Der Datendiebstahl der keiner war

und andere Geschichten aus dem Alltag des A1-CERT Teams

07 June 2024, Leopold Rehberger

OneSEC

Empowering a secure digital life.

IoT-Geräte: Ein Quiz

OneSEC

Was glaubt ihr, war das bisher ausgefallenste IoT-Gerät, das uns im A1-CERT beschäftigt hat?

A) Bohrmaschine
B) Schneekanone
C) Kühlschrank
D) Bügeleisen

Whoami?

OneSEC

Leopold Rehberger

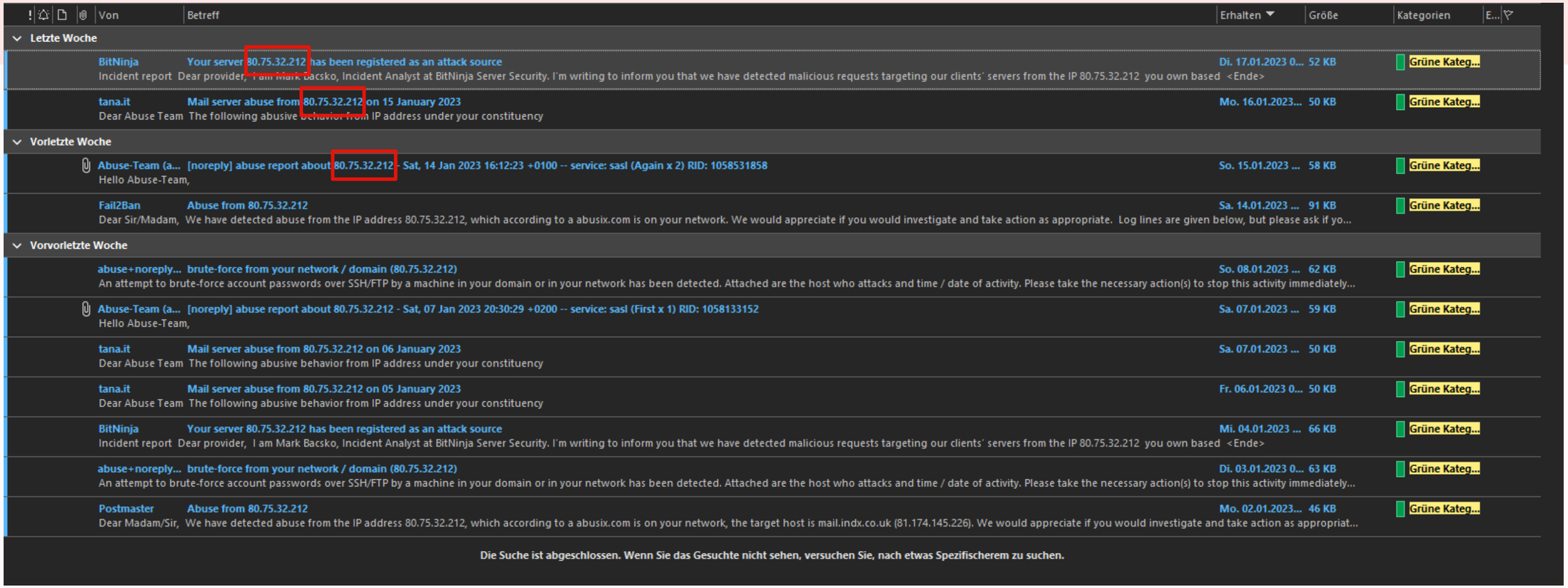
- Mitarbeiter im CERT Team von A1
- Leopold.rehberger@a1.at
- Seit ~2011 im A1-CERT
- Informationssicherheit
- Data Loss Prevention

