CyberDB

The Cyber Research Databank

Deception Technology

Facts and Emerging Vendors

September 27th, 2016

Contents

1. Introduction to deception technology

Despite well-rounded anti-virus, firewall and various threat intelligence technologies, Attackers can always identify certain system vulnerabilities to slip through the existing security measures, notably by analyzing the human aspect of the targeted institution and launching spear phishing to achieve initial system compromise. The attacker can then move on to implement lateral infection within the victim's network. This attack path, known as the kill chain, can maximize the victim's loss and damages. According to the "Kill Chain" the attacker follows these steps: 1) Reconnaissance, 2) Initial compromise, 3) Establish foothold, 4) Escalate privileges, 5) Internal reconnaissance, 6) Move laterally, 7) Maintain Presence, 8) Repeat escalating privileges, to fulfill the attack objectives. The following diagram retrieved from Mandiant's APT1 cyber-espionage investigation report demonstrates the kill chain structure:

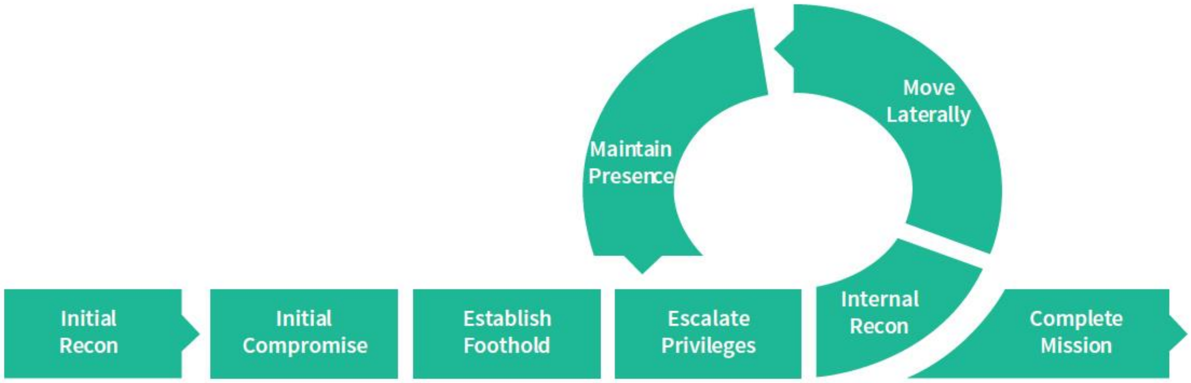

Figure 1: Kill chain structure

As displayed in the diagram, once the attacker is inside the victim's system, it will be difficult to recognize all infected areas and mitigate the intrusion. Hence, the attacker can keep repeating the kill chain cycle until he is satisfied with his gain. High profile data breach news share more or less the same victim story and considerable loss.

Nowadays, most organizations assume compromise, meaning the first few steps of the "Kill Chain" are assumed in progress or complete. Deception technology, therefore, provides a corresponding perspective in coping with cyberattacks. The concept comes from the ubiquitous tactic used in real armed conflicts—decoy. Adopting this decoy strategy has two main objectives. On the one hand, it can gain time for the decoy user to evacuate or diversify the attack intensity. On the other hand, the decoy user can observe from a safe distance his adversaries' attack pattern to come up with the appropriate response. Deception technology turns the defender's passive position into a proactive one. In addition, to setting up defensive tools to guard the institution's real IT assets against the attackers' intrusion, deception technology invites and encourages the attackers to strike their (decoy) targets to the fullest by using advanced luring techniques and decoy assets and services. The illustration below provides a straightforward architecture of deception technology:

A new generation of deception technology, stemming from its older "honeypot" and based on this core concept emphasizes on developing a highly persuasive deception strategy. If the bait is too elementary and obvious, the attacker will be able to avoid the trap. Deception engaging assets are created on virtual machines to resemble as if they are an integral part of the real network. They may contain real operating systems, licensed software and data which can dynamically match the attacker's preference, In other words, effective deception technology mirrors the exact attack destinations and path. Every layer of the deception scheme can be a pseudo legitimate part of a real attack. Using this method, an alternate "reality" is constructed to lure the attacker to deploy his attack tools and methods.

