4th IAP North American & Caribbean Regional Conference 2016

IAP

International Association of Prosecutors

Tackling Financial Organised Crimes: Computer Fraud, Hacking and Identity Theft

SWIFT Fraud Impact

Society for Worldwide Interbank Financial Telecommunication

- Founded in 1973 Exploited in 2016
- Secure network for transmitting payment orders
- SWIFT does not facilitate funds transfer directly just the message to do so
- All that is required is for two financial institutions to have banking relationships
- 2016 Victims included Bank of Bangladesh (81M USD)
- Hackers are emptying Bank safes without the use of any guns

IAP
International Association of Prosecutors

Largest Organized Fraud of 2016 is SWIFT Fraud

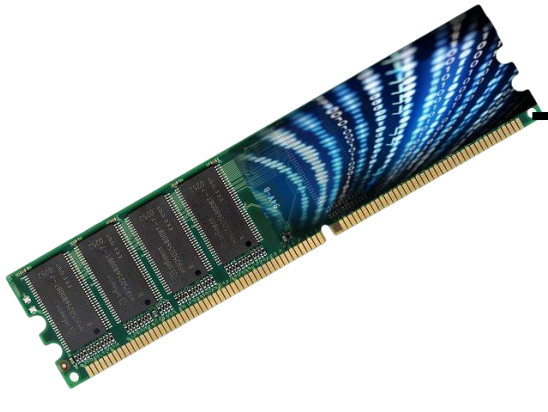
SL.NO	TT REF.NO	REMITTER REG. NO	REMITTER NAME	BENEF. A/C NO.	BENEF. NAME	BENEF. BANK	CCY	AMOUNT	DRAWEE BANK	STATUS
1	TT 0	[redacted]		112498001838	HARBOUR WORLD TRADING LIMITED	HSBC	USD	765920.50	SCB - New York	Debited
2	TT 0			817634587838	HONG KONG HAIXIN GROUP HOLDING CO	HSBC	USD	758400.30	SCB - New York	Debited
3	TT 0			817634587838	HONG KONG HAIXIN GROUP HOLDING CO	HSBC	USD	723452.02	SCB - New York	Debited
4	TT 0			817634587838	HONG KONG HAIXIN GROUP HOLDING CO	HSBC	USD	652020.90	SCB - New York	Debited
5	TT 0			OSA11443631287058	HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	628055.50	SCB - New York	Debited
6	TT 0			OSA11443631287058	HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	708055.50	SCB - New York	Debited
7	TT 0			OSA11443631287058	HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	761500.90	SCB - New York	Debited
8	TT 0			OSA11443631287058	HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	495275.25	SCB - New York	Debited
9	TT 0			OSA11443631287058	HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	595390.25	SCB - New York	Debited
10	TT 0			OSA11443633433205	KOTON MAGAZACILIK TEKSTIL SANAYI	SHANGHAI PUDONG DEVELOPMENT BANK	USD	591406.90	SCB - New York	Debited
11	TT 0			OSA11443633433205	KOTON MAGAZACILIK TEKSTIL SANAYI	SHANGHAI PUDONG DEVELOPMENT BANK	USD	757046.25	SCB - New York	Debited
12	TT 0			OSA11443633433205	KOTON MAGAZACILIK TEKSTIL SANAYI	SHANGHAI PUDONG DEVELOPMENT BANK	USD	641000.50	SCB - New York	Debited
13	TT 0			OSA11443633455090	BO RAN HONGKONG CO LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	626417.29	SCB - New York	Debited
14	TT 0			819721150838	LIANCHENG HK TRADE LIMITED	HSBC	USD	322500.90	SCB - New York	Debited
15	TT 0			819721150838	LIANCHENG HK TRADE LIMITED	HSBC	USD	327142.50	SCB - New York	Debited
16	TT 0			819721150838	LIANCHENG HK TRADE LIMITED	HSBC	USD	302080.40	SCB - New York	Debited
17	TT 0			OSA11443632017855	TARGET POWER INTERNATIONAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	706675.07	SCB - New York	Debited
18	TT 0			OSA11443632017855	TARGET POWER INTERNATIONAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	645729.10	SCB - New York	Debited
19	TT 0			OSA11443632017855	TARGET POWER INTERNATIONAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	640275.50	SCB - New York	Debited
20	TT 0			OSA11443633455090	BO RAN HONGKONG CO LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	725875.25	SCB - New York	Debited
21	TT 0			OSA11443633455090	BO RAN HONGKONG CO LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	798820.50	SCB - New York	Debited
22	TT 0			OSA11443633433205	KOTON MAGAZACILIK TEKSTIL SANAYI	SHANGHAI PUDONG DEVELOPMENT BANK	USD	790960.50	SCB - New York	Debited
23	TT 0			OSA11443631287058	HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	702000.50	SCB - New York	Debited
24	TT 1			819721150838	LIANCHENG HK TRADE LIMITED	HSBC	USD	307722.56	Deutsche Bank-New York	Debited
25	TT 1			819721150838	LIANCHENG HK TRADE LIMITED	HSBC	USD	352758.80	Deutsche Bank-New York	Debited
26	TT 1			819721150838	LIANCHENG HK TRADE LIMITED	HSBC	USD	315982.90	Deutsche Bank-New York	Debited
27	TT 1			817634587838	HONG KONG HAIXIN GROUP HOLDING CO	HSBC	USD	450250.50	HabibAmerican-NewYork	Debited
28	TT 1			OSA11443633433205	KOTON MAGAZACILIK TEKSTIL SANAYI	SHANGHAI PUDONG DEVELOPMENT BANK	USD	720250.50	HabibAmerican-NewYork	Debited
29	TT 1			OSA11443632017855	TARGET POWER INTERNATIONAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	653850.50	HabibAmerican-NewYork	Debited
30	TT 1			OSA11443632017855	TARGET POWER INTERNATIONAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	724985.50	HabibAmerican-NewYork	Debited
31	TT 0			OSA11443633465984	HONGKONG WIFORT INDUSTRIAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	690577.27	SCB - New York	Recredited
32	TT 0			OSA11443633465984	HONGKONG WIFORT INDUSTRIAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	703673.18	SCB - New York	Recredited
33	TT 0			OSA11443633465984	HONGKONG WIFORT INDUSTRIAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	721333.90	SCB - New York	Recredited
34	TT 0			OSA11443633465984	HONGKONG WIFORT INDUSTRIAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	706722.72	SCB - New York	Recredited
35	TT 0			112498001838	HARBOUR WORLD TRADING LIMITED	HSBC	USD	693290.25	SCB - New York	Cancelled
36	TT 1			OSA11443631287058	HONG KONG UBS GROUP LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	696100.25	Deutsche Bank-New York	Cancelled
37	TT 1			OSA11443633433205	KOTON MAGAZACILIK TEKSTIL SANAYI	SHANGHAI PUDONG DEVELOPMENT BANK	USD	605240.25	Deutsche Bank-New York	Cancelled
38	TT 1			OSA11443633455090	BO RAN HONGKONG CO LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	505750.65	Deutsche Bank-New York	Cancelled
39	TT 1			OSA11443632017855	TARGET POWER INTERNATIONAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	610557.97	Deutsche Bank-New York	Cancelled
40	TT 1			OSA11443633465984	HONGKONG WIFORT INDUSTRIAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	697930.60	Deutsche Bank-New York	Cancelled
41	TT 1			OSA11443633465984	HONGKONG WIFORT INDUSTRIAL LIMITED	SHANGHAI PUDONG DEVELOPMENT BANK	USD	672100.50	Deutsche Bank-New York	Cancelled
						TOTAL	USD	25495081.08		

