Revealed: Operation Shady RAT

Dmitri Alperovitch, VP Threat Research

An investigation of targeted intrusions into 70+ global companies, governments and non-profit organizations during the last 5 years

For the last few years, especially since the public revelation of Operation Aurora, the targeted successful intrusion into Google and two dozen other companies, I have often been asked by our worldwide customers if they should worry about such sophisticated penetrations themselves or if that is a concern only for government agencies, defense contractors, and perhaps Google. My answer in almost all cases has been unequivocal: absolutely.

Having investigated intrusions such as Operation Aurora and Night Dragon (systemic long-term compromise of Western oil and gas industry), as well as numerous others that have not been disclosed publicly, I am convinced that every company in every conceivable industry with significant size and valuable intellectual property and trade secrets has been compromised (or will be shortly), with the great majority of the victims rarely discovering the intrusion or its impact. In fact, I divide the entire set of Fortune Global 2000 firms into two categories: those that *know they've been compromised* and those that *don't yet know*.

Lately, with the rash of revelations about attacks on organizations such as RSA, Lockheed Martin, Sony, PBS, and others, I have been asked by surprised reporters and customers whether the rate of intrusions is increasing and if it is a new phenomenon. I find the question ironic because these types of exploitations have occurred relentlessly for at least a half decade, and the majority of the recent disclosures in the last six months have, in fact, been a result of relatively unsophisticated and opportunistic exploitations for the sake of notoriety by loosely organized political hacktivist groups such as Anonymous and Lulzsec. On the other hand, the targeted compromises — known as 'Advanced Persistent Threats (APTs)' (although this term lately lost much of its original meaning due to overzealous marketing tactics of various security companies, as well as to the desire by many victims to call anything they discover being successful at compromising their organizations as having been an APT) — we are focused on are much more insidious and occur largely without public disclosures. They present a far greater threat to companies and governments, as the adversary is tenaciously persistent in achieving their objectives. The key to these intrusions is that the adversary is motivated by a massive hunger for secrets and intellectual property; this is different from the immediate financial gratification that drives much of cybercrime, another serious but more manageable threat.

What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth — closely guarded national secrets (including from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, SCADA configurations, design schematics and much more has "fallen off the truck" of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries.

McAfee®

What is happening to all this data — by now reaching petabytes as a whole — is still largely an open question. However, if even a fraction of it is used to build better competing products or beat a competitor at a key negotiation (due to having stolen the other team's playbook), the loss represents a massive economic threat not just to individual companies and industries but to entire countries that face the prospect of decreased economic growth in a suddenly more competitive landscape and the loss of jobs in industries that lose out to unscrupulous competitors in another part of the world, not to mention the national security impact of the loss of sensitive intelligence or defense information.
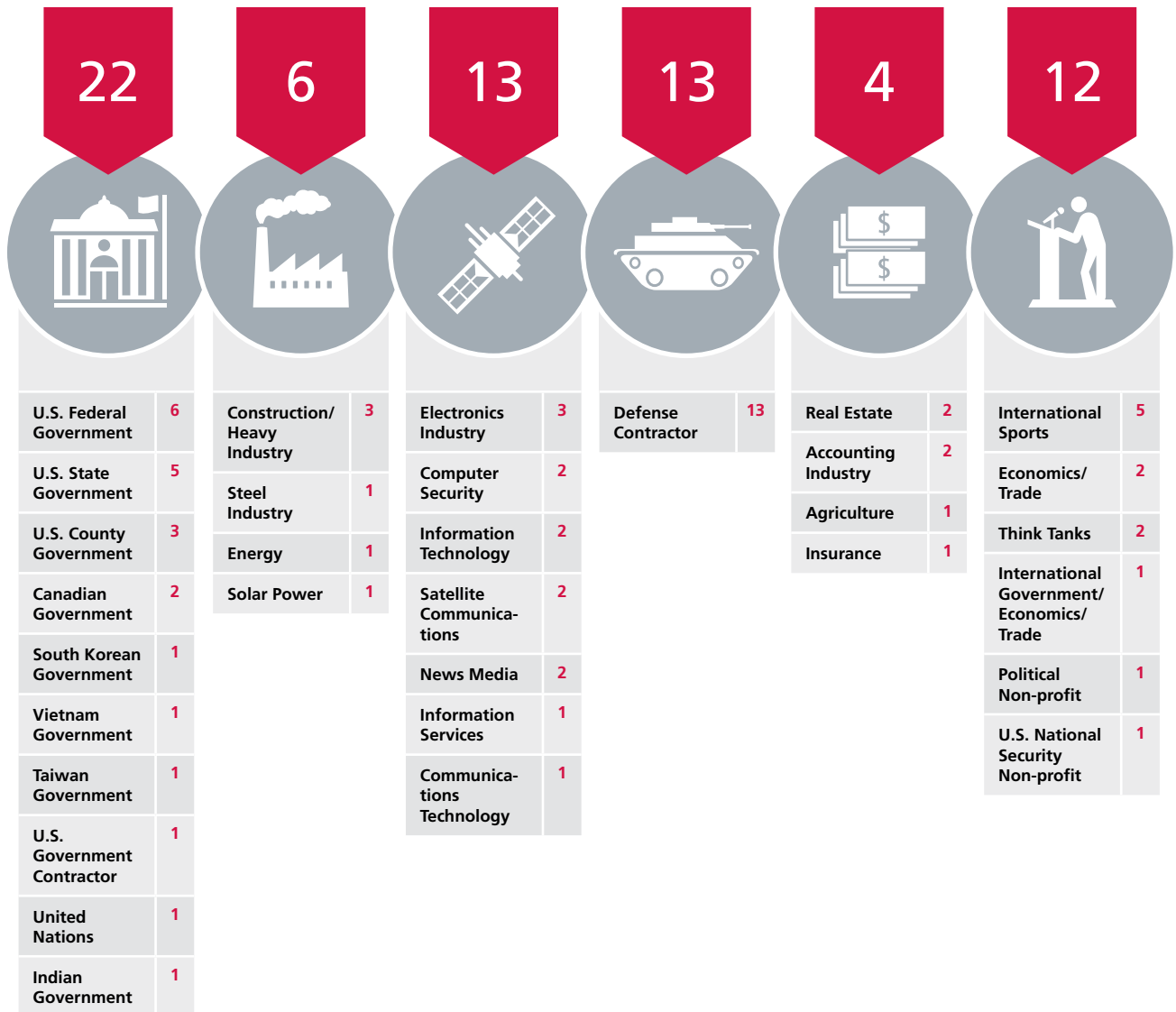
Yet, the public (and often the industry) understanding of this significant national security threat is largely minimal due to the very limited number of voluntary disclosures by victims of intrusion activity compared to the actual number of compromises that take place. With the goal of raising the level of public awareness today we are publishing the most comprehensive analysis ever revealed of victim profiles from a five year targeted operation by one specific actor — *Operation Shady RAT*, as I have named it at McAfee (RAT is a common acronym in the industry which stands for Remote Access Tool).