A successful deception mechanism has to support a real attack scenario. The detailed steps illustrated in Cohren's approach aim to mirror the attacker's every decision when he proceeds in his attack. It is therefore a good deception technology model for cybersecurity companies to follow. Once the bait convinced the attacker, deception technology could trap him inside the honeypot server, allowing him to upload malware and exploit data. In practice, the attack and defense flow may follow the pattern in the following diagram:

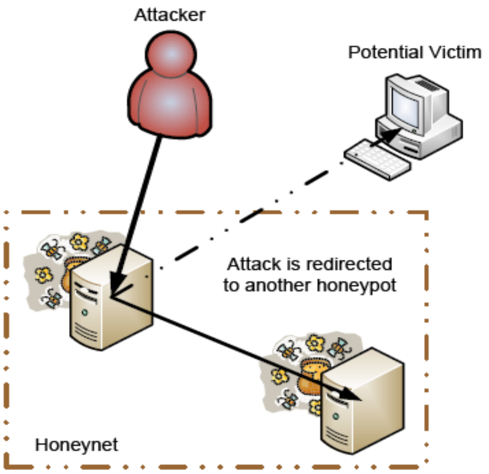

Figure 2: How honeypot/ deception technology diverts attack (Eric Peter and Todd Schiller)

As shown in figure 2, since the potential victim has succeeded in preventing the final parts of the attack, he can observe from a safe distance how the rest of attack is played out. The institution's security officer can seamlessly witness the used malware and targeted data to identify the attacker's technique and interests. Furthermore, as the attack is launched in the deception engaging server (honeynet or honeyfarm), it is segregated from the real operating system. The security officer can destroy it after use or restore a new one to prepare for future attacks.

2. Notable Deception Technology Market Vendors

Company	Country	Deception technology products	Solution summary
TrapX	United States	DeceptionGrid Crytotrap Advanced Incident Response Module Global Threat Intelligence	DeceptionGrid deploys automatically an integrated array of decoys and breadcrumbs that shows ongoing live attacks while preventing the attackers from valuable assets. The defender can understand attackers' tactics over a specific timeline to collect valuable counter intelligence so as to acquire deep insights into the cyber adversaries' technics, tactics and procedures. CryptoTrap deceives, contains and mitigates ransomware at the earliest phase of exploitation cycle, halting attacks while protecting valuable network assets. It generates traps that appear to ransomware as standard SMB network shares. CryptoTrap also allows users to upload their fabricated decoy data. Its endpoint lures are deployed on users systems to divert network-based ransomware attacks to the traps thereby protecting the real files from being encrypted.
Allure Security Technology	United States	Novo Active User Behavioral Analytics software	Novo combines machine learning and decoy technology. It empowers security professionals to protect enterprise devices by taking immediate and efficient actions against insider threats, regardless of targeted attacks, employee error or masqueraders. Novo studies the actual behavioral patterns of individual users, not statistical groups of assumed users, to investigate anomalies. Therefore, strange user behavior plus exfiltrated documents can be an actual intrusion going on. Instead of guessing the unusual activity, Nova provides a well recorded behavior analytics for its users to react rapidly.

Company	Country	Deception technology products	Solution summary
Attivo Networks	India	Threat Matrix Deception Platform	Attivo's solution provides real-time dynamic detection of internal and external threat actors. The purpose is to deceive and lead attackers to infect decoy endpoints, servers/VM in an attempt to reveal their identities. After the attacker is lured into the Attivo deception platform, users can either automatically or manually quarantine and study for further details. Moreover, once the malware is quarantined, the Attivo BOTsink can destroy the attack completely inside the controlled virtual system.
Cymmetria	United States	Mazerunner	MazeRunner follows attentively attacker movement at the earliest stage. It intercepts attackers during the reconnaissance phase. They are led through a carefully planned path toward a monitored engaging server. It also collects valuable information about the attacker's tools and tactics, approach vector, and behavior of the attacker. Each recorded attack move contributes to the user's understanding of his enemy. So, the defender can react with the best information against the attacker.
ForeScout	United States	ForeScout CounterACTForeScout Extended modulesCounterACT Entreprise ManagerControl Fabric architecture	Unique ability to monitor devices, including non-traditional digital devices. The instant they get connected to the network. The ForeScout products execute policy-based control of these devices. Monitored information are shared across different platforms so that the automate workflow linking relevant security and IT management tool will be activated.
GuardiCore	United states/Israel	GuardiCore Centra Security Platform	GuardiCore isolates blocked and filtered connections to keep them running while diverting them to a dynamic and highly interactive honeypot server. GuardiCore’s deception technology adopts real machines, services and IP addresses instead of less effective emulation techniques.

