# Inhaltsverzeichnis



# 1 Das erste Jahresdrittel 2021

## 1.1 Vorfälle und Aussendungen

### 1.1.1 DnSpooq

Am 2021-01-19 veröffentlichte JSOF eine Reihe von Schwachstellen in `dnsmasq`, einer populären DNS-Resolver Software für kleine Netzwerke, und nannte diese kumulativ “DnSpooq”.[1]

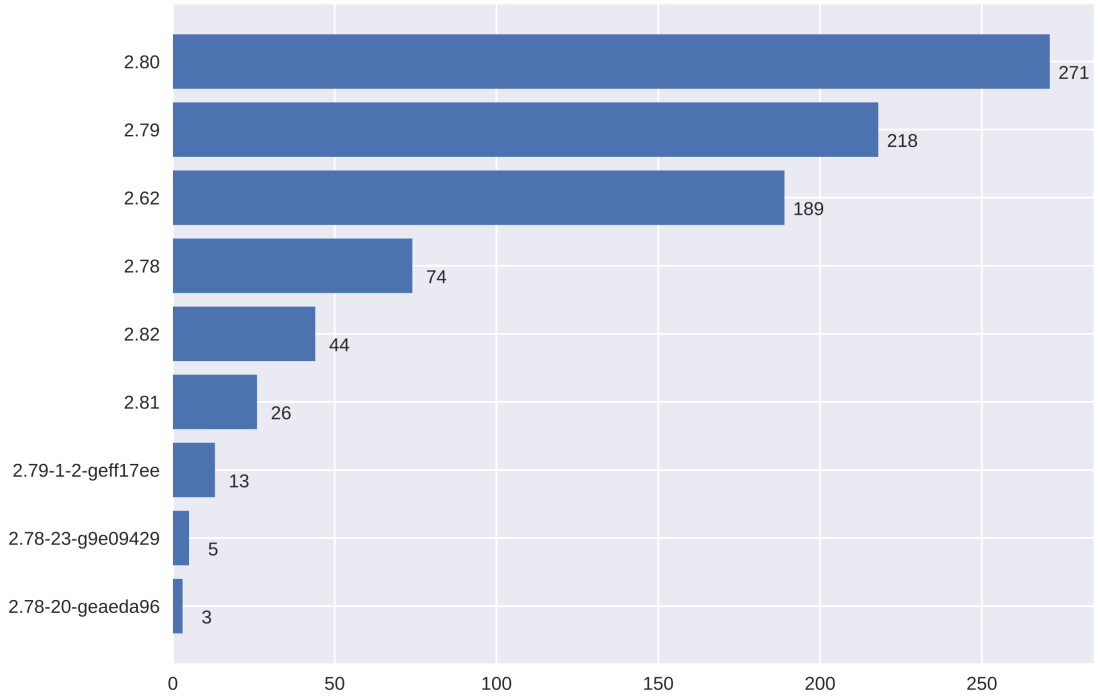


Abbildung 1: Häufigste `dnsmasq` Versionen in AT (Stand 2021-01)

[1] Nähere Informationen dazu finden sich im Blogpost von JSOF.

CERT.at suchte daraufhin via Shodan nach `dnsmasq` Installationen und deren Versionen in Österreich – die Ergebnisse haben wir in einem Blogpost festgehalten und eine kurze Übersicht zu den häufigsten Versionen ist in Abbildung 1 zu sehen.

Wir kontaktierten alle BetreiberInnen potentiell verwundbarer Installationen. Ein erneuter Scan, um festzustellen, wieviel sich bisher verändert hat, ist noch ausständig.

### 1.1.2 Emotet-Takedown und die Folgen

Emotet war für mehrere Jahre eine der gefährlichsten Malware-Arten; die Software wurde immer wieder mit neuen Features versehen und obwohl sie als Banking-Trojaner gestartet war, fand sie im späteren Verlauf ihrer Entwicklung vor allem als "Stager" Verwendung, d.h. Schadsoftware, die dazu genutzt wird, um andere Malware nachzuladen. Als solcher war Emotet beispielsweise bei diversen Ransomware-Gruppen beliebt.

