Project Grey Goose Report on Critical Infrastructure:

Attacks, Actors, and Emerging Threats

January 21, 2010

greylogic

About Project Grey Goose

Project Grey Goose is an Open Source Intelligence (OSINT) initiative launched on August 22, 2008 whose original remit was to examine how the Russian cyber war was conducted against Georgian Web sites and if the Russian government was involved or if it was entirely a grass roots movement by patriotic Russian hackers.

Starting in 2009, Project Grey Goose has evolved into a formal business entity – GreyLogic; a consultancy and information services provider to governments.

This report features GreyLogic's information and analysis services for Computer Network Exploitation and Cyber Intelligence. Western government agencies for Intelligence, Law Enforcement, and Defense are invited to contact GreyLogic for more information on our services.

Executive Summary

Introduction

This Project Grey Goose investigation was launched on October 16, 2009 to answer the question of whether there has been any successful hacker attacks against the power grid, both domestically and internationally.

Today, January 21, 2010, we are able to answer that question. Our Key Findings are particularly relevant now as Smart Grid research and development ramps up and implementation of Smart Grid technology occurs across the globe.

There are many reports in the public domain which discuss vulnerabilities in the power grid. This is not one of them. Instead, this report looks at the broader threat landscape, some (not all) of the key actors involved, and most importantly, how U.S. Energy companies as a self-regulating and predominantly privately owned industry contribute to making the U.S power grid less secure.

Key Findings

State and/or Non-state actors from the Peoples Republic of China, the Russian Federation/Commonwealth of Independent States, and Turkey are almost certainly targeting and penetrating the networks of energy providers and other critical infrastructures in the U.S., Brazil, the Russian Federation, and the European Union.

Network attacks against the bulk power grid will almost certainly escalate steadily in frequency and sophistication over the next 12 months due in part to international emphasis among the G20 nations on Smart Grid research, collaborative development projects and the rich environment that creates for acts of cyber espionage.

The appeal of network intrusions against the U.S. Grid is enhanced by two key factors:

1. 90% of the U.S. Department of Defense's most critical assets are entirely dependent on the bulk power grid.
2. Most Grid asset owners and operators have been historically resistant to report cyber attacks against their networks as well as make the necessary investments to upgrade and secure their networks.

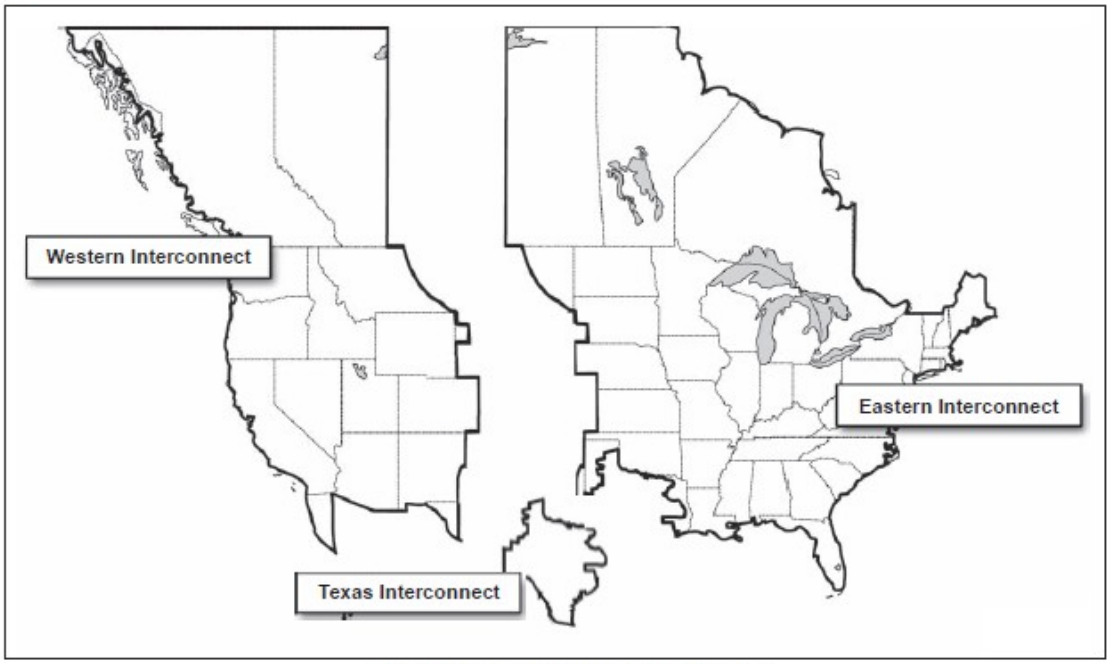
1

General Discussion

FERC, NERC, and the Bulk Power Grid

The U.S. bulk power grid is a system of synchronized power providers and consumers connected by transmission and distribution lines and operated by one or more control centers. The U.S. power grid serving the contiguous 48 states is composed of three distinct power grids, or “interconnections”—the Eastern Interconnection, the Western Interconnection, and the Electric Reliability Council of Texas Interconnection. These interconnections provide power to the continental United States, Canada, and a small portion of northern Mexico.

