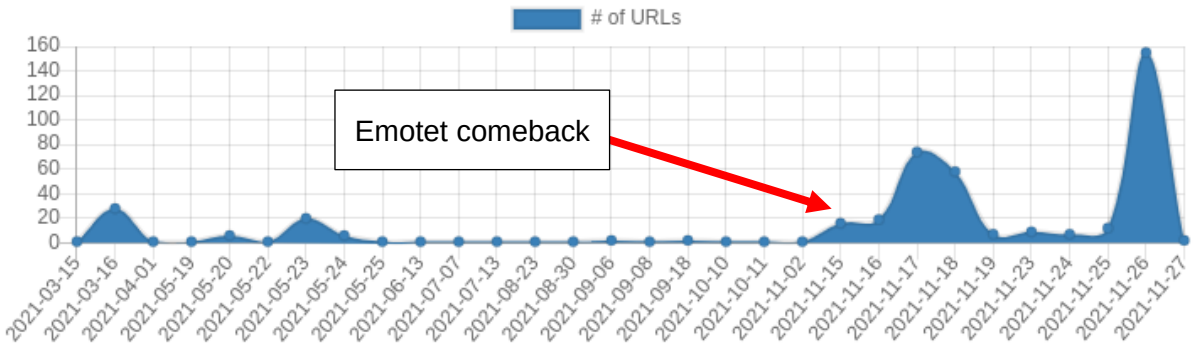
Mitte November 2021 sorgte die Rückkehr des Trojaners «Emotet» für viel Wirbel. Zudem wurden erneut mehrere Cyberangriffe auf ausländische Organisationen aus dem Gesundheitssektor gemeldet. In der Schweiz wurden im Monat November glücklicherweise keine solche Angriffe gemeldet.

Das aktuelle Healthcare Update behandelt folgende Themen:

- «Emotet» kehr zurück
- «BlackMatter» Ransomware Gang stellt Aktivitäten ein
- Cyber-Angriffe gegen Gesundheitseinrichtungen

«Emotet» kehrt zurück

Am 15. November 2021 meldeten IT-Sicherheitsexperten[1] die Rückkehr des berüchtigten «Emotet» Trojaners. Emotet wurde in den Jahren 2019 und 2020 grossflächig für Cyberangriffe auf Unternehmen und Regierungsnetzwerke verwendet, um diese mit Ransomware zu verschlüsseln und folglich zu erpressen. Auch in der Schweiz sind mehrere Dutzend Fälle bekannt. Im Januar 2021 erfolgte dann der «Takedown» des Botnetz, geführt durch EUROPOL[2] in der Aktion Ladybird. Danach wurde es ruhig um Emotet. Nun ist der Trojaner zurück.



Die Wiederbelebung von Emotet ermöglicht hat der Trojaner «TrickBot». IT-Sicherheitsexperten haben beobachtet[3], dass dieser Mitte November auf bereits infizierten Windows Geräten Emotet nachgeladen hat. Gut möglich, dass sich die Emotet-Gang bei TrickBot eingekauft hat, um neue Bots zu rekrutieren («Pay-Per-Install» - PPI). Auf diesen wurden auch sogleich E-Mail Konversationen aus den Postfächer von Microsoft Outlook und Mozilla Thunderbird gestohlen, um diese mittels «E-Mail conversation hijacking» (auch bekannt als «Dynamit-Phishing») für die Weiterverbreitung von Emotet zu verwenden. Diese Technik wurde bereits 2020 von Emotet für die Weiterverbreitung verwendet. Dabei werden bestehende E-Mail Konverstationen gestohlen und die Malware daran angehängt. So erscheint es für das Opfer glaubwürdiger und die Wahrscheinlichkeit, dass jemand auf das Attachment klickt steigt.

Auch sonst hat sich am «Modus Operandi» von Emotet nicht viel geändert. Der Trojaner verwendet weiterhin Macro-Code in Microsoft Office Excel und Word Dokumenten, welche beim Ausführen Emotet von gehackten Webseiten aus dem Internet lädt.

