IBM Security

At risk: the energy and utilities sector infrastructure

From network break-ins to ransomware to seizing control of control systems, attacks against energy and utility companies are on the rise

IBM X-Force® Research

IBM

Click here to start ►

Contents

Executive overview

Governments and energy and utility organizations worldwide are focusing increasingly on cyber security, and with good reason.[1] Attacks on critical infrastructure like fuel, electricity and drinking water supply carry the potential for damage far beyond their purely economic impact. From the notorious shutdown of several Iranian nuclear centrifuges by Stuxnet malware in 2010[2] to the Shamoon malware attacks in November 2016 and January 2017 against Gulf state organizations[3], these urgent reminders make it clear that today the stakes for energy and utility companies are higher than ever. The health and welfare of whole regions or even nations could potentially be at risk.

Definition of terms

Security event: Activity on a system or network detected by a security device or application.

Attack: A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Security incident: An attack or security event that has been reviewed by IBM security analysts and deemed worthy of deeper investigation.

Figure 1. Comparison of organizations monitored by IBM Security in 2016, cross-industry clients versus energy and utilities sector clients. (See sidebar “Definition of terms” for definitions of event, attack and security incident.) Source: IBM Managed Security Services data, January 1 – December 31, 2016.

Contents

The energy and utilities sector is a diverse landscape encompassing organizations involved in mining and quarrying activities, the operation of electric and gas utilities, and activities related to the management of various forms of waste and water supply. Although the sector was not one of the top targeted industries among the client security environments monitored by IBM X-Force in 2016[4], our data shows it being targeted increasingly in 2017, falling just shy of the top five at mid-year.

Other threats common to all industries are also affecting the energy and utilities sector. From the attacks on Ukrainian energy facilities[5] to distributed denial of service (DDoS) attacks on water, heating and ventilation systems in Finland[6] to the ransomware infection that forced a Michigan utilities company to pay $25,000 to regain access to critical accounting and email servers[7], the threats are very real and very disruptive. IBM Managed Security Services data further reveals that attacks targeting industrial control systems (ICS) are rising.

About this report

This IBM X-Force Research report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources, including event data, activity and trends sourced from endpoints managed and monitored by IBM.

Contents

Attackers set their sights on industrial control systems

Incidents in this sector are not often disclosed publicly, but 2016 saw a few more reports than in previous years.[8] In December 2016, “external sources” targeted the Supervisory Control and Data Acquisition (SCADA) systems of a Ukrainian energy provider to cause a power outage in Kiev, the country’s capital city, forcing technicians to restore power by switching to manual overrides. History seemed to be repeating itself; back in December 2015, a Ukrainian power grid was compromised by attackers using the Black Energy malware to harvest employee credentials and remotely log in to the targeted company’s SCADA network. More recently, disruption caused by the NotPetya ransomware went beyond energy companies to affect multiple Ukrainian government agencies, transportation companies and banks.[9]

SCADA is essentially a subset of the industrial control systems (ICS) used to monitor and control industrial processes. A great many ICS configurations, including SCADA systems, distributed control systems (DCS) and programmable logic controllers (PLCs), are operating in the energy and utilities industry. The IBM report "Security attacks on industrial control systems" details the potential susceptibility of these systems to certain attacks and outlines ways organizations can help protect their systems.

In January 2016 the software development platform GitHub released a penetration testing solution containing a brute-force tool that can be used against Modbus, a serial communication protocol. The rise in malicious activity against ICS may be linked to the use of this tool by various unknown actors.

What attack vectors are available to those wanting to compromise ICS systems? A review of the Alerts and Advisories released by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reveals a plethora of vulnerabilities that could have a number of impacts if left unpatched, including an attacker gaining remote access to a vulnerable system.

Contents

Malware targeting ICS is another vector attackers use to infiltrate energy and utilities companies. CrashOveride, also known as Industroyer, is the latest ICS malware to make headlines. This malware is capable of directly controlling switches and circuit breakers, wiping data and causing a denial of service (DoS) to affected devices.[10]

As threats rise and attack tools advance, the numbers are more alarming than ever. IBM X-Force Threat Research reported in December 2016 that attacks targeting industrial control systems (ICS) had increased by more than 110 percent over 2015.[11] At mid-year 2017, attacks are projected to equal or possibly surpass the volume observed in 2016 (see Figure 2).

