Verhindern von Malware-Ausbreitung in Datennetzen

Jakob Döring
Lucas Schröder
Nils Trampel

Chemnitzer StudentenNetz

14. März 2021

CSN
Chemnitzer StudentenNetz

Inhalt

CSN
Chemnitzer StudentenNetz

Überblick

- Internetprovider für Studenten in Wohnheimen
- 10 Wohnheime am Campus Reichenhainer Straße
- etwa 1800 aktive Nutzer
- Uplink: URZ, Deutsches Forschungsnetz

DFN Warnmails

- Information über Malwarebefall
- Manuelle Bearbeitung

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Details zu den Ereignissen pro IP:
================================================================================
IP-Adresse:    134.109.84.
Ereignistyp:   Bot
Zeitstempel:   2020-08-30T20:22:13+02:00
Anzahl:        1
Beschreibung: Auf dem System scheint eine Bot-Software betrieben zu
              werden, die versucht, einen HTTP- oder IRC-basierten Bot-
              Netz Control-Server zu erreichen. Zu den unterschiedlichen
              Malwaretypen finden Sie unter der folgender Webseite mehr
              Informationen: http://www.cert.dfn.de/index.php?id=bot

Zuletzt gesehen            IP-Protokoll   Quellport          Ziel-IP    Zielport  Malware
--------------------------------------------------------------------------------
2020-08-30T20:22:13+02:00                    27994                          80  android.bakdoor.prizmes
   occurences: 1

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Abbildung: Ausschnitt aus einer DFN Warnmail

CSN
Chemnitzer StudentenNetz

Netzwerk

- Identifizierung der Nutzer im Netz
- Nutzernetzwerke:
  - Geteilte /23
  - Gateway am Router
- Quarantänenetzwerke:
  - Gleiche Adressierung wie normale Netze
  - Gateway an Proxy VM
- Verschieben von Nutzerports in Quarantänenetze

Proxy

- squid
- Selbstsignierte Zertifikate für HTTPS
- Nur Whitelist erlaubt
  - TU Chemnitz Debian Mirror
  - Antivirus
  - Windows Updates

Prozess

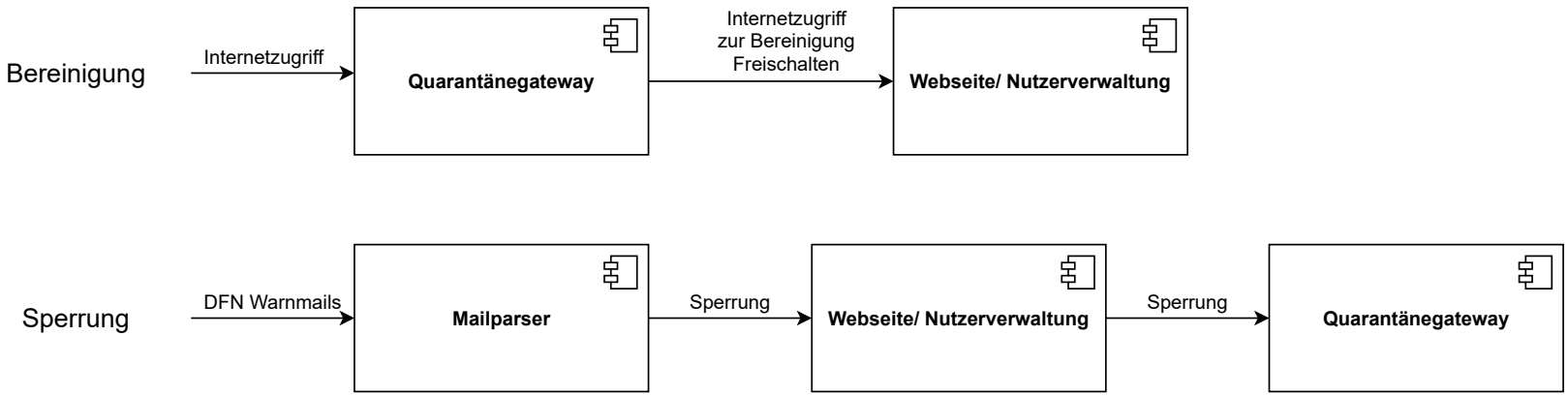


Abbildung: Prozessablauf

Implementierung

Mailverarbeitung

- Informationen aus der DFN Warnmail extrahieren
- Sperrung des Nutzers auslösen

Implementierung

Informationen in der Warnmail

- IP-Adresse des Nutzers
- Zeitpunkt
- Grund der Warnung
- Angriffsziele
- Informationen über Malware

