Landespolizeipräsidium · Mainzer Straße 134-146. ·66121 Saarbrücken

Landespolizeipräsidium
LPP 2 Kriminalitätsbekämpfung/
Landeskriminalamt

Dezernat LPP 222

Dienst-gebäude: Hellwigstraße 8-10
66121 Saarbrücken

Bearbeiter_in: Schmitt M.O.KHK
Tel.: 0681 962 – 2431
Fax: 0681 962 –2445
E-Mail: cybercrime@polizei.slpol.de

Az: 38/2021

Datum: 18.11.2021

Information der
Zentralen Ansprechstelle Cybercrime (ZAC) des Landespolizeipräsidiums Saarland

Warnmeldung der zentralen Ansprechstelle Cybercrime (ZAC) Saarland vor

- **neuer Angriffswelle mittels Emotet**
- **immer noch verwundbaren Exchange Servern**

Emotet

Emotet galt bis Anfang 2021 als die mit gefährlichste Schadsoftware. Mit sehr ausgeklügeltem Phishing gelang es den Tätern auch in gut gesicherte Netze einzudringen. Anfang des Jahres gelang mehreren Behörden der Schlag gegen das Emotet-Netzwerk: Es konnten eine Vielzahl von Server außer Verkehr gezogen werden.

Jetzt konnte festgestellt werden, dass mit der Malware Trickbot infizierte Computer angefangen, neue Emotet-Varianten zu installieren.

Seit Sonntag, 14.11.2021, haben mit Trickbot infizierte Systeme angefangen, neue DLLs herunterzuladen, die die automatisierten (Antivir-)Analysesysteme als Emotet klassifizierten. Es handelt sich offenbar um eine modifizierte Version der altbekannten Schadsoftware.

Code und Arbeitsweise der neuen Version ähneln den bekannten Emotet-Samples. Laut einer Antivirenfirma nutzen die Server nun anders als die letzten Emotetversionen aus dem vergangenen Jahr https mit selbst signierten Zertifikaten zur Absicherung der Kommunikation und die Verschlüsselung zum Verstecken der Daten ist leicht verändert.

Wie schon in der Vergangenheit arbeiten die Täter hinter Emotet offenbar wieder mit den Trickbot-Tätern arbeitsteilig zusammen.

Schlussendlich droht neben Datenverlust die Verschlüsselung kompromittierter Systeme.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

Vorgehensweise - Dynamit-Phishing

Durch die Täter hinter wird Phishing, sogenanntes Dynamit-Phishing, angewandt. Dabei erhalten die ausgewählten Ziele personalisierte E-Mails, die scheinbar von Kollegen oder Geschäftspartnern stammen und sogar frühere E-Mails des Empfängers zitieren, welche zuvor automatisiert ausgespäht wurden. Ziel ist es, den oder die Empfänger/in zum Öffnen der angehängten Office- oder Excel- Datei zu verleiten.

In der aktuellen Version verschickt Emotet dazu speziell präparierte Dokumente als .docm, xlsm oder passwortgeschützte ZIPs an potenzielle Opfer.

Warnmeldung des Bundesamtes für Sicherheit in der Informationstechnik (BSI), siehe Anlage.

Exchange

Aktuell laufen in Deutschland noch tausende über das Internet erreichbare Exchange-Server, deren Basis nicht mehr im Support befindliche Versionen sind.

Seit geraumer Zeit werden solche Exchange-Server angegriffen und zu kriminellen Zwecken missbraucht.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI), CERT-Bund, warnt derzeitig, dass in Deutschland noch tausende öffentlich erreichbare potenziell verwundbare Server in Betrieb sind.

Derzeit sind noch immer über 8000 direkt über das Internet via Outlook Web Access (OWA) erreichbare Exchange-Server mit der veralteten Version 2010 online. Das sind rund 15 Prozent alle über OWA erreichbaren Exchange Server in Deutschland.

Für Exchange 2010 ist der Support je nach installiertem Service Pack schon seit acht Jahren ausgelaufen. Den Großteil machen Exchange 2010 mit SP3 aus. Hier lief der Support vor rund einem Jahr aus. Diese Ausgaben bekommen seitdem keine Sicherheitsupdates mehr; sie sind durch Attacken gefährdet.

Die Polizei rät:

- Installieren Sie stets sämtliche Sicherheitsupdates für Anwendungsprogramme und Betriebssysteme.
- Nutzen Sie Virenschutzsoftware und halten Sie diese stets aktuell.
- Fertigen Sie regelmäßig Sicherungen (Backups) Ihrer Daten an.
- Öffnen Sie auch bei vermeintlich bekannten Absendern nur mit Vorsicht Dateianhänge und Links in E-Mails.
- Verifizieren Sie den Absender der Email (Mit der Maus auf angezeigten Absendername, damit die Emailabsendeadresse angezeigt wird / ggf. Rückruf beim vermeintlichen Absender).
- Überprüfen Sie den Patchstand bei der Anwendung von Programmen wie Exchange. Insbesondere ob nicht noch Test- oder veraltete Installationen solcher Anwendungen auf den Systemen vorhanden sind.

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken

- *Was Sie tun können, wenn Sie betroffen sind:*

  - Trennen Sie das infizierte System sofort vom Internet.
  - Informieren Sie Ihr Umfeld über die Infektion, da Ihre Email-Kontakte besonders gefährdet sind.
  - Ändern Sie alle auf dem betroffenen System verwendeten Zugangsdaten.
  - Setzen Sie den infizierten Rechner neu auf (Neuinstallation).
  - Erstatten sie Strafanzeige bei der Polizei.

Quellen:

https://twitter.com/certbund/status/1460942013256323072
https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-microsoft-exchange-server-2019-2016-and-2013-may-11-2021-kb5003435-028bd051-b2f1-4310-8f35-c41c9ce5a2f1
https://www.heise.de/news/Exchange-Server-jetzt-patchen-Angreifer-suchen-aktiv-nach-neuer-Luecke-6158190.html
https://www.heise.de/news/Patchday-Microsoft-warnt-vor-Attacken-auf-Excel-und-Exchange-6263036.html
https://www.heise.de/hintergrund/Das-bedeutet-Microsofts-neuer-Notausschalter-fuer-Exchange-6206287.html

Liste von IP's welche Emotet Schadsoftware verteilen:

https://feodotracker.abuse.ch/browse/emotet/

Mit freundlichen Grüßen,
i.A.
KHK M.O. Schmitt

Zentrale Ansprechstelle Cybercrime (ZAC)
Ansprechpartner:
KHK Marc Schmitt
Telefon: 0681-962-2448
Telefax: 0681-962-2445
Email : cybercrime@polizei.slpol.de
Web: https://www.saarland.de/polizei/DE/themen-aufgaben/kriminalitaet/zac/zac_node.html

Landespolizeipräsidium Saarland
Direktion 2 Kriminalitätsbekämpfung/Landeskriminalamt
Hellwigstraße 8-10
66121 Saarbrücken