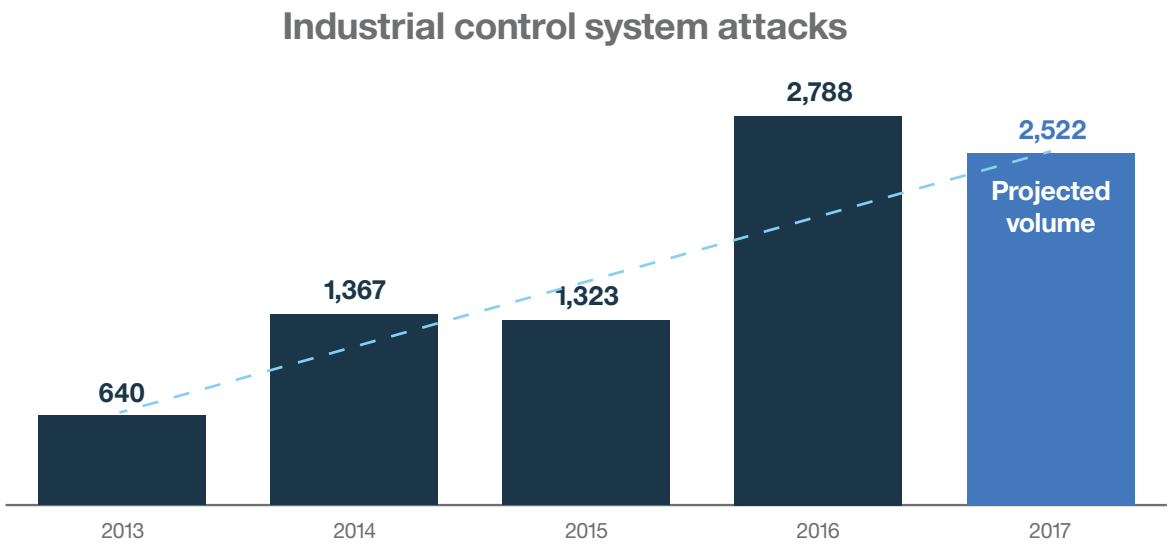

Figure 2. This graphic shows the volume of industrial control system attacks since 2013, with 2017 attacks as of July 15. Source: IBM Managed Security Services data, January 1, 2013 – July 15, 2017.

Contents

Where are the "bad guys"? Insiders versus outsiders

Dealing with multiple attacks year in and year out, security executives and their teams must continually keep tabs on where threats are coming from in order to prioritize their defenses and budgets. One of a security investigation team's first steps is to identify the source and destination IPs as internal or external, then further investigate the associated attack pattern to determine malicious or inadvertent intent.

What are they finding these days? Are most attackers identified as outsiders, or do insiders make up a larger part of the organization's overall attack surface?

In the energy and utilities sector, IBM Managed Security Services 2016 data reveals 60 percent outsiders to 40 percent insiders as the source of unintentional or malicious attacks. Within the insider group there were more inadvertent actors (24 percent) than malicious insiders (16 percent).

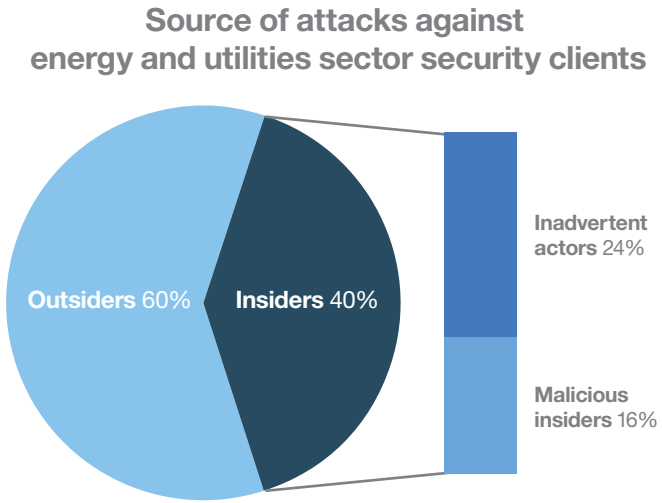

Figure 3. In 2016, outsiders were 20 percent more responsible for energy and utilities sector attacks than insiders. Source: IBM Managed Security Services data, January 1 – December 31, 2016.

Contents

The number of insider attacks in this sector is notable considering that in three of the five sectors most targeted in 2016—information and communication technology, manufacturing and retail—insiders accounted for less than ten percent of the attacks. Malicious insiders could further be involved in business- or state-sponsored espionage. Corporate or state-sponsored attackers, including advanced persistent threat (APT) groups, might for instance be working to obtain SCADA data and power flow models to help locate weak or hard-to-replace parts of the grid, creating the potential for additional, harmful attacks against a particular target.