Was Raspberries mit Mosquittos zu tun haben

OneSEC

Meldungen über eine „Rogue“ IP im IP Range von A1

OneSEC



Von	Betreff	Erhalten	Größe	Kategorien
Letzte Woche				
BitNinja	Your server 80.75.32.212 has been registered as an attack source	Di. 17.01.2023 0...	52 KB	Grüne Kateg...
Incident report	Dear provider, I am Mark Bacsko, Incident Analyst at BitNinja Server Security. I'm writing to inform you that we have detected malicious requests targeting our clients' servers from the IP 80.75.32.212 you own based <Ende>			
tana.it	Mail server abuse from 80.75.32.212 on 15 January 2023	Mo. 16.01.2023...	50 KB	Grüne Kateg...
Dear Abuse Team	The following abusive behavior from IP address under your constituency			
Vorletzte Woche				
Abuse-Team (a...	[noreply] abuse report about 80.75.32.212 - Sat, 14 Jan 2023 16:12:23 +0100 -- service: sasl (Again x 2) RID: 1058531858	So. 15.01.2023 ...	58 KB	Grüne Kateg...
Hello Abuse-Team,				
Fail2Ban	Abuse from 80.75.32.212	Sa. 14.01.2023 ...	91 KB	Grüne Kateg...
Dear Sir/Madam,	We have detected abuse from the IP address 80.75.32.212, which according to a abusix.com is on your network. We would appreciate if you would investigate and take action as appropriate. Log lines are given below, but please ask if yo...			
Vorvorletzte Woche				
abuse+noreply...	brute-force from your network / domain (80.75.32.212)	So. 08.01.2023 ...	62 KB	Grüne Kateg...
An attempt to brute-force account passwords over SSH/FTP by a machine in your domain or in your network has been detected. Attached are the host who attacks and time / date of activity. Please take the necessary action(s) to stop this activity immediately...				
Abuse-Team (a...	[noreply] abuse report about 80.75.32.212 - Sat, 07 Jan 2023 20:30:29 +0200 -- service: sasl (First x 1) RID: 1058133152	Sa. 07.01.2023 ...	59 KB	Grüne Kateg...
Hello Abuse-Team,				
tana.it	Mail server abuse from 80.75.32.212 on 06 January 2023	Sa. 07.01.2023 ...	50 KB	Grüne Kateg...
Dear Abuse Team	The following abusive behavior from IP address under your constituency			
tana.it	Mail server abuse from 80.75.32.212 on 05 January 2023	Fr. 06.01.2023 0...	50 KB	Grüne Kateg...
Dear Abuse Team	The following abusive behavior from IP address under your constituency			
BitNinja	Your server 80.75.32.212 has been registered as an attack source	Mi. 04.01.2023 ...	66 KB	Grüne Kateg...
Incident report	Dear provider, I am Mark Bacsko, Incident Analyst at BitNinja Server Security. I'm writing to inform you that we have detected malicious requests targeting our clients' servers from the IP 80.75.32.212 you own based <Ende>			
abuse+noreply...	brute-force from your network / domain (80.75.32.212)	Di. 03.01.2023 0...	63 KB	Grüne Kateg...
An attempt to brute-force account passwords over SSH/FTP by a machine in your domain or in your network has been detected. Attached are the host who attacks and time / date of activity. Please take the necessary action(s) to stop this activity immediately...				
Postmaster	Abuse from 80.75.32.212	Mo. 02.01.2023...	46 KB	Grüne Kateg...
Dear Madam/Sir,	We have detected abuse from the IP address 80.75.32.212, which according to a abusix.com is on your network, the target host is mail.indx.co.uk (81.174.145.226). We would appreciate if you would investigate and take action as appropriat...			

Die Suche ist abgeschlossen. Wenn Sie das Gesuchte nicht sehen, versuchen Sie, nach etwas Spezifischerem zu suchen.

Problem erkennen

Wer ist der Owner der IP?

OneSEC

Nachschauen in den Asset Management Systemen und im SIEM
➔ Leider kein eindeutiges Ergebnis. Nur ein Hinweis auf „M2M“.

