Anticipating and out-maneuvering attackers

Using big data, artificial intelligence and behavior analytics to help prevent, detect and mitigate cyberattacks

Executive summary

Each day brings new examples of cyber-attacks that are more ingenious and harmful than before. Some security experts advise that the proper defense is to patch software, secure the human element, be vigilant and respond quickly. Companies are doing all of the above, and yet the attacks continue and accelerate.

AT&T is deploying advanced analytics across multiple data sources to learn about these attacks and open up new lines of proactive defense. These include advanced artificial intelligence techniques such as machine learning to spot underlying patterns before and after attacks. A few examples of attacks that could be detected:

- Through highly targeted data mining, an attacker gains key facts on a human target who has an important role in asset security. The attacker sends well-crafted, personal messages to trick the human into clicking on a link to a malicious payload. Once the payload is delivered, the adversary can cause harm by encrypting key databases until the business pays a ransom (ransomware).

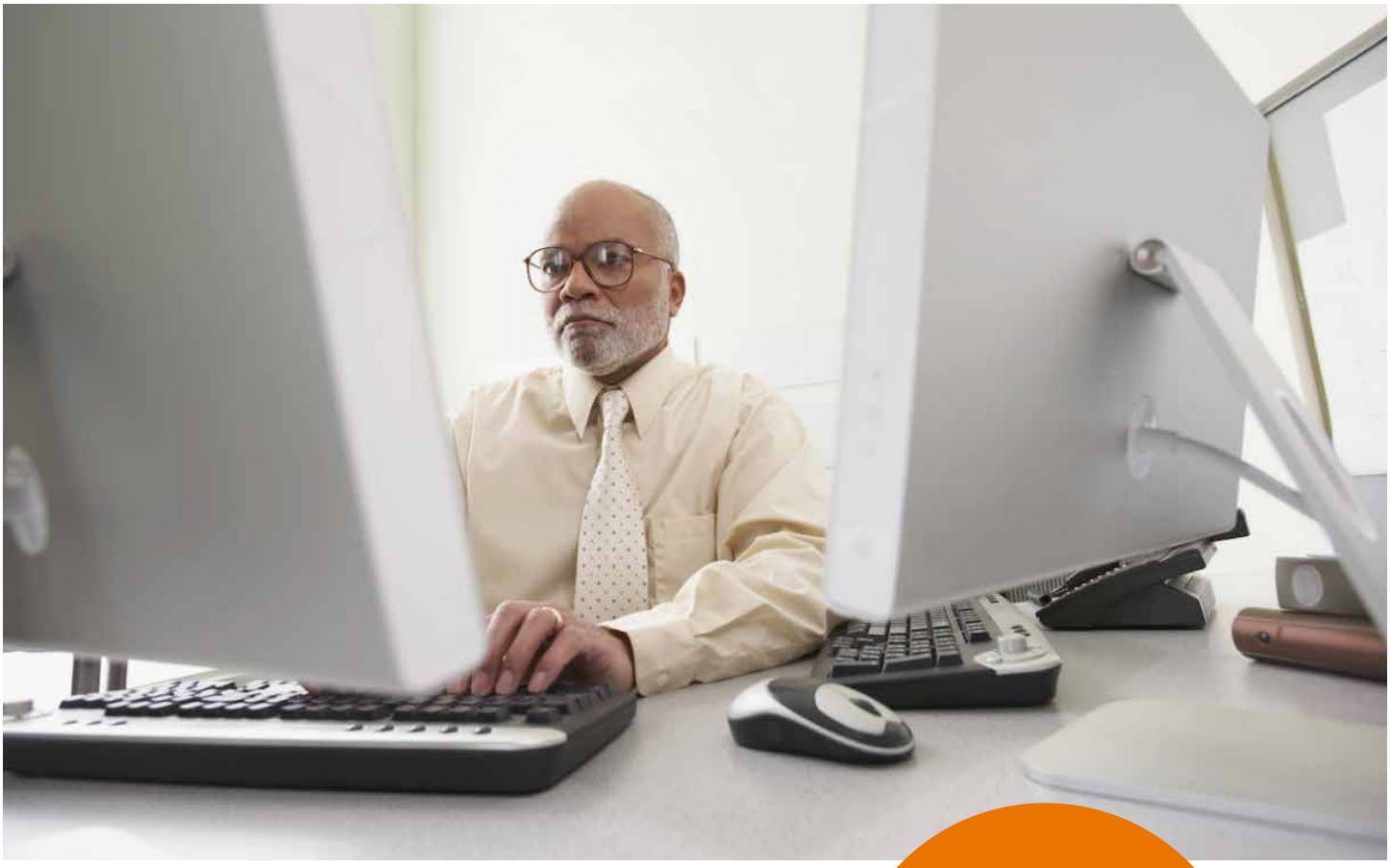
- An attacker breaches a company's defense through a low-priority, poorly protected entry point, whether human or machine. Once past the defenses, the attacker cautiously and discretely probes for additional vulnerabilities. If a vulnerability is found or opens up, or is announced prior to the company patching the system, the inside agent reports the vulnerability for a more active quick-strike exploit by others.