Company	Country	Deception technology products	Solution summary
Hexis Cyber Solutions	United States	HawkEye G HawkEye AP HexisCARE	HawkEye G and HawkEye AP adopt a big-data platform supporting trillions of events, which is 10x more performing than traditional RDBMS, to ingest and analyze information for a great variety of network devices and users, including popular security products such as SourceFire, Palo Alto Networks, Cisco, FireEye, etc. Hexis partners with considerable security technology vendors to enhance detection capabilities so as to provide full spectrum threat remediation. Thanks to this alliance, Hexis can keep updating the latest threat information and countermeasures keeps the system as agile as the threats themselves. HexisCARE provides assurance including professional services, customer support, training and a Hexis Security Operations center as back up service. Users can share threat intelligence across the Hexis user community.
Illusive Networks	Israel	Deceptions Everywhere Attacker View Illusive Advanced Ransomware Guard	Attackers rely on credentials such as users, servers and shares which they can take advantage of progressing lateral movement within the victim's network. Attacker View allows security officers to overview the complete network landscape from the attacker's point of view. Illusive Advanced Ransomware Guard deals with Advanced Ransomware Technologies via full detection and immediate automatic blocking of the suspected Ransomware deployment prior to its going effective and encrypting the real digital assets.
LogRhythm	United States	Unified Security Intelligence Platform Next-Gen SIEM Security Analytics Elasticsearch Network & Endpoint Monitoring and Forensics	Determine intrusion scale and reach relevant compromised data and systems. Then, LogRhythm security platform can generate irrefutable network-based evidence for threat analysis, policy enforcement, and legal action. Besides, it can reconstruct files transferred across networks to investigate suspected data exfiltration, malware infiltration, or unauthorized data access. LogRhythem products support end-to-end threat detection and response workflow as well as file integrity monitoring system. Notably, the Elastic-search-powered forensic analytics uses a combination of contextual and full-text criteria to recognize attackers' vestige.

Company	Country	Deception technology products	Solution summary
Percipient Networks STRONGARM	United States	StrongArm Malware Protection	Strongarm focuses on where attackers' infrastructure are set up. It constantly searches for new attacker infrastructure and adding it to the centralized blacklist. Strongarm does this by gathering open source feeds, developing private intelligence and working with third parties like ThreatConnect and to maintain a thorough database of command and control sites. Moreover, Strongarm communicates with the infected host to start gathering valuable information about the attacker. It determines automatically whether it should uninstall or destroy various types of identified malware. Strongarm can also be configured as Response Policy Zone master.
Rapid7 RAPID7	United States	InsightUBA InsightIDR	InsightIDR first identifies attackers in their initial network infiltration. It automatically separates all the good data of the organization generates from that of an intruder posing as a valid user. InsightUBA allows its user to detect and investigate security incidents faster. It captures intruders using stealthy attack methods, such as stolen credentials and lateral movement.
Shape Security SHAPE	United States	Shape Solution	Shape solution aims at large scale fraud, account takeover, content scraping, and denial of service. It continuously improves defenses against automated attacks through the use of advanced custom feature collection and a unique combination of supervised and unsupervised machine learning.
Topspin Security TOPSPIN SECURITY	Israel	DecoyNet	DecoyNet studies the organizational network and deploys decoys that resemble valuable assets, applications and data. Then, it sets up endpoint and server mini-traps to lure attackers into the shadow server. It aims at exposing their presence, slowing and ultimately defusing their attack.