Figure 1: The U.S. Commercial Electrical Power Grid Interconnects



Sources: GAO-04-204 and North American Electric Reliability Corporation.

The Energy Policy Act 2005 gave the Federal Energy Regulatory Commission (FERC) the power to require the mostly privately owned power industry to designate an Electric Reliability Organization (ERO) which would then develop standards for all of the owner/operators of the bulk power system and submit them to FERC for approval. Once approved, the ERO would enforce them under FERC's oversight. FERC chose the North America Electric Reliability Council (NERC) for the role of ERO who, in 2006, submitted 107 proposed standards for approval. In March, 2007 FERC approved 83 of them grouped into 8 Critical Infrastructure Protection (CIP) standards and after a review and commenting period, issued a final set of CIPs on January 17, 2008 with a three year implementation period. The eight CIP reliability standards address the following topics:

- Critical Cyber Asset Identification;
- Security Management Controls;
- Personnel and Training;
- Electronic Security Perimeters;
- Physical Security of Critical Cyber Assets;
- Systems Security Management;
- Incident Reporting and Response Planning; and
- Recovery Plans for Critical Cyber Assets.

As of this writing, power industry compliance remains voluntary, historically driven by what NERC and its members have termed "reasonable business judgment", which NERC has defined as giving "responsible entities a significant degree of flexibility in implementing these standards". A NERC FAQ document provided a further explanation of the concept:

Courts generally hold that the phrase indicates reviewing tribunals should not substitute their own judgment for that of the entity under review other than in extreme circumstances. A common formulation indicates the business judgment of an entity — even if incorrect in hindsight —should not be overturned as long as it was made (1) in good faith (not an abuse or indiscretion), (2) without improper favor or bias, (3) using reasonably complete (if imperfect) information as available at the time of the decision, (4) based on a rational belief that the decision is in the entity's business interest. This principle, however, does not protect an entity from simply failing to make a decision.

Although this terminology did not survive the commenting period for the new CIP standards and references to it in the CIPs should have been removed by now, it reflects a legacy mindset commonly found in the power industry of prioritizing profitability over security.

Another example of that business-first attitude was the concept of "Acceptance of risk", which gave NERC members the right to simply opt out of certain reliability standards by assuming the responsibility of what may happen as a result. FERC rejected this proposal as well:

> 84. *Further, there is no requirement that a responsible entity communicate to a responsible authority information related to the potential vulnerabilities created by a decision to accept risk and how they could affect Bulk-Power System reliability. The resulting uncertainty concerning who had invoked "acceptance of risk" and in what connection would mean that neither the ERO, Regional Entities nor others would know whether adequate cyber security precautions are in place to protect critical assets. The possibility that*

appropriate security measures for critical assets have not been implemented due to acceptance of risk and that no corresponding compensating or mitigating steps have been taken presents an undue and unacceptable risk to Bulk-Power System reliability.

85. *Moreover, the Commission believes the acceptance of risk language does not serve any justifiable purpose. To the extent that an entity would invoke this exception because compliance is not technically feasible, it should rely on that exception, which with the Commission's proposal would have specific safeguards and limitations. To the extent that a responsible entity would invoke the acceptance of risk language because its business preference is not to expend resources on cyber vulnerability, we believe that is inappropriate for all the reasons discussed previously. A responsible entity should not be able to jeopardize critical assets of others, and create a significant and unknown risk to Bulk-Power System reliability, simply because it is willing to "accept the risk" that its own assets may be compromised.*
86. *Accordingly, the Commission proposes to direct that the ERO remove the "acceptance of risk" language from the CIP Reliability Standards.*

As the implementation period grows shorter, owner/operators and their vendors are struggling to make sense of CIP regulations which are more like guidelines, and voluminous NIST guidance that defies any kind of logical order:

- The NIST Risk Management Framework runs over 1200 pages.
- 15 Federal Information Processing Standard publications
- 100+ Security Related Special Publications
- 35+ Interagency Reports
- 65+ Security Bulletins

Withholding Hard Attack Data

This background information is a microcosmic view of the power struggle that is ongoing between FERC and NERC. It also depicts a traditional mindset that is prevalent among the commercial companies who comprise the bulk power grid; that if enhanced security interferes with profitability, security loses out. This is due, in part, to the high costs associated with making SCADA systems more secure and the difficulty in making a business case to asset owner/operators which justifies their making the investment. The fact that many attacks go unreported, or are reported with missing or omitted data weakens the business case even further.