With more than half of the insider attacks coming from inadvertent actors, the energy and utilities sector must also focus on mitigating this threat. Victims in these attacks often unwittingly open malicious emails and attachments that allow attackers to exploit the targeted systems. In one publicly disclosed incident, thousands of files were stolen over an eight-month period from an infected computer at a Japanese university's nuclear research lab.[12] Reportedly an employee opened a malicious email that caused the system to become infected and remotely accessible. The recent targeting of nuclear facilities in the US also involved spear-phishing, malicious Microsoft Word documents and a watering-hole attack.[13]

Inadvertent actors—often employees who open malicious email attachments or click on malicious links in an email—are responsible for more than half of insider attacks targeting the energy and utilities sector in 2016.

Prevalent methods of attack in monitored energy and utilities clients

To classify and better understand the types of threats affecting the energy and utilities industry, IBM X-Force has grouped 2016 observed attack types according to the standard set by the MITRE Corporation’s Common Attack Pattern Enumeration and Classification (CAPEC™) effort. As MITRE states, their system “organizes attack patterns hierarchically based on mechanisms that are frequently employed in exploiting a vulnerability.”[14] (See Figure 4)

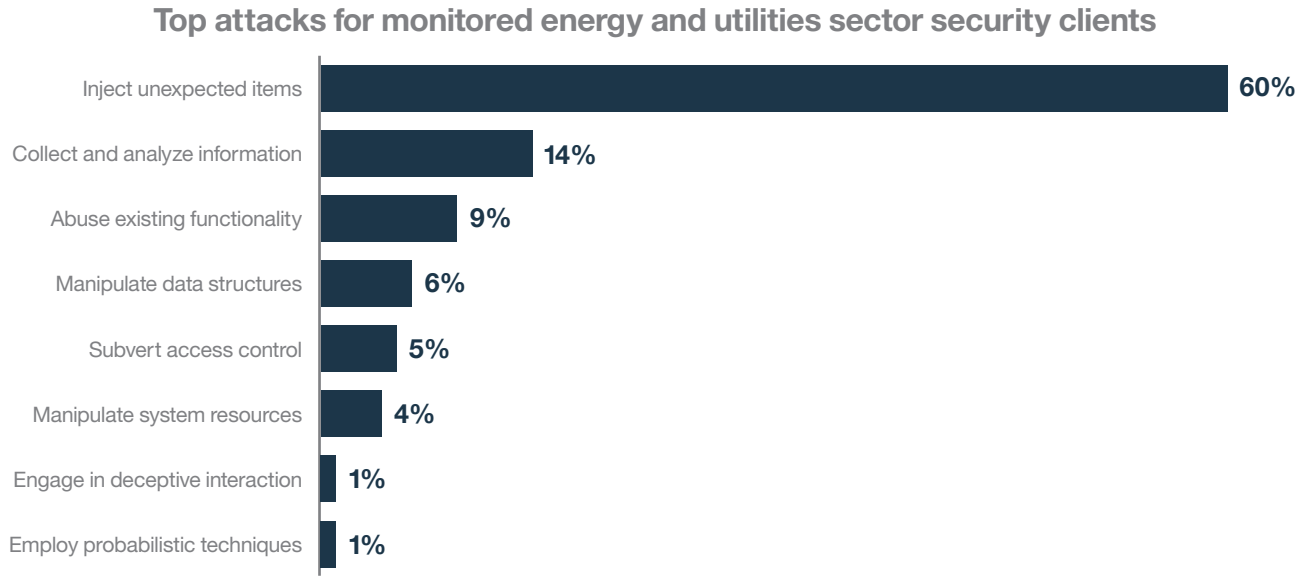

Figure 4. Injection-type incidents made up just over half of the attacks on the energy and utilities sector in 2016. Source: IBM Managed Security Services data, January 1 – December 31, 2016.

Contents

The following sections present further details on each attack type.

Inject unexpected items

According to IBM Managed Security Services analysis of 2016 data, this number one attack vector, involving the use of malicious input data to attempt to control or disrupt a system, targeted 60 percent of the energy and utilities clients monitored by IBM X-Force. That figure was notably higher than the 42 percent average across all industries.

