Woche 12: Schadsoftware «FluBot» in der Schweiz wieder aktiv und Web-Administratoren erhalten Drohmails von angeblich ukrainischen Hackern

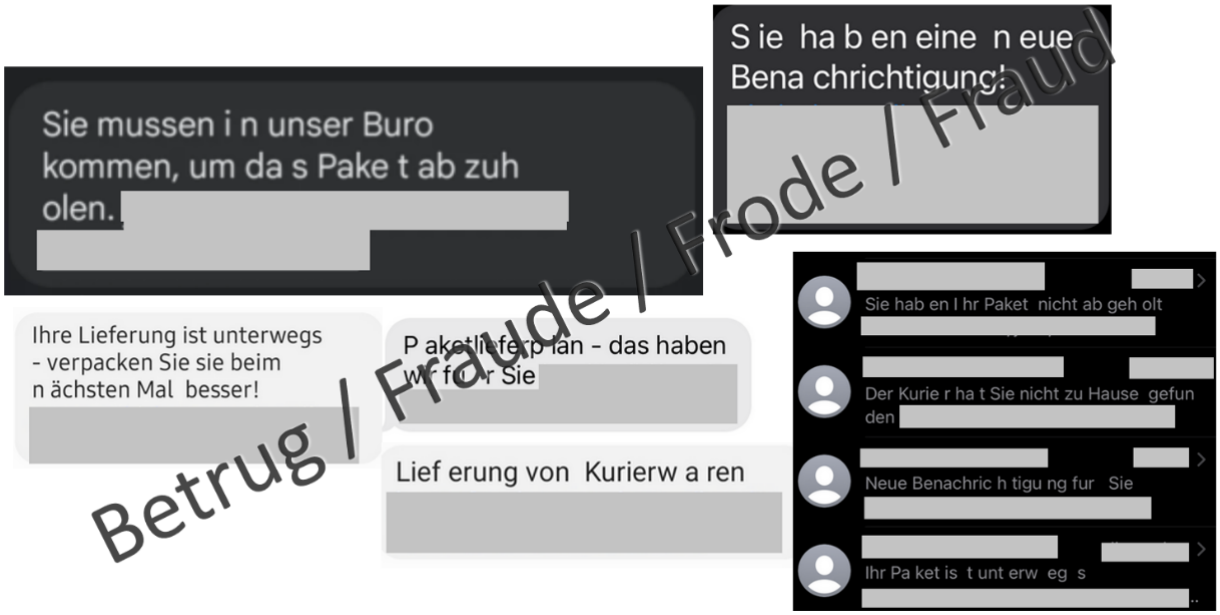
ncsc.admin.ch/22w12-de

Navigation

29.03.2022 - Der Meldeeingang beim NCSC war in der letzten Woche leicht erhöht. Dem NCSC wurden SMS gemeldet, mit welchen erneut versucht wird, das Opfer zu verleiten, die Schadsoftware «FluBot» auf dem Smartphone zu installieren. Zudem erhielten Website-Besitzer elektronische Post von angeblichen ukrainischen Hackern, welche vorgaben, die Website gehackt zu haben und einen «Spendenbeitrag» forderten.

Die Schadsoftware «FluBot» ist zurück

In der letzten Woche wurden dem NCSC zahlreiche SMS mit Benachrichtigungen zu angeblichen Paketlieferungen in diversen Textvarianten gemeldet. Bei der Formatierung gab es allerdings Gemeinsamkeiten: In den Wörtern waren jeweils zahlreiche Leerzeichen enthalten. Der Link unter dem Text führte auf eine Webseite, welche das Opfer aufforderte, eine Software des Paketdienstleisters auf das Android Smartphone herunterzuladen und zu installieren.



Beispiele versendeter SMS-Texte mit angeblichen Paketbenachrichtigungen

Bei der Software handelt es sich jedoch um die in der Schweiz nicht unbekannte Schadsoftware «FluBot». Die letzte grosse Welle traf die Schweiz im Herbst 2021. Damals wurden SMS mit einer angeblichen Sprachnachricht in grosser Zahl versendet. Das NCSC hat darüber berichtet (Wochenrückblick 41). International werden auch SMS mit dem Text «Bist Du das auf dem Video» beobachtet aber auch gefälschte Aufforderungen zur Aktualisierung von Browser oder Betriebssystem gehören zum Repertoire von «FluBot». Typischerweise wechseln die Angreifer ihre Zielgebiete in kürzester Zeit, meistens bereits nach wenigen Tagen. Kampagnen wurden seit Dezember 2021 vor allem in Australien und Deutschland beobachtet. In der Schweiz werden die SMS mit den Paketbenachrichtigungen seit dem 18. März 2022 versandt.

