Bayerisches Landesamt für Verfassungsschutz

Cyber-Allianz-Zentrum Bayern

Bayerisches Landesamt für Verfassungsschutz · Postfach 45 01 45 · 80901 München

Ihre Zeichen, Ihre Nachricht vom	Unser Zeichen		München
	337-S-060000.1/306/3		08.06.2016
Bearbeiter/in	**E-Mail**	**Telefon**	**Telefax**
Hr. Dr. Stelte	caz@lfv.bayern.de	089 31201-222	

Warnmeldung - Phishing-Email mit infiziertem Wordattachment

Sehr geehrte Damen und Herren,

im Rahmen des Wirtschaftsschutzes möchten wir Sie auf eine aktuelle Email-Kampagne mit einer infizierten Word-Datei hinweisen. Hierbei wird vorgegeben eine Rechnung per Email an LinkedIn-Nutzer zu versenden.

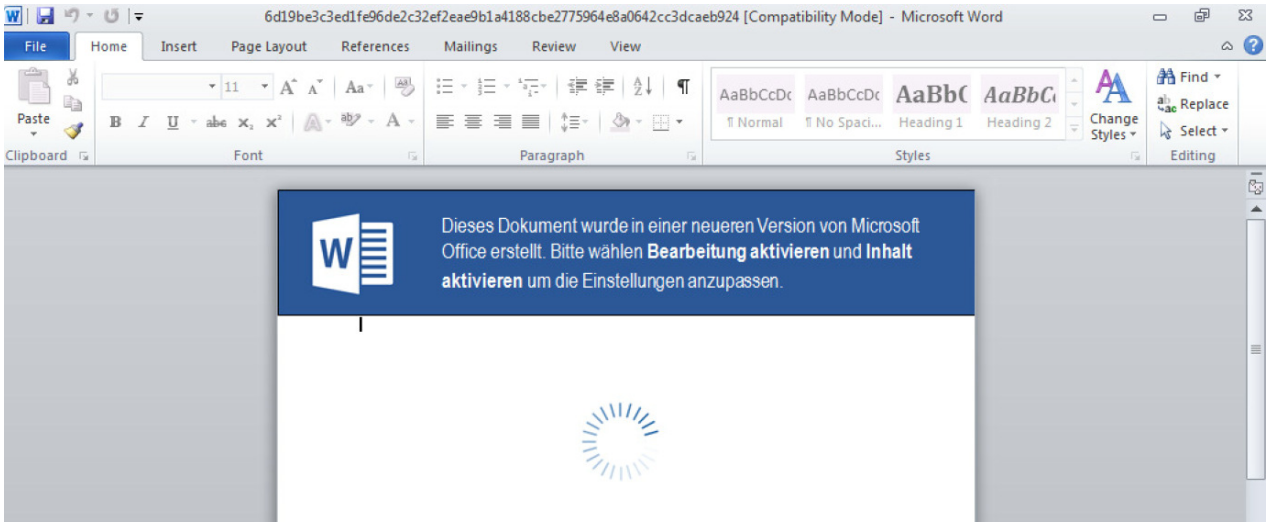

Abbildung 1: Word-Datei - Quelle: hybrid-analysis.com

Telefon: 089 31201-0
Telefax: 089 31201-380

E-Mail: poststelle@lfv.bayern.de
Internet: www.lfv.bayern.de

Knorrstraße 139 · 80937 München
U2 (Frankfurter Ring)

Der Email ist eine Word-Datei beigelegt, die VBA-Makros enthält. Der Inhalt des Dokumentes soll den Nutzer zu einer Aktivierung der Makros verleiten. Bei Aktivierung der Makros wird zunächst eine Geo-Lokation des Opfers über den Webdienst MAXMIND vorgenommen.

URL https://www.maxmind.com/geoip/v2.1/city/me
REFERER: https://www.maxmind.com/en/locate-my-ip-address
USER-AGENT: Mozilla/5.0 (Compatible; MSIE 9.0; Windows NT 7.1; Trident/5.0)

Die über den Webdienst erhaltenen Informationen werden durch das Makro mit hinterlegten Zeichenketten verglichen. Nachfolgende Zeichenketten führen zu einem Abbruch des Makros:

Anonymous
Amazon
Bitdefender
Blackoakcomputers
Blue Coat Systems
Cisco Systems
Cloud
Data Center
Dedicated
ESET, spol
Russia
FireEye
Forcepoint
Hetzner
Hosted
Hosting
LeaseWeb
Microsoft
NForce
North America
OVH SAS
Security
Server
Strong Technologies
Trend Micro
Trustwave

Nach einer erfolgreichen Überprüfung der Gateway IP-Adresse wird versucht das Schadprogramm herunterzuladen und auszuführen. Hierbei sind uns zwei URLs für den Download bekannt:

http://kinzatops.com/catalog/worddata.bin
http://ledpronto.com/app/office.bin

Nach den jetzigen Erkenntnissen handelt es sich bei dem Schadcode um eine Variante des ZEUS Banking-Trojaners. Die Anti-Viren-Hersteller haben bereits aktuelle Signaturen zu diesem Trojaner erstellt.

Derzeit ist als Rückkanalweg die nachfolgende Domain / IP-Adresse bekannt:

skorianial.com
107.171.187.182
107.181.187.111

Es wird eine Verbindung über TCP Port 443 aufgebaut.

Sollten Sie hierzu ergänzende Informationen oder Fragen haben, stehen wir Ihnen gerne als Ansprechpartner zur Verfügung.

Sollten Sie durch diesen Angriff bereits geschädigt worden sein und eine Anzeige erstatten wollen, wenden Sie sich bitte an die Polizei unter zac@polizei.bayern.de.

Mit freundlichen Grüßen

gez. Schinabeck
Leitender Regierungsdirektor