Medium   🔍 Search   ✎ Write   👤

ShadowBrokers: The NSA compromised the SWIFT Network

Matt Suiche · Follow

entire SWIFT network. This would fit within standard procedure as a covert entity entrusted with covert actions that may or may not be legal in a technical sense. If the US had a specific target in the region's financial system, NSA penetration offers redundancy and other options than merely relying upon good faith compliance procedures, standard diplomatic requests, or collaborating with SWIFT Service Bureau.

First, here are few points to re-explain what SWIFT and SWIFT Service Bureau are.

ShadowBrokers' new release

Few hours ago, (14 April Release) ShadowBrokers just released a new archive divided in three different categories:

- **swift**

IMHO, the most interesting archive as it contains the evidences of the largest infection of a SWIFT Service Bureau to date.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- JEEPFLEA_MARKET

- JEEPFLEA_POWDER

This is the second significant SWIFT hack revealed in less than 2 years, the first one being the 2016 Bangladesh Bank heist allegedly executed by the North Korean government.

This archive contains several evidences, credentials, internal architecture information of the largest SWIFT Service Bureau of the Middle East:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Middle East

Provider	Country	Certification Status	Valid until	Compliant with	
Allied Engineering Group	Lebanon	Standard	21 September 2017	SIP Release 2013	⌄
ABS Emirates	United Arab Emirates	Standard	13 May 2019	SIP Release 2013	⌄
EastNets	United Arab Emirates	Standard	11 April 2019	SIP Release 2013	⌃

EastNets
...enabling confidentiality

Provider information:
Contact: Elsa L. Magsombol
Mail: emagsombol@eastnets.com
Phone: +971 4 3913217
Website: http://www.eastnets.com/

Standard Operational Level Information:
This Service Bureau has successfully acquired the Standard Certification level in compliance with the Terms and Conditions of the Shared Infrastructure Programme

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

since they have access to all those transactions as their are the hosting entity for the SWIFT Alliance Access (SAA) of their clients.

Each SAA represents a bank or financial institution, as we can see below:

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Many hardcoded passwords can be retrieved from the EastNets machine configuration files.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

infrastructure. All of that are very valuable information (such as infrastructure map, scripts, tools etc.) for an attacker.

It's very valuable for an attack to know the relationship between Front-End/Middleware/Backend interfaces. Remember, CISCO had to release an emergency patches for ASA Firewalls last year in emergency after the initial ShadowBrokers exploit releases if EPICBANANA and EXTRABACON.

Medium

Sign up to discover human stories that deepen your understanding of the world.

intercept the messsage sent for printing if an attacker which to manipulate the transaction messages and see his orders succeeding.

Targets

Below we can see an example of target, *Al Quds Bank for Development and Investment*, a Bank based in Ramallah, Palestine as a target — its host was running Windows 2008 R2 which is vulnerable to the exploits catalog of the exploit framework FUZZBUNCH.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Al Quds Bank for Development and Investment vulnerable to FUZZBUNCH's NSA exploit Framework

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

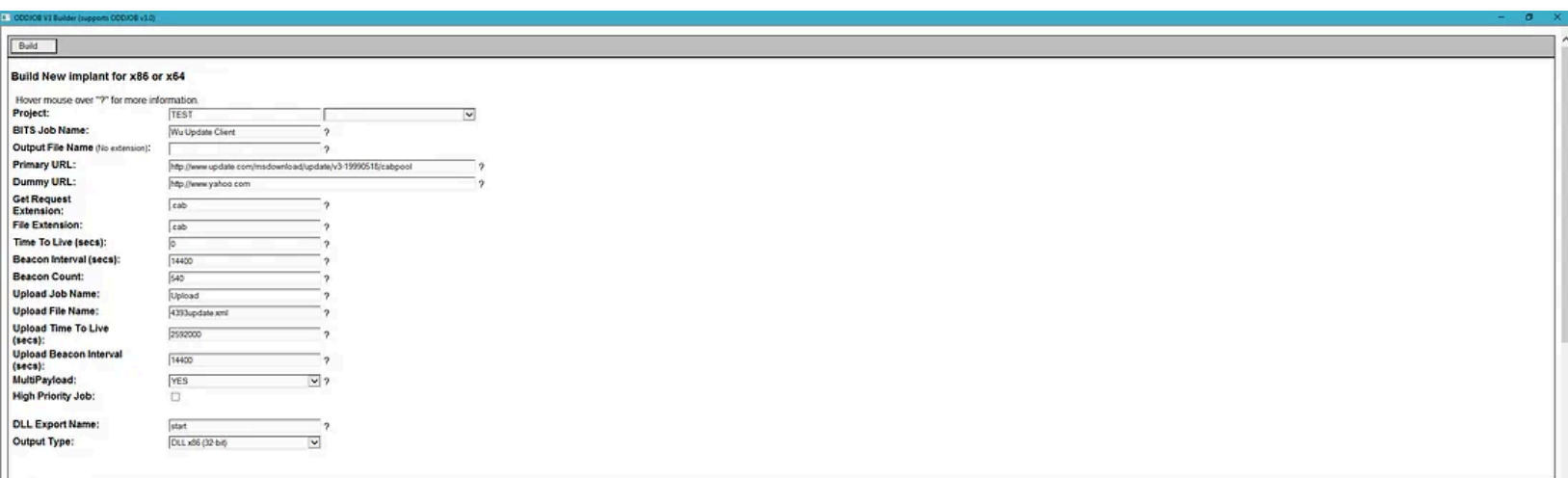- ETERNALBLUE is Remote Exploit via SMB & NBT (Windows XP to Windows 2012)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ **Membership**

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free	Membership
✓ Distraction-free reading. No ads.	✓ Read member-only stories
✓ Organize your knowledge with lists and highlights.	✓ Support writers you read most
✓ Tell your story. Find your audience.	✓ Earn money for your writing
	✓ Listen to audio narrations
	✓ Read offline with the Medium app

Alternative to SWIFTs?

China and Russia focused on SWIFT alternatives over the past few years such as China International Payments System (CIPS) ready since 2015 and last month Russia announced to have its alternative system for transfer of financial messages (SPFS) ready.

Although since as we just saw the exploitation of the SWIFT Service Bureau required Firewall and Windows remote exploits, having a SWIFT alternative

Reminder from Ned Pyle — SMB's Program Manager at Microsoft

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

The <del>ploy ~~ma~~ly it</del> failod <del>on ~~Win~~dows 10</del> <del>although ~~they~~ exploited</del>

Medium

Sign up to discover human stories that deepen your understanding of the world.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Written by Matt Suiche

3.3K Followers · Editor for Comae Technologies

Follow

Hacker, Microsoft MVP, Founder of @ComaeIo — Co-Founder of @CloudVolumes (now @VMWare)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app