- A human agent accesses databases according to the company operating procedures, but in this case he or she is copying data and transmitting it outside of the company. Advanced threat analytics can spot behavior that is unexpected and not previously anticipated. Is an internal user inserting a USB device significantly more than others? Does he send more or larger email than his peers? Does she switch her computer on and off the VPN frequently? Does she move across records substantially faster than her peers?

In the above cases, the traditional computer protection methods can fail because the attackers are using more information than expected, or they are operating below detection thresholds, or they are quick to take advantage of a weakness before it is fixed.

Communications carriers have the advantage of having massive amounts of information — the large amounts of data that pass through the company network. This is where AT&T can help by joining advanced threat intelligence with data, and to do it in a way that protects individual company information yet allows each customer to take advantage of the latest knowledge. The key is to learn from past attacks, find the behavior patterns between humans and machines that preceded the attack, and then search for patterns in current data. Couple this with the ability to take automated responses, and attacks can be detected, stopped or mitigated prior to actual damage.

Machine learning is one technique that learns from the data and creates a model. By learning from multiple company data sets, AT&T can create a more effective model that does not release any proprietary customer information.



On average, data breaches take more than 200 days to discover.

Introduction

The risks and the threats from cyberattacks continue to increase. Sophisticated cyberattacks are becoming more prevalent, and cyberattacks are becoming easier to launch. However, innovations such as big data analysis, machine learning and user behavioral analytics can help us to anticipate cyberattacks more effectively, protect critical information more assuredly, and utilize our security analysts more efficiently. These tools offer greater flexibility, scalability and convenience for threat management.

Background

The cost and frequency of breaches grow every year. The average data breach in the U.S. now costs the victim organization about $7 million – a figure that has risen every year since 2011 and will likely continue to increase.[1]

Cyberattacks can be costly in other ways. Data breaches often make national news, which then may lead to loss of trust from consumers and harm to the organization's brand. Not only can breaches be damaging to finances and reputation, they can be hard to find. On average, data breaches take more than 200 days to discover.[2]

