Evolución de amenazas APT

Vicente Díaz
@trompi

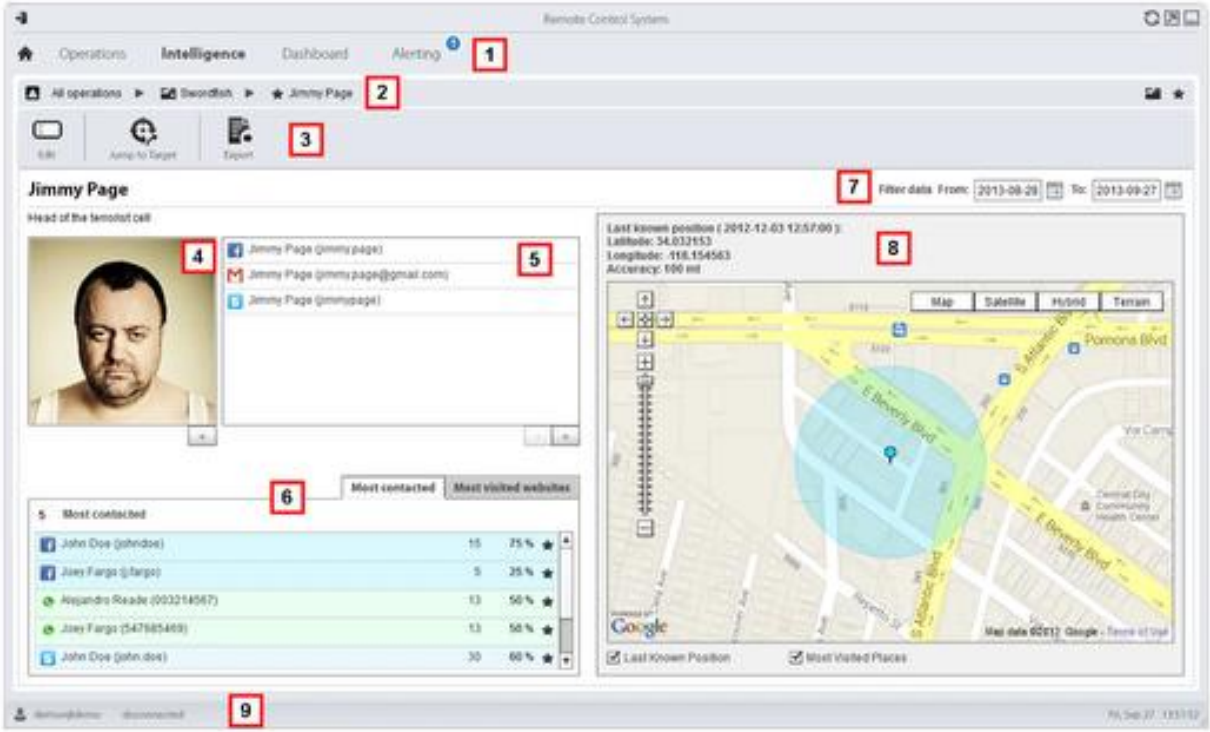
VirusTotal

According to Symantec's security expert, Brian Tillett, traces of more than 30 programmers were found in the Stuxnet source code.[29] The task of testing the worm in a faithful test bed site alone would have taken 10 developers at least six months.[30]
Other sources hypothesise that "*building the worm cost at least 3 million dollars and required a team of as many as 10 skilled programmers working about six months*". [31]
Microsoft has estimated that at least 30 cyber experts have together spent more than 10,000 man-days (equivalent to 27 man-years) in the project.
According to Siemens engineers, to create this malware would take months if not years of work if done by one person.
The New York Times reported that Stuxnet was developed jointly by Americans and Israelis over the past two years (see later → *Origins of Stuxnet*).
Finally, Langner's estimation for Stuxnet code is 15000 Lines of Code.

