RSA CONFERENCE ASIA PACIFIC 2013

Security in knowledge

2013: ATTACK TRENDS FOR THE YEAR AHEAD

Ali Islam
FireEye, Inc.

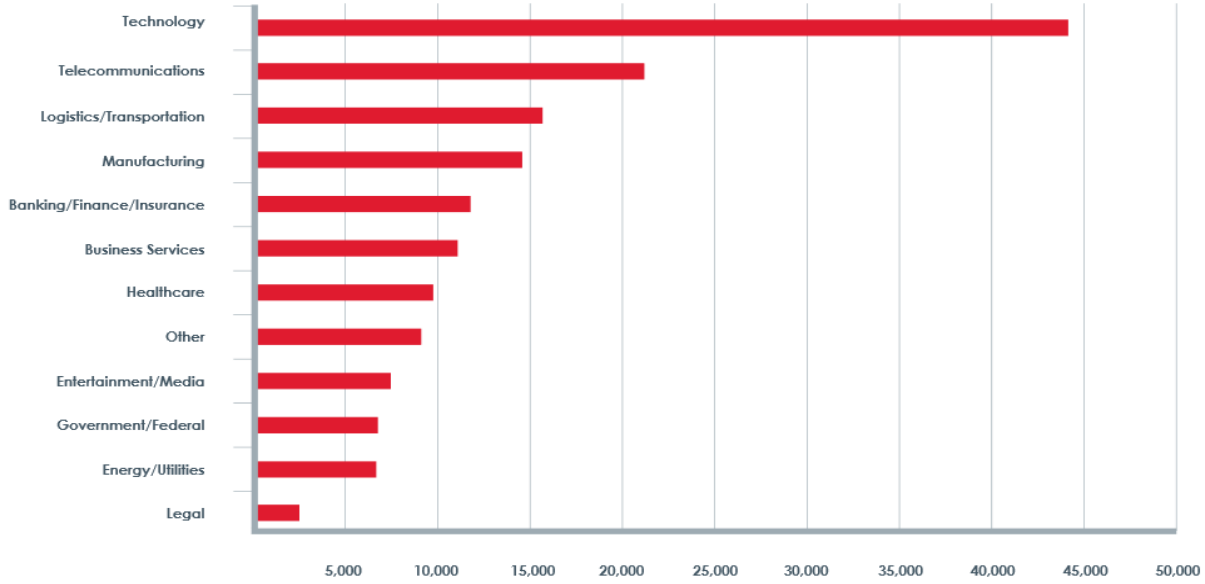
Session ID: SPO-W01A
Session Classification: Intermediate

APT CONTEXT: Start to End

- Initial Compromise
- Establish Communication Channel
- Internal Reconnaissance
- Lateral Movement
- Maintain Presence
- Ex-filtrate Data/Complete Mission

APT SUCCESS

- If you have something important they will get you
- APT actor properties: Extremely patient, Extremely Organized
- Compromises across all major industries in 2012
  - Technology is the top target industry
    - High concentration of Intellectual Property (IP)



2013: DANGEROUS TRENDS BY EXAMPLE

- Network Based Evasion Using Public Infrastructure
- Sandbox Based Evasion Using New and Effective Techniques
- Use of Public Key Certificates to Fly Under The Radar
- All Found in Advanced Malwares and APTs Discovered Recently by FireEye