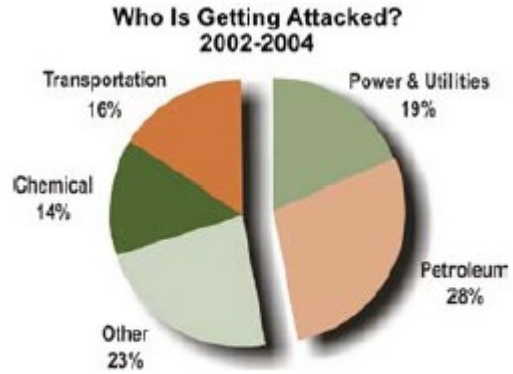


Exhibit 2.4 – Attacks on Industrial Control Systems

Source: Industrial Security Incident Database (Byres 2005)

According to the *Roadmap to Secure Control Systems in the Energy Sector*:

"*The energy sector represents a tempting target for cyber attack. Although many attacks go unreported, energy and power control systems have been the target of a number of attempted attacks in recent years. As shown in Exhibit 2.4, the somewhat limited data collected in the Industrial Security Incident Database suggest that the energy sector is a common target for control system attacks.*"

The problem of limited threat data was repeated that same year (2005) in a report written by Robert J. Turk of Idaho National Laboratories which said:

"Much of the available information about cyber incidents represents a characterization as opposed to an analysis of events. The lack of good analyses reflects an overall weakness in reporting requirements as well as the fact that to date there have been very few serious cyber attacks on control systems. Most companies prefer not to share cyber attack incident data because of potential financial repercussions. Uniform reporting requirements will do much to make this information available to Department of Homeland Security (DHS) and others who require it."

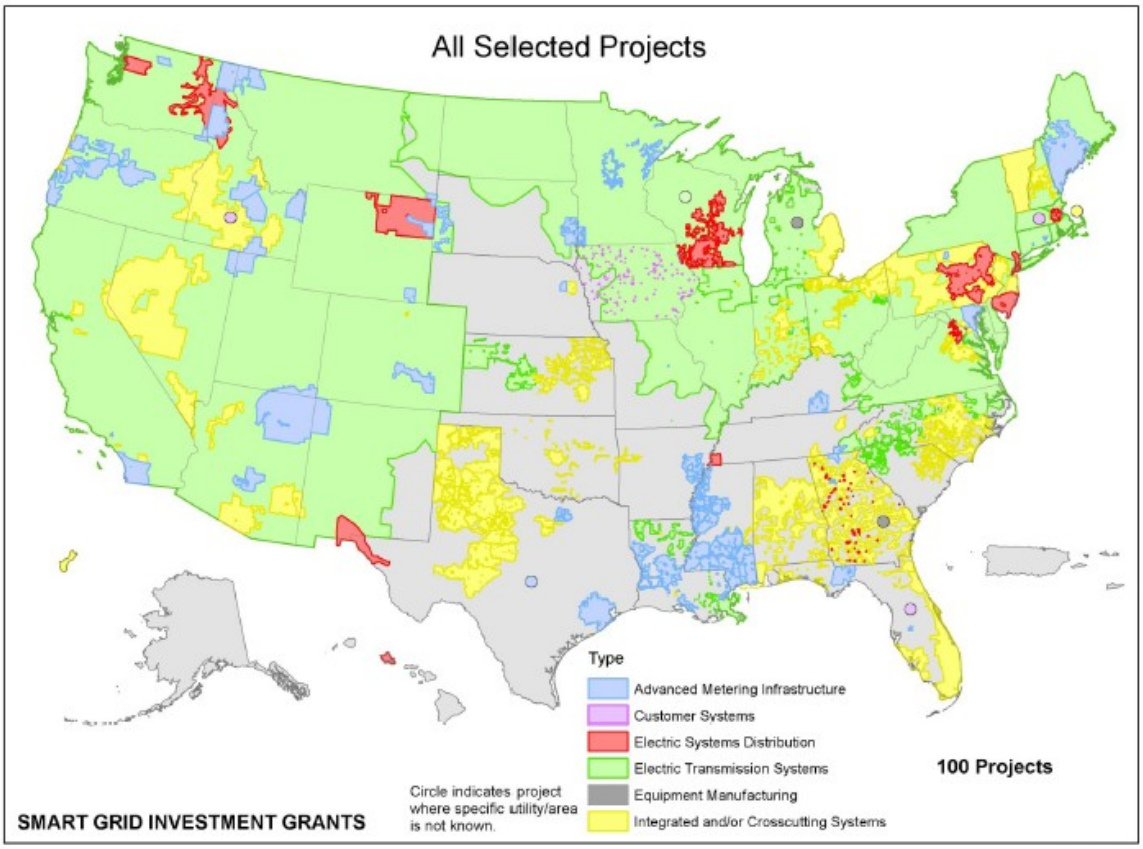
Sandia National Labs has experienced the same problems as Idaho National Labs and, as a result, researchers there have developed a generic threat matrix which utilizes theoretical models instead of hard data as part of the National Scada Test Bed project. In his paper "*Categorizing Threat: Building and Using a Generic Threat Matrix*" (David P. Duggan, et al, SAND2007-5791, Sep 2007), Duggan writes:

"Exacerbating the problem (of building defenses capable of withstanding cyber attacks) for critical infrastructure entities is the fact that the majority of detailed threat information for higher-level threats is held in classified status and is not available for general use, such as the design of defenses and the development of mitigation strategies."

