Abstract

Switzerland has been the target of a wide-range of DDoS and Ransom Denial of Service (RDoS) attacks over the past week, resulting in network outages and the website for Swiss Federal Railway (SBB) going offline. Additionally, two of the country's largest retailers, Coop and Migros, had their websites taken down, preventing customers from accessing their sites (see figure 1). Swiss financial service companies were also blackmailed and threatened via a DDoS attack unless a ransom was paid, according to local news websites. To date, one victim has paid the ransom.[i]

Figure 1: Digitec.ch on suspected DDoS attack

Background

A number of Swiss online retailers and the Swiss Federal Railway (SBB) experienced a series of network outages since Saturday, March 12, due to attacks. These attacks persisted throughout the week for several companies, including InterDiscount and Microspot. On March 17, both InterDiscount and Microspot came back online after prolonged outages.

InterDiscount, Microspot and SSB have acknowledged that they had experienced a denial of service attack.

"It is correct that our Webshop did not work for a short time. We currently believe that it was a DDoS attack. We can confirm that the customer data is safe and not affected. The shop is now again," said Nadine, Media Spokesperson at Interdiscount.

Figure 2: Tweet referencing SBB outage

On Friday, March 11, the Swiss Governmental Computer Emergency Response Team issued an alert suspecting the Armada Collective[ii] was responsible for the outages. This alert was issued after ten

financial institutions received a DDoS for ransom notes from the Armada Collective (see figure 3). Armada known in Switzerland following a similar ransom campaign they launched in November against ProtonMail[iii].

```
From: Armada Collective
Subject: DDOS ATTACK!!!
Date: Wed, 9 Mar 2016 XX:XX:XX +0000

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers

All your servers will be DDoS-ed starting Monday (March 14) if you
don't pay protection - 25 Bitcoins @
17j7onEtLgS2pd6qLekKQCteqTrnAFXZVS
If you don't pay by Monday, attack will start, price to stop will
increase to 50 BTC and will go up 20 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second.
So, no cheap protection will help.

Prevent it all with just 25 BTC @ 17j7onEtLgS2pd6qLekKQCteqTrnAFXZVS

Do not reply, we will not read. Pay and we will know its you. AND YOU
WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.
```

Figure 3: Ransom letter according to GovCERT.gov

These attacks display a similar pattern to those seen during the email service outage that plagued ProtonMail, HushMail and other encrypted email services in November 2015. During this campaign, attacks exceeded 100Gbps, targeting not only the datacenter, but also routers in Zurich, Frankfurt and other locations where ProtonMail had nodes. The first wave of attacks included huge volumetric attacks. During the second wave, more complex and sophisticated attacks targeting additional weak points in the infrastructure were executed. The coordinated assault on key infrastructures successfully brought down both the datacenter and the ISP, affecting not only ProtonMail, but hundreds of other companies.

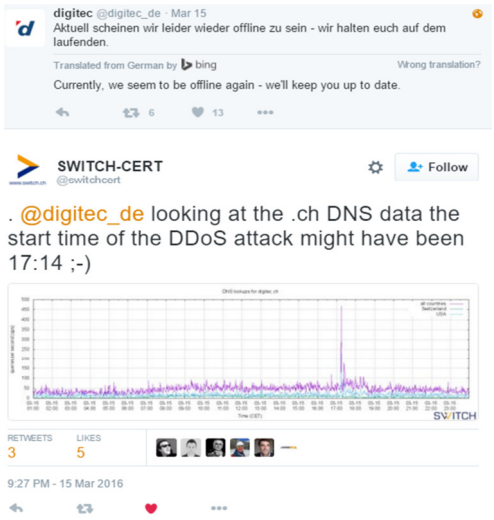

Figure 4: Switch CERT DNS statistics

Targets

- Digitec.ch
- Fust.ch
- Microspot.ch
- Interdiscount.ch
- Denner.ch
- Leshop.ch
- Coop.ch
- Galaxus.com
- SBB.ch
- Brack.ch