SANNY APT AND PUBLIC BOARD

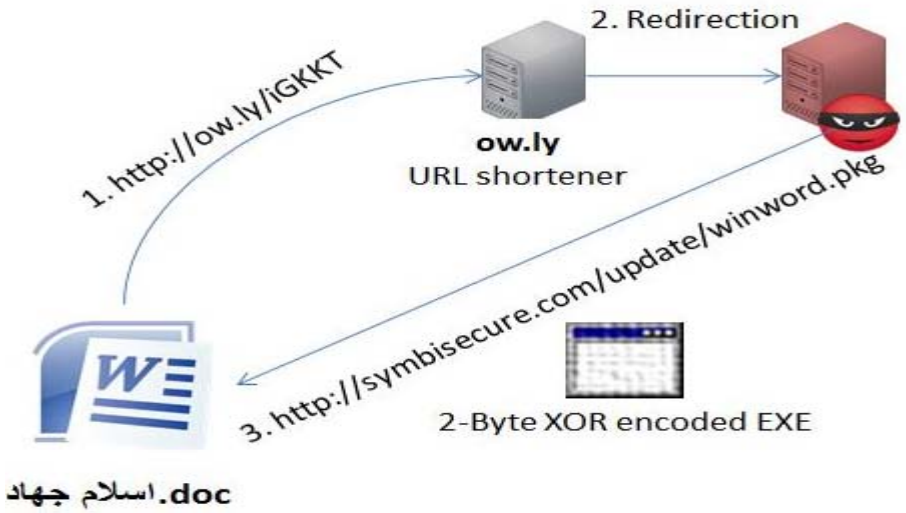
- Originating from Korea attacking Russian interests
- **Public message board** instead of dedicated CnC
- Attacker logged into the message board to get the Stolen data
- Will evade network based detection system

1605	MIKHAIL-PLANET_(0_0) [new]	zz◆zz◆	2012-12-05
1604	VLADIMIR_(1_0) [new]	Vladimir	2012-12-05
1603	VLADIMIR_(0_0) [new]	Vladimir	2012-12-05
1602	ROOT_(1_0) [new]	User	2012-12-05
1601	ROOT_(0_0) [new]	User	2012-12-05
1600	ITFRIEND_(1_0) [new]	Admin	2012-12-05
1599	ITFRIEND_(0_0) [new]	Admin	2012-12-05
1598	VLADIMIR_(1_0) [new]	Vladimir	2012-12-05
1597	VLADIMIR_(0_0) [new]	Vladimir	2012-12-05
1596	INFO-5BCC1AE731_(1_0)	IT	2012-12-04

POST	/write.php HTTP/1.1	Mozilla/5.0 (Windows; U; Windows NT 5.1; ko; rv:1.8.1.20) Gecko/20081217 Firefox/2.0.0.20
Others	*Accept*: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 *Accept-Language*: ko-kr,ko;q=0.8,en-us;q=0.5,en;q=0.3 *Accept-Encoding*: gzip,deflate *Accept-Charset*: EUC-KR,utf-8;q=0.7,*;q=0.7 *Keep-Alive*: 300 *Referer*: http://board.nboard.net/form.php?db=kbaksan_1 *Content-Type*: application/x-www-form-urlencoded *Content-Length*: 4863 *Parameters*: db=kbaksan_1&ch=19&name=&email=&pw=1917qaz&ulink=&title= _(0_0)&e5=0&e6=&e7=&html=2&text=fndp	

