IBM Security

Know your cyber enemy

Understanding the motives behind cyber attacks

IBM X-Force® Research
Managed Security Services Report

IBM

Click here to start ▶

Contents

Executive overview

We are often asked what motivates cyber attacks—why attackers do what they do. Sometimes it's obvious: if a breach yields credit and debit card details[1] which are then sold on the Dark Web[2], profit is quite clearly the motive. Then again, what seems obvious might be deceptive. A simple profit motive scenario can be a smokescreen hiding a different, deeper kind of attack. Here we present some broad categories of motivation and offer high-level recommendations for mitigating the major attack vectors used.

Espionage

Usually associated with a nation state or corporate entity, espionage attacks are typically aimed at gathering information from the victim. While some things in espionage remain the same—monitoring of communications, for instance, is still as important as ever—others have changed. Stealing secrets used to be the job of individuals physically penetrating or compromising an asset from within a targeted organization—spies, that is—but today the craft is more electronic than physical. Computers now store the information once kept in a company's ledgers, blueprints and papers, and the locks that need to be picked are online.

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 thousands of endpoints managed and monitored by IBM.

Contents

Typically, espionage attacks are the work of corporate or state-sponsored groups, including advanced persistent threat (APT) groups, but there is already some blurring of motivation. Some professional groups acting as independent contractors perform espionage primarily for profit.

Espionage is a clandestine activity and attackers strive to avoid detection, at least until they achieve their primary objective. These are also among the most persistent of attackers, often continuing to try different attack vectors even after they've been detected.

Attacks motivated by espionage can be defined as having a reconnaissance phase in which the attackers seek the vector most likely to yield access to systems and information. The initial vector may be indirect, for example exploiting a known and trusted third party such as a disgruntled employee with access to the target system.

Once inside the system, attackers usually have to move laterally through an organization's systems and gain sufficient rights to allow them access to the company's data stores or repositories. They locate their primary objective—CAD diagrams for a new aircraft design, for instance—and then exfiltrate the target data and move on to secondary objectives. An example of such an attack is the breach of Sony Pictures Entertainment, for which the attackers had multiple objectives.[3] At this point they could exit the systems and cover their tracks, or try retaining access through a backdoor created for later use. If they succeed either way, the target organization might never know that its defenses have been penetrated.[4]

Espionage may be the end goal of a nation state or a corporation, but it may also be carried out by a contractor whose motive is profit.

Contents

Profit

Direct financial gain is the aim of profit-motivated attacks and the driver behind the most active areas of cybercrime. Profit-driven attackers abound and their methods vary widely. The group(s) behind the infamous Dyre malware gained a very significant income, with targeted organizations losing between USD 500,000 and USD 1.5 million.[5] The Anunak group stole millions through breaching Russian and other banking systems.[6] Retail point-of-sale (PoS) malware breaches[7] have been responsible for the theft of millions of debit and credit card information which is then often offered for sale online[8].

A common profit-driven attack in use today is ransomware, covered in detail by IBM X-Force® Research report *What You Need to Know About Ransomware*.[9] In one disturbing recent ransomware attack, a US-based healthcare institution reportedly paid cybercriminals approximately $17,000 (USD) in Bitcoin for the keys required to decrypt its hijacked drives.[10] That same month, the FBI's Cyber Division published an alert warning of several ransomware incidents in which the initial compromise occurred through a vulnerable JBoss application server program.[11] Rather than infecting a single machine, as in a conventional ransomware incident, that kind of attack allows encryption of data on a number of systems.

Distributed denial of service (DDoS) extortion attacks can also be classed as profit-driven[12], with various groups like the Armada Collective and the now hopefully defunct DDoS for Bitcoin (DD4BC) trying to extort payment from organizations in the form of Bitcoin[13]. Not all extortion attacks are motivated by direct financial gain[14], however, and we treat extortion as a separate category later in this paper.

The many methods in play for profit-driven attackers include theft and resale of credit card information, ransomware and DDoS extortion attacks.

Contents

Politics or social justice

The motivation behind cybercrimes committed by hacktivists like the Anonymous Collective[15] is political or social. Today the Anonymous Collective is a largely disconnected collection of small self-interested groups, but for some time it staged quite large operations in which many members combined to target one entity or another for a social or political reason. However, with an issue that resonates with the wider collective, Anonymous may still be capable of significant attacks.