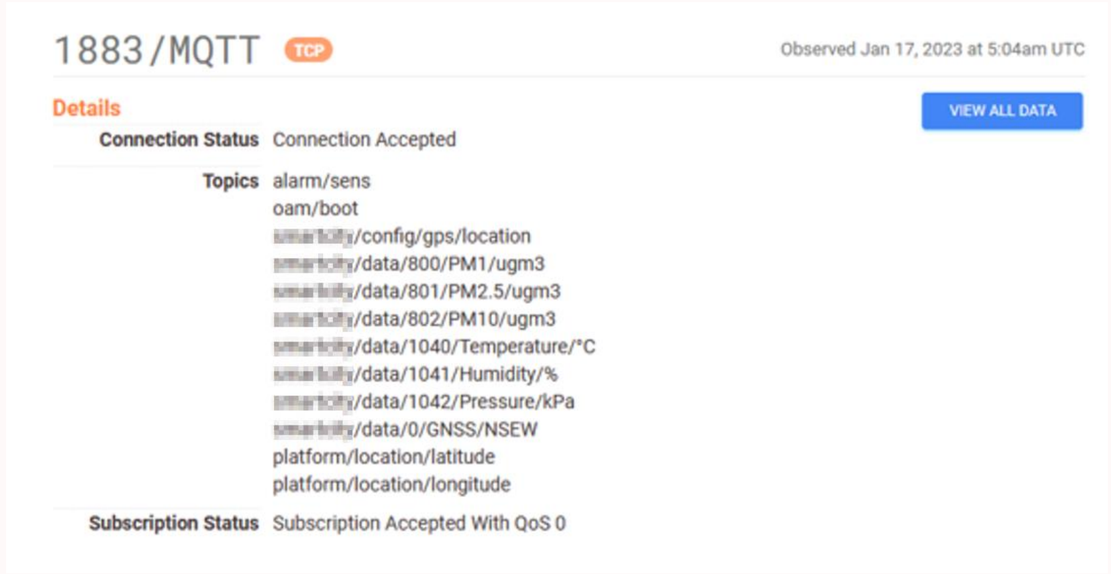
Problem erkennen | Owner finden A1 Systeme

SIEM: Security Information and Event Management
M2M: Machine to Machine
SIAM: Security Informations & Attribute Management

Was findet man im Internet über die IP/das Device?

OneSEC

- Shodan ➔ kein Ergebnis
- Censys



Problem erkennen → Info A1 Systeme → Info OSINT

*MQTT: Ist ein Standard für IoT Messaging (Message Queuing Telemetry Transport)

Was findet man im Internet über die IP/das Device?

OneSEC

MQTT Explorer

Application Edit View

MQTT Explorer Search...

▼ 80.75.32.212
- ▼ alarm
  - sens = Failed to send sensor data; a connection error occurred (Repeated 2 times since last report)
- ▼ oam
  - boot = active;2018-07-03-[redacted]
- ▼ [redacted]
  - ▼ config
    - ▼ gps
      - location = N:47.05563692 E:15.41658055
  - ▼ data
    - ▼ 0
      - ▼ GNSS
        - NSEW = N:47.05563692 E:15.41658055

▼ 800
- ▼ PM1
  - ugm3 = 0

▼ 801
- ▼ PM2.5
  - ugm3 = 0

▼ 802
- ▼ PM10
  - ugm3 = 0

▼ 1040
- ▼ Temperature
  - °C = 0

▼ 1041
- ▼ Humidity
  - % = 0

▼ 1042
- ▼ Pressure
  - kPa = 0

▼ platform
- ▼ datalake
  - dump_sensor_data = true

▶ platform (2 topics, 2 messages)