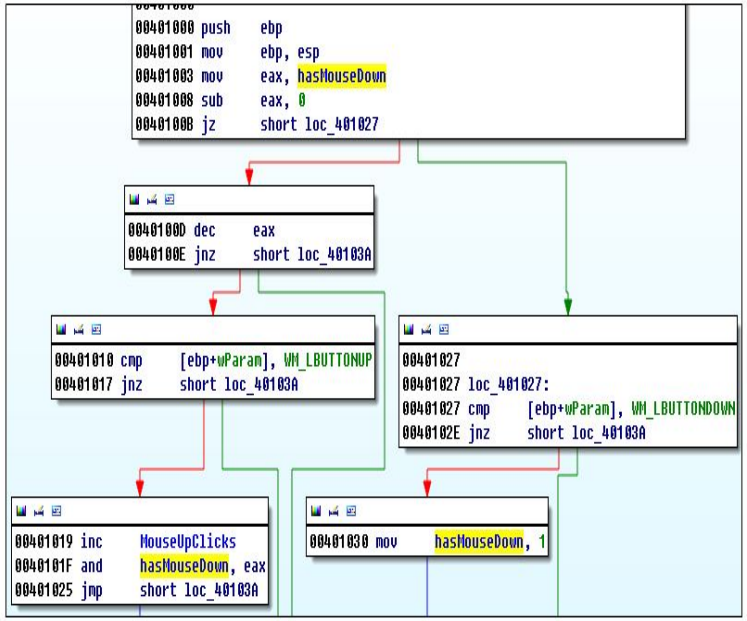
BANECHANT APT AND Evernote

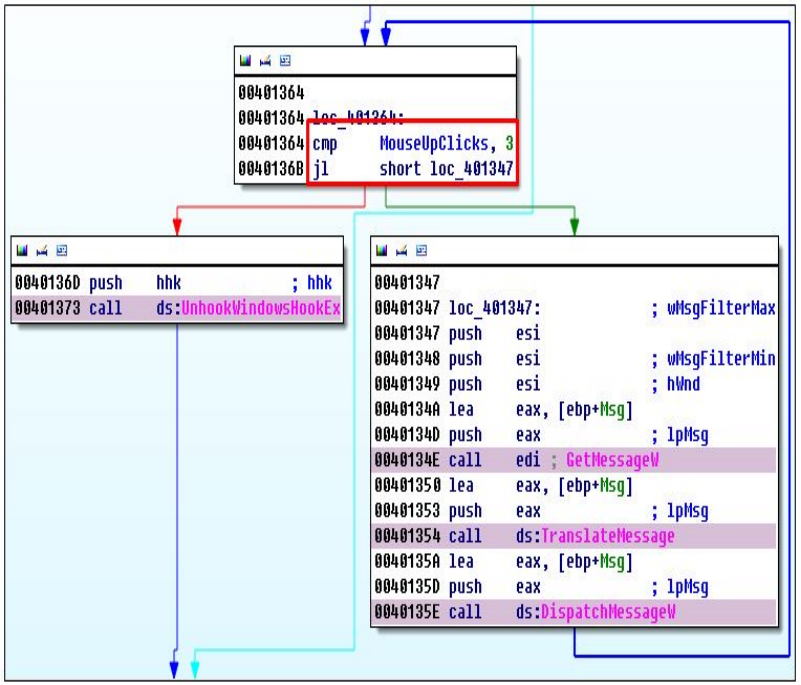
- Targeting governments of Middle East and Central Asia
- Used a **public URL shortening service**
- Recently discovered powerful backdoor was using a public note-taking tool called Evernote (very popular) as CnC
- Attacker saved commands in a public notepad service



BANECHANT APT AND MOUSE CLICK TECHNIQUE

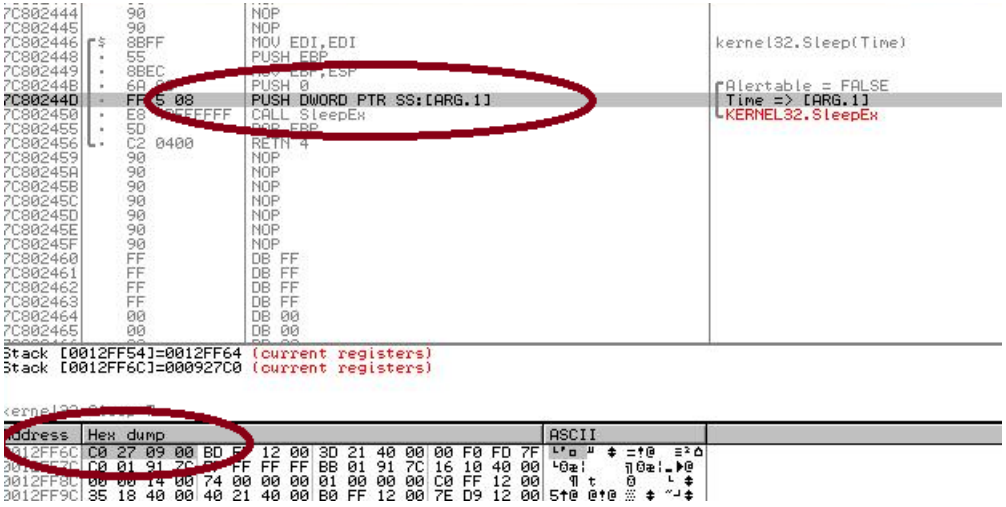
- Mouse click based evasion
- Upclicker detects one mouse click
- Banechant waits for atleast 3 left clicks