Possible attack vectors

- SSDP
- NTP
- DNS
- TCP RST
- TCP SYN
- SYN Flood
- SYN ACK
- ICMP

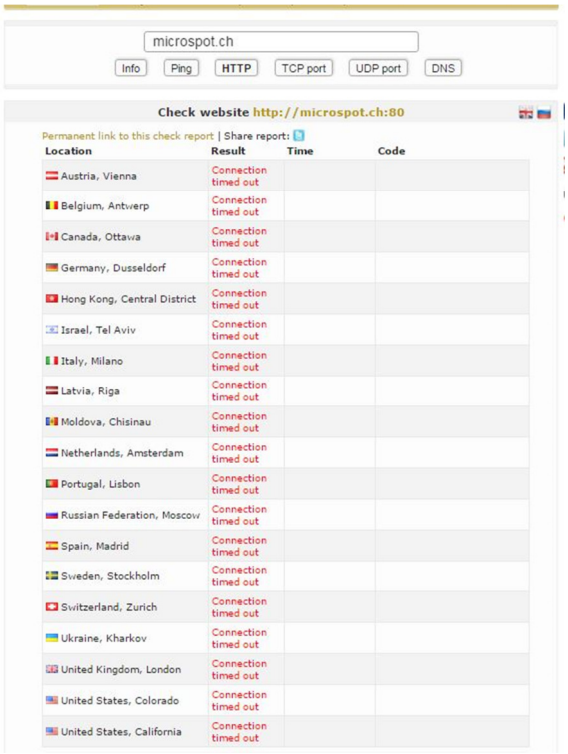

Figure 5: Microspot.ch offline (3-15 2pm EST)

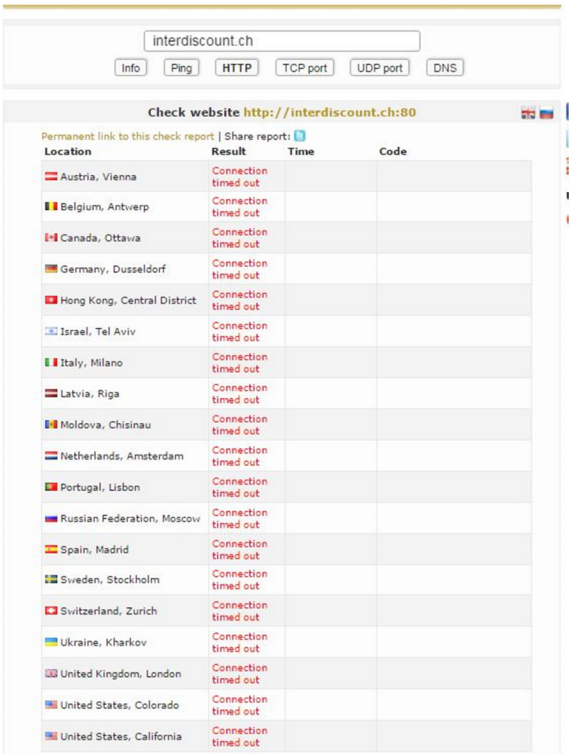

Figure 6: Interdiscount.ch offline (3-15 2pm EST)

How to Prepare

While it is impossible to predict the next target of a ransom attack, organizations need to proactively prepare networks and have an emergency plan in place for such an incident. If faced with a threat from a blackmail group, it is important to take the proper steps to mitigate the attack. We recommend reviewing network security policies, and patching the system accordingly. Maintaining and inspecting your network often is necessary to defend against these types of risks and threats.

Organizations under Threat Should Consider

- A hybrid solution that includes on premise detection and mitigation with cloud-based protection for volumetric attacks. This provides quick detection, immediate mitigation and protects networks from volumetric attacks that aim to saturate the Internet pipe.
- A solution that provides protection against sophisticated web-based attacks and web site intrusions to prevent defacement and information theft.
- A cyber-security emergency response plan that includes an emergency response team and process in place. Identify areas where help is needed from a third party.
- Monitor security alerts and examine triggers carefully. Tune existing policies and protections to prevent false positives and allow identification of real threats if and when they occur.

Radware's hybrid attack mitigation solution provides a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced threats. Dedicated hardware and cloud solutions protect against attacks in real time and help ensure service availability.

Under Attack and in Need of Expert Emergency Assistance?

Radware offers a full range of solutions to help networks properly mitigate attacks similar to these. Our attack mitigation solutions provide a set of patented and integrated technologies designed to detect, mitigate and report todays most advanced DDoS attacks and cyber threats. With dedicated hardware, fully managed services and cloud solutions that protect against attacks, Radware can help ensure service availability. To understand how Radware's attack mitigation solutions can better protect your network contact us today.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

Contact us:

Global:
575 Corporate Drive
Mahwah, NJ 07430
Tel: +1 (201) 512-9771
U.S. Toll Free: 1 (888) 234-5763
Fax: +1 (201) 512-9774
info@radware.com

Germany:
Robert-Bosch-Str.
11a – 2nd floor 63225 Langen
Tel: +49-6103-70657-0
Fax: +49-6103-70657-66
info_de@radware.com

Switzerland:
Hotelstrasse,
Zurich Airport
8058 Zurich
Tel: +41 44 51 52 117

---

[i] http://www.20min.ch/digital/news/story/20521137
[ii] http://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland
[iii] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/email-service-providers-under-attack/