Because of a lack of hard data, researchers at Sandia are forced to base their threat analysis upon certain assumptions which, when closely examined, are either misconstrued or not representative of the current state of Open Source Intelligence gathering for the following reasons:

1. None of Sandia's defining characteristics for assigning a threat rating can be determined nor relied upon from utilizing open sources, as recommended in SAND2007-5792, due to the movement by bad actors away from public forums to private channels for pre-attack planning discussions.
2. Accurate assessment of skill level relies upon at least two findings: (a) a complete forensic breakdown of the attack and (b) obtaining the true identity of the attacker (s); neither of which is being done (for different reasons).
3. Internet security firms rarely have the expertise to assess State resources and intentions; a necessary part of attribution.

Security Weaknesses in the Smart Grid



100 Smart Grid projects distributed across 49 states have been funded by federal grants and industry contributions equaling about $8 billion. The bulk of the funding will go to the purchase of hardware allowing for remote load shifting during peak and non-peak times as well as the wireless communication of data collected from an estimated 18 million smart meters. The positive benefits of investing in Smart Grid technology are laudable; however the rush to implement this technology before serious vulnerabilities are addressed and patched serves to make the Grid more vulnerable to cyber attacks. The following is a brief survey of documented vulnerabilities in Smart Grid technology by three different SCADA security experts.

Making a Secure Smart Grid a Reality [1]

"Most alarming is that "worm-able" code execution on standard smart meters has been achieved. The smart meter's chipset used for radio communication is publicly available in a developer kit format, and the radio interface's lack of authentication can be leveraged to produce a worm. If an attacker installed a malicious program on one meter, the internal firmware could issue commands to flash adjacent meters until all devices within an area were infected with the malicious firmware.

"Once the worm has spread to the meters, the attacker gains several abilities including:

- *Connecting and disconnecting customers at predetermined times.*

- *Changing metering data and calibration constants.*
- *Changing the meter's communication frequency.*
- *Rendering the meter non-functional.*

"If a truly malicious worm were to infect meters in a given area, there would be a best- and a worst-case scenario. Under the best-case scenario, the utility would simply push a firmware update across the standard wireless network to all the affected meters, overwrite the worm, and return the meters to normal operation. This assumes the attacker had not damaged the remote flashing capabilities, changed the frequency on which the meter operates, or changed the calibration of the meter.

"Unfortunately, during malicious attacks the worst-case scenario is more likely to be true. In this case, the normal wireless update mechanisms would no longer be intact, or the calibration of the meters would have been changed. If meters supported remote disconnect capability they could be instructed to simultaneously or individually disconnect service to customers' homes. To return power to affected homes, the utility would need to take time to understand the vulnerability and develop a patch. Then the utility would need to physically repair or replace each meter to return it to normal operation. Restoring power to homes would likely be an expensive and long process, detrimental to the utility and frustrating to the customers."

The Dark Side of the Smart Grid: Smart Meters (in)Security[2]

This white paper by Israeli security company C4, who specialize in performing penetration tests against SCADA systems and military C4I systems, among others, identifies several attack vectors against smart grid technology, one of which is "Lack of Authentication":

"1.3 Lack of Authentication
C4 Security has encountered numerous meters that didn't have any authentication or encryption support. This design flaw makes it possible for an attacker to impersonate the control center and send unauthorized commands to meters or read metering data. The consequence of a successful attack on meters with disconnection capabilities is particularly destructive.
It should be noted that although some of the metering protocols support encryption, which can be viewed as a network access password, most of the deployments we've encountered so far did not enable these features. Since every metering standard includes support for "no encryption" or "no authentication", it usually poses too great a temptation for the integration teams which prefer to choose these settings in order to avoid additional deployment problems."

Low Level Design Vulnerabilities in Wireless Control Systems Hardware (Travis Goodspeed, Darren R. Highfill and Bradley A. Singletary, SR 2009 Papers)[3]

"This paper demonstrates the relevance of common control systems communications hardware vulnerabilities that lead to direct control systems compromise. The paper describes several enabling vulnerabilities exploitable by an attacker, the design principles that causing them to arise, the economic and electronic design constraints that restrict their defense, and ideas for vulnerability avoidance. Topics include design induced vulnerabilities such as the extraction and modification of

communications device firmware, man-in-the-middle attacks between chips of a communications devices, circumvention of protection measures, bus snooping, and other attacks. Specific examples are identified in this report, ranked by attack feasibility. Each attack was investigated against actual IEEE 802.15.4 radio architectures."

Goodspeed was also the principal researcher in discovering a Pseudo Random Number Generator (PRNG) flaw that could allow attackers to bypass the encryption of Texas Instruments's Z-stack software for microcontrollers used in Smart Grid devices. Texas Instruments just announced that it has begun working on a patch[4].