Implementierung

Verarbeitung

- Python Skript
- DOM-Parser
- REST-API

Implementierung

Webseite - Überblick

- Django Projekt
- Verwaltung von
  - Nutzern
  - Nutzerhost
  - Portzuordnungen
  - Infrastruktur
  - Interne Hosts
- Statusseite

Implementierung

Webseite - APIs

`POST /api/v2/quarantine/lock`

- Nutzerstatus
- Ruft RPC von Gateway auf (Blockierung des Angriffsziels)
- Plausibilitätsprüfung

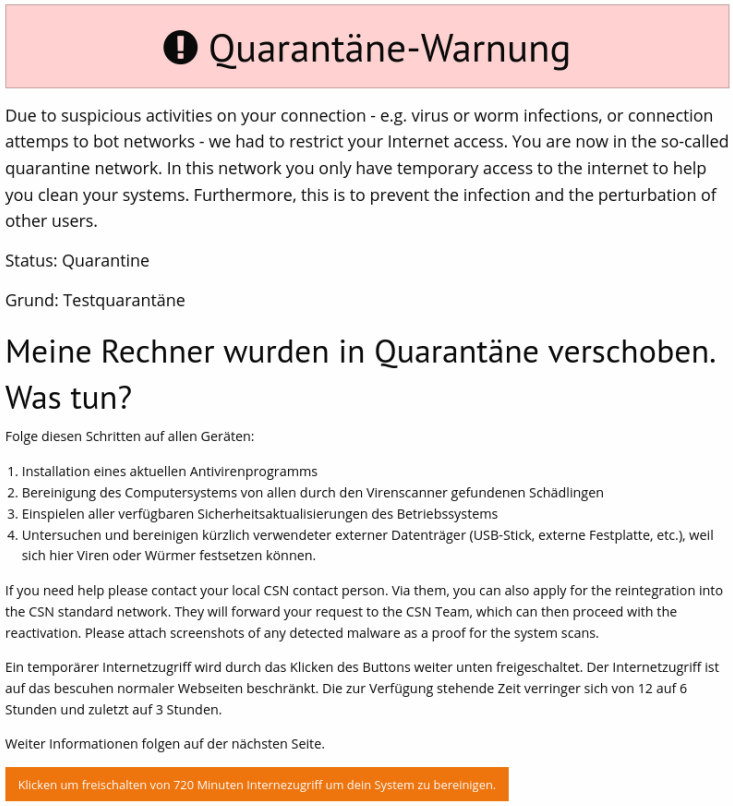
`GET /api/v2/quarantine/grants`

- Liste aller vollständig gesperrter IPs

Implementierung

Webseite - Nutzerseite

`GET /quarantine/<encrypted_mac>`



Quarantäne-Warnung

Due to suspicious activities on your connection - e.g. virus or worm infections, or connection attemps to bot networks - we had to restrict your Internet access. You are now in the so-called quarantine network. In this network you only have temporary access to the internet to help you clean your systems. Furthermore, this is to prevent the infection and the perturbation of other users.

Status: Quarantine

Grund: Testquarantäne

Meine Rechner wurden in Quarantäne verschoben. Was tun?

Folge diesen Schritten auf allen Geräten:

1. Installation eines aktuellen Antivirenprogramms
2. Bereinigung des Computersystems von allen durch den Virenscanner gefundenen Schädlingen
3. Einspielen aller verfügbaren Sicherheitsaktualisierungen des Betriebssystems
4. Untersuchen und bereinigen kürzlich verwendeter externer Datenträger (USB-Stick, externe Festplatte, etc.), weil sich hier Viren oder Würmer festsetzen können.

If you need help please contact your local CSN contact person. Via them, you can also apply for the reintegration into the CSN standard network. They will forward your request to the CSN Team, which can then proceed with the reactivation. Please attach screenshots of any detected malware as a proof for the system scans.

Ein temporärer Internetzugriff wird durch das Klicken des Buttons weiter unten freigeschaltet. Der Internetzugriff ist auf das bescuhen normaler Webseiten beschränkt. Die zur Verfügung stehende Zeit verringer sich von 12 auf 6 Stunden und zuletzt auf 3 Stunden.