Political motivation also drives most nation-state actors. Some government organizations active in the field, for example the US Army Cyber Command[16], are recognized publicly, but it's also likely that traditional espionage groups and agencies in many nation states have been transformed into cyber operations[17]. Such attackers, either government employees or contractors hired as needed, are likely to be well managed, well organized and well supported in terms of resources.

Politically motivated attackers seek mainly to acquire secret or sensitive information of one sort or another, but sabotage is another very real objective, especially in times of heightened tensions or military conflict. Nation states may also perpetrate attacks designed to damage another nation's economy.[18]

Many groups outside the government sphere claim political motivation for their attacks, but it might be more accurate to call them ego- or vanity-driven. A political goal may be stated, but often they attack at random, purely to deface a victim's website by displaying their own images. They also incline towards grandiose, demonstrably false claims.[19]

Contents

Patriotic or ideological motives

One class of attacker operates primarily from a perspective of patriotism or ideology, perhaps spurred into action by political and social events or motives such as revenge. There are many documented cases of attacks attributed to politically motivated attackers from countries such as the United States[20], Russia[21], China[22], Ukraine[23], Indonesia[24], India[25], Pakistan[26] and Australia[27]. Such attackers may not be directly politically motivated however; a state political organization may encourage such attackers.[28]

The ideological attackers most easily identified are those acting in support of groups such as ISIS or al Qaida. The story of one particular individual, Junaid Hussain[29], illustrates this type of motivation. His first real public brush with notoriety came when he was using the name "TriCk" and associating with a hacking group called "TeaMp0isoN."[30] Hussain, brought up in Birmingham (UK), was sentenced to a jail term in 2012 for breaking into accounts and posting online information belonging to Tony Blair, the former British Prime Minister. After serving his jail sentence he moved to Syria and became a cyber-attacker and recruiter for ISIS.

Sabotage

Every year articles are published on how the power grid and air traffic control, water or other critical systems are vulnerable to attack by hackers and nation states. Typically attackers in this category seek to damage or disrupt infrastructure and critical systems for various reasons—state-operated cyber groups to reduce an adversary's effectiveness, extortionists for money, malicious actors purely for their own self-gratification.[31]

A current example of cyber sabotage apparently driven by conflict and politically motivated is the campaign of attacks on Ukrainian infrastructure and critical systems.[32] These have been coordinated, synchronized attacks involving malware known as Black Energy.[33]

Stuxnet is perhaps the best-known malware used in an act of sabotage, an attack on Iran's nuclear program widely viewed as being state sponsored.[34] The malware's objective was to destabilize and cause failures in a process while simultaneously reporting that systems were functioning normally. This was a very sophisticated piece of malware. Introduced blind into the target systems through removable media, Stuxnet attempted to avoid detection while carrying out its objectives, replicating itself through systems until the correct ones were located and brought under its control.

Contents

Extortion

While the motivation for most ransomware and DDoS extortion attacks is usually simple—profit—other extortion attacks may seek different rewards. One involves the attacker using an element of the victim's personal information, ideally something embarrassing, to coerce him or her into acting on the attacker's behalf. In such a scenario, the victim may be persuaded to install a VPN client (or use an existing one) and establish a connection to an attacker-controlled system, providing access to the victim's system. These connections can be difficult to detect since they neither involve malware nor produce an unnecessarily large volume of unusual traffic.

Ego or vanity

Attackers motivated by vanity or ego seek fame, or infamy, through cyber attacks. They might try to legitimize their obsession under the banner of a political or social cause, but in reality they just want to see their name up in lights. Although they claim to target specific entities, typically they use vulnerability scanning tools to identify hosts that are easy to attack. In other words, their victims aren't chosen for any particular reason, such as looking like good sources of profit or information; they're just targets of opportunity.[35] Attackers in the ego motivation category want to promote their own name. They make boasts and claims on social media and report any news article that mentions them.[36]

Revenge

The disgruntled ex-employee is one of the most easily identifiable attackers motivated by revenge. This person may still have active credentials to access their target's resources, or has retained corporate documents that may be sold or made public. All scenarios are detrimental to the target.

Another example is the unhappy customer who manages to strike a nerve with other consumers and organizes a negative social media campaign directed at a target. Such campaigns might not qualify as cyber attacks, but in today's world they can severely impact a company's reputation.