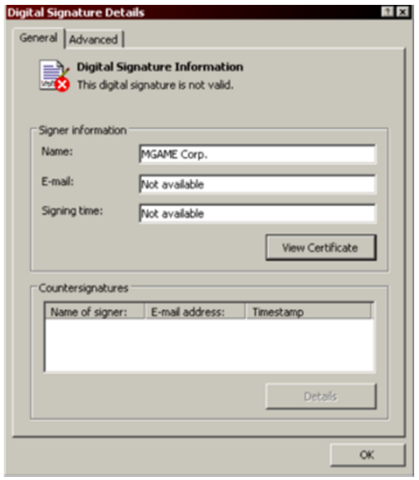
TROJAN NAP AND EXTENDED SLEEP

- Most sandboxes has default analysis time
- Recently identified Trojan NAP aka latest version of Kelihos use extend sleep calls (SleepEx) and undocumented API NtDelayExecution() to avoid sandbox based analysis
- Has a 10 min wait time before it starts.
- The botnet has survived multiple takedown attempts.



LADYBOYLE AND DIGITAL CERTIFICATES

- Exploited zero-day Adobe Flash (CVE-2013-0634)
- Rising trend in the amount of malware that is digitally signed
- Many security companies trust the presence of cert and dont go further
- Payload was signed with an invalid certificate from MGAME Corporation, a Korean gaming company
- Operation Hangover (India/Pak) successfully used an expired certificate



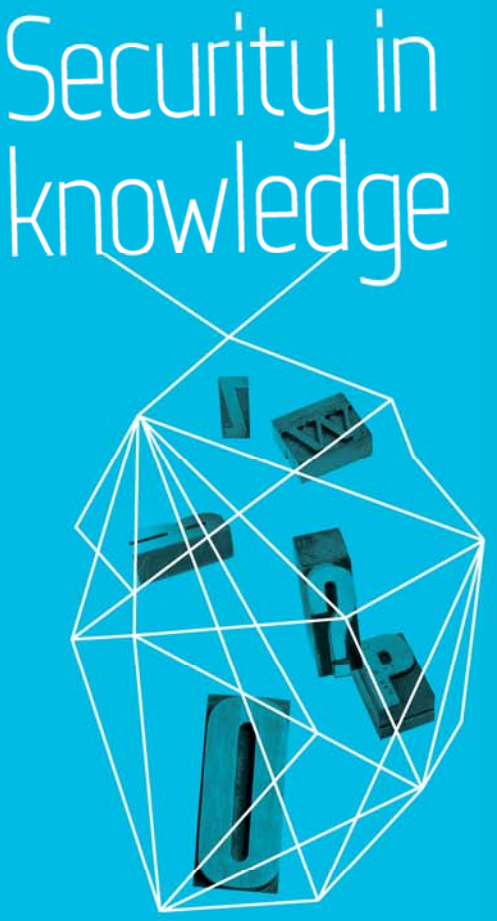
SUGGESTIONS AND PRECAUTIONS

- Properly verify the digital certificate, don't just check the presence of a certificate.
- Bad guys continuously innovate and come up with amazing new ways to evade
- We should anticipate and act instead of waiting .
- How about particular mouse co-ordinates?

Continued..

- Think like a hacker
- Don’t trust every communication going to legitimate websites. Esp. websites like dropbox, rapidshare etc.
- Check/Hook all APIs or the base API.

RSA CONFERENCE ASIA PACIFIC 2013



Thank You

Ali Islam
FireEye, Inc.

Session ID: SPO-W01A
Session Classification: Intermediate