This is not a new attack, and the vast majority of the victims have long since remediated these specific infections (although whether most realized the seriousness of the intrusion or simply cleaned up the infected machine without further analysis into the data loss is an open question). McAfee has detected the malware variants and other relevant indicators for years with *Generic Downloader.x* and Generic *BackDoor.t* heuristic signatures (those who have had prior experience with this specific adversary may recognize it by the use of encrypted HTML comments in web pages that serve as a command channel to the infected machine).

McAfee has gained access to one specific Command & Control server used by the intruders. We have collected logs that reveal the full extent of the victim population since mid-2006 when the log collection began. Note that the actual intrusion activity may have begun well before that time but that is the earliest evidence we have for the start of the compromises. The compromises themselves were standard procedure for these types of targeted intrusions: a spear-phishing email containing an exploit is sent to an individual with the right level of access at the company, and the exploit when opened on an unpatched system will trigger a download of the implant malware. That malware will execute and initiate a backdoor communication channel to the Command & Control web server and interpret the instructions encoded in the hidden comments embedded in the webpage code. This will be quickly followed by live intruders jumping on to the infected machine and proceeding to quickly escalate privileges and move laterally within the organization to establish new persistent footholds via additional compromised machines running implant malware, as well as targeting for quick exfiltration the key data they came for.

After painstaking analysis of the logs, even we were surprised by the enormous diversity of the victim organizations and were taken aback by the audacity of the perpetrators. Although we will refrain from explicitly identifying most of the victims, describing only their general industry, we feel that naming names is warranted in certain cases, not with the goal of attracting attention to a specific victim organization, but to reinforce the fact that virtually everyone is falling prey to these intrusions, regardless of whether they are the United Nations, a multinational Fortune 100 company, a small non-profit think-tank, a national Olympic team, or even an unfortunate computer security firm.