Weiter Informationen folgen auf der nächsten Seite.

Klicken um freischalten von 720 Minuten Internezugriff um dein System zu bereinigen.

Abbildung: Quarantäneansicht für Nutzer

CSN
Chemnitzer StudentenNetz

Implementierung

Webseite - Administrationsseite

`GET /secure/user/<user_id>/quarantine`

- Netzzugriffe überwachen, hinzufügen
- Quarantäne beenden

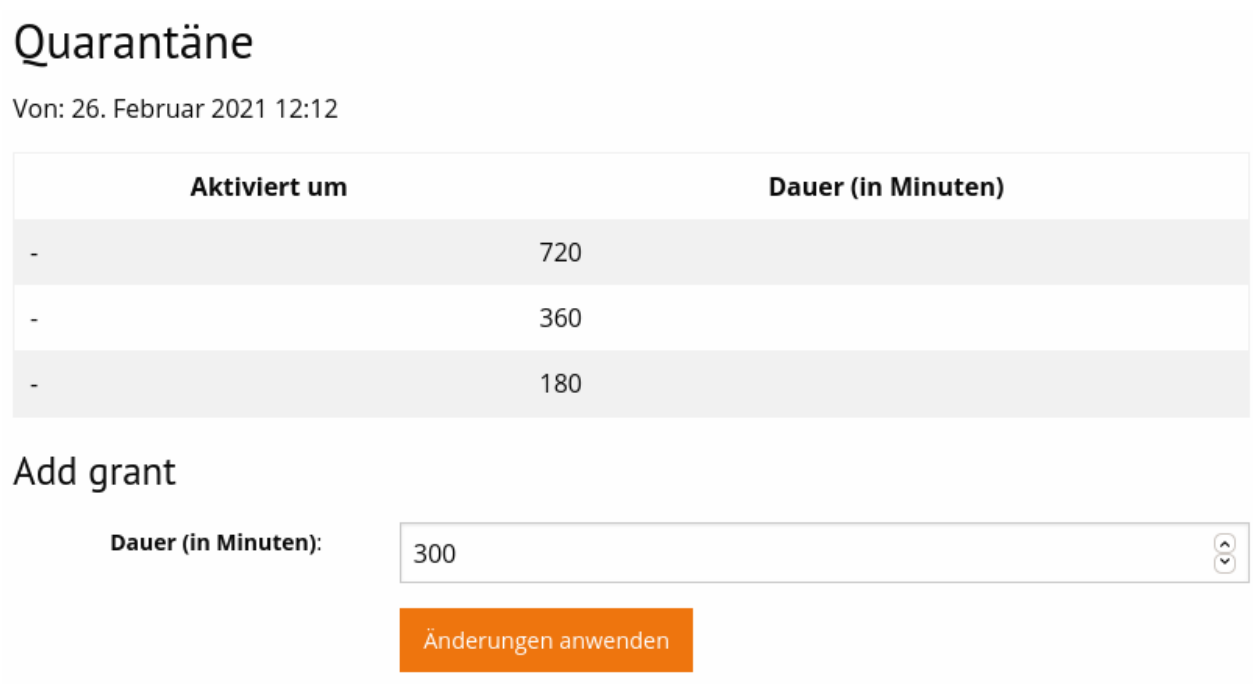


Abbildung: Verwaltung der Nutzerquarantäne

CSN
Chemnitzer StudentenNetz

Implementierung

Anforderungen Quarantänegateway

Ziele:

- Personalisierte Informationen
- Eingebunden in CSN-Website
- Zeitlich beschränkte Selbstfreischaltung
- Kein Zugriff auf restliches Netzwerk oder Angriffsziele
- Existierende Lösung verwenden:
  - Frei und Open Source
  - Aktuell
  - Gut dokumentiert
  - Einfach automatisiert konfigurierbar

Implementierung

Betrachtete Anwendungen

- WiFiDog
- PacketFence
- CoovaChilli
- pfSense
- **OPNsense**

Implementierung

Problem 1 - Personalisierte Website

- Persönliche Informationen nur in Nutzerdatenbank
- OPNsense hat keinen direkten Zugriff

Implementierung

Problem 2 - Freischaltung

- Voucher können nur vom CSN-Webserver aus generiert werden
- OPNsense geht von "physischen" Vouchern aus
- Freischaltung nur über HTML-Template möglich