Aktuell befindet sich das Emotet Botnetz und dessen Infrastruktur weiterhin im Aufbau. Darauf lässt das Volumen der Emotet Spam-Emails sowie die Anzahl der (vergleichsweise) wenigen aktiven Emotet Botnetz C&C Servern schliessen. Während die Spam-Kampagnen anfänglich gegen europäische und amerikanische Internet Nutzer gerichtet waren, kamen in der KW 47 weitere Länder, darunter Japan, Australien und auch die Schweiz dazu. In der Schweiz war letztlich lediglich das Emotet Botnetz «epoch5» aktiv (Emotet ist in verschiedene Botnetze aufgeteilt, die jeweils zu unterschiedlichen Zeiten neue Payloads erhalten und die über eine in sich geschlossene C&C Infrastruktur verfügen).

[1] https://twitter.com/Cryptolaemus1/status/1460302706954981385

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

[3] https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back/

GovCERT beobachtet die Situation genau und hat bereits am 15. November mit der Sperrung von aktiven Emotet Botnetz C&C Servern begonnen. Organisationen, welche die BGP Firewall (MELANI BGP feed) und MELANI RPZ (oder den Secure DNS Resolver) verwenden, erhalten bereits automatisch einen Grundschutz gegen Emotet und TrickBot.