McAfee®

In all, we identified 72 compromised parties (many more were present in the logs but without sufficient information to accurately identify them). Of these, the breakdown of 32 unique organization categories follows:

22	6	13	13	4	12

Government		Manufacturing	Defense	Finance	Other

U.S. Federal Government	6	Construction/ Heavy Industry	3	Electronics Industry	3	Defense Contractor	13	Real Estate	2	International Sports	5
U.S. State Government	5	Steel Industry	1	Computer Security	2			Accounting Industry	2	Economics/ Trade	2
U.S. County Government	3	Energy	1	Information Technology	2			Agriculture	1	Think Tanks	2
Canadian Government	2	Solar Power	1	Satellite Communica-tions	2			Insurance	1	International Government/ Economics/ Trade	1
South Korean Government	1			News Media	2					Political Non-profit	1
Vietnam Government	1			Information Services	1					U.S. National Security Non-profit	1
Taiwan Government	1			Communica-tions Technology	1						
U.S. Government Contractor	1										
United Nations	1										
Indian Government	1										

Source: McAfee

McAfee®

And for those who believe these compromises occur only in the United States, Canada and Europe, allow me change that perception with the following statistics on 14 geographic locations of the targets:
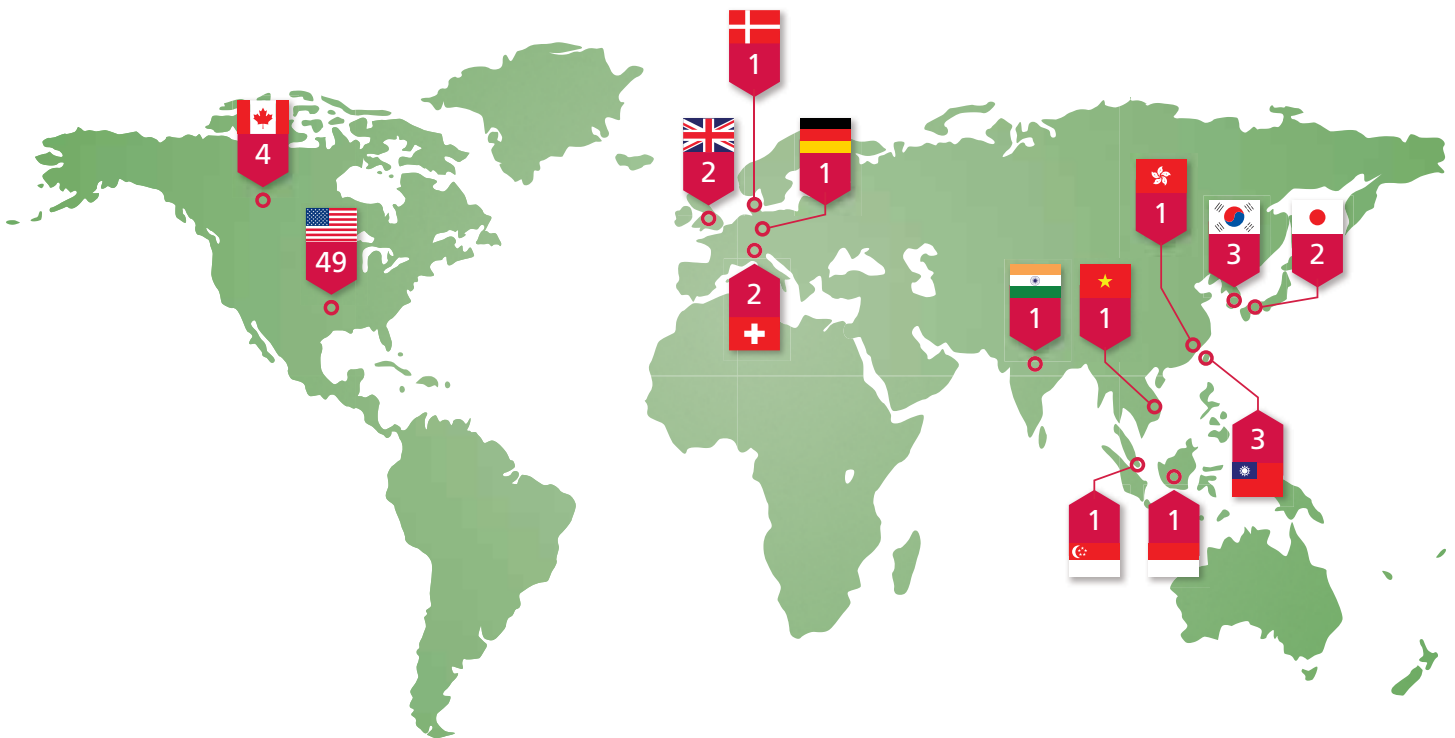
Victim's Country of Origin		Victim Count
USA		49
Canada		4
South Korea		3
Taiwan		3
Japan		2
Switzerland		2
United Kingdom		2

Victim's Country of Origin		Victim Count
Indonesia		1
Vietnam		1
Denmark		1
Singapore		1
Hong Kong		1
Germany		1
India		1

Source: McAfee

The interest in the information held at the Asian and Western national Olympic Committees, as well as the International Olympic Committee (IOC) and the World Anti-Doping Agency in the lead-up and immediate follow-up to the 2008 Olympics was particularly intriguing and potentially pointed a finger at a state actor behind the intrusions, because there is likely no commercial benefit to be earned from such hacks. The presence of political non-profits, such as the a private western organization focused on promotion of democracy around the globe or U.S. national security think tank is also quite illuminating. Hacking the United Nations or the ASEAN (Association of Southeast Asian Nations) Secretariat is also not likely a motivation of a group interested only in economic gains.

