



Cyber Security

Helping secure one network at a time



Infragard
Will Hatcher
patriskms@gmail.com
504-247-4878





THE GLOBAL INTERNET POPULATION

2.3 Billion World Wide

33% of Pop. (End of 2011)

<u>Region</u>	<u>Percentage of Internet Penetration Of Population</u>	<u>Percentage of WWW Usage</u>
Asia	26 Percent	45 Percent
Europe	61 Percent	22 Percent
North America	79 Percent	12 Percent
Latin America/Caribbean	40 Percent	11 Percent
Africa	14 Percent	6 Percent
Middle East	36 Percent	3 Percent
Oceania/Australia	68 Percent	1 Percent



Garden Variety Hacker



@UGBrazil

open computer ofc fbi computer name 23
acees with ssh open scan ok open
#Leaked #FBI #Computer #23
(205.128.71.87) [1000 ports] Discovered
open port 80/tcp on 205.128.71.87
Discovered open port 443/tcp on
205.128.71.87

Tweets



Knew Eyes @Kneweyes

5m

Target down! tel-aviv.gov.il #opisrael #anonymous #gaza
#standonisrael goooooooooo Anonymous!

Retweeted by CWN

Expand





Professional Hackers Organized Crime – Mercenary Largest Group in Numbers



UNCLASSIFIED



Advance Persistent Threat State Sponsored

لا إله إلا الله
الله أكبر
لا حول ولا قوة إلا بالله

An anti-recruitment Muslim "agency" advised the detainees, Iraqi & Lebanese
(against the U.S. & Iraq)
IT'S "BETTER" ABOUT LIBERATION - BE APT BEARS NECESSARY
That's the only way oppressed people will free themselves from U.S. or Zionist invaders