Network attacks against the Bulk Power Grid

Obtaining specific information on hacker attacks against the power grid was the most difficult aspect of this investigation. No one who was in a position to know would reveal any information for this report that was not already publicly known. This included NERC, FERC, the Dept. of Energy, the Dept of Homeland Security, WaterISAC, National Laboratories, SCADA researchers, the RISI database and several SCADA conference organizers. Fortunately, the question of whether or not such attacks have occurred is moot. Idaho National Laboratories issued a 2005 report "Cyber Incidents Involving Control Systems"[5] written by Robert J. Turk that documented 120 cyber security incidents gleaned from the following sources:

- the British Columbia Institute of Technology (BCIT) Industrial Security Incident Database
- the 2003 CSI/FBI Computer Crime and Security Survey
- the KEMA, Inc., Database,
- Lawrence Livermore National Laboratory
- the Energy Incident Database
- the INL Cyber Incident Database
- open-source data

The report did not, however, reveal any specific or identifying information for any of those incidents for the following reasons: (1) INL has non-disclosure agreements in place as do many vendors with the power companies that they service; (2) a formalized incident reporting structure did not exist for network intrusions five years ago, and there is no evidence that it exists today.

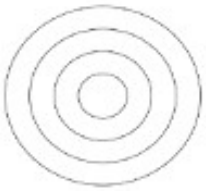
The Internet is an ideal platform for conducting cyber attacks under cover of anonymity (i.e., we don't know who you are) or misdirection (i.e., we think you are someone you're not). A purely technical solution to attribution has yet to be discovered, which compounds the dilemma faced by Nation states when seeking to deter or respond to cyber attacks. In the 16 months since the issuance of the first Project Grey Goose report, GreyLogic analysts have developed a more robust, multi-layered model for determining attribution called PRIM3 (pronounced Prime), whose component parts are Policy, Regional events, Intelligence, Means, Method, and Motive. Since hard data on attacks against the Grid remains unavailable, GreyLogic investigators began to layer investigative approaches to build a body of evidence identifying certain State and Non-State actors with a reasonable degree of certainty. The following data has been developed using one or more of those layers.

State Actors

The Peoples Republic of China

Although the Beijing government clearly prefers a peaceful and profitable relationship with the West, particularly in view of its massive financing of U.S. debt and its reliance on the U.S. economy, its military leadership has adopted a strategy of active defense; meaning that if it deems an attack from a superior adversary to be imminent, it will launch a preemptive strike of sufficient magnitude to either slow or stop its opponent's war plans. An important component of its preemptive strategy is its development of Information Warfare capabilities which can be used to attack the vital points of a network-centric adversary.

Col. Yu's 4 Circle Strategy of Information Warfare



- Ring 1 – Enemy's Command System
- Ring 2 – Command's Theatre Support Network
- Ring 3 – Operational Support
- Ring 4 – Individual Combat Units
- Source: Yu Guohua, "A Study on Modern Offensive Campaigns" (English translation), Beijing, NDU Press, 1999.

The strategic focus of the People's Liberation Army is complemented by civilian research projects funded through the National Natural Science Foundation of China. One such project was a study entitled "Cascade-based Attack Vulnerability on the U.S. Power Grid" by Jian-Wei Wang and Li-Li Rong from the Institute of System Engineering, Dalian University of Technology. Apart from the obvious military applications of this study, further research by GreyLogic investigators revealed that as of 2006, the NSFC took over the dual role of funding both civilian and military research and Dalian University was the frequent recipient of both types of grants.

Wang and Rong referenced an earlier research paper by researchers from the National University of Defense Technology (Changsha, People's Republic of China) - "Vulnerability of complex networks under intentional attack with incomplete information". China's interest in research related to the Power Grid is not surprising considering the many problems that the PRC has had meeting the power needs of its own people, however this research may serve both a civilian and military purpose should Beijing find itself facing an imminent attack from a superior netcentric force such as the U.S. Military.

Because it is currently in Beijing's interest to maintain good relations with the United States and because of its own pressing energy demands, it is unlikely that Chinese hackers would be involved in an attack against the U.S. power grid without extenuating circumstances, however it is not only likely but necessary that Chinese hackers penetrate the grid and test vulnerability points in anticipation of the need for the PLA to execute its preemptive strategy. Opportunities which provide agents of State ministries with access to U.S. Companies, such as foreign R&D labs operating on Chinese soil or collaborative development agreements such as the recent deal signed between Duke Energy and China Huaneng Group, China's biggest electric utility, are potential problem areas that deserve closer attention.