Another fascinating aspect that the logs have revealed to us has been the changing tasking orders of the perpetrators as the years have gone by. In 2006, the year that the logs begin, we saw only eight intrusions: two on South Korean steel and construction companies, and one each on a South Korean Government agency, a Department of Energy Research Laboratory, a U.S. real-estate firm, international trade organizations of an Asian and Western nations and the ASEAN Secretariat. (That last intrusion began in October, a month prior to the organization's annual summit in Singapore, and continued for another 10 months.) In 2007, the pace of activity jumped by a whopping 260 percent to a total of 29 victim organizations. That year we began to see new compromises of no fewer than four U.S. defense contractors, Vietnam's government-owned technology company, US federal government agency, several U.S. state and county governments, and one computer network security company. The compromises of the Olympic Committees of two nations in Asia and one Western country began that year as well. In 2008, the count went up further to 36 victims, including the United Nations and the World Anti-Doping Agency, and to 38 in 2009. Then the number of intrusions fell to 17 in 2010 and to 9 in 2011, likely due to the widespread availability of the countermeasures for the specific intrusion indicators used by this specific actor. These measures caused the perpetrator to adapt and increasingly employ a new set of implant families and command & control infrastructure (and causing activity to disappear from the logs we have analyzed). Even news media was not immune to the targeting, with one major U.S. news organization compromised at its New York Headquarters and Hong Kong Bureau for more than 21 months.

The shortest time that an organization remained compromised was less than a single month; nine share that honor: International Olympic Committee (IOC), Vietnam's government-owned technology company, trade organization of a nation in Asia, one Canadian government agency, one US defense contractor, one US general government contractor, one US state and one county government, and a US accounting firm. I must, however, caution that this may not necessarily be an indication of the rapid reaction of information security teams in those organizations, but perhaps merely evidence that the actor was interested only in a quick smash and grab operation that did require a persistent compromise of the victim. The longest compromise was recorded at an Olympic Committee of a nation in Asia; it lasted on and off for 28 months, finally terminating in January 2010.

Below is the complete list of all 72 targets, with country of origin, start date of the initial compromise and duration of the intrusions:

Victim	Country Intrusion	Start Date	Intrusion Duration (Months)
South Korean Construction Company	South Korea	July 2006	17
South Korean Steel Company	South Korea	July 2006	11
Department of Energy Research Laboratory	USA	July 2006	3
Trade Organization	Country in Asia	July 2006	1
South Korean Government Agency	South Korea	August 2006	27
U.S. International Trade Organization	USA	September 2006	12
ASEAN (Association of Southeast Asian Nations) Secretariat	Indonesia	October 2006	10
U.S. Real-Estate Firm #1	USA	November 2006	8
Vietnam's Government-owned Technology Company	Vietnam	March 2007	1
U.S. Real-Estate Firm #2	USA	April 2007	17
U.S. Defense Contractor #1	USA	May 2007	21
U.S. Defense Contractor #2	USA	May 2007	20
U.S. Northern California County Government	USA	June 2007	7
U.S. Southern California County Government	USA	June 2007	24
U.S. State Government #1	USA	July 2007	6
U.S. Federal Government Agency #1	USA	July 2007	8
Olympic Committee of Asian Country #1	Country in Asia	July 2007	28
U.S. State Government #2	USA	August 2007	1
U.S. State Government #3	USA	August 2007	25
U.S. Federal Government Agency #2	USA	August 2007	7
Olympic Committee of Western Country	Western Country	August 2007	7
Taiwanese Electronics Company	Taiwan	September 2007	8
U.S. Federal Government Agency #3	USA	September 2007	4
U.S. Federal Government Agency #4	USA	September 2007	8
Western Non-profit Democracy-promoting Organization	Western Country	September 2007	4
Olympic Committee of Asian Country #2	Country in Asia	September 2007	7
International Olympic Committee	Switzerland	November 2007	1
U.S. Defense Contractor #3	USA	November 2007	7
U.S. Network Security Company	USA	December 2007	3