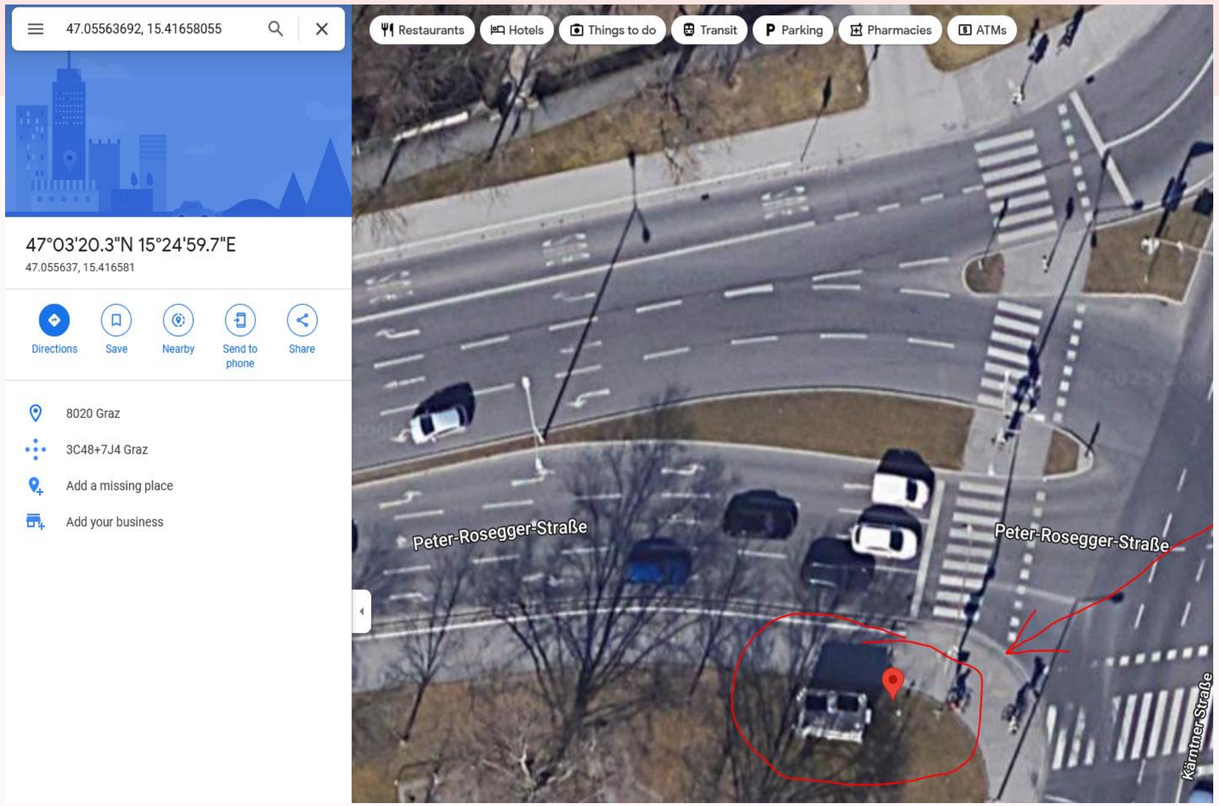
▼ $SYS
- ▼ broker

Problem erkennen → Info A1 Systeme → Info OSINT

*Mosquitto: ist ein open source MQTT Message broker

Was findet man im Internet über die IP/das Device?

OneSEC



Problem erkennen → Info A1 Systeme → Info OSINT

Was findet man im Internet über die IP/das Device?

OneSEC

Roadtrip

Problem erkennen → Info A1 Systeme → Info OSINT

Lösung des Problems

OneSEC

Shutdown

AW: [AK17593] General Question [redacted] - IoT Gerät mit M2M Sim-karte für

Support
An [redacted]
Cc [redacted]
Aufbewahrungsrichtlinie A1 - E-Mail-Policy: Inbox - remove after 3 years (3 Jahre)
Sie haben diese Nachricht am 18.01.2023 18:37 weitergeleitet.

Lieber Michael,
ich habe die Sim suspendiert.
LG Stefan

Gesendet: Mittwoch, 18. Jänner 2023 17:14

Betreff: [AK17593] General Question: [redacted] - IoT Gerät mit M2M Sim-karte für schädliche Zwecke genutzt
Priorität: Hoch

Liebes [redacted] Team,

Danke für die Information Christoph.
@Support bitte um Sperre (Suspendierung) der SIM- IMSI [redacted] mit IP: 80.75.32.212

Bitte um Rückmeldung

Problem erkennen → Info A1 Systeme → Info OSINT → Check → Mitigation

Der Datendiebstahl, der keiner war

OneSEC

Worum geht’s?

OneSEC

Web Elektronik Spiele

CYBER-ABWEHR AKTIV

Hacker richten mysteriöse Lösegeldforderung an A1

Web | 22.08.2023 20:00

A1 soll Opfer eines massiven Hacker-Angriffs geworden sein. (Bild: A1 Telekom Austria AG/APA-Fotoservice/Juhasz)

Erpresser-Krimi um die Telekom: Die A1 sieht sich mit dem Angriff einer neuen Cybercrime-Gruppe konfrontiert. Die Hacker behaupten, ins System eingedrungen zu sein, und setzen ein Ultimatum für die Lösegeldzahlung! Cybersecurity-Experte Cornelius Granig erklärt die Hintergründe.