The revenge motivation can also be seen in the attacks directed recently at a well-known technology journalist. Those attacks included swatting, where the hacker tricks 911 systems into deploying a SWAT team to an unsuspecting victim's home[37], DDoS, and even drugs sent to his home address in the hope that he would be arrested[38].

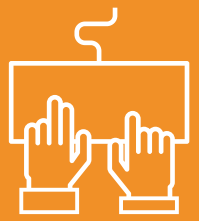
Contents

The outrage trolls

An Internet troll seeks to upset other individuals through attacks on their character or preposterous statements designed to cause outrage. There is also a much darker aspect to such trolls when they begin to make physical threat against individuals or their families.

An attacker in this class may use a DDoS attack to cause outages in online gaming systems, causing annoyance to both the company providing the resources and the people unable to use them. One particular group gained significant notoriety for their DDoS attacks on gaming systems, the most infamous being their attack against the PlayStation and Xbox Live networks on Christmas day, 2014.[39] Consoles and games are popular Christmas gifts, so a lot of people couldn't play their new games, and Sony and Microsoft felt the backlash. It wasn't the first time the group had attacked the two networks, but doing so on Christmas day can certainly be construed as mean-spirited and was definitely designed to cause annoyance.

The group also often taunts their victims, and their efforts to cause annoyance and outrage don't stop there. After seeing a Sony executive's travel details posted online, they allegedly called in a phony bomb threat to his flight[40], causing it to be diverted, landed and searched. In another malicious hoax they defaced a website, leaving imagery and words that made them appear to be acting out of support for ISIS. They also tried to sell access to their own DDoS system, introducing a profit motive. Talk about mixed motivations—here we have outrage, annoyance, ego, vanity and profit too.



Attackers known as Internet trolls seek gratification by attacking the character of individuals or organizations.

Contents

Recommendations

If you understand the motives behind attacks, you can better understand the attack vectors that can be used against you. For example, an organization with sensitive defense data to protect should probably consider themselves at risk from attackers motivated more by espionage than anything else. Some vectors are common across motivations. Arguably the most successful and widely used attacks remain the two simplest, phishing and spear phishing.

What follow are general recommendations only. Every environment is different and each reader should assess these recommendations against their specific environment.

Mail hygiene

An organization's email system can be fortified by physical defensive mechanisms, but defense against phishing by cybercriminal organizations really begins with the user. And there, education is the key. An in-depth look at phishing and a very useful list of recommendations and mitigation techniques can be found in the IBM X-Force Research report *The perils of phishing: How cybercriminals are targeting your weakest link*.[41]

Vulnerability patching and anti-virus

All types of attackers will attempt to exploit systems through known vulnerabilities, and the best defense against these types of attacks is relatively simple: keep your systems patched and up to date. Anti-virus solutions remain highly recommended, but just like operating systems and applications, the solution and its relevant signatures must be kept current.

Security intelligence platform

Use tools, for example the IBM QRadar® Security Intelligence Platform, that combine traditional security information and event management (SIEM) and log management capabilities with network behaviour anomaly detection (NBAD), vulnerability assessment and management, risk analysis and simulation, and forensic data inspection.[42]

Exchange information

Platforms like the IBM X-Force Exchange allow organizations to research security threats, aggregate intelligence and collaborate with peers.[43] Incorporating external threat intelligence into your security operations can enhance your decision making.

Contents

Access management

Users' access should be managed throughout their entire employment, not just after they've left the company. IBM Security Privileged Identity Manager provides a solution for organizations with the above concerns. It includes an identity manager and account provisioning component that helps an organization centrally manage and audit the use of privileged IDs across different scenarios.[44]

Determined attackers constantly find new methods to outwit traditional security systems, using an arsenal of techniques to attack from every angle. Knowing who is behind different types of attacks and what motivates them can help you implement security measures designed to address threats you are most likely to face.

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We 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. Identity and Access Management Services can help you ensure that the right people have the right access to the right information across your organization. Security Intelligence Operations and Consulting Services are designed to help your organization develop more maturity in intelligence-driven operations so you can identify and respond to threats faster. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

Contents

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 and development, 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 3,000 security patents.

About the author

Lyndon Sutherland, Senior Threat and Intelligence Analyst, has been involved in network engineering and security for more than twenty years, fourteen of which have been with IBM. His work with IBM as a researcher and analyst led him to joining the IBM X-Force Threat Analysis Service (XFTAS) in 2008. In addition to XFTAS, he also works with the Managed Security Services Threat Research Group writing and contributing to research papers.