Aber damit war Ende Jänner 2021 Schluss: Behörden aus Deutschland, den Niederlanden, UK, Litauen, Frankreich, der Ukraine, Kanada und den USA ist es in Zusammenarbeit mit Europol und Eurojust gelungen, die Infrastruktur hinter Emotet zu übernehmen[2] und die Malware damit effektiv auszuschalten. Dass diese Aktion ein so durchschlagender Erfolg wurde, ist keine Selbstverständlichkeit, wie nur wenige Monate zuvor der missglückte Takedown-Versuch gegen Trickbot gezeigt hatte.[3]

Im Zuge dieser Operation erlangten die ErmittlerInnen auch Zugriff auf zahlreiche Datenbanken der Kriminellen hinter Emotet und werteten sie aus. Dabei kamen unter anderem Informationen zu potentiell sämtlichen Opfern Emotets zu Tage, die an die jeweils zuständigen nationalen CERTs/CSIRTs weitergeleitet wurden – auf diesem Weg erhielt CERT.at entsprechend die Daten für Österreich.

Obwohl diese teilweise mehrere Jahre alt waren, kontaktierten wir alle potentiellen Opfer bzw. die jeweiligen BetreiberInnen der Plattformen, zu denen Login-Daten gestohlen worden waren, damit diese ihre KundInnen informieren konnten. Insgesamt erstellten wir im Jänner und Februar 14 Aussendungen zu Emotet mit mehreren zehntausend Betroffenen.

Abschließend ist anzumerken, dass die Behörden die Emotet-Malware so veränderten, dass sie sich am 25. April 2021 selbst deinstalliert hat und diese langjährige Bedrohung damit endgültig ein Ende gefunden hat. Leider ist aber davon auszugehen, dass die Kriminellen hinter Emotet mit ihrer Erfahrung und genügend Zeit ihre Infrastruktur mit neuer Schadsoftware wieder aufbauen können, oder dass andere Malware Emotets Platz einnimmt – von einem merklichen Rückgang der Cyber-Kriminalität ist jedenfalls auch nach Emotets Verschwinden nichts zu bemerken.

### 1.1.3 Microsoft Exchange Notfallpatches

Während mit CVE-2019-19781 a.k.a. "Shitrix" das Jahr 2020 direkt mit einer großflächig ausgenutzten Lücke begonnen hatte, ließ sich 2021 ein bisschen mehr Zeit, um dann aber wirklich alle Register zu ziehen: Anfang März wurden Notfallpatches für Microsoft Exchange, also Microsofts E-Mail-Server, veröffentlicht und die hatten es in sich: AngreiferInnen konnten durch die Kombination mehrerer Schwachstellen ohne jegliche Authentifizierung beliebigen Code als `NT Authority\SYSTEM` auf ungepachten Servern ausführen.

Aber damit nicht genug; diese Lücken wurden zum Zeitpunkt der Patch-Veröffentlichung bereits von mindestens einer Gruppe großflächig ausgenutzt, d.h. selbst wenn ein Server sofort

[2] Siehe dazu die Pressemitteilung von Europol.
[3] Mehr Informationen dazu finden Sie z.B. hier.

nach dem Erscheinen der Patches aktualisiert wurde, war nicht auszuschließen, dass er zuvor bereits kompromittiert worden war.

Microsoft veröffentlichte auch ein Script, mit dessen Hilfe verwundbare Installationen von außen identifiziert werden konnten. Dadurch war es uns möglich, schnell einen Scan für ganz Österreich zu erstellen und potentiell Betroffene zu informieren.