7

| Victim	Country Intrusion	Start Date	Intrusion Duration (Months)
U.S. Defense Contractor #4	USA	December 2007	7
U.S. Accounting Firm	USA	January 2008	1
U.S. Electronics Company	USA	February 2008	13
UK Computer Security Company	United Kingdom	February 2008	6
U.S. National Security Think Tank	USA	February 2008	20
U.S. Defense Contractor #5	USA	February 2008	9
U.S. Defense Contractor #6	USA	February 2008	2
U.S. State Government #4	USA	April 2008	2
Taiwan Government Agency	Taiwan	April 2008	8
U.S. Government Contractor #1	USA	April 2008	1
U.S. Information Technology Company	USA	April 2008	7
U.S. Defense Contractor #7	USA	April 2008	16
U.S. Construction Company #1	USA	May 2008	19
U.S. Information Services Company	USA	May 2008	6
Canadian Information Technology Company	Canada	July 2008	4
U.S. National Security Non-Profit	USA	July 2008	8
Denmark Satellite Communications Company	Denmark	August 2008	6
United Nations	Switzerland	September 2008	20
Singapore Electronics Company	Singapore	November 2008	4
U.K. Defense Contractor	United Kingdom	January 2009	12
U.S. Satellite Communications Company	USA	February 2009	25
U.S. Natural Gas Wholesale Company	USA	March 2009	7
U.S. Nevada County Government	USA	April 2009	1
U.S. State Government #5	USA	April 2009	3
U.S. Agricultural Trade Organization	USA	May 2009	3
U.S. Construction Company #2	USA	May 2009	4
U.S. Communications Technology Company	USA	May 2009	7
U.S. Defense Contractor #8	USA	May 2009	4
U.S. Defense Contractor #9	USA	May 2009	3
U.S. Defense Contractor #10	USA	June 2009	11
U.S. News Organization, Headquarters	USA	August 2009	8
U.S. News Organization, Hong Kong Bureau	Hong Kong	August 2009	21
U.S. Insurance Association	USA	August 2009	3
World Anti-Doping Agency	Canada	August 2009	14

McAfee®

| Victim	Country Intrusion	Start Date	Intrusion Duration (Months)
German Accounting Firm	Germany	September 2009	10
U.S. Solar Power Energy Company	USA	September 2009	4
Canadian Government Agency #1	Canada	October 2009	6
U.S. Government Organization #5	USA	November 2009	2
U.S. Defense Contractor #11	USA	December 2009	2
U.S. Defense Contractor #12	USA	December 2009	1
Canadian Government Agency #2	Canada	January 2010	1
U.S. Think-Tank	USA	April 2010	13
Indian Government Agency	India	September 2010	2