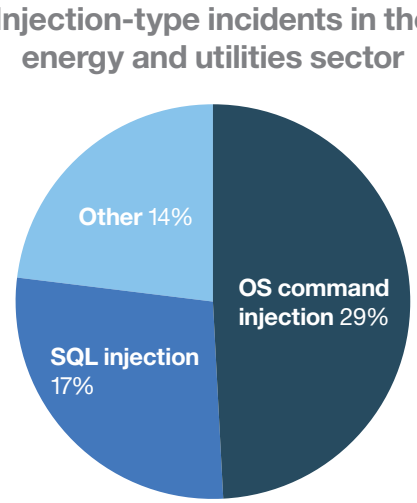

Figure 5. Breakdown of injection-type incidents in the energy and utilities sector in 2016. Source: IBM Managed Security Services data, January 1 – December 31, 2016.

Command injections, which include operating system command injection (OS CMDi) and SQL injections (SQLi), belong in this category. OS CMDi, also known as "shell command injection"—after which the widely prevalent Shellshock vulnerability is named—made up 29 percent. SQLi made up 17 percent of these. Another 14 percent of the attacks involved other types of injection methods.

Collect and analyze information

Attacks focused on the collection and theft of information made up 14 percent of attacks targeting organizational devices in the energy and utilities sector, higher than the cross-industry average of nine percent. Most of these attacks involved fingerprinting, often viewed as reconnaissance to gather information on potential targets and discover their existing weaknesses. Essentially, an attacker compares output from a target system to known "fingerprints" that uniquely identify specific details about the target, such as the type or version of its operating system or an application. Attackers can use the information to identify known vulnerabilities in the target organization's IT infrastructure and better prepare their tactical penetration plans.

The now-infamous Stuxnet used fingerprinting to determine intended targets, checking for the PLC type/family and the System Data Blocks (SDB).[15] In June 2010, this ICS malware targeted an Iranian nuclear facility, causing the shutdown of several nuclear centrifuges. A more recent ICS malware discovery, called Irongate, shares the same fingerprinting capabilities as its predecessor Stuxnet.[16]

Abuse existing functionality

Attempts to abuse or manipulate "one or more functions of an application to deplete a resource to the point that the target's functionality is affected"[17] made up nine percent of the activity, most of it shown by our analysis to involve Communication Channel Manipulation attacks[18] that can result in an attacker bypassing security. Attacks in this category were notably higher than the cross-industry client average of two percent.

Manipulate data structures

This attack vector involves attempts to gain unauthorized access by manipulating system data structures. As CAPEC™ states, "Often, vulnerabilities [such as buffer overflow vulnerabilities], and therefore the exploitability of these data structures, exist due to ambiguity and assumption in their design and prescribed handling."[19] At just six percent, this attack vector is substantially less prevalent in the energy and utilities sector than the cross-industry client average of 32 percent.

Subvert access control

Five percent of activity involved attacks attempting to subvert access controls through the "exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication."[20]

Most of the attacks we observed in this category involved the exploitation of vulnerabilities in the target's client-server communication channel for authentication and data integrity by leveraging the implicit trust a server places in what it believes to be a valid client.

Man-in-the-middle (MITM) attacks, in which attackers attempt to intercept and relay messages between two parties (people or systems), fall under this category. This technique could allow an attacker to steal or become privy to the information going back and forth, or to insert malicious code into the connection.

Contents

Manipulate system resources

Attacks attempting to manipulate some aspect of a system’s resource state or availability accounted for four percent of all attacks. Resources include files, applications, libraries and configuration information. Successful attacks in this category could allow the attacker to be granted access to the company’s network, cause a denial of service, infect a machine to become part of a botnet, or execute arbitrary code on the target.

Engage in deceptive interaction

One percent of attacks attempted to convince a victim to perform an action through spoofing, such as in a clickjacking or user interface redress attack. In this type of attack, the attacker attempts to hijack the victim's click actions and possibly launch further attacks.

Employ probabilistic techniques

One percent of attacks involved an attacker using what CAPEC™ describes as “probabilistic techniques to explore and overcome security properties of the target.”[21] Most of the activity involved brute-force password attacks, a tactic in which an intruder tries to guess a username and password combination to gain unauthorized access to a system or data. Most of the attacks observed by IBM X-Force targeted the Secure Shell (SSH) network protocol. Users favor SSH because it can provide secure remote access. The downside is that it can give attackers shell account access across the network.

Injection-type incidents in the energy and utilities sector, at 60 percent, were notably higher than the 42 percent average across all industries in 2016.

Contents

Recommendations and mitigation

This report outlines a number of risks and attack vectors targeting the energy and utilities industry. A proper assessment of information security risk is critical to the effective direction of your IT investment, critical assets and utilization of resources. We offer the following recommendations for your organization’s security team to consider when making strategic decisions to help safeguard your business.