★ IRANIAN CYBER ARMY ★





Symantec



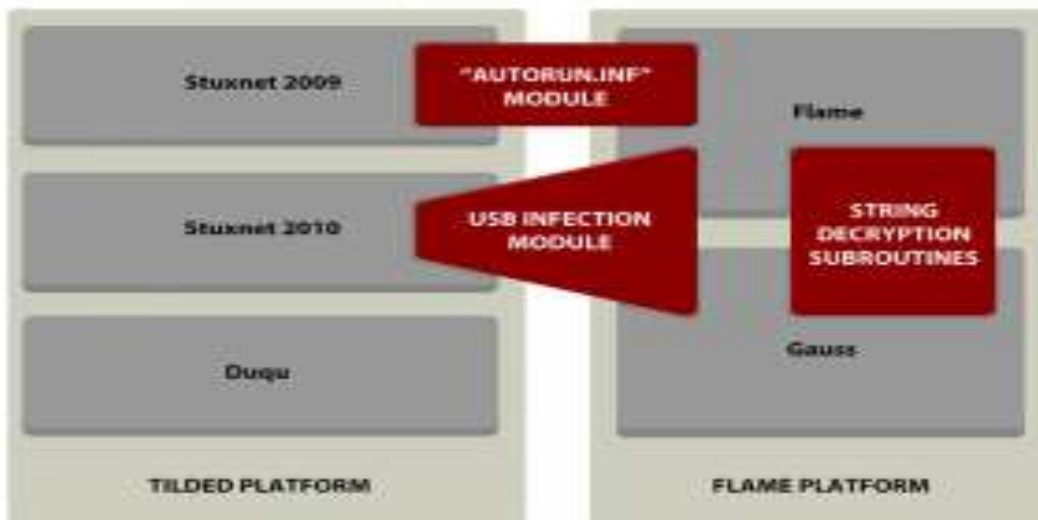


STUXNET

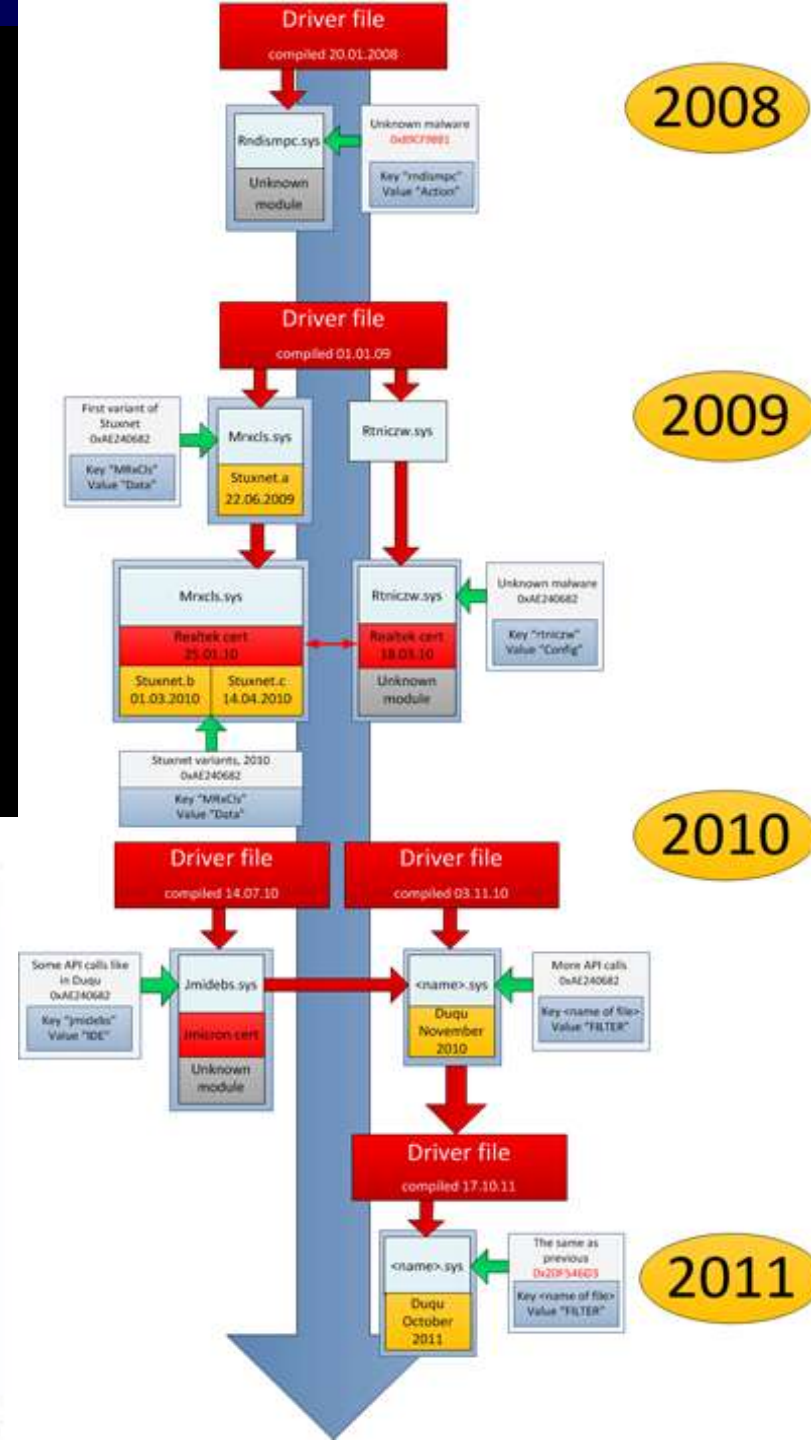
YOU... are my father

ICBNHRSCHBEEZBURGER.COM

The relationship of Stuxnet, Duqu, Flame and Gauss



© 2012 Kaspersky Lab ZAO. All Rights Reserved.