Hacker behaupten

- Sie haben Daten von A1 gestohlen
  - 18 Tsd Mitarbeiter
  - 11 Mio Kunden
- Sie haben eine Lösegeldforderung an A1 gerichtet
- A1 hat (teilweise bezahlt)

Zum Zeitpunkt des Krone Artikels hatten wir bereits an dem Fall gearbeitet. Wir wurden von einem Mitarbeiter des Energy CERT darüber informiert, dass im Darkweb jemand behauptet, Daten von A1 gestohlen zu haben

Worum geht’s?

OneSEC

PENDING PAYMENT

(Updated Non-Stop)

A1 Data Provider

Comment from the author

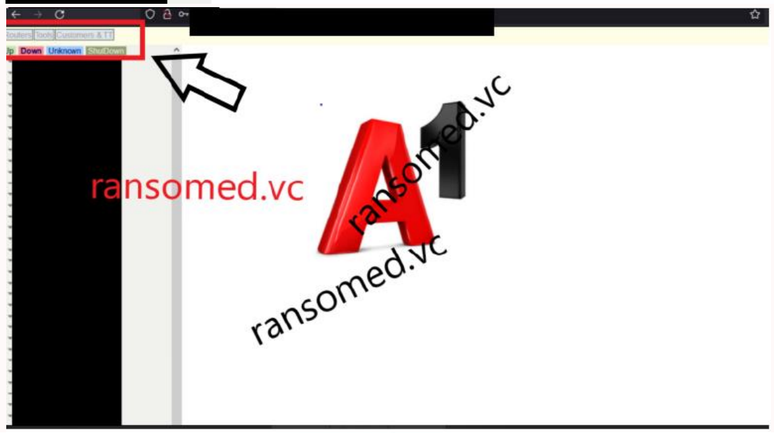
A1 has been recently compromised. Our group was able to gather access to multiple control panels. In the following countries:
. Austria (MAin Country of Operator)
. Serbia
. Bulgaria
. Croatia
. N. Macedonia

CHILD COMPANIES AFFECTED:
. BoB
. Yesss!
. Red Bull Mobile

EMPLOYEs AFFECTED:
Average: 18,000

CUSTOMERS AFFECTED:
Around 11M

The payment is due until 9/01/2023



Reaktion auf den Vorfall?

OneSEC

Informationen verifizieren, erstes Lagebild
- Sichten der Webseite, Screenshots machen

Suche nach dem betroffenem System
- Screenshots an alle Mitarbeiter schicken, die Portale betreiben
- Screenshots an Schwesterfirmen schicken
- Suche in Asset Management Systemen nach den Begriffen in den Screenshots

Monitoring von Telegram Kanälen / Tätergruppenanalyse
- Die Biographie eines Hackers zeigt Text in bulgarischer Sprache
- Eine weitere betroffene Firma ist in Bulgarien ansässig
- BTC Adressen rausgefunden

Suche nach dem Erpresserschreiben
- "Durchtelefonieren" aller Stellen, die Kommunikation von außen bearbeiten
- E-Mail Metadaten durchsuchen (nach Schlüsselwörtern)
- Office 365 Metadaten durchsuchen (nach Schlüsselwörtern)
- Volltext-Suchen in allen E-Mails und Office Dokumenten nach einer Ransomnote

Entwickeln von Angriffserkennungs Use Cases
- Alarmierung basierend auf Metadaten
- Alarmierung basierend auf IOCs

Außerbetriebnahme des betroffenen Systems
- Forensik
- System wurde abgedreht

Kommunikation
- CISO, Head of Security
- Mitarbeiter
- Medien
- Kunden und Lieferanten

Finales Lagebild

OneSEC

Der Angriff und die Erpressung haben nicht stattgefunden. Das ganze Szenario war ein Fake.

- Keine Lösegeldforderung an A1
- Keine Bezahlung durch A1
- Keine Bezahlung an irgendeine der rausgefundenen BTC Adressen (auch nicht auf den Adressen, die anderen „Opfern" zugeordnet waren)
- Die Gruppe Ransomed.vc hat keine A1 Systeme gehackt
- Sie hatten auch keinen Zugriff auf das betroffene System
- **Sie hatten sich den Screenshot mit hoher Wahrschenlichkeit im Darkweb besorgt, von einer anderen Tätergruppe**

Thank you

Leopold Rehberger

Leopold.Rehberger@a1.at

OneSEC