Mitigate internal threats

IBM X-Force Interactive Security Incidents data reveals that several compromises in the energy and utilities industry over the last few years were caused by inadvertent actors, with phishing and spear-phishing the common denominators. Neglecting to provide cyber security training within an organization could potentially increase employee susceptibility to social engineering attacks and other inadvertent incidents resulting from a lack of policy understanding.

Ensure that employees are fully aware of the organization’s security policies and the threats that make them necessary. Use education and role-based training to foster awareness of the various types of phishing scams, malware delivery tricks and possible in-person impersonators. Employ a variety of approaches—video, webinars, in-person instruction—to educate both management and employees. Consider running simulated phishing attacks to test employees at regular intervals and provide metrics for action plans. Encourage employees to report suspicious emails, phone calls and visitors for further investigation.

Inadvertent security lapses are of course just one side of the internal threat coin. The other is the intentional actor. Malicious insiders who compromise sensitive data are often security-aware and able to act undetected. Their legitimate access to the information makes it difficult to spot a breach: They could interact with that data every day as part of their job, and then one day decide to access it for nefarious ends. Therefore security teams need to take an integrated approach across several technology and business areas to monitor access to critical or sensitive systems and data for timely detection of suspicious activity.

Contents

To further reduce exposure to insider threats, energy and utilities organizations must address both data security and identity and access management to help protect their sensitive data and govern the access of all legitimate users. The more users that have access to sensitive information, the greater the chance that someone will put it at risk—either mistakenly or maliciously. Exercise need-to-know and least-privilege principles and apply role-based access to systems. When employees change job titles within the organization, revoke their access rights accordingly. If they leave the company, completely terminate all their access rights, being sure to include mobile device decommission.

Companies must be certain they are limiting access to only those users who absolutely need it, and that controls stay current as the user population changes and evolves over time. Most importantly, they must always be guided by the critical fact: the more easily accessed their sensitive information is, and the more places it resides, the greater are the chances that an insider, or an outsider with stolen credentials, will access it for the wrong reasons.

Solutions that include an identity manager and account-provisioning component, such as IBM Security Privileged Identity Manager, can help an organization centrally manage and audit the use of privileged IDs across different scenarios. Solutions like IBM Security Guardium® software can help organizations protect sensitive data.

Security incident response plan and team

A comprehensive incident response plan, or IRP, can help you shift your security stance from reactive mode to proactive, potentially saving you a great deal of time and money. According to the "2017 Cost of Data Breach Study: Global Analysis," sponsored by IBM Security and conducted by Ponemon Institute, “an incident response (IR) team reduced the cost by as much as $19 per compromised record.” Your IRP should be a dynamic document reviewed regularly, with changes made wherever they’re needed after an incident.

Contents

Well-documented procedures, vital as they are, can only go so far. Every organization must also have staff capable of carrying out the IRP and calming the chaos of a security incident. Only a team well versed in the response program can deliver the consistency and efficiency needed to streamline responsiveness. Above all, the team must be well trained and must constantly measure the organization’s improvement toward meeting response and remediation objectives.

Outside help may be useful. Engaging the services of a company that manages and runs “capture the flag” exercises, or booking time at a third-party cyber range such as an IBM X-Force Command Center, can provide virtual environments in which to interact with real-world scenarios. Such dynamic training can help organizations understand the threat landscape and their level of exposure, and test the resilience of their cyber response strategy.

Participate in a trusted cyber threat information-sharing network

Very few incidents in the energy and utilities industry are publicly disclosed, so organizations have to learn about attack vectors and the impact of incidents by examining breaches in other industries and then incorporate that knowledge into an effective risk management strategy. Therefore it’s essential to establish an internal team that can digest and act on the lessons of external threat intelligence. Platforms like the IBM X-Force Exchange allow organizations to readily incorporate the results of research into security threats, aggregated intelligence and collaboration with other security teams across the globe.

When an incident is underway there’s no time to waste; fast, effective response to an active attack is vital. Often the ability to provide it depends on having trusted partnerships across the energy and utilities industry. The smaller your organization, the truer this is, so small organizations should seek the assistance of larger companies with more experience and resources. In the US, organizations such as the North American Electric Reliability Corporation (NERC) provide a wealth of intelligence and can be a valuable resource during a cyber incident. Another US-based resource for sector-specific cyber and physical threat intelligence is the Electricity Information Sharing and Analysis Center (E-ISAC).