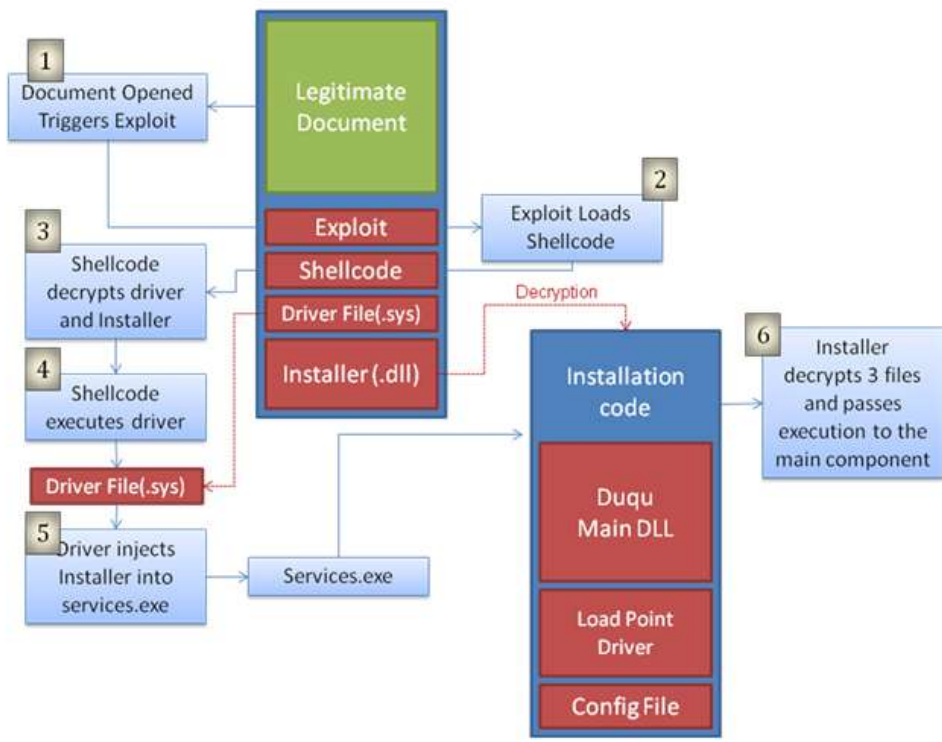
DUQU

Gusano Duqu

www.ne



DUQU



"The attackers intend to use this capability to gather intelligence from a private entity to aid future attacks on a third party. While suspected, no similar precursor files have been recovered that predate the Stuxnet attacks."

Key points:

- Executables using the Stuxnet source code have been discovered. They appear to have been developed since the last Stuxnet file was recovered.
- The executables are designed to capture information such as keystrokes and system information.
- Current analysis shows no code related to industrial control systems, exploits, or self-replication.
- The executables have been found in a limited number of organizations, including those involved in the manufacturing of industrial control systems.
- The exfiltrated data may be used to enable a future Stuxnet-like attack.

'FLAME' WARS HOW ESPIONAGE WENT VIRAL

The Flame virus has been dubbed the world's most sophisticated piece of malware. How does it work?

1 Infection begins with a computer in a high-security network. How it gets there is unknown; the virus could be delivered by USB stick, via an email or through an internet hack attack.



CONTROL AND COMMAND

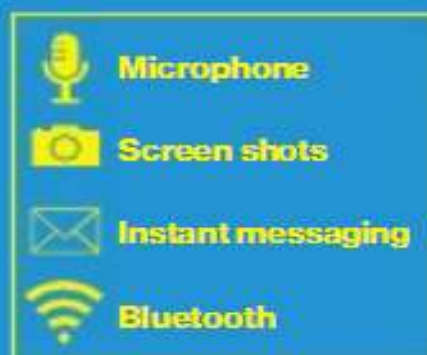


2 Virus scans for other networks and accounts to infect. Rather than being virulent, it carefully chooses its targets and communicates with 'control and command' for advice.



Hidden servers are used by cyber attackers to talk with virus and access the data.

3 Flame is masterful in sweeping for data, listening in to microphones, monitoring instant messenger chats, taking screen shots and hacking connected Bluetooth devices.



DROPBOX



4 Gathered information is broken down into small pieces and smuggled out in normal network traffic. It is reassembled and placed in a 'drop box' on the internet.