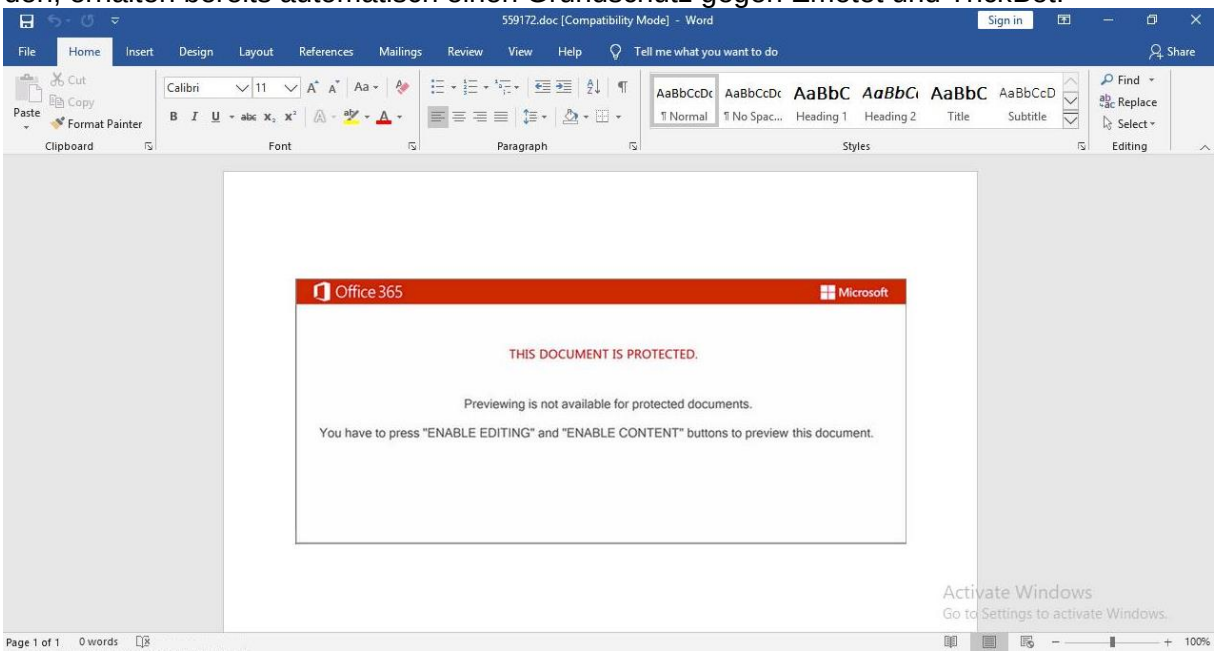


Figure 1 - Emotet Office Word Dokument

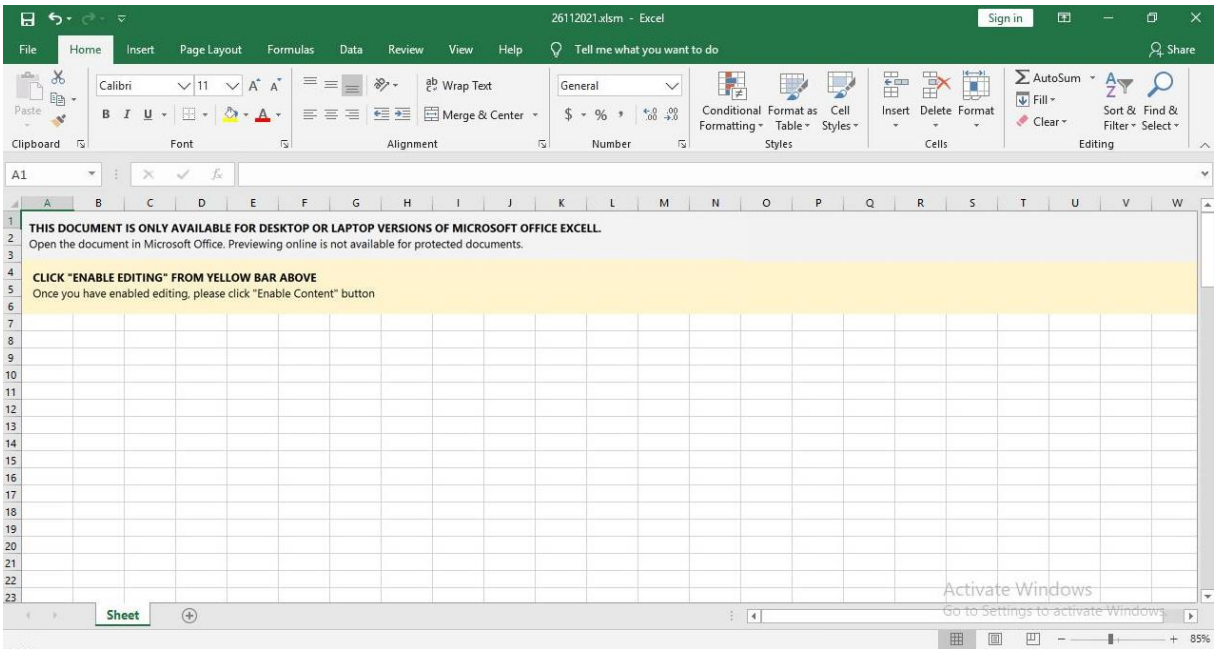


Figure 2 - Emotet Office Excel Dokument

«BlackMatter» Ransomware Gang stellt Aktivitäten ein

Im November gab die Gang hinter der «BlackMatter» Ransomware bekannt, dass diese ihre Aktivitäten wohl einstellen wird. Bei BlackMatter handelt es sich um eine Neuauflage der einschlägig bekannten Ransomware «DarkSide», welche unter anderem durch Cyberangriffe

auf den US-Pipelinebetreiber Colonial Pipeline und den Technologiekonzern Toshiba bekannt wurde. Auf einem von «BlackMatter» betriebenen Online-Portal, wo die Gruppierung ihren «Ransomware-as-a-Service» anbietet, gab die Gruppierung am 1. November 2021 bekannt, dass diese ihre Aktivitäten «aufgrund von Druck von lokalen Behörden» einstellen werden. Gemäss deren eigenen Aussagen steht «ein Teil des Teams nicht mehr zur Verfügung». Die Vermutung liegt nahe, dass einige Akteure der Gruppierung verhaftet wurden oder aus Angst vor Repressionen durch Behörden den Rückzug aus den BlackMatter Aktivitäten angekündigt haben.

```
Due to certain unsolvable circumstances associated with
pressure from the authorities (part of the team is no
longer available, after the latest news) - the project is
closed. After 48 hours, the entire infrastructure will be
turned off, it is allowed to:

-Issue mail to companies for further communication.
-Get decryptors, for this write "give a decryptor" inside
the company chat where they are needed.

We wish you all success, we were glad to work.
```

Quelle: VX-UNDERGROUND

Cyber-Angriff gegen Gesundheitseinrichtungen

Auch im November wurden mehrere Cyber-Angriffe gegen Gesundheitseinrichtungen im Ausland bekannt. Ein kurzer Überblick:

In Kanada wurden gleich mehrere Cyber-Angriffe auf Organisationen im Sektor Gesundheit bekannt [4] [5]. Vom Angriff ebenfalls betroffen war die Notfallnummer «911», welche gemäss Bürgerinnen und Bürger während Stunden nicht mehr erreichbar war. Zeitweise wurde in den Arztpraxen und Spitäler auf Stift und Papier umgestellt, da einen Zugriff auf die Systeme nicht mehr möglich war. Folge dessen mussten auch Termine für Chemotherapien, Röntgen und Operationen verschoben oder abgesagt werden. Während zunächst keine weiteren Details zum Cyber-Angriff bekannt waren, liegt die Vermutung nahe, dass es sich um einen Ransomware-Angriff handelte.