Below are the complete timelines for each year of intrusion activity. It could be an interesting exercise to map some of these specific compromises to various geopolitical events that occurred around these times (The gaps in the timelines for continuous infections at specific victims may not necessarily be an indication of a successful cleanup before a new reinfection, but rather an artifact of our log collection process that did not mark every activity that occurred on the adversary's infrastructure, potentially leading to these gaps in the data)
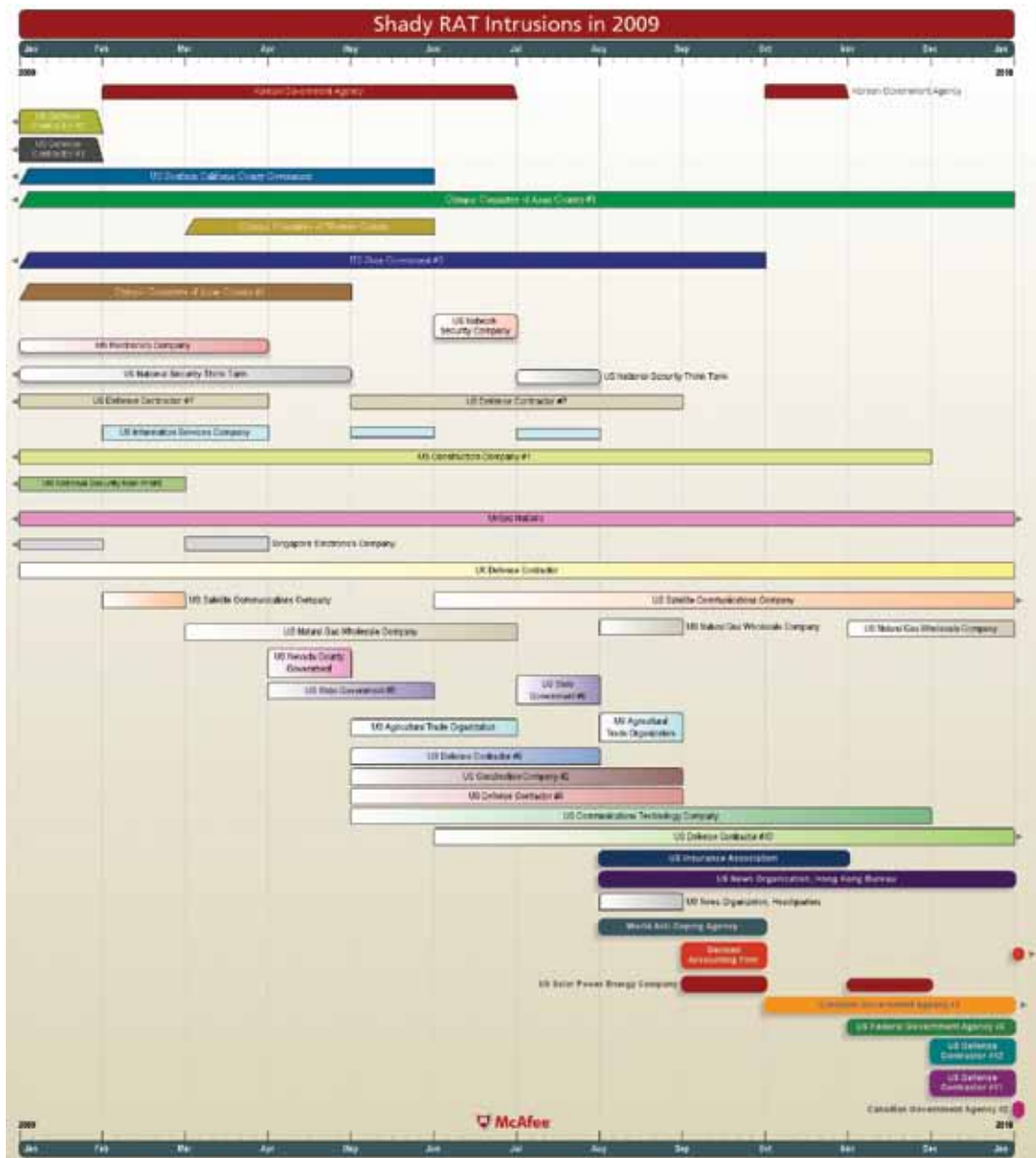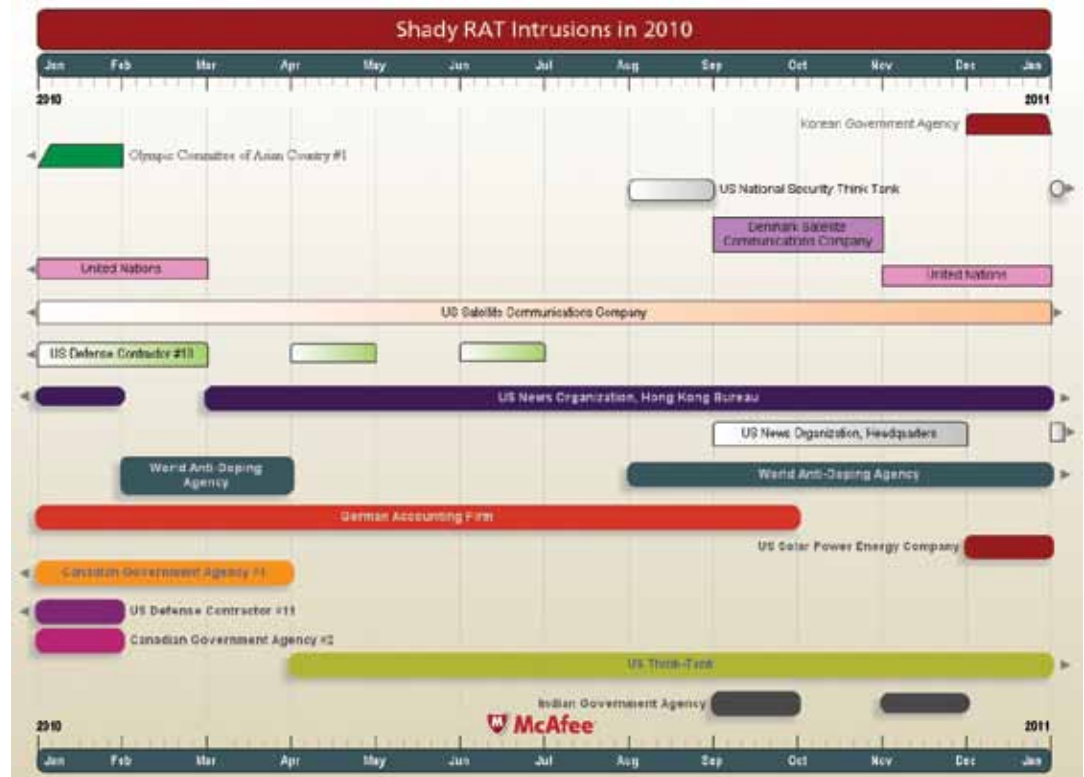