Emerging and maturing technologies to apply to threat defense	
Big data	Big data refers to the collection and processing of information from traditional, structured data sources such as relational databases, and unstructured data sources like network logs, email and threat intelligence.
Artificial intelligence	Historically, artificial intelligence has been ascribed four facets: acting like a human, thinking like a human, thinking rationally (according to the rules of logic) and acting rationally. Cyber defense can make best use of the rational agent. A rational agent is a computer program that operates autonomously, perceives the environment, persists over a long period of time, adapts to change, and creates and pursues goals to achieve the best outcome – or in the face of uncertainty, the best expected outcome.[3] The term "autonomous agent" describes computer programs that can learn and take action without human intervention.
Machine learning	Machine learning encompasses the math-based techniques that can detect patterns in data without any prior knowledge (unsupervised learning), and extract key characteristics from thousands or millions of characteristics given some external source of attack classification (supervised learning). Rational agent machine learning enhances the agent's ability to make better actions – better in the sense that the goals are reached. Machine learning can also be used to supplement human learning, especially in cases where the actions must be taken by a human, or actions are taken jointly as part of a human-agent partnership.
Natural language processing	Current advances in Natural Language processing rely on the same underlying statistical techniques as machine learning. In the context of cybersecurity, human language is parsed for facts and meaning that can help predict the intent and sentiment behind a human-authored communication. This can help with more advanced threats such as spearfishing, where the attacker uses specific knowledge of the target to lower the recipients guard and increase the chances of a click on the malicious payload. Less sophisticated phishing attacks can be detected by looking for specific phrases or misspellings. Advanced Natural Language processing can sense that an email is wrong because of the misplaced sentiment (e.g., high urgency) or the request for an unusual task (e.g., please transfer $10 million). It can either screen the email automatically if confidence is high that the message is malicious, or present a warning to the user that the email appears to follow patterns linked to other malicious emails.
Behavior analytics	Behavior analytics can spot unusual user interactions with computer systems and suggest that a human is engaging in attack activity. By studying the individual data points of activity, behavior analytics can spot anomalous sequences of interactions or anomalous timing in normal sequences of interaction, whether faster or slower than normal.
Threat intelligence	According to UK's Centre for the Protection of National Infrastructure (CPNI), there are four types of threat intelligence:[4] • Tactical: Attacker methodologies, tools and tactics • Technical: Indicators of specific malware • Operational: Details of a specific incoming attack • Strategic: High-level information on changing risk (strategic shifts) Currently threat intelligence shapes the behavior of humans involved in cybersecurity. In the future, as threat intelligence is treated as semi-structured data itself, autonomous agents can be fed with new threat intelligence to enhance the agent capability.

Emerging and maturing technologies to apply to threat defense (continued)

Threat management	Threat management refers to the whole range of preventive measures that a company or service provider can take to reduce the impact of an attack. Common examples are firewalls, intrusion detection systems, network-edge virus and spam blockers, web content filtering and protocol blocking to prevent data loss. In the future, additional benefit can be gained by controlling these threat-management techniques with a computer program that takes action without human intervention – an autonomous agent. Additionally, logs can serve as valuable input to the learning engine.

Putting it all together

Companies using the available technologies should have more success against cyberattacks than those that do not take such steps. With each new exploit found, with each new technique probed, persistent autonomous agents of protection will increase their ability to detect unusual patterns. Nearly all such responses will be automated. In those cases, where the autonomous agent is not highly confident, security analyst experts will be engaged to dig deeper into the detected anomalies to determine if the attack is real or if the anomaly is benign.

Conclusion

Data should drive businesses. Losing data to a malicious hack or leak can cripple an organization. By employing technological advancements such as big data, machine learning and user behavior analytics, a company can enhance threat management capabilities to get ahead of cyber attackers.

About AT&T Cybersecurity

Learn more about threat management solutions at http://att.com/threat-management . Find out which solution might be most appropriate with security consulting solutions. Learn about the security consulting opportunities that offer expertise at optimizing cybersecurity infrastructure at http://att.com/security-consulting .

Read more about threats, targets and best practices at the AT&T Security Resource Center, where news, advice and security-related topics are updated several times a week. Also, please check out the Cybersecurity Insights reports series available at www.att.com/cybersecurity-insights.

Sources and endnotes

1. *"2016 Cost of Data Breach Study,"* Ponemon Institute LLC, 2016
2. *"Cyberthreat Defense Report 2016,"* CyberEdge Group, 2016
3. *Artificial Intelligence: A Modern Approach*, 3rd Ed. Russell, S. and Peter Norvig. Prentice Hall, 2010.
4. https://www.cpni.gov.uk/Documents/Publications/2015/11-June-2015-Threat%20Intelligence%20-%20Infographic.pdf

To learn more about threat management solutions, visit http://att.com/threat-management or have us contact you.

Share this with your peers