In den Vereinigten Staaten von Amerika wurde das Krebszentrum von Las Vegas Opfer eines Ransomware-Angriffs[6]. Der Angriff wurde erst im November 2021 öffentlich, ereignete sich aber bereits im September. Weitere Informationen über den Ransomware-Angriff waren zunächst nicht bekannt.

In Deutschland wurde der IT-Dienstleister Medatixx Opfer eines Ransomware-Angriffs[7]. Der IT-Dienstleister bietet unter anderem Softwareprodukte für Ärzte an, welche in rund einem

[4] https://www.bleepingcomputer.com/news/security/canadian-province-health-care-system-disrupted-by-cyberattack/

[5] https://ottawacitizen.com/news/local-news/rideau-valley-health-centre-service-disrupted-due-to-cyber-security-incident

[6] https://www.databreaches.net/las-vegas-cancer-center-hit-by-ransomware-over-labor-day-weekend-3000-patients-notified/

[7] https://www.heise.de/news/Ransomware-Attacke-auf-Medatixx-Grossalarm-im-Gesundheitswesen-6260613.html

Viertel der deutschen Praxen im Einsatz sind. Da der IT-Dienstleister auch über Fernwartungssysteme bei den Kunden verfügt, droht ein sehr grosser Angriff auf das deutsche Gesundheitswesen, sollten diese Zugänge ebenfalls kompromittiert worden sein. Über das Ausmass des Cyber-Angriffs sowie eine Lösegeldforderung war zunächst nichts bekannt.

Empfehlungen:

- Gegen das Internet hin exponierte Systeme wie RDP, VPN Dienste, etc. müssen stets auf dem aktuellen Patch-Level gehalten werden. **Sicherheitsaktualisierungen müssen zeitnah eingespielt werden.**

- Administrationszugänge sollten nie ins Internet exponiert werden, sondern Beispielsweise nur über eine separate Netzzone («Management-Zone») zugänglich sein. Der Zugang auf eine solche Zone muss stark authentisiert (Zwei-Faktor-Authentisierung - 2FA) und sämtliche Zugriffe sollten aufgezeichnet werden. Geräte, welche für die Administration verwendet werden, sollten für keine anderen Zwecke gebraucht werden (insbesondere nicht für das Surfen im Web oder für E-Mails).

- **Remotezugänge** wie VPN und RDP sowie sämtliche andere Zugänge auf interne Ressourcen (z.B. Webmail, Sharepoint, etc) müssen zwingend mit einem zweiten Faktor abgesichert werden (**Zwei-Faktor-Authentisierung** – 2FA). Stellen Sie sicher, dass sie über einen genügend langen Zeitraum Logdaten aller erfolgreichen und fehlgeschlagenen Zugriffsversuchen haben. Speichern Sie diese Logdaten zentral und werten Sie diese regelmässig aus.

- 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** für den Gesundheitssektor (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, besser 3). 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**.

- Einsatz einer Liste wie URLHaus[8], um das Nachladen von Malware zu verhindern.

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

- Schützen und Überwachen sie zentrale Ressourcen wie ein Active Directory und bereiten Sie Notfallpläne für eine mögliche Kompromittierung vor.

- Nehmen Sie Meldungen von Behörden betreffend IT-Sicherheitsprobleme in Ihrem Unternehmen ernst. Bei Zweifel der Authentizität einer Meldung, fragen Sie telefonisch bei der Absenderbehörde nach.

- Stellen Sie sicher, dass Sicherheitsupdates zeitnah eingespielt werden. Hoch kritische Sicherheitsupdates müssen zudem sofort eingespielt und dürfen nicht auf das nächste Wartungsfenster verschoben werden.

- Wählen Sie Ihre Zulieferer (Supplier), insbesondere solche von IT-Dienstleistungen, sorgfältig aus und achten Sie darauf, dass Ihr Dienstleister «Best Practices» im Bezug zur Cybersicherheit ebenfalls umgesetzt hat. Stellen Sie vertraglich sicher, dass der Zulieferer Sie über relevante Cybervorfälle in seiner Firma sowie den möglichen Diebstahl von Kundendaten (Data breach) zeitnah informiert. Gewähren Sie Dienstleistern keine uneingeschränkten Remote Zugänge und sichern Sie diese soweit als möglich ab.

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 GovCERT Dienstleistungen:

outreach@govcert.ch