GRAPHIC: JOHN BRADLEY

COUNTRIES INVOLVED

IRAN

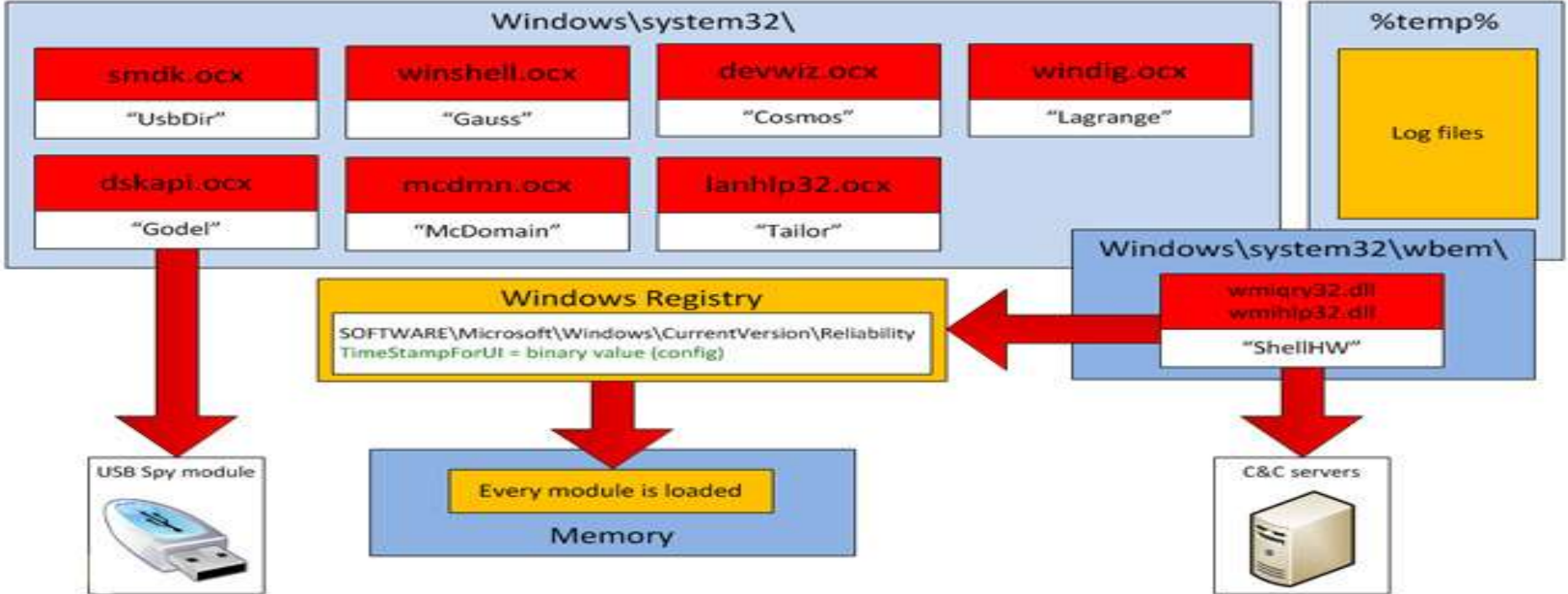
The country with the largest number of infections, though they have also been found in Sudan, Syria, Lebanon and Egypt. President Mahmoud Ahmadinejad (right) has warned of the dangerous new threat.



ISRAEL

The government of Benjamin Netanyahu (right) hinted they might be behind the virus, even though computers also infected in Israel.