By interpolating the above estimations, and correlating them with those from Charlie Miller, Langner, and other OSINT sources, the following data can be empirically hypothesised:

Profile	**Number**
ICS consultant	2
SCADA/ PLC architect/ engineer	2
Simatic PLC programmer	3
Nuclear fuel production expert	2
Windows internal system programmer	5-10
Vulnerability analyst	2
Exploit writer	3
Quality assurance operator	3
Lab field tester	3
IT/ C&C infrastructure maintainer	5
On-site intelligence operator	1-10?
On-site installer	1-2?
TOTAL	**≈ 45**

Tab. 3: Estimation of knowledge profiles of personnel needed for the Stuxnet development, deployment and operational management


Remote Control System
Operations
Intelligence
Dashboard
Alerting
1
All operations
Swordfish
Jimmy Page
2
3
Jimmy Page
Head of the terrorist cell
7
Filter data From: 2013-08-28 To: 2013-09-27
4
Jimmy Page (jimmy.page)
Jimmy Page (jimmy.page@gmail.com)
Jimmy Page (jimmypage)
5
Last known position (2012-12-03 12:57:00):
Latitude: 34.032153
Longitude: -118.154563
Accuracy: 100 mt
8
Map
Satellite
Hybrid
Terrain
Pomona Blvd
E Beverly Blvd
S Atlantic Blvd
Google
Last Known Position
Most Visited Places
6
Most contacted
Most visited websites
5 Most contacted
John Doe (johndoe) 15 75 %
Joey Fargo (j.fargo) 5 25 %
Alejandro Reade (003214567) 13 50 %
Joey Fargo (547985469) 13 50 %
John Doe (john.doe) 30 60 %
9

VirusTotal

Once the exploit worked, it deployed the first stage payload: a compiled AutoIt script. This script then bypassed UAC using a known method called UACME, the code for which was taken from an online forum.

With higher privileges, the first stage payload ran PowerSploit to download code to run a reverse shell with Meterpreter – the RAT of the well known MetaSploit framework.

The next stage was exfiltration of document files that are also used to validate the value of the infection. If the infected system was deemed valuable enough, the threat actor then infected the target host with a second stage payload, which was once again a module built from code taken from various online forums and resources.

The attack vector is a spear phishing email with a PPS file attachment. It utilizes the exploit of CVE-2014-4114 (Sandworm). The exploit code closely resembles a public proof of concept exploit found on exploit-db1[3]. The exploit enables the attacker to drop files and execute an INF file, which is a Windows driver descriptor file.