Bald wurde außerdem klar, dass viele AngreiferInnen Webshells auf kompromittierten Systemen hinterließen und einige Firmen und Organisationen machten sich daran, diese Webshells zu finden. Darunter war auch Shadowserver, die diese Informationen an nationale CERTs/CSIRTs weiterleiteten, um Opfer von erfolgreichen Attacken warnen zu können.[4]

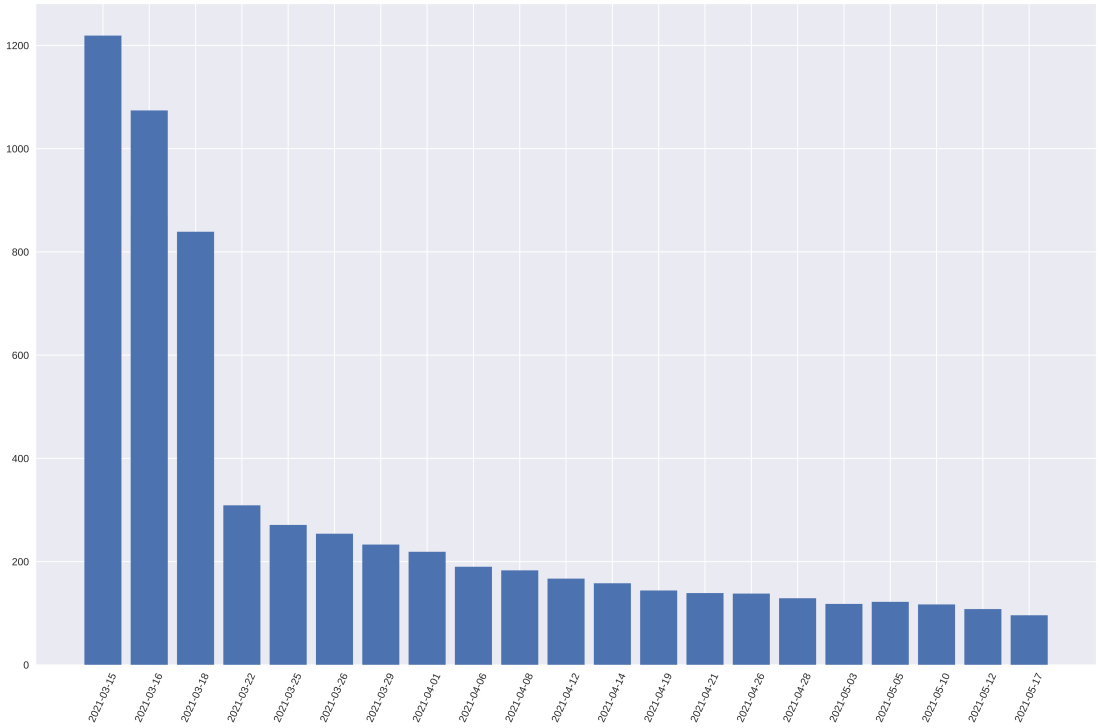


Abbildung 2: Anzahl verwundbarer Exchange Installationen in AT

Insgesamt verschickte CERT.at im März und April 20 anlassbezogene Aussendungen zu ungepatchten oder kompromittierten Microsoft Exchange Installationen in Österreich. Wie Abbildung 2 zeigt, sind nach unseren Scans Mitte Mai noch etwa 100 Exchange Server in Österreich nicht gepatcht, wobei wir natürlich nicht wissen, wieviele davon Honeypots o.Ä. sind.

### 1.1.4 SilverFish APT

Die IT-Sicherheitsfirma PRODAFT veröffentlichte im März einen Bericht zu einer Hacking-Gruppe, der sie den Namen “SilverFish” gegeben und auf deren Infrastruktur sie Zugriff erlangt hatten. Die AngreiferInnen arbeiteten nach den dort gefundenen Informationen in mehreren Teams und hatten geregelte Arbeitszeiten, was für eine hohe Professionalisierung spricht – leider nichts Ungewöhnliches bei kriminellen Gruppen im Cyber-Bereich. Der vollständige Bericht ist hier als PDF abrufbar.