The Russian Federation

Russian Deputy Chief of the General Staff Aleksandr Burutin, in a speech at InfoForum 10 "Wars of the Future will be Information Wars" (February, 2008) spoke about how information warfare is changing the landscape of modern combat: *"According to the opinions of Ministry of Defense experts, presently, military conflicts, as a rule, are generated not by a single factor, but by the complex interaction of various sociopolitical, economic, national, religious and other contradictions and reasons. Therefore, in the foreseeable future, achieving the ultimate goals in wars and confrontations will be brought about not so much by the destruction of enemy groups of troops and forces, but rather by the suppression of his state and military control systems, navigation and communication systems, and also by influencing other crucial information facilities that the stability of controlling the state's economy and Armed Forces depends on."*

The smart grid and securing critical infrastructure are key R&D objectives for the Russian Federation. Of the 8 priorities listed by ISTOK.ru for international collaboration, Grid technologies is number four. The Moscow Institute of Electronic Technology -Technical University (Faculty of Micro-devices and Technical Cybernetics) focuses on critical IT security projects. Russia's Ministry of Science and Education rates MIET as one of Russia's ten best technical and engineering institutions. Strategic research for this institution includes nanotechnology and embedded devices used, for example, in the process control systems (SCADA) for critical infrastructure.[6]

Non-state Actors

Chinese hacker crews

Historically, Chinese hackers attack targets that have acted against PRC interests. A few well-known triggering events for past hacker attacks against U.S. government and commercial websites include the May 7, 1999 accidental bombing of the Chinese embassy in Kosovo and the April 1, 2001 collision between a U.S. EP-3 surveillance aircraft and a PLA J-811 interceptor with the subsequent death of the Chinese pilot.

Following the death of the PLA pilot on April 1, 2001, thousands of Chinese hackers launched attacks against U.S. websites in what the New York Times dubbed "The First World Hacker War". This was particularly focused between May 6 -12, 2001. On May 7, the two year anniversary of the May 7, 1999 bombing of the Chinese embassy, California experienced rolling blackouts for 2 days which affected about 400,000 customers. A subsequent investigation by the California Independent System Operator revealed that hackers had gained access to two Solaris web servers located in CAL ISO's development network and had access from April 25 until May 12. CAL ISO claimed that this breach had nothing to do with the blackout, however a reporter for the L.A. Times who had inside information said it was close to a "catastrophic breach". The attack was traced to Guangdong province, routed through China telecom.

Turkish hacker crews

The 2003 network penetration of the National Science Foundation's Amundsen-Scott South Pole Station science research facility by a Romanian hacker is an event frequently referred to when SCADA-related attacks by hackers are discussed. However, the NSF facility was breached by a Turkish hacker crew named PoizonB0x less than 60 days prior who successfully accessed servers (DASI) controlling the station's radiotelescope.

On December 26, 2006, PoizonB0x hacked the website of Tascomp, a U.K. Company which develops and markets industrial automation software for SCADA systems. It has an extensive customer list including well-known defense contractors BAE and QinetiQ, as well as operators of critical infrastructure facilities like Network Rail, which owns and operates Britain's entire rail infrastructure.

Turkish hackers tend not to attract as much international attention as their Russian and Chinese counterparts, and Turkish police are engaged in investigating and prosecuting them as seen recently with the arrest of Agd_Scorp, a prolific and technically accomplished hacker whose exploits during Operation Cast Lead against DoD and NATO websites were documented in Project Grey Goose's Phase II report. A hacker colleague of Agd_Scorp known as SQL_Master, who is part of a Moroccan hacker crew called Jurm Team, was also active in attacking Israeli websites during Operation Cast Lead. Most recently, SQL_Master defaced an NSA (National Security Agency) web page, with proof of his exploit posted at ZoneH.

Turkish hackers have shown both religious and political motivations which make them difficult to profile as a group. Besides their involvement in supporting Arabic hackers during the 2009 Gaza war, in July 2009 Turkish hackers defaced Chinese government websites after the Turkish government expressed concern over the treatment of the Uighur people in the Xinjiang region of China.

Turkish hacker crews have also targeted a number of Department of Energy Service Provider websites.

HONEYWELL		
07/21/07	Tul2K	www.asia.security.honeywell.com
07/21/07	Tul2K	www.cn.security.honeywell.com
08/31/06	CyberLord	Buildingsforum.honeywell.com
08/07/01	PoizonB0x	Content.honeywell.com
LOGAN ENERGY		
10/23/08	Sanalkurt	Loganergy.com
SEIMENS		
09/17/09	M0sted	www.automation.siemens.com
09/17/09	M0sted	Mall.automation.siemens.com
08/14/07	Tul2k	automation.usa.siemens.com
08/02/07	Tul2K	sea.siemens.com/motosport

In the case of Logan Energy, a fuel cell energy provider for residential, commercial, and industrial systems, it's customers have included the U.S. Army base at Ft. Jackson, the Dept of the Navy's Pacific Missile Range in Kuai, Hawaii, and the FAA's Remote Communications Air/Ground (RCAG) facilities equipment (a critical link in maintaining communications between aircraft and air traffic controllers) at Kaolin Field airport in Sanderson, GA. In each of the above cases, the hackers left a defacement announcing their belief in Islam.