Contents

Timely communication within your organization on threats and security recommendations goes a long way to protecting networks. For that to happen, your internal cyber security team must have timely intelligence, so we recommend joining an established, collaborative information-sharing organization that collects and disseminates information and alerts about sector-specific threats. We anticipate that advanced tools such as Watson™ for Cyber Security will become essential to an organization’s understanding of threats and decisions about protection and remediation.

Secure your ICS resources

ICS and SCADA systems are high-profile targets and potential gateways for an attacker to penetrate energy and utility company networks. It’s important to define your ICS network infrastructure and ensure that practices such as monitoring all ICS critical applications and infrastructure are in place. Several of these practices are outlined in the IBM report “Security attacks on industrial control systems.” Connecting ICS systems to IT systems such as enterprise resource planning (ERP) systems, for the purposes of key performance indicator (KPI) dashboards, may cause a security exposure if the IT system also has outside connections, such as an electronic purchase order portal.

Another vital part of mitigating risk that’s especially applicable to legacy systems is ICS vulnerability analysis and penetration testing. Regular penetration testing can help you uncover gaps in your network. Penetration testing services such as those performed by the IBM X-Force Red security experts allow organizations to focus on the management of vulnerability data and develop actionable plans to test any target. Additionally, connecting security components such as IBM QRadar® to SCADA-aware business partner products can provide some safeguards to legacy systems.

Vulnerability patching

As in other critical infrastructure sectors, the task of scaling security with the growing demands on the energy and utilities sector’s systems and infrastructure is challenging. The industry’s trend towards privatization, for example, means that the responsibility for identifying critical cyber infrastructure and applying patches falls on each individual owner or operator, so patch management policies can vary widely from one organization to the next.

Contents

The Department of Homeland Security notes that in the US, “more than 80 percent of the country's energy infrastructure is owned by the private sector.”[22] There are almost 200 large investor-owned electric utilities in the US, plus another 2,000 smaller publicly-owned utilities, all with varying levels of internal cyber security but all connected to the same electric grid.[23]

Many attack vectors exploit unpatched vulnerabilities, so timely patch management is vital in organizations of any size. With the analysis you gather from security intelligence and data analytics tools such as the IBM QRadar Advisor with Watson and IBM BigFix® Patch Management solutions, you need to identify the greatest vulnerabilities in your sector and define your organization’s appetite for risk. No matter what that appetite is, we recommend that you always—always!—keep your systems patched and up to date.

Help protect your enterprise

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services offer expertise to help you safeguard your company’s critical assets. We help protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data and safeguard cloud and mobile. Security intelligence Operations and Consulting Services can assess your security posture and maturity against industry best practices in security. With IBM X-Force Incident Response and Intelligence Services, IBM experts proactively hunt and respond to threats, and apply the latest threat intelligence before breaches occur. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that can help you improve your security posture—often at a fraction of the cost of in-house security resources.

Contents

IBM Security

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,500 security patents.

Contributors

Michelle Alvarez - Threat Researcher, IBM Security
Scott Craig - Threat Researcher, IBM Security

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

For more information on security services, visit:
ibm.com/security/services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

Contents

1 https://www.c-span.org/video/?414308-1/discussion-focuses-cybersecurity-energy-sector

2 http://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

3 https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

4 https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-13655&S_PKG=ov57325

5 http://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA

6 http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter

7 http://www.lansingstatejournal.com/story/news/local/2016/11/08/bwl-paid-25000-ransom-after-cyberattack/93488502/

8 https://www.ibm.com/security/xforce/xfisi/

9 https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#3948aee06b89

10 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01

11 https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/

12 http://www.asahi.com/ajw/articles/AJ201610110055.html

13 https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

14 https://capec.mitre.org/data/definitions/1000.html

15 https://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process

16 http://www.digitalbond.com/blog/2016/06/02/why-irongate-is-a-big-ics-security-story/

17 https://capec.mitre.org/data/definitions/210.html

18 https://capec.mitre.org/data/definitions/216.html

19 https://capec.mitre.org/data/definitions/255.html

20 https://capec.mitre.org/data/definitions/225.html

21 https://capec.mitre.org/data/definitions/223.html

22 https://www.dhs.gov/energy-sector

23 http://www.publicpower.org/files/PDFs/USElectricUtilityIndustryStatistics.pdf

Contents

IBM Security

IBM Security
75 Binney Street
Cambridge MA 02142

Produced in the United States of America
September 2017

SEL03135-USEN-01