Recent SWIFT fraud investigation revealed over 25 Million Hack

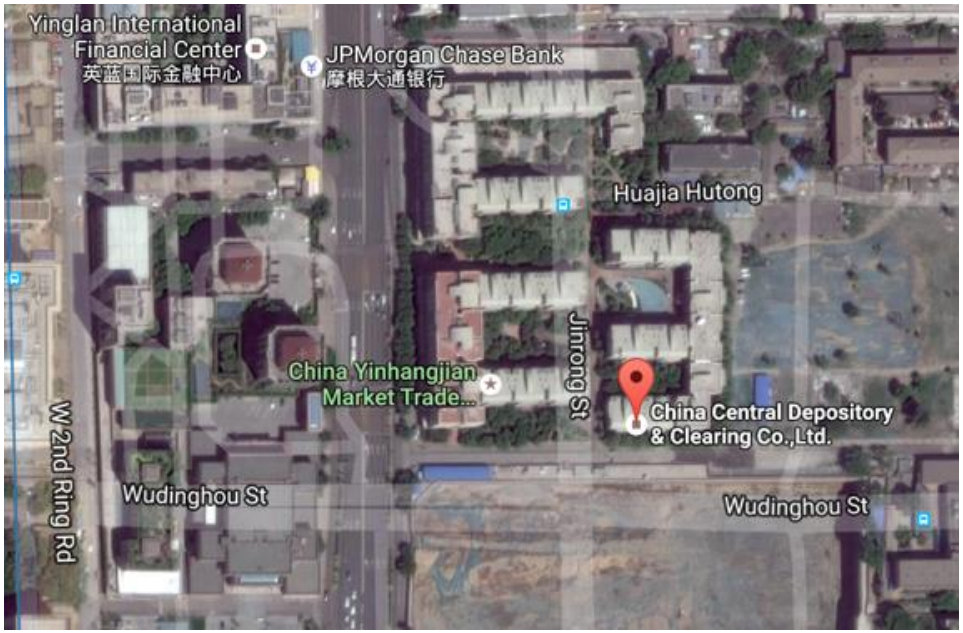
Source of Hacking

SWIFT System Malware Discovery

Financial data and passwords were actively being captured and syphoned. Below is the capture data destination and source file of stolen data:



Hacker commands and data send information:
.CREATETEXT
FTP.TXT
OPEN 202.108.90.13



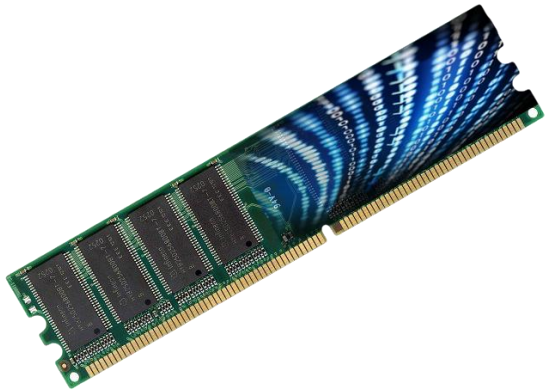
IP Address: 202.108.90.13
Country: China (CN)
City: Beijing
ISP: China Unicom Beijing
China Government Securities Depository

IAP
International Association of Prosecutors

How the Organized Hackers Compromised the Financial Network

Malware Assessment and Analysis Revealed

100% infected by:



SATYR
INSTALLED!
/SECLPD
VICTIM
\XCD\X80
ONELOVE
INJECT
PACKET
forkt~

IAP
International Association of Prosecutors

Forensically Boring Slide to Read Later

How the Memory Resident Malware

Linux.Satyr is classified as the Trojan horse infection which can perform malicious activities on your computer. Usually it spread over the internet and embed the malicious codes onto the free software downloads or suspicious websites. Once it gets itself installed on your computer, it is capable to disable the firewall to make your system vulnerable, which is why your computer is easily attacked by other malware.

This malicious Trojan when enters your system generates malicious codes and hamper your system performance. Generally compromises systems through malicious websites links, performing infected downloads, using removable media and opening emails links such as Spoofed Bank alerts.

HIDDEN – POLYMORPHIC – OBFUSCATED – DATA CAPTURE

IAP
International Association of Prosecutors

Taking Control of Administrators Systems

SWIFT Compromise by Hackers

It is well designed by cyber criminals to damage the target machine in order to gain illegal profits. It will connect to the remote attackers and help them take full control of your computer. Once the Trojan enters your computer, it will modify the system startup settings and drop its kernel code into the infected system so that it can be loaded up immediately whenever the computer starts up. It can also make some changes to the Windows Registry and default system configurations. It has the ability to keep track of your cookies and browsing data so as to capture your valuable information such as SWIFT transactions, modify SWIFT Transaction logs to avoid detection, and capture all financial records including the discovery of:

More than 5,000 passwords captured and found in a memory as a result of the Rootkit infection.

Pay *MORE* Attention to the Obvious Issues

Result of Linux.Satyr infections

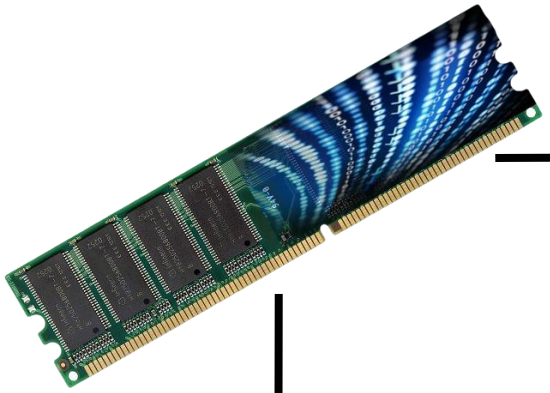
- Slower than normal system performance
- Appearance of DDOS attack
- Unexpected shut down of system
- Stop and Restart and Execution of various system applications and services (Security Motion Light False Positives)
  - Firewall
  - Policy Manager
  - AV
  - EXEs running in Prefetch
  - Processes
- Occurrence of Blue Screen error
- Modification or Attempted Changes to Windows Registry

IAP
International Association of Prosecutors

Skip the AV Logs and Alerts and Focus on Memory Analysis

Attacks are Occurring in/from Memory

One compromise lead to another and additional Running memory resident malware was located



al round!35 cowboy :)Aeý
LOGNAME=shitdown
USERNAME=shitdown
*Ä(€
make pid invisible
make pid visible

Suckit
hidden file-hiding
MM]ZZb
/etc/lpd
config
login:
(
[*] Dropping
Root Privileges
passwd
/passwd
ps_filter
ps_filter
su_pass
listen
ps_filter
su_pass
ps_filter
su_pass
ps_filter
su_pass
Password
listen
Server

IAP
International Association of Prosecutors

Assessment revealed all XP Systems were Compromised …Windows 7 to Follow

Update or segment if system critical i.e. SCADA System

Prosecutors with technical knowledge and training will be able to challenge digital forensic experts and their reports and findings and better assist victims of Fraud