[4] Siehe dazu Shadowservers Blogpost, in dem auch auf alle ihre Aktivitäten in Bezug auf die Exchange-Schwachstellen verlinkt wird.

Da PRODAFT bei Ihrer Arbeit auch eine Liste der Opfer erlangten, kontaktierten sie kurz vor der Veröffentlichung nationale CERTs/CSIRTs, in deren Ländern es Betroffene gab. Auf diesem Weg erhielt auch CERT.at die Liste mit den (wenigen) Opfern in Österreich und kontaktierte diese umgehend.

### 1.1.5 Pulse Connect Secure

Da die Anzahl von Unauthenticated RCEs in kritischer Software, die bei der Veröffentlichung von Updates oder Workarounds bereits aktiv ausgenutzt werden, in den ersten vier Monaten von 2021 eindeutig noch zu niedrig war, sorgte CVE-2021-22893 für Nachschub. Diese betraf Pulse Connect Secure, einer VPN Software der Firma Ivanti. Am 2021-04-20 wurden Workarounds veröffentlicht, "echte" Updates kamen allerdings erst rund zwei Wochen später.

CERT.at erhielt eine Liste von Pulse Connect Secure Installationen in Österreich und kontaktierte die BetreiberInnen mit der Bitte, die Workarounds möglichst schnell einzuspielen.

### 1.1.6 SonicWall Email Security

Am selben Tag, an dem Workarounds zur Schwachstelle in Pulse Secure Connect veröffentlicht wurden, gab auch SonicWall bekannt, dass es in einigen Versionen von SonicWall Email Security schwerwiegende Sicherheitslücken gibt, die in Kombination zur vollständigen Übernahme des Systems führen können und bereits aktiv ausgenutzt werden. Hier kam allerdings der mildernde Umstand hinzu, dass für den initialen Exploit ein administratives Web-Interface aus dem offenen Internet erreichbar sein muss, was für die Funktionalität der Software nicht notwendig ist.

FireEye erwähnt in einem Blogpost dazu, dass sie bei einem Internet-weiten Scan etwa 700 Installationen gefunden hatten, bei denen dieses Interface erreichbar war. CERT.at erhielt eine Liste der betroffenen Instanzen in Österreich und kontaktierte die BetreiberInnen.

## 1.2 Projekte und Konferenzen

### 1.2.1 MeliCERTes 2 (SMART-2018-2014)

In den ersten vier Monaten des Jahres floss die meiste Arbeit in das Identifizieren und Bewerten von Single-Sign-On Lösungen, da im Zuge des Projekts eine solche für das gesamte CSIRTs Network (CNW) gefunden und implementiert werden soll.

Dazu mussten initial die Bedürfnisse des CNW genau erfasst werden, um sicherzustellen, dass die sich daraus ergebenden Anforderungen auch erfüllt werden können. Dazu fanden mehrere (virtuelle) Treffen statt, deren Ergebnisse verschriftlicht wurden.

Das Ziel ist es, eine SSO Lösung zu schaffen, mit der sich MitarbeiterInnen sämtlicher Organisationen des CNW bei den zentralen Services anmelden können sowie bei Bedarf auch bei solchen, die andere Mitglieder des CNW lokal betreiben werden und für die Partner öffnen. Aktuell werden die zentralen Services teils von der ENISA, aber auch von Teams im CNW bereitgestellt. Außerdem wurde im April der erste Workshop zu IntelMQ für Angehörige des CNW durchgeführt.

Allgemeine Projektinformationen finden Sie auf unserer Webseite.

### 1.2.2 "Enhancing Cybersecurity in Austria" (2018-AT-IA-0111)

**International Engagement** Im Jänner 2021 fand das 62. TF-CSIRT Meeting virtuell statt, an dem Sebastian Wagner und Benedikt Olszewski für CERT.at teilnahmen.