Targeted SQL injection attacks on company websites such as Honeywell, Logan Energy, and Siemens rarely end with a simple defacement. The fact that a defacement has been made signals that the hackers had access to backend data servers containing employee usernames and passwords. Armed with that information, these hackers could implement Phishing schemes against company employees in the hopes of compromising one or more hosts thus gaining deeper access to privileged and sensitive data on Smart Grid or Industrial Control

technology which would certainly be of interest to the Turkish government. Another factor to consider is that Turkish intelligence has been undergoing a restructuring since 2009. Fielding non-state hackers to engage in corporate espionage on technology that supports Turkey's regional aspirations is one sure way to quickly establish credibility for an agency that is struggling to regain its former influence.

Russian hacker crews

Unlike Turkish and Chinese hackers, the following examples are of hacker attacks against Russian critical infrastructure, most likely carried out by disaffected hackers from States formerly part of the Soviet Union, now known as the Commonwealth of Independent States.

In 2000, according to Russia's Interior Ministry Col. Konstantin Machabili, the state-run gas monopoly, Gazprom, was hit by hackers who collaborated with a Gazprom insider. The hackers were said to have used a trojan to gain control of the central switchboard which controls gas flows in pipelines, although Gazprom, the world's largest natural gas producer and the largest supplier to Western Europe refuted the report.

On 23 May 2008, hackers attacked nuclear power websites that provided information on background radiation levels while issuing false rumors of a nuclear accident at the Leningrad Nuclear Power Plant near St. Petersburg according to officials with Rosatom Nuclear Energy State Corporation. "*This was a planned action by hackers which brought down almost all sites providing access to the Automatic Radiation Environment Control System (ASKRO), including the Leningrad NPP site, the Rosatom.ru site, and others. For several hours users were unable to reach the sites and obtain reliable information on the situation at the plant.*"[7]

ASKRO is part of a permanent environment and sanitary control system, one of whose functions is to inform the population on radiation security. Access to the system is open to all visitors on a number of Russian nuclear industry websites. The system works in real-time.

2

Incidents

The following is a list of network attacks (by year) against private and state-owned utilities which provide electricity to the national and international grid. This information has come from publicly available sources and/or through interviews with industry experts who in some cases have requested confidentiality. In a few instances, attacks against water utilities are included since they are also part of critical infrastructure and they use Process Control (SCADA) software.

2009
12 NOV; ONS, Brazil

Operador nacional do Sistema Eletrico (ONS) is Brazil's national system operator responsible for controlling the transmission of electricity as well as the operation of generation facilities throughout the nation. On November 12th, a hacker gained access to its corporate network but stopped short of accessing its operational network.

Source: G1

10 NOV; Itaipu Dam, Brazil: (suspicious incident under investigation)

At 10:13pm local time, the Itaipu Dam which supplies 20% of the electricity for Brazil and all of the electricity for Paraguay suddenly shut down. This occurred 48 hrs after the 60 Minutes episode which said that two earlier Brazilian blackouts (2007 and 2005) resulted from successful hacker attacks, and 24 hrs after the Brazilian government and Brazil's Independent System Operator (Operador Nacional do Sistema) denied that hackers were involved. The ONS placed the blame on bad weather, however according to Instituto Nacional de Pesquisas technicians no electrical charge had hit the power lines at Itaipu dam on that evening. A government investigation is pending.

Source: eBand

01 OCT; Australia: A virus compromised about 1,000 computers at Integral Energy but it impacted business systems only. No outage resulted.

Source: The Sydney Morning Herald, October 1, 2009 "'Sinister' Integral Energy virus outbreak a threat to power grid".

?/2009; U.S.: A cyber attack against a U.S. utility company's process control system resulted in a plant shutdown. The date, location, and name of utility were not disclosed to this investigation.

Source: Confidential

19 APR; U.S.; NRG Texas Power LLC - "On Apr 19 at 23:00 the utilities corporate IT monitoring system identified a high number of failed attempts to log into corporate computers, which emanated from a plant computer at one of the utilities generating stations. This same event was again detected at 00:30 on Apr 20, emanating from a different plant computer at the same generating facility. The computers in question were isolated from the corporate network and virus scans on the computers were performed, which indicated that they had been infected with a virus. The affected computers do not have control authority for power control systems, and as such, could not be utilized to control the units or to trip them off-line, so it is felt that these incidents did could not affect the electric power system. The cyber attack that did NOT affect the adequacy or vulnerability of the electric power system. The investigation is on-going."

Source: NERC January - June 2009 Disturbance Index, p. 49

2008

23 May 2008; Russian Federation; Leningrad Nuclear Power Plant
Hackers attacked Nuclear power websites that provided information on background radiation levels while issuing false rumors of a nuclear accident at the Leningrad Nuclear Power Plant near St. Petersburg according to officials with Rosatom Nuclear Energy State Corporation.