Contributors

Michelle Alvarez - Threat Researcher, Publisher and Editor

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://securityintelligence.com/the-top-5-retail-breaches/

[2] http://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/

[3] https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

[4] https://securityintelligence.com/news/global-security-report-shows-majority-of-companies-do-not-detect-breaches-on-their-own/

[5] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03040USEN&attachment=SEL03040USEN.PDF

[6] http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf

[7] https://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/

[8] https://securityintelligence.com/news/security-experts-tie-target-home-depot-attacks-online-store-selling-stolen-credit-cards/

[9] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEL03042USEN&attachment=SEL03042USEN.PDF

[10] http://www.ibtimes.com/turkish-hackers-claim-credit-hollywood-hospital-ransomware-attack-2327065

[11] http://eweb.cabq.gov/CyberSecurity/Security%20Related%20Documents/FLASH%20MC-000068-MW.pdf

[12] https://securityintelligence.com/ddos-extortion-ransomwares-older-cousin/

[13] https://securityintelligence.com/pay-us-the-money-or-the-website-gets-it-extortion-by-ddos/

[14] https://securityintelligence.com/ransomware-the-enterprises-boogeyman/

[15] https://en.wikipedia.org/wiki/Anonymous_%28group%29

[16] http://www.arcyber.army.mil/

[17] http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025

[18] http://www.theguardian.com/technology/2015/apr/01/obama-targets-foreign-hackers-state-owned-companies-sanctions

[19] https://portal.sec.ibm.com/mss/html/en_US/support_resources/pdf/Fake_iTunes_Compromise_MSS_Threat_Report.pdf

[20] http://www.atlanticcouncil.org/blogs/new-atlanticist/us-should-discourage-patriotic-hackers-from-attacking-north-korea

[21] http://www.foxnews.com/politics/2016/01/16/patriotic-hackers-attacking-on-behalf-mother-russia.html

[22] http://world.time.com/2013/02/21/chinas-red-hackers-the-tale-of-one-patriotic-cyberwarrior/

[23] https://www.asil.org/insights/volume/19/issue/1/cyber-operations-private-actors-ukraine-russia-conflict-cyber-war-cyber

[24] http://jakartaglobe.beritasatu.com/news/hackers-paradise-or-host-nation-indonesian-officials-weigh-cyber-threat/

[25] http://www.newindianexpress.com/states/kerala/Indian-Hackers-Launch-Counter-Attack/2015/09/28/article3051109.ece

[26] http://pkpolitics.com/discuss/topic/pakistani-hackers-take-revenge-take-down-200-indian-sites

[27] http://www.thejakartapost.com/news/2013/11/17/ri-oz-cyber-war-heats.html

[28] http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

[29] https://en.wikipedia.org/wiki/Junaid_Hussain

[30] https://en.wikipedia.org/wiki/TeaMp0isoN

[31] http://www.cnet.com/news/cyber-attacks-rise-at-critical-infrastructure-firms/

[32] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[33] http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/

[34] https://en.wikipedia.org/wiki/Stuxnet

[35] http://krebsonsecurity.com/wp-content/uploads/2013/05/DHSEM-01-SAU-02-UFOUO-HSN-OpUSA-Criminal-Hackers-Planning-Cyber-Attacks-05012013.pdf

[36] http://www.cnet.com/au/news/anonymous-targets-israel-in-another-cyberattack/

[37] https://en.wikipedia.org/wiki/Swatting

[38] http://krebsonsecurity.com/2015/10/hacker-who-sent-me-heroin-faces-charges-in-u-s/

[39] http://www.theguardian.com/technology/2014/dec/26/xbox-live-and-psn-attack-christmas-ruined-for-millions-of-gamers

[40] https://en.wikipedia.org/wiki/Lizard_Squad

[41] https://www.ibm.com/marketing/iwm/iwm/web/signup.do?source=ibm-WW_Security_Services&S_PKG=ov37386&S_TACT=C40501AW&dynform=19254

[42] https://securityintelligence.com/qradars-new-audit-and-security-incident-event-monitoring-for-openstack/

[43] https://exchange.xforce.ibmcloud.com/

[44] http://www-03.ibm.com/software/products/en/pim

Contents

IBM Security

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

IBM

SEL03089-USEN-00