Ebenfalls im Jänner 2021 nahm Thomas Pribitzer aus dem Handler Team an einem virtuellen TRANSITS I Training teil. TRANSITS-Trainings richten sich speziell an CERT/CSIRT MitarbeiterInnen und dienen dem Austausch und der Vernetzung in diesem Bereich.

Nach der Absolvierung eines SANS SEC504 Trainings Ende des Vorjahres bestand Thomas Pribitzer im Februar die Prüfung zum GIAC Certified Incident Handler (GCIH), wir gratulieren.

Im Februar 2021 hielten Sebastian Wagner und Birger Schacht einen Vortrag zum Thema IntelMQ auf dem virtuellen IHAP Meeting.

Am 13. CNW Meeting, das im März 2021 virtuell stattfand, nahmen Otmar Lendl und Wolfgang Rosenkranz für CERT.at teil.

**Tooling** Im Februar 2021 veröffentlichten wir gemeinsam mit der R&D Abteilung der Nic.at das Open Source Tool OpenINTEL-lookup: Dabei handelt es sich um ein User Interface und eine API, um Daten von OpenINTEL abzufragen.

OpenINTEL ist ein Projekt der Universität Twente in Zusammenarbeit mit SURFnet, SIDN Labs und NLnet Labs. Ziel ist es, sämtliche DNS-Einträge aller teilnehmenden DNS-Zonen aktiv abzufragen, um eine qualitativ hochwertige Datenbasis zu erstellen, die den Zustand des DNS-Systems im Laufe der Zeit erfasst.

Anfang März veröffentlichten wir IntelMQ 2.3.0 inklusive dazugehöriger Tools wie dem IntelMQ Manager und der neuen IntelMQ API.

Es war auch das erste Release mit einem Docker Image verfügbar auf Dockerhub unter certat/intelmq-full. Details zu allen Neuerungen finden Sie im dazugehörigen Blogpost.

Im April wurde mit IntelMQ 2.3.2 das letzte Maintenance Release für das erste Drittel 2021 veröffentlicht, welches Bugfixes sowie Verbessungen für Shadowserver and Shodan enthielt.

Im gleichen Monat gab es einige Neuerungen bei tag2domain im Zusammenhang mit flexibleren Taxonomien. Ausführliche Beschreibungen finden sich in unserem Blog Post.

### 1.2.3 Vorträge

- Im Jänner 2021 hielt Dimitri Robl von CERT.at im Rahmen der Vorlesung ”Netzwerktechnologien” an der Universität Wien einen Gastvortrag. Dabei wurden die Aufgaben von CERT.at und CERTs/CSIRTs generell vorgestellt sowie einige Beispiele für netzwerkbezogene Schwachstellen und Angriffe mit den Studierenden besprochen.

- Am 23. April fand das erste Treffen der Cyber Sicherheit Plattform von 2021 statt. Die Cyber Sicherheit Plattform hat den Zweck, VertreterInnen von Verwaltung, Wirtschaft und Wissenschaft zu einem regelmäßigen Informationsaustausch und zur Vorstellung aktueller Themen zusammenzubringen. In der Regel finden dazu seit 2015 jedes Jahr zwei Veranstaltungen statt, seit Beginn der Pandemie natürlich virtuell. Neben rechtlichen und technischen Themen wurden durch Wolfgang Rosenkranz von CERT.at aktuelle Entwicklungen im Themenkomplex der Cybersecurity-Fachkräfteausbildung vorgestellt. Eine interessante Entwicklung sind beispielsweise die Arbeiten der ENISA zur Anpassung des “Workforce Framework for Cybersecurity” (NICE Framework) von NIST, dessen Bausteine eine bessere Definition und Vergleichbarkeit von Rollen, Aufgaben und Fähigkeiten von Personen, die im Cybersecurity-Bereich arbeiten, ermöglichen sollen.