Source: RIA Novosti

2007

27 JUL; 7/27/2009 Tennessee Valley Authority (SERC) 5:05 a.m. Chattanooga, Tennessee Failure of Computer Hardware Used for Monitoring N/A N/A 5:47 a.m. July 27

Source: U.S. Energy Information Administration Independent Statistics and Analysis: Major Disturbances and Unusual Occurrences

26-27 SEP; Espirito Santo, Brazil: A two day outage effecting 3,000,000 people was the result of an attack by hackers according to a 60 Minutes episode airing on 06 Nov 09. The show refers to a rare public statement by CIA senior analyst Tom Donahoe at a SANS conference in January, 2008 who did not name the affected country or city. The Brazilian government disputes that claim, conducted its own investigation and issued its findings which placed the blame on sooty insulators.

Source: 06 Nov 09 CBS news / 60 Minutes, "Cyber War: Sabotaging the System"

?/2007; Willows, CA: An intruder installed unauthorized software and damaged the computer used to divert water from the Sacramento River.

Source: McMillan, Robert. IDG News Service. California Canal Management System Hacked. PCWorld. December 1, 2007.

2006

19 AUG; Athens, AL: Unit 3 of the Brown's Ferry nuclear power plant went into a shutdown after two water recirculation pumps failed. An investigation found that the controllers for the pumps locked up due to a flood of computer data traffic on the plant's internal control system network. The GAO found that TVA's Internet-connected corporate network was linked with systems used to control power production, and that security weaknesses pervasive in the corporate side could be used by attackers to manipulate or destroy vital control systems. The agency also warned that computers on TVA's corporate network lacked security software updates and anti-virus protection, and that firewalls and intrusion detection systems on the network were easily bypassed and failed to record suspicious activity.

Source: 05 JUN 08; The Washington Post "Cyber Incident Blamed for Nuclear Power Plant Shutdown"

Source: 05 MAY 08: GAO Report "Information Security: TVA needs to address weaknesses in control systems and networks"

09 OCT; U.S.: A hacker gained control of a computer which controlled critical systems at a Harrisburg, PA water treatment plant through an employee's laptop. A spokesman from WaterISAC said it was the fourth attack on a water system in 4 years. In one of those cases, the hacker left a message: "*I enter in your server like you in Iraq.*"

Source: GAO. 2007. Government Accountability Office. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain (GAO-07-1036). Washington, DC.

2005
?/JAN; Rio de Janerio: In January, a cyber attack knocked out power in three cities north of Rio De Janeiro, affecting tens of thousands of people.
Source: CBS News; ibid

?/2005; St. Louis, MO: The gauges at the Sauk Water Storage Dam read differently than the gauges at the dam's remote monitoring station, causing a catastrophic failure which released one billion gallons of water.

Source: GAO. 2007. Government Accountability Office. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain (GAO-07-1036). Washington, DC.

2003

?/JAN; Ohio: Slammer worm stopped operations at Davis Besse nuclear power plant.
Source: 19 AUG 03; Security Focus "Slammer worm crashed Ohio nuke plant network"

2001

7-8 MAY; CA: Power outages impacted 400,000 California households during May 7 and 8. The California Independent System Operator (CAL ISO) which is responsible for the purchasing and distribution of power had two Solaris web servers hacked and the hackers active in their network from April 25 to May 11.
Source: SANS report "Can Hackers Turn Your Lights Out: Vulnerability of the U.S. Power Grid"

Credits and Acknowledgments

Project Grey Goose

Principal Investigators

Jeffrey Carr, Founder/CEO GreyLogic

Sanjay Goel, Director of Research, NYS Center for Information Forensics and Assurance; Associate Professor, Information Technology Management, School of Business, University at Albany, State University of New York

Researchers

Mike Himley, President/CEO Eagle Intelligence

Andrew Lasko, PMP, Senior Federal Solutions Engineer, Kapow Technologies

Thomas J. Saly

Reviewers

Kristan Wheaton

Acknowledgments

Thank you to all of the individuals who volunteered to assist with this project and who have requested confidentiality. I'd also like to acknowledge the generous ongoing support of Palantir Technologies, Basis Technology, Kapow Technologies, and our latest corporate sponsor Anonymizer, Inc.

1 David Baker “Making a Secure Smart Grid a Reality”, Journal of Energy Security, 20 Oct 2009
2 C4 White Paper “The Dark Side of the Smart Grid”
3 Travis Goodspeed, et al, “Low Level Design Vulnerabilities in Wireless Control System Hardware”, S4 2009 papers
4 “Texas Instruments to patch smart meter crypto blunder” by Dan Goodin, The Register, 14 Jan 2010
5 Robert J. Turk, “Cyber Incidents Involving Control Systems”, Idaho National Laboratories, 2005
6 IntelFusion FLASH Traffic 18 January 2010 profiled MIET as part of its ongoing series on RF institutions engaged in InfoSec research.
7 RIA Novosti, “Russian nuclear power websites attacked amid accident rumors”, 23 May 2008