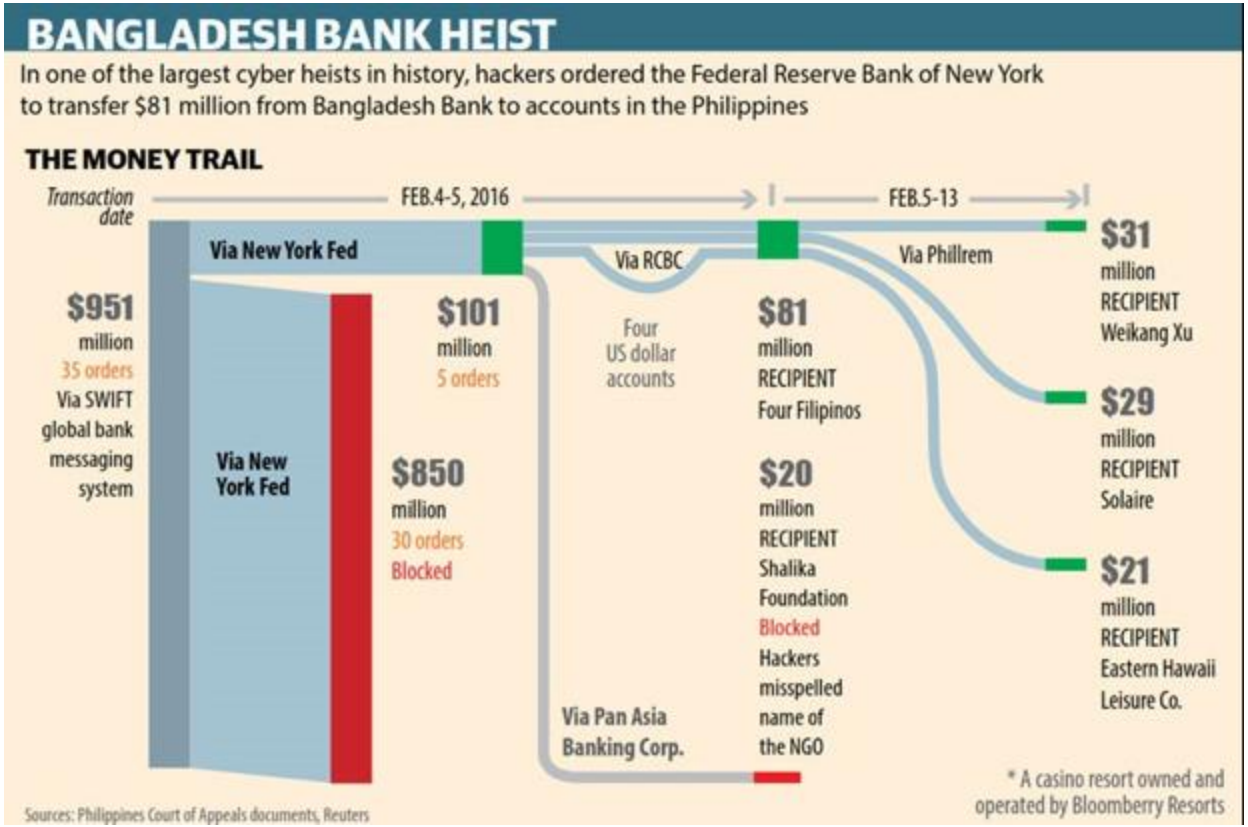
HERE'S THE PUBLIC EVIDENCE RUSSIA HACKED THE DNC — IT'S NOT ENOUGH

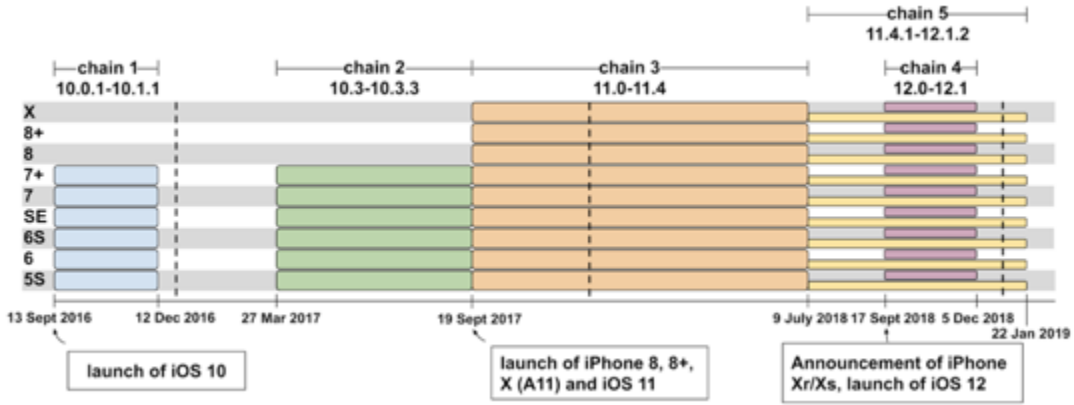
Sam Biddle

December 14 2016, 5:30 p.m.

The New York Times

Russian Hackers Who Targeted Clinton Appear to Attack France's Macron


BANGLADESH BANK HEIST
In one of the largest cyber heists in history, hackers ordered the Federal Reserve Bank of New York to transfer $81 million from Bangladesh Bank to accounts in the Philippines
THE MONEY TRAIL
Transaction date
FEB.4-5, 2016
FEB.5-13
$951 million 35 orders Via SWIFT global bank messaging system
Via New York Fed
Via New York Fed
$850 million 30 orders Blocked
$101 million 5 orders
Via RCBC
Four US dollar accounts
Via Pan Asia Banking Corp.
$81 million RECIPIENT Four Filipinos
$20 million RECIPIENT Shalika Foundation Blocked Hackers misspelled name of the NGO
Via Philrem
$31 million RECIPIENT Weikang Xu
$29 million RECIPIENT Solaire
$21 million RECIPIENT Eastern Hawaii Leisure Co.
* A casino resort owned and operated by Bloomberry Resorts
Sources: Philippines Court of Appeals documents, Reuters


chain 1
10.0.1-10.1.1
chain 2
10.3-10.3.3
chain 3
11.0-11.4
chain 4
12.0-12.1
chain 5
11.4.1-12.1.2
X
8+
8
7+
7
SE
6S
6
5S
13 Sept 2016
12 Dec 2016
27 Mar 2017
19 Sept 2017
9 July 2018
17 Sept 2018
5 Dec 2018
22 Jan 2019
launch of iOS 10
launch of iPhone 8, 8+, X (A11) and iOS 11
Announcement of iPhone Xr/Xs, launch of iOS 12

Gracias

www.virustotal.com/contact

@virustotal
@trompi