Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
GovCERT.ch

Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	30. Dezember 2020
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN

Aktuelles (Dezember 2020)

Die Situation im Bereich Cyber Sicherheit bleibt aufgrund von aktuellen Angriffen auf kritische Infrastrukturen und im Speziellen auf Organisationen im Gesundheitssektor sowie den weiterhin hohen COVID19 Neuinfektionen angespannt.

- Die im November 2020 gemeldeten DDoS Angriffe gegen Grossunternehmen und Betreiber kritischer Infrastrukturen in der Schweiz hat sich im Dezember 2020 fortgesetzt. Jedoch ist die Anzahl der Angriffe stark gesunken.
- Die von uns detektierten Malspam-Wellen bleiben auf einem hohen Niveau.
- Nach einer Pause im November konnten wir kurz vor Weihnachten wieder Emotet-Aktivität feststellen.
- Mitte Dezember wurde bekannt, dass vermutlich staatliche Akteure durch eine Kompromittierung einer legitimen, breit eingesetzten Software des Herstellers SolarWinds (SolarWinds Orion) Angriffe auf hochrangige Ziele weltweit durchgeführt haben (Supply Chain Attacks)[1].

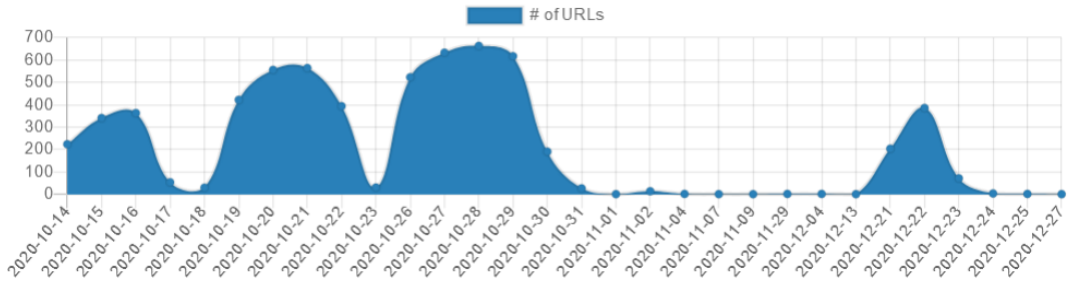
Emotet ist zurück

Emotet, auch bekannt unter dem Namen «Heodo» und «Geodo», hat sich nach einer über einmonatigen Pause zurückgemeldet. Als Infketionsvektor verwenden die Akteure hinter Emotet weiterhin Emails (Malspam), welche einen Link auf ein schädliches Word-Dokument enthalten oder ein entsprechendes Office Dokument als Dateianhang beinhalten. Das Word-Dokument ist so konstruiert, dass mittels Social Engineering versucht wird, den Benutzer dazu zu bringen, Makros für das Dokument zu aktivieren. Gelingt dies, lädt das bösartige Makro-Script den Emotet Payload aus dem Internet nach.

[1] https://www.solarwinds.com/securityadvisory

Die Letzte Malspam-Kampagne konnte NCSC am 31. Oktober 2020 sichten. Nach einer längeren Pause von über einem Monat haben die Akteure hinter Emotet am 21. Dezember erneut damit begonnen, Malspam zu versenden, um ihr Botnetz zu vergrössern.

Die folgende Grafik zeigt die Aktivität von Emotet (gemessen an der Anzahl neu gemeldeter URLs welche Emotet verbreiten) über die letzten 2 Monate. Klar ersichtlich sind die teilweise sehr grossen Malspam-Kampagnen im Oktober, die von Emotet eingelegte Pause im November sowie die Rückkehr kurz vor Weihnachten.



Emotet Aktivität von Oktober bis Dezember 2020

Akteure verwenden Emotet weiterhin dazu, Unternehmensnetzwerke auszuhorchen, um diese Zugänge dann im Darkweb an andere Akteure weiter zu verkaufen. Dies führt früher oder später in den meisten Fällen zu einer Verschlüsselung grosser Teile des Netzwerks durch Ransomware. **Das NCSC beurteilt die Bedrohung durch Emotet daher weiterhin als hoch**.

Empfehlungen:

- Sperrung von IP-Adressen bekannter Botnetz Command&Control Server (C&Cs) durch Implementierung des **MELANI BGP Feeds und/oder der Response Policy Zone oder des Secure Resolvers** (Kontakt: incidents@govcert.ch). Ob Sie oder Ihr Provider diesen 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: incidents@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**.

Supply Chain Attack durch SolarWinds

Mitte Dezember 2020 wurde bekannt, dass es staatlichen Akteuren gelungen ist, den automatischen Update-Mechanismus von SolarWinds Orion zu kompromittieren. Die Software wird von Grossunternehmen und Behörden Weltweit für die Überwachung und Verwaltung von IT-Infrastrukturen eingesetzt. Durch die Kompromittierung des Update-Mechanismus wurden Unternehmen weltweit über die automatische Update-Funktion und somit ohne Interkation eines Administrators mit Malware namens SUNBURST und SUPERNOVA infiziert. FireEye und weitere Firmen haben eine vertiefte Analyse der Schadsoftware durchgeführt[2] [3].

NCSC hat Kenntnis von einigen, wenigen Opfern in der Schweiz und hat diese bereits kurz nach bekannt werden des Hacks informiert. Falls Sie SolarWinds Orion in Ihrem Netzwerk einsetzen empfiehlt Ihnen das NCSC dennoch folgendes.

Empfehlungen:

- **Überprüfung der Systeme** und allfällig vorhandenen Logs nach den Indicators Of Compromise. Für kritische Infrastrukturen sind die entsprechenden IOCs in MISP Event 6154 verfügbar. Öffentlich verfügbare IOCs werden unter anderem von FireEye auf GitHub publiziert[4].

- **Einschränken des Internet-Zugriffs für Server** auf nur für den Betrieb explizit nötigen Internet-Ressourcen wie z.B. Windows Update (Whitelist-Approach). Somit kann eine Infektion zwar nicht verhindert jedoch eine Kommunikation der Malware mit der Täterschaft somit Datenabfluss verhindert werden.

- Out of Band Management (Management über ein dediziertes LAN oder VLAN) für besonders heikle Komponenten (Netzwerk Monitoring, Router, Firewalls, Switches).

- Falls Ihr Unternehmen Microsoft 365 Defender einsetzt: https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

Angriffe auf Hersteller von COVID-19 Impfstoffen

Vereinzelt hat es Meldungen[5] über Angriffe auf Hersteller von COVID-19 Impfstoffen gegeben. Leider sind uns bislang keine Details bekannt. Wir beobachten die Situation und werden informieren, sollten wir weitere Erkenntnisse haben. Eine Gruppierung, die in diesem Zusammenhang genannt wird, ist "Lazarus". Gemäss Kaspersky haben diese Akteure Angriffe gegen Impfstoffhersteller durchgeführt. IOCs aus diesen Angriffen finden sich hier: https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/

[2] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[3] https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

[4] https://github.com/fireeye/sunburst_countermeasures

[5] https://www.bleepingcomputer.com/news/security/us-treasury-warns-of-ransomware-targeting-covid-19-vaccine-research/

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 Services:

outreach@govcert.ch