Implementierung

Problem 3 - Ende der temporären Freischaltung

- Aktive Sitzungen werden nicht unterbrochen
- Hartes Timeout muss und fest für alle Nutzer gleich konfiguriert werden
- Keine individuellen/veränderbaren Freischaltezeiten möglich

Implementierung

Problem 4 - Automatische Sperrung von Angriffszielen

- Angriffsziele dürfen nicht erreichbar sein
- Firewallregeln müssen automatisiert hinzugefügt werden
- Plugin ist schlecht dokumentiert
- Fehlerhaft

Implementierung

Fazit

- Sehr fragile Lösung
- Viele ungelöste Probleme
- Nicht benötigte Funktionalität

Neu-Implementierung

Captive Portal

Nutzergruppen

Nicht aktiviert default state	Aktiviert
Netzblockade*	Freischaltung*
Umleitung zum Web-Portal	
	Zeitbeschränkung ← automatische Rückkehr

* mit Ausnahmen

Captive-Portal-Router

Architektur - Eigenschaften

- Adressen: DHCP
- Nutzergruppierung nach Source-MAC
- Protokoll-/Port-/Adress-basiertes Firewalling
- HTTP-Weiterleitung zu Portal
- API für Nutzerfreischaltung

Captive-Portal-Router

Aufbau

Grundlagen

Linux-Host als Router, 2 Interfaces, DHCP-Server, iptables + ipset, Python

Komponenten

fw_setup	*ipsets* und *iptables*-Regeln konfigurieren
http_redirector	HTTP-Server für Redirect zum Web-Portal
xmlrpcapi	Nutzer freischalten, sperren; Firewall-Blacklisting

Captive-Portal-Router

Firewall

ipset

- Freigeschaltete Nutzer

```
ipset create activated_quarantine_macs hash:mac
ipset add activated_quarantine_macs 01:23:45:67:89:ab
```

- IP-Blacklist

```
ipset create blocked_targets hash:ip
ipset add blocked_targets 192.0.2.1
```

iptables

Captive-Portal-Router

Firewall

ipset

iptables

- DNS-Umleitung

```
iptables -t nat -A PREROUTING -p udp
  --dport 53 -j DNAT --to-destination [DNS-Server]
```

- Umleitung gesperrter Nutzer

```
iptables -t nat -A PREROUTING_DEACTIVATED_USERS -p tcp
   --dport 80 -j DNAT --to-destination [Device-IP]:80
```

- Blocken nach IP-Blacklist

```
iptables -A FORWARD -m set --match-set
   blocked_targets dst -j DROP
```

- Gruppenbasierte Netzfreigabe

```
iptables -A FORWARD_DEACTIVATED_USERS -p tcp -m multiport
   --dports 80,443,[...] -m set --match-set important dst
   -j ACCEPT
iptables -A FORWARD_ACTIVATED_USERS -p tcp
   -m multiport --dports 80,443,[...] -j ACCEPT
```

Captive-Portal-Router

HTTP-Umleitung

Ermittlung der MAC-Adresse

Linux-Bordmittel:

```
$ ip neigh show
[...]
192.0.2.5 dev eth1 lladdr 01:23:45:67:89:ba REACHABLE
```

→ HTTP-302-Redirect nach

`https://example.org/portal/?mac=01:23:45:67:89:ba`

Verschlüsselung möglich

Problem: Manipulation fremder Freischaltungen in gemeinsamer Layer-2-Domain → Verschlüsselung der MAC mit AES Crypt

Captive-Portal-Router

API

auf Basis von XML RPC

reload	Neukonfiguration der Firewall
activate	Nutzerfreischaltung für *n* Minuten
clear_activations	Entfernen aller Nutzerfreischaltungen
block	Neufassung der Blacklist

Ergebnis

- voll funktionales selbstgebautes System[1]
- Inbetriebnahme Oktober 2020
- Rund 30 Quarantänefälle
- Begrenzte Stabilität des *HTTPServer*s aus Python
  - Abstürze durch HTTP-Requests von Nutzergeräten aus exotischen Ländern
  - Alternative: Flask-Framework mit *uWSGI*
- kaum Meldungen zur Nutzererfahrung

[1] https://github.com/camelusferus/cpob

Vielen Dank für
die Aufmerksamkeit

Fragen?

web: www.csn.tu-chemnitz.de
mail: kontakt@csn.tu-chemnitz.de