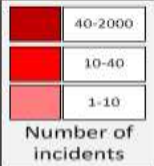
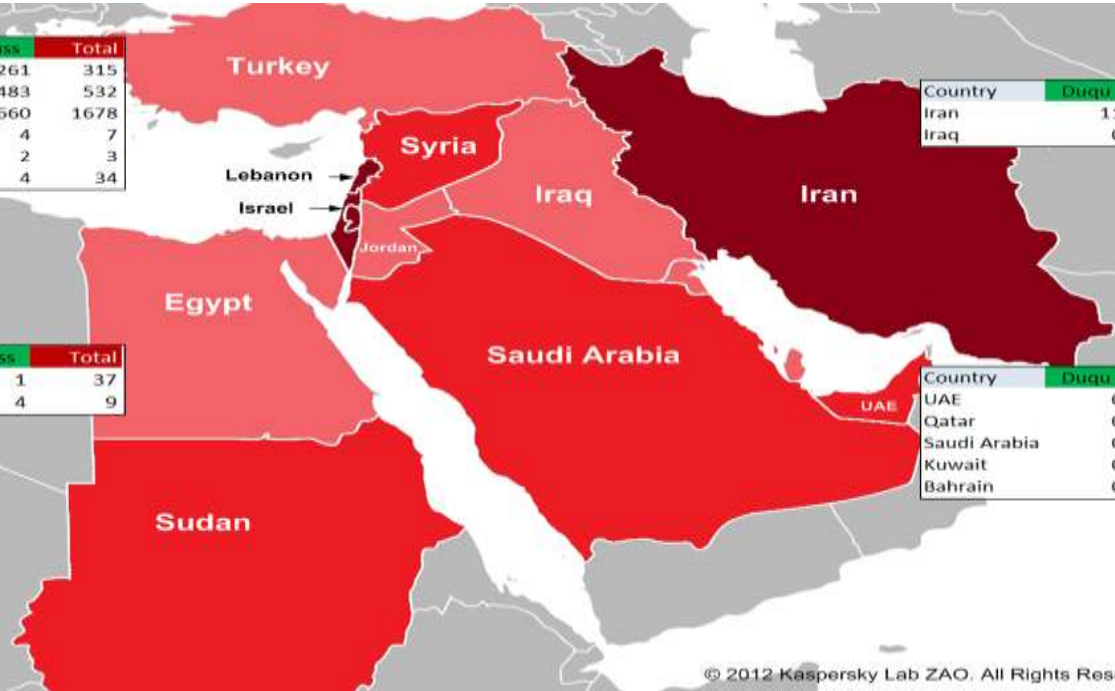


Country	Duqu	Flame	Gauss	Total
Palestinian Territories	0	54	261	315
Israel	0	49	483	532
Lebanon	0	18	1660	1678
Jordan	0	3	4	7
Turkey	0	1	2	3
Syria	0	30	4	34

Country	Duqu	Flame	Gauss	Total
Iran	11	199	1	211
Iraq	0	3	2	5

Country	Duqu	Flame	Gauss	Total
Sudan	4	32	1	37
Egypt	0	5	4	9

Country	Duqu	Flame	Gauss	Total
UAE	0	2	11	13
Qatar	0	1	4	5
Saudi Arabia	0	12	4	16
Kuwait	0	0	1	1
Bahrain	0	1	1	2





SHAMOON

C:\Shamoon\ArabianGulf\wiper\release\wiper.pdb

Saudi Aramco geoscientists and petroleum engineers





NEXT TARGET?



MONSANTO

"Control the food supply, and you control the people."



BYOD

Bring Your Own Disaster





MINI - FLAME

Cyber security experts say uncovered a new powerful espionage virus in the Middle East that's reserved for high-value targets....

Lebanese banks that U.S. officials say are suspected of laundering money for Iran and Hezbollah, its powerful Lebanese proxy, have also been hit in recent weeks.

Read more: http://www.upi.com/Business_News/Security-Industry/2012/10/16/Mini-Flame-virus-hikes-Mideast-cyberwar/UPI-72041350405555/#ixzz29aIDeFpc

UNCLASSIFIED//FOUO





Footnotes

1. <http://blog.thomsonreuters.com/index.php/deconstructing-the-flame-virus/>
2. <http://www.techypod.com/2012/07/flame-virus-usisrael-trying-hard-to.html>
3. <http://rt.com/news/gauss-virus-stuxnet-flame-276/>
4. <http://www.livehacking.com/tag/stuxnet/>
5. <http://www.hardwarezone.com.sg/tech-news-duqu-trojan-james-bond-cyberattacks>
6. <http://www.aftershell.com/2011/11/03/w32-duqu-analysis/>
7. http://www.securelist.com/en/blog/208193795/Shamoon_the_Wiper_in_details
8. http://www.securelist.com/en/blog/208193808/What_was_that_Wiper_thing#page_top
9. [https://www.securelist.com/en/blog/208193786/Shamoon the Wiper Copycats at Work](https://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work)
10. http://www.upi.com/Business_News/Security-Industry/2012/10/16/Mini-Flame-virus-hikes-Mideast-cyberwar/UPI-72041350405555/#ixzz29aDeFpc
11. usa.kaspersky.com

UNCLASSIFIED//FOUO