«FluBot» hat sich unter anderem auf den Diebstahl von SMS auf Mobiltelefonen spezialisiert. Ziel dabei ist, in den gestohlenen SMS so genannte Einmal-Passwörter zu finden. Nach einer Infektion wird zudem das ganze Adressbuch des infizierten Smartphones an den Kontrollserver der Angreifer gesendet. Das Smartphone erhält danach eine Liste mit Telefonnummern, die von anderen gehackten Smartphones stammen, an die es die bösartige SMS senden soll.

Auch wenn diese Schadsoftware lediglich Android-Geräte angreift, müssen sich auch Nutzende von Geräten mit dem iOS-Betriebssystem in Acht nehmen und sollten keine Links in SMS anklicken.

- **Installieren Sie keine Software, die ausserhalb der offiziellen Stores der Betriebssysteme angeboten wird**

- **Insbesondere sollten Sie keine Software installieren, welche Sie über einen Link in einer SMS oder über einen anderen Messenger-Dienst (WhatsApp, Telegram usw.) erhalten haben.**
- **Falls Sie dennoch eine solche Software installiert haben, sollten Sie das Gerät von einer Fachperson überprüfen lassen und während dieser Zeit weder Bankgeschäft noch Online-Einkäufe tätigen. Geben Sie auch keine Passwörter ein.**
- **Das Zurücksetzten des befallenen Geräts auf die Werkseinstellungen ist nahezu die einzige Möglichkeit, diese Schadsoftware vom Gerät zu entfernen.**

Angebliche Hacker aus der Ukraine fordern eine «Spende»

Das NCSC erhielt letzte Woche ausserdem mehrerer Meldungen zu Drohnachrichten an Website-Besitzende von angeblichen ukrainischen Hackern. Die Schreiben wurden jeweils über das Kontaktformular der Webseiten abgesetzt. Die Hacker gaben dabei vor, eine Schwachstelle in der Webseite gefunden zu haben und forderten den Webseitenbesitzer auf, eine «Spende» von 0.05 BTC (aktuell ca. 2000 CHF) auf ein vorgegebenes Bitcoin-Konto zu transferieren.

Sollte der Webseitenbesitzer der Forderung nicht nachkommen, dann werde die Seite gekapert und ein Banner eingeblendet, welches alle Besucher auffordere, der Ukraine zu helfen. Sollte das Banner durch den Besitzer entfernt oder die Schwachstelle geschlossen werden, werde das Banner erneut installiert und eine neue Schwachstelle gefunden. Sollte das nicht funktionieren, drohten die Angreifer, die Domäne bei der Registrierungsstelle dauerhaft zu löschen.

Anfrage: Hello. We are Ukrainian hackers and we hacked your site What do we want? We want you to make a donation in support of Ukraine to this Bitcoin (BTC) wallet by March 25 in the amount of 0.05 BTC, this is a small amount: If you do not make a donation, then a huge full-screen banner will appear on your site asking all visitors to your site to help Ukraine (your site will not be visible, only our banner), if you remove it, we will hang it again, if you fix the vulnerability, then we find a new one and hang the banner again. As a last resort, we will have the domain name registrar block your domain permanently.

Drohmail angeblich im Namen von ukrainischen Hackern

Dieses Schreiben war selbstverständlich nur ein «Bluff». Der Fall zeigt aber, dass die Tragödie des Krieges in der Ukraine in verschiedenster Weise auch von Betrügern für ihre Zwecke ausgenutzt wird. Das NCSC hat bereits am 8. März 2022 darauf aufmerksam. Auch die Kantonspolizei ZH hat letzte Woche vor Betrugsversuchen gewarnt.

- **Lassen Sie sich nicht einschüchtern. Melden Sie im Zweifelsfall verdächtige Nachrichten dem NCSC oder der Polizei.**
- **Natürlich sollten Sie aber Webserver und alle Webapplikationen auf dem neuesten Stand halten.**

- **Generell für Spenden gilt:**
  - **Gehen Sie nicht auf Kontaktaufnahmen per E-Mail ein**
  - **Vermeiden Sie Spendenzahlungen per Kreditkarte**
  - **Überweisen Sie keine Kryptowährungsguthaben**
  - **Versenden Sie keine Geschenkgutschein Codes (Google Play, Apple iTunes etc.)**
- **Am besten nutzen Sie Sie nur IBAN-Konten von Hilfswerken, welche ZEWO zertifiziert sind:**
  https://zewo.ch/de/

Aktuelle Zahlen und Statistiken

Die Anzahl Meldungen der letzten Woche nach Kategorien sind publiziert unter:

Aktuelle Zahlen

Letzte Änderung 29.03.2022