Source: McAfee
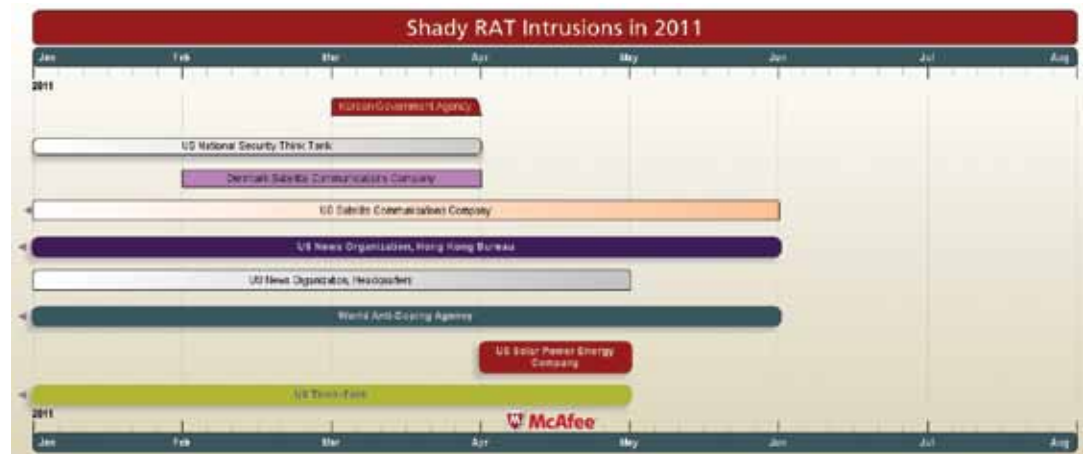
![McAfee]