3. Market Forecast

The cybersecurity market has been expanding rapidly in recent years given all the high profile network breaches. A 2015 global information security survey conducted by PwC, suggested that middle sized corporations with revenues from 100 million USD to one billion USD had spent an average of three million dollars on information security service in 2014. In another study conducted by Marketsandmarkets in the same year suggested that the cybersecurity market size is estimated to grow from 122.45 billion USD in 2016 to 202.36 billion USD by 2021, at a compound annual growth rate (CAGR) of 10.6% in the forecast period. (Marketsand markets, 2016) This strong market growth reflects the urgency that institutions face vis-à-vis their increasingly sophisticated cybersecurity challenges. In this global cybersecurity market, it is further suggested by Technavio that deception technology will likely to generate one billion dollar USD revenue by 2020. The same report suggests that the U.S. will have the biggest market share (an estimate of 42%) in deception technology.

The pioneers in this market such as TrapX have proven initial market success. The company has successfully raised 19 million USD since its establishment in 2010. High profile investor such as Strategic Cyber Ventures LLC, Intel Capital and BRM Group are involved. It is expected that more and more new players will join the development of deception technology given such a high estimated market growth.

4. Conclusion

Deception technology integrates real world military tactics into a new generation of cybersecurity solutions. It enhances the cyber defense landscape and allows real, "while being attacked" intervention capabilities. Instead of taking a passive role, deception technology introduces technical solutions to create engaging assets and services to lure the attackers. A significant number of Cyber security solution pioneers have launched various products to educate the market on this new approach for coping with cyberattacks. The fast development and market adoption suggests a foreseeable future that deception technology will continue to grow and be employed as a common practice in cyber defense.

5. Reference

Biggest online data breaches worldwide 2016 | Statistic, 2016. . Statista. URL http://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/ (accessed 9.13.16).

Capaccio, T., Lerman, D., Strohm, C., 2015. Iran Behind Cyber-Attack on Adelson's Sands Corp., Clapper Says. Bloomberg.com.

Cohen, F., 2006. The use of deception techniques: Honeypots and decoys. Handbook of Information Security, 3(1), pp.646-655.

Crandall, C., 2016. The ins and outs of deception for cyber security. Network World. URL http://www.networkworld.com/article/3019760/network-security/the-ins-and-outs-of-deception-for-cyber-security.html (accessed 9.13.16).

Cyber Crime, 2015. . Statista. URL https://www.statista.com/markets/424/topic/1065/cyber-crime/ (accessed 9.13.16).

Cyber Security Market by Solutions & Services - 2021 | MarketsandMarkets, 2016. URL http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html (accessed 9.13.16).

Dragland, Å., 2013. Big Data, for better or worse: 90% of world's data generated over last two years. ScienceDaily. URL https://www.sciencedaily.com/releases/2013/05/130522085217.htm (accessed 8.28.16).

Dornseif, M., Holz, T., Müller, S., 2005. Honeypots and Limitations of Deception.

Kuranda, S., 2015. The Art Of Deception: New Class Of Security Startups Use Decoys To Disrupt A Hacker's Movement. CRN. URL http://www.crn.com/news/security/300077992/the-art-of-deception-new-class-of-security-startups-use-decoys-to-disrupt-a-hackers-movement.htm (accessed 9.13.16).

Montalbano, E., 2015. Gartner: Deception is a Key Emerging Security. URL http://thevarguy.com/network-security-and-data-protection-software-solutions/090115/gartner-deception-key-emerging-security-tech (accessed 9.13.16).

Tiana, 2015. Send attackers on a wild goose chase with deception technologies - National Cyber Security | Hacker News. URL http://nationalcybersecurity.com/send-attackers-on-a-wild-goose-chase-with-deception-technologies/ (accessed 9.13.16).

Techsci Research, 2016. Deception Technology Market to Cross $1.7 Billion by 2021: TechSci Research Report. URL http://www.prnewswire.com/news-releases/deception-technology-market-to-cross-17-billion-by-2021-techsci-research-report-579815411.html (accessed 9.13.16).

vARMOUR, 2016. Beginner's Guide To Cyber Deception Whitepaper. URL https://www.varmour.com/pdf/whitepaper/beginners-guide-to-cyber-deception-whitepaper.pdf (accessed 9.13.16).