Source: McAfee

Source: McAfee

Source: McAfee

Source: McAfee

Source: McAfee

13
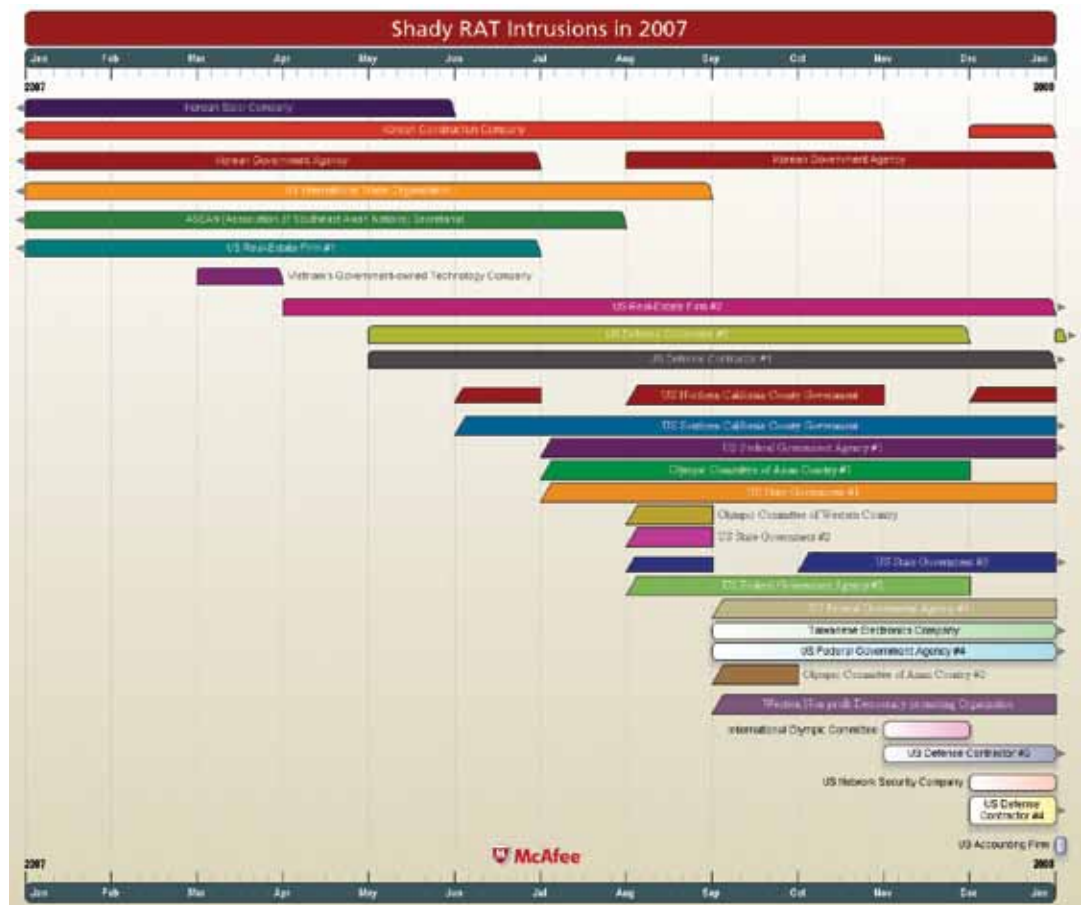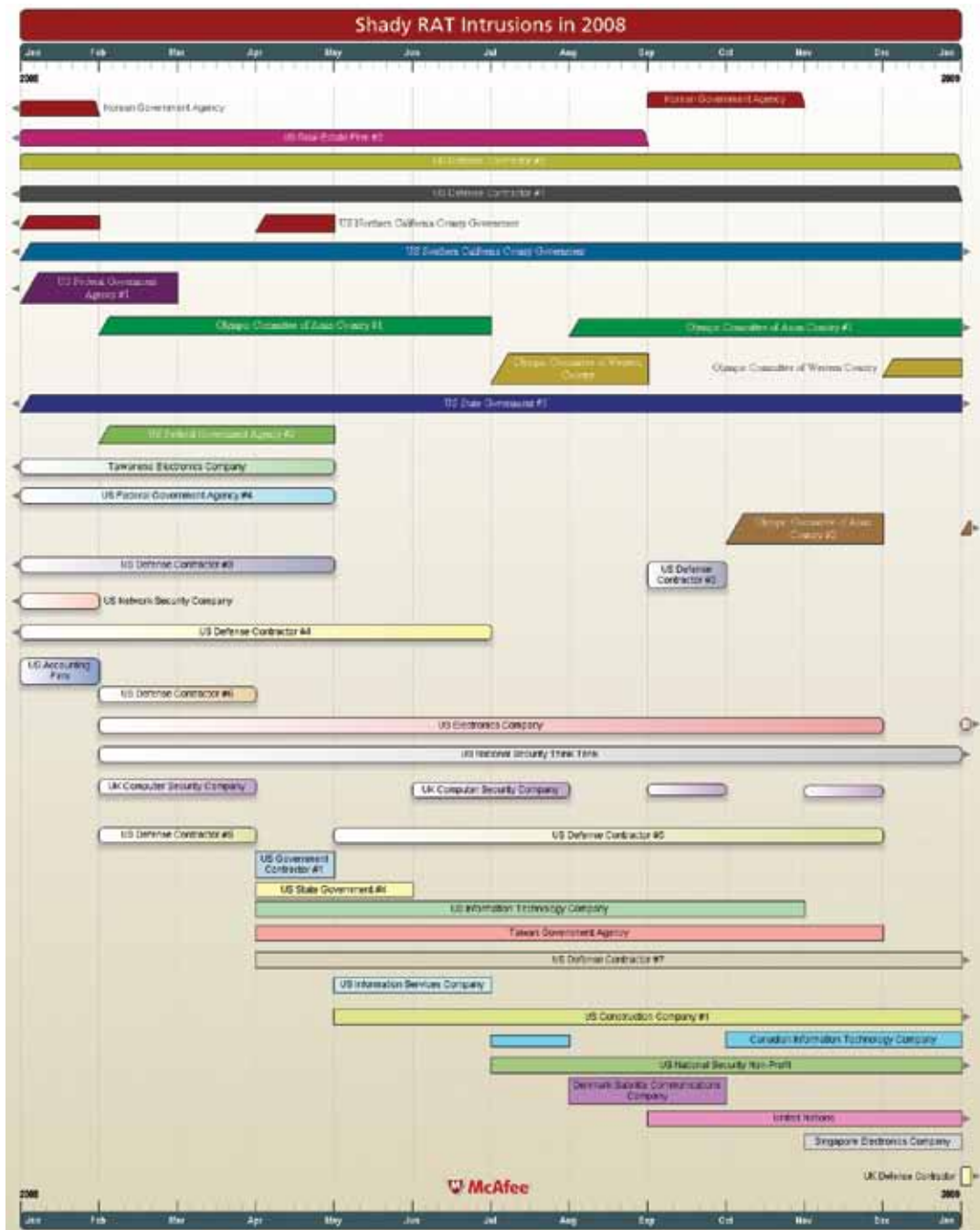
Although Shady RAT's scope and duration may shock those who have not been as intimately involved in the investigations into these targeted espionage operations as we have been, I would like to caution you that what I have described here has been one specific operation conducted by a single actor/group. We know of many other successful targeted intrusions (not counting cybercrime-related ones) that we are called in to investigate almost weekly, which impact other companies and industries. This is a problem of massive scale that affects nearly every industry and sector of the economies of numerous countries, and the only organizations that are exempt from this threat are those that don't have anything valuable or interesting worth stealing.

Dmitri

P.S. I would like to thank Adam Meyers for the invaluable support and assistance he provided to us during this investigation

You can follow Dmitri Alperovitch, McAfee's VP of Threat Research, on Twitter at *http://twitter.